Isogeny-based PAKE protocols

Sabrina Kunzweiler
Inria, Institut de Mathématiques Bordeaux

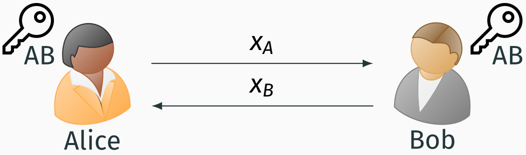
December 08, 2023

joint work with Michel Abdalla, Thorsten Eisenhofer, Eike Kiltz and Doreen Riepel

Password-Authenticated Key Exchange

Public key exchange

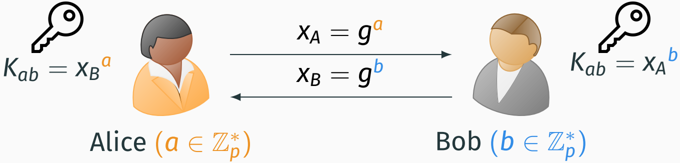
Idea: Alice and Bob want to create a secure session key.
They can only communicate over a public channel.



- Everyone can read the messages x_A, x_B.
- Only Alice and Bob can compute the shared key K_{AB}.

Example: Diffie-Hellman key exchange

Setup: $(\mathbb{G}, \cdot)$ is a group of prime order p, and g a generator of $\mathbb{G}$.

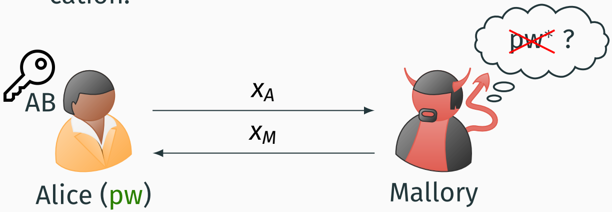


Cryptographic assumptions:
The following problems are assumed to be hard.

- **DLOG** Given x_A, g, find a.
- **CDH** Given g, x_A, x_B, find K_{ab}.

Password-Authenticated Key Exchange (PAKE)

Alice and Bob share a password.
They want to use the password for authentication.



Properties:

- Passwords are small `1234`.
- Keys are large `t3Bas51z5eeuWJITma6B45Vo`.

Security requirements:

- Provide authentication.
- Survive online attacks.
- Prevent offline dictionary attacks.

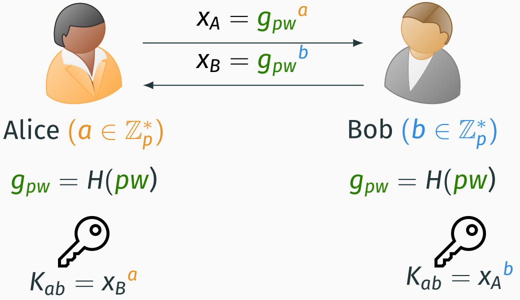
Example: SPEKE

Simple **P**assword **E**xponential **K**ey **E**xchange Protocol by Jablon ’96

$(\mathbb{G}, \cdot)$ group of prime order p

$\mathcal{PW}$ password space $\subset \{0,1\}^*$

H hash function $\{0,1\}^* \to \mathbb{G} \setminus \{id\}$

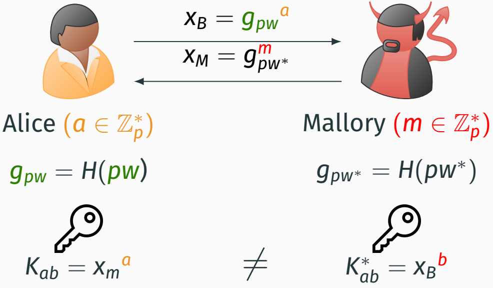


[0]This description is simplified. The key should be $H'(A, B, x_A, x_B, K_{AB})$. We ignore this technicality in the talk.

Security of SPEKE:

What happens if Mallory  participates in the protocol?

- **Online attack:** Best attack is to guess a password pw^*.
- **Dictionary attack:** An attacker cannot test different passwords in an offline phase.
  Testing pw** requires solving DLOG$(g_{pw^{**}}, g_{pw^*})$.



This work: Can SPEKE be generalized to isogeny-based group actions?

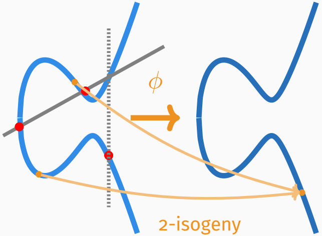
Isogeny-based Group Actions

Elliptic Curves

An **Elliptic Curve** E over $\mathbb{F}_{p^k}$ is defined by an equation

$$E : y^2 = x^3 + ax + b,$$

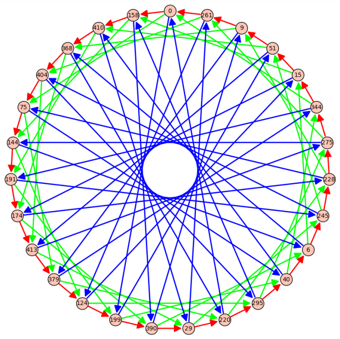
where $4a^3 + 27b^2 \neq 0$.



- Points of E form an additive group.

  $\Rightarrow$ This group is used in the Diffie-Hellman protocol from before.
- An **isogeny** is a non-zero group homomorphism between elliptic curves $\phi : E \to E'$.
- For $p \nmid \ell$, an **ℓ-isogeny** is an isogeny with $\ker(\phi) \equiv \mathbb{Z}/\ell\mathbb{Z}$.

CSIDH [CLMPR, AsiaCrypt'18] Isogeny Graph



Isogeny Graph over $\mathbb{F}_{419}$ with 3-, 5-, and 7- isogenies.

Vertices: supersingular elliptic curves over $\mathbb{F}_p$

- cardinality: $O(\sqrt{p})$
- labeled by Montgomery coefficient A
  $\Rightarrow E_A : y^2 = x^3 + Ax^2 + x$

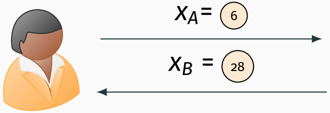
Edges: ℓ_i-isogenies for different small primes $\ell_1, \dots, \ell_n$

- 2-regular for each ℓ_i
- directed graph
- *dual isogenies* allow to go back

Commutative Supersingular Isogeny Diffie-Hellman (CSIDH)

Key Idea: Alice and Bob take secret walks on the isogeny graphs.
They only exchange the end vertices.

An example with $p = 59$. The starting vertex is fixed to 0.



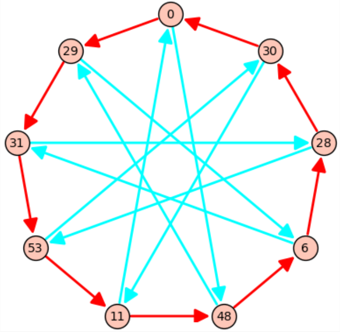
Alice: $\boxed{a = (2, -1)}$

$\Rightarrow x_A = 6$

Bob: $\boxed{b = (-1, -2)}$

$\Rightarrow x_B = 28$

$K_{ab} = 11$



Graph with 3- and 5- isogenies.

Abstract view on CSIDH: Cryptographic group actions [ADMP, AsiaCrypt '20].

Group Action

A map $\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$, with $\mathcal{G}$ a group and $\mathcal{X}$ a set, is a group action if:

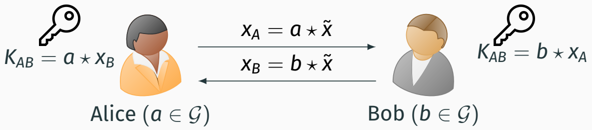
1. $id \star x = x$ for all $x \in \mathcal{X}$ (identity),
2. $(g \circ h) \star x = g \star (h \star x)$ for all $g, h \in \mathcal{G}$, $x \in \mathcal{X}$ (compatibility).

Cryptographic assumptions

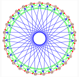
$\mathcal{G}$ is commutative and the following problems are required to be hard.

- **DLOG** Given $x, y \in \mathcal{X}$, find $g \in \mathcal{G}$ with $y = g \star x$.
- **CDH** Given $x, y, z \in \mathcal{X}$, determine $w \in \mathcal{X}$ so that $w = \text{DLOG}(x, y) \star z$.

Diffie Hellman key exchange with group actions



Examples and special properties



Classical Diffie-Hellman

- $\mathcal{X} = \mathbb{G}$, a group of order p.
- $\mathcal{G} = (\mathbb{Z}/p\mathbb{Z})^*$.
- $\star$: exponentiation $(g, x) \mapsto x^g$.

CSIDH

- $\mathcal{X}$: vertices in the isogeny graph
- $\mathcal{G}$: exponent vectors
- $\star$: taking paths in the graph

- Given x^{g_1}, x^{g_2}, we can compute $x^{g_1+g_2} = x^{g_1} \cdot x^{g_2}$.

  quantum poly-time attack (Shor)

- No group structure on $\mathcal{X}$.

  best-known quantum attack is subexponential (Kuperberg)

- "Twisting" is believed to be hard.

- Twisting: Given $y = g \star \tilde{x}$, we can compute $\texttt{twist}(y) = g^{-1} \star \tilde{x}$ (here: $\tilde{x}$ is $E_0 : y^2 = x^3 + x$)

Translating SPEKE to group actions

How not to create a CSIDH-PAKE

Most currently used PAKE protocols are based on (classical) Diffie-Hellman key exchange. But the translation to the CSIDH group action has shown to be difficult.

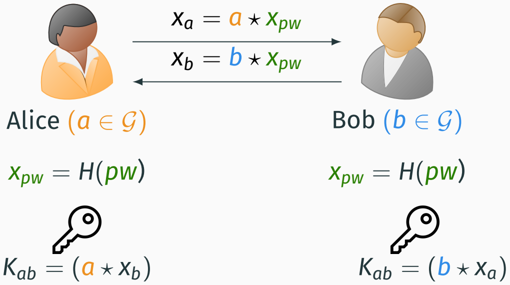
Table 1. Survey of Diffie-Hellman-based PAKEs schemes and their translation to isogeny-based problems

DH PAKE	Safe for Isogenies?	Comment
EKE [5]	×	Public keys are distinguishable from random bitstrings
SPEKE [30]	?	Hashing to a public key is difficult
Dragonfly [27]		
PAK [8]	×	Public keys are not commutative to achieve vanishing effect
J-PAKE [26]		

Figure 1: "How not to create an Isogeny-Based PAKE (AJKLST, ACNS'20)

A "literal" translation of SPEKE to group actions (GA-PAKE-0)

$(\mathcal{G}, \mathcal{X}, \star)$ cryptographic group action
$\mathcal{PW}$ password space $\subset \{0,1\}^*$
H hash function $\{0,1\}^* \to \mathcal{X}$



Two problems when $(\mathcal{G}, \mathcal{X}, \star)$ is the CSIDH group action:

- ✗ We need a secure hash function $H : \{0,1\}^* \to \mathcal{X}$.
  - This is an open problem (Failing to hash into supersingular isogeny graphs, BBDFG**K**MPSSTVVWZ, Eprint '22)
- ✗ The twisiting property makes the protocol insecure.

Problem 1: Secure hash function

Possible attempt

It is easy to define a hash function into the group

$$H' : \{0,1\}^* \to \mathcal{G}, \quad \mathsf{pw} \mapsto g_{\mathsf{pw}}.$$

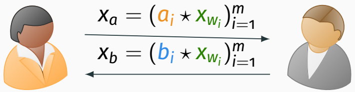
Then define

$$H : \{0,1\}^* \to \mathcal{X}, \quad \mathsf{pw} \mapsto g_{\mathsf{pw}} \star \tilde{x}.$$

- ✗ This hash function is not considered secure.
  Here, secure means no information about the DLOG of an element.
- ⚠ There is an **offline dictionary attack** against the resulting PAKE protocol.
  Note: This kind of hash function can also not be used in the classical SPEKE protocol.

Solution to Problem 1 (GA-PAKE-1)

Idea: Replace the hash function by a bit-by-bit approach
We fix two element $x_0, x_1 \in \mathcal{X}$ (crs), and $\mathcal{PW} = \{0,1\}^m$.



$x_a = (a_i \star x_{w_i})_{i=1}^m$

$x_b = (b_i \star x_{w_i})_{i=1}^m$

Alice $(a_1, \ldots, a_m \in \mathcal{G})$ Bob $(b_1, \ldots, b_m \in \mathcal{G})$

$pw = (w_1, \ldots, w_m)$ $pw = (w_1, \ldots, w_m)$

$K_{ab} = ((a_i \star x_{b,i})_{i=1}^m)$ $K_{ab} = ((b_i \star x_{a,i})_{i=1}^m)$

Security

- ✓ Security against passive adversaries can be reduced to (strong) CDH.
- ✗ This does not solve Problem 2 (twisting) yet!

Problem 2: Twists in CSIDH

There is an offline dictionary attack against both GA-SPEKE-0 (also applies to GA-SPEKE-1).

$$x_a = a \star x_{pw} \longrightarrow$$

$$\longleftarrow x_m = m \star x_a^t$$

Alice ($a \in \mathcal{G}$)

Mallory ($m \in \mathcal{G}$)

$$x_{pw} = H(pw)$$

$$x_a^t = \texttt{twist}(x_a)$$

$$K_{ab} = a \star x_m = (a \cdot m \cdot a^{-1}) \star x_{pw}^t$$

$$K_{ab} = ?$$

$$\boxed{K_{ab} = m \star {x_{pw}}^t}$$

After this execution of the protocol, Mallory can test all passwords pw $\in \mathcal{PW}$ until finding the correct session key K_{ab}.

First solution to problem 2: Com-GA-PAKE

Com = Commitment: Bob cannot choose x_B depending on the Alice's message.

Alice

$(a_1, \ldots, a_m \in \mathcal{G})$

$pw = (w_1, \ldots, w_m)$

$$\xleftarrow{\hspace{2em}\texttt{com}\hspace{2em}}$$

$$\xrightarrow{\hspace{1em}x_a = (a_i \star x_{w_i})_{i=1}^{m}\hspace{1em}}$$

$$\xleftarrow{\hspace{1em}x_b = (b_i \star x_{w_i})_{i=1}^{m}\hspace{1em}}$$

Bob

$(b_1, \ldots, b_m \in \mathcal{G})$

$pw = (w_1, \ldots, w_m)$

$\boxed{\texttt{com} = H(x_b)}$

$\boxed{\text{if } \texttt{com} = H(x_b)\text{:}}$

$K_{ab} = ((a_i \star x_{b,i})_{i=1}^{m})$

$K_{ab} = ((b_i \star x_{a,i})_{i=1}^{m})$

Second solution to problem 2: X-GA-PAKE

X = **Cross-Terms:** An adversary can compute only 2 of 3 possible cross-terms.

$$x_a = (a_i \star x_{w_i})_{i=1}^m$$
$$\hat{x}_a = (\hat{a}_i \star x_{w_i})_{i=1}^m$$

$$\xrightarrow{\hspace{6em}}$$

$$x_b = (b_i \star x_{w_i})_{i=1}^m$$
$$\hat{x}_b = (\hat{b}_i \star x_{w_i})_{i=1}^m$$

$$\xleftarrow{\hspace{6em}}$$

Alice

$$\begin{pmatrix} a_1, \ldots, a_m, & \\ \hat{a}_1, \ldots, \hat{a}_m & \in \mathcal{G} \end{pmatrix}$$

$$pw = (w_1, \ldots, w_m)$$

$$K_{ab} = \begin{pmatrix} (a_i \star x_{b,i})_{i=1}^m \\ (a_i \star \hat{x}_{b,i})_{i=1}^m \\ (\hat{a}_i \star x_{b,i})_{i=1}^m \end{pmatrix}$$

Bob

$$\begin{pmatrix} b_1, \ldots, b_m & \\ \hat{b}_1, \ldots, \hat{b}_m & \in \mathcal{G} \end{pmatrix}$$

$$pw = (w_1, \ldots, w_m)$$

$$K_{ab} = \begin{pmatrix} (b_i \star x_{a,i})_{i=1}^m \\ (\hat{b}_i \star x_{a,i})_{i=1}^m \\ (b_i \star \hat{x}_{a,i})_{i=1}^m \end{pmatrix}$$

Comparison of Com-GA-PAKE and X-GA-PAKE

	Com-GA-PAKE	X-GA-PAKE
Total Communication	$2m+1$	$4m$
Total Computation	$4m$	$10m$
No of Rounds	3	1
Security Assumption	CDH	Square-Inverse
Tight	no	yes

Parameter Choice: e.g. $m = 128$ and $|\mathcal{PW}| \subset \{0,1\}^m$.

Summary

X-GA-PAKE and **Com-GA-PAKE** are the first direct constructions and provably secure PAKE protocols based on CSIDH.

- Twists are important in the security analysis.
- Hash function into the set $\mathcal{X}$ can be replaced with a bit-by-bit approach.

Further Optimizations

- Decrease computational cost by increasing the size of the crs.
- Double the crs using twists.
- Recent improvements by Ishibashi, Yoneyama [ACISP '23].

Thank you!

Literature

Abdalla, Eisenhofer, Kiltz, Kunzweiler, Riepel: Password-authenticated key exchange from group actions. *CRYPTO 2022*. `https://eprint.iacr.org/2022/770.pdf`

Alamati, De Feo, Montgomery, Patranabis: Cryptographic Group Actions and Applications. *ASIACRYPT 2020*. `https://eprint.iacr.org/2020/1188`

Azarderakhsh, Jao, Koziel, LeGrow, Soukharev, Taraskin: How Not to Create an Isogeny-Based PAKE. *ACNS 2020*. `https://eprint.iacr.org/2020/361.pdf`

Castryck, Lange, Martindale, Panny, Renes: CSIDH: an efficient post-quantum commutative group action. *ASIACRYPT 2018*. `https://eprint.iacr.org/2018/383.pdf`

Couveignes: Hard homogeneous spaces. *Eprint*. `https://eprint.iacr.org/2006/291.pdf`

Jablon: Strong password-only authenticated key exchange. *ACM SIGCOMM 1996*. `https://dl.acm.org/doi/pdf/10.1145/242896.242897`