Supersingular Isogeny and Ring Learning With Errors-Based Diffie-Hellman Cryptosystems: A Performance and Security Comparison

Claudio Téllez
Diogo Pereira
Fábio Borges

Laboratório Nacional de Computação Científica - LNCC

10 de dezembro de 2018

Introduction

Both supersingular isogeny and ring learning with errors-based cryptosystems are promising candidates for a post-quantum era.

The expected disruptive capacity of quantum computing raises the need to foster the technical development of feasible post-quantum cryptosystems that take into account security standards and performance requirements.

Introduction

For this reason, our purpose is to analyze the trade-off between performance of security of two post-quantum key exchange protocols.

Our discussion addresses the feasibility of supersingular isogeny Diffie-Hellman (SIDH), based on isogenies between supersingular elliptic curves, and of lattice-based ring learning with errors key exchange (RLWE).

Introduction

- Introduction
- Theoretical foundations
- Performance and security analysis
- Conclusions

Theoretical Foundations - SIDH

- Elliptic curves in cryptography (ECC): mid-80's (Koblitz 1987, Miller 1985).
- Isogenies between ordinary elliptic curves: Rostovtsev and Stolbunov, 2006.
- Diffie-Hellman based on isogenies between supersingular elliptic curves (SIDH): Jao and De Feo, 2011.

Theoretical Foundations - SIDH

- ECC is vulnerable to quantum attacks.

  Shor's algorithm could break a 128-bit security level (256-bit module) curve using 2330 qubits and 1.26×10^{11} Toffoli gates.

- Isogeny-based cryptography with ordinary elliptic curves are unfeasible for a post-quantum era.

  Childs et al (2010) showed how to construct elliptic curve isogenies in quantum subexponential time.

Theoretical Foundations - SIDH

An isogeny $\varphi : E_1 \to E_2$ between elliptic curves E_1 and E_2 is a rational morphism that preserves both the geometry of elliptic curves and their group structures.

Isogeny-based cryptosystems are based on *isogeny graphs* whose vertices are equivalence classes of elliptic curves (defined by the j-invariant) and whose edges are isogenies between them.

Rostovtsev and Stolbunov's original formulation: isogeny graphs encompassing prime numbers of elliptic curves connected by isogenies are called *isogeny stars*. They used *routes* on wide enough isogeny stars for constructing cryptographic algorithms.

Theoretical Foundations - SIDH

Given a isogeny star of order n, the required complexity of attacks is estimated at $O(n)$ isogeny computations. The *meet-in-the-middle* technique provides an estimation of $O(\sqrt{n})$ computations. For elliptic curves over the field $\mathbb{F}_p$, Galbraith (1999) provided an estimation of $O(p^{1/4})$ computations.

Besides, as the j-invariant changes at every step, q equations must be solved consecutively in order to compute a chain of q isogenies. Hence, computations cannot be parallelized.

However, Childs et al (2010) found a subexponential algorithm to construct elliptic curve isogenies. Hence, cryptosystems based on isogenies between ordinary elliptic curves could be vulnerable to quantum attacks in subexponential time.

Theoretical Foundations - SIDH

An elliptic curve over a field k of characteristic $p > 0$ is *supersingular* iff its endomorphism ring over $\overline{k}$ has rank 4 (an order in a quaternion algebra).

Jao and De Feo's (2011) proposal for a Diffie-Hellman based on isogenies between supersingular elliptic curves (SIDH) relies onthe non-abelian structure of the set of isogenies of a supersingular elliptic curve. SIDH uses supersingular isogeny classes and replaces exponentiations by quotients.

Theoretical Foundations - RLWE

- Lattice-based cryptosystems (Ajtai, 1996).
- Learning With Errors problem (LWE) (Regev, 2009).
- Ring LWE (RLWE) (Lyubashevsky et al., 2013).
- RLWE Diffie-Hellman protocol (Peikert, 2014).

Theoretical Foundations - RLWE

The basic algebraic structure of RLWE is a *ring*. For example:

$$R = \mathbb{Z}_q[x]/\Phi(x)$$

(polynomials modulo a cyclotomic polynomial $\Phi(x)$ with coefficients in the field $\mathbb{F}_q$)

Theoretical Foundations - RLWE

The LWE problem in a ring R is defined by fixing an error distribution χ over R concentrated on small elements (i.e., relative to a small bound B). The objetive is to recover a secret $s(x) \in R$ by means of a sequence of approximations

$$(a_i(x), b_i(x))$$

where $a_i(x)$ are random known polynomials, $e_i(x)$ are random unknown polynomials (relative to the bound B), and

$$b_i(x) = a_i(x)s_i(x) + e_i(x)$$

If $\Phi(x)$ in $R = \mathbb{Z}_q/\Phi(x)$ is cyclotomic, the difficulty of solving the RLWE is equivalent to the difficulty of solving the SVP_δ lattice problem (the Approximate Shortest Vector Problem).

Theoretical Foundations - RLWE

The common parameters of the cryptosystem are:

- n, the degree of $\Phi(x)$
- $a(x) \in R$, a fixed polynomial of the ring
- q, a prime number
- χ, a probability distribution

The secret polynomials are $s(x) \in R$ and $e(x) \in R$ (with coefficients small in the integers, relative to a bound B). The coefficients of $s(x)$ and $e(x)$ are chosen according to χ. The public key is $b(x) = a(x)s(x) + e(x)$.

Theoretical Foundations

Table 1 shows a comparison between several Diffie-Hellman protocols:

Table 1: Comparison between the algorithms.

	DH	ECDH	SIDH	RLWEDH
Elements	Ints. g	Points P in E	Curves E in isogeny classes	Polynomials $a(x) \in R$
Secrets	exp. x	scalars k	isog. ϕ	small errors s, $e \in R$
Comp.	$g, x \mapsto g^x$	$k, P \mapsto [k]P$	$\phi, E \mapsto \phi(E)$	a, s, $e \mapsto a \cdot s + e$
Hard Problem	Given g, g^x, find x	Given P, $[k]P$, find k	Given E, $\phi(E)$, find ϕ	given a and $a \cdot s + e$, find s

Performance and Security Analysis

The security of the SIDH protocol depends on the problem of computing an isogeny between isogenous supersingular curves. The known complexities for solving this problem are:

- $O(p^{1/4})$ against classical attacks
- $O(p^{1/6})$ against quantum attacks

The pertinent classical and quantum complexities to solve the SVP_δ (provable) in any lattice are:

- $2^{0.804n+o_\delta(n)}$ in the classical case
- $2^{0.603n+o_\delta(n)}$ in the quantum case (ListSieve-Birthday algorithm)

Performance and Security Analysis

For the IFP (Integer Factorization Problem), we use the general number field sieve (GNFS) and compare a brute force attack with the GNFS. Matching the complexity, we have

$$2^x = \exp\left(\left(\left(\frac{64}{9}\right)^{1/3} + O(1)\right)(\ln n)^{1/3}(\ln\ln n)^{2/3}\right)$$

where n is the number for factorization.
To solve the DLP (Discrete Logarithm Problem), we use Pollard‘s Rho algorithm. Matching the complexities, we have

$$2^x = \sqrt{\frac{\pi o}{2}}$$

where o is the order of the group.

Performance and Security Analysis

Matching complexities, we have:

$2^x = p^{1/4}$	CI
$2^x = p^{1/6}$	QI
$2^x = 2^{0.804n}$	C-RLWE
$2^x = 2^{0.603n}$	Q-RLWE

Where CI corresponds to the best known algorithm to solve the isogeny problem (classical case), QI corresponds to the best known algorithm to solve the isogeny problem (quantum case), C-RLWE corresponds to the best known algorithm to solve the SVP_δ (classical case), and Q-RLWE corresponds to the best known algorithm to solve the SVP_δ (quantum case).

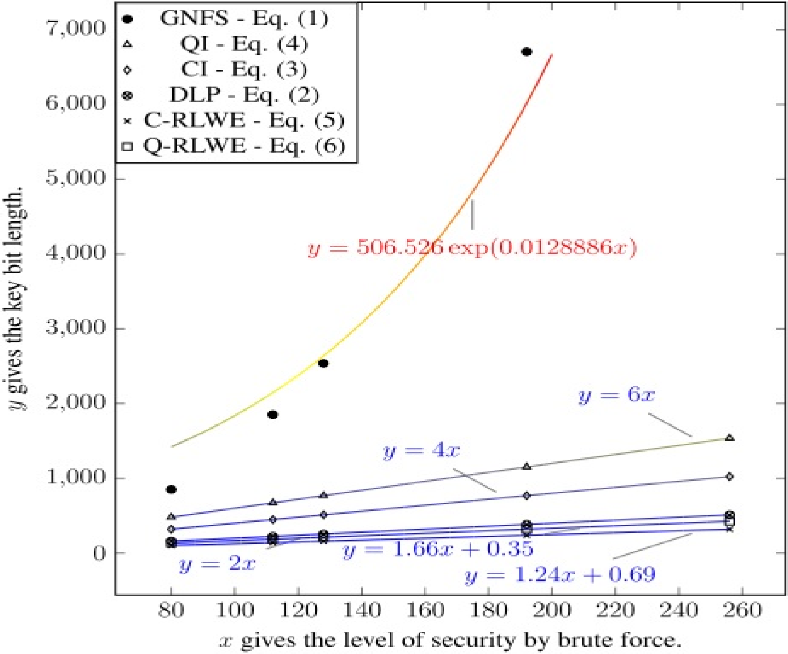
Performance and Security Analysis

Table 2 summarizes the results found. We added a column with the NIST recommended values.

Table 2: Comparison between brute force and minimum key length.

Brute Force	DLP	GNFS	NIST	CI	QI	C-RLWE	Q-RLWE
80	160	851	1 024	320	480	100	133
112	224	1 853	2 048	448	672	140	186
128	256	2 538	3 072	512	768	160	213
192	384	6 707	7 680	768	1152	239	319
256	512	13 547	15 360	1024	1536	319	425

As Grover's algorithm can find a n-bits key with complexity $O(\sqrt{n})$, any algorithm should at least double the key length to keep the same level of security against a quantum attacker. The next figure shows the trade-off between security and key bit lenght, with the interpolation polynomials from the data in Table 2.


GNFS - Eq. (1)
QI - Eq. (4)
CI - Eq. (3)
DLP - Eq. (2)
C-RLWE - Eq. (5)
Q-RLWE - Eq. (6)
$y = 506.526 \exp(0.0128886x)$
$y = 6x$
$y = 4x$
$y = 2x$
$y = 1.66x + 0.35$
$y = 1.24x + 0.69$
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
80
100
120
140
160
180
200
220
240
260
y gives the key bit length.
x gives the level of security by brute force.

Performance and Security Analysis

As for costs, in the case of SIDH, the main point is to compute isogenies. Both known algorithms to perform this task (multiplication-oriented or isogeny-oriented) have a cost of $O(log^2 p)$ (where the major cost corresponds to the isogeny evaluation).

For the RLWE key exchange, the more pertinent cost relates to the random sampling of error polynomials. To use $a(x)$ as a global constant allows further optimization. In the simplified key exchange described in the paper, the procedure required a total of 8 polynomial multiplications, 1 application of the *Sig* function and 2 computations of key streams.

Conclusions

- SSI achieves small key sizes with good performance at the practical security levels recommended by NIST.
- When the security level increases, the cost for SIDH increases exponentially slower than for classical cryptographic algorithms.
- The same result applies to RLWE - that outperforms SSI regarding both key sizes and performance.
- Hence, we conclude that both analyzed cryptosystems are good candidates against quantum attacks in the near future.


Thank you