SQIsign2D

Dimensional Goldilocks

Joint work with: Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, **GP**, Damien Robert, Benjamin Wesolowski

Giacomo Pope | University of Bristol

SQIsign2D

- A **post-quantum** digital signature protocol
- As **compact** as SQIsign
- **As safe as SQIsign8D** (safer than SQIsign4D, SQIsign)
- The **fastest verification** of all SQIsign protocols
- Aim is to update the SQIsign **NIST submission** to 2D

East vs West vs Prime

- Within a few days, **three variants** of SQISign were published
- Today I’ll be talking about **SQIsign2D-West**
- **SQIsign2D-East** is very similar to West, but with **heuristics and faster signing**
- **SQIsignPrime** is more similar to **SQIsign4D** with a new challenge
- Neither East or Prime has an implementation

	Sizes (Bytes)		Timing (ms)		
	Public Key	Signature	Keygen	Sign	Verify
NIST I	66	148	30	80	4.5
NIST III	98	222	85	230	14.5
NIST V	130	294	180	470	31

SQIsign2D

Very compact signatures

	Sizes (Bytes)		Timing (ms)		
	Public Key	Signature	Keygen	Sign	Verify
NIST I	66	148	30	80	4.5
NIST III	98	222	85	230	14.5
NIST V	130	294	180	470	31

SQIsign2D

Isogenists: very fast algorithms?!

	Sizes (Bytes)		Timing (ms)		
	Public Key	Signature	Keygen	Sign	Verify
NIST I	66	148	30	80	4.5
NIST III	98	222	85	230	14.5
NIST V	130	294	180	470	31

SQIsign2D

Slow algorithms

	Sizes (Bytes)		Timing (ms)		
	Public Key	Signature	Keygen	Sign	Verify
NIST I	66	148	30	80	4.5
NIST III	98	222	85	230	14.5
NIST V	130	294	180	470	31

SQIsign2D

Can SQIsign2D be fast enough when size-restrictions force its use?

Overview

- Understanding SQIsign signatures
- Why is dimension two “just right”
- How does SQIsign2D compare
- What next?

Isogenies and Friends

Isogeny World

- Elliptic curves are **curves**: maps between curves are rational maps
- Elliptic curves are **groups**: maps between groups are homomorphisms
- An **isogeny** $\varphi : E_1 \to E_2$ is a map between curves which additionally preserves the group structure

$$\varphi(P + Q) = \varphi(P) + \varphi(Q), \quad P, Q \in E_1$$

- An isogeny $\theta : E \to E$ is an **endomorphism**, the set of endomorphisms is a ring $\mathrm{End}(E)$

Supersingular Isogeny World

- Supersingular curves have particularly large endomorphism rings
- For the curves we consider: $E/\mathbb{F}_{p^2}$, End(E) has rank four
- Isogenies have finite kernels and we're interested in separable isogenies: $\#\mathrm{ker}(\varphi) = \deg(\varphi)$
- For efficiency, we generally can only compute smooth degree isogenies
- For a given ℓ, we can compute the ℓ-isogeny graph which are $(\ell + 1)$ regular and Ramanujan (it's easy to get lost in the graph)

HD Isogeny World

- We can generalise the notion of isogenies to **higher dimensional varieties**

- A **trendy** isogeny is one between elliptic products:

$$\Phi : E_1 \times E_4 \to E_2 \times E_3$$

- We can think of this as one two-dimensional isogeny or a matrix of **four** one-dimensional isogenies:

$$\Phi = \begin{pmatrix} \varphi_{12} & \widehat{\varphi}_{34} \\ -\varphi_{13} & \widehat{\varphi}_{24} \end{pmatrix}$$

$$\begin{tikzcd}
E_1 \arrow[r, "\varphi_{12}"] \arrow[d, "\varphi_{13}"'] & E_2 \arrow[d, "\varphi_{24}"] \\
E_3 \arrow[r, "\varphi_{34}"] & E_4
\end{tikzcd}$$

Quaternion World

- An "extension" of complex numbers, elements look like: $\alpha = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$
- For $\alpha \in \mathcal{B}_{p,\infty} = \mathbb{Q}\langle i, j \rangle$ we have $\mathbf{i}^2 = -1, \ \mathbf{j}^2 = -p, \ \mathbf{ij} = \mathbf{k} = -\mathbf{ji}$
- Given a **fractional ideal** I, the **left order** is $\mathcal{O}_L(I) = \{\alpha \in \mathcal{B}_{p,\infty} \mid \alpha I \subset I\}$
- Why quaternions? When $\mathrm{End}(E)$ has rank four, $\mathrm{End}(E) \cong \mathcal{O}$ (maximal)
- We'll discuss this more **Deuring** the talk... 🥁

Hard Problems

Or at least not easy yet...

- Given two supersingular elliptic curves, find an isogeny connecting them
- Given a supersingular elliptic curve, compute its endomorphism ring
- In (2021/919) Wesolowski showed these problems are equivalent
- There are other “hard” isogeny problems, some of which are now understood to be easy
- Given an isogeny-based cryptographic primitive, convince people that it’s practical

Digital Signatures

I know something you don't know and I can <u>prove</u> it to you.

SQIsign

I know the...

Endomorphism ring of this supersingular curve

Public set-up

E_0

- A prime p
- A supersingular elliptic curve $E_0/\mathbb{F}_{p^2}$ with known endomorphism ring $\mathcal{O}_0 \cong \mathrm{End}(E_0)$
- $E_0 : y^2 = x^3 + x \qquad (p \equiv 3 \mod 4)$

$$E_0 \xrightarrow{\varphi_{sk}} E_{pk}$$

Keygen

- Prover generates a secret random isogeny φ_{sk}
- Prover publishes the codomain E_{pk}

$$
\begin{tikzcd}
E_0 \arrow[r, "\varphi_{sk}"] \arrow[d, "\varphi_{com}"'] & E_{pk} \\
E_{com} &
\end{tikzcd}
$$

Commitment

- Prover generates a secret random isogeny φ_{com}
- Prover publishes the codomain E_{com}

$$\begin{tikzcd} E_0 \arrow[r, "\varphi_{sk}"] \arrow[d, "\varphi_{com}"'] & E_{pk} \arrow[d, "\varphi_{chl}"] \\ E_{com} & E_{chl} \end{tikzcd}$$

Challenge

Verifier generates a public, random, smooth degree isogeny $\varphi_{chl} : E_{pk} \to E_{chl}$

$$\begin{tikzcd}
E_0 \arrow[r, "\varphi_{sk}"] \arrow[d, "\varphi_{com}"'] & E_{pk} \arrow[d, "\varphi_{chl}"] \\
E_{com} \arrow[r, "\varphi_{rsp}"'] & E_{chl}
\end{tikzcd}$$

Response

Prover generates an isogeny $\varphi_{resp} : E_{com} \to E_{chl}$ for which $\widehat{\varphi}_{rsp} \circ \varphi_{chl}$ is cyclic

$$
\begin{tikzcd}
E_0 \arrow[r, "\varphi_{sk}"] \arrow[d, "\varphi_{com}"'] & E_{pk} \arrow[dr, "\varphi_{chl}"] & \\
E_{com} \arrow[rr, "\varphi_{rsp}"'] & & E_{chl}
\end{tikzcd}
$$

That's it!

Signatures from Identification Protocols

- We use the Fiat-Shamir transform to obtain an asymmetric signature
- Interactive challenge is replaced by a deterministic challenge
- Commitment recoverability reduces signature size
- Verification of a signature is ensuring response validity

Where’s the endomorphism ring?

The Deuring Correspondence

- Deuring showed that there's **equivalences** between the isogeny world and quaternion world
- In supersingular isogeny world, we have **curves**, **points** on curves and **isogenies** between curves
- In quaternion world we have (maximal) **orders**, **quaternions** and **ideals**
- Importantly, hard isogeny problems can be **easy** quaternion problems
- The dictionary we need is the **endomorphism ring** of a curve

Some Cool Facts

Impress your friends at dinner!

- An isogeny connecting two curves is equivalent to an ideal connecting two orders
- If two ideals are equivalent then the corresponding isogenies have isomorphic (co)domains
- Endomorphisms are equivalent to principle ideals
- The dual isogeny is equivalent to the conjugate ideal
- An isogeny of degree d is equivalent to an ideal of norm n

Easy Problems

- Given $\mathrm{End}(E)$ compute the corresponding **maximal order**
- Given two maximal orders, compute the **connecting ideal**
- **KLPT**: Given an ideal compute an equivalent ideal with smooth norm
- Given an ideal compute the **corresponding isogeny**

Calculating the Response

- As we know (a basis) of $\mathrm{End}(E_0)$ and we know φ_{com} and $\varphi_{sk} \circ \varphi_{chl}$, we know a basis of $\mathrm{End}(E_{com})$ and $\mathrm{End}(E_{chl})$
- We then know $\mathcal{O}_{com}$ and $\mathcal{O}_{chl}$
- Compute the connecting ideal with left order $\mathcal{O}_{com}$ and right order $\mathcal{O}_{chl}$ (easy)
- This ideal is equivalent to φ_{rsp}
- Only possible because we know secrets!

$$\begin{tikzcd}
E_0 \arrow[r, "\varphi_{sk}"] \arrow[d, "\varphi_{com}"'] & E_{pk} \arrow[d, "\varphi_{chl}"] \\
E_{com} \arrow[r, "\varphi_{rsp}"'] & E_{chl}
\end{tikzcd}$$

SQIsign in dimensions 1, 2, 4, …

Dimension One

- For dimension one the response was computed using the KLPT algorithm
- Practical concerns restricted suitable characteristics, which meant higher security levels were hard to find parameters for
- The response (2^n)-isogeny was very long: with $\deg(\varphi_{rsp}) = p^{15/4}$
- This meant the isogeny was computed in many smaller steps (slow!)
- Recent work (ApresSQI) tries to speed up verification by allowing larger step sizes

SQIsign in dimensions 1, 2, 4, 8

Dimension Four and Eight

- For SQIsignHD the response isogeny no longer needed to be smooth
- If you work in dimension eight, we get great security proofs, but no one has yet implemented dimension eight isogenies
- If you work in dimension four, you introduce heuristics and weaken the security proof
- Resulting protocol was even more compact than SQIsign
- Signing was much faster than SQIsign and parameters easy to choose
- Verification needed $(2^n,2^n,2^n,2^n)$-isogenies which are slow

SQIsign in dimensions 1, 2, 4, 8

Dimension Two

- In SQIsign2D we obtain the same strong security guarantees of rigorous SQIsign8D but with “fast” 2D isogenies
- Signatures are less compact than SQIsign4D but more compact that SQIsign
- Signing is much faster than SQIsign and but slower than SQIsign4D
- Verification is the fastest of all variants (potentially even ApresSQI)

SQIsign Goldilocks

Evaluate a random isogeny of given degree

Translate an ideal into a two-dimensional isogeny

Fixed Degree Isogeny

- Input: a curve with known End(E_0), a basis $E[2^e] = \langle P, Q \rangle$ and odd integer $u < 2^e$
- Output: the image of the basis under the action of an isogeny of degree u and the codomain E' and the corresponding ideal
  - Sample $\theta \in$ End(E_0) with degree $u(2^e - 2)$
  - Compute the 2D-kernel: $\langle ([u]P, \theta(P)), ([u]Q, \theta(Q)) \rangle$
  - Compute the isogeny from this kernel: $\Phi : E_0 \times E_0 \to E \times E'$
  - Evaluate $\Phi(P,0)$ and $\Phi(Q,0)$ to obtain the image of $\varphi : E_0 \to E$
  - Set $I = \mathcal{O}\theta + \mathcal{O}u$

Ideal To Isogeny

- More complicated!
- Rough Idea:
  - Given an ideal, compute the action of the corresponding isogeny on $E[2^e]$
  - Requires two calls to fixed degree isogeny built from the basis of I
  - Output allows the construction of a third 2D isogeny
  - We evaluate this to get the action desired

Computing the response is still complex

$$
\begin{tikzcd}
& E_0 \arrow[rr, "\varphi_{\mathsf{sk}}"] \arrow[dl, "\varphi_{\mathsf{com}}"'] & & E_{\mathsf{pk}} \arrow[dr, "\varphi'_{\mathsf{chl}}"'] \arrow[ddrr, bend left, "\varphi_{\mathsf{chl}}"] & & \\
E_{\mathsf{com}} \arrow[rr, "\varphi^{(1)}_{\mathsf{rsp}}"] \arrow[dd, "\varphi_{\mathsf{aux}}"'] \arrow[ddrr, phantom, "\circlearrowright"] & & E'_{\mathsf{chl}} \arrow[rr, "\varphi^{(0)}_{\mathsf{rsp}}"] \arrow[dd, "\varphi'_{\mathsf{aux}}"] & & E^0_{\mathsf{chl}} \arrow[dr] & \\
& & & & & E_{\mathsf{chl}} \\
E_{\mathsf{aux}} \arrow[rr, dotted] & & E'_{\mathsf{aux}} & & &
\end{tikzcd}
$$

Is SQIsign2D Secure

SQIsign2D Security Assumptions

Key Recovery

- As with preceding work of SQIsign*, key recovery requires solving the endomorphism ring problem
- We're fairly confident that this is hard
- Much more fundamentally hard than SIDH
- There's always the horror of maths to keep us worried

SQIsign2D Security Assumptions

Knowledge Soundness

- A nice SQIsign trait is the high soundness of the identification protocol
- This means we only need to run the identification protocol a single time
- Proof of soundness comes from the degree of the challenge isogeny
- This is easy to control and set up for optimal parameters

SQIsign2D Security Assumptions

Zero Knowledge

- Proof that the protocol has the zero-knowledge property
- Uses a simulator producing transcripts indistinguishable from a honest run of the protocol
- This simulator runs in polynomial time if it has access to an oracle producing random isogenies
- Much of our work is based on the previous work of SQIsignHD
- Things work nicely in dimension two because of Fixed Degree Isogeny

SQIsign2D Security Assumptions

The Oracle known as FIDIO

A fixed degree isogeny oracle (FIDIO) is an oracle taking as input a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ and an integer N, and outputs a uniformly random isogeny $\varphi : E \to E'$ (in efficient representation) with domain E and degree N.

SQIsign vs The World

SQIsign2D is a significant improvement

	SQIsign			SQIsign2D		
	Keygen	Sign	Verify	Keygen	Sign	Verify
NIST I	2,800	4,600	93	120	290	25
NIST III	21,300	39,000	641	440	1,040	98
NIST V	91,600	165,000	2,080	1,070	2,490	247

Results measured in 10^6 cycles (Intel Ice Lake, 2Ghz)

SQIsign2D is a significant improvement

	SQIsign			SQIsign2D		
	Keygen	Sign	Verify	Keygen	Sign	Verify
NIST I	1,700	2,400	39	60	160	9
NIST III				170	460	29
NIST V				360	940	62

Results measured in 10^6 cycles (Intel Ice Lake, 2Ghz)

SQIsign2D is a significant improvement

	SQIsign			SQIsign2D		
	Keygen	Sign	Verify	Keygen	Sign	Verify
NIST I	1,700	2,400	39	28x	160	9
NIST III	21,300	39,000	641	125x	460	29
NIST V	91,600	165,000	2,080	254x	940	62

Keygen is up to 254x faster than SQIsign

SQIsign2D is a significant improvement

	SQIsign			SQIsign2D		
	Keygen	Sign	Verify	Keygen	Sign	Verify
NIST I	1,700	2,400	39	60	15x	9
NIST III	21,300	39,000	641	170	85x	29
NIST V	91,600	165,000	2,080	360	175x	62

Signing is up to 85x faster than SQIsign

SQIsign2D is a significant improvement

	SQIsign			SQIsign2D		
	Keygen	Sign	Verify	Keygen	Sign	Verify
NIST I	1,700	2,400	39	60	160	4x
NIST III	21,300	39,000	641	170	460	22x
NIST V	91,600	165,000	2,080	360	940	34x

Verification is up to 34x faster than SQIsign

SQIsign2D gets close to “classical” sizes

	ECDSA		ML-DSA		SQIsign2D	
	PK	Sig	PK	Sig	PK	Sig
NIST I	32	64	1,312	2,420	66	148
NIST III	48	96	1,952	3,309	98	222
NIST V	64	128	2,592	4,627	130	294

SQIsign2D gets close to “classical” sizes

	ECDSA		Falcon		SQIsign2D	
	PK	Sig	PK	Sig	PK	Sig
NIST I	32	64	897	666	66	148
NIST III	48	96			98	222
NIST V	64	128	1,793	1,280	130	294

SQIsign2D is still magnitudes slower

	ML-DSA (Dilithium)		SQIsign2D	
	Sign	Verify	Sign	Verify
NIST I	333	118	160,000	9,000
NIST III	529	179	460,000	29,000
NIST V	642	279	940,000	62,000

Results measured in 10^3 cycles

SQIsign2D is still magnitudes slower

	ML-DSA (Dilithium)		SQIsign2D	
	Sign	Verify	Sign	Verify
NIST I	333	118	480x	9,000
NIST III	529	179	870x	29,000
NIST V	642	279	1464x	62,000

Results measured in 10^3 cycles

SQIsign2D is still magnitudes slower

	ML-DSA (Dilithium)		SQIsign2D	
	Sign	Verify	Sign	Verify
NIST I	333	118	160,000	76x
NIST III	529	179	460,000	162x
NIST V	642	279	940,000	222x

Results measured in 10^3 cycles

What should we be working on?

Future Work

What's Next?

- Cryptographic implementations
    - The current implementation has no side-channel protection
    - Constant time SQIsign is an open-problem!
- Efficient Implementations
    - Now the isogenies are faster, aspects of quaternions appear slow
    - How much more speed can we get by throwing every trick $\mathbb{F}_{p^2}$ at the protocol?

Future Work

What's Next?

- Dimension two isogenies are still the bottleneck
  - Can we find (4,4)-isogenies to improve performance
  - Can we make size/speed trade-offs to improve performance
- Generalised Deuring for dimension two:
  - Long term goal, but would halve the characteristic
  - Convince masters students to take this as a PhD problem!

Thank You