Isogeny-based Cryptography - Talk 0

Diana Mocanu

THE UNIVERSITY OF WARWICK

Diffie-Hellman Key Exchange

- Method of securely exchanging a cryptographic key over a public channel

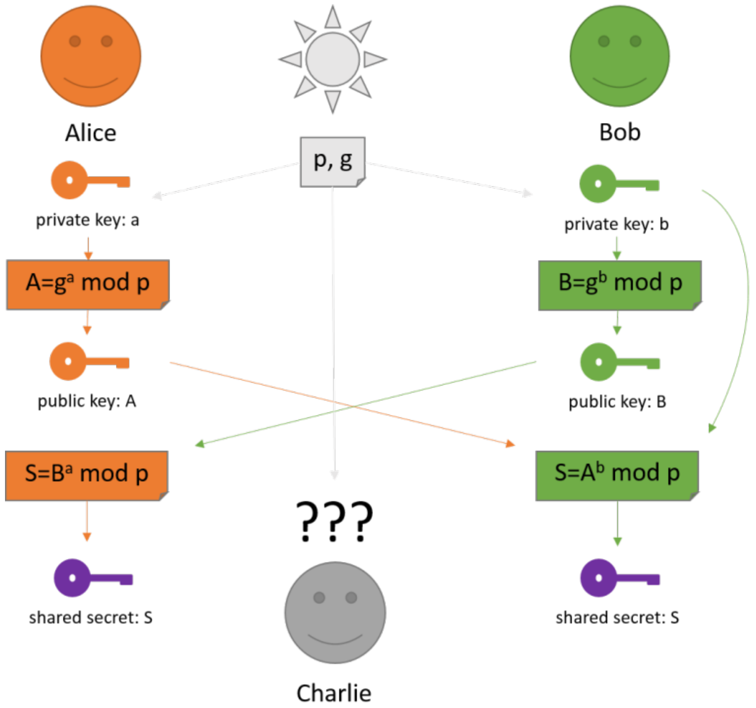
Diffie-Hellman Key Exchange

- Method of securely exchanging a cryptographic key over a public channel
- Earliest practical examples of public key exchange (published in 1976 by Diffie and Hellman)

Diffie-Hellman Key Exchange

- Method of securely exchanging a cryptographic key over a public channel
- Earliest practical examples of public key exchange (published in 1976 by Diffie and Hellman)
- The key can then be used to encrypt subsequent communications using a symmetric-key cipher.

Finite Field Diffie-Hellman



Discrete log problem

Definition

In its most standard form, the **discrete logarithm problem** in a finite group G can be stated as follows: given $a \in G$ and $b \in \langle a \rangle$, find the least positive integer x such that $a^x = b$.

Discrete log problem

Definition

In its most standard form, the **discrete logarithm problem** in a finite group G can be stated as follows: given $a \in G$ and $b \in \langle a \rangle$, find the least positive integer x such that $a^x = b$.

Example

The discrete logarithm problem is easy when $G = (\mathbb{R}^*, \times)$ as it will reduce to finding $\log_a b$ which is a well known real function.

Discrete log problem

Definition

In its most standard form, the **discrete logarithm problem** in a finite group G can be stated as follows: given $a \in G$ and $b \in \langle a \rangle$, find the least positive integer x such that $a^x = b$.

Example

The discrete logarithm problem is easy when $G = (\mathbb{R}^*, \times)$ as it will reduce to finding $\log_a b$ which is a well known real function.

Example

In $G = \mathbb{F}_{17}$, the equation $3^x = 13$ has an infinite number of solutions, namely $x = 4 + 16n$.

The discrete logarithm problem

Fact

If $G = E(\mathbb{F}_p)$, it turns out that the discrete logarithm problem is **very hard** $\rightarrow$ Elliptic-Curve Diffie–Hellman (ECDH), a cryptosystem based on the hardness of this problem.

Elliptic Curves over $\mathbb{Q}$

Definition

An **elliptic curve over** $\mathbb{Q}$ consists of solutions (x, y) to an equation of the form:

$$E : Y^2 = X^3 + aX + b$$

where $a, b \in \mathbb{Q}$. Moreover, we require that the following quantity, (called the **discriminant**) is non-zero $\Delta = 4a^3 + 27b^2 \neq 0$.
We think of the elliptic curve E as having a distinguished point called the **point at infinity** and denoted by ∞.

Elliptic Curves over $\mathbb{Q}$

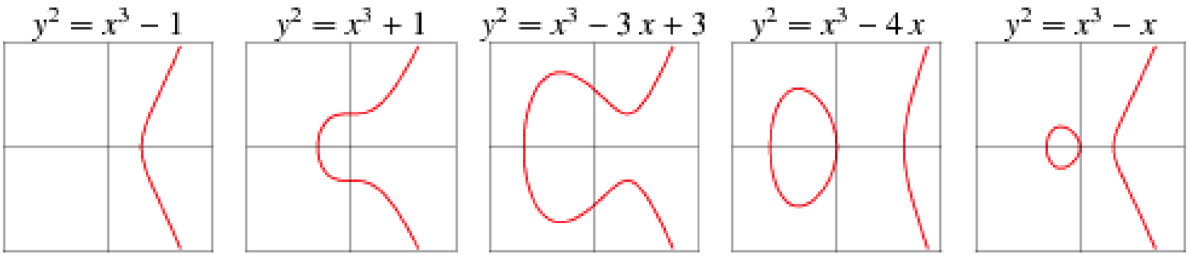


Figure 1: Elliptic curves for various values of a and b.

Group Law

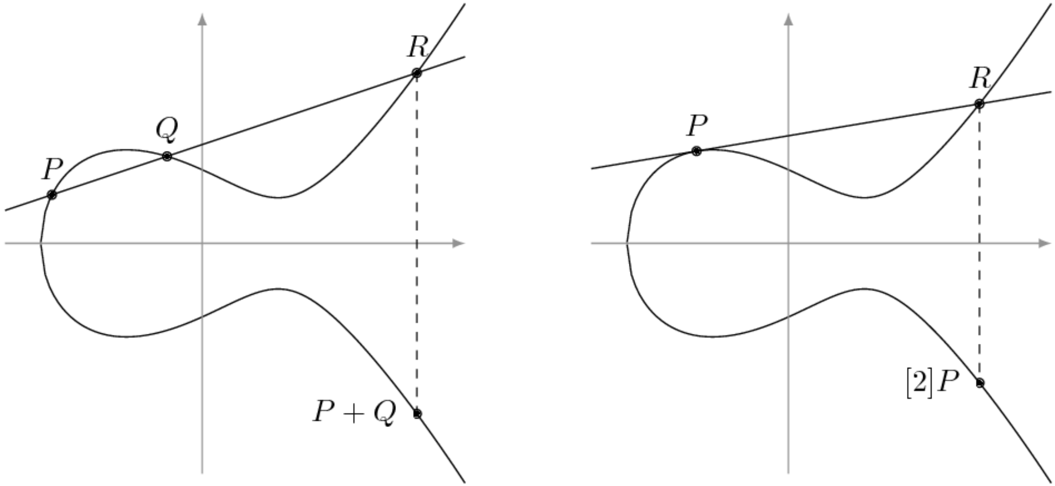


Figure 2: The Group law on an elliptic curve.

Elliptic Curves over finite fields

Definition

An **elliptic curve over** $\mathbb{F}_q$ with characteristic $\neq 2, 3$ consists of solutions (x, y) to an equation of the form:

$$E : Y^2 = X^3 + aX + b$$

where $a, b \in \mathbb{F}_q$, with $\Delta = 4a^3 + 27b^2 \neq 0$.
We think of the elliptic curve E as having a distinguished point called the **point at infinity** and denoted by ∞.
We define $P = (x, y)$ to be an $\mathbb{F}_q$-**rational point** if P lies on E and $x, y \in \mathbb{F}_q$ and take $E(\mathbb{F}_q)$ to be the all of the $\mathbb{F}_q$-rational points, together with the point at infinity.

Elliptic curves over finite fields

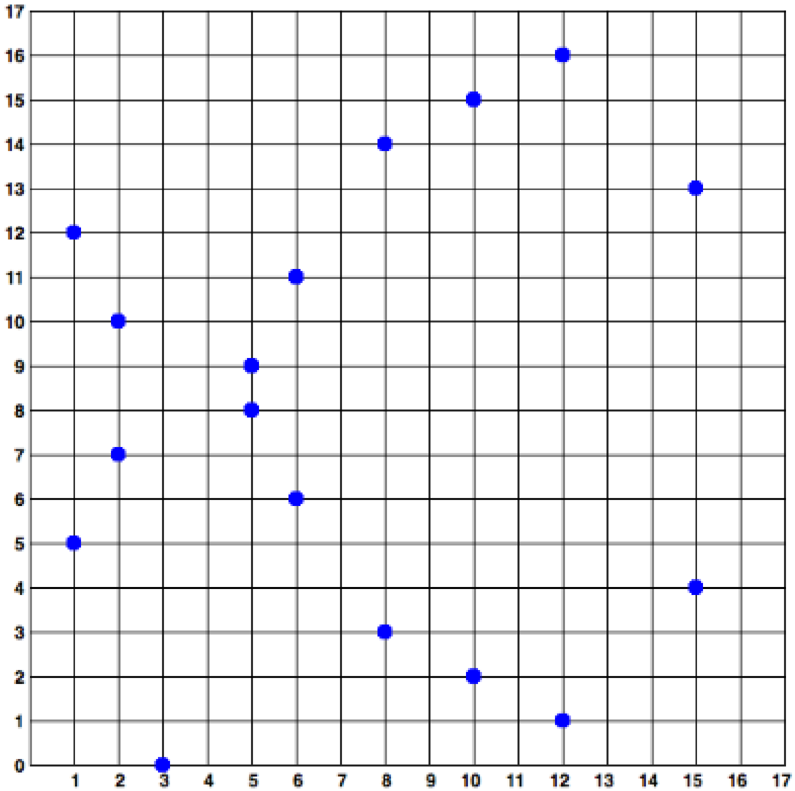


Figure 3: $E : Y^2 = X^3 + 7$ over $\mathbb{F}_{17}$

Elliptic curves over finite fields

Theorem (Hasse bound)

Let $E/\mathbb{F}_q$. *Then* $\#E(\mathbf{F}_q) = q + 1 - t$ *where* $|t| \leq 2\sqrt{q}$.

Elliptic curves over finite fields

Theorem (Hasse bound)

Let $E/\mathbb{F}_q$. Then $\#E(\mathbf{F}_q) = q + 1 - t$ where $|t| \leq 2\sqrt{q}$.

Definition

An elliptic curve E defined over a finite field $\mathbb{F}_q$ of characteristic p is **supersingular** if and only if p divides t. The opposite of supersingular is **ordinary**.

Group Law over finite fields

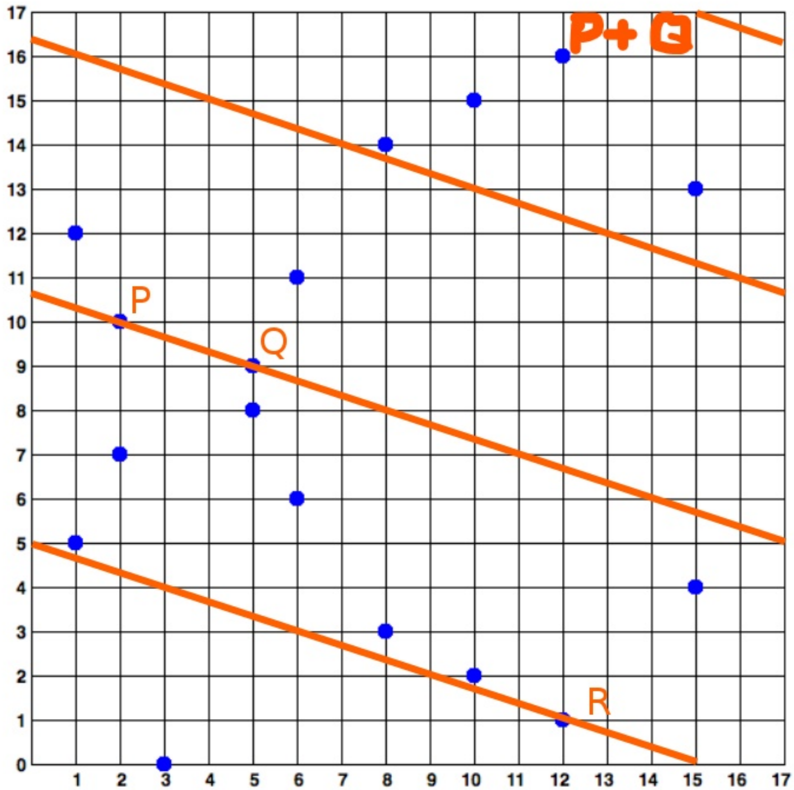
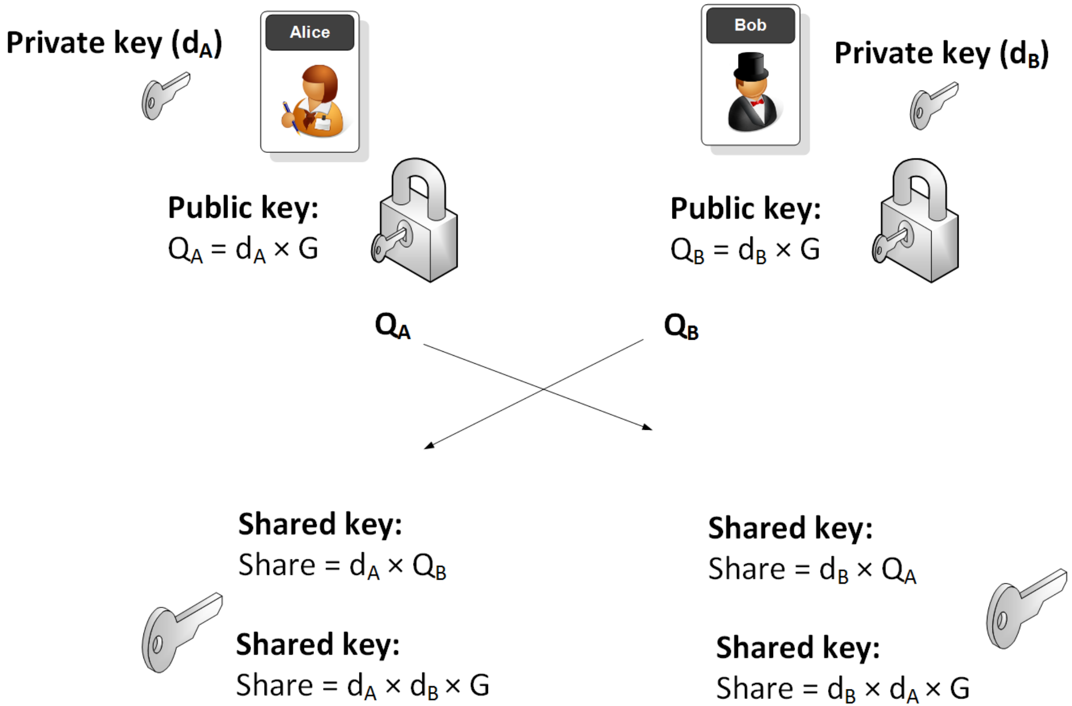


Figure 4: Here $P = (2, 10), Q = (5, 9)$ and $P + Q = (12, 16)$ and E as in Figure 12

ECDH

Initialisation: $E : Y^2 = X^3 + AX + B$ over a fixed field $\mathbb{F}_p$, where p is a prime, a fixed point $G \in E(\mathbb{F}_p)$ and n the order of G.



Post Quantum Crypography

- Post-quantum cryptography (PQC) = a set of classical cryptographic algorithms that are believed to be “quantum-safe,” meaning that they are expected to remain safe even in the presence of quantum computers.

Post Quantum Crypography

- Post-quantum cryptography (PQC) = a set of classical cryptographic algorithms that are believed to be "quantum-safe", meaning that they are expected to remain safe even in the presence of quantum computers.
- Examples: RSA, FFDH, ECDH $\rightarrow$ not quantum-safe $\rightarrow$ Schor's Algorithm

Isogeny-based cryptography

- 2006 (Couveignes and Rostovtsev–Stolbunov) - isogeny-based cryptography

Isogeny-based cryptography

- 2006 (Couveignes and Rostovtsev–Stolbunov) - isogeny-based cryptography
- 2010 - can be broken with a sub-exponential quantum attack due to Kuperberg

Isogeny-based cryptography

- 2006 (Couveignes and Rostovtsev–Stolbunov) - isogeny-based cryptography
- 2010 - can be broken with a sub-exponential quantum attack due to Kuperberg
- 2011 (Jao and De Feo) - supersingular isogeny-based cryptography $\rightarrow$ exponential quantum security

Isogeny-based cryptography

- 2006 (Couveignes and Rostovtsev–Stolbunov) - isogeny-based cryptography
- 2010 - can be broken with a sub-exponential quantum attack due to Kuperberg
- 2011 (Jao and De Feo) - supersingular isogeny-based cryptography $\rightarrow$ exponential quantum security
- SIDH= supersingular isogeny Diffie-Hellman

Isogenies

Definition

An **isogeny** φ between two elliptic curves $E_1/\mathbb{F}_{p^n}$ and $E_2/\mathbb{F}_{p^n}$ is a non-constant rational function that maps points from E_1 to points on E_2 and is compatible with the group law. For this talk, the **degree** of an isogeny is defined to be $|\mathrm{Ker}(\varphi)|$.

Isogenies

From now on, we only work with elliptic curves over finite fields.

Definition

An **isogeny** φ between two elliptic curves $E_1/\mathbb{F}_{p^n}$ and $E_2/\mathbb{F}_{p^n}$ is a non-constant rational function that maps points from E_1 to points on E_2 and is compatible with the group law. For this talk, the **degree** of an isogeny is defined to be $|\mathrm{Ker}(\varphi)|$.

Example

Multiplication by l map denoted $[l]_E \colon E/\mathbb{F} \to E/\mathbb{F}$ is an isogeny of degree $1, l$ or l^2 if l is prime and coprime with $\mathrm{char}(\mathbb{F})$.

SIDH

$$
\begin{tikzcd}
 & E_A \arrow[dr, "\psi_B"] \arrow[dd, dotted, shift left] & \\
E \arrow[ur, "\phi_A"] \arrow[dr, "\phi_B"'] & & E_{AB} \\
 & E_B \arrow[ur, "\psi_A"'] \arrow[uu, dotted, shift left] &
\end{tikzcd}
$$

Initialisations:

- E a supersingular elliptic curve over $\mathbb{F}_{p^2}$ such that $E(\mathbb{F}_{p^2}) = (p+1)^2$;
- $p + 1 = l_A^a l_B^b$;

Secret Data:

- Alice: the isogeny ϕ_A of degree l_A^a
- Bob: the isogeny ϕ_B of degree l_B^b

Isogeny Graphs

The graph of isogenies of prime degree $l \neq p$

Fix a finite field $\mathbb{F}$ and a prime $l \neq \mathrm{char}(\mathbb{F})$. We look at the graph with **vertices** isomorphism classes of elliptic curves and **edges** isogenies of degree l between them, up to isomorphism.

Isogeny Graphs

The graph of isogenies of prime degree $l \neq p$

Fix a finite field $\mathbb{F}$ and a prime $l \neq \mathrm{char}(\mathbb{F})$. We look at the graph with **vertices** isomorphism classes of elliptic curves and **edges** isogenies of degree l between them, up to isomorphism.

In our case: Supersingular case (algebraic closure)
The graph is $\mathbf{l+1}$ **regular**.
There is **a unique (finite) connected component made of all supersingular curves** with the same number of points.

The SIDH System

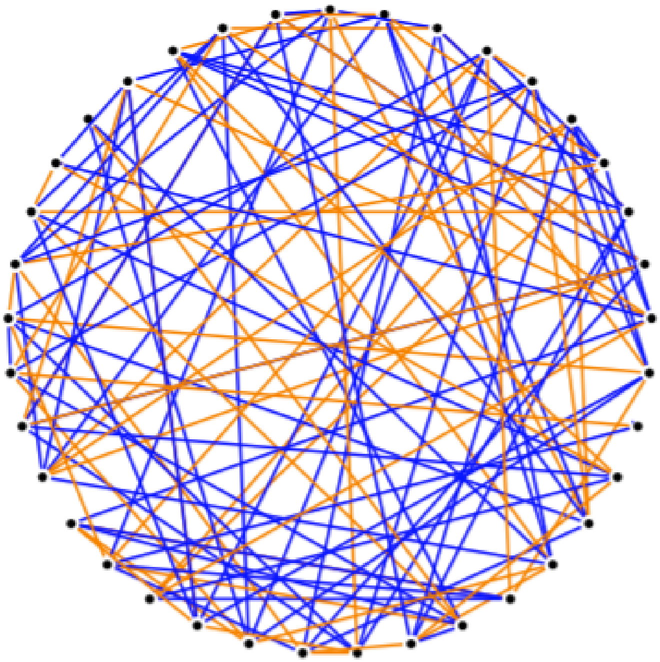


Figure 5: Vertices: Supersingular elliptic curves $\mathbb{F}_{419^2}$, edges are 2 and 3 isogenies.

The SIDH system

Security:

- For SIDH an attacker is confronted with the problem of finding E_{AB} knowing E_A, E_B and some torsion information.

The SIDH system

Security:

- For SIDH an attacker is confronted with the problem of finding E_{AB} knowing E_A, E_B and some torsion information.
- This is equivalent to finding one of the specific isogenies ϕ_A or ϕ_B by knowing their value at some torsion points. The isogeny finding problem is up to date believed to be quantum-hard.

Security:

- For SIDH an attacker is confronted with the problem of finding E_{AB} knowing E_A, E_B and some torsion information.
- This is equivalent to finding one of the specific isogenies ϕ_A or ϕ_B by knowing their value at some torsion points. The isogeny finding problem is up to date believed to be quantum-hard.
- The additional points have raised some concern but no attack has managed to break the security of SIDH yet $\rightarrow$ we are going to study torsion-points attacks as given in Christophe Petit's paper.

KLPT

- D. Kohel, K. Lauter, C. Petit, and J.-P. Tignol. *On the quaternion l-isogeny path problem*

KLPT

- D. Kohel, K. Lauter, C. Petit, and J.-P. Tignol. *On the quaternion l-isogeny path problem*
- KLPT algorithm is a probabilistic algorithm to solve a quaternion ideal analog of the path problem in supersingular l-isogeny graphs.

KLPT

- D. Kohel, K. Lauter, C. Petit, and J.-P. Tignol. *On the quaternion l-isogeny path problem*
- KLPT algorithm is a probabilistic algorithm to solve a quaternion ideal analog of the path problem in supersingular l-isogeny graphs.
- The Deuring correspondence gives a bijection between supersingular isomorphism classes of elliptic curves and maximal orders in quaternion algebras.

KLPT

- D. Kohel, K. Lauter, C. Petit, and J.-P. Tignol. *On the quaternion l-isogeny path problem*
- KLPT algorithm is a probabilistic algorithm to solve a quaternion ideal analog of the path problem in supersingular l-isogeny graphs.
- The Deuring correspondence gives a bijection between supersingular isomorphism classes of elliptic curves and maximal orders in quaternion algebras.
- KLPT gives a polynomial-time algorithm to solve the equivalent problem (under Deuring correspondence) of finding an isogeny between two elliptic curves.

KLPT

Supersingular j-invariants over $\mathbb{F}_{p^2}$ $j(E)$ (up to galois conjugacy)	Maximal orders in $\mathcal{B}_{p,\infty}$ $\mathcal{O} \cong \mathrm{End}(E)$ (up to isomorpshim)
(E_1, φ) with $\varphi : E \to E_1$	I_φ integral left $\mathcal{O}$-ideal and right $\mathcal{O}_1$-ideal
$\theta \in \mathrm{End}(E_0)$	Principal ideal $\mathcal{O}\theta$
$\deg(\varphi)$	$n(I_\varphi)$
$\hat{\varphi}$	$\bar{I_\varphi}$
$\varphi : E \to E_1, \psi : E \to E_1$	Equivalent Ideals $I_\varphi \sim I_\psi$
Supersingular j-invariants over $\mathbb{F}_{p^2}$	$\mathrm{Cl}(\mathcal{O})$
$\tau \circ \rho : E \to E_1 \to E_2$	$I_{\tau\circ\rho} = I_\rho \cdot I_\tau$

Table 1. The Deuring correspondence, a summary.

Signature Schemes

- A **digital signature** is a mathematical scheme for verifying the authenticity of digital messages or documents.

Signature Schemes

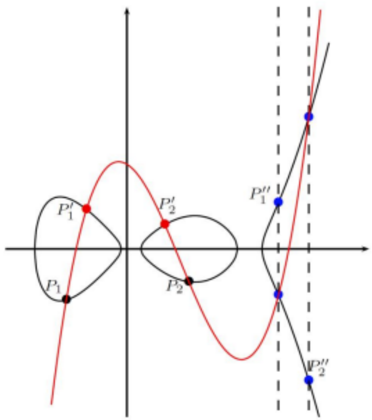
- A **digital signature** is a mathematical scheme for verifying the authenticity of digital messages or documents.
- Many signature algorithms are based on **sigma protocols**. A sigma protocol is a type of proof of knowledge protocol between a prover $\mathcal{P}$ and a verifier $\mathcal{V}$, where the prover wants to convince the verifier that for some statement x, he knows a witness w, such that $(x, w) \in \mathcal{R}$, for some relation $\mathcal{R}$.

Signature Schemes

- A **digital signature** is a mathematical scheme for verifying the authenticity of digital messages or documents.
- Many signature algorithms are based on **sigma protocols**. A sigma protocol is a type of proof of knowledge protocol between a prover $\mathcal{P}$ and a verifier $\mathcal{V}$, where the prover wants to convince the verifier that for some statement x, he knows a witness w, such that $(x, w) \in \mathcal{R}$, for some relation $\mathcal{R}$.
- Challenge: Design a SIDH-based sigma protocol for proving knowledge of the secret key.

Genus 2 group law

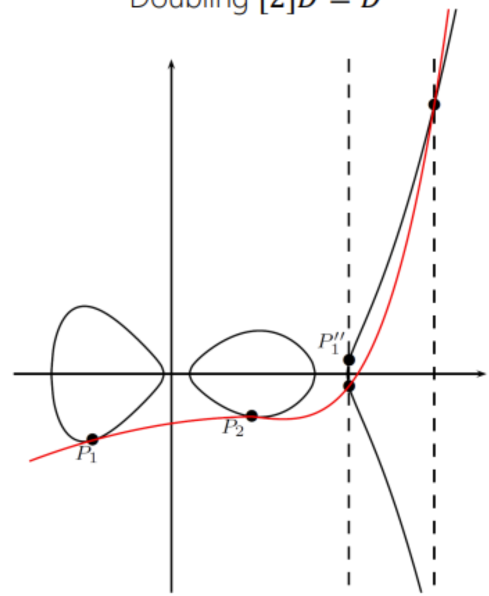
Addition $D \oplus D' = D''$



$$C/K : y^2 = x^5 + \cdots$$

$$D = (P_1) + (P_2) - 2(\infty)$$
$$D' = (P_1{}') + (P_2{}') - 2(\infty)$$
$$D'' = (P_1{}'') + (P_2{}'') - 2(\infty)$$

Doubling $[2]D = D''$



$$\mathrm{div}(\ell) = (P_1) + (P_2) + (P_1{}') + (P_2{}') + (\iota(P_1'')) + (\iota(P_2'')) - 6(\infty)$$

$$\mathrm{div}(\ell) = 2(P_1) + 2(P_2) + (\iota(P_1'')) + (\iota(P_2'')) - 6(\infty)$$

Genus 2 (hyperelliptic) cryptography

- It is possible to define DH with respect to the group law described above.

Genus 2 (hyperelliptic) cryptography

- It is possible to define DH with respect to the group law described above.
- It is possible to define an analogue for genus 2 isogeny-based cryptography $\rightarrow$ Last talk

Genus 2 (hyperelliptic) cryptography

- It is possible to define DH with respect to the group law described above.
- It is possible to define an analogue for genus 2 isogeny-based cryptography $\rightarrow$ Last talk
- Why stop at genus 2?

Plan of the talks

We will follow the isogeny-based cryptography school organized in 2020 by Christophe Petite and Chloe Martindale.
Most of the materials can be found on the school's website:
`https://isogenyschool2020.co.uk/`.

Plan of the talks

Talk 1: Elliptic Curves over finite fields
Talk 2: CSIDH & SIDH
Talk 3: Class Groups
Talk 4: Quaternion Algebras
Talk 5: KLPT - D. Kohel, K. Lauter, C. Petit, and J.-P. Tignol. *On the quaternion l-isogeny path problem*
Talk 6: Torsion Point Attacks on SIDH - C. Petite *Faster Algorithms for Isogeny Problems using Torsion Point Images*
Talk 7: Signature schemes
Talk 8: Hyperelliptic curves and Jacobian varieties
Talk 9: Hyperelliptic isogeny-based cryptography - E.V. Flynn and Yan Bo Ti *Genus Two Isogeny Cryptography*


Thank you