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

Claudio Téllez[1]
Diogo Pereira[1]
Fábio Borges[1]

[1] Laboratório Nacional de Computação Científica (LNCC)
25651-075, Petrópolis - RJ - Brasil

{ctellez,dpereira,borges}@lncc.br

Abstract. *The purpose of this work is to provide a complexity analysis of the trade-off between performance and security for two post-quantum cryptosystems: isogeny cryptosystems based on supersingular elliptic curves (SSI) and the lattice-based ring learning with errors key exchange (RLWE), considered to be secure against quantum attacks. The intractability of the Computational Supersingular Isogeny Problem (CSSIP) and of the Decisional Supersingular Product Problem (DSSPP) form the basis of the security for cryptosystems based on isogenies between supersingular elliptic curves. As for the RLWE cryptosystem, its security rests on the hardness of the Learning With Errors problem, proven to be as hard as the Shortest Vector Problem (SVP). We analyze the trade-off between performance and security for both SSI and RLWE cryptosystems in comparison with Discrete Logarithm Problem (DLP) and Integer Factorization Problem (IFP). As complexities increase for the attack algorithms when the key lengths become longer, RLWE outperforms all the other algorithms (including SSI) regarding key sizes at practical security levels.*

1. Introduction

The current scene of research in the field of cryptography is characterized by the search for quantum-safe cryptosystems. In theory, the hard mathematical problems that guarantee the security of most current cryptosystems, the Integer Factorization Problem (IFP) and the Discrete Logarithm Problem (DLP), could be solved using quantum algorithms as [Shor 1995] and [Grover 1996]. Such potential vulnerability poses an important challenge to privacy and information security.

According to a NIST's report [Chen et al. 2016], we expect the appearance of quantum computers with cryptographic capacity around the year 2030. As information assets are crucial for the proper functioning of the banking system, of global finance, of military security and, ultimately, of the international system as a whole, further efforts in post-quantum cryptography are necessary in order to cope with information security challenges in the near future [Mosca 2018]. While some scholars are skeptic regarding the disruptive capacity of quantum computing and its political impact on international security [Lindsay 2018], a recent report by RAND Corporation points quantum computing as a potential cause of loss of data security just a few decades from now [Hoehn et al. 2018].

This prospective raises the need to both critically address the evolution of the political-military-social context in the world to come [Davis and Nacht 2018] and to foster the technical development of feasible post-quantum cryptosystems that take into account security standards and performance requirements.

In this paper, we perform a complexity analysis of the trade-off between performance and security for two post-quantum cryptosystems that appear as promising candidates for a post-quantum world: isogeny cryptosystems based on supersingular elliptic curves (SSI) and the lattice-based ring learning with errors key exchange (RLWE), both considered to be secure against attacks performed by an adversary using a quantum computer. The hardness of the Computational Supersingular Isogeny Problem (CSSIP) and of the Decisional Supersingular Product Problem (DSSPP) form the basis of the security for cryposystems based on isogenies between supersingular elliptic curves. Regarding the RLWE cryptosystem, its security rests on the hardness of the Learning With Errors (LWE) problem, proven to be as hard as the Shortest Vector Problem (SVP) for lattices. We analyze the trade-off between performance and security for both SSI and RLWE cryptosystems in comparison with Discrete Logarithm Problem (DLP) and Integer Factorization Problem (IFP). Our purpose is to analyze whether those cryptosystems are capable to meet performance goals for desired levels of security, that is a pertinent discussion regarding the feasibility of these protocols as quantum-safe cryptosystems.

In the next section, we present a short theoretical introduction to both SSI and RLWE cryptosystems. In the third section of the paper, we discuss the performance and security of both SSI and RLWE in comparison to other relevant cryptosystems and the practical security levels recommended by NIST. The closing section presents our conclusions and directions for further research.

2. Theoretical foundations

2.1. Supersingular Isogeny-based (SSI) cryptosystems

As Shor's algorithm rends conventional elliptic curve cryptosystems vulnerable and inadequate for post-quantum cryptography [Roetteler et al. 2017], Rostotsev and Stolbunov proposed an approach based on isogenies between ordinary elliptic curves [Rostovtsev and Stolbunov 2006]. However, using an approach based on the Generalized Riemann Hypothesis (GRH) and expansion properties of Cayley graphs, [Childs et al. 2010] showed a way to obtain elliptic curve isogenies in quantum subexponential time, thus rendering isogeny-based cryptosystems unfeasible for a post-quantum era. We refer the reader to [Téllez and Borges 2018] for a more detailed exposition regarding the foundations of Rostotsev and Stolbunov's approach based on isogenies between ordinary elliptic curves.

While cryptosystems based on isogenies between ordinary elliptic curves were shown to be quantum vulnerable, the supersingular case seems to be quantum-resistant. In 2011, [Jao and Feo 2011] proposed a Diffie-Hellman protocol based on isogenies between supersingular elliptic curves (SIDH). It is important to remark that ECDH is based on the group of rational points of a fixed ordinary elliptic curve, for which the related endomorphism ring is abelian. Supersingular elliptic curves, however, have endomorphism rings isomorphic to an order in a quaternion algebra. SIDH's security against quantum

attacks relies precisely on the non-commutative structure of the set of isogenies of a supersingular elliptic curve (together with the composition operation).

The original foundations of the basic theory of supersingular elliptic curves can be found at [Deuring 1941]. For a more detailed presentation of the mathematical foundations of SIDH and of the key exchange protocol algorithm, see [Téllez and Borges 2018].

2.2. Lattice-based Ring Learning With Errors (RLWE) cryptosystems

Lattice-based cryptosystems were first proposed by [Ajtai 1996]. Learning With Errors (LWE) problem was introduced by [Regev 2009] and the RLWE appeared in [Lyubashevsky et al. 2013]. A Diffie-Hellman key exchange protocol based on RLWE was proposed by [Peikert 2014]. We follow closely the exposition put forth by [Singh 2015] and by [Singh and Chopra 2015].

The basic algebraic structure that underlies RLWE is a ring $R = \mathbb{Z}_q[x]/\Phi(x)$ of polynomials modulo a cyclotomic polynomial $\Phi(x)$ with coefficients in the field $\mathbb{F}_q$ of integers $\mod q$ where q is a prime. Other parameters are: n, a prime number or a power of 2, a fixed polynomial $a(x) \in R$, a secret polynomial $s(x) \in R$, a secret polynomial $e(x) \in R$ of degree less than n with coefficients "small" in the integers, and a public polynomial $b(x) = a(x)s(x) + e(x)$. For "small" coefficients, we fix a bound B much less than q, for example $B = 5$ [Singh 2015] and chose the coefficients from the set $\{q-5, q-4, q-3, q-2, q-1, 0, 1, 2, 3, 4, 5\}$.

The LWE problem in the ring R is defined by fixing an error distribution χ over R concentrated on "small" elements. The coefficients of $s(x)$ and $e(x)$ are chosen according to the distribution χ. Hence, the parameters of RLWE cryptosystem are n, q, $\Phi(x)$, $a(x)$, and the probability distribution χ that produces the coefficients for the secret polynomials $s(x)$ and $e(x)$, which constitute together the private key. The public key is $b(x)$.

We recall from algebra that for any positive integer n the n-th cyclotomic polynomial is the unique irreducible polynomial (with integer coefficients) that divides x^n-1 and does not divide x^k-1 if $k < n$. If n is a prime number, $\Phi_n(x) = 1+x+x^2+\ldots+x^{n-1}$ and if $n = 2p$ where p is an odd prime we have $\Phi_n(x) = 1-x+x^2-\ldots+x^{p-1} = \sum_{i=0}^{p-1}(-x)^i$.

The key exchange works as follows. Both Alice and Bob know q, n, $a(x)$. Alice generates two polynomials s_A and e_A with "small" coefficients by sampling from χ. She calculates $p_A = a \cdot s_A + 2e_A$ and sends it to Bob. Bob generates two polynomials s_B and e_B with "small" coefficients by sampling from χ, and computes $p_B = a \cdot s_B + 2e_B$. He also generates a small e'_B from the distribution χ and computes $k_B = p_A \cdot s_B + 2e'_B = a \cdot s_A \cdot s_B + 2e_A \cdot s_B + 2e'_B$. Using the signal function Sig, Bob finds $w = Sig(k_B)$ by applying Sig on each coefficient of k_B. The Sig function is defined using the subset $E = \{-\lfloor \frac{q}{4} \rfloor, \ldots, \lfloor \frac{q}{4} \rceil\} \subset \mathbb{Z}_q = \{-\frac{q-1}{2}, \ldots, \frac{q-1}{2}\}$, where $\lfloor\ \rfloor$ denotes the floor and $\lfloor\ \rceil$ denotes rounding to the nearest integer. Then, $Sig(v) = 0$ if $v \in E$ and $Sig(v) = 1$ if $v \notin E$. Subgaussian errors with parameters as tight as possible are desirable in order to guarantee that the security parameters of the errors can be smoothly controlled once combined in the shared secret values [Singh and Chopra 2015].

Then, Bob calculates the key stream $sk_B = Mod_2(k_B, w)$, where $Mod_2(v, w) = \left(v + w \cdot \frac{q-1}{2}\right) \mod q \mod 2$. After that step, Bob sends p_B and w to Alice.

Finally, Alice generates e'_A from the distribution χ and computes $k_A = p_B \cdot s_A + 2e'_A = a \cdot s_A \cdot s_B + 2e_B \cdot s_A + 2e'_A$. Alice's key stream is produced as $sk_A = Mod_2(k_A, w)$.

Observe that $k_A \approx k_B$, and the Sig function is a reconciliation function that serves to obtain a shared key from these values. As for the parameter choices, [Singh 2015] suggests $n = 1024$, $q = 40961$, a uniform distribution χ and a public key size of 2048 bytes to a security claim greater than 2^{256}. The parameters proposed by [Alkim et al. 2015] are $n = 1024$, $q = 12289$, a binomial distribution χ and a public key size of 1792 bytes to a security claim greater than 2^{128}, a significant improvement in the key size in comparison to the proposal by [Singh 2015].

Table 1 summarizes the main components of the original Diffie-Hellman (DH), Elliptic Curve Diffie-Hellman (ECDH), Supersingular Isogeny Diffie-Hellman (SIDH), and RLEW Diffie-Hellman (RLWEDH).

Table 1. Comparison between the algorithms.

	DH	ECDH	SIDH	RLWEDH
Elements	Integers g	Points P in E	Curves E in isogeny classes	Polynomials $a(x) \in R = \mathbb{Z}_q[x]/\langle\Phi_n(x)\rangle$
Secrets	exponents x	scalars k	isogenies ϕ	small errors $s, e \in R$
Computations	$g, x \mapsto g^x$	$k, P \mapsto [k]P$	$\phi, E \mapsto \phi(E)$	$a, s, e \mapsto a \cdot s + e$
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

3. Performance and security analysis

3.1. Security of the SIDH

[Jao and Feo 2011] argue that the DSSPP is at least easier than the CSSIP. For this reason, the security of the SIDH protocol depends on the problem of computing an isogeny between isogenous supersingular curves. In the general case, the fastest known algorithm to accomplish this task has complexity of $O(\sqrt{p}\, log^2 p)$ [Charles et al. 2009]. However, we use a more specific case, with known complexities for solving the CSSIP of $O(p^{1/4})$ against classical attacks [Feo et al. 2011] and $O(p^{1/6})$ against quantum attacks [Tani 2009].

To solve the IFP, we use the general number field sieve (GNFS), a subexponential complexity approach. We compare a brute force attack in a key of x bits with the GNFS. Matching the complexity for brute force with the complexity of GNFS, we have

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

where n is the number for factorization. As parameters for brute force are known, we can find the length of n.

To solve the DLP, we use Pollard's Rho algorithm for logarithms, that is the best current algorithm to deal with the DLP. Similarly, matching the complexities, we have

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

where o is the order of the group.

Let us name classic isogeny (CI) for the algorithm of Galbraith and Stolbunov [Galbraith and Stolbunov 2013], currently the best algorithm for classic computers to solve the isogeny problem [Feo et al. 2011]. The matching of CI complexity is given by

$$2^x = p^{1/4}, \tag{3}$$

where p is the characteristic of the field, where the classes of supersingular elliptic curves are defined. Similarly, let us name quantum isogeny (QI) for Tani's algorithm [Tani 2009], known as the best quantum algorithm to solve the isogeny problem [Adj et al. 2018]. The matching of QI complexity is given by

$$2^x = p^{1/6}. \tag{4}$$

3.2. Security of the RLWE

The security of RLWE relies on the worst-case hardness of problems in ideal lattices. In particular, for the RLWE protocol, its security is based on the underlying hardness of ring learning with errors problem that has been proven to be as hard as the worst case solution to the shortest vector problem (SVP) in an ideal lattice [Khot 2005, van Emde Boas 1981]. Given a basis of a lattice L, the SVP consists of finding a shortest non-zero vector in L. However, to find a reasonable short vector may be sufficient for several practical applications. In this case, we use an approximation factor $\delta > 1$ and the *approximate* SVP$_\delta$ consists of finding a non-zero vector $v \in L$ of length at most $\delta \cdot \lambda(L)$, where $\lambda(L) = \min_{v \in L \setminus \{0\}} ||v||$ corresponds to the length of the shortest non-zero vector in L.

Using the Euclidean norm, lattice basis reduction provides the best known approaches to the SVP$_\delta$. In this case, for large $\delta = 2^{\Omega(n)}$ (where n is the lattice dimension), the Lenstra-Lenstra-Lovász algorithm (LLL) is capable to find a solution in polynomial time in n [Lenstra et al. 1982]. For smaller values of δ, the Block Korkine-Zolotarev algorithm (BKZ) is commonly used [Schnorr and Euchner 1994]. Currently, the best known lattice reduction algorithm is the BKZ 2.0 that incorporates improvements as the Gama-Nguyen-Regev pruning [Chen and Nguyen 2011].

The pertinent classical and quantum complexities to solve SVP$_\delta$ (provable) in any lattice are presented by [Laarhoven et al. 2015] as $2^{0.804n+o_\delta(n)}$ in the classical case and $2^{0.603n+o_\delta(n)}$ with quantum search and correspond to the ListSieve-Birthday algorithm [Wei et al. 2015].

Let us name C-RLWE the best algorithm for classical computers to solve the SVP$_\delta$. Hence, the matching of C-RLWE complexity is given by

$$2^x = 2^{0.804n} \tag{5}$$

Where n corresponds to the lattice dimension. Similarly, Q-RLWE denotes the quantum algorithm to solve the SVP$_\delta$. The matching of Q-RLWE complexity is given by

$$2^x = 2^{0.603n} \tag{6}$$

We removed the term $o_\delta(n)$ from equations 5 and 6 because we are assuming the worst case, that would correspond to the instantaneous solution of the part with complexity $o_\delta(n)$.

Table 2 summarizes the values found with the equations. We have one more column with the values recommended by the National Institute of Standards and Technology (NIST) [Barker 2016]. [Téllez and Borges 2018] and [Borges de Oliveira 2017] present similar values for DLP given by Eq. (2) and for GNFS given by Eq. (1).

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

Brute Force	DLP Eq. (2)	GNFS Eq. (1)	NIST	CI Eq. (3)	QI Eq. (4)	C-RLWE Eq. (5)	Q-RLWE Eq. (6)
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

It is important to remark that using the Grover's algorithm for brute force attack, a n-bits key can be found with complexity $O(\sqrt{n})$. Therefore, every cryptographic algorithm should at least double the key length to keep the same level of security against an attacker using a quantum computer. The performance is directly proportional to the key length. Figure 1 depicts a trade-off between security and key bit length, with the interpolation polynomials from the data in Table 2.

3.3. Performance

[Jao and Feo 2011] provide two algorithms for the task of computing isogenies of a given kernel in a key exchange protocol. The main point is to compute

$$\phi_A : E_0 \to E_A, \text{ where } E_A = E_0/\langle [m_A]P_A + [n_A]Q_A \rangle.$$

Defining $R_0 := [m_A]P_A + [n_A]Q_A$, the order of R_0 is $l_A^{e_A}$. Then, for $0 \leq i < e_A$, we have

$$E_{i+1} = E_i/\langle l_A^{e_A-i-1}R_i \rangle, \quad \phi_i : E_i \to E_{i+1}, \quad R_{i+1} = \phi_i(R_i),$$

where ϕ_i is a l_A-isogeny. Hence, $E_A = E_{e_A}$ and ϕ_A is found by composition

$$\phi_{e_A-1} \circ \ldots \circ \phi_0.$$

As presented in [Téllez and Borges 2018], walks on expander (Ramanujan) graphs can be used to compute the isogenies that compose ϕ_A. There are two cost-equivalent strategies, *multiplication-oriented* and *isogeny-oriented*, for the iterative computation of the required isogenies.

For key exchanges, Alice and Bob can choose between two algorithms (multiplication-oriented or isogeny-oriented). Both have a cost of $O(log^2 p)$ in the chosen finite field. The major cost corresponds to the isogeny evaluation. Hence, as l_A grows, the multiplication-oriented algorithm becomes preferable over the isogeny-based algorithm. Thus, the performance cost is 2 times the key length, which grows by a factor of 4 for classic computers and of 6 by quantum computers. Therefore, its performance cost increases by a factor of 8 and 18, respectively.

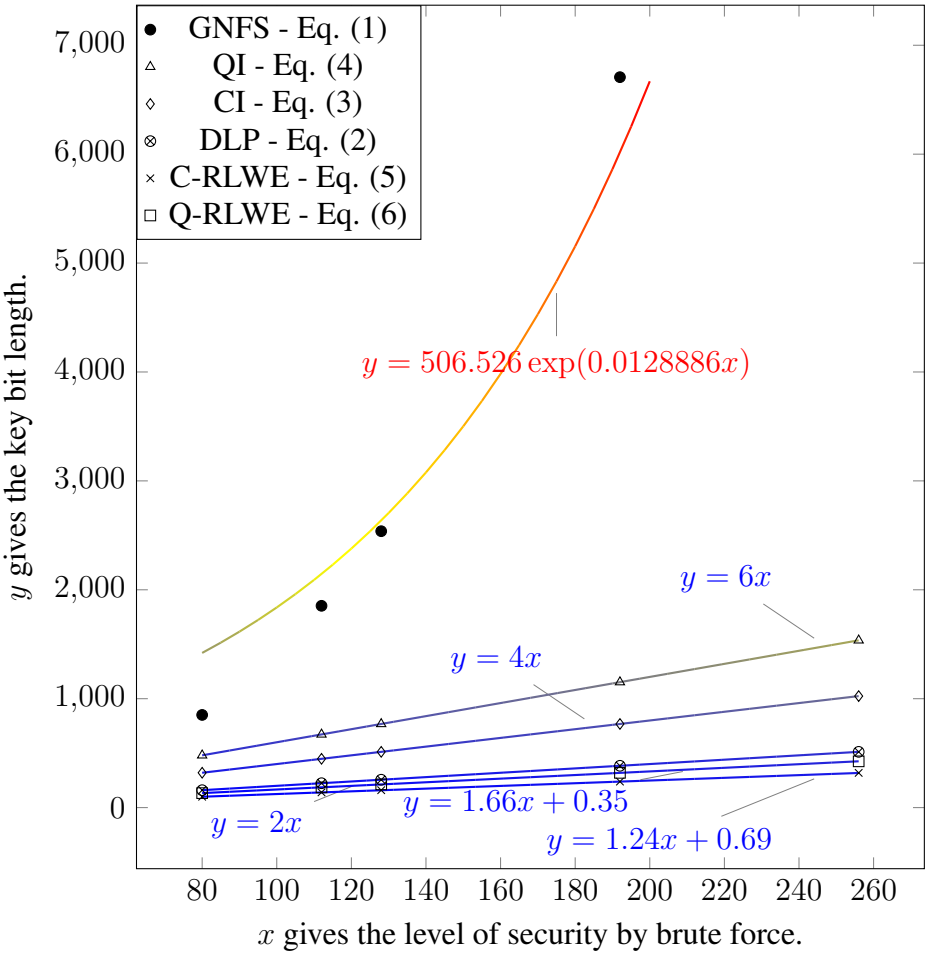

Figure 1. Comparison between brute force and minimum key length.

The complexity for modular exponentiation is $O(\log e)$, where e is the exponent [Borges et al. 2017]. Therefore, its performance cost increases by a factor of 2. If e is chosen randomly, it has the size of the module. Therefore, its performance cost increases exponentially. See Figure 1.

As for RLWE key exchange, it is desirable to obtain subgaussian errors with parameters as tight as possible in order to guarantee that the security parameters of the errors can be smoothly controlled once combined in the shared secret values. [Singh 2015] observes that sampling the errors terms using Gaussian distributions is fairly expensive. Uniform sampling from a B bounded interval (for example, using $B = 5$) is simpler and more efficient.

In the key generation procedure, the more pertinent cost relates to the random sampling of the error polynomials and the use of $a(x)$ as a global constant allows further optimization.

The simplified key exchange procedure is described in section 2.2. In total, the RLWE procedure requires 8 polynomial multiplications, 1 application of the Sig function and 2 computations of key streams.

4. Conclusions

In this paper, we discussed the trade-off between performance and security for two post-quantum cryptosystems that appear as promising candidates for a post-quantum world: isogeny cryptosystems based on supersingular elliptic curves (SSI) and the lattice-based ring learning with errors key exchange (RLWE). Both cryptosystems are considered to be secure against quantum attacks. While the security of SIDH rests on the Computational Supersingular Isogeny Problem (CSSIP) and on the Decisional Supersingular Product Problem (DSSPP), the security of the RLWE cryptosystem is based on the hardness of the LWE problem, proven to be as hard as the SVP for lattices.

In our analysis, we compared performance and security for both SSI and RLWE cryptosystems related to the Discrete Logarithm Problem (DLP) and the Integer Factorization Problem (IFP). Our results show that SSI achieves small key sizes with good performance at the practical security levels recommended by NIST. Moreover, 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.

As research towards the advancement of quantum computers progresses, it is reasonable to expect that quantum attacks may improve. Further research is required in order to cope with this challenge. Apart from new theoretical suggestions based on the algebraic foundations of both SSI and RLWE, practical implementations would be welcome in order to evaluate security and performance in the real world, and to provide feasible benchmarks to the development of strong post-quantum candidates.

Acknowledgements

We would like to thank Pronametro, CNPq, and FAPERJ for supporting the development of this work.

References

Adj, G., Cervantes-Vázquez, D., Chi-Domínguez, J.-J., Menezes, A., and Rodríguez-Henríquez, F. (2018). On the cost of computing isogenies between supersingular elliptic curves. *IACR Cryptology ePrint Archive*, 2018:313.

Ajtai, M. (1996). Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 99–108, New York, NY, USA. ACM.

Alkim, E., Ducas, L., Pöppelmann, T., and Schwabe, P. (2015). Post-quantum key exchange - a new hope. Cryptology ePrint Archive, Report 2015/1092. `https://eprint.iacr.org/2015/1092`.

Barker, E. (2016). Recommendation for Key Management. Part 1: General. NIST Special Publication 800-57 Part 1 Revision 4 [Online]. Available: `http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4` [January 2016]. National Institute of Standards and Technology, Gaithersburg, MD.

Borges, F., Lara, P., and Portugal, R. (2017). Parallel algorithms for modular multi-exponentiation. *Applied Mathematics and Computation*, 292:406–416.

Borges de Oliveira, F. (2017). *Selected Privacy-Preserving Protocols*, pages 61–100. Springer International Publishing, Cham.

Charles, D. X., Lauter, K. E., and Goren, E. Z. (2009). Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113.

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., and an Daniel Smith-Tone, R. P. (2016). NIST Report on Post-Quantum Cryptography NISTIR 8105 [Online]. Available: `http://dx.doi.org/10.6028/NIST.IR.8105` [April 2016]. National Institute of Standards and Technology, Gaithersburg, MD.

Chen, Y. and Nguyen, P. Q. (2011). Bkz 2.0: Better lattice security estimates. In Lee, D. H. and Wang, X., editors, *Advances in Cryptology – ASIACRYPT 2011*, pages 1–20, Berlin, Heidelberg. Springer Berlin Heidelberg.

Childs, A. M., Jao, D., and Soukharev, V. (2010). Constructing elliptic curve isogenies in quantum subexponential time. *CoRR*, abs/1012.4019.

Davis, Z. S. and Nacht, M. (2018). Closing thoughts: Humanity, machines and power. In Davis, Z. S. and Nacht, M., editors, *Strategic Latency: Red, White, and Blue: Managing the National and International Security Consequences of Disruptive Technologies*, chapter 18, pages 288–295. Center for Global Security Research, Lawrence Livermore National Laboratory, Livermore, CA.

Deuring, M. (1941). Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 14(1):197–272.

Feo, L. D., Jao, D., and Plût, J. (2011). Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Cryptology ePrint Archive, Report 2011/506. `https://eprint.iacr.org/2011/506`.

Galbraith, S. and Stolbunov, A. (2013). Improved algorithm for the isogeny problem for ordinary elliptic curves. *Applicable Algebra in Engineering, Communication and Computing*, 24(2):107–131.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *ANNUAL ACM SYMPOSIUM ON THEORY OF COMPUTING*, pages 212–219. ACM.

Hoehn, A. R., Parasiliti, A., Efron, S., and Strongin, S. (2018). Discontinuities and Distractions - rethinking Security for the Year 2040: Findings from a RAND Corporation Workshop, CF-384. Technical report, RAND Corporation. Available at: https://www.rand.org/pubs/conf_proceedings/CF384.html.

Jao, D. and Feo, L. D. (2011). Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Yang, B.-Y., editor, *Post-Quantum Cryptography*, pages 19–34. Springer-Verlag.

Khot, S. (2005). Hardness of approximating the shortest vector problem in lattices. *J. ACM*, 52(5):789–808.

Laarhoven, T., Mosca, M., and van de Pol, J. (2015). Finding shortest lattice vectors faster using quantum search. *Designs, Codes and Cryptography*, 77(2):375–400.

Lenstra, A. K., Lenstra, H. W., and Lovasz, L. (1982). Factoring polynomials with rational coefficients. *MATH. ANN*, 261:515–534.

Lindsay, J. (2018). Why quantum computing will not destabilize international security: The political logic of cryptology. Available at SSRN: https://ssrn.com/abstract=3205507.

Lyubashevsky, V., Peikert, C., and Regev, O. (2013). On ideal lattices and learning with errors over rings. *J. ACM*, 60(6):43:1–43:35.

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5):38–41.

Peikert, C. (2014). Lattice cryptography for the internet. In Mosca, M., editor, *Post-Quantum Cryptography*, pages 197–219, Cham. Springer International Publishing.

Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40.

Roetteler, M., Naehrig, M., Svore, K. M., and Lauter, K. (2017). Quantum resource estimates for computing elliptic curve discrete logarithms. In *Proc. ASIACRYPT 2017*, volume 10625, pages 241–270. Springer.

Rostovtsev, A. and Stolbunov, A. (2006). Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Report 2006/145. `https://eprint.iacr.org/2006/145`.

Schnorr, C. P. and Euchner, M. (1994). Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Mathematical Programming*, 66(1):181–199.

Shor, P. W. (1995). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509.

Singh, V. (2015). A practical key exchange for the internet using lattice cryptography. *IACR Cryptology ePrint Archive*, 2015:138.

Singh, V. and Chopra, A. (2015). Even more practical key exchanges for the internet using lattice cryptography. Cryptology ePrint Archive, Report 2015/1120. `https://eprint.iacr.org/2015/1120`.

Tani, S. (2009). Claw finding algorithms using quantum walk. *Theoretical Computer Science*, 410(50):5285 – 5297.

Téllez, C. and Borges, F. (2018). Trade-off between performance and security for supersingular isogeny-based cryptosystems. *Anais do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)*, pages 113–126.

van Emde Boas, P. (1981). *Another Np-complete Partition Problem and the Complexity of Computing Short Vectors in a Lattice*. Mathematical preprints series. Universiteit van Amsterdam. Mathematisch Instituut.

Wei, W., Liu, M., and Wang, X. (2015). Finding shortest lattice vectors in the presence of gaps. In Nyberg, K., editor, *Topics in Cryptology — CT-RSA 2015*, pages 239–257, Cham. Springer International Publishing.