Hybrid hash function based on the DLP and SIS problems

Dimitri Koshelev[1] and Francesc Sebé[2]

[1] National Academy of Sciences of Belarus, Institute of Mathematics, Department of Algebra, Minsk, Belarus
dimitri.koshelev@gmail.com
[2] University of Lleida, Department of Mathematics, Lleida, Spain
francesc.sebe@udl.cat

Abstract. This short note discusses in detail a folklore but little-known hybrid hash function grounded on both the discrete logarithm and short integer solution problems. In particular, specific satisfactory parameters are provided to ensure the standard 128-bit security level for the lattice problem with 256-bit module, which may be useful in its own right. The hash function is a natural generalization of the classical Pedersen and Ajtai ones. Nevertheless, to the authors' knowledge, no one has previously explicitly analysed their hybrid version. Besides, the obtained result is probably prone to significant further optimizations by applying many tricks from elliptic curve and lattice cryptographies. Hashing is known to be a basic operation for constructing more complex and important cryptographic schemes. The authors intend to explore such hybrid ones in future articles. However, the hash function under consideration may be precious by itself due to its double provable security. Thus, this introductory work represents a kind of reincarnation of curve-based cryptography whose development has been severely and unfairly undermined by the potential but still vague quantum threat.

Keywords: discrete logarithm problem · hashing to elliptic curves · hybrid cryptography · relation lattices · short integer solution problem

1 Introduction

The discovery of quantum algorithms, most notably of Shor's algorithm [58] (cf. Regev's recent one [5,55]) for integer factorization and computing discrete logarithms, demonstrated that traditional public-key cryptographic primitives are fundamentally vulnerable in the presence of large-scale quantum computers. At the same time, transitioning fully to modern presumably post-quantum (PQ) alternatives remains suspicious due to their shorter term of scrutiny and difficulty of safe practical implementation. For example, several NIST finalists, namely the digital signature Rainbow [18,23] and key exchange/encapsulation mechanism SIDH [34]/SIKE [33] were completely broken in [12] and [16,44,56], respectively. What is most striking is that these schemes were invented more than a dozen years ago before the attacks were carried out.

In contrast, elliptic curve cryptography (ECC) recently celebrated a respectable age (40 years) [47], although for many years there has been no any progress in breaking it (as well as RSA) by classical algorithms. Meanwhile, today's quantum capacities continue to be negligible according to [28,31]. As a consequence, considerable attention has been devoted to hybrid approaches [24] (mainly for key establishment [6,35,59,60,61] and digital signing [7,13,32,49,53,57]) combining conventional and post-quantum assumptions within a single scheme. Such dual-mode cryptographic protocols are thereby designed to remain secure even if one of the computational assumptions is eventually broken. Hybrid deployments are particularly attractive during the current PQ transition period, since they provide compatibility with most quantum-oriented regulator recommendations without sacrificing the time-tested ECC layer.

Hash functions [48] are perhaps the most elementary cryptographic primitive. Typically, those of the form $\{0,1\}^* \to \{0,1\}^\ell$, where $\ell \in \mathbb{N}$, are used in practice. However, algebraic hash functions (see, e.g., [10,15]) have been actively developed in the last decade towards zero-knowledge proofs. For such hashes, the domain, codomain, or both consist of vectors over large finite fields for the sake of efficiency. Furthermore, most real-world hash functions are not provably secure, meaning that the belief in them is based not on a mathematical task but on careful community analysis. And hybrid hashes are extremely rare even in the scientific literature. Despite this well-established practice, mathematical hash functions often anticipate new rich areas of cryptographic science. The authors hope that the same will happen also with hybrids.

There are two classical (algebraic) hash functions attributed to Pedersen [50] (cf. [17]) and Ajtai [2] (cf. [3,29]). The former relies on the hardness of the (multidimensional) discrete logarithm problem (DLP) in a cyclic group. In turn, the latter is grounded on the (inhomogeneous) short integer solution ((I)SIS) problem and related worst-case lattice assumptions. Both constructions are provably one-way and collision-resistant under their assumptions. In addition, due to their homomorphism property, they naturally support multiset operations (including incremental/decremental updates) on hash values without rehashing from scratch. The given technique is called multiset or incremental hashing [8,9,20,45], positively distinguishing the Pedersen/Ajtai hashes from generally accepted ones.

1.1 New contribution

Most existing hybrid constructions combine independent cryptographic mechanisms at the protocol level. In this setting, the underlying algebraic structures are not related inherently to each other. For instance, two hash functions can be sequentially applied one after the other as their composition. Nonetheless, when considering more advanced primitives, the form of the hash functions is still public but internally depends on chosen secret trapdoors. One of the trapdoors may be determined by resolving only one hard problem. Even if this circumstance does not directly lead to the hacking of the corresponding hybrid cryptosystem, its use in the real world may be more questionable. In short, an attacker is able

to exploit in some way such partial key information if one of the honest parties does not completely execute the hybrid scheme by carelessness. At the same time, another honest party may suffer from such sloppy actions even if perfectly follows the scheme description. This is why truly hybrid cryptography should be one in which obtaining even a part of the secret key requires solving two underlying problems.

One possible approach to desirable "non-separable" hybridization is founded on the relation lattice associated with fixed points on an elliptic curve (in fact, any DLP-strong group is suitable). If the discrete logarithms between the points are unknown, this lattice is hidden. Therefore, there is no sense in even talking about a lattice problem, let alone solving it. Even if an adversary has a sufficiently powerful quantum computer, this only allows it to formulate the given lattice challenge. Inter alia, if the DLP or SIS is weak for certain parameters, the paper's hash function (essentially) degenerates into the Ajtai or Pedersen extreme instance, respectively.

The described idea is not new at all. It was briefly mentioned in a series of publications [9, Section 4.3], [45, Section 8]. However, to the authors' knowledge, no one has previously discussed concrete (optimal) parameters for the SIS problem with enormous module. In comparison, such modules occur for the "dual" learning with errors (LWE) problem [54] in the works [22,51]. The former is especially relevant to the present article, since it is equally devoted to the hybrid mode, although RSA groups are preferred there instead of elliptic curves. Unfortunately, the cited article has not received much attention, possibly because hybrid (and even pure lattice) cryptography was not very pertinent in its presentation year (namely 2015) and the chosen venue is less known for the global cryptographic community.

The main goal of this short note is to rigorously define and analyse the announced Pedersen–Ajtai-type hash function (see Section 2). To make the text more self-contained, we will independently demonstrate that the resistance of the resulting construction is reduced to resolving sequentially the DLP and SIS problems. This simple fact should in no way be recognized as our merit. Furthermore, in Section 3 specific parameters will be provided that ensure at least the standard 128-bit security level for both computational problems. This would be extremely difficult to achieve without the renowned lattice estimator [4,21] being maintained by Albrecht's team. In addition, the authors prepared in SageMath a reference implementation [41] of the hash function. Finally, Section 4 briefly comments on a logical continuation of the current research direction.

2 Hybrid hash function

Consider an additive group G of large prime order r with fixed generator $P_0 \in G$ and zero $\mathcal{O}$. Keeping in mind an elliptic curve $E \subset \mathbb{A}^2_{(x,y)}$ in Weierstrass form over a finite field $\mathbb{F}_q$, we will call elements of G points. That is why the symbol r will be preferred over q for module order unlike the conventional notation in lattice-based cryptography. For conciseness, let's put $\ell := \lceil \log_2(r) \rceil$ and $\ell' := \lceil \log_2(q) \rceil$,

bearing in mind the inequality $\ell \leqslant \ell'$. To be definite, vectors will be assumed to be columns. We will deal exclusively with the infinity norm $|v|_\infty := \max_{i=1}^{m} |v_i|$ for $v \in \mathbb{Z}^m$ and $m \in \mathbb{N}$. Also, we introduce the closed hypercube $C := \{v \in \mathbb{Z}^m \mid |v|_\infty \leqslant b\}$ of radius $b \in \mathbb{N}$ in general, although $b = 1$ throughout this note for the sake of simplicity.

Given a matrix $A \in (\mathbb{Z}/r)^{n \times m}$ with $0 < n \leqslant m$, we have the lattice

$$L := \Lambda_r^\perp(A) = \{v \in \mathbb{Z}^m \mid Av \equiv 0 \pmod{r}\},$$

which is r-ary, i.e., $r\mathbb{Z}^m \subset L$. It obviously coincides with the kernel of the group homomorphism

$$\rho\colon \mathbb{Z}^m \to G^n \qquad v \mapsto Pv,$$

where $P \in G^{n \times m}$ is the point matrix corresponding to A, that is, $P_{i,j} := A_{i,j}P_0$. In the literature, L is called relation lattice or discrete logarithm lattice [25].

Despite their definition, the points $P_{i,j}$ have to be generated for safety in such a way that nobody knows any non-trivial relation between them, i.e., any non-zero vector of the lattice L. In particular, the matrix entries $A_{i,j}$ are also unknown. Such points can be rapidly obtained by means of the simple x-coordinate rejection sampling or of constant-time maps [19,26,40]. Alternatively, one can resort to more complicated batch point generation approaches [36,39] or [38, Section 5]. Each one has its own (dis)advantages, but all of them are justified in the light of considerable number nm (see Section 3).

Our hash function $H : \{0,1\}^m \to \{0,1\}^{m'}$ is the composition $\chi \circ \rho$ of the restricted map $\rho : \{0,1\}^m \to G^n$ and some auxiliary one $\chi : G^n \to \{0,1\}^{m'}$, where $m' \approx n\ell$ in ideal situation. When $G \subset E(\mathbb{F}_q)$ is a subgroup of the $\mathbb{F}_q$-point group on E, the second map is logically just the n-time projection to the coordinate x supplied with the sign bit of the coordinate y. [3] In this scenario, $m' = n(\ell' + 1)$, which is close to $n\ell$ whenever $\ell \approx \ell'$. As is usual, we require that $m > m'$ in order to compress input binary strings. The compression ratio of H is therefore $c := m/m' > 1$. The hash function is recursively extended to arbitrary length via the classical Merkle–Damgård transformation [48, Section 13.1]:

$$H^*\colon \{0,1\}^* \to \{0,1\}^{m'} \qquad v \mapsto H\big(v_1|H(v_2|\cdots|H(v_k|\overline{0})\big),$$

where $v = v_1|v_2|\cdots|v_k$ such that the lengths $\mathrm{len}(v_i) = d := m - m'$ and $\mathrm{len}(\overline{0}) = m'$. [4] Evidently, the greater the ratio c (i.e., the difference $d = (c-1)m'$), the smaller the value k or, equivalently, the faster the recursion process.

[3] The zero point $\mathcal{O} = (0 : 1 : 0)$ can be always embedded into $\ell' + 1$ bits in some manner, as $\ell < \ell' + 1$.

[4] Since $\mathrm{len}(v)$ is not necessarily a multiple of d, some collision-preserving padding must be applied first of all. The Merkle–Damgård proposal consists in adding to v the minimum quantity z of zeros up to the last t bits sufficient for representing the length of v in its binary form. To put it another way, $\mathrm{len}(v) + z + t = kd$, where t, d are fixed once and forever, while z, k are variable and $z < d$. For example, the value $t = 64$ is more than enough in every conceivable use case of H^*.

Lemma 1. *The hash function H (and hence H^*) is immune to finding collisions and preimages once the underlying DLP or SIS problem is hard.*

Proof. Since the projection χ is without collisions (due to the sign of y) and easily invertible, which costs determining n square roots in $\mathbb{F}_q$, it is enough to analyse the first map ρ. Searching for its collision, i.e., a pair $v_1, v_2 \in \{0,1\}^m$ such that $v_1 \neq v_2$ and $\rho(v_1) = \rho(v_2)$ boils down to searching for the short vector $v = v_1 - v_2 \in C \setminus \{\overline{0}\}$ such that $Pv = \overline{\mathcal{O}}$. We deal with the multidimensional DLP [5,27] also known as the representation problem [14], abstracting for a moment from the shortness of v. Under the assumption that it is malleable, so is the ordinary DLP in G according to [14, Proposition 7]. As a result, the matrix A is entirely recovered, allowing to formulate the corresponding SIS problem, which is already equipped with the solution v.

Similarly, if someone is able to sample $v \in \{0,1\}^m$ such that $Pv = Q$ given $Q \in G^n \setminus \{\overline{\mathcal{O}}\}$, the matrix A is again recovered as well as the discrete logarithms $u_i := \log_{P_0}(Q_i)$. This implies facing the (already solved) ISIS challenge $Av \equiv u \pmod r$. In other words, the attacking party has the solution $(v, 1)$ of the SIS problem of dimension $m+1$ with respect to the concatenated matrix $(A \mid -u)$. Notice that this SIS instance is slightly easier than the former (for $Q = \overline{\mathcal{O}}$), because the remaining parameters r, n, and $b = 1$ are the same. □

Remark 1. Unlike ρ, the composite function H is not homomorphic because of the component χ. Thereby, H does not enjoy incremental hashing compared to ρ. As is seen in the proof of the previous lemma, the function ρ is by itself immune to finding collisions and inverse images. That is why ρ is a self-sufficient useful construction if input binary strings are always of length $\leqslant m$. Otherwise, it is necessary to represent output points in a certain bit form, loosing the homomorphism property.

3 An instance for the 128-bit security level

Let's instantiate the foregoing hybrid hash function H (as well as H^*) on the secp256k1 curve $E\colon y^2 = x^3+7$ (see, e.g., [1]) of j-invariant 0. It is one of the most widespread 128-bit elliptic curves, leveraged in particular in the cryptocurrency Bitcoin. Being defined over a 256-bit prime field $\mathbb{F}_q$, secp256k1 is a curve of prime order r. In other words, $G = E(\mathbb{F}_q)$ and the bit length $\ell = \ell' = 256$. In order to obtain a satisfactory rate of H^*, it is suggested to take the value c close to 1.5, imposing the condition $m = \lceil 1.5 \cdot m' \rceil$. First, since $m \geqslant 256$ a priori, Grover's quantum algorithm [30] is not a threat to the 128-bit security of H (not to mention H^*).

Launching a short script uploaded to [41] for the lattice estimator [21] (derivative of the seminal paper [4]), we see that $n = 2$ is the smallest natural number such that the SIS security level $\lambda \geqslant 128$. More precisely, the estimator returns the parameters

$$n = 2, \qquad m = 771, \qquad m' = 514, \qquad c = 1.5, \qquad d = 257, \qquad \lambda \approx 173.$$

Note that our dimension m is an order of magnitude smaller than in [22, Section 4.3, Table 5], namely than 270000, albeit this is not a fair comparison: SIS with elliptic curves versus LWE with RSA groups. Besides, the estimator was initiated only in 2021, hence the authors of [22] might choose the too conservative m by mistake. Unfortunately, calls with dimensions so enormous fail to check for the estimator version at our disposal.

Clearly, the worst running time of evaluating H at $v \in \{0,1\}^m$ takes place whenever all $v_i = 1$. In this scenario, $n(m-1) = 1540$ additions on E are required. Of course, this is the true cost as well as when H must be deterministically evaluated (i.e., regardless of v) to protect against side channel attacks. Nonetheless, only $m/2 = 385.5$ units occur in average in the uniformly sampled vector v. Consequently, there are $n(m/2-1) = 769$ curve additions for computing H with public v. [5] This is comparable in time with just a couple of general scalar multiplications on E, especially if the addition and doubling operations are identical as for twisted Edwards curves [11] popular among implementers. Indeed, the simple double-add algorithm launched twice performs $2(\ell+\ell/2) = 768$ curve operations. With the help of our proof-of-concept implementation [41] in SageMath the reader can verify that H and H^* do work correctly and pretty efficiently.

4 Future work

A drawback of the presented hybrid hash function consists in its speed relatively slow compared to conventional ones. Nevertheless, the construction appears to be subject to essential acceleration, moving from the SIS problem to its more algebraic versions Ring-SIS (R-SIS) [43,46,52] and Module-SIS (M-SIS) [42]. The former problem enables significantly smaller keys and improved computational efficiency by exploiting the rich algebraic structure of univariate polynomial rings over $\mathbb{Z}/r$. In turn, the latter problem generalizes both SIS and R-SIS by considering modules over such rings. M-SIS provides a compromise between the conservative security of SIS and the performance of R-SIS. By adjusting the module rank, cryptographic schemes can balance these two aspects while mitigating structural concerns inherent for the purely ring setting. However, we can entirely rely on the ring version in hybrid mode. Even if a specific non-quantum attack on R-SIS is found one day, a cryptosystem will be saved by the ECC part.

Acknowledgements. Dimitri Koshelev was supported by the Belarusian State Research Program "Convergence–2030", 1.02.1. The authors express their gratitude to Damien Stehlé, Elena Kirshanova, Iván Blanco Chacón, Joël Felderhoff, Jordi Pujolàs, Léo Ducas, Martin Albrecht, Mike Edward Moras, Samuel Neves, Steven Galbraith, Weiqiang Wen, and Youssef El Housni for fruitful discussions on this article.

[5] The number of additions on E can be in fact reduced even more provided that the points $P_{i,j}$ are generated via the non-trivial but still safe way from [37].

References

1. secp256k1, https://github.com/bitcoin-core/secp256k1
2. Ajtai, M.: Generating hard instances of lattice problems. In: STOC 1996: Symposium on Theory of Computing. pp. 99–108. Association for Computing Machinery, New York (1996), https://doi.org/10.1145/237814.237838
3. Ajtai, M.: Generating hard instances of the short basis problem. In: Wiedermann, J., van Emde Boas, P., Nielsen, M. (eds.) Automata, Languages and Programming. Lecture Notes in Computer Science, vol. 1644, pp. 1–9. Springer, Berlin, Heidelberg (1999), https://doi.org/10.1007/3-540-48523-6_1
4. Albrecht, M.R., Player, R., Scott, S.: On the concrete hardness of learning with errors. Journal of Mathematical Cryptology **9**(3), 169–203 (2015), https://doi.org/10.1515/jmc-2015-0016
5. Barbulescu, R., Barcau, M., Paşol, V.: Extending Regev's quantum algorithm to elliptic curves. In: Escudero, D., Damgård, I. (eds.) Progress in Cryptology – LATINCRYPT 2025. Lecture Notes in Computer Science, vol. 16129, pp. 234–266. Springer, Cham (2026), https://doi.org/10.1007/978-3-032-06754-8_9
6. Barnes, R., Connolly, D.: Post-quantum and post-quantum/traditional hybrid algorithms for HPKE (2026), https://datatracker.ietf.org/doc/draft-ietf-hpke-pq
7. Becker, A., Guthrie, R., Jenkins, M.: Related certificates for use in multiple authentications within a protocol (RFC 9763) (2025), https://datatracker.ietf.org/doc/rfc9763
8. Bellare, M., Goldreich, O., Goldwasser, S.: Incremental cryptography: The case of hashing and signing. In: Desmedt, Y.G. (ed.) Advances in Cryptology – CRYPTO 1994. Lecture Notes in Computer Science, vol. 839, pp. 216–233. Springer, Berlin, Heidelberg (1994), https://doi.org/10.1007/3-540-48658-5_22
9. Bellare, M., Micciancio, D.: A new paradigm for collision-free hashing: Incrementality at reduced cost. In: Fumy, W. (ed.) Advances in Cryptology – EUROCRYPT 1997. Lecture Notes in Computer Science, vol. 1233, pp. 163–192. Springer, Berlin, Heidelberg (1997), https://doi.org/10.1007/3-540-69053-0_13
10. Ben-Sasson, E., Goldberg, L., Levit, D., with an appendix by Faugère, J.-C., Perret, L.: STARK friendly hash – survey and recommendation (2020), https://eprint.iacr.org/2020/948
11. Bernstein, D.J., Birkner, P., Joye, M., Lange, T., Peters, C.: Twisted Edwards curves. In: Vaudenay, S. (ed.) Progress in Cryptology – AFRICACRYPT 2008. Lecture Notes in Computer Science, vol. 5023, pp. 389–405. Springer, Berlin, Heidelberg (2008), https://doi.org/10.1007/978-3-540-68164-9_26
12. Beullens, W.: Breaking Rainbow takes a weekend on a laptop. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology – CRYPTO 2022. Lecture Notes in Computer Science, vol. 13508, pp. 464–479. Springer, Cham (2022), https://doi.org/10.1007/978-3-031-15979-4_16
13. Bindel, N., Hale, B., Connolly, D., D, F.: Hybrid signature spectrums (2025), https://datatracker.ietf.org/doc/draft-ietf-pquip-hybrid-signature-spectrums
14. Brands, S.A.: An efficient off-line electronic cash system based on the representation problem (1993), https://ir.cwi.nl/pub/5303
15. Canteaut, A., Beyne, T., Dinur, I., Eichlseder, M., Leander, G., Leurent, G., Naya-Plasencia, M., Perrin, L., Sasaki, Y., Todo, Y., Wiemer, F.: Report on the security of STARK-friendly hash functions (version 2.0) (2020), https://eips.ethereum.org/assets/eip-5988/papers/report_security_stark_friendly_hash.pdf

16. Castryck, W., Decru, T.: An efficient key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023. Lecture Notes in Computer Science, vol. 14008, pp. 423–447. Springer, Cham (2023), https://doi.org/10.1007/978-3-031-30589-4_15
17. Chaum, D., van Heijst, E., Pfitzmann, B.: Cryptographically strong undeniable signatures, unconditionally secure for the signer. In: Feigenbaum, J. (ed.) Advances in Cryptology – CRYPTO 1991. Lecture Notes in Computer Science, vol. 576, pp. 470–484. Springer, Berlin, Heidelberg (1992), https://doi.org/10.1007/3-540-46766-1_38
18. Chen, M.S., Ding, J., Kannwischer, M., Patarin, J., Petzoldt, A., Schmidt, D., Yang, B.Y.: Rainbow signature, https://www.pqcrainbow.org
19. Chávez-Saab, J., Rodríguez-Henríquez, F., Tibouchi, M.: SwiftEC: Shallue-van de Woestijne indifferentiable function to elliptic curves. In: Agrawal, S., Lin, D. (eds.) Advances in Cryptology – ASIACRYPT 2022. Lecture Notes in Computer Science, vol. 13791, pp. 63–92. Springer, Cham (2022), https://doi.org/10.1007/978-3-031-22963-3_3
20. Clarke, D., Devadas, S., van Dijk, M., Gassend, B., Suh, G.E.: Incremental multiset hash functions and their application to memory integrity checking. In: Laih, C.S. (ed.) Advances in Cryptology – ASIACRYPT 2003. Lecture Notes in Computer Science, vol. 2894, pp. 188–207. Springer, Berlin, Heidelberg (2003), https://doi.org/10.1007/978-3-540-40061-5_12
21. Curtis, B., Yun, C., Lefebvre, C., Virdia, F., Göpfert, F., Hunt, H., Kippen, H., Owen, J., Ducas, L., Pulles, L., Schmidt, M., Albrecht, M.R., Walter, M., Abapour, N., Player, R., Scott, S.: Security estimates for lattice problems, https://github.com/malb/lattice-estimator
22. Dagdelen, O., Gajek, S., Göpfert, F.: Learning with errors in the exponent. In: Kwon, S., Yun, A. (eds.) Information Security and Cryptology – ICISC 2015. Lecture Notes in Computer Science, vol. 9558, pp. 69–84. Springer, Cham (2016), https://doi.org/10.1007/978-3-319-30840-1_5
23. Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. In: Ioannidis, J., Keromytis, A., Yung, M. (eds.) Applied Cryptography and Network Security. ACNS 2005. Lecture Notes in Computer Science, vol. 3531, pp. 164–175. Springer, Berlin, Heidelberg (2005), https://doi.org/10.1007/11496137_12
24. Driscoll, F., Parsons, M., Hale, B.: Terminology for post-quantum traditional hybrid schemes (RFC 9794) (2025), https://datatracker.ietf.org/doc/rfc9794
25. Ducas, L., Pierrot, C.: Polynomial time bounded distance decoding near Minkowski's bound in discrete logarithm lattices. Designs, Codes and Cryptography **87**(8), 1737–1748 (2019), https://doi.org/10.1007/s10623-018-0573-3
26. Faz-Hernandez, A., Scott, S., Sullivan, N., Wahby, R.S., Wood, C.A.: Hashing to elliptic curves (RFC 9380) (2023), https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve
27. Galbraith, S.D., Ruprai, R.S.: An improvement to the Gaudry–Schost algorithm for multidimensional discrete logarithm problems. In: Parker, M.G. (ed.) Cryptography and Coding. IMACC 2009. Lecture Notes in Computer Science, vol. 5921, pp. 368–382. Springer, Berlin, Heidelberg (2009), https://doi.org/10.1007/978-3-642-10868-6_22
28. Gidney, C.: Why haven't quantum computers factored 21 yet? (2025), https://algassert.com/post/2500
29. Goldreich, O., Goldwasser, S., Halevi, S.: Collision-free hashing from lattice problems. In: Goldreich, O. (ed.) Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation. Lecture Notes

in Computer Science, vol. 6650, pp. 30–39. Springer, Berlin, Heidelberg (2011), https://doi.org/10.1007/978-3-642-22670-0_5
30. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: STOC 1996: Symposium on Theory of Computing. pp. 212–219. Association for Computing Machinery, New York (1996), https://doi.org/10.1145/237814.237866
31. Gutmann, P., Neuhaus, S.: Replication of quantum factorisation records with an 8-bit home computer, an abacus, and a dog (2025), https://eprint.iacr.org/2025/1237
32. Hu, J., Morioka, Y., Wang, G.: Post-quantum traditional (PQ/T) hybrid PKI authentication in the Internet key exchange version 2 (IKEv2) (2026), https://datatracker.ietf.org/doc/draft-hu-ipsecme-pqt-hybrid-auth
33. Jao, D., Azarderakhsh, R., Campagna, M., Costello, C., De Feo, L., Hess, B., Hutchinson, A., Jalali, A., Karabina, K., Koziel, B., LaMacchia, B., Longa, P., Naehrig, M., Pereira, G., Renes, J., Soukharev, V., Urbanik, D.: SIKE – Supersingular isogeny key encapsulation, https://sike.org
34. Jao, D., De Feo, L.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: Yang, B.Y. (ed.) Lecture Notes in Computer Science. Post-Quantum Cryptography. PQCrypto 2011, vol. 7071, pp. 19–34. Springer, Berlin, Heidelberg (2011), https://doi.org/10.1007/978-3-642-25405-5_2
35. Kampanakis, P., Stebila, D., Hansen, T.: PQ/T hybrid key exchange with ML-KEM in SSH (2026), https://datatracker.ietf.org/doc/draft-ietf-sshm-mlkem-hybrid-kex
36. Koshelev, D.: Generation of "independent" points on elliptic curves by means of Mordell–Weil lattices. Mathematical Cryptology **4**(1), 11–22 (2024), https://journals.flvc.org/mathcryptology/article/view/132727
37. Koshelev, D.: Application of Mordell–Weil lattices with large kissing numbers to acceleration of multiscalar multiplication on elliptic curves. Journal of Mathematical Cryptology **19**(1, Special Issue based on CIFRIS24), article 20240034 (2025), https://doi.org/10.1515/jmc-2024-0034
38. Koshelev, D.: Batch point compression in the context of advanced pairing-based protocols. Applicable Algebra in Engineering, Communication and Computing **36**(4), 611–629 (2025), https://doi.org/10.1007/s00200-023-00625-3
39. Koshelev, D.: Generation of two "independent" points on an elliptic curve of j-invariant $\neq 0, 1728$. In: Bruin, N., Kohel, D., Martindale, C. (eds.) Arithmetic, Geometry, Cryptography and Coding Theory (AGCCT-19). Contemporary Mathematics, vol. 832, pp. 145–156. American Mathematical Society, Providence (2026), https://doi.org/10.1090/conm/832/16610
40. Koshelev, D.: Simultaneously simple universal and indifferentiable hashing to elliptic curves. In: Nitaj, A., Petkova-Nikova, S., Rijmen, V. (eds.) Progress in Cryptology – AFRICACRYPT 2025. Lecture Notes in Computer Science, vol. 15651, pp. 395–413. Springer, Cham (2026), https://doi.org/10.1007/978-3-031-97260-7_18
41. Koshelev, D., Sebé, F.: SageMath code (2026), https://github.com/Dimitri-Koshelev/Hybrid-hash-function-based-on-the-DLP-and-SIS-problems
42. Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography **75**(3), 565–599 (2015), https://doi.org/10.1007/s10623-014-9938-4
43. Lyubashevsky, V., Micciancio, D.: Generalized compact knapsacks are collision resistant. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) Automata, Languages and Programming. ICALP 2006. Lecture Notes in Computer Science,

vol. 4052, pp. 144–155. Springer, Berlin, Heidelberg (2006), https://doi.org/10.1007/11787006_13

44. Maino, L., Martindale, C., Panny, L., Pope, G., Wesolowski, B.: A direct key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023. Lecture Notes in Computer Science, vol. 14008, pp. 448–471. Springer, Cham (2023), https://doi.org/10.1007/978-3-031-30589-4_16
45. Maitin-Shepard, J., Tibouchi, M., Aranha, D.F.: Elliptic curve multiset hash. The Computer Journal. Section D: Security in Computer Systems and Networks **60**(4), 476–490 (2017), https://doi.org/10.1093/comjnl/bxw053
46. Micciancio, D.: Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. Computational Complexity **16**(4), 365–411 (2007), https://doi.org/10.1007/s00037-007-0234-9
47. Miller, V., Koblitz, N., Boneh, D., Lauter, K., Galbraith, S., Lange, T.: Workshop on elliptic curve cryptography. ECC 2025, https://eccworkshop.org/2025
48. Mittelbach, A., Fischlin, M.: The theory of hash functions and random oracles. An approach to modern cryptography. Information Security and Cryptography, Springer, Cham (2021), https://doi.org/10.1007/978-3-030-63287-8
49. Ounsworth, M., Gray, J., Pala, M., Klaußner, J., Fluhrer, S.: Composite module-lattice-based digital signature algorithm (ML-DSA) for use in X.509 public key infrastructure (2026), https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs
50. Pedersen, T.P.: Non-interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum, J. (ed.) Advances in Cryptology – CRYPTO 1991. Lecture Notes in Computer Science, vol. 576, pp. 129–140. Springer, Berlin, Heidelberg (1992), https://doi.org/10.1007/3-540-46766-1_9
51. Peikert, C.: Public-key cryptosystems from the worst-case shortest vector problem. In: STOC 2009: Symposium on Theory of Computing. pp. 333–342. Association for Computing Machinery, New York (2009), https://doi.org/10.1145/1536414.1536461
52. Peikert, C., Rosen, A.: Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In: Halevi, S., Rabin, T. (eds.) Theory of Cryptography. TCC 2006. Lecture Notes in Computer Science, vol. 3876, pp. 145–166. Springer, Berlin, Heidelberg (2006), https://doi.org/10.1007/11681878_8
53. Prabel, L., Wang, G., Janneck, J., Reddy K, T., Mattsson, J.P.: Hybrid digital signatures with strong unforgeability (2026), https://datatracker.ietf.org/doc/draft-prabel-cfrg-suf-hybrid-sigs
54. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM **56**(6), article 34 (2009), https://doi.org/10.1145/1568318.1568324
55. Regev, O.: An efficient quantum factoring algorithm. Journal of the ACM **72**(1), article 10 (2025), https://doi.org/10.1145/3708471
56. Robert, D.: Breaking SIDH in polynomial time. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023. Lecture Notes in Computer Science, vol. 14008, pp. 472–503. Springer, Cham (2023), https://doi.org/10.1007/978-3-031-30589-4_17
57. Shekh-Yusef, R., Reddy K, T., Tschofenig, H., Ounsworth, M., Rosomakho, Y.: Post-quantum traditional (PQ/T) hybrid authentication with dual certificates in TLS 1.3 (2026), https://datatracker.ietf.org/doc/draft-yusef-tls-pqt-dual-certs

58. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review **41**(2), 303–332 (1999), https://doi.org/10.1137/S0036144598347011
59. Stebila, D., Fluhrer, S., Gueron, S.: Hybrid key exchange in TLS 1.3 (2025), https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design
60. Tjhai, C., Tomlinson, M., Bartlett, G., Fluhrer, S., Van Geest, D., Garcia-Morchon, O., Smyslov, V.: Multiple key exchanges in the Internet key exchange protocol version 2 (IKEv2) (RFC 9370) (2023), https://datatracker.ietf.org/doc/rfc9370
61. Wang, G., Wang, H.: HMAC based hybrid key combiners for multiple keys (2026), https://datatracker.ietf.org/doc/draft-wang-cfrg-key-combiners