Swiss Crypto Day, 4th of April 2025

PEGASIS
Practical Efficient Class Group Action using 4-dimensional isogenies

Joint with Pierrick Dartois, Jonathan Komada Eriksen, Tako Boris Fouotsa, Arthur Herlédan Le Merdy, Riccardo Invernizzi, Damien Robert, Frederik Vercauteren and Benjamin Wesolowski

https://eprint.iacr.org/2025/401

Ryan Rueger
IBM Research Zurich & Technical University of Munich

PEGASIS

Cryptographic Group Action

PEGASIS

Cryptographic Group Action

$\rightsquigarrow G \curvearrowright X$: hard to recover g from (x, gx)

PEGASIS

Cryptographic Group Action

$\rightsquigarrow$ $G \curvearrowright X$: hard to recover g from (x, gx)

$\rightsquigarrow$ Can build many primitives: NIKE, (Threshold) Signatures, SSP-OT, PRF, ...

PEGASIS

Cryptographic Group Action

$\rightsquigarrow G \curvearrowright X$: hard to recover g from (x, gx)

$\rightsquigarrow$ Can build many primitives: NIKE, (Threshold) Signatures, SSP-OT, PRF, ...

Quantum Resistant

PEGASIS

Cryptographic Group Action

$\rightsquigarrow G \curvearrowright X$: hard to recover g from (x, gx)

$\rightsquigarrow$ Can build many primitives: NIKE, (Threshold) Signatures, SSP-OT, PRF, ...

Quantum Resistant

Asymptotically and Practically Efficient

PEGASIS

Cryptographic Group Action

$\rightsquigarrow G \curvearrowright X$: hard to recover g from (x, gx)

$\rightsquigarrow$ Can build many primitives: NIKE, (Threshold) Signatures, SSP-OT, PRF, ...

Quantum Resistant

Asymptotically and Practically Efficient

Arises from Isogeny Class Group Action between Supersingular Elliptic Curves

PEGASIS

Cryptographic Group Action

⇝ $G \curvearrowright X$: hard to recover g from (x, gx)

⇝ Can build many primitives: NIKE, (Threshold) Signatures, SSP-OT, PRF, ...

Quantum Resistant

Asymptotically and Practically Efficient

Arises from Isogeny Class Group Action between Supersingular Elliptic Curves

Unrestricted instantiation

⇝ Can compute gx efficiently for *all* g in G and x in X

PEGASIS

Cryptographic Group Action

$\rightsquigarrow$ $G \curvearrowright X$: hard to recover g from (x, gx)

$\rightsquigarrow$ Can build many primitives: NIKE, (Threshold) Signatures, SSP-OT, PRF, ...

Quantum Resistant

Asymptotically and Practically Efficient

Arises from Isogeny Class Group Action between Supersingular Elliptic Curves

Unrestricted instantiation

$\rightsquigarrow$ Can compute gx efficiently for *all* g in G and x in X

Before PEGASIS

Pick two {Asymptotically efficient, Practically efficient, Unrestricted}

What is restriction and why care?

Restricted action $G \curvearrowright X$

What is restriction and why care?

Restricted action $G \curvearrowright X$

Can only compute action gx efficiently for specific set of generators $g_1, \ldots, g_n$

What is restriction and why care?

Restricted action $G \curvearrowright X$

Can only compute action gx efficiently for specific set of generators $g_1, \ldots, g_n$

Evaluate $g = \prod g_i^{e_i}$ action by e_i-successive g_i-actions $\rightsquigarrow$ costs $O(\sum e_i)$

What is restriction and why care?

Restricted action $G \curvearrowright X$

Can only compute action gx efficiently for specific set of generators $g_1, \dots, g_n$

Evaluate $g = \prod g_i^{e_i}$ action by e_i-successive g_i-actions $\rightsquigarrow$ costs $O(\sum e_i)$

Problem (Efficiency)

Successive action becomes more expensive

What is restriction and why care?

Restricted action $G \curvearrowright X$

Can only compute action gx efficiently for specific set of generators $g_1, \dots, g_n$

Evaluate $g = \prod g_i^{e_i}$ action by e_i-successive g_i-actions $\rightsquigarrow$ costs $O(\sum e_i)$

Problem (Efficiency)
Successive action becomes more expensive

Problem (Security)
Building complex primitives is difficult

Results

		Lang.	128	256	375	512	1024
Restricted	CSIDH*	C	40ms				
	SQALE*	C					5.75s**
	dCTIDH*	C				350ms**	
Unrestricted	SCALLOP*	C++	35s	750s			
	SCALLOP-HD*	Sage	88s	1140s			
	PEARL-SCALLOP*	C++	30s	58s	710s		
	KLaPoTi	Sage	207s				
		Rust	1.95s				
	PEGASIS	Sage	1.53s	4.21s	10.5s	21.3s	121s

Table: *Measured on different hardware, **Converted from cycles to time @4GHz.

How higher dimensions can help

How higher dimensions can help

The Isogeny Class Group action

$X = \mathrm{Ell}_{\mathrm{SS}}(\mathcal{O}), G = \mathrm{Cl}(\mathcal{O})$

How higher dimensions can help

The Isogeny Class Group action

$X = \mathrm{Ell}_{\mathrm{SS}}(\mathcal{O})$, $G = \mathrm{Cl}(\mathcal{O})$

Action of $g = \prod g_i^{e_i}$ on E corresponds to computing an isogeny $E \to E_g$

How higher dimensions can help

The Isogeny Class Group action

$X = \mathrm{Ell}_{\mathrm{SS}}(\mathcal{O})$, $G = \mathrm{Cl}(\mathcal{O})$

Action of $g = \prod g_i^{e_i}$ on E corresponds to computing an isogeny $E \to E_g$

$\rightsquigarrow$ Cost in dimension 1 is $O(\sum e_i)$

How higher dimensions can help

The Isogeny Class Group action

$X = \mathrm{Ell}_{\mathrm{SS}}(\mathcal{O})$, $G = \mathrm{Cl}(\mathcal{O})$

Action of $g = \prod g_i^{e_i}$ on E corresponds to computing an isogeny $E \to E_g$

$\rightsquigarrow$ Cost in dimension 1 is $O(\sum e_i)$

Idea

Given $g = \prod g_i^{e_i}$, find equivalent element $h = \prod g_i^{f_i}$ $\quad (\forall E \in \mathrm{Ell}_{\mathrm{SS}}(\mathcal{O}) : hE = gE)$

How higher dimensions can help

The Isogeny Class Group action

$X = \mathrm{Ell}_{\mathrm{SS}}(\mathcal{O})$, $G = \mathrm{Cl}(\mathcal{O})$

Action of $g = \prod g_i^{e_i}$ on E corresponds to computing an isogeny $E \to E_g$

$\rightsquigarrow$ Cost in dimension 1 is $O(\sum e_i)$

Idea

Given $g = \prod g_i^{e_i}$, find equivalent element $h = \prod g_i^{f_i}$ $\quad (\forall E \in \mathrm{Ell}_{\mathrm{SS}}(\mathcal{O}) : hE = gE)$

$\rightsquigarrow$ 2-dimensional isogeny $E \times E \to E_g \times E_{h^{-1}}$ is easy!

How higher dimensions can help

The Isogeny Class Group action

$X = \mathrm{Ell}_{\mathrm{SS}}(\mathcal{O})$, $G = \mathrm{Cl}(\mathcal{O})$

Action of $g = \prod g_i^{e_i}$ on E corresponds to computing an isogeny $E \to E_g$

$\rightsquigarrow$ Cost in dimension 1 is $O(\sum e_i)$

Idea

Given $g = \prod g_i^{e_i}$, find equivalent element $h = \prod g_i^{f_i}$ $\quad (\forall E \in \mathrm{Ell}_{\mathrm{SS}}(\mathcal{O}) : hE = gE)$

$\rightsquigarrow$ 2-dimensional isogeny $E \times E \to E_g \times E_{h^{-1}}$ is easy!

Slogan

"*Things become easier in higher dimensions*"