Low Memory Attacks on Small Key CSIDH

21st International Conference on Applied Cryptography and Network Security

(ACNS 2023)

Jesús-Javier Chi-Domínguez [1], Andre Esser [1], Sabrina Kunzweiler[2,3], and Alexander May[3]

[1] Cryptography Research Center, Technology Innovation Institute, Abu Dhabi, UAE

[2] Univ. Bordeaux, CNRS, Bordeaux INP, Inria, France

[3] Ruhr University Bochum, Germany

{jesus.dominguez, andre.esser}@tii.ae,
sabrina.kunzweiler@math.u-bordeaux.fr,
alex.may@rub.de

June 20, 2023

Technology
Innovation
Institute

REGA overview

Group Action

Let $(\mathcal{G}, \circ)$ 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: $(g \circ h) \star x = g \star (h \star x)$ for all $g, h \in \mathcal{G}$ and $x \in \mathcal{X}$.

Restricted Effective Group Action

Let $(\mathcal{G}, \mathcal{X}, \star)$ be a group action and let $\mathbf{g} = (g_1, \ldots, g_n)$ be a set of elements in $\mathcal{G}$ and denote $\mathcal{H} = \langle g_1, \ldots, g_n \rangle$ for the subgroup generated by these elements. Assume that the following properties are satisfied:

1. $\mathcal{G}$ is finite, commutative, and $n = \mathrm{poly}(\log(\#\mathcal{H}))$.
2. $\mathcal{X}$ is finite, and there exist efficient algorithms for membership testing and computing a unique representation.
3. There exists a distinguished element $\tilde{x} \in \mathcal{X}$ with known representation.
4. There exists an efficient algorithm that given $g_i \in \mathbf{g}$ and $x \in \mathcal{X}$, outputs $g_i \star x$ and $g_i^{-1} \star x$.

Then we call $(\mathcal{G}, \mathcal{H}, \mathcal{X}, \star, \tilde{x})$ a restricted effective group action (REGA).

Group Action

Let $(\mathcal{G}, \circ)$ 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: $(g \circ h) \star x = g \star (h \star x)$ for all $g, h \in \mathcal{G}$ and $x \in \mathcal{X}$.

Restricted Effective Group Action

Let $(\mathcal{G}, \mathcal{X}, \star)$ be a group action and let $\mathbf{g} = (g_1, ..., g_n)$ be a set of elements in $\mathcal{G}$ and denote $\mathcal{H} = \langle g_1, \ldots, g_n \rangle$ for the subgroup generated by these elements. Assume that the following properties are satisfied:

1. $\mathcal{G}$ is finite, commutative, and $n = \mathrm{poly}(\log(\#\mathcal{H}))$.
2. $\mathcal{X}$ is finite, and there exist efficient algorithms for membership testing and computing a unique representation.
3. There exists a distinguished element $\tilde{x} \in \mathcal{X}$ with known representation.
4. There exists an efficient algorithm that given $g_i \in \mathbf{g}$ and $x \in \mathcal{X}$, outputs $g_i \star x$ and $g_i^{-1} \star x$.

Then we call $(\mathcal{G}, \mathcal{H}, \mathcal{X}, \star, \tilde{x})$ a restricted effective group action (REGA).

REGA overview

Vector representation. Let $(\mathcal{G}, \mathcal{H}, \mathcal{X}, \star, \tilde{x})$ be a REGA with $\mathbf{g} = (g_1, \ldots, g_n)$. Elements in $\mathcal{H}$ can be represented as vectors $\mathbf{v} \in \mathbb{Z}^n$ under the mapping $\phi : \mathbb{Z}^n \to \mathcal{H}$, where

$$\phi : \mathbf{v} = (v_1, \ldots, v_n) \mapsto \prod_{i=1}^{n} {g_i}^{v_i}.$$

Via the map ϕ, we define the action of $\mathbb{Z}^n$ on $\mathcal{X}$. Slightly abusing notation, we denote $\mathbf{v} \star x = \phi(\mathbf{v}) \star x$.

REGA-based Diffie-Hellman protocol

Setup: A REGA $(\mathcal{G}, \mathcal{H}, \mathcal{X}, \star, \tilde{x})$ with $\mathbf{g} = (g_1, \ldots, g_n)$ and a finite set $\mathrm{SK} \subset \mathbb{Z}^n$.

$$
\begin{array}{rcl}
\text{Alice} & & \text{Bob} \\
\mathbf{a} \xleftarrow{\$} \mathrm{SK} & & \mathbf{b} \xleftarrow{\$} \mathrm{SK} \\
x_a \leftarrow \mathbf{a} \star \tilde{x} & & x_b \leftarrow \mathbf{b} \star \tilde{x} \\
 & \xrightarrow{\quad x_a \quad} & \\
 & \xleftarrow{\quad x_b \quad} & \\
K_a \leftarrow \mathbf{a} \star x_b = (\mathbf{a} + \mathbf{b}) \star \tilde{x} & & K_b \leftarrow \mathbf{b} \star x_a = (\mathbf{b} + \mathbf{a}) \star \tilde{x}
\end{array}
$$

Figure: A REGA-based Diffie-Hellman protocol.

Security. For this protocol to be secure, the following problems need to be hard.

Setup: A REGA $(\mathcal{G}, \mathcal{H}, \mathcal{X}, \star, \tilde{x})$ with $\mathbf{g} = (g_1, \ldots, g_n)$ and a finite set $\mathrm{SK} \subset \mathbb{Z}^n$.

Alice		Bob
$\mathbf{a} \xleftarrow{\$} \mathrm{SK}$		$\mathbf{b} \xleftarrow{\$} \mathrm{SK}$
$x_a \leftarrow \mathbf{a} \star \tilde{x}$		$x_b \leftarrow \mathbf{b} \star \tilde{x}$
	$\xrightarrow{x_a}$	
	$\xleftarrow{x_b}$	
$K_a \leftarrow \mathbf{a} \star x_b = (\mathbf{a} + \mathbf{b}) \star \tilde{x}$		$K_b \leftarrow \mathbf{b} \star x_a = (\mathbf{b} + \mathbf{a}) \star \tilde{x}$

Figure: A REGA-based Diffie-Hellman protocol.

Security. For this protocol to be secure, the following problems need to be hard.

1. GA-DLOG: Given $(x, y) \in \mathcal{X}^2$, determine $g \in \mathcal{G}$ such that $y = g \star x$.
2. GA-CDH: Given $(x, y, z) \in \mathcal{X}^3$, find $w \in \mathcal{X}$ such that there exists $g \in \mathcal{G}$ with $y = g \star x$ and $w = g \star z$.

Group actions satisfying these hardness assumptions are known as *cryptographic group actions* [1].

Setup: A REGA $(\mathcal{G}, \mathcal{H}, \mathcal{X}, \star, \tilde{x})$ with $\mathbf{g} = (g_1, \ldots, g_n)$ and a finite set $\mathrm{SK} \subset \mathbb{Z}^n$.

Alice		Bob
$\mathbf{a} \xleftarrow{\$} \mathrm{SK}$		$\mathbf{b} \xleftarrow{\$} \mathrm{SK}$
$x_a \leftarrow \mathbf{a} \star \tilde{x}$		$x_b \leftarrow \mathbf{b} \star \tilde{x}$
	$\xrightarrow{x_a}$	
	$\xleftarrow{x_b}$	
$K_a \leftarrow \mathbf{a} \star x_b = (\mathbf{a} + \mathbf{b}) \star \tilde{x}$		$K_b \leftarrow \mathbf{b} \star x_a = (\mathbf{b} + \mathbf{a}) \star \tilde{x}$

Figure: A REGA-based Diffie-Hellman protocol.

Security. For this protocol to be secure, the following problems need to be hard.

1. GA-DLOG: Given $(x, y) \in \mathcal{X}^2$, determine $g \in \mathcal{G}$ such that $y = g \star x$.
2. GA-CDH: Given $(x, y, z) \in \mathcal{X}^3$, find $w \in \mathcal{X}$ such that there exists $g \in \mathcal{G}$ with $y = g \star x$ and $w = g \star z$.
3. REGA-DLOG$_{\mathrm{SK}}$: Given $(x, y) \in \mathcal{X}^2$, determine $\mathbf{v} \in \mathrm{SK}$ such that $y = \mathbf{v} \star x$ if such a vector $\mathbf{v}$ exists.

Group actions satisfying these hardness assumptions are known as *cryptographic group actions* [1].

Lemma

Let $(\mathcal{G}, \mathcal{H}, \mathcal{X}, \star, \tilde{x})$ *be a* REGA *with* $\mathbf{g} = (g_1, \ldots, g_n)$. *Let* $m \in \mathbb{N}$ *and consider*

$$\mathrm{SK}_1 = \{-m, \ldots, m\}^n, \quad \mathrm{SK}_2 = \{0, \ldots, 2m\}^n, \quad \textit{and} \quad \mathrm{SK}_3 = \{-2m, -2(m-1), \ldots, 2m\}^n.$$

Then REGA-DLOG$_{\mathrm{SK}_1}$ *and* REGA-DLOG$_{SK_2}$ *are equivalent.*

Further let $\tilde{\mathcal{H}} = \{g \circ g \mid g \in \mathcal{H}\} \subset \mathcal{H}$*, and* $\tilde{\mathbf{g}} = (\tilde{g_1} = g_1 \circ g_1, \ldots, \tilde{g_n} = g_n \circ g_n)$.

2. *An instance* $(\mathcal{G}, \mathcal{H}, \mathcal{X}, \star, \tilde{x}, \mathbf{g}, x, y)$ *of* REGA-DLOG$_{\mathrm{SK}_3}$ *can be transformed to an instance* $\left(\mathcal{G}, \tilde{\mathcal{H}}, \mathcal{X}, \star, \tilde{x}, \tilde{\mathbf{g}}, x, y\right)$ *of* REGA-DLOG$_{\mathrm{SK}_1}$.
3. *In particular if* $\#\mathcal{H}$ *is odd, then* REGA-DLOG$_{\mathrm{SK}_3}$ *reduces to* REGA-DLOG$_{\mathrm{SK}_1}$.

Isogeny-based REGAs. The analysis in the original CSIDH paper [2] illustrates a practical example of a REGA, where

$\mathcal{G}$ is the ideal class group $cl(\mathcal{O})$ with $\mathcal{O} = \mathbb{Z}[\pi]$,

$\mathcal{H}$ is the subgroup generated by $\mathbf{g} = ([\mathfrak{l}_1], \ldots, [\mathfrak{l}_n])$ with $\mathfrak{l}_i = (\ell_i, \pi - 1) \lhd \mathcal{O}$,

$\mathcal{X}$ is $\mathcal{E}\ell\ell_p(\mathcal{O}) = \{E_A : y^2 = x^3 + Ax^2 + x \mid A \in \mathbb{F}_p$ and E_A is supersingular$\}$,

$\star$ is the CSIDH group action, and

$\tilde{x}$ is the supersingular curve $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_p$.

Lemma

Let $(\mathcal{G}, \mathcal{H}, \mathcal{X}, \star, \tilde{x})$ be a REGA with $\mathbf{g} = (g_1, \ldots, g_n)$. Let $m \in \mathbb{N}$ and consider

$$\mathrm{SK}_1 = \{-m, \ldots, m\}^n, \quad \mathrm{SK}_2 = \{0, \ldots, 2m\}^n, \quad \text{and} \quad \mathrm{SK}_3 = \{-2m, -2(m-1), \ldots, 2m\}^n.$$

Then REGA-DLOG$_{\mathrm{SK}_1}$ and REGA-DLOG$_{SK_2}$ are equivalent.
Further let $\tilde{\mathcal{H}} = \{g \circ g \mid g \in \mathcal{H}\} \subset \mathcal{H}$, and $\tilde{\mathbf{g}} = (\tilde{g}_1 = g_1 \circ g_1, \ldots, \tilde{g}_n = g_n \circ g_n)$.

2. *An instance $(\mathcal{G}, \mathcal{H}, \mathcal{X}, \star, \tilde{x}, \mathbf{g}, x, y)$ of REGA-DLOG$_{\mathrm{SK}_3}$ can be transformed to an instance $\left(\mathcal{G}, \tilde{\mathcal{H}}, \mathcal{X}, \star, \tilde{x}, \tilde{\mathbf{g}}, x, y\right)$ of REGA-DLOG$_{\mathrm{SK}_1}$.*
3. *In particular if $\#\mathcal{H}$ is odd, then REGA-DLOG$_{\mathrm{SK}_3}$ reduces to REGA-DLOG$_{\mathrm{SK}_1}$.*

Isogeny-based REGAs. The analysis in the original CSIDH paper [2] illustrates a practical example of a REGA, where

$$\begin{aligned}
\mathcal{G} &\text{ is the ideal class group } cl(\mathcal{O}) \text{ with } \mathcal{O} = \mathbb{Z}[\pi],\\
\mathcal{H} &\text{ is the subgroup generated by } \mathbf{g} = ([\mathfrak{l}_1], \ldots, [\mathfrak{l}_n]) \text{ with } \mathfrak{l}_i = (\ell_i, \pi - 1) \lhd \mathcal{O},\\
\mathcal{X} &\text{ is } \mathcal{E}\ell\ell_p(\mathcal{O}) = \{E_A : y^2 = x^3 + Ax^2 + x \mid A \in \mathbb{F}_p \text{ and } E_A \text{ is supersingular}\},\\
\star &\text{ is the CSIDH group action, and}\\
\tilde{x} &\text{ is the supersingular curve } E_0 : y^2 = x^3 + x \text{ over } \mathbb{F}_p.
\end{aligned}$$

Given $x, y \in \mathcal{X}$, we want to find $\mathbf{v} \in \mathrm{SK}_1$ with $y = \mathbf{v} \star x$. Let us focus on the case $m = 1$ for simplicity. Let $N = \#\mathcal{H}$, $N_m = 3^n \ll N$, and $W = 3^{\omega n}$ for some $\omega \in [\![0, 0.5]\!]$.
Let

$$\mathrm{SK}_1 = \{-1, 0, 1\}^n, \quad \mathrm{SK}_2 = \{0, 1, 2\}^n, \quad \text{and} \quad \mathrm{SK}_3 = \{-2, 0, 2\}^n.$$

- Pollard-style random walks based on [5, 4]. Time complexity: $\mathcal{O}(\sqrt{N})$;
- Meet-in-the-Middle (MitM). Memory and Time complexities: $\mathcal{O}(3^{0.5n})$.
- Parallel Collision Search (PCS): Memory complexity $\widetilde{\mathcal{O}}(W)$, and Time complexity $\widetilde{\mathcal{O}}\left(3^{(0.75-0.5\omega)n}\right)$.
- Representation-based Approach (This work): $\alpha = 1/3$ implies Memory complexity $\widetilde{\mathcal{O}}(W)$, and Time complexity $\widetilde{\mathcal{O}}\left(3^{(0.675-0.5\omega)n}\right)$ when $\omega \leq 0.22$.
- Partial Representation (This work):

Given $x, y \in \mathcal{X}$, we want to find $\mathbf{v} \in \mathrm{SK}_1$ with $y = \mathbf{v} \star x$. Let us focus on the case $m = 1$ for simplicity. Let $N = \#\mathcal{H}$, $N_m = 3^n \ll N$, and $W = 3^{\omega n}$ for some $\omega \in [\![0, 0.5]\!]$.
Let

$$\mathrm{SK}_1 = \{-1, 0, 1\}^n, \quad \mathrm{SK}_2 = \{0, 1, 2\}^n, \quad \text{and} \quad \mathrm{SK}_3 = \{-2, 0, 2\}^n.$$

- Pollard-style random walks based on [5, 4]. Time complexity: $\mathcal{O}(\sqrt{N})$;
- Meet-in-the-Middle (MitM). Memory and Time complexities: $\mathcal{O}(3^{0.5n})$.
- Parallel Collision Search (PCS): Memory complexity $\widetilde{\mathcal{O}}(W)$, and Time complexity $\widetilde{\mathcal{O}}\left(3^{(0.75-0.5\omega)n}\right)$.
- Representation-based Approach (This work): $\alpha = 1/3$ implies Memory complexity $\widetilde{\mathcal{O}}(W)$, and Time complexity $\widetilde{\mathcal{O}}\left(3^{(0.675-0.5\omega)n}\right)$ when $\omega \leq 0.22$.
- Partial Representation (This work):

Adapting Techniques to the REGA-DLOG$_m$ Setting

Given $x, y \in \mathcal{X}$, we want to find $\mathbf{v} \in \mathrm{SK}_1$ with $y = \mathbf{v} \star x$. Let us focus on the case $m = 1$ for simplicity. Let $N = \#\mathcal{H}$, $N_m = 3^n \ll N$, and $W = 3^{\omega n}$ for some $\omega \in [\![0, 0.5]\!]$.
Let

$$S_{m,0} := \{-1, 0, 1\}^{\frac{n}{2}} \times \{0\}^{\frac{n}{2}}, \quad \text{and} \quad S_{m,1} := \{0\}^{\frac{n}{2}} \times \{1, 0, 1\}^{\frac{n}{2}}.$$

- Pollard-style random walks based on [5, 4]. Time complexity: $\mathcal{O}(\sqrt{N})$;
- Meet-in-the-Middle (MitM). Memory and Time complexities: $\mathcal{O}(3^{0.5n})$. It reduces to finding two vectors $\mathbf{v}_0 \in S_{m,0}$ and $\mathbf{v}_1 \in S_{m,1}$ with $\mathbf{v}_0 \star x = (-\mathbf{v}_1) \star y$. The solution is $\mathbf{v} = \mathbf{v}_0 + \mathbf{v}_1$.
- Parallel Collision Search (PCS): Memory complexity $\widetilde{\mathcal{O}}(W)$, and Time complexity $\widetilde{\mathcal{O}}\left(3^{(0.75-0.5\omega)n}\right)$.
- Representation-based Approach (This work): $\alpha = 1/3$ implies Memory complexity $\widetilde{\mathcal{O}}(W)$, and Time complexity $\widetilde{\mathcal{O}}\left(3^{(0.675-0.5\omega)n}\right)$ when $\omega \leq 0.22$.
- Partial Representation (This work):

Given $x, y \in \mathcal{X}$, we want to find $\mathbf{v} \in \mathrm{SK}_1$ with $y = \mathbf{v} \star x$. Let us focus on the case $m = 1$ for simplicity. Let $N = \#\mathcal{H}$, $N_m = 3^n \ll N$, and $W = 3^{\omega n}$ for some $\omega \in [\![0, 0.5]\!]$.
Let

$$S_m^{n/2} := \{-m, \ldots, m\}^{\frac{n}{2}}, \quad \mathrm{H}\colon \{0,1\}^* \to S_m^{n/2}, \quad f_0 : \mathbf{v} \mapsto \mathrm{H}(\mathbf{v} \star x), \text{ and } \quad f_1 : \mathbf{v} \mapsto \mathrm{H}\big((-\mathbf{v}) \star y\big)$$

- Pollard-style random walks based on [5, 4]. Time complexity: $\mathcal{O}(\sqrt{N})$;
- Meet-in-the-Middle (MitM). Memory and Time complexities: $\mathcal{O}(3^{0.5n})$.
- Parallel Collision Search (PCS): Memory complexity $\widetilde{\mathcal{O}}(W)$, and Time complexity $\widetilde{\mathcal{O}}\left(3^{(0.75-0.5\omega)n}\right)$.
It reduces to finding the *golden* collision $f_0(\mathbf{v}_0) = f_1(\mathbf{v}_1)$ that leads to $\mathbf{v} = (\mathbf{v}_0, \mathbf{0}) + (\mathbf{0}, \mathbf{v}_1)$.
- Representation-based Approach (This work): $\alpha = 1/3$ implies Memory complexity $\widetilde{\mathcal{O}}(W)$, and Time complexity $\widetilde{\mathcal{O}}\left(3^{(0.675-0.5\omega)n}\right)$ when $\omega \leq 0.22$.
- Partial Representation (This work):

Adapting Techniques to the REGA-DLOG$_m$ Setting

Given $x, y \in \mathcal{X}$, we want to find $\mathbf{v} \in \mathrm{SK}_1$ with $y = \mathbf{v} \star x$. Let us focus on the case $m = 1$ for simplicity. Let $N = \#\mathcal{H}$, $N_m = 3^n \ll N$, and $W = 3^{\omega n}$ for some $\omega \in [\![0, 0.5]\!]$.
Let $\alpha \in [\![0, 1]\!]$, $\quad f_0 : \mathbf{v} \mapsto \mathrm{H}(\mathbf{v} \star x)$, $\quad f_1 : \mathbf{v} \mapsto \mathrm{H}\big((-\mathbf{v}) \star y\big)$,
$\mathcal{T}^n(\alpha) := \{\mathbf{x} \in \{-1, 0, 1\}^n \mid \mathbf{x}$ contains exactly αn $(+1)$ and αn (-1) entries$\}$, and $\quad \mathrm{H} \colon \{0, 1\}^* \to \mathcal{T}^n(\alpha)$.

- Pollard-style random walks based on [5, 4]. Time complexity: $\mathcal{O}(\sqrt{N})$;
- Meet-in-the-Middle (MitM). Memory and Time complexities: $\mathcal{O}(3^{0.5n})$.
- Parallel Collision Search (PCS): Memory complexity $\widetilde{\mathcal{O}}\,(W)$, and Time complexity $\widetilde{\mathcal{O}}\left(3^{(0.75-0.5\omega)n}\right)$.
- Representation-based Approach (This work): $\alpha = 1/3$ implies Memory complexity $\widetilde{\mathcal{O}}\,(W)$, and Time complexity $\widetilde{\mathcal{O}}\left(3^{(0.675-0.5\omega)n}\right)$ when $\omega \leq 0.22$. The solution is $\mathbf{v} = \mathbf{v}_0 + \mathbf{v}_1$.
- Partial Representation (This work):

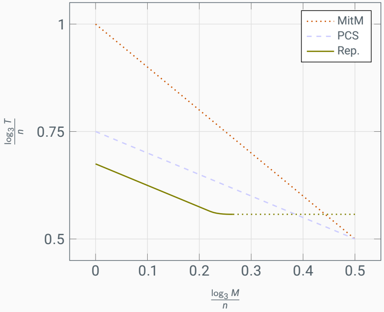
Given $x, y \in \mathcal{X}$, we want to find $\mathbf{v} \in \mathrm{SK}_1$ with $y = \mathbf{v} \star x$. Let us focus on the case $m = 1$ for simplicity. Let $N = \#\mathcal{H}$, $N_m = 3^n \ll N$, and $W = 3^{\omega n}$ for some $\omega \in [\![0, 0.5]\!]$.
Let $\alpha \in [\![0, 1]\!]$, $\quad f_0 : \mathbf{v} \mapsto \mathrm{H}(\mathbf{v} \star x)$, $\quad f_1 : \mathbf{v} \mapsto \mathrm{H}\big((-\mathbf{v}) \star y\big)$,
$\mathcal{T}^n(\alpha) := \{\mathbf{x} \in \{-1, 0, 1\}^n \mid \mathbf{x}$ contains exactly αn $(+1)$ and αn (-1) entries$\}$, and $\quad \mathrm{H}\colon \{0,1\}^* \to \mathcal{T}^n(\alpha)$.

- Pollard-style random walks based on [5, 4]. Time complexity: $\mathcal{O}(\sqrt{N})$;
- Meet-in-the-Middle (MitM). Memory and Time complexities: $\mathcal{O}(3^{0.5n})$.
- Parallel Collision Search (PCS): Memory complexity $\widetilde{\mathcal{O}}\,(W)$, and Time complexity $\widetilde{\mathcal{O}}\left(3^{(0.75-0.5\omega)n}\right)$.
- Representation-based Approach (This work): $\alpha = 1/3$ implies Memory complexity $\widetilde{\mathcal{O}}\,(W)$, and Time complexity $\widetilde{\mathcal{O}}\left(3^{(0.675-0.5\omega)n}\right)$ when $\omega \leq 0.22$.
- Partial Representation (This work): This time $f_i\colon D_i \to D$ where $D := \mathcal{T}^{\frac{(1-\delta)n}{2}}(1/3) \times \mathcal{T}^{\delta n}(\alpha)$,

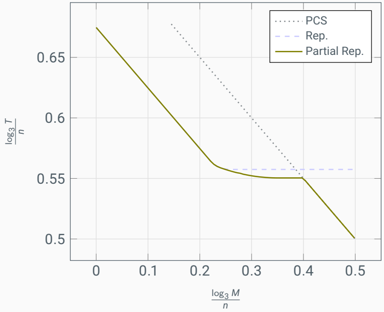
$$\begin{aligned} D_0 &:= \mathcal{T}^{\frac{(1-\delta)n}{2}}(1/3) \times \{0\}^{\frac{(1-\delta)n}{2}} \times \mathcal{T}^{\delta n}(\alpha) \quad \text{and} \\ D_1 &:= \{0\}^{\frac{(1-\delta)n}{2}} \times \mathcal{T}^{\frac{(1-\delta)n}{2}}(1/3) \times \mathcal{T}^{\delta n}(\alpha), \end{aligned} \tag{1}$$

The solution is $\mathbf{v} = \mathbf{v}_0 + \mathbf{v}_1$.

Adapting Techniques to the REGA-DLOG$_m$ Setting

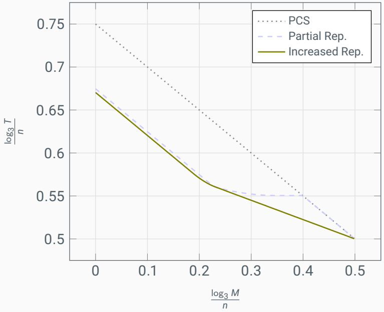


(a) Complexity of PCS, MitM and the representation-based trade-off

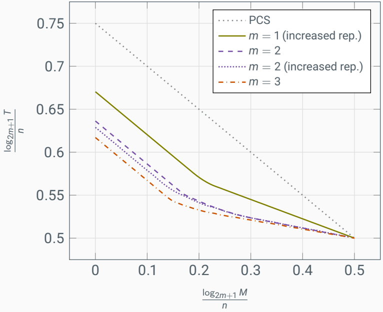


(b) Complexity of PCS, the representation trade-off, and partial representations.

Adapting Techniques to the REGA-DLOG$_m$ Setting



(a) Complexity of different approaches.



(b) Complexity for different choices of m.

Figure: On the left: Comparison of different representation based methods.
On the right: Comparison of representation based methods for different m.

Potential Impact on Bit Security Level: CSIDH scenario

In the SQALEd-CSIDH [3], three concrete parameter instantiations for ternary-key are given, respectively, aiming at satisfying NIST security level L_1, L_2 and L_3. To match the security definition of category L_i the authors impose restrictions on the memory and time complexity of $M_i = 2^{w_i}$ and $T_i = 2^{t_i}$ with

$$(w_1, w_2, w_3) = (80, 100, 119) \quad \text{and} \quad (t_1, t_2, t_3) = (128, 128, 192).$$

Additionally,

- The number of generators n_i are equal to $n_1 = 139$ for L_1, $n_2 = 148$ for L_2 and $n_3 = 210$ for L_3.
- The security of those parameter sets is determined via the PCS time-memory trade-off.
- In the memory restrictions, the authors of [3] conservatively ignore polynomial factors.

Consequently, it holds $M_i = 3^{c_i n_i} = 2^{w_i}$, which allows to determine the asymptotic memory exponent as $c_i = \frac{w_i}{n_i \cdot \log_2 3}$. Then, we obtain

1. $c_1 \approx 0.3631$ and running time $T_{\mathrm{PCS}} = 3^{0.5685n}$.
2. $c_2 \approx 0.4263$ and running time $T_{\mathrm{PCS}} = 3^{0.5369n}$.
3. $c_3 \approx 0.3575$ and running time $T_{\mathrm{PCS}} = 3^{0.5713n}$.

Potential Impact on Bit Security Level: CSIDH scenario

In the SQALEd-CSIDH [3], three concrete parameter instantiations for ternary-key are given, respectively, aiming at satisfying NIST security level L_1, L_2 and L_3. To match the security definition of category L_i the authors impose restrictions on the memory and time complexity of $M_i = 2^{w_i}$ and $T_i = 2^{t_i}$ with

$$(w_1, w_2, w_3) = (80, 100, 119) \quad \text{and} \quad (t_1, t_2, t_3) = (128, 128, 192).$$

Additionally,

- The number of generators n_i are equal to $n_1 = 139$ for L_1, $n_2 = 148$ for L_2 and $n_3 = 210$ for L_3.
- The security of those parameter sets is determined via the PCS time-memory trade-off.
- In the memory restrictions, the authors of [3] conservatively ignore polynomial factors.

Consequently, it holds $M_i = 3^{c_i n_i} = 2^{w_i}$, which allows to determine the asymptotic memory exponent as $c_i = \frac{w_i}{n_i \cdot \log_2 3}$. Then, we obtain

1. $c_1 \approx 0.3631$ and running time $T_{\mathrm{PCS}} = 3^{0.5685n}$.
2. $c_2 \approx 0.4263$ and running time $T_{\mathrm{PCS}} = 3^{0.5369n}$.
3. $c_3 \approx 0.3575$ and running time $T_{\mathrm{PCS}} = 3^{0.5713n}$.

Potential Impact on Bit Security Level: CSIDH scenario

In the SQALEd-CSIDH [3], three concrete parameter instantiations for ternary-key are given, respectively, aiming at satisfying NIST security level L_1, L_2 and L_3. To match the security definition of category L_i the authors impose restrictions on the memory and time complexity of $M_i = 2^{w_i}$ and $T_i = 2^{t_i}$ with

$$(w_1, w_2, w_3) = (80, 100, 119) \quad \text{and} \quad (t_1, t_2, t_3) = (128, 128, 192).$$

Additionally,

- The number of generators n_i are equal to $n_1 = 139$ for L_1, $n_2 = 148$ for L_2 and $n_3 = 210$ for L_3.
- The security of those parameter sets is determined via the PCS time-memory trade-off.
- In the memory restrictions, the authors of [3] conservatively ignore polynomial factors.

Consequently, it holds $M_i = 3^{c_i n_i} = 2^{w_i}$, which allows to determine the asymptotic memory exponent as $c_i = \frac{w_i}{n_i \cdot \log_2 3}$. Then, we obtain

1. $c_1 \approx 0.3631$ and running time $T_{\mathrm{PCS}} = 3^{0.5685n}$. This work: $T_{\mathrm{Rep}} = 3^{0.5316n}$ (gain of 8.13 bits).
2. $c_2 \approx 0.4263$ and running time $T_{\mathrm{PCS}} = 3^{0.5369n}$. This work: $T_{\mathrm{Rep}} = 3^{0.5174n}$ (gain of 4.57 bits).
3. $c_3 \approx 0.3575$ and running time $T_{\mathrm{PCS}} = 3^{0.5713n}$. This work: $T_{\mathrm{Rep}} = 3^{0.5330n}$ (gain of 12.75 bits).

Questions?

Thanks for attending!

References I

[1] 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.

[2] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes.
CSIDH: an efficient post-quantum commutative group action.
In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part III*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427. Springer, 2018.

[3] Jorge Chávez-Saab, Jesús-Javier Chi-Domínguez, Samuel Jaques, and Francisco Rodríguez-Henríquez.
The SQALE of CSIDH: sublinear vélu quantum-resistant isogeny action with low exponents.
J. Cryptogr. Eng., 12(3):349–368, 2022.

[4] Steven Galbraith and Anton Stolbunov.
Improved algorithm for the isogeny problem for ordinary elliptic curves.
Applicable Algebra in Engineering, Communication and Computing, 24(2):107–131, 2013.

References II

[5] Steven D. Galbraith, Florian Hess, and Nigel P. Smart.
Extending the GHS Weil descent attack.
In Lars R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 29–44. Springer, Heidelberg, April / May 2002.