The Discrete Logarithm Problem (DLP) and its Generalization to the Semigroup Action Problem (SAP)

Joachim Rosenthal
University of Zürich

Graduate Workshop on
Linear Algebra over Finite Fields & Applications
ICERM
August 18-29, 2025.

University of Zurich

Outline

University of Zurich

The Discrete Logarithm Problem (DLP)

Definition

Let G be an arbitrary group, $\alpha \in G$ an arbitrary element and $H := < \alpha > \subset G$ the cyclic group generated by α. Assume $\beta \in H$ is an arbitrary element. The unique integer n having the property that $1 \leq n < |H|$ and $\alpha^n = \beta$ is called the discrete logarithm of β to the base α.

University of Zurich

The Discrete Logarithm Problem (DLP)

Definition

Let G be an arbitrary group, $\alpha \in G$ an arbitrary element and $H := <\alpha> \subset G$ the cyclic group generated by α. Assume $\beta \in H$ is an arbitrary element. The unique integer n having the property that $1 \leq n < |H|$ and $\alpha^n = \beta$ is called the discrete logarithm of β to the base α.

Notation

$$\log_\alpha \beta = n.$$

University of Zurich

The Discrete Logarithm Problem (DLP)

Definition

Let G be an arbitrary group, $\alpha \in G$ an arbitrary element and $H :=< \alpha >\subset G$ the cyclic group generated by α. Assume $\beta \in H$ is an arbitrary element. The unique integer n having the property that $1 \leq n < |H|$ and $\alpha^n = \beta$ is called the discrete logarithm of β to the base α.

Notation

$$\log_\alpha \beta = n.$$

One has the usual computations:

$$\alpha^{(\log_\alpha \beta)} = \beta, \quad \log_\alpha(\alpha^n) = n$$

$$\log_\alpha(\beta_1\beta_2) = \log_\alpha(\beta_1) + \log_\alpha(\beta_2) \mod |H|$$

Diffie-Hellman protocol [DH76]

Alice and Bob want to exchange a secret key over some insecure channel. In order to achieve this goal Alice and Bob agree on a group H and a common base $\alpha \in H$.

Diffie-Hellman protocol [DH76]

Alice and Bob want to exchange a secret key over some insecure channel. In order to achieve this goal Alice and Bob agree on a group H and a common base $\alpha \in H$.

Alice chooses a random integer $a \in \mathbb{N}$ and Bob chooses a random integer $b \in \mathbb{N}$. Alice transmits to Bob α^a and Bob transmits to Alice α^b. Their common secret key is $k := \alpha^{ab}$.

Diffie-Hellman protocol [DH76]

Alice and Bob want to exchange a secret key over some insecure channel. In order to achieve this goal Alice and Bob agree on a group H and a common base $\alpha \in H$.

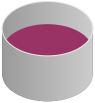
Alice chooses a random integer $a \in \mathbb{N}$ and Bob chooses a random integer $b \in \mathbb{N}$. Alice transmits to Bob α^a and Bob transmits to Alice α^b. Their common secret key is $k := \alpha^{ab}$.

Remark

Using so called 'consecutive squaring' allows Alice efficiently α^a *even for very large integers a. (polynomial time in the number of input bits). On the other hand the best algorithm known to compute* $\log_\alpha \beta = n$ *has exponential running time in the number of input bits.*

University of Zurich

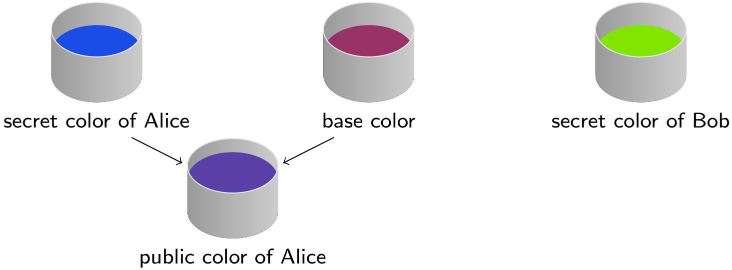
Illustration of Diffie-Hellman-Protocol



base color

Illustration of Diffie-Hellman-Protocol

Illustration of Diffie-Hellman-Protocol



University of Zurich

Illustration of Diffie-Hellman-Protocol

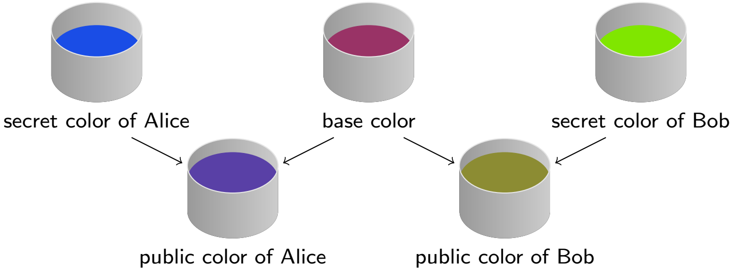
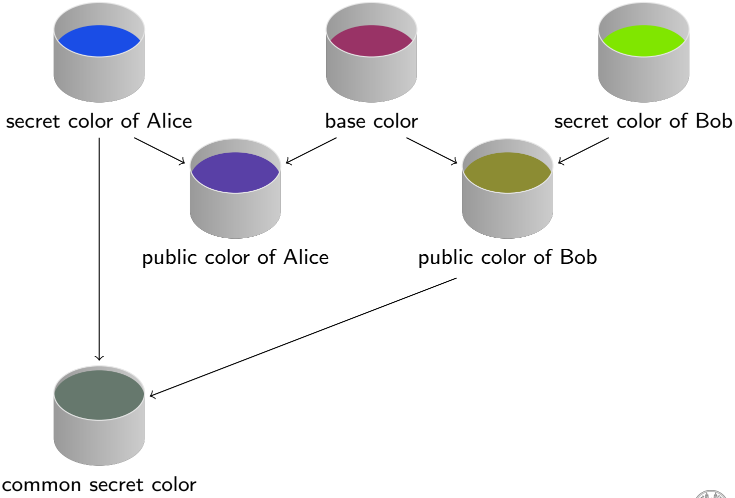
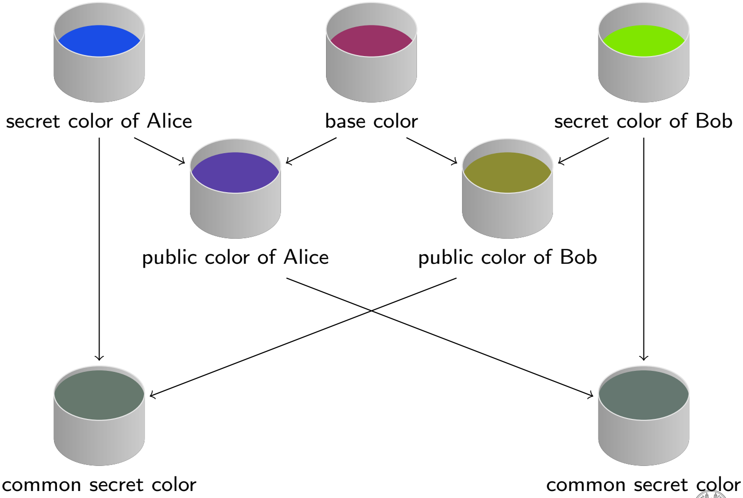


Illustration of Diffie-Hellman-Protocol



University of Zurich

Illustration of Diffie-Hellman-Protocol



One way trapdoor functions and asymmetric keys [DH76]

Definition

A one way trapdoor function is a one-way function $\varphi : X \longrightarrow Y$*, which has the property:*

One way trapdoor functions and asymmetric keys [DH76]

Definition

A one way trapdoor function is a one-way function $\varphi : X \longrightarrow Y$, *which has the property:*

- φ *is injective*

One way trapdoor functions and asymmetric keys [DH76]

Definition

A one way trapdoor function is a one-way function $\varphi : X \longrightarrow Y$*, which has the property:*

- φ *is injective*
- *With the help of a 'private key' it is possible to compute:*

$$\varphi^{-1} : \varphi(X) \longrightarrow X.$$

Principle of public key cryptography

Principle of public key cryptography

- Alice constructs a one-way trapdoor function $\varphi : X \longrightarrow Y$ and publishes it.

Principle of public key cryptography

- Alice constructs a one-way trapdoor function $\varphi : X \longrightarrow Y$ and publishes it.
- Bob wants to send to Alice the message $x \in X$. He computes $\varphi(x) \in Y$ and sends this to Alice.

Principle of public key cryptography

- Alice constructs a one-way trapdoor function $\varphi : X \longrightarrow Y$ and publishes it.
- Bob wants to send to Alice the message $x \in X$. He computes $\varphi(x) \in Y$ and sends this to Alice.
- Only Alice knows how to compute $x = \varphi^{-1}(\varphi(x))$.

Principle of public key cryptography

- Alice constructs a one-way trapdoor function $\varphi : X \longrightarrow Y$ and publishes it.
- Bob wants to send to Alice the message $x \in X$. He computes $\varphi(x) \in Y$ and sends this to Alice.
- Only Alice knows how to compute $x = \varphi^{-1}(\varphi(x))$.

Remark

In practices $x \in X$ represents often the key for some secret key system. The importance of one-way trapdoor functions was recognized by Diffie and Hellman in 1976.

El Gamal one way trapdoor function:

Let $<\alpha>= H$ be a cyclic group, where it is known that the discrete logarithm problem is 'hard'. Let n be an integer $1 < n < |H|$ and Bob computes $\beta := \alpha^n$.

El Gamal one way trapdoor function:

Let $<\alpha>= H$ be a cyclic group, where it is known that the discrete logarithm problem is 'hard'. Let n be an integer $1 < n < |H|$ and Bob computes $\beta := \alpha^n$.

Bob's Public Key:	(α, β, G)
Bob's Private Key:	$n = \log_\alpha \beta$.
Encryption:	$H \longrightarrow H \times H$
	$x \longmapsto (\alpha^k, x\beta^k) =: (c_1, c_2)$,

where k has been randomly chosen by Alice.

University of Zurich

El Gamal one way trapdoor function:

Let $<\alpha>= H$ be a cyclic group, where it is known that the discrete logarithm problem is 'hard'. Let n be an integer $1 < n < |H|$ and Bob computes $\beta := \alpha^n$.

Bob's Public Key:	(α, β, G)
Bob's Private Key:	$n = \log_\alpha \beta$.
Encryption:	$H \longrightarrow H \times H$
	$x \longmapsto (\alpha^k, x\beta^k) =: (c_1, c_2)$,

where k has been randomly chosen by Alice.

Bob, with the knowledge of n is able to compute x from the cipher text c_1, c_2:

$$x = c_2 \left((c_1)^n\right)^{-1}.$$

Semigroups and Loops

Because of Shor's algorithm [Sho94], neither the Diffie-Hellman protocol nor the El Gamal one way trapdoor function are quantum safe if used with a finite group. This motivates to consider more general structures.

Semigroups and Loops

Because of Shor's algorithm [Sho94], neither the Diffie-Hellman protocol nor the El Gamal one way trapdoor function are quantum safe if used with a finite group. This motivates to consider more general structures.

Definition

A semigroup *G is a set that comes with an associative binary operation $(a, b) \longmapsto ab$.*

Semigroups and Loops

Because of Shor's algorithm [Sho94], neither the Diffie-Hellman protocol nor the El Gamal one way trapdoor function are quantum safe if used with a finite group. This motivates to consider more general structures.

Definition

A semigroup *G is a set that comes with an associative binary operation $(a, b) \longmapsto ab$.*

Definition

Let L be a set with a binary operation $(a, b) \longmapsto ab$. Then L is a loop if:

- *For $a, b, c \in L$, the knowledge of any two elements in the equation $ab = c$ uniquely specifies the third.*
- *There exists a neutral element e such that $ea = ae = a$ for all $a \in L$.*

Moufang Loops

Definition

A loop M is called a Moufang loop if the Moufang identities

$$(ab)(ca) = a((bc)a)$$
$$a(b(ac)) = ((ab)a)c$$
$$a(b(cb)) = (a(bc))b$$

are satisfied for every $a, b, c \in M$.

Moufang Loops

Definition

A loop M is called a Moufang loop if the Moufang identities

$$(ab)(ca) = a((bc)a)$$
$$a(b(ac)) = ((ab)a)c$$
$$a(b(cb)) = (a(bc))b$$

are satisfied for every $a, b, c \in M$.

Remark

One can show that if M is Moufang loop and $\alpha \in M$ *then the subloop* $< \alpha > \subset M$ *forms a group. In particular the discrete logarithm problem* $\log_\alpha \beta$ *is well defined and efficient algorithms such as square and multiply are possible.*

Ruth Moufang, 1905–1977

Cryptanalysis in Paige loops

Definition

A Moufang loop M is a Paige loop if it is non-associative, finite and simple.

Cryptanalysis in Paige loops

Definition

A Moufang loop M is a Paige loop if it is non-associative, finite and simple.

G. Maze in his 2003 dissertation [Maz03] could cryptanalyse the DLP in a Paige loop. The problem could be translated to the problem of the DLP in the finite group $SL_2(\mathbb{F}_q)$. The problem is hence certainly not quantum-safe.

Cryptanalysis in Paige loops

Definition

A Moufang loop M is a Paige loop if it is non-associative, finite and simple.

G. Maze in his 2003 dissertation [Maz03] could cryptanalyse the DLP in a Paige loop. The problem could be translated to the problem of the DLP in the finite group $SL_2(\mathbb{F}_q)$. The problem is hence certainly not quantum-safe.

For general Moufang loops and general semigroups it seems to be unknown if a quantum-polynomial algorithm exists.

University of Zurich

Semigroups and actions on sets

Another natural generalization to the DLP are semigroup actions first introduced by G.Maze, C.Monico and the speaker in 2002 [MMR02, MMRC02, Mon02, Maz03].

Semigroups and actions on sets

Another natural generalization to the DLP are semigroup actions first introduced by G.Maze, C.Monico and the speaker in 2002 [MMR02, MMRC02, Mon02, Maz03].

Let G be a semigroup, let X be a set. A *semigroup action* of G on X is a map

$$\begin{array}{rrcl} \varphi: & G \times X & \longrightarrow & X \\ & (a,x) & \longmapsto & ax \end{array}$$

having the property, that

$$(a \cdot b)x = a(bx) \text{ for all } a,b \in G \text{ and } x \in X.$$

Semigroup Action Problem (SAP)

Definition

Given a semigroup action G on X and elements $a \in G$ and $x \in X$. Given the elements x and $y := ax$. The semigroup action problem *asks for the computation of an element $\tilde{a} \in G$ such that $y = \tilde{a}x$.*

Semigroup Action Problem (SAP)

Definition

Given a semigroup action G on X and elements $a \in G$ and $x \in X$. Given the elements x and $y := ax$. The semigroup action problem *asks for the computation of an element $\tilde{a} \in G$ such that $y = \tilde{a}x$.*

Notation

$$\log_x y := \{a \in G \mid ax = y\}.$$

Semigroup Action Problem (SAP)

Definition

Given a semigroup action G on X and elements $a \in G$ and $x \in X$. Given the elements x and $y := ax$. The semigroup action problem *asks for the computation of an element $\tilde{a} \in G$ such that $y = \tilde{a}x$.*

Notation

$$\log_x y := \{a \in G \mid ax = y\}.$$

Remark

Given a semigroup action. It has been shown in [MMR07] that

$$\mathrm{Stab}(x) := \{g \in G \mid gx = x\}$$

is a sub-semigroup and for cryptographic purposes what matters is the size of

$$\frac{\#G}{\#\mathrm{Stab}(x)}$$

Generalization of the DLP

Remark

Integers $(\mathbb{Z}, \cdot)$ *act on a group* G *through* $(a, g) \mapsto g^a$. *This leads to the usual discrete logarithm problem.*

University of Zurich

Generalization of the DLP

Remark

Integers $(\mathbb{Z}, \cdot)$ act on a group G through $(a, g) \mapsto g^a$. This leads to the usual discrete logarithm problem.

Remark

Note that $(\mathbb{Z}, \cdot)$ respectively $(\mathbb{Z}/n\mathbb{Z}, \cdot)$, respectively $(\mathbb{Z}/p\mathbb{Z}, \cdot)$, p a prime, is a semigroup but not a group. This has been one of the main reasons to look immediately at semigroup actions and not to restrict to group actions as considered in the recent literature [ADFMP20]

Generalized Diffie-Hellman protocol

Let X be a finite set, G an abelian semigroup and an action of G on X as just defined. The Extended Diffie-Hellman key exchange is the following protocol:

Generalized Diffie-Hellman protocol

Let X be a finite set, G an abelian semigroup and an action of G on X as just defined. The Extended Diffie-Hellman key exchange is the following protocol:

- Alice and Bob agree on an element $x \in X$.

Generalized Diffie-Hellman protocol

Let X be a finite set, G an abelian semigroup and an action of G on X as just defined. The Extended Diffie-Hellman key exchange is the following protocol:

- Alice and Bob agree on an element $x \in X$.
- Alice chooses $a \in G$ and computes ax. Alice's secret key is a, her public key is ax.

Generalized Diffie-Hellman protocol

Let X be a finite set, G an abelian semigroup and an action of G on X as just defined. The Extended Diffie-Hellman key exchange is the following protocol:

- Alice and Bob agree on an element $x \in X$.
- Alice chooses $a \in G$ and computes ax. Alice's secret key is a, her public key is ax.
- Bob chooses $b \in G$ and computes bx. Bob's secret key is b, his public key is bx.

Generalized Diffie-Hellman protocol

Let X be a finite set, G an abelian semigroup and an action of G on X as just defined. The Extended Diffie-Hellman key exchange is the following protocol:

- Alice and Bob agree on an element $x \in X$.
- Alice chooses $a \in G$ and computes ax. Alice's secret key is a, her public key is ax.
- Bob chooses $b \in G$ and computes bx. Bob's secret key is b, his public key is bx.
- Their common secret key is then

$$a(bx) = (a \cdot b)x = (b \cdot a)x = b(ax)$$

Extended El Gamal public key system

If X has a group structure with respect to some operation $\circ$, then the Extended El Gamal public key system is the following protocol:

Extended El Gamal public key system

If X has a group structure with respect to some operation $\circ$, then the Extended El Gamal public key system is the following protocol:

- Bob's public key is (x, bx), the private key is $\log_x bx$.

Extended El Gamal public key system

If X has a group structure with respect to some operation $\circ$, then the Extended El Gamal public key system is the following protocol:

- Bob's public key is (x, bx), the private key is $\log_x bx$.
- Alice chooses a random element $a \in G$ and encrypts a message m using the encryption function

$$(m, a) \longmapsto (ax, (a(bx)) \circ m) = (c_1, c_2).$$

Extended El Gamal public key system

If X has a group structure with respect to some operation $\circ$, then the Extended El Gamal public key system is the following protocol:

- Bob's public key is (x, bx), the private key is $\log_x bx$.
- Alice chooses a random element $a \in G$ and encrypts a message m using the encryption function

$$(m, a) \longmapsto (ax, (a(bx)) \circ m) = (c_1, c_2).$$

- Bob can decrypt the message using

$$m = (a(bx))^{-1} \circ c_2 = (bc_1)^{-1} \circ c_2.$$

Zero Knowledge proof

The idea to build zero-knowledge proofs from group actions on sets goes back to Brassard and Yung [BY91].

Zero Knowledge proof

The idea to build zero-knowledge proofs from group actions on sets goes back to Brassard and Yung [BY91].

The procedures go also under the name 'MPC in the head' and we refer to the survey of Antoine Joux [Jou23].

Zero Knowledge proof

The idea to build zero-knowledge proofs from group actions on sets goes back to Brassard and Yung [BY91].

The procedures go also under the name 'MPC in the head' and we refer to the survey of Antoine Joux [Jou23].

In the sequel we outline how to do it for situations where a general SAP is hard.

Zero Knowledge proof

The idea to build zero-knowledge proofs from group actions on sets goes back to Brassard and Yung [BY91].

The procedures go also under the name 'MPC in the head' and we refer to the survey of Antoine Joux [Jou23].

In the sequel we outline how to do it for situations where a general SAP is hard.

Given a semigroup G not necessarily abelian and an action $\varphi: \ G \times X \longrightarrow X$ where SAP is hard.

Zero Knowledge proof

The idea to build zero-knowledge proofs from group actions on sets goes back to Brassard and Yung [BY91].

The procedures go also under the name 'MPC in the head' and we refer to the survey of Antoine Joux [Jou23].

In the sequel we outline how to do it for situations where a general SAP is hard.

Given a semigroup G not necessarily abelian and an action $\varphi : \; G \times X \longrightarrow X$ where SAP is hard.

- Prover convinces Verifier, that she knows $\log_x y = a$, i.e. she knows $a \in G$ such that $ax = y$.

University of Zurich

Zero Knowledge proof

The idea to build zero-knowledge proofs from group actions on sets goes back to Brassard and Yung [BY91].

The procedures go also under the name 'MPC in the head' and we refer to the survey of Antoine Joux [Jou23].

In the sequel we outline how to do it for situations where a general SAP is hard.

Given a semigroup G not necessarily abelian and an action $\varphi: \; G \times X \longrightarrow X$ where SAP is hard.

- Prover convinces Verifier, that she knows $\log_x y = a$, i.e. she knows $a \in G$ such that $ax = y$.
- Prover chooses randomly elements $b_i \in G$ and computes $z_i := b_i y = b_i a x$ for $i = 1, \ldots, n$.

Zero Knowledge proof

The idea to build zero-knowledge proofs from group actions on sets goes back to Brassard and Yung [BY91].

The procedures go also under the name 'MPC in the head' and we refer to the survey of Antoine Joux [Jou23].

In the sequel we outline how to do it for situations where a general SAP is hard.

Given a semigroup G not necessarily abelian and an action $\varphi: \ G \times X \longrightarrow X$ where SAP is hard.

- Prover convinces Verifier, that she knows $\log_x y = a$, i.e. she knows $a \in G$ such that $ax = y$.
- Prover chooses randomly elements $b_i \in G$ and computes $z_i := b_i y = b_i ax$ for $i = 1, \ldots, n$.
- For each index i Verifier can either ask $\log_x z_i = b_i a$ or $\log_y z_i = b_i$.

Chebyshev action

Definition

$$T_n(x) = \cos(n \cos^{-1} x) = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} (-1)^k x^{n-2k} (1-x^2)^k$$

is called the nth Chebyshev polynomial.

Theorem

$T_{nm}(x) = T_n(T_m(x))$ in $\mathbb{Z}[x]$. In particular if R is any finite semiring then $T_n(r)$ can be efficiently computed for any $r \in R$ and $n \in \mathbb{N}$.

University of Zurich

Action on Endomorphism Ring

Example

Any abelian group H comes with its ring of endomorphisms $\operatorname{End} H$ where addition is defined pointwise and multiplication via composition of maps. There is a natural action of $\operatorname{End} H$ on H as follows :

$$\begin{aligned} \operatorname{End} H \times H &\longrightarrow H \\ (\varphi, h) &\longmapsto \varphi(h) \end{aligned}$$

For a given $\varphi \in \operatorname{End} H$, the subring $\mathbb{Z}[\varphi]$ of $\operatorname{End} H$ is commutative and yields to a Diffie-Hellman protocol.

University of Zurich

Special situation

Let $\mathbb{F}_p$ be a prime finite field ($p > 3$), $\overline{\mathbb{F}_p}$ its algebraic closure and $E\ :\ y^2 = x^3 + ax + b$ an ordinary elliptic curve over $\mathbb{F}_p$ with complex multiplication. In this case, it is known that $\mathrm{End}\, E(\overline{\mathbb{F}_p}) \cong \mathbb{Z} \oplus \mathbb{Z}\varphi$, where φ is the Frobenius endomorphism:

$$\begin{array}{rcl} \varphi : E(\overline{\mathbb{F}_p}) & \longrightarrow & E(\overline{\mathbb{F}_p}) \\ (x, y) & \longrightarrow & (x^p, y^p) \end{array}$$

Actions on semi-modules

Let R be a semiring, not necessarily finite.
(Two operations '$+$' and '$\cdot$' which are distributive and associative. We assume also that '$+$' is commutative. No neutral elements assumed.)
Let M be a finite semi-module over R. With this we mean that M has the structure of a finite semigroup and there is an action $R \times M \longrightarrow M$ such that

$$\begin{aligned} r(sm) &= (rs)m, \\ (r+s)m &= rm + sm, \\ r(m+n) &= rm + rn. \end{aligned}$$

for all $r, s \in R$ and $m, n \in M$.

University of Zurich

Actions on semi-modules

Let $Mat_{n\times n}(R)$ be the set of all $n \times n$ matrices with entries in R. The semiring structure on R induces a semiring structure on $Mat_{n\times n}(R)$. Moreover the semi-module structure on M lifts to a semi-module structure on M^n via the matrix multiplication:

$$\begin{aligned} Mat_{n\times n}(R) \times M^n &\longrightarrow M^n \\ (A, x) &\longmapsto Ax. \end{aligned} \tag{1}$$

Actions on semi-modules

Let $Mat_{n\times n}(R)$ be the set of all $n \times n$ matrices with entries in R. The semiring structure on R induces a semiring structure on $Mat_{n\times n}(R)$. Moreover the semi-module structure on M lifts to a semi-module structure on M^n via the matrix multiplication:

$$\begin{array}{rcl} Mat_{n\times n}(R) \times M^n & \longrightarrow & M^n \\ (A, x) & \longmapsto & Ax. \end{array} \tag{1}$$

One readily verifies that $Mat_{n\times n}(R) \times M^n \longrightarrow M^n$ is an action by a semigroup, indeed one readily computes that $A(Bg) = (AB)g$.

Commutative semigroups

Let $R[t]$ be the polynomial ring in the indeterminant t and let $A \in Mat_{n \times n}(R)$ be a fixed matrix. Let $C \subset R$ be the center of R.

University of Zurich

Commutative semigroups

Let $R[t]$ be the polynomial ring in the indeterminant t and let $A \in Mat_{n\times n}(R)$ be a fixed matrix. Let $C \subset R$ be the center of R.If

$$p(t) = r_0 + r_1 t + \cdots + r_k t^k \in C[t]$$

then we define in the usual way $p(A) = r_0 I_n + r_1 A + \cdots + r_k A^k$, where $r_0 I_n$ is the $n \times n$ diagonal matrix with entry r_0 in each diagonal element.
Consider the semigroup

$$G := C[A] := \{p(A) \mid p(t) \in C[t]\}.$$

Clearly G has the structure of an abelian semigroup.

Diffie-Hellman protocol

Alice and Bob agree on an R-module $\mathcal{M}$, an element $b \in \mathcal{M}^n$ and a matrix $A \in Mat_{n\times n}(R)$.
Alice chooses secretly $p(t) \in C[t]$ and computes $p(A)b$ and sends the result to Bob. Bob chooses secretly $q(t) \in C[t]$ and computes $q(A)b$ and sends the result to Alice.
As a common secret key serves $k := p(A)q(A)b$

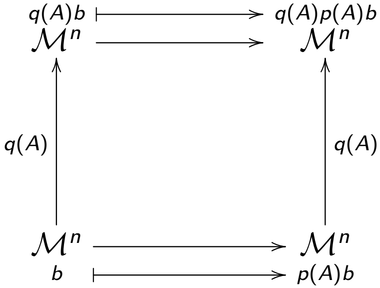
Nota Bene:

It should be difficult to find $\tilde{p}(t) \in C[t]$ such that

$$\tilde{p}(A)b = p(A)b.$$

University of Zurich

In Diagram:


$q(A)b \longmapsto q(A)p(A)b$
$\mathcal{M}^n \longrightarrow \mathcal{M}^n$
$q(A)$
$q(A)$
$\mathcal{M}^n \longrightarrow \mathcal{M}^n$
$b \longmapsto p(A)b$

Lattice isomorphism problem (LIP)

$\mathrm{Sym}_n(\mathbb{Z})$ the set of symmetric $n \times n$ matrices over the integers parameterizing quadratic forms.

University of Zurich

Lattice isomorphism problem (LIP)

$\mathrm{Sym}_n(\mathbb{Z})$ the set of symmetric $n \times n$ matrices over the integers parameterizing quadratic forms.

$Gl_n(\mathbb{Z})$ the set of $n \times n$ unimodular matrices over the integers.

Lattice isomorphism problem (LIP)

$\mathrm{Sym}_n(\mathbb{Z})$ the set of symmetric $n \times n$ matrices over the integers parameterizing quadratic forms.

$Gl_n(\mathbb{Z})$ the set of $n \times n$ unimodular matrices over the integers.

Group action:

$$\begin{aligned} \varphi: \quad Gl_n(\mathbb{Z}) \times \mathrm{Sym}_n(\mathbb{Z}) &\longrightarrow \mathrm{Sym}_n(\mathbb{Z}) \\ (U, T) &\longmapsto U^t T U. \end{aligned}$$

Lattice isomorphism problem (LIP)

$\mathrm{Sym}_n(\mathbb{Z})$ the set of symmetric $n \times n$ matrices over the integers parameterizing quadratic forms.

$Gl_n(\mathbb{Z})$ the set of $n \times n$ unimodular matrices over the integers.

Group action:

$$\begin{array}{rrcl} \varphi : & Gl_n(\mathbb{Z}) \times \mathrm{Sym}_n(\mathbb{Z}) & \longrightarrow & \mathrm{Sym}_n(\mathbb{Z}) \\ & (U, T) & \longmapsto & U^t T U. \end{array}$$

If one restricts the group action to the positive definite matrices then it follows from Ducas and van Woerden [DvW22] that the SAP in this case is equivalent to the lattice isomorphism problem.

University of Zurich

Lattice isomorphism problem (LIP)

$\mathrm{Sym}_n(\mathbb{Z})$ the set of symmetric $n \times n$ matrices over the integers parameterizing quadratic forms.

$Gl_n(\mathbb{Z})$ the set of $n \times n$ unimodular matrices over the integers.

Group action:

$$\begin{array}{rrcl} \varphi : & Gl_n(\mathbb{Z}) \times \mathrm{Sym}_n(\mathbb{Z}) & \longrightarrow & \mathrm{Sym}_n(\mathbb{Z}) \\ & (U, T) & \longmapsto & U^t T U. \end{array}$$

If one restricts the group action to the positive definite matrices then it follows from Ducas and van Woerden [DvW22] that the SAP in this case is equivalent to the lattice isomorphism problem.

Remark

It should be possible to build signature schemes if one allows general quadratic forms, not necessarily positive definite.

Code equivalence problem

$\mathrm{Grass}(k, \mathbb{F}^n)$ the Grassman variety of k-dimensional subspaces inside the vector space $\mathbb{F}^n$.

Code equivalence problem

$\mathrm{Grass}(k, \mathbb{F}^n)$ the Grassman variety of k-dimensional subspaces inside the vector space $\mathbb{F}^n$.

$M_n(\mathbb{F})$ the set of $n \times n$ monomial matrices over the finite field $\mathbb{F}$.

Code equivalence problem

$\mathrm{Grass}(k, \mathbb{F}^n)$ the Grassman variety of k-dimensional subspaces inside the vector space $\mathbb{F}^n$.

$M_n(\mathbb{F})$ the set of $n \times n$ monomial matrices over the finite field $\mathbb{F}$.

Group action:

$$\begin{aligned} \varphi : \quad M_n \times \mathrm{Grass}(k, \mathbb{F}^n) &\longrightarrow \mathrm{Grass}(k, \mathbb{F}^n) \\ (U, \mathrm{rowsp}(G)) &\longmapsto \mathrm{rowsp}(GU) \end{aligned}$$

University of Zurich

Code equivalence problem

$\mathrm{Grass}(k, \mathbb{F}^n)$ the Grassman variety of k-dimensional subspaces inside the vector space $\mathbb{F}^n$.

$M_n(\mathbb{F})$ the set of $n \times n$ monomial matrices over the finite field $\mathbb{F}$.

Group action:

$$\begin{array}{llll} \varphi : & M_n \times \mathrm{Grass}(k, \mathbb{F}^n) & \longrightarrow & \mathrm{Grass}(k, \mathbb{F}^n) \\ & (U, \mathrm{rowsp}(G)) & \longmapsto & \mathrm{rowsp}(GU) \end{array}$$

Above SAP describes the linear code equivalence problem heavily studied for building signature algorithms [BBPS23, BBP$^+$24].

Further interesting cryptographic group actions

Isogeny-based Cryptography

The study of isogeny-based cryptography was initiated by Couveignes [Cou06]. Couveignes already pointed out that some protocols can be seen as a group action on a set.

Further interesting cryptographic group actions

Isogeny-based Cryptography

The study of isogeny-based cryptography was initiated by Couveignes [Cou06]. Couveignes already pointed out that some protocols can be seen as a group action on a set.

Alamati e.a. [ADFMP20] provide a framework for group actions covering situations such as the Commutative Supersingular Isogeny Diffie-Hellman (CSIDH) group action.

Further interesting cryptographic group actions

Isogeny-based Cryptography

The study of isogeny-based cryptography was initiated by Couveignes [Cou06]. Couveignes already pointed out that some protocols can be seen as a group action on a set.

Alamati e.a. [ADFMP20] provide a framework for group actions covering situations such as the Commutative Supersingular Isogeny Diffie-Hellman (CSIDH) group action.

Semidirect Discrete Logarithm Problem (SDLP)

Battarbee e.a. show [BKS24] that the SDLP can be viewed as a group action and the underlying problem is hence also a SAP.

Generic Algorithms for the SAP

Given a semigroup action $\varphi : \ G \times X \longrightarrow X$.

University of Zurich

Generic Algorithms for the SAP

Given a semigroup action $\varphi : \ G \times X \longrightarrow X$.

In the survey article on semigroup actions [GZ24] Gnilke and Zumbrägel focused also on the generic complexity.

Generic Algorithms for the SAP

Given a semigroup action $\varphi: \ G \times X \longrightarrow X$.

In the survey article on semigroup actions [GZ24] Gnilke and Zumbrägel focused also on the generic complexity.

They explain that for group actions the generic complexity has both a square-root lower bound and a square-root upper bound. For proper semigroup actions one is lacking inversion in the group and the situation is less clear what the generic complexity is concerned.

Semirings

Definition

A semiring R is a non-empty set together with two associative operations $+$ and $\cdot$. with regard to addition $(R, +)$ is a commutative semigroup. The following distributive laws hold:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (a + b) \cdot c = a \cdot c + b \cdot c.$$

University of Zurich

Semirings

Definition

A semiring R is a non-empty set together with two associative operations $+$ and $\cdot$. with regard to addition $(R, +)$ is a commutative semigroup. The following distributive laws hold:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Example

Consider the finite ring $R = \mathbb{Z}_6$. Consider the semigroup $G := \mathrm{Mat}_{n \times n}(R)$ consisting of $n \times n$ matrices with entries in R.

University of Zurich

Semirings

Definition

A semiring R is a non-empty set together with two associative operations $+$ and $\cdot$. with regard to addition $(R, +)$ is a commutative semigroup. The following distributive laws hold:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Example

Consider the finite ring $R = \mathbb{Z}_6$. Consider the semigroup $G := \mathrm{Mat}_{n \times n}(R)$ consisting of $n \times n$ matrices with entries in R.

Reduction modulo 2 and modulo 3 reduces the problem to two simpler instances which can be solved efficiently.

Semirings

Definition

A semiring R is a non-empty set together with two associative operations $+$ and $\cdot$. with regard to addition $(R,+)$ is a commutative semigroup. The following distributive laws hold:

$$a\cdot(b+c)=a\cdot b+a\cdot c,\qquad (a+b)\cdot c=a\cdot c+b\cdot c.$$

Example

Consider the finite ring $R=\mathbb{Z}_6$. Consider the semigroup $G:=\mathrm{Mat}_{n\times n}(R)$ consisting of $n\times n$ matrices with entries in R.

Reduction modulo 2 and modulo 3 reduces the problem to two simpler instances which can be solved efficiently.

Remark

For above reason it is advisable to consider somehow 'simple rings'.

Simple semirings

Definition

A **congruence relation** *on a semiring R is an equivalence relation $\sim$ that also satisfies*

$$x_1 \sim x_2 \Rightarrow \begin{cases} c + x_1 & \sim & c + x_2, \\ x_1 + c & \sim & x_2 + c, \\ cx_1 & \sim & cx_2, \\ x_1 c & \sim & x_2 c, \end{cases}$$

for all $x_1, x_2, c \in R$. A semiring R that admits no congruence relations other than the trivial ones, id_R and $R \times R$, is said to be **congruence-simple**, *or* **c-simple**.

University of Zurich

Results on simple semirings

Theorem (Monico [Mon02])

Let R be a finite, additively commutative, congruence-simple semiring. Then one of the following holds:

1. $|R| = 2$.
2. $R \cong \mathrm{Mat}_{n\times n}(\mathbb{F}_q)$ *for some finite field* $\mathbb{F}_q$ *and some* $n \geq 1$.
3. R *is a zero multiplication ring of prime order.*
4. R *is additively idempotent.*
5. *There is an infinite element* ∞ *having the property that* $\infty r = r\infty = \infty + r = r + \infty = \infty$.

Results on simple semirings

Theorem (Monico [Mon02])

Let R be a finite, additively commutative, congruence-simple semiring. Then one of the following holds:

1. $|R| = 2$.
2. $R \cong \mathrm{Mat}_{n\times n}(\mathbb{F}_q)$ *for some finite field* $\mathbb{F}_q$ *and some* $n \geq 1$.
3. R *is a zero multiplication ring of prime order.*
4. R *is additively idempotent.*
5. *There is an infinite element* ∞ *having the property that* $\infty r = r\infty = \infty + r = r + \infty = \infty$.

Theorem (Zumbraegel [Zum08])

A finite semiring of order > 2 with zero which is not a ring is congruence-simple if and only if it is isomorphic to a "dense" subsemiring of the endomorphism semiring of a finite idempotent commutative monoid.

Some simple semirings of small order

A Simple Semiring of order 2

+	0	1
0	0	1
1	1	1

*	0	1
0	0	0
1	1	1

Some simple semirings of small order

A Simple Semiring of order 2

+	0	1
0	0	1
1	1	1

*	0	1
0	0	0
1	1	1

A Simple Semiring of order 3

+	0	1	2
0	0	1	2
1	1	1	2
2	2	2	2

*	0	1	2
0	0	0	0
1	0	1	2
2	2	2	2

A simple semiring of order 6, called S_6

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	1	1	1	1	5
2	2	1	2	1	2	5
3	3	1	1	3	3	5
4	4	1	2	3	4	5
5	5	5	5	5	5	5

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	2	0	0	5
3	0	3	4	3	4	3
4	0	4	4	0	0	3
5	0	5	2	5	2	5

Example of DLP in a matrix group over S_6

Assume a matrix is given as:

$$\begin{pmatrix} 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \\ 2 & 0 & 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 3 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \end{pmatrix}$$

University of Zurich

Example of DLP in a matrix group over S_6

What exponent results in the matrix

$$\begin{pmatrix} 2 & 3 & 3 & 3 & 3 & 3 & 2 & 2 & 3 & 2 \\ 3 & 2 & 3 & 3 & 3 & 2 & 1 & 3 & 2 & 3 \\ 0 & 5 & 2 & 1 & 5 & 5 & 5 & 0 & 5 & 5 \\ 5 & 0 & 5 & 2 & 1 & 5 & 1 & 5 & 0 & 5 \\ 5 & 5 & 5 & 5 & 2 & 5 & 1 & 5 & 5 & 5 \\ 3 & 3 & 3 & 4 & 3 & 3 & 3 & 3 & 3 & 2 \\ 3 & 3 & 3 & 3 & 4 & 2 & 4 & 3 & 3 & 3 \\ 0 & 3 & 0 & 4 & 3 & 3 & 2 & 0 & 3 & 3 \\ 3 & 0 & 3 & 0 & 4 & 0 & 4 & 2 & 0 & 3 \\ 3 & 3 & 3 & 3 & 3 & 3 & 3 & 4 & 2 & 3 \end{pmatrix}$$

University of Zurich

Semigroup action on itself

$G := \mathrm{Mat}_{n \times n}(R)$ be the semigroup consisting of $n \times n$ matrices over some simple semiring R.

University of Zurich

Semigroup action on itself

$G := \mathrm{Mat}_{n\times n}(R)$ be the semigroup consisting of $n \times n$ matrices over some simple semiring R.

Consider the semigroup action on itself:

$$\begin{array}{rcl} G \times G & \longrightarrow & G \\ (A, X) & \longmapsto & AX = Y. \end{array}$$

Semigroup action on itself

$G := \mathrm{Mat}_{n\times n}(R)$ be the semigroup consisting of $n \times n$ matrices over some simple semiring R.

Consider the semigroup action on itself:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (A, X) & \longmapsto & AX = Y. \end{array}$$

Remark

Over a field this is a trivial linear algebra problem. Over a non-commutative simple semiring where neither multiplicative nor additive inverses exist in general, we do not know how to solve the problem efficiently.

A two-sided abelian group action

Alice and Bob agree on a simple semiring R having center $C \subset R$ and agree on three matrices

$$A, B, M \in \mathrm{Mat}_{n \times n}(R).$$

University of Zurich

A two-sided abelian group action

Alice and Bob agree on a simple semiring R having center $C \subset R$ and agree on three matrices

$$A, B, M \in \mathrm{Mat}_{n \times n}(R).$$

Alice chooses secretly $p_1(t), p_2(t) \in C[t]$ and computes $p_1(A)Mp_2(B)$ and sends the result to Bob. Bob chooses secretly $q_1(t), q_2(t) \in C[t]$ and computes $q_1(A)Mq_2(B)$ and sends the result to Alice.

A two-sided abelian group action

Alice and Bob agree on a simple semiring R having center $C \subset R$ and agree on three matrices

$$A, B, M \in \mathrm{Mat}_{n\times n}(R).$$

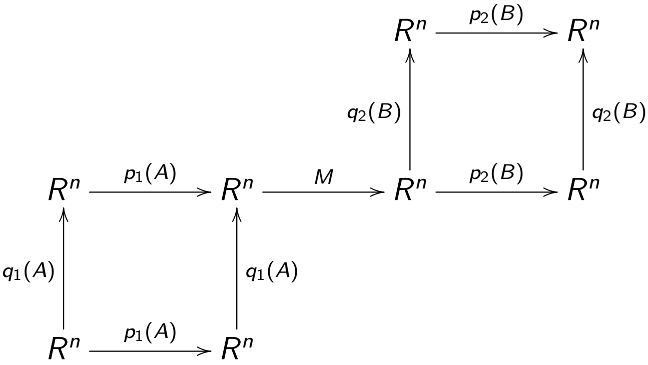
Alice chooses secretly $p_1(t), p_2(t) \in C[t]$ and computes $p_1(A)Mp_2(B)$ and sends the result to Bob. Bob chooses secretly $q_1(t), q_2(t) \in C[t]$ and computes $q_1(A)Mq_2(B)$ and sends the result to Alice.

As a common secret key serves

$$k := p_1(A)q_1(A)Mq_2(B)p_2(B)$$

which both can easily compute.

In Diagram:



As a concrete choice let assume that $n = 20$. Consider the matrices

$$A = \begin{bmatrix} 10000000000000000000 \\ 00100000000000000000 \\ 00010000000000000000 \\ 00001000000000000000 \\ 01000000000000000000 \\ 00000010000000000000 \\ 00000002000000000010 \\ 00000100000000000000 \\ 00000000010000000000 \\ 00000000001000000000 \\ 00000000000200000000 \\ 00000000000010000000 \\ 00000000100000000000 \\ 00000000000000100000 \\ 00000000000000010000 \\ 00000000000000001000 \\ 00000000000000000100 \\ 00000000000000000010 \\ 00000000000000000001 \\ 00000000000001000000 \end{bmatrix} \quad B = \begin{bmatrix} 00000000000000000010 \\ 00000000000100000000 \\ 00000010000000000000 \\ 00100000000000000000 \\ 00000000000000000004 \\ 00000000000000010000 \\ 01000000000000000000 \\ 00000000000000000100 \\ 00010000100000000000 \\ 00000000000310000000 \\ 00000000000000200000 \\ 00010000000000000100 \\ 00000000001000000000 \\ 00000100000000000000 \\ 00000000010000000000 \\ 00000001000000000000 \\ 10000000000000000000 \\ 00001000000000000000 \\ 00000000000000001000 \\ 00000000000001000000 \end{bmatrix}$$

Example

$$M = \begin{bmatrix} 00200000000000000100 \\ 01000000010001000000 \\ 00000001000000000030 \\ 20020000000010000000 \\ 00000010000000001000 \\ 00000005000100000001 \\ 00000000200010000001 \\ 01000000030000000003 \\ 00000002000000010001 \\ 01000100000010000000 \\ 00000000000050100000 \\ 00000000000004000000 \\ 00000000000000100500 \\ 00300000002000100000 \\ 00001000000200001000 \\ 00000002000000000100 \\ 00002000001000000000 \\ 00100000000100000000 \\ 00020001000000000030 \\ 10000001000010000001 \end{bmatrix} \qquad T = \begin{bmatrix} 02020000000204000200 \\ 00111411002100241114 \\ 30111011002000240134 \\ 12000020020200202034 \\ 22111424020100201110 \\ 12222020022220222212 \\ 11111014222124211122 \\ 21111014222124222124 \\ 00222020022022200200 \\ 00002000022020220000 \\ 00222020020000200200 \\ 00000000022022200000 \\ 00002000000000020200 \\ 03333404021324040300 \\ 02202420020020001010 \\ 01111014000104040104 \\ 32000020020220000034 \\ 11111014020104211104 \\ 31333424021124040334 \\ 12202420020000211014 \end{bmatrix}.$$

University of Zurich

Example

$$M = \begin{bmatrix} 00200000000000000100 \\ 01000000010001000000 \\ 00000001000000000030 \\ 20020000000010000000 \\ 00000010000000001000 \\ 00000005000100000001 \\ 00000000200010000001 \\ 01000000030000000003 \\ 00000002000000010001 \\ 01000100000010000000 \\ 00000000000050100000 \\ 00000000000004000000 \\ 00000000000000100500 \\ 00300000002000100000 \\ 00001000000200001000 \\ 00000002000000000100 \\ 00002000001000000000 \\ 00100000000100000000 \\ 00020001000000000030 \\ 10000001000010000001 \end{bmatrix} \quad T = \begin{bmatrix} 02020000000204000200 \\ 00111411002100241114 \\ 30111011002000240134 \\ 12000020020200202034 \\ 22111424020100201110 \\ 12222020022220222212 \\ 11111014222124211122 \\ 21111014222124222124 \\ 00222020022022200200 \\ 00002000022020220000 \\ 00222020020000200200 \\ 00000000022022200000 \\ 00002000000000020200 \\ 03333404021324040300 \\ 02202420020020001010 \\ 01111014000104040104 \\ 32000020020220000034 \\ 11111014020104211104 \\ 31333424021124040334 \\ 12202420020000211014 \end{bmatrix}.$$

The task of Eve will be to find $p_1(t), p_2(t) \in C[t]$ such that $p_1(A)Mp_2(B) = T$. See Steinwandt and Suárez Corona, [SSC11] and Otero and Lopez Ramos [ALR25].

University of Zurich

Thank you for your attention. Special thanks to:

Gianira Alfarano, Marco Baldi, Jessica Bariffi, Franco Chiaraluce, Josep Climent, Michele Elia, Felix Fontein, Niklas Gassner, Elisa Gorla, Anna-Lena Horlemann, Karan Khathuria, Julia Lieb, Javier Lobillio, Juan Antonio Lopez Ramos, Felice Manganiello, Abhinaba Mazumder, Gerard Maze, Carlo Matteotti, Chris Monico, Alessandro Neri, Paolo Santini, Davide Schipani, Reto Schnyder, Amin Shokrollahi, Abigail Sutton, Simran Tinani, Violetta Weger, Jens Zumbrägel.

N. Alamati, L. De Feo, H. Montgomery, and S. Patranabis.

Cryptographic group actions and applications.

In *Advances in cryptology—ASIACRYPT 2020. Part II*, volume 12492 of *Lecture Notes in Comput. Sci.*, pages 411–439. Springer, Cham, [2020] ©2020.

Otero S. A. and J. A. López Ramos.

Cryptanalysis of a key exchange protocol based on a congruence-simple semiring action.

Journal of Algebra and Its Applications, 0(0):2550229, 2025.

M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, and V. Weger.
Zero knowledge protocols and signatures from the restricted syndrome decoding problem.
In *Public-key cryptography—PKC 2024. Part II*, volume 14602 of *Lecture Notes in Comput. Sci.*, pages 243–274. Springer, Cham, [2024] ©2024.

A. Barenghi, J.-F. Biasse, E. Persichetti, and P. Santini.
On the computational hardness of the code equivalence problem in cryptography.
Adv. Math. Commun., 17(1):23–55, 2023.

C. Battarbee, D. Kahrobaei, and S. F. Shahandashti.
Semidirect product key exchange: the state of play.
J. Algebra Appl., 23(7):Paper No. 2550066, 16, 2024.

G. Brassard and M. Yung.
One-way group actions.
In A. J. Menezes and S. A. Vanstone, editors, *Advances in Cryptology-CRYPTO' 90*, pages 94–107, Berlin, Heidelberg, 1991. Springer Berlin Heidelberg.

J.M. Couveignes.
Hard homogeneous spaces.
Cryptology ePrint Archive, Paper 2006/291, 2006.

W. Diffie and M. E. Hellman.
New directions in cryptography.
IEEE Trans. Inform. Theory, IT-22(6):644–654, 1976.

University of Zurich

L. Ducas and W. van Woerden.
On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography.
In *Advances in cryptology—EUROCRYPT 2022. Part III*, volume 13277 of *Lecture Notes in Comput. Sci.*, pages 643–673. Springer, Cham, [2022] ©2022.

D. Grigoriev and V. Shpilrain.
Tropical cryptography II: extensions by homomorphisms.
Comm. Algebra, 47(10):4224–4229, 2019.

O. W. Gnilke and J. Zumbrägel.
Cryptographic group and semigroup actions.
J. Algebra Appl., 23(7):Paper No. 2530001, 14, 2024.

A. Joux.
MPC in the head for isomorphisms and group actions.
Cryptology ePrint Archive, Paper 2023/664, 2023.

G. Maze.
Algebraic Methods for Constructing One-Way Trapdoor Functions.
PhD thesis, University of Notre Dame, May 2003.
Available at http://www.math.uzh.ch/user/gmaze.

G. Maze, C. Monico, and J. Rosenthal.
A public key cryptosystem based on actions by semigroups.
In *Proceedings of the 2002 IEEE International Symposium on Information Theory*, page 266, Lausanne, Switzerland, 2002.

University of Zurich

G. Maze, C. Monico, and J. Rosenthal.
Public key cryptography based on semigroup actions.
Adv. in Math. of Communications, 1(4):489–507, 2007.
arXiv:cs/0501017.

G. Maze, C. Monico, J. Rosenthal, and J. J. Climent.
Public key cryptography based on simple modules over simple rings.
In D. Gilliam and J. Rosenthal, editors, *Proceedings of the 15-th International Symposium on the Mathematical Theory of Networks and Systems*, University of Notre Dame, August 2002.

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

University of Zurich

Peter W. Shor.
Algorithms for quantum computation: discrete logarithms and factoring.
In *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994)*, pages 124–134. IEEE Comput. Soc. Press, Los Alamitos, CA, 1994.

R. Steinwandt and A. Suárez Corona.
Cryptanalysis of a 2-party key establishment based on a semigroup action problem.
Adv. Math. Commun., 5(1):87–92, 2011.

Jens Zumbrägel.
Classification of finite congruence-simple semirings with zero.
J. Algebra Appl., 7(3):363–377, 2008.