ΚΡΥΠΤΟΓΡΑΦΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ ΒΑΣΙΖΟΜΕΝΟΙ ΣΕ ΜΗ ΓΡΑΜΜΙΚΑ ΣΥΣΤΗΜΑΤΑ

ΧΡΙΣΤΟΠΟΥΛΟΥ ΜΑΡΙΑ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΝΟΕΜΒΡΙΟΣ 2004

Η μεταπτυχιακή αυτή εργασία κατατέθηκε το Νοέμβριο του 2004 στο Πανεπιστήμιο Κρήτης. Την επιτροπή αξιολόγησής της αποτέλεσαν, εκτός του επιβλέποντα καθηγητή κ.Θεόδουλου Γαρεφαλάκη, οι κ.Νικόλαος Τζανάκης και κ.Αλέξανδρος Κουβιδάκης.

Ευχαριστίες

Η περάτωση της μεταπτυχιακής μου εργασίας δεν είναι μόνο αποτέλεσμα προσωπικής μου εργασίας αλλά και συνεργασιάς με ανθρώπους που με βοήθησαν πολύ. Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγήτη μου κ.Θεόδουλο Γαρεφαλάκη για την άψογη συνεργασία μας και την συστηματική προσπάθειά του να μου μεταδώσει λίγες απο τις γνώσεις του, τον κ.Γιάννη Μιχό για την βοήθεια του στο Gap 4 που χρησιμοποιήθηκε για τις πράξεις στα παραδείγματα και για την ψυχική στήριξη που μου παρείχε. Επίσης, πολλα ευχαριστώ χρωστώ στους συμφοιτητές μου στη Γ114, τον Ανδρέα Τσιλιφώνη, Ελένη Μηλάκη, Βαγγέλη Λάτο, Κώστα Ραμπαλάκο και Γιώργο Ζάρακα για την βοήθειά τους στα μαθήματα, τα ευχάριστα διαλείματα κατα την διάρκεια των απεριόριστων ωρών μελέτης και την υπομονή τους στις δύσκολες ώρες. Τέλος, ένα μεγάλο ευχαριστώ στους γονείς μου Κώστα και Αγγελική και τις αδερφές μου Νικολέττα και Σταυρούλα για την απεριόριστη στήριξή τους όλα αυτά τα χρόνια.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Η κλασική κρυπτογραφία χρησιμοποιεί τη μέθοδο secret key ή symmetric cryptography για την κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων, η οποία βασίζεται στην χρήση ενός κοινού μυστικού κλειδιού ανάμεσα στον αποστολέα και στον παραλήπτη του μηνύματος. Το κύριο πρόβλημα που εμφανίζεται είναι στην συμφωνία του μυστικού κλειδιού μεταξύ των χρηστών, διαδικασία που καθίσταται δύσκολη όταν ο αριθμός των χρηστών είναι μεγάλος ή βρίσκονται σε διαφορετικές τοποθεσίες, οπότε είναι απαραίτητη η χρήση μέσων επικοινωνίας και συνεπως είναι σε κίνδυνο η ασφάλεια του μυστικού κλειδιού.

Η ιδέα του δημοσίου κλειδιού στην κρυπτογραφία παρουσιάστηκε το 1976 από τους Whitfield Diffie και Martin Hellman, προκειμένου να επιλύσουν το πρόβλημα διαχείρισης του μυστικού κλειδιού. Σύμφωνα με αυτήν, κάθε χρήστης διαθέτει ένα ζευγάρι κλειδιών, το δημόσιο κλειδί που το δημοσιοποιεί και το ιδιωτικό του κλειδί, που παραμένει κρυφό. Όλες οι επικοινωνίες κάνουν χρήση των δημοσίων κλειδιών, ενώ κανένα ιδιωτικό κλειδί δεν μεταφέρεται ποτέ ή μοιράζεται. Η κρυπτογραφία με δημόσιο κλειδί μπορεί να χρησιμοποιηθεί όχι μόνο για ανταλλαγή μηνυμάτων αλλά και για πιστοποίηση ψηφιακών υπογραφών, σε αντίθεση με την κρυπτογραφία κρυφού κλειδιού όπου η έννοια της ψηφιακής υπογραφής δεν υφίσταται.

Κρυπτογράφηση-Αποκρυπτογράφηση
Όταν η Αλίκη θέλει να στείλει ένα κρυφό μήνυμα στο Βίκτορα χρησιμοποιεί το δημόσιο κλειδί του, κρυπτογραφεί το μήνυμα και του το στέλνει. Ο Βίκτορας στην συνέχεια χρησιμοποιώντας το ιδιωτικό του κλειδί αποκρυπτογραφεί το μήνυμα και το διαβάζει. Οποιοσδήποτε μπορεί να στείλει ένα κρυπτογραφημένο μήνυμα στον Βίκτορα αλλά μόνο ο τελευταίος μπορεί να το αποκρυπτογραφήσει.

Ψηφιακή υπογραφή

Η Αλίκη για να υπογράψει ένα μήνυμα κάνει έναν υπολογισμό χρησιμοποιώντας το μυστικό της κλειδί και το μήνυμα και το αποτέλεσμα του υπολογισμού (υπογραφή) στέλνεται στον Βίκτορα. Ο Βίκτωρας για να επαληθεύσει την υπογραφή κάνει έναν υπολογισμό που εμπλέκει το μήνυμα, την δηλούμενη υπογραφή και το δημόσιο κλειδί της Αλίκης και εάν το αποτέλεσμα είναι αληθές τότε η υπογραφή γίνεται δεκτή αλλιώς η υπογραφή απορρίπτεται.

Παρά το γεγονός ότι τα συστήματα δημοσίου κλειδιού δεν απαιτούν την μεταφορά και την αποκάλυψη των ιδιωτικών κλειδιών και προάγουν μεθόδους ψηφιακών υπογραφών, το μειονέκτημά τους είναι ότι η μέθοδος κρυπτογράφησης με αυτά είναι πιο αργή από οποιαδήποτε άλλη υπάρχουσα μέθοδο κρυπτογράφησης μυστικού κλειδιού. Για κρυπτογράφηση η καλύτερη λύση είναι ο συνδυασμός των συστημάτων κρυφού κλειδιού και δημόσιου κλειδιού ώστε να έχουμε την ασφάλεια που εξασφαλίζει το δημόσιο κλειδί όσο και την ταχύτητα που δίνει το κρυφό κλειδί. Το σύστημα δημοσίου κλειδιού μπορεί να χρησιμοποιηθεί για να κρυπτογραφήσει αρχικά το κρυφό κλειδί ώστε στην συνέχεια να χρησιμοποιηθεί το κρυπτοσύστημα κρυφού κλειδιού προκειμένου να κρυπτογραφηθεί ένα μεγάλο μήνυμα. Ένα τέτοιο πρωτόκολλο καλείται Ψηφιακός φάκελος (Digital envelope).

Στην συγκεκριμένη μεταπτυχιακή εργασία παρουσιάζονται κρυπτοσυστήματα δημοσίου κλειδιού, των οποίων το δημόσιο κλειδί είναι ένα σύστημα πολυωνυμικών εξισώσεων και το ιδιωτικό κλειδί είναι, είτε ένα σύνολο παραμέτρων για την κατασκευή των εξισώσεων, είτε ένα πολυώνυμο συγκεκριμένης μορφής. Στο δεύτερο κεφάλαιο περιγράφεται το κρυπτοσύστημα κρυμμένων μονωνύμων που προτάθηκε από τους Imai και Matsumoto στο Eurocrypt'88 [MI] και οι βελτιωμένες εκδόσεις του, τα Little Dragon και Big Dragon που πρότεινε ο Patarin, αφού κατάφερε στο Eurocrypt'95 [NK], [P95] να σπάσει το κρυπτοσύστημά τους. Στην συνέχεια περιγράφουμε ένα νέο κρυπτοσύστημα κρυμμένων πολυωνύμικών εξισώσεων το HPE του Ilia Toli [IT1] όπου το ιδιωτικό κλειδί είναι ένα πολυώνυμο δυο μεταβλητών με συντελεστές από ένα πεπερασμένο σώμα. Μια παραλλαγή αυτού του κρυπτοσυστήματος έδωσε ο Patarin [P96] το HFE, ο οποίος χρησιμοποίησε ως ιδιωτικό κλειδί ένα πολυώνυμο μιας μεταβλητής.

Στο τρίτο κεφάλαιο αναφέρουμε δυο σχήματα ψηφιακών υπογραφών πρώτον, το Sflash^{v3} [CGP], το οποίο σχεδιάστηκε για συγκεκριμένη χρήση αφού το κόστος των κλασσικών αλγορίθμων (RSA, DSA, ελλειπτικές καμπύλες) είναι πολύ μεγάλο και χρησιμοποιείται, τόσο για παραγωγή υπογραφής, όσο και για πιστοποίηση υπογραφής. Δεύτερον, ένα σύστημα υπογραφής που προκύπτει από το κρυπτοσύστημα HPE του Ilia Toli [IT1].

Το δημόσιο κλειδί των παραπάνω κρυπτοσυστημάτων, όπως αναφέραμε, είναι σύστημα δευτεροβάθμιων πολυωνυμικών εξισώσεων πολλών μεταβλητών.

Για την κρυπτανάλυση αυτών των κρυπτοσυστημάτων απαιτείται η επίλυση αυτών των συστημάτων που είναι γνωστό ως ένα δύσκολο πρόβλημα πάνω από οποιοδήποτε σώμα. Στο τέταρτο κεφάλαιο περιγράφουμε κάποιες μεθόδους επίλυσης αυτών των συστημάτων όπως οι βάσεις Gröbner [JGJG], [CLO], η τεχνική της επαναγραμμικοποίησης, η οποία προτάθηκε από τους Aviad Kipnis και Adi Shamir στο [KS] και χρησιμοποείται για την επίθεση του HFE κρυπτοσυστήματος και τέλος ένας νέος αλγόριθμος, ο XL (eXtended Linearization) αλγόριθμος, [SPCK], [SKI] που ουσιαστικά απλοποιεί την μέθοδο της επαναγραμμικοποίησης.

Στο παράρτημα παρουσιάζεται ένα παράδειγμα βασισμένο στο HFE κρυπτοσύστημα, περιγράφεται η διαδικασία παραγωγής του δημοσίου κλειδιού, η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος καθώς και η κρυπτανάλυση του συστήματος με τις βάσεις Gröbner, την τεχνική της επαναγραμμικοποίησης και τέλος τον XL αλγόριθμο.

Κεφάλαιο 2

Κρυπτοσυστήματα

2.1 Το κρυπτοσύστημα των Imai, Matsumoto. Κρυπτοσύστημα κρυμμένων μονωνύμων

Οι Imai, Matsumoto στο [MI] πρότειναν ένα κρυπτοσυστήματα δημοσίου κλειδιού κρυμμένων μονωνύμων (Hidden Monomial Cryptosystem), το οποίο υπήρξε η απαρχή για την ανάπτυξη αυτού του είδους των κρυπτοσυστημάτων. Τα χαρακτηριστικά του είναι ότι το δημόσιο κλειδί είναι ένα σύστημα πολυωνυμικών, μη γραμμικών εξισώσεων ενώ το ιδιωτικό κλειδί αποτελείται από ένα σύνολο παραμέτρων που επιλέγει ο χρήστης για να κατασκευάσει τις εξισώσεις.

Έστω $\mathbb{K}$ επέκταση βαθμού n πάνω από το σώμα $\mathbb{F}_q$, όπου q είναι δύναμη του 2 και $\beta_1,\beta_2,\ldots,\beta_n \in \mathbb{K}$ μια βάση του $\mathbb{K}$ ως $\mathbb{F}_q-$ διανυσματικού χώρου. Τόσο τα καθαρά μηνύματα όσο και τα κρυπτογραφημένα μηνύματα παριστάνονται ως n-άδες πάνω από το $\mathbb{F}_q$. Θα χρησιμοποιούμε $\bar{x} = (x_1, x_2, \ldots, x_n) \in {\mathbb{F}_q}^n$ για το καθαρό μήνυμα και $\bar{y} = (y_1, y_2, \ldots, y_n) \in {\mathbb{F}_q}^n$ για το κρυπτογραφημένο μήνυμα.

Για την κρυπτογράφηση ενός μηνύματος θα δουλεύουμε με δυο ενδιάμεσα διανύσματα, $\bar{u} = (u_1, u_2, \ldots, u_n) \in {\mathbb{F}_q}^n$ και $\bar{v} = (v_1, v_2, \ldots, v_n) \in {\mathbb{F}_q}^n$. Δοσμένου διανύσματος του ${\mathbb{F}_q}^n$ θα χρησιμοποιούμε έντονα γράμματα για να δηλώσουμε το αντίστοιχο στοιχείο του $\mathbb{K}$ ως προς την βάση β_j. Για παράδειγμα εάν $\bar{u} = (u_1, u_2, \ldots, u_n) \in {\mathbb{F}_q}^n$ τότε θέτουμε $\mathbf{u} = u_1\beta_1 + u_2\beta_2 + \ldots + u_n\beta_n \in \mathbb{K}$.

Η Αλίκη, η οποία θέλει να κρυπτογραφήσει ένα μήνυμα, επιλέγει ένα h, $0 < h < q^n$ της μορφής:

$$h = q^\theta + 1$$

που ικανοποιεί την συνθήκη Μ.Κ.Δ.$(h, q^n - 1) = 1$.
Προφανώς, αφού το q έχει επιλεγεί ως δύναμη του 2, ισχύει Μ.Κ.Δ.$(h, q^n - 1) = 1$ και από τη σχέση αυτή προκύπτει ότι η απεικόνιση $\mathbf{u} \mapsto \mathbf{u}^h$ είναι αμφιμονοσήμαντη (ενώ η αντίστροφή της απεικόνιση ορίζεται ως $\mathbf{u} \mapsto \mathbf{u}^{h'}$,

όπου h' είναι ο πολλαπλασιαστικός αντίστροφος του $h \pmod{q^n-1}$). Η Αλίκη μπορεί να μη δημοσιοποιήσει το h, αλλά εφόσον υπάρχουν μόνο λίγες επιλογές για το h, μπορεί να θεωρηθεί ότι είναι γνωστό.

Επιπλέον, επιλέγει δυο κρυφές αφινικές απεικονίσεις, για παράδειγμα δυο αντιστρέψιμους $n \times n$-πίνακες $A = \{a_{ij}\}_{1\leq i,j\leq n}$ και $B = \{b_{ij}\}_{1\leq i,j\leq n}$ με στοιχεία από το $\mathbb{F}_q$ και δυο σταθερά διανύσματα $\bar{c} = (c_1, c_2, \ldots, c_n)$ και $\bar{d} = (d_1, d_2, \ldots, d_n)$. Ο λόγος ύπαρξης των δυο αφινικών απεικονίσεων είναι να κρύψουν την απεικόνιση μονωνύμων $\mathbf{u} \mapsto \mathbf{u}^h$ (για το λόγο αυτό και το όνομα hidden monomial cryptosystem).

Αρχικά, για να μετατρέψει η Αλίκη το καθαρό μήνυμα $\bar{x} \in {\mathbb{F}_q}^n$ σε κρυπτογραφημένο $\bar{y} \in {\mathbb{F}_q}^n$ θέτει

$$\bar{u} = A\bar{x} + \bar{c}$$

Στη συνέχεια θέλει το $\mathbf{v} \in \mathbb{K}$ να είναι ίσο με την h-οστή δύναμη του $\mathbf{u} \in \mathbb{K}$ ($\mathbf{v} = \mathbf{u}^h$) καθώς επίσης

$$\bar{y} = B^{-1}(\bar{v} - \bar{d}),$$

(δηλαδή $\bar{v} = B\bar{y} + \bar{d}$), όπου $\bar{v} \in {\mathbb{F}_q}^n$ είναι το διάνυσμα που αντιστοιχεί στο $\mathbf{v} \in \mathbb{K}$. Προκειμένου να αναπτύξει μια μέθοδο ώστε να περνά απευθείας από το $\bar{x}$ στο $\bar{y}$, η Αλίκη χρησιμοποιεί ότι $\mathbf{v} = \mathbf{u}^h$ και $h = q^\theta + 1$, οπότε και έχει:

$$\mathbf{v} = \mathbf{u}^{q^\theta} \cdot \mathbf{u}. \tag{2.1}$$

Ο τελεστής ύψωσης στην q^k-οστή δύναμη στο $\mathbb{K}$ για οποιοδήποτε $k = 1, 2, \ldots, n$ είναι μια $\mathbb{F}_q$-γραμμική απεικόνιση και έστω $P^k = \{p_{ij}^k\}_{1\leq i,j\leq n}$ ο πίνακας αυτής της απεικόνισης ως προς την βάση β_1,...,β_n για παράδειγμα,

$$\beta_i^{q^k} = \sum_{j=1}^{n} p_{ij}^{(k)} \beta_j, \qquad p_{ij}^{(k)} \in \mathbb{F}_q, \tag{2.2}$$

με $1 \leq i, k \leq n$. Η Αλίκη, επιπλέον, γράφει όλα τα παραγόμενα στοιχεία της βάσης συναρτήσει των στοιχείων της, για παράδειγμα

$$\beta_i \beta_j = \sum_{l=1}^{n} m_{ijl} \beta_l, \qquad m_{ijl} \in \mathbb{F}_q \tag{2.3}$$

για κάθε $1 \leq i, j \leq n$. Οπότε η Εξίσωση (2.1) γράφεται ως,

$$\begin{aligned} \sum_{1\leq l\leq n} v_l \beta_l &= \Big(\sum_{i=1}^{n} u_i \beta_i^{q^\theta}\Big)\Big(\sum_{j=1}^{n} u_j \beta_j\Big) \\ &= \Big(\sum_{1\leq i,\mu\leq n} p_{i\mu}^{(\theta)} u_i \beta_\mu\Big)\Big(\sum_{j=1}^{n} u_j \beta_j\Big) \end{aligned} \tag{2.4}$$

Χρησιμοποιώντας την Εξίσωση (2.3) και συγκρίνοντας τους συντελεστές των β_l στο δεξιό και αριστερό μέλος της Εξίσωσης (2.4) για κάθε l προκύπτουν εξισώσεις της μορφής:

$$v_l = \sum_{1 \leq i,j,\mu \leq n} p_{i\mu}^{(\theta)} m_{\mu jl} u_i u_j, \tag{2.5}$$

οι οποίες είναι πρώτου βαθμού ως προς το $v_1, \ldots, v_n$ και δευτέρου βαθμού ως προς το $u_1, \ldots, v_n$. Χρησιμοποιεί στη συνέχεια στην Εξίσωση (2.5) τις δυο σχέσεις,

$$\bar{u} = A\bar{x} + \bar{c}, \qquad \bar{v} = B\bar{y} + \bar{d}$$

οπότε και έχει n εξισώσεις, γραμμικές ως προς το $y_1, \ldots, y_n$ και δευτέρου βαθμού ως προς το $x_1, \ldots, x_n$. Χρησιμοποιώντας γραμμική άλγεβρα προκύπτει ένα σύστημα n εξισώσεων όπου κάθε y_i εκφράζεται ως πολυώνυμο συνολικά δευτέρου βαθμού ως προς τα $x_1, x_2, \ldots, x_n$. Η Αλίκη δημοσιοποιεί αυτές τις εξισώσεις.

Κρυπτογράφηση
Ο Βίκτορας για να της στείλει ένα μήνυμα $(x_1, x_2, \ldots, x_n)$, αντικαθιστά τα x_i στις δημόσιες εξισώσεις και παίρνει ένα σύστημα εξισώσεων γραμμικό ως προς τα y_i. Το λύνει και στέλνει στην Αλίκη το $\bar{y} = (y_1, y_2, \ldots, y_n)$. Αντίθετα ο ωτακουστής, γνωρίζοντας μόνο το κρυπτογραφημένο μήνυμα και τις δημόσιες εξισώσεις, αντικαθιστά τα $(y_1, y_2, \ldots, y_n)$ στις εξισώσεις και έχει να λύσει ένα μη-γραμμικό σύστημα με αγνώστους τα x_i.

Αποκρυπτογράφηση:
Για να αποκρυπτογραφήσει η Αλίκη το μήνυμα γνωρίζοντας τα $A, B, \bar{c}, \bar{d}$ και το h μπορεί να υπολογίσει το $\bar{x}$ χωρίς να χρειάζεται να λύσει τις δημόσιες εξισώσεις ως προς τα x_i. Το παρακάτω διάγραμμα περιγράφει την διαδικασία αποκρυπτογράφησης της Αλίκης:

$$\begin{array}{c} y_1, y_2, \ldots, y_n \\ \Downarrow \\ \bar{v} = B\bar{y} + \bar{d} \\ \Downarrow \\ \mathbf{v} = \sum v_i \beta_i \\ \Downarrow \\ \mathbf{u} = \mathbf{v}^{h'} \\ \Downarrow \\ \bar{x} = A^{-1}(\bar{u} - \bar{c}). \end{array}$$

Το παρακάτω παράδειγμα περιγράφει την διαδικασία παραγωγής ενός τέτοιου κρυπτοσυστήματος με πολύ μικρές τιμές στις παραμέτρους.

Παράδειγμα 2.1.1 *Έστω* $q = 2, n = 5$ *και* $f(X) = X^5+X^4+X^3+X+1 \in \mathbb{F}_2[X]$ *ανάγωγο πολυώνυμο πέμπτου βαθμού.Έστω* $\mathbf{K}$ *επέκταση βαθμού πέντε πάνω από το* $\mathbf{F}_2$ *και μια βάση του* $\{\beta_1, \beta_2, \ldots, \beta_n\} = \{1, X, X^2, X^3, X^4\}$. *Επιπλέον,* $\theta = 3, h = 9, h' = 7$ *και* $\bar{c} = (1, 0, 1, 1, 1), \bar{d} = (1, 0, 1, 0, 0)$,

$$A = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Τότε,

$$A^{-1} = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}, \quad B^{-1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

Θέτουμε, $\bar{u} = A\bar{x} + \bar{c}$ *οπότε προκύπτουν οι παρακάτω εξισώσεις:*

$$\begin{aligned} u_1 &= x_1 + x_3 + x_4 + 1, \\ u_2 &= x_2 + x_3 + x_5, \\ u_3 &= x_1 + x_2 + x_5 + 1, \\ u_4 &= x_2 + x_4 + 1, \\ u_5 &= x_4 + x_5 + 1. \end{aligned}$$

Επιπλέον έχουμε,
$\mathbf{v} = \mathbf{u}^9 = (u_1+u_2X+u_3X^2+u_4X^3+u_5X^4)(u_1+u_2X^8+u_3X^{16}+u_4X^{24}+u_5X^{32})$
ανάγουμε το δεξιό μέλος modulo $f(X)$, *οπότε εκφράζουμε το* $\bar{v}$ *συναρτήσει του* $\bar{x}$:

$$\begin{aligned} v_1 &= 1 + x_1^2 + x_1x_3 + x_1x_2 + x_4 + x_4x_5 + x_1x_4 + x_2x_4 + x_1 + x_2 + x_3x_5 + x_2^2. \\ v_2 &= x_5x_1 + x_3x_2 + x_1^2 + x_2x_5 + x_5^2 + x_4 + x_1x_4 + x_1 + x_3^2 + x_2 + x_3x_5. \\ v_3 &= x_1x_3 + x_1 + x_1x_2 + x_3x_2 + x_3x_4 + x_2 + x_3 + x_4^2 + x_3x_5 + x_2^2. \\ v_4 &= x_3x_4 + x_1^2 + x_5^2 + x_3 + 1 + x_1x_3 + x_1x_4 + x_2x_4 + x_4^2 + x_2^2. \\ v_5 &= x_3x_2 + 1 + x_5x_1 + x_3 + x_5 + x_5^2 + x_1x_3 + x_1x_2 + x_4 + x_1x_4 + x_3^2 + x_2 + x_4^2 + x_3x_5. \end{aligned}$$

Τέλος, οι εξισώσεις που σχετίζουν το $\bar{y}$ με το $\bar{x}$ και γίνονται δημόσιες είναι:

$$
\begin{aligned}
y_1 &= x_3x_2 + 1 + x_5x_1 + x_3 + x_5 + x_5^2 + x_1x_3 + x_1x_2 + x_4 + x_1x_4 + x_3^2 + x_2 + x_4^2 + x_3x_5.\\
y_2 &= x_3x_4 + x_1^2 + x_2x_4 + x_2^2 + x_3x_2 + x_5x_1 + x_5 + x_1x_2 + x_4 + x_3^2 + x_2 + x_3x_5.\\
y_3 &= 1 + x_1^2 + x_1 + x_3 + x_4 + x_5 + x_4^2 + x_1x_2 + x_4x_5 + x_3x_2 + x_2^2 + x_2x_5 + x_5^2.\\
y_4 &= 1 + x_1x_4 + x_3^2 + x_2 + x_3 + x_5 + x_4^2 + x_3x_5 + x_5x_1 + x_1x_2 + x_4x_5 + x_2^2.\\
y_5 &= x_1 + x_1x_2 + x_3x_2 + x_2 + x_3x_5 + x_1^2 + x_5^2 + x_1x_4 + x_2x_4.
\end{aligned}
$$

Κρυπτανάλυση

Ο Jacques Patarin στο [P95] έδειξε πώς μπορεί κανείς εύκολα να σπάσει το κρυπτοσύστημα. Παρατήρησε ότι, εάν πάρει την εξίσωση $\mathbf{v} = \mathbf{u}^{q^\theta+1}$ υψώσει και τα δύο μέλη της στην $(q^\theta-1)$ δύναμη και στην συνέχεια τα πολλαπλασιάσει με $\mathbf{uv}$, τότε θα έχει:

$$\mathbf{uv}^{q^\theta} = \mathbf{u}^{q^{2\theta}}\mathbf{v} \tag{2.6}$$

η οποία οδηγεί σε εξισώσεις γραμμικές ως προς τα $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n$.

Ο ωτακουστής χρησιμοποιώντας γραμμική άλγεβρα μπορεί να βρει αυτές τις εξισώσεις ακόμα και αν δεν γνωρίζει τις παραμέτρους της Αλίκης. Πιθανόν αυτές οι εξισώσεις να μην επιτρέπουν να προσδιοριστεί μονοσήμαντα το καθαρό μήνυμα από το κρυπτογραφημένο αλλά μια διεξοδική αναζήτηση θα είναι αποδοτική.

Ο ωτακουστής γνωρίζοντας ότι η Αλίκη έχει χρησιμοποιήσει το παραπάνω κρυπτοσύστημα, ξέρει ότι η Εξίσωση (2.6) κρύβεται και ότι οδηγεί σε εξισώσεις της μορφής:

$$\Big(\sum_{1\le i,j\le n} a_{ijl}x_iy_j\Big) + \Big(\sum_{1\le i\le n} (\beta_{il}x_i + \gamma_{il}y_i)\Big) + \delta_l = 0, \tag{2.7}$$

$l = 1, \ldots, n$. Στόχος του είναι να αγνοήσει τις δημόσιες εξισώσεις και να βρεί καινούριες καλύτερες εξισώσεις (2.7) που θα είναι γραμμικές και ως προς τις δυο μεταβλητές $\bar{x}, \bar{y}$. Αρχικά, δεν γνωρίζει τους συντελεστές αυτών των εξισώσεων επειδή δεν ξέρει ούτε την βάση $\beta_1, \ldots, \beta_n$ ούτε τους συντελεστες των (2.2),(2.3), μπορεί όμως να παράγει ένα μεγάλο αριθμό από ζεύγη καθαρών και κρυπτογραφημένων μηνυμάτων $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n$ χρησιμοποιώντας απλά τις δημόσιες εξισώσεις της Αλίκης. Κάθε τέτοιες $2n$-άδες αντικαθίστανται στην (2.7) και δίνουν μια γραμμική εξίσωση με $(n+1)^2$ άγνωστους συντελεστές $a_{ij}, \beta_i, \gamma_i, \delta$ σε μια Εξίσωση του τύπου (2.7). Με αυτόν τον τρόπο θα μπορεί να βρεί ένα μέγιστο σύνολο από L γραμμικά ανεξάρτητες εξισώσεις που ικανοποιούνται από όλα τα ζεύγη των καθαρών και κρυπτογραφημένων μηνυμάτων.

Στην συνέχεια επιλέγει ένα κρυπτογραφημένο μήνυμα $\bar{y}_0$ και αντικαθιστά τις συντεταγμένες του σε όλες τις Εξισώσεις (2.7), οπότε και έχει L γραμμικές εξισώσεις με n αγνώστους $x_1, \ldots, x_n$. Έστω ότι από τις L αυτές εξισώσεις οι Λ είναι ανεξάρτητες. Από την γραμμική άλγεβρα ο χώρος λύσεων του συστήματος αυτών των εξισώσεων είναι $(n-\Lambda)$-διάστατος υπόχωρος του $\mathbb{F}_q^n$. Με άλλα λόγια αν δούμε τις εξισώσεις (2.7) ως σύστημα γραμμικών εξισώσεων με αγνώστους τα $x_1, \ldots, x_n$, μετά την αντικατάσταση $\bar{y} = \bar{y}_0$, τότε αυτό θα έχει ακριβώς $q^{n-\Lambda}$ λύσεις.

Από την άλλη μεριά, αυτές οι εξισώσεις είναι ισοδύναμες με την Εξίσωση (2.6), οπότε υπάρχει ένα προς ένα αντιστοιχία μεταξύ των λύσεων της (2.6) και των λύσεων του συστήματος (2.7). Για καθορισμένο $\mathbf{v} = \mathbf{v}_0$ η (2.6) εκτός από την τετριμμένη λύση $\mathbf{u} = 0$, έχει και μοναδική λύση $\mathbf{u}_0 = \mathbf{v}_0^{h'}$ της εξίσωσης $\mathbf{u} = \mathbf{v}^h$ που όταν υψωθεί στην $(q^\theta - 1)$-οστή δύναμη προκύπτει η (2.6). Εάν $\mathbf{u}$ είναι μια ακόμη μη μηδενική λύση της (2.6) με $\mathbf{v} = \mathbf{v}_0$, τότε ισχύει:

$$\mathbf{v}_0^{q^\theta - 1} = \mathbf{u}_0^{h(q^\theta - 1)} \quad \kappa\alpha\iota \ \mathbf{v}_0^{q^\theta - 1} = \mathbf{u}^{h(q^\theta - 1)}$$

Υψώνοντας και τα δύο μέλη της $\mathbf{u}_0^{h(q^\theta-1)} = \mathbf{u}^{h(q^\theta-1)}$ στην h'-οστή δύναμη προκύπτει ότι $\mathbf{u}_0^{q^\theta-1} = \mathbf{u}^{q^\theta-1}$. Αυτό σημαίνει ότι η $\mathbf{u}$ διαφέρει από την $\mathbf{u}_0$ κατά έναν παράγοντα, ο οποίος είναι η $(q^\theta - 1)$-οστή ρίζα της μονάδας στο $\mathbb{K}$. Υπάρχουν τόσες ρίζες της μονάδας στο $\mathbb{K}$ όσες ο Μ.Κ.Δ$(q^\theta - 1, q^n - 1) = q^d - 1$, όπου $d =$Μ.Κ.Δ.(θ, n). Αν υπολογίσουμε και την μηδενική λύση τότε υπάρχουν ακριβώς q^d λύσεις ως προς $\mathbf{u}$ της (2.6) (με $\mathbf{v} = \mathbf{v}_0$) και επομένως q^d λύσεις ως προς $\bar{x}$ της (2.7) όταν $\bar{y} = \bar{y}_0$. Επομένως,

$$n - \Lambda = d = M.K.\Delta.(\theta, n). \tag{2.8}$$

Ο αριθμός στην (2.8) δηλώνει ότι ο ωτακουστής χρειάζεται να ψάξει μεταξύ q^d διανυσμάτων προκειμένου να βρεί το καθαρό μήνυμα. Αφού το θ έχει επιλεγεί έτσι ώστε Μ.Κ.Δ.$(q^\theta + 1, q^n - 1) = 1$ είναι πιθανόν να είναι το $d = n$ και $d = n/2$ αλλά και $d = n/3$. Επομένως, ο ωτακουστής έχει να ψάξει στο $1/3$ της διάστασης του συνολικού χώρου των πιθανών μηνυμάτων. Αυτό σημαίνει ότι το παραπάνω κρυπτοσύστημα δεν είναι καθόλου ασφαλές.

2.2 Το κρυπτοσύστημα Little Dragon.

Ο Patarin [NK] μετά την κρυπτανάλυση του συστήματος των Imai,Matsumoto πρότεινε ένα νέο κρυπτοσύστημα το οποίο φαίνεται πιο ανθεκτικό στην παραπάνω τύπου κρυπτανάλυση.

Όπως και πριν, έστω $\mathbb{K}$ επέκταση βαθμού n πάνω από το πεπερασμένο σώμα $\mathbb{F}_q$ και $\beta_1, \beta_2, \ldots, \beta_n \in \mathbb{K}$ μια βάση του $\mathbb{K}$ ως $\mathbb{F}_q$ διανυσματικού χώρου. Η Αλίκη

βλέπει κάθε στοιχείο του $\mathbb{K}$ ως μια n-άδα πάνω από το $\mathbb{F}_q^n$ και χρησιμοποιεί το $\bar{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ για το καθαρό μήνυμα και το $\bar{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$ για το κρυπτογραφημένο μήνυμα. Δουλεύει με δυο ενδιάμεσα διανύσματα $\bar{u} = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$ και $\bar{v} = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$ και για δοσμένο διάνυσμα του $\mathbb{F}_q^n$ δηλώνει με έντονα γράμματα το αντίστοιχο στοιχείο του $\mathbb{K}$ ως προς την μυστική βάση β_j.

Στο κρυπτοσύστημα Little Dragon ο εκθέτης h έχει μια μικρή διαφορά από αυτόν του συστήματος των Imai, Matsumoto. Η Αλίκη επιλέγει έναν εκθέτη h, $0 \leq h \leq q^n$, τέτοιος ώστε ο $h+1$ να γράφεται ως άθροισμα δυο διαφορετικών δυνάμεων του q,

$$h = q^\theta + q^\varphi - 1, \tag{2.9}$$

και επιπλέον να ισχύει ότι ο Μ.Κ.Δ.$(h, q^n - 1) = 1$. Δεν είναι απαραίτητο πια το q να είναι άρτιος ενώ οι ακέραιοι θ και φ επιλέγονται αυθαίρετα από το σύνολο $\{1, \ldots, n-1\}$, έτσι ώστε το h να είναι πρώτο προς το $q^n - 1$. Το h μπορεί και να μην γίνει γνωστό, αλλά σίγουρα η ασφάλεια του συστήματος δεν μπορεί να βασισθεί σε αυτό.

Επιπλέον, επιλέγει δυο κρυφές αφινικές απεικονίσεις, για παράδειγμα δυο αντιστρέψιμους $n \times n$-πίνακες $A = \{a_{ij}\}_{1 \leq i,j \leq n}$ και $B = \{b_{ij}\}_{1 \leq i,j \leq n}$ με στοιχεία από το $\mathbb{F}_q$. Αρχικά, θέτει

$$\bar{u} = A\bar{x}, \ \kappa\alpha\iota \ \ \bar{y} = B^{-1}\bar{v},$$

θέλει το $\mathbf{v} \in \mathbb{K}$ να είναι ίσο με την h-οστή δύναμη του $\mathbf{u} \in \mathbf{K}, (\mathbf{v} = \mathbf{u}^h)$ οπότε από την (2.9) η σχέση αυτή γίνεται:

$$\mathbf{uv} = \mathbf{u}^{q^\theta}\mathbf{u}^{q^\varphi} \tag{2.10}$$

Στην συνέχεια χρησιμοποιεί το γεγονός ότι για οποιαδήποτε $k = 1, \ldots, n$ η ύψωση στην q^k-οστή δύναμη στο $\mathbb{K}$ είναι $\mathbb{F}_q$-γραμμική απεικόνιση. Πάλι, έστω $P^k = \{p_{ij}^{(k)}\}_{1 \leq i,j \leq n}$ ο πίνακας αυτής της απεικόνισης ως προς την βάση $\beta_1, \ldots, \beta_n$ (2.2) και έστω m_{ijl} οι συντελεστές όταν τα $\beta_i\beta_j$ γράφονται ως γραμμικός συνδυασμός των β_l (2.3). Οπότε η (2.10) δίνει ότι:

$$\begin{aligned} \sum_{1 \leq i,j \leq n} u_i v_j \beta_i \beta_j &= (\sum_{i=1}^{n} u_i \beta_i^{q^\theta})(\sum_{j=1}^{n} u_j \beta_j^{q^\varphi}) \\ &= (\sum_{1 \leq i,\mu \leq n} p_{i\mu}^{(\theta)} u_i \beta_\mu)(\sum_{1 \leq j,\nu \leq} p_{j\nu}^{(\varphi)} u_j \beta_\nu), \end{aligned} \tag{2.11}$$

εάν χρησιμοποιήσουμε την Εξίσωση (2.3) και στην συνέχεια συγκρίνουμε τους συντελεστές των β_l στο δεξιό και αριστερό μέλος της (2.11), παίρνουμε για κάθε l:

$$\sum_{1\leq i,j\leq n} m_{ijl}u_iv_j = \sum_{1\leq i,j,\mu,\nu\leq n} p_{i\mu}^{(\theta)}p_{j\nu}^{(\varphi)}m_{\mu\nu l}u_iu_j. \tag{2.12}$$

Η Αλίκη γνωρίζει τους συντελεστές m_{ijl} και p_{ij}^k, χρησιμοποιεί στην συνέχεια τις σχέσεις

$$\bar{u} = A\bar{x}, \quad \bar{v} = B\bar{y},$$

για να αντικαταστήσει τα u_i με $\sum_\rho a_{i\rho}x_\rho$ και τα v_j με $\sum_\sigma b_{j\sigma}y_\sigma$ στην (2.12), οπότε προκύπτουν n εξισώσεις της μορφής:

$$\sum_{1\leq i,j\leq n} c_{ij}x_iy_j + \sum_{1\leq i\leq j\leq n} d_{ij}x_ix_j = 0 \quad l = 1,\ldots,n. \tag{2.13}$$

Η Αλίκη δημοσιεύει την Εξίσωση (2.13).

Κρυπτογράφηση
Ο Βίκτορας για να στείλει ένα μήνυμα $\bar{x}$ αντικαθιστά τα x_i στην Εξίσωση (2.13) οπότε έχει ένα σύστημα n εξισώσεων γραμμικό ως προς τα y_i, το οποίο συνέχεια λύνει με απαλοιφή Gauss ως προς τα y_i. Από την άλλη, ο ωτακουστής έχει να λύσει ένα μη γραμμικό σύστημα ως προς τους αγνώστους x_i.
Αποκρυπτογράφηση
Η Αλίκη λάμβανει το κρυπτογραφημένο μήνυμα $\bar{y}$ και γνωρίζοντας τα A, B $\kappa\alpha\iota$ h προσπαθεί να ανακτήσει το $\bar{x}$ χωρίς να χρειάζεται να λύσει την Εξίσωση (2.13) ως προς τα x_i. Έστω h' ο πολλαπλασιαστικός αντίστροφος του h $modulo$ q^n-1 έτσι ώστε η απεικόνιση $\mathbf{u} = \mathbf{v}^{h'}$ να είναι η αντίστροφη της απεικόνισης $\mathbf{u} = \mathbf{v}^h$ πάνω από το $\mathbb{K}$. Αρχικά υπολογίζει το $\bar{v} = B\bar{y}$, υψώνει το $\mathbf{v} = \sum v_i\beta_i \ \in \mathbb{K}$ στην h'-οστή δύναμη το οποίο ισούται με $\mathbf{u}$ και τελικά υπολογίζει το $\bar{x} = A^{-1}\bar{u}$. Το παρακάτω διάγραμμα περιγράφει την διαδικασία αποκρυπτογράφησης:

$$\begin{array}{c} y_1, y_2, \ldots, y_n \\ \Downarrow \\ \bar{v} = B\bar{y} \\ \Downarrow \\ \mathbf{v} = \sum v_i\beta_i \\ \Downarrow \\ \mathbf{u} = \mathbf{v}^{h'} \\ \Downarrow \\ \bar{x} = A^{-1}\bar{u}. \end{array}$$

2.3 Το κρυπτοσύστημα Big Dragon

Έστω $\mathbb{K}$ επέκταση βαθμού n πάνω από το πεπερασμένο σώμα $\mathbb{F}_q$ χαρακτηριστικής 2 και $\beta_1, \beta_2, \ldots, \beta_n \in \mathbb{K}$ μια βάση του $\mathbb{K}$ ως $\mathbb{F}_q$-διανυσματικού χώρου. Όπως και πριν με $\bar{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ δηλώνουμε το καθαρό μήνυμα, με $\bar{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$ το κρυπτογραφημένο μήνυμα και με $\bar{u} = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$ $\bar{v} = (= v_1, \ldots, v_n) \in \mathbb{F}_q^n$ δυο ενδιάμεσα διανύσματα τα οποία σχετίζονται με τα $\bar{x}$ και $\bar{y}$ με τις εξισώσεις:

$$\bar{u} = A\bar{x} + \bar{c}, \qquad \bar{v} = B\bar{y} + \bar{d},$$

όπου οι πίνακες A και B και τα καθορισμένα διανύσματα $\bar{c}$ και $\bar{d}$ θεωρούνται κρυφά.

Η Αλίκη επιλέγει έναν ακέραιο h της μορφής:

$$h = q^{\theta_1} + q^{\theta_2} - q^{\varphi_1} - q^{\varphi_2} \tag{2.14}$$

τέτοιο ώστε ο Μ.Κ.Δ.$(h, q^n - 1) = 1$. Στην συνέχεια επιλέγει μια κρυφή $\mathbb{F}_q$-γραμμική απεικόνιση (μπορεί να είναι και αφινική) $\psi : \mathbb{K} \longrightarrow \mathbb{K}$. Η σχέση ανάμεσα στα $\mathbf{u}$ και $\mathbf{v}$ είναι:

$$\mathbf{u}^h = \frac{\psi(\mathbf{v})}{\mathbf{v}} \quad \gamma\iota\alpha \quad \mathbf{u}, \mathbf{v} \in \mathbb{K}, \mathbf{v} \neq 0. \tag{2.15}$$

Ισοδύναμα, έχουμε:

$$\mathbf{u}^{q^{\theta_1}+q^{\theta_2}}\mathbf{v} = \mathbf{u}^{q^{\varphi_1}+\varphi_2}\psi(\mathbf{v}) \tag{2.16}$$

Εφόσον θέλει να υπάρχει μια ένα προς ένα αντιστοιχία μεταξύ των $\mathbf{u}$ και $\mathbf{v}$, η ψ θα πρέπει να επιλεγεί έτσι ώστε η απεικόνιση $\mathbf{v} \longrightarrow \psi(\mathbf{v})/\mathbf{v}$ να είναι ένα προς ένα πάνω από το σύνολο $\mathbb{K}^*$ των μη-μηδενικών στοιχείων του $\mathbb{K}$. Επαναλαμβάνοντας την διαδικασία που έκανε και στα δυο παραπάνω κρυπτοσυστήματα για να παράγει τις δημόσιες εξισώσεις ξεκινά από την Εξίσωση (2.16) και με ανάλογο τρόπο καταλήγει σε n πολυωνυμικές εξισώσεις συνολικά τρίτου βαθμού ως προς τις μεταβλητές $\{x_1, \ldots, x_n, y_1, \ldots, y_n\}$ αλλά μόνο πρώτου βαθμού ως προς y_i και τις δημοσιοποιεί.

Κρυπτογράφηση
Ο Βίκτορας, ο οποίος θέλει να στείλει ένα μήνυμα $\bar{x}$ στην Αλίκη αντικαθιστά τις συντεταγμένες του μηνύματος $\bar{x}$ στις εξισώσεις και λύνει το γραμμικό σύστημα ως προς τα y_i για να ανακτήσει το κρυπτογραφημένο μήνυμα $\bar{y}$.

Αποκρυπτογράφηση
Η Αλίκη μπορεί να χρησιμοποιήσει την Εξίσωση (2.15) για να αποκρυπτογραφήσει το μήνυμα. Αρχικά, από την σχέση $\bar{v} = B\bar{y} + \bar{d}$ βρίσκει το $\mathbf{v}$ και υπολογίζει:

$$\mathbf{u} = (\psi(\mathbf{v})/\mathbf{v})^{h'}$$

όπου h' ο αντίστροφος του h $(mod\ q^n - 1)$. Τελικά από την εξίσωση $\bar{u} = A\bar{x} + \bar{c}$ ανακτά το $\bar{x}$.

2.4 Κρυπτοσύστημα κρυμμένων πολυωνυμικών εξισώσεων (HPE)

Ο Ilia Toli στο [IT1] πρότεινε ένα νέο κρυπτοσύστημα με δημόσιο κλειδί ένα σύστημα πολυωνυμικών εξισώσεων και ιδιωτικό κλειδί ένα πολυώνυμο δυο μεταβλητών. Στόχος της Αλίκης είναι να κρύψει από τον ωτακουστή αυτό το πολυώνυμο.

Η Αλίκη επιλέγει δυο πεπερασμένα σώματα $\mathbb{F}_q < \mathbb{K}$ και μια βάση $\beta_1, \beta_2, \ldots, \beta_n$ του $\mathbb{K}$ ως $\mathbb{F}_q$ διανυσματικού χώρου. Συνήθως είναι $q = 2$, αλλά μπορεί να είναι οποιοδήποτε p^r για κάθε p πρώτο και $r \in \mathbb{N}$. Στην συνέχεια παίρνει ένα πολυώνυμο δύο μεταβλητών της μορφής:

$$f(\mathbf{x}, \mathbf{y}) = \sum_{ij} \mathbf{a}_{ij} \mathbf{x}^i \mathbf{y}^j \in \mathbb{K}[\mathbf{x}, \mathbf{y}] \tag{2.17}$$

έτσι ώστε να μπορεί να βρεί όλες τις ρίζες στο $\mathbb{K}$ ως προς $\mathbf{x}, \forall\ \mathbf{y} \in \mathbb{K}$, εάν υπάρχουν. Για την κρυπτογράφηση ενός μηνύματος η Αλίκη θα δουλέψει με δύο ενδιάμεσα διανύσματα, $\bar{u} = (u_1, \ldots, u_n)$ και $\bar{v} = (v_1, \ldots, v_n)$, με $\bar{u}, \bar{v} \in \mathbb{F}_q^n$ και $\mathbf{u}, \mathbf{v}$ τα αντίστοιχα στοιχεία του $\mathbb{K}$, οπότε θέτει:

$$\sum_{ij} \mathbf{a}_{ij} \mathbf{u}^i \mathbf{v}^j = 0. \tag{2.18}$$

Για $a_{ij} \neq 0$ έχει:

$$i = \sum_{k=1}^{n_i} q^{\theta_{ik}} \quad \kappa\alpha\iota \quad j = \sum_{k=1}^{n_j} q^{\theta_{jk}}, \tag{2.19}$$

Στην συνέχεια η Αλίκη αντικαθιστά την Εξίσωση (2.19) στους εκθέτες της Εξίσωσης (2.18) και παίρνει:

$$\sum_{ij} (\mathbf{a}_{ij} \exp(\mathbf{u}, \sum_{k=1}^{n_i} q^{\theta_{ik}}) \exp(\mathbf{v}, \sum_{k=1}^{n_j} q^{\theta_{jk}})) = 0 \tag{2.20}$$

η οποία είναι:

$$\sum_{ij}(\mathbf{a}_{ij}\prod_{k=1}^{n_i}\mathbf{u}^{q^{\theta_{ij}}}\prod_{k=1}^{n_j}\mathbf{v}^{q^{\theta_{jk}}}) = 0 \tag{2.21}$$

Δεδομένου ότι ο τελεστής ύψωσης στην q^k-οστή δύναμη είναι $\mathbb{F}_q$ γραμμική απεικόνιση ισχύουν οι Εξισώσεις (2.2) και (2.3). Στην συνέχεια αντικαθιστά τα $\bar{u} = (u_1, u_2, \ldots, u_n), \mathbf{a}_{ij} = (a_{ij1}, a_{ij2}, \ldots, a_{ijn}), \bar{v} = (v_1, v_2, \ldots, v_n)$ και τις εξισώσεις (2.2), (2.3) στην (2.21) και αναπτύσσει. Έτσι προκύπτει ένα σύστημα n εξισώσεων βαθμού t ως προς u, v, όπου

$$t = \max\{n_i + n_j : \mathbf{a}_{ij} \neq 0\}. \tag{2.22}$$

Επομένως ο συνολικός βαθμός του $\mathbf{u}^i\mathbf{v}^j$ είναι $n_i + n_j$. Σκοπός αυτού του κρυπτοσυστήματος είναι να παράγει ένα σύνολο πολυωνύμικών εξισώσεων, γραμμικών ως προς το ένα σύνολο μεταβλητών και μη γραμμικών ως προς το άλλο. Για το λόγο αυτό συσχετίζουμε τις Εξισώσεις (2.18), (2.19) ώστε να έχουμε: $\mathbf{a}_{ij} \neq 0 \Rightarrow \{n_i > 1, n_j = 1\}$. Από την άλλη μεριά το μέγεθος του δημοσίου κλειδιού PK είναι $\mathcal{O}(n^{t+1})$, δηλαδή αυξάνεται πολυωνυμικά ως προς n και εκθετικά ως προς t. Θέλει να κρατήσει το t αρκετά μικρό, δηλαδή $t = 2, 3$, περίπου, οπότε επιλέγει τα i, j στην Εξίσωση (2.19) προκειμένου να κρατήσει το t κάτω από ένα καθορισμένο φράγμα.

Στην συνέχεια παίρνει $\bar{c}, \bar{d} \in \mathbb{F}_q^n$ και θέτει:

$$\bar{u} = \bar{x} + \bar{c} \quad \kappa\alpha\iota \quad \bar{v} = \bar{y} + \bar{d} \tag{2.23}$$

όπου $\bar{x} = (x_1, x_2, \ldots, x_n), \bar{y} = (y_1, y_2, \ldots, y_n)$ είναι τα διανύσματα των μεταβλητών. Αντικαθιστά την Εξίσωση (2.23) στις παραπάνω εξισώσεις των $\mathbf{u}, \mathbf{v}$ και αναπτύσσει, οπότε και παίρνει ένα σύστημα n-εξισώσεων γραμμικό ως προς y και μη-γραμμικό ως προς x.

Το δημόσιο κλειδί είναι:
- Το σύστημα των εξισώσεων ως προς x, y.
- Το σώμα $\mathbb{F}_q$.
- Το αλφάβητο: ένα σύνολο στοιχείων του $\mathbb{F}_q$ ή συμβολοσειρές αυτών.

Το ιδιωτικό κλειδί είναι:
- Το πολυώνυμο (2.17).
- Οι Εξισώσεις (2.18) εως (2.23).
- Η βάση $\{\beta_1, \ldots, \beta_n\}$.

Κρυπτογράφηση:
Ο Βίκτορας αντικαθιστά το μήνυμα $\bar{x} = (x_1, x_2, \ldots, x_n)$ στις δημόσιες εξισώσεις, βρίσκει μια λύση $\bar{y} = (y_1, y_2, \ldots, y_n)$ και στέλνει το $\bar{y}$ στην Αλίκη.

Αποκρυπτογράφηση:
Η Αλίκη υπολογίζει το $\bar{v} = \bar{y} + \bar{d} \in \mathbb{K} > \mathbb{F}_q$, υπολογίζει το $\mathbf{v}$, αντικαθιστά στην (2.18) και βρίσκει όλες τις λύσεις στο $\mathbb{K}$, υπάρχει τουλάχιστον μια. Εάν είναι $\bar{x}$ το καθαρό μήνυμα και το $\bar{u}$ όπως στην Εξίσωση (2.23), αντικαθιστά το $\bar{x} = \bar{u} - \bar{c}$ και με πιθανότητα $\simeq 1$ όλα τα αποτελέσματα, εκτός από ένα του Βίκτορα, δεν έχουν καμμια σχέση με το αλφάβητο.

2.5 Το κρυπτοσύστημα δημοσίου κλειδιού (HFE)

Ο Patarin στο [P96] έδωσε μια παραλλαγή του κρυπτοσυστήματος HPE, το κρυπτοσύστημα HFE (Hidden Field Equation). Όπως και πριν δουλεύει πάνω από ένα πεπερασμένο σώμα $\mathbb{K} \supset \mathbb{F}_q$ με $[\mathbb{K} : \mathbb{F}_q] = n$ και $\{\beta_1, \beta_2, \ldots, \beta_n\}$ μια βάση του $\mathbb{K}$ ως $\mathbb{F}_q$ διανυσματικού χώρου.
Επιλέγει ένα κρυφό πολυώνυμο μιας μεταβλητής της μορφής:

$$f(\mathbf{x}) = \sum_{ij} \beta_{ij} \mathbf{x}^{q^{\theta_{ij}} + q^{\varphi_{ij}}} + \sum_i a_i \mathbf{x}^{q^{\xi_i}} + \mu_0,$$

το οποίο μπορεί να εκφρασθεί ως σύστημα n πολυωνυμικών εξισώσεων $P_1, \ldots, P_n$ με n μεταβλητές $x_1, \ldots, x_n$. Η αυστηρή επιλογή των εκθετών του P διασφαλίζει ότι όλα τα P_i είναι ομογενή δευτεροβάθμια πολυώνυμα.

Στην συνέχεια χρησιμοποιούνται δυο κρυφές τυχαίες αντιστρέψιμες γραμμικές απεικονίσεις S και T πάνω από n-άδες στοιχείων του $\mathbb{F}_q$.
Η διαδικασία παραγωγής του δημοσίου κλειδιού περιγράφεται στο παρακάτω διάγραμμα:

$$\begin{array}{c} \bar{x} = (x_1, x_2, \ldots, x_n) \\ \Downarrow \\ S(\bar{x}) = \bar{u} \overset{\beta_i}{=} u \\ \Downarrow \\ f(u) = v \overset{\beta_i}{=} \bar{v} \\ \Downarrow \\ T(\bar{v}) = \bar{y} \end{array}$$

Επομένως αν $\bar{x}$ είναι το καθαρό μήνυμα και $\bar{y}$ το κρυπτογραφημένο τότε ισχύει:

$$\bar{y} = T(f(S(\bar{x}))) \quad \kappa\alpha\iota \quad \begin{cases} y_1 = G_1(x_1, \ldots, x_n) \\ \vdots \\ y_n = G_n(x_1, \ldots, x_n) \end{cases}$$

Οι n πολυωνυμικές εξισώσεις $G_1, \ldots, G_n$ που προκύπτουν, οι οποίες είναι δευτέρου βαθμού ως προς τα x_i και γραμμικές ως προς τα y_i, αποτελούν το δημόσιο κλειδί.

Τα **κρυφά κλειδιά** είναι:
• Η βάση του $\mathbb{K}$ ως $\mathbb{F}_q$-διανυσματικός χώρος.
• Το πολυώνυμο $f(\mathbf{x}) \in \mathbb{K}[\mathbf{x}]$.
• Οι γραμμικές αντιστρέψιμες απεικονίσεις S, T.

Κρυπτογράφηση
Η κρυπτογράφηση ενός μηνύματος απαιτεί μόνο την επίλυση ενός γραμμικού συστήματος ως προς τα y_i.

Αποκρυπτογράφηση:
Για να αποκρυπτογραφήσει η Αλίκη το μήνυμα ακολουθεί την εξής διαδικασία:
• Εφαρμόζει την T^{-1} στο $\bar{y}$.
• Αναπαριστά το $T^{-1}(\bar{y})$ ως στοιχείο του $\mathbb{K}$.
• Με δεξιό μέλος αυτό το στοιχείο παραγοντοποιεί το κρυφό πολυώνυμο μιας μεταβλητής που επέλεξε στην αρχή.
• Εφαρμόζει την S^{-1} στις συνιστώσες της λύσης και παίρνει το $\bar{x} = (x_1, \ldots, x_n)$.

Το παρακάτω διάγραμμα περιγράφει την διαδικασία αποκρυπτογράφησης:

$$\begin{array}{c} \bar{y} = (y_1, y_2, \ldots, y_n) \\ \Downarrow \\ T^{-1}(\bar{y}) \stackrel{\beta_i}{=} Y \\ \Downarrow \\ f(\mathbf{x}) - Y \\ \Downarrow \qquad\qquad (παραγοντοποίηση) \\ S^{-1}(x) = \bar{x} \end{array}$$

Ο ωτακουστής δεν μπορεί να χρησιμοποιήσει αυτήν την διαδικασία εφόσον δεν γνωρίζει τις απεικονίσεις S, T. Ένα παράδειγμα με βάση το HFE κρυπτοσύστημα βρίσκεται στο παράρτημα.

Κεφάλαιο 3

Σχήματα Ψηφιακών Υπογραφών

3.1 Σχήμα υπογραφής με βάση το κρυπτοσύστημα HPE.

Ο Ilia Toli στο [IT1] έδωσε ένα σχήμα ψηφιακής υπογραφής βασισμένο στο κρυπτοσύστημα HPE. Ο Βίκτορας, για να μπορέσει να υπογράψει ένα μήνυμα, φτιάχνει ένα κρυπτοσύστημα HPE όπως παραπάνω με $[\mathbb{K}_B : \mathbb{F}_{q_B}] = n_B$. Υποθέτουμε ότι οι συναρτήσεις "κόφτες "(Hash Functions) είναι δημόσια δοσμένες και στέλνουν τα μηνύματα σε n-άδες με στοιχεία από το $\mathbb{F}_{q_B}$.
Ο Βίκτορας υπογράφει ένα μήνυμα ως εξής:

- Υπολογίζει το $H(M) = (y_1, y_2, \ldots, y_{n_B}) = \bar{y}_B$ και θέτει $\bar{v}_B = \bar{y}_B + \bar{d}_B$.
- Υπολογίζει το $\mathbf{v}_B \in \mathbb{K}_B$ και βρίσκει μια λύση $\mathbf{u}_B$ του κρυφού πολυωνύμου $f_B(\mathbf{u}_B, \mathbf{v}_B) = 0$ στο $\mathbb{K}_B$.
- Υπολογίζει το $\bar{u}_B$ και θέτει $\bar{x} = \bar{u}_B - \bar{c}_B$.
- Το $(x_1, x_2, \ldots, x_{n_B})$ είναι η υπογραφή του μηνύματος M.

Για να πιστοποιήσει η Αλίκη την υπογραφή υπολογίζει το $H(M) = (y_1, y_2, ..$ $\ldots, y_{n_B})$. Εάν $(x_1, x_2, \ldots, x_{n_B}), (y_1, y_2, \ldots, y_{n_B})$ είναι λύση του δημοσίου κλειδιού του Βίκτορα τότε αποδέχεται το υπογεγραμμένο μήνυμα, αλλιώς καταλαβαίνει ότι έχει επέμβει ο ωτακουστής και το απορρίπτει.

Εάν ο ωτακουστής θέλει να υποδυθεί τον Βίκτορα για να στείλει στην Αλίκη το δικό του μήνυμα με τιμή ΄κόφτη΄ $\mathbf{y} = (y_1, y_2, \ldots, y_{n_B})$, τότε για να βρεί μια υπογραφή $(x_1, x_2, \ldots, x_{n_B})$ πρέπει να λύσει τις εξισώσεις του συστήματος του Βίκτορα ως προς $(x_1, x_2, \ldots, x_{n_B})$. Η δυσκολία αυτού του προβλήματος εξασφαλίζει και την ασφάλεια της αυθεντικότητας της υπογραφής. Με όμοιο τρόπο δουλεύει και το σχήμα υπογραφής του κρυπτοσυστήματος HFE.

3.2 Σχήμα υπογραφής Sflash^{v3}.

Οι N.Courtois, L.Goubin και J.Patarin στο [CGP] πρότειναν ένα σχήμα υπογραφής δημοσίου κλειδιού το Sflash^{v3} το οποίο αποτελεί μια νέα έκδοση των Sflash^{v1} και Sflash^{v2}. Το Sflash^{v3} έχει σχεδιαστεί για συγκεκριμένες απαιτήσεις, για τις οποίες το κόστος των κλασσικών κρυπτογραφικών αλγορίθμων (RSA, DSA, ελλειπτικές καμπύλες) είναι πολύ μεγάλο, είτε είναι πολύ αργοί, είτε το μέγεθος της υπογραφής είναι μεγάλο. Αντίθετα το Sflash^{v3} είναι ένα πολύ γρήγορο σχήμα υπογραφής τόσο για την παραγωγή υπογραφής όσο και για την επαλήθευσή της. Επιπλέον, το επίπεδο ασφάλειάς του είναι 2^{80} πράξεις με τα υπάρχοντα δεδομένα στην ικανότητα κρυπτανάλυσης, ενώ η καλύτερη επίθεση που έχει γίνει απαιτεί 2^{100} πράξεις.

Θα δηλώνουμε με $\|$ την διαδικασία συναρμογής, δηλαδή εάν $\lambda = (\lambda_0, \ldots, \lambda_m)$ και $\mu = (\mu_0, \ldots, \mu_n)$ δυο σύνολα στοιχείων ενός δοσμένου σώματος, τότε με $\lambda \| \mu$ θα έχουμε το εξής σύνολο στοιχείων:

$$\lambda \| \mu = (\lambda_0, \ldots, \lambda_m, \mu_0, \ldots, \mu_n).$$

Επίσης, για δοσμένο $\lambda = (\lambda_0, \ldots, \lambda_m)$ και δυο ακέραιους r, s τέτοιους ώστε $0 \leq r \leq s \leq m$, ορίζουμε το $[\lambda]_{r \to s}$ να είναι:

$$[\lambda]_{r \to s} = (\lambda_r, \lambda_{r+1}, \ldots, \lambda_{s-1}, \lambda_s).$$

Παράμετροι του Αλγορίθμου.
Ο αλγόριθμος χρησιμοποιεί τρια πεπερασμένα σώματα.
• Το $\mathbb{K} = \mathbb{F}_{128}$, το οποίο είναι ορισμένο ως $\mathbb{K} = \mathbb{F}_2[X]/\ mod\ (X^7 + X + 1)$. Ορίζουμε την απεικόνιση $\pi : \{0,1\}^7 \to \mathbb{K}$ έτσι ώστε:

$$\forall\ b = (b_0, \ldots, b_6) \in \{0,1\}^7,\ \pi(b) = b_6 X^6 + \ldots + b_1 X + b_0\ mod\ (X^7 + X + 1).$$

• Το $\mathcal{L} = \mathbb{K}[X]/(X^{67} + X^5 + X^2 + X + 1)$. Ορίζουμε την απεικόνιση $\varphi : \mathbb{K}^{67} \to \mathcal{L}$ τέτοια ώστε:

$$\forall\, \omega = (\omega_0, \ldots, \omega_6) \in \mathbb{K}^{67}, \varphi(\omega) = \omega_{66} X^{66} + \ldots + \omega_1 X + \omega_0\ mod\,(X^{67} + X^5 + X^2 + X + 1).$$

Ο αλγόριθμος χρησιμοποιεί δυο αφινικές απεικονίσεις s και t από το $\mathbb{K}^{67}$ στο $\mathbb{K}^{67}$, καθεμιά αποτελείται από ένα κρυφό γραμμικό μέρος S_L αντίστοιχα T_L και από ένα σταθερό μέρος S_C αντίστοιχα T_C.

Κρυφές παράμετροι.
• Μία κρυφή γραμμική απεικόνιση από το $\mathbb{K}^{67}$ στο $\mathbb{K}^{67}$ παριστάνεται με έναν 67×67 τετραγωνικό πίνακα με στοιχεία από το $\mathbb{K}$ γραμμένα ως προς την κανονική βάση του $\mathbb{K}^{67}$. Δηλώνουμε με S_L αυτόν τον πίνακα.
• Μία ακόμη γραμμική απεικόνιση από το $\mathbb{K}^{67}$ στο $\mathbb{K}^{67}$ παριστάνεται με έναν 67×67 τετραγωνικό πίνακα με στοιχεία από το $\mathbb{K}$, ο οποίος δηλώνεται με T_L.
• Μία 80-bit κρυφή συμβολοσειρά που δηλώνεται με Δ.

Ημι-δημόσιες παράμετροι.
Τα σταθερά μέρη των s και t ορίζονται ως:
• Ένα διάνυσμα από το $\mathbb{K}^{67}$, το οποίο παριστάνεται από έναν πίνακα στήλη 67×1 τον S_C.
• Άλλο ένα διάνυσμα από το $\mathbb{K}^{67}$, το οποίο παριστάνεται από τον πίνακα στήλη T_C.

Δεν έχει νόημα να κρατήσουμε κρυφά τα σταθερά μέρη των s και t γιατί και να γίνουν γνωστά δεν επηρεάζεται η ασφάλεια του Sflash, απλά δεν συνίσταται να δημοσιεύονται προκειμένου να γλιτώσουμε χώρο και χρόνο διάδοσης του δημόσιου κλειδιού.

Δημόσιες παράμετροι.
Το δημόσιο κλειδί αποτελείται από μια συνάρτηση $G : \mathbb{K}^{67} \to \mathbb{K}^{56}$ τέτοια ώστε:

$$G(X) = \Big[t\Big(\varphi^{-1}\Big(F(\varphi(s(X)))\Big)\Big)\Big]_{0\to 391}$$

όπου $F : \mathcal{L} \to \mathcal{L}$, είναι μια συνάρτηση που ορίζεται ως:

$$\forall A \in \mathcal{L},\ F(A) = A^{128^{33}+1}$$

και το $_{0\to 391}$ μας επιτρέπει να πάρουμε 56 από τις 67 εξισώσεις.

Από την κατασκευή του αλγορίθμου, η G είναι μια δευτεροβάθμια απεικόνιση πάνω από το $\mathbb{K}$, δηλαδή εάν $(Y_0, \ldots, Y_{55}) = G(X_0, \ldots, X_{66})$ τότε μπορεί ισοδύναμα να γραφεί ως:

$$\begin{cases} Y_0 = P_0(X_0, \ldots, X_{66}) \\ \quad \vdots \\ Y_{55} = P_{55}(X_0, \ldots, X_{66}) \end{cases}$$

όπου κάθε P_i είναι ένα δευτεροβάθμιο πολυώνυμο της μορφής:

$$P_i(X_0, \ldots, X_n) = \sum_{0\le j<k<67} \zeta_{i,j,k} X_j X_k + \sum_{0\le j<67} \nu_{i,j} X_j + \rho_i,$$

και όλα τα στοιχεία $\zeta_{i,j,k}, \nu_{i,j}$ και ρ_i είναι μέσα από το $\mathbb{K}$.

Παραγωγή Υπογραφής Μηνύματος.
Το μήνυμα M δίνεται σαν ακολουθία από bits και η υπογραφή του S λαμβάνεται κάνοντας την παρακάτω διαδικασία:

1. Έστω M_0, M_1, M_2 $\kappa\alpha\iota$ M_3 να είναι τρεις ακολουθίες 160-bit ορισμένες ως:

$$\begin{aligned} M_0 &= SHA-1(M), \\ M_1 &= SHA-1(M_0 \| 0x00), \\ M_2 &= SHA-1(M_0 \| 0x01), \\ M_3 &= SHA-1(M_0 \| 0x02), \end{aligned}$$

   με $0x00$ έως $0x02$ δηλώνουμε έναν χαρακτήρα 8-bit που προστίθεται στο M_0.

2. Έστω V μια 392-bit τυχαία ακολουθία που ορίζεται ως:

$$V = [M_1]_{0\to 159} \parallel [M_2]_{0\to 159} \parallel [M_3]_{0\to 71}.$$

3. Έστω W μια ακολουθία από 77-bit ορισμένη ως:

$$W = [SHA-1(V \parallel \Delta)]_{0\to 76}.$$

4. Έστω Y μια ακολουθία 56 στοιχείων του $\mathbb{K}$ που ορίζονται ως:

$$Y = \Big(\pi([V]_{0\to 6}, \pi([V]_{7\to 13}), \ldots, \pi([V]_{385\to 391})\Big).$$

5. Έστω R μια ακολουθία από 11-bit ορισμένη ως:

$$R = \Big(\pi([W]_{0\to 6}, \pi([W]_{7\to 13}), \ldots, \pi([W]_{70\to 76})\Big).$$

6. Έστω B στοιχείο του $\mathcal{L}$ που ορίζεται ως:

$$B = \varphi(t^{-1}(Y \parallel R)).$$

7. Έστω A στοιχείο του $\mathcal{L}$ που ορίζεται ως:

$$A = F^{-1}(B).$$

   Η συνάρτηση F έχει οριστεί παραπάνω οπότε το $A = F^{-1}(B)$ μπορούμε να το πάρουμε από την σχέση $A = B^h$ όπου h είναι ο αντίστροφος του $128^{33} + 1$ modulo $(128^{67} - 1)$.

8. Έστω $X = (X_0, \ldots, X_{66})$ μια ακολουθία από 67 στοιχεία του $\mathbb{K}$:

$$X = (X_0, \ldots, X_{66}) = s^{-1}(\varphi^{-1}(A)).$$

9. Τέλος, η υπογραφή S είναι η 469-bit συμβολοσειρά που δίνεται ως:

$$S = \pi^{-1}(X_0) \parallel \ldots \parallel \pi^{-1}(X_{66}).$$

Πιστοποίηση Υπογραφής.
Ο παρακάτω αλγόριθμος, για δεδομένο μήνυμα M και υπογραφή S, αποφασίζει την εγκυρότητα ή όχι της υπογραφής.

1. Έστω M_0, M_1, M_2 *και* M_3 να είναι τρεις ακολουθίες 160-bit ορισμένες ως:

$$\begin{aligned} M_0 &= SHA-1(M), \\ M_1 &= SHA-1(M_0 \| 0x00), \\ M_2 &= SHA-1(M_0 \| 0x01), \\ M_3 &= SHA-1(M_0 \| 0x02), \end{aligned}$$

   με $0x00$ έως $0x02$ δηλώνουμε έναν χαρακτήρα 8-bit που προστίθεται στο M_0.

2. Έστω V μια 392-bit τυχαία ακολουθία που ορίζεται ως:

$$V = [M_1]_{0 \to 159} \parallel [M_2]_{0 \to 159} \parallel [M_3]_{0 \to 71}.$$

3. Έστω Y μια ακολουθία από 56 στοιχεία του $\mathbb{K}$ που ορίζεται ως:

$$Y = \Big(\pi([V]_{0 \to 6}, \pi([V]_{7 \to 13}), \ldots, \pi([V]_{385 \to 391})\Big).$$

4. Έστω Y' μια ακολουθία από 56 στοιχεία του $\mathbb{K}$ που ορίζεται ως:

$$Y' = \Big(\pi([S]_{0 \to 6}, \pi([S]_{7 \to 13}), \ldots, \pi([S]_{385 \to 391})\Big).$$

5. • Εάν $Y = Y'$ τότε η υπογραφή γίνεται δεκτή.
   • Αλλιώς, η υπογραφή απορρίπτεται .

Η ασφάλεια του Sflash βασίζεται κυρίως στο NP-πρόβλημα επίλυσης συστημάτων δευτεροβάθμιων εξισώσεων πάνω από ένα πεπερασμένο σώμα. Αν και οι επιθέσεις που γίνονται σε αυτό το πρόβλημα έχουν σημειώσει μεγάλη

πρόοδο τα τελευταία χρόνια, εντούτοις φαίνεται ότι περιορίζονται από αλγεβρικές ιδιότητες του ιδεώδους που παράγουν αυτά τα δημόσια πολυώνυμα καθώς και από την ταχύτητα των αλγορίθμων.

Γενικά Χαρακτηριστικα του Sflash^{v3}.

- Μήκος υπογραφής: 469 bits.
- Μήκος δημοσίου κλειδιού: $112,3$ Kbytes.
- Μήκος κρυφού κλειδιού: $7,8$ Kbytes.
- Χρόνος υπογραφής μηνύματος: λιγότερο από 1 ms.
- Χρόνος πιστοποίησης υπογραφής: λιγότερο από 1 ms.
- Χρόνος παραγωγής ενός ζεύγους δημοσίου\ιδιωτικού κλειδιού: λιγότερο από 1 ms.
- Καλύτερη επίθεση: περισσότεροι από 2^{90} υπολογισμοί.

Κεφάλαιο 4

Κρυπτανάλυση

4.1 Περιγραφή των βάσεων Gröbner.

Η κρυπτανάλυση των συστημάτων δημοσίου κλειδιού που περιγράψαμε στηρίζεται στην επίλυση ενός συστήματος δευτεροβάθμιων εξισώσεων πολλών μεταβλητών πάνω από ένα πεπερασμένο σώμα. Ένας τρόπος επίλυσης είναι οι βάσεις Gröbner [JGJG],[CLO], οι οποίες στοχεύουν στην εύρεση μιας βάσης για το ιδεώδες που παράγουν οι εξισώσεις του συστήματος με αποτέλεσμα να αναγόμαστε στην επίλυση ενός ευκολότερου συστήματος.

Έστω $\mathbb{F}$ σώμα, $R = \mathbb{F}[x_1, \ldots, x_n]$ ένας πολυωνυμικός δακτύλιος με n μεταβλητές πάνω από το $\mathbb{F}$ και $f_1, \ldots, f_s \in R$. Τα πολυώνυμα $f_1, \ldots, f_s \in R$ παράγουν το ιδεώδες

$$I = \langle f_1, \ldots, f_s \rangle = \{ \sum_{1 \leq i \leq s} q_i f_i : \ q_i \in R \},$$

ενώ

$$V(I) = \{u \in \mathbb{F}^n : f(u) = 0 \ \gamma\iota\alpha \ \ o\lambda\alpha \ \ \tau\alpha \ \ f \in I\}$$

είναι το αλγεβρικό σύνολο που ορίζεται από το I, το οποίο θα συμβολίζουμε με $V(f_1, \ldots, f_s)$ αντί του $V(< f_1, \ldots, f_s >)$.

Μερική διάταξη $<$ ενός συνόλου S είναι μια μη-ανακλαστική και μεταβατική σχέση:

$$\acute{o}\chi\iota \ (\alpha < \alpha) \ \kappa\alpha\iota \ \alpha < \beta < \gamma \Rightarrow \alpha < \gamma \ \gamma\iota\alpha \ \acute{o}\lambda\alpha \ \tau\alpha \ \alpha, \beta, \gamma, \in S.$$

Οι συνθήκες υποδηλώνουν ότι δεν είναι συμμετρική. Μια μερική διάταξη λέγεται και **ολική διάταξη** εάν, για κάθε ζεύγος $(\alpha, \ \beta) \ \in S \times S$ ισχύει: $\alpha = \beta$, είτε $\alpha < \beta$, είτε $\alpha > \beta$ και **καλή διάταξη** εάν, επιπρόσθετα, κάθε μη κενό υποσύνολο του S έχει ένα ελάχιστο στοιχείο.

Ταυτοποιούμε το διάνυσμα $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ με το μονώνυμο

$$\mathbf{x}^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$$

Ορισμος 4.1.1 *Μια* ***διάταξη μονωνύμων*** *στο* $R = \mathbb{F}[x_1, \ldots, x_n]$ *είναι μια σχέση* $\prec$ *στο* $\mathbb{N}^n$ *τέτοια ώστε:*

1. $H \prec$ *είναι ολική διάταξη,*
2. $\alpha \prec \beta \Rightarrow \alpha + \gamma \prec \beta + \gamma$ *για όλα τα* $\alpha, \beta, \gamma \in \mathbb{N}^n$,
3. $H \prec$ *είναι καλή διάταξη.*

Παράδειγμα 4.1.1 *Τρεις διαφορετικές διατάξεις μονωνύμων είναι οι εξής: Έστω* $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$. *Τότε:*

1. ***Λεξικογραφική διάταξη:***
   $\alpha \prec_{lex} \beta \iff$ *το πιο αριστερό μη-μηδενικό στοιχείο του* $\alpha - \beta$ *είναι αρνητικό.*
2. ***Βαθμωτή λεξικογραφική διάταξη:***
   $$\alpha \prec_{grlex} \beta \iff \sum_{1 \le i \le n} \alpha_i < \sum_{1 \le i \le n} \beta_i \text{ ή } \Big(\sum_{1 \le i \le n} \alpha_i = \sum_{1 \le i \le n} \beta_i \text{ και } \alpha \prec_{lex} \beta \Big).$$
3. ***Αντίστροφη βαθμωτή λεξικογραφική διάταξη:***
   $$\alpha \prec_{grevlex} \beta \iff \sum_{1 \le i \le n} \alpha_i < \sum_{1 \le i \le n} \beta_i \text{ ή } \Big(\sum_{1 \le i \le n} \alpha_i = \sum_{1 \le i \le n} \beta_i \text{ και}$$
   $$\text{το πιο δεξιό στοιχείο του } \alpha - \beta \in \mathbb{Z}^n \text{ είναι θετικό.} \Big)$$

Θεώρημα 4.1.2 *Οι* $\prec_{lex}, \prec_{grlex}$ *και* $\prec_{grevlex}$, *είναι διατάξεις μονωνύμων.*

Απόδειξη:
Για την απόδειξη του παραπάνω θεωρήματος απλά ελέγχεται εάν ισχύουν οι συνθήκες 1, 2, 3 του ορισμού 4.1.1 για κάθε μια από τις διατάξεις ξεχωριστά. Συγκεκριμένα, για την βαθμωτή αντίστροφη λεξικογραφική διάταξη, $\prec_{grevlex}$, ξέρουμε ότι είναι μερική διάταξη και για κάθε $\alpha, \beta \in \mathbb{N}^n$ με $\alpha \neq \beta$, έχουμε είτε $\sum_{1 \le i \le n} \alpha_i < \sum_{1 \le i \le n} \beta_i$ ή $\sum_{1 \le i \le n} \beta_i < \sum_{1 \le i \le n} \alpha_i$ ή $\sum_{1 \le i \le n} \alpha_i = \sum_{1 \le i \le n} \beta_i$ και στην τελευταία περίπτωση είτε το πιο δεξιό μη-μηδενικό στοιχείο του $\alpha - \beta$ είναι θετικό, είτε το πιο δεξιό μη-μηδενικό στοιχείο του $\beta - \alpha$ είναι θετικό. Επομένως, η $\prec_{grevlex}$ είναι ολική διάταξη.

Για την συνθήκη 2 έχουμε:

$$\sum_{1\leq i\leq n}\alpha_i < \sum_{1\leq i\leq n}\beta_i \Longleftrightarrow \sum_{1\leq i\leq n}(\alpha_i+\gamma_i) < \sum_{1\leq i\leq n}(\beta_i+\gamma_i),$$

ομοίως για " = "και $\alpha-\beta=(\alpha+\gamma)-(\beta+\gamma)$. Τέλος για την συνθήκη 3, εάν $S\subseteq\mathbb{N}^n$ ένα μη κενό σύνολο και $T\subseteq S$ το σύνολο των μονωνύμων του S με συνολικά μικρότερο βαθμό, τότε το T είναι πεπερασμένο (εφόσον για οποιοδήποτε $m\in\mathbb{N}$ υπάρχουν πεπερασμένα μονώνυμα συνολικού βαθμού m) και $\min T=\min S$.□

Ορισμος 4.1.3 *Έστω $f=\sum_{\alpha\in\mathbb{N}^n}c_\alpha x^\alpha\in R$ ένα μη-μηδενικό πολυώνυμο με $c_\alpha\in\mathbb{F}$ και $\prec$ μια διάταξη μονωνύμων. Τοτε:*

1. *Κάθε $c_\alpha x^\alpha$ με $c_\alpha\neq 0$ είναι όρος του f.*
2. *Ο **πολυβαθμός** του f είναι: $mdeg(f)=\max_\prec\{\alpha\in\mathbb{N}^n : c_\alpha\neq 0\}$, όπου $\max_\prec$ είναι το maximum ως προς την $\prec$.*
3. *Ο **επικεφαλής συντελεστής** του f είναι: $lc(f)=c_{mdeg(f)}\in\mathbb{F}\setminus\{0\}$.*
4. *Το **επικεφαλής μονώνυμο** του f είναι: $lm(f)=x^{mdeg(f)}\in R$.*
5. *Ο **επικεφαλής όρος** του f είναι: $lt(f)=lc(f)\cdot lm(f)\in R$.*

Λήμμα 4.1.4 *Έστω $\prec$ μια διάταξη μονωνύμων πάνω από το R και $f,g\in R\backslash\{0\}$. Ισχύει:*

1. *$mdeg(fg)=mdeg(f)+mdeg(g)$.*
2. *Εάν $f+g\neq 0$ τότε $mdeg(f+g)\preceq\max\{mdeg(f),mdeg(g)\}$, με ισότητα εάν $mdeg(f)\neq mdeg(g)$.*

Στόχος μας είναι να δώσουμε έναν αλγόριθμο διαίρεσης με υπόλοιπο στο R. Εάν $f,f_1,\ldots,f_s\in R$ πολυώνυμα θέλουμε να γράψουμε $f=q_1f_1+\ldots+q_sf_s+r$ με $q_1,\ldots,q_s,r$ από το R.

Αλγόριθμος διαίρεσης πολυωνύμων πολλών μεταβλητών με υπόλοιπο.

Είσοδος: Μη μηδενικά πολυώνυμα $f, f_1, \ldots, f_s \in R = \mathbb{F}[x_1, \ldots, x_n]$, όπου το $\mathbb{F}$ είναι σώμα και $\prec$ είναι διάταξη μονωνύμων πάνω από το R.
Έξοδος: $q_1, \ldots, q_s, r \in R$. τέτοια ώστε $f = q_1 f_1 + \ldots + q_s f_s + r$ και κανένα μονώνυμο του r δεν διαιρείται από τα $lt(f_1), \ldots, lt(f_s)$.

1. $r \longleftarrow 0, \quad p \longleftarrow f$
   Για $i = 1, \ldots, s$ **θέσε** $q_i \longleftarrow 0$

2. **Όσο** το $p \neq 0$ **κάνε**

3. **Εάν** το $lt(f_i)$ διαιρεί το $lt(p)$ για κάποιο $i \in \{1, \ldots, s\}$
   τότε επέλεξε κάποιο i, $\quad q_i \longleftarrow q_i + \frac{lt(p)}{lt(f_i)}, \quad p \longleftarrow p - \frac{lt(p)}{lt(f_i)} f_i$
   αλλιώς $r \longleftarrow r + lt(p), \quad p \longleftarrow p - lt(p)$

4. **επίστρεψε** $q_1, \ldots, q_s, r$.

Εάν κάνουμε τον αλγόριθμο αιτιοκρατικό, επιλέγοντας κάθε φορά το μικρότερο i στο βήμα 3, τότε τα πηλίκα $q_1, \ldots, q_s$ και το υπόλοιπο r είναι μοναδικά ορισμένα.

Ορισμος 4.1.5 *Ένα* ***ιδεώδες μονωνύμων*** $I \subseteq R$ *είναι το ιδεώδες που παράγεται από τα μονώνυμα του* R*, για τα οποία υπάρχει υποσύνολο* $A \subseteq \mathbb{N}^n$ *με:*

$$I = \langle x^A \rangle = \langle \{x^\alpha : \alpha \in A\} \rangle.$$

Λήμμα 4.1.6 *Έστω* $I = \langle x^A \rangle \subseteq R$ *ένα ιδεώδες μονωνύμων και* $\beta \in \mathbb{N}^n$*. Τότε:*

$$x^\beta \in I \Longleftrightarrow \exists \alpha \in A \;\; x^\alpha \mid x^\beta.$$

Απόδειξη
"$\Longleftarrow$ "Εάν το x^β είναι πολλαπλάσιο του x^α για κάποιο $\alpha \in A$, τότε το $x^\beta \in I$ εξ ορισμού του ιδεώδους.
"$\Longrightarrow$ "Εάν $x^\beta \in I$, τότε $x^\beta = \sum_i q_i x^{\alpha_i}$ με $\alpha_1, \ldots, \alpha_s \in A$ και $q_1, \ldots, q_s \in R$. Κάθε μονώνυμο του δεξιού μέλους διαιρείται από κάποιο x^α με $\alpha \in A$, οπότε αυτό θα ισχύει και για το αριστερό μέλος, το x^β.□

Λήμμα 4.1.7 *Έστω $I \subseteq R$ ένα ιδεώδες μονωνύμων και $f \in R$. Τότε τα παρακάτω είναι ισοδύναμα:*

1. *$f \in I$,*
2. *Κάθε όρος του f είναι στο I,*
3. *Το f είναι $\mathbb{F}$-γραμμικός συνδυασμός των μονωνύμων του I.*

Θεώρημα 4.1.8 ***Το λήμμα του Dickson***
Κάθε ιδεώδες μονωνύμων παράγεται από ένα πεπερασμένο σύνολο μονωνύμων. Συγκεκριμένα, για κάθε $A \subseteq \mathbb{N}^n$ υπάρχει πεπερασμένο υποσύνολο $B \subseteq A$ τέτοιο ώστε: $\langle x^A \rangle = \langle x^B \rangle$.

Για κάθε υποσύνολο $G \subseteq R$ διαφορετικό του Ø και του $\{0\}$ ορίζουμε $lt(G) = \{lt(g) : g \in G\}$. Έαν $I \subseteq R$ είναι ένα ιδεώδες, τότε υπάρχει πεπερασμένο υποσύνολο $G \subseteq R$ τέτοιο ώστε $\langle lt(G) \rangle = \langle I \rangle$ (από το λήμμα του Dickson). Μπορεί όμως να συμβεί το πεπερασμένο σύνολο G να παράγει το I αλλά $\langle lt(G) \rangle \subset \langle I \rangle$.

Λήμμα 4.1.9 *Έστω I ένα ιδεώδες του $R = \mathbb{F}[x_1, \ldots, x_n]$. Εάν $G \subseteq I$ ένα πεπερασμένο υποσύνολο τέτοιο ώστε: $\langle lt(G) \rangle = \langle lt(I) \rangle$, τότε $\langle G \rangle = I$.*

Απόδειξη
Έστω $G = \{g_1, \ldots, g_s\}$. Εάν το f είναι ένα αυθαίρετο πολυώνυμο του I, τότε από τον αλγόριθμο διαίρεσης με υπόλοιπο έχουμε, $f = q_1 g_1 + \ldots + q_s g_s + r$, με $q_1, \ldots, q_s, r \in R$ τέτοιο ώστε, είτε $r = 0$, είτε κανένας όρος του r δεν διαιρείται από κανένα πρώτιστο όρο των g_i. Όμως, $r = f - q_1 g_1 - \ldots - q_s g_s \in I$, οπότε $lt(r) \in lt(I) \subseteq \langle lt(g_1), \ldots, lt_(g_s) \rangle$. Αυτό μαζί με το **Λήμμα 4.1.6** προκύπτει ότι $r = 0$. Άρα, $f \in \langle g_1, \ldots, g_s \rangle = \langle G \rangle$.□

Θεώρημα 4.1.10 ***(Θεώρημα βάσης του Hilbert)***
Κάθε ιδεώδες I του $R = \mathbb{F}[x_1, \ldots, x_n]$ είναι πεπερασμένα παραγόμενο. Ειδικότερα, υπάρχει πεπερασμένο υποσύνολο $G \subseteq I$ τέτοιο ώστε $\langle G \rangle = I$ και $\langle lt(G) \rangle = \langle lt(I) \rangle$.

Ορισμος 4.1.11 *Έστω $\prec$ μια διάταξη μονωνύμων και $I \subseteq R$ ένα ιδεώδες. Ένα πεπερασμένο σύνολο $G \subseteq I$ είναι βάση Gröbner του I ως προς την $\prec$, εάν $\langle lt(G) \rangle = \langle lt(I) \rangle$.*

Πόρισμα 4.1.12 *Κάθε ιδεώδες I του $R = \mathbb{F}[x_1, \ldots, x_n]$ έχει βάση Gröbner.*

Λήμμα 4.1.13 *Έστω G μια βάση Gröbner ενός ιδεώδους $I \subseteq R$ και $f \in R$. Τότε υπάρχει μοναδικό πολυώνυμο $r \in R$ με*

1. $f - r \in I$,
2. *κανένας όρος του r δεν διαιρείται από κανένα μονώνυμο του $lt(G)$.*

Απόδειξη
Ο αλγόριθμος διαίρεσης δίνει ότι $f = \alpha_1 g_1 + \ldots + \alpha_t g_t + r$ όπου το r ικανοποιεί την συνθήκη 2 καθώς και την συνθήκη 1 αφού $f - r = \alpha_1 g_1 + \ldots + \alpha_t g_t \in I$. Αυτό αποδεικνύει την ύπαρξη του r. Για να αποδείξουμε την μοναδικότητα υποθέτουμε ότι υπάρχουν δυο τέτοια πολυώνυμα r_1, r_2 τέτοια ώστε $f = g_1 + r_1 = g_2 + r_2$ με $g_1, g_2 \in I$ και κανένας όρος των r_1, r_2 δεν διαιρείται από κανένα όρο του $lt(G)$. Τότε $r_1 - r_2 = g_2 - g_1 \in I$ και το $lt(r_1 - r_2)$ θα διαιρείται από κάποιο $lt(g_i)$ με $g_i \in G$ από το λήμμα 4.1.6. Τότε προκύπτει ότι $r_1 - r_2 = 0$.□

Θεώρημα 4.1.14 *Έστω G μια βάση Gröbner ενός ιδεώδους $I \subseteq R$ ως προς την διάταξη μονωνύμων $\prec$ και $f \in R$. Τότε, το $f \in I$ εάν το υπόλοιπο της διαίρεσης του f με το G είναι μηδέν.*

Το θεώρημα βάσης του Hilbert δεν μας δίνει τον τρόπο υπολογισμού μιας βάσης Gröbner ενός ιδεώδους I από μια δοσμένη βάση G. Προκειμένου να κατασκευάσουμε μια βάση Gröbner ερευνούμε πότε η G θα αποτύγχανε να είναι βάση Gröbner. Ένας πιθανός λόγος είναι ότι ο γραμμικός συνδυασμός $ax^\alpha g + bx^\beta h$ δυο πολυωνύμων g, h με $a, b \in \mathbb{F}$ και $\alpha, \beta \in \mathbb{N}^n$ μπορεί να οδηγήσει σε ένα πολυώνυμο του οποίου ο πρώτιστος όρος να μην διαιρείται από κανένα $lt(G)$ με απαλοιφή των πρωτίστων ορών.

Ορισμος 4.1.15 *Έστω $g, h \in R$ μη μηδενικά,$\alpha = (\alpha_1, \ldots, \alpha_n) = mdeg(g)$, $\beta = (\beta_1, \ldots, \beta_n) = mdeg(h)$ και $\gamma = (\max\{\alpha_1, \beta_1\}, \ldots, \max\{\alpha_n, \beta_n\})$. Το S-πολυώνυμο των g, h είναι:*

$$S(g,h) = \frac{x^\gamma}{lt(g)}\, g - \frac{x^\gamma}{lt(h)}\, h \in R$$

Ισχύει ότι, $S(g,h) = -S(h,g)$ και εφόσον $x^\gamma / lt(g), x^\gamma / lt(h) \in R$ τότε $S(g,h) \in \langle g, h \rangle$.

Θεώρημα 4.1.16 *Ένα πεπερασμένο σύνολο $G = \{g_1, \ldots, g_s\} \subseteq R$ είναι βάση Gröbner του ιδεώδους $\langle G \rangle$ αν και μόνον αν το υπόλοιπο της διαίρεσης του $S(g_i, g_j)$ με το $(g_1, \ldots, g_s)$ είναι ίσο με μηδέν για $1 \leq i < j \leq s$.*

Στην συνέχεια περιγράφουμε τον αλγόριθμο του **Buchberger,** ο οποίος μας επιτρέπει να υπολογίζουμε βάσεις Gröbner.

Αλγόριθμος υπολογισμού βάσεων Gröbner

Είσοδος: Τα πολυώνυμα $f_1, \ldots, f_s \in R = \mathbb{F}[x_1, \ldots, x_n]$ και η διάταξη μονωνύμων $\prec$.
Έξοδος: Μια βάση Gröbner $G \subseteq R$ για το ιδεώδες $I = \langle f_1, \ldots, f_s \rangle$ ως προς την διάταξη $\prec$ με $f_1, \ldots, f_s \in G$.

1. $G \longleftarrow \{f_1, \ldots, f_s\}$
2. **επανάλαβε**
3. $\mathcal{S} \longleftarrow \emptyset$
   διέταξε με κάποιο τρόπο τα στοιχεία του G ως $g_1, \ldots, g_t$
   Για $1 \leq i < j \leq t$ **κάνε**
   $r \longleftarrow$ υπόλοιπο των $\{S(g_i, g_j), (g_1, \ldots, g_t)\}$
   Έαν $r \neq 0$ **τότε** $\mathcal{S} \longleftarrow \mathcal{S} \cup \{r\}$.
4. **Εάν** $\mathcal{S} = \emptyset$ **τότε επίστρεψε** το G **αλλιώς** $G \longleftarrow G \cup \mathcal{S}$.

Παράδειγμα 4.1.2 *Στο παράδειγμα αυτό θα υπολογίσουμε μια βάση Gröbner για το ιδεώδες $I = \langle f_1, f_2 \rangle$. Θα δηλώνουμε με* **f rem G** *το υπόλοιπο της διαίρεσης του f με το G.*

Έστω $\prec = \prec_{grlex}$ με $y \prec x$, $f_1 = x^3 - 2xy$ και $f_2 = x^2y - 2y^2 + x \in \mathbb{Q}[x, y]$. Το $G = \{f_1, f_2\}$ δεν είναι βάση Gröbner αφού $S(f_1, f_2) = -x^2$ και $lt(S(f_1, f_2)) = -x^2 \notin \langle x^3, x^2y \rangle = \langle lt(G) \rangle$. Στην συνέχεια περιλαμβάνουμε το $f_3 = S(f_1, f_2)$ $rem(f_1, f_2) = -x^2$ στην βάση μας οπότε θα έχουμε:

$$S(f_1, f_2)\ rem(f_1, f_2, f_3) = 0.$$

Ακόμη,

$$S(f_1, f_3) = 1 \cdot f_1 - (-x) \cdot f_3 = -2xy,$$
$$S(f_1, f_3) rem(f_1, f_2, f_3) = -2xy = f_4,$$

το οποίο προσθέτουμε στην βάση μας, έτσι ώστε $S(f_1, f_3)$ rem $(f_1, f_2, f_3, f_4) = 0$. Έχουμε,

$$S(f_1, f_4) = y \cdot f_1 - (-\frac{1}{2}x^2) \cdot f_4 = -2xy^2 = y \cdot f_4,$$

οπότε $S(f_1, f_4)$ rem $(f_1, f_2, f_3, f_4) = 0$ και

$$S(f_2, f_3) = 1 \cdot f_2 - (-y) f_3 = -2y^2 + x.$$

Αφού προσθέσουμε και το $f_5 = S(f_2, f_3)\ rem\ (f_1, f_2, f_3, f_4) = -2y^2 + x$, *ελέγχουμε και προκύπτει ότι:*

$$S(f_i, f_j)rem(f_1, \ldots, f_5) = 0\ \gamma\iota\alpha\ 1 \leq i < j \leq 5,$$

επομένως η βάση Gröbner είναι $\{f_1, \ldots, f_5\}$.

Λήμμα 4.1.17 *Εάν* G *βάση Gröbner του* $I \subseteq R$, $g \in G$ *και* $lt(g) \in \langle lt(G\backslash\{g\})\rangle$, *τότε το* $G\backslash\{g\}$ *είναι βάση Gröbner του* I.

Ορισμος 4.1.18 *Ένα υποσύνολο* $G \subseteq R$ *καλείται* **ελάχιστη** *βάση Gröbner του* $I = \langle G\rangle$, *εάν αυτό είναι βάση Gröbner του* I *και για κάθε* $g \in G$ *ισχύει:*

1. $lc(g) = 1$,
2. $lt(g) \notin \langle lt(G\backslash\{g\})\rangle$.

Ένα στοιχείο g μιας βάσης Gröbner είναι **ανηγμένο ως προς το** G εάν κανένα μονώνυμο του g δεν είναι στο $\langle lt(G\backslash\{g\})\rangle$. Μια ελάχιστη βάση Gröbner G του $I \subseteq R$ καλείται **ανηγμένη** εάν όλα τα στοιχεία της είναι ανηγμένα ως προς το G.

Θεώρημα 4.1.19 *Κάθε ιδεώδες έχει μοναδική ανηγμένη βάση Gröbner.*

Οι βάσεις Gröbner χρησιμοποιούνται προκειμένου να βοηθήσουν στην επίλυση συστημάτων πολυωνυμικών εξισώσεων πολλών μεταβλητών. Συγκεκριμένα, βρίσκοντας την βάση Gröbner του ιδεώδους που παράγουν οι εξισώσεις του συστήματος και δεδομένου ότι το αλγεβρικό σύνολο που ορίζεται από αυτήν ταυτίζεται με το αλγεβρικό σύνολο που ορίζει το ιδεώδες, συχνά είναι πιο εύκολο να βρούμε τις λύσεις του συστήματος.

Θεωρούμε ένα σύστημα $\mathcal{A}$ δευτεροβάθμιων εξισώσεων πολλών μεταβλητών $l_j = 0,\ (1 \leq j \leq m)$ πάνω από ένα πεπερασμένο σώμα $\mathbb{K}$, όπου κάθε l_j είναι της μορφής $f_j(x_1, \ldots, x_n) - b_j$ με $f_j \in \mathbb{K}[\mathbf{x}] : \mathbb{K}[x_1, \ldots, x_n]$ και $b_j \in \mathbb{K}$,

$$\mathcal{A} : \begin{cases} l_1(x_1, \ldots, x_n) = 0 \\ \quad \vdots \\ l_n(x_1, \ldots, x_n) = 0. \end{cases}$$

Τότε με την βοήθεια της παρακάτω πρότασης μπορούμε να βρούμε τη λύση του συστήματος, εάν αυτή είναι μοναδική.

Παρατήρηση 4.1.1 *Η ανηγμένη βάση Gröbner του ιδεώδους που παράγεται από όλες τις εξισώσεις του $\mathcal{A}$ και τις $x_i^q - x_i,\ i = 1, 2, \ldots, n$ είναι η $\{x_1 - a_1, \ldots, x_n - a_n\}$.*

Πρόταση 4.1.1 *Έστω $\mathcal{A}$ ένα σύστημα πολυωνυμικών εξισώσεων από το $\mathbb{F}_q[x_1, \ldots, x_n]$ και $\mathcal{I}_A$ το ιδεώδες που παράγεται από τις εξισώσεις του $\mathcal{A}$ και τις $x_i^q - x_i,\ i = 1, 2, \ldots, n$. Τότε το $\mathcal{A}$ έχει ως λύση την $(x_1, \ldots, x_n) = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ αν και μονο αν το $\{x_1 - a_1, \ldots, x_n - a_n\}$ είναι η ανηγμένη βάση Gröbner του $\mathcal{I}_A$.*

Παράδειγμα 4.1.3 *Θεώρούμε το σύστημα εξισώσεων:*

$$\begin{aligned} x^2 + y^2 + z^2 &= 1 \\ x^2 + z^2 &= y \\ x &= z \end{aligned}$$

στο $\mathbb{C}^3$.
Αυτές οι εξισώσεις ορίζουν το $I = \langle x^2+y^2+z^2-1, x^2+z^2-y, x-z\rangle \subset \mathbb{C}[x, y, z]$. Θέλουμε να βρούμε όλα τα σημεία του $V(I)$. Αρχικά υπολογίζουμε την βάση Gröbner του I, η οποία είναι $G = \{g_1, g_2, g_3\}$ με

$$\begin{aligned} g_1 &= x - z \\ g_2 &= -y + 2z^2 \\ g_3 &= z^4 + (1/2)z^2 - 1/4 \end{aligned}$$

Παρατηρούμε ότι το πολυώνυμο g_3 εξαρτάται μόνο από το z, οπότε εύκολα βρίσκουμε τις τέσσερις ρίζες του,

$$z = \pm\frac{1}{2}\sqrt{\pm\sqrt{5} - 1}.$$

Στην συνέχεια αντικαθιστάμε τις τιμές του z στις εξισώσεις $g_1 = 0,\ g_2 = 0$, οι οποίες επιλύονται μοναδικά ως προς $x,\ y$. Τέλος, προκύπτουν τέσσερις λύσεις για τις εξισώσεις $g_1 = g_2 = g_3 = 0$ δυο πραγματικές και δυο φανταστικές. Εφόσον, $V(I) = V(g_1, g_2, g_3)$ έχουμε βρει όλες τις λύσεις του αρχικού συστήματος.

Το κόστος υπολογισμού των βάσεων Gröbner παρουσιάζει εκθετική αύξηση. Όταν δουλεύουμε πάνω από το σώμα $\mathbb{F}_2$, τότε ο μέγιστος βαθμός D των πολυωνύμων που σημειώνονται στον υπολογισμό των βάσεων Gröbner, περιλαμβανομένων των εξισώσεων του σώματος $x_i^2 = x_i$, είναι μικρότερος από n. Η πολυπλοκότητα του συνολικού υπολογισμού είναι φραγμένη από ένα πολυώνυμο της τάξεως 2^n.

4.2 Κρυπτανάλυση του κρυπτοσυστήματος HFE με βάση την τεχνική της επαναγραμμικοποίησης.

Οι A.Kipnis, A.Shamir στο [KS] επιχείρησαν με την τεχνική της επαναγραμμικοποιήσης να σπάσουν το HFE κρυπτοσύστημα. Η επίθεση στηρίζεται στην παρατήρηση ότι οποιοδήποτε σύστημα n πολυωνύμων με n μεταβλητές πάνω από ένα μικρό σώμα $\mathbb{F}$ μπορεί να παρασταθεί ως ένα πολυώνυμο μιας μεταβλητής, συγκεκριμένης μορφής, πάνω από μια επέκταση $\mathbb{K}$ του $\mathbb{F}$ βαθμού n. Χρησιμοποιούμε αυτήν την αναπαράσταση προκειμένου να ανάγουμε το αρχικό πρόβλημα επίλυσης συστήματος n δευτεροβάθμιων εξισώσεων με n μεταβλητές πάνω από το μικρό σώμα $\mathbb{F}$, σε ένα νέο πρόβλημα ϵm^2 δευτεροβάθμιων εξισώσεων με m μεταβλητές πάνω από το μεγάλο σώμα $\mathbb{K}$ όπου $\epsilon > 0$. Η κλασσική τεχνική γραμμικοποίησης για την επίλυση τέτοιων συστημάτων αντικαθιστά κάθε γινόμενο μεταβλητών της μορφής $x_i x_j$ με μια νέα μεταβλητή y_{ij} οπότε προκύπτουν ϵm^2 γραμμικές εξισώσεις με $m^2/2$ νέες μεταβλητές y_{ij}.

Στην επίθεσή μας είναι αναγκαίο να είναι το $\epsilon < 1/2$, αλλά τότε η τεχνική της γραμμικοποίησης παράγει πολλές άχρηστες λύσεις που δεν ανταποκρίνονται στις πραγματικές λύσεις των αρχικών δευτεροβάθμιων εξισώσεων. Το πρόβλημα αυτό αντιμετωπίζεται αναπτύσσοντας μια νέα τεχνική, την επαναγραμμικοποίηση, η οποία αναμένεται να λύσει τυχαία συστήματα δευτεροβάθμιων εξισώσεων σε πολυωνυμικό χρόνο για οποιοδήποτε $\epsilon > 0$.

Λήμμα 4.2.1 *Έστω A μια γραμμική απεικόνιση από n-άδες σε n-άδες με τιμές από το $\mathbb{F}$. Τότε υπάρχουν συντελεστές $\alpha_0, \ldots, \alpha_{n-1}$ από το $\mathbb{K}$ τέτοιοι ώστε για οποιεσδήποτε δυο n-άδες με στοιχεία από το $\mathbb{F}$, $(x_0, \ldots, x_{n-1})$ (που αντιστοιχεί στο $x = \sum_{i=0}^{n-1} x_i \omega_i$ στο $\mathbb{K}$) και $(y_0, \ldots, y_{n-1})$ (που αντιστοιχεί στο $y = \sum_{i=0}^{n-1} y_i \omega_i$ στο $\mathbb{K}$), ισχύει: $(y_0, \ldots, y_{n-1}) = A(x_0, \ldots, x_{n-1})$ αν και μόνο αν $y = \sum_{i=0}^{n-1} \alpha_i x^{q^i}$.*

Λήμμα 4.2.2 *Έστω $P_0(x_0, \ldots, x_{n-1}), \ldots, P_{n-1}(x_0, \ldots, x_{n-1})$ ένα σύνολο n πολυωνύμων με n μεταβλητές πάνω από το $\mathbb{F}$. Τότε υπάρχουν συντελεστές $\alpha_0, \ldots, \alpha_{q^n-1}$ από το $\mathbb{K}$ τέτοιοι ώστε για οποιεσδήποτε δυο n-άδες $(x_0, \ldots, x_{n-1})$, $(y_0, \ldots, y_{n-1})$ με στοιχεία από το $\mathbb{F}$, $y_j = P_j(x_0, \ldots, x_{n-1})$ για όλα τα $0 \leq j \leq n-1$ αν και μόνο αν $y = \sum_{i=0}^{q^n-1} \alpha_i x^i$, όπου $x = \sum_{i=0}^{n-1} x_i \omega_i$ και $y = \sum_{i=0}^{n-1} y_i \omega_i$ είναι τα στοιχεία του $\mathbb{K}$ που αντιστοιχούν σε δυο διανύσματα πάνω από το $\mathbb{F}$.*

Λήμμα 4.2.3 *Έστω $\mathcal{C}$ μια συλλογή από n ομογενή πολυώνυμα n μεταβλητών βαθμού d πάνω από το $\mathbb{F}$. Οι μόνες δυνάμεις του x που παρατηρούνται με μημηδενικούς συντελεστές στην αντίστοιχη παράσταση τους από ένα πολυώνυμο*

$G(x)$ μιας μεταβλητής πάνω από το $\mathbb{K}$ είναι αθροίσματα ακριβώς d δυνάμεων του q, όχι απαραιτήτως διαφορετικών, $q^{i_1} + q^{i_2} + \ldots + q^{i_d}$. Εάν το d είναι μια σταθερά τότε το $G(x)$ είναι αραιό και οι συντελεστές του μπορούν να βρεθούν σε πολυωνυμικό χρόνο.

Στο κρυπτοσύστημα δημοσίου κλειδιού HFE του Patarin [P96] θεωρούμε το δημόσιο σύστημα των δευτεροβάθμιων πολυωνύμων $G_0, \ldots, G_{n-1}$ με μεταβλητές $x_0, \ldots, x_{n-1}$. Κάθε πολυώνυμο μπορεί να γραφεί στην τετραγωνική του μορφή $\bar{x}G_i\bar{x}^t$ όπου G_i είναι ένας $n \times n$ πίνακας συντελεστών, το $\bar{x}$ είναι το διάνυσμα γραμμή των μεταβλητών $(x_0, \ldots, x_{n-1})$ και $\bar{x}^t$ το ανάστροφο του. Για την επίθεση χρησιμοποιούμε το λήμμα 4.2.3 για την παράσταση του δημοσίου κλειδιού ως πολυώνυμο μιας μεταβλητής πάνω από το $\mathbb{K}$:

$$G(x) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} g_{ij}x^{q^i+q^j} = \underline{x}G\underline{x}^t \;\; \textit{οπου} \;\; G = [g_{ij}] \; \textit{και} \; \underline{x} = (x^{q^0}, x^{q^1}, \ldots, x^{q^{n-1}}).$$

Η παραπάνω τετραγωνική μορφή είναι αρκετά ασυνήθιστη αφού το διάνυσμα $\underline{x}$ αποτελείται από συσχετιζόμενες μεταβλητές και οχι ανεξάρτητες, καθώς και ότι το $\bar{x}$ είναι διάνυσμα με στοιχεία από το $\mathbb{F}$, ενώ το $\underline{x}$ είναι διάνυσμα με στοιχεία από το $\mathbb{K}$. Ακόμη, οι γραμμικές απεικονίσεις S, T μπορούν να παρασταθούν ως πολυώνυμα μιας μεταβλητής και επομένως το δημόσιο κλειδί να προκύψει ως σύνθεση πολυωνύμων μιας μεταβλητής $G(x) = T(P(S(x)))$ πάνω από το $\mathbb{K}$. Ξαναγράφουμε την εξίσωση $T^{-1}(G(x)) = P(S(x))$, όπου το S έχει την μορφή $S(x) = \sum_{i=0}^{n-1} s_i x^{q^i}$ και το T^{-1} που είναι επίσης γραμμική απεικόνιση έχει την μορφή $T^{-1}(x) = \sum_{i=0}^{n-1} t_i x^{q^i}$. Στόχος μας είναι να μελετήσουμε την επίδραση της πολυωνυμικής σύνθεσης $T^{-1}(G(x))$ και $P(S(x))$ στους πίνακες αναπαράστασής τους σε τετραγωνική μορφή.

Θεώρημα 4.2.4 *Ο πίνακας της τετραγωνικής μορφής στο $\underline{x}$ που παριστάνει την πολυωνυμική σύνθεση $T^{-1}(G(x))$ είναι $\sum_{k=0}^{n-1} t_k G^{*k}$, όπου G^{*k} προκύπτει από τον $n \times n$ πίνακα παράστασης του G υψώνοντας κάθε στοιχείο του στην q^k δύναμη στο $\mathbb{K}$ και κυκλικά εναλλάσσοντας σε k βήματα τόσο τις γραμμές όσο και τις στήλες του αποτελέσματος. Ο πίνακας της τετραγωνικής μορφής στο $\underline{x}$ που παριστάνει την πολυωνυμική σύνθεση $P(S(x))$ είναι WPW^t, όπου ο $W = [w_{ij}]$ είναι ένας $n \times n$ πίνακας που ορίζεται ως $w_{ij} = (s_{j-i})^{q^i}$, με τα $j - i$ να υπολογίζονται modulo n.*

Απόδειξη

Η πολυωνυμική αναπαράσταση του $T^{-1}(x)$ είναι $\sum_{k=0}^{n-1} t_k x^{q^k}$ και του $G(x)$ είναι $\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} g_{ij}x^{q^i+q^j}$. Η πολυωνυμική τους σύνθεση μπορεί να υπολογιστεί

χρησιμοποιώντας το γεγονός ότι η ύψωση αθροισμάτων στην q^i δύναμη είναι γραμμική απεικόνιση:

$$T^{-1}(G(x)) = \sum_{k=0}^{n-1} t_k (\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} g_{ij} x^{q^i+q^j})^{q^k} = \sum_{k=0}^{n-1} t_k \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} (g_{ij})^{q^k} x^{(q^i+q^j)q^k}$$

Οι εκθέτες του q μπορούν να αναχθούν modulo n αφού $x^{q^n} = x^{q^0} = x$ και τα αθροίσματα μπορούν να εναλλάσσονται κυκλικά εάν έχουν υπολογισθεί modulo n.

$$T^{-1}(G(x)) = \sum_{k=0}^{n-1} t_k \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} (g_{ij})^{q^k} x^{q^{i+k}+q^{j+k}} = \sum_{k=0}^{n-1} t_k \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} (g_{i-k,j-k})^{q^k} x^{q^i+q^j}.$$

Ο πίνακας στην αναπαράσταση αυτού του πολυωνύμου σε τετραγωνική μορφή με όρους ως προς $\underline{x}$ είναι $G' = \sum_{k=0}^{n-1} t_k G^{*k}$, όπου τα στοιχεία του G^{*k} στις θέσεις (i,j) είναι $g_{i-k,j-k}^{q^k}$.
Με όμοιο τρόπο αποδεικνύεται και η σύνθεση $P(S(x))$:

$$P(S(x)) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} p_{ij} (\sum_{k=0}^{n-1} s_k x^{q^k})^{q^i+q^j} = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} p_{ij} (\sum_{u=0}^{n-1} s_u x^{q^u})^{q^i} (\sum_{v=0}^{n-1} s_v x^{q^v})^{q^j}$$

Όπως και πριν, χρησιμοποιώντας την γραμμικότητα και την κυκλική εναλλαγή των δεικτών έχουμε:

$$\begin{aligned} P(S(x)) &= \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} p_{ij} (\sum_{u=0}^{n-1} s_u^{q^i} x^{q^{u+i}})(\sum_{v=0}^{n-1} s_v^{q^j} x^{q^{v+j}}) \\ &= \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} p_{ij} (\sum_{u=0}^{n-1} s_{u-i}^{q^i} x^{q^u})(\sum_{v=0}^{n-1} s_{v-j}^{q^j} x^{q^v}) \end{aligned}$$

Αναδιατάσσοντας την σειρά των αθροισμάτων και των πολλαπλασιαστικών όρων παίρνουμε:

$$P(S(x)) = \sum_{u=0}^{n-1}\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}\sum_{v=0}^{n-1} x^{q^u} s_{u-i}^{q^i} p_{ij}\ s_{v-j}^{q^j}\ x^{q^v} = \underline{x} W P W^t \underline{x}^t. \square$$

Η επίθεση, δεδομένου του δημόσιου κλειδιού, βασίζεται στην εξίσωση πινάκων πάνω από το $\mathbb{K}$ την $G' = WPW^t$ που καλείται θεμελιώδης εξίσωση. Ο πίνακας G μπορεί εύκολα να υπολογισθεί από την παράσταση του δημόσιου κλειδιού ως πολυώνυμο μιας μεταβλητής πάνω από το $\mathbb{K}$ και εν συνεχεία από την εύρεση της τετραγωνικής του μορφής. Θεωρούμε τον πίνακα $G' = \sum_{k=0}^{n-1} t_k G^{*k}$

με στοιχεία του να είναι γραμμικοί συνδυασμοί των γνωστών $(g_{i-k,j-k})^{q^k}$ με άγνωστους συντελεστές $t_0, t_1, \ldots, t_{n-1}$ από το $\mathbb{K}$. Ο πίνακας P είναι κυριώς γνωστός αφού μόνο τα πάνω αριστερά $r \times r$ στοιχεία του $n \times n$ πίνακα είναι μη-μηδενικά και $r << n$. Ο πίνακας W είναι άγνωστος, αλλά υπάρχουν πολλές σχέσεις μεταξύ των n^2 στοιχείων του αφού όλα αυτά καθορίζονται από n παραμέτρους, μέσω των $w_{ij} = s_{j-i}^{q^i}$. Στόχος μας είναι να χρησιμοποιήσουμε όλες αυτές τις παρατηρήσεις προκειμένου να λύσουμε την θεμελιώδη εξίσωση σε πολυωνυμικό χρόνο.

Ανάκτηση του T

Αρχικά, θα περιγράψουμε την διαδικασία ανάκτησης των $t_0, \ldots, t_{n-1}$ από την θεμελιώδη εξίσωση $G' = WPW^t$, όπου κάθε στοιχείο του G' είναι γραμμικός συνδυασμός των t_k μεταβλητών. Ο πίνακας P αποτελείται το πολύ από r μη-μηδενικές γραμμές οπότε τόσο η βαθμίδα του όσο και η βαθμίδα του WPW^t δεν μπορεί να ξεπεράσει το r. Για τυχαία επιλογή τιμών των t_k η αναμενόμενη βαθμίδα του πίνακα G' είναι πολύ κοντά στο n. Αυτό που κάνει την επιλογή των τιμών t_k σωστή είναι ότι υποχρεωνούμε το G' να έχει ασυνήθιστη μικρή βαθμίδα ίση με r.

Η βασική προσέγγιση γίνεται εκφράζοντας την συνθήκη που υπάρχει για την βαθμίδα του πίνακα ως ένα μεγάλο αριθμό εξισώσεων με μικρό αριθμό μεταβλητών. Η βαθμίδα του πίνακα G' είναι το πολύ r και ο αριστερός πυρήνας του, ο οποίος ορίζεται ως το σύνολο όλων των διανυσμάτων με γραμμές $\widetilde{x}$ πάνω από το $\mathbb{K}$ που ικανοποιούν την $\widetilde{x}G' = 0$, είναι ένας $(n-r)$-διάστασης γραμμικός υπόχωρος. Επομένως, αναμένεται να βρεθούν $n-r$ γραμμικά ανεξάρτητα διανύσματα $\widetilde{x}_1, \ldots, \widetilde{x}_{n-r}$, ακόμη και αν υποχρεώσουμε τα πρώτα $n-r$ στοιχεία του $\widetilde{x}_k$ να έχουν συγκεκριμένες τιμές. Τα υπόλοιπα r στοιχεία σε κάθε ένα από τα $n-r$ διανύσματα $\widetilde{x}_k$ ορίζονται ως νέες μεταβλητές. Κάθε διανυσματική εξίσωση $\widetilde{x}G' = 0$ μπορούμε να την δούμε σαν n βαθμωτές εξισώσεις πάνω από το $\mathbb{K}$ οπότε παίρνουμε συνολικά $n(n-r)$ εξισώσεις με $r(n-r)+n$ μεταβλητές, όπου οι $r(n-r)$ μεταβλητές προέρχονται από τα $\widetilde{x}_k$ ενώ οι n από τα t_i. Το πρόβλημα είναι ότι αυτές οι εξισώσεις είναι δευτεροβάθμιες και δεν ξέρουμε πως να λύσουμε τέτοια μεγάλα συστήματα δευτεροβάθμιων εξισώσεων σε πολυωνυμικό χρόνο αλλά το θετικό είναι ότι αντί του συστήματος των n εξισώσεων με n αγνώστους προκύπτει ένα σύστημα n^2 εξισώσεων με περίπου rn αγνώστους, όπου $r << n$. Θα χρησιμοποιήσουμε την τεχνική της επαναγραμμικοποίησης προκειμένου να λύσουμε το παραπάνω σύστημα.

Θεωρούμε το γενικό πρόβλημα επίλυσης e τυχαίων παραγόμενων ομογενών δευτεροβάθμιων εξισώσεων με n μεταβλητές. Η τεχνική της γραμμικοποίησης αντικαθιστά κάθε δυο μεταβλητές $x_i x_j$ για $i \leq j$ από μια νέα μεταβλητή y_{ij}, με αποτέλεσμα ο συνολικός αριθμός των νέων μεταβλητών να είναι $n(n+1)/2$. Επομένως, κάθε αρχική δευτεροβάθμια εξίσωση με μεταβλητές ως προς x μπορεί να γραφεί ως γραμμική εξίσωση με νέες μεταβλητές ως προς y. Εάν το πλήθος των εξισώσεων ικανοποιεί την $e \geq n(n+1)/2$ περιμένουμε το σύστημα να έχει μοναδική λύση, όμως εάν $e << n(n+1)/2$ περιμένουμε το γραμμικό σύστημα να έχει εκθετικό πλήθος άχρηστων λύσεων y που δεν αντιστοιχούν σε λύσεις του αρχικού συστήματος.

Στη περίπτωση μας έχουμε $m \approx rn$ μεταβλητές αλλά μόνο $e = \epsilon m^2$ εξισώσεις όπου το $\epsilon = 1/r^2$ είναι μικρότερο από $1/2$ και έτσι η μέθοδος της γραμμικοποίησης αποτυγχάνει. Στη συνέχεια περιγράφουμε την τεχνική της επαναγραμμικοποίησης που αναμένεται να λύσει τέτοια συστήματα δευτεροβάθμιων εξισώσεων για οποιοδήποτε $\epsilon > 0$ σε πολυωνυμικό χρόνο.

Η Τεχνική της Επαναγραμμικοποίησης

Θεωρούμε ένα σύστημα ϵm^2 ομογενών δευτεροβάθμιων εξισώσεων με m μεταβλητές $x_1, \ldots, x_m$. Με την αντικατάσταση $y_{ij} = x_i x_j$ για $i \leq j$ προκύπτει ένα σύστημα ϵm^2 εξισώσεων με $m^2/2$ νέες μεταβλητές y_{ij}, του οποίου ο χώρος λύσεων είναι γραμμικός υπόχωρος διάστασης $(1/2-\epsilon)m^2$ οπότε και κάθε λύση μπορεί να εκφρασθεί ως γραμμική συνάρτηση των $(1/2-\epsilon)m^2$ νέων μεταβλητών z_k. Αυτή η παραμετρική λύση μπορεί εύκολα να βρεθεί με απαλοιφή Gauss. Οι περισσότερες από τις y_{ij} λύσεις που βρίσκονται με αυτήν την διαδικασία δεν αντιστοιχούν σε πιθανές x_i λύσεις. Για το λόγο αυτό πρέπει να προσθέσουμε επιπλέον συνθήκες που να συνδέουν τις y_{ij} μεταβλητές μεταξύ τους από τον τρόπο ορισμού τους.
Έστω μια τετράδα δεικτών $1 \leq a \leq b \leq c \leq d \leq m$, τότε στο γινόμενο $x_a x_b x_c x_d$ μπορούμε να βάλουμε τις παρενθέσεις με τρεις διαφορετικούς τρόπους:

$$(x_a x_b)(x_c x_d) = (x_a x_c)(x_b x_d) = (x_a x_d)(x_b x_c) \implies y_{ab} y_{cd} = y_{ac} y_{bd} = y_{ad} y_{bc}$$

Υπάρχουν $m^4/4!$ διαφορετικοί τρόποι για να επιλέξουμε διατεταγμένες τετράδες των διακριτών δεικτών. Κάθε μια επιλογή δίνει 2 εξισώσεις, οπότε παίρνουμε $m^4/12$ δευτεροβάθμιες ξισώσεις με $m^2/2$ y_{ij} μεταβλητές, οι οποίες είναι γραμμικά ανεξάρτητες. Μπορούμε να μειώσουμε τον αριθμό των μεταβλητών σε $(1/2-\epsilon)m^2$ αντικαθιστώντας κάθε μια από τις y_{ij} μεταβλητές από την παραμετρική τους αναπαράσταση ως γραμμικός συνδυασμός των νέων z_k μεταβλητών.

Η μέθοδος της επαναγραμμικοποίησης βασίζεται στην παρατήρηση ότι οι νέες $m^4/12$ δευτεροβάθμιες εξισώσεις με τις νέες $(1/2-\epsilon)m^2$ z_i μεταβλητές μπορούν να γραμμικοποιηθούν ξανά αντικαθιστώντας κάθε z_iz_j για $i \leq j$ από μια νέα μεταβλητή v_{ij}. Το νέο σύστημα έχει $m^4/12$ γραμμικές εξισώσεις με $((1/2-\epsilon)m^2)^2/2$ v_{ij} μεταβλητές. Περιμένουμε αυτό γραμμικό σύστημα να έχει μοναδική λύση όταν $m^4/12 \geq ((1/2-\epsilon)m^2)^2/2$. Αυτό ικανοποιείται όταν $\epsilon \geq 1/2 - 1/\sqrt{6} \approx 0.1$ που είναι το ένα πέμπτο του πλήθους των εξισώσεων που απαιτούνται στην απλή γραμμικοποίηση. Θα δείξουμε ότι για οποιοδήποτε $\epsilon > 0$ υπάρχει ένα σχήμα επαναγραμμικοποίησης το οποίο αναμένεται να λύσει σε πολυωνυμικό χρόνο τυχαία συστήματα ϵm^2 δευτεροβάθμιων εξισώσεων με m μεταβλητές.

Επιστρέφουμε στο αρχικό πρόβλημα ανάκτησης του T από την θεμελιώδη εξίσωση $G' = WPW^t$. Εφόσον έχουμε n^2 δευτεροβάθμιες εξισώσεις με rn μεταβλητές παίρνουμε $\epsilon \approx 1/r^2$. Για μεγάλα σώματα $\mathbb{F}$, το r και το n πέφτουν αρκετά εάν κρατήσουμε καθορισμένα τόσο το βαθμό q^r του κρυφού πολυωνύμου όσο και το μέγεθος q^n του καθαρού μηνύματος. Η χειρότερη περίπτωση είναι όταν $q = 2$ και $r = 13$ οπότε το $\epsilon \approx 0.006$, τότε χρησιμοποιώντας το σχήμα της επαναγραμμικοποίησης όταν έχουμε 8 διαφορετικά x_i έχουμε να λύσουμε ένα μεγάλο σύστημα από $\mathcal{O}(n^8)$ γραμμικές εξισώσεις με $\mathcal{O}(n^8)$ μεταβλητές, το οποίο είναι πολυωνυμικό αλλά μη πρακτικό. Για παράδειγμα εάν αντικαταστήσουμε το $\mathbb{F}_2$ από το $\mathbb{F}_7$, τότε το r πέφτει από το 13 στο 4 και το n από το 100 στο 36. Όσο μικρότερο το r τόσο αυξάνεται το ϵ με αποτέλεσμα χρησιμοποιώντας το σχήμα της επαναγραμμικοποίησης να προκύπτουν μικρότερα συστήματα από $\mathcal{O}(n^6)$ ή και $\mathcal{O}(n^4)$ εξισώσεις με μικρότερο n που δίνει πιο εφικτές λύσεις.

Ανάκτηση του S

Το τελευταίο στάδιο της επίθεσης είναι η ανάκτηση του S, P όταν το T είναι γνωστό. Ο πίνακας $G' = \sum_{k=0}^{n-1} t_k G^{*k}$ στην θεμελιώδη εξίσωση $G' = WPW^t$ είναι πια ένας γνωστός πίνακας. Ο πίνακας P περιέχει το πολύ r μη μηδενικές γραμμές οπότε η βαθμίδα του και η βαθμίδα του $G' = WPW^t$ δεν μπορούν να ξεπεράσουν το r. Υποθέτουμε, χωρίς βλάβη της γενικότητας, ότι η βαθμίδα του P είναι ακριβώς r και ότι η βαθμίδα του W είναι ακριβώς n. Έστω $v_1, \ldots, v_{n-r}$ να είναι μια βάση του αριστερού πυρήνα του G'. Εφόσον ο W^t είναι αντιστρέψιμος, ο αριστερός πυρήνας του WPW^t είναι ίσος με τον αριστερό πυρήνα του WP. Ο αριστερός πυρήνας του P αποτελείται ακριβώς από εκείνα τα διανύσματα που έχουν μηδέν στις πρώτες r-θέσεις και έτσι τα v_i αντιστοιχίζονται μέσω του W σε διανύσματα αυτής της μορφής. Εφόσον ο G' είναι γνωστός, ο αριστερός του πυρήνας μπορεί εύκολα να υπολογισθεί και καθένα από τα $n-r$ διανύσματα βάσης οδηγούν σε r εξισώσεις με άγνωστα τα στοιχεία του W.

Το πρόβλημα μοιάζει να είναι απροσδιόριστο έχοντας $r(n-r)$ γραμμικές εξισώσεις και n^2 μεταβλητές. Μπορούμε να μειώσουμε το πλήθος των μεταβλητών από n^2 σε n αντικαθιστώντας κάθε w_{ij} από $s_{j-i}^{q^i}$ αλλά τότε θα πάρουμε μη-γραμμικές εξισώσεις. Η βασική παρατήρηση είναι ότι αυτές οι μη-γραμμικές εξισώσεις πάνω από το $\mathbb{K}$ γίνονται γραμμικές εάν τις εκλάβουμε ως εξισώσεις πάνω από το $\mathbb{F}$:
Αντικαθιστούμε κάθε s_i από $\sum_{j=1}^{n-1} s_{ij}w_j$ όπου τα s_{ij} είναι ένα νέο σύνολο από n^2 μεταβλητές πάνω από το $\mathbb{F}$. Κάθε $s_{j-i}^{q^i}$ γράφεται ως γραμμικός συνδυασμός s_{uv} μεταβλητών και κάθε εξίσωση πάνω από το $\mathbb{K}$ δίνει μια συλλογή από n γραμμικές εξισώσεις πάνω από το $\mathbb{F}$. Επομένως έχουμε $r(n-r)n$ εξισώσεις με n^2 νέες μεταβλητές πάνω από $\mathbb{F}$ και για κάθε $r > 1$ σύστημα είναι καλά ορισμένο εφόσον $r(n-r)n >> n^2$. Οι λύσεις των ομογενών εξισώσεων προσδιορίζονται πολλαπλασιασμένες με μια σταθερά αλλά κάθε τέτοια λύση είναι ικανοποιητική. Στο παράρτημα υπάρχει κρυπτοσύστημα που κρυπταναλύεται με την τεχνικη της επαναγραμμικοποίησης.

4.3 Ο Αλγόριθμος XL.

Οι Patarin, Courtois, Klimov και Shamir στο [SPCK] Eurocrypt 2000 παρουσίασαν μια επέκταση της μεθόδου επαναγραμμικοποίησης, τον XL (eXtended Linearization) αλγόριθμο, για την επίλυση συστημάτων δευτεροβάθμιων εξισώσεων με πολλές μεταβλητές. Ο αλγόριθμος μπορεί να θεωρηθεί ως συνδυασμός των Gröbner βάσεων (περιορισμένου βαθμού) και της μεθόδου γραμμικοποίησης. Η βασική του ιδέα είναι η παραγωγή από κάθε πολυωνυμική εξίσωση ενός μεγάλου αριθμού μεταβλητών μεγάλου βαθμού που προκύπτουν από τον πολλαπλασιασμό κάθε εξίσωσης με όλα τα πιθανά μονώνυμα φραγμένου βαθμού και στη συνέχεια η γραμμικοποίηση του παραγόμενου συστήματος.

Περιγραφή του Αλγόριθμου XL
Έστω $\mathbb{K}$ ένα πεπερασμένο σώμα και $\mathcal{A}$ ένα σύστημα δευτεροβάθμιων εξισώσεων πολλών μεταβλητών $l_j = 0,\ (1 \leq j \leq m)$ όπου κάθε l_j είναι της μορφής $f_j(x_1, \ldots, x_n) - b_j$ με $f_j \in \mathbb{K}[\mathbf{x}] : \mathbb{K}[x_1, \ldots, x_n]$ και $b_j \in \mathbb{K}$.

$$\mathcal{A} : \begin{cases} l_1(x_1, \ldots, x_n) = 0 \\ \quad \vdots \\ l_n(x_1, \ldots, x_n) = 0 \end{cases}$$

Οι εξισώσεις l_j είναι πάντα δευτεροβάθμιες αλλά μπορούν να περιέχουν ταυτόχρονα γραμμικούς όρους και σταθερές.

Υποθέτοντας ότι το σύστημα $\mathcal{A}$ έχει μοναδική λύση, το πρόβλημα έγκειται στο να βρούμε μια λύση $x = (x_1, \ldots, x_n) \in \mathbb{K}^n$ για δοσμένο $b = (b_1, \ldots, b_n) \in \mathbb{K}^n$. Επειδή το δεξιό μέλος των εξισώσεων $l_j(x_1, \ldots, x_n)$ είναι πάντα μηδέν, η εξίσωση $x_1 \cdot l_2(x_1, \ldots, x_n) = 0$ δηλώνεται απλώς ως εξίσωση $x_1 l_2$. Θα λέμε ότι οι εξισώσεις της μορφής $\prod_{j=1}^{k} x_{i_j} \cdot l_j = 0$, με όλα τα i_j να είναι κατά ζεύγη διαφορετικά, είναι του τύπου $x^k l$ και θα συμβολίζουμε με $x^k l$ το σύνολο όλων αυτών των εξισώσεων. Για παράδειγμα οι αρχικές εξισώσεις του $\mathcal{A}$ είναι του τύπου l. Παρατηρούμε ακόμη ότι κάθε x που είναι λύση των εξισώσεων l_j θα είναι λύση και των εξισώσεων του τύπου $x^k l$ για οποιοδήποτε $k \geq 0$. Επιπλέον, θα δηλώνουμε με x^k το σύνολο όλων των όρων με βαθμό ακριβώς k, $\prod_{j=1}^{k} x_{i_j}$.

Έστω $D \in \mathbb{N}$, θεωρούμε όλα τα πολυώνυμα $\prod_j x_{i_j} l_j$ συνολικού βαθμού $\leq D$ και $\mathcal{I}_D$ ο γραμμικός χώρος που παράγει το σύνολο αυτών των εξισώσεων, δηλαδή το $\mathcal{I}_D$ θα είναι ο γραμμικός χώρος που παράγεται από όλα τα $x^k l, 0 \leq k \leq D-2$ και $\mathcal{I}_D \subseteq \mathcal{I}$, όπου $\mathcal{I}$ το ιδεώδες που παράγεται από τα l_j. Ο σκοπός του αλγόριθμου XL είναι να βρεί ένα σύστημα εξισώσεων στο $\mathcal{I}_D$ που θα επιλύεται ευκολότερα από ότι το αρχικό σύστημα εξισώσεων.

Ο αλγόριθμος ακολουθεί τα παρακάτω βήματα:

1. **Πολλαπλασιασμός:** Παραγωγή όλων των στοιχείων $\prod_{j=1}^{k} x_{i_j} \cdot l_j \in \mathcal{I}_D$ με $k \leq D-2$.

2. **Γραμμικοποίηση:** Θεωρούμε κάθε μονώνυμο του x_i με βαθμό $\leq D$ ως μια νέα μεταβλητή και εφαρμόζουμε Απαλοιφή Gauss στις εξισώσεις του πρώτου βήματος. Η διάταξη των μονωνύμων πρέπει να είναι τέτοια ώστε όλοι οι όροι που περιέχουν μια μεταβλητή (έστω την x_1) να απαλείφονται τελευταίοι.

3. **Επίλυση:** Υποθέτουμε ότι το βήμα 2 δίνει τουλάχιστον μια εξίσωση με δυνάμεις μιας μεταβλητής οπότε και λύνουμε αυτήν την εξίσωση πάνω από το πεπερασμένο σώμα.

4. **Επανάληψη:** Απλοποιούμε τις εξισώσεις και επαναλαμβάνουμε την διαδικασία εύρεσης των τιμών των άλλων μεταβλητών.

Ο XL αλγόριθμος περιέχει τα αποτελέσματα των πολλαπλασιασμών των αρχικών m εξισώσεων l_j με όλα τα πιθανά μονώνυμα βαθμού το πολύ έως $D-2$, έτσι ώστε ο συνολικός βαθμός των τελικών εξισώσεων να είναι D. Σύμφωνα με τις παραπάνω παρατηρήσεις το σύνολο αυτών των εξισώσεων καλείται $\mathcal{I}_D$. Έστω R ο αριθμός των εξισώσεων που παράγουν το $\mathcal{I}_D$ και T ο αριθμός όλων των μονωνύμων. Τότε έχουμε:

$$R = m \cdot \left(\sum_{i=0}^{D-2} \left(\begin{array}{c} n \\ i \end{array} \right) \right) \approx m \cdot \left(\begin{array}{c} n \\ D-2 \end{array} \right)$$

Είναι πιθανόν οι εξισώσεις να μην είναι γραμμικά ανεξάρτητες, για το λόγο αυτό θα δηλώνουμε με Free την διάσταση του $\mathcal{I}_D$ οπότε θα ισχύει $Free \leq R$ και απαραιτήτως $Free \leq T$. Η βασική αρχή του αλγόριθμου είναι η ακόλουθη: για κάποιο D θα έχουμε $R \geq T$ και περιμένουμε να είναι Free$\approx T$ αφού δεν μπορεί να ξεπεράσει το T. Όταν Free$\geq T - D$ τότε είναι πολύ πιθανό να προκύψει μια εξίσωση με μια μεταβλητή, οπότε ο αλγόριθμος επιτυγχάνει.

Παράδειγμα 4.3.1 *Έστω $\mu \neq 0$. Θεωρούμε το πρόβλημα επίλυσης του συστήματος:*

$$x_1^2 + \mu x_1 x_2 = \alpha \quad (4.1)$$
$$x_2^2 + \nu x_1 x_2 = \beta \quad (4.2)$$

Για $D = 4$ και άρτιου βαθμού μονώνυμα οι εξισώσεις που παράγονται στο πρώτο βήμα είναι $l \cup x^2 l$, οι οποίες είναι οι δυο αρχικές εξισώσεις και οι $6 = 2*3$ επιπλέον εξισώσεις που παράγονται από τον πολλαπλασιασμό των δυο αρχικών εξισώσεων l_j με τους τρεις όρους : $x_1^2, x_1x_2, x_2^2 \in x^2$ βαθμού 2.

$$\begin{aligned} x_1^4 + \mu x_1^3 x_2 &= \alpha x_1^2 && (4.3)\\ x_1^2 x_2^2 + \nu x_1^3 x_2 &= \beta x_1^2 && (4.4)\\ x_1^2 x_2^2 + \mu x_1^3 x_2 &= \alpha x_1^2 && (4.5)\\ x_2^4 + \nu x_2^3 x_1 &= \beta x_2^2 && (4.6)\\ x_1^3 x_2 + \mu x_1^2 x_2^2 &= \alpha x_1 x_2 && (4.7)\\ x_1 x_2^3 + \nu x_1^2 x_2^2 &= \beta x_1 x_2 && (4.8) \end{aligned}$$

Στο δεύτερο βήμα απαλείφουμε και υπολογίζουμε:
Από (4.1): $x_1x_2 = \frac{\alpha}{\mu} - \frac{x_1^2}{\mu}$
Από (4.2): $x_2^2 = (\beta - \frac{\alpha\nu}{\mu}) + \frac{\nu}{\mu}x_1^2$
Από (4.3): $x_1^3x_2 = \frac{\alpha}{\mu}x_1^2 - \frac{x_1^4}{\mu}$
Από (4.4): $x_1^2x_2^2 = \beta - \frac{\alpha\nu}{\mu})x_1^2 + \frac{\nu}{\mu}x_1^4$
Από (4.8): $x_1x_2^3 = \frac{\alpha\beta}{\mu} + (\frac{\alpha\nu^2}{\mu} - \beta\nu - \frac{\beta}{\mu})x_1^2 - \frac{\nu^2}{\mu}x_1^4$
Από (4.6): $x_2^4 = (\beta^2 - \frac{2\alpha\beta\nu}{\mu}) + (\frac{2\nu\beta}{\mu} + \beta\nu^2 - \frac{\alpha\nu^2}{\mu})x_1^2 + \frac{\nu^3}{\mu}x_1^4$
Τελικά από την (4.5) παίρνουμε μια εξίσωση με μια μόνο μεταβλητή την x_1 :

$$\alpha^2 + x_1^2(\alpha\mu\nu - \beta\mu^2 - 2\alpha) + x_1^4(1 - \mu\nu) = 0.$$

και την επιλύουμε. Γνωρίζοντας το x_1 υπολογίζουμε στην συνέχεια και το x_2.

Ο XL αλγόριθμος επιτυγχάνει πάντα την επίλυση συστημάτων πολυωνυμικών εξισώσεων όταν βρισκόμαστε πάνω από ένα πεπερασμένο σώμα $\mathbb{F}_q$ [SKI].

Κεφάλαιο 5

Παράρτημα

5.1 Παράδειγμα βασισμένο στο κρυπτοσύστημα HFE.

Στο παράδειγμα που ακολουθεί περιγράφουμε την διαδικασία παραγωγής του δημοσίου κλειδιού για το κρυπτοσύστημα HFE, την κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος καθώς και τρεις επιθέσεις στο κρυπτοσύστημα με τις βάσεις Gröbner, την τεχνική της επαναγραμμικοποίησης και τον XL αλγόριθμο. Για το παράδειγμά μας οι απεικονίσεις S, T που εμφανίζονται στην περιγραφή του κρυπτοσυστήματος θα είναι οι ταυτοτικές.

Έστω $q = 2$ και $f(x) = x^3 + x^2 + 1$ ανάγωγο πολυώνυμο πάνω από το $\mathbb{F}_q[x]$. Θεωρούμε την επέκταση $\mathbb{K} = \mathbb{F}_2[x]/ < x^3 + x^2 + 1 >$ πάνω από το $\mathbb{F}_2$ βαθμού 3 και $\{1, \beta, \beta^2\}$ μια βάση του ως $\mathbb{F}_2$-διανυσματικού χώρου, όπου β η κλάση του $x \ mod \ f(x)$. Συμβολίζουμε με $\bar{x} = (x_0, x_1, x_2) \in \mathbb{F}_2^3$ το καθαρό μήνυμα και με $\bar{y} = (y_0, y_1, y_2) \in \mathbb{F}_2^3$ το κρυπτογραφημένο μήνυμα, οπότε θα είναι $X = x_0 + x_1\beta + x_2\beta^2 \in \mathbb{K}$ και $Y = y_0 + y_1\beta + y_2\beta^2 \in \mathbb{K}$.

Παραγωγή δημοσίου κλειδιού

• Το κρυφό πολυώνυμο που επιλέγει ο χρήστης είναι:

$$F(X) = X^{q^2+1} + X^{q+1} = X^5 + X^3$$

Αντικαθιστώντας με $X = x_0 + x_1\beta + x_2\beta^2$ και με πράξεις (Maple) έχουμε:

$F(X) = (x_2 + x_0x_1 + x_0x_2) + (x_1 + x_2 + x_0x_1 + x_2x_1)\beta + (x_1 + x_2x_1 + x_0x_2)\beta^2.$

Οπότε το δημόσιο κλειδί είναι:

$$\begin{cases} y_0 = x_2 + x_0x_1 + x_0x_2 \\ y_1 = x_1 + x_2 + x_0x_1 + x_2x_1 \\ y_2 = x_1 + x_2x_1 + x_0x_2 \end{cases}$$

Κρυπτογράφηση
Για να κρυπτογραφήσουμε το μήνυμα $(x_0, x_1, x_2) = (1, 1, 1)$, αντικαθιστούμε τα x_i στις δημόσιες εξισώσεις και παίρνουμε $(y_0, y_1, y_2) = (1, 0, 1)$ να είναι το κρυπτογραφημένο μήνυμα.
Αποκρυπτογράφηση
Για την αποκρυπτογράφηση γνωρίζοντας το κρυφό πολυώνυμο $F(X) = Y$, υπολογίζουμε αρχικά το $Y = y_o + y_1\beta + y_2\beta^2 = 1 + \beta^2$ και στην συνέχεια παραγοντοποιούμε το $F(X) - Y$, όπου $F(X)$ πολυώνυμο του X πάνω από το $\mathbb{K}$. Το καθαρό μήνυμα θα δίνεται από τους γραμμικούς όρους που εμφανίζονται στην παραγοντοποίηση, δηλαδή θα έχουμε:

$$F(X) - Y = (X + \beta^2 + \beta + 1)(X + \beta + 1)(X^3 + \beta^2 X + \beta X + \beta).$$

Παρατηρούμε ότι προκύπτουν δυο πιθανά μηνύματα, είτε $X = \beta^2 + \beta + 1 \Rightarrow \bar{x} = (1, 1, 1)$ είτε $X = \beta + 1 \Rightarrow \bar{x} = (1, 1, 0)$. Ένα από τα δυο θα ταιριάζει στο αλφάβητο μας ώστε να έχει νόημα το μήνυμα που στάλθηκε και αυτή θα είναι η πραγματική λύση.

Ο ωτακουστής γνωρίζοντας μόνο τις δημόσιες εξισώσεις και το κρυπτογραφημένο μήνυμα έχει να λύσει το παρακάτω μη γραμμικό σύστημα:

$$\mathcal{A} : \begin{cases} x_2 + x_0x_1 + x_0x_2 - 1 = 0 \\ x_1 + x_2 + x_0x_1 + x_2x_1 = 0 \\ x_1 + x_2x_1 + x_0x_2 - 1 = 0 \end{cases}$$

• Κρυπτανάλυση με βάσεις Gröbner.
Με την βοήθεια του Buchberger αλγορίθμου και επιλέγοντας την λεξικογραφική διάταξη ο ωτακουστής προσπαθεί να υπολογίσει την Gröbner βάση του ιδεώδους $I = \langle f_1, f_2, f_3 \rangle$, όπου:

$$\begin{aligned} f_1(x_0, x_1, x_2) &= x_2 + x_0x_1 + x_0x_2 - 1 \\ f_2(x_0, x_1, x_2) &= x_1 + x_2 + x_0x_1 + x_2x_1 \\ f_3(x_0, x_1, x_2) &= x_1 + x_2x_1 + x_0x_2 - 1 \end{aligned}$$

Ο αλγόριθμος ξεκινά από την βάση $G = (f_1, f_2, f_3)$, υπολογίζει τα $S(f_i, f_j)$, $1 \leq i < j \leq 3$ και ελέγχει εάν το υπόλοιπο της διαίρεσης τους με το (f_1, f_2, f_3) είναι μηδέν.

$$\begin{aligned} S(f_1, f_2) &= x_0x_2 + x_1x_2 + x_1 + 1, \quad S(f_1, f_2)\ rem\ (f_1, f_2, f_3) = 0 \\ S(f_1, f_3) &= x_0x_2 + x_1x_2, \quad S(f_1, f_3)\ rem\ (f_1, f_2, f_3) = x_1 + 1 \neq 0. \end{aligned}$$

Στην συνέχεια, αφού $S(f_1, f_3)\ rem\ (f_1, f_2, f_3) \neq 0$, θέτει $f_4 = x_1 + 1$ και το προσθέτει στη βάση G, οπότε θα έχει:

$$\begin{aligned} S(f_1, f_2)\ rem\ (f_1, f_2, f_3, f_4) = 0 \\ S(f_1, f_3)\ rem\ (f_1, f_2, f_3, f_4) = 0 \\ S(f_2, f_3)\ rem\ (f_1, f_2, f_3, f_4) = 0 \\ S(f_3, f_4)\ rem\ (f_1, f_2, f_3, f_4) = 0 \end{aligned}$$

Αλλά προκύπτει και ότι:

$$\begin{aligned} S(f_1, f_4)\ rem\ (f_1, f_2, f_3, f_4) = x_0 + 1 \neq 0 \\ S(f_2, f_4)\ rem\ (f_1, f_2, f_3, f_4) = x_0 + 1 \neq 0 \end{aligned}$$

Άρα, στο επόμενο βήμα προσθέτει το $f_5 = x_0 + 1$ στην βάση G, υπολογίζει τα $S(f_i, f_j), 1 \leq i < j \leq 5$ και προκύπτει ότι:

$$S(f_i, f_j)\ rem\ (f_1, f_2, f_3, f_4, f_5) = 0 \ \ \forall\ i, j\ \mu\epsilon\ 1 \leq i < j \leq 5.$$

Επομένως, η Gröbner βάση του I είναι:

$$G = \{f_1, f_2, f_3, x_0 + 1, x_1 + 1\}.$$

Ενώ η ανηγμένη Gröbner βάση του I είναι:

$$G' = \{x_0 + 1, x_1 + 1\}.$$

Επειδή το αλγεβρικό σύνολο $V(I)$ που ορίζεται από το I είναι ίδιο με το αλγεβρικό σύνολο $V(G')$ που ορίζεται από το G', το σύνολο λύσεων του αρχικού συστήματος $\mathcal{A}$ είναι: $\{x_0 = 1, x_1 = 1, x_2 \ \in \ \mathbb{F}_2\}$. Επομένως, προκύπτουν δυο λύσεις:

$$(x_0, x_1, x_2) = (1, 1, 1)\ \kappa\alpha\iota\ (x_0, x_1, x_2) = (1, 1, 0).$$

• **Κρυπτανάλυση με την τεχνική της επαναγραμμικοποίησης.**
Αρχικά, προκειμένου να γραμμικοποιήσει το σύστημα $\mathcal{A}$ θέτει $y_{ij} = x_i x_j$ με $y_{01} = x_0x_1,\ y_{02} = x_0x_2,\ y_{21} = x_1x_2,\ y_1 = x_1,\ y_2 = x_2$ και $y_{ij} \in \mathbb{F}_2$ οπότε το γραμμικό σύστημα $\mathcal{A}'$ που προκύπτει είναι:

$$\begin{aligned} y_{01} + y_{02} + y_2 + 1 &= 0 \\ y_{01} + y_{21} + y_1 + y_2 &= 0 \\ y_{02} + y_{21} + y_1 + 1 &= 0 \end{aligned}$$

Λύνοντας το σύστημα με απαλοιφή Gauss έχουμε:

$$\begin{aligned} y_{01} &= y_{21} + y_1 + y_2 \\ y_{02} &= y_{21} + y_1 + 1 \\ y_{21} &= y_{21} \\ y_1 &= y_1 \\ y_2 &= y_2 \end{aligned}$$

Θέτω $y_{21} = z_3,\ y_1 = z_1,\ y_2 = z_2$ οπότε έχω:

$$y_{01} = z_3 + z_1 + z_2,\ y_{02} = z_3 + z_1 + 1$$

Οι επιπλέον συνθήκες που προστίθενται είναι:
$\triangleright\ (x_0x_1)(x_2x_1) = (x_0x_2)(x_1x_1)$
$\Rightarrow y_{01}y_{21} = y_{02}y_1$
$\Rightarrow (z_3 + z_1 + z_2)z_3 = (z_3 + z_1 + 1)z_1$
$\Rightarrow \boxed{z_3 + z_3z_2 = 0}$

$\triangleright\ x_2(x_0x_1) = (x_2x_0)x_1 \Rightarrow y_2y_{01} = y_{02}y_1$
$\Rightarrow z_2(z_3 + z_1 + z_2) = (z_3 + z_1 + 1)z_1$
$\Rightarrow \boxed{z_3z_2 + z_1z_2 + z_3z_1 + z_2 = 0}$

$\triangleright\ x_2(x_2x_1) = (x_2x_2)x_1$
$\Rightarrow y_2y_{21} = y_2y_1$
$\Rightarrow z_2z_3 = z_2z_1$
$\Rightarrow \boxed{z_2z_3 + z_2z_1 = 0}$

Γραμμικοποιώ το σύστημα των τριών τελευταίων εξισώσεων και θέτω:
$v_{ij} = z_iz_j$ με $v_{23} = z_2z_3,\ v_{12} = z_1z_2\ v_{13} = z_1z_3,\ v_3 = z_3$.
Το γραμμικό σύστημα που προκύπτει είναι:

$$\begin{cases} v_3 + v_{23} = 0 \\ v_{23} + v_{12} + v_{13} + v_2 = 0 \\ v_{23} + v_{12} = 0 \end{cases}$$

Λύνοντας το έχουμε:

$$v_{13} = v_2,\ v_{23} = v_{12} = v_3.$$

$\triangleright\ v_2 = 1 \Rightarrow z_2 = y_2 = x_2 = 1$
Συνδυάζοντας τις εξισώσεις προκύπτει ότι
$x_0 = x_1 = x_2 = 1$, οπότε το καθαρό μήνυμα θα είναι: $(x_0, x_1, x_2) = (1, 1, 1)$.

$\triangleright\ v_2 = 0 \Rightarrow z_2 = y_2 = x_2 = 0$
Με ανάλογες πράξεις έχουμε ότι ένα επιπλέον πιθανό μήνυμα είναι:
$(x_0, x_1, x_2) = (1, 1, 0)$.

- **Κρυπτανάλυση με τον αλγόριθμο XL.**

Θέλουμε να λύσουμε το παρακάτω σύστημα:

$$\begin{cases} l_1: \ x_2 + x_0x_1 + x_0x_2 + 1 = 0 \\ l_2: \ x_1 + x_2 + x_0x_1 + x_2x_1 = 0 \\ l_3: \ x_1 + x_2x_1 + x_0x_2 + 1 = 0 \end{cases}$$

• Επιλέγω $D = 4,\ 0 \leq k \leq 2$.
• Παράγω όλα τα μονώνυμα βαθμού $k = 2$, τα οποία είναι: x_0x_1, x_0x_2, x_1x_2.
• Πολλαπλασιάζω κάθε εξίσωση l_j του συστήματος με τα παραπάνω μονώνυμα.
Οι επιπλέον εξισώσεις που προκύπτουν είναι:

$$\begin{cases} x_0x_1x_2 + x_1x_2 = 0 \\ x_2x_0 + x_0x_1x_2 = 0 \end{cases}$$

• Θέτω: $z_1 = x_1, z_2 = x_2, z_3 = x_0x_1, z_4 = x_0x_2, z_5 = x_2x_1, z_6 = x_0x_1x_2$, και λύνω το σύστημα που προκύπτει με απαλοιφή *Gauss*.

$$\begin{cases} z_2 + z_3 + z_4 + 1 = 0 \\ z_1 + z_2 + z_3 + z_5 = 0 \\ z_1 + z_4 + z_5 + 1 = 0 \\ z_5 + z_6 = 0 \\ z_4 + z_6 = 0 \end{cases}$$

Οι λύσεις είναι:

$$z_1 = 1, z_4 = z_5 = z_6, z_2 + z_3 + z_4 = 1.$$

Αφου $z_1 = x_1 = 1$ επιλέγω:

• Αν $z_5 = 0 \Rightarrow x_2 x_1 = 0 \Rightarrow x_2 = 0$.

$z_2 + z_3 = 1 \Rightarrow x_2 + x_0 x_1 = 1 \Rightarrow x_0 = 1$.

Άρα, $(x_0, x_1, x_2) = (1, 1, 0)$.

• Αν $z_5 = 1 \Rightarrow x_2 x_1 = 1 \Rightarrow x_2 = 1$.

$z_2 + z_3 = 0 \Rightarrow x_2 + x_0 x_1 = 1 \Rightarrow x_0 = 1$.

Άρα, $(x_0, x_1, x_2) = (1, 1, 1)$.

Επομένως, προκύπτουν πάλι δυο πιθανά καθαρά μηνύματα.

Βιβλιογραφία

[CGP] Nicolas Courtois, Louis Goubin, Jacques Patarin:"Sflash^{v3}, a fast asymmetric signature scheme ". New third version of Sflash specification (Sflash^{v3}). Available on **eprint.org/2003/211/**.

[CLO] David Cox, John Little, Donal O'Shea: "Ideals, Varieties and Algorithms," Springer Verlag.

[FJ] Jean-Charles Faugere and A.Joux: "Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases, "Crypto 2003, LNCS 2729, pp.44-60, Springer.

[IT1] Ilia Toli: "Hidden Polynomial Cryptosystems"

[IT2] Ilia Toli: "Cryptanalysis of HFE "

[JGJG] Joachim von zur Gathen and Jürgen Gerhard:"Modern Computer Algebra" Cambridge University Press 1999.

[KS] A.Kipnis and A.Shamir, "Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization." In M.Wiener, editor, Advances in Cryptology - Crypto'99, volume 1666 of LNCS, pages 19-30. SpringerVerlag, 1999.

[MI] T.Matsumoto and H.Imai, "Public Quadratic Polynomial-tuples for efficient signature-verification and message-encryption,"EYROCRYPT'88, Springer Verlag 1998, pp.419-453.

[NK] Neal Koblitz: "Algebraic aspects of cryptography" Springer-Verlag, ACM3, 1998, Chapter 4 "Hidden Monomial Cryptosystems" , pp.80-102.

[P95] J.Patarin, "Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88."In Proc. of th 15th Annual International Cryptology Conference on Advances in Cryptology-CRYPTO'95, pages 248-261, Santa Barbara, California, 1995.

[P96] J.Patarin, "Hidden Field Equations (HFE) and Isomorphisms of Polynomials(IP): The New Families of Asymmetric Algorithms, Eyrocrypt'96, Springer Verlag, pp.33-48.

[SKI] Makoto Sugita, Mitsuru Kawazoe, Hideki Imai: "Relation between XL algorithm and Gröbner Bases Algorithms ".

[SPCK] Adi Shamir, Jacques Patarin, Nicolas Courtois, Alexander Klimov, "Efficient Algorithms for solving Overdefined Systems of Multivariate Polynomial Equations," Eurocrypt'2000, LNCS 1807, Springer, pp.392-407.