Advances Towards Practical Implementations of Isogeny Based Signatures

Robert Gorrie

McMaster University – Department of Computing & Software

gorrierw@mcmaster.ca

November 13, 2018

Overview

Public-key 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

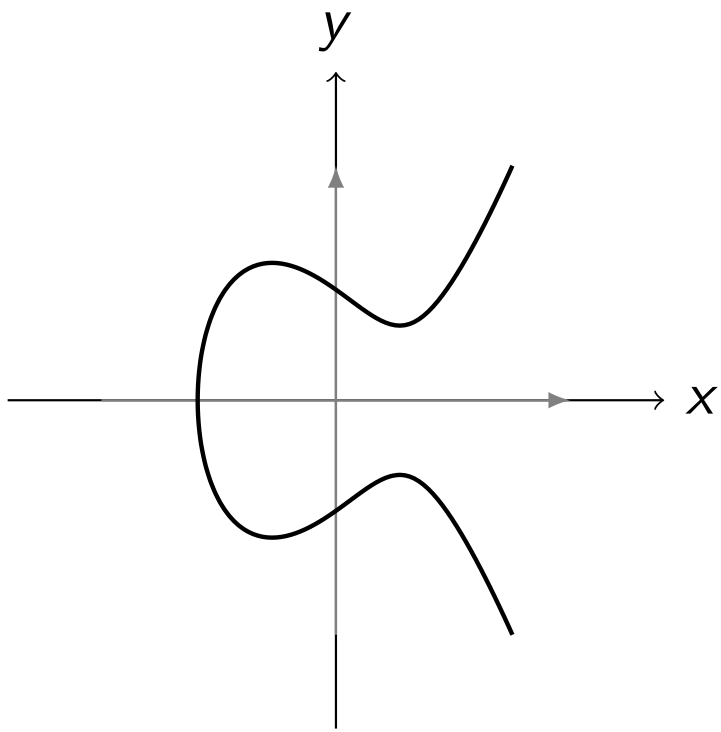
Elliptic Curves as a Group

Elliptic curves are a class of algebraic curves satisfying

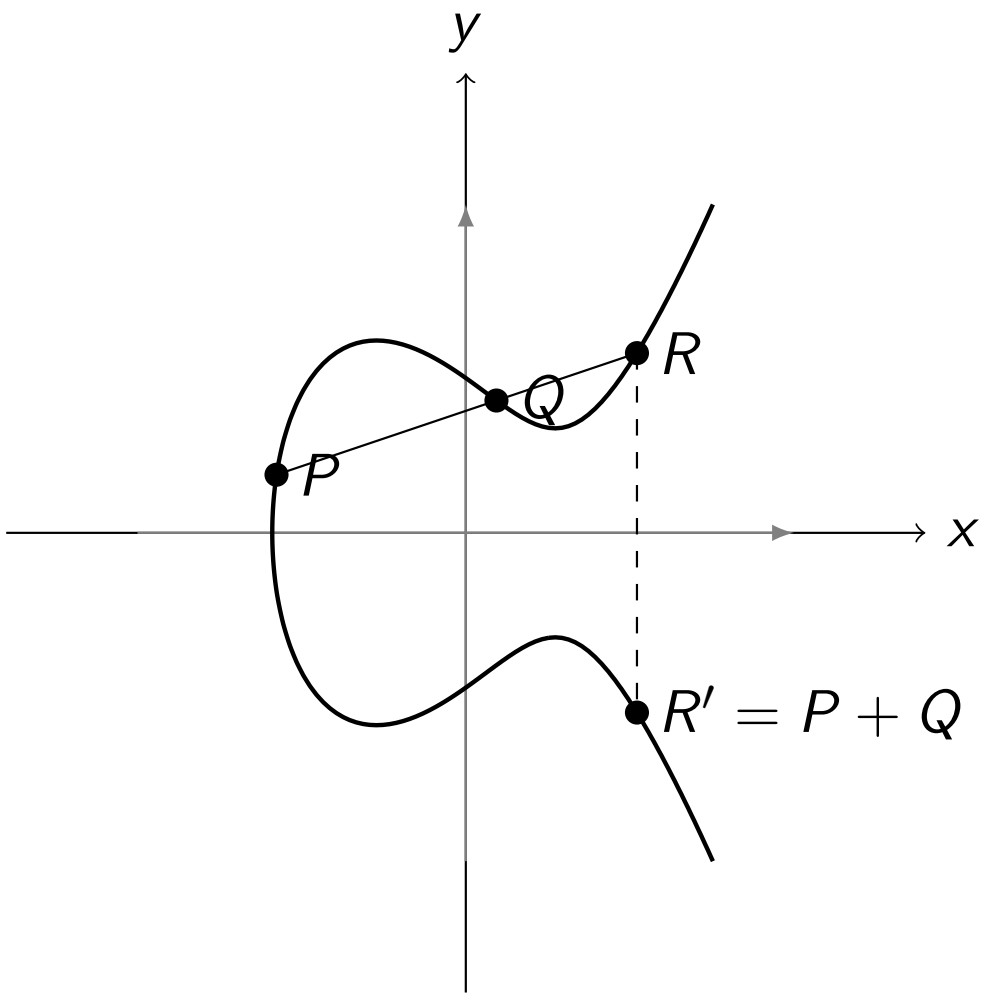
$$E : y^2 = x^3 + ax + b.$$

We can define a group

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



Elliptic Curves as a Group



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

$$\phi : E_1 \rightarrow E_2$$

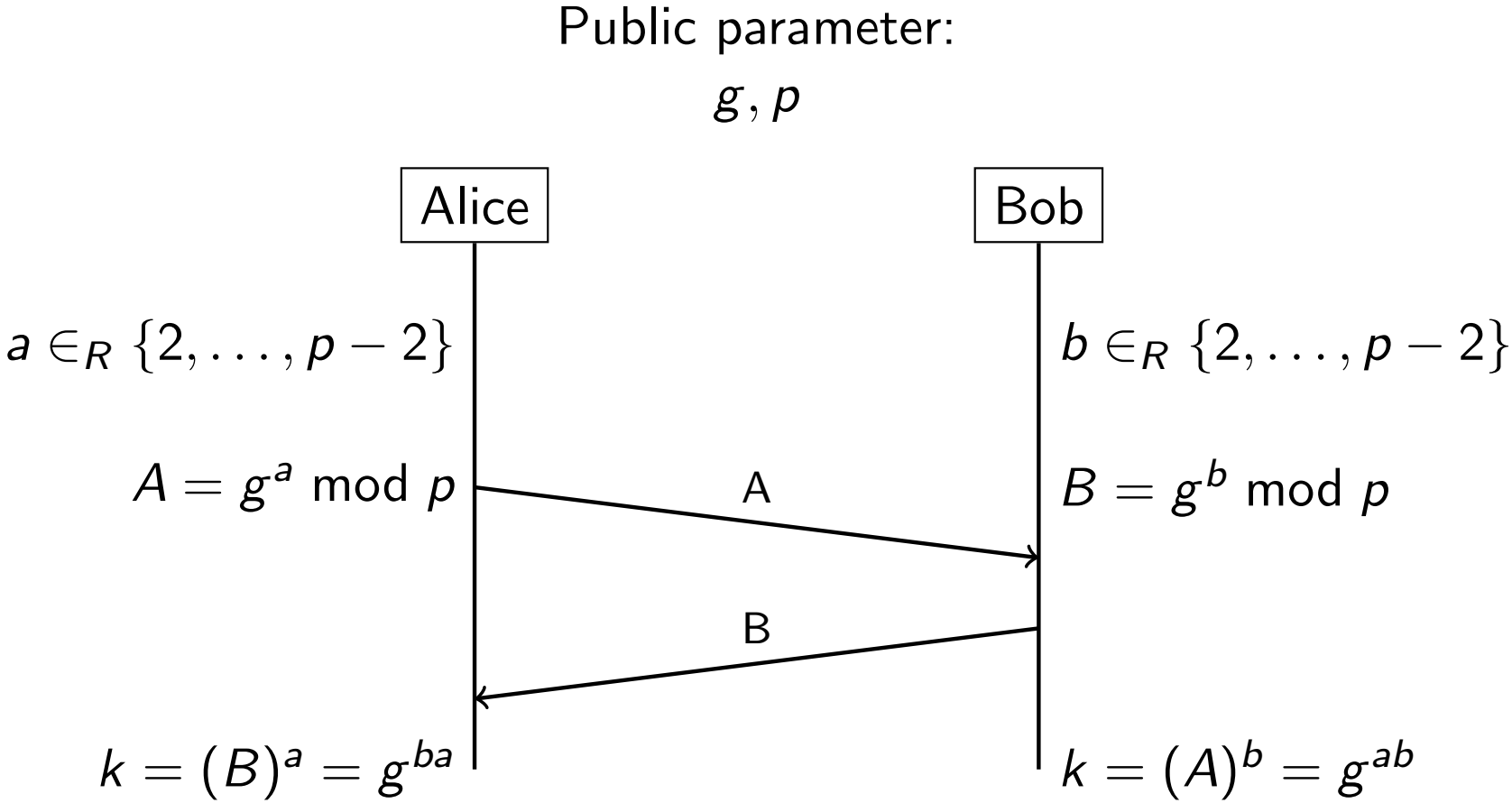
These maps have the following two properties

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

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
$\Pi_{kex} = (\textbf{KeyGen}, \textbf{SecAgr})$.

Key Exchange Protocols



Supersingular Isogeny Diffie-Hellman

Interactive Identification Schemes

Theorem (Mass–energy equivalence)

$E = mc^2$

Signature Schemes

Theorem (Mass–energy equivalence)

$E = mc^2$

Fiat-Shamir Transform

Theorem (Mass–energy equivalence)

$E = mc^2$

Yoo Signatures

Theorem (Mass–energy equivalence)

$E = mc^2$

Table

Treatments	**Response 1**	**Response 2**
Treatment 1	0.0003262	0.562
Treatment 2	0.0015681	0.910
Treatment 3	0.0009271	0.296

Table: Table caption

Signature Schemes

Theorem (Mass–energy equivalence)

$E = mc^2$

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