ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

Χρήση Ελλειπτικών Καμπυλών για την Πιστοποίηση Ταυτότητας Και την Συμφωνία Κλειδιών στις Έξυπνες Κάρτες Χωρίς Επαφή

Με Μηχανισμό Διαχείρισης της Μνήμης

Διομήδης Δ. Καστάνης

Μεταπτυχιακή Εργασία

Ηράκλειο, Οκτώβριος 2002

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

Χρήση Ελλειπτικών Καμπυλών για την Πιστοποίηση Ταυτότητας Και την Συμφωνία Κλειδιών στις Έξυπνες Κάρτες Χωρίς Επαφή

Με Μηχανισμό Διαχείρισης της Μνήμης

Εργασία που υποβλήθηκε από τον
ΔΙΟΜΗΔΗ Δ. ΚΑΣΤΑΝΗ
ως μερική εκπλήρωση των απαιτήσεων απόκτησης
ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΔΙΠΛΩΜΑΤΟΣ ΕΙΔΙΚΕΥΣΗΣ

Συγγραφέας:

Διομήδης Δ. Καστάνης
Τμήμα Επιστήμης Υπολογιστών
Πανεπιστήμιο Κρήτης

Εξεταστική Επιτροπή:

Απόστολος Τραγανίτης, Αναπληρωτής Καθηγητής
Επόπτης

Ευάγγελος Μαρκάτος, Αναπληρωτής Καθηγητής
Μέλος

Δημήτρης Πλεξουσάκης, Επίκουρος Καθηγητής
Μέλος

Δεκτή:

Πάνος Κωνσταντόπουλος, Καθηγητής
Πρόεδρος Επιτροπής Μεταπτυχιακών Σπουδών

Οκτώβριος 2002

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

Μεταπτυχιακή Εργασία

Χρήση Ελλειπτικών Καμπυλών για την Πιστοποίηση Ταυτότητας Και την Συμφωνία Κλειδιών στις Έξυπνες Κάρτες Χωρίς Επαφή

Με Μηχανισμό Διαχείρισης της Μνήμης

Διομήδης Δ. Καστάνης

Περίληψη

Οι έξυπνες κάρτες χωρίς επαφή, αποτελούν ένα είδος καρτών ιδιαίτερα βολικό στη χρήση τους, που αναμένεται να επεκτείνει τα πεδία εφαρμογής του σε ποικίλους χώρους όπως, αυτός της οικονομίας, του ηλεκτρονικού χρήματος, της δημόσιας συγκοινωνίας και μεταφοράς, της ηλεκτρονικής πιστοποίησης ταυτότητας, της δημόσιας υγείας. Η είσοδός τους στους χώρους αυτούς, αναμένεται να δώσει το έναυσμα της εμφάνισης και της δημιουργίας νέων και ποικίλων υπηρεσιών.

Αυτού του είδους οι κάρτες ωστόσο, εμπεριέχουν περιορισμούς δυνατοτήτων όπως, στο εύρος φάσματος, στην χρησιμοποιούμενη διαθέσιμη μνήμη, αλλά και στην υπολογιστική ισχύ, κάνοντας έτσι δύσκολη την εκτέλεση περίπλοκων διαδικασιών, όπως η επεξεργασία στοιχείων και δεδομένων υπό το πρίσμα της Κρυπτογραφίας βάσει δημόσιου ή ιδιωτικού κλειδιού. Λαμβάνοντας υπόψη, τη σημασία της ασφάλειας των προσωπικών δεδομένων στο χώρο της πληροφορικής, τόσο στο επίπεδο της διαφύλαξης τους, όσο και στο επίπεδο της μεταφοράς και της μετάδοσης τους, καθώς και το ότι η κρυπτογραφία είναι ο παράγοντας που διασφαλίζει την εγκυρότητα και την προστασία των δεδομένων, η περίπτωση των Έξυπνων Καρτών και ειδικότερα των ασφαλών εφαρμογών τους παρουσιάζει εξαιρετικό ενδιαφέρον.

Τη λύση σε αυτά τα ζητήματα, έρχονται να δώσουν οι Ελλειπτικές Καμπύλες και οι μοναδικές τους ιδιότητες, οι οποίες θα λέγαμε ότι ταιριάζουν ιδανικά στις εφαρμογές των Έξυπνων Καρτών, καθώς έχουν τη δυνατότητα να παρέχουν τη μεγαλύτερη δυνατή ασφάλεια ανά δυαδικό ψηφίο, με το μικρότερο δυνατό κόστος, από κάθε άλλο γνωστό σημερινό κρυπτοσύστημα. Οι Ελλειπτικές Καμπύλες επιτρέπουν την μείωση του μεγέθους του κλειδιού, κάτι το οποίο μεταφράζεται σε ανάγκη για λιγότερη μνήμη και υπολογιστική ισχύ, το οποίο με τη σειρά του συνεπάγεται μικρότερο κόστος.

Η εργασία αυτή, εστιάζει κυρίως στην υλοποίηση κρυπτογραφικών υπηρεσιών, αναλύοντας τον τρόπο με τον οποίο οι Ελλειπτικές Καμπύλες και η κατάλληλη εφαρμογή τους μπορεί όχι μόνο να μειώσει το κόστος υλοποίησης και παραγωγής, αλλά επίσης να επιταχύνει την ανάπτυξη και την υλοποίηση εφαρμογών στο τομέα των έξυπνων καρτών και ιδιαίτερα στο τομέα των έξυπνων καρτών χωρίς επαφή.

Επιτυγχάνουμε, την χρησιμοποίηση τεχνικών βέλτιστης εφαρμογής της αριθμητικής των Ελλειπτικών Καμπυλών προκειμένου να αποφύγουμε την χρησιμοποίηση συνεπεξεργαστή, κάτι το οποίο αποτελεί μια επιπλέον σημαντική μείωση του κόστους και της απαιτούμενης ισχύος. Επίσης, προτείνουμε ένα πρωτόκολλο βάσει του οποίου παρέχουμε αμοιβαία πιστοποίηση ταυτότητας μεταξύ δύο συμβαλλόμενων οντοτήτων και ταυτόχρονη δημιουργία δημοσίων και ιδιωτικών κλειδιών, στο πλαίσιο της Κρυπτογραφίας Δημόσιου Κλειδιού, για τη διασφάλιση του καναλιού επικοινωνίας και ανταλλαγής δεδομένων μεταξύ των δύο οντοτήτων.

Τέλος, προτείνουμε ένα τρόπο με την βοήθεια του οποίου θα μπορέσουμε να καταπολεμήσουμε φαινόμενα διακοπής της τροφοδοσίας του ρεύματος, που έχουν προκληθεί τόσο από την κακή τοπολογία της κάρτας ως προς το τερματικό, όσο και από κακόβουλες επιθέσεις ανεπιθύμητων τρίτων, με σκοπό την απόκτηση σημαντικών δεδομένων για την κάρτα.

Επόπτης

Απόστολος Τραγανίτης
Αναπληρωτής Καθηγητής
Τμήμα Επιστήμης Υπολογιστών
Πανεπιστήμιο Κρήτης

UNIVERSITY OF CRETE
COMPUTER SCIENCE DEPARTMENT

MSc. Thesis

Elliptic Curve Usage for the Mutual Authentication And Key Agreement on Contactless SmartCards

With Memory Management Mechanism.

Diomedes Kastanis

Abstract

Contactless SmartCards represent particular type of SmartCards, with a very convenient usage, and it is expected that they will expand their application capabilities in a variety of different fields. The potential intrusion fields, could be Electronic-money, the Public Transportation, the Electronic Authentication, Health Care and more. Their entrance within these fields, will generate new and more improved services.

However, this type of SmartCards are subject to several constraints, such as bandwidth availability, available memory space, and computational effort. This makes more difficult the execution of complicated procedures, such as processing data, under the prism of Public or Private Cryptography Schemes. Having in mind, the importance of the security in the Informatics area, not only data storage security, but also transmission security, together with the fact that Cryptography ensures the integrity and the protection of data, SmartCards, and their secure applications, implies a great interest.

The solution to these matters is given by the usage of Elliptic Curves, which due to their unique capabilities, match perfectly to the constraints posed by Contactless SmartCard's and their applications. Their unique capabilities provide the strongest security per Binary digit, in comparison with other different Cryptosystems already proposed. This ability of the Elliptic Curves offers smaller sized keys, that need less computational effort and memory space usage. These aspects, provide Elliptic Curve Cryptosystems with higher computation speed and less hardware cost.

This project mainly focuses on the implementation of Cryptographic services, by explaining the way that Elliptic Curves, and their proper use, can result in cost reduction and speed increase, in terms of secure application deployment and implementation in the Contactless SmartCard field.

Throughout this project, we implement the use of optimized techniques in Elliptic Arithmetic, to avoid the use of a co-processor, to maintain the cost at a low level . Thus, we ensure the high levels of security, without increasing the cost. We also propose a Mutual Authentication Protocol, between two entities, (i.e a Contactless SmartCard and a Terminal), while at the same time a key agreement is established. The keys, are being published in a way so as to avoid a -man in the middle- attack, without the use of certificates.

We are also securing the communication channel, since every transmitted quantity is being encrypted, using the agreed keys and a random number is c-reated by the terminal for the cause of every transaction.

Finally, we propose a mechanism to manage the SmartCard's non volatile memory, through which, we can account for to the lack of electrical power, invoked, either by the SmartCard's bad topology in the Magnetic Field, or from the interference by an unauthorized person who might want to obtain important information.

Advisor

Apostolos Traganitis
Associate Professor
Department of Computer Science
University of Crete

Περιεχόμενα

1 Γενικά Στοιχεία Εργασίας **1**
1.1 Περίληψη Εργασίας 1
1.2 Δομή της Εργασίας 1

2 Τύποι Καρτών **2**
2.1 Η Ιστορία των Έξυπνων Καρτών 2
2.2 Τύποι καρτών 2
2.2.1 Ανάγλυφες Κάρτες 3
2.2.2 Κάρτες με μαγνητική ταινία 4
2.2.3 Έξυπνες Κάρτες 5
2.2.4 Κάρτες Μνήμης 6
2.2.5 Κάρτες με Μικροεπεξεργαστή 7
2.2.6 Έξυπνες Κάρτες χωρίς Επαφή 8
2.2.7 Οπτικές Κάρτες Μνήμης 9
2.3 Ο κύκλος ζωής μιας Έξυπνης Κάρτας 10
2.4 Λογική Δομή και Έλεγχος Πρόσβασης Έξυπνων Καρτών 11
2.4.1 Λογική Δομή Αρχείων 12

3 Πεπερασμένα Πεδία **14**
3.1 Περιγραφή Πεπερασμένων Πεδίων 14
3.2 Πολυώνυμα σε Πεπερασμένα Πεδία 15
3.3 Το Πεπερασμένο Πεδίο $\mathcal{F}_p$ 15
3.4 Το Πεπερασμένο Πεδίο $\mathcal{F}_{2^m}$ 16
3.4.1 Αναπαράσταση Πολυωνυμικής Βάσης 16
3.4.2 Αναπαράσταση Κανονικής Βάσης 17

4 Ελλειπτικές Καμπύλες σε Πεπερασμένα Πεδία **19**
4.1 Εισαγωγή στις Ελλειπτικές Καμπύλες 19
4.2 Ελλειπτικές Καμπύλες στο $\mathcal{F}_p$ 20
4.3 Ελλειπτικές Καμπύλες στο Πεδίο $\mathcal{F}_{2^m}$ 23
4.4 Περιγραφή Βελτιστοποίησης Αλγορίθμου Υπολογισμού Γραμμικού Πολλαπλασιασμού 24
4.4.1 Αλγόριθμος Πρόσθεσης και Διπλασιασμού σημείου 24
4.4.2 Αναπαράσταση Προσημασμένου Ψηφίου. 25
4.5 Βέλτιστη Μορφή Αλγορίθμου Διπλασιασμού και Πρόσθεσης σημείου . 26
4.6 Ανάλυση βάση της Κατανάλωσης Ρεύματος 27
4.7 Βασικά στοιχεία 28
4.7.1 Τάξη σώματος 28

5 Παράμετροι Χώρου **29**
5.1 Απαιτήσεις Χώρου 29
5.2 Απαιτήσεις Ελλειπτικής Καμπύλης 29
5.2.1 Επισημοποίηση Παραμέτρων Πεδίου 30
5.3 Δημιουργία Ελλειπτικής Καμπύλης με τυχαίο Τρόπο 31
5.3.1 Η Περίπτωση όπου q=p 31
5.3.2 Η Περίπτωση όπου $q = 2^m$ 33
5.4 Δημιουργία Ελλειπτικής Καμπύλης βάσει του Complex Multiplication 35
5.5 Το Πρόβλημα του Διακριτού Λογάριθμου στις Ελλειπτικές Καμπύλες . 36
5.5.1 Εισαγωγή 36
5.5.2 Το πρόβλημα του Διακριτού Λογαρίθμου 37
5.5.3 Γνωστές Επιθέσεις 38
5.5.4 Δημιουργία Ζεύγους Κλειδιών 39
5.5.5 Επισημοποίηση Δημόσιου Κλειδιού 40
5.5.6 Ενσωματωμένη Επισημοποίηση Δημόσιου Κλειδιού 40

6 Στοιχεία Αλγορίθμου **41**
6.1 Γενικοί Κανόνες Ασφάλειας Αλγορίθμου 41
6.2 Κρυπτοσύστημα Menezes - Vanstone 42

7 Αλγόριθμος Συμφωνίας Κλειδιών και Πιστοποίησης Ταυτότητας **44**
7.1 Εισαγωγή στην Κρυπτογραφία 44
7.1.1 Ασύμμετρη και Συμμετρική Κρυπτογραφία 45
7.2 Υποδομή Δημόσιου Κλειδιού 46
7.2.1 Εγκαθίδρυση Κλειδιού 47
7.2.2 Διαχείριση Κλειδιών 48
7.2.3 Διαφοροποίηση Κλειδιών 48
7.2.4 Εκδόσεις Κλειδιών 48
7.3 Πιστοποίηση Ταυτότητας 49
7.3.1 Εισαγωγή στην Πιστοποίηση Ταυτότητας 49
7.3.2 Διαχωρισμός των Χαρακτηριστικών της Πιστοποίηση Ταυτότητας 50
7.4 Περιγραφή Πρωτοκόλλου 51
7.4.1 Γενικά Στοιχεία 51
7.4.2 Υλοποίηση του Πρωτοκόλλου 52
7.4.3 Πλεονεκτήματα - Συμπεράσματα 61
7.4.4 Μετρήσεις - Συγκρίσεις 62
7.4.5 Παρατηρήσεις - Σημειώσεις 65

8 Διαχείριση Στατικής Μνήμης **68**
8.1 Εισαγωγή 68
8.2 Περιγραφή Μηχανισμού Διαχείρισης 69
8.2.1 Γενικός Σκοπός Μηχανισμού 69
8.2.2 Υλοποίηση Μηχανισμού 70
8.3 Περιγραφή Παραδείγματος 75

9 Επίλογος και Συμπεράσματα **86**

10 Βιβλιογραφία **87**

Κατάλογος Σχημάτων

2.1 Η μορφή του ID-1 format 3
2.2 Οι Ανάγλυφες Περιοχές σύμφωνα με το ISO 7811-3 3
2.3 Οι Περιοχές των Μαγνητικών Ταινιών σε Κάρτα του [ID-1 format] . . . 4
2.4 Ταξινόμηση Έξυπνων Καρτών 6
2.5 Το block διάγραμμα μιας κάρτας μνήμης. 6
2.6 Το block διάγραμμα μιας κάρτας με μικροεπεξεργαστή. 8
2.7 Το block διάγραμμα μιας Έξυπνης Κάρτας χωρίς Επαφή. 9
2.8 Μορφή μιας Οπτικής Έξυπνης Κάρτας. 10
2.9 Μορφή του Λογικού συστήματος αρχείων μιας Έξυπνης Κάρτας . . . 12

4.1 Γεωμετρική Αναπαράσταση πρόσθεσης Διαφορετικών σημείων 22
4.2 Γεωμετρική Αναπαράσταση Διπλασιασμού Σημείου 22
4.3 Η μηχανή πεπερασμένων καταστάσεων του SPA αλγορίθμου Πρόσθεσης και Διπλασιασμού Σημείου 28

6.1 Γενική μορφή των κατακερματικών συναρτήσεων 42

7.1 Σχηματική Παράσταση Συμμετρικής Κρυπτογραφίας 45
7.2 Σχηματική Παράσταση Ασύμμετρης Κρυπτογραφίας 46
7.3 Μέθοδος δημιουργίας Διαφοροποιημένου Κλειδιού βάσει του Αριθμού Κάρτας και του Κύριου Κλειδιού 49
7.4 Κατηγοριοποίηση της Πιστοποίηση ταυτότητας στην περιοχή των Έξυπνων Καρτών 50
7.5 Πρώτη Μετάδοση Δεδομένων [Τερματικό → Κάρτα] 53
7.6 Δεύτερη Μετάδοση Δεδομένων [Κάρτα → Τερματικό] 56
7.7 Τρίτη Μετάδοση Δεδομένων [Τερματικό → Κάρτα] 59
7.8 Σχηματική παράσταση βημάτων ολοκλήρωσης του Πρωτοκόλλου. . . . 61
7.9 Η διεπαφή χρήστη του Πρωτοκόλλου 66

8.1 Οργάνωση της διαρκούς, `non Volatile`, μνήμης 72
8.2 Πίνακας σύγκρισης μνημών από την `Fujitsu`. 72
8.3 Αρχικό στάδιο αποθήκευσης του σημείου βάσης P στη διαρκή, `non Volatile`, μνήμη 76
8.4 Αρχικό στάδιο αποθήκευσης του σημείου $2P$ στη διαρκή, `non Volatile`, μνήμη 76
8.5 Αρχικό στάδιο αποθήκευσης του σημείου $R[1]$ στη διαρκή, `non Volatile`, μνήμη 77
8.6 Αρχικό στάδιο αποθήκευσης του σημείου $R[-1]$ στη διαρκή, `non Volatile`, μνήμη 77

8.7 Αρχικό στάδιο αποθήκευσης των παραμέτρων α, b στη διαρκή, non Volatile, μνήμη 78
8.8 Αρχικό στάδιο αποθήκευσης του κρυφού κλειδιού στη διαρκή, non Volatile, μνήμη 78
8.9 Στιγμιότυπο ολοκληρωμένης αποθήκευσης του σημείου βάσης P στη διαρκή, non Volatile, μνήμη 79
8.10 Στιγμιότυπο αποθήκευσης του διπλασίου σημείου βάσης $2P$ στη διαρκή, non Volatile, μνήμη 79
8.11 Στιγμιότυπο της αποθήκευσης της ποσότητας $R[1]$, στη διαρκή, non Volatile, μνήμη 80
8.12 Στιγμιότυπο της αποθήκευσης της ποσότητας $R[-1]$, στη διαρκή, non Volatile, μνήμη 80
8.13 Στιγμιότυπο της αποθήκευσης των ποσοτήτων α, b, στη διαρκή, non Volatile, μνήμη 81
8.14 Στιγμιότυπο της αποθήκευσης του κρυφού κλειδιού, στη διαρκή, non Volatile, μνήμη 81
8.15 Στιγμιότυπο ολοκληρωμένης αποθήκευσης του σημείου βάσης P στη διαρκή, non Volatile, μνήμη στο τέλος της πρώτης φάσης. 82
8.16 Στιγμιότυπο της ολοκληρωμένης αποθήκευσης του διπλασίου σημείου βάσης $2P$ στη διαρκή, non Volatile, μνήμη στο τέλος της πρώτης φάσης. 82
8.17 Στιγμιότυπο της ολοκληρωμένης αποθήκευσης της ποσότητας $R[1]$, στη διαρκή, non Volatile, μνήμη στο τέλος της πρώτης φάσης. 83
8.18 Στιγμιότυπο της ολοκληρωμένης αποθήκευσης της ποσότητας $R[-1]$, στη διαρκή, non Volatile, μνήμη στο τέλος της πρώτης φάσης. . . 83
8.19 Στιγμιότυπο της ολοκληρωμένης αποθήκευσης των α, b, στη διαρκή, non Volatile, μνήμη στο τέλος της πρώτης φάσης. 84
8.20 Στιγμιότυπο της ολοκληρωμένης αποθήκευσης του κρυφού κλειδιού, στη διαρκή, non Volatile, μνήμη στο τέλος της πρώτης φάσης. . . 84
8.21 Στιγμιότυπο της ολοκληρωμένης αποθήκευσης του κρυφού κλειδιού, στη διαρκή, non Volatile, μνήμη στο τέλος της τρίτης φάσης. . . . 85

Κατάλογος Πινάκων

4.1 Παράδειγμα Εύρεσης σημείων Ελλειπτικής Καμπύλης 21

7.1 Τυπικοί χρόνοι εκτέλεσης του RSA 63
7.2 Τυπικοί χρόνοι εκτέλεσης του προτεινόμενου Πρωτοκόλλου Ελλειπτικών Καμπυλών, με βελτιστοποιήσεις. 64
7.3 Τυπικοί χρόνοι εκτέλεσης του προτεινόμενου Πρωτοκόλλου Ελλειπτικών Καμπυλών, χωρίς τις βελτιστοποιήσεις. 64

Ευχαριστίες

Η παρούσα εργασία δε θα μπορούσε να ολοκληρωθεί χωρίς τη πολύτιμη βοήθεια ορισμένων ανθρώπων. Θα προσπαθήσω μέσα σε λίγες γραμμές να εκφράσω τις ευχαριστίες μου σε αυτούς τους ανθρώπους ως το λιγότερο που θα μπορούσε κανείς να κάνει για να δείξει την ευγνωμοσύνη του. Πρώτα θέλω να ευχαριστήσω τον επόπτη και σύμβουλο μου κύριο Απόστολο Τραγανίτη για την επιστημονική και όχι μόνο συμβολή του στη διεκπεραίωση αυτής της εργασίας. Τους καθηγητές του τμήματος κύριους, Δημήτρη Πλεξουσάκη και Ευάγγελο Μαρκάτο για τη προσφορά τους στη σταδιοδρομία μου με τη συμμετοχή τους στην εξεταστική επιτροπή, τον καθηγητή του Μαθηματικού Τμήματος Γιάννη Αντωνιάδη για την πολύτιμή βοήθεια του στο μαθηματικό μέρος αυτής της εργασίας, και την καθηγήτρια των Αγγλικών Χεντρίκα Βαρδαβά, για την βοήθεια της στη συγγραφή του Αγγλικού κειμένου.

Επίσης θα ήθελα να ευχαριστήσω το προσωπικό του τμήματος Επιστήμης Υπολογιστών, τις κυρίες Μαρία Σταυρακάκη, Ρένα Καλαϊτζάκη, Μαρία Μαμαλάκη, και Χριστίνα Βαλίνι, καθώς και τον κύριο Γιάννη Σουρλατζή διότι με την πολύτιμη συμβολή τους κατάφεραν να εξασφαλήσουν την απρόσκοπη και συνεχή εργασία μου. Θα ήθελα επίσης να ευχαριστήσω το Ινστιτούτο Τεχνολογίας και Ερεύνας για την οικονομική του υποστήριξη, η οποία αποτέλεσε ζωτικής σημασίας παράγοντα στην ολοκλήρωση αυτής της εργασίας.

Περισσότερο όμως, θα ήθελα να ευχαριστήσω τους γονείς μου και την αδερφή μου, οι οποίοι μου έδωσαν τη δυνατότητα να φθάσω σε αυτό το σημείο και των οποίων οι συμβουλές και οι αγωνίες αποτελούσαν και αποτελούν πολύτιμο μάθημα για μένα.

Τέλος θα ηθέλα να ευχαριστήσω όλους τους συναδέλφους και συμφοιτητές μου, με τους οποίους πέρασα αυτά τα δύο χρόνια στην Κρήτη και να τους ευχηθώ καλή τύχη και καλή σταδιοδρομία σε ότι και αν επιλέξουν να κάνουν.

Κεφάλαιο 1

Γενικά Στοιχεία Εργασίας

1.1 Περίληψη Εργασίας

Η εργασία αυτή έχει σαν στόχο την υλοποίηση ενός πρωτοκόλλου πιστοποίησης της ταυτότητας μεταξύ δύο συμβαλλόμενων οντοτήτων και την παράλληλη διασφάλιση του καναλιού επικοινωνίας τους μέσω της δημιουργίας δημόσιων και ιδιωτικών κλειδιών κρυπτογράφησης. Επιπλέον, προκειμένου να ενισχυθεί η αποτελεσματικότητα του συγκεκριμένου πρωτοκόλλου, προτείνουμε ένα μηχανισμο διαχείρισης της στατικής μνήμης της ασύρματης έξυπνης κάρτας για την αποθήκευση κρίσιμων δεδομένων. Όλα τα παραπάνω εφαρμόζονται έχοντας σαν βάση την θεωρία των Ελλειπτικών Καμπυλών σε Πεπερασμένα Πεδία, με στόχο την αξιοποίηση των μοναδικων τους ιδιοτήτων.

1.2 Δομή της Εργασίας

Αρχικά, θα αναφερθούμε στην γενικότερη αναφορά και κατηγοριοποίηση των καρτών του τύπου `[ID-1]`, επικεντρώνοντας τον ενδιαφέρον μας κυρίως στις Έξυπνες Κάρτες, με ή χωρίς επαφή, και στα χαρακτηριστικά τους. Το επόμενο κεφάλαιο έχει να κάνει με την ανάλυση του μαθηματικού πλαισίου πάνω στο οποίο θα στηριχθούμε για την υλοποίηση της συγκεκριμένης εργασίας. Η ανάλυση αυτή θα επιτελεσθεί μέσω της μελέτης των πεπερασμένων πεδίων, και της θεωρίας των Ελλειπτικών Καμπυλών πάνω σε αυτά. Στο επόμενο κεφάλαιο θα αναλύσουμε τόσο τις απαιτήσεις των παραμέτρων του χώρου των Ελλειπτικών Καμπυλών προκειμένου να μπορούμε να απαιτήσουμε υψηλά επίπεδα ασφάλειας, όσο και τα απαιτούμενα στοιχεία του προτεινόμενου Αλγορίθμου που αφορούν την ορθή και ασφαλή εκτέλεση του. Στο επόμενο κεφάλαιο θα ακολουθήσει η πλήρης και αναλυτική περιγραφή του πρωτοκόλλου που προτείνουμε για την πιστοποίηση της ταυτότητας και τη διασφάλιση του καναλιού επικοινωνίας, η παρουσίαση μετρήσεων και συγκριτικών αποτελεσμάτων, και σχετική αναφορά αναγκαίων και σημαντικών παρατηρήσεων. Τέλος, θα περιγράψουμε τον αλγόριθμο διαχείρισης της μνήμης δίνοντας επιπλέον και ένα γραφικό παράδειγμα για την καλύτερη κατανόηση του, θα παρουσιάσουμε μετρήσεις και συγκριτικά αποτελέσματα και θα κλείσουμε την εργασία αυτή με ένα επίλογο εφοδιασμένο με τα κατάλληλα συμπεράσματα που εξήχθησαν με την υλοποίηση της παρούσας εργασίας.

Κεφάλαιο 2

Τύποι Καρτών

2.1 Η Ιστορία των Έξυπνων Καρτών

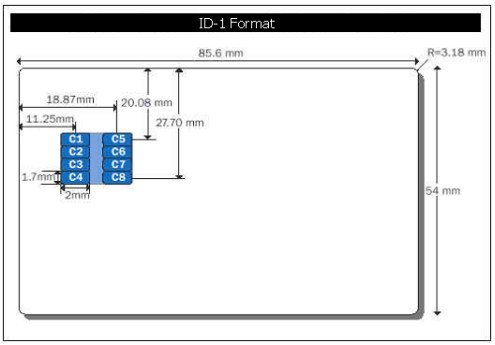
Η χρησιμοποίηση των πλαστικών καρτών ξεκίνησε στις Η.Π.Α στις αρχές της δεκαετίας του 1950. Η χαμηλή τιμή του συνθετικού υλικού του PVC επιτρέπουν την παραγωγή εύρωστων και με μεγάλη διάρκεια ζωής, καρτών. Αυτές οι κάρτες άρχισαν να είναι περισσότερο βολικές έναντι του χαρτιού που χρησιμοποιώταν μέχρι τότε, το οποίο προφανώς δεν είναι το ίδιο ανθεκτικό, όσο οι πλαστικές κάρτες. Η πρώτη πλαστική κάρτα πληρωμής γενικού σκοπού εκδόθηκε από την Diners Club το 1950. Προοριζόταν για μια συγκεκριμένη, υψηλή, τάξη ανθρώπων και είχε τον χαρακτήρα επικύρωσης της ισχυρής οικονομικής κατάστασης. Η εισαγωγή της Visa και της MasterCard στο πεδίο, οδήγησε στην εξάπλωση της χρησιμοποίησης του πλαστικού χρήματος, αρχικά στις Η.Π.Α, με την Ευρώπη και τον υπόλοιπο κόσμο να ακολουθεί αυτή την τάση λίγα χρόνια αργότερα.

Αρχικά η λειτουργία των καρτών ήταν σχετικά τετριμμένη. Αποτελούσαν φορείς δεδομένων οι οποίοι παρείχαν ασφάλεια ενάντια της πλαστογραφίας. Γενικές πληροφορίες, όπως το όνομα του κατόχου της κάρτας, ήταν τυπωμένες πάνω στην επιφάνεια της, ενώ τα προσωπικά δεδομένα του κατόχου της, και ο αριθμός της, ήταν σε ανάγλυφη μορφή. Επιπλέον πολλές κάρτες είχαν ένα πεδίο προκειμένου ο κάτοχος της κάρτας να έχει την δυνατότητα να υπογράφει. Οι κάρτες που μόλις περιγράψαμε ήταν αυτές της πρώτης γενιάς, και παρείχαν προστασία απέναντι στην πλαστογραφίας μέσω μεθόδων που κυρίως ήταν εμφανείς, δηλαδή μέσω του πεδίου της υπογραφής και των εκτυπωμένων πεδίων που περιγράψαμε. Αρα η ασφάλεια του συστήματος είχε να κάνει κυρίως με την ποιότητα και την ευσυνειδησία του υπαλλήλου που δεχόταν ή όχι, τις κάρτες αυτού του είδους. Αρχικά αυτό δεν ήταν τόσο μεγάλο πρόβλημα, αφού οι κάρτες ήταν λίγες σε αριθμό. Ωστόσο καθώς η χρησιμοποίηση των καρτών γινόταν μεγαλύτερη, τόσο μεγαλύτερος γινόταν και ο κίνδυνος για κακόβουλη χρήση της κάρτας θέτοντας την ανάγκη για ύπαρξη μεθόδων ασφάλειας έγινε επιτακτική.

2.2 Τύποι καρτών

Αυτή η ενότητα έχει σαν σκοπό την παρουσίαση διαφόρων τύπων καρτών, που ωστόσο έχουν τα ίδια φυσικά χαρακτηριστικά, όπως την ευλυγισία flexibility, την αντίσταση σε διάφορες συνθήκες θερμοκρασίας, και συγκεκριμένες διαστάσεις. Όλοι οι τύποι ανήκουν στο πλαίσιο μιας συγκεκριμένης μορφής την οποία καλούμε

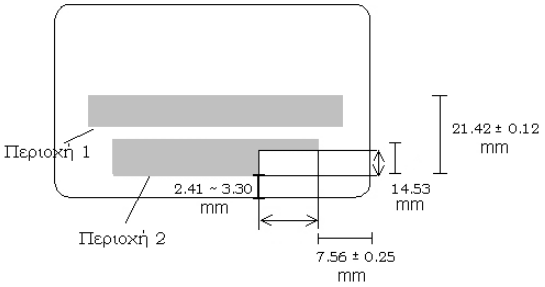
[ID-1 format] και είναι ορισμένη από το [ISO standard 7810].



Σχήμα 2.1: Η μορφή του ID-1 format

2.2.1 Ανάγλυφες Κάρτες

Η ανάγλυφη μορφή, είναι η παλιότερη τεχνική για την εφαρμογή αναγνωρίσιμων από μηχάνημα στιγμάτων, Machine-readable markings για την αναγνώριση της ταυτότητας των καρτών. Οι ανάγλυφοι χαρακτήρες στην κάρτα μπορούν να μεταφερθούν σε χαρτί χρησιμοποιώντας απλές και φθηνές συσκευές. Η οπτική ανάγνωση της ανάγλυφης μορφής είναι εντελώς απλή, και η φύση και η τοπολογία της θέσης των ανάγλυφων χαρακτήρων καθορίζονται από το [ISO stanard 7811, Identification Cards - Recording Technique].



Σχήμα 2.2: Οι Ανάγλυφες Περιοχές σύμφωνα με το ISO 7811-3

Το [ISO 7811 Part 1] καθορίζει τις απαιτήσεις για τους ανάγλυφους χαρακτήρες, όπως για παράδειγμα την μορφή τους, το μέγεθος τους και διάφορα άλλα χαρακτηριστικά. Το τρίτο τμήμα [ISO 7811 Part 3] ορίζει την ακριβή θέση των χαρακτήρων στην κάρτα, και ορίζει επίσης δύο ξεχωριστές περιοχές. Η πρώτη περιοχή διατηρείται για την τοποθέτηση του Αριθμού Αναγνώρισης της Κάρτας, Identification Card Number, το οποίο θα ταυτοποιεί τόσο την κάρτα όσο και τον χρήστη αυτής. Η δεύτερη περιοχή διατηρείται για επιπλέον δεδομένα που αφορούν τον ιδιοκτήτη της κάρτας, όπως για παράδειγμα το όνομα και τη διεύθυνση.

Από πρώτη ματιά, η μεταφορά δεδομένων με αποτύπωση ανάγλυφων χαρακτήρων

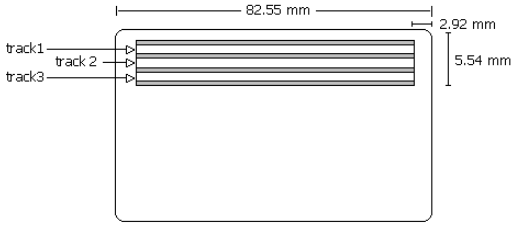
μπορεί να εμφανίζεται πρωτόγονη, ωστόσο η απλότητα της την έκανε αποδεκτή ακόμα και σε τεχνολογικά εξελιγμένες χώρες.

2.2.2 Κάρτες με μαγνητική ταινία

Το ουσιαστικό πρόβλημα των ανάγλυφων καρτών είναι ότι δημιουργούν ένα μεγάλο αριθμό από χάρτινες αποδείξεις, οι οποίες είναι δύσκολο να επεξεργαστούν. Μία λύση σε αυτό το θέμα είναι η ψηφιακή κωδικοποίηση των δεδομένων της κάρτας σε μια μαγνητική ταινία η οποία βρίσκεται στο πίσω μέρος της κάρτας.

Η μαγνητική ταινία διαβάζεται με το να τη διαπεράσουμε κατά μήκος μιας κεφαλής ανάγνωσης, είτε με μηχανικό, είτε με αυτόματο τρόπο. Η επεξεργασία αυτή δεν απαιτεί την χρήση χαρτιού.

Τα μέρη `[ISO 7811 2,3,4]` καθορίζουν τις ιδιότητες μιας μαγνητικής κάρτας, τις τεχνικές κωδικοποίησης, και την θέση των μαγνητικών ταινιών. Η μαγνητική ταινία μπορεί να περιέχει μέχρι τρεις τομείς, `tracks`. Οι τομείς (1) και (2) είναι καθορισμένοι έτσι ώστε να έχουν μόνο δυνατότητα ανάγνωσης, ενώ ο τομέας (3) έχει και δικαιώματα γραφής. Ακόμα και αν η αποθηκευτική δυνατότητα μιας μαγνητικής ταινίας είναι περίπου 1000 bits, κάτι το οποίο δεν είναι πολύ, είναι ωστόσο υπεραρκετό για την αποθήκευση των στοιχείων που υπάρχουν στις ανάγλυφες κάρτες. Επιπλέον τα δεδομένα μπορούν να γραφούν ή να διαβαστούν στον τρίτο τομέα, όπως για παράδειγμα η τελευταία, πιο πρόσφατη, δοσοληψία που έλαβε χώρα στο τρέχον χρονικό διάστημα της ζωής της κάρτας.



Σχήμα 2.3: Οι Περιοχές των Μαγνητικών Ταινιών σε Κάρτα του [ID-1 f ormat]

Το κύριο αρνητικό στοιχείο της τεχνολογίας της μαγνητικής ταινίας είναι ότι τα αποθηκευμένα δεδομένα μπορούν πολύ εύκολα να αλλαχτούν κακοβούλως. Η περίπτωση της πλαστογραφίας, μιας ανάγλυφης κάρτας απαιτεί τουλάχιστον ένα σημαντικό ποσοστό επιδεξιότητας, μπορεί όμως εύκολα να γίνει αντιληπτή από ένα έμπειρο και εκπαιδευμένο μάτι. Η αλλαγή των κωδικοποιημένων δεδομένων σε μια μαγνητική ταινία είναι σχετικά εύκολη να γίνει με την χρησιμοποίηση μιας απλής, `standard read/write` μηχανής, και είναι πολύ δύσκολο στην συνέχεια και αφού το η διαδικασία αλλαγής έχει πραγματοποιηθεί, να αποδείξει κάποιος ότι τα δεδομένα δεν είναι τα σωστά. Επιπλέον, οι μαγνητικές κάρτες συχνά χρησιμοποιούνται σε αυτοματοποιημένα συστήματα στα οποία η οπτική επιθεώρηση είναι αδύνατη, όπως για παράδειγμα στις Αυτόματες Ταμιακές Μηχανές. Ο ενδεχόμενος αντίπαλος ο οποίος έχει λάβει σωστά δεδομένα από την κάρτα, μπορεί εύκολα να χρησιμοποιεί διπλές, `duplicated` κάρτες σε χωρίς επίβλεψη μηχανές, χωρίς να χρειάζεται να πλαστογραφήσει οπτικά στίγματα ασφαλείας.

Οι κατασκευαστές αυτού του είδους καρτών χρησιμοποιούν διάφορα μέσα προκειμένου να μπορούν να προστατεύουν τα δεδομένα που υπάρχουν στην μαγνητική ταινία απέναντι στην πλαστογραφία. Για παράδειγμα, οι κάρτες `German Eurocheck` περιέχουν ένα αόρατο και χωρίς την δυνατότητα αλλαγής, `unaltered`, κώδικα στο σώμα της κάρτας, ο οποίος κάνει αδύνατη τη δυνατότητα αλλοίωσης ή αναπαραγωγής της μαγνητικής ταινίας. Ωστόσο, αυτή όπως και άλλες τεχνικές απαιτούν ένα ειδικό αισθητήρα, `sensor` στο τερματικό της κάρτας, το οποίο αυξάνει αρκετά το κόστος.

2.2.3 Έξυπνες Κάρτες

Οι Έξυπνες κάρτες είναι το νεότερο και το πιο εξελιγμένο μέλος της οικογένειας καρτών ταυτοποίησης του `[ID-1 format]`. Το χαρακτηριστικό τους στοιχείο είναι η ύπαρξη ενός ολοκληρωμένου κυκλώματος πάνω στην κάρτα, το οποίοο έχει στοιχεία για μετάδοση, αποθήκευση, και επεξεργασία δεδομένων. Η μετάδοση δεδομένων μπορεί να πραγματοποιηθεί είτε μέσω επαφών που βρίσκονται πάνω στην επιφάνεια της κάρτας, είτε μέσω ηλεκτρομαγνητικού πεδίου, χωρίς την χρήση τέτοιων επαφών.

Οι έξυπνες κάρτες προσφέρουν ένα αριθμό πλεονεκτημάτων σε σύγκριση με τις κάρτες μαγνητικής ταινίας. Για παράδειγμα, η μέγιστη αποθηκευτική ικανότητα μιας Έξυπνης Κάρτας είναι πολλές φορές μεγαλύτερη από αυτή μιας Κάρτας με μαγνητική ταινία. Ολοκληρωμένα κυκλώματα με αποθηκευτική ικανότητα πάνω από 32 `KiloBytes` μνήμης είναι διαθέσιμα στην αγορά με τάση να αυξάνονται αρκετά με την πάροδο του χρόνου. Μόνο οι Οπτικές Κάρτες που θα αναφέρουμε στην επόμενη ενότητα έχουν τη δυνατότητα μεγαλύτερης αποθηκευτικής ικανότητας.

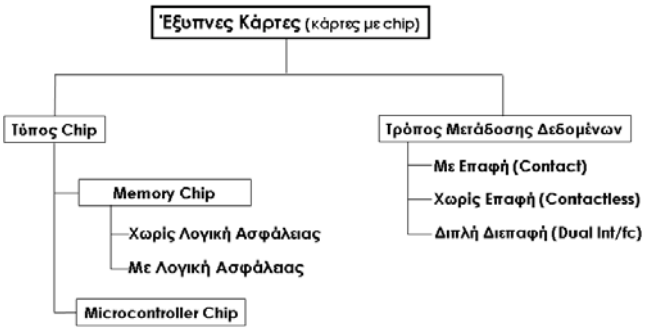
Ωστόσο, ένας από τους πιο σημαντικούς παράγοντες για τον οποίο οι Έξυπνες Κάρτες υπερτερούν έναντι όλων των άλλων τύπων καρτών είναι το γεγονός ότι τα αποθηκευμένα δεδομένα μπορούν να προστατεύονται έναντι στη μη εξουσιοδοτημένη πρόσβαση και στην πλαστογραφία. Καθώς η πρόσβαση στα δεδομένα λαμβάνει χώρα μόνο από μια σειριακή διεπαφή η οποία ελέγχεται από ένα λειτουργικό σύστημα και λογική ασφάλειας, είναι δυνατόν να εγγραφούν εμπιστευτικά δεδομένα στην κάρτα, έτσι ώστε να μην μπορούν ποτέ να διαβαστούν από τον έξω κόσμο. Αυτά τα εμπιστευτικά δεδομένα μπορεί κανείς να τα επεξεργαστεί μόνο εσωτερικά από την υπολογιστική μονάδα. Οι λειτουργίες της μνήμης της εγγραφής, ανάγνωσης, και διαγραφής μπορούν να περιοριστούν σε συγκεκριμένους όρους τόσο από την μεριά του Υλικού όσο και από την μεριά του Λογισμικού. Αυτό επιτρέπει την ανάπτυξη και τον σχεδιασμό πλήθους μηχανισμών ασφάλειας, οι οποίοι μπορούν να προσαρμοστούν στις ειδικές ρυθμίσεις συγκεκριμένων εφαρμογών.

Το γεγονός αυτό μαζί με τη δυνατότητα του υπολογισμού κρυπτογραφικών αλγορίθμων επιτρέπει την χρησιμοποίηση των Έξυπνων Καρτών στο σχεδιασμό και στην ανάπτυξη ασφαλών εφαρμογών οι οποίες μπορούν να εφαρμοστούν σε κάθε περίπτωση. Επιπλέον, τα πλεονεκτήματα των Έξυπνων Καρτών έχουν να κάνουν με την υψηλό βαθμό αξιοπιστίας που προσφέρουν, και την μεγάλη διάρκεια ζωής που διαθέτουν σε σύγκριση με αυτή των μαγνητικών καρτών.

Οι έξυπνες κάρτες μπορούν να χωριστούν σε δύο σύνολα, ανάλογα με τις διαφορές στη λειτουργία και στην τιμή:

- Κάρτες Μνήμης, `memory cards`.
- Κάρτες με μικροεπεξεργαστή, `microprocessor cards`.

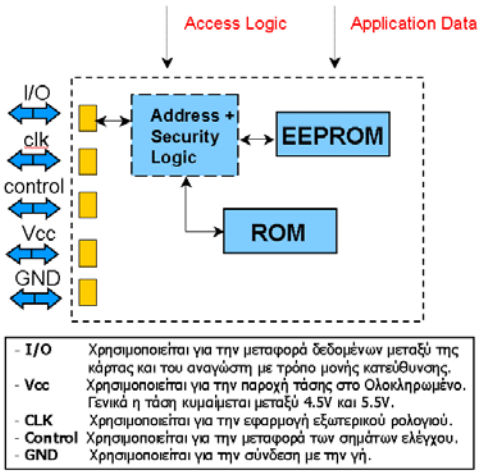
Δίνουμε και ένα πίνακα ταξινόμησης της παραπάνω διάκρισης.



Σχήμα 2.4: Ταξινόμηση Έξυπνων Καρτών

2.2.4 Κάρτες Μνήμης

Το σχήμα που παρουσιάζουμε στη συνέχεια περιγράφει τη δομή του αρχιτεκτονικού διαγράμματος μιας κάρτας Μνήμης.



Σχήμα 2.5: Το block διάγραμμα μιας κάρτας μνήμης.

Τα δεδομένα που απαιτούνται για την εφαρμογή, αποθηκεύονται στην μνήμη, η οποία είναι συνήθως η μνήμη `EEPROM`. Η πρόσβαση στην μνήμη ελέγχεται από μια μονάδα έλεγχου λογικής, `security logic`, η οποία στην πιο απλή περίπτωση αποτελείται μόνο από προστασία γραφής ή διαγραφής για όλη ή για κάποιες περιοχές της μνήμης. Ωστόσο υπάρχουν και κυκλώματα τα οποία περιέχουν πιο περίπλοκες δομές ασφάλειας, και τα οποία μπορούν να εκτελέσουν απλές κρυπτογραφικές λειτουργίες. Τα δεδομένα μεταφέρονται από και προς την κάρτα μέσω του I/O `port`. Το τρίτο τμήμα `[Part 3]` του `[ISO 7816]` πρωτοκόλλου ορίζει έναν ειδικό σύγχρονο τρόπο μεταφοράς ο οποίος επιτρέπει την ανάπτυξη απλών και οικονομικών κυκλωμά-

των. Ωστόσο κάποιες κάρτες χρησιμοποιούν το I^2C `bus`, το οποίο χρησιμοποιείται κυρίως σε συνδυασμό με σειριακής πρόσβασης μνήμες.

Οι λειτουργίες μιας κάρτας μνήμης είναι βελτιστοποιημένες για μια συγκεκριμένη εφαρμογή. Αν και αυτό περιορίζει την ευελιξία, τις καθιστά πιο οικονομικές. Οι κάρτες μνήμης χρησιμοποιούνται κυρίως για προπληρωμένες τηλεφωνικές συνδιαλέξεις, και κάρτες ασφάλειας υγείας.

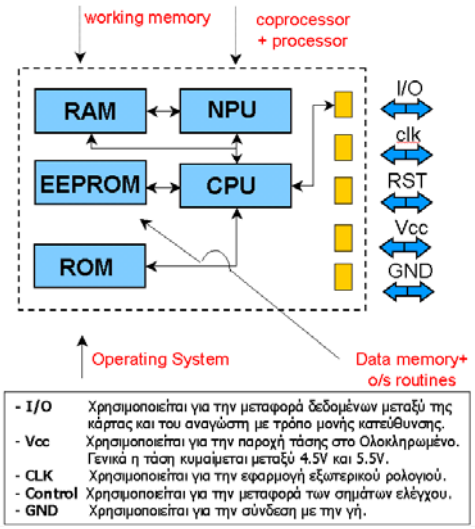
2.2.5 Κάρτες με Μικροεπεξεργαστή

Η καρδιά του κυκλώματος σε μία κάρτα με μικροεπεξεργαστή, όπως φαίνεται και από το όνομα της, είναι ένας επεξεργαστής, ο οποίος περιβάλλεται από τέσσερις επιπλέον λειτουργικές μονάδες οι οποίες είναι:

- ROM. Αυτή η μνήμη περιλαμβάνει το λειτουργικό σύστημα του κυκλώματος, το οποίο γίνεται `burned in` κατά την κατασκευή του κυκλώματος. κυκλώματος. Το περιεχόμενο της ROM είναι πανομοιότυπο για κάθε κύκλωμα κάθε παραγωγικού κύκλου και δεν μπορεί να αλλάξει κατά τη διάρκεια της ζωής του κυκλώματος.
- EEPROM. Αυτή η μνήμη είναι η διαρκής, `non volatile`, μνήμη. Τα δεδομένα και ο κώδικας του προγράμματος μπορεί να γραφούν και να διαβαστούν από αυτή την μνήμη, κάτω από τον έλεγχο του λειτουργικού συστήματος.
- RAM. Η μνήμη αυτή είναι είναι η μνήμη εργασίας του επεξεργαστή. Είναι `volatile` μνήμη και όλα τα δεδομένα χάνονται όταν χαθεί και η τροφοδοσία του ρεύματος προς το κύκλωμα.
- I/O PORT. Η σειριακή I/O διεπαφή συνήθως αποτελείται από ένα καταχωρητή, διαμέσω του οποίου τα δεδομένα μεταφέρονται με ένα δυαδικό ψηφίο την φορά.

Οι κάρτες με μικροεπεξεργαστή είναι πολύ ευέλικτες στην χρήση. Κατά την πιο απλή περίπτωση περιέχουν ένα βελτιστοποιημένο πρόγραμμα για μια εφαρμογή, και έτσι μπορούν να χρησιμοποιηθούν μόνο για τη δεδομένη εφαρμογή. Ωστόσο, το λειτουργικό σύστημα των σύγχρονων καρτών επιτρέπει την ενσωμάτωση πολλών διαφορετικών εφαρμογών σε μια κάρτα. Κατά την περίπτωση αυτή η `ROM` περιέχει μόνο βασικές εντολές του λειτουργικού συστήματος, και το ειδικό τμήμα για την εφαρμογή του προγράμματος φορτώνεται στην `EEPROM` αφού η κάρτα έχει κατασκευαστεί. Ειδικά βελτιστοποιημένα κυκλώματα με υψηλές δυνατότητες επεξεργασίας και μεγάλη αποθηκευτική ικανότητα έχουν αναπτυχθεί προκειμένου να εκτελούν υψηλής απόδοσης εφαρμογές με ανάγκη για υψηλή ασφάλεια και υπολογισμό περίπλοκων κρυπτογραφικών αλγορίθμων.

Παραθέτουμε στη συνέχεια το `block` διάγραμμα μιας κάρτας με μικροεπεξεργαστή.

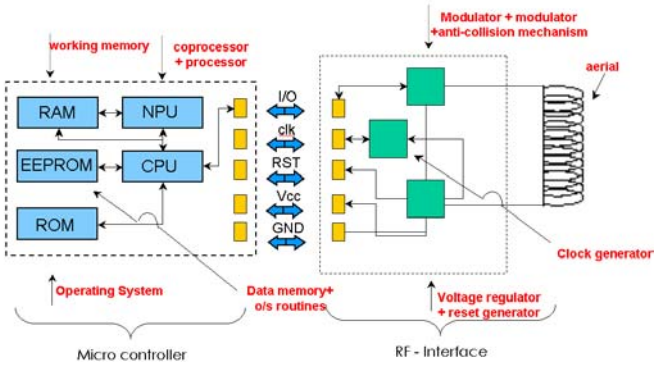


Σχήμα 2.6: Το block διάγραμμα μιας κάρτας με μικροεπεξεργαστή.

2.2.6 Έξυπνες Κάρτες χωρίς Επαφή

Οι Έξυπνες Κάρτες με Επαφή συμμορφώνονται με τα πρότυπα του `[standard ISO 7816 part 1]`. Η αξιοπιστία των καρτών αυτών αυξάνεται συνεχώς με την πάροδο των ετών, εξαιτίας της αυξανόμενης εμπειρίας στον χώρο των κατασκευών τέτοιου είδους καρτών. Ένα χαρακτηριστικό παράδειγμα είναι το γεγονός ότι ο ρυθμός βλαβών των καρτών τηλεφωνικών συνδιαλέξεων, έναντι στην αναμενόμενη διάρκεια ζωής τους, που είναι ένας χρόνος, είναι κάτω του 0.1%. Ωστόσο, η επαφή εξακολουθεί να παραμένει ένας από τους βασικότερους λόγους των πιο συχνών πηγών βλαβών στα ηλεκτρομηχανικά συστήματα. Οι βλάβες μπορούν να προκύψουν από την φθορά των επαφών. Στα μη σταθερά συστήματα, οι δονήσεις μπορούν να προκαλέσουν σύντομες μη ολοκληρωμένες φορτίσεις, και αφού οι επαφές βρίσκονται στην επιφάνεια της κάρτας και συνδέονται απευθείας στις εισόδους δεδομένων του ολοκληρωμένου κυκλώματος της κάρτας, ο κίνδυνος καταστροφής ή βλάβης του ολοκληρωμένου κυκλώματος λόγω ηλεκτροστατικών αποφορτίσεων - φορτίσεων μερικών χιλιάδων `volts` είναι πολύ μεγάλος.

Αυτά τα προβλήματα τεχνικού είδους αποφεύγονται με την χρησιμοποίηση Έξυπνων Καρτών χωρίς Επαφή. Έκτος των τεχνικών πλεονεκτημάτων που υπάρχουν, η τεχνολογία των Έξυπνων Καρτών χωρίς Επαφή, προσφέρει στον κατασκευαστή της κάρτας, καθώς και στον ιδιοκτήτη της, μια πληθώρα από νέες ενδεχόμενες εφαρμογές. Για παράδειγμα, οι Έξυπνες Κάρτες χωρίς Επαφή δεν χρειάζεται να εισαχθούν σε κάποιο τερματικό αναγνώστη, αφού είναι συστήματα τα οποία λειτουργούν μέχρι και σε απόσταση ενός μέτρου. Αυτό είναι ένα πολύ σημαντικό πλεονέκτημα σε σύστημα ελέγχου πρόσβασης, `access control`. Έτσι για παράδειγμα μια πόρτα που χρειάζεται να ανοίξει, πλέον μπορεί να ανοίξει χωρίς το άτομο το οποίο επιθυμεί την πρόσβαση να χρειάζεται να βγάλει από την τσέπη του ή το πορτοφόλι του την



Σχήμα 2.7: Το block διάγραμμα μιας Έξυπνης Κάρτας χωρίς Επαφή.

κάρτα, αφού δεν απαιτείται η εισαγωγή της κάρτας σε κάποιο μηχάνημα ανάγνωσης. Μια άλλη επεκταμένη εφαρμογή για αυτή την τεχνολογία είναι η αυτή της τοπικής δημόσιας συγκοινωνίας, κατά την οποία ένας μεγάλος αριθμός ανθρώπων χρειάζεται να αναγνωρισθεί στο μικρότερο δυνατό χρόνο. Ωστόσο, η ασύρματη τεχνολογία έχει πλεονέκτημα ακόμα και στην περίπτωση συστημάτων που απαιτούν την αναγκαστική εισαγωγή της κάρτας στον αναγνώστη, αφού ο τρόπος εισαγωγής δεν παίζει κανένα ρόλο. Αυτό έρχεται σε αντίθεση με τις μαγνητικές κάρτες, ή τις κάρτες με επαφή, οι οποίες πρέπει να εισάγονται με συγκεκριμένο τρόπο στο μηχάνημα του αναγνώστη. Έτσι η ελευθερία που προσφέρουν έναντι στους περιορισμούς που θέτουν οι άλλες μορφές καρτών αυξάνει τη λειτουργικότητα των Καρτών χωρίς Επαφή και συνεπώς την αποδοχή τους από τους απλούς χρήστες.

Μια επιπλέον ενδιαφέρουσα παραλλαγή στην χρήση καρτών χωρίς Επαφή, σχετίζεται με την χρήση ενός τερματικού επιφάνειας. Κατά αυτή την περίπτωση η κάρτα δεν εισάγεται σε κάποια υποδοχή του τερματικού, αλλά απλά εφάπτεται στην μαρκαρισμένη επιφάνεια ενός αναγνώστη. Εκτός της ευκολίας χρήσης, αυτή η λύση είναι ενδιαφέρουσα καθώς έχει την ιδιότητα να αποφεύγει τυχόν βανδαλισμούς, όπως για παράδειγμα την εισαγωγή κόλλας ή άλλων κολλοειδών ουσιών στην υποδοχή του αναγνώστη.

Όσον αφορά την εμπορική εκμετάλλευση των καρτών χωρίς επαφή, υπάρχει το πλεονέκτημα ότι κανένα τεχνικό στοιχείο, `technical element`, δεν είναι εμφανές στην επιφάνεια της κάρτας, και έτσι ο οπτικός σχεδιασμός τέτοιων καρτών δεν περιορίζεται από μαγνητικές ταινίες ή επιφανειακές επαφές. Μέχρι τη δεδομένη στιγμή οι κάρτες αυτές χρησιμοποιούνται κυρίως για την τοπική συγκοινωνία, όπου εκεί λειτουργούν σαν εισιτήρια. Τα σημερινά συστήματα χρησιμοποιούν κάρτες μιας κύριας λειτουργίας, για τις οποίες κυκλώματα με φθηνή λογική έχουν αναπτυχθεί. Ωστόσο υπάρχουν σοβαρά δείγματα ότι οι κάρτες με πολυλειτουργικότητα θα γίνουν σύντομα οι αντικαταστάτες των ήδη υπαρχόντων, σχετικά απλών, καρτών.

2.2.7 Οπτικές Κάρτες Μνήμης

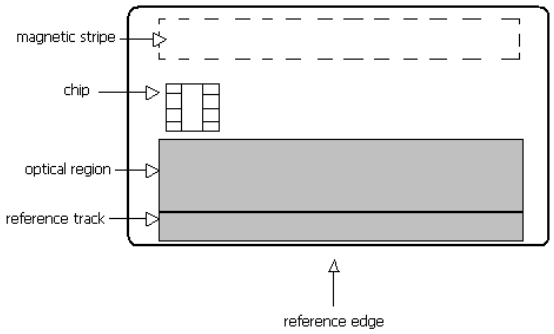
Στις εφαρμογές στις οποίες η αποθηκευτική ικανότητα που απαιτείται είναι μεγαλύτερη από αυτή που μπορούν να προσφέρουν οι Έξυπνες Κάρτες, έχουμε την χρησιμοποίηση Οπτικών Καρτών Μνήμης, οι οποίες μπορούν να αποθηκεύσουν ένα μεγάλο ποσό από `megabytes` δεδομένων. Ωστόσο, με την υπάρχουσα τεχνολογία

αυτές οι κάρτες μπορούν να εκτελούν εγγραφές μόνο μια φορά και δεν μπορούν να διαγραφούν.

Το [ISO/IEC 11 693-94] καθορίζει τις διαστάσεις και τα φυσικά χαρακτηριστικά των οπτικών καρτών, καθώς και την τεχνική εγγραφής δεδομένων.

Ο συνδυασμός της υψηλής αποθηκευτικής ικανότητας των Οπτικών Καρτών με την ευφυΐα των Έξυπνων καρτών απορρέει νέα ενδιαφέροντα χαρακτηριστικά. Για παράδειγμα τα δεδομένα μπορούν να γραφούν κρυπτογραφημένα σε μία οπτική κάρτα, ενώ το ιδιωτικό κλειδί είναι ασφαλώς αποθηκευμένο στην μνήμη του κυκλώματος της κάρτας. Έτσι τα δεδομένα της οπτικής κάρτας είναι ασφαλώς προστατευμένα έναντι σε αναρμόδια πρόσβαση.

Παραθέτουμε την μορφή μιας τέτοιας κάρτας, δηλαδή μιας Οπτικής Έξυπνης Κάρτας στο παρακάτω σχήμα.



Σχήμα 2.8: Μορφή μιας Οπτικής Έξυπνης Κάρτας.

2.3 Ο κύκλος ζωής μιας Έξυπνης Κάρτας

Όπως ήδη έχουμε αναφέρει κάθε έξυπνη κάρτα περιέχει στο εσωτερικό της ένα λειτουργικό σύστημα, το οποίο μπορεί να περιέχει έναν Αριθμό Αναγνώρισης Ταυτότητας της κάρτας `Identification Card Number`, ο οποίος είναι μοναδικά ορισμένος και τον τοποθετεί ο κατασκευαστής, ένα σειριακό αριθμό, πληροφορίες για το προφίλ και άλλα. Επίσης, η περιοχή του συστήματος μπορεί να περιέχει διαφορετικά κλειδιά ασφάλειας, όπως το κλειδί του κατασκευαστή, ή το κλειδί της κατασκευής, `fabrication key`, και το κλειδί της ταυτοποίησης, `Personalization key`. Όλες αυτές οι πληροφορίες πρέπει να διατηρηθούν κρυφές και να μην αποκαλυφθούν σε ξένα πρόσωπα.

Η παραγωγή μιας Έξυπνης κάρτας χωρίζεται σε διαφορετικά στάδια, τα οποία είναι πέντε στον αριθμό και παρουσιάζονται παρακάτω:

- Φαση Κατασκευης. Αυτή η φάση υλοποιείται από τους κατασκευαστές του κυκλώματος. Το ολοκληρωμένο κύκλωμα από σιλικόνη δημιουργείται από τους κατασκευαστές του κυκλώματος. Το ολοκληρωμένο κύκλωμα από σιλικόνη

δημιουργείται και ελέγχεται κατά τη διάρκεια αυτής της φάσης. Ένα κλειδί κατασκευής, `fabrication key (fk)`, προστίθεται στο κύκλωμα για να προστατεύσει από πλαστή τροποποίηση μέχρι να συναρμολογηθεί στην πλαστική υποστήριξη της κάρτας. Το `fk` κάθε κυκλώματος είναι μοναδικό και προέρχεται από ένα Κύριο Κλειδί Κατασκευαστή,`Master manifacturer key`. Αλλα δεδομένα της συναρμολόγησης θα γραφτούν στο ολοκληρωμένο κύκλωμα στο τέλος αυτής της φάσης.

- Φαση Προ-Προσωποποιησης. Η φάση αυτή υλοποιείται από τους προμηθευτές των καρτών. Κατά τη διάρκεια αυτής της φάσης το κύκλωμα θα επικολληθεί στην πλαστική κάρτα η οποία μπορεί να περιέχει και το σήμα του παροχέα υπηρεσιών. Η σύνδεση μεταξύ του κυκλώματος και του τυπωμένου κυκλώματος θα πραγματοποιηθεί και όλη η μονάδα θα ελεγχθεί. Για επιπλέον ασφάλεια και για την ασφαλή μετάβαση της κάρτας το κλειδί της κατασκευής θα αντικατασταθεί από το κλειδί προσωποποίησης, `personalization key`. Μετά από αυτό η ασφάλεια της προσωποποίησης V_{PER} θα γραφεί προκειμένου να εμποδίσει τυχόν μετατροπή του κλειδιού προσωποποίησης . Επιπλέον, η πρόσβαση στην φυσική μνήμη θα γίνει ανενεργής. Η πρόσβαση θα γίνεται μόνο χρησιμοποιώντας διευθυνσιοδότηση λογικής μνήμης, προκειμένου να αποφεύγεται η πρόσβαση στην περιοχή κατασκευής, `facrication area`.

- Φαση Προσωποποιησης. Αυτή η φάση ολοκληρώνεται από τους εκδότες της κάρτας και είναι η φάση κατά την οποία ολοκληρώνεται η δημιουργία των λογικών δομών δεδομένων. Τα περιεχόμενα των αρχείων δεδομένων και των δεδομένων εφαρμογών γράφονται στην κάρτα. Το `PIN, unblocking PIN`, θα αποθηκευτούν στην κάρτα. Τέλος μια ασφάλεια χρησιμοποίησης V_{UTIL}, θα γραφεί προκειμένου να υποδείξει ότι η κάρτα βρίσκεται στην φάση χρησιμοποίησης, `utilisation phase`.

- Φαση Χρησιμοποιησης. Αυτή είναι η φάση κανονικής λειτουργίας της κάρτας από τον χρήστη. Όλα τα ενεργά μέρη της κάρτας βρίσκονται σε λειτουργία.

- Φαση Απενεργοποιησης της Καρτας. Υπάρχουν δύο τρόποι για να σταλεί μια κάρτα σε αυτό το στάδιο. Ο ένας τρόπος έχει να κάνει με την εφαρμογή η οποία γράφει μια ασφάλεια απενεργοποίησης σε ένα ξεχωριστό αρχείο ή στο `Master` αρχείο, απενεργοποιώντας έτσι όλες τις δυνατές λειτουργίες της κάρτας. Η μόνη λειτουργία που παραμένει ενεργή είναι αυτή της ανάγνωσης. Ο άλλος τρόπος είναι να τεθεί η κάρτα σε αυτήν την φάση, όταν το σύστημα ελέγχου κλειδώνει αμετάκλητα την πρόσβαση και στη συνέχεια το `PIN` όσο και το `Unblocking PIN` μπλοκάρονται έτσι ώστε καμιά λειτουργία να μην μπορεί εκτελεστεί.

2.4 Λογική Δομή και Έλεγχος Πρόσβασης Έξυπνων Καρτών

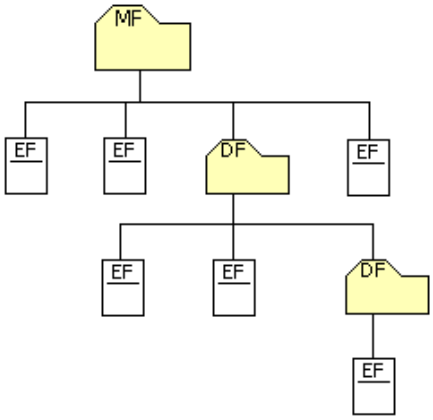
Όταν μια κάρτα διανέμεται σε ένα καταναλωτή από τον παροχέα εφαρμογών, η ασφάλεια της κάρτας ελέγχεται κυρίως από λειτουργικό σύστημα της εφαρμογής. Η κατάσταση φυσικής διευθυνσιοδότησης δεν είναι πλέον διαθέσιμη. Η πρόσβαση στα δεδομένα πρέπει να γίνει μέσω της Λογικής Δομής Αρχείων της κάρτας. Αυτή η ενότητα θα ασχοληθεί με το πως το λειτουργικό σύστημα επιτυγχάνει την προστασία ασφάλειας των δεδομένων που αποθηκεύονται στην κάρτα με το να εξετάζει την Λογική Δομή Αρχείων και το σχετικό έλεγχο πρόσβασης της κάρτας.

2.4.1 Λογική Δομή Αρχείων

Γενικά, όσον αφορά την αποθήκευση δεδομένων, μια Έξυπνη Κάρτα μπορεί να θεωρηθεί σαν ένας σκληρός δίσκος όπου τα αρχεία είναι οργανωμένα σε ιεραρχική δομή μέσω καταλόγων. Παρόμοια με το λειτουργικό σύστημα MS-DOS, υπάρχει μόνο ένα κύριο αρχείο το οποίο είναι σαν τον root κατάλογο. Κάτω από το root κατάλογο, έχουμε διαφορετικά αρχεία τα οποία καλούμε στοιχειώδη, elementary, EFs, αρχεία. Επίσης, έχουμε ποικίλους υποκαταλόγους, τους οποίους καλούμε αφιερωμένα,

στοιχειώδες αρχείο. Η κύρια διαφορά του συστήματος αρχείων της Έξυπνης Κάρτας και του MS-DOS έγκειται στο ότι τα αφιερωμένα αρχεία της Έξυπνης Κάρτας μπορούν να περιέχουν δεδομένα.

Παρακάτω δίνουμε σχηματικά την μορφή του συστήματος αρχείων της Έξυπνης Κάρτας.



Σχήμα 2.9: Μορφή του Λογικού συστήματος αρχείων μιας Έξυπνης Κάρτας

Στην ορολογία έξυπνων καρτών, η ρίζα ή το κύριο αρχείο Master File, MF, εκτός από το μέρος επικεφαλίδων που περιέχει, περιλαμβάνει και τις επικεφαλίδες όλων των αφιερωμένων αρχείων και στοιχειωδών αρχείων που περιέχουν το κύριο αρχείο στη γονική τους ιεραρχία. Το αφιερωμένο αρχείο DF είναι μια λειτουργική ομαδοποίηση των αρχείων που αποτελείται από τον εαυτό και όλα τα αρχεία που είναι άμεσα παιδιά του. Το στοιχειώδες αρχείο EF αποτελείται απλά από την επικεφαλίδα του και το σώμα που καταχωρεί τα στοιχεία.

Οι τρόποι κατά τους οποίους τα δεδομένα ρυθμίζονται μέσα σε ένα αρχείο διαφέρουν, και εξαρτώνται από τα διαφορετικά λειτουργικά συστήματα που χρησιμοποιούνται. Μερικοί από τους τρόπους με τους οποίους μπορούν τα δεδομένα μπορούν να διαχειριστούν τα δεδομένα είναι, απλά μέσω του offset και του μήκους, ενώ άλλα μπορούν να οργανώσουν τα δεδομένα τους σε σταθερά ή μεταβλητά μήκη αρχείων όπως το [Global System Mobile Communication]. Κάθε μια από αυτές τις περιπτώσεις αυτές απαιτεί το αρχείο να πρέπει να επιλεχθεί πριν εκτελεστεί οποιαδήποτε άλλη λειτουργία.

Οι λογικοί μηχανισμοί πρόσβασης και επιλογής ενεργοποιούνται αφότου διοχετευτεί ρεύμα στην κάρτα ενώ το κύριο αρχείο επιλέγεται αυτόματα. Η λειτουργία

επιλογής επιτρέπει τη μετακίνηση γύρω από το δέντρο. Μπορεί να είναι κίνηση πτωτική με την επιλογή ενός από το EF ή DF, ή μπορεί να είναι κίνηση προοδευτική με την επιλογή ενός MF ή DF. Η οριζόντια μετακίνηση μπορεί να γίνει με την επιλογή ένος EF.

Μετά από την επιτυχία της επιλογής, η επικεφαλίδα του αρχείου μπορεί να ανακτηθεί, και η ανάκτηση της θα μπορέσει να μας πληροφορήσει σχετικά με στοιχεία όπως ο αριθμός αναγνώρισης, περιγραφές, τύπους, και το μέγεθος. Ιδιαίτερα, επικεφαλίδα καταχωρεί τις ιδιότητες του αρχείου που δηλώνουν τους όρους πρόσβασης και την παρούσα κατάσταση. Η πρόσβαση των δεδομένων στο αρχείο εξαρτάται από εάν οι όροι μπορούν να τηρηθούν ή όχι.

Εν ολίγοις, η δομή αρχείων του λειτουργικού συστήματος έξυπνων καρτών είναι παρόμοια με άλλα κοινά λειτουργικά συστήματα όπως το MS-DOS και το UNIX. Εντούτοις, προκειμένου να παρασχεθεί μεγαλύτερος έλεγχος ασφάλειας, η ιδιότητα κάθε αρχείου ενισχύεται με την προσθήκη όρων πρόσβαση και πεδίων θέσης αρχείων, status fields, στην επικεφαλίδα αρχείων. Επιπλέον, παρέχεται το κλείδωμα αρχείων, για να αποτραπεί η πρόσβαση στο αρχείο. Αυτοί οι μηχανισμοί και οι αλγόριθμοι ασφάλειας παρέχουν μια λογική προστασία της έξυπνης κάρτας.

Κεφάλαιο 3

Πεπερασμένα Πεδία

3.1 Περιγραφή Πεπερασμένων Πεδίων

Ορισμός 1 *Ένα πεπερασμένο πεδίο (ή πεδίο* `Galois` *είναι ένα σύνολο από πεπερασμένα στοιχεία στο οποίο μπορούν να εφαρμοστούν οι συνηθισμένες αλγεβρικές πράξεις (προσθήκη, αφαίρεση, πολλαπλασιασμός, διαίρεση στοιχείων διαφορετικών του μηδενός), και στο οποίο οι συνηθισμένοι αλγεβρικοί νόμοι ισχύουν.*

Ορισμός 2 *Η τάξη ενός πεπερασμένου πεδίου είναι ο αριθμός στοιχείων που περιλαμβάνει. Εάν $q > 1$ είναι ένας ακέραιος αριθμός, έπεται ότι ένα πεπερασμένο πεδίο τάξης q υπάρχει εάν το q είναι μια πρωταρχική δύναμη, δηλαδή δύναμη πρώτου αριθμού, και όχι ειδάλλως.*

Το πεπερασμένο πεδίο μιας δεδομένης τάξης είναι μοναδικό, υπό την έννοια ότι οποιαδήποτε δύο πεδία τάξης q παρουσιάζουν την ίδια αλγεβρική δομή. Εντούτοις, υπάρχουν συχνά πολλοί τρόποι να αναπαρασταθεί ένα πεδίο. Είναι σύνηθες να συμβολίζουμε το πεπερασμένο πεδίο της τάξης q σαν $\mathcal{F}_q$ ή σαν $GF(q)$.

Όπως ήδη έχουμε αναφέρει τα πεπερασμένα πεδία, μπορούν να προέρχονται από οποιαδήποτε δύναμη πρώτου αριθμού, ωστόσο στην περίπτωση της Κρυπτογραφίας δύο ειδών πεπερασμένα πεδία χρησιμοποιούνται.

- Όταν το q είναι πρώτος αριθμός p, τότε το πεδίο ονομάζεται Πεπερασμένο Πεδίο Πρώτων Αριθμών.
- Όταν το q είναι $q = 2^m$ για κάποιο m, τότε καλείται Δυαδικό Πεπερασμένο Πεδίο.

3.2 Πολυώνυμα σε Πεπερασμένα Πεδία

Ορισμός 3 *Ένα πολυώνυμο πάνω από το πεδίο $GF(q)$ είναι ουσιαστικά ένα πολυώνυμο με συντελεστές στο $GF(q)$. Η πρόσθεση και ο πολλαπλασιασμός πολυωνύμων στο $GF(q)$ είναι καθορισμένος ως και στην βασική αριθμητική πολυωνύμων, μόνο που οι πράξεις των συντελεστών εκτελούνται πάνω από το $GF(q)$.*

Ορισμός 4 *Ένα πολυώνυμο πάνω από ένα πεδίο Πρώτων Αριθμών $GF(p)$ συνήθως καλείται πολυώνυμο modulo p.*

Παράδειγμα: Πάνω από το πεδίο Πρώτων Αριθμών $GF(7)$

$$(t^2 + 4t + 5) + (t^3 + t + 3) = t^3 + t^2 + 5t + 1$$
$$(t^2 + 3t + 4) \cdot (t + 4) = t^3 + 2t + 2$$

Ορισμός 5 *Ένα πολυώνυμο πάνω από το $GF(q)$ καλείται όχι ανάγωγο όταν προέρχεται σαν γινόμενο δύο μικρότερου βαθμού πολυώνυμων πάνω από το $GF(q)$, αλλιώς καλείται ανάγωγο.*

Έτσι το πολυώνυμο $t^3 + 2t + 2$ στο προηγούμενο παράδειγμα είναι όχι ανάγωγο πάνω από το $GF(7)$, αφού προέρχεται σαν γινόμενο των πολυωνύμων $t^2 + 3t + 4$ και $t+4$. Κάθε μη μηδενικό πολυώνυμο πάνω από το $GF(q)$ έχει μοναδική αναπαράσταση σαν γινόμενο δυνάμεων ανάγωγων πολυωνύμων.

3.3 Το Πεπερασμένο Πεδίο $\mathcal{F}_p$

Έστω ότι p είναι ένας πρώτος αριθμός. Το Πεπερασμένο πεδίο $\mathcal{F}_p$ καλείται πεδίο Πρώτων Αριθμών και αποτελείται από τους ακεραίους:

$$\{0, 1, 2, 3, ..., p - 1\}$$

Τα πεπερασμένα πεδία $\mathcal{F}_p$ επιτρέπουν τη διαίρεση πηλίκο για κάθε δυνατό παρανομαστή εκτός του 0. Το σύνολο των μη μηδενικών στοιχείων ενός πεπερασμένου πεδίου $\mathcal{F}_p$ συμβολίζεται με $\mathcal{F}_p^*$.

Περιγράφουμε ακολούθως τα χαρακτηριστικά των Πεπερασμένων Πεδίων.

- Τάξη στοιχείου: Η τάξη ενός στοιχείου του πεπερασμένου πεδίου $\mathcal{F}_p$ είναι ο μικρότερος ακέραιος n τέτοιος ώστε $c^n \equiv 1(modp)$. Η τάξη πάντα υπάρχει και διαιρεί την ποσότητα $p - 1$. Αν το k και το l είναι ακέραιοι, τότε $c^k \equiv c^l(modp)$ αν και μόνο αν ισχύει $k \equiv l(modn)$.
- Γεννήτορας Πεπερασμένου Πεδίου: Αν το n διαιρεί το $p - 1$, τότε υπάρχει ένα στοιχείο του $\mathcal{F}_p$ το οποίο έχει τάξη n. Πιο συγκεκριμένα, πάντα υπάρχει ένα στοιχείο g τάξης $p - 1$ που να ανήκει στο $\mathcal{F}_p^*$. Κάθε τέτοιο στοιχείο καλείται γεννήτορας του χώρου, γιατί κάθε στοιχείο του $\mathcal{F}_p^*$ είναι μια δύναμη του g. Επίσης, το g καλείται και πρωταρχική ρίζα για το p.

Επιπλέον τα Πεπερασμένα πεδία είναι εφοδιασμένα και με τις ακόλουθες πράξεις.

- ΠΡΟΣΘΕΣΗ: Αν $a, b \in \mathcal{F}_p$ τότε $a + b = r$, όπου r είναι το υπόλοιπο της διαίρεσης της ποσότητα $a + b$, με το p και ισχύει ότι $0 \leq r \leq p - 1$. Αυτή η πρόσθεση είναι γνωστή και σαν *πρόσθεση modulo p*.
- ΠΟΛΛΑΠΛΑΣΙΑΣΜΟΣ: Αν $a, b \in \mathcal{F}_p$ τότε $a \cdot b = s$, όπου s είναι το υπόλοιπο της διαίρεσης με την ποσότητα $a \cdot b$, με το p και $0 \leq s \leq p - 1$. Αυτός ο πολλαπλασιασμός είναι γνωστός και σαν *πολλαπλασιασμός modulo p*.
- ΑΝΤΙΣΤΡΟΦΟ ΣΤΟΙΧΕΙΟ: Αν α είναι ένα μη-μηδενικό στοιχείο στο $\mathcal{F}_p$ τότε το αντίστροφο στοιχείο a^{-1} του a, είναι ο μοναδικός ακέραιος $c \in \mathcal{F}_p$ τέτοιος ώστε $a \cdot c = 1$.

3.4 Το Πεπερασμένο Πεδίο $\mathcal{F}_{2^m}$

Ορισμός 6 *Το πεδίο $\mathcal{F}_{2^m}$ καλείται Πεπερασμένο Πεδίο Χαρακτηριστικής Δύο ή Δυαδικό Πεπερασμένο Πεδίο, και μπορεί να θεωρηθεί σαν ένας διανυσματικός χώρος διάστασης m πάνω από το Πεδίο $\mathcal{F}_2$. Το σώμα $\mathcal{F}_2$ είναι το πεπερασμένο σώμα το οποίο αποτελείται από τα στοιχεία 0, και 1. Δηλαδή υπάρχουν m στοιχεία $a_0, a_1, a_2, ..., a_{m-1}$ στο $\mathcal{F}_2$ τέτοια ώστε κάθε στοιχείο $\alpha \in \mathcal{F}_{2^m}$ μπορεί να γραφεί στην μορφή:*

$$a = c_0 a_0 + c_1 a_1 + c_2 a_2 + ... + c_{m-1} a_{m-1}\}, c_i \in \{0, 1\}$$

Ένα τέτοιο σύνολο $\{a_0, a_1, a_2, ..., a_{m-1}\}$ καλείται *βάση* του $\mathcal{F}_{2^m}$ πάνω από $\mathcal{F}_2$. Υπάρχουν πολλών ειδών βάσεις στο $\mathcal{F}_{2^m}$, ορισμένες όμως οδηγούν σε ποιο αποτελεσματικές εφαρμογές της αριθμητικής στο $\mathcal{F}_{2^m}$ από μερικές άλλες. Το `[ANSI X9.62]` επιτρέπει την αναπαράσταση ως προς δύο είδη βάσεων:

- Τις πολυωνυμικές και,
- τις κανονικές.

3.4.1 Αναπαράσταση Πολυωνυμικής Βάσης

Τα στοιχεία του $\mathcal{F}_{2^m}$ είναι πολυώνυμα με βαθμό μικρότερο του m, με συντελεστές από το $\mathcal{F}_2$, δηλαδή:

$$a_{m-1} x^{m-1} + a_{m-2} x^{m-2} + ... + a_2 x^2 + a_1 x + a_0, \mid a_i = 0 \| 1$$

Τα στοιχεία αυτά επίσης μπορούν να γραφούν και σε μορφή διανύσματος σαν:

$$(a_{m-1}, \vec{a_{m-2}}, ..., a_0).$$

Το $\mathcal{F}_{2^m}$ έχει 2^m στοιχεία. Οι κύριες λειτουργίες στο $\mathcal{F}_{2^m}$ είναι ο πολλαπλασιασμός και η πρόσθεση. Αυτές οι πράξεις περιλαμβάνουν και ένα πολυώνυμο της μορφής:

$$f(x) = x^m + f_{m-1} x^{m-1} + f_{m-2} x^{m-2} + ... + f_1 x + f_0, f_i \in \mathcal{F}_2$$

Το πολυώνυμο f_x πρέπει να είναι ανάγωγο δηλαδή να μην γράφεται σαν γινόμενο άλλων πολυωνύμων του $\mathcal{F}_2$ με βαθμό μικρότερο του m.

Πράξεις Πεδίου

- ΠΡΟΣΘΕΣΗ: Αν $a = (a_{m-1}, a_{m-2}, ..., a_0)$, και $b = (b_{m-1}, b_{m-2}, ..., b_0) \in \mathcal{F}_{2^m}$ τότε $a + b = c$, όπου $c = (c_{m-1}, c_{m-2}, ..., c_0)$, και $c_i = (a_i + b_i) mod 2$.

- ΠΟΛΛΑΠΛΑΣΙΑΣΜΟΣ: Αν $a = (a_{m-1}, ..., a_0)$, και $b = (b_{m-1}, ..., b_0) \in \mathcal{F}_{2^m}$ όπου $a \cdot b = c$, όπου $c = (c_{m-1}, c_{m-2}, ..., c_0)$ είναι το υπόλοιπο της διαίρεσης του γινομένου των πολυωνύμων $(a \cdot b)$ δια το πολυώνυμο $f(x)$ πάνω από το F_2. Το τετράγωνο ενός πολυωνύμου σε ένα (modulo 2) πεδίο είναι μια γραμμική πράξη. Όσον αφορά την σχέση για τον τετραγωνισμό ενός διωνύμου, $(\alpha+\beta)^2 = \alpha^2 + 2 \cdot \alpha \cdot \beta + \beta^2$, ο μεσαίος όρος $(2 \cdot \alpha \cdot \beta) \longmapsto 0$ λόγω του (modulo 2) και έτσι το τετράγωνο γίνεται $\alpha^2 + \beta^2$.Έτσι μπορούμε να τετραγωνίσουμε ένα άθροισμα με το να τετραγωνίσουμε απλά τον κάθε όρο του αθροίσματος.

  Για παράδειγμα έστω, $(u^3 + u + 1)^2 = u^6 + u^2 + 1$.
  Αν δούμε το πολυώνυμο σε μορφή αναπαράστασης από bits τότε ο τετραγωνισμός γίνεται τοποθετώντας ένα μηδενικό bit μεταξύ κάθε bit του πολυωνύμου. Δηλαδή αναφερόμενοι στο προηγούμενο παράδειγμα το

  $$(u^3 + u + 1) \longmapsto 1011$$

  γίνεται με αυτή την τεχνική

  $$1000101 \longmapsto u^6 + u^2 + 1.$$

- ΑΝΤΙΣΤΡΟΦΟ ΣΤΟΙΧΕΙΟ: Αν α είναι ένα μη-μηδενικό στοιχείο στο $\mathcal{F}_{2^m}$ τότε το αντίστροφο στοιχείο a^{-1} είναι ο μοναδικός ακέραιος $c \in \mathcal{F}_{2^m}$ τέτοιος ώστε $a \cdot c = 1$.

- ΑΠΑΛΟΙΦΗ ΥΠΟΛΟΙΠΟΥ *(Modular Reduction)*: Τα στοιχεία του πεδίου είναι πολυώνυμα με συντελεστές στο δακτύλιο $\mathcal{Z}_2$. Μετά από κάθε πολλαπλασιασμό ή τετραγωνισμό το αποτέλεσμα πρέπει να απαλείφεται βάση του ανάγωγου πολυωνύμου *T(υ)* (*modulo T(υ)*).

3.4.2 Αναπαράσταση Κανονικής Βάσης

Ορισμός 7 *Μια κανονική βάση του $\mathcal{F}_{2^m}$ πάνω από το $\mathcal{F}_2$ είναι μία βάση της μορφής $\{\beta, \beta^2, \beta^{2^2}, ..., \beta^{2^{m-1}}\}$, και το $\beta \in \mathcal{F}_{2^m}$. Μια τέτοια βάση πάντα υπάρχει. Οποιοδήποτε στοιχείο $\alpha \in \mathcal{F}_{2^m}$ μπορεί να γραφεί στην μορφή*

$$\alpha = \sum_{i=0}^{m-1} \alpha_i \beta^{2^i},$$

όπου

$$\alpha \in \{0, 1\}$$

Βέλτιστη Κανονική Βάση

Για πολλές τιμές του m το πεδίο $\mathcal{F}_{2^m}$ έχει μια Βέλτιστη Κανονική Βάση. Οι Βέλτιστες Κανονικές Βάσεις ταξινομούνται είτε σαν αυτές με *Τύπο I* είτε σε αυτές με *Τύπο II*. Η τιμή του m καθορίζει τον τύπο ο οποίος θα χρησιμοποιηθεί. Διακρίνουμε δύο περιπτώσεις αναλόγως με τον τύπο της Βέλτιστης Κανονικής Βάσης.

- Αν το πεδίο $\mathcal{F}_{2^m}$ έχει μόνο Τύπου I Βέλτιστη Κανονική Βάση τότε θέτουμε $f(x) = x_m + x_{m-1} + ... + x_2 + x + 1$.
- Αν το πεδίο $\mathcal{F}_{2^m}$ έχει μόνο Τύπου II Βέλτιστη Κανονική Βάση τότε θέτουμε $f(x) = f_m(x)$ και ακολουθούμε την παρακάτω επαναληπτική μεθοδολογία.

$$f_0(x) = 1,\ f_1(x) = x + 1,\ f_{i+1}(x) = xf_i(x) + f_{i-1}(x), i = 1, ..., m.$$

Οι συντελεστές των πολυωνύμων $f_i(x)$ ακολουθούν τον κανόνα του υπόλοιπου 2 σε κάθε στάδιο. Έτσι το $f(x)$ είναι πολυώνυμο βαθμού m με συντελεστές $\mathcal{F}_2$. Το σύνολο των πολυωνύμων $\{x, x^2, x^{2^2}, ..., x^{2^{m-1}}\}$ είναι μια βάση του $\mathcal{F}_{2^m}$ πάνω από το $\mathcal{F}_2$ η οποία καλείται κανονική βάση.

- Κατασκευάζουμε ένα πίνακα $A_{m\times m}$ του οποίου η i γραμμή, $i = 0, ..., m-1$ είναι η γραμμή από bits που σχετίζονται με το πολυώνυμο $x^{2^i} mod f(x) i$. Τα στοιχεία του πίνακα A είναι στοιχεία του πεδίου $\mathcal{F}_2$.
- Καθορισμός του αντιστρόφου του πίνακα A, (τον πίνακα A^{-1} στο πεδίο $\mathcal{F}_2$).
- Κατασκευή του πίνακα $T^{'}$ του οποίου η i γραμμή, $(i = 0, ..., m-1)$ είναι ίση με την ποσότητα:

  $$x \cdot x^{2^i} mod f(x).$$

  Έπεται ο υπολογισμός του πίνακα $T = T^{'} \cdot A^{-1}$ πάνω στο πεδίο του $\mathcal{F}_2$.
- Καθορισμός των όρων του γινομένου l_{ij} για $i, j = 0, ..., m-1$ καθώς $l_{ij} = T(j-i, -i)$. Με τον όρο $T(g, h)$ συμβολίζουμε την (g, h) είσοδο του πίνακα T με στοιχεία τα οποία ακολουθούν τον νόμο μείωσης υπολοίπου m. Κάθε όρος l_{ij} είναι στοιχείο του $\mathcal{F}_2$.

  Πρέπει επίσης να σημειώσουμε ότι $l_{0j} = 1$ για ακριβώς ένα j με j :, $0 \leq j \leq m-1$ και ότι για κάθε i,με $i : 0 \leq i \leq m-1$ έχω $l_{ij} = 1$ για ακριβώς 2 διακριτά μεταξύ των $j : 0 \leq j \leq m-1$. Έτσι έπεται ότι μόνο 2^{m-1} από τις m^2 εισόδους του πίνακα T είναι ίσες με 1 και οι υπόλοιπες είναι 0. Αυτή η έλλειψη από 1 είναι ο λόγος για τον οποίο η κανονική βάση καλείται *Βέλτιστη Κανονική Βάση*.

Κεφάλαιο 4

Ελλειπτικές Καμπύλες σε Πεπερασμένα Πεδία

4.1 Εισαγωγή στις Ελλειπτικές Καμπύλες

Οι Ελλειπτικές Καμπύλες επινοήθηκαν γύρω στο 1985 από τους `Miller` και `Koblitz`. Μετά την εισαγωγή τους στον χώρο της Κρυπτολογίας, μια ευρεία συζήτηση άρχισε να εξελίσσεται σχετικά με την ασφάλεια και αποδοτικότητα τους. Τα δύο αυτά χαρακτηριστικά, είναι που τις κάνουν τόσο ενδιαφέρουσες για μας σήμερα, και αυτό είναι κάτι το οποίο οφείλεται και στην εξέλιξη της τεχνολογίας της πληροφορίας. Η αυξανόμενη χρήση των υπολογιστών χειρός και των κινητών τηλεφώνων, η τάση δημιουργίας ασύρματων δικτύων και γενικότερα η στρέψη προς την ασύρματη επικοινωνία προϋποθέτουν ένα ασφαλές και αξιόπιστο υπόβαθρο πάνω στο οποίο θα στηριχθούν οι διάφορες εφαρμογές. Πάνω σε αυτό το πλαίσιο επέρχεται και η εισαγωγή των Ελλειπτικών Καμπύλων οι οποίες χάρη στις μοναδικές τους ιδιότητες μπορούν να προσφέρουν τόσο υψηλό επίπεδο ασφάλειας, όσο και ευελιξία στον χώρο αυτό.

Η επιλογή των Ελλειπτικών Καμπυλών για την περίπτωση των Έξυπνων Καρτών χωρίς επαφή δεν είναι τυχαία, άλλα πηγάζει κυρίως από τις ειδικές απαιτήσεις που έχουν αυτές οι κάρτες για αυξημένη ασφάλεια, αλλά και από τους περιορισμούς στους οποίους υπόκεινται λόγω κατασκευής.

Έτσι πρέπει να ληφθούν υπόψη οι παρακάτω περιορισμοί:

- Η ύπαρξη πολύ περιορισμένης μνήμης σε αυτές τις συσκευές.

- και η μικρή τους υπολογιστική ικανότητα.

Επίσης δεν πρέπει να παραλείψουμε να επισημάνουμε την αδυναμία που υπάρχει για κατανάλωση μεγάλου εύρους φάσματος. Αυτό που χρειαζόμαστε στην περίπτωση των συσκευών αυτών είναι ένα κρυπτοσύστημα με μικρά σε μέγεθος κλειδιά και μικρές σε μέγεθος ψηφιακές υπογραφές. Τα Κρυπτοσυστήματα Ελλειπτικών Καμπυλών έχουν ακριβώς τις απαιτούμενες ιδιότητες. Αυτό απορρέει από το γεγονός, ότι δεν υπάρχουν υποεκθετικοί αλγόριθμοι για το Πρόβλημα Διακριτού Λογαρίθμου Ελλειπτικών Καμπύλων που είναι γνωστοί σήμερα, με αποτέλεσμα να μπορούμε να χρησιμοποιήσουμε μικρότερα σε μέγεθος κλειδιά (σε σύγκριση με τα άλλα κρυπτοσυστήματα) για τα ίδια επίπεδα υψηλής ασφάλειας.

Κάνουμε στο σημείο αυτό μια εισαγωγή σχετικά με την θεωρία των Ελλειπτικών Καμπυλών σε μαθηματικό επίπεδο. Θα μελετήσουμε τόσο τις Ελλειπτικές Καμπύλες στο πεδίο $\mathcal{F}_p$, όσο και τις καμπύλες στο πεδίο $\mathcal{F}_{2^m}$. Στη συνέχεια θα παρουσιάσουμε ένα βέλτιστο αλγόριθμο για τον υπολογισμό του γραμμικού πολλαπλασιασμού ενός σημείου της Ελλειπτικής Καμπύλης με μια αυθαίρετη σταθερά. Η πράξη αυτή θα αποτελέσει το κύριο συστατικό της σταθερότητας και της ασφάλειας του συστήματος, αφού αποτελεί την βάση του Προβλήματος του Διακριτού Λογάριθμου για τις Ελλειπτικές Καμπύλες, το οποίο θεωρητικά είναι αδύνατον να επιλυθεί. Ο στόχος μας είναι να κάνουμε την πράξη αυτή όσον το δυνατόν πιο βέλτιστη από άποψη κόστους πράξεων, υπολογιστικής ισχύς, και απαιτούμενης μνήμης. Ο τρόπος με τον οποίο το επιτυγχάνουμε θα περιγράφει αναλυτικά.

4.2 Ελλειπτικές Καμπύλες στο $\mathcal{F}_p$

Ορισμός 1 *Έστω $p > 3$ ένας πρώτος αριθμός. Μια Ελλειπτική Καμπύλη E στο $\mathcal{F}_p$, ορίζεται από την εξίσωση της μορφής:*

$$y^2 = x^3 + \alpha \cdot x + b, 3$$

όπου

$$\alpha, b \in \mathcal{F}_p$$

και

$$4 \cdot \alpha^3 + 27 \cdot b^2 \neq 0 (mod p).$$

Το σύνολο $\mathcal{E}(\mathcal{F}_p)$ αποτελείται από όλα τα σημεία $(x, y), x \in \mathcal{F}_p$, $y \in \mathcal{F}_p$ που ικανοποιούν την εξίσωση (3), μαζί με ένα ειδικό σημείο που καλείται Επ' Άπειρου σημείο και συμβολίζεται με I.

Ευρεση σημειων Ελλειπτικης Καμπυλης.

Για κάθε $x \in \mathcal{F}_p$ υπολογίζουμε την ποσότητα $x^3 + \alpha \cdot x + b$ και ελέγχουμε αν αυτή η ποσότητα αποτελεί τετραγωνικό υπόλοιπο (modulo p). Ο τρόπος για να υπολογίσουμε ένα τετραγωνικό υπόλοιπο είναι, είτε μέσω εξαντλητικής δοκιμής, είτε μέσω του συμβόλου `Jacobi`. Αυτό που ουσιαστικά αναπαριστά το τετραγωνικό υπόλοιπο είναι σε μαθηματική έκφραση:

$$y \in F_p \exists x \in F_p : x^2 (mod p) = y,$$

δηλαδή την εύρεση ενός αριθμού, x,του οποίου το τετράγωνο μειωμένο κατά p θα δίνει το δεδομένο αριθμό, y. Όταν έχουμε θετική περίπτωση, δηλαδή υπάρχει τετραγωνικό υπόλοιπο, βρίσκουμε δύο λύσεις για το y, διαφορετικά δεν βρίσκουμε καμία λύση.

Παραθέτουμε ένα παράδειγμα εύρεσης σημείων μιας Ελλειπτικής Καμπύλης.

Θεωρούμε την Ελλειπτική Καμπύλη:

$$y^2 = x^3 + x + 6, \in F_{11},$$

τότε για κάθε $x \in F_{11}$, υπολογίζουμε την ποσότητα $z = x^3 + x + 6 (mod 11)$ και ελέγχουμε αν το z είναι τετραγωνικό υπόλοιπο $mod 11$, βάσει των δύο μεθόδων. Αν έχουμε θετική απάντηση τότε βρίσκουμε δύο λύσεις για το y, αλλιώς καμία. Τέλος

δεν πρέπει να παραλείψουμε να συμπεριλάβουμε το Επ Άπειρον σημείο.
Για το συγκεκριμένο παράδειγμα και για την πρώτη στήλη του πίνακα έχουμε:

$$x = 2 \rightarrow z = 2^3 + 2 + 6 = 16 = 5 mod 11,$$

και έτσι με δοκιμή επιλέγουμε $y = 4, 7$ αφού:

$$y = 4 \rightarrow y^2 = 4^2 = 16 = 5 mod 11 = z,$$

και

$$y = 7 \rightarrow y^2 = 7^2 = 49 = 5 mod 11 = z.$$

Ο πλήρης πίνακας για όλες τις τιμές του x, φαίνεται παρακάτω:

x	$z = x^3 + x + 6 (mod 11)$	Τετραγωνικό Υπόλοιπο	y
0	6	ΟΧΙ	–
1	8	ΟΧΙ	–
2	5	ΝΑΙ	$4, 7$
3	3	ΝΑΙ	$5, 6$
4	8	ΟΧΙ	–
5	4	ΝΑΙ	$2, 9$
6	8	ΟΧΙ	–
7	4	ΝΑΙ	$2, 9$
8	9	ΝΑΙ	$3, 8$
9	7	ΟΧΙ	–
10	4	ΝΑΙ	$2, 9$

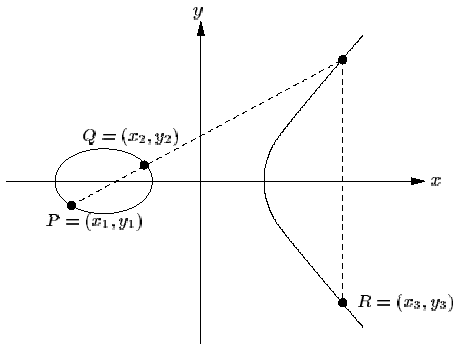
Πίνακας 4.1: Παράδειγμα Εύρεσης σημείων Ελλειπτικής Καμπύλης

Παρατηρούμε ότι τα ρητά σημεία της Καμπύλης $\mathcal{E}(\mathcal{F}_{11})$ είναι 12, δηλαδή 6 ζεύγη και το Επ Άπειρον σημείο.

Κανονας Προσθεσης.
Υπάρχει ένας κανόνας ο οποίος ονομάζεται Κανόνας Χορδής και Εφαπτομένης για την πρόσθεση δύο σημείων πάνω σε μία ελλειπτική καμπύλη $\mathcal{E}(\mathcal{F}_p)$.Βάσει αυτού του κανόνα λαμβάνουμε σαν αποτέλεσμα ένα τρίτο σημείο το οποίο είναι επίσης σημείο της Ελλειπτικής Καμπύλης. Αυτή η πράξη πρόσθεσης μαζί με το σύνολο των σημείων της ελλειπτικής $\mathcal{E}(\mathcal{F}_p)$ και το *Επ' Άπειρον σημείο* το οποίο αποτελεί και το ουδέτερο σημείο της καμπύλης δημιουργούν ένα Πεπερασμένο σώμα. Αυτό το σώμα χρησιμοποιείται για την κατασκευή των κρυπτοσυστήματων Ελλειπτικών Καμπυλών.

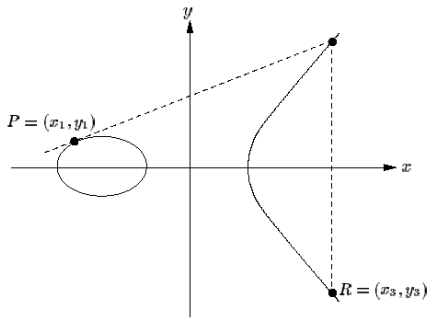
Ο κανόνας χορδής και Εφαπτομένης εξηγείται καλύτερα γεωμετρικά. Έστω $P = (x_1, y_1)$ και $Q = (x_2, y_2)$ δύο διαφορετικά σημεία μιας Ελλειπτικής Καμπύλης. Τότε το άθροισμα των σημείων P και Q το θέτουμε $R = (x_3, y_3)$ και ορίζεται ως ακολούθως. Κατ' αρχάς φέρουμε μια ευθεία γραμμή που διαπερνά το P και το Q. Αυτή η γραμμή τέμνει την Ελλειπτική Καμπύλη σε ένα τρίτο σημείο. Τότε το R είναι η προβολή του

σημείου αυτού στον άξονα$xx^{'}$. Αυτό που μόλις περιγράψαμε, δηλαδή η πρόσθεση δύο διαφορετικών σημείων της Ελλειπτικής Καμπύλης αναπαρίσταται και στο σχήμα 3.1. Η ελλειπτική καμπύλη της εικόνας αποτελείται από δύο τμήματα, το ελλειψοειδές κομμάτι και μία άπειρη καμπύλη.



Σχήμα 4.1: Γεωμετρική Αναπαράσταση πρόσθεσης Διαφορετικών σημείων

Αν $P = (x_1, y_1)$ τότε το διπλάσιο του σημείο P το ονομάζουμε $R = (x_3, y_3)$ και ορίζεται ως ακολούθως. Πρώτα σχεδιάζουμε μια εφαπτόμενη γραμμή προς την Ελλειπτική Καμπύλη στο σημείο $P \in \mathcal{E}(\mathcal{F}_p)$. Αυτή η γραμμή τέμνει την ελλειπτική Καμπύλη σε ένα δεύτερο σημείο. Τότε το $R = (x_3, y_3)$ ορίζεται σαν η προβολή του σημείου στον άξονα $[x]$. Και σχηματικά:



Σχήμα 4.2: Γεωμετρική Αναπαράσταση Διπλασιασμού Σημείου

Οι παρακάτω αλγεβρικές σχέσεις για την πρόσθεση και τον διπλασιασμό σημείων απορρέουν από την Γεωμετρική Περιγραφή.

- $\mathcal{P} + 0 = 0 + \mathcal{P} = \mathcal{P}$, για όλα τα $\mathcal{P} \in \mathcal{E}(\mathcal{F}_p)$.
- Αν $P = (x, y) \in \mathcal{E}(\mathcal{F}_p)$ τότε $(x, y) + (x, -y) = 0$. Το σημείο $(x, -y)$ συμβολίζεται ως $-P$ και ονομάζεται Αντίθετο του σημείου P. Το $-P$ επίσης ανήκει πάνω στην Καμπύλη. Γενικά υπάρχει μια πλήρως γεωμετρική ερμηνεία για την πρόσθεση σημείων. Αν συμφωνήσουμε ότι το μηδενικό σημείο βρίσκεται πάνω σε όλες τις ευθείες που είναι παράλληλες στον άξονα y, τότε μπορεί να αποδειχθεί ότι όλες οι ευθείες τέμνουν την καμπύλη σε τρία σημεία. Καταλήγουμε λοιπόν ότι η

πρόσθεση ορίζεται σαν τον κανόνα κατά τον οποίο το άθροισμα των τριών αυτών σημείων δίνει το Επ Άπειρον σημείο. Έτσι, τα σημεία P_1, P_2 και $-(P_1 + P_2)$ βρίσκονται όλα στην ίδια ευθεία. Επιπλέον το $-P$ είναι το άλλο σημείο της καμπύλης το οποίο έχει την ίδια x συνιστώσα με το P.

- Προσθεση Σημειων Έστω $P = (x_1, y_1) \in \mathcal{E}(\mathcal{F}_p)$ και $Q = (x_2, y_2) \in \mathcal{E}(\mathcal{F}_p)$ όπου $P \neq \pm Q$. Τότε το $P + Q = (x_3 + y_3)$, όπου

$$x_3 = (\tfrac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2$$

και

$$y_3 = (\tfrac{y_2 - y_1}{x_2 - x_1}) \cdot (x_1 - x_3) - y_1.$$

- Διπλασιασμος Σημειου. Έστω $P = (x_1, y_1) \in \mathcal{E}(\mathcal{F}_p)$ και $P \neq -P$. Τότε $2 \cdot P = (x_3, y_3)$, όπου:

$$x_3 = (\tfrac{3 \cdot x_1^2 + \alpha}{2 \cdot y_1})^2 - 2 \cdot x_1$$

και

$$y_3 = (\tfrac{3 \cdot x_1^2 + \alpha}{2 \cdot y_1})(x_1 - x_3) - y_1.$$

Παρατηρούμε ότι η πρόσθεση δύο σημείων της Ελλειπτικής Καμπύλης $\mathcal{E}(\mathcal{F}_p)$ δεν αποτελεί μια απλή πρόσθεση σημείων, αλλά απαιτεί μερικές επιπλέον αριθμητικές πράξεις, (πρόσθεση, αφαίρεση πολλαπλασιασμό και αντιστροφή), προκειμένου να υλοποιηθεί στο πεδίο $\mathcal{F}_p$.

4.3 Ελλειπτικές Καμπύλες στο Πεδίο $\mathcal{F}_{2^m}$

Μια Ελλειπτική Καμπύλη $\mathcal{E}$ στο $\mathcal{F}_{2^m}$ είναι ορισμένη από μια εξίσωση της μορφής

$$y^2 + x \cdot y = x^3 + \alpha \cdot x + b, \alpha, b \in \mathcal{F}_{2^m} \wedge b \neq 0.$$

Το σύνολο $\mathcal{E}(\mathcal{F}_{2^m})$ αποτελείται από όλα τα σημεία (x, y), : $x, y \in \mathcal{E}(\mathcal{F}_{2^m})$, και ικανοποιούν την παραπάνω ισότητα, μαζί με ένα ειδικό σημείο που καλείται *Επ' Άπειρον σημείο* και συμβολίζεται με $\prime$.

Κανονας Προσθεσης. Όπως και στην περίπτωση της Ελλειπτικής Καμπύλης που είναι ορισμένη στο σώμα $\mathcal{F}_p$,έτσι και εδώ υπάρχει ο Κανόνας Χορδής και Εφαπτομένης για την πρόσθεση δύο σημείων σε μία ελλειπτική καμπύλη $\mathcal{E}(\mathcal{F}_{2^m})$ προκειμένου να λάβουμε σαν αποτέλεσμα ένα τρίτο σημείο που επίσης ανήκει στην Ελλειπτικής Καμπύλης. Αυτή η πράξη πρόσθεσης, μαζί με το σύνολο των σημείων της ελλειπτικής καμπύλης $\mathcal{E}(\mathcal{F}_{2^m})$ και το Επ'Απειρον σημείο, το οποίο αποτελεί και το ουδέτερο σημείο της Ελλειπτικής Καμπύλης, δημιουργούν ένα σώμα. Αυτό το σώμα χρησιμοποιείται για την κατασκευή των κρυπτοσυστήματων Ελλειπτικών Καμπυλών.

Οι παρακάτω αλγεβρικές σχέσεις για την πρόσθεση και των διπλασιασμό σημείων απορρέουν από την Γεωμετρική Περιγραφή.

- $\mathcal{P} + 0 = 0 + \mathcal{P} = \mathcal{P}$, για όλα τα $\mathcal{P} \in \mathcal{E}(\mathcal{F}_{2^m})$.
- Αν $P = (x, y) \in \mathcal{E}(\mathcal{F}_{2^m})$ τότε $(x, y) + (x, x + y) = \prime$
- Το σημείο $(x, -y)$ συμβολίζεται ως $-P$ και ονομάζεται Αντίθετο του P. Το $-P$ επίσης ανήκει πάνω στην Καμπύλη.
- Προσθεση Σημειων. Έστω $P = (x_1, y_1) \in \mathcal{E}(\mathcal{F}_p)$ και $Q = (x_2, y_{x2}) \in \mathcal{E}(\mathcal{F}_p)$ όπου $P \neq \pm Q$. Τότε το $P + Q = (x_3, y_3)$, όπου

$$x_3 = (\tfrac{y_1+y_2}{x_1+x_2})^2 + \tfrac{y_1+y_2}{x_1+x_2} + x_1 + x_2 + \alpha$$

και

$$y_3 = (\tfrac{y_1+y_2}{x_1+x_2}) \cdot (x_1 + x_3) + x_3 + y_1$$

- Διπλασιασμος Σημειου. Έστω $P = (x_1, y_1) \in \mathcal{E}(\mathcal{F}_{2^m})$ και $P \neq -P$. Τότε $2 \cdot P = (x_3, y3)$,όπου

$$x_3 = x_1^2 + \frac{b}{x_1^2}$$

και

$$y_3 = x_1^2 + (x_1 + \frac{y_1}{x_1})x_3 + x_3$$

4.4 Περιγραφή Βελτιστοποίησης Αλγορίθμου Υπολογισμού Γραμμικού Πολλαπλασιασμού

Αυτήν η ενότητα παρουσιάζει μια βελτιστοποίηση ενός αλγορίθμου με εφαρμογή στον γραμμικό πολλαπλασιασμό. Όπως ήδη έχουμε αναφέρει, ο γραμμικός πολλαπλασιασμός ενός σημείου της Ελλειπτικής Καμπύλης και μιας αυθαίρετης σταθεράς, είναι η θεμελιώδης πράξη πάνω στην οποία στηρίζεται η ασφάλεια των Ελλειπτικών κρυπτοσυστημάτων, και κατά επέκταση η ασφάλεια του πρωτοκόλλου που θα προτείνουμε. Η χρησιμοποίηση ενός τέτοιου αλγορίθμου, δηλαδή με βέλτιστη μορφή, είναι επιτακτική στην περίπτωση μας, μιας και που το κύριο ζητούμενο είναι τόσο η ταχύτητα και ο χρόνος εκτέλεσης, όσο και η ελαχιστοποίηση των υπολογιστικών απαιτήσεων, λόγω των περιορισμών των Έξυπνων Καρτών χωρίς επαφή. Αυτός ο αλγόριθμος μπορεί να εφαρμοστεί σε οποιοδήποτε σώμα, αλλά εμείς θεωρούμε ότι τον εφαρμόζουμε για τις ανάγκες μιας ελλειπτικής καμπύλης που ανήκει στο σώμα $\mathcal{E}(\mathcal{F}_p)$.

4.4.1 Αλγόριθμος Πρόσθεσης και Διπλασιασμού σημείου

Ο αλγόριθμος Πρόσθεσης και διπλασιασμού σημείου είναι ένας αλγόριθμος βέλτιστης μεθόδου υπολογισμού του γραμμικού πολλαπλασιασμού. Η βασική ιδέα είναι να υπολογίσουμε την ποσότητα $k \cdot P$, όπου P ένα σημείο της Ελλειπτικής Καμπύλης και k ένα τυχαίος ακέραιος, σαν ένα άθροισμα σημείων $P_i = 2^i \cdot P$. Το ποια από τα P_i θα προστεθούν καθορίζεται από τη δυαδική αναπαράσταση του k. Δηλαδή έχουμε την παρακάτω μορφή πολλαπλασιασμού:

$$k \cdot P = (\sum k_i \cdot 2^i) \cdot P = \sum k_i \cdot P_i.$$

Ένα επίσης σημαντικό στοιχείο είναι ότι η απαιτούμενη για την υλοποίηση μνήμη που χρειάζεται ο Αλγόριθμος κυμαίνεται σε αρκετά καλό επίπεδο, αφού σε κάθε βήμα αρκεί η ταυτόχρονη αποθήκευση μόνο δύο σημείων. Η περιγραφή του αλγορίθμου δίνεται παρακάτω:

ΠΕΡΙΓΡΑΦΗ ΑΛΓΟΡΙΘΜΟΥ ΔΙΠΛΑΣΙΑΣΜΟΥ ΚΑΙ ΠΡΟΣΘΕΣΗΣ ΣΗΜΕΙΟΥ

```
1. if k_0 = 0 then R ← 0
2. else R ← P
3. for i = 1 to n − 1 do
4.        P ← 2P
5.        if k_i = 1 then R ← R + P
6. Return R
```

Είναι φανερό ότι χρειαζόμαστε $n-1$ διπλασιασμούς και $w(k)-1$ προσθέσεις, όπου το $w(k)$ αναπαριστά των αριθμό των 1 στην δυαδική αναπαράσταση του k.

4.4.2 Αναπαράσταση Προσημασμένου Ψηφίου.

Μια άλλη προσέγγιση που χρησιμοποιείται προκειμένου να μειώσουμε το πλήθος των προσθέσεων στον αλγόριθμο Διπλασιασμού και Πρόσθεσης σημείου και να επιτύχουμε μεγαλύτερο ποσοστό βελτιστοποίησης. Αυτό επιτυγχάνεται αντικαθιστώντας την χρησιμοποιούμενη δυαδική αναπαράσταση του αυθαίρετου ακεραίου k με μια αναπαράσταση η οποία έχει λιγότερους μη μηδενικούς όρους. Μιας και που η δυαδική αναπαράσταση είναι μοναδική, η εύρεση μιας αναπαράστασης με λιγότερους μη μηδενικούς όρους έχει σαν αποτέλεσμα την χρησιμοποίηση και άλλων στοιχείων διαφορετικών από το 0 και το 1. Πολλές τεχνικές έχουν προταθεί, αλλά εμείς επιλέγουμε την χρησιμοποίηση της μεθόδου που καλείται Αναπαράσταση Προσημασμένου Ψηφίου.

Ορισμός 2 *Αν* $k = \sum_{i=0}^{t} d_i 2^i$, *όπου* $d_i \in \{0, 1, -1\}$, *και* $i : 0 \leq i \leq t$, *τότε* $(d_t, d_{t-1}, d_1, d_0)_{SD}$ *καλείται μια* Αναπαράσταση Προσημασμένου Ψηφίου με Ακτίνα 2 *για τον ακέραιο* k.

Σε αντίθεση με τη δυαδική αναπαράσταση, η αναπαράσταση προσημασμένου ψηφίου ενός ακεραίου δεν είναι μοναδική. Η μορφή της δυαδικής αναπαράστασης αποτελεί ένα παράδειγμα της μεθόδου αναπαράστασης προσημασμένου ψηφίου. Έστω ότι το k είναι ένας θετικός ακέραιος του οποίου η δυαδική αναπαράσταση έχει την γενική μορφή $(k_{t+1}k_tk_{t-1}...k_1k_0)$, με $k_{t+1} = k_t = 0$. Ο αλγόριθμος τον οποίο θα παρουσιάσουμε παρακάτω κατασκευάζει μια αναπαράσταση προσημασμένου ψηφίου για το k με πληθικό αριθμό το πολύ $t+1$ ψηφία και τον μικρότερο δυνατόν αριθμό από μη μηδενικά στοιχεία.

ΑΛΓΟΡΙΘΜΟΣ ΑΝΑΠΑΡΑΣΤΑΣΗΣ ΠΡΟΣΗΜΑΣΜΕΝΟΥ ΨΗΦΙΟΥ.

ΔΕΔΟΜΕΝΑ : Ένας θετικός ακέραιος με δυαδική αναπαράσταση $(k_{t+1}k_tk_{t-1}...k_1k_0)$, και $k_{t+1} = k_t = 0$.

ΕΞΑΓΟΜΕΝΑ: Η προσημασμένη αναπαράσταση ψηφίου $(d_t, d_{t-1}, d_1, d_0)_{SD}$ για το k.

1. $c_0 \leftarrow 0$,
2. **for** $i = 0$ **to** t **do**
3. $\quad c_{i+1} \leftarrow \lfloor \frac{(k_i + k_{i+1} + c_i)}{2} \rfloor$,
4. $\quad d_i = k_i + c_i - 2c_{i+1}$
5. **Return** $(d_t, d_{t-1}, d_1, d_0)_{SD}$

Ορισμός 3 *Μια αναπαράστασης προσημασμένου ψηφίου ενός ακεραίου k καλείται* αραιή,*(sparse), αν δεν υπάρχουν ψηφία $c_i, ci + 1, \forall i$ έτσι ώστε να είναι μη μηδενικά.*

Πόρισμα

- Κάθε ακέραιος έχει μια μοναδική αναπαράσταση προσημασμένου ψηφίου.
- Μια αραιή αναπαράσταση προσημασμένου ψηφίου έχει τον ελάχιστο αριθμό μη μηδενικών ψηφιών μεταξύ όλων των αναπαραστάσεων προσημασμένου ψηφίου για ένα ακέραιο k.
- Η αναπαράσταση ενός ακεραίου που προκύπτει από την εφαρμογή του αλγορίθμου Αναπαράστασης Προσημασμένου Ψηφίου έχει την ιδιότητα να είναι αραιή.

4.5 Βέλτιστη Μορφή Αλγορίθμου Διπλασιασμού και Πρόσθεσης σημείου

Κατά την περιγραφή του αλγορίθμου Διπλασιασμού και Πρόσθεσης σημείου στην προηγούμενη ενότητα, είχαμε επισημάνει ότι το πλήθος των προσθέσεων που πρέπει να εκτελέσει ο αλγόριθμος είναι $w(k) - 1$, όπου το $w(k)$ αναπαριστά των αριθμό των "1" στη δυαδική αναπαράσταση του k. Ωστόσο στην προηγούμενη ενότητα δείξαμε ένα βέλτιστο τρόπο αναπαράστασης της δυαδικής μορφής ενός ακεραίου. Έτσι λοιπόν με την χρησιμοποίηση της μορφής αυτής, δηλαδή της αναπαράστασης προσημασμένου ψηφίου, θα μπορούσαμε να μειώσουμε το πλήθος αυτών των προσθέσεων αα έτσι να επιτύχγουμε σημαντική μείωση στο κόστος υπολογισμού του γραμμικού πολλαπλασιασμού μεταξύ ενός σημείου της Ελλειπτικής Καμπύλης και ενός ακεραίου. Σύμφωνα με τα παραπάνω παρουσιάζουμε τον βέλτιστο αλγόριθμο Διπλασιασμού και Πρόσθεσης σημείου, δεδομένου ότι ο ακέραιος k αυτή την φορά είναι σε μορφή προσημασμένου ψηφίου, δηλαδή $k = \sum_{i=0}^{t} d_i 2^i$, όπου $d_i \in \{0, 1, -1\}, 0 \leq i \leq t$.

1. $R \leftarrow 0$
2. **if** $k_0 = 1$ **then** $R \leftarrow P$
3. **if** $k_0 = -1$ **then** $R \leftarrow -P$
4. **for** $i = 1$ **to** $n-1$ **do** $P \leftarrow 2P$
5. **if** $k_i = 1$ **then** $R \leftarrow R + P$
6. **if** $k_i = -1$ **then** $R \leftarrow R - P$
7. **Return** R

Όπως και στην απλή περίπτωση του αλγόριθμου Διπλασιασμού και Πρόσθεσης Σημείου χρειαζόμαστε $n-1$ διπλασιασμούς και $w(k)-1$ προσθέσεις. Ωστόσο, σε αυτή την περίπτωση έχουμε ότι $w(k) \leq \lceil \frac{(n+1)}{2} \rceil$. Επίσης, έχουμε να υπολογίζουμε το $-P$ το οποίο όμως είναι αμελητέο σε σχέση με το κόστος μιας πρόσθεσης που θα έπρεπε να κάνουμε επιπλέον αν χρησιμοποιούσαμε την απλή δυαδική αναπαράσταση.

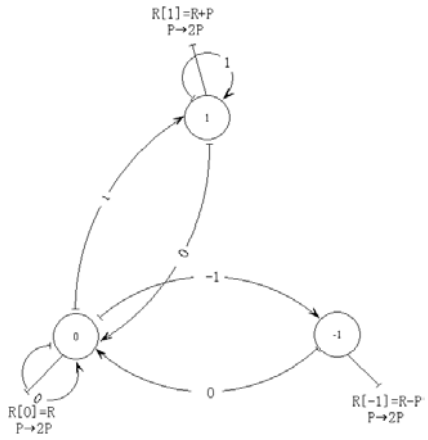
4.6 Ανάλυση βάση της Κατανάλωσης Ρεύματος

Οι επιθέσεις ανάλυσης ρεύματος είναι επιθέσεις που βασίζονται το γεγονός ότι η στιγμιαία κατανάλωση ισχύος μιας συσκευής υλικού, συσχετίζεται με τις στιγμιαία υπολογιζόμενες εντολές εκτέλεσης και την αντίστοιχη επεξεργασία δεδομένων. Μια ανειδίκευτη εφαρμογή ενός διπλασιασμού ή πρόσθεσης σημείου μίας ελλειπτικής καμπύλης, μπορεί επομένως να χρησιμοποιηθεί εύκολα για να πραγματοποιηθεί μια απλή επίθεση ρεύματος, ή μιας απλής ανάλυσης φάσματος του ηλεκτρικού ρεύματος, `Short SPA`. Ένας εχθρός προκειμένου να υλοποιήσει τις παραπάνω μορφές επιθέσεων, απλά πρέπει να παρακολουθεί στις συσκευές, στη δική μας περίπτωση την κάρτα και τον τερματικό - αναγνώστη, την κατανάλωση του ρεύματος και να αναγνωρίζει το ίχνος της ενέργειας που αντιστοιχεί στις προσθέσεις και τους διπλασιασμούς των σημείων της Ελλειπτικής καμπύλης. Αυτή η διαδικασία είναι ικανή να φανερώσει στοιχεία σχετικά με το ιδιωτικό κλειδί κάτι το οποίο θα ήταν καταστροφικό για την υλοποίηση του αλγορίθμου ταυτοποίησης και αναγνώρισης, και πολύ περισσότερο για την κρυπτογράφηση των δεδομένων. Έτσι λοιπόν, είναι φανερό, ότι προκειμένου να μπορεί να υπάρχει υψηλή στάθμη ασφάλειας σχετικά με επιθέσεις που έχουν να κάνουν με την ανάλυση της ένταση του ηλεκτρικού ρεύματος που καταναλώνεται, πρέπει ο αλγόριθμος που υλοποιείται να αποφεύγει τις διακλαδώσεις που εξαρτώνται από τα δεδομένα, `Data Depended Brances`. Για αυτό το λόγο προσαρμόζουμε την μορφή του παραπάνω αλγορίθμου Πρόσθεσης και Διπλασιασμού σημείου.

Τροποποίηση του βέλτιστου Αλγορίθμου Διπλασιασμού και Πρόσθεσης για την αποφυγή της ανάλυσης της ένταση του ηλεκτρικού ρεύματος.

1. $R[0] \leftarrow P$
2. **for** $i = n-2$ **to** 0
3. $R[0]$=$2R[0]$
4. $R[1]$=$R[0] + P$
5. $R[-1]$=$R[0] - P$
6. $R[0] = \mathrm{R}[k_i]$
7. **Return** $R[0]$

Παρακάτω δίνουμε σε μορφή μηχανής πεπερασμένων καταστάσεων τη δομή του παραπάνω αλγορίθμου:



Σχήμα 4.3: Η μηχανή πεπερασμένων καταστάσεων του SPA αλγορίθμου Πρόσθεσης και Διπλασιασμού Σημείου

4.7 Βασικά στοιχεία

4.7.1 Τάξη σώματος

Έστω E είναι μια Ελλειπτική Καμπύλη πάνω από ένα σώμα $\mathcal{F}_q$. Το θεώρημα του Hasse δηλώνει ότι ο αριθμός των σημείων μιας Ελλειπτικής Καμπύλης, περιλαμβανομένου του Επ' Απειρου σημείου είναι:

$$\#\mathcal{E}(\mathcal{F}_q) = q + 1 - t$$

όπου

$$t \leq 2\sqrt{q}.$$

Το σύμβολο $\#\ \mathcal{E}(\mathcal{F}_q)$ το ονομάζουμε Τάξη της E και το t το ονομάζουμε Ίχνος της E. Με άλλα λόγια, η Τάξη μιας Ελλειπτικής Καμπύλης $\mathcal{E}(\mathcal{F}_q)$ είναι σχεδόν ίδια με το μέγεθος q του σώματος.

Δομή σώματος

Η ομάδα $\mathcal{E}(\mathcal{F}_q)$ είναι μια αβελιανή ομάδα τάξης 1, ή 2. Αυτό σημαίνει ότι η $\mathcal{E}(\mathcal{F}_q)$ είναι ισόμορφη με το καρτεσιανό γινόμενο $\mathcal{Z}_{n1} \times \mathcal{Z}_{n2}$, όπου n_2 διαιρεί το n_1, για θετικούς ακεραίους n_1, n_2. Με $\mathcal{Z}_n$, συμβολίζουμε την κυκλική ομάδα τάξης n. Επιπλέον το n_2 διαιρεί το $q-1$. Αν το $n_2 = 1$ τότε η $\mathcal{E}(\mathcal{F}_q)$ ονομάζεται κυκλική. Τότε λέμε ότι η $\mathcal{E}(\mathcal{F}_q)$ είναι ισόμορφη με το $\mathcal{Z}_{n1}$ και υπάρχει σημείο $P \in \mathcal{E}(\mathcal{F}_q)$ τέτοιο ώστε

$$\mathcal{E}(\mathcal{F}_q) = \{\kappa P : 0 \leq \kappa \leq n_1 - 1\}.$$

Το σημείο αυτό ονομάζεται γεννήτορας της $\mathcal{E}(\mathcal{F}_q)$.

Κεφάλαιο 5

Παράμετροι Χώρου

Προκειμένου να διευκολύνουμε τη διαλειτουργικότητα, μερικοί περιορισμοί προστίθενται στο υποκείμενο σώμα διάστασης q καθώς και στην αναπαράσταση που χρησιμοποιείται για τα στοιχεία του $\mathcal{F}_q$. Επιπλέον προκειμένου να αποφύγουμε κάποιες συγκεκριμένες − γνωστές επιθέσεις, τοποθετούνται κάποιοι περιορισμοί τόσο στην Ελλειπτική Καμπύλη όσο και στην τάξη του σημείου βάσης της Ελλειπτικής Καμπύλης, δηλαδή του επιλεγμένου εκείνου σημείου της Ελλειπτική Καμπύλη με τις κατάλληλες ιδιότητες τις οποίες θα περιγράψουμε παρακάτω.

5.1 Απαιτήσεις Χώρου

Η τάξη του υποκείμενου χώρου πρέπει είτε να είναι ένας περιττός πρώτος αριθμός p, είτε μια δύναμη του 2 δηλαδή της μορφής $q = 2^m$.

Στην περίπτωση κατά την οποία το q είναι ένας περιττός πρώτος αριθμός p, τότε το υποκείμενο πεδίο είναι το $\mathcal{F}_p$, δηλαδή όλοι οι ακέραιοι *modulo p*, ενώ στην περίπτωση που το $q = 2^m$, το υποκείμενο πεδίο είναι το $\mathcal{F}_{2^m}$ του οποίου τα στοιχεία αναπαρίστανται ως προς ένα ανάγωγο πολυώνυμο τάξης m, είτε ως προς μια κανονική βάση.

5.2 Απαιτήσεις Ελλειπτικής Καμπύλης

Προκειμένου να αποφύγουμε τις επιθέσεις `Pohlig − Hellman`,[PHe78] και `Pollard's Rho`,[Pol78] σχετικά με το πρόβλημα του Διακριτού Λογάριθμου για τις Ελλειπτικές Καμπύλες, είναι αναγκαίο το πλήθος των σημείων της Ελλειπτικής Καμπύλης να διαιρείται από ένα αρκετά μεγάλο πρώτο αριθμό n. Ένα ικανοποιητικό δείγμα μεγέθους για το n είναι $n > 2^{160}$. Έχοντας κατασκευάσει το υποκείμενο πεδίο $\mathcal{F}_q$, το n θα πρέπει να επιλεγεί κατά τέτοιο τρόπο ώστε να είναι όσον το δυνατόν μεγαλύτερο γίνεται, δηλαδή $n \approx q$, έτσι ώστε η τάξη $\# \mathcal{E}(\mathcal{F}_q)$ να είναι σχεδόν πρώτος αριθμός. Στη συνέχεια θα θεωρούμε ότι το $n > 2^{160}$ και ότι $n > 4 \cdot \sqrt{q}$. Ορίζουμε επίσης τον όρο $h = \frac{\#\mathcal{E}(\mathcal{F}_q)}{n}$ τον οποίο καλούμε και συμπαράγοντα `(co−factor)`.

Κάποιες επιπλέον προφυλάξεις πρέπει να παρθούν σχετικά με την επιλογή της Ελλειπτικής Καμπύλης. Προκειμένου να αποφύγουμε τους Αλγόριθμους Απαλοιφής του `Menezes, Okamoto, Vanstone`,[MOV93], `Frey` και `Ruck`,[FrRu94], η

καμπύλη δεν πρέπει να είναι Υπεργραμμική,(Super Singular), (Δηλαδή το p να μην διαιρεί (q+1-# $\mathcal{E}(\mathcal{F}_q)$). Πιο γενικά θα λέγαμε ότι θα έπρεπε να διασφαλιστεί το γεγονός ότι τάξη n,του σημείου δεν διαιρεί το $q^k - 1$ για όλα τα $1 \leq k \leq C$, όπου C είναι αρκετά μεγάλο ώστε να είναι αδύνατος ο υπολογισμός του Διακριτού Λογάριθμου στο $\mathcal{F}_q^C$. *Στην πράξη το $C = 20$ είναι αρκετό.*

Τέλος για την αποφυγή της επίθεσης του Semaev[Sem98], Smart[Sma99], Satoh και Araki [SAr98] που αναφέρονται σε $\mathcal{F}_q$ − Ανώμαλες Καμπύλες. Έτσι η Καμπύλη δεν πρέπει να είναι $\mathcal{F}_q$ − Ανώμαλη, δηλαδή

$$(\#\mathcal{E}(\mathcal{F}_q) \neq q)$$

.

Ένας τρόπος ώστε να διασφαλιστούμε από αυτές τις επιθέσεις είναι να επιλέξουμε την Ελλειπτική Καμπύλη $\mathcal{E}$ τυχαία, με την προϋπόθεση όμως ότι ικανοποιεί τον όρο ότι η τάξη της # $[\mathcal{E}(\mathcal{F}_q)]$ διαιρείται από ένα μεγάλο πρώτο αριθμό. Η πιθανότητα για μια τυχαία Ελλειπτική Καμπύλη να υποκύψει σε τέτοιες επιθέσεις ειδικού σκοπού είναι αμελητέα. Μια καμπύλη μπορεί να επιλεγεί τυχαία με το να επιλεχθούν οι συντελεστές της να αποτελούν τα εξαγόμενα μιας μονόδρομης Συνάρτησης όπως για παράδειγμα η συνάρτηση Κατακερματισμού SHA−1.

Ανακεφαλαίωση των Παραμέτρων Πεδίου

Οι Παράμετροι του Πεδίου αποτελούνται από:

- Ένα πεδίο μεγέθους q, όπου $q = p$ ή $q = 2^m$.
- Μια ένδειξη FR (Field Representation) Αναπαράσταση Πεδίου σχετικά με το πως θα αναπαρίστανται τα στοιχεία του χώρου $\mathcal{F}_q$. Αν δηλαδή πρόκειται για τον χώρο $\mathcal{F}_{2^m}$, τότε με το FR δηλώνουμε το είδος της αναπαράστασης των στοιχείων είτε ως προς Πολυωνυμική είτε ως προς Κανονική Βάση.
- Δύο στοιχεία του χώρου $\alpha, b \in \mathcal{F}_q$ τα οποία καθορίζουν την εξίσωση της Ελλειπτικής Καμπύλης $\mathcal{E}$ πάνω από το $\mathcal{F}_q$.
  (Στην περίπτωση όπου $p > 3y^2 = x^3 + \alpha \cdot x + b$ και $p = 2y^2 + x \cdot y = x^3 + \alpha \cdot x + b$,.
- Δύο στοιχεία του χώρου x_G και $y_G \in \mathcal{F}_q$ τα οποία ορίζουν ένα σημείο $G = (x_G, y_G)$ τάξης πρώτου αριθμού στο $\mathcal{E}(\mathcal{F}_q)$.
- Η τάξη n του σημείου G με $n > 2^{160}$ και $n > 4 \cdot \sqrt{q}$ και τέλος.
- Και ο συμπαράγοντας $h = \frac{\#\mathcal{E}(\mathcal{F}_q)}{n}$.

5.2.1 Επισημοποίηση Παραμέτρων Πεδίου

Το σύνολο παραμέτρων πεδίου $(q, FR, \alpha, b, P = (x_P, y_P), n, h)$ μπορεί να εξακριβωθεί αν τηρεί τις παραπάνω απαιτήσεις βάσει της διαδικασίας που ονομάζεται Επισημοποίηση Παραμέτρων Πεδίου.

- Επιβεβαίωση ότι το q είναι πρώτη δύναμη.
- Επιβεβαίωση ότι το FR (Field Representation) Αναπαράσταση Πεδίου είναι σωστή.

- Επιβεβαίωση ότι τα στοιχεία του χώρου $\alpha, b \in \mathcal{F}_q$ και ότι καθορίζουν την εξίσωση μιας `Non - Singular` Ελλειπτικής Καμπύλης $\mathcal{E}$ πάνω από το $\mathcal{F}_q$. Δηλαδή ότι $(4\alpha^3 + 27b^2 \neq 0)$ στην περίπτωση όπου $p > 3$ και $b \neq 0$ στην περίπτωση που $p = 2$.
- Επιβεβαίωση ότι το P ικανοποιεί την εξίσωση της Ελλειπτικής Καμπύλης και ότι $P \neq 0$.
- Επιβεβαίωση ότι το $n > 2^{160}$ και $n > 4 \cdot \sqrt{q}$.
- Επιβεβαίωση ότι $n \cdot P = 0$
- Υπολογισμός της ποσότητας $h' = \lfloor \frac{(sqrtq+1)^2}{n} \rfloor$ και επιβεβαίωση ότι $h = h'$.
- Προκειμένου να υπάρχει προστασία κατά των γνωστών επιθέσεων σε Ελλειπτικές Καμπύλες, πρέπει να διασφαλιστεί ότι το n δεν διαιρεί το $q^k - 1$ για κάθε $1 \leq k \leq 20$ και ότι $n \neq q$.

5.3 Δημιουργία Ελλειπτικής Καμπύλης με τυχαίο Τρόπο

Η παράγραφος αυτή περιγράφει τον τρόπο δημιουργίας μιας Ελλειπτικής Καμπύλης με τυχαίο τρόπο. Οι ορισμένες παράμετροι της Καμπύλης καθορίζονται να είναι τα εξαγόμενα μιας μονόδρομης κατακερματικής συνάρτησης της `SHA-1`, (όπως καθορίζεται από το `FIPS 180-1`). Το εισαγόμενο δεδομένο, το οποίο καλούμε και σπόρο (`seed`), παίζει και τον ρόλο της απόδειξης, (κάτω από την υπόθεση ότι η συνάρτηση δεν μπορεί να αντιστραφεί), στο ότι η Ελλειπτική Καμπύλη πράγματι δημιουργήθηκε με τυχαίο τρόπο. Αυτό αποτελεί μια επιβεβαίωση ότι για τον χρήστη της Ελλειπτικής Καμπύλης ότι η οντότητα που δημιούργησε την καμπύλη δεν την έκανε μια σκόπιμα άδύναμη' Ελλειπτική Καμπύλη, η οποία τελικά θα οδηγούσε στην εύρεση του ιδιωτικού κρυφού κλειδιού του χρήστη.

5.3.1 Η Περίπτωση όπου q=p

Ο παρακάτω συμβολισμός χρησιμοποιείται: $t = \lceil log_2 p \rceil, s = \lfloor (t-1)/160 \rfloor$, $u = t - 160s$

Αλγόριθμος 1 : Δημιουργία Ελλειπτικής Καμπύλης με τυχαίο τρόπο στο F_p.

Εισοδος: Το μέγεθος του πεδίου p, όπου p είναι ένας περιττός πρώτος αριθμός.

Εξοδος: Μια ακολουθία από bits το οποίο ονομάζουμε **seedE** μήκους τουλάχιστον 160 bits και στοιχεία του χώρου $\alpha, \beta \in F_p$, τα οποία ορίζουν μια ελλειπτική καμπύλη E στο F_p.

1. Επέλεξε μία αυθαίρετη ακολουθία από bits, **seedE** με μήκος $g \geq 160$ bits.
2. Υπολόγισε την ποσότητα H= SHA-1(**seedE**) και έστω ότι c_0 συμβολίζει την ακολουθία από bits μήκους u η οποία προέρχεται λαμβάνοντας τα u δεξιότερα bits του H.
3. Έστω ότι με W_0 συμβολίζουμε την ακολουθία από bits μήκους u η οποία προέρχεται θέτοντας το αριστερότερο bit του c_0 ίσο με 0. (Με αυτόν τον τρόπο εξασφαλίζουμε ότι $r < p$.)

4. Έστω z ο ακέραιος του οποίου η δυαδική αναπαράσταση δίνεται από την $g-bit$ ακολουθία από bits, **seedE**.

5. Για i από 1 έως s επανέλαβε:

   5.1 Έστω s_i η $g-bit$ ακολουθία από bits, του οποίου είναι η δυαδική αναπαράσταση του ακεραίου $(z+i)mod2^g$.

   5.2 Υπολόγισε $W_i = SHA-1(s_i)$

6. Έστω W να είναι η ακολουθία από bits που προέρχεται από την συνένωση των $W_0, W_1, ..., W_s$ ως εξής $W = W_0||W_1||...||W_s$.

7. Έστω r να είναι ο ακέραιος του οποίου η δυαδική αναπαράσταση δίνεται από το W.

8. Αν $r = 0$ ή $4r + 27 \equiv 0$ τότε πήγαινε στο βήμα 1.

9. Επέλεξε αυθαίρετα $\alpha, \beta \in F_p$, όχι και τα δύο μηδέν τέτοια ώστε

$$r\beta^2 \equiv \alpha^3 modp.$$

   (Για παράδειγμα κάποιος μπορεί να επιλέξει $\alpha = r$ και $\beta = r$).

10. Η Ελλειπτική καμπύλη που επιλέγεται πάνω από το F_p είναι

$$E : y^2 = x^3 + \alpha x + \beta$$

11. Εξαγόμενο(**seedE**,α, β).

Παρουσιάζουμε στη συνέχεια ένα αλγόριθμο ο οποίος πιστοποιεί ότι η Ελλειπτική Καμπύλη όντως δημιουργήθηκε με τυχαίο τρόπο βάσει του αλγορίθμου 1 πάνω από το σώμα F_p.

Αλγόριθμος 2 : Πιστοποίηση δημιουργίας Ελλειπτικής Καμπύλης με τυχαίο τρόπο πάνω από το σώμα F_p.

Εισοδος:Το μέγεθος του πεδίου p, μια ακολουθία από bits **seedE** μήκους τουλάχιστον 160 bits, τα στοιχεία του χώρου $\alpha, \beta \in F_p$, τα οποία ορίζουν μια ελλειπτική καμπύλη $E : y^2 = x^3 + \alpha x + \beta$ πάνω από το F_p

Εξοδος: Αποδοχή ή Απόρριψη του ισχυρισμού ότι μια Ελλειπτική Καμπύλη Ε δημιουργήθηκε με τυχαίο τρόπο πάνω από το σώμα F_p βάσει του αλγορίθμου 1

1. Υπολόγισε την ποσότητα H= SHA-1(**seedE**) και έστω ότι c_0 συμβολίζει την ακολουθία από bits μήκους u η οποία προέρχεται λαμβάνοντας τα u δεξιότερα bits του H.

2. Έστω ότι με W_0 συμβολίζουμε την ακολουθία από bits μήκους u η οποία προέρχεται θέτοντας το αριστερότερο bit του c_0 ίσο με 0.

3. Έστω z ο ακέραιος του οποίου η δυαδική αναπαράσταση δίνεται από την μήκους $g-bit$ ακολουθία από bits, **seedE**.

4. Για i από 1 έως s επανέλαβε:

4.1 Έστω s_i η $g - bit$ ακολουθία από bits, του οποίου είναι η δυαδική αναπαράσταση του ακεραίου $(z + i) mod 2^g$.

4.2 Υπολόγισε $W_i = SHA - 1(s_i)$

5. Έστω $W^{'}$ να είναι η ακολουθία από bits που προέρχεται από τη συνένωση των $W_0, W_1, ..., W_s$ ως εξής $W^{'} = W_0||W_1||...||W_s$.

6. Έστω $r^{'}$ να είναι ο ακέραιος του οποίου η δυαδική αναπαράσταση δίνεται από το $W^{'}$.

7. Αν $r^{'}\beta^2 \equiv \alpha^3 (mod p)$ τότε Αποδοχή, αλλιώς Απόρριψη.

Ισόμορφες Κλάσεις Ελλειπτικών Καμπυλών στο F_p

Δύο Ελλειπτικές Καμπύλες

$$E_1 : y^2 = x^3 + \alpha_1 x + \beta_1$$

και

$$E_2 : y^2 = x^3 + \alpha_2 x + \beta_2$$

ορισμένες στο F_p καλούνται ισόμορφες στο F_p αν και μόνο αν

$$\exists u \in F_p, u \neq 0,$$

τέτοιο ώστε

$$\alpha_1 = u^4 \alpha_2$$

και

$$\beta_1 = u^6 \beta_2.$$

Οι ισόμορφες καμπύλες είναι ουσιαστικά ίδιες. Πιο συγκεκριμένα, αν E_1 είναι ισόμορφη με E_2, τότε τα σώματα $E_1(F_p)$ και $E_2(F_p)$ είναι ισόμορφα σαν αβελιανές ομάδες.

5.3.2 Η Περίπτωση όπου $q = 2^m$

Ο παρακάτω συμβολισμός χρησιμοποιείται: $s = \lfloor (t-1)/160 \rfloor$, και επίσης $u = m - 160s$.

Αλγόριθμος 3 : Δημιουργία Ελλειπτικής Καμπύλης με τυχαίο τρόπο στο F_{2^m}.

Εισοδος: Το μέγεθος του πεδίου $q = 2^m$.

Εξοδος: Μια ακολουθία από bits το οποίο ονομάζουμε **seedE** μήκους τουλάχιστον 160 bits και στοιχεία του χώρου $\alpha, \beta \in F_{2^m}$, τα οποία ορίζουν μια ελλειπτική καμπύλη στο F_{2^m}.

1. Επέλεξε μία αυθαίρετη ακολουθία από bits, **seedE** με μήκος $g \geq 160$ bits.

2. Υπολόγισε την ποσότητα H= SHA-1(**seedE**) και έστω ότι το β_0 συμβολίζει την ακολουθία από bits μήκους u η οποία προέρχεται λαμβάνοντας τα u δεξιότερα bits του H.

3. Έστω z ο ακέραιος του οποίου η δυαδική αναπαράσταση δίνεται από την μήκους $g - bit$ ακολουθία από bits, **seedE**.

4. Για i από 1 έως s επανέλαβε:

   4.1 Έστω s_i η $g - bit$ ακολουθία από bits, του οποίου είναι η δυαδική αναπαράσταση του ακεραίου $(z + i) mod 2^g$.

   4.2 Υπολόγισε $b_i = SHA - 1(s_i)$

5. Έστω β να είναι η ακολουθία από bits που προέρχεται από τη συνένωση των $\beta_0, \beta_1, ..., \beta_s$ ως εξής $\beta = \beta_0||\beta_1||...||\beta_s$.

6. Αν $b = 0$, τότε πήγαινε στο βήμα 1.

7. Η Ελλειπτική καμπύλη που επιλέγεται πάνω από το F_{2^m} είναι $E : y^2 = x^3 + \alpha x + \beta$.

8. Εξαγόμενο(seedE,α, β).

Όπως και στην περίπτωση όπου $q = p$, έτσι και εδώ παρουσιάζουμε ένα αλγόριθμο ο οποίος πιστοποιεί ότι η Ελλειπτική Καμπύλη η οποία δημιουργήθηκε βάσει του **Αλγόριθμου 3** έχει όντως δημιουργηθεί με τυχαίο τρόπο πάνω από το σώμα F_{2^m}.

Αλγόριθμος 4 : Πιστοποίηση δημιουργίας Ελλειπτικής Καμπύλης με τυχαίο τρόπο πάνω από το σώμα F_{2^m}.

Εισοδος: Το μέγεθος του πεδίου $q = 2^m$, μια ακολουθία από **seedE** μήκους τουλάχιστον 160 bits, τα στοιχεία του χώρου $\alpha, \beta \in F_{2^m}$, τα οποία ορίζουν μια ελλειπτική καμπύλη $E : y^2 = x^3 + \alpha x + \beta$ πάνω από το F_{2^m}

Εξοδος: Αποδοχή ή Απόρριψη του ισχυρισμού ότι μια Ελλειπτική Καμπύλη Ε δημιουργήθηκε με τυχαίο τρόπο πάνω από το σώμα F_{2^m} βάσει του αλγορίθμου 3.

1. Υπολόγισε την ποσότητα H= SHA-1(seedE) και έστω ότι β_0 συμβολίζει την ακολουθία από bits μήκους u η οποία προέρχεται λαμβάνοντας τα u δεξιότερα bits του H.

2. Έστω z ο ακέραιος του οποίου η δυαδική αναπαράσταση δίνεται από την $g - bit$ ακολουθία από bits, **seedE**.

3. Για i από 1 έως s επανέλαβε:

   3.1 Έστω s_i η $g - bit$ ακολουθία από bits, του οποίου είναι η δυαδική αναπαράσταση του ακεραίου $(z + i) mod 2^g$.

   3.2 Υπολόγισε $\beta_i = SHA - 1(s_i)$

4. Έστω $\beta^{'}$ να είναι η ακολουθία από bits που προέρχεται από τη συνένωση των $\beta_0, \beta_1, ..., \beta_s$ ως εξής $\beta^{'} = \beta_0||\beta_1||...||\beta_s$.

5. Αν $\beta = \beta^{'}$ τότε Αποδοχή, αλλιώς Απόρριψη.

Ισόμορφες Κλάσεις Ελλειπτικών Καμπυλών στο F_{2^m}

Δύο Ελλειπτικές Καμπύλες

$$E_1 : y^2 = x^3 + \alpha_1 x + \beta_1$$

και

$$E_2 : y^2 = x^3 + \alpha_2 x + \beta_2$$

ορισμένες στο F_{2^m} καλούνται ισόμορφες στο F_{2^m} αν και μόνο αν $\beta_1 = \beta_2$ και $Tr(\alpha_1) = Tr(\alpha_2)$, όπου Tr είναι η συνάρτηση ίχνους πάνω στο F_{2^m}, δηλαδή $Tr : F_{2^m} \to F_{2^m}$, ορισμένη από την απεικόνιση

$$Tr(\alpha) = \alpha + \alpha^2 + \alpha^{2^2} + ... + \alpha^{2^{m-1}}.$$

Οι ισόμορφες καμπύλες είναι ουσιαστικά ίδιες. Πιο συγκεκριμένα, αν E_1 είναι ισόμορφη με E_2, τότε τα σώματα $E_1(F_p)$ και $E_2(F_p)$ είναι ισόμορφα σαν αβελιανές ομάδες.

5.4 Δημιουργία Ελλειπτικής Καμπύλης βάσει του Complex Multiplication

Μια άλλη μέθοδος για τη δημιουργία κατάλληλων Ελλειπτικών Καμπυλών είναι η μέθοδος του `Complex Multiplication`. Η μέθοδος αυτή επιλέχθηκε για τη δική μας υλοποίηση, και προτιμήθηκε έναντι των άλλων μεθόδων της παραγράφου [§4.3] γιατί παρέχει τα ίδια επίπεδα ασφάλειας, χωρίς όμως η πολυπλοκότητα της να είναι τόσο μεγάλη. Για παράδειγμα αυτή η μέθοδος δεν έχει την ανάγκη εισαγωγής συναρτήσεων Κατακερματισμού που αυξάνουν κατά πολύ τις καθυστερήσεις, δεν έχουν την ανάγκη αρχικού σπόρου, (**seed**), και γενικότερα έχει πιο βέλτιστη υλοποίηση. Όταν βρισκόμαστε στο σώμα F_p ή μέθοδος καλείται και `Atkin - Morain`, [Mor91] μέθοδος, ενώ όταν βρισκόμαστε στο σώμα F_{2^m} καλείται `Lay-Zimmer`, [LZi94] μέθοδος. Έστω E μια όχι υπεργραμμική, `non-Supersingular`, Ελλειπτική Καμπύλη πάνω στο σώμα F_P τάξης u. Με τον όρο όχι υπεργραμμική, εννοούμε ότι το p δεν διαιρεί την ποσότητα $(q + 1 - \#E(F_q))$, όπου $\#E(F_q)$ είναι η τάξη της Ελλειπτικής Καμπύλης, δηλαδή το πλήθος των σημείων που την αποτελούν συμπεριλαμβανομένου του Επ Άπειρον σημείου. Η ποσότητα $Z = 4q - (q + 1 - u)^2$ είναι θετική, εξαιτίας του ορίου του `Hasse`, έτσι έπεται ότι υπάρχει μοναδική παραγοντοποίηση

$$Z = DV^2,$$

όπου D είναι ένας αριθμός ελεύθερος τετραγώνου, δεν περιέχει δηλαδή παράγοντες που είναι τέλεια τετράγωνα.

Ορισμός 1 *Για κάθε όχι υπεργραμμική Ελλειπτική Καμπύλη πάνω από το F_q τάξης u, υπάρχει ένας μοναδικός, θετικός, ελεύθερος τετραγώνου, ακέραιος D τέτοιος ώστε:*

$$4q = W^2 + DV^2 (*),$$

$$u = q + 1 \pm W (**)$$

για κάποια W και V.

Έτσι λέμε ότι η E ελλειπτική καμπύλη έχει έναν `Complex Multiplication` από το D, (ή πιο σαφώς από το $\sqrt{-D}$). Το D καλείται `CM` διακρίνουσα, `(CM discriminant)` για το q. Αν κάποιος γνωρίζει το D για μία δεδομένη Ελλειπτική Καμπύλη E, τότε μπορεί μέσω των $(*)$, $(**)$ να υπολογίσει και την τάξη της. Παρόλο που είναι δυνατόν (πάνω από το F_p), να επιλέξουμε πρώτα την τάξη και μετά το πεδίο στο οποίο θα ορισθεί η Ελλειπτική Καμπύλη, είναι προτιμότερο να επιλέγουμε πρώτα το πεδίο, αφού υπάρχουν πεδία στα οποία οι πράξεις γίνονται με βέλτιστο τρόπο.

Δύο είναι τα βασικά βήματα που εκτελούνται:

1. Η εύρεση μιας κατάλληλης τάξης.
2. Η κατασκευή της καμπύλης που θα έχει αυτή την τάξη.

Πιο συγκεκριμένα κάποιος ξεκινά επιλέγοντας το επιθυμητό μέγεθος του πεδίου q, την ελάχιστη τάξη, r_{min}, του σημείου βάσης, και ένα δοκιμαστικό όριο διαχωρισμού l_{max}. Δεδομένων αυτών των ποσοτήτων, το D καλείται *κατάλληλο* αν υπάρχει μια ελλειπτική καμπύλη πάνω από το F_q με `CM` του D που να έχει τάξη σχεδόν πρώτο αριθμό.

Βήμα 1° Εύρεση τάξης που είναι σχεδόν πρώτος αριθμός:
Εύρεση κατάλληλου D. Όταν βρεθεί τέτοιο D, κατέγραψε το D, το μεγάλο πρώτο αριθμό r, και τον θετικό ακέραιο k, τέτοιο ώστε η ποσότητα $u = kr$ να είναι η τάξη της καμπύλης και επιπλέον να είναι και σχεδόν πρώτος αριθμός.

Βήμα 2° Κατασκευή Καμπύλης και σημείου:
Δεδομένου του D, k, r κατασκεύασε μια Ελλειπτική Καμπύλη πάνω από το F_q και ένα σημείο τάξης r.

Η αναλυτικότερη και πλήρης περιγραφή αυτού του τρόπου δημιουργίας μιας Ελλειπτικής Καμπύλης και η επιλογή του κατάλληλου σημείου υπάρχουν στο πρότυπο `P1363`, το οποίο αποτελεί το πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού και το οποίο βασίζεται σε τρεις οικογένειες συστημάτων:

- Συστήματα Διακριτού Λογάριθμου.
- Συστήματα Διακριτού Λογάριθμου Ελλειπτικών Καμπυλών.
- Συστήματα Παραγοντοποίησης Ακεραίων.

5.5 Το Πρόβλημα του Διακριτού Λογάριθμου στις Ελλειπτικές Καμπύλες

5.5.1 Εισαγωγή

Αυτή η ενότητα παρέχει τη διατύπωση του Προβλήματος του Διακριτού Λογάριθμου στις Ελλειπτικές Καμπύλες, καθώς και σύγχρονους αλγόριθμους για την επίλυση του προβλήματος αυτού. Παράλληλα παρουσιάζουμε ποιες συνθήκες πρέπει να τηρούνται προκειμένου το συγκεκριμένο πρόβλημα να είναι δύσκολο να επιλυθεί.

5.5.2 Το πρόβλημα του Διακριτού Λογαρίθμου

Μιλώντας γενικά, θα λέγαμε πως το πρόβλημα του Διακριτού Λογαρίθμου είναι ουσιαστικά το πρόβλημα της αντιστροφής της εκθετικής διαδικασίας. Το πρόβλημα αυτό μπορεί να τεθεί υπό μια ποικιλία αλγεβρικών χαρακτηριστικών, ανάλογα κυρίως με την πεπερασμένη ομάδα που χρησιμοποιείται. Αυτό που βγαίνει σαν συμπέρασμα της μελέτης του προβλήματος του Διακριτού Λογαρίθμου, είναι πως το συγκεκριμένο πρόβλημα μπορεί να είναι εύκολο ή αντίστοιχα δύσκολο να επιλυθεί, ανάλογα με την παράσταση της κυκλικής ομάδας που χρησιμοποιείται. Έτσι ο στόχος μας ανέρχεται στην εύρεση ομάδων όπου το πρόβλημα του Διακριτού Λογαρίθμου είναι δύσκολο.

Οι υποψήφιες κλάσεις ομάδων που χρησιμοποιούνται είναι:

1. Η πολλαπλασιαστική Ομάδα των πεπερασμένων σωμάτων, (GF_p).
2. Η ομάδα σημείων μιας Ελλειπτικής Καμπύλης ορισμένης στο πεπερασμένο σώμα (K=GF_p).

Ορισμός Προβλημάτων

Το πρόβλημα του Διακριτού Λογάριθμου σε ένα πεπερασμένο πεδίο F_q ορίζεται ως εξής:

Θεώρημα 1 *(DLP): Δεδομένου ενός πεπερασμένου σώματος, (GF_p), και στοιχείων $g, h \in$ (GF_p), να βρεθεί ακέραιος l τέτοιος ώστε, $g^l = h, \in GF_p$, δεδομένου ότι ένας τέτοιος ακέραιος υπάρχει.*

Το Πρόβλημα του Διακριτού Λογάριθμου στις Ελλειπτικές Καμπύλες διατυπώνεται ως ακολούθως:

Θεώρημα 2 *(ECDLP): Δεδομένης μιας Ελλειπτικής Καμπύλης $\mathcal{E}$ ορισμένης πάνω από ένα πεδίο $\mathcal{F}_q$, και ενός σημείου $P \in \mathcal{E}(\mathcal{F}_q)$ τάξης n και ενός σημείου Q το οποίο ορίζεται από τη σχέση $Q = l \cdot P$, όπου $0 \leq l \leq n-1$, να υπολογιστεί το l.*

Στην επιφάνεια τους τα δύο αυτά προβλήματα δείχνουν διαφορετικά. Το πρώτο έχει να κάνει με πολλαπλασιαστικό συμβολισμό, g^l, και αναφέρεται στη διαδικασία πολλαπλασιασμού του g με τον εαυτό του l φορές. Το δεύτερο πρόβλημα έχει να κάνει με προσθετικό συμβολισμό, $l \cdot P$ και αναφέρεται στη διαδικασία πρόσθεσης του P με τον εαυτό του l φορές.

Αν κάποιος αφήσει αυτές τις συμβολικές διαφορές στην άκρη, τότε τα δύο προβλήματα είναι τα ίδια. Το ενδιαφέρον όσον αφορά τα δύο αυτά προβλήματα είναι ότι το δεύτερο εμφανίζεται να είναι πολύ πιο δύσκολο από το πρώτο. Ο θεμελιώδης λόγος είναι ότι τα αλγεβρικά στοιχεία στο πρώτο πρόβλημα είναι εφοδιασμένα με δύο βασικές πράξεις, τον πολλαπλασιασμό και την πρόσθεση στοιχείων του χώρου ενώ αντίθετα τα αλγεβρικά στοιχεία στο δεύτερο πρόβλημα είναι εφοδιασμένα με μια μόνο βασική πράξη, την πρόσθεση σημείων της Ελλειπτικής Καμπύλης. Η επιπλέον δομή του πρώτου προβλήματος οδήγησε στην ανακάλυψη μεθόδων, `index-calculus`, οι οποίες κατέχουν υπεκθετικό χρόνο εκτέλεσης. Οι Ελλειπτικές Καμπύλες δεν περιέχουν την επιπλέον δομή και για αυτό το λόγο δεν έχουν βρεθεί μέθοδοι με υπεκθετικό χρόνο εκτέλεσης, κάνοντας τις Ελλειπτικές Καμπύλες ιδανικές για Κρυπτογραφικές Πρακτικές Εφαρμογές.

5.5.3 Γνωστές Επιθέσεις

Αυτή η ενότητα παρουσιάζει το σύνολο των γνωστών αλγορίθμων για την επίλυση του Προβλήματος του Διακριτού Λογάριθμου για τις Ελλειπτικές Καμπύλες και προτείνει τρόπους για την αποφυγή τους στην πράξη.

- Η Εξαντλητικη Αναζητηση. Η μέθοδος αυτή έχει να κάνει με τον υπολογισμό των πολλαπλάσιων του σημείου P, δηλαδή ο υπολογισμός των ποσοτήτων $P, 2P, 3P, 4P, ...$ μέχρι να αποκτηθεί το Q. Αυτή απαιτεί στην χειρότερη περίπτωση n βήματα.

- Αλγοριθμος Μικρου και Μεγαλου βηματος. Αυτός ο αλγόριθμος είναι μια συνεχής ανταλλαγή, `trade off` μεταξύ χρόνου και μνήμης της μεθόδου της εξαντλητικής αναζήτησης. Απαιτεί αποθήκευση περίπου $\sqrt{n}$ σημείων, και ο χρόνος εκτέλεσης είναι σχεδόν $\sqrt{n}$ στην χειρότερη περίπτωση.

- Η Pollard's ρ μεθοδος. Ο αλγόριθμος αυτός, [Pol78], είναι μια πιο τυχαιοκρατική, (`randomized`), μορφή του προηγούμενου αλγορίθμου. Έχει σχεδόν τον ίδιο χρόνο εκτέλεσης ($\sqrt{\frac{\pi n}{2}}$) βήματα), αλλά απαιτεί ένα σχεδόν αμελητέο ποσοστό αποθήκευσης.

- Κατανεμημενη μορφη του Pollard's ρ αλγοριθμου. Ο `Van Oorschot` και ο `Wiener`, [VWi99], έδειξαν πως ο παραπάνω αλγόριθμος μπορεί να εκτελεστεί παράλληλα από m επεξεργαστές. Τότε, ο χρόνος εκτέλεσης γίνεται $\frac{\sqrt{\pi n}}{2m}$ βήματα. Αυτή η κατανεμημένη μορφή αποτελεί και τον γρηγορότερο αλγόριθμο γενικού σκοπού για την επίλυση του `ECDLP`.

- Ο Αλγοριθμος του Pohlig Hellamn. Αυτός ο αλγόριθμος, [PoHel78], εκμετελεύτεται την παραγοντοποίηση του n, την τάξη του σημείου P. Ο αλγόριθμος αυτός ανάγει το πρόβλημα της εύρεσης του l στο πρόβλημα εύρεσης του l modulo κάθε φορά τον παράγοντα του n. Το επιθυμητό l θα υπολογιστεί βάσει του Θεωρήματος Υπολοίπου του Κινέζου, `Chinese Remainder Theorem`.

  Προκειμένου να κατασκευάσουμε την ποιο δύσκολη μορφή του προβλήματος του Διακριτού Λογάριθμου στις Ελλειπτικές Καμπύλες `ECDLP` πρέπει να επιλέξουμε ελλειπτική καμπύλη της οποίας η τάξη να διαιρείται από ένα μεγάλο πρώτο αριθμό n. Θα ήταν προτιμότερο η τάξη της Ελλειπτικής Καμπύλης να είναι πρώτος αριθμός, ή σχεδόν πρώτος αριθμός, με μορφή ένας μεγάλος πρώτος n επί ένα μικρό ακέραιο h.

- Η Pollard's λ μεθοδος. Ο αλγόριθμος αυτός, [Pol78], όπως και αυτός της ρ μεθόδου είναι μια πιο τυχαιοκρατική, `randomized` μορφή του Pollard αλγορίθμου. Αυτός ο αλγόριθμος έχει επίσης τη δυνατότητα να εκτελεστεί κατανεμημένα, με γραμμική επιτάχυνση, `linear speedup`, ωστόσο είναι λίγο πιο αργός από την Κατανεμημένη μορφή του `Pollard's` ρ αλγορίθμου, `[VWi99]`. Υπάρχουν βέβαια κάποιες περιπτώσεις κατά τις οποίες η μέθοδος λ είναι πιο γρήγορη και αυτές έχουν να κάνουν με το όταν ο λογάριθμος γνωρίζουμε ότι βρίσκεται στην περιοχή $[0, b] \subset [0, n-1], b < 0.39n$

- Πολλαπλοι Αλγοριθμοι. Ο `R.Silvermann` και ο `Stapleton` [SSt97], παρατήρησαν ότι αν μια συγκεκριμένη μορφή, `instance`, του `ECDLP`, (για συγκεκριμένη Ελλειπτική Καμπύλη E, και συγκεκριμένο σημείο P), βρεθεί μια λύση βάσει της κατανεμημένης μορφής του `Pollard's` ρ αλγορίθμου, τότε η δουλειά που έχει γίνει μπορεί να βοηθήσει στο να επιταχυνθεί η επίλυση άλλων

στιγμιότυπων του ECDLP για την ίδια Ελλειπτική Καμπύλη και σημείο. Πιο συγκεκριμένα, η επίλυση k στιγμιότυπων instances του ECDLP (για συγκεκριμένη Ελλειπτική Καμπύλη E, και συγκεκριμένο σημείο P), χρειάζεται $\sqrt{k}$ της δουλειάς που χρειάζεται να επιλυθεί για ένα στιγμιότυπο του ECDLP. Ωστόσο αυτή η ανάλυση δεν λαμβάνει υπόψη τις απαιτήσεις σε αποθηκευτικό χώρο.

- Supersingular Καμπυλες. Ο Menezes[Men93], και Okamoto, Vanstone [MOV93] και αργότερα ο Frey και Ruck [FR94] έδειξαν πως κάτω από κάποιους ήπιους περιορισμούς, το ECDLP για μια Ελλειπτική Καμπύλη που είναι ορισμένη πάνω από ένα πεπερασμένο πεδίο F_q, μπορεί να αναχθεί στο πιο εύκολο DLP σε κάποιες επεκτάσεις πεδίων του F_q^B, για κάποιο $B \geq 1$, όπου ο number sieve αλγόριθμος εφαρμόζει. Ο αλγόριθμος απαλοιφής είναι πρακτικός εάν το B είναι μικρό. Προκειμένου να διασφαλίσουμε ότι ο απαλοιφής αλγόριθμος δεν εφαρμόζεται σε μια συγκεκριμένη καμπύλη, πρέπει να ελέγξουμε ότι το n, η τάξη του σημείου P, δεν διαιρεί την ποσότητα $q^B - 1$ για μικρά B. Αρκεί στην πράξη να το ελέγξουμε για το διάστημα $B \in [1, \frac{2000}{log_2 q}]$.

- Ανωμαλες Καμπυλες. Ο Semaev [Sem98], *Smart* [Sma99], Satoh, και Araki [SAr98] έδειξαν ότι το ECDLP για την ειδική κλάση των ανώμαλων καμπυλών είναι εύκολο να επιλυθεί. Μια ανώμαλη καμπύλη πάνω από το σώμα F_q, είναι μια Ελλειπτική Καμπύλη πάνω από το σώμα F_q που έχει ακριβώς q σημεία. Η επίθεση δεν επεκτείνεται σε άλλες κλάσεις Ελλειπτικών Καμπυλών. Συνεπώς με το να επιβεβαιώνουμε ότι το πλήθος των σημείων μιας Ελλειπτικής Καμπύλης δεν είναι ίσο με το πλήθος των στοιχείων του υποκείμενου σώματος, μπορούμε σχετικά εύκολα να αποφύγουμε μια επίθεση αυτής της μορφής.

- Καμπυλες Ορισμενες πανω απο Μικρα σωματα. Έστω ότι η E είναι μια Ελλειπτική Καμπύλη ορισμένη πάνω από ένα πεπερασμένο πεδίο F_2^e. Οι Galland, Lampert, Vanstone [GLVmc] και οι Wiener, Zuccherato [WZu99] έδειξαν πως η Pollard's ρ μέθοδος για τον υπολογισμό Ελλειπτικών Καμπυλών στο $E(F_2^{ed})$, μπορεί να επιταχυνθεί κατά ένα παράγοντα $\sqrt{d}$, έποντας έτσι το αναμενόμενο χρόνο εκτέλεσης της Pollard's ρ μεθόδου να είναι ίσο με $(\frac{\sqrt{\frac{\pi n}{d}}}{2})$ βήματα.

- Καμπυλες Ορισμενες πανω απο το σωμα F_2^m, οπου m συνθετο. Οι Galbraith, Smart [GSm99]επεκτείνοντας τη δουλειά του Frey, [Fre98] συζητούν πως μπορεί η επίθεση του Weil να χρησιμοποιηθεί προκειμένου να λυθεί το ECDLP για Ελλειπτικές Καμπύλες ορισμένες πάνω από το σώμα F_2^m, όπου m σύνθετο. Πιο πρόσφατα οι Gaudry, Hess και ο Smart [GHS00] βελτιώσανε αυτές τις ιδέες προκειμένου να εξασφαλίσουν ένα ισχυρή απόδειξη ότι όταν το m έχει διαιρέτη μικρό αριθμό, για παράδειγμα το $l = 4$, το ECDLP επιλύεται πιο γρήγορα από ότι με την μέθοδο του Pollard.

5.5.4 Δημιουργία Ζεύγους Κλειδιών

Στο σημείο αυτό περιγράφουμε τον τρόπο με τον οποίο δημιουργούμε ένα ζεύγος Κλειδιών για την κάθε οντότητα η οποία λαμβάνει μέρος σε ένα πρωτόκολλο Συμφωνίας Κλειδιού. Έτσι δεδομένου ενός έγκυρου συνόλου παραμέτρων πεδίου όπως αυτές που έχουν ήδη περιγραφεί σε προηγούμενη παράγραφο, (δηλαδή το σύνολο της μορφής $(q, FR, \alpha, b, P, n, h)$ για το οποίο ισχύουν οι περιορισμοί με την μορφή

που τους έχουμε ήδη θέσει), ονομάζουμε ιδιωτικό κλειδί (private key) μιας οντότητας A έναν ακέραιο d ο οποίος έχει επιλεγεί τυχαία στο διάστημα $[1, n-1]$, όπου n είναι η τάξη του σημείου P. Το δημόσιο κλειδί της οντότητας A `Public Key` είναι το σημείο της Ελλειπτικής Καμπύλης το οποίο προκύπτει από τη σχέση $Q = d \cdot P$. Έτσι το ζεύγος Κλειδιών είναι το (Q, d). Κάθε φορά που εκτελείται το πρωτόκολλο ένα νέο ζεύγος Κλειδιών δημιουργείται για την κάθε οντότητα με την επιλογή διαφορετικού ακεραίου κάθε φορά, στο διάστημα $[1, n-1]$ και κατά συνέπεια διαφορετικού δημόσιου κλειδιού.

5.5.5 Επισημοποίηση Δημόσιου Κλειδιού

Πριν την χρησιμοποίηση του δημόσιου Κλειδιού Q μιας οντότητας είναι αναγκαίο να γίνει μια επικύρωση ότι το δημόσιο κλειδί κατέχει τις αριθμητικές ιδιότητες που υποτίθεται ότι έχει, δηλαδή ότι το Q να είναι ένα ορισμένο σημείο της υποομάδας που δημιουργείται από το σημείο της Ελλειπτικής Καμπύλης P. Αυτή η διαδικασία καλείται Επισημοποίηση Δημόσιου Κλειδιού `(Public Key Validation)` και έχει ως εξής:

Δεδομένου ενός έγκυρου συνόλου παραμέτρων πεδίου $(q, FR, \alpha, b, P, n, h)$ ένα δημόσιο κλειδί $Q = (x_Q, y_Q)$ μπορεί να επισημοποιηθεί με τον παρακάτω τρόπο:

- Το Q δεν είναι ίσο με τον Επ Άπειρον Σημείο 0.
- Η τεταγμένη x_Q και η τετμημένη y_Q είναι στοιχεία του $\mathcal{F}_q$. Δηλαδή έχουν την κατάλληλη αναπαράσταση για σημεία του χώρου $\mathcal{F}_q$.
- Το Q ικανοποιεί την εξίσωση της Ελλειπτικής Καμπύλης $\mathcal{E}$.
- $n \cdot Q = 0$.

5.5.6 Ενσωματωμένη Επισημοποίηση Δημόσιου Κλειδιού

Το κόστος υπολογισμού των πράξεων κατά την Επισημοποίηση Δημόσιου Κλειδιού έγκειται κυρίως στο τελευταίο βήμα όπου έχουμε τον βαθμωτό πολλαπλασιασμό. Έτσι προκειμένου να μειώσουμε το κόστος του υπολογισμού το τελευταίο βήμα, όταν η επισημοποίηση γίνεται από την μεριά της κάρτα, μπορεί να παραληφθεί κατά τη διάρκεια της Επισημοποίησης Δημόσιου Κλειδιού. Ανακεφαλαιώνοντας, δεδομένου ενός έγκυρου συνόλου παραμέτρων πεδίου $(q, FR, \alpha, b, P, n, h)$ ένα δημόσιο κλειδί $Q = (x_Q, y_Q)$ μπορεί να επισημοποιηθεί με τον παρακάτω τρόπο:

- Το Q δεν είναι ίσο με τον Επ Απειρον Σημείο 0.
- Η τεταγμένη x_Q και η τετμημένη y_Q είναι στοιχεία του $\mathcal{F}_q$. Δηλαδή έχουν την κατάλληλη αναπαράσταση για σημεία του χώρου $\mathcal{F}_q$.
- Το Q ικανοποιεί την εξίσωση της Ελλειπτικής Καμπύλης $\mathcal{E}$.

Κεφάλαιο 6

Στοιχεία Αλγορίθμου

6.1 Γενικοί Κανόνες Ασφάλειας Αλγορίθμου

Ένας ασφαλής αλγόριθμος πρέπει να έχει τη δυνατότητα να μπορεί να αντεπεξέλθει τόσο σε παθητικές επιθέσεις, δηλαδή σε επιθέσεις κατά τις οποίες ένας αντίπαλος προσπαθεί να αποτρέψει τον αλγόριθμο να πετύχει το σκοπό του, με το παρακολουθεί γνήσιες οντότητες να τον διεκπεραιώνουν, όσο και σε ενεργητικές επιθέσεις, όπου ένας αντίπαλος προσπαθεί να υπονομεύσει την επικοινωνία των οντοτήτων, είτε παραποιώντας, είτε σβήνοντας μηνύματα. Επιπλέον προκειμένου να υλοποιηθεί ένα ασφαλές Πρωτόκολλο Συμφωνίας Κλειδιών, πρέπει να ακολουθηθούν μια σειρά από *Γνωρίσματα Ασφάλειας,* τα οποία παρουσιάζονται παρακάτω:

- Ασφαλεια Γνωστου Κλειδιου. Κάθε επανάληψη του πρωτοκόλλου συμφωνίας κλειδιού μεταξύ δύο οντοτήτων A και B πρέπει να παράγει ένα μοναδικό κλειδί, το οποίο ονομάζεται Κλειδί συνεδρίασης `Session Key`. Το πρωτόκολλο πρέπει να διεξάγεται χωρίς πρόβλημα ακόμα και αν κάποιος εχθρός, `Adversary`, με κάποιον άλλον τρόπο έχει μάθει άλλα κλειδιά συνεδρίασης.
- Ελεγχος Κλειδιου. Καμία από της οντότητες δεν πρέπει να έχει τη δυνατότητα να εξαναγκάσει το κλειδί συνεδρίασης να έχει μια προκαθορισμένη τιμή.
- Αγνωστος Διαμοιρασμος Κλειδιου. Καμία από τις οντότητες δεν μπορεί να εξαναγκάζεται να μοιραστεί ένα κλειδί με μια άλλη οντότητα χωρίς τη συγκατάθεση και την γνώση της πρώτης.

Επιθυμητά Γνωρίσματα Απόδοσης Πρωτοκόλλου

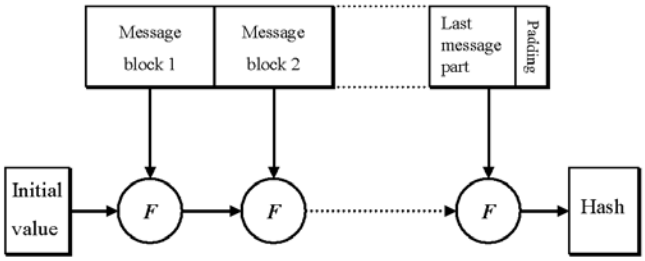
Τα γνωρίσματα αυτά, περιλαμβάνουν την χρησιμοποίηση όσον το δυνατόν μικρότερου αριθμού ανταλλαγής μηνυμάτων μεταξύ δύο οντοτήτων, κατά τη διάρκεια της διεξαγωγής του πρωτοκόλλου, καθώς και τον μικρότερο δυνατό φόρτο σε πράξεις. Κάποια άλλα γνωρίσματα τα οποία είναι χρήσιμο να υπάρχουν είναι :

- Ασυσχετιστα Μηνυματα. Δηλαδή η ασυσχέτιστη μετάδοση μηνυμάτων μεταξύ οντοτήτων.

- Κατακερματικεσ συναρτησεις (Hash Functions).

  Οι κατακερματικές συναρτήσεις είναι μαθηματικές, συνήθως μονόδρομες συναρτήσεις οι οποίες απεικονίζουν ένα μεγάλο πεδίο ορισμού domain σε ένα μικρότερο και καθορισμένο πεδίο τιμών. Ο λόγος της μονόδρομης φοράς είναι η ασφάλεια των δεδομένων. Κατά την υλοποίηση του πρωτοκόλλου της πιστοποίησης ταυτότητας που προτείνουμε στη συνέχεια, θα θεωρήσουμε ότι χρησιμοποιούμε την κατακερματική συνάρτηση - Αλγόριθμο Secure Hash Algorithm-1 η οποία περιγράφεται από το Processing Standards Publication 180-1. Ο συγκεκριμένος αλγόριθμος που θα χρησιμοποιήσουμε έχει την δυνατότητα να λαμβάνει σαν δεδομένα εισόδου οποιοδήποτε μηνύματα μεγέθους μέχρι 2^{64} δυαδικών ψηφίων και να παράγει εξαγόμενα μεγέθους 160 δυαδικών ψηφίων. Ουσιαστικά, αποτελεί μια βελτιωμένη έκδοση της έκδοσης Secure Hash Algorithm, SHA, και προτάθηκε στο [NIS94c], το $1994 - 5$. Η βελτιωμένη αυτή έκδοση, διόρθωσε μια αδημοσίευτη αδυναμία, του SHA ή οποία καθιστούσε το συγκεκριμένο αλγόριθμο ανασφαλή.

  Αναπαριστούμε στη συνέχεια σχηματικά την γενική μορφή των κατακερματικών συναρτήσεων – Αλγορίθμων προκειμένου να δώσουμε μια εικόνα του πως λειτουργούν σε γενικές γραμμές.



Σχήμα 6.1: Γενική μορφή των κατακερματικών συναρτήσεων

- Χρονοσημανση. Δηλαδή σήμανση των μηνυμάτων ως προς τον χρόνο, βάσει ενός ανεξάρτητου ρολογιού του συστήματος.

6.2 Κρυπτοσύστημα Menezes - Vanstone

Το κρυπτοσύστημα των Menezes - Vanstone, [Men95], είναι μια βέλτιστη παραλλαγή του κρυπτοσυστήματος του ElGamal, [Elg85]. Σε αυτή την παραλλαγή η Ελλειπτική καμπύλη χρησιμοποιείται σαν ¨μάσκα¨, και τα κρυπτογραφήματα, καθώς και τα καθαρά κείμενα plaintext, επιτρέπεται να είναι οποιοδήποτε ζεύγος

στοιχείων του χώρου. Εμείς ωστόσο, θα περιγράψουμε μια ελαφρώς παραλλαγμένη μορφή του κρυπτοσυστήματος των `Menezes` και `Vanstone`, από την από αυτή που προτείνεται στο [MenVan93], προκειμένου να αποφύγουμε την αδυναμία που έχει υποδείξει ο `Klaus Kiefer` στο [KKi97]. Η αδυναμία αυτή είχε να κάνει με το γεγονός ότι ο αρχικός αλγόριθμος, με την μορφή που προτάθηκε από τους `Menezes, Vanstone` [MenVan93], δεν είναι ένας αυστηρά πιθανοκρατικός αλγόριθμος. Τα κρυπτογραφήματα που έχουν προέλθει βάσει του αλγορίθμου αυτού, διαρρέουν κάποια πληροφορία η οποία μπορεί να χρησιμοποιηθεί για την μη εξουσιοδοτημένη αποκρυπτογράφηση. Η αδυναμία επιβεβαιώνεται με την χρήση του **dc test** [Kief97]. Αυτή την αδυναμία ωστόσο, κατάφερε να ξεπεραστεί χάρη στους `Araki, Satoh` και `Miura` στο [ASM98], με την εισαγωγή μόνο της x συνιστώσας του σημείου, στη διαδικασία της υλοποίησης του πρωτοκόλλου, έναντι της χρησιμοποίησης όλου του σημείου όπως αρχικά είχε ορισθεί στο [MenVan93]. Η επιλογή αυτού του Κρυπταλγορίθμου έγινε λόγω του ότι αυτός ο αλγόριθμος δεν απαιτεί τα προς κρυπτογράφηση δεδομένα να είναι σημεία της Ελλειπτικής Καμπύλης, αλλά απλά στοιχεία του Πεπερασμένου Πεδίου πάνω στο οποίο ορίζεται η Ελλειπτική Καμπύλη. Ουσιαστικά αυτό που κάνει, είναι να χρησιμοποιεί την Ελλειπτική Καμπύλη σαν μάσκα κρυπτογράφησης, προσφέροντας έτσι ένα μεγαλύτερο χώρο δυνατών `PlainText`, από αυτόν των σημείων μιας Ελλειπτικής Καμπύλης.

Παρουσιάζουμε την ελαφρώς παραλλαγμένη μορφή του Κρυπταλγόριθμου `Menezes - Vanstone`, των `Araki,Satoh` και Miura,[ASM98].

- [**Αρχικές θεωρήσεις**] Έστω $f : Z/nZ \to H$, και $t \in Z/nZ$, με $f(t) = t \times Base(Point) \in H$.
- [**Κρυφό Κλειδί**] $t \in Z/nZ$, και
  [**Δημόσιο Κλειδί**] $u = f(t) \in H$.
- [**Κρυπτογράφηση**] $m \in F_q$: καθαρό κείμενο.
  $r \in Z/nZ$: τυχαίος αριθμός τέτοιος ώστε : $x(ru) \neq 0$.
  Όπου $x()$ ή x συνιστώσα ενός σημείου.
  Ακόμα $c_1 = f(r) \in H$.
  Και $c_2 = mx(ru) \in F_q$.
- [**Κρυπτογράφημα**] του σημείου $(c_1, c_2) \in H \times F_q$.
- [**Αποκρυπτογράφηση**] $m = c_2/x(tc_1) \in F_q$

Κεφάλαιο 7

Αλγόριθμος Συμφωνίας Κλειδιών και Πιστοποίησης Ταυτότητας

7.1 Εισαγωγή στην Κρυπτογραφία

Η κρυπτογραφία είναι μια επιστήμη που βασίζεται στα μαθηματικά με σκοπό την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες, αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Το αρχικό μήνυμα ονομάζεται απλό κείμενο `plaintext`, ενώ το ακατάληπτο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται κρυπτογράφημα `ciphertext`.

Η αποκρυπτογράφηση, είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή του αντίστροφου αλγορίθμου. Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική, όταν μόνο τα άτομα που συμμετέχουν σε αυτή μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος.

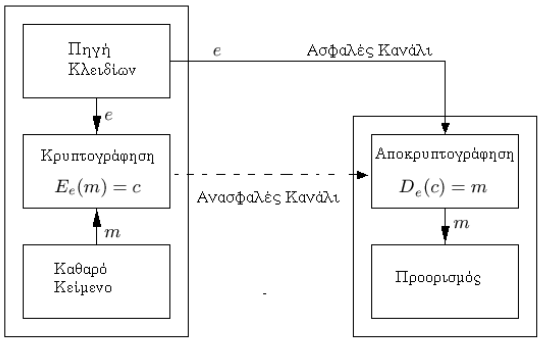
Η κρυπτογραφία δεν πρέπει να συγχέεται με την κρυπτανάλυση, που ορίζεται ως η επιστήμη για την ανάλυση και αποκωδικοποίηση κωδικοποιημένων πληροφοριών χωρίς την χρήση του αντίστροφου αλγορίθμου κρυπτογράφησης.

Ο αλγόριθμος κρυπτογράφησης είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Όσο αυξάνει ο βαθμός πολυπλοκότητας του αλγορίθμου, τόσο μειώνεται η πιθανότητα να το διαβάλλει κάποιος. Ο αλγόριθμος κρυπτογράφησης λειτουργεί σε συνδυασμό με ένα κλειδί `key`, για την κρυπτογράφηση του απλού κειμένου. Το ίδιο απλό κείμενο κωδικοποιείται σε διαφορετικά κρυπτογραφήματα όταν χρησιμοποιούνται διαφορετικά κλειδιά.

7.1.1 Ασύμμετρη και Συμμετρική Κρυπτογραφία

Συμμετρική Κρυπτογραφία

Στη συμμετρική κρυπτογραφία, χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση, όσο και για την αποκρυπτογράφηση. Επομένως, το κλειδί αυτό πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, άρα, απαιτείται ασφαλές μέσο για τη μετάδοσή του, για παράδειγμα μία προσωπική συνάντηση κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική.



Σχήμα 7.1: Σχηματική Παράσταση Συμμετρικής Κρυπτογραφίας

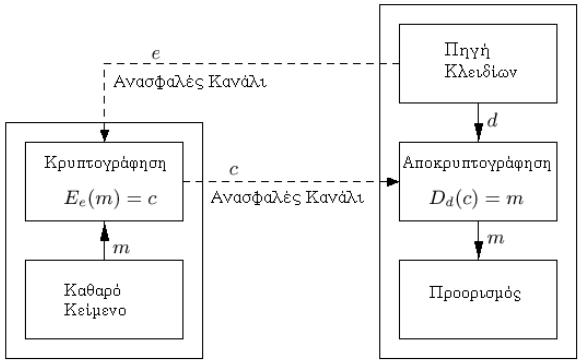
Υπάρχουν αρκετοί αλγόριθμοι που ανήκουν στην κατηγορία αυτή, με περισσότερο γνωστό τον `Data Encryption Standard (DES)`, ο οποίος αναπτύχθηκε αρχικά από την `IBM` και υιοθετήθηκε το 1977 από την κυβέρνηση των Η.Π.Α. ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών.
Τα συστήματα συμμετρικής κρυπτογραφίας προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού, για την ανταλλαγή των μυστικών κλειδιών. Τέτοια συστήματα που επιτρέπουν την ασφαλή ανταλλαγή κλειδιών μέσα από δημόσια δίκτυα έχουν αναπτυχθεί και χρησιμοποιούνται, με περισσότερο διαδεδομένο το σύστημα `Kerberos` που έχει αναπτυχθεί στο `MIT`.
Τα σχήματα αυτά παρουσιάζουν το μειονέκτημα ότι δεν είναι εύκολο να επεκταθούν για την εξυπηρέτηση μεγάλων πληθυσμών και απαιτούν επίσης πρόσθετες διαδικασίες ασφάλειας, όπως την αποθήκευση των κλειδιών σε ένα κεντρικό ασφαλή εξυπηρετητή.

Ασύμμετρη Κρυπτογραφία

Στην ασύμμετρη κρυπτογραφία, χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων, το δημόσιο `public` και το ιδιωτικό `private` κλειδί αντίστοιχα. Τα κλειδιά αυτά παράγονται έτσι ώστε να έχουν τις εξής ιδιότητες:

- Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα.

- Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο.



Σχήμα 7.2: Σχηματική Παράσταση Ασύμμετρης Κρυπτογραφίας

Η βασική αυτή αρχή της κρυπτογραφίας δημόσιου κλειδιού διατυπώθηκε το 1976 από τους Diffie και Hellman, ενώ το 1977 οι Rivest, Shamir και Adleman βασιζόμενοι σε αρχές της θεωρίας των πεπερασμένων πεδίων δημιούργησαν το κρυπτοσύστημα RSA, [RSA78] την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημοσίου κλειδιού. Γύρω στο 1985 ο Miller και Koblitz ανεξάρτητα ο ένας από τον άλλο επινόησαν τις Ελλειπτικές Καμπύλες, ένα νέο είδος κρυπτογραφίας δημόσιου κλειδιού, το οποίο είναι και το είδος κρυπτογραφίας με το οποίο ασχολείται η παρούσα εργασία.

Για να αποκατασταθεί επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας, ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί.

Το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία κι έτσι μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δε μεταδίδεται ποτέ. Όταν ένα μήνυμα έχει κρυπτογραφηθεί με το δημόσιο κλειδί κάποιου χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί. Και επειδή μόνο ο ίδιος ο χρήστης γνωρίζει το ιδιωτικό του κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν. Ούτε καν το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα, κι έτσι η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα.

Η ασύμμετρη κρυπτογραφία προσφέρει μεγαλύτερη ασφάλεια από τη συμμετρική. Έχει όμως το μειονέκτημα ότι οι αλγόριθμοι ασύμμετρης κρυπτογράφησης είναι πολύ πιο αργοί από τους αλγόριθμους συμμετρικής κρυπτογράφησης.

7.2 Υποδομή Δημόσιου Κλειδιού

Η Υποδομή Δημόσιου Κλειδιού Public Key Infrastructure - PKI είναι ένας συνδυασμός λογισμικού, τεχνολογιών κρυπτογραφίας και υπηρεσιών που επιβεβαιώνουν και πιστοποιούν την εγκυρότητα της κάθε οντότητας που εμπλέκεται σε μια

συναλλαγή με το Διαδίκτυο, και παράλληλα προστατεύουν την ασφάλεια της συναλλαγής.

Η Υποδομή Δημοσίου Κλειδιού ενσωματώνει ψηφιακά πιστοποιητικά, κρυπτογραφία δημόσιου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό σχήμα. Μια τυπική υλοποίηση της Υποδομής Δημοσίου Κλειδιού περιλαμβάνει την παροχή ψηφιακών πιστοποιητικών σε χρήστες, σε εξυπηρετητές, σε λογισμικό χρηστών, καθώς επίσης και εργαλείων για τη διαχείριση, ανανέωση και ανάκληση των πιστοποιητικών αυτών.

7.2.1 Εγκαθίδρυση Κλειδιού

Η εγκαθίδρυση κλειδιού είναι η διαδικασία κατά την οποία δύο, ή περισσότερες οντότητες είτε εγκαθιδρύουν μια συμφωνία σχετικά με ένα αμοιβαίο `shared` μυστικό κλειδί, είτε ολοκληρώνουν τη διαδικασία παραγωγής ενός ιδιωτικού και δημόσιου κλειδιού και την μετάδοση του δεύτερου. Τα κλειδιά αυτά χρησιμοποιούνται προκειμένου να επιτευχθούν τέσσερις κρυπτογραφικοί σκοποί:

- Εμπιστευτικοτητα, `Confidentiality`. Δηλαδή η δυνατότητα που έχει ο προκαθορισμένος παραλήπτης, και μόνον αυτός, να αποκρυπτογραφήσει το περιεχόμενο ενός μηνύματος.
- Εντιμοτητα, `Integrity`. Δηλαδή η παροχή αποδείξεων σχετικά με την ακεραιότητα των στοιχείων, για να δοθεί έμφαση σε οποιαδήποτε τροποποίηση των υπογεγραμμένων στοιχείων. Για παράδειγμα, ο παραλήπτης ενός ψηφιακά υπογεγραμμένου ηλεκτρονικού ταχυδρομείου μπορεί να έχει την εμπιστοσύνη ότι το μήνυμα δεν έχει αλλοιωθεί καθόδόν από τον αποστολέα.
- Αυθεντικοτητα, `Authenticity`. Δηλαδή η παροχή αποδείξεων σχετικά με την αυθεντικότητα της οντότητας που έχει υπογράψει, προκειμένου να καταπολεμηθεί η απειλή των επιθέσεων κατά τις οποίες ένα άτομο προσποιείται να είναι κάποιος άλλος. Για παράδειγμα, δεδομένου ότι μια ψηφιακή υπογραφή μπορεί να παραχθεί μόνο από τον κάτοχο του κατάλληλου ιδιωτικού κλειδιού, ο παραλήπτης ενός ηλεκτρονικού ταχυδρομείου μπορεί να έχει τη σιγουριά, ότι ο αποστολέας είναι ο ίδιος με αυτόν που υποστηρίζει ότι είναι.
- Μη Αποκηρυξη`Non - Repudiaton`. Η μη-αποκήρυξη σημαίνει ότι ένα άτομο δεν μπορεί εύκολα να αρνηθεί τη συμμετοχή του σε μια συναλλαγή.

Γενικά υπάρχουν δύο ειδών πρωτόκολλα Εγκαθίδρυσης Κλειδιών:

- Το Πρωτοκολλο Εγκαθιδρυσης Κλειδιων μεσω μεταφορας. Κατά το πρωτόκολλο αυτό το κλειδί δημιουργείται από την μία οντότητα και μεταφέρεται. Παράδειγμα αυτού του είδους εγκαθίδρυσης είναι η Ασύμμετρη Κρυπτογραφία.
- Το Πρωτοκολλο Εγκαθιδρυσης Κλειδιων μεσω Συμφωνιας. Κατά το πρωτόκολλο αυτό οι δύο οντότητες συνεισφέρουν πληροφορία και από κοινού εγκαθιδρύουν το αμοιβαίο μυστικό Κλειδί. Ο δικός μας αλγόριθμός έχει την μορφή της δεύτερης περίπτωσης, δηλαδή είναι ένας αλγόριθμός Συμφωνίας Κλειδιού. Χαρακτηριστικό παράδειγμα αυτού του είδους είναι η Συμμετρική Κρυπτογραφία.

7.2.2 Διαχείριση Κλειδιών

Ο μοναδικός σκοπός όλων των αρχών διαχείρισης κλειδιών σχετικά με Κρυπτογραφικούς Αλγόριθμους είναι η ελαχιστοποίηση των συνεπειών του συστήματος, και των εφαρμογών των Έξυπνων Καρτών, σε περίπτωση που ένα ή παραπάνω κρυφά κλειδιά γίνουν γνωστά σε μη εξουσιοδοτημένους χρήστες. Αν ήταν δυνατόν να εξασφαλιστεί, ότι τα κλειδιά θα παρέμεναν πάντα μυστικά, τότε ένα μοναδικό κλειδί για όλες τις κάρτες θα ήταν αρκετό. Ωστόσο, κάνεις δεν μπορεί να εγγυηθεί αυτή την μυστικότητα κάνοντας την παραπάνω υπόθεση αδύνατη. Η χρησιμοποίηση αρχών ενδυνάμωσης της ασφάλειας κλειδιών που θα περιγράψουμε παρακάτω έχει σαν αποτέλεσμα την αύξηση του αριθμού των κλειδιών.

7.2.3 Διαφοροποίηση Κλειδιών

Αφού οι Έξυπνες Κάρτες σε αντίθεση με τους Αναγνώστες Έξυπνων Καρτών, μπορούν να μεταφερθούν οπουδήποτε και από οποιονδήποτε, συνεπάγεται ότι οι επιθέσεις που μπορούν να γίνουν σε αυτές είναι περισσότερες τόσο σε πλήθος όσο και σε μορφή. Αν στην Έξυπνη Κάρτα δεν υπάρχει η παρουσία ενός κύριου Κλειδιού, `Master Key`, τότε οι συνέπειες μιας επιτυχημένης προσπάθειας ανάγνωσης των περιεχομένων της κάρτας μπορεί να ελαχιστοποιηθεί. Έπεται λοιπόν, ότι είναι προτιμότερο τα κλειδιά τα οποία είναι αποθηκευμένα σε μία κάρτα να είναι κλειδιά, τα οποία έχουν παραχθεί από τη συναίνεση ενός Κύριου Κλειδιού.

Τα διαφοροποιημένα κλειδιά, `Diversify Keys`, δημιουργούνται χρησιμοποιώντας ένα κρυπτογραφικό αλγόριθμο. Τα εισαγόμενα δεδομένα είναι το Κύριο κλειδί, το οποίο διατηρείται από την εταιρία παραγωγής των καρτών, και ειδικά επιλεγμένα γνωρίσματα της συγκεκριμένης κάρτας. Οι κρυπτογραφικοί αλγόριθμοι που συνήθως χρησιμοποιούνται για τη λειτουργία αυτή είναι ο [DES], [triple-DES]. Για λόγους απλότητας, σαν το επιλεγμένο χαρακτηριστικό γνώρισμα της κάρτας χρησιμοποιείται ο αριθμός της κάρτας, ο οποίος δημιουργείται και αποθηκεύεται στην κάρτα κατά την εργοστασιακή παραγωγή της. Όντας μοναδικός για την κάθε κάρτα, μπορεί να χρησιμοποιηθεί διαμέσου του συστήματος για την ταυτοποίηση της κάρτας.

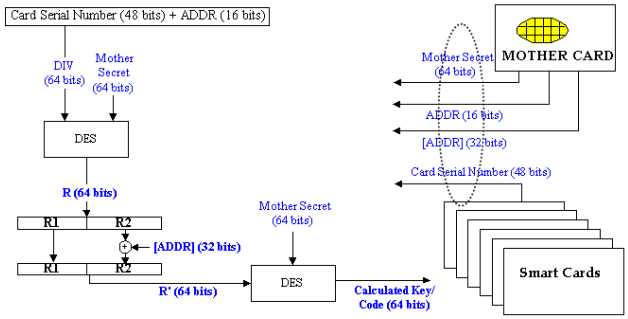
Δίνουμε στη συνέχεια ένα σχήμα υλοποίησης μιας τέτοιας διαδικασίας κατά την οποία οι παράμετροι εισόδου για την υλοποίηση του κρυπτογραφικού αλγορίθμου, στην περίπτωση αυτή του `DES`, είναι:

- Το κύριο Κλειδί, `Master Key`.
- Μια προκαθορισμένη διεύθυνση μνήμης της Κύριας Κάρτας, `MotherCard`.
- Τα περιεχόμενα αυτής της διεύθυνσης μνήμης.
- Τον Αριθμό Αναγνώρισης της Κάρτας.

Η διεύθυνση μνήμης της Κύριας Κάρτας που χρησιμοποιείται για κάθε κάρτα, και ο Αριθμός Αναγνώρισης της Κάρτας είναι διαφορετικοί κάθε φορά, διασφαλίζοντας έτσι την μοναδικότητα του διαφοροποιημένου κλειδιού.

7.2.4 Εκδόσεις Κλειδιών

Δεν είναι ιδιαίτερα ασφαλές για μία κάρτα να διατηρεί για όλη την διάρκεια της ζωής της ένα συγκεκριμένο κλειδί. Υποθέστε ότι ένα Κύριο κλειδί υπολογίζεται σαν αποτέλεσμα μιας επίθεσης. Σε αυτήν την περίπτωση, όλοι οι πωλητές εφαρμογών θα



Σχήμα 7.3: Μέθοδος δημιουργίας Διαφοροποιημένου Κλειδιού βάσει του Αριθμού Κάρτας και του Κύριου Κλειδιού

έπρεπε να κλείσουν τα συστήματα τους και οι κάτοχοι καρτών θα έπρεπε να αλλάξουν τις κάρτες τους, και έτσι η απορρέουσα ζημία θα ήταν τεράστια. Συνεπώς, είναι πιθανόν να αλλάξει ο τρόπος παραγωγής κλειδιών σε μοντέρνα συστήματα.

Η μεταφορά σε μια νέα γενιά κλειδιών μπορεί να ενισχυθεί από το γεγονός ότι ένα κλειδί έχει υπολογιστεί σαν αποτέλεσμα μιας επίθεσης, αλλά επίσης μπορεί να γίνεται σαν μια διαδικασίας ρουτίνας σε καθορισμένα ή μεταβλητά χρονικά διαστήματα. Το αποτέλεσμα της μεταφοράς αυτής, είναι ότι τα κλειδιά στο σύστημα αντικαθίστανται από νέα, χωρίς να χρειάζεται να αντικατασταθούν οι κάρτες. Αφού τα Κύρια κλειδιά βρίσκονται στα τερματικά και στα τμήματα υψηλότερης βαθμίδας, `Higher Level Parts` του συστήματος, η ασφαλής ανταλλαγή δεδομένων είναι το μόνο που χρειάζεται να γίνει προκειμένου να επιτευχθεί η νέα σειρά νέων και άγνωστων κλειδιών στους αναγνώστες.

7.3 Πιστοποίηση Ταυτότητας

7.3.1 Εισαγωγή στην Πιστοποίηση Ταυτότητας

Ο αντικειμενικός σκοπός της πιστοποίησης ταυτότητας είναι να επαληθεύει την ταυτότητα και την αυθεντικότητα μίας οντότητας. Πιο συγκεκριμένα, στην περίπτωση των έξυπνων καρτών, αυτό σημαίνει ότι η κάρτα ή ο τερματικός αναγνώστης καθορίζει αν ο επικοινωνιακός συνέταιρος είναι γνήσιος.

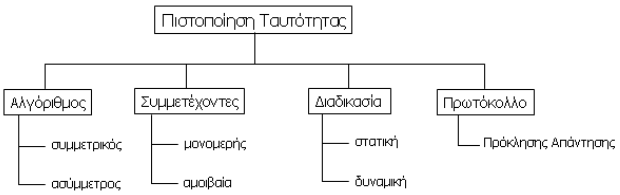
Προκειμένου να λάβει χώρα η πιστοποίηση ταυτότητας, πρέπει και οι δύο οντότητες να έχουν κάποιο κοινό μυστικό, το οποίο μπορεί να επαληθευτεί μέσω μιας διαδικασίας πιστοποίησης ταυτότητας. Μια τέτοια διαδικασία είναι σαφώς πιο ασφαλής σε σχέση με την απλή διαδικασία ταυτοποίησης, η οποία αναπαρίσταται από την εισαγωγή του PIN και την επαλήθευση του. Αυτή η διαδικασία έχει το μειονέκτημα ότι το μυστικό στέλνεται από την μία οντότητα στην άλλη χωρίς καμία προφύλαξη, κάτι το οποίο είναι αρκετά επικίνδυνο καθώς κάποιος εχθρός θα μπορεί σχετικά εύκολα να μάθει το μυστικό. Επίσης, η συγκεκριμένη διαδικασία έχει το μειονέκτημα ότι ένας υποτιθέμενος εχθρός θα μπορούσε με τη διαδικασίας της εξαντλητικής δοκιμής να υπολογίσει την τιμή του PIN και έτσι να μπορεί να έχει μη εξουσιοδοτημένη πρόσβαση στα δεδομένα της οντότητας.

Με τη διαδικασία πιστοποίησης ταυτότητας, δεν είναι δυνατόν κάποιος να μάθει το κοινό μυστικό, ή τα δεδομένα που μπορεί να συγκροτούν το κοινό μυστικό, απλά

παρακολουθώντας το κανάλι όπως στην προηγούμενη περίπτωση. Αυτό συμβαίνει γιατί κατά την υλοποίηση ενός πρωτοκόλλου πιστοποίησης ταυτότητας, τα δεδομένα δεν στέλνονται απροστάτευτα πάνω από το κανάλι επικοινωνίας, αλλά αντιθέτως στις περισσότερες περιπτώσεις όπως και στη δική μας, πρώτα κρυπτογραφούνται και μετά αποστέλλονται. Άρα το να μάθει κάποιος τα δεδομένα αυτά απαιτεί τον υπολογισμό συχνά πολύ δύσκολων συναρτήσεων, που στις πλειοψηφία των περιπτώσεων είναι αδύνατον να υπολογιστούν μονοσήμαντα.

7.3.2 Διαχωρισμός των Χαρακτηριστικών της Πιστοποίηση Ταυτότητας

Παρατηρούμε στο παρακάτω σχήμα κάποιους διαχωρισμούς που έχουν γίνει σχετικά με τα πεδία της πιστοποίησης ταυτότητας και θα τους αναλύσουμε παρακάτω:



Σχήμα 7.4: Κατηγοριοποίηση της Πιστοποίηση ταυτότητας στην περιοχή των Έξυπνων Καρτών

- ΣΥΜΜΕΤΡΙΚΗ — ΑΣΥΜΜΕΤΡΗ. Η διαφορά σε αυτήν την περίπτωση έγκειται στο γεγονός ότι οι αλγόριθμοι που χρησιμοποιούνται μπορεί να είναι είτε συμμετρικοί, δηλαδή να χρησιμοποιούν το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων, είτε ασύμμετροι, δηλαδή να χρησιμοποιούν διαφορετικά κλειδιά κρυπτογράφησης και αποκρυπτογράφησης.
- ΜΟΝΟΜΕΡΗΣ — ΑΜΟΙΒΑΙΑ. Εδώ η διαφορά έγκειται στο γεγονός ότι η πιστοποίηση της ταυτότητας μπορεί να γίνεται μόνο προς την μία κατεύθυνση, δηλαδή να πιστοποιείται η ταυτότητα μόνο της μίας οντότητας, είτε η πιστοποίηση μπορεί να γίνεται και προς τις δύο κατευθύνσεις, δηλαδή να πιστοποιούν και οι δύο οντότητες την ταυτότητα τους.
- ΣΤΑΤΙΚΗ — ΔΥΝΑΜΙΚΗ. Η διαφοροποίηση που γίνεται μεταξύ της στατικής και της δυναμικής πιστοποίησης ταυτότητας, έχει να κάνει με το γεγονός ότι στη στατική, χρησιμοποιούνται πάντα τα ίδια στατικά δεδομένα για επίτευξη της πιστοποίησης. Αντίθετα, η δυναμική προσέγγιση, κατασκευάζεται με τρόπο τέτοιο, ώστε να προστατεύεται ενάντια σε επιθέσεις με μορφή εισαγωγής δεδομένων τα οποία έχουν καταγραφεί κατά την διάρκεια μιας προηγούμενης επικοινωνίας μεταξύ των δύο οντοτήτων. Αυτό επιτυγχάνεται εξαιτίας του γεγονότος ότι πιστοποίηση είναι βασισμένη σε διαφορετικά δεδομένα.

Η αρχή της πιστοποίησης ταυτότητας στο πεδίο των έξυπνων καρτών είναι πάντα βασισμένη στη διαδικασία Πρόκλησης και Απάντησης, `Chalenge - Response`. Σύμφωνα με αυτή τη διαδικασία αυτή, η μια εκ των δύο οντοτήτων θέτει στην άλλη οντότητα μία παραγόμενη ερώτηση, την πρόκληση. Η δεύτερη οντότητα υπολογίζει μια

απάντηση χρησιμοποιώντας κάποιον αλγόριθμο και στέλνει την απάντηση πίσω στην πρώτη οντότητα. Ο αλγόριθμος που χρησιμοποιείται, είναι συνήθως ένας αλγόριθμος κρυπτογράφησης ο οποίος χρησιμοποιεί ένα διαμοιραζόμενο κλειδί, ή ζευγάρια κλειδιών (δημόσια και ιδιωτικά), για την κρυπτογράφηση των δεδομένων.

Στη συνέχεια, κατατάσσουμε την πιστοποίηση ταυτότητας σε τέσσερις διαφορετικές κατηγορίες, ανάλογα με τον αλγόριθμο που χρησιμοποιείται, τους συμμετέχοντες, και τη διαδικασία που χρησιμοποιείται. Έτσι καταλήγουμε στον παρακάτω διαχωρισμό:

- ΣΥΜΜΕΤΡΙΚΗ ΜΟΝΟΜΕΡΗΣ ΠΙΣΤΟΠΟΙΗΣΗ ΤΑΥΤΟΤΗΤΑΣ. Η μορφή της πιστοποίησης ταυτότητας αυτής της κατηγορίας έχει, να κάνει με την πιστοποίηση της ταυτότητας της μιας μόνο οντότητας που επέρχεται με την χρησιμοποίηση ενός συμμετρικού αλγορίθμου.

- ΣΥΜΜΕΤΡΙΚΗ ΑΜΟΙΒΑΙΑ ΠΙΣΤΟΠΟΙΗΣΗ ΤΑΥΤΟΤΗΤΑΣ. Η πιστοποίηση της ταυτότητας αυτής της κατηγορίας επιτυγχάνεται αμοιβαία και προς τις δύο συμμετέχοντες οντότητες, με την χρησιμοποίηση ενός συμμετρικού αλγόριθμου.

- ΑΣΥΜΜΕΤΡΗ ΜΟΝΟΜΕΡΗΣ ΠΙΣΤΟΠΟΙΗΣΗ ΤΑΥΤΟΤΗΤΑΣ. Η πιστοποίηση της ταυτότητας αυτής της κατηγορίας επιτυγχάνεται μονομερώς προς μια οντότητα, με την χρησιμοποίηση ενός ασύμμετρου αλγόριθμου.

- ΑΣΥΜΜΕΤΡΗ ΑΜΟΙΒΑΙΑ ΠΙΣΤΟΠΟΙΗΣΗ ΤΑΥΤΟΤΗΤΑΣ. Η πιστοποίηση της ταυτότητας αυτής της κατηγορίας επιτυγχάνεται αμοιβαία και προς τις δύο συμμετέχοντες οντότητες, με την χρησιμοποίηση ενός ασύμμετρου αλγόριθμου.

7.4 Περιγραφή Πρωτοκόλλου

7.4.1 Γενικά Στοιχεία

Στο σημείο αυτό και πριν περάσουμε στην ακριβή περιγραφή του Πρωτοκόλλου, πρέπει να κάνουμε κάποιες υποθέσεις σχετικά με τη διαδικασία πιστοποίησης ταυτότητας, που θα εξελιχθεί μεταξύ των δύο ενεργών οντοτήτων. Καταρχάς, ορίζουμε την μία οντότητα να είναι η Ασύρματη Έξυπνη κάρτα, και την άλλη οντότητα να είναι η τερματική συσκευή - Αναγνώστης. Ας ονομάσουμε την πρώτη οντότητα, δηλαδή την Ασύρματη Έξυπνη κάρτα, ως Οντότητα A και τη δεύτερη, δηλαδή την τερματική συσκευή - Αναγνώστη, ως Οντότητα B. Επίσης, πρέπει να αναφέρουμε μερικά στοιχεία τα οποία έχουν να κάνουν με την περαιτέρω ορθή και πλήρη εξέλιξη του πρωτοκόλλου. Θεωρούμε λοιπόν ότι η Οντότητα B περιέχει ένα Κύριο κλειδί το `Master Key` το οποίο είναι μοναδικό για κάθε συγκεκριμένο τύπο κάρτας, όπως ήδη έχουμε αναφέρει, και μάλιστα τα διαφορετικά του πεδία είναι ικανά να προσδιορίσουν τον συγκεκριμένο τύπο, εταιρία και χώρα κατασκευής κάθε κάρτας. Αυτό το κλειδί είναι αποθηκευμένο στην μνήμη της Οντότητας B, είτε στη μνήμη μιας άλλης έξυπνης κάρτας η οποία βρίσκεται μέσα στην οντότητα B, γενικότερα σε μέρος που δεν μπορεί να γίνει προσβάσιμο από ανεπιθύμητους τρίτους με κανένα τρόπο.

Κάθε κάρτα, κατά τη διαδικασία της εξατομίκευσης `Personalization`, εφοδιάζεται με ένα προσωπικό, μοναδικά ορισμένο αριθμό, τον οποίο καλούμε Αριθμό Αναγνώρισης Κάρτας, `Identification Card Number`. Στη συνέχεια ο αριθμός αυτός και το Κύριο κλειδί εισάγονται σαν δεδομένα σε έναν αλγόριθμο διαφοροποίησης με αποτέλεσμα να έχουμε τη δημιουργία ενός κλειδιού, το οποίο ονομάζεται

διαφοροποιημένο κλειδί `Diversify Key`, αυτή τη διαδικασία την έχουμε περιγράψει στην παράγραφο [§6.2.3]. Το κλειδί αυτό αποθηκεύεται στην μνήμη ανάγνωσης, `Read Only Memory` της κάρτας και αποτελεί τον κύριο παράγοντα της στη διαδικασία της αυθεντικοποίησης μεταξύ της κάρτας και του αναγνώστη − τερματικής συσκευής.

Κάτι άλλο που πρέπει να σημειωθεί, είναι ότι το κύριο κλειδί δεν αποθηκεύεται στην κάρτα, απλά συμμετέχει στη διαδικασία δημιουργίας του διαφοροποιημένου κλειδιού. Επομένως η κάρτα δεν γνωρίζει την τιμή του Κύριου κλειδιού και έτσι δεν υπάρχει φόβος να αποκτηθεί η τιμή του, μέσω κάποιας κακόβουλης πρόσβασης στην Κάρτα.

Το πρωτόκολλο που προτείνουμε, είναι ένα πρωτόκολλο της κατηγορίας πρόκλησης και απόκρισης, το οποίο έχουμε ήδη περιγράψει στην παράγραφο [§6.3.2]. Σύμφωνα με τα πρωτόκολλα αυτής της κατηγορίας, μια εκ των δύο οντοτήτων, στην περίπτωση μας η οντότητα B, θα εκτελέσει μια πρόκληση προς την άλλη οντότητα, η οποία με τη σειρά της θα απαντήσει. Κυρίαρχο στοιχείο στα σενάρια αυτού του είδους, παίζει η ορθότητα της απόκρισης της οντότητας που προκαλείται. Αν όντως η απάντηση κριθεί από τη άλλη οντότητα σωστή, σε σχέση με την πρόκληση που έκανε, τότε το πρωτόκολλο συνεχίζεται μέχρι τέλους, αλλιώς τερματίζεται.

7.4.2 Υλοποίηση του Πρωτοκόλλου

Περνώντας σε πιο συγκεκριμένο πλαίσιο, παραθέτουμε, σε μορφή βημάτων, τη διαδικασία που πρέπει να ακολουθήσουν οι δύο οντότητες της περίπτωσης μας, προκειμένου να ολοκληρωθεί επιτυχώς το πρωτόκολλο πιστοποίησης ταυτότητας που προτείνουμε.

1. Από την πλευρά της οντότητας B έχουμε αρχικά την επιλογή ενός πρώτου αριθμού p, ο οποίος θα αποτελέσει και το μέγεθος του πεδίου $\mathcal{F}_p$. Αφού ολοκληρωθεί αυτή η διαδικασία, έχουμε την δημιουργία μιας Ελλειπτικής Καμπύλης πάνω από το πεδίο $\mathcal{F}_p$ και την ταυτόχρονη επιλογή ενός σημείου P τάξης n της Ελλειπτικής Καμπύλης. Το σημείο αυτό θα αποτελέσει και το σημείο βάσης, πάνω στο οποίο θα στηριχθεί η ασφάλεια όλου του πρωτοκόλλου. Στη συνέχεια, εκτελούμε τον έλεγχο του κατά πόσο οι παράμετροι του πεδίου,

   $$[p, FR, \alpha, b, P = (x_P, y_P), n, h],$$

   που μόλις δημιουργήθηκαν από την οντότητα B, ικανοποιούν τις συνθήκες Επισημοποίησης Παραμέτρων Πεδίου που έχουμε περιγράψει στην παράγραφο [§4.2.1]. Η επισημοποίηση των παραμέτρων σε αυτό το στάδιο γίνεται στην μεριά της οντότητας B. Η δημιουργία της Ελλειπτικής Καμπύλης καθώς και η επιλογή του σημείου P γίνονται βάσει του αλγορίθμου `Complex Multiplication` στο πρότυπο [$P1363$], που ήδη έχουμε περιγράψει στην παράγραφο [§4.4]. Η τελική επιλογή της εγκυρότητας τόσο της Ελλειπτικής καμπύλης, όσο και του σημείου βάσης, γίνεται βάσει των διαφόρων περιορισμών που έχουν ήδη τεθεί, σχετικά με την αποφυγή τυχόν γνωστών επιθέσεων που έχουμε περιγράψει στην παράγραφο [§4.5.3]. Αν όντως αυτοί οι περιορισμοί ικανοποιούνται, τότε η διαδικασία της εκτέλεσης του πρωτοκόλλου συνεχίζεται με την οντότητα B να επιλέγει ένα τυχαίο αριθμό στο διάστημα $\{0 < k < Order(P)\}$, και την εκτέλεση της πράξης του γραμμικού πολλαπλασιασμού μεταξύ του σημείου βάσης της Ελλειπτικής Καμπύλης P και του ακεραίου αριθμού k, βάσει των

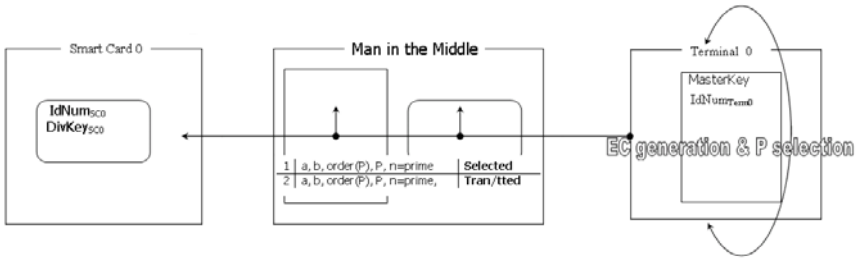
εξισώσεων που έχουμε περιγράψει στην παράγραφο [§3.2] και βάσει της βέλτιστης μορφής του αλγορίθμου Διπλασιασμού και πρόσθεσης της παραγράφου [§3.5]. Αναγκαία συνθήκη για την χρησιμοποίηση της βέλτιστης μορφής του αλγορίθμου Διπλασιασμού και πρόσθεσης της παραγράφου [§3.5], είναι η μετατροπή της μορφής του ακεραίου k σε μορφή προσημασμένου ψηφίου. Αφού αυτή η διαδικασία ολοκληρωθεί στην μεριά της οντότητας B, έχουμε την υλοποίηση του γραμμικού πολλαπλασιασμού κατά τα γνωστά, και το αποτέλεσμα της πράξης, δηλαδή το σημείο $Q = kP$, θα αποτελέσει το δημόσιο κλειδί της τερματικής συσκευής, οντότητας B, και θα το ονομάσουμε, $[K_{pubTerm}]$, ενώ ο ακέραιος k, θα αποτελεί το προσωπικό - κρυφό κλειδί της τερματικής συσκευής και θα το ονομάσουμε $[K_{privTerm}]$. Η δημιουργία των κλειδιών αυτών, έχει να κάνει με την ανάγκη διασφάλισης του καναλιού επικοινωνίας με φορά από την Κάρτα προς την τερματική συσκευή, με την βοήθεια κάποιου κρυπτογραφικού αλγορίθμου, στη συγκεκριμένη περίπτωση του [Menezes - Vanstone], καθώς και με την ανάγκη διασφάλισης των δεδομένων, μέσω της κρυπτογράφησης τους.

2. Το βήμα αυτό έχει να κάνει με την αποστολή δεδομένων από την πλευρά της οντότητας B προς την οντότητα A, δηλαδή της Τερματικής συσκευής προς την Ασύρματη Έξυπνη Κάρτα. Τα δεδομένα που θα αποσταλούν περιλαμβάνουν:

   i. Το σημείο της Ελλειπτικής Καμπύλης P που επιλέχθηκε από την Οντότητα B και θα αποτελεί το σημείο βάσης για τις δύο οντότητες.

   ii. Την παράμετρο α και την παράμετρο b από την εξίσωση της Ελλειπτικής Καμπύλης, $y^2 = x^3 + \alpha \cdot x + b$

   iii. Το μέγεθος q του πεδίου F_q πάνω στο οποίο δημιουργήθηκε η Ελλειπτική Καμπύλη και συνεπώς πάνω στο οποίο θα εκτελεστούν οι απαιτούμενες πράξεις.



Σχήμα 7.5: Πρώτη Μετάδοση Δεδομένων [Τερματικό → Κάρτα]

Τα δεδομένα δεν περιλαμβάνουν το δημόσιο κλειδί της οντότητας B καθώς δεν έχουμε ακόμα πιστοποιήσει την ταυτότητα της. Η αποστολή του κλειδιού χωρίς την πιστοποίηση της ταυτότητας κρύβει τον κίνδυνο ότι σε ενδεχόμενη παρουσία ενός ενδιάμεσου εχθρού, αυτός θα μπορεί να αλλάξει την τιμή του δημόσιου κλειδιού χωρίς ο παραλήπτης να το καταλάβει. Αυτό μπορεί να επιτευχθεί με τη διακοπή της μετάδοσης των δεδομένων από την έγκυρη οντότητα B και την παρεμβολή δεδομένων από τον ενδιάμεσο εχθρό. Καθώς ο παραλήπτης δεν γνωρίζει την ταυτότητα του αποστολέα, δεν μπορεί να γνωρίζει εάν τα δεδομένα είναι ορθά ή όχι.

3. Το βήμα αυτό εκτελείται στην μεριά της οντότητας Α. Αφού γίνει η λήψη των δεδομένων που αποστάλησαν από την οντότητα Β, η Οντότητα Α θα εφαρμόσει την επικύρωση τριών ιδιοτήτων προκειμένου να εξασφαλίσει την εγκυρότητα καθώς και την ασφάλεια της ελλειπτικής καμπύλης.

   i. Εξασφαλίζει ότι $4a^3 + 27b^2 \neq 0$ προκειμένου να υπάρχει λύση στην εξίσωση της Ελλειπτικής Καμπύλης.

   ii. Εξασφαλίζει ότι ο συμπαράγοντας `h` είναι περίπου ίσο με 1, έτσι ώστε να πιστοποιήσει ότι η τάξη του σημείου είναι κοντά στην τάξη της Ελλειπτικής Καμπύλης, η οποία με τη σειρά της είναι μεγαλύτερη ίση με 2^{160}.

   iii. Εξασφαλίζει ότι δεν ικανοποιούνται οι συνθήκες απαλοιφής με την μέθοδο `Menezes Okamoto Vanstone` όπως έχουμε περιγράψει στην παράγραφο [§4.1].

   iv. Στη συνέχεια και αφού η παραπάνω λειτουργίες ολοκληρωθούν επιτυχώς, η οντότητα Α επιλέγει ένα ακέραιο αριθμό στο σύνολο $[0, Order(P) - 1]$ ο οποίος θα αποτελέσει το κρυφό ιδιωτικό κλειδί της Έξυπνης Κάρτας, και το οποίο θα ονομάζουμε $[K_{PrivSmCd}]$. Παράλληλα υπολογίζεται και το δημόσιο κλειδί της Οντότητας Α, $[K_{PubSmCd}]$ το οποίο χρησιμοποιείται για την κρυπτογράφηση δεδομένων, και την διασφάλιση του καναλιού με φορά από την Τερματική συσκευή προς την Κάρτα. Όπως και στην περίπτωση της Οντότητας Β, έτσι και εδώ, το δημόσιο κλειδί υπολογίζεται μέσω του πολλαπλασιασμού του ιδιωτικού κλειδιού και του αποσταλώμενου από την οντότητα Β σημείου βάσης P, βάσει των βελτιστοποιημένων τύπων υπολογισμού γινομένου ακεραίου επί σημείου Ελλειπτικής Καμπύλης της παραγράφου [§3.2] και [§3.5]. Και σε αυτή την περίπτωση, όπως και σε αυτή της οντότητας Β, το κρυφό κλειδί πρέπει να μετατραπεί σε μορφή προσημασμένου σημείου, προκειμένου να μπορεί να επιτευχθεί η χρησιμοποίηση των βελτιστοποιημένων τύπων υπολογισμού γινομένου ακεραίου επί σημείου Ελλειπτικής Καμπύλης της παραγράφου [§3.2] και [§3.5].

   v. Το βήμα αυτό έχει να κάνει με τον υπολογισμό ενός προσωρινού κλειδιού το οποίο ονομάζουμε $[R1]$ και αποτελεί ένα σημείο της ελλειπτικής καμπύλης. Η παραγωγή του $[R1]$ γίνεται με τον πολλαπλασιασμό της `Hashed` τιμής, μέσω του Κατακερματικού Αλγορίθμου SHA-1, της μοναδικής ανά κάρτα ποσότητας $[Diversify_{key}]$ πολλαπλασιαζόμενης `modulo(n)`, με την παράμετρο α της Ελλειπτικής Καμπύλης, και του δημόσιου κλειδιού της οντότητας Α, $[K_{PubSmCd}]$. Δηλαδή είναι της μορφής:

   $$R1 = Hashed(Diversify_{key} \times \alpha, p) \times K_{PubSmCd}.$$

   Ο παραπάνω μετασχηματισμός του διαφοροποιημένου κλειδιού γίνεται, προκειμένου η ποσότητα με την οποία πολλαπλασιάζουμε το δημόσιο κλειδί να μην είναι η ίδια σε κάθε συναλλαγή, και συνεπώς να μην είναι το ίδιο και το προσωρινό κλειδί $[R1]$. Η επιλογή ενός τέτοιου μετασχηματισμού είναι σχεδόν επιτακτική, καθώς η ποσότητα $Diversify_{key}$ είναι πάντα η ίδια, δηλαδή είναι στατική, με αποτέλεσμα να χρειάζεται την μέγιστη δυνατή ασφάλεια. Η επιλογή του `SHA-1` γίνεται καθώς ο αλγόριθμος είναι ιδιαίτερα ασφαλής και παράλληλα η έξοδος του παράγει

ποσότητες μήκους 160 δυαδικών ψηφίων, κάτι το οποίο μας βολεύει για Ελλειπτικές καμπύλες τέτοιου μεγέθους.

Το συγκεκριμένο κλειδί δημιουργείται με τέτοιο τρόπο έτσι ώστε αν κάποιος ανεπιθύμητος τρίτος θέλει να εκτελέσει μία επίθεση ενδιάμεσου εχθρού, να μην έχει νόημα αυτή να υλοποιηθεί. Αυτό εξηγείται καθώς το συγκεκριμένο κλειδί δημιουργείται σαν γινόμενο ενός κρυφού μοναδικού ακεραίου και ενός σημείου τάξης περίπου ίσης με 2^{160}.

$$R1 = Hashed(Diversify_{key} \times \alpha, p) \times K_{PubSmCd}$$

$$R1 = Hashed(Diversify_{key} \times \alpha, p) \times (K_{PubSmCd} \times P)$$

δηλαδή,

$$R1 = (Hashed(Diversify_{key} \times \alpha, p) \times K_{PubSmCd}) \times P$$

$$R1 = c \times P, c \in \mathcal{F}_n, n \geq 2^{160}$$

Έτσι λοιπόν, σχετικά με το πρόβλημα της ψευδούς προσωποποίησης, θα λέγαμε ότι προκειμένου κάποιος εχθρός να καταφέρει να προσωποποιήσει ψευδώς την ταυτότητα μιας κάρτας πρέπει να εκτελέσει τα εξής:

1. Πρέπει να υπολογίσει μια ποσότητα $[K'_{PubSmCd}]$ τέτοια ώστε

   $$Hashed(Diversify_{key} \times \alpha, p) \times K'_{PubSmCd} = R1.$$

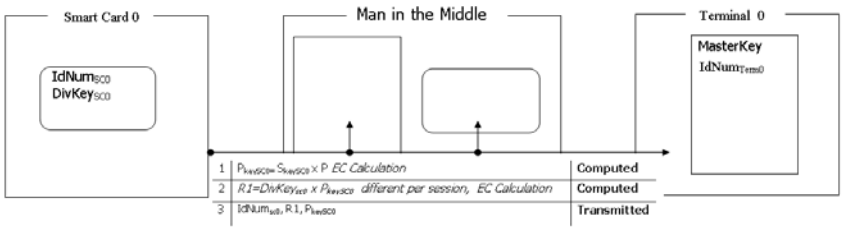
   Αυτό όμως είναι αδύνατον να υπολογισθεί καθώς ο εχθρός δεν γνωρίζει την ποσότητα $[Diversify_{key}]$, και έτσι το πρόβλημα ανάγεται στο πρόβλημα του διακριτού λογάριθμου για Ελλειπτικές Καμπύλες, στην εύρεση δηλαδή μιας ποσότητας τέτοιας ώστε πολλαπλασιαζόμενη με το δημόσιο κλειδί της Κάρτας να δίνει την ποσότητα $[R1]$. Η επιλογή ενός σωστού νέου κλειδιού είναι επιτακτική καθώς ο εχθρός θα θέλει να αποκρυπτογραφεί τα μηνύματα που μεταδίδονται προς την αυθεντική κάρτα.
2. Να κατασκευάσει την ποσότητα $[Diversify_{key}]$, προκειμένου να υπολογίσει την ποσότητα $[R1]$. Αυτό όμως είναι αδύνατον καθώς ο μόνος που μπορεί να κατασκευάσει αυτή την ποσότητα είναι το σωστό τερματικό.
3. Η ιδέα του να αλλάξει τον αριθμό της κάρτας, δεν έχει πρακτικό νόημα αφού τότε δεν θα μπορεί να πιστοποιήσει την άλλη κάρτα. Επίσης, το νέο $[Diversify_{key}]$ δεν θα είναι το ίδιο με της αυθεντικής κάρτας.

vi. Αφού ολοκληρωθεί ο υπολογισμός των νέων τιμών, $[K_{PubSmCd}]$, και $[R1]$, προχωράμε στην αποστολή των τιμών αυτών πάνω από το κανάλι επικοινωνίας (Κάρτας - Αναγνώστη) με φορά από την οντότητα Α προς την οντότητα Β. Με την αποστολή αυτών των ποσοτήτων, ουσιαστικά επιθυμούμε να διασφαλίσουμε το κανάλι επικοινωνίας μεταξύ των δύο οντοτήτων, αφού οι ποσότητες οι οποίες ανταλλάσσονται πάνω από το κανάλι επικοινωνίας, είναι μονοσήμαντες για κάθε ξεχωριστή Ελλειπτική

Καμπύλη και συνεπώς μπορούν να υπολογιστούν σωστά μόνο από τον κατάλληλο παραλήπτη. Επιπλέον θα αποστείλουμε και το δημόσιο κλειδί της Οντότητας Α.

Πιο συγκεκριμένα, τα δεδομένα που αποστέλλονται στην οντότητα Β, διαμέσου του καναλιού επικοινωνίας είναι:

- Ο αριθμός Αναγνώρισης Κάρτας, `Identification Card Number`, της οντότητας Α.
- Την ποσότητα $[R1]$, της οντότητας Α.
- Το δημόσιο κλειδί, $[K_{PubSmCd}]$, της οντότητας Α.



Σχήμα 7.6: Δεύτερη Μετάδοση Δεδομένων [Κάρτα → Τερματικό]

4. Το επόμενο βήμα αφορά την οντότητα Β και έχει να κάνει με την αναγνώριση, την πιστοποίηση της ταυτότητας και την ταύτιση του Δημόσιου κλειδιού της Κάρτας με τον Αριθμό Αναγνώρισης της.

   Προκειμένου να επιτελεστούν οι σκοποί αυτοί, εκτελούνται τα παρακάτω βήματα.

   - Αφού ολοκληρωθεί η λήψη και η αποθήκευση των δεδομένων,

     $$[IdentificationCardNumber, (R1), K_{PubSmCd}]$$

     από την οντότητα Β, το επόμενο βήμα έχει να κάνει την επισημοποίηση του Δημόσιου Κλειδιού της Οντότητας Α, και της ποσότητας $R1$, από την μεριά του Τερματικού. Δηλαδή το Τερματικό θα ελέγξει κατά πόσο οι ποσότητες αυτές, που είναι σημεία της Ελλειπτικής Καμπύλης, όντως ανήκουν στην Ελλειπτική Καμπύλη που το Τερματικό δημιούργησε. Αυτό γίνεται προκειμένου να διασφαλισθεί ότι τα δεδομένα που δέχεται η τερματική συσκευή είναι πράγματι ορθά και όχι προκατασκευασμένα, και δεν προέρχονται ως αποτελέσματα υπολογισμών πάνω σε άλλες αδύναμες Ελλειπτικές Καμπύλες.

   - Αφού η παραπάνω λειτουργία ολοκληρωθεί επιτυχώς, η Οντότητα Β θα δημιουργήσει από την μεριά της, την ποσότητα $[Diversify_{key}]$, αφού είναι η μόνη οντότητα η οποία μπορεί να τη δημιουργήσει, βάσει του ίδιου αλγορίθμου και δεδομένων που χρησιμοποιήθηκαν κατά τη διαδικασία της Προσωποποίησης της Κάρτας. Στη συνέχεια θα υπολογίσει μέσω του Δημόσιου Κλειδιού της Κάρτας το οποίο της έχει αποσταλεί, την ποσότητα $[R1]$, ως γινόμενο της `Hashed` τιμής, μέσω του Κατακερματικού Αλγορίθμου SHA-1, της μοναδικής ανά κάρτα ποσότητας $[Diversify_{key}]$ πολλαπλασιαζόμενης, `modulo(n)`, με την παράμετρο α της Ελλειπτικής Καμπύλης, και του Δημόσιου Κλειδιού της Κάρτας, $[K_{PubSmCd}]$. Εν συνεχεία, θα ελέγξει κατά πόσο η ποσότητα $[R1]$ που δημιούργησε, την ονομάζουμε $[Calc(R1)]$, είναι ίση με την ποσότητα $[R1]$ που έλαβε από την κάρτα. Αν αυτό συμβαίνει, τότε η κάρτα με το συγκεκριμένο αριθμό

Αναγνώρισης, `Identification Card Number` ταυτίζεται με το Δημόσιο Κλειδί που έχει παραληφθεί από την Οντότητα Β. Έτσι η τερματική συσκευή πλέον θα κρυπτογραφεί βάσει αυτού του δημόσιου κλειδιού, οποιαδήποτε δεδομένα έχουν προορισμό την κάρτα - Οντότητα Α.

Η διαδικασία αυτή εξασφαλίζει ότι δεν είναι δυνατή η ψευδής προσωποποίηση της Κάρτας, από κάποιο τρίτο πρόσωπο αφού δεν μπορεί να γνωρίζει την ποσότητα $[Diversify_{key}]$, και η πιθανότητα να την υπολογίσει δεδομένου του $[R1]$ και του $[K_{PubSmCd}]$, είναι ίση με $\frac{1}{2^{ord(P)}} \times \frac{1}{2^{63}}$, καθώς αυτή βρίσκεται `Hashed`, βάσει του `SHA-1` αλγορίθμου. Η ίδια πιθανότητα υπάρχει και στην περίπτωση που κάποιος τρίτος θέλει να χρησιμοποιήσει ένα δικό του δημόσιο κλειδί, $[K^{'}_{PubSmCd}]$, για το οποίο γνωρίζει το μυστικό κλειδί. Και σε αυτή την περίπτωση ο εχθρός πρέπει να βρει μια ποσότητα $Enemy_{quantity}$, τέτοια ώστε:

$$Enemy_{quantity} \times K^{'}_{PubSmCd} \equiv Hashed(Diversify_{key} \times \alpha, p) \times K_{PubSmCd}$$

Αν η ποσότητα που υπολογίζει το τερματικό, είναι διαφορετική από αυτή την οποία έχει λάβει, τότε πρέπει να τερματίσει το πρωτόκολλο στο σημείο αυτό. Ένα επιπλέον βήμα εκτελείται στην περίπτωση που η κάρτα απορριφθεί. Η κάρτα με το συγκεκριμένο Αριθμό Αναγνώρισης Κάρτας, δεν μπορεί να επαναλάβει τη διαδικασία της ταυτοποίησης, προτού συγκεκριμένος χρόνος αδρανείας μεσολαβήσει. Ο χρόνος αυτός, θα είναι εκθετικά κατανεμημένος έχοντας συγκεκριμένη μέση τιμή.

Αφού ολοκληρωθεί επιτυχώς αυτή η διαδικασία, στη συνέχεια η τερματική συσκευή θα εκτελέσει τις παρακάτω λειτουργίες:

i. Θα παράγει ένα τυχαίο αριθμό $R3$ τέτοιο ώστε $0 \leq R3 \leq ord(P)$, ο οποίος θα παίξει τον ρόλο του χαρακτηριστικού γνωρίσματος της συνδιαλλαγής. Δηλαδή θα είναι ένας αριθμός ο οποίος θα είναι έγκυρος μόνο κατά τη διάρκεια της συνδιαλλαγής του τερματικού και της κάρτας, και θα πρέπει να συνοδεύει κάθε μήνυμα που ανταλλάσσεται μεταξύ των δύο οντοτήτων μετά την εγκαθίδρυση των κλειδιών τους. Ο αριθμός αυτός θα αποτελεί το ιδιαίτερο χαρακτηριστικό κάθε συναλλαγής της κάρτας και του τερματικού και το τερματικό θα πρέπει να εξασφαλίζει ότι ο συγκεκριμένος αριθμός μπορεί να εμφανίζεται σε μια και μόνο μια συνδιαλλαγή κάθε φορά. Αυτό συμβαίνει προκειμένου να εξασφαλίσουμε ότι δεν θα υπάρχουν ταυτόχρονες συνδιαλλαγές μεταξύ διαφορετικών Καρτών και του ίδιου τερματικού, με κοινό το χαρακτηριστικό γνώρισμα της συνδιαλλαγής τους.

ii. Το βήμα αυτό δεν είναι υποχρεωτικό. Αν όμως η Οντότητα Α θέλει να ελέγξει άμεσα και ευθέως την εγκυρότητα του διαφοροποιημένου κλειδιού, τότε το βήμα αυτό είναι κατάλληλο για την επικύρωση αυτού του ελέγχου. Έτσι, αν όντως υλοποιηθεί το βήμα αυτό, τότε η οντότητα Β θα υπολογίσει την ποσότητα $[R2]$ η οποία θα παίξει τον ρόλο ενός προσωρινού κλειδιού και θα είναι ίση με:

$$R2 = Hashed(Diversify_{key} \times \alpha, p) \times K_{pubTerm}.$$

iii. Θα υπολογίσει την ποσότητα $[R4]$ η οποία και αυτή θα παίξει τον ρόλο ενός προσωρινού κλειδιού και θα είναι ίση με:

$$R4 = K_{PubTerm} \times Hashed(Diversify_{key} \times \alpha, p) \times R3 \times Term_{number}).$$

Αυτή η ποσότητα μπορεί να εξασφαλίσει από μόνη της, την εγκυρότητα τόσο της ταυτότητας του τερματικού, όσο και την αυθεντικότητα των τιμών $R3, Term_{number}$, χωρίς τη συνδρομή της ποσότητας $R2$, της οποίας ο υπολογισμός είπαμε πως είναι προαιρετικός.

iv. Θα κρυπτογραφήσει τις ποσότητες $R3$, $Term_{number}$ βάσει του αλγόριθμου κρυπτογράφησης Δημόσιου Κλειδιού `Menezes - Vanstone`, χρησιμοποιώντας το δημόσιο κλειδί της Κάρτας [$K_PubSmCd$], που ωστόσο έχει πρωτίστως πιστοποιήσει.

v. Τέλος, Θα αποστείλει στην Κάρτα τις ποσότητες,

$$[R4], [enc(R3)], [enc(Term_{number})], [K_{pubTerm}]$$

και αν επιθυμούμε θα αποστείλει και την ποσότητα $[R2]$.

Το δημόσιο κλειδί της τερματικής συσκευής, $[K_{pubTerm}]$, θα χρησιμοποιηθεί για την κρυπτογράφηση δεδομένων βάσει του Αλγορίθμου `Menezes - Vanstone`, που θα αποσταλούν από την Ασύρματή Κάρτα προς την Τερματική συσκευή.

Λόγος δημιουργίας των προσωρινών κλειδιών

Ο λόγος δημιουργίας των προσωρινών κλειδιών, $[R4]$, και ενδεχόμενα του $[R2]$ αν επιθυμούμε, είναι η αποφυγή της ψευδούς προσωποποίησης της ταυτότητας του τερματικού, από κάποιον εχθρό. Δηλαδή αν το τερματικό απλά έστελνε τις κρυπτογραφημένες ποσότητες,

$$[enc(R3), enc(Term_{number}]$$

χωρίς την προσθήκη του $[R4]$, κάποιος ενδεχόμενος εχθρός θα μπορούσε να διακόψει την μετάδοση τους και να τις αλλάξει με κάποιες της αρεσκείας του, χωρίς η κάρτα να μπορεί να διαπιστώσει αν οι ποσότητες που λαμβάνει είναι έγκυρες ή όχι. Τώρα όμως αυτό δεν είναι δυνατόν να γίνει αφού το $[R4]$ είναι μονοσήμαντα κατασκευασμένο για την δεδομένη καμπύλη που αποστέλλει το τερματικό, καθώς και άμεσα εξαρτώμενο με τις ποσότητες $[R3]$ και $[Term_{number}]$. Επιπλέον το προσωρινό αυτό κλειδί ανήκει και στην καμπύλη, κάνοντας έτσι ακόμα πιο δύσκολο των υπολογισμό του από κάποιο εξωτερικό παράγοντα. Ο τρόπος υπολογισμού των κλειδιών αυτών καθώς και το γεγονός ότι αποτελούν σημεία της Ελλειπτικής Καμπύλης δίδεται παρακάτω:

Σημείωση: Το $[R2]$ όπως ήδη έχουμε αναφέρει, δεν υποχρεωτικό να υπολογισθεί.

$$R2 = Hashed(Diversify_{key} \times \alpha, p) \times K_{pubTerm}$$

$$R2 = Hashed(Diversify_{key} \times \alpha, p) \times (K_{privTerm} \times P)$$

$$R2 = (Hashed(Diversify_{key} \times \alpha, p) \times K_{privTerm}) \times P$$

$$R2 = d \times P \in EC, d \in \mathcal{F}_n, n \geq 2^{160}$$

και,

$$R4 = K_{PubTerm} \times (Hs(Div_{key} \times \alpha, p) \times R3 \times Term_{number})$$

$$R4 = (K_{privTerm} \times P) \times (Hs(Div_{key} \times \alpha, p) \times R3 \times Term_{num})$$

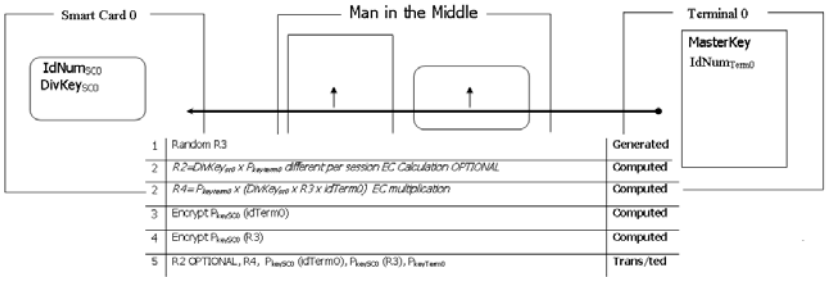
$$R4 = (K_{privTerm} \times Hs(Div_{key} \times \alpha, p) \times R3 \times Term_{number}) \times P$$

$$R4 = e \times P \in EC, e \in \mathcal{F}_n, n \geq 2^{160}$$

$$Hs() \equiv Hashed(), Div_{key} \equiv Diversify_{key}$$

Συνεπως έτσι ώστε κάποιος να μπορεί να παράγει αυτές τις ποσότητες πρέπει, αφενός να γνωρίζει τις τιμές του $R3$ και $[Term_{number}]$, και αφετέρου να γνωρίζει την τιμή του $[Diversify_{key}]$. Διαφορετικά, το πρόβλημα του υπολογισμού των ποσοτήτων $[R2]$ και $[R4]$ είναι ταυτόσημο του προβλήματος του Διακριτού Λογάριθμου για τις Ελλειπτικές Καμπύλες καθώς και επίλυσης του Αλγορίθμου SHA-1. Επιπλέον η χρησιμοποίηση τυχαίων παραμέτρων $R3$ και $[Term_{number}]$ από την μεριά του εχθρού προκειμένου να επιτύχει αποτέλεσμα ίδιο με το αυθεντικό, παρουσιάζει πιθανότητα ίση με $\frac{1}{2^{ord(P)}}$. Επίσης, οι κρυπτογραφημένες τιμές $enc(R3)$, και $[enc(Term_{number})]$, μπορούν να αποκρυπτογραφηθούν μόνο από τη σωστή κάρτα, μιας και που μόνο αυτή γνωρίζει το σωστό κρυφό κλειδί.

Μια σημείωση που πρέπει να γίνει στο σημείο αυτό, είναι πως η τερματική συσκευή κατά τη διάρκεια του υπολογισμού των διαφόρων ποσοτήτων χρησιμοποιεί το διαφοροποιημένο κλειδί που η ίδια έχει παράγει από μόνη της. Έτσι κανείς δεν μπορεί να αλλάξει την τιμή του, και να χρησιμοποιήσει κάποιο ψευδές στην θέση του, θέλοντας έτσι να μειώσει την αξιοπιστία του πρωτοκόλλου.



Σχήμα 7.7: Τρίτη Μετάδοση Δεδομένων [Τερματικό → Κάρτα]

5. Στη συνέχεια η Οντότητα A λαμβάνει τις αποσταλούμενες από την οντότητα B και εκτελεί τις παρακάτω λειτουργίες:

   i. Η οντότητα A εφαρμόζει την μέθοδο της Ενσωματωμένης Επισημοποίησης Δημόσιου Κλειδιού για να διαπιστώσει αν όντως το δημόσιο κλειδί, και το $[R4]$ που έχει λάβει, κατέχει τις αριθμητικές ιδιότητες που πρέπει. Αν αυτό δεν συμβαίνει, τότε το πρωτόκολλο τερματίζεται σε αυτό το σημείο. Γενικά, πρέπει τουλάχιστον να εξασφαλισθεί ότι το δημόσιο κλειδί και το

$[R4]$ είναι σημεία της Ελλειπτικής Καμπύλης που η κάρτα χρησιμοποιεί, προκειμένου να αποφύγουμε τυχών επιθέσεις που θέλουν να χρησιμοποιήσουν διαφορετικές Ελλειπτικές Καμπύλες στις οποίες το πρόβλημα του Διακριτού Λογάριθμου είναι πιο εύκολο να επιλυθεί.

Η ασφάλεια έναντι σε αυτές τις επιθέσεις εξασφαλίζεται και με την βοήθεια του αρχικού ελέγχου της Ελλειπτικής Καμπύλης από την κάρτα.

Το προσωρινό κλειδί $[R2]$ δεν το εξετάζουμε αφού περιέχεται στο κλειδί $[R4]$, και κυρίως επειδή ο αντικειμενικός σκοπός του πρωτοκόλλου, εκτός της παροχής της μέγιστης δυνατής ασφάλειας, είναι και η ελαχιστοποίηση του χρόνου εκτέλεσης πράξεων στη μεριά της Οντότητας Α. Επιπλέον, και γιατί η επιλογή του υπολογισμού και αποστολής του στην κάρτα δεν είναι υποχρεωτική.

ii. Η οντότητα Α στη συνέχεια θα προβεί στην αποκρυπτογράφηση των κρυπτογραφημένων δεδομένων που έχει λάβει, χρησιμοποιώντας τον ίδιο κρυπτογραφικό αλγόριθμο `Menezes - Vanstone`, έχοντας όμως σαν κλειδί αποκρυπτογράφησης το προσωπικό ιδιωτικό κλειδί της οντότητας Α, $(K_{PrivSmCd})$. Εκτελώντας τη διαδικασία της αποκρυπτογράφησης λαμβάνουμε τις ποσότητες

$$dec(enc((R3))) = R3$$

και

$$dec(enc(Term_{number})) = [Term_{number}].$$

Οι αποκρυπτογραφημένες ποσότητες αποθηκεύονται στην οντότητα Α με σκοπό να δημιουργηθούν από την μεριά της κάρτας η ποσότητα $[R4]$ και ενδεχόμενα αν αυτό έχει αποσταλεί το $R2$.

iii. Το βήμα αυτό έχει να κάνει με τον υπολογισμό των ποσοτήτων, $[R2]$ προαιρετικά και σαφώς της $[R4]$ τις οποίες θα ονομάζουμε $[Calc(R2)]$ και $[Calc(R4)]$ αντιστοίχως, από την μεριά της οντότητας Α. Έτσι η οντότητα Α, χρησιμοποιώντας τις ποσότητες που μόλις αποκρυπτογράφησε, δηλαδή το διαφοροποιημένο κλειδί της $R3$ και το Αριθμό Αναγνώρισης του Τερματικού, `Identification Terminal Number`, σε συνδυασμό με το δημόσιο κλειδί της Οντότητας Β $K_{pubTerm}$, θα είναι σε θέση να παράγει τις ποσότητες $[Calc(R2)]$, και $[Calc(R4)]$, εκτελώντας τα ίδια ακριβώς βήματα που εκτέλεσε και η οντότητα Β για τον υπολογισμο τους. Επίσης και σε αυτό το σημείο επισημαίνουμε ότι ο υπολογισμός του $[Calc(R2)]$, είναι υποχρεωτικός μόνο εάν έχει αποσταλεί στην Οντότητα Α το $[R2]$, από την Οντότητα Β.

$$Calc(R2) = Hashed(Diversify_{key} \times \alpha, p) \times K_{pubTerm}$$
$$Calc(R2) = Hashed(Diversify_{key} \times \alpha, p) \times (K_{privTerm} \times P)$$

και,

$$Calc(R4) = K_{PubTerm} \times (Hs(Div_{key} \times \alpha, p) \times R3 \times Term_{num})$$

$$Hs() \equiv Hashed(), Div_{key} \equiv Diversify_{key}$$

iv. Το τελευταίο βήμα αφορά την αποδοχή ή την απόρριψη της οντότητας B από την μεριά της οντότητας A μέσω της σύγκρισης των ποσοτήτων που η κάρτα υπολόγισε και αυτών που έλαβε. Έτσι αν,

$$[Calc(R2)] = [R2]$$

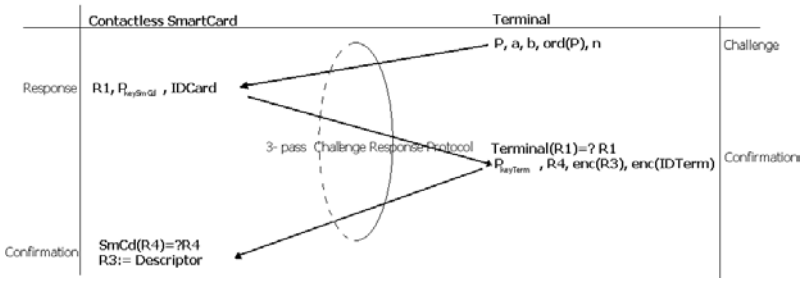
και

$$[Calc(R4)] = [R4]$$

η Οντότητα A πιστοποιεί την ταυτότητα της Οντότητας B μέσω της εγκυρότητας της απάντησης της και εν συνεχεία ταυτίζει το δημόσιο κλειδί της με το συγκεκριμένο αριθμό, $Term_{number}$. Γνωρίζει από αυτή τη στιγμή, ότι οποιοδήποτε μήνυμα έχει να στείλει στην οντότητα B θα το κρυπτογραφεί βάσει του δημόσιου κλειδιού της $[K_{pubTerm}]$. Επιπλέον γνωρίζει ότι κάθε μήνυμα που θα αποστέλλει στην οντότητα B θα πρέπει να συνοδεύεται από την παράμετρο $R3$. Αν όλα τα παραπάνω δεν συμβαίνουν τότε η κάρτα πρέπει να τερματίσει το πρωτόκολλο.

Σημείωση: Και σε αυτό το σημείο επισημαίνουμε ότι η σύγκριση των δυο ποσοτήτων, $Calc(R2), R2$, δεν είναι υποχρεωτική, αλλά προαιρετική προκειμένου να αυξήσουμε το επίπεδο ασφάλειας του πρωτοκόλλου.

Δίνουμε τέλος σε μια σχηματική παράσταση τα βήματα ολοκλήρωσης του πρωτοκόλλου.



Σχήμα 7.8: Σχηματική παράσταση βημάτων ολοκλήρωσης του Πρωτοκόλλου.

7.4.3 Πλεονεκτήματα - Συμπεράσματα

Σε αυτή την ενότητα, θα παρουσιάσουμε το βασικό πλεονέκτημα το οποίο κατέχει ο προτεινόμενος από εμάς αλγόριθμος, έναντι σε άλλους αλγόριθμους οι οποίοι προτείνονται. Οι περισσότεροι προτεινόμενοι αλγόριθμοι βασίζονται στη συμφωνία ενός κοινού κλειδιού, μεταξύ των δύο οντοτήτων.

Η βασική μέθοδος που συνήθως προτείνεται, και αφορά δύο οντότητες, την οντότητα Α, O_A, και την οντότητα Β, O_B είναι:

1. Επιλογή σημείου P.
2. Υπολογισμός του $Q_A = k_A \times P$ από την O_A.
3. Αποστολή του P και του Q_A από την $O_A \rightarrow O_B$.
4. Υπολογισμός του $Q_B = k_B \times P$ από την O_B.
5. Υπολογισμός του $Q_K = k_B \times Q_A = k_B \times k_A \times P$.
6. Αποστολή του Q_K και του Q_B στην O_A.
7. Υπολογισμός του $Q_K = k_A \times Q_B = k_A \times k_B \times P$ από 0_A.
8. Κοινό κλειδί για την O_A, O_B το Q_K.

Αυτή η μέθοδος κρύβει τον κίνδυνο, ότι κάποιος ενδιάμεσος τρίτος θα μπορούσε να συνάψει συμφωνία και με τις δύο οντότητες ξεχωριστά, και έτσι να μπορεί να αλλοιώνει τα μηνύματα τους. Θα μπορούσε δηλαδή, μια όχι σωστή κάρτα να συνάψει συμφωνία με το σωστό τερματικό, και ένα όχι σωστό τερματικό με τη σωστή κάρτα. Έτσι, η όχι σωστή κάρτα θα μπορούσε να αποσπά στοιχεία από το σωστό τερματικό να τα δίνει στο όχι σωστό τερματικό και αυτό με τη σειρά να τα χρησιμοποιεί στην σωστή κάρτα με την οποία έχει συνάψει συμφωνία.

Αυτό στην περίπτωση μας αποφεύγεται, με το να πιστοποιούμε πρώτα την ταυτότητα του άλλου, με τη δημιουργία των ποσοτήτων [$R1$], [$R4$], που μόνο η σωστές οντότητες μπορούν να δημιουργήσουν, προτού μοιραστούμε μαζί του οποιαδήποτε πληροφορία. Επιπλέον η δημιουργία του τυχαίου αριθμού $R3$, έχει σαν σκοπό να μην μπορεί κανείς άλλος να παρέμβει σε μια συνομιλία δύο οντοτήτων.

Το παραπάνω πρόβλημα που περιγράψαμε, η πλειοψηφία των πρωτοκόλλων το επιλύει με την χρήση πιστοποιητικών. Στη δική μας περίπτωση, δεν επιθυμούμε την χρήση τέτοιων μεθόδων, καθώς θα προσέδιδαν επιπλέον καθυστέρηση στην ολοκλήρωση του πρωτοκόλλου. Προτιμάμε αντάυτού να χρησιμοποιούμε τις ποσότητες που ήδη κατέχουμε για να πιστοποιούμε την ταυτότητα μιας οντότητας, κερδίζοντας χρόνο και προπάντων χωρίς να χάνουμε σε ασφάλεια.

7.4.4 Μετρήσεις - Συγκρίσεις

Σε αυτή την ενότητα θα παρουσιάσουμε ένα πλήθος μετρήσεων που υλοποιήσαμε προκείμενου να συγκρίνουμε, σε επίπεδα ταχύτητας και κόστους υπολογιστικής ισχύς, το πρωτόκολλο που προτείνουμε σε σχέση με ένα αντίστοιχο πρωτόκολλο το οποίο όμως βασίζεται στο κρυπτοσύστημα του RSA, [RSA78]. Πριν όμως περάσουμε στην παρουσίαση των αποτελεσμάτων θα δώσουμε μια γενική ιδέα σχετικά με κρυπτοσύστημα του RSA. Η όλη ιδέα στο κρυπτοσύστημα του RSA, βασίζεται στη δυσκολία παραγοντοποίησης μεγάλων ακεραίων αριθμών, σε αντίθεση με τα κρυπτοσυστήματα των Ελλειπτικών Καμπυλών, των οποίων η βασική ιδέα είναι η δυσκολία υπολογισμού διακριτού λογαρίθμου πάνω σε ελλειπτικές καμπύλες οι οποίες είναι ορισμένες πάνω σε κάποιο πεπερασμένο σώμα. Αυτή η διαφορά κάνει τις Ελλειπτικές Καμπύλες να κατέχουν μεγαλύτερη ασφάλεια ανά δυαδικό ψηφίο, κάτι το οποίο ήταν και η αιτία της μελέτης τους σε αυτή την εργασία. Πιο συγκεκριμένα, η αντιστοίχηση που γίνεται στο πλαίσιο της ασφάλειας, είναι μεταξύ κρυπτοσυστημάτων RSA με κλειδί μεγέθους 1024 δυαδικά ψηφία και Ελλειπτικών Καμπυλών με κλειδί μεγέθους 160 δυαδικών ψηφίων.

Το κρυπτοσύστημα του RSA

Δίνουμε σε αυτό το σημείο, περιγραφικά την μορφή του κρυπτοσυστήματος RSA.

1. Επιλέγουμε δύο μεγάλους πρώτους ακεραίους p, q
2. Υπολογίζουμε το $n = p \times q$ και $\phi(n) = (p-1) \times (q-1)$.
3. Επιλέγουμε δύο ακεραίους α, b :, το $(\alpha \times b) - 1 = d \times \phi(n), d \in Z$.
4. Οι ακέραιοι α, b : πρέπει επίσης να ικανοποιούν:
   - $\alpha = b^{-1} mod \phi(n)$
   - ΜΚΔ$(b, \phi(n)) = 1$
5. Δημοσιοποιούμε τα n, b.
6. [Κρυπτογράφηση] $y = x^b(n)$, όπου x το αρχικό κείμενο.
7. [Αποκρυπτογράφηση] $x = y^a(n)$.

Για τις παρακάτω μετρήσεις χρησιμοποιήθηκαν σαν παράμετροι κάρτας και Τερματικού τα εξής:

- Αριθμός Αναγνώρισης Κάρτας: 1099511627776
- Αριθμός Αναγνώρισης Τερματικού: 1099511627775
- Κύριο Κλειδί: 18446744073709551614

Οι αριθμοί αυτοί επιλέχθηκαν, δεδομένου ότι θεωρούμε πως οι Αριθμοί Αναγνώρισης είναι μεγέθους `5 Bytes`, και το Κύριο κλειδί `8 bytes`.
Έτσι για την περίπτωση του RSA είχαμε:

RSA Type	RSA-1024	RSA-512	RSA-128
p	5.448 ms	701 ms	60ms
q	5.448 ms	701 ms	60ms
$N = p \times q$	≤ 1 ms	≤ 1 ms	≤ 1ms
Total RSA Construction Time	10.896 ms	1.402 ms	120 ms
$Public_{key}$	90 ms	71 ms	50 ms
$Private_{key}$	40 ms	10ms	≤ 1ms
Encryption	460 ms	160 ms	≤ 1ms
Decryption	901 ms	314 ms	65 ms
SmartCard Time	1.491 ms	555 ms	115 ms
Total Protocol Time	12.297 ms	1.957 ms	235 ms

Πίνακας 7.1: Τυπικοί χρόνοι εκτέλεσης του RSA

Επίσης κατά την εκτέλεση του αλγορίθμου του RSA η κατανάλωση της υπολογιστικής ισχύς άγγιζε το 100%.

Στην περίπτωση των Ελλειπτικών Καμπυλών, με τις δικές μας βελτιστοποιήσεις, είχαμε:

EC-type	EC-161	EC-81	EC-47
Total EC generation Time	430 ms	191 ms	5 ms
$Public_{key}$	10 ms	$\leq$ 1ms	$\leq$ 1ms
$Private_{key}$	$\leq$ 1 ms	$\leq$ 1 ms	$\leq$ 1ms
Encryption	70 ms	40 ms	30 ms
Decryption	60 ms	41 ms	30 ms
SmartCard Time	140 ms	81ms	60 ms
Total Protocol Time	570 ms	172ms	65 ms

Πίνακας 7.2: Τυπικοί χρόνοι εκτέλεσης του προτεινόμενου Πρωτοκόλλου Ελλειπτικών Καμπυλών, με βελτιστοποιήσεις.

Παρατηρούμε την μεγάλη διαφορά στους χρόνους μεταξύ των δύο πρωτοκόλλων, κάτι το οποίο επιβεβαιώνει την αρχική μας υπόθεση. Επίσης ο χρόνος παραγωγής των Ελλειπτικών Καμπυλών βλέπουμε ότι ποικίλει. Αυτό οφείλεται στην ποσότητα D της παραγωγής των Ελλειπτικών Καμπυλών βάσει του Complex Multiplexing. Η ποσότητα αυτή, την έχουμε ήδη περιγράψει στην παράγραφο [§4.4], είπαμε ότι είναι ελεύθερη τετραγώνου και εξαρτάται από το πεδίο το οποίο χρησιμοποιούμε. Η εξάρτηση αυτή περιγράφεται πλήρως στο [P1363 Annex A]. Όσο μικρότερη είναι, τόσο καλύτερη απόδοση, σε θέματα ταχύτητας υπολογισμών, έχουμε στη δημιουργία των Ελλειπτικών Καμπυλών.

Επίσης κατά την εκτέλεση του προτεινόμενου Πρωτοκόλλου Ελλειπτικών Καμπυλών η κατανάλωση της υπολογιστικής ισχύς άγγιζε το πολύ το 95%. Δηλαδή και στο θέμα της Υπολογιστικής ισχύς υπερτερούν οι Ελλειπτικές Καμπύλες.

Δίνουμε επίσης ένα πίνακα με μετρήσεις στις ίδιες Ελλειπτικές Καμπύλες με πριν, χωρίς όμως τις βελτιστοποιήσεις.

EC-type	EC-161	EC-81	EC-47
Total EC generation Time	430 ms	191 ms	5 ms
$Public_{key}$	30 ms	9 ms	2 ms
$Private_{key}$	$\leq 1ms$	$\leq$ 1 ms	$\leq$ 1ms
Encryption	100 ms	70 ms	40 ms
Decryption	145 ms	60 ms	35 ms
SmartCard Time	275ms	139ms	77 ms
Total Protocol Time	705ms	330ms	82 ms

Πίνακας 7.3: Τυπικοί χρόνοι εκτέλεσης του προτεινόμενου Πρωτοκόλλου Ελλειπτικών Καμπυλών, χωρίς τις βελτιστοποιήσεις.

7.4.5 Παρατηρήσεις - Σημειώσεις

Η πρώτη παρατήρηση σχετικά με το πρωτόκολλο το οποίο προτείνουμε έχει να κάνει με τις ποσότητες βάσει των οποίων υπολογίζονται τα γινόμενα των σημείων των Ελλειπτικών Καμπυλών. Σε όλες τις περιπτώσεις θεωρούμε ότι οι ποσότητες με τις οποίες πολλαπλασιάζουμε τα σημεία είναι ακέραιοι αριθμοί στο διάστημα $[0, ord(P)]$. Ωστόσο αυτό στην πράξη μπορεί να μην είναι πάντα εφικτό. Για αυτόν το λόγο κάνουμε τις εξής θεωρήσεις:

- Εάν η ποσότητα με την οποία θα πολλαπλασιαστεί το σημείο της Ελλειπτικής Καμπύλης είναι στο διάστημα $[0, ord(P)]$, τότε εκτελούμε κανονικά την πράξη.
- Εάν η ποσότητα με την οποία θα πολλαπλασιαστεί το σημείο της Ελλειπτικής Καμπύλης δεν ανήκει στο διάστημα $[0, ord(P)]$, αλλά σε ένα υπερσύνολο αυτού του συνόλου τότε εκτελούμε την πράξη διαίρεσης $modulo(ord(P))$.

Όσον αφορά την αναπαράσταση των αριθμών, θεωρούμε ότι είναι η δεκαδική, αλλά ακόμα και στην περίπτωση που ο αριθμός δεν βρίσκεται σε δεκαδική αναπαράσταση, μπορούμε εύκολα να τον μετατρέψουμε σε αυτή.

Προκειμένου να αποφύγουμε μορφές επιθέσεων όπου κάποιο μη αυθεντικό τερματικό αποστέλλει συνεχώς το ίδιο σημείο και την ίδια Ελλειπτική Καμπύλη, διακόπτοντας συνεχώς την παροχή ρεύματος, ώστε να μπορέσει να έχει τη δυνατότητα να υπολογίσει την τιμή του διαφοροποιημένου κλειδιού, προτείνουμε την αποθήκευση των ποσοτήτων $[\alpha, b, P, n]$ στη διαρκή,`non volatile`, μνήμη σε συνδυασμό με ένα μετρητή, ο οποίος θα αυξάνει κάθε φορά που αποστέλλεται η ίδια Ελλειπτική Καμπύλη και το ίδιο σημείο. Έτσι όταν ο μετρητής φτάσει μια συγκεκριμένη τιμή, η οποία μπορεί να ποικίλει αναλόγως με το επίπεδο ασφάλειας που θέλουμε να προσδώσουμε, τότε η κάρτα απορρίπτει το συγκεκριμένο τερματικό.

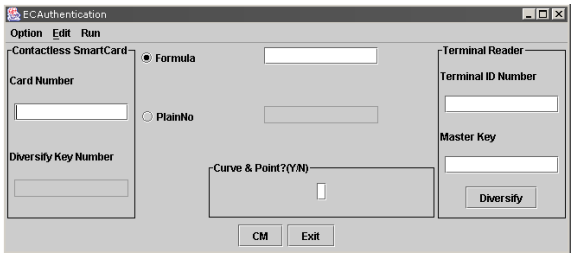
Με την υλοποίηση του παραπάνω πρωτοκόλλου επιτυγχάνουμε τόσο την διασφάλιση της εγκυρότητας της ταυτότητας των οντοτήτων, όσο και την ταυτόχρονη δημιουργία Δημόσιων και ιδιωτικών κλειδιών για την ανταλλαγή ασφαλών μηνυμάτων δια μέσω ενός καναλιού επικοινωνίας, βάσει ενός κοινού χαρακτηριστικού αριθμού συνδιαλλαγής. Παράλληλα με την εισαγωγή χρονικής καθυστέρησης που ακολουθεί την εκθετική κατανομή, παρέχουμε επιπλέον δυσκολία στην παράνομη και κακόβουλη προσπάθεια διείσδυσης. Η εκμετάλλευση των ιδιοτήτων των Ελλειπτικών Καμπυλών κάνει το Πρωτόκολλο να είναι πιο αποδοτικό στα πλαίσια υπολογιστικής ισχύς και χρόνου διεκπεραίωσης.

Εργαλεία και Μέθοδος Υλοποίησης Πρωτοκόλλου

Το παραπάνω πρωτόκολλο υλοποιήθηκε σε γλώσσα προγραμματισμού `C++` και `Java` με την βοήθεια της βιβλιοθήκης `Miracle`, η οποία είναι μια βιβλιοθήκη που έχει δημιουργηθεί για την υλοποίηση εφαρμογών των Ελλειπτικών Καμπυλών. Κατά την υλοποίηση του πρωτοκόλλου, τροποποιήσαμε τη συγκεκριμένη βιβλιοθήκη για λόγους βέλτιστης απόδοσης και ταχύτητας. Οι τροποποιήσεις που έγιναν, αφορούσαν όπως έχουμε ήδη περιγράψει στις παραγράφους [§3.5] και [§3.6], την μετατροπή του ακεραίου σε μορφή προσημασμένου σημείου προκειμένου να υλοποιηθεί ο βέλτιστος πολλαπλασιασμός ακεραίου και σημείου Ελλειπτικής Καμπύλης, την αφαίρεση των εξαρτημένων από τα δεδομένα διακλαδώσεων για την αποφυγή επιθέσεων λόγω ανάλυσης του φάσματος του ηλεκτρικού ρεύματος, και την αναπαράσταση των ποσοτήτων

ως προς μια βέλτιστη πολυωνυμική βάση. Τέλος όπως ήδη έχουμε αναφέρει η δημιουργία της Ελλειπτικής Καμπύλης και η επιλογή του κατάλληλου σημείου βάσης, έγινε βάση του `P1363 Standard Annex A`.

Επίσης, δημιουργήθηκε και μια διεπαφή χρήστη `User's Inteface` σε γλώσσα προγραμματισμού `Java`, για την ευκολότερη και πιο κατανοητή μορφή του πρωτοκόλλου.



Σχήμα 7.9: Η διεπαφή χρήστη του Πρωτοκόλλου

Ένα σημείο που επίσης πρέπει να επισημάνουμε, αφορά την υλοποίηση του αλγορίθμου RSA βάσει του οποίου έγιναν οι συγκρίσεις. Πρέπει να αναφέρουμε πως ο συγκεκριμένος αλγόριθμος δεν υλοποιήθηκε από εμάς, αλλά απλά προσαρμόστηκε για τις δικές μας ανάγκες. Αυτό που ουσιαστικά κάναμε, ήταν η τροποποίηση των υπαρχόντων παραμέτρων, σε παραμέτρους μεγέθους 1024 δυαδικά ψηφία, προκειμένου να εκτελέσουμε τη σύγκριση με το δικό μας προτεινόμενο πρωτόκολλο και εισαγωγή ενός γραφικού περιβάλλοντος για λόγους ευκολίας. Η αρχική υλοποίηση, καθώς και οι δικές μας παρεμβάσεις στον αλγόριθμο του RSA έχουν γίνει σε γλώσσα προγραμματισμού `Java`. Επίσης είναι σημαντικό να επισημάνουμε τον τρόπο επιλογής των δύο μεγάλων πρώτων αριθμών p, q κατά τη δημιουργία του RSA κρυπταλγορίθμου. Η συγκεκριμένη υλοποίηση έγινε, όπως ήδη έχουμε αναφέρει, σε γλώσσα προγραμματισμού `Java`. Στην `Java` ένας μεγάλος τυχαίος αριθμός κατασκευάζεται με τον κονστράκτορα:

$$BigInteger(intbitLength, java.util.Randomrandom);$$

ενώ ένας μεγάλος τυχαίος πρώτος αριθμός κατασκευάζεται με τον κονστράκτορα:

$$BigInteger(intbitLength, intcertainty, java.util.Randomrandom);$$

και ένας αριθμός ελέγχεται αν είναι πρώτος με την μέθοδο:

$$booleanisProbablePrime(intcertainty);$$

Και στις δύο περιπτώσεις η `Java` χρησιμοποιεί πιθανοθεωρητικούς, `Probabilistic`, αλγορίθμους, και η χρήση τους είναι αποδεκτή. Αρκεί, ένας αριθμός να έχει δημιουργηθεί ή ελεγχθεί με αυτόν τον τρόπο για να θεωρηθεί πρώτος, (η τιμή της παραμέτρου `certainty` αρκεί να είναι 10). Αυτό ισχύει γιατί η `Java`, σύμφωνα με την μέθοδο που υλοποιεί παρέχει πιθανότητα ίση με

$$Probablity = 1 - \frac{1}{2^{certainty}}$$

$$certainty = 10 \rightarrow Probability = 1 - \frac{1}{1024} = 1 - 0.001 = 0.99 = 99.9\%$$

Ουσιαστικά η μέθοδος εύρεσης ή παραγωγής πρώτων αριθμών βασίζεται στο τέστ των `Miller Rabin, [MRtes]`, καθώς και στη διαίρεση του προς έλεγχο αριθμού, με 1000 μικρούς πρώτους αριθμούς. Η υλοποίηση του τέστ των `Miller Rabin, [MRtes]` χρησιμοποιεί τον αλγόριθμο του τετραγωνισμού και πολλαπλασιασμού, `Square and Multiply, [SqMul]`.

Κεφάλαιο 8

Διαχείριση Στατικής Μνήμης

8.1 Εισαγωγή

Στο κεφάλαιο αυτό, θα παρουσιάσουμε ένα τρόπο με την βοήθεια του οποίου θα μπορέσουμε να καταπολεμήσουμε φαινόμενα διακοπής του ρεύματος, που έχουν προκληθεί τόσο από την κακή θέση της κάρτας ως προς το τερματικό, όσο και από κακόβουλες επιθέσεις ανεπιθύμητων τρίτων με σκοπό την απόκτηση σημαντικών δεδομένων για την κάρτα όπως για παράδειγμα το κρυφό της κλειδί.

Όπως ήδη έχουμε περιγράψει στην παράγραφο [§1.2.6], το ρεύμα το οποίο διαρρέει την κάρτα χωρίς επαφή, είναι αναγκαίο προκειμένου να εκτελεστούν οι διάφορες λειτουργίες της. Το ρεύμα αυτό, προέρχεται ως αποτέλεσμα της μεταβολής του μαγνητικού πεδίου, το οποίο δημιουργείται από την τερματική συσκευή και αυτό έχει σαν αποτέλεσμα, δεδομένου ότι η κάρτα δεν έχει από μόνη της δικό της ρεύμα, οποιεσδήποτε ανωμαλίες ή αλλαγές σχετικά με το μαγνητικό πεδίο, να έχουν άμεσες επιπτώσεις στην ομαλή λειτουργία της.

Καθώς η ένταση του μαγνητικού πεδίου δεν είναι ιδιαίτερα ισχυρή, η διαδικασία δημιουργίας ρεύματος λόγω μεταβολής του μαγνητικού πεδίου, είναι μια ιδιαίτερα ευαίσθητη διαδικασία. Για παράδειγμα, η απομάκρυνση της κάρτας πέρα μίας δεδομένης απόστασης, ή η στρέψη της κατά συγκεκριμένη γωνία, θα μπορούσε να καταστήσει την κάρτα ανενεργή λόγω της έλλειψης ηλεκτρικού ρεύματος, εξαιτίας της κακής τοπολογίας της μέσα στο μαγνητικό πεδίο. Με άλλα λόγια, στην θέση στην οποία βρίσκεται η κάρτα, το μαγνητικό πεδίο δεν έχει την απαραίτητη ισχύ ώστε η μεταβολή του να είναι σε θέση να δημιουργήσει ηλεκτρικό ρεύμα.

Τέτοια φαινόμενα, δηλαδή της έλλειψης του ηλεκτρικού ρεύματος, μπορούν να εμφανιστούν όχι μόνο λόγω της κακής τοπολογίας της κάρτας μέσα στο μαγνητικό πεδίο, αλλά και από την κακόβουλη προσπάθεια ανεπιθύμητων τρίτων για την απόκτηση μη εγκεκριμένων δεδομένων. Για παράδειγμα, κάποιο εχθρικό πρόσωπο θα μπορούσε να διακόπτει αλλεπάλληλα την τροφοδοσία ηλεκτρικού ρεύματος στην τερματική συσκευή, κάτι το οποίο θα είχε σαν αποτέλεσμα την αντίστοιχη κατάργηση του μαγνητικού πεδίου, το οποίο με τη σειρά του θα δημιουργούσε αλλεπάλληλες διακοπές ρεύματος στην κάρτα χωρίς επαφή. Αυτό το φαινόμενο θα μπορούσε να συμβεί είτε στα πλαίσια της προσπάθειας του εχθρικού προσώπου να αποκτήσει πληροφορίες πάνω από το κανάλι μετάδοσης, είτε στην προσπάθεια του να καθυστερήσει τη διάρκεια της συνδιαλλαγής μεταξύ της κάρτας και της τερματικής συσκευής.

Στη δική μας περίπτωση προσπαθούμε να καταπολεμήσουμε και τα δύο αυτά

ενδεχόμενα με την εισαγωγή ενός μηχανισμού αποθήκευσης κρίσιμων δεδομένων για την υλοποίηση του πρωτοκόλλου αμοιβαίας πιστοποίησης, πού ήδη έχουμε προτείνει στο προηγούμενο κεφάλαιο. Το όλο θέμα στο πρόβλημα αυτό, έγκειται στο να αποφύγουμε να αποστέλλουμε κάθε φορά που συμβαίνει μία διακοπή, είτε από κακόβουλη χρήση, είτε από κακή θέση της κάρτας, πληροφορία πάνω από το κανάλι επικοινωνίας, προκειμένου να εξοικονομούμε χρόνο, υπολογιστική ισχύ και βέβαια να εξαλείφουμε τον κίνδυνο των επιθέσεων που έχουν στόχο το κανάλι επικοινωνίας.

Πιο συγκεκριμένα, στο πρωτόκολλο πιστοποίησης ταυτότητας που προτείνουμε, θέλουμε να αποφύγουμε την επαναμετάδοση του σημείου βάσης και των άλλων χαρακτηριστικών της επιλεγόμενης, από την τερματική συσκευή ελλειπτικής καμπύλης, ώστε από την μία πλευρά να ελαχιστοποιήσουμε τον απαιτούμενο χρόνο συνδιαλλαγής των δύο οντοτήτων, αλλά επίσης να μειώσουμε και την ποσότητα της πληροφορίας που διαπερνά το κανάλι ώστε να εμποδίσουμε την προσπάθεια υπολογισμού δεδομένων για κάθε μη εγκεκριμένη πρόσβαση. Παράλληλα, επιθυμούμε να ελαχιστοποιήσουμε τον χρόνο τέλεσης και ολοκλήρωσης του πρωτοκόλλου. Καθώς η βασική ιδέα της ασφάλειας του πρωτοκόλλου που προτείνουμε, είναι οι Ελλειπτικές Καμπύλες και η θεωρητικά μονόδρομη πράξη του γινομένου ενός ακεραίου του χώρου και ενός σημείου της Ελλειπτικής Καμπύλης, η όλη ιδέα της διατήρησης κρίσιμών δεδομένων έγκειται πάνω στον αλγόριθμο του διπλασιασμού και πρόσθεσης που έχουμε προτείνει στην παράγραφο [§3.5].

Τρόπος αποφυγής συνεχούς επαναμετάδοσης του σημείου βάσης

Σχετικά με το θέμα της συνεχούς επαναμετάδοσης του σημείου βάσης με σκοπό τον υπολογισμό του διαφοροποιημένου κλειδιού, όπως έχουμε περιγράψει στην παράγραφο [§6.4.3], προτείνουμε την εγγραφή των παραμέτρων $[P, \alpha, b, n]$ και ενός μετρητή σε κάποια προκαθορισμένη θέση της διαρκούς, `non Volatile`, μνήμης, προκειμένου να ελέγχουμε τον αριθμό της επανάληψης του ίδιου σημείου και της ίδιας Ελλειπτικής Καμπύλης. Όταν ο αριθμός αυτός, ο οποίος ουσιαστικά αποτελεί το περιεχόμενο του μετρητή, ξεπεράσει κάποιο δεδομένο κατώφλιο, τότε η κάρτα απορρίπτει τη συγκεκριμένη Ελλειπτική Καμπύλη μαζί με το σημείο της.

Σχετικά με το θέμα της ελαχιστοποίησης του απαιτούμενου χρόνου συνδιαλλαγής των δύο οντοτήτων και την αποφυγή της επαναμετάδοσης πληροφορίας από την μεριά του τερματικού προτείνουμε τον παρακάτω μηχανισμό.

8.2 Περιγραφή Μηχανισμού Διαχείρισης

8.2.1 Γενικός Σκοπός Μηχανισμού

Προκειμένου να υλοποιήσουμε το συγκεκριμένο μηχανισμό θα χρησιμοποιήσουμε σαν πρότυπο μια διαρκή μνήμη, `non-Volatile memory`, δηλαδή μια μνήμη η οποία έχει τη δυνατότητα να μην χάνει τα δεδομένα που περιέχει, ακόμα στην περίπτωση που υπάρχει διακοπή της τροφοδοσίας του ηλεκτρικού ρεύματος. Αυτή η μνήμη θα χρησιμοποιηθεί προκειμένου να αποθηκεύουμε κρίσιμα δεδομένα για τον υπολογισμό των απαιτούμενων ποσοτήτων. Οι ποσότητες που θα αποθηκευτούν, είναι αυτές που χρησιμοποιούνται κατά τη διεκπεραίωση του πρωτοκόλλου της αμοιβαίας ταυτοποίησης των δύο οντοτήτων και ο μηχανισμός που προτείνουμε μας δίνει τη δυνατότητα γνώσης του σταδίου στο οποίο βρίσκεται το πρωτόκολλο.

8.2.2 Υλοποίηση Μηχανισμού

Η όλη διαδικασία στηρίζεται στην γνώση του σταδίου υπολογισμού, κάτι το οποίο επιτελείται με την βοήθεια των δυαδικών ψηφίων του κρυφού κλειδιού. Πιο συγκεκριμένα, κάθε δύο δυαδικά ψηφία του κρυφού κλειδιού αντιστοιχίζονται με ένα άλλο δυαδικό ψηφίο το οποίο αποτελεί το δυαδικό ψηφίο ετοιμότητας του. Η επιλογή της μορφής της αντιστοίχησης αυτής είναι η συγκεκριμένη, καθώς εμείς θεωρούμε σαν δυνατές τιμές του Κρυφού κλειδιού το $\{-1, 0, 1\}$. Έτσι αναγκαστικά χρειαζόμαστε τα διπλάσια δυαδικά ψηφία για να αποθηκεύσουμε το κρυφό κλειδί μιας και με ένα δυαδικό ψηφίο δεν είναι δυνατόν να αποθηκεύσουμε το ψηφίο $[-1]$. Μια ενδεχόμενη αντιστοίχηση η οποία θα είναι και ελεύθερου προθέματος θα ήταν:

$$[-1] \rightarrow [11]$$
$$[0] \rightarrow [00]$$
$$[1] \rightarrow [01]$$

Όταν το δυαδικό ψηφίο ετοιμότητας του κρυφού κλειδιού, γίνει 1, τότε γνωρίζουμε ότι για αυτό το στάδιο υπολογισμού όλες οι ποσότητες έχουν υπολογισθεί σωστά. Από την μεριά τους οι κρίσιμες ποσότητες εγγράφονται στη διαρκή, `non-volatile`, μνήμη σε προκαθορισμένες θέσεις αντιστοιχίζοντας την κάθε διεύθυνση μνήμης με ένα δυαδικό ψηφίο το οποίο επιδεικνύει το αν η συγκεκριμένη διεύθυνση έχει γίνει προσβάσιμη, (εγγραφεί ή διαβαστεί) ή όχι.Το δυαδικό ψηφίο αυτό θα το καλούμε `Dirty Bit`. Τέλος, η κάθε κρίσιμη ποσότητα αντιστοιχίζεται με ένα μοναδικό δυαδικό ψηφίο ετοιμότητας το οποίο όταν είναι ίσο με 1 μας πληροφορεί πως όλα τα `Dirty Bit` έχουν τεθεί ίσα με 1, δηλαδή ότι οι αντιστοιχιζόμενες διευθύνσεις τους, έχουν πλήρως εγγραφεί ή διαβαστεί.

1° ΣΤΑΔΙΟ

Στο αρχικό στάδιο κατά το οποίο η κάρτα πρόκειται να λάβει τα πρώτα δεδομένα από την τερματική συσκευή έχει όλα τα δυαδικά ψηφία ετοιμότητας και τα `Dirty Bit`, είναι ίσα με το 0. Η αρχική δηλαδή κατάσταση, `initial state`, προϋποθέτει ότι αφού καμία ποσότητα δεν έχει ληφθεί ή υπολογισθεί, τα αντιστοιχιζόμενα δυαδικά ψηφία τους πρέπει να είναι ίσα με 0.

2° ΣΤΑΔΙΟ

Σε αυτό το στάδιο, τα δυαδικά ψηφία αρχίζουν το ένα μετά το άλλο να τίθενται ίσον με 1, καθώς τα δεδομένα αποθηκεύονται στην κάρτα, αναλόγως πάντα με τη σημασία του κάθε δυαδικού ψηφίου. Δηλαδή, πρώτα θα τεθούν ίσον με 1 τα δυαδικά ψηφία εγγραφής ή ανάγνωσης, `Dirty Bits`, κάθε φορά που ένα τμήμα νέας ποσότητας γράφεται ή διαβάζεται και γενικότερα γίνει προσβάσιμο, και αφού όλα τα δυαδικά ψηφία εγγραφής ή ανάγνωσης της ποσότητας ανάψουν, τότε και μόνο τότε θα τεθεί ίσον με 1 και το δυαδικό ψηφίο ετοιμότητας της κρίσιμης ποσότητας.

3° ΣΤΑΔΙΟ

Αυτό το στάδιο αφορά τη χρονική στιγμή που όλα τα δυαδικά ψηφία ετοιμότητας όλων των κρίσιμων ποσοτήτων θα τεθούν ίσον με 1. Στο σημείο αυτό θα τεθεί ίσον με 1 και το κατάλληλο ψηφίο ετοιμότητας του κρυφού κλειδιού. Όταν αυτή η διαδικασία

ολοκληρωθεί, τότε όλα τα ψηφία ετοιμότητας και ψηφία εγγραφής ή ανάγνωσης, όλων των κρίσιμών ποσοτήτων, θα τεθούν πάλι ίσον με 0, μέχρι να αρχίσει εκ νέου υπολογισμός για τα επόμενα δύο δυαδικά ψηφία του κρυφού κλειδιού. Η μόνη ποσότητα της οποίας τα δυαδικά ψηφία ετοιμότητας δεν μηδενίζονται, είναι το κρυφό κλειδί αφού βάσει αυτών των ψηφίων ετοιμότητας γνωρίζουμε σε ποιο στάδιο του υπολογισμού βρισκόμαστε.

Γενικότερα αυτό που πρέπει να επισημάνουμε, είναι ότι το στάδιο των υπολογισμών που όπως έχουμε αναφέρει διατηρείται από τα δυαδικά ψηφία του κρυφού κλειδιού της κάρτας, προκύπτει από την μορφή του αλγορίθμου πρόσθεσης και Πολλαπλασιασμού της παραγράφου [§3.5]. Όπως ήδη έχουμε περιγράψει στην παράγραφο [§3.5], τα δυαδικά ψηφία του κλειδιού καθορίζουν την ποσότητα του $R[i]$ που πρέπει να επιλεγεί κάθε φορά και για το λόγο αυτό το κρυφό κλειδί επιλέγεται να είναι και η παράμετρος που θα καθορίζει το στάδιο των υπολογισμών στο οποίο βρισκόμαστε.

Για παράδειγμα, αν το κρυφό κλειδί είναι ίσο με $[15]$ σε δεκαδικό σύστημα, τότε η δυαδική του αναπαράσταση είναι $[1111]$ και η αναπαράσταση του προσημασμένου σημείου είναι $[1000 - 1]$. Άρα κατά την εξέλιξη του αλγορίθμου πρόσθεσης και Πολλαπλασιασμού της παραγράφου [§3.5], θα είχαμε:

- Για το πρώτο ψηφίο του κρυφού κλειδιού [1] υποδηλώνει ότι πρέπει να γίνει Διπλασιασμός σημείου και επιλογή του $R[1]$.
- Για το δεύτερο, τρίτο, τέταρτο ψηφίο του κρυφού κλειδιού [0] υποδηλώνει ότι πρέπει να γίνει μόνο Διπλασιασμός σημείου.
- Για το πέμπτο ψηφίο του κρυφού κλειδιού [-1] υποδηλώνει ότι πρέπει να γίνει Διπλασιασμός σημείου και επιλογή του $R[-1]$.

Άρα διαφαίνεται, ότι η γνώση του σε ποια δύο δυαδικά ψηφία του κρυφού κλειδιού βρισκόμαστε, είναι πολύ σημαντική για την ορθότητα των πράξεων και της εξέλιξης του πρωτοκόλλου.

Αυτό που συμβαίνει κάθε φορά που υπολογίζεται μια κρίσιμη ποσότητα, είναι η αποθήκευση της σε μια προκαθορισμένη θέση μέσα στην μνήμη και η παράλληλη ενημέρωση των κατάλληλων δυαδικών στοιχείων, όλων των τύπων, με τα οποία η κρίσιμη αυτή ποσότητα αντιστοιχίζεται. Τα συγκεκριμένα δυαδικά ψηφία βρίσκονται και αυτά σε προκαθορισμένες θέσεις προκειμένου να μην υπάρχουν καθυστερήσεις σε επίπεδο εύρεσης ελεύθερης θέσης μνήμης για εγγραφή. Η καθορισμένες θέσεις είναι αναγκαίες και στην περίπτωση κατά την οποία έχουμε αναγνώσεις. Αν τα δεδομένα που πρόκειται να διαβαστούν δεν βρίσκονται σε προκαθορισμένες και γνωστές θέσεις τότε θα έχουμε καθυστερήσεις καθώς θα πρέπει πριν διαβάσουμε τις ποσότητες αυτές, να τις εντοπίσουμε σε κάποια τυχαία κάθε φορά διεύθυνση της μνήμης.

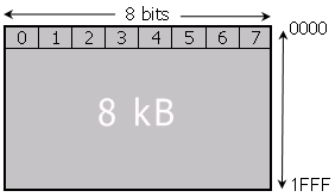
Σε περίπτωση που κάποια διακοπή ρεύματος λάβει χώρα, τότε ο τρόπος με τον οποίο θα λειτουργήσει ο μηχανισμός κατά την αποκατάσταση της έλλειψης ηλεκτρικού ρεύματος και τη σταθεροποίηση του, είναι ο εξής:

- Αρχικά θα διαβάσει όλα τα δυαδικά ψηφία ετοιμότητας προκειμένου να διαπιστώσει ποιές από τις κρίσιμες ποσότητες έχουν εγγραφεί πλήρως. Όσες από αυτές έχουν πλήρως υπολογισθεί, διατηρούνται ως έχουν και μπορούν να χρησιμοποιηθούν για τη συνέχιση των υπολογισμών.
- Όσα δυαδικά ψηφία ετοιμότητας δεν έχουν εγγραφεί τότε οι αντιστοιχιζόμενες σε αυτά κρίσιμες ποσότητες πρέπει να υπολογιστούν εκ νέου. Ο υπολογισμός

θα γίνει βάσει του σταδίου στο οποίο βρίσκεται ο αλγόριθμος, το οποίο υποδεικνύεται από τα δύο δυαδικά ψηφία του κρυφού κλειδιού των οποίων τα δύο προηγούμενα έχουν το αντιστοιχιζόμενο δυαδικό του ψηφίο ετοιμότητας ίσο με 1. Έτσι, αποφεύγουμε να ξεκινήσουμε τον υπολογισμό της ποσότητας από την αρχή, αλλά τον ξεκινάμε στο σημείο στο οποίο η πτώση τάσης έλαβε χώρα.

Έτσι στο προηγούμενο παράδειγμα κατά το οποίο το κρυφό κλειδί είναι ίσο με $[15]$ σε δεκαδικό σύστημα, δηλαδή έχει αναπαράσταση του προσημασμένου σημείου $[1000 - 1]$, αν ήταν $[1]$ το δυαδικό ψηφίο ετοιμότητας του πρώτου ψηφίου τότε μετά την αποκατάσταση θα εκτελούσαμε μόνο διπλασιασμό, ενώ αν ήταν το δυαδικό ψηφίο ετοιμότητας του τέταρτου ψηφίου θα εκτελούσαμε διπλασιασμό και αφαίρεση.

Στη συνέχεια θα δώσουμε ένα γραφικό παράδειγμα του τρόπου με το οποίο εξελίσσεται ο μηχανισμός. Θα ξεκινήσουμε από το αρχικό στάδιο, `initial state` και θα θεωρήσουμε ότι η οργάνωση της μνήμης είναι όπως φαίνεται στο παρακάτω σχήμα:



Σχήμα 8.1: Οργάνωση της διαρκούς, `non Volatile`, μνήμης

Η διαρκής μνήμη αυτή είναι μια μνήμη τύπου `Ferroelectric Random Access Memory, FeRAM`. Η `FeRAM`, έχει το πλεονέκτημα έναντι στις διαρκείς μνήμες `EEPROM, FLASH`, ότι έχει μικρότερο χρόνο πρόσβασης, ανάγνωσης και εγγραφής. Δίνουμε ένα πίνακα συγκρίσεως των διαρκών μνημών, από την εταιρία `[Fujitsu Microelectronics Europe, FME]`, ο οποίος επιβεβαιώνει τα παραπάνω.

	SRAM*1	SDRAM*2	E2PROM*3	FLASH*4	FRAM*5
Memory type	Volatile Backup	Volatile	Non Volatile	Non Volatile	Non Volatile
Cell structure	6T	1T/1C	2T	1T	2T/2C
Read cycle(Ns)	12	70	200	70	180
Internal write voltage(V)	3.3	3.3	20 (supply voltage 3.3V)	12 (supply voltage 3.3V)	5
Write cycle	12ns	70ns	3ms	1 sec.	180ns
Data write	Overwrite	Overwrite	Erase + Write	Erase + Write	Overwrite
Data erase	Bit	Bit	Byte (64 byte page)	Sector (8K, 16K, 32K, 64K)	Bit
Endurance	∞	∞	1E5	1E5	$1E10^{*6}$
Standby current (uA)	50000	1000	20	5	20
Read operation current (ma/operation)	180	80	30	15	15
Write operation current (ma/operation)	180	80	30	35	15

Σχήμα 8.2: Πίνακας σύγκρισης μνημών από την `Fujitsu`.

Παρατηρούμε ότι ο χρόνος εγγραφής και ο χρόνος ανάγνωσης είναι $180ns$, ενώ ο χρόνος πρόσβασης σε κάθε διεύθυνση μνήμης είναι $90ns$.

Επιπλέον πρέπει να σημειώσουμε ότι η κάθε ποσότητα αποτελείται στο παράδειγμα από 160 δυαδικά ψηφία, για λόγους ασφάλειας, και βάση αυτής της υπόθεσης χρειαζόμαστε:

Απαιτήσεις Μνήμης - Πρωτοκόλλου

- 20 διαφορετικές διευθύνσεις μνήμης για την αποθήκευση 160 δυαδικών ψηφίων δεδομένων όλων των ποσοτήτων εκτός από το κρυφό κλειδί που απαιτεί 40 διαφορετικές διευθύνσεις μνήμης, λόγω του ότι χρειάζεται δύο δυαδικά ψηφία για το κάθε ψηφίο προσημασμένης αναπαράστασης, (320 δυαδικά ψηφία).
- 3 διαφορετικές διευθύνσεις μνήμης για την αποθήκευση 20 δυαδικών ψηφίων εγγραφής - ανάγνωσης θέσης μνήμης, `Dirty bits`.
- 1 διεύθυνση μνήμης για την αποθήκευση 1 δυαδικού ψηφίου ετοιμότητας.

Για την περίπτωση του κρυφού κλειδιού, όπως ήδη είπαμε θα χρειαστούμε 40 διαφορετικές διευθύνσεις μνήμης για την αποθήκευση 320 δυαδικών ψηφίων δεδομένων, και 160 δυαδικών ψηφίων ετοιμότητας. Άρα για την εκτέλεση ενός Ελλειπτικού Πολλαπλασιασμού ενός ακεραίου, με ένα σημείο της Ελλειπτικής Καμπύλης χρειαζόμαστε συνολικά:

$$160 \times 9 + 320 \times 1 + 20 \times 8 + 1 \times 8 = 1.928bits.$$

Ο παραπάνω υπολογισμός έγινε για τις ποσότητες:

$$P(x, y), 2P(x, y), R[1](x, y), R[-1](x, y), K_{PrivSmCd}$$

Επιπλέον θα χρειαστούμε:

$$(160 + 20 + 1) \times 2 = 362bits$$

για τα `dirty` και `ready bits` των α, b.

Σύμφωνα με το πρωτόκολλο που προτείνουμε θα χρειαστούμε να επαναλάβουμε την πράξη του πολλαπλασιασμού μεταξύ ενός ακεραίου και ενός Ελλειπτικού σημείου 6 φορές.

1. Μια φορά για τον υπολογισμό του Δημόσιου Κλειδιού.
2. Μια φορά για τον υπολογισμό της ποσότητας $R1$.
3. Μια φορά για τον υπολογισμό της ποσότητας $R4$.
4. Τρεις φορές για τον υπολογισμό των Ελλειπτικών ποσοτήτων κατά την υλοποίηση του Κρυπταλγορίθμου `Menezes - Vanstone`.

Οι επιπλέον ποσότητες, οι οποίες είναι αναγκαίο να αποθηκευτούν στην μνήμη για την επιτυχή ολοκλήρωση του πρωτοκόλλου είναι:

- Το μέγεθος του πεδίου n.
- Η τάξη του σημείου P,$ord(P)$.
- Το δημόσιο κλειδί του τερματικού $K_{pubTerm}$.

- Η ποσότητα $R4$.
- Η κρυπτογραφημένη ποσότητα $enc(R3)$.
- Η κρυπτογραφημένη ποσότητα $enc(idTerm)$.
- Η `Hashed` τιμή του διαφοροποιημένου κλειδιού της κάρτας.

Άρα τα δυαδικά ψηφία που θα χρειαστούμε επιπλέον είναι:

$$(160 + 20 + 1) \times 7 = 1.267$$

Το μόνο πλέον που μένει, είναι να υπολογίζουμε το χρόνο που απαιτείται προκειμένου να ολοκληρωθεί η διαδικασία. Έτσι έχουμε:

Για κάθε ποσότητα με 160 δυαδικά ψηφία δεδομένων, 20 `Dirty bits` και 1 `Ready bit` χρειαζόμαστε:

$$((90ns + 180ns) \times 23)x2 = 12.420ns$$

Ο αριθμός 23 δηλώνει τις διευθύνσεις μνήμης που απαιτούνται, για την αποθήκευση $160 + 20 + 1$ δυαδικών ψηφίων, και το 2 δηλώνει ότι συμπεριλαμβάνουμε και τις δύο συνιστώσες του Ελλειπτικού σημείου. Ο παραπάνω χρόνος, αντιπροσωπεύει το χρόνο εγγραφής ενός Ελλειπτικού σημείου, για παράδειγμα το P. Εμείς, ανανεώνουμε αυτή την τιμή 160 φορές προκειμένου να έχουμε τον πλήρη υπολογισμό του. Άρα,

$$12.420ns \times 160 = 1.987.200ns$$

Αυτή η ανανέωση γίνεται για 4 ποσότητες τις:

$$P(x, y), 2P(x, y), R[1](x, y), R[-1](x, y)$$

Άρα έχουμε ότι:

$$1.987.200ns \times 4 = 7.948.800ns$$

Και για 7 ποσότητες: $P_{pubSmCd}, R1, R4$ και r_1, r_2, r_3 στο `Menezes - Vanstone`.

$$7.948.800ns \times 7 = 55.641.600ns$$

Επιπλέον έχουμε την ανάγνωση 160 φορές των ποσοτήτων $K_{privSmCd}, hash(R1), \alpha, b$

$$(((90 + 180) \times 40) + (90 + 180) \times 23) \times 3) \times 160) = 4.708.800ns$$

Τέλος έχουμε μια εγγραφή για το $encR3$, $encR3$ δηλαδή,

$$(((90 + 180) \times 23) \times 2) = 12420ns$$

Άρα συνολικά χρειαζόμαστε για πλήρη αποθήκευση όλων των κρίσιμων δεδομένων:

$$55.641.600ns + 4.708.800ns + 12420ns = 60.362.820ns$$

Σύμφωνα με τα παραπάνω, καταλήγουμε στο εξής:

- Χρειάζεται να αποθηκεύσουμε 3557 δυαδικά ψηφία, δεδομένων,`State, Dirty` και `Ready`.
- Ο χρόνος που απαιτείται προκειμένου να ολοκληρωθεί αυτή η διαδικασία είναι 60.362.820ns=60ms.

Αν αναλογιστούμε ότι ο ρυθμός με τον οποίο τα δεδομένα αποστέλλονται από την μια οντότητα στην άλλη είναι `106kbits/s`, και ότι το συνολικό πλήθος δεδομένων που αποστέλλεται είναι 3.280 δυαδικά ψηφία για τις ποσότητες

$$\alpha, b, n, P, R1, P_{pubTerm}, P_{pubSmCd}, , P_{privSmCd}, R2, R4, enc(R3), encId_{Term}, idCard,$$

τότε ο χρόνος μετάδοσης θα είναι ίσος με

$$\frac{3.280}{106.000} = 0.031sec = 31ms$$

Αν δεν εφαρμόσουμε τη διαδικασία του μηχανισμού αποθήκευσης, τότε μόνο η αποστολή των νέων δεδομένων θα μας κοστίσει όσο ο χρόνος αποθήκευσης τους μέσω του μηχανισμού που προτείνουμε, χωρίς να συμπεριλαμβάνουμε το κόστος λόγω των πράξεων του πρωτοκόλλου. Επίσης, δεν πρέπει να ξεχνάμε και τον χρόνο που θα μεσολαβήσει μέχρι να γίνει εκ νέου η επικοινωνία μεταξύ της κάρτας και του τερματικού, μετά τη σταθεροποίηση του ηλεκτρικού ρεύματος.

Άρα συμπεραίνουμε ότι σε κάθε περίπτωση υπερέχουμε με την υλοποίηση του συγκεκριμένου μηχανισμού αποθήκευσης των κρίσιμων δεδομένων.

8.3 Περιγραφή Παραδείγματος

Το παράδειγμα που θα παρουσιάσουμε, όπως ήδη έχουμε αναφέρει, αφορά την μορφή της μνήμης κατά το αρχικό πρώτο στάδιο του υπολογισμού της βασικής πράξης των Ελλειπτικών καμπυλών, δηλαδή του πολλαπλασιασμού ακεραίου του χώρου και του σημείου βάσης της Ελλειπτικής Καμπύλης, μέσω του αλγορίθμου της πρόσθεσης και πολλαπλασιασμού που έχει εισαχθεί και περιγραφεί στην παράγραφο [§3.5] αλλά για λόγους ευκολίας δίδεται και παρακάτω.

1. $R[0] \leftarrow P$
2. **for** $i = n - 2$ **to** 0
3. $R[0]$=2$R[0]$
4. $R[1]$=$R[0] + P$
5. $R[-1]$=$R[0] - P$
6. $R[0]$ = R[k_i]
7. **Return** $R[0]$

Πρέπει να επισημάνουμε, ότι στο σημείο αυτό τα δεδομένα δεν έχουν ληφθεί ακόμα από την κάρτα, έτσι δείχνουμε την μορφή που θα έχει η μνήμη προκειμένου να αποθηκεύσει τα δεδομένα και να υλοποιηθεί ο μηχανισμός που προτείνουμε.

Έτσι για το σημείο βάσης της Ελλειπτικής Καμπύλης P έχουμε:

CRUCIAL QUANTITY P

	address	8 bits
P(x)	xxx0h : xx13h	data : data
dirty bits P(x) dirty bits P(x) dirty bits P(x)	xxx0h xxx1h xxx2h	00000000 00000000 0000xxxx
Ready bit P(x)	xxx3h	0xxxxxxxx
P(y)	xxx0h : xx13h	data : data
dirty bits P(y) dirty bits P(y) dirty bits P(y)	xxx0h xxx1h xxx2h	00000000 00000000 0000xxxx
Ready bit P(y)	xxx3h	0xxxxxxx

Σχήμα 8.3: Αρχικό στάδιο αποθήκευσης του σημείου βάσης P στη διαρκή, `non Volatile`, μνήμη

Για το διπλάσιο του σημείου P, δηλαδή το σημείο $2P$ έχουμε:

CRUCIAL QUANTITY 2P

	address	8 bits
2P(x)	xxx0h : xx13h	data : data
dirty bits 2P(x) dirty bits 2P(x) dirty bits 2P(x)	xxx0h xxx1h xxx2h	00000000 00000000 0000xxxx
Ready bit 2P(x)	xxx3h	0xxxxxxx
2P(y)	xxx0h : xx13h	data : data
dirty bits 2P(y) dirty bits 2P(y) dirty bits 2P(y)	xxx0h xxx1h xxx2h	00000000 00000000 0000xxxx
Ready bit 2P(y)	xxx3h	0xxxxxxx

Σχήμα 8.4: Αρχικό στάδιο αποθήκευσης του σημείου $2P$ στη διαρκή, `non Volatile`, μνήμη

Για την ποσότητα $R[1]$ το οποίο είναι σημείο της Ελλειπτικής Καμπύλης:

CRUCIAL QUANTITY R[1]

	address	8 bits
R[1](x)	xxx0h : xx13h	data : data
dirty bits R[1](x)	xxx0h	00000000
dirty bits R[1](x)	xxx1h	00000000
dirty bits R[1](x)	xxx2h	0000xxxx
Ready bit R[1](x)	xxx3h	0xxxxxxx
R[1](y)	xxx0h : xx13h	data : data
dirty bits R[1](y)	xxx0h	00000000
dirty bits R[1](y)	xxx1h	00000000
dirty bits R[1](y)	xxx2h	0000xxxx
Ready bit R[1](y)	xxx3h	0xxxxxxx

Σχήμα 8.5: Αρχικό στάδιο αποθήκευσης του σημείου $R[1]$ στη διαρκή, `non Volatile`, μνήμη

Για την ποσότητα $R[-1]$ το οποίο είναι σημείο της Ελλειπτικής Καμπύλης:

CRUCIAL QUANTITY R[-1]

	address	*8 bits*
R[-1](x)	xxx0h : xx13h	data : data
dirty bits R[-1](x)	xxx0h	00000000
dirty bits R[-1](x)	xxx1h	00000000
dirty bits R[-1](x)	xxx2h	0000xxxx
Ready bit R[-1](x)	xxx3h	0xxxxxxx
R[1](y)	xxx0h : xx13h	data : data
dirty bits R[-1](y)	xxx0h	00000000
dirty bits R[-1](y)	xxx1h	00000000
dirty bits R[-1](y)	xxx2h	0000xxxx
Ready bit R[-1](y)	xxx3h	0xxxxxxx

Σχήμα 8.6: Αρχικό στάδιο αποθήκευσης του σημείου $R[-1]$ στη διαρκή, `non Volatile`, μνήμη

Για την παράμετρο α, b της Ελλειπτικής Καμπύλης:

CRUCIAL QUANTITIES α,b

	address	8 bits
α	xxx0h	data
	:	:
	xx13h	data
dirty bits α	xxx0h	00000000
dirty bits α	xxx1h	00000000
dirty bits α	xxx2h	0000xxxx
Ready bit α	xxx3h	0xxxxxxx
b	xxx0h	data
	:	:
	xx13h	data
dirty bits b	xxx0h	00000000
dirty bits b	xxx1h	00000000
dirty bits b	xxx2h	0000xxxx
Ready bit b	xxx3h	0xxxxxxx

Σχήμα 8.7: Αρχικό στάδιο αποθήκευσης των παραμέτρων α, b στη διαρκή, non Volatile, μνήμη

Και φυσικά για το κρυφό κλειδί, ή τον ακέραιο ο οποίος θα πολλαπλασιαστεί με το σημείο βάσης P προκειμένου να έχουμε τη δημιουργία του δημόσιου κλειδιού:

SECRET KEY

address	8 bits	STATE bits
xxx0h	data	00000000
xxx1h	data	00000000
:	:	:
:	:	:
xx13h	data	00000000
xxa0h	data	------
:	:	:
:	:	:
xx27h	data	------

Σχήμα 8.8: Αρχικό στάδιο αποθήκευσης του κρυφού κλειδιού στη διαρκή, non Volatile, μνήμη

Μια σημείωση η οποία πρέπει να γίνει στο σημείο αυτό, αφορά την διευθυνσιοδότηση της μνήμης. Στα σχήματα τα δυαδικά ψηφία της διεύθυνσης της μνήμης από $1-$ το δυαδικό ψηφίο που καθορίζει την ευθυγράμμιση της μνήμης συμβολίζονται με x, καθώς το μόνο που απαιτούμε είναι η κάθε ποσότητα να αποθηκεύεται σε διαφορετική θέση μνήμης έτσι ώστε να μην υπάρχουν επανεγγραφές διαφορετικών ποσοτήτων στην ίδια θέση μνήμης. Ωστόσο, δεν έχουμε ιδιαίτερους περιορισμούς σχετικά με το ποια θέση μνήμης θα είναι αυτή, αρκεί αυτή να είναι ευθυγραμμισμένη, κάτι το οποίο το εξασφαλίζουμε με τα απαιτούμενα κάθε φορά δυαδικά ψηφία. Επίσης, με τον όρο data συμβολίζουμε την θέση μνήμης εκείνη στην οποία θα αποθηκευτούν τα δεδομένα τα οποία θα συμβολίζουμε με Received.

Στη συνέχεια δίνουμε ένα στιγμιότυπο της κατάστασης της μνήμης, έτσι όπως αυτή φαίνεται να είναι κατά τη διάρκεια αποθήκευσης των κρίσιμων ποσοτήτων. Σημειώνουμε ότι ο υπολογισμός αυτός είναι κατά τη διάρκεια του πρώτου σταδίου, και πριν τον πλήρη υπολογισμό όλων των ποσότητων. Η ποσότητες που κατά τη διάρκεια του στιγμιότυπου έχουν πλήρως αποθηκευτεί είναι το κρυφό κλειδί και το σημείο βάσης P.

Για το σημείο βάσης P έχουμε:

CRUCIAL QUANTITY P

CRUSIAL QUANTITY P	address	8 bits
P(x)	xxx0h : xx13h	received : received
dirty bits P(x)	xxx0h	11111111
dirty bits P(x)	xxx1h	11111111
dirty bits P(x)	xxx2h	1111xxxx
Ready bit P(x)	xxx3h	1xxxxxxxx
P(y)	xxx0h : xx13h	received : received
dirty bits P(y)	xxx0h	11111111
dirty bits P(y)	xxx1h	11111111
dirty bits P(y)	xxx2h	1111xxxx
Ready bit P(y)	xxx3h	1xxxxxxx

Σχήμα 8.9: Στιγμιότυπο ολοκληρωμένης αποθήκευσης του σημείου βάσης P στη διαρκή, `non Volatile`, μνήμη

Για το διπλάσιο του σημείου βάσης $2P$:

CRUCIAL QUANTITY 2P

	address	8 bits
2P(x)	xxx0h : xx13h	received : data
dirty bits 2P(x)	xxx0h	11111111
dirty bits 2P(x)	xxx1h	11111111
dirty bits 2P(x)	xxx2h	0000xxxx
Ready bit 2P(x)	xxx3h	0xxxxxxxx
2P(y)	xxx0h : xx13h	received : data
dirty bits 2P(y)	xxx0h	11111111
dirty bits 2P(y)	xxx1h	00000000
dirty bits 2P(y)	xxx2h	0000xxxx
Ready bit 2P(y)	xxx3h	0xxxxxxx

Σχήμα 8.10: Στιγμιότυπο αποθήκευσης του διπλασίου σημείου βάσης $2P$ στη διαρκή, `non Volatile`, μνήμη

Για την ποσότητα $R[1]$:

CRUCIAL QUANTITY R[1]

	address	8 bits
R[1](x)	xxx0h : xx13h	received : data
dirty bits R[1](x)	xxx0h	11111111
dirty bits R[1](x)	xxx1h	00000000
dirty bits R[1](x)	xxx2h	0000xxxx
Ready bit R[1](x)	xxx3h	0xxxxxxx
R[1](y)	xxx0h : xx13h	data : data
dirty bits R[1](y)	xxx0h	00000000
dirty bits R[1](y)	xxx1h	00000000
dirty bits R[1](y)	xxx2h	0000xxxx
Ready bit R[1](y)	xxx3h	0xxxxxxx

Σχήμα 8.11: Στιγμιότυπο της αποθήκευσης της ποσότητας $R[1]$, στη διαρκή, non `Volatile`, μνήμη

Για την ποσότητα $R[-1]$:

CRUCIAL QUANTITY R[-1]

	address	*8 bits*
R[-1](x)	xxx0h : xx13h	received : data
dirty bits R[-1](x)	xxx0h	11111111
dirty bits R[-1](x)	xxx1h	00000000
dirty bits R[-1](x)	xxx2h	0000xxxx
Ready bit R[-1](x)	xxx3h	0xxxxxxx
R[1](y)	xxx0h : xx13h	received : data
dirty bits R[-1](y)	xxx0h	11111111
dirty bits R[-1](y)	xxx1h	00000000
dirty bits R[-1](y)	xxx2h	0000xxxx
Ready bit R[-1](y)	xxx3h	0xxxxxxx

Σχήμα 8.12: Στιγμιότυπο της αποθήκευσης της ποσότητας $R[-1]$, στη διαρκή, non `Volatile`, μνήμη

Για τις ποσότητες α, b:

CRUCIAL QUANTITIES α,b

	address	8 bits
α	xxx0h : xx13h	received : data
dirty bits α	xxx0h	11111111
dirty bits α	xxx1h	00000000
dirty bits α	xxx2h	0000xxxx
Ready bit α	xxx3h	0xxxxxxx
b	xxx0h : xx13h	received : data
dirty bits b	xxx0h	11111111
dirty bits b	xxx1h	00000000
dirty bits b	xxx2h	0000xxxx
Ready bit b	xxx3h	0xxxxxxx

Σχήμα 8.13: Στιγμιότυπο της αποθήκευσης των ποσοτήτων α, b, στη διαρκή, non `Volatile`, μνήμη

Και για το κρυφό κλειδί:

SECRET KEY

address	8 bits	STATE bits
xxx0h	data	00000000
xxx1h	data	00000000
:	:	:
:	:	:
xx13h	data	00000000
xxa0h	data	------
:	:	:
:	:	:
xx27h	data	------

Σχήμα 8.14: Στιγμιότυπο της αποθήκευσης του κρυφού κλειδιού, στη διαρκή, non `Volatile`, μνήμη

Στο σημείο αυτό δίνουμε τη σχηματική αναπαράσταση της τελικής μορφής της πρώτης φάσης του μηχανισμού, όπου όλες οι κρίσιμες ποσότητες έχουν υπολογισθεί, δηλαδή όλα τα δυαδικά ψηφία εγγραφής, ανάγνωσης και ετοιμότητας έχουν τεθεί ίσον με 1.

Έτσι για το σημείο βάσης P έχουμε:

CRUCIAL QUANTITY P

CRUSIAL QUANTITY P	address	8 bits
P(x)	xxx0h : xx13h	received : received
dirty bits P(x)	xxx0h	11111111
dirty bits P(x)	xxx1h	11111111
dirty bits P(x)	xxx2h	1111xxxx
Ready bit P(x)	xxx3h	1xxxxxxx
P(y)	xxx0h : xx13h	received : received
dirty bits P(y)	xxx0h	11111111
dirty bits P(y)	xxx1h	11111111
dirty bits P(y)	xxx2h	1111xxxx
Ready bit P(y)	xxx3h	1xxxxxxx

Σχήμα 8.15: Στιγμιότυπο ολοκληρωμένης αποθήκευσης του σημείου βάσης P στη διαρκή, `non Volatile`, μνήμη στο τέλος της πρώτης φάσης.

Για το διπλάσιο του σημείου βάσης $2P$:

CRUCIAL QUANTITY 2P

	address	8 bits
2P(x)	xxx0h : xx13h	received : received
dirty bits 2P(x)	xxx0h	11111111
dirty bits 2P(x)	xxx1h	11111111
dirty bits 2P(x)	xxx2h	1111xxxx
Ready bit 2P(x)	xxx3h	1xxxxxxx
2P(y)	xxx0h : xx13h	received : received
dirty bits 2P(y)	xxx0h	11111111
dirty bits 2P(y)	xxx1h	11111111
dirty bits 2P(y)	xxx2h	1111xxxx
Ready bit 2P(y)	xxx3h	1xxxxxxx

Σχήμα 8.16: Στιγμιότυπο της ολοκληρωμένης αποθήκευσης του διπλασίου σημείου βάσης $2P$ στη διαρκή, `non Volatile`, μνήμη στο τέλος της πρώτης φάσης.

Για την ποσότητα $R[1]$:

CRUCIAL QUANTITY R[1]

	address	8 bits
R[1](x)	xxx0h : xx13h	received : received
dirty bits R[1](x)	xxx0h	11111111
dirty bits R[1](x)	xxx1h	11111111
dirty bits R[1](x)	xxx2h	1111xxxx
Ready bit R[1](x)	xxx3h	1xxxxxxx
R[1](y)	xxx0h : xx13h	data : data
dirty bits R[1](y)	xxx0h	11111111
dirty bits R[1](y)	xxx1h	11111111
dirty bits R[1](y)	xxx2h	1111xxxx
Ready bit R[1](y)	xxx3h	1xxxxxxx

Σχήμα 8.17: Στιγμιότυπο της ολοκληρωμένης αποθήκευσης της ποσότητας $R[1]$, στη διαρκή, `non Volatile`, μνήμη στο τέλος της πρώτης φάσης.

Για την ποσότητα $R[-1]$:

CRUCIAL QUANTITY R[-1]

	address	8 bits
R[-1](x)	xxx0h : xx13h	received : received
dirty bits R[-1](x)	xxx0h	11111111
dirty bits R[-1](x)	xxx1h	11111111
dirty bits R[-1](x)	xxx2h	1111xxxx
Ready bit R[-1](x)	xxx3h	1xxxxxxx
R[1](y)	xxx0h : xx13h	received : received
dirty bits R[-1](y)	xxx0h	11111111
dirty bits R[-1](y)	xxx1h	11111111
dirty bits R[-1](y)	xxx2h	1111xxxx
Ready bit R[-1](y)	xxx3h	1xxxxxxx

Σχήμα 8.18: Στιγμιότυπο της ολοκληρωμένης αποθήκευσης της ποσότητας $R[-1]$, στη διαρκή, `non Volatile`, μνήμη στο τέλος της πρώτης φάσης.

Για τις ποσότητες α, b:

CRUCIAL QUANTITIES α , b

	address	8 bits
α	xxx0h	received
	:	:
	xx13h	received
dirty bits α	xxx0h	11111111
dirty bits α	xxx1h	11111111
dirty bits α	xxx2h	1111xxxx
Ready bit α	xxx3h	1xxxxxxx
b	xxx0h	received
	:	:
	xx13h	received
dirty bits b	xxx0h	11111111
dirty bits b	xxx1h	11111111
dirty bits b	xxx2h	1111xxxx
Ready bit b	xxx3h	1xxxxxxx

Σχήμα 8.19: Στιγμιότυπο της ολοκληρωμένης αποθήκευσης των α, b, στη διαρκή, `non Volatile`, μνήμη στο τέλος της πρώτης φάσης.

Και για το κρυφό κλειδί:

SECRET KEY

address	8 bits	STATE bits
xxx0h	received	10000000
xxx1h	received	00000000
:	:	:
:	:	:
xx13h	received	00000000
xxa0h	received	------
:	:	:
:	:	:
xx27h	received	------

Σχήμα 8.20: Στιγμιότυπο της ολοκληρωμένης αποθήκευσης του κρυφού κλειδιού, στη διαρκή, `non Volatile`, μνήμη στο τέλος της πρώτης φάσης.

Παρατηρούμε ότι το πρώτο δυαδικό ψηφίο του κρυφού κλειδιού τίθεται ίσον 1, σηματοδοτώντας έτσι το τέλος των υπολογισμών για τη πρώτη φάση του μηχανισμού. Αν βρισκόμασταν για παράδειγμα, στο τέλος της τρίτης φάσης τότε σύμφωνα με το μηχανισμό θα είχε τεθεί με ίσο με 1, το τρίτο κατά σειρά δυαδικό ψηφίο του κρυφού κλειδιού. Όλες οι υπόλοιπες κρίσιμες ποσότητες θα είχαν μορφή όπως και αυτή που παρουσιάζεται στο τελευταίο στάδιο της πρώτης φάσης, δηλαδή έχοντας όλα τα δυαδικά ψηφία εγγραφής, ανάγνωσης, και ετοιμότητας ίσα με 1. Το κρυφό κλειδί θα είχε σε αυτό το στάδιο την παρακάτω μορφή:

SECRET KEY

address	8 bits	STATE bits
xxx0h	received	00100000
xxx1h	received	00000000
:	:	:
:	:	:
xx13h	received	00000000
xxa0h	received	------
:	:	:
:	:	:
xx27h	received	------

Σχήμα 8.21: Στιγμιότυπο της ολοκληρωμένης αποθήκευσης του κρυφού κλειδιού, στη διαρκή, `non Volatile`, μνήμη στο τέλος της τρίτης φάσης.

Κεφάλαιο 9

Επίλογος και Συμπεράσματα

Στην εργασία αυτή, ο πρωταρχικός στόχος ήταν η πιστοποίηση της ταυτότητας δύο οντοτήτων, της ασύρματης έξυπνης κάρτας και της τερματικής συσκευής, μέσω της συμφωνίας των δημόσιων κλειδιών τους και η διασφάλιση του καναλιού επικοινωνίας τους. Η επίτευξη αυτού του στόχου, έγινε με την πρόταση ενός πρωτοκόλλου, το οποίο χρησιμοποιώντας τις ιδιότητες των Ελλειπτικών Καμπυλών, κατάφερε όχι μόνο να πιστοποιήσει με ασφάλεια την ταυτότητα των δύο συμβαλλόμενων οντοτήτων, αλλά επίσης να διασφαλίσει την επικοινωνία τους δημιουργώντας δημόσια κλειδιά, τα οποία θα μπορούν να χρησιμοποιηθούν για την κρυπτογράφηση των δεδομένων τους.

Οι Ελλειπτικές Καμπύλες κατάφεραν χάρη στις μοναδικές τους ιδιότητες, να προσδώσουν ταχύτητα στη διεκπεραίωση του πρωτοκόλλου και παράλληλα ελάττωση της απαιτούμενης υπολογιστικής ισχύος, χωρίς να επιβάλουν κανένα κόστος στο πλαίσιο της ασφάλειας. Χρησιμοποιώντας μεθόδους βελτιστοποίησης των πράξεων των Ελλειπτικών Καμπύλων, καταφέραμε να προσδώσουμε ακόμα μεγαλύτερη ταχύτητα , κάνοντας έτσι ακόμα πιο αποδοτικό το πρωτόκολλο που προτείνουμε. Αυτή η υπόθεση επιβεβαιώθηκε και από τις μετρήσεις τις οποίες κάναμε, σε σχέση ήδη επιτυχημένο αλγόριθμο RSA, αλλά συγκριτικά και με μη βελτιστοποιημένα, από άποψη πράξεων, μοντέλα πιστοποίησης ταυτότητας που έχουν σαν βάση της ασφάλειας τους την θεωρία των Ελλειπτικών Καμπυλών.

Επιπλέον, στη συγκεκριμένη εργασία προτείναμε έναν μηχανισμό διαχείρισης της στατικής μνήμης της ασύρματης κάρτας. Ουσιαστικά προτείναμε, την αποθήκευση στη στατική μνήμη, κάποιων αναγκαίων για την εξέλιξη του πρωτοκόλλου ποσοτήτων, στις οποίες αντιστοιχίσαμε δυαδικά ψηφία εγγραφής, ανάγνώσης και ετοιμότητας, προκειμένου να γνωρίζουμε την κατάσταση υπολογισμού τους, ανά πάσα στιγμή. Έτσι, ακόμα κι αν κάποια στιγμή συμβεί διακοπή ηλεκτρικού ρεύματος, δεν θα χρειαστεί να επαναποσταλλούν οι αναγκαίες ποσότητες από την μεριά του τερματικού, αφού η κάρτα θα μπορεί να τις επαναφέρει από τη δική της μνήμη. Με αυτό τον τρόπο, καταφέραμε να μειώσουμε τον χρόνο συνδιαλλαγής μεταξύ των δύο οντοτήτων και παράλληλα, να μειώσουμε τον κίνδυνο επιθέσεων, που έχουν σαν στόχο την παρακολούθηση του καναλιού μέσω ηθελημένων διακοπών του ηλεκτρικού ρεύματος.

Τέλος, προτείναμε τη διατήρηση ενός μετρητή στη διαρκή μνήμη της κάρτας, ο οποίος θα ελέγχει το πλήθος των επαναλήψεων αποστολής του ίδιου σημείου από το τερματικό, ώστε να αποφύγουμε επιθέσεις που έχουν σαν στόχο, την εύρεση του κρυφού κλειδιού, μέσω της διαρκούς αποστολής ενός επαναλαμβανόμενου σημείου.

Κεφάλαιο 10

Βιβλιογραφία

[ASM98] Kiyomichi Araki, Takakazu Satoh, Shinji Miura, *"Overview of Elliptic Curve Cryptography"*. PKC98 proceedings, eds: H. Imai, Y. Zheng, Lect. Notes in Computer Science Vol.1431, 29-49, (1998), Springer-Verlag.

[CLa00] C. Lambrinoudakis, *"Using Smart Cards in an Educational Environment"*, University of the Aegean, Department of Information and Communication Systems, (2000).

[Cer02] Certicom ECC Challenge (2002), available at: ***http://www.certicom.com***.

[DES83] American National Standards Institute, American National Standard for Information Systems: Data Link Encryption, ANSI X3.106, (1983).

[DOW92] W.Diffie, P. van Oorschot and M. Wienner, *"Authentication and authenticated key exchanges"*, Designs Codes and Cryptography 2 (1992) 107-105.

[Elg85] Taher El Gamal: *"A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms"*. CRYPTO (1984): 10-18.

[FIP95] FIPS PUB 180-1, Secure Hash Standard, Federal Information Processing Standards Publication 180-1, U.S. Department of Commerce/National Institute of Standards and Technology, National Technical Information Service, Springfield, Virginia, April 17, (1995) (supersedes FIPS PUB 180). Available at ***http://www.itl.nist.gov/div897/pubs/fip180-1.htm***.

[Fre98] G. Frey, *"How to disguise an Elliptic Curve (Weil descent)"*, talk ECC'98. Available at: ***http://www.cacr.math.uwaterloo.ca***.

[GSm99] S. Galbraith and N. Smart, *"A cryptographic application of Weil Descent"*, LNCS 1746 (1999), Springer-Verlag 191-200.

[GHS00] P. Gaurdy, F. Hess and N.Smart *"Constructive and destructive facets of Weil descent on elliptic curves"*, preprint (January 2000).

[GLVmc] R. Gallant, R. Lambert and S.Vanstone, *"Improving the parallised Pollard lambda search on binary anomalous curves"*, to appear in Mathematics of Computation.

[I7811] ISO/IEC 7811 *Identification Cards - Recording Techniques*.

[14443] ISO 14443, *Identification cards - Contactless integrated circuit(s) cards - Proximity cards*.

[JMe00] D. Johnson, A. Menezes, *"The Elliptic Curve Digital Signature Algorithm (ECDSA)"*, Technical Report CORR 99-34 Dept of C&O, Univ. Waterloo, Canada.

[KKi97] K. Kiefer, *"A Weakness of the Menezes-Vanstone Cryptosystem"*, University of Saarlandes, CS department, Germany (1997).

[KOB94] N.Koblitz, *"A Course in Number Theory and Cryptography"*, 2nd edition Springer-Verlag, (1994).

[LZi94] G.Lay and H.Zimmer,*"Constructing elliptic curves with given group order over large finite fields"*, `Algorithmic Number Theory`, Lecture Notes in Computer Science, 877 (1994), Springer Verlag.

[Men93] A. Menezes *"Elliptic Curve Public key Cryptosystems"*, Kluwer, Academic Publisher, Boston, (1993).

[Men95] A. Menezes, *"Elliptic Curve Cryptosystems"*, CryptoBytes vol.1 no.2 (1995), RSA Labs, available at:***ftp://ftp.rsa.com/pub/cryptobytes/crypto1n2.pdf***

[Mor91] F. Morain, *"Building cyclic elliptic curves modulo large primes"*, D. W. Davies, editor, Advances in Cryptology - EUROCRYPT 91, Lecture Notes in Computer Science 547 (1991), Springer-Verlag, 328-336.

[MOV93] A. Menezes, T. Okamoto and S. Vanstone, *"Reducing elliptic curve logarithms to logarithms in a finite field"*, IEEE Transactions on Information Theory 39 (1993), 1639-1646.

[MOV96] A. Menezes, P. van Oorschot and S. Vanstone, *"Handbook of Applied Cryptography"*, CRC Press,(1996), ***http://www.cacr.math.uwaterloo.ca/hac/***.

[P1363] IEEE P1363, *Standard Specifications for Public-Key Cryptography*, ballot draft (1999). Available at: ***http://grouper.ieee.org/groups/1363/index.html***.

[Pol78] J. M. Pollard, *"Monte Carlo methods for index computation (mod p)"*, Mathematics of Computation 32 (1978), 918-924.

[PHe78] S. Pohlig and M. Hellman, *"An improved algorithm for computing logarithms over GF(p) and its cryptographic significance"*, IEEE Transactions on Information Theory, 24 (1978), 106-110.

[ROSbk] *"Implementing Elliptic Curve Cryptography"*, Michael Rosing, Manning.

[RSA78] R. Rivest, A. Shamir, and L. M. Adleman, *"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems."* Communications of the ACM, 21, 2, 120-126, Feb 1978.

[SAr98] T. Satoh and K. Araki, *"Fermat quotients and the polynomial time log algorithm for anomalous elliptic curves"*, Commentarii Mathematici Universitatis Sancti Pauli, 47, (1998), 81-92.

[ScHb0] Rankl Effing, *"Smart Card Handbook"*, Wiley, Second edition 2000.

[Sem98] I. Semaev *"Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p"*, Mathematics of Computation, 67, (1998), 353-356.

[SHA-1] National Institute of Standards and Technology, U.S. Department of Commerce, Secure Hash Standard: Work in Progress, NIST FIPS PUB 180-1, May 31, (1994).

[SSt97] R. Silverman and J. Stapleton, Contribution to ANSI X9F1, working group, 1997.

[Sma99] N. Smart *"The discrete logarithm problem on elliptic curves of trace one"*, Journal of Cryptology, 12 ,(1999) 193-196.

[VWi99] P. van Oorschot and M. Wiener, *"Parallel collision search with cryptanalytic application"*, Journal of Cryptology, 12 (1999), 1-28.

[WZu99] R. Zuccherato, *"The equivalence between elliptic curve and quadratic function field discrete logarithms in characteristic 2"*, in J.P Buhler, editor, Algorithmic Number Theory, Proceedings Third Intern. Symp., ANTS-III, LNCS, 1423 (1998), Springer-Verlag 621-638.

[MipsA] ***http://www.mips.com***.

[GempA] ***http://www.gemplus.com***.

[PhilA] ***http://www.philips.com***.