Improved algorithms of post-quantum cryptographic group actions

Valerie Gilchrist

Nov 25, 2025

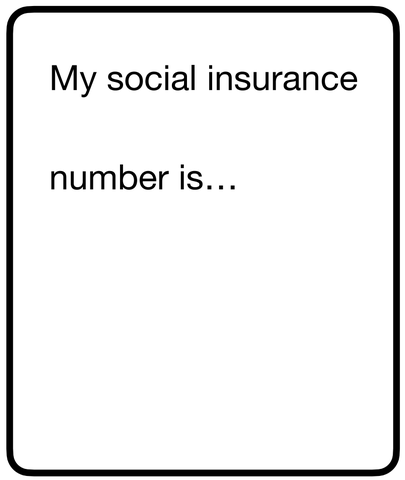
Story time

My social insurance number is…

Story time

My social insurance

number is…



0101001011101010

1111110111010111

1010100011100110

0101001001111010

1010010101101001

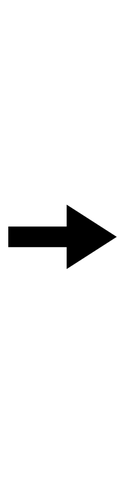
0101001011101010

1111110111010111

1010100011100110

0101001001111010

1010010101101001



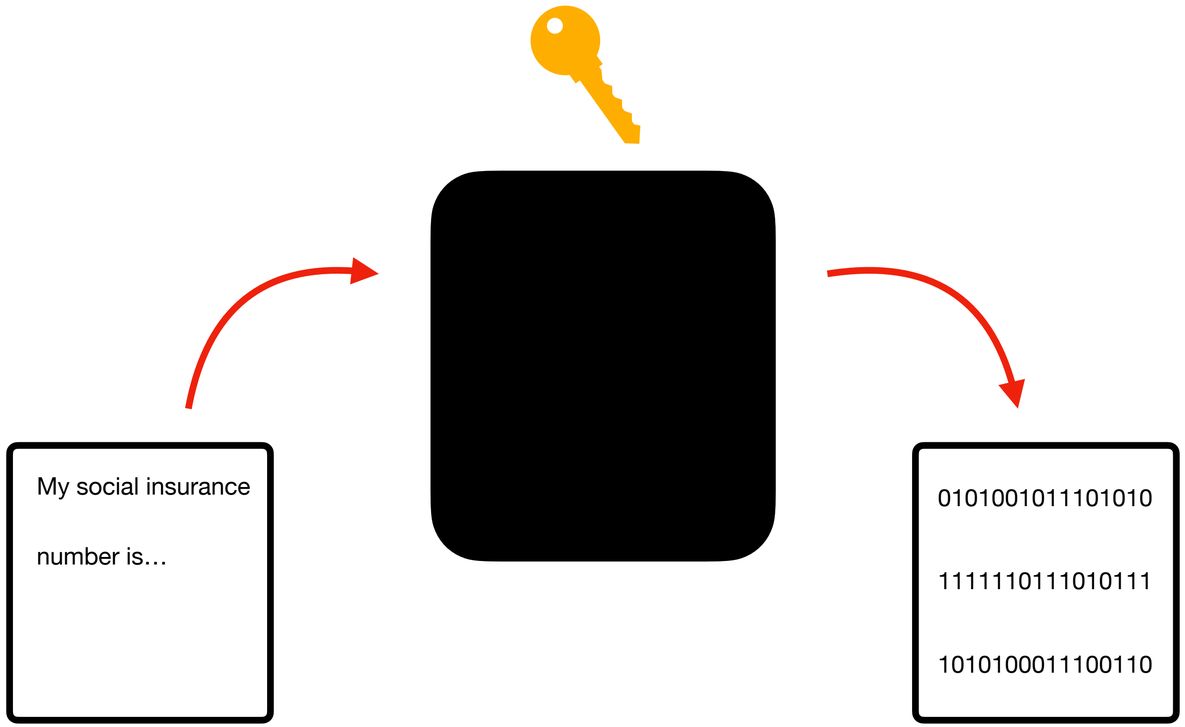
My social insurance

number is…

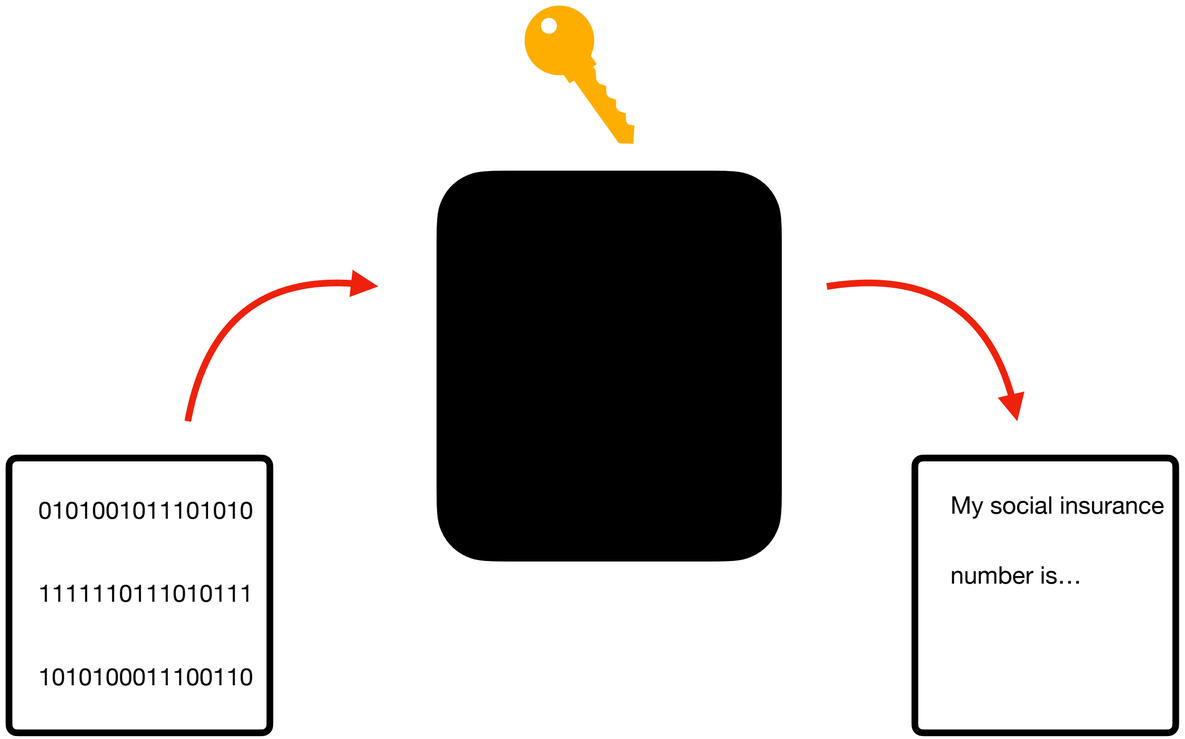
encryption

decryption

How can we encrypt/decrypt?

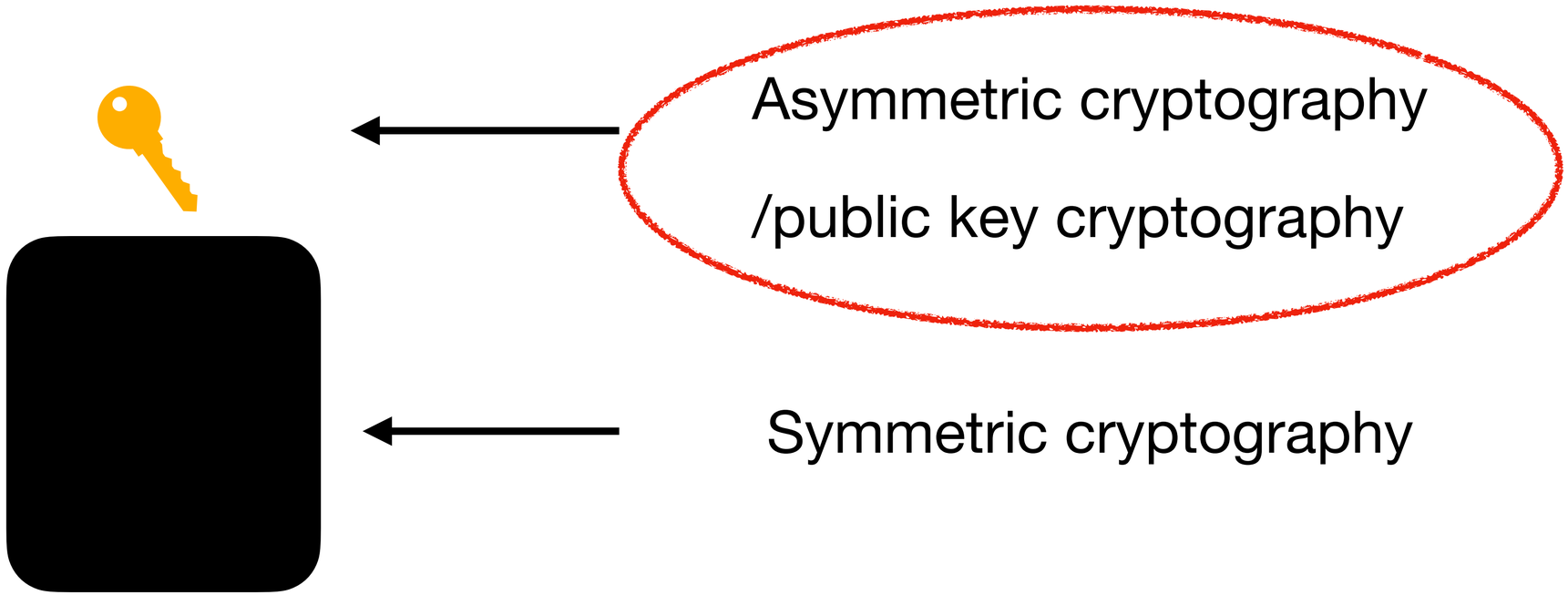


encryption



decryption

How can we encrypt/decrypt?



Diffie-Hellman key exchange

$G = \langle g \rangle$

$g^a \qquad g^b$

$a \in \mathbb{Z}$

g^a

g^b

$(g^b)^a$

$b \in \mathbb{Z}$

g^b

g^a

$(g^a)^b$

Diffie-Hellman key exchange

Discrete Log

Problem : $G = \langle g \rangle$. Given g, g^a, recover a.

Computational Diffie-Hellman

Problem : $G = \langle g \rangle$. Given g, g^a, g^b, recover g^{ab}.

→ hard for computers (and mailmen!)

…NOT HARD for quantum computers

Group actions

Let G be a group and X a set

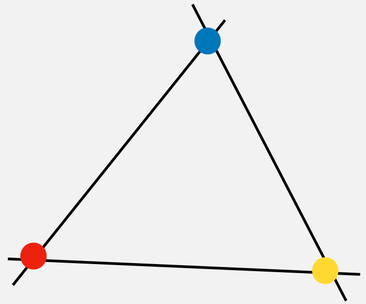
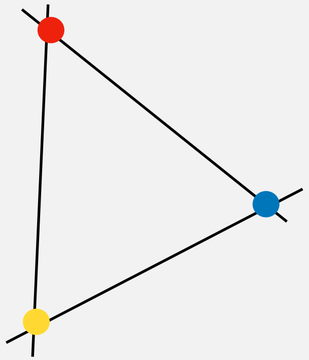
A *group action* is a map $\star : G \times X \to X$ that satisfies

1. *Compatibility :* $\forall g_1, g_2 \in G, x \in X, \quad g_1 \star (g_2 \star x) = g_1 g_2 \star x$

2. *Identity :* $\exists e \in G : \forall x \in X, \quad e \star x = x$

Group actions

e.g. $\star$: (rotations) $\times$ (triangles) $\rightarrow$ (triangles)

$90°$ CW $\star$  $=$ 

-identity: $0°$ CW

-compatibility: $X° \star (Y° \star \triangle) = (X° + Y°) \star \triangle$

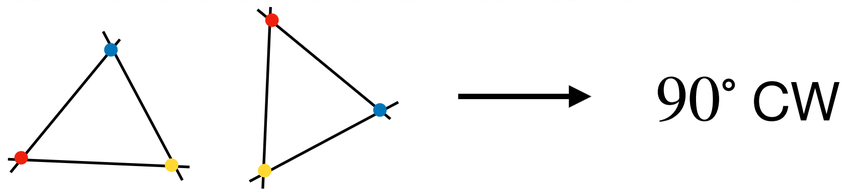
Group actions

Discrete Log

Problem : $G = \langle g \rangle$. Given g, g^a, recover a.

Vectorization

Problem : $(\star , G, X)$. Given $x, g \star x$, recover g.



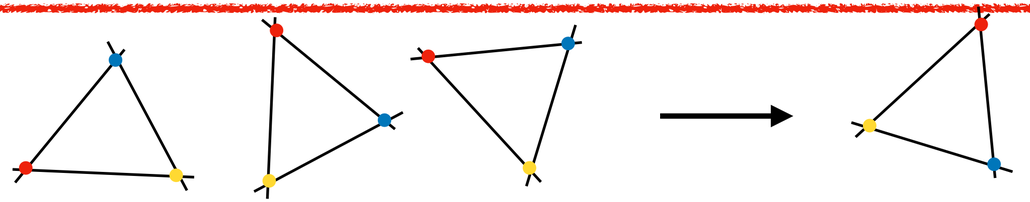
Computational Diffie-Hellman

Problem : $G = \langle g \rangle$. Given g, g^a, g^b, recover g^{ab}.

Parallelization

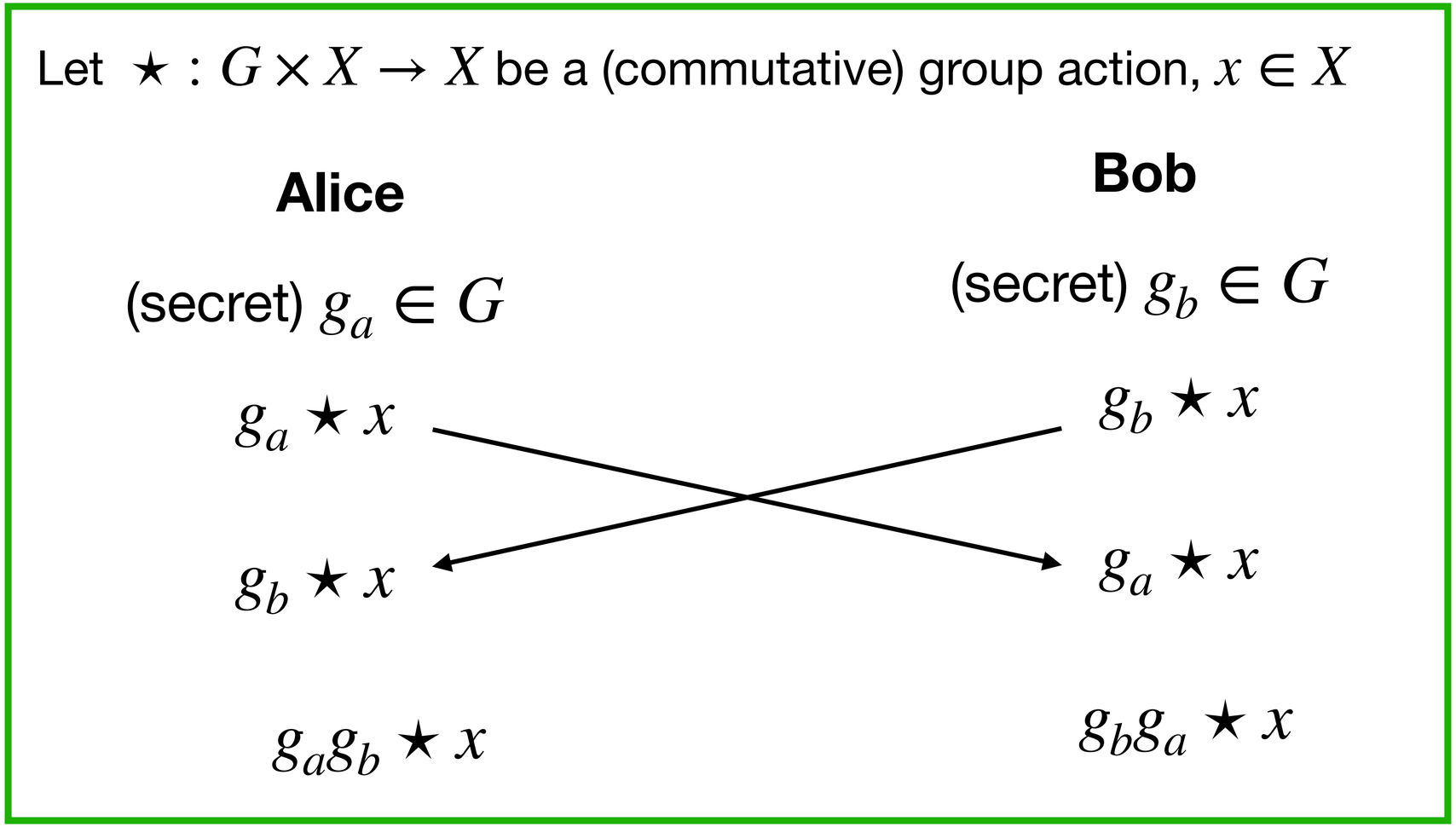
Problem : $(\star , G, X)$.

Given $x, g_A \star x, g_B \star x$, recover $g_A g_B \star x$.

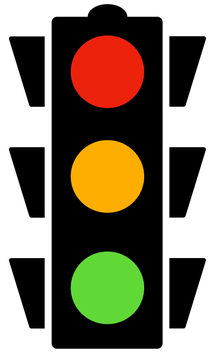


Group actions

Let $\star : G \times X \to X$ be a (commutative) group action, $x \in X$



Contributions



group action + an instance from the literature + our contribution

Contribution 1

[In submission]

On the security of two blind signatures from code equivalence problems

Valerie Gilchrist[1], Laurane Marco[2], Christophe Petit[1,3] and Gang Tang[3]

[1] Université Libre de Bruxelles, Belgium
[2] EPFL, Switzerland
[3] University of Birmingham, United Kingdom

Abstract. The Linear Code Equivalence (LCE) problem and the Matrix Code Equivalence (MCE) problem are two examples of code-based hard problems that have gained attention as candidates for use in post-quantum cryptography. They are straightforward to implement, can be viewed as group actions, and offer a good trade-off between compactness and performance in the realm of post-quantum group actions.

With the community gaining confidence in the security of these problems, new

Linear code group action

An $[n, m]$ linear code $\mathscr{C}$ is an m-dimensional linear subspace of $\mathbb{F}_q^n$

e.g. Consider $\mathbb{F}_{101}^4$

$$\mathscr{C} = \langle [1,0,0,0], [0,1,0,0] \rangle = \{[a, b, 0, 0] : a, b \in \mathbb{F}_{101}\}$$

$$= \{[a \quad b] \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} : [a \quad b] \in \mathbb{F}_{101}^2\}$$

Generator matrix

Linear code group action

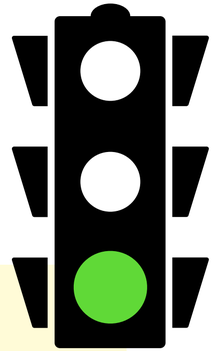
Let G be the generator matrix of a code

e.g. $G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$

For A invertible, D diagonal, P permutation, the following is a group action:

$$(A, DP) \star G = AGDP$$

Linear code group action (contribution 1)



[DKQ+25] Blind Signatures from Cryptographic Group Actions. Duong, Khuc, Qiao, Susilo, Zhang. Eprint 2025.

Problem :

Given generator matrices G_0, G_1, G_2 such that

$$G_0 \xrightarrow{\star\,(A_0, D_0P)} G_1 \xrightarrow{\star\,(A_1, D_1P^{-1})} G_2$$

(D_i diagonal, P permutation), compute P.

-we gave a polynomial time reduction between this problem and pure vectorization

Contribution 2

[In submission]

On the security of two blind signatures from code equivalence problems

Valerie Gilchrist[1], Laurane Marco[2], Christophe Petit[1,3] and Gang Tang[3]

[1] Université Libre de Bruxelles, Belgium
[2] EPFL, Switzerland
[3] University of Birmingham, United Kingdom

Abstract. The Linear Code Equivalence (LCE) problem and the Matrix Code Equivalence (MCE) problem are two examples of code-based hard problems that have gained attention as candidates for use in post-quantum cryptography. They are straightforward to implement, can be viewed as group actions, and offer a good trade-off between compactness and performance in the realm of post-quantum group actions.

With the community gaining confidence in the security of these problems, new

Matrix code group action

A $[m \times n, k]$ *matrix code* $\mathscr{C}$ is a k-dimensional $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{m \times n}$

e.g. Consider $\mathbb{F}_{101}^{2\times 2}$

$$\mathscr{C} = \langle \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \rangle = \{ \begin{bmatrix} a & b \\ b & 0 \end{bmatrix} : a, b \in \mathbb{F}_{101} \}$$

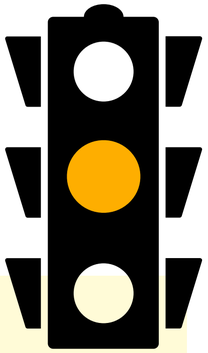
$$A\mathscr{C} = \{A \begin{bmatrix} a & b \\ b & 0 \end{bmatrix} : a, b \in \mathbb{F}_{101} \}, \qquad \mathscr{C}B = \{ \begin{bmatrix} a & b \\ b & 0 \end{bmatrix} B : a, b \in \mathbb{F}_{101} \}$$

Matrix code group action

Let A, B be invertible, then the following is a group action:

$$(A, B) \star \mathscr{C} = A\mathscr{C}B$$

Matrix code group action (contribution 2)



[KLP25] Post-Quantum Blind Signatures from Matrix Code Equivalence. Kuchta, LeGrow, Persichetti. Eprint 2025.

Problem : Given matrix codes $\mathscr{C}_0, \mathscr{C}_1, \mathscr{C}_2,$ such that

$$\mathscr{C}_2 \xleftarrow{\star\,(A^{-1}, B^{-1})} \mathscr{C}_0 \xrightarrow{\star\,(A, B)} \mathscr{C}_1$$

for A, B (anti)symmetric matrices… compute A, B.

$$\mathscr{D}_2 \xleftarrow{\star\,(A^{-1}, B^{-1})} \mathscr{D}_0 \xrightarrow{\star\,(A, B)} \mathscr{D}_1$$

-we showed that repeating the same secret key even once would leak the secret

Contribution 3

[CRYPTO 2024]

Solving the Tensor Isomorphism Problem for special orbits with low rank points: Cryptanalysis and repair of an Asiacrypt 2023 commitment scheme

Valerie Gilchrist[1], Laurane Marco[2], Christophe Petit[13], Gang Tang[43]

[1] Université Libre de Bruxelles, Brussels, Belgium
[2] EPFL, Lausanne, Switzerland
[3] University of Birmingham, Birmingham, United Kingdom
[4] University of Technology Sydney, NSW, Australia

Abstract. The Tensor Isomorphism Problem (TIP) has been shown equivalent to the matrix code equivalence problem, making it an interesting candidate on which to build post-quantum cryptographic primitives. These hard problems have already been used in protocol development. One of these, MEDS, is currently in Round 1 of NIST's call for additional

Tensor group action

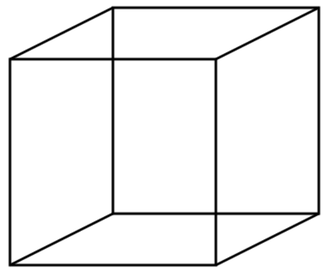
We would like to compute the tensor $\mathbf{u} \otimes \mathbf{v} \otimes \mathbf{w}$ where $\mathbf{u} = [u_1, u_2], \mathbf{v} = [v_1, v_2], \mathbf{w} = [w_1, w_2]$.

We proceed by first expanding the matrix $\mathbf{v} \cdot \mathbf{w}^T$:

$$\mathbf{v} \cdot \mathbf{w}^T = \begin{bmatrix} v_1 w_1 & v_1 w_2 \\ v_2 w_1 & v_2 w_2 \end{bmatrix}$$

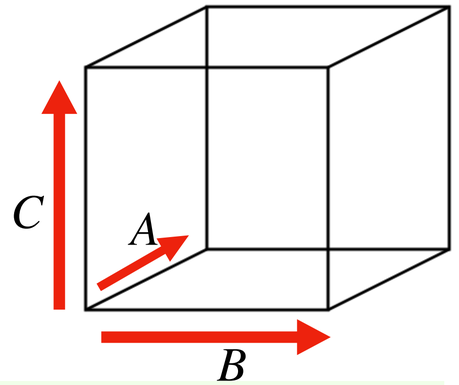
Now we multiply this matrix by each entry of $\mathbf{u}$, storing them in a list as we go:

$$u_1 \begin{bmatrix} v_1 w_1 & v_1 w_2 \\ v_2 w_1 & v_2 w_2 \end{bmatrix}, u_2 \begin{bmatrix} v_1 w_1 & v_1 w_2 \\ v_2 w_1 & v_2 w_2 \end{bmatrix}$$



Tensor group action

Let $\mathbf{V}$ be the tensor space $\sum_i u_i \otimes v_i \otimes w_i = \sum_{ijl} v(i,j,l) e_i \otimes e_j \otimes e_l$



Then the following is a group action :

$$(A,B,C) \star \sum_{i,j,l=1}^{k,m,n} v(i,j,l) e_i \otimes e_j \otimes e_l = \sum_{i,j,l=1}^{k,m,n} v(i,j,l) A e_i \otimes B e_j \otimes C e_l$$

Tensor group action

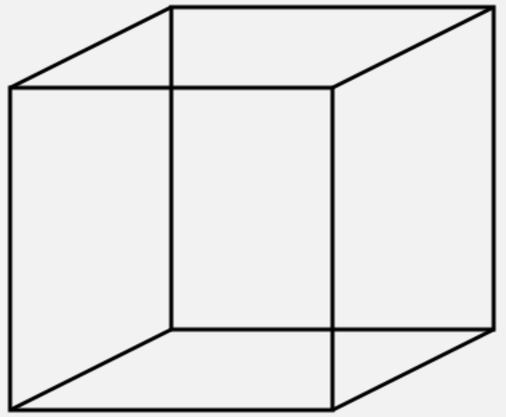
An example over $\mathbb{F}_7$:

$$t = \sum_{i,j,k} e_i \otimes e_j \otimes e_k = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \qquad A = \begin{bmatrix} 6 & 3 & 6 \\ 5 & 6 & 3 \\ 4 & 4 & 4 \end{bmatrix}$$

$$(A, I, I) \star t := \sum_{i,j,k} Ae_i \otimes e_j \otimes e_k = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 5 & 5 & 5 \\ 5 & 5 & 5 \\ 5 & 5 & 5 \end{bmatrix},$$

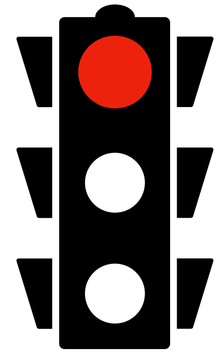
$$(I, A, I) \star t := \sum_{i,j,k} e_i \otimes Ae_j \otimes e_k = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 5 & 5 & 5 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 5 & 5 & 5 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 5 & 5 & 5 \end{bmatrix},$$

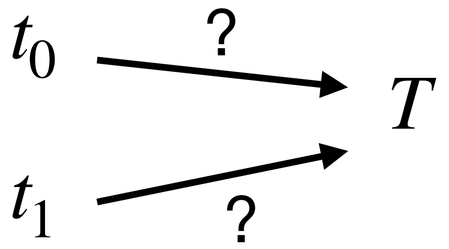
$$(I, I, A) \star t := \sum_{i,j,k} e_i \otimes e_j \otimes Ae_k = \begin{bmatrix} 1 & 0 & 5 \\ 1 & 0 & 5 \\ 1 & 0 & 5 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 5 \\ 1 & 0 & 5 \\ 1 & 0 & 5 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 5 \\ 1 & 0 & 5 \\ 1 & 0 & 5 \end{bmatrix},$$



Tensor group action (contribution 3)

[DFG23] Non-Interactive Commitment from Non-Transitive Group Actions. D'Alconzo, Flamini, Gangemi. Asiacrypt 2023.





Problem :

Let $t_0 = \begin{bmatrix}1&0&0\\0&0&0\\0&0&0\end{bmatrix}, \begin{bmatrix}0&0&0\\0&1&0\\0&0&0\end{bmatrix}, \begin{bmatrix}0&0&0\\0&0&0\\0&0&1\end{bmatrix}$

$t_1 = \begin{bmatrix}1&0&0\\0&0&0\\0&0&0\end{bmatrix}, \begin{bmatrix}0&0&0\\0&1&0\\0&0&0\end{bmatrix}, \begin{bmatrix}0&0&0\\0&0&0\\0&0&0\end{bmatrix}$

Given $(A, B, C) \star t_b$ where $b \in \{0,1\}$,

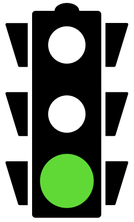
recover b.

-we gave a polynomial time attack

that recovers b

-we showed how to recover

A, B, C

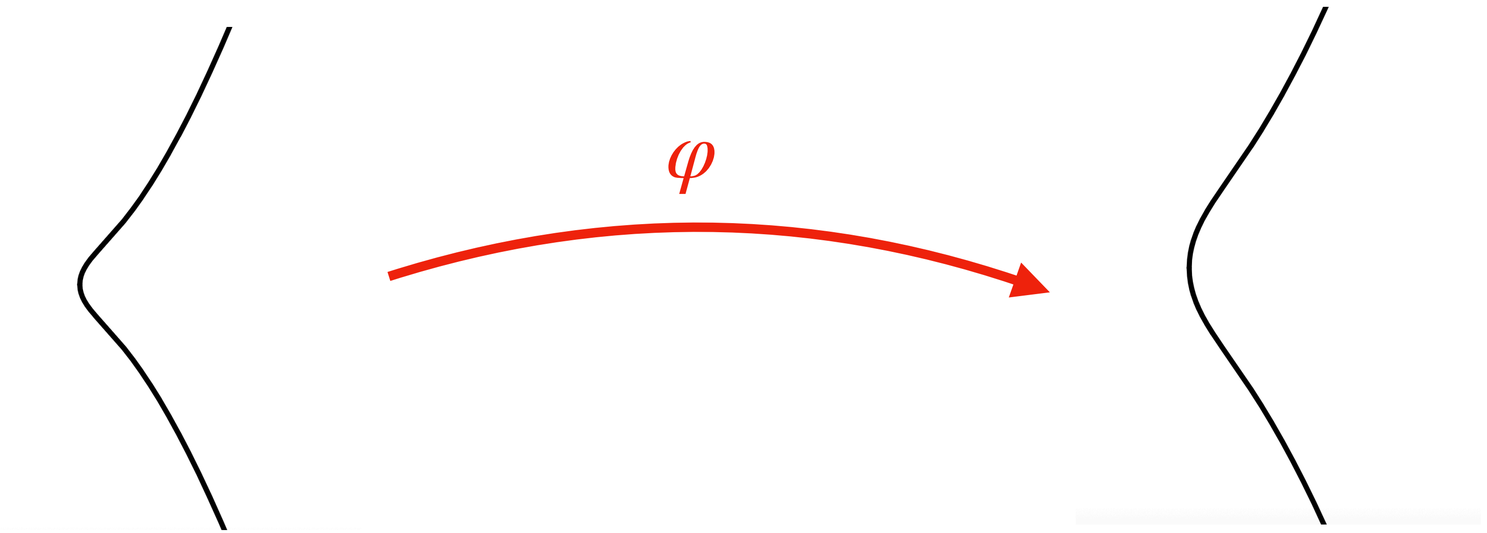


-we offered a repair to the scheme

and described a compatible ZKP

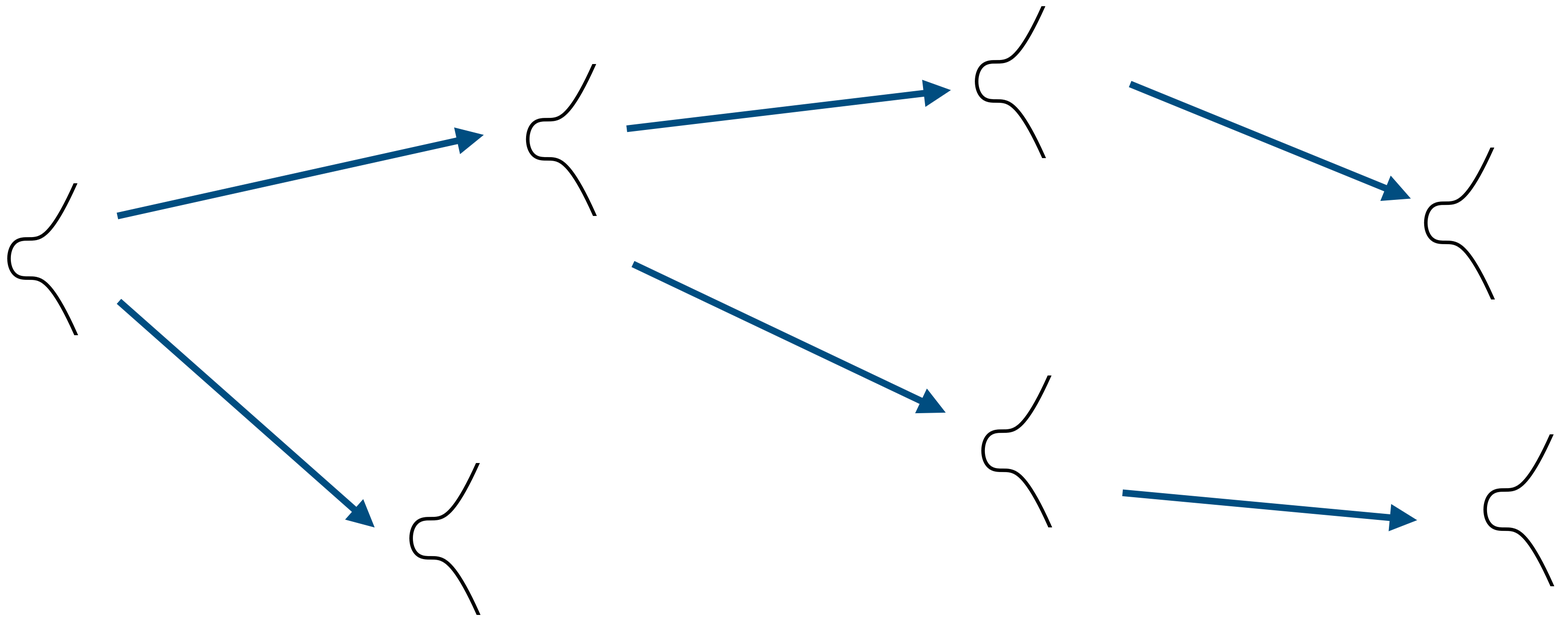
Isogeny group action

An isogeny $\varphi : E \to E'$ is a non-constant rational map between two elliptic curves



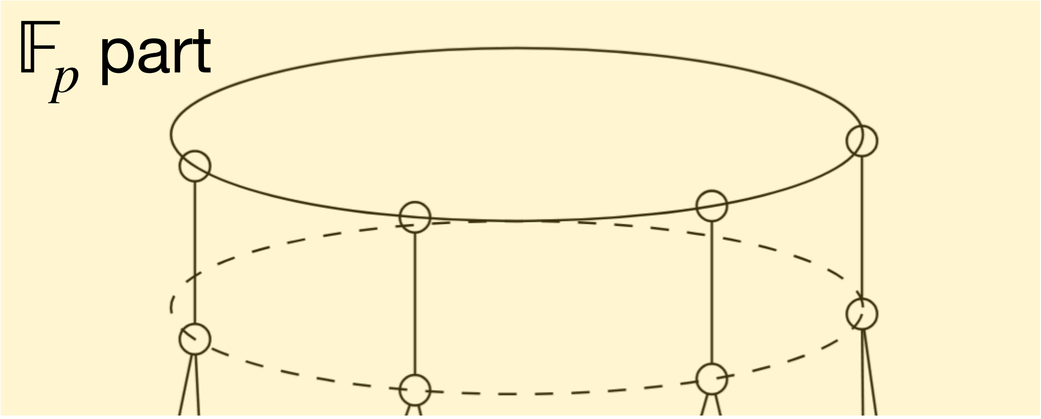
Isogeny group action

An "ℓ-isogeny" = an isogeny of degree ℓ



Vertices = elliptic curves, edges = ℓ-isogenies

Isogeny group action



—restrict to isogenies of degree ℓ

—over $\mathbb{F}_p$ we get an isogeny **volcano**

—over $\mathbb{F}_{p^k}, k > 1$ only *some* graphs will be volcanoes (ordinary curves)

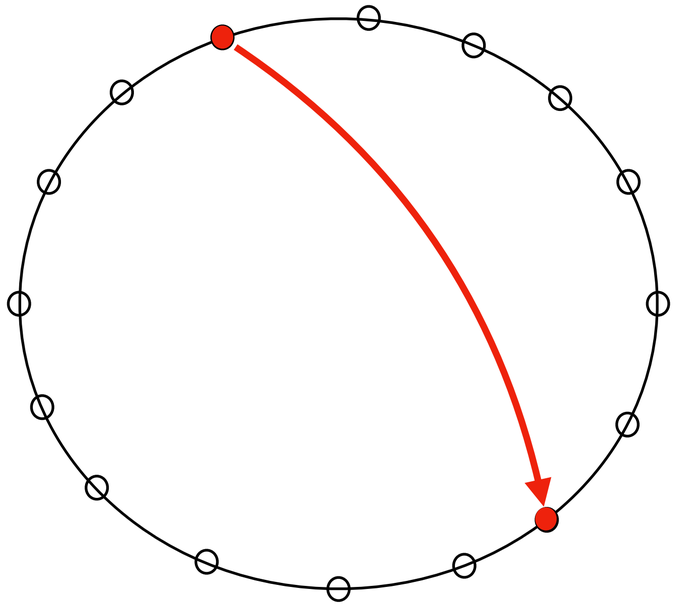
Isogeny group action

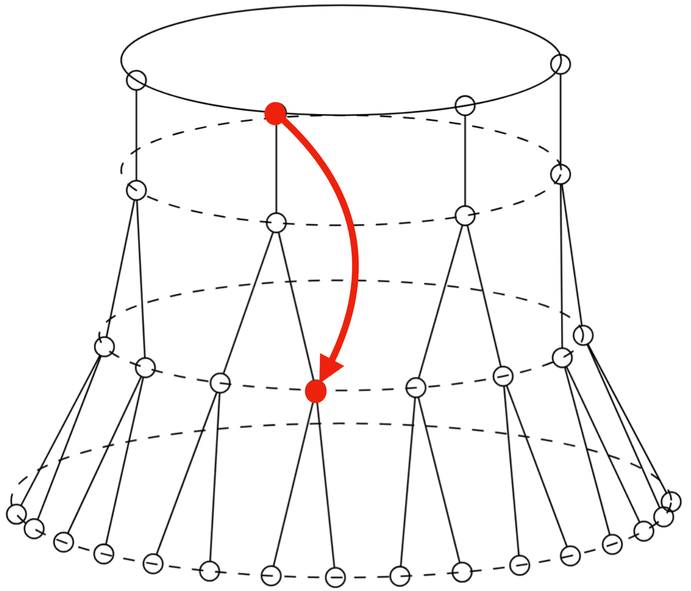
Supersingular graph

[image by Craig Costello]

Isogeny group action

$\star$: “walks” in the graph $\times$ (some particular) elliptic curves $\longrightarrow$ (some particular) elliptic curves





Contribution 4

[In submission]

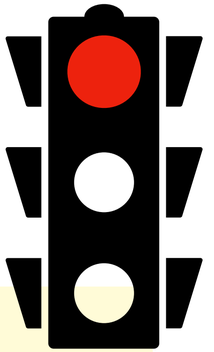
Another Look at the Quantum Security of the Vectorization Problem with Shifted Inputs

Paul Frixons[1], Valerie Gilchrist[1], Péter Kutas[2,3], Simon-Philipp Merz[4], Christophe Petit[1,3], Lam L. Pham[5]

[1] Université Libre de Bruxelles, Belgium
[2] Eötvös Loránd University, Hungary
[3] University of Birmingham, United Kingdom
[4] ETH Zürich, Switzerland
[5] Ghent University, Belgium

Abstract. Cryptographic group actions provide a basis for simple post-quantum generalizations of many cryptographic protocols based on the discrete logarithm problem (DLP). However, many advanced group action-based protocols do not solely rely on the core group action problem (the so-called vectorization problem), but also on *variants* of this problem, to either improve efficiency or enable new functionalities. For example, the security of the CSI-SharK threshold signature protocol relies on the hardness of the *Vectorization Problem with Shifted Inputs* where (in DLP

Isogeny group action (contribution 4)



[ABCP23] CSI-SharK: CSI-FiSh with Sharing-friendly Keys. Atapoor, Baghery, Cozzo, Pedersen. ACISP 2023.

Problem :

$$E_0 \xrightarrow{\star\, \mathfrak{g}^z} E_1 \xrightarrow{\star\, \mathfrak{g}^z} E_2 \xrightarrow{\star\, \mathfrak{g}^z} E_3 \cdots \xrightarrow{\star\, \mathfrak{g}^z} E_M$$

compute z.

-we presented the quantum algorithm from Childs and van Dam for use in cryptography and used it to analyze the security of this problem

-we specialized relevant subroutines in order to obtain a concrete security estimate

-this approach improved upon the state-of-the-art (Kuperberg on one instance)

Contribution 5

[Latincrypt 2025]

Improved algorithms for ascending isogeny volcanoes, and applications

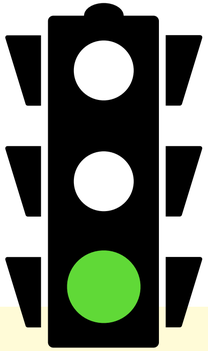
Steven D. Galbraith[1], Valerie Gilchrist[2], Damien Robert[3]

[1] University of Auckland, Auckland, New Zealand
[2] Université Libre de Bruxelles, Brussels, Belgium
[3] Inria Bordeaux, Institut de Mathématiques de Bordeaux, France

Abstract. Given two elliptic curves over $\mathbb{F}_q$, computing an isogeny mapping one to the other is conjectured to be classically and quantumly hard. This problem plays an important role in the security of elliptic curve cryptography. In 2024, Galbraith applied recently developed techniques for isogenies to improve the state-of-the-art for this problem.

In this work, we focus on computing ascending isogenies with respect to an orientation. Our results apply to both ordinary and supersingular curves. We give a simplified framework for computing self-pairings, and show how they can be used to improve upon the approach from

Isogeny group action (contribution 5)



Problem :

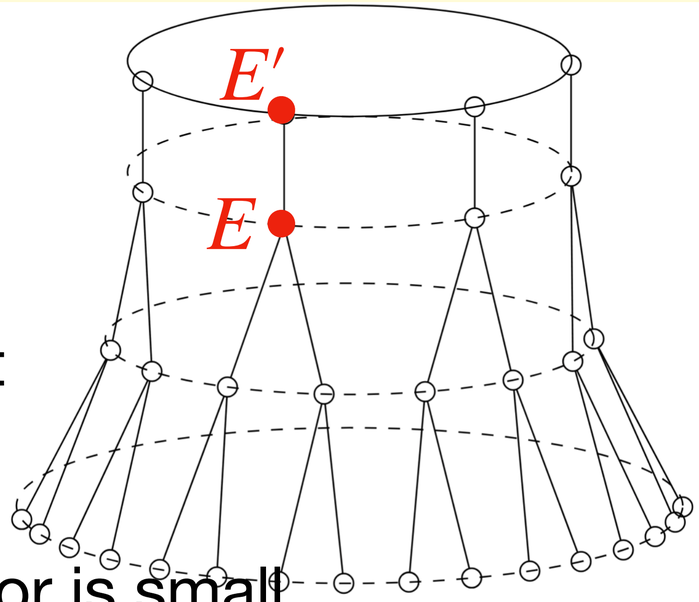
Given $E, E' = \mathfrak{a} \star E$, where $\mathfrak{a}$ corresponds to a vertical isogeny of known degree,

compute $\mathfrak{a}$.

-we considered special cases of the worst case of this problem

-we removed a heuristic assumption from the state-of-the-art when the conductor is large

-we gave an improved complexity analysis when the conductor is small



Contribution 6

[Latincrypt 2023]

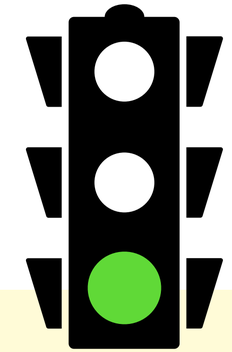
Fast and Frobenius: Rational Isogeny Evaluation over Finite Fields

Gustavo Banegas[1], Valerie Gilchrist[2], Anaëlle Le Dévéhat[3], Benjamin Smith[3]

[1] Qualcomm France SARL, Valbonne, France
[2] Université Libre de Bruxelles and FRIA, Brussels, Belgium
[3] Inria and Laboratoire d'Informatique de l'École polytechnique, Institut Polytechnique de Paris, Palaiseau, France

Abstract. Consider the problem of efficiently evaluating isogenies $\phi : \mathcal{E} \to \mathcal{E}/H$ of elliptic curves over a finite field $\mathbb{F}_q$, where the kernel $H = \langle G \rangle$ is a cyclic group of odd (prime) order: given $\mathcal{E}$, G, and a point (or several points) P on $\mathcal{E}$, we want to compute $\phi(P)$. This problem is at the heart of efficient implementations of group-action- and isogeny-based post-quantum cryptosystems such as CSIDH. Algorithms based on Vélu's formulæ give an efficient solution when the kernel generator G is defined over $\mathbb{F}_q$, but for general isogenies G is only defined over some extension $\mathbb{F}_{q^k}$, even though $\langle G \rangle$ as a whole (and thus ϕ) is defined over the base field $\mathbb{F}_q$; and the performance of Vélu-style algorithms degrades rapidly as k grows. In this article we revisit isogeny evaluation with a special

Isogeny group action (contribution 6)



Problem :

Given E and a kernel generator G (possibly defined over an extension field),

evaluate the isogeny $\phi : E \to E'$ with kernel $\langle G \rangle$ on some point P.

-we describe an algorithm for computing the kernel polynomial of ϕ

that improves upon the number of arithmetic operations necessary

-we show how to achieve further savings when G is defined over some field

extension up to degree 12 using the Frobenius map

Contribution 7

[Mathcrypt 2022]

Efficient supersingularity testing over $\mathbb{F}_p$ and CSIDH key validation

Gustavo Banegas[1], Valerie Gilchrist[2,1,*], Benjamin Smith[1]

[1]Inria and Laboratoire d'Informatique de l'École polytechnique, Institut Polytechnique de Paris, Palaiseau, France
[2]University of Waterloo, Canada

Abstract *Many public-key cryptographic protocols, notably non-interactive key exchange (NIKE), require incoming public keys to be validated to mitigate some adaptive attacks. In CSIDH, an isogeny-based post-quantum NIKE, a key is deemed legitimate if the given Montgomery coefficient specifies a supersingular elliptic curve over the prime field. In this work, we survey the current supersingularity tests used for CSIDH key validation, and implement and measure two new alternative algorithms. Our implementation shows that we can determine supersingularity substantially faster, and using less memory, than the state-of-the-art.*

Keywords: Isogenies, Key validation, Supersingularity, Elliptic Curves

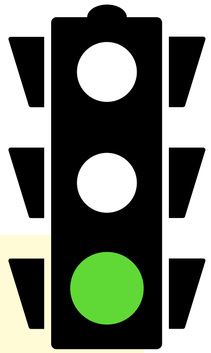
1 INTRODUCTION

The security of many public-key cryptosystems assumes that public keys are honestly generated: that is, that public keys have not been manipulated by adversaries. *Key validation* is the process of determining whether an incoming public key was plausibly constructed following the protocol.

The simplest example of this is in non-interactive key exchange (NIKE). Consider classic static Diffie–Hellman in a finite field: the system parameters fix a prime modulus p and a generator g in $\mathbb{F}_p$ for a subgroup $G = \langle g \rangle \subset \mathbb{F}_p^\times$ of prime order r. Alice samples a long-term secret integer a, and binds to the corresponding public key $A = g^a$. An honest Bob computes his keypair $(B = g^b, b)$, and the shared secret is $S = A^b = B^a$. However, if G is a proper subgroup of $\mathbb{F}_p^\times$, then a dishonest Bob can choose some h in $\mathbb{F}_p^\times \setminus G$, of order $s \mid (p-1)/r$, and transmit the malformed public key $B' = B \cdot h$. The shared secret as computed by Alice is now $S' = (B')^a = S \cdot h^a$, while Bob derives the original $S = A^b$. The success or failure of subsequent encrypted communication tells Bob whether $S = S'$, and hence whether a is $0 \pmod{s}$.

To avoid leaking information on her long-term private key to adaptive adversaries, then, Alice must validate incoming public keys as being honestly generated. In the example above, this amounts to checking that Bob's

Isogeny group action (contribution 7)



Problem :

Given an elliptic curve E decide whether E is supersingular or ordinary

-we presented two algorithms from the literature for use in cryptography

-we improved upon these algorithms to give improvements over the state-of-the-art from CSIDH for the cases when E is *expected* to be supersingular or ordinary

Conclusion

Improved algorithms of post-quantum cryptographic group actions