Elliptic Curve Cryptography 2.0

Gaurish Korpal

Theory

Introduction: ECC 1.0

Identity-based encryption

Pairing-based cryptography: ECC 2.0

Applications

Group signatures

Homomorphic encryption

Secure multiparty computation

Post-quantum cryptography

Lattice-based cryptography

Supersingular Isogeny Graphs: ECC 3.0

References

Elliptic Curve Cryptography 2.0

Gaurish Korpal

The University of Arizona, Tucson

February 22, 2021

Theory
Introduction: ECC 1.0
Identity-based encryption
Pairing-based cryptography: ECC 2.0
Applications
Group signatures
Homomorphic encryption
Secure multiparty computation
Post-quantum cryptography
Lattice-based cryptography
Supersingular Isogeny Graphs: ECC 3.0
References

Outline

1. Theory
   - Introduction: ECC 1.0
   - Identity-based encryption
   - Pairing-based cryptography: ECC 2.0
2. Applications
   - Group signatures
   - Homomorphic encryption
   - Secure multiparty computation
3. Post-quantum cryptography
   - Lattice-based cryptography
   - Supersingular Isogeny Graphs: ECC 3.0
4. References

Theory
Introduction: ECC 1.0
Identity-based encryption
Pairing-based cryptography: ECC 2.0
Applications
Group signatures
Homomorphic encryption
Secure multiparty computation
Post-quantum cryptography
Lattice-based cryptography
Supersingular Isogeny Graphs: ECC 3.0
References

Theory

Introduction: ECC 1.0

The use of elliptic curves in cryptography was suggested independently by Neal Koblitz [Kob87] and Victor S. Miller [Mil86] in 1985.

We begin with an elliptic curve E given by equation $\boxed{y^2 = x^3 + ax + b}$ over a finite field $\mathbb{F}_q$ such that $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$.

Let $E(\mathbb{F}_q)$ denote the set of $\mathbb{F}_q$-rational points satisfying the equation of E and the special point $\mathcal{O}$ lying at infinity. Then, $(E(\mathbb{F}_q), +)$ forms an abelian group with $\mathcal{O}$ as the identity element.

The traditional elliptic curve cryptosystems are constructed on the group of $E(\mathbb{F}_q)$ with the security depending on the difficulty of computing the discrete logarithm problem of $E(\mathbb{F}_q)$:

Elliptic curve discrete logarithm problem

Compute $x \in \mathbb{N}$, given P and Q, where $P \in E(\mathbb{F}_q)$ and $Q = xP = \underbrace{P + \cdots + P}_{x \text{ times}}$

Introduction: ECC 1.0 (contd.)

We can also design an elliptic curve cryptosystem scheme in a manner similar to that of a scheme based on the multiplicative discrete logarithm problem.

The advantage of elliptic curve based cryptosystems over other public-key cryptosystems is their short key size, high processing throughput, and low bandwidth. For example, the typical key size of ECC that guarantees the security comparable to that of 1024 bit key size with the RSA cryptosystems is considered to be just 160 bits [Oka06].

The reason why elliptic curve cryptosystems have such short key lengths is that the index calculus technique is considered to be ineffective for computing the discrete logarithm of the elliptic curve group over finite fields, while it can effectively compute integer factoring and discrete logarithm of the multiplicative group of a finite field [Fre01].

Identity-based encryption

Elliptic Curve Cryptography 2.0

Gaurish Korpal

Theory

Introduction: ECC 1.0

Identity-based encryption

Pairing-based cryptography: ECC 2.0

Applications

Group signatures

Homomorphic encryption

Secure multiparty computation

Post-quantum cryptography

Lattice-based cryptography

Supersingular Isogeny Graphs: ECC 3.0

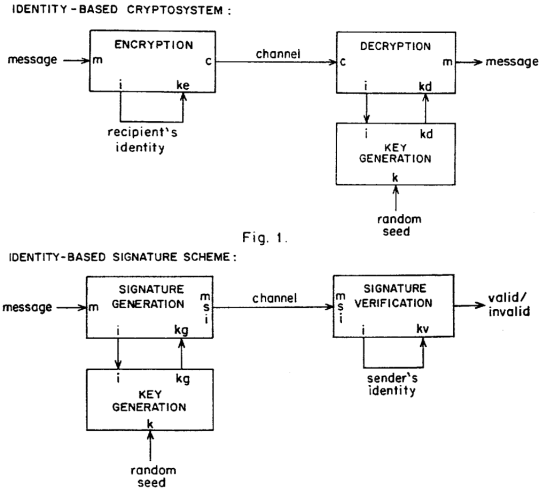
References

In 1984, A. Shamir proposed a variant of public-key encryption (PKE), called identity-based encryption (IBE), in which the identity of a user is employed in place of the user's public-key [Sha85].

Assumptions

There exist trusted key generation centers, whose sole purpose is to give each user a personalized smart card when they first join the network. The smart card contains a microprocessor, an I/O port, a RAM, a ROM with secret key, and programs for message encryption/decryption and signature generation/verification, such that the information embedded in this card for perfoming these tasks is totally independent of the identity of the other party. Previously issued cards and user database do not have to be updated when new users join the network and the centers can be closed after all the cards are issued.

Identity-based encryption (contd.)



When Bob wants to send a message to Alice, he signs it with the secret key in his smart card, encrypts the result by using Alice's name and network address, adds his own name and network address to the message and sends it to Alice. When Alice receives the message, she decrypts it using the secret key in her smart card, and then verifies the signature using the sender's name and network address as a verification key.

Identity-based encryption (contd.)

Note that, $ke = i$ since encryption key is the user's identity i and $kd = f(i, k)$ since decription key is derived from the user's idntity i and a random seed k. Therefore, the overall security of this cryptosystem depends on the following points:

1. The security of the underlying cryptographic functions
2. The secrecy of the priveleged information stored at the key generation centers.
3. The thoroughness of the identity checks performed by the centers before issuing cards.
4. The precautions taken by users to prevent the loss, duplication, or unautherised use of their card.

Hence, to implement such a cryptosystem, we need PKE to have two additional properties (RSA couldn't satisfy these simultaneously):

1. When the seed k is known, secret keys can be easily computed for a non-negligiable fractions of the possible public keys.
2. The problem of computing the seed k from specific public/secret key pairs generated with k is intractable.

Pairing-based cryptography: ECC 2.0

Let $E/\mathbb{F}_q$ be an elliptic curve and $m \geq 2$ be an integer prime to $p = \mathrm{char}(\mathbb{F}_q)$.

m-torsion subgroup of E

It is the set of points of E of order m, denoted by $E(\mathbb{F}_q)[m]$. That is,

$$E(\mathbb{F}_q)[m] = \{P \in E(\mathbb{F}_q) : mP = \mathcal{O}\}$$

embedding degree of E [HPS14, §6.9.1]

The embedding degree of E with respect to m is the smallest value of k such that

$$E(\mathbb{F}_{q^k})[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

In fact, we have $E[m] = E(\overline{\mathbb{F}}_q)[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ [Sil09, Corollary III.6.4]. This allows us to define Weil pairing

$$e_m : E[m] \times E[m] \to \mu_m$$

Pairing-based cryptography: ECC 2.0 (contd.)

where μ_m is the group of m^{th} roots of unity in $\overline{\mathbb{F}}_q^*$, i.e. $e_m(P, Q)^m = 1$ for all $P, Q \in E[m]$, with the following properties:

1. Bilinear: for any $P, Q, P_1, P_2, Q_1, Q_2 \in E[m]$ we have
$$e_m(P_1 + P_2, Q) = e_m(P_1, Q)e_m(P_2, Q)$$
$$e_m(P, Q_1 + Q_2) = e_m(P, Q_1)e_m(P, Q_2)$$
2. Alternating: for any $P, Q \in E[m]$, $e_m(P, Q) = e_m(Q, P)^{-1}$ since $e_m(P, P) = 1$ for any $P \in E[m]$.
3. Non-degenerate: If $e_m(P, Q) = 1$ for all $P \in E[m]$ then $Q = \mathcal{O}$.

There are many other instances of pairings on ellitpic curves, for example Tate pairing [Gal05].

Historically, Weil pairing [MOV93] and Tate pairing [FMR99] were used to attack elliptic curve cryptosystems by reducing the discrete logarithm (DL) problem on certain (supersingular) elliptic curves to the DL in the multiplicative group of an extension of the underlying finite field

Pairing-based cryptography: ECC 2.0 (contd.)

The Weil pairing is alternating, that is, $e_m(P, P) = 1$ for all P. In cryptographic applications we generally want to evaluate the pairing at points $P_1 = aP$ and $P_2 = bP$, but using the Weil pairing directly is not helpful, since

$$e_m(P_1, P_2) = e_m(aP, bP) = e_m(P, P)^{ab} = 1^{ab} = 1$$

One way around this dilemma is to choose a nice elliptic curve (supersingualr curve) that has (efficiently computable) isogeny $\phi : E \to E$, called distortion map, with the property that $E[m]$ has a basis of the form $\{P, \phi(P)\}$ [Sil09, §IX.7]. For more detials, see [HPS14, §6.9].

modified Weil pairing

Let $P \in E[m]$ and ϕ be a distortion map for P, then the modified Weil pairing $\hat{e}_m$ on $E[m]$ is defined by

$$\hat{e}_m(P, Q) = e_m(P, \phi(Q))$$

Pairing-based cryptography: ECC 2.0 (contd.)

Note that $\hat{e}_m(P, P) \neq 1$ and $\hat{e}_m(P, Q) = \hat{e}_m(Q, P)$ [Oka06, §4]. In

2000, A. Joux [Jou00] showed that this modified Weil (and Tate) pairing can be used for a protocol for three party one round Diffie-Hellman key exchange, and Sakai et al. [SOK00] used it for key exchange. Then in 2001, E. Verheul [Ver01] used it to construct an ElGamal encryption scheme where each public key has two corresponding private keys. Finally, D. Boneh and M. Franklin [BF01] used the modified Weil pairing of a specific supersingular elliptic curve to propose the first ever identity-based encryption system.

The pairing-based cryptography is possible because [KM05, §2]:

1. there exits a prime $\ell \neq p$ such that Diffie-Hellman problem is intractable in $E[\ell]$.
2. the Weil pairing $e_\ell(P, \phi(Q))$ can be efficietly computed using Miller's algorithm [Sil09, §XI.8].

Pairing-based cryptography: ECC 2.0 (contd.)

a basic version of the Boneh-Franklin scheme [KM05]

Bob wants to send Alice a message $\mathfrak{m}$, which we suppose is an element of $\mathbb{F}_{q^k}$ where k is the embedding degree of E, and he wants to do this using nothing other than her identity, which we suppose is hashed and then embedded in some way as a point $I_A \in E(\mathbb{F}_q)[\ell]$. In addition to the field $\mathbb{F}_q$ and the curve E, the system-wide parameters include a basepoint $P \in E(\mathbb{F}_{q^k})[\ell]$ and another point $K \in \langle P \rangle$ that is the public key of the Trusted Authority (TA). The TA's secret key is the integer s that it used to generate the key $K = sP$.

To send the message m, Bob first chooses a random r and computes the point rP and the Weil pairing $\hat{e}_\ell(K, I_A)^r = \hat{e}_\ell(rK, I_A) \in \mathbb{F}^*_{q^k}$. He sends Alice both the point rP and the field element $u = \mathfrak{m} + \hat{e}_\ell(rK, I_A)$. In order to decrypt the message, Alice must get the decryption key D_A from the TA; this is the point $D_A = sI_A \in E(\mathbb{F}_q)$ that the TA computes using the secret key s. Finally, Alice can now decrypt by subtracting $\hat{e}_\ell(rP, D_A)$ from u, since by billinearlity we have $\hat{e}_\ell(rP, D_A) = \hat{e}_\ell(rK, I_A)$.

Theory
Introduction: ECC 1.0
Identity-based encryption
Pairing-based cryptography: ECC 2.0
Applications
Group signatures
Homomorphic encryption
Secure multiparty computation
Post-quantum cryptography
Lattice-based cryptography
Supersingular Isogeny Graphs: ECC 3.0
References

Applications

Group signatures

In 1991, D. Chaum and E. van Heyst [CH91] introduced a new type of signature for a group of people, called group signature, which has the following properties:

1. only the group members can sign the messages
2. the receiver can verify that it is a valid group signature, but cannot discover which group member signed it.
3. if necessary, the signature can be "opened", so that the person who signed the message is revealed.

Therefore, group signatures were introduced as a generalization of credential mechanisms and memebership schemes in which a group memeber can convince the verifier that they belong to a certain group, without revealing their identity.

Moreover, they introduced four schemes that satisfy these properties, based on different cryptographic assumptions like:

1. For each person it is unfeasible to compute RSA roots.

Group signatures (contd.)

2. For each person it is unfeasible to compute the discrete logarithm modulo a large prime number.

Scheme number	Based on assumption	$\mathcal{Z}$ needed to open a signature	Group fixed in advance	Type of signature	Length of the group's public key	Number of computations during conf. pr.	Number of bits transmitted during conf. pr.
1	Any	Yes	Yes	Any type	Linear	Independent	Independent
2	1	No	Yes	Undeniable	Linear	Linear	Independent
3	1	No	No	Undeniable	Linear	Linear	Independent
4	2	No	No	Undeniable	Linear	Linear	Linear

Figure: Here $\mathcal{Z}$ denotes the Trusted Authority, conf. pr. = confirmation protocol, and "independent/linear" means that the number is independent/linear in the number of group members. In the last three schemes, the signatures made by the group members are undeniable signatures, but it is possible to make digital signatures.

In 2004, using pairing-based cryptography, new group schemes were proposed based on the Strong Diffie-Hellman [BBS04] and a discrete-logarithm-based assumption called LRSW [CL04]. Both of these are a shorter alternative to the RSA group signature schemes based on strong RSA assumption. Later, in 2006, these group schemes were modified to be provably secure without random oracles [ACH05] [BW06], just like the ones based on strong RSA assumption.

Homomorphic encryption

In 1978, R. L. Rivest, L. Aldeman, and M. L. Dertouzos [RAD78] gave four simple examples to illustrate the existance of special encryption functions called "privacy homomorphisms" which would permit encryped data to be operated on without preliminary decryption of the operands.

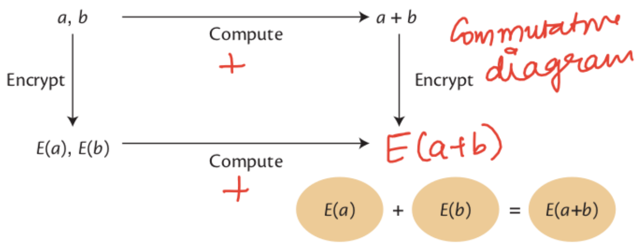


Figure: Homomorphic encryption lets the owner exchange the order of operations withou changing the result; that is, one can encrypt then compute, or compute then encrypt.

Homomorphic encryption (contd.)

In 2009, Craig Gentry proposed the first plausible construction for a fully homomorphic encryption (FHE) scheme using lattice-based cryptography. Before that many partial results were published. Among them, the first ever "doubly homomorphic" encryption scheme was Boneh-Goh-Nissim cryptosystem, proposed in 2005 [BGN05]. It is based on pairing-based cryptography and supports unlimited number of addition operations but at most one multiplication. However, Gentry's scheme supports unlimited number of both addition and multiplication operations on ciphertexts, making it possible to perform computations on data while it is encrypted.

The current homomorphic encryption solutions are based on the learning with errors (LWE) problem or the ring version (RLWE), proposed between 2005 and 2010 [Lau17]. A list of open-source FHE libraries implementing second-generation and/or third-generation FHE schemes is maintained by the Homomorphic Encryption Standardization consortium to advance secure computation.

Secure multiparty computation

In 1982, A. C. Yao [Yao82] proposed the following problem:

Millionires' problem

Two millionaires wish to know who is richer; however, they do not want to find out inadvertently any additional information about each other's wealth. How can they carry out such a conversation?

Many solutions have been introduced for the problem. This was the beginning example of secure multiparty computation.

The aim of secure multiparty computation (MPC) is to enable parties to carry out such distributed computing tasks in a secure manner. Following are the two special cases of MPC:

1. Private set intersection (PSI): It's about the secure computation of the intersection of private sets. That is, it allows two parties holding sets to compare encrypted versions of these sets in order to compute the intersection.

Secure multiparty computation (contd.)

2. Threshold cryptography: It's about the secure computation of digital signatures and decryption, where no single party holds the key. That is, in order to decrypt an encrypted message or to sign a message, several parties (more than some threshold number) must cooperate in the decryption or signature protocol.

Theoretically, secure multiparty protocol exist for any distributed computing task [Lin21]. However, there are major differences between the practical protocols proposed for two party computation (2PC) and multiparty computation (MPC).

- We can use the garbled circuit protocol for 2PC. In 2017, S. Garg and A. Srinivasan provide constructions for garbling arbitrary protocols based on pairing-based cryptography [GS17].
- Most MPC protocols, as opposed to 2PC protocols, make use of secret sharing schemes like Shamir secret sharing.

Theory
Introduction: ECC 1.0
Identity-based encryption
Pairing-based cryptography: ECC 2.0
Applications
Group signatures
Homomorphic encryption
Secure multiparty computation
Post-quantum cryptography
Lattice-based cryptography
Supersingular Isogeny Graphs: ECC 3.0
References

Post-quantum cryptography

Lattice-based cryptography

Theory
Introduction: ECC 1.0
Identity-based encryption
Pairing-based cryptography: ECC 2.0
Applications
Group signatures
Homomorphic encryption
Secure multiparty computation
Post-quantum cryptography
Lattice-based cryptography
Supersingular Isogeny Graphs: ECC 3.0
References

So far, lattice-based solutions are not known to be vulnerable to polynomial-time quantum attacks; however, depending on the underlying security assumption, quantum attacks on lattice-based systems might be possible.

Efficient lattice-based systems built on number-theoretic constructions, such as number rings, have been shown to be provably secure in the sense adopted by the cryptographic community.

For details, see [HPS14, Chapter 7] and [MR09].

Supersingular Isogeny Graphs: ECC 3.0

A supersingular isogeny graph is specified by a large prime number p, of cryptographic size-that is, at least 256 bits-satisfying some conditions, and a small prime ℓ. The nodes of the graph are the isomorphism classes of supersingular elliptic curves modulo p, and the edges are the isogenies of degree ℓ. The number of nodes is approximately $p/12$ (the Eichler class number), and the graph is $(\ell + 1)$ regular. Isogenies of low degree can be efficiently computed using Velu's formulae.

For details, see [CGL09] and [Feo17].

Elliptic Curve Cryptography 2.0
Gaurish Korpal
Theory
Introduction: ECC 1.0
Identity-based encryption
Pairing-based cryptography: ECC 2.0
Applications
Group signatures
Homomorphic encryption
Secure multiparty computation
Post-quantum cryptography
Lattice-based cryptography
Supersingular Isogeny Graphs: ECC 3.0
References

References

References

[RAD78] Rivest R., Adleman L., Dertouzos M. (1978) On data banks and privacy homomorphisms. Foundations of Secure Computation. Academic Press, Inc. https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.452.8956

[Yao82] Yao A. (1982) Protocols for secure computations. In: IEEE 54th Annual Symposium on Foundations of Computer Science. https://doi.org/10.1109/SFCS.1982.88

[Sha85] Shamir A. (1985) Identity-Based Cryptosystems and Signature Schemes. In: Blakley G.R., Chaum D. (eds) Advances in Cryptology. CRYPTO 1984. Lecture Notes in Computer Science, vol 196. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-39568-7_5

[Mil86] Miller V.S. (1986) Use of Elliptic Curves in Cryptography. In: Williams H.C. (eds) Advances in Cryptology — CRYPTO '85 Proceedings. CRYPTO 1985. Lecture Notes in Computer Science, vol 218. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-39799-X_31

[Kob87] Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of Computation, vol 48. https://doi.org/10.2307/2007884

[CH91] Chaum D., van Heyst E. (1991) Group Signatures. In: Davies D.W. (eds) Advances in Cryptology — EUROCRYPT '91. EUROCRYPT 1991. Lecture Notes in Computer Science, vol 547. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-46416-6_22

[MOV93] Menezes A. J., Okamoto T., Vanstone S. A. (1993) Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transactions on Information Theory, vol 39, no 5. https://doi.org/10.1109/18.259647

[FMR99] Frey G., Muller M., Rück H. (1999) The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. IEEE Transactions on Information Theory, vol 45, no. 5. https://doi.org/10.1109/18.771254

[Jou00] Joux A. (2000) A One Round Protocol for Tripartite Diffie–Hellman. In: Bosma W. (eds) Algorithmic Number Theory. ANTS 2000. Lecture Notes in Computer Science, vol 1838. Springer, Berlin, Heidelberg. https://doi.org/10.1007/10722028_23

[SOK00] Sakai R., Ohgishi K., Kasahara M. Cryptosystems Based on Pairings. Proceedings of Symposium on Cryptography and Information Security, Japan (SCIS '00).

[Ver01] Verheul E.R. (2001) Evidence that XTR Is More Secure than Supersingular Elliptic Curve Cryptosystems. In: Pfitzmann B. (eds) Advances in Cryptology — EUROCRYPT 2001. EUROCRYPT 2001. Lecture Notes in Computer Science, vol 2045. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44987-6_13

References (contd.)

[BF01] Boneh D., Franklin M. (2001) Identity-Based Encryption from the Weil Pairing. In: Kilian J. (eds) Advances in Cryptology — CRYPTO 2001. CRYPTO 2001. Lecture Notes in Computer Science, vol 2139. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44647-8_13

[Fre01] Frey G. (2001) Applications of Arithmetical Geometry to Cryptographic Constructions. In: Jungnickel D., Niederreiter H. (eds) Finite Fields and Applications. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-56755-1_13

[BBS04] Boneh D., Boyen X., Shacham H. (2004) Short Group Signatures. In: Franklin M. (eds) Advances in Cryptology – CRYPTO 2004. CRYPTO 2004. Lecture Notes in Computer Science, vol 3152. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-28628-8_3

[CL04] Camenisch J., Lysyanskaya A. (2004) Signature Schemes and Anonymous Credentials from Bilinear Maps. In: Franklin M. (eds) Advances in Cryptology – CRYPTO 2004. CRYPTO 2004. Lecture Notes in Computer Science, vol 3152. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-28628-8_4

[Gal05] Galbraith (2005) Pairings. In: Blake I.F., Seroussi G., Smart N.P. (eds.) Advances in Elliptic Curve Cryptography, vol 2, Cambridge University Press, Cambridge. https://doi.org/10.1017/CBO9780511546570

[Pet05] Peterson K.G. (2005) Cryptography from Pairings. In: Blake I.F., Seroussi G., Smart N.P. (eds.) Advances in Elliptic Curve Cryptography, vol 2, Cambridge University Press, Cambridge. https://doi.org/10.1017/CBO9780511546570

[KM05] Koblitz N., Menezes A. (2005) Pairing-Based Cryptography at High Security Levels. In: Smart N.P. (eds) Cryptography and Coding. Cryptography and Coding 2005. Lecture Notes in Computer Science, vol 3796. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11586821_2

[BGN05] Boneh D., Goh EJ., Nissim K. (2005) Evaluating 2-DNF Formulas on Ciphertexts. In: Kilian J. (eds) Theory of Cryptography. TCC 2005. Lecture Notes in Computer Science, vol 3378. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-30576-7_18

[ACH05] Ateniese G., Camenisch J., Hohenberger S., de Medeiros B. (2005) Practical Group Signatures without Random Oracles. Cryptology ePrint Archive, Report 2005/385. https://eprint.iacr.org/2005/385

[BW06] Boyen X., Waters B. (2006) Compact Group Signatures Without Random Oracles. In: Vaudenay S. (eds) Advances in Cryptology - EUROCRYPT 2006. EUROCRYPT 2006. Lecture Notes in Computer Science, vol 4004. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11761679_26

References (contd.)

[Oka06] Okamoto T. (2006) Cryptography Based on Bilinear Maps. In: Fossorier M.P.C., Imai H., Lin S., Poli A. (eds) Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. AAECC 2006. Lecture Notes in Computer Science, vol 3857. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11617983_3

[Bon07] Boneh D. (2007) A Brief Look at Pairings Based Cryptography. In: 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07). IEEE, Providence, Rhode Island. https://doi.org/10.1109/FOCS.2007.51

[MR09] Micciancio D., Regev O. (2009) Lattice-based Cryptography. In: Bernstein D.J., Buchmann J., Dahmen E. (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-88702-7_5

[CGL09] Charles D.X., Lauter K.E., Goren E.Z. (2009) Cryptographic Hash Functions from Expander Graphs. Journal of Cryptology vol 22. https://doi.org/10.1007/s00145-007-9002-x

[Sil09] Silverman J.H. (2009) The Arithmetic of Elliptic Curves. 2nd edition (corrected 2012 printing). Graduate Texts in Mathematics, vol 106. Springer-Verlag, New York. https://doi.org/10.1007/978-0-387-09494-6

[HPS14] Hoffstein J., Pipher J., Silverman J.H. (2014) An Introduction to Mathematical Cryptography. Undergraduate Texts in Mathematics. Springer-Verlag New York. https://doi.org/10.1007/978-1-4939-1711-2

[GS17] Garg S., Srinivasan A. (2017) Garbled Protocols and Two-Round MPC from Bilinear Maps. In: IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS), Berkeley. https://doi.org/10.1109/FOCS.2017.60

[Feo17] Feo L.D. (2017) Mathematics of Isogeny Based Cryptography. arXiv:1711.04062. https://arxiv.org/abs/1711.04062

[Lau17] Lauter K. (2017) Postquantum Opportunities: Lattices, Homomorphic Encryption, and Supersingular Isogeny Graphs. IEEE Security & Privacy, vol 15, no 04. https://doi.org/10.1109/MSP.2017.3151338

[Lin21] Lindell T. (2021) Secure multiparty computation. Communications of the ACM vol 64, no 01. https://doi.org/10.1145/3387108