Password-Authenticated Key Exchange from Group Actions

Michel Abdalla[1,2], Thorsten Eisenhofer[3], Eike Kiltz[3], Sabrina Kunzweiler[3], Doreen Riepel[3]

November 8, 2022

[1]DIENS, École normale supérieure, CNRS, PSL University, Paris, France
[2]DFINITY, Zürich, Switzerland
[3]Ruhr-Universität Bochum, Germany

Motivation

Password Authenticated Key Exchange

- Establish a session key based on a (potentially weak) password

Motivation

Password Authenticated Key Exchange

- Establish a session key based on a (potentially weak) password

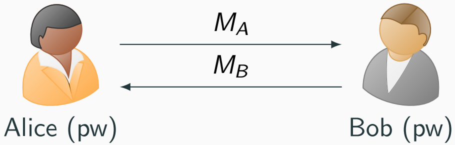
Alice (pw)

Bob (pw)

Motivation

Password Authenticated Key Exchange

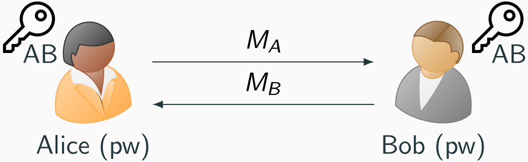
- Establish a session key based on a (potentially weak) password



Motivation

Password Authenticated Key Exchange

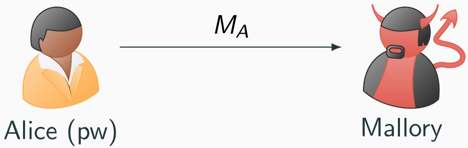
- Establish a session key based on a (potentially weak) password



Motivation

Password Authenticated Key Exchange

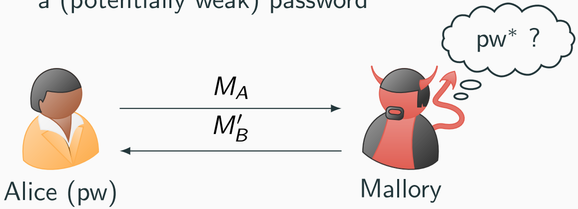
- Establish a session key based on a (potentially weak) password



Motivation

Password Authenticated Key Exchange

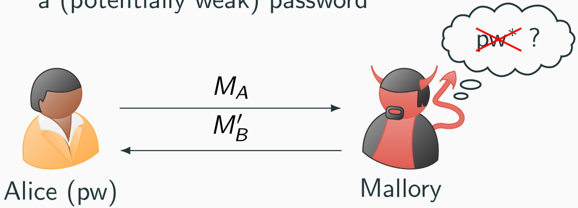
- Establish a session key based on a (potentially weak) password



Motivation

Password Authenticated Key Exchange

- Establish a session key based on a (potentially weak) password

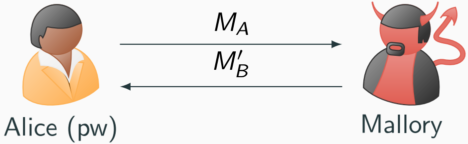


- Best attack: online dictionary attack

Motivation

Password Authenticated Key Exchange

- Establish a session key based on a (potentially weak) password



- Best attack: online dictionary attack

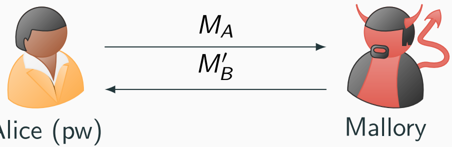
Group Actions

- Abstraction is close to the classical DH-setting

Motivation

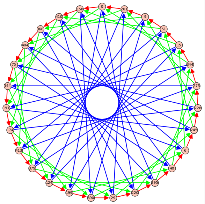
Password Authenticated Key Exchange

- Establish a session key based on a (potentially weak) password



- Best attack: online dictionary attack

Group Actions

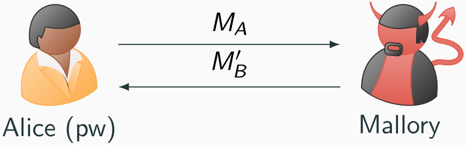


- Abstraction is close to the classical DH-setting
- CSIDH as candidate for post-quantum security
- Public-Key Encryption, Signatures, Oblivious Transfer, ...

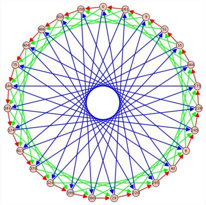
Motivation

Password Authenticated Key Exchange from **Group Actions** ?

- Establish a session key based on a (potentially weak) password



- Best attack: online dictionary attack



- Abstraction is close to the classical DH-setting
- CSIDH as candidate for post-quantum security
- Public-Key Encryption, Signatures, Oblivious Transfer, ...

Motivation

Password Authenticated Key Exchange from **Group Actions** ?

Motivation

Password Authenticated Key Exchange from **Group Actions** ?

Difficulties (e.g., [AJK$^+$20])

- Limited structure of the group action
- Special properties of CSIDH

$\Rightarrow$ Known DH-based constructions cannot be directly translated to the group action setting

Motivation

Password Authenticated Key Exchange from **Group Actions** ?

Difficulties (e.g., [AJK+20])

- Limited structure of the group action
- Special properties of CSIDH

$\Rightarrow$ Known DH-based constructions cannot be directly translated to the group action setting

Generic Constructions

- Quite inefficient construction using OT
- Unclear how to use the HPS of [ADMP20]

Cryptographic Group Actions

Group Actions

Group Action

Let $(\mathcal{G}, \cdot)$ be a group with identity element $id \in \mathcal{G}$, and $\mathcal{X}$ a set. A map $\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$ is a group action if it satisfies the following properties:

1. Identity: $id \star x = x$ for all $x \in \mathcal{X}$.
2. Compatibility: $(g \cdot h) \star x = g \star (h \star x)$ for all $g, h \in \mathcal{G}$ and $x \in \mathcal{X}$.

Group Actions

Group Action

Let $(\mathcal{G}, \cdot)$ be a group with identity element $id \in \mathcal{G}$, and $\mathcal{X}$ a set. A map $\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$ is a group action if it satisfies the following properties:

1. Identity: $id \star x = x$ for all $x \in \mathcal{X}$.
2. Compatibility: $(g \cdot h) \star x = g \star (h \star x)$ for all $g, h \in \mathcal{G}$ and $x \in \mathcal{X}$.

Technical Assumptions

- $\mathcal{G}$ and $\mathcal{X}$ are finite.
- $\mathcal{G}$ is commutative.
- $\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$ is regular.
- A distinguished element $\tilde{x} \in \mathcal{X}$ ("origin").

Group Actions

Group Action

Let $(\mathcal{G}, \cdot)$ be a group with identity element $id \in \mathcal{G}$, and $\mathcal{X}$ a set. A map $\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$ is a group action if it satisfies the following properties:

1. Identity: $id \star x = x$ for all $x \in \mathcal{X}$.
2. Compatibility: $(g \cdot h) \star x = g \star (h \star x)$ for all $g, h \in \mathcal{G}$ and $x \in \mathcal{X}$.

Technical Assumptions

- $\mathcal{G}$ and $\mathcal{X}$ are finite.
- $\mathcal{G}$ is commutative.
- $\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$ is regular.
- A distinguished element $\tilde{x} \in \mathcal{X}$ ("origin").

⚠ In general, we cannot combine two elements of the set $\mathcal{X}$!

The CSIDH Group Action

CSIDH [CLM$^+$18] can be seen as a *restricted effective* group action [ADMP20]:

$\mathcal{G} =$ corresponds to isogenies between elliptic curves

$\mathcal{X} =$ supersingular elliptic curves over $\mathbb{F}_p$

The CSIDH Group Action

CSIDH [CLM$^+$18] can be seen as a *restricted effective* group action [ADMP20]:
$\mathcal{G} =$ corresponds to isogenies between elliptic curves
$\mathcal{X} =$ supersingular elliptic curves over $\mathbb{F}_p$

Computational Assumptions

- DLOG: Given $g \star \tilde{x} \in \mathcal{X}$, it is hard to find $g \in \mathcal{G}$.
- CDH: Given $(g \star \tilde{x}, h \star \tilde{x}) \in \mathcal{X}^2$, it is hard to find $z = gh \star \tilde{x} \in \mathcal{X}$.
- DDH: Given $(g \star \tilde{x}, h \star \tilde{x}, gh \star \tilde{x}) \in \mathcal{X}^3$ or $(g \star \tilde{x}, h \star \tilde{x}, u \star \tilde{x}) \in \mathcal{X}^3$, decide which is the case.

The CSIDH Group Action

CSIDH [CLM+18] can be seen as a *restricted effective* group action [ADMP20]:
$\mathcal{G} =$ corresponds to isogenies between elliptic curves
$\mathcal{X} =$ supersingular elliptic curves over $\mathbb{F}_p$

Computational Assumptions

- DLOG: Given $g \star \tilde{x} \in \mathcal{X}$, it is hard to find $g \in \mathcal{G}$.
- CDH: Given $(g \star \tilde{x}, h \star \tilde{x}) \in \mathcal{X}^2$, it is hard to find $z = gh \star \tilde{x} \in \mathcal{X}$.
- DDH: Given $(g \star \tilde{x}, h \star \tilde{x}, gh \star \tilde{x}) \in \mathcal{X}^3$ or $(g \star \tilde{x}, h \star \tilde{x}, u \star \tilde{x}) \in \mathcal{X}^3$, decide which is the case.
- Strong/Gap CDH: same as CDH but with access to a decision oracle DDH, where

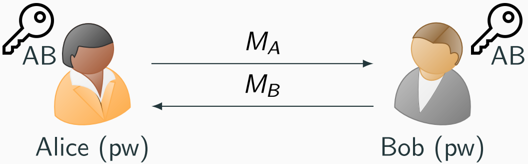
$$\mathrm{DDH}(x, y, z) = \begin{cases} 1 & \mathrm{CDH}(x, y) = z \\ 0 & \text{otherwise} \end{cases}$$

Password-Authenticated Key Exchange

Password-Authenticated Key Exchange (PAKE)

Focus

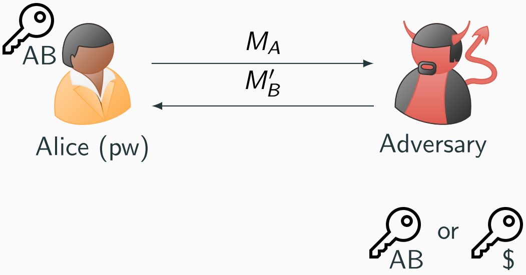
- balanced PAKE



Password-Authenticated Key Exchange (PAKE)

Focus

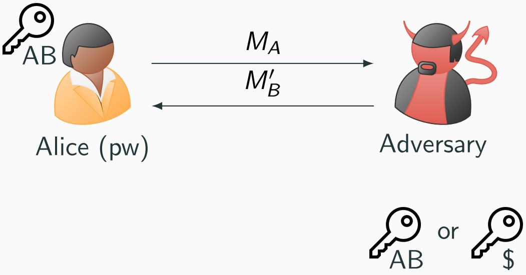
- balanced PAKE
- BPR security model (game-based) with extension to multiple test queries



Password-Authenticated Key Exchange (PAKE)

Focus

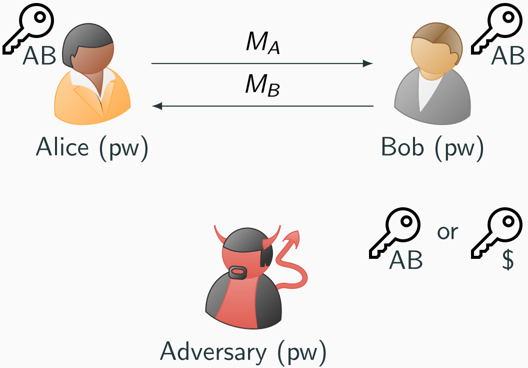
- balanced PAKE
- BPR security model (game-based) with extension to multiple test queries
- perfect forward secrecy



Password-Authenticated Key Exchange (PAKE)

Focus

- balanced PAKE
- BPR security model (game-based) with extension to multiple test queries
- ~~perfect~~ weak forward secrecy



How Not To Construct a CSIDH-PAKE (1/3)[1]

Encrypted Key Exchange (EKE) by Bellovin and Merritt '92

[1] Azarderakhsh et al., https://eprint.iacr.org/2020/361.pdf

How Not To Construct a CSIDH-PAKE (1/3)[1]

Encrypted Key Exchange (EKE) by Bellovin and Merritt '92

Alice A		**Bob** B
	$\mathsf{pw} \in \mathcal{PW}$	
$a \xleftarrow{\$} \mathcal{G}$ $x_{\mathsf{A}} := a \star \tilde{x}$	$\xrightarrow{\mathsf{Enc}_{\mathsf{pw}}(x_{\mathsf{A}})}$	$b \xleftarrow{\$} \mathcal{G}$ $x_{\mathsf{B}} := b \star \tilde{x}$
$K := a \star x_{\mathsf{B}}$	$\xleftarrow{\mathsf{Enc}_{\mathsf{pw}}(x_{\mathsf{B}})}$	$K := b \star x_{\mathsf{A}}$

[1] Azarderakhsh et al., https://eprint.iacr.org/2020/361.pdf

How Not To Construct a CSIDH-PAKE (1/3)[1]

Encrypted Key Exchange (EKE) by Bellovin and Merritt '92

Alice A		**Bob** B
	$\mathsf{pw} \in \mathcal{PW}$	
$a \xleftarrow{\$} \mathcal{G}$		$b \xleftarrow{\$} \mathcal{G}$
$x_\mathsf{A} := a \star \tilde{x}$	$\xrightarrow{\mathsf{Enc}_\mathsf{pw}(x_\mathsf{A})}$	$x_\mathsf{B} := b \star \tilde{x}$
$K := a \star x_\mathsf{B}$	$\xleftarrow{\mathsf{Enc}_\mathsf{pw}(x_\mathsf{B})}$	$K := b \star x_\mathsf{A}$

Offline Dictionary Attack: Decrypt messages and check if the output lies in $\mathcal{X}$ (is a supersingular curve).

[1] Azarderakhsh et al., https://eprint.iacr.org/2020/361.pdf

How Not To Construct a CSIDH-PAKE (2/3)

Simple Password Exponential Key Exchange (SPEKE) by Jablon ’96

How Not To Construct a CSIDH-PAKE (2/3)

Simple Password Exponential Key Exchange (SPEKE) by Jablon ’96

Alice A		**Bob** B
	$\mathsf{pw} \in \mathcal{PW}$	
$x = \mathsf{G}(\mathsf{pw}) \in \mathcal{X}$		$x = \mathsf{G}(\mathsf{pw}) \in \mathcal{X}$
$a \xleftarrow{\$} \mathcal{G}$		$b \xleftarrow{\$} \mathcal{G}$
$x_{\mathsf{A}} := a \star x$	$\xrightarrow{x_{\mathsf{A}}}$	$x_{\mathsf{B}} := b \star x$
	$\xleftarrow{x_{\mathsf{B}}}$	
$z := a \star x_{\mathsf{B}}$		$z := b \star x_{\mathsf{A}}$
	$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_{\mathsf{A}}, x_{\mathsf{B}}, \mathsf{pw}, z)$	

How Not To Construct a CSIDH-PAKE (2/3)

Simple Password Exponential Key Exchange (SPEKE) by Jablon ’96

Alice A		**Bob** B
	$\mathsf{pw} \in \mathcal{PW}$	
$x = \mathsf{G}(\mathsf{pw}) \in \mathcal{X}$		$x = \mathsf{G}(\mathsf{pw}) \in \mathcal{X}$
$a \xleftarrow{\$} \mathcal{G}$		$b \xleftarrow{\$} \mathcal{G}$
$x_{\mathsf{A}} := a \star x$	$\xrightarrow{x_{\mathsf{A}}}$	$x_{\mathsf{B}} := b \star x$
	$\xleftarrow{x_{\mathsf{B}}}$	
$z := a \star x_{\mathsf{B}}$		$z := b \star x_{\mathsf{A}}$
	$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_{\mathsf{A}}, x_{\mathsf{B}}, \mathsf{pw}, z)$	

Problem: A hash function $\mathsf{G} : \mathcal{PW} \to \mathcal{X}$ is still an open problem for CSIDH [BBD+22, MMP22].

How Not To Construct a CSIDH-PAKE (2/3)

Simple Password Exponential Key Exchange (SPEKE) by Jablon '96

Alice A		**Bob** B
	$\mathsf{pw} \in \mathcal{PW}$	
$x = \mathsf{G}(\mathsf{pw}) \in \mathcal{X}$		$x = \mathsf{G}(\mathsf{pw}) \in \mathcal{X}$
$a \xleftarrow{\$} \mathcal{G}$		$b \xleftarrow{\$} \mathcal{G}$
$x_{\mathsf{A}} := a \star x$	$\xrightarrow{\quad x_{\mathsf{A}} \quad}$	$x_{\mathsf{B}} := b \star x$
	$\xleftarrow{\quad x_{\mathsf{B}} \quad}$	
$z := a \star x_{\mathsf{B}}$		$z := b \star x_{\mathsf{A}}$
	$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_{\mathsf{A}}, x_{\mathsf{B}}, \mathsf{pw}, z)$	

Problem: A hash function $\mathsf{G} : \mathcal{PW} \to \mathcal{X}$ is still an open problem for CSIDH [BBD+22, MMP22].

No trivial translation of other DH-based approaches, e.g. SPAKE(2), TBPEKE, CPace, JPAKE.

Our First Protocol

Our Group Action PAKE

Idea: Replace the hash function by a bit-by-bit approach.

Our Group Action PAKE

Idea: Replace the hash function by a bit-by-bit approach.

$$
\begin{array}{ccc}
\textbf{Alice } \mathsf{A} & & \textbf{Bob } \mathsf{B} \\
& \mathsf{pw} \in \mathcal{PW} & \\
x = \mathsf{G}(\mathsf{pw}) \in \mathcal{X} & & x = \mathsf{G}(\mathsf{pw}) \in \mathcal{X} \\
a \xleftarrow{\$} \mathcal{G} & & b \xleftarrow{\$} \mathcal{G} \\
x_{\mathsf{A}} := a \star x & \xrightarrow{\quad x_{\mathsf{A}} \quad} & x_{\mathsf{B}} := b \star x \\
& \xleftarrow{\quad x_{\mathsf{B}} \quad} & \\
z := a \star x_{\mathsf{B}} & & z := b \star x_{\mathsf{A}} \\
& K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_{\mathsf{A}}, x_{\mathsf{B}}, \mathsf{pw}, z) &
\end{array}
$$

Idea: Replace the hash function by a bit-by-bit approach.

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$,	
	$\mathsf{pw} := (\beta_1, \dots, \beta_\ell) \in \{0,1\}^\ell$	
$a \xleftarrow{\$} \mathcal{G}$		$b \xleftarrow{\$} \mathcal{G}$
$x_\mathsf{A} := a \star x$	$\xrightarrow{x_\mathsf{A}}$	$x_\mathsf{B} := b \star x$
	$\xleftarrow{x_\mathsf{B}}$	
$z := a \star x_\mathsf{B}$		$z := b \star x_\mathsf{A}$
	$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z)$	

Our Group Action PAKE

Idea: Replace the hash function by a bit-by-bit approach.

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2,$	
	$\mathsf{pw} := (\beta_1, \ldots, \beta_\ell) \in \{0,1\}^\ell$	
$(a_1, \ldots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, \ldots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$		**for** $i \in [\ell]$
$x_{\mathsf{A},i} := a_i \star x_{\beta_i}$	$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \ldots, x_{\mathsf{A},\ell})}$	$x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
	$\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})}$	
$z := a \star x_\mathsf{B}$		$z := b \star x_\mathsf{A}$
	$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z)$	

Our Group Action PAKE

Idea: Replace the hash function by a bit-by-bit approach.

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$,	
	$\mathsf{pw} := (\beta_1, ..., \beta_\ell) \in \{0,1\}^\ell$	
$(a_1, ..., a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, ..., b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$		**for** $i \in [\ell]$
$x_{\mathsf{A},i} := a_i \star x_{\beta_i}$	$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, ..., x_{\mathsf{A},\ell})}$	$x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
	$\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, ..., x_{\mathsf{B},\ell})}$	
for $i \in [\ell]$		**for** $i \in [\ell]$
$z_i := a_i \star x_{\mathsf{B},i}$		$z_i := b_i \star x_{\mathsf{A},i}$
	$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z_1, \ldots, z_\ell)$	

(In)Security of our Protocol

Security against Passive Adversaries

- secure under Strong CDH + ROM

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$, $\mathsf{pw} := (\beta_1, \dots, \beta_\ell) \in \{0,1\}^\ell$	
$(a_1, \dots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, \dots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$ $x_{\mathsf{A},i} := a_i \star x_{\beta_i}$	$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \dots, x_{\mathsf{A},\ell})}$ $\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \dots, x_{\mathsf{B},\ell})}$	**for** $i \in [\ell]$ $x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
for $i \in [\ell]$ $z_i := a_i \star x_{\mathsf{B},i}$		**for** $i \in [\ell]$ $z_i := b_i \star x_{\mathsf{A},i}$
	$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z_1, \dots, z_\ell)$	

(In)Security of our Protocol

Security against Passive Adversaries

- secure under Strong CDH + ROM

Security against Active Adversaries

- secure under Strong Simultaneous DH + ROM
- but: insecure when instantiated with CSIDH

Alice A		**Bob** B

$$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2, \quad \mathsf{pw} := (\beta_1, \ldots, \beta_\ell) \in \{0,1\}^\ell$$

Alice A		Bob B
$(a_1, \ldots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, \ldots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$	$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \ldots, x_{\mathsf{A},\ell})}$	**for** $i \in [\ell]$
$x_{\mathsf{A},i} := a_i \star x_{\beta_i}$	$\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})}$	$x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
for $i \in [\ell]$		**for** $i \in [\ell]$
$z_i := a_i \star x_{\mathsf{B},i}$		$z_i := b_i \star x_{\mathsf{A},i}$

$$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z_1, \ldots, z_\ell)$$

(In)Security of our Protocol

Security against Passive Adversaries

- secure under Strong CDH + ROM

Security against Active Adversaries

- secure under Strong Simultaneous DH + ROM
- but: insecure when instantiated with CSIDH

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$,	
	$\mathsf{pw} := (\beta_1, \ldots, \beta_\ell) \in \{0,1\}^\ell$	
$(a_1, \ldots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, \ldots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$	$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \ldots, x_{\mathsf{A},\ell})}$	**for** $i \in [\ell]$
$x_{\mathsf{A},i} := a_i \star x_{\beta_i}$	$\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})}$	$x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
for $i \in [\ell]$		**for** $i \in [\ell]$
$z_i := a_i \star x_{\mathsf{B},i}$		$z_i := b_i \star x_{\mathsf{A},i}$
	$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z_1, \ldots, z_\ell)$	

Additional Structure of the CSIDH Group Action

- For any $x \in \mathcal{X}$, we can efficiently compute its *twist* denoted by x^t.
- Let $x = g \star \tilde{x}$, then $x^t = g^{-1} \star \tilde{x}$. In particular $\tilde{x}^t = \tilde{x}$.

How Not To Construct a CSIDH-PAKE (3/3)

Twists yield an Offline Dictionary Attack!

Alice A		**Adversary** $\mathcal{B}$
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$, $\mathsf{pw} := \beta \in \{0,1\}$	
$a \xleftarrow{\$} \mathcal{G}$		
$x_\mathsf{A} := a \star x_\beta$	$\xrightarrow{x_\mathsf{A}}$	

How Not To Construct a CSIDH-PAKE (3/3)

Twists yield an Offline Dictionary Attack!

Alice A		**Adversary** $\mathcal{B}$
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$, $\mathsf{pw} := \beta \in \{0,1\}$	
$a \xleftarrow{\$} \mathcal{G}$		$b \xleftarrow{\$} \mathcal{G}$
$x_A := a \star x_\beta$	$\xrightarrow{x_A}$	

How Not To Construct a CSIDH-PAKE (3/3)

Twists yield an Offline Dictionary Attack!

Alice A		**Adversary** $\mathcal{B}$
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$, $\mathsf{pw} := \beta \in \{0,1\}$	
$a \xleftarrow{\$} \mathcal{G}$ $x_\mathsf{A} := a \star x_\beta$	$\xrightarrow{\quad x_\mathsf{A} \quad}$	$b \xleftarrow{\$} \mathcal{G}$ $x_\mathsf{B} := b \star (x_\mathsf{A})^t$

How Not To Construct a CSIDH-PAKE (3/3)

Twists yield an Offline Dictionary Attack!

Alice A		**Adversary** $\mathcal{B}$
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$, $\mathsf{pw} := \beta \in \{0,1\}$	
$a \xleftarrow{\$} \mathcal{G}$		$b \xleftarrow{\$} \mathcal{G}$
$x_\mathsf{A} := a \star x_\beta$	$\xrightarrow{x_\mathsf{A}}$	$x_\mathsf{B} := b \star (x_\mathsf{A})^t$
	$\xleftarrow{x_\mathsf{B}}$	

How Not To Construct a CSIDH-PAKE (3/3)

Twists yield an Offline Dictionary Attack!

Alice A		**Adversary** $\mathcal{B}$
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$, $\mathsf{pw} := \beta \in \{0,1\}$	
$a \xleftarrow{\$} \mathcal{G}$		$b \xleftarrow{\$} \mathcal{G}$
$x_\mathsf{A} := a \star x_\beta$	$\xrightarrow{x_\mathsf{A}}$	$x_\mathsf{B} := b \star (x_\mathsf{A})^t$
	$\xleftarrow{x_\mathsf{B}}$	
$z := a \star x_\mathsf{B}$		

How Not To Construct a CSIDH-PAKE (3/3)

Twists yield an Offline Dictionary Attack!

Alice A		**Adversary** $\mathcal{B}$
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$, $\mathsf{pw} := \beta \in \{0,1\}$	
$a \xleftarrow{\$} \mathcal{G}$		$b \xleftarrow{\$} \mathcal{G}$
$x_{\mathsf{A}} := a \star x_\beta$	$\xrightarrow{x_{\mathsf{A}}}$	$x_{\mathsf{B}} := b \star (x_{\mathsf{A}})^t$
	$\xleftarrow{x_{\mathsf{B}}}$	
$z := a \star x_{\mathsf{B}}$		
$K_{\mathsf{AB}} := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_{\mathsf{A}}, x_{\mathsf{B}}, \mathsf{pw}, z)$		

How Not To Construct a CSIDH-PAKE (3/3)

Twists yield an Offline Dictionary Attack!

Alice A		**Adversary** $\mathcal{B}$
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$, $\mathsf{pw} := \beta \in \{0,1\}$	
$a \xleftarrow{\$} \mathcal{G}$		$b \xleftarrow{\$} \mathcal{G}$
$x_\mathsf{A} := a \star x_\beta$	$\xrightarrow{x_\mathsf{A}}$	$x_\mathsf{B} := b \star (x_\mathsf{A})^t = b \star (a^{-1} \star x_\beta^t)$
	$\xleftarrow{x_\mathsf{B}}$	
$z := a \star x_\mathsf{B}$		
$K_{\mathsf{AB}} := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z)$		

How Not To Construct a CSIDH-PAKE (3/3)

Twists yield an Offline Dictionary Attack!

Alice A		**Adversary** $\mathcal{B}$
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$, $\mathsf{pw} := \beta \in \{0,1\}$	
$a \xleftarrow{\$} \mathcal{G}$		$b \xleftarrow{\$} \mathcal{G}$
$x_\mathsf{A} := a \star x_\beta$	$\xrightarrow{x_\mathsf{A}}$	$x_\mathsf{B} := b \star (x_\mathsf{A})^t = b \star (a^{-1} \star x_\beta^t)$
	$\xleftarrow{x_\mathsf{B}}$	
$z := a \star x_\mathsf{B} = a \star (ba^{-1} \star x_\beta^t)$		
$K_{\mathsf{AB}} := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z)$		

How Not To Construct a CSIDH-PAKE (3/3)

Twists yield an Offline Dictionary Attack!

Alice A		**Adversary** $\mathcal{B}$
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$, $\mathsf{pw} := \beta \in \{0,1\}$	
$a \xleftarrow{\$} \mathcal{G}$		$b \xleftarrow{\$} \mathcal{G}$
$x_A := a \star x_\beta$	$\xrightarrow{x_A}$	$x_B := b \star (x_A)^t = b \star (a^{-1} \star x_\beta^t)$
	$\xleftarrow{x_B}$	
$z := a \star x_B = a \star (ba^{-1} \star x_\beta^t) = b \star x_\beta^t$		
$K_{AB} := \mathsf{H}(A, B, x_A, x_B, \mathsf{pw}, z)$		

How Not To Construct a CSIDH-PAKE (3/3)

Twists yield an Offline Dictionary Attack!

Alice A		**Adversary** $\mathcal{B}$
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$, $\mathsf{pw} := \beta \in \{0,1\}$	
$a \xleftarrow{\$} \mathcal{G}$		$b \xleftarrow{\$} \mathcal{G}$
$x_A := a \star x_\beta$	$\xrightarrow{x_A}$	$x_B := b \star (x_A)^t = b \star (a^{-1} \star x_\beta^t)$
	$\xleftarrow{x_B}$	
$z := a \star x_B = a \star (ba^{-1} \star x_\beta^t) = b \star x_\beta^t$		$z_0 := b \star x_0^t$, $z_1 := b \star x_1^t$
$K_{AB} := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_A, x_B, \mathsf{pw}, z)$		

How Not To Construct a CSIDH-PAKE (3/3)

Twists yield an Offline Dictionary Attack!

Alice A		**Adversary** $\mathcal{B}$
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2,$ $\mathsf{pw} := \beta \in \{0,1\}$	
$a \xleftarrow{\$} \mathcal{G}$ $x_\mathsf{A} := a \star x_\beta$	$\xrightarrow{x_\mathsf{A}}$	$b \xleftarrow{\$} \mathcal{G}$ $x_\mathsf{B} := b \star (x_\mathsf{A})^t = b \star (a^{-1} \star x_\beta^t)$
	$\xleftarrow{x_\mathsf{B}}$	
$z := a \star x_\mathsf{B}$ $= a \star (ba^{-1} \star x_\beta^t)$ $= b \star x_\beta^t$		$z_0 := b \star x_0^t$ $z_1 := b \star x_1^t$
$K_\mathsf{AB} := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z)$		**for** $\beta' \in \{0,1\}$ $K' := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z_{\beta'})$ Check $K' = K_\mathsf{AB}$

Two New PAKE Protocols

Two New PAKE Protocols

1. **Use a Commitment (**Com-GA-PAKE**)**
   - The server commits on its message using a hash function (random oracle).
   - An adversary cannot choose x_{B} depending on the user's message.

Two New PAKE Protocols

1. **Use a Commitment (**Com-GA-PAKE**)**
   - The server commits on its message using a hash function (random oracle).
   - An adversary cannot choose x_{B} depending on the user's message.
2. **Use "Cross-Terms" (**X-GA-PAKE**)**
   - Double the communication and combine elements in three ways.
   - $\mathcal{A}$ can compute at most two of the three combinations.

Com-GA-PAKE

Alice A		**Bob** B
	crs $:= (x_0, x_1) \in \mathcal{X}^2$, pw $:= (\beta_1, \dots, \beta_\ell) \in \{0,1\}^\ell$	
$(a_1, \dots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$ **for** $i \in [\ell]$ $\quad x_{\mathsf{A},i} := a_i \star x_{\beta_i}$		$(b_1, \dots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$ **for** $i \in [\ell]$ $\quad x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
	$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \dots, x_{\mathsf{A},\ell})}$	
	$\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \dots, x_{\mathsf{B},\ell})}$	
for $i \in [\ell]$ $\quad z_i := a_i \star x_{\mathsf{B},i}$		**for** $i \in [\ell]$ $\quad z_i := b_i \star x_{\mathsf{A},i}$
	$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z_1, \dots, z_\ell)$	

Com-GA-PAKE

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$,	
	$\mathsf{pw} := (\beta_1, \dots, \beta_\ell) \in \{0,1\}^\ell$	
$(a_1, \dots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, \dots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$		**for** $i \in [\ell]$
$\quad x_{\mathsf{A},i} := a_i \star x_{\beta_i}$		$\quad x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
		$\mathsf{com} = \mathsf{G}(x_{\mathsf{B},1}, \dots, x_{\mathsf{B},\ell})$
	$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \dots, x_{\mathsf{A},\ell})}$	
	$\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \dots, x_{\mathsf{B},\ell})}$	
for $i \in [\ell]$		**for** $i \in [\ell]$
$\quad z_i := a_i \star x_{\mathsf{B},i}$		$\quad z_i := b_i \star x_{\mathsf{A},i}$

$$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z_1, \dots, z_\ell)$$

Com-GA-PAKE

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$,	
	$\mathsf{pw} := (\beta_1, \ldots, \beta_\ell) \in \{0,1\}^\ell$	
$(a_1, \ldots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, \ldots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$		**for** $i \in [\ell]$
$x_{\mathsf{A},i} := a_i \star x_{\beta_i}$		$x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
	$\xleftarrow{\mathsf{com}}$	$\mathsf{com} = \mathsf{G}(x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})$
	$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \ldots, x_{\mathsf{A},\ell})}$	
	$\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})}$	
for $i \in [\ell]$		**for** $i \in [\ell]$
$z_i := a_i \star x_{\mathsf{B},i}$		$z_i := b_i \star x_{\mathsf{A},i}$
	$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z_1, \ldots, z_\ell)$	

Com-GA-PAKE

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$,	
	$\mathsf{pw} := (\beta_1, \ldots, \beta_\ell) \in \{0,1\}^\ell$	
$(a_1, \ldots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, \ldots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$		**for** $i \in [\ell]$
$\quad x_{\mathsf{A},i} := a_i \star x_{\beta_i}$		$\quad x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
	$\xleftarrow{\mathsf{com}}$	$\mathsf{com} = \mathsf{G}(x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})$
	$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \ldots, x_{\mathsf{A},\ell})}$	
if $\mathsf{com} = \mathsf{G}(x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})$	$\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})}$	
$\quad$**for** $i \in [\ell]$		**for** $i \in [\ell]$
$\quad\quad z_i := a_i \star x_{\mathsf{B},i}$		$\quad z_i := b_i \star x_{\mathsf{A},i}$

$$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z_1, \ldots, z_\ell)$$

Security of Com-GA-PAKE

Security against Passive Adversaries:

- secure under Strong CDH + ROM

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$, $\mathsf{pw} := (\beta_1, \ldots, \beta_\ell) \in \{0,1\}^\ell$	
		$(b_1, \ldots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$ **for** $i \in [\ell]$ $x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
$(a_1, \ldots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$ **for** $i \in [\ell]$ $x_{\mathsf{A},i} := a_i \star x_{\beta_i}$	$\xleftarrow{\mathsf{com}}$	$\mathsf{com} = \mathsf{G}(x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})$
	$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \ldots, x_{\mathsf{A},\ell})}$	
	$\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})}$	
if $\mathsf{com} = \mathsf{G}(x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})$ **for** $i \in [\ell]$ $z_i := a_i \star x_{\mathsf{B},i}$		**for** $i \in [\ell]$ $z_i := b_i \star x_{\mathsf{A},i}$
	$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{com}, \mathsf{pw}, z_1, \ldots, z_\ell)$	

Security of Com-GA-PAKE

Security against Active Adversaries:

- secure under Strong Interactive Simultaneous DH + ROM

Alice A | **Bob** B

$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2,$

$\mathsf{pw} := (\beta_1, \dots, \beta_\ell) \in \{0,1\}^\ell$

Bob:

$(b_1, \dots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$

for $i \in [\ell]$

$\quad x_{\mathsf{B},i} := b_i \star x_{\beta_i}$

$\mathsf{com} = \mathsf{G}(x_{\mathsf{B},1}, \dots, x_{\mathsf{B},\ell})$

Alice:

$(a_1, \dots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$

for $i \in [\ell]$

$\quad x_{\mathsf{A},i} := a_i \star x_{\beta_i}$

$\mathsf{A} \xleftarrow{\mathsf{com}} \mathsf{B}$

$\mathsf{A} \xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \dots, x_{\mathsf{A},\ell})} \mathsf{B}$

$\mathsf{A} \xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \dots, x_{\mathsf{B},\ell})} \mathsf{B}$

Alice:

if $\mathsf{com} = \mathsf{G}(x_{\mathsf{B},1}, \dots, x_{\mathsf{B},\ell})$

$\quad$ **for** $i \in [\ell]$

$\quad\quad z_i := a_i \star x_{\mathsf{B},i}$

Bob:

for $i \in [\ell]$

$\quad z_i := b_i \star x_{\mathsf{A},i}$

$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{com}, \mathsf{pw}, z_1, \dots, z_\ell)$

Security against Active Adversaries:

- secure under Strong Interactive Simultaneous DH + ROM

ISimDH

ISimDH		$\mathcal{A}$
$(g_0, g_1) \xleftarrow{\$} \mathcal{G}^2$	$\xrightarrow{g_0 \star \tilde{x},\ g_1 \star \tilde{x}}$	
	$\xleftarrow{y}$	
$g \xleftarrow{\$} \mathcal{G}$	$\xrightarrow{g \star \tilde{x}}$	
	$\xleftarrow{z_0, z_1}$	
Output 1 if $z_0 = g g_0^{-1} \star y$, $z_1 = g g_1^{-1} \star y$		

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$, $\mathsf{pw} := (\beta_1, \ldots, \beta_\ell) \in \{0,1\}^\ell$	
		$(b_1, \ldots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$ **for** $i \in [\ell]$ $x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
		$\mathsf{com} = \mathsf{G}(x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})$
$(a_1, \ldots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$ **for** $i \in [\ell]$ $x_{\mathsf{A},i} := a_i \star x_{\beta_i}$	$\xleftarrow{\mathsf{com}}$	
	$\xrightarrow{x_{\mathsf{A}} = (x_{\mathsf{A},1}, \ldots, x_{\mathsf{A},\ell})}$	
	$\xleftarrow{x_{\mathsf{B}} = (x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})}$	
if $\mathsf{com} = \mathsf{G}(x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})$ **for** $i \in [\ell]$ $z_i := a_i \star x_{\mathsf{B},i}$		**for** $i \in [\ell]$ $z_i := b_i \star x_{\mathsf{A},i}$

$$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_{\mathsf{A}}, x_{\mathsf{B}}, \mathsf{com}, \mathsf{pw}, z_1, \ldots, z_\ell)$$

Security of Com-GA-PAKE

Security against Active Adversaries:

- secure under Strong Interactive Simultaneous DH + ROM

ISimDH

$(g_0, g_1) \xleftarrow{\$} \mathcal{G}^2$

$\xrightarrow{\;g_0 \star \tilde{x},\, g_1 \star \tilde{x}\;}$ $\mathcal{A}$

$\xleftarrow{\;y\;}$

$g \xleftarrow{\$} \mathcal{G}$

$\xrightarrow{\;g \star \tilde{x}\;}$

$\xleftarrow{\;z_0, z_1\;}$

Output 1 if

$z_0 = gg_0^{-1} \star y$

$z_1 = gg_1^{-1} \star y$

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$,	
	$\mathsf{pw} := (\beta_1, \ldots, \beta_\ell) \in \{0,1\}^\ell$	
		$(b_1, \ldots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
		for $i \in [\ell]$
		$x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
$(a_1, \ldots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$	$\xleftarrow{\;\mathsf{com}\;}$	$\mathsf{com} = \mathsf{G}(x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})$
for $i \in [\ell]$	$\xrightarrow{\;x_\mathsf{A} = (x_{\mathsf{A},1}, \ldots, x_{\mathsf{A},\ell})\;}$	
$x_{\mathsf{A},i} := a_i \star x_{\beta_i}$	$\xleftarrow{\;x_\mathsf{B} = (x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})\;}$	
if $\mathsf{com} = \mathsf{G}(x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})$		
for $i \in [\ell]$		**for** $i \in [\ell]$
$z_i := a_i \star x_{\mathsf{B},i}$		$z_i := b_i \star x_{\mathsf{A},i}$
	$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{com}, \mathsf{pw}, z_1, \ldots, z_\ell)$	

Main idea: If $\mathcal{A}$ queries H on two different passwords, we can solve ISimDH.

Security of Com-GA-PAKE

Security against Active Adversaries:

- secure under Strong Interactive Simultaneous DH + ROM

ISimDH

$(g_0, g_1) \xleftarrow{\$} \mathcal{G}^2$ $\xrightarrow{g_0 \star \tilde{x},\, g_1 \star \tilde{x}}$ $\mathcal{A}$

$\xleftarrow{y}$

$g \xleftarrow{\$} \mathcal{G}$ $\xrightarrow{g \star \tilde{x}}$

$\xleftarrow{z_0, z_1}$

Output 1 if

$z_0 = g g_0^{-1} \star y$

$z_1 = g g_1^{-1} \star y$

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$, $\mathsf{pw} := (\beta_1, \ldots, \beta_\ell) \in \{0,1\}^\ell$	
		$(b_1, \ldots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
		for $i \in [\ell]$
		$x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
$(a_1, \ldots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$	$\xleftarrow{\mathsf{com}}$	$\mathsf{com} = \mathsf{G}(x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})$
for $i \in [\ell]$	$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \ldots, x_{\mathsf{A},\ell})}$	
$x_{\mathsf{A},i} := a_i \star x_{\beta_i}$	$\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})}$	
if $\mathsf{com} = \mathsf{G}(x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})$		
for $i \in [\ell]$		**for** $i \in [\ell]$
$z_i := a_i \star x_{\mathsf{B},i}$		$z_i := b_i \star x_{\mathsf{A},i}$
	$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{com}, \mathsf{pw}, z_1, \ldots, z_\ell)$	

Main idea: If $\mathcal{A}$ queries H on two different passwords, we can solve ISimDH.

- Proof requires guessing (non-tight).

Security against Active Adversaries:

- secure under Strong Interactive Simultaneous DH + ROM

ISimDH		$\mathcal{A}$
$(g_0, g_1) \xleftarrow{\$} \mathcal{G}^2$	$\xrightarrow{g_0 \star \tilde{x},\, g_1 \star \tilde{x}}$	
	$\xleftarrow{y}$	
$g \xleftarrow{\$} \mathcal{G}$	$\xrightarrow{g \star \tilde{x}}$	
	$\xleftarrow{z_0, z_1}$	
Output 1 if $z_0 = g g_0^{-1} \star y$, $z_1 = g g_1^{-1} \star y$		

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$, $\mathsf{pw} := (\beta_1, \dots, \beta_\ell) \in \{0,1\}^\ell$	
		$(b_1, \dots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$ **for** $i \in [\ell]$ $x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
$(a_1, \dots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$ **for** $i \in [\ell]$ $x_{\mathsf{A},i} := a_i \star x_{\beta_i}$	$\xleftarrow{\mathsf{com}}$ $\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \dots, x_{\mathsf{A},\ell})}$ $\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \dots, x_{\mathsf{B},\ell})}$	$\mathsf{com} = \mathsf{G}(x_{\mathsf{B},1}, \dots, x_{\mathsf{B},\ell})$
if $\mathsf{com} = \mathsf{G}(x_{\mathsf{B},1}, \dots, x_{\mathsf{B},\ell})$ **for** $i \in [\ell]$ $z_i := a_i \star x_{\mathsf{B},i}$		**for** $i \in [\ell]$ $z_i := b_i \star x_{\mathsf{A},i}$
	$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{com}, \mathsf{pw}, z_1, \dots, z_\ell)$	

Main idea: If $\mathcal{A}$ queries H on two different passwords, we can solve ISimDH.

- Proof requires guessing (non-tight).
- Strong ISimDH reduces to GapCDH (using rewinding).

X-GA-PAKE

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$,	
	$\mathsf{pw} := (\beta_1, \ldots, \beta_\ell) \in \{0,1\}^\ell$	
$(a_1, \ldots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, \ldots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$ $x_{\mathsf{A},i} := a_i \star x_{\beta_i}$	$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \ldots, x_{\mathsf{A},\ell})}$	**for** $i \in [\ell]$ $x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
for $i \in [\ell]$ $z_i := a_i \star x_{\mathsf{B},i}$	$\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})}$	**for** $i \in [\ell]$ $z_i := b_i \star x_{\mathsf{A},i}$

$$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z_1, \ldots, z_\ell)$$

X-GA-PAKE

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2,$ $\mathsf{pw} := (\beta_1, \ldots, \beta_\ell) \in \{0,1\}^\ell$	
$(a_1, \ldots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$ $(\hat{a}_1, \ldots, \hat{a}_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, \ldots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$ $(\hat{b}_1, \ldots, \hat{b}_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$ $x_{\mathsf{A},i} := a_i \star x_{\beta_i}$	$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \ldots, x_{\mathsf{A},\ell})}$	**for** $i \in [\ell]$ $x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
	$\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})}$	
for $i \in [\ell]$ $z_i := a_i \star x_{\mathsf{B},i}$		**for** $i \in [\ell]$ $z_i := b_i \star x_{\mathsf{A},i}$

$$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z_1, \ldots, z_\ell)$$

X-GA-PAKE

Alice A

Bob B

$$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2,$$
$$\mathsf{pw} := (\beta_1, \dots, \beta_\ell) \in \{0,1\}^\ell$$

Alice A		Bob B
$(a_1, \dots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, \dots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
$(\hat{a}_1, \dots, \hat{a}_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(\hat{b}_1, \dots, \hat{b}_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$	$\xrightarrow{x_A = (x_{A,1}, \dots, x_{A,\ell})}$	**for** $i \in [\ell]$
$x_{A,i} := a_i \star x_{\beta_i}$		$x_{B,i} := b_i \star x_{\beta_i}$
$\hat{x}_{A,i} := \hat{a}_i \star x_{\beta_i}$		$\hat{x}_{B,i} := \hat{b}_i \star x_{\beta_i}$
	$\xleftarrow{x_B = (x_{B,1}, \dots, x_{B,\ell})}$	
for $i \in [\ell]$		**for** $i \in [\ell]$
$z_i := a_i \star x_{B,i}$		$z_i := b_i \star x_{A,i}$

$$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_A, x_B, \mathsf{pw}, z_1, \dots, z_\ell)$$

X-GA-PAKE

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2,$ $\mathsf{pw} := (\beta_1, \ldots, \beta_\ell) \in \{0,1\}^\ell$	
$(a_1, \ldots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$ $(\hat{a}_1, \ldots, \hat{a}_\ell) \xleftarrow{\$} \mathcal{G}^\ell$ **for** $i \in [\ell]$ $x_{A,i} := a_i \star x_{\beta_i}$ $\hat{x}_{A,i} := \hat{a}_i \star x_{\beta_i}$	$\xrightarrow{x_A = (x_{A,1}, \ldots, x_{A,\ell}, \hat{x}_{A,1}, \ldots, \hat{x}_{A,\ell})}$	$(b_1, \ldots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$ $(\hat{b}_1, \ldots, \hat{b}_\ell) \xleftarrow{\$} \mathcal{G}^\ell$ **for** $i \in [\ell]$ $x_{B,i} := b_i \star x_{\beta_i}$ $\hat{x}_{B,i} := \hat{b}_i \star x_{\beta_i}$
	$\xleftarrow{x_B = (x_{B,1}, \ldots, x_{B,\ell}, \hat{x}_{B,1}, \ldots, \hat{x}_{B,\ell})}$	
for $i \in [\ell]$ $z_i := a_i \star x_{B,i}$		**for** $i \in [\ell]$ $z_i := b_i \star x_{A,i}$

$$K := \mathsf{H}(A, B, x_A, x_B, \mathsf{pw}, z_1, \ldots, z_\ell)$$

X-GA-PAKE

Alice A

Bob B

$$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2,$$
$$\mathsf{pw} := (\beta_1, \dots, \beta_\ell) \in \{0,1\}^\ell$$

Alice A:

$(a_1, \dots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$

$(\hat{a}_1, \dots, \hat{a}_\ell) \xleftarrow{\$} \mathcal{G}^\ell$

for $i \in [\ell]$

$\quad x_{\mathsf{A},i} := a_i \star x_{\beta_i}$

$\quad \hat{x}_{\mathsf{A},i} := \hat{a}_i \star x_{\beta_i}$

$$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \dots, x_{\mathsf{A},\ell}, \hat{x}_{\mathsf{A},1}, \dots, \hat{x}_{\mathsf{A},\ell})}$$

$$\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \dots, x_{\mathsf{B},\ell}, \hat{x}_{\mathsf{B},1}, \dots, \hat{x}_{\mathsf{B},\ell})}$$

for $i \in [\ell]$

$\quad z_i := (a_i \star x_{\mathsf{B},i}, \hat{a}_i \star x_{\mathsf{B},i}, a_i \star \hat{x}_{\mathsf{B},i})$

Bob B:

$(b_1, \dots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$

$(\hat{b}_1, \dots, \hat{b}_\ell) \xleftarrow{\$} \mathcal{G}^\ell$

for $i \in [\ell]$

$\quad x_{\mathsf{B},i} := b_i \star x_{\beta_i}$

$\quad \hat{x}_{\mathsf{B},i} := \hat{b}_i \star x_{\beta_i}$

for $i \in [\ell]$

$\quad z_i := (b_i \star x_{\mathsf{A},i}, b_i \star \hat{x}_{\mathsf{A},i}, \hat{b}_i \star x_{\mathsf{A},i})$

$$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z_1, \dots, z_\ell)$$

Security against Passive Adversaries

- secure under Strong CDH + ROM

Alice A		**Bob** B
$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$, $\mathsf{pw} := (\beta_1, \ldots, \beta_\ell) \in \{0,1\}^\ell$	
$(a_1, \ldots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$ $(\hat{a}_1, \ldots, \hat{a}_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, \ldots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$ $(\hat{b}_1, \ldots, \hat{b}_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$ $x_{\mathsf{A},i} := a_i \star x_{\beta_i}$ $\hat{x}_{\mathsf{A},i} := \hat{a}_i \star x_{\beta_i}$	$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \ldots, x_{\mathsf{A},\ell}, \hat{x}_{\mathsf{A},1}, \ldots, \hat{x}_{\mathsf{A},\ell})}$ $\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell}, \hat{x}_{\mathsf{B},1}, \ldots, \hat{x}_{\mathsf{B},\ell})}$	**for** $i \in [\ell]$ $x_{\mathsf{B},i} := b_i \star x_{\beta_i}$ $\hat{x}_{\mathsf{B},i} := \hat{b}_i \star x_{\beta_i}$
for $i \in [\ell]$ $z_i := (a_i \star x_{\mathsf{B},i}, \hat{a}_i \star x_{\mathsf{B},i}, a_i \star \hat{x}_{\mathsf{B},i})$		**for** $i \in [\ell]$ $z_i := (b_i \star x_{\mathsf{A},i}, b_i \star \hat{x}_{\mathsf{A},i}, \hat{b}_i \star x_{\mathsf{A},i})$
$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z_1, \ldots, z_\ell)$	

Security of X-GA-PAKE

Security against Passive Adversaries

- secure under Strong CDH + ROM

Security against Active Adversaries

- secure under Strong Square-Inverse DH + ROM

Alice A | **Bob** B

$$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2, \quad \mathsf{pw} := (\beta_1, \dots, \beta_\ell) \in \{0,1\}^\ell$$

Alice A:

$(a_1, \dots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$

$(\hat{a}_1, \dots, \hat{a}_\ell) \xleftarrow{\$} \mathcal{G}^\ell$

for $i \in [\ell]$

$x_{\mathsf{A},i} := a_i \star x_{\beta_i}$

$\hat{x}_{\mathsf{A},i} := \hat{a}_i \star x_{\beta_i}$

Bob B:

$(b_1, \dots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$

$(\hat{b}_1, \dots, \hat{b}_\ell) \xleftarrow{\$} \mathcal{G}^\ell$

for $i \in [\ell]$

$x_{\mathsf{B},i} := b_i \star x_{\beta_i}$

$\hat{x}_{\mathsf{B},i} := \hat{b}_i \star x_{\beta_i}$

$$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \dots, x_{\mathsf{A},\ell}, \hat{x}_{\mathsf{A},1}, \dots, \hat{x}_{\mathsf{A},\ell})}$$

$$\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \dots, x_{\mathsf{B},\ell}, \hat{x}_{\mathsf{B},1}, \dots, \hat{x}_{\mathsf{B},\ell})}$$

Alice A:

for $i \in [\ell]$

$z_i := (a_i \star x_{\mathsf{B},i}, \hat{a}_i \star x_{\mathsf{B},i}, a_i \star \hat{x}_{\mathsf{B},i})$

Bob B:

for $i \in [\ell]$

$z_i := (b_i \star x_{\mathsf{A},i}, b_i \star \hat{x}_{\mathsf{A},i}, \hat{b}_i \star x_{\mathsf{A},i})$

$$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z_1, \dots, z_\ell)$$

Security of X-GA-PAKE

Security against Passive Adversaries

- secure under Strong CDH + ROM

Security against Active Adversaries

- secure under Strong Square-Inverse DH + ROM
- given $(g \star \tilde{x})$ compute (y, z_0, z_1) such that

$$z_0 = g^2 \star y$$
$$z_1 = g^{-1} \star y$$

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2$, $\mathsf{pw} := (\beta_1, \ldots, \beta_\ell) \in \{0,1\}^\ell$	
$(a_1, \ldots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$ $(\hat{a}_1, \ldots, \hat{a}_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, \ldots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$ $(\hat{b}_1, \ldots, \hat{b}_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$ $x_{A,i} := a_i \star x_{\beta_i}$ $\hat{x}_{A,i} := \hat{a}_i \star x_{\beta_i}$	$\xrightarrow{x_A = (x_{A,1}, \ldots, x_{A,\ell}, \hat{x}_{A,1}, \ldots, \hat{x}_{A,\ell})}$ $\xleftarrow{x_B = (x_{B,1}, \ldots, x_{B,\ell}, \hat{x}_{B,1}, \ldots, \hat{x}_{B,\ell})}$	**for** $i \in [\ell]$ $x_{B,i} := b_i \star x_{\beta_i}$ $\hat{x}_{B,i} := \hat{b}_i \star x_{\beta_i}$
for $i \in [\ell]$ $z_i := (a_i \star x_{B,i}, \hat{a}_i \star x_{B,i}, a_i \star \hat{x}_{B,i})$		**for** $i \in [\ell]$ $z_i := (b_i \star x_{A,i}, b_i \star \hat{x}_{A,i}, \hat{b}_i \star x_{A,i})$
	$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_A, x_B, \mathsf{pw}, z_1, \ldots, z_\ell)$	

Optimizations

Decrease the Communication and Computation Cost

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1) \in \mathcal{X}^2,$	
	$\mathsf{pw} := (\beta_1, \ldots, \beta_\ell) \in \{0,1\}^\ell$	
$(a_1, \ldots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, \ldots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$	$\xrightarrow{x_{\mathsf{A}} = (x_{\mathsf{A},1}, \ldots, x_{\mathsf{A},\ell})}$	**for** $i \in [\ell]$
$x_{\mathsf{A},i} := a_i \star x_{\beta_i}$	$\xleftarrow{x_{\mathsf{B}} = (x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})}$	$x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
for $i \in [\ell]$		**for** $i \in [\ell]$
$z_i := a_i \star x_{\mathsf{B},i}$		$z_i := b_i \star x_{\mathsf{A},i}$
	$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_{\mathsf{A}}, x_{\mathsf{B}}, \mathsf{pw}, z_1, \ldots, z_\ell)$	

Decrease the Communication and Computation Cost

Alice A		**Bob** B

$$\mathsf{crs} := (x_0, x_1, \dots, x_{n-1}) \in \mathcal{X}^n,$$
$$\mathsf{pw} := (\beta_1, \dots, \beta_\ell) \in \{0,1\}^\ell$$

Alice A		Bob B
$(a_1, \dots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, \dots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$	$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \dots, x_{\mathsf{A},\ell})}$	**for** $i \in [\ell]$
$x_{\mathsf{A},i} := a_i \star x_{\beta_i}$	$\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \dots, x_{\mathsf{B},\ell})}$	$x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
for $i \in [\ell]$		**for** $i \in [\ell]$
$z_i := a_i \star x_{\mathsf{B},i}$		$z_i := b_i \star x_{\mathsf{A},i}$

$$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z_1, \dots, z_\ell)$$

Decrease the Communication and Computation Cost

Alice A | **Bob** B

$\mathsf{crs} := (x_0, x_1, \ldots, x_{n-1}) \in \mathcal{X}^n,$

$\mathsf{pw} := (\beta_1, \ldots, \beta_\ell) \in \{0, 1, \ldots, n-1\}^\ell$

Alice A		Bob B
$(a_1, \ldots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, \ldots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$	$\xrightarrow{x_A = (x_{A,1}, \ldots, x_{A,\ell})}$	**for** $i \in [\ell]$
$x_{A,i} := a_i \star x_{\beta_i}$	$\xleftarrow{x_B = (x_{B,1}, \ldots, x_{B,\ell})}$	$x_{B,i} := b_i \star x_{\beta_i}$
for $i \in [\ell]$		**for** $i \in [\ell]$
$z_i := a_i \star x_{B,i}$		$z_i := b_i \star x_{A,i}$

$$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_A, x_B, \mathsf{pw}, z_1, \ldots, z_\ell)$$

Decrease the Communication and Computation Cost

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1, \ldots, x_{n-1}) \in \mathcal{X}^n$,	
	$\mathsf{pw} := (\beta_1, \ldots, \beta_\ell) \in \{0, 1, \ldots, n-1\}^\ell$	
$(a_1, \ldots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, \ldots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$ $x_{\mathsf{A},i} := a_i \star x_{\beta_i}$	$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \ldots, x_{\mathsf{A},\ell})}$ $\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})}$	**for** $i \in [\ell]$ $x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
for $i \in [\ell]$ $z_i := a_i \star x_{\mathsf{B},i}$		**for** $i \in [\ell]$ $z_i := b_i \star x_{\mathsf{A},i}$
	$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z_1, \ldots, z_\ell)$	

$\Rightarrow$ By increasing the number of public parameters n, we can choose a smaller ℓ.

Use Twists in the Setup

Alice A		**Bob** B

$$\mathsf{crs} := (x_0, x_1, \dots, x_{n-1}) \in \mathcal{X}^n,$$
$$\mathsf{pw} := (\beta_1, \dots, \beta_\ell) \in \{0, 1, \dots, n-1\}^\ell$$

Alice A		Bob B
$(a_1, \dots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, \dots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$	$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \dots, x_{\mathsf{A},\ell})}$	**for** $i \in [\ell]$
$x_{\mathsf{A},i} := a_i \star x_{\beta_i}$	$\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \dots, x_{\mathsf{B},\ell})}$	$x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
for $i \in [\ell]$		**for** $i \in [\ell]$
$z_i := a_i \star x_{\mathsf{B},i}$		$z_i := b_i \star x_{\mathsf{A},i}$

$$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z_1, \dots, z_\ell)$$

Use Twists in the Setup

Alice A		**Bob** B
	$\mathsf{crs} := (x_0, x_1, \ldots, x_{n/2-1}) \in \mathcal{X}^{n/2}$,	
	$\mathsf{pw} := (\beta_1, \ldots, \beta_\ell) \in \{0, 1, \ldots, n-1\}^\ell$	
$(a_1, \ldots, a_\ell) \xleftarrow{\$} \mathcal{G}^\ell$		$(b_1, \ldots, b_\ell) \xleftarrow{\$} \mathcal{G}^\ell$
for $i \in [\ell]$		**for** $i \in [\ell]$
$x_{\mathsf{A},i} := a_i \star x_{\beta_i}$	$\xrightarrow{x_\mathsf{A} = (x_{\mathsf{A},1}, \ldots, x_{\mathsf{A},\ell})}$	$x_{\mathsf{B},i} := b_i \star x_{\beta_i}$
	$\xleftarrow{x_\mathsf{B} = (x_{\mathsf{B},1}, \ldots, x_{\mathsf{B},\ell})}$	
for $i \in [\ell]$		**for** $i \in [\ell]$
$z_i := a_i \star x_{\mathsf{B},i}$		$z_i := b_i \star x_{\mathsf{A},i}$
	$K := \mathsf{H}(\mathsf{A}, \mathsf{B}, x_\mathsf{A}, x_\mathsf{B}, \mathsf{pw}, z_1, \ldots, z_\ell)$	

Here we implicitly define $x_{n/2+i} := x_i^t$ for $i \in \{0, 1, \ldots, n-1\}$.

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

	Using OT [CDVW12, LGd21]	Com-GA-PAKE	X-GA-PAKE
Set Elements	384	16	32
Evaluations	1408	32	80
Rounds	4	3	1
Security Assumption	CDH	Gap CDH	Strong Square-Inverse
Tight	no	no	yes

Here we assume $\mathcal{PW} \subset \{0,1\}^{128}$ for all schemes, i.e.,

- $\ell = 128$ for the OT-based construction
- $\ell = 16$, $n = 8$ for our optimized variants

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

	Using OT [CDVW12, LGd21]	Com-GA-PAKE	X-GA-PAKE
Set Elements	384	16	32
Evaluations	1408	32	80
Rounds	4	3	1
Security Assumption	CDH	Gap CDH	Strong Square-Inverse
Tight	no	no	yes

Here we assume $\mathcal{PW} \subset \{0,1\}^{128}$ for all schemes, i.e.,

- $\ell = 128$ for the OT-based construction
- $\ell = 16$, $n = 8$ for our optimized variants

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

	Using OT [CDVW12, LGd21]	Com-GA-PAKE	X-GA-PAKE
Set Elements	384	16	32
Evaluations	1408	32	80
Rounds	4	3	1
Security Assumption	CDH	Gap CDH	Strong Square-Inverse
Tight	no	no	yes

Here we assume $\mathcal{PW} \subset \{0,1\}^{128}$ for all schemes, i.e.,

- $\ell = 128$ for the OT-based construction
- $\ell = 16$, $n = 8$ for our optimized variants

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

	Using OT [CDVW12, LGd21]	Com-GA-PAKE	X-GA-PAKE
Set Elements	384	16	32
Evaluations	1408	32	80
Rounds	4	3	1
Security Assumption	CDH	Gap CDH	Strong Square-Inverse
Tight	no	no	yes

Here we assume $\mathcal{PW} \subset \{0,1\}^{128}$ for all schemes, i.e.,

- $\ell = 128$ for the OT-based construction
- $\ell = 16$, $n = 8$ for our optimized variants

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

	Using OT [CDVW12, LGd21]	Com-GA-PAKE	X-GA-PAKE
Set Elements	384	16	32
Evaluations	1408	32	80
Rounds	4	3	1
Security Assumption	CDH	Gap CDH	Strong Square-Inverse
Tight	no	no	yes

Here we assume $\mathcal{PW} \subset \{0,1\}^{128}$ for all schemes, i.e.,

- $\ell = 128$ for the OT-based construction
- $\ell = 16$, $n = 8$ for our optimized variants

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

	Using OT [CDVW12, LGd21]	Com-GA-PAKE	X-GA-PAKE
Set Elements	384	16	32
Evaluations	1408	32	80
Rounds	4	3	1
Security Assumption	CDH	Gap CDH	Strong Square-Inverse
Tight	no	no	yes

Here we assume $\mathcal{PW} \subset \{0,1\}^{128}$ for all schemes, i.e.,

- $\ell = 128$ for the OT-based construction
- $\ell = 16$, $n = 8$ for our optimized variants

Outlook and Conclusion

Follow-Up and Open Questions

(1) Security proof in the QROM

- Need a stronger assumption [DHKKLR22b]: CDH with oracle access to a quantum DDH oracle, i.e., $\mathsf{DDH}(x, |\cdot\rangle, |\cdot\rangle) \to |b\rangle$
- Alternative: use an additional round of key confirmation!

Follow-Up and Open Questions

(1) Security proof in the QROM

- Need a stronger assumption [DHKKLR22b]: CDH with oracle access to a quantum DDH oracle, i.e., $\mathsf{DDH}(x, |\cdot\rangle, |\cdot\rangle) \to |b\rangle$
- Alternative: use an additional round of key confirmation!

(2) Analysis of our assumptions

- Use a (quantum) GGM and AGM for group actions [MZ22, DHKKLR22a]
- In the AGM Square-Inverse DH is equivalent to DLOG

Follow-Up and Open Questions

(1) Security proof in the QROM

- Need a stronger assumption [DHKKLR22b]: CDH with oracle access to a quantum DDH oracle, i.e., $\mathrm{DDH}(x, |\cdot\rangle, |\cdot\rangle) \to |b\rangle$
- Alternative: use an additional round of key confirmation!

(2) Analysis of our assumptions

- Use a (quantum) GGM and AGM for group actions [MZ22, DHKKLR22a]
- In the AGM Square-Inverse DH is equivalent to DLOG

(3) PAKE in practice and further efficiency improvements

Follow-Up and Open Questions

(1) Security proof in the QROM

- Need a stronger assumption [DHKKLR22b]: CDH with oracle access to a quantum DDH oracle, i.e., $\mathrm{DDH}(x, |\cdot\rangle, |\cdot\rangle) \to |b\rangle$
- Alternative: use an additional round of key confirmation!

(2) Analysis of our assumptions

- Use a (quantum) GGM and AGM for group actions [MZ22, DHKKLR22a]
- In the AGM Square-Inverse DH is equivalent to DLOG

(3) PAKE in practice and further efficiency improvements

(4) Asymmetric PAKE from group actions

Summary

Results

- Group actions with twists as abstraction for CSIDH
- The first direct constructions and provably secure PAKE protocols from CSIDH
- Better efficiency than generic constructions, e.g. based on OT

Summary

Results

- Group actions with twists as abstraction for CSIDH
- The first direct constructions and provably secure PAKE protocols from CSIDH
- Better efficiency than generic constructions, e.g. based on OT

Thank you!

ePrint: `ia.cr/2022/770`

doreen.riepel@rub.de

Navid Alamati, Luca De Feo, Hart Montgomery, and Sikhar Patranabis.
Cryptographic group actions and applications.
In Shiho Moriai and Huaxiong Wang, editors, ASIACRYPT 2020, Part II, volume 12492 of LNCS, pages 411–439. Springer, Heidelberg, December 2020.

Reza Azarderakhsh, David Jao, Brian Koziel, Jason T. LeGrow, Vladimir Soukharev, and Oleg Taraskin.
How not to create an isogeny-based PAKE.
In Mauro Conti, Jianying Zhou, Emiliano Casalicchio, and Angelo Spognardi, editors, ACNS 20, Part I, volume 12146 of LNCS, pages 169–186. Springer, Heidelberg, October 2020.

Jeremy Booher, Ross Bowden, Javad Doliskani, Tako Boris Fouotsa, Steven D. Galbraith, Sabrina Kunzweiler, Simon-Philipp Merz, Christophe Petit, Benjamin Smith, Katherine E. Stange, Yan Bo Ti, Christelle Vincent, José Felipe Voloch, Charlotte Weitkämper, and Lukas Zobernig.
Failing to hash into supersingular isogeny graphs.
Cryptology ePrint Archive, Report 2022/518, 2022.
`https://eprint.iacr.org/2022/518`.

Ran Canetti, Dana Dachman-Soled, Vinod Vaikuntanathan, and Hoeteck Wee.
Efficient password authenticated key exchange via oblivious transfer.
In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, PKC 2012, volume 7293 of LNCS, pages 449–466. Springer, Heidelberg, May 2012.

Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes.
CSIDH: An efficient post-quantum commutative group action.
In Thomas Peyrin and Steven Galbraith, editors, ASIACRYPT 2018, Part III, volume 11274 of LNCS, pages 395–427. Springer, Heidelberg, December 2018.

Julien Duman, Dominik Hartmann, Eike Kiltz, Sabrina Kunzweiler, Jonas Lehmann, and Doreen Riepel.
Generic group action models, 2022.

Julien Duman, Dominik Hartmann, Eike Kiltz, Sabrina Kunzweiler, Jonas Lehmann, and Doreen Riepel.
Group action key encapsulation and non-interactive key exchange in the QROM.
ASIACRYPT 2022, 2022.
`https://eprint.iacr.org/2022/1230`.

Yi-Fu Lai, Steven D. Galbraith, and Cyprien de Saint Guilhem.
Compact, efficient and UC-secure isogeny-based oblivious transfer.
In Anne Canteaut and François-Xavier Standaert, editors, EUROCRYPT 2021, Part I, volume 12696 of LNCS, pages 213–241. Springer, Heidelberg, October 2021.

Marzio Mula, Nadir Murru, and Federico Pintore.
On random sampling of supersingular elliptic curves.
Cryptology ePrint Archive, Paper 2022/528, 2022.
https://eprint.iacr.org/2022/528.

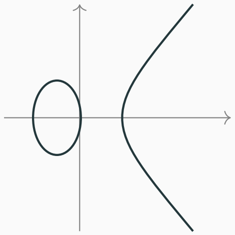
Hart Montgomery and Mark Zhandry.
Full quantum equivalence of group action DLog and CDH, and more.
ASIACRYPT 2022, 2022.

Elliptic Curves

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

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

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

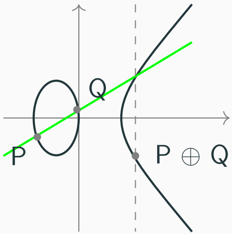


Elliptic Curves

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

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

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



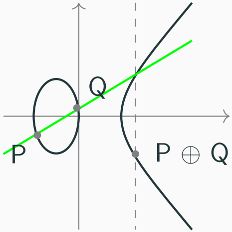
- Points of E form an additive group (with identity element ∞).
  - $\Rightarrow$ Classical ECC

Elliptic Curves

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

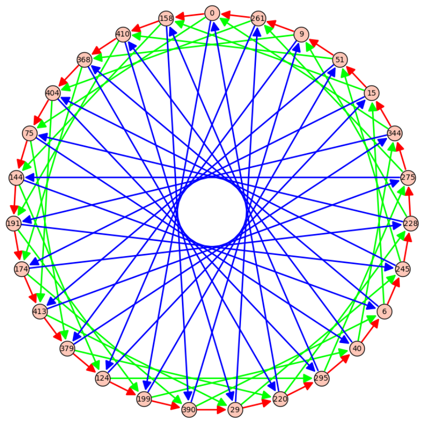
$$E : y^2 = x^3 + ax + b,$$

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



- Points of E form an additive group (with identity element ∞).
  $\Rightarrow$ Classical ECC
- An **isogeny** is a non-zero group homomorphism between elliptic curves $\phi : E \to E'$. The degree of ϕ is $\deg(\phi) = \# \ker(\phi)$ (for separable isogenies).

CSIDH Isogeny Graph

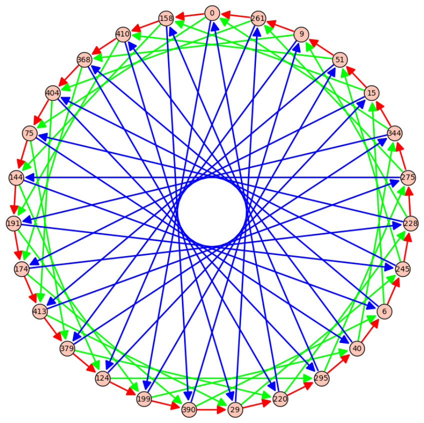


Isogeny graph over $\mathbb{F}_{419}$

vertices: supersingular elliptic curves over $\mathbb{F}_p$ (with prescribed endomorphism ring)

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

CSIDH Isogeny Graph



Isogeny graph over $\mathbb{F}_{419}$

vertices: supersingular elliptic curves over $\mathbb{F}_p$ (with prescribed endomorphism ring)

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

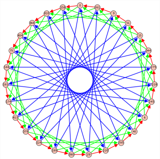
edges: isogenies of degrees $\ell_1, \ldots, \ell_n$ for small odd primes ℓ_i

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

CSIDH protocol

Setup

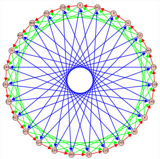
- prime $p = 4 \cdot \ell_1 \cdots \ell_n - 1$, where $\ell_1, \ldots, \ell_n$ are small odd primes.
- $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_p$.
- $\mathcal{X} = \{E : y^2 = x^3 + Ax^2 + x \text{ supersingular}, A \in \mathbb{F}_p\}$
- $M = \{-m, \ldots, m\}$ small range
- $\mathcal{G} = \langle \mathfrak{l}_1, \ldots, \mathfrak{l}_n \rangle$ is a "group of isogenies".



CSIDH protocol

Setup

- prime $p = 4 \cdot \ell_1 \cdots \ell_n - 1$, where $\ell_1, \dots, \ell_n$ are small odd primes.
- $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_p$.
- $\mathcal{X} = \{E : y^2 = x^3 + Ax^2 + x \text{ supersingular}, A \in \mathbb{F}_p\}$
- $M = \{-m, \dots, m\}$ small range
- $\mathcal{G} = \langle \mathfrak{l}_1, \dots, \mathfrak{l}_n \rangle$ is a "group of isogenies".



Key Exchange

Alice:

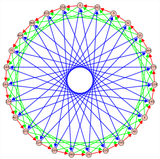
- $a = (a_1, \dots, a_n) \in M^n$
- $E_0 \xrightarrow{a} E_A$
- $E_A : y^2 = x^3 + Ax^2 + x$

E_A

$\rightarrow$

CSIDH protocol

Setup



- prime $p = 4 \cdot \ell_1 \cdots \ell_n - 1$, where $\ell_1, \ldots, \ell_n$ are small odd primes.
- $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_p$.
- $\mathcal{X} = \{E : y^2 = x^3 + Ax^2 + x \text{ supersingular}, A \in \mathbb{F}_p\}$
- $M = \{-m, \ldots, m\}$ small range
- $\mathcal{G} = \langle \mathfrak{l}_1, \ldots, \mathfrak{l}_n \rangle$ is a "group of isogenies".

Key Exchange

Alice:

- $a = (a_1, \ldots, a_n) \in M^n$
- $E_0 \xrightarrow{a} E_A$
- $E_A : y^2 = x^3 + Ax^2 + x$

E_A

$\rightarrow$

E_B

$\leftarrow$

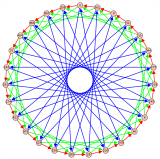
Bob:

- $b = (b_1, \ldots, b_n) \in M^n$
- $E_0 \xrightarrow{b} E_B$.
- $E_B : y^2 = x^3 + Bx^2 + x$

CSIDH protocol

Setup

- prime $p = 4 \cdot \ell_1 \cdots \ell_n - 1$, where $\ell_1, \ldots, \ell_n$ are small odd primes.
- $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_p$.
- $\mathcal{X} = \{E : y^2 = x^3 + Ax^2 + x \text{ supersingular}, A \in \mathbb{F}_p\}$
- $M = \{-m, \ldots, m\}$ small range
- $\mathcal{G} = \langle \mathfrak{l}_1, \ldots, \mathfrak{l}_n \rangle$ is a "group of isogenies".



Key Exchange

Alice:

- $a = (a_1, \ldots, a_n) \in M^n$
- $E_0 \xrightarrow{a} E_A$
- $E_A : y^2 = x^3 + Ax^2 + x$

E_A
$\rightarrow$
E_B
$\leftarrow$

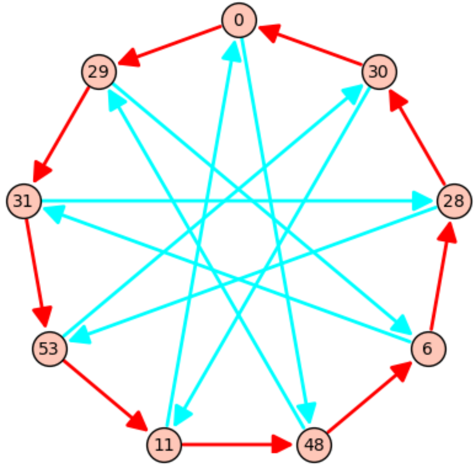
Bob:

- $b = (b_1, \ldots, b_n) \in M^n$
- $E_0 \xrightarrow{b} E_B$.
- $E_B : y^2 = x^3 + Bx^2 + x$

$$E_B \xrightarrow{a} E_{B*A} = E_{A*B} \xleftarrow{b} E_A$$

CSIDH example

- Alice: $a = (2, -1)$
  $\Rightarrow \; E_A : y^2 = x^3 + 6x^2 + x$

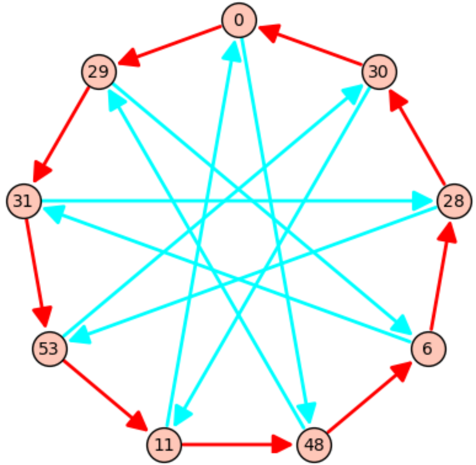


$p = 59 = 4 \cdot 3 \cdot 5 - 1.$

CSIDH example

- Alice: $a = (2, -1)$
  $\Rightarrow \; E_A : y^2 = x^3 + 6x^2 + x$

- Bob: $b = (-1, -2)$
  $\Rightarrow \; E_B : y^2 = x^3 + 28x^2 + x$



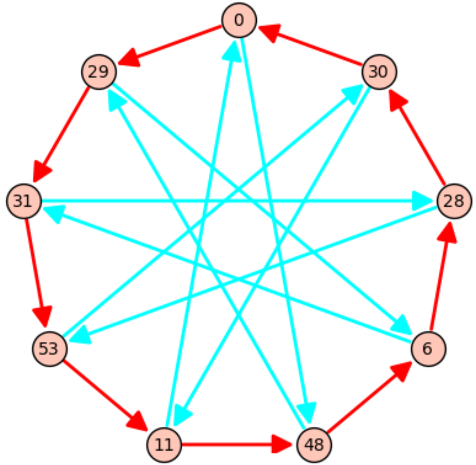
$p = 59 = 4 \cdot 3 \cdot 5 - 1.$

CSIDH example

- Alice: $a = (2, -1)$
  $\Rightarrow \ E_A : y^2 = x^3 + 6x^2 + x$

- Bob: $b = (-1, -2)$
  $\Rightarrow \ E_B : y^2 = x^3 + 28x^2 + x$

- shared secret:
  $E_{A*B} = E_{B*A}$:
  $y^2 = x^3 + 11x^2 + x$.



$p = 59 = 4 \cdot 3 \cdot 5 - 1.$