Advances Towards Practical Implementations of Isogeny Based Signatures

Robert Gorrie

McMaster University – Department of Computing & Software

gorrierw@mcmaster.ca

November 14, 2018

Concerns of Cryptography

There are five rudimentary concerns of information security:

- *Confidentiality*: information must be kept private from unauthorized individuals
- *Integrity*: information must not be altered by unauthorized individuals
- *Availability*: information must be available for authorized individuals
- *Authenticity*: information must have a verifiable source
- *Non-repudiation*: the source of information must be publicly verifiable

Public-key Cryptography

The goal of cryptography is to define mathematically precise means of ensuring these information security goals.

Cryptographic protocols can be either *private-key* or *public-key* systems.

Public-key systems require that every party takes ownership of both a public key (pk), the value of which is known by everyone on the network, and a private key (sk), known only to the owner.

Quantum Cryptanalysis

Efficient large-scale quantum computing $\rightarrow$ breaking most modern public-key cryptosystems.

This has lead to the development of the field known as post-quantum cryptography – the aim of which is to develop cryptosystems resistant to quantum cryptanalysis.

Post-quantum Cryptography

Common approaches to post-quantum cryptography include

- Lattice-based cryptography
- Hash-based cryptography
- Multivariate-based cryptography
- Code-based cryptography
- Isogeny-based cryptography

Post-quantum Cryptography

	Key Gen	Sign	Verify
SIDH	84,499,270	4,950,023,141.65	3,466,703,991.09
Sphincs	17,535,886.94	653,013,784	27,732,049
qTESLA	1,059,388	460,592	66,491
Picnic	13,272	9,560,749	6,701,701
RSA	12,800,000	1,113,600	32400
ECDSA	1,470,000	128,928	140,869

My Contributions

Overview

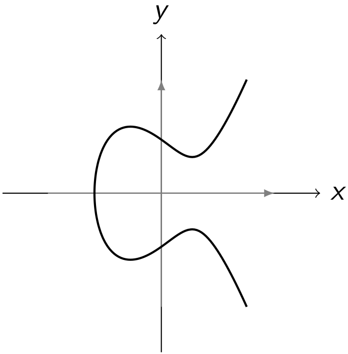
Elliptic Curves as a Group

Elliptic curves are a class of algebraic curves satisfying

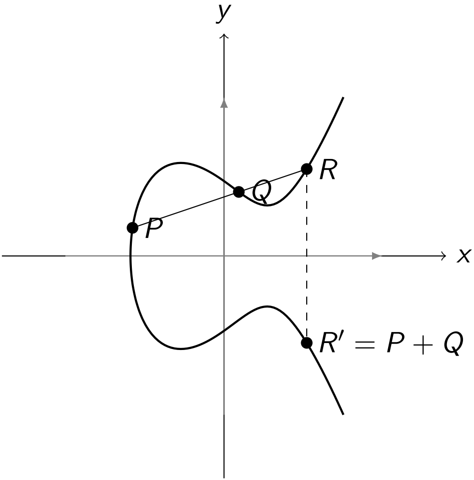
$$E : y^2 = x^3 + ax + b.$$

We can define a group

composed of all the points $P = (x, y)$ satisfying E.



Elliptic Curves as a Group



Torsion Subgroups

Isogenies

Isogenies are maps that take a point on one elliptic curve to a point on another. For an isogeny ϕ mapping from E_1 to E_2, we can write

$$\phi : E_1 \rightarrow E_2$$

These maps have the following two properties

$$\phi(\mathcal{O}) = \mathcal{O}$$
$$\phi(P^{-1}) = (\phi(P)^{-1})$$

Isogenies

Lemma (Uniquely identifying isogenies)

Let E be an elliptic curve and let Φ be a finite subgroup of E. There is a unique elliptic curve E' and a seperable isogeny $\phi : E \to E'$ satisfying $\ker(\phi) = \Phi$.

Key Exchange Protocols

Key exchange protocols are cryptographic schemes used to establish a shared secret between two party members

These can be defined by a tuple of algorithms $\Pi_{kex} = (\mathbf{KeyGen}, \mathbf{SecAgr})$.

Key Exchange Protocols

Public parameter:

g, p

Alice		Bob
$a \in_R \{2, \ldots, p-2\}$		$b \in_R \{2, \ldots, p-2\}$
$A = g^a \bmod p$	$\xrightarrow{A}$	$B = g^b \bmod p$
	$\xleftarrow{B}$	
$k = (B)^a = g^{ba}$		$k = (A)^b = g^{ab}$

Supersingular Isogeny Diffie-Hellman

SIDH is a key-exchange protocol where Alice and Bob use Isogenies as their public keys and points on a curve as their private keys.

Here's how it works...

Supersingular Isogeny Diffie-Hellman

We are concerned with curves over the field $\mathbb{F}_{p^2}$ where

$$p = \ell_A^{e_A} \ell_B^{e_B} \cdot f \pm 1$$

with f chosen such that p is prime.

We then choose a curve E, and bases $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$ generating $E[\ell_A^{e_A}]$ and $E[\ell_B^{e_B}]$.

And so, our set of public parameters is

$$\{p, E, \ell_A, \ell_B, e_A, e_B, P_A, Q_A, P_B, Q_B\}.$$

Interactive Identification Schemes

Identification schemes are used to confirm the identity of a user on a network. These protocols are typically composed by the tuple of algorithms (**KeyGen**, **Commit**, **Prove**, **Verify**).

For Bob to prove his identity to Alice, a protocol of this type would run as follows:

(i) Bob runs **KeyGen**(1^λ) to generate his keypair (sk, pk).

(ii) Bob runs **Commit**() to generate *com* and sends it to Alice.

(iii) Alice sends a randomly generated "challenge" value $ch \in \omega$ and sends it to Bob.

(iv) Bob runs **Prove**(*sk*, *com*, *ch*) with output *resp*, the response to Alice's challenge.

(v) Alice runs **Verify**(*pk*, *com*, *ch*, *resp*) with output $b \in 0, 1$. Bob has successfully proven his identity to Alice if $b = 1$.

Isogeny-based Proof of Identity

Signature schemes are used to prove that a particular party supplied a given message. These schemes consist of the algorithms **Sign**, **Verify**, and **Prove**.

Signature Schemes

Signature schemes are used to prove that a particular party supplied a given message. These schemes consist of the algorithms **Sign**, **Verify**, and **Prove**.

Fiat-Shamir Transform

The Fiat-Shamir transform is a process by which an interactive identification scheme can be turned into a signature scheme.

Yoo Signatures

The signature scheme derived by Yoo et al. applies the Fiat-Shamir transform to the isogeny-based identification scheme to construct the first ever isogeny-based signature scheme.

Recap

SIDH Key Exchange → Isogeny-based Proof of Identity → Yoo Signatures

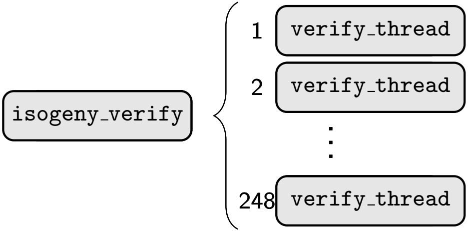
Partial $\mathbb{F}_{p^2}$ Inversions

Batching Inversions

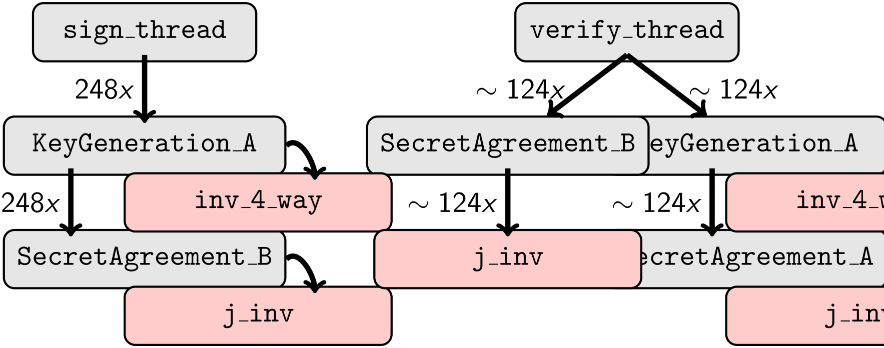
Partial Batched Inversions

for `i = 0..(n-1)` **do**
  $den_i \leftarrow (x_i)_a^2 + (x_i)_b^2 \pmod{p}$
$a_0 \leftarrow den_0$
for `i = 1..(n-1)` **do**
  $a_i \leftarrow a_{i-1} \cdot den_i \pmod{p}$
$inv \leftarrow a_{n-1}^{-1} \pmod{p}$
for `i = n-1..1` **do**
  $a_i \leftarrow inv \cdot dest_{i-1} \pmod{p}$
  $inv \leftarrow inv \cdot den_i \pmod{p}$
$a_0 \leftarrow a_{inv}$
for `i = 0..(n-1)` **do**
  $(xinv_i)_a \leftarrow a_i \cdot (x_i)_a \pmod{p}$
  $(xinv_i)_b \leftarrow a_i \cdot -(x_i)_b \pmod{p}$
  $x_i^{-1} \leftarrow \{(xinv_i)_a, (xinv_i)_b\}$
return $\{x_0^{-1}, x_1^{-1}, ..., x_{n-1}^{-1}\}$

Structure of the Yoo Signature Implementation



Signature Schemes



Verbatim

Example (Theorem Slide Code)

```
\begin{frame}
\frametitle{Theorem}
\begin{theorem}[Mass--energy equivalence]
$E = mc^2$
\end{theorem}
\end{frame}
```

Figure

Uncomment the code on this slide to include your own image from the same directory as the template .TeX file.

Citation

An example of the `\cite` command to cite within the presentation:

This statement requires citation [Smith, 2012].

Citation

An example of the `\cite` command to cite within the presentation:

This statement requires citation [Smith, 2012].

Questions?

References

John Smith (2012)
Title of the publication
Journal Name 12(3), 45 – 678