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

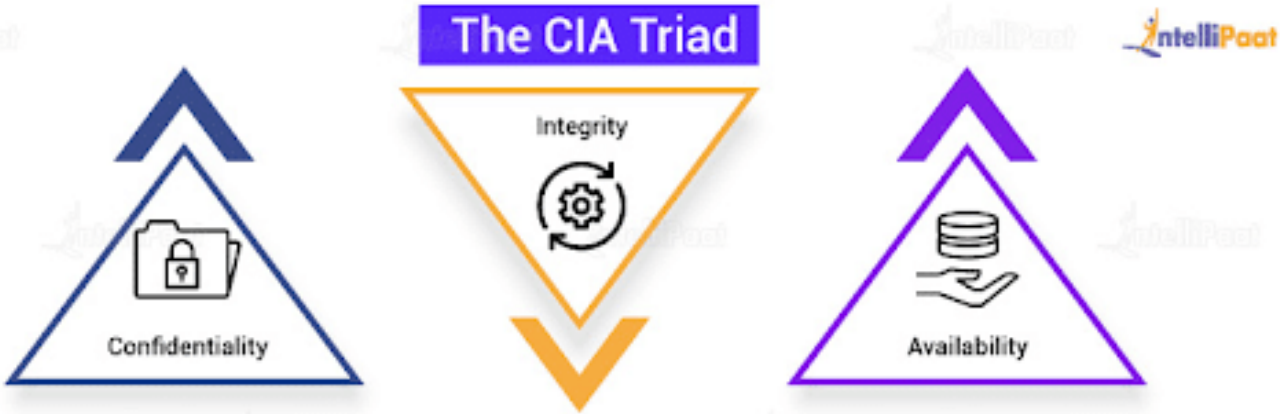
June 9, 2023

Introduction

Introduction

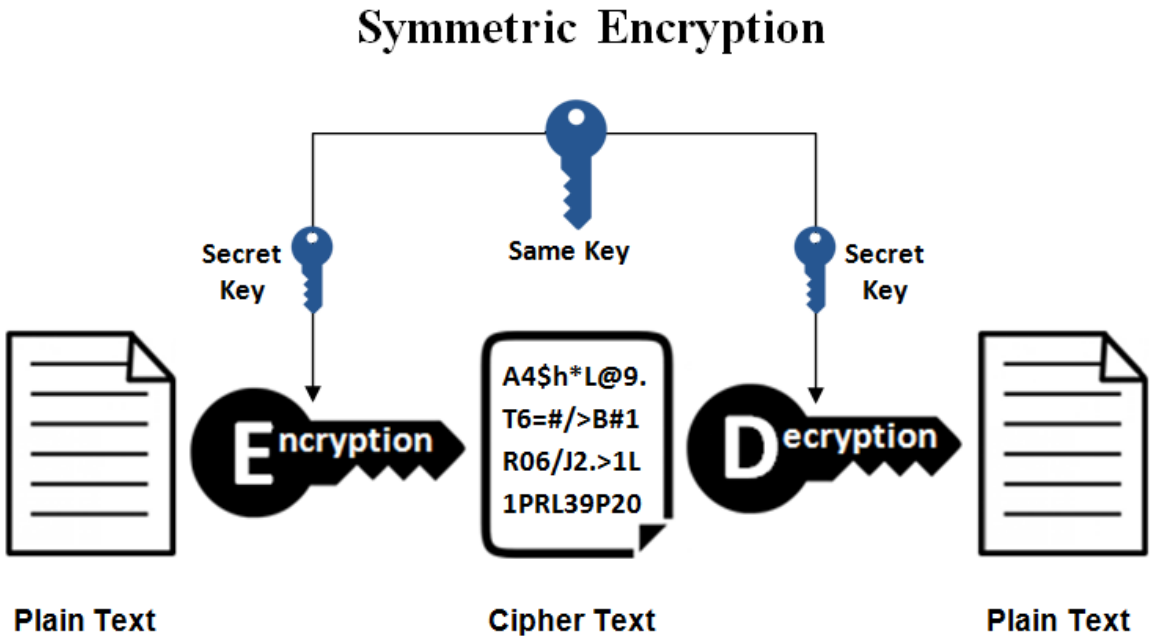
Cryptography is the science and art of securing communication from unauthorized access. CIA triad model of information security:

- Confidentiality: Information is kept secret from unauthorized parties.
- Integrity: Messages are not modified in transit.
- Authentication: the verification of a user or system's identity



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

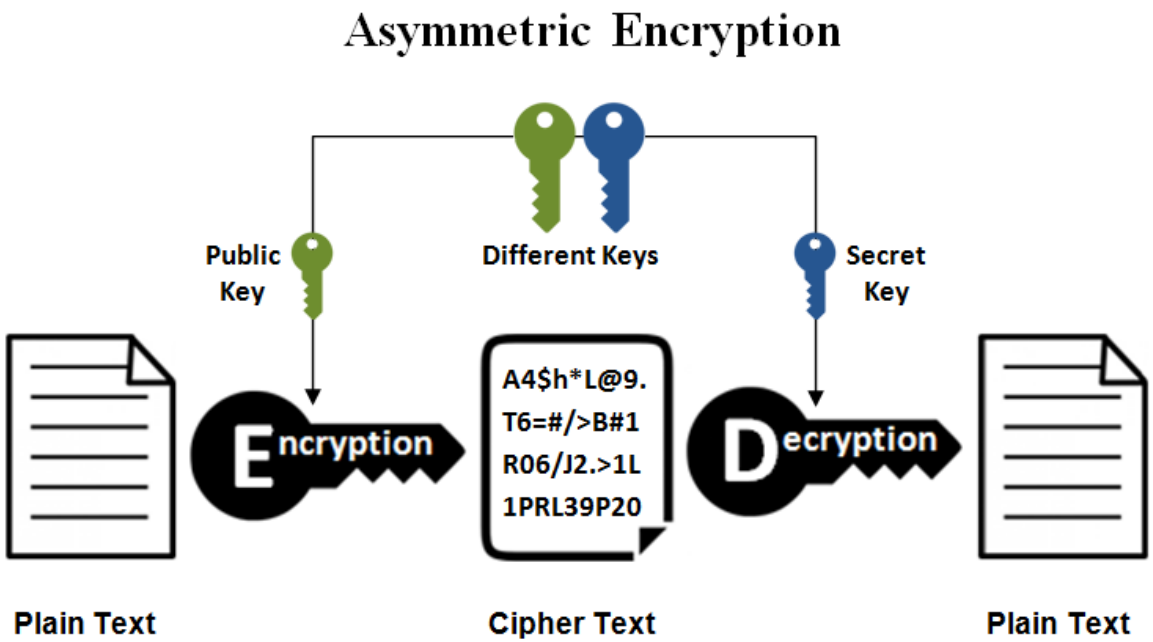
Private-Key Cryptography



- Some popular private-key ciphers: Data Encryption Standard (DES), Advanced Encryption Standard (AES), Triple DES, Blowfish, and RC4.
- Repeated application of mixing operations combined in a way that they are hard to reverse without the private key.

https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

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.

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

Discrete Logarithm and Diffie-Hellman Problems

Definition (Discrete Logarithm Problem (DLP))

Let G be a finite cyclic group with generator g and 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 and is denoted by $\log_g(h)$.

Definition (Diffie-Hellman Problem (DHP))

Let G be a finite cyclic group with generator g let $h_1 = g^{n_1}$ and $h_2 = g^{n_2}$ be elements of G, provided so that the values of the exponents n_1 and n_2 are concealed. The Diffie-Hellman problem requires 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 Thesis

- 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?

DLP in a Semigroup

DLP in a Semigroup

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

- 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 algorithm solves the discrete logarithm problem $g^x = h$ in $\mathcal{O}(\sqrt{N} \log N)$ steps using storage size of $O(\sqrt{N})$.

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

Definition (Semigroup DLP)

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

The Discrete Logarithm Problem in a Semigroup

Definition (Torsion Element)

Let S be a semigroup. An element $x \in S$ is called a torsion element if the sub-semigroup $\langle x \rangle := \{x^k \mid k \in \mathbb{N}\}$ generated by x, is finite.

Definition (Cycle Start)

Smallest positive integer s_x s.t. $x^{s_x} = x^b$ for some $b \in \mathbb{N}$, $b > s_x$.

Definition (Cycle Length)

The smallest positive integer L_x such that $x^{s_x + L_x} = x^{s_x}$.

Definition (Element order)

Cardinality of the sub-semigroup $\langle x \rangle$. Note that $N_x = s_x + L_x - 1$.

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.

Discrete Logarithm Problem in a Semigroup

Lemma 1 (Banin and Tsaban, 2016)

The set $G_x = \{x^{s_x+k} \mid k \geq 0\}$ *of* $x \in S$ *forms a finite cyclic group of order* L_x *with identity* x^{tL_x}*, where* t *is the minimum positive integer such that* $x^{tL_x} \in G_x$.

- The authors of (Banin and Tsaban, 2016) assume the availability of a 'Discrete Logarithm Oracle' for the group G_x, which returns values $\log_x h$ for $h \in G_x$.
- They state that these values need not be smaller than the group order but are polynomial in the size of G_x and the element x.
- The representation of the identity in G_x is unknown, and a method to compute inverses is not available.
- A different probabalistic approach is also described in (Monico, 2002).

Algorithm 2: Deterministic Algorithm for Cycle Length

Input A semigroup S and a torsion element $x \in S$.
Output Cycle length L_x of x

- Initialize $N \leftarrow 1$.
- Set $q \leftarrow \lceil \sqrt{N} \rceil$.
- Compute, one by one, $x^N, x^{N+1}, \ldots, x^{N+q}$ and check for the equality $x^N = x^{N+j}$ at each step $j \geq 1$. Store these values in a table as pairs $(N+j, x^{N+j})$, $0 \leq j < q$. If $x^N = x^{N+j}$ for any $j < q$, then set $L_x \leftarrow j$ and end the process. If not, proceed to the next step.
- For $0 \leq i \leq q$, compute, one by one, the values $x^{N+q}, x^{N+2q}, \ldots, x^{N+iq}$ and at each step i, look for a match in the table of values calculated in Step (3).
- Suppose that a match $x^{N+iq} = x^{N+j}$ is found, and i is the smallest integer such that this happens. Set $L_x \leftarrow iq - j$ and end the process.
- If no match is found in steps 3 or 5, set $N \leftarrow 2 \cdot N$ and go back to Step (2).

Once cycle length is known, cycle start can be found in polynomial time using binary search.

Correctness and Complexity

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, Algorithm 2 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 3: 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 $m = m'(tL_x + 1) - (b + c)L_x$.

Results

Proposition 1

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

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

Background: Nonabelian Group-based Cryptography

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 this Section

- For linear platform groups (i.e. those that embed faithfully into a matrix group over a field), several polynomial time attacks exist (Kreuzer, Myasnikov, and Ushakov, 2014), (Myasnikov and Roman'kov, 2015), (Tsaban, 2015), (Ben-Zvi, Kalka, and Tsaban, 2018).
- Often impractical to implement for standard parameter values.
- Computation of an efficient linear representation may pose a serious roadblock for an adversary.
- Protocol-specific and focus on retrieving the private shared key without solving the CSP
- So far, the true difficulty of the CSP in different platforms has not been sufficiently investigated.

Motivation for this Section

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.

We are specifically interested in the case where A is cyclic.

- In Ko-Lee, commutativity of conjugators is needed. Interesting abelian subgroups of several proposed platforms are cyclic.
- In Anshel et al., 2007, the amount of information the adversary has is "proportional" to the number of generators of A.
- Case A cyclic is most basic, reductions to it may be possible

Polycyclic Groups

- Suggested as platforms for CSP 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}.

Polycyclic Groups with Two Generators

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

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

Lemma 2

The conjugated word $(x_1^c x_2^d)^{-1}(x_1^a x_2^b)(x_1^c x_2^d) = x_1^g x_2^h$ *with* $g = a$,

$$h = \begin{cases} -dL^a + bL^c + d; \ \textit{if } c, \ a \geq 0 \\ -dL^a + bD^{-c} + d; \ \textit{if } c < 0, \ a \geq 0 \\ -dD^{-a} + bL^c + d; \ \textit{if } c \geq 0, \ a < 0 \\ -dD^{-a} + bD^{-c} + d; \ \textit{if } c, \ a < 0 \end{cases}$$

CSP in 2-Polycyclic Groups

Theorem 3

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

Theorem 4

If $N_2 = \mathrm{ord}(x_2)$ 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 $(\mathbb{Z}/N_2\mathbb{Z})^*$.

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 $f/b \in \mathbb{Z}$.

$\langle x_1 \rangle$-restricted CSP in a Finite 3-Polycyclic group

$$G = \langle s, t_1, t_2 \mid t_1^{\theta_1} = 1 = t_2^{\theta_2}, t_2^{t_1} = t_2^{L}, {t_1}^{s} = t_1^{a_1^{(1)}} t_2^{a_2^{(1)}}, {t_2}^{s} = t_1^{a_1^{(2)}} t_2^{a_2^{(2)}} \rangle$$

$\langle t_1, t_2 \rangle$ is 2-polycyclic and $s^{-i}(t_1^A t_2^B)s^i = t_1^{A_i} t_2^{B_i}$ where for $i \geq 0$,

$$\begin{aligned} A_{i+1} &= a_1^{(1)} A_i + a_1^{(2)} B_i \pmod{\theta_1}, \\ B_{i+1} &= a_2^{(1)} L^{A_i a_1^{(2)}} \frac{L^{A_i a_1^{(1)}} - 1}{L^{a_1^{(1)}} - 1} + a_2^{(2)} \frac{L^{B_i a_1^{(2)}} - 1}{L^{a_1^{(2)}} - 1} \pmod{\theta_2}. \end{aligned}$$

Solving the $\langle s \rangle$-restricted CSP $\equiv$ finding N from (A_N, B_N). For $a_1^{(2)} = 0 = a_2^{(1)}$, this is a DLP in $(\mathbb{Z}/\theta_1\mathbb{Z})^*$.

CSP in a Finite $(n+1)$-PC Group; n Generators Commute

$$G = \langle s, t_1, \ldots, t_n \mid t_i^{\theta_i} = 1, t_i t_j = t_j t_i,\ {t_i}^s = t_1^{a_i^{(1)}} \ldots t_n^{a_i^{(n)}}, 1 \leq i, j \leq n \rangle$$

Representing elements of T as column vectors $(r_1 \ldots, r_n)$, we can describe the conjugation action of s on T by the map

$$\mathbb{Z}_{o_1} \times \mathbb{Z}_{o_2} \times \ldots \times \mathbb{Z}_{o_n} \to \mathbb{Z}_{o_1} \times \mathbb{Z}_{o_2} \times \ldots \times \mathbb{Z}_{o_n}$$

$$(r_1, \ldots, r_n) \to \begin{bmatrix} a_1^{(1)} & \ldots & a_1^{(n)} \\ a_2^{(1)} & \ldots & a_2^{(n)} \\ \vdots & \ldots & \vdots \\ a_n^{(1)} & \ldots & a_n^{(n)} \end{bmatrix} \cdot \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{bmatrix}$$

The $\langle s \rangle$-restricted CSP constitutes recovering N from the N^{th} power of the above matrix.

Matrix Groups

- The DLP in $GL_n(\mathbb{F}_q)$ was studied in (Menezes and Wu, 1997) and (Freeman, 2004) and shown to be no more difficult than the DLP over a small extension of $\mathbb{F}_q$.
- Most known nonabelian platform groups are linear. If a faithful representation and its inverse can efficiently be computed, the security of the system depends on that of the matrix CSP rather than that in the original platform.
- 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 $r \in \mathbb{Z}$.

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

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 $\mathbb{F}_{q^k}$.

Applications in Cryptanalysis

- Protocol in (Sin and Chen, 2019) based on a "decomposition problem" in (polycyclic) generalized quaternion groups Q_{2^n} is broken by collection and solving linear equations $(\mathrm{mod}\ N)$.

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

- Protocol in (Valluri and Narayan, 2016) is based on the a $\langle Z \rangle$-restricted CSP over quaternions mod p, H_p.

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

  There is an explicit isomorphism with efficiently computable inverse $H_p \cong Mat_2(\mathbb{Z}/p\mathbb{Z})$ (Tsopanidis, 2020).

- "Subgroup CSP" in (Gu and Zheng, 2014) corresponds exactly to the A-restricted CSP for A cyclic. Suggested platforms are $\mathrm{GL}_n(\mathbb{F}_q)$, a subgroup of it, and a braid group.

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 $\sum_{g\in G} a_g g$, 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 $a = \sum_{g\in G} a_g g \in \mathbb{F}^{\alpha}G$ we define its adjunct as $\hat{a} := \sum_{g\in G} a_g \alpha(g, g^{-1})g^{-1}$.

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

Protocol 3 (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 $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})^T \in {\mathbb{F}_q}^n$, $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})^T \in {\mathbb{F}_q}^n$, $0 \leq \ell \leq n-1$

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

.

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

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

Lemma 3

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

Cryptanalysis

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

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

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 4

Equation (1) *is equivalent to the matrix equation* $M_{\mathbf{z}}(\mathbf{b}, \mathbf{c}) \cdot \mathbf{a} = \mathbf{w}$ *over* $\mathbb{F}_q$.
Equation (2) *is equivalent to the matrix equation* $\lambda M_{\mathbf{z}}(\mathbf{b}, \mathbf{d}) \cdot \mathbf{a} = \mathbf{v}$ *over* $\mathbb{F}_q$.

Proposition 2

Suppose $\mathbf{b} = (b_0, \ldots, b_{n-1})$ *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* $sht = \gamma$.

Proposition 3

Let the vectors $\mathbf{c}$ *and* $\mathbf{d}$ *be such that* $M_{\mathbf{c}}$ *and* $M_{\mathbf{d}}$ *are invertible. Assume that 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 4: Cryptanalysis of Key Exchange over $\mathbb{F}_q^\alpha D_{2n}$

Input Parameter λ 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 $\mathbb{F}_{q^n}$: $\mathbf{c} := (c_0, \ldots, c_{n-1})$, $\mathbf{d} := (d_0, \ldots, d_{n-1})$, $\mathbf{v} := (v_0, \ldots, v_{n-1})$, $\mathbf{w} := (w_0, \ldots, w_{n-1})$.
- If $M_\mathbf{c}$ or $M_\mathbf{d}$ is not invertible
  Return Fail
- Pick a vector $\mathbf{b} = (b_0, \ldots, b_{n-1}) \leftarrow \Gamma_\alpha$ 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 $\mathbf{a} = (a_0, \ldots, a_{n-1})$, 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 4 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 $sht = \gamma$.

Algebraic Hash Functions

Methods for Collisions in some Algebraic Hash Functions

$\mathcal{A}$: alphabet; $\mathcal{A}^*$: all finite-length words in $\mathcal{A}$; $\mathcal{A}^n$: words up to length n in $\mathcal{A}$.

Definition

A length n hash function, or compression function, is a map $\mathcal{A}^* \to \mathcal{A}^n$. A hash function $h : \mathcal{A}^* \to \mathcal{A}^n$ is called a cryptographic hash function if it satisfies the following properties:

- *Collision-resistance: it is computationally infeasible to find a pair x, x' of distinct messages such that $h(x) = h(x')$.*
- *Second pre-image resistance: given a message x, it is computationally infeasible to find another message $x' \neq x$ such that $h(x) = h(x')$.*
- *One-wayness: given a hash value $y \in \mathcal{A}^n$ it is computationally infeasible to find a pre-image $x \in \mathcal{A}$ such that $h(x) = y$.*

Used in password storage, for verifying the integrity of files, in digital signatures, and in the construction of MACs (Message Authentication Code).

Cayley Hash Functions

G: finite group with generator set $S = \{s_1, \ldots, s_k\}$; $|\mathcal{A}| = |S|$

Definition (Cayley hash function)

Given an injective map $\pi : \mathcal{A} \to S$, one may define the hash value of the message $x_1 x_2 \ldots x_k$ to be the group element $\pi(x_1)\pi(x_2)\ldots\pi(x_k)$.

Security $\equiv$ some concise mathematical problem; inherently parallelizable.

Definition (Factorization problem)

Let $L > 0$ be a fixed constant. Given $g \in G$, return $m_1, \ldots, m_L$ and $\ell \leq L$, with $m_i \in \{1, \ldots, k\}$ such that $\prod_{i=1}^{\ell} s_{m_i} = g$.

Babai's Conjecture: "short" factorisations always exist for finite non-abelian groups, for all generating sets. Known to be true for some groups, e.g. $SL_2(2, \mathbb{F}_p), SL_2(2, \mathbb{F}_{2^k})$. However, existing proofs are non-constructive.

Famous Cayley Hash Functions

Definition (Zémor Hash Function, (Zémor, 1991))

For generators $A_0 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $A_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ *of* $SL_2(\mathbb{F}_p)$, *a message* $m = m_1 m_2 \dots m_k \in \{0,1\}^*$ *define* $H(m_1 \dots m_k) = A_{m_1} \dots A_{m_k}$.

- Euclidean algorithm attack: Specific to generators A_0 and A_1. Claim in (Petit and Quisquater, 2011): system is secure with generators A_0^2, A_1^2.

Definition (Tillich-Zémor Hash function)

Let $n > 0$ *and* $q(x)$ *be an irreducible polynomial over* $\mathbb{F}_2$. *Write* $K = \mathbb{F}_2[x]/q(x)$. *Consider* $A_0 = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}$ *and* $A_1 = \begin{pmatrix} x & x+1 \\ 1 & 1 \end{pmatrix}$, *which are generators of* $SL_2(K)$. *For a message* $m = m_1 m_2 \dots m_k \in \{0,1\}^*$ *define* $H(m_1 \dots m_k) = A_{m_1} \dots A_{m_k} \pmod{q(x)}$.

- Collisions found in (Grassl et al., 2011) using the structure in hash values of palindromic messages. Security is an open problem for general parameters.

Generalizations of Algebraic Hash Functions

Definition (Generalized Zémor hash functions)

Consider the generators $A_0 = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ *and* $A_1 = \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}$ *in the group* $SL_2(\mathbb{F}_{p^k})$. *For a message* $m = m_1 m_2 \dots m_k \in \{0,1\}^*$ *define the hash value* $H(m_1 \dots m_k) = A_{m_1} \dots A_{m_k}$.

A_0, A_1 have order p, so one trivially has collisions of length p with the empty word. Want to find collisions with length at most, say $\mathcal{O}(\sqrt{p})$.

Definition (Generalized Tillich-Zémor hash functions)

Consider the generators$A_0 = \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}$ *and* $A_1 = \begin{pmatrix} \beta & 1 \\ 1 & 0 \end{pmatrix}$ *where* $\alpha, \beta \in \mathbb{F}_{p^k}$, *in the group* $SL_2(\mathbb{F}_{p^k})$. *For a message* $m = m_1 m_2 \dots m_k \in \{0,1\}^*$ *define the hash value* $H(m_1 \dots m_k) = A_{m_1} \dots A_{m_k}$.

Collisions from Triangular and Diagonal Matrices

- (Petit et al., 2009): if one can produce "sufficiently many" messages whose images in the matrix groups are upper/lower triangular, then one can find collisions of the generalized Zémor and Tillich-Zémor hash functions.
- The authors use random probabilistic search to find pre-images of upper/lower triangular matrices
- In contrast to some of the previous approaches, we attempt to construct collisions in a structured and deterministic manner

Problem 1 (Triangularising Zémor Hashes)

Given a matrix $C \in SL_2(\mathbb{F}_{p^k})$ formed as product of A_0 and A_1, find the conditions under which there exist integers m and n (of size significantly smaller than p^k) such that $CA_0^m A_1^n$ is upper/lower triangular, or even diagonal. Compute m and n if they exist.

Extending Messages for Triangular Zémor Hashes

Lemma 5

Let $k \geq 1$ and $\alpha \cdot \beta \in \mathbb{F}_p$. Let z be any message and $C := H(z)$ be its corresponding hash value. Assume that $a := C[0,0] \neq 0$. Then, there exist integers $m, n \in \{0, 1, \ldots, p-1\}$ such that $C \cdot A_0^m \cdot A_1^n$ is upper triangular.

Corollary 1

Let δ be a bound. Let $C := h(z) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $m \in \{0, 1, \ldots, p-1\}$ be such that both m and $n = -c/(\beta(mc\alpha + d)) \in \mathbb{F}_p$ are smaller than δ. Then $CA_0^m A_1^n$ has length at most 2δ more than C and is upper triangular.

For larger values of p, experiments indicate a very low probability of finding such values. For $30 - 40$ digit primes, brute force could no longer find any such examples.

Condition for Triangularisability

Proposition 4

If $\alpha \cdot \beta \notin \mathbb{F}_p$, then $C \cdot A_0^m \cdot A_1^n$ is upper triangular for $m, n \in \mathbb{F}_p$ if and only if for

$$\gamma = \left(\frac{d((d\beta)^{p-1} - c^{p-1})}{\alpha c^p (1 - (\alpha\beta)^{p-1})} \right), \tag{3}$$

we have $\gamma^p = \gamma$, and $m = \gamma$; $n = \dfrac{-c}{\beta(mc\alpha + d)}$.

Lemma 6 (Case $k = 2$)

Let $k = 2$ and $\alpha \cdot \beta \notin \mathbb{F}_p$. As before, let $C = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{F}_{p^2})$ be an arbitrary product of finitely many copies of A_0 and A_1. Then with γ defined as in (3), $\gamma^p = \gamma$ always holds.

Condition for Triangularisability

Can we generalize this method to make $C \cdot A_0^{m_1} A_1^{n_1} \dots A_0^{m_r} A_1^{n_r}$ upper/lower triangular and thereby extend the result to all $SL_2(\mathbb{F}_{p^k})$? For an extension where multiplication by a product $A_0^m A_1^n$ is allowed twice:

Lemma 7

For $C := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, *there exits integers* m_1, m_2, n_1, n_2 *such that* $CA^{m_1}B^{n_1}A^{m_2}B^{n_2}$ *is upper triangular if and only if the equation*

$$q_3 x^2 y + q_2 xy + q_1 y + q_0 = 0 \tag{4}$$

has a solution $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$, *where* q_0, q_1, q_2, q_3 *are given by*

$$\begin{aligned} q_3 &= c^{p^2} \alpha\beta((\alpha\beta)^{p^2-1} - 1), \\ q_2 &= c^{p^2} \gamma\alpha\beta(\gamma^{p-1} - (\alpha\beta)^{p^2-1}) + d\beta((d\beta)^{p^2-1} - 1), \\ q_1 &= d\beta\gamma(c^{p^2}\gamma^{p-1} - (d\beta)^{p^2-1}), \\ q_0 &= c^{p^2}\gamma(\gamma^{p-1} - 1). \end{aligned} \tag{5}$$

Example: Condition for Triangularisability

Example 1

For simplicity, consider the field $\mathbb{F}_{2^5}$ with generator z_5 and $\alpha = z_5^3 + 1$, $\beta = z_5^3 + z_5^2 + 1$. Consider the hash matrix

$$C = \begin{pmatrix} z_5^4 + z_5^3 + z_5^2 + z_5 & z_5^4 + z_5^3 + z_5^2 + z_5 \\ z_5^3 & z_5^4 + z_5^3 + z_5^2 \end{pmatrix}.$$

Here, we have $\gamma = z_5^4 + z_5 + 1$ and the polynomial in Equation (4) is $(z_5^2 + z_5)x^2y + (z_5^3 + z_5^2 + 1)xy + (z_5^3)y + (z_5^4 + z_5^2 + z_5)$. The $\langle (z_5^2 + z_5)x^2y + (z_5^3 + z_5^2 + 1)xy + z_5^3 y + (z_5^4 + z_5^2 + z_5), x^p - x, y^p - y \rangle$ is trivial, so its Gröbner basis is $\{1\}$. So, no solution exists.

Generalized Tillich-Zémor Hash Functions

Consider the generalized Tillich-Zémor hash function ϕ with the generators $A_0 = \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}$ and $A_1 = \begin{pmatrix} \beta & 1 \\ 1 & 0 \end{pmatrix}$ where $\alpha, \beta \in \mathbb{F}_{p^k}$.

Consider the matrix $Y = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}$ and first compute its powers.

$$Y^n = \begin{pmatrix} f_n(x) & f_{n-1}(x) \\ f_{n-1}(x) & f_{n-2}(x) \end{pmatrix}, \ n \geq 2 \tag{6}$$

where $f_0(x) = 0$, $f_1(x) = 1$, and

$$f_n(x) = x f_{n-1}(x) + f_{n-2}(x) \tag{7}$$

It is clear that the recurrence relation (7) fully describes the powers of the matrix Y.

Computing $f_n(x)$ for characteristic $p \neq 2$

We may solve (7) by finding roots of the auxiliary polynomial $t^2 - xt - 1 = 0$.
It can be shown that for any $n \geq 1$, we have

$$f_n(x) = \frac{1}{2^{n+1}} \left[\sum_{0 \leq i \leq n,\ n-i \text{ is even}} \sum_{j=0}^{(n-i)/2} \binom{n+1}{i} \binom{(n-i)/2}{j} 2^{n-2j} x^{i+2j} \right] \in \mathbb{F}_p[x]$$

Powers of A_0 and A_1 may therefore be computed in constant time.

Condition for Collisions

- $\mathbb{F}_{p^k}$ is viewed through the isomorphism $\mathbb{F}_{p^k} \cong \mathbb{F}_p[x]/\langle q(x)\rangle$ where $q(x)$ is an irreducible polynomial of degree k over $\mathbb{F}_p$.
- Thus, $\gamma \in \mathbb{F}_{p^k}$ is a polynomial of degree smaller than k, say $\gamma = g_\gamma(x)$.
- $f_n(\gamma)$ can be calculated as a polynomial modulo $q(x)$ by simply composing f_n and g, i.e. $f_n(\gamma) = f_n(g_\gamma(x)) \pmod{q(x)}$.

Lemma 8

Suppose that the adversary can compute integers m and n such that $f_{n-1}(g_\alpha(x)) = f_{m-1}(g_\beta(x)) \pmod{q(x)}$ and $f_{n-2}(g_\alpha(x)) = f_{m-2}(g_\beta(x)) \pmod{q(x)}$. Then, the adversary can compute a collision of size $\mathcal{O}(\max(m,n))$ for the Generalized Tillich-Zémor hash function ϕ.

- Even for the simplest equation $f_n(x) = 0 \pmod{q(x)}$, finding a solution for n is not straightforward, since n occurs both as a polynomial term and in the exponent of 2.

Condition for Collisions

Lemma 9

Let $\mathbb{F}_p[x]/\langle q(x)\rangle$ be a finite field. If an adversary can find integers m and n such that the following relations hold

$$\begin{aligned}
f_m(f_n(x)) + f_{m-1}(f_{n-1}(x)) &= 1 \pmod{q(x)} \\
f_m(f_{n-1}(x)) + f_{m-1}(f_{n-2}(x)) &= 0 \pmod{q(x)} \\
f_{m-1}(f_n(x)) + f_{m-2}(f_{n-1}(x)) &= 0 \pmod{q(x)} \\
f_{m-1}(f_{n-1}(x)) + f_{m-2}(f_{n-2}(x)) &= 1 \pmod{q(x)},
\end{aligned}$$

then $H(0^m 1^n) = H()$ gives a collision with the hash $H()$ of the empty word.

Malicious Design for Finite Field

- If $q(x)$ is chosen such that Y has a known and "small enough" multiplicative order n_y, then also A_0 and B_0 have small multiplicative orders which divide n_y, and can therefore be calculated easily.

Proposition 5

- *If one can find N such that $\gcd(f_N(x) - 1, f_{N-1}(x))$ has an irreducible divisor $q(x)$ of degree d, one can find a collision of size $\mathcal{O}(N)$ for the hash function $\phi(x)$ over the finite field $\mathbb{F}_p[x]/\langle q(x)\rangle$.*
- *Given a fixed finite field $\mathbb{F}_p[x]/\langle q(x)\rangle$, if one can find an integer N such that $q(x)$ divides $\gcd(f_N(x) - 1, f_{N-1}(x))$ then one can find collisions of size $\mathcal{O}(N)$ for ϕ.*

Conclusions

Conclusions

- 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.
- 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 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.


Anshel, Iris et al. (2007). "Key agreement, the Algebraic Eraser™, and lightweight cryptography". In: *Contemporary Mathematics* 418, pp. 1–34.


Banin, M. and B. Tsaban (Oct. 2016). "A Reduction of Semigroup DLP to Classic DLP". In: *Des. Codes Cryptography* 81.1, 75–82. ISSN: 0925-1022. DOI: 10.1007/s10623-015-0130-2.


Ben-Zvi, Adi, Arkadius Kalka, and Boaz Tsaban (2018). "Cryptanalysis via algebraic spans". In: *Annual International Cryptology Conference*. Springer, pp. 255–274.


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*.

References II

 Freeman, David (2004). "The Discrete Logarithm Problem in Matrix Groups". In: URL: http://theory.stanford.edu/~dfreeman/papers/discretelogs.pdf.

 Grassl, Markus et al. (Jan. 2011). "Cryptanalysis of the Tillich–Zémor Hash Function". In: *Journal of Cryptology* 24.1, pp. 148–156. ISSN: 1432-1378. DOI: 10.1007/s00145-010-9063-0. URL: https://doi.org/10.1007/s00145-010-9063-0.

 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.

 Ko, Ki Hyoung et al. (2000). "New public-key cryptosystem using braid groups". In: *Annual International Cryptology Conference*. Springer, pp. 166–183.

References III


Kreuzer, Martin, Alexey D Myasnikov, and Alexander Ushakov (2014). "A linear algebra attack to group-ring-based key exchange protocols". In: *International Conference on Applied Cryptography and Network Security*. Springer, pp. 37–43.


Menezes, Alfred and Yihong Wu (1997). "The Discrete Logarithm Problem in $GL(n, q)$". In: *Ars Comb.* 47.


Monico, C. (May 2002). "Semirings and Semigroup Actions in Public-Key Cryptography". PhD thesis. University of Notre Dame.


Myasnikov, Alexei and Vitaliĭ Roman'kov (2015). "A linear decomposition attack". In: *Groups Complexity Cryptology* 7.1, pp. 81–94. DOI: doi:10.1515/gcc-2015-0007. URL: https://doi.org/10.1515/gcc-2015-0007.


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.

References IV


Petit, Christophe and Jean-Jacques Quisquater (Jan. 2011). "Rubik's for cryptographers.". In: *IACR Cryptology ePrint Archive* 2011, p. 638.


Petit, Christophe et al. (2009). "Hard and Easy Components of Collision Search in the Zémor-Tillich Hash Function: New Attacks and Reduced Variants with Equivalent Security". In: *Topics in Cryptology – CT-RSA 2009*. Ed. by Marc Fischlin. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 182–194. ISBN: 978-3-642-00862-7.


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.


Tsaban, Boaz (2015). "Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography". In: *Journal of Cryptology* 28.3, pp. 601–622.

References V


Tsopanidis, Nikolaos (2020). "The Hurwitz and Lipschitz Integers and Some Applications". PhD thesis. Universidade do Porto.


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.


Zémor, Gilles (1991). "Hash Functions And Graphs With Large Girths". In: *International Conference on the Theory and Application of Cryptographic Techniques*.