Algebraic Methods in Asymmetric Cryptography –

Algorithms, Constructions, and Attacks

Simran Tinani

Supervisor: Prof. Dr. Joachim Rosenthal

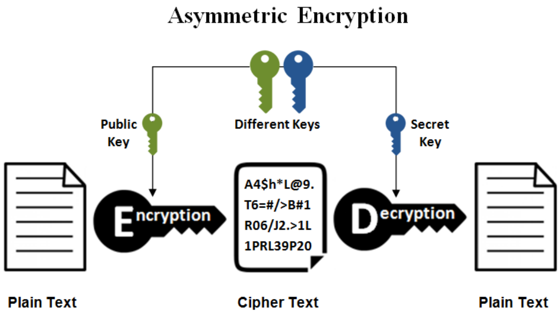
University of Zurich UZH

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

June 22, 2023

Introduction

Public-Key Cryptography



- Exchange of confidential information between people who can communicate only via an insecure channel
- First demonstrated in a paper by (Diffie and Hellman, 1976)
- Alice and Bob can communicate in public, yet establish a shared, secret key which is known only to the both of them.

https://intellipaat.com/blog/the-cia-triad/?US

One-Way Trapdoor Functions

- One-way function: easily and efficiently be calculated in one direction, but is difficult or computationally infeasible to invert.
- Trapdoor information: additional piece of information that allows an efficient inversion
- Used to conceal information in public-key cryptographic systems, to ensure that an adversary cannot invert the function and thereby decrypt the message, whereas the intended receiver (who has the trapdoor information) can easily do so.
- The existence of a true one-way function has not been proven, but many functions have been proposed to be one-way, and are used as such with this assumption.

Starting Point: Public Key Establishment

Protocol 1 (Diffie-Hellman Key Exchange)

- *Alice and Bob agree on a large prime p and an integer g with large prime order in $\mathbb{F}_p^*$.*
- *Alice chooses a secret $a \in \mathbb{Z}$, computes $A = g^a \pmod{p}$. She sends A to Bob. Her secret key is a, her public key is A.*
- *Bob chooses a secret $b \in \mathbb{Z}$ and computes $B = g^b \pmod{p}$. He sends B to Alice. His secret key is b, his public key is B.*
- *Alice computes her shared secret key, $K_A = B^a \pmod{p}$.*
- *Bob computes his shared secret key, $K_B = A^b \pmod{p}$.*

Shared key: $K = K_A = B^a = (g^b)^a = g^{ba} = g^{ab} = (g^a)^b = A^b = K_B \pmod{p}$.

Starting Point: Discrete Logarithm and Diffie-Hellman Problems

Let G be a finite cyclic group with generator g, i.e. $G = \langle g, g^2, g^3, \ldots, g^{n-1}, g^n = 1\rangle$.

Definition (Discrete Logarithm Problem (DLP))

Let h be an element of G. Find an exponent x such that $g^x = h$ in G.

The number x (computed modulo the order of G) is called the discrete logarithm of h to the base g.

Definition (Diffie-Hellman Problem (DHP))

Let $h_1 = g^{n_1}$ and $h_2 = g^{n_2}$ be elements of G. Finding the element $g^{n_1 n_2}$ in G.

The choice of the representation of G is crucial. Most commonly used are $G = \mathbb{F}_p^*$ or $G = E(\mathbb{F}_p)$.

Post-Quantum One-Way Functions

- The discrete logarithm problem and integer factorization are the most widely used for public key cryptography.

- In (Shor, 1994) an efficient (polynomial time) solution to these problems (more generally, *Hidden Subgroup Problem* for finite abelian groups) was shown using a quantum algorithm.

- Most present-day public-key cryptosystems will be broken by a quantum computer with sufficient computational power

- 2016: NIST Post-Quantum Cryptography Standardization program

- Several approaches have been explored: lattice-based cryptography, code-based cryptography, multivariate cryptography, and isogeny-based cryptography.

This Work

- Current cryptographic systems and proposals are altogether based on a relatively small number of one-way functions and mathematical structures (lattices, codes, elliptic curves, finite fields).
- The risk of a novel, efficient attack in the future always looms.
- From a long term perspective, it is interesting and important to sustain research on alternative mathematical structures, algorithms, and one-way functions
- A number of different frameworks have been conceived and investigated using algebraic objects such as semigroups, non-abelian groups, semirings, rings, group algebras and modifications thereof.
- Alternative structures and one-way functions?
- Can we use the rich algebraic structure of these objects to build new cryptosystems and attacks?

Discrete Logarithm Problem in a Semigroup

Discrete Logarithm Problem in a Semigroup

A semigroup is a set of elements with an associative binary operation

$$\star : G \times G \to G$$

If G also has a neutral element 1 such that for every $g \in G$, $g \star 1 = g = 1 \star g$ and inverses g^{-1} such that $g \star g^{-1} = 1 = g^{-1} \star g$, then it is a group.

Algorithm 1: Shanks' Baby-Step Giant-Step Algorithm for Groups

```
▶ Set $n = 1 + \left\lfloor \sqrt{N} \right\rfloor$.
▶ Create two lists, $L_1 = \{1, g, g^2, g^3, \ldots, g^n\}$,
  $L_2 = \{h, hg^{-n}, hg^{-2n}, hg^{-3n}, \ldots, hg^{-n^2}\}$
▶ Find a match between the two lists, say $g^i = hg^{-jn}$.
▶ Return $x = i + jn$. Clearly, $x$ is a solution to $g^x = h$.
```

This solves the DLP $g^x = h$ in $\mathcal{O}(\sqrt{N} \log N)$ steps using storage size $O(\sqrt{N})$.

Definition (Semigroup DLP)

Given $y \in \langle x \rangle := \{x^k \mid k \in \mathbb{N}\}$, find $m \in N$ such that $x^m = y$.

What changes without inverses

- Collision-based algorithms for order and discrete log computations in a group do not adapt directly to a semigroup.
- Principle for collision-based algorithms for an order N group element x: $N = A - B \iff x^A = x^B$ for $A, B \geq 0$.
- For a semigroup element x with cycle start s_x and cycle length $L_x = A - B$ for $A, B \geq 0$, $x^A = x^B \iff A, B \geq s_x$.
- Example $L_x = 15$, $s_x = 10$, $y = x^5$. Then $y \cdot x^6 = x^{11} = x^{26}$ is obtained as a collision. Unlike in the group case, the conclusion $y = x^{26-6} = x^{20}$ is wrong since $x^5 \neq x^{20}$. Problem: x is not invertible.

Contributions: 1

- A novel collision-based deterministic algorithm for the cycle length of a semigroup element x (i.e. the smallest positive integer L_x such that there exists some stage s_x such that $x^{s_x+L_x} = x^{s_x}$). Trick: Generate collisions and pick the ‘‘optimal" indices for which they occur.

Theorem 1

Let S be a semigroup and $x \in S$ a torsion element with order N_x. If an upper bound on N_x is known, the algorithm returns the correct value of the cycle length L_x with

$$\mathcal{O}\left(\sqrt{N_x} \cdot (\log N_x)^2\right)$$

steps. The total space complexity is $\mathcal{O}\left(\sqrt{N_x}\right)$ semigroup elements.

Solving the DLP once the cycle length is known

Algorithm 2: Algorithm for Discrete Logarithm

Input A semigroup S, a torsion element $x \in S$, with cycle length L_x and cycle start s_x, and $y \in S$ with $y = x^m$.

Output The discrete logarithm m of y with base x.

- Compute $t = \left\lceil \frac{s_x}{L_x} \right\rceil$ and define $x' = x^{tL_x+1} \in G_x$.
- Find the minimum number $0 \leq b \leq t$ such that $y' = y \cdot x^{bL_x} \in G_x$ using binary search.
- Use Shanks' Baby-Step Giant-Step algorithm for the group $\langle x' \rangle \subseteq G_x$ to compute $m' \in \{0, 1, \ldots, L_x - 1\}$ such that $(x')^{m'} = y'$.
- Find the maximum number $c \geq 0$ such that $x^{(tL_x+1)m' - cL_x} \in G_x$ using binary search.
- Return $m = m'(tL_x + 1) - (b + c)L_x$.

Contributions: 2

Let S be a semigroup, $x \in S$ a torsion element and $y \in \langle x \rangle$ any element.

Proposition 1

The discrete logarithm $m = \log_x(y)$ can be computed deterministically in

$$\mathcal{O}\left(\sqrt{N_x} \cdot (\log N_x)^2\right)$$

steps, with a required storage of $\mathcal{O}\left(\sqrt{N_x}\right)$ semigroup elements.

Theorem 2 (Pohlig-Hellman in a Semigroup)

Assume the cycle start s_x of x is known and assume the integer factorization of the cycle length L_x is known to be $L_x = \prod_{i=1}^{r} p_i^{e_i}$. Then the discrete logarithm $\log_x y$ can be computed deterministically in $\mathcal{O}\left(\sum_{i=1}^{r} e_i \left(\log L_x + \sqrt{p_i}\right) + (\log N_x)^2\right)$ steps. The space complexity of the algorithm is $\mathcal{O}\left(\sum_{i=1}^{r} e_i \sqrt{p_i}\right)$ semigroup elements.

Nonabelian Group-Based Cryptography

$$a * b \neq b * a$$

Background

Definition (Discrete Logarithm Problem (DLP))

Given $g, h \in G$ with $h \in \langle g \rangle$, find $n \in \mathbb{Z}$ such that $h = g^n$.

Definition (Conjugacy Search Problem (CSP))

Given $g, h \in G$, find an element x of G such that $h = x^{-1}gx$, given that it exists. We adopt the notation $g^x := x^{-1}gx$.

- (Anshel, Anshel, and Goldfeld, 1999) and (Ko et al., 2000), built the first protocols based on the CSP in braid groups.
- Several attacks (Hofheinz and Steinwandt, 2002), (Myasnikov, Shpilrain, and Ushakov, 2006) show that braid groups are not suitable platforms. Proposed alternatives: polycyclic groups, p-groups, Thompson groups, matrix groups.

Key Exchange using Conjugation

Protocol 2 (Ko-Lee protocol)

G is a suitable finitely generated group, with subgroups A and B that commute element-wise, i.e. $ab = ba \; \forall \; a \in A, \; b \in B$. A base element $w \in G$ is chosen. The parameters G, A, B, and w are made public.

- *Alice chooses a secret element $a \in A$, and publishes $w^a = a^{-1}wa$.*
- *Bob chooses a secret element $b \in B$, and publishes $w^b = b^{-1}wb$.*
- *Alice computes $K_A = (w^b)^a$, and Bob computes $K_B = (w^a)^b$.*

Since a and b commute, we have a common shared secret $K_A = K_B = a^{-1}b^{-1}wab$.

Motivation

- For linear platform groups (i.e. those that embed faithfully into a matrix group over a field), several polynomial time attacks exist.
- Often impractical to implement for standard parameter values.
- Protocol-specific, retrieve private shared key without solving CSP
- Computation of an efficient linear representation may pose a roadblock.
- True difficulty of CSP in different platforms not sufficiently investigated.

Definition (A-restricted CSP)

Given a subgroup $A \leq G$ and elements g and h of a group G, find an element $x \in A$ such that $h = x^{-1}gx$, given that it exists.

Polycyclic Groups

- Suggested as platforms for CSP-based key exchange in (Eick and Kahrobaei, 2004).
- Length-based attacks and other heuristic methods for braid groups may be ineffective.

Definition (Polycyclic Group)

A polycyclic group is a group G with a subnormal series $G = G_1 > G_2 > \ldots > G_{n+1} = 1$ with cyclic quotient G_i/G_{i+1}.

For $g_i \in G_i,\ g_{i+1} \in G_{i+1},\ g_i^{-1} g_{i+1} g_i \in G_{i+1}$.

Results: CSP in 2-Polycyclic Groups

In the case $n = 2$, we have the group presentation

$$\langle x_1, x_2 \mid x_1^C = x_2^E, x_1^{-1} x_2 x_1 = x_2^L, x_1 x_2 x_1{}^{-1} = x_2^D \rangle$$

Theorem 3

If $N_2 = \operatorname{ord}(x_2)$ is finite, the CSP has a polynomial time solution.

If $N_2 = \infty$, the CSP reduces to the Diophantine integer equation $f = -dL^a + bL^c + d$. The $\langle x_1 \rangle$-restricted CSP $f = bL^c$ here is easily solved by taking the real number base-L logarithm of $f/b \in \mathbb{Z}$.

Theorem 4

If $N_2 = \operatorname{ord}(x_2)$ is finite, the $\langle x_1 \rangle$-restricted CSP in G_2 reduces to a DLP. Further, the elements can be chosen so that it is exactly equivalent to a DLP in $(\mathbb{Z}/N_2\mathbb{Z})^*$.

Matrix Groups: $\langle Z\rangle$-restricted CSP in $GL_n(\mathbb{F}_q)$

- Let $X \in Mat_n(\mathbb{F}_q)$, $Z \in GL_n(\mathbb{F}_q)$ and $Y = Z^{-r}XZ^r$ be public matrices. The $\langle Z\rangle$-restricted CSP comprises finding $r \in \mathbb{Z}$.

Let J_Z be the Jordan Normal form of Z and θ_Z be the order of Z in the group $\mathrm{GL}_n(\mathbb{F}_q)$.

Theorem 5

If J_Z is diagonal then the retrieval of $r \pmod{\theta_Z}$ reduces to solving at most n^2 DLPs over $\mathbb{F}_{q^k}$.

Theorem 6

Let J_Z be non-diagonal, and composed of s Jordan blocks. Then, the computation of r is polynomial time reducible to a set of s^2 DLPs over $\mathbb{F}_{q^k}$.

Application in Cryptanalysis

Cryptanalysis: Quaternion Decomposition (Sin and Chen, 2019)

$$Q_{2^n} = \langle x, y \mid x^N = 1, y^2 = x^{N/2}, yx = x^{-1}y, N = 2^{n-1} \rangle.$$

The public parameters are $G = Q_{2^n}$ and subgroups $A_1, A_2 \subseteq \langle x \rangle$.

Protocol 3

- - *Alice picks secret elements $a \in G$, $b_1, b_2 \in A_1$ and sends $x_1 = b_1 a b_2$ to Bob.*
  - *Bob picks secret elements $d_i \in A_2$ and sends $x_2 = d_1 x_1 d_2$ to Alice.*
  - *Alice sends $x_3 = b_1^{-1} x_2 b_2^{-1} (= d_1 a d_2)$ to Bob.*
- - *Bob picks a secret element $c \in G$ and sends $y_1 = d_1 c d_2$ to Alice.*
  - *Alice sends $y_2 = b_1 y_1 b_2$ to Bob.*
  - *Bob sends $y_3 = b_1 c b_2 (= d_1^{-1} y_2 d_2^{-1})$ to Alice.*

The shared secret is $b = ac = a(b_1^{-1} y_3 b_2^{-1}) = (d_1^{-1} x_3 d_2^{-1})c$.

The secret key is recovered in polynomial time by collection and solving linear equations $\pmod N$. This cryptanalysis is applicable in any group of the form $\langle x \rangle \rtimes \langle y \rangle, y^2 \in \langle x \rangle$.

Cryptanalysis: Hurwitz Quaternions (Valluri and Narayan, 2016)

$H_p = \{a_1 + a_2 i + a_3 j + a_4 k \mid a_i \in \mathbb{Z}/p\mathbb{Z}\}$.

$i * i = j * j = k * k = -1;\ i * j = k;\ j * i = -k;\ j * k = i; k * j = -i; k * i = j; i * k = -j.$

Protocol 4

- *Alice and Bob agree to choose randomly public elements* $x \in H_p$, $z \in H_p^*$.
- *Alice picks two secret integers* $r, s \in \mathbb{Z}$ *such that* $1 \leq r \leq p-1$ *and* $2 \leq s \leq p-1$ *and computes* $y_A = z^r x^s z^{-r}$, *and sends* $y_A \in H_p$ *to Bob.*
- *Bob picks two secret integers* $u, v \in \mathbb{Z}$ *such that* $1 \leq u \leq p-1$ *and* $2 \leq v \leq p-1$ *and computes* $y_B = z^u x^v z^{-u}$, *and sends* $y_B \in H_p$ *to Alice.*
- *Alice computes* $K_A = z^r {y_B}^s z^{-r}$ *as the shared session key.*
- *Bob computes* $K_B = z^u {y_A}^v z^{-u}$ *as the shared session key.*

There is an explicit isomorphism with efficiently computable inverse $H_p \cong Mat_2(\mathbb{Z}/p\mathbb{Z})$ (Tsopanidis, 2020). The cryptanalysis for matrix groups thus reduces the problem to at most two DLP's.

Cryptanalysis: Subgroup Conjugacy Search (Gu and Zheng, 2014)

- Key exchange with suggested platforms $\mathrm{GL}_n(\mathbb{F}_q)$ and a subgroup of it.
- The Subgroup Conjugacy Search Problem corresponds exactly to the A-restricted Conjugacy Search Problem for A cyclic.
- We therefore have a direct cryptanalysis of this protocol, reducing its security to that of a set of $\mathcal{O}(n^2)$ DLPs over a small extension of $\mathbb{F}_q$.
- The Subgroup Conjugacy Search Problem is not at least as hard as the Conjugacy Search Problem in general, as the authors claim. This is shown in both the matrix and polycyclic case.

Cryptanalysis: Twisted Group-Algebra Key Exchange

Cryptanalysis of a System based on Twisted Dihedral Group Algebras

Let G be a group and $\mathbb{F}$ be a field.

Definition (Group Algebra)

The group algebra $\mathbb{F}[G]$ *is the set of the formal sums* $\sum_{g \in G} a_g g$*, with* $a_g \in \mathbb{F}$*,* $g \in G$*. Addition is defined componentwise:*
$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g := \sum_{g \in G} (a_g + b_g) g$*. Multiplication is defined as*
$\sum_{g \in G} a_g g \cdot \sum_{g \in G} b_g g := \sum_{g \in G} \sum_{h \in G} (a_g b_h) gh = \sum_{k \in G} \sum_{g \in G,\ h \in G : gh = k} a_g b_h k.$

Definition (2-Cocycle)

A map $\alpha : G \times G \to \mathbb{F}^*$ *is called a 2-cocycle of* G *if* $\alpha(1,1) = 1$ *and for all* $g, h, k \in G$ *we have* $\alpha(g, hk)\alpha(h, k) = \alpha(gh, k)\alpha(g, h)$*.*

Definition (Twisted Group Algebra)

Let α be a 2-cocycle of G. The twisted group algebra $\mathbb{F}^{\alpha}G$ is the set of all formal sums $\sum\limits_{g \in G} a_g g$, where $a_g \in \mathbb{F}$, with the following twisted multiplication: $g \cdot h = \alpha(g,h)gh$, for $g, h \in G$. The multiplication rule extends linearly to all elements of the algebra:

$$(\sum_{g \in G} a_g g) \cdot (\sum_{h \in G} b_h h) = \sum_{g \in G} \sum_{h \in G} a_g b_h \alpha(g,h) gh.$$

Addition is given componentwise.

$\mathbb{F}^{\alpha}G$ is associative if and only if α is a 2-cocycle.

Definition (Adjunct)

For an element $a = \sum\limits_{g \in G} a_g g \in \mathbb{F}^{\alpha}G$ we define its adjunct as

$\hat{a} := \sum\limits_{g \in G} a_g \alpha(g, g^{-1}) g^{-1}$.

Public Parameters

- $m \in \mathbb{N}$ and prime $p > 2$, $p \mid 2n$. Set $q := p^m$; $C_n := \langle x \rangle$.
- $D_{2n} = \langle x, y : x^n = y^2 = 1, yxy^{-1} = x^{-1} \rangle$ is the dihedral group of order $2n$.
- 2-cocycle $\alpha = \alpha_\lambda$ for non-square $\lambda \in \mathbb{F}_q^*$ so $\mathbb{F}_q^\alpha D_{2n} \ncong \mathbb{F}_q D_{2n}$.

  $\alpha_\lambda(g, h) = \lambda$ for $g = x^i y,\ h = x^j y$ with $i, j \in \{0, \ldots, n-1\}$ and $\alpha_\lambda(g, h) = 1$ otherwise

- $h = h_1 + h_2$ for random $0 \neq h_1 \in \mathbb{F}_q^\alpha C_n$ and $0 \neq h_2 \in \mathbb{F}_q^\alpha C_n y$.
- $\Gamma_\alpha := \{a = \sum_{i=0}^{n-1} a_i x^i y \in \mathbb{F}_q^\alpha C_n y \mid a_i = a_{n-i}$ for $i = 1, \ldots, n-1\}$.
- The multiplicative ring of $\mathbb{F}_q^\alpha C_n$ is commutative, and $a\hat{b} = b\hat{a}\ \forall a, b \in \Gamma_\alpha$.

The Protocol

Protocol 5 (Cruz and Villanueva-Polanco, 2022)

- *Alice chooses a secret pair* $(s_1, t_1) \in \mathbb{F}_q^{\alpha} C_n \times \Gamma_\alpha$, *sends* $\mathrm{pk}_A = s_1 h t_1$ *to Bob.*
- *Bob chooses a secret pair* $(s_2, t_2) \in \mathbb{F}_q^{\alpha} C_n \times \Gamma_\alpha$, *sends* $\mathrm{pk}_B = s_2 h t_2$ *to Alice.*
- *Alice computes* $K_A = s_1 \, \mathrm{pk}_B \, \hat{t_1}$,
- *Bob computes* $K_B = s_2 \, \mathrm{pk}_A \, \hat{t_2}$
- *The shared key is* $K = K_A = K_B$

Security Assumption

Definition (Dihedral Product Decomposition (DPD) Problem)

Let $(s,t) \in \mathbb{F}_q^{\alpha} C_n \times \Gamma_{\alpha_\lambda}$ *be a secret key. Given a public element* $h = h_1 + h_2 \in \mathbb{F}_q^{\alpha} D_{2n},\ h_1 \in \mathbb{F}_q^{\alpha} C_n,\ h_2 \in \mathbb{F}_q^{\alpha} C_n y$*, and a public key* $\mathrm{pk} = sht$*, the DPD problem requires an adversary to compute* $(\tilde{s}, \tilde{t}) \in \mathbb{F}_q^{\alpha} C_n \times \Gamma_{\alpha}$ *such that* $\mathrm{pk} = \tilde{s}h\tilde{t}$*.*

Definition (DPD Assumption)

The DPD assumption is said to hold for $\mathbb{F}_q^{\alpha} D_{2n}$ *if for all efficient adversaries* $\mathcal{A}$ *the quantity* $DPD_{adv}[\mathcal{A},\ \mathbb{F}_q^{\alpha} D_{2n}] := Prob(\tilde{s}h\tilde{t} = sht)$ *is negligible.*

Circulant Matrices

Definition

A matrix over $\mathbb{F}_q$ *of the form* $\begin{pmatrix} c_0 & c_{n-1} & \dots & c_1 \\ c_1 & c_0 & \dots & c_2 \\ \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & c_{n-2} & \dots & c_0 \end{pmatrix}$ *with* $c_i \in \mathbb{F}_q$*, is called circulant. Given a vector* $\mathbf{c} = (c_0, c_1, \dots, c_{n-1})^T \in \mathbb{F}_{q^n}$*, we use the notation* $M_{\mathbf{c}}$ *to denote the circulant matrix* $M_{\mathbf{c}} := \begin{pmatrix} c_0 & c_{n-1} & \dots & c_1 \\ c_1 & c_0 & \dots & c_2 \\ \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & c_{n-2} & \dots & c_0 \end{pmatrix}$.

Definition

For $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})^T \in \mathbb{F}_q{}^n$, $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})^T \in \mathbb{F}_q{}^n$, $0 \leq \ell \leq n-1$

$$z_\ell(\mathbf{b}, \mathbf{c}) := \sum_{i+j=\ell \pmod n} b_i c_j = \begin{pmatrix} c_\ell, & c_{\ell-1}, & \ldots, & c_{\ell+1} \end{pmatrix} \cdot \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix}$$

.

$$\mathbf{z}_{\mathbf{b},\mathbf{c}} = \mathbf{z}_{\mathbf{b},\mathbf{c}} := (z_0(\mathbf{b}, \mathbf{c}), \ldots, z_\ell(\mathbf{b}, \mathbf{c}), \ldots, z_{n-1}(\mathbf{b}, \mathbf{c}))^T = M_{\mathbf{c}} \cdot \mathbf{b}.$$

$$M_{\mathbf{z}}(\mathbf{b}, \mathbf{c}) := \begin{pmatrix} z_0(\mathbf{b}, \mathbf{c}) & \ldots & z_1(\mathbf{b}, \mathbf{c}) \\ z_1(\mathbf{b}, \mathbf{c}) & \ldots & z_2(\mathbf{b}, \mathbf{c}) \\ \vdots & \ddots & \vdots \\ z_{n-1}(\mathbf{b}, \mathbf{c}) & \ldots & z_0(\mathbf{b}, \mathbf{c}) \end{pmatrix}.$$

Lemma 1

$M_{\mathbf{z}}(\mathbf{b}, \mathbf{c}) = M_{\mathbf{c}} \cdot M_{\mathbf{b}}$.

Cryptanalysis

The adversary is given an equation $sht = \gamma$ over $\mathbb{F}_q^\alpha D_{2n}$, where

$$s = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{F}_q^\alpha C_n, \; t = \sum_{i=0}^{n-1} b_i x^i y \in \Gamma_\alpha \subseteq \mathbb{F}_q{}^{\alpha\lambda} D_{2n}$$

are unknown, and $h = \sum_{i=0}^{n-1} c_i x^i + \sum_{i=0}^{n-1} d_i x^i y$ is known. These reduce to the following two equations

$$\sum_{i,j,k=0}^{n-1} a_i c_j b_k x^{i+j+k} y = \sum_{i=0}^{n-1} w_i x^i y, \tag{1}$$

$$\lambda \sum_{i,j,k=0}^{n-1} a_i d_j b_k x^{i+j+k} = \sum_{i=0}^{n-1} v_i x^i \tag{2}$$

Define vectors $\mathbf{a} = (a_0, \ldots, a_{n-1})^T$, $\mathbf{b} = (b_0, \ldots, b_{n-1})^T$, $\mathbf{c} = (c_0, \ldots, c_{n-1})^T$, $\mathbf{d} = (d_0, \ldots, d_{n-1})^T$, $\mathbf{w} = (w_0, \ldots, w_{n-1})^T$, $\mathbf{v} = (v_0, \ldots, v_{n-1})^T$ in $\mathbb{F}_{q^n}$. Here, $b_i = b_{n-i}$ for each $i = 1, \ldots, n-1$. Vectors $\mathbf{a}$ and $\mathbf{b}$ are unknown to the adversary, while $\mathbf{c}$, $\mathbf{d}$, $\mathbf{v}$, and $\mathbf{w}$ are publicly known.

Cryptanalysis: Reduction to matrix equations

Lemma 2

Equations (1) *and* (2) *are equivalent respectively to the matrix equations* $M_{\mathbf{z}}(\mathbf{b},\mathbf{c}) \cdot \mathbf{a} = \mathbf{w}$ *and* $\lambda M_{\mathbf{z}}(\mathbf{b},\mathbf{d}) \cdot \mathbf{a} = \mathbf{v}$ *over* $\mathbb{F}_q$.

Proposition 2

Suppose $\mathbf{b}$ *is such that the system of simultaneous equations* $\lambda M_{\mathbf{z}}(\mathbf{b},\mathbf{d})\mathbf{a} = \mathbf{v}$ *and* $M_{\mathbf{z}}(\mathbf{b},\mathbf{c})\mathbf{a} = \mathbf{w}$ *has a simultaneous solution* $\mathbf{a} = (a_0, \ldots, a_{n-1})$*. Then,* $s = \sum_{i=0}^{n-1} a_i x^i$, $t = \sum_{i=0}^{n-1} b_i x^i y$ *is a solution of the equation* $sht = \gamma$.

Theorem 7

Assume that $M_{\mathbf{c}}$ *and* $M_{\mathbf{d}}$ *are invertible, and at least one simultaneous solution* $(\mathbf{a},\mathbf{b})$ *exists to the matrix equations* $\lambda M_{\mathbf{z}}(\mathbf{b},\mathbf{d})\mathbf{a} = \mathbf{v}$ *and* $M_{\mathbf{z}}(\mathbf{b},\mathbf{c})\mathbf{a} = \mathbf{w}$*. Then, for any randomly chosen* $\mathbf{b} \in \Gamma_\alpha$ *such that* $M_{\mathbf{b}}$ *is invertible, the equations* $\lambda M_{\mathbf{z}}(\mathbf{b},\mathbf{d})\mathbf{a} = \mathbf{v}$ *and* $M_{\mathbf{z}}(\mathbf{b},\mathbf{c})\mathbf{a} = \mathbf{w}$ *have a simultaneous solution* $\mathbf{a}$ *computable in polynomial time.*

Algorithm for Cryptanalysis

```
Algorithm 3: Cryptanalysis of Key Exchange over $\mathbb{F}_q^{\alpha} D_{2n}$
  Input Parameter $\lambda$ and the cocycle $\alpha = \alpha_\lambda$, public element
  $h = \sum_{i=0}^{n-1} c_i x^i + \sum_{i=0}^{n-1} d_i x^i y$, public key $\gamma = \sum_{i=0}^{n-1} v_i x^i + \sum_{i=0}^{n-1} w_i x^i y$.
  Output A solution $(s, t) \in \mathbb{F}_q^{\alpha} C_n \times \Gamma_\alpha$ satisfying $sht = \gamma$. This tuple is
  a solution to the DPD problem.
  ▶ Define vectors in $\mathbb{F}_{q^n}$: $\mathbf{c} := (c_0, \dots, c_{n-1})$, $\mathbf{d} := (d_0, \dots, d_{n-1})$,
    $\mathbf{v} := (v_0, \dots, v_{n-1})$, $\mathbf{w} := (w_0, \dots, w_{n-1})$.
  ▶ If $M_{\mathbf{c}}$ or $M_{\mathbf{d}}$ is not invertible
        Return Fail
  ▶ Pick a vector $\mathbf{b} = (b_0, \dots, b_{n-1}) \leftarrow \Gamma_\alpha$ at random.
  ▶ If $M_{\mathbf{b}}$ is not invertible, repeat step above. If it is invertible, go to next step.
  ▶ Compute $\mathbf{a} = \lambda^{-1} M_{\mathbf{z}}(\mathbf{b}, \mathbf{c})^{-1} \mathbf{w}$ $(= M_{\mathbf{b}}^{-1} M_{\mathbf{d}}^{-1} \mathbf{v})$.
  ▶ With $\mathbf{a} = (a_0, \dots, a_{n-1})$, set $s = \sum_{i=0}^{n-1} a_i x^i$ and $t = \sum_{i=0}^{n-1} b_i x^i y$.
  ▶ Return $(s, t)$.
```

Success Rate

- Probability(algorithm fails) = Probability(one of $M_{\mathbf{c}}$ and $M_{\mathbf{d}}$ is not invertible)$= 1 - (1 - \frac{1}{q})^2$.
- This quantity shrinks with increasing values of q and n.
- In (Cruz and Villanueva-Polanco, 2022) the smallest values of these parameters are $q = n = 19$, for which this probability is ≈ 0.1.
- Thus, Algorithm 3 succeeds in cryptanalyzing the system with a probability of at least 90 percent.

An immediate corollary is that the two-sided multiplication action

$$(\mathbb{F}_q^\alpha C_n \times \Gamma_\alpha) \times \mathbb{F}_q^\alpha D_{2n} \to \mathbb{F}_q^\alpha D_{2n}$$

$$(s, t) \cdot h \mapsto sht, \; s \in \mathbb{F}_q^\alpha C_n, \; t \in \Gamma_\alpha$$

is not injective. In fact, for most values of t and $\gamma \in \mathbb{F}_q^\alpha D_{2n}$, there is a unique pre-image $s \in \mathbb{F}_q^\alpha C_n$ such that $sht = \gamma$.

Conclusions

Conclusions

- Algebraic structures such as nonabelian groups and (twisted) group algebras have multiple options for promising one-way functions.
- However, the construction of public key systems often requires one to introduce a great deal of mathematical structure which also brings in more attack surface.
- E.g. restriction of conjugating elements to certain sets, choice of the 2-cocycle. Resulting cryptosystems rely on more complicated problems that may not be one-way.
- Workarounds to extend existing attack methods exist for certain modified problems, such as semigroup DLPs.
- The generalized Zémor and Tillich-Zémor hash functions have several novel theoretical attack methods, but in practice they show resilience to these and remain promising with certain generator sets.
- The right combination of an efficient platform, a reliable one-way function, and a method to exploit these to construct a cryptosystem, is rare!

Thank You!

References I

- Anshel, Iris, Michael Anshel, and Dorian Goldfeld (1999). "An algebraic method for public-key cryptography". In: *Math. Res. Lett.* 6.3-4, pp. 287–291.
- Cruz, Javier de la and Ricardo Villanueva-Polanco (2022). "Public key cryptography based on twisted dihedral group algebras". In: *Advances in Mathematics of Communications* 16.2, pp. 195–215.
- Diffie, Whitfield and Martin Hellman (1976). "New Directions in Cryptography". In: *ieeeit* IT-22.6, pp. 644–654.
- Eick, Bettina and Delaram Kahrobaei (2004). "Polycyclic groups: a new platform for cryptology?" In: *arXiv preprint. arXiv:0411077*.
- Gu, Lize and Shihui Zheng (2014). "Conjugacy Systems Based on Nonabelian Factorization Problems and Their Applications in Cryptography". In: *J. Appl. Math.* 2014, 630607:1–630607:10.
- Hofheinz, Dennis and Rainer Steinwandt (2002). "A Practical Attack on Some Braid Group Based Cryptographic Primitives". In: *Public Key Cryptography — PKC 2003*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 187–198. ISBN: 978-3-540-36288-3.

References II

- Ko, Ki Hyoung et al. (2000). "New public-key cryptosystem using braid groups". In: *Annual International Cryptology Conference*. Springer, pp. 166–183.
- Myasnikov, Alexei, Vladimir Shpilrain, and Alexander Ushakov (2006). "Random Subgroups of Braid Groups: An Approach to Cryptanalysis of a Braid Group Based Cryptographic Protocol". In: *Public Key Cryptography - PKC 2006*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 302–314. ISBN: 978-3-540-33852-9.
- Shor, Peter W. (1994). "Algorithms for quantum computation: discrete logarithms and factoring". In: *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994)*. Los Alamitos, CA: IEEE Comput. Soc. Press, pp. 124–134.
- Sin, Chang Seng and Huey Voon Chen (2019). "Group-Based Key Exchange Protocol Based on Complete Decomposition Search Problem". In: *Information Security Practice and Experience*. Springer International Publishing. ISBN: 978-3-030-34339-2.
- Tsopanidis, Nikolaos (2020). "The Hurwitz and Lipschitz Integers and Some Applications". PhD thesis. Universidade do Porto.

References III

📄 Valluri, Maheswara Rao and Shailendra Vikash Narayan (2016). "Quaternion public key cryptosystems". In: *2016 World Congress on Industrial Control Systems Security (WCICSS)*, pp. 1–4. DOI: 10.1109/WCICSS.2016.7882612.