How to be Ready for Tomorrow's Quantum Attacks

Dr. Vladimir Soukharev

InfoSec Global Inc.

May 17, 2017

Outline

- Capabilities of Quantum Computers
- How Quantum Computers Affect Public-Key Cryptography
- When Do We Need to be Ready for Quantum Attacks?
- Solutions
- Introduction to Post-Quantum Cryptography
- Post-Quantum ECC
- Summary and Conclusion

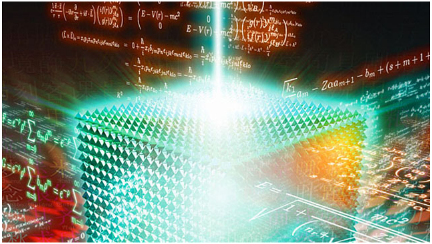
INFOSEC GLOBAL

Introduction

- Ongoing practical research and development paves the way for building large-scale quantum computers.
- Small scale quantum computers already exist.
- In about 20 years, large-scale quantum computers will become a reality.
- Their computational power is much higher than that of the classical computers used today.
- Their computational capabilities can be used to attack cryptosystems!

Capabilities of Quantum Computers

- Quantum computers will be able to perform compuatations much faster.
- In some areas much, much faster...exponential to polynomial running time.
- Search algorithms can be performed in square root time (Grover's algorithm).
- Factorization and discrete logs can be computed in polynomial time (Shor's algorithm).



How is Cryptography Affected?

Symmetric:

- Generic square root quantum search algorithms apply.
- Need to double the key length.

Public-Key:

- Schemes, whose security is based on integer factorization (RSA), can be broken in quantum polynomial time.
- Schemes, based on DLOG problem, can be broken in quantum polynomial time.
- All of the currently standardized asymmetric cryptography (RSA, ECC) can be efficiently broken by a quantum adversary!
- No 'easy fix' as for symmetric cryptography.

Why Do We Need to Worry About It *Today?*

"It will be too late to worry about it when quantum computers are here."

- It takes years to switch.
- For many products, the production cycle could be a decade or two.
- The messages encrypted using classical techniques today can be successfully decrypted tomorrow by quantum adversaries.
- Quantum computers might be here sooner than we expect...

INFOSEC GLOBAL

Solution: Post-Quantum Cryptography

- We need classical cryptographic schemes, that would be immune to quantum attacks.
- **Post-Quantum Cryptography**!
- Protects you today, against the threats of tomorrow.
- NIST is working on it.
- NSA is working on it.
- We are working on it and have solutions!

INFOSEC GLOBAL

Post-Quantum Cryptography

- Elliptic Curve Isogeny-Based Cryptography.
- Hash-Based Signatures.
- Lattice-Based Cryptography.
- Code-Based Systems.
- Multivariate Polynomials-Based Systems.

Elliptic Curves

We assume that F is a *finite field* of characteristic *greater than* 3. "Finite field" is essential, because cryptography uses finite fields. "Characteristic greater than 3" is not essential, but it simplifies matters greatly.

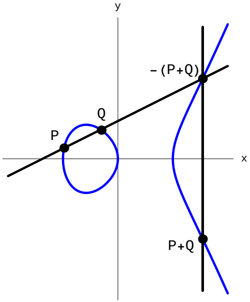
Definition

An *elliptic curve* over F is the set of solutions $(x, y) \in F^2$ to an equation

$$y^2 = x^3 + ax + b, \quad a, b \in F,$$

plus an additional point ∞ (at infinity).

Group Law



Elliptic curves admit an abelian group operation with identity element ∞. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. Then

$$P+Q = \left(\left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2, \right.$$

$$\left. - \left(\frac{y_2-y_1}{x_2-x_1}\right) \left(\left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - 2x_1 - x_2 \right) - y_1 \right)$$

INFOSEC GLOBAL

Isogenies

Definition

Let E and E' be elliptic curves over F.

- An *isogeny* $\phi\colon E \to E'$ is a non-constant algebraic morphism

  $$\phi(x, y) = \left(\frac{f_1(x, y)}{g_1(x, y)}, \frac{f_2(x, y)}{g_2(x, y)}\right)$$

  satisfying $\phi(\infty) = \infty$ (equivalently, $\phi(P + Q) = \phi(P) + \phi(Q)$).
- The *degree* of an isogeny is its degree as an algebraic map.
- The *endomorphism ring* $\mathrm{End}(E)$ is the set of isogenies from $E(\bar{F})$ to itself, together with the constant homomorphism. This set forms a ring under pointwise addition and composition.

INFOSEC GLOBAL

Examples

Example (Scalar multiplication)

- Let $E : y^2 = x^3 + ax + b$.
- For $n \in \mathbb{Z}$, define $[n] \colon E \to E$ by $[n](P) = nP$. Then $[n]$ is an isogeny of degree n^2.
- When $n = 2$,

$$[2](x, y) = \left(\frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}, \frac{(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b - a)y}{8(x^3 + ax + b)^2} \right)$$

- An explicit formula for $[n]$ is given recursively by the so-called *division polynomials*.

INFOSEC GLOBAL

Ordinary and Supersingular Curves

Theorem

Let E be an elliptic curve defined over a finite field. As a $\mathbb{Z}$-module, $\dim_{\mathbb{Z}} \mathrm{End}(E)$ is equal to either 2 or 4.

Definition

An elliptic curve E over a finite field is *supersingular* if $\dim_{\mathbb{Z}} \mathrm{End}(E) = 4$, and *ordinary* otherwise.

- Ordinary curves are more secure for DLOG cryptography.
- For any isogeny $\phi \colon E \to E'$, the curves E and E' are always either both ordinary or both supersingular.

Isogenies and Kernels

- Given any finite subgroup $K \subset E$ of size n, there exists a unique isogeny (up to isomorphism)

$$\phi \colon E \to E'$$

  such that

$$\ker \phi = K.$$

- $\deg \phi = n = \#K$.
- Denote E' by E/K.
- Example:
  - Let $P \in E$ and $\operatorname{ord}(P) = n$.
  - Set $K = \langle P \rangle = \{xP : x \in \mathbb{Z}\}$.
  - $\phi \colon E \to E/\langle P \rangle$ and $\deg \phi = n$.
  - Compute this with Vélu's formulas.

m-Torsion Points and Their Applications

- For a curve $E/\mathbb{F}_q$ and m relatively prime to q, the set of *m-torsion* points is

$$E[m] = \{P \in E(\bar{\mathbb{F}}_q) : mP = \infty\}.$$

- $E[m]$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^2$.

Setup:

- Fix a prime p of the form $\ell_A^{e_A}\ell_B^{e_B} \cdot f \pm 1$.
- Fix a supersingular curve E defined over $\mathbb{F}_{p^2}$, and bases $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$ which generate $E[\ell_A^{e_A}]$ and $E[\ell_B^{e_B}]$ respectively.

INFOSEC GLOBAL

Determining Isogenous-ity

Theorem (Tate 1966)

Two curves E and E' are isogenous over $\mathbb{F}_q$ if and only if $\#E = \#E'$.

Remark

The cardinality $\#E$ of E can be calculated in polynomial time using Schoof's algorithm [Schoof 1985], which, incidentally, is also based on isogenies.

Brief Summary (Background)

- It's easy to figure out if two curves are isogenous, but hard to find that isogeny.
- We only use supersingular elliptic curves, as they are more secure.
- Isogenies are group homomorphisms, i.e. for points $P, Q \in E$ and integers m, n, $\phi(m \cdot P + n \cdot Q) = \phi(m \cdot P) + \phi(n \cdot Q) = m \cdot \phi(P) + n \cdot \phi(Q)$.
- Rather than working with isogenies, we work with the kernel of isogenies, which can be represented with one elliptic curve point.
- Let K be the corresponding kernel point to isogeny ϕ, then we can denote $\phi\colon E \to E' = E/\langle K \rangle$.
- Prime p is of the form $\ell_A^{e_A} \ell_B^{e_B} \cdot f \pm 1$.

Underlying Hard Problem

Given two isogenous elliptic curves E and E', find an isogeny between them.

- For supersingular elliptic curves, this problem is fully *quantum* exponential.

Keys

Scheme's public parameters:

- Elliptic curve E defined over $\mathbb{F}_{p^2}$.
- Bases $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$.

User A decides to use basis $\{P_A, Q_A\}$ and does the following:

- Randomly selects integers $m_A, n_A \in \mathbb{Z}_{\ell_A^{e_A}}$.
- Computes the elliptic curve point $K_A = m_A \cdot P_A + n_A \cdot Q_A$.
- Computes the image curve $\phi_A \colon E \to E/\langle K_A \rangle = E_A$.
- Evaluates $\phi_A(P_B)$ and $\phi_A(Q_B)$.

User A's private key is: integers m_A, n_A.

User A's public key is: elliptic curve E_A and elliptic curve points $\phi_A(P_B)$ and $\phi_A(Q_B)$.

Key Agreement

User A's parameters:

- Private: integers m_A, n_A.
- Public: elliptic curve E_A and elliptic curve points $A_1 = \phi_A(P_B)$ and $A_2 = \phi_A(Q_B)$.

User B's parameters:

- Private: integers m_B, n_B.
- Public: elliptic curve E_B and elliptic curve points $B_1 = \phi_B(P_A)$ and $B_2 = \phi_B(Q_A)$.

User A and user B exchange their *public* information.

INFOSEC GLOBAL

Key Agreement (A's side)

User A does the following:

1. Using user B's public points and user A's own private integers, computes the elliptic curve point $K_{BA} = m_A \cdot B_1 + n_A \cdot B_2$.
   Note:

$$\begin{aligned} m_A \cdot B_1 + n_A \cdot B_2 &= m_A \cdot \phi_B(P_A) + n_A \cdot \phi_B(Q_A) \\ &= \phi_B(m_A \cdot P_A) + \phi_B(n_A \cdot Q_A) \\ &= \phi_B(m_A \cdot P_A + n_A \cdot Q_A) \\ &= \phi_B(K_A). \end{aligned}$$

2. Using user B's curve and value K_{BA}, computes $\phi_{BA} \colon E_B \to E_B/\langle K_{BA} \rangle = E_{BA}$.
   OBSERVATION:
   $E_{BA} = E_B/\langle \phi_B(K_A) \rangle = E/\langle K_B \rangle / \langle \phi_B(K_A) \rangle = E/\langle K_B, K_A \rangle$.
3. Computes j-invariant(E_{BA}).

INFOSEC GLOBAL

Key Agreement (B's side)

User B does the following:

1. Using user A's public points and user B's own private integers, computes the elliptic curve point $K_{AB} = m_B \cdot A_1 + n_B \cdot A_2$.
   Note:
$$\begin{aligned} m_B \cdot A_1 + n_B \cdot A_2 &= m_B \cdot \phi_A(P_B) + n_B \cdot \phi_A(Q_B) \\ &= \phi_A(m_B \cdot P_B) + \phi_A(n_B \cdot Q_B) \\ &= \phi_A(m_B \cdot P_B + n_B \cdot Q_B) \\ &= \phi_A(K_B). \end{aligned}$$
2. Using user A's curve and value K_{AB}, computes $\phi_{AB} \colon E_A \to E_A/\langle K_{AB}\rangle = E_{AB}$.
   OBSERVATION:
   $E_{AB} = E_A/\langle \phi_A(K_B)\rangle = E/\langle K_A\rangle/\langle \phi_A(K_B)\rangle = E/\langle K_A, K_B\rangle$.
3. Computes j-invariant(E_{AB}).

INFOSEC GLOBAL

Key Agreement (Aftermath)

Value obtained by user A is $E_{BA} = E/\langle K_B, K_A \rangle$.
Value obtained by user B is $E_{AB} = E/\langle K_A, K_B \rangle$.

But! $\langle K_B, K_A \rangle = \langle K_A, K_B \rangle$.

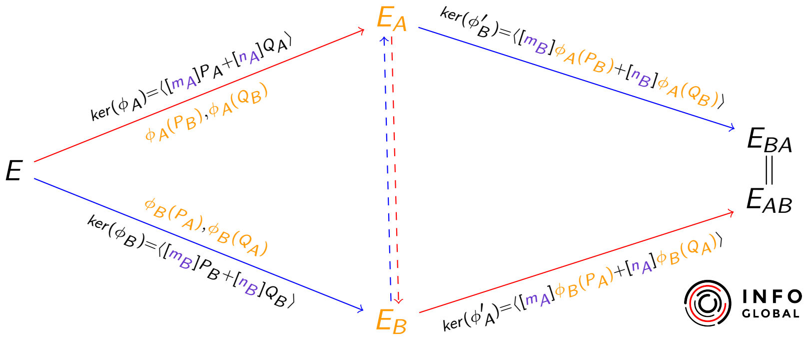
This means that E_{AB} and E_{BA} are the same curves (up to isomorphism).

Result: $\text{j-invariant}(E_{BA}) = \text{j-invariant}(E_{BA}) \leftarrow$ common key.

Key Agreement

Private parameters	Public parameters
Alice: $m_A, n_A \in_R \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$	**Alice:** E_A
$\phi_A \colon E \to E_A$	$\phi_A(P_B), \phi_A(Q_B) \in E_A$
Bob: $m_B, n_B \in_R \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$	**Bob:** E_B
$\phi_B \colon E \to E_B$	$\phi_B(P_A), \phi_B(Q_A) \in E_B$

Shared secret: E_{AB}.



What Else Can be Done?

- Public-Key Encryption
- Undeniable Signatures
- Strong Designated Verifier Signatures
- Entity Authentication
- Authenticated Encryption
- Integrated Encryption
- *Much more in progress...successful progress...!*

INFOSEC GLOBAL

Why Isogenies?

- Elliptic Curve Cryptography is a well-understood area
- Can reuse a lot of implementations from classical ECC
- Clear security parameters
- Mathematical proofs
- Short key sizes
- Small communication overhead

Timeline of Required Post-Quantum Solutions

Now:

- Public-Key Encryption
- Key Agreement
- Authenticated Encryption
- Integrated Encryption

Between now and the emergence of quantum computers:

- Digital Signatures
- Entity Authentication
- Authentication-related blocks of any scheme

INFOSEC GLOBAL

Summary, Remarks and Future Development

- Quantum computers are likely to become a reality within approximately 20 years.
- We need to be protected against quantum adversaries today.
- The protection must be on the present-day computer; *Post-Quantum Cryptography!*
- ECC survives; *Elliptic Curve Isogenies!*
- Protection against quantum adversaries is available *today*!
- It is possible to replace classical components with quantum-resistant solutions in PKI (and other infrastructures) today.
- Research, development, standardisation, and integration are in progress and will continue.

INFOSEC GLOBAL

Thank You!