Public-Key Cryptosystem Based on Isogenies

Alexander Rostovtsev
Anton Stolbunov

Saint-Petersburg State Polytechnical University
Quantum Computer

Public-key cryptosystems

Problem of calculation of group order and structure
   RSA  Rabin

Discrete logarithm problem
   Diffie-Hellman  DSA

Shor's algorithm

Quantum computer

Breaking with polynomial complexity

2 of 18
Basic conceptions

- Non-supersingular elliptic curves over a finite field $F_p$: $Y^2 = X^3 + aX + b; \quad j \neq 0, 1728$
- $\pi^2 - t\pi + p = 0$ - a Frobenius equation
- $D_{\pi} = t^2 - 4p$ - a Frobenius discriminant
- Isogenous elliptic curves
- Isogeny degree
- Isogeny kernel
- Modular equation: $\Phi_l (S, T) = 0$
Branchless Cycles

- Elkies criterion: for an elliptic curve given, if
  \[
  \left( \frac{D \pi}{l} \right) = 1,
  \]
  then there are two \( l \)-isogenous elliptic curves over \( \mathbb{F}_p \).
- Isogenies of an Elkies degree form branchless cycles:

![Graphical representation of branchless cycles](image-url)
Direction Determination

- Frobenius equation for points of order \( l \):
  \[ \pi^2 - t\pi + \rho = 0 \pmod{l} \]

  \[ \left( \frac{t^2 - 4\rho}{l} \right) = 1 \quad \Rightarrow \quad \text{there are 2 roots: } \pi_1, \pi_2 \text{ over } F_l \]
  – the Frobenius eigenvalues

- Action of the Frobenius endomorphism on an isogeny kernel is equivalent to multiplication of points by an eigenvalue [Elkies 1998]:
  \[ (X^p, Y^p) = \pi \cdot (X, Y) \text{ in } F_p[X, Y] / (Y^2 - X^3 - aX - b, H(X)) \]
Directed Step

**Input:** field \( F_p \), curve \( E \), degree \( l \), direction \( \pi \)

**Algorithm:**

- Find a root \( j_1 \) of \( \Phi_1(j, T) = 0 \) over \( F_p \)
- Compute an isogenous elliptic curve \( E_1 \)
- Compute the polynomial \( H_1(X) \) which determines the isogeny kernel [Müller 1995]
- Check whether \( (X^p, Y^p) = \pi \cdot (X, Y) \) in \( F_p [X, Y] / (Y^2 - X^3 - aX - b, H_1(X)) \)
  - If not, then compute \( E_2 \) using the root \( j_2 \)
Cycle of Prime Length

- $U$ - a set of isogenous elliptic curves over $F_p$
- $\#U = H(D_{\pi})$ - a class number [Schoof 1987]
- Practical observation:
  $\#U$ is prime $\Rightarrow$ single isogeny cycle
Isogeny Star

Example over $\mathbb{F}_{83}$:

Isogenies of degree 3

Star

Isogenies of degree 5

A graph of prime number of elliptic curves, connected by isogenies of Elkies degrees
Route on Star

- For given
  - $F_p$ - a finite field
  - $E$ - an elliptic curve in a star
  - $\{ l_i \}$ - a set of isogeny degrees
  - $\{ \pi_i \}$ - a set of positive directions

- A route is a set $R=\{ r_i \}$, where $r_i$ is a number of steps by $l_i$-isogeny in the direction $\pi_i$

- Routes are commutative: $R_A R_B = R_B R_A$
Key Agreement

\[ A \xrightarrow{R_A(E_0)} B \]
\[ A \xleftarrow{R_B(E_0)} B \]

\[ R_A R_B(E_0) = R_B R_A(E_0) \]
Key Agreement - Algorithm

Common parameters:
- $F_p$ – a finite field
- $E_0$ – an initial elliptic curve
- $\{ l_i \}$ – a set of Elkies isogeny degrees
- $\{ \pi_i \}$ - a set of Frobenius eigenvalues

Algorithm:
- A randomly chooses a route $R_A$ and sends $E_A = R_A(E_0)$
- B randomly chooses a route $R_B$ and sends $E_B = R_B(E_0)$
- A computes $E_K = R_A(E_B)$, B computes $E_K = R_B(E_A)$
- Resulting key is the $j$-invariant of $E_K$
Public-Key Encryption

\[ E_{\text{init}} - \text{initial elliptic curve} \quad \rightarrow \quad R_{\text{priv}} - \text{computation of public key} \quad \rightarrow \quad E_{\text{pub}} - \text{public-key elliptic curve} \]

\[ R_{\text{enc}} - \text{encryption} \quad \rightarrow \quad E_{\text{add}} - \text{additional elliptic curve} \quad \rightarrow \quad R_{\text{priv}} - \text{decryption} \quad \rightarrow \quad E_{\text{enc}} - \text{encryption elliptic curve} \]

\[ \quad \rightarrow \quad R_{\text{priv}} - \text{private-key route} \quad \rightarrow \quad R_{\text{enc}} - \text{encryption route} \]
Security

- Problem of searching for a route between elliptic curves

- Solving methods on an \#U-curves star:
  - Brute-force: $O(\#U)$ isogenous steps
  - Meet-in-the-middle: $O(\sqrt{\#U})$ isogenous steps
  - Others - ?
Quantum Computer Resistance

- An algorithm of a route search requires a subroutine, which calculates a chain of isogeny steps

- Calculation of an isogeny chain requires consecutive solving of modular equation $\Phi_j(j, T) = 0$, where $j$ is being changed with every step

- Leads to exponential time of the algorithm
Complexity and Sizes

- Key agreement complexity:
  - $O(\log \#U)$ isogeny steps, or
  - $O(\log^4 p)$ field operations

- Consuming operations:
  - $X^p \mod H(X)$
  - solving of $\Phi_i(j, T) = 0$

- For $2^{80}$ secrecy:
  - field characteristic: $p \sim 2^{320}$
  - star size $\sim 2^{160}$
  - number of isogeny degrees $\sim 40$
  - steps per degree: 0 ... ±8
Parameters Selection

- Obtaining a large prime \#U is very complicated
- Hypothesis: \#U must have a large prime divisor
- Choose $D_{\pi} = D \cdot f^2$, where $f$ is a large prime conductor and $h(D)$ is small. Then [Cohen, 1996]

\[
h_{D_{\pi}} = h_D \cdot \left( f - \left( \frac{D}{f} \right) \right) = h_D \cdot (f \pm 1)
\]

Choose $f$ such that $\frac{f \pm 1}{2}$ is prime
Test Implementation

- Mathematica 5.0
- $F_{2038074743}$
- Star of 55103 elliptic curves (prime), chosen by direct computation of a class number
- 6 isogeny degrees: $\{3, 5, 7, 11, 13, 17\}$
- 0...9 steps per each isogeny degree
A. Rostovtsev and A. Stolbunov
Public-Key Cryptosystem Based on Isogenies
http://eprint.iacr.org/2006/145