One-Round Authenticated Group Key Exchange from Isogenies

Atsushi Fujioka[1], Katsuyuki Takashima[2], and Kazuki Yoneyama[3(✉)]

[1] Kanagawa University, Yokohama, Japan
[2] Mitsubishi Electric, Kamakura, Japan
[3] Ibaraki University, Hitachi, Japan
kazuki.yoneyama.sec@vc.ibaraki.ac.jp

Abstract. This paper proposes two one-round authenticated group key exchange protocols from newly employed *cryptographic invariant maps* (CIMs): one is secure in the quantum random oracle model and the other resists against maximum exposure where a non-trivial combination of secret keys is revealed. The security of the former (resp. latter) is proved under the n-way decisional (resp. n-way gap) Diffie–Hellman assumption on the CIMs in the quantum random (resp. random) oracle model.

We instantiate the proposed protocols on the *hard homogeneous spaces* with limitation where the number of the user group is two. In particular, the protocols instantiated by using the *CSIDH, commutative supersingular isogeny Diffie–Hellman*, key exchange are currently more realistic than the general n-party CIM-based ones due to its realizability. Our two-party one-round protocols are secure against quantum adversaries.

Keywords: One-round authenticated group key exchange · Cryptographic invariant maps · Hard homogeneous spaces · Commutative supersingular isogeny Diffie–Hellman · G-CK model · G-CK$^+$ model · Quantum adversary

1 Introduction

1.1 Background

Recently, National Institute of Standards and Technology (NIST) has initiated a process to standardize quantum-resistant public-key cryptographic algorithms [17], so, to study quantum-resistant cryptosystems is a hot research area. A wide range of quantum-resistant primitives (i.e., mathematical foundations) have been scrutinized by experts on cryptography and mathematics over the world. They include lattice-based, code-based, and multivariate cryptography. We treat with one (relatively) newly entered quantum-resistant primitive, which is called isogeny-based cryptography.

Key establishing over insecure channels is one of important cryptographic techniques. Recent researches on this have led to *authenticated key exchange*

R. Steinfeld and T. H. Yuen (Eds.): ProvSec 2019, LNCS 11821, pp. 330–338, 2019.
https://doi.org/10.1007/978-3-030-31919-9_20

(AKE) and its multiparty extension, that is, *authenticated group key exchange* (AGKE). We then propose quantum-resistant AKE and AGKE schemes from isogenies on elliptic curves. In fact, we establish them on some abstract notions obtained from isogenies called *cryptographic invariant maps* (CIMs) and *hard homogeneous spaces* (HHSs).

HHS, CIM and CSIDH Key Exchange. In an unpublished but seminal paper [3], Couveignes initiated the research of isogeny-based cryptography where he formulated the basic notion of HHSs which is an abstract form of isogeny graphs and class groups of endomorphism rings of (ordinary) elliptic curves.

Independently, Rostovtsev and Stolbunov [18] proposed a Diffie–Hellman type key exchange from ordinary elliptic curve isogenies, which is now called RS key exchange and intensively studied very recently in [4]. While the RS key exchange uses ordinary curves, De Feo et al. employed supersingular isogenies for a practical key exchange protocol called supersingular isogeny Diffie–Hellman (SIDH) key exchange since ordinary isogeny problems suffer from subexponential quantum attacks. Jao et al. submitted an isogeny-based encryption scheme called SIKE (supersingular isogeny key encapsulation) to the NIST post-quantum cryptography competition, and the scheme is an enhanced form of the SIDH key exchange.

Castryck et al. [2] put forward a new HHS-based cryptographic construction called CSIDH (commutative SIDH) key exchange, which is constructed from a group action on the set of *supersingular elliptic curves defined over a prime field*. This ingenious key exchange opened a new research avenue in isogeny cryptography. As another new proposal, Boneh et al. [1] initiated to study a candidate multiparty non-interactive key exchange on CIMs, whose underlying structure is given by a HHS, (X, G), where X is a finite set and G is a finite abelian group, and the invariant map is defined on the n-th product X^n equipped with nice homomorphic (or equivariant) properties. As in the traditional Diffie–Hellman and pairing primitives, we can consider n-way computational, decisional, and gap Diffie–Hellman problems and assumptions on CIMs.

The notions of HHS and CIM give very concise conceptualizations of the above wonderful recent developments. We propose a generic conversion method from these key exchanges to authenticated ones.

We omit definitions, proofs and discussions because of page limitation. See [6] in details.

1.2 Our Contributions

One-Round AGKE from CIM. We propose two one-round AGKE protocols on the CIMs. One is called n-UM (n-Unified Model) which satisfies the G-CK security. The security of n-UM is proved under the n-way DDH assumption in the *quantum* random oracle model. The other is called BC n-DH (biclique n-Diffie–Hellman) which satisfies the G-CK$^+$ security. The security of BC n-DH is proved under the n-way GDH assumption in the random oracle model. The

Table 1. Comparison of one-round AGKE protocols.

	#parties	Assumption	Model	Post-quantum	Proof
[10]	n	KEM, PRF	weak G-CK[a]	Based on ingredients	StdM
[16]	3	gap-BDH	G-eCK	No	ROM
[19]	3	DBDH	G-CK$^+$	No	StdM
[14]	n	MLMs	G-eCK	No	StdM
[12]	n	iO	G-CK	No	StdM
n-UM	n	n-DDH	G-CK	Yes	QROM
BC n-DH	n	n-GDH	G-CK$^+$	Yes	ROM

[a]The model does not capture weak perfect forward secrecy (wPFS).

BC n-DH protocol requires that the number of the user group is bounded by logarithm of the security parameter. Comparison with existing one-round AGKE protocols is shown in Table 1.

Instantiating One-Round Two-Party AKE from HHS. We instantiate the proposed protocols on the HHS with limitation where the number of the user group is two. In particular, the CSIDH-based protocols are currently more realistic than the general n-party CIM-based ones due to its realizability. Our two-party one-round protocols are secure against quantum adversaries.

Compared to the previous SIDH-based one-round (two-party) AKE protocols [5,7], the proposed protocols have several merits. While Galbraith et al. [8] proposed an active attack on the SIDH protocol by using the auxiliary points exchanged between users, the attack cannot be applied to our CSIDH-based ones since they include no auxiliary points. In [9], one attack scenario for the

Table 2. Comparison of isogeny-based AKE protocols.

	Assumption	Model	#rounds	Proof
SIDH TS2 [7]	SI-CDH	CK	1[a]	ROM
AKE-SIDH-SIKE [15]	SI-DDH	CK$^+$	2	ROM
LJA [13]	SI-DDH	qCK	2	QROM
$\text{AKE}_{\text{SIDH-2}}$ [20]	SI-DDH	CK$^+$	2	ROM
SIDH UM [5]	SI-DDH	CK	1	QROM
biclique SIDH [5]	di-SI-GDH	CK$^+$	1	ROM
HKSU [11]	IND-CPA PKE	modified CK	2	QROM
HHS-UM	2-DDH	CK	1	QROM
HHS-BC	2-GDH	CK$^+$	1	ROM

[a]Galbraith claims that the protocol is one-round however the description shows that it is two-round as the responder generates the response after receiving the first message [7].

gap Diffie–Hellman (GDH) problem on the SIDH protocol is given since the degrees of isogenies used are fixed by public parameters as $\ell_i^{e_i}$ for small primes ℓ_i, e.g., $\ell_1 = 2, \ell_2 = 3$. As the CSIDH protocol uses random multiples consisting of several primes ℓ_i $(i = 1, \ldots, n)$ for the degrees and they are not fixed by public parameters, the attack cannot be applied to the CSIDH setting. Thus, the GDH assumption on CSIDH has no effective attacks at present, and we have a strong confidence on the security of our CSIDH-based BC protocol, which is reduced from the CSIDH GDH assumption. Comparison with existing isogeny-based AKE protocols is shown in Table 2.

2 n-UM: G-CK Secure n-Party Authenticated Group Key Exchange

2.1 Protocol

Public Parameters. We set Π = nUM. Let λ be a security parameter. Let MapGen be a generation algorithm of a cryptographic invariant map, and $(X, S, G, e) \leftarrow_R \mathsf{MapGen}(1^\lambda)$ and $x \leftarrow_R X$ are chosen. Let $H : \{0,1\}^* \to \{0,1\}^\lambda$ be a hash function modeled as a quantum random oracle. Public parameters are (Π, X, S, G, e, x, H).

Static Secret and Public Keys. Party U_i chooses $t_i \in G$ as the SSK. Then, U_i computes $T_i = t_i * x$ as the SPK.

Key Exchange. W.l.o.g, we suppose a session executed by $\mathbf{U} = (U_1, \ldots, U_n) \subseteq \mathcal{U}$.

1. U_i chooses $r_i \leftarrow_R G$ as the ESK, and computes $R_i = r_i * x$ as the EPK. Then, U_i broadcasts $(\Pi, \mathsf{role}_{i'}, U_i, R_i)$ to $\mathbf{U} \setminus U_i$.
2. On receiving $(\Pi, \mathsf{role}_{j'}, U_j, R_j)$ for all $j \neq i$, U_i computes $Z_1 = e_{n-1}(T_1, \ldots, T_{i-1}, t_i * T_{i+1}, \ldots, T_n)$ and $Z_2 = e_{n-1}(R_1, \ldots, R_{i-1}, r_i * R_{i+1}, \ldots, R_n)$.[1] Then, U_i generates the session key $SK = H(\Pi, U_1, \ldots, U_n, R_1, \ldots, R_n, Z_1, Z_2)$, and completes the session (Fig. 1).

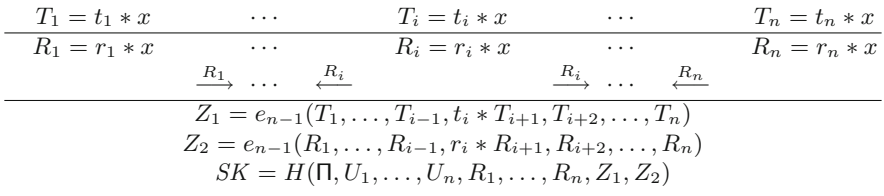

Fig. 1. Outline of n-UM protocol.

[1] T_i and R_i are indexed in the cyclic manner in modulo n. For example, when $i = n$, then $Z_1 = e_{n-1}(t_n * T_1, \ldots, T_n)$ and $Z_2 = e_{n-1}(r_n * R_1, \ldots, R_n)$.

2.2 Security

Theorem 2.1. *Suppose that H is modeled as a quantum random oracle and that the n-DDH assumption holds. Then the n-UM protocol is a post-quantum* G-CK*-secure n-party authenticated group key exchange protocol in the quantum random oracle model.*

In particular, for any quantum adversary $\mathcal{A}$ against the n-UM protocol that runs in time at most t, involves at most n_u honest parties and activates at most n_s sessions, and makes at most n_h queries to the quantum random oracle and n_q SessionReveal *queries, there exists a n-DDH quantum solver $\mathcal{S}$ such that*

$$\mathbf{Adv}^{n\text{-DDH}}_{\mathcal{S}}(\lambda) \geq \frac{2\mathbf{Adv}^{\text{g-ck}}_{\text{nUM},\mathcal{A}}(\lambda)^2}{n_u^2 n_s^2 (8n_h n_q + 3(n_h + n_q + 1)^4)},$$

where $\mathcal{S}$ runs in time t plus time to perform $\mathcal{O}\big((n_u + n_s)\lambda\big)$ group action operations.

3 Biclique n-DH : G-CK$^+$ Secure n-Party Authenticated Group Key Exchange

3.1 Protocol

Public Parameters. We set Π = BCnDH. Let λ be a security parameter. Let MapGen be a generation algorithm of a cryptographic invariant map, and $(X,\ S,\ G,\ e) \leftarrow_R \mathsf{MapGen}(1^\lambda)$ and $x \leftarrow_R X$ are chosen. Let $H : \{0,1\}^* \to \{0,1\}^\lambda$ be a hash function modeled as a random oracle. Public parameters are (Π, X, S, G, e, x, H).

Static Secret and Public Keys. Party U_i chooses $t_i \in G$ as the SSK. Then, U_i computes $T_i = t_i * x$ as the SPK.

Key Exchange. As in Sect. 2, we suppose a session executed by $\mathbf{U} = (U_1, \ldots, U_n) \subseteq \mathcal{U}$.

1. U_i chooses $r_i \leftarrow_R G$ as the ESK, and computes $R_i = r_i * x$ as the EPK. Then, U_i broadcasts $(\Pi, \mathsf{role}_{i'}, U_i, R_i)$ to $\mathbf{U} \setminus U_i$.
2. On receiving $(\Pi, \mathsf{role}_{j'}, U_j, R_1, \ldots, R_n)$, U_i computes $Z_\emptyset = e_{n-1}(T_1, \ldots, T_{i-1}, t_i * T_{i+1}, T_{i+2}, \ldots, T_n), \ldots, Z_I = e_{n-1}(R_1, \ldots, R_{i-1}, r_i * R_{i+1}, R_{i+2}, \ldots, R_n)$ as follows:[2] for all $P \in \mathcal{P}(I)$,
   - if $i \in P$, then $v_i = r_i$, and else if $i \notin P$, then $v_i = t_i$,
   - for all $k \in I$ $(k \neq i)$, if $k \in P$, then $V_k = R_k$, and else if $k \notin P$, then $V_k = T_k$, and
   - U_i computes Z_P as $Z_P = e_{n-1}(V_1, \ldots, V_{i-1}, v_i * V_{i+1}, V_{i+2}, \ldots, V_n)$.

   Then, U_i generates the session key $SK = H(\Pi,\ U_1, \ldots,\ U_n,\ R_1, \ldots,\ R_n,\ Z_\emptyset, \ldots,\ Z_I)$, and completes the session (Fig. 2).

[2] T_i and R_i are indexed in the cyclic manner in modulo n.

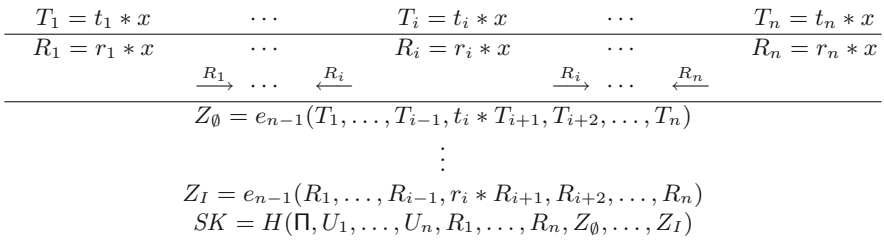

Fig. 2. Outline of biclique n-DH protocol.

It is worth to note here that we need to assume that the number of the user group is bounded by logarithm of the security parameter, λ.

Otherwise, we need exponential computations in λ as the number of the shared values is 2^n.

3.2 Security

Theorem 3.1. *Suppose that H is modeled as a random oracle and that the n-way GDH assumption holds for $\mathcal{S}$. Then the biclique n-DH protocol is a post-quantum* G-CK$^+$ *secure n-party authenticated group key exchange protocol in the random oracle model.*

In particular, for any AGKE quantum adversary $\mathcal{A}$ against the biclique n-DH protocol that runs in time at most t, involves at most n_u honest parties and activate at most n_s sessions, and makes at most n_h queries to the random oracle, there exists a n-way GDH quantum solver $\mathcal{S}$ such that

$$\mathbf{Adv}_{\mathcal{S}}^{n\text{-GDH}}(\lambda) \geq \min\left\{\frac{1}{n_u^n}, \frac{1}{n_u^{n-1} n_s}, \ldots, \frac{1}{n_u n_s^{n-1}}, \frac{1}{n_s^n}\right\} \cdot \mathbf{Adv}_{\text{BCnDH},\mathcal{A}}^{\text{g-ck+}}(\lambda),$$

where $\mathcal{S}$ runs in time t plus time to perform $\mathcal{O}\big((n_u + n_s)\lambda\big)$ group action operations and make $\mathcal{O}(n_h + n_s)$ queries to the n-DDH oracle.

4 Two-Party Authenticated Key Exchanges from Hard Homogeneous Spaces

4.1 G-CK Secure AKE Protocol (from HHS)

We give our HHS-based UM protocol. Public parameters are $pp = (X, G)$. We set Π = HHS-UM, that is, the protocol ID is "HHS-UM." The secret-key space for initiators and responders is given by the group G.

User U_1 has static public key, $T_1 = t_1 * x$, where $t_1 \leftarrow_R G$, and t_1 is U_1's static secret key. User U_2 has static public key, $T_2 = t_2 * x$, where $t_2 \leftarrow_R G$, and t_2 is U_2's static secret key. Here, ephemeral secret keys for U_1 and U_2 are given as $r_1 \leftarrow_R G$, and $r_2 \leftarrow_R G$, respectively. U_1 sends a ephemeral public key R_1

$T_1 = t_1 * x$		$T_2 = t_2 * x$
$R_1 = r_1 * x$	$\xrightarrow{R_1}$ $\xleftarrow{R_2}$	$R_2 = r_2 * x$
$Z_1 = t_1 * T_2$		$Z_1 = t_2 * T_1$
$Z_2 = r_1 * R_2$		$Z_2 = r_2 * R_1$
$SK = H(\Pi, U_1, U_2, R_1, R_2, Z_1, Z_2)$		

Fig. 3. Outline of HHS UM protocol.

$T_1 = t_1 * x$		$T_2 = t_2 * x$
$R_1 = r_1 * x$	$\xrightarrow{R_1}$ $\xleftarrow{R_2}$	$R_2 = r_2 * x$
$Z_1 = t_1 * T_2$		$Z_1 = t_2 * T_1$
$Z_2 = r_1 * T_2$		$Z_2 = t_2 * R_1$
$Z_3 = t_1 * R_2$		$Z_3 = r_2 * T_1$
$Z_4 = r_1 * R_2$		$Z_4 = r_2 * R_1$
$SK = H(\Pi, U_1, U_2, R_1, R_2, Z_1, Z_2, Z_3, Z_4)$		

Fig. 4. Outline of HHS biclique protocol.

as $R_1 = r_1 * x$ to U_2, U_2 sends back a ephemeral public key R_2 as $R_2 = r_2 * x$ to U_1.

U_1 computes $Z_1 = t_1 * T_2$, and $Z_2 = r_1 * R_2$, and then, obtains the session key SK as $SK = H(\Pi, U_1, U_2, R_1, R_2, Z_1, Z_2)$, where H is a hash function.

U_2 can computes the session key SK as $SK = H(\Pi, U_1, U_2, R_1, R_2, Z_1, Z_2)$ from $Z_1 = t_2 * T_1$, and $Z_2 = r_2 * R_1$ (Fig. 3).

It is clear that the session keys of both parties are equal.

The security of this scheme is given as a corollary of Theorem 2.1.

Corollary 4.1. *Suppose that H is modeled as a quantum random oracle and that the 2-DDH assumption holds on the HHS (X, G). Then the 2-UM protocol is a post-quantum* G-CK*-secure 2-party authenticated key exchange protocol in the quantum random oracle model.*

4.2 G-CK$^+$ Secure AKE Protocol (from HHS)

We give our HHS-based biclique protocol. Public parameters are $pp = (X, G)$. We set Π = HHS-BC, that is, the protocol ID is "HHS-BC." Static and ephemeral keys are the same as our HHS UM protocol. The secret-key space for initiators and responders is given by the group G.

User U_1 has static public key, $T_1 = t_1 * x$, where $t_1 \leftarrow_R G$, and t_1 is U_1's static secret key. User U_2, also, has static public key, $B = t_2 * x$, where $t_2 \leftarrow_R G$, and t_2 is U_2's static secret key. Here, ephemeral secret keys for U_1 and U_2 are given as $r_1 \leftarrow_R G$, and $r_2 \leftarrow_R G$, respectively. U_1 sends an ephemeral public key R_1 as $R_1 = r_1 * x$ to U_2, U_2 sends back an ephemeral public key R_2 as $R_2 = r_2 * x$ to U_1.

U_1 computes the non-trivial combinations of the ephemeral and static public keys as $Z_1 = t_1 * T_2$, $Z_2 = r_1 * T_2$, $Z_3 = t_1 * R_2$, and $Z_4 = r_1 * R_2$, and then, obtains the session key SK as $SK = H(\Pi, U_1, U_2, R_1, R_2, Z_1, Z_2, Z_3, Z_4)$, where H is a hash function.

U_2 can computes the session key SK as $SK = H(\Pi, U_1, U_2, R_1, R_2, Z_1, Z_2, Z_3, Z_4)$ from $Z_1 = t_2 * T_1$, $Z_2 = t_2 * R_1$, $Z_3 = r_2 * T_1$, and $Z_4 = r_2 * R_1$ (Fig. 4).

It is clear that the session keys of both parties are equal.

The security of this scheme is given as a corollary of Theorem 3.1.

Corollary 4.2. *Suppose that H is modeled as a random oracle and that the 2-way GDH assumption holds on the HHS (X, G). Then the biclique 2-DH protocol is a post-quantum* G-CK$^+$ *secure authenticated key exchange protocol in the random oracle model.*

References

1. Boneh, D., et al.: Multiparty non-interactive key exchange and more from isogenies on elliptic curves. In: MATHCRYPT 2018 (2018). https://eprint.iacr.org/2018/665
2. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: an efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018, Part III. LNCS, vol. 11274, pp. 395–427. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03332-3_15
3. Couveignes, J.M.: Hard homogeneous spaces. IACR Cryptology ePrint Archive 2006, 291 (2006). http://eprint.iacr.org/2006/291
4. De Feo, L., Kieffer, J., Smith, B.: Towards practical key exchange from ordinary isogeny graphs. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018, Part III. LNCS, vol. 11274, pp. 365–394. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03332-3_14
5. Fujioka, A., Takashima, K., Terada, S., Yoneyama, K.: Supersingular isogeny Diffie–Hellman authenticated key exchange. In: Lee, K. (ed.) ICISC 2018. LNCS, vol. 11396, pp. 177–195. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-12146-4_12
6. Fujioka, A., Takashima, K., Yoneyama, K.: One-round authenticated group key exchange from isogenies. IACR Cryptology ePrint Archive 2018, 1033 (2018). http://eprint.iacr.org/2018/1033
7. Galbraith, S.D.: Authenticated key exchange for SIDH. IACR Cryptology ePrint Archive 2018, 266 (2018). http://eprint.iacr.org/2018/266
8. Galbraith, S.D., Petit, C., Shani, B., Ti, Y.B.: On the security of supersingular isogeny cryptosystems. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part I. LNCS, vol. 10031, pp. 63–91. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53887-6_3
9. Galbraith, S.D., Vercauteren, F.: Computational problems in supersingular elliptic curve isogenies. IACR Cryptology ePrint Archive 2017, 774 (2017). http://eprint.iacr.org/2017/774
10. Gorantla, M.C., Boyd, C., González Nieto, J.M., Manulis, M.: Generic one round group key exchange in the standard model. In: Lee, D., Hong, S. (eds.) ICISC 2009. LNCS, vol. 5984, pp. 1–15. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14423-3_1
11. Hövelmanns, K., Kiltz, E., Schäge, S., Unruh, D.: Generic authenticated key exchange in the quantum random oracle model. IACR Cryptology ePrint Archive 2018, 928 (2018). http://eprint.iacr.org/2018/276
12. Lan, X., Xu, J., Guo, H., Zhang, Z.: One-round cross-domain group key exchange protocol in the standard model. In: Chen, K., Lin, D., Yung, M. (eds.) Inscrypt 2016. LNCS, vol. 10143, pp. 386–400. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-54705-3_24
13. LeGrow, J., Jao, D., Azarderakhsh, R.: Modeling quantum-safe authenticated key establishment, and an isogeny-based protocol. IACR Cryptology ePrint Archive 2018, 282 (2018). http://eprint.iacr.org/2018/282

14. Li, Y., Yang, Z.: Strongly secure one-round group authenticated key exchange in the standard model. In: Abdalla, M., Nita-Rotaru, C., Dahab, R. (eds.) CANS 2013. LNCS, vol. 8257, pp. 122–138. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-02937-5_7
15. Longa, P.: A note on post-quantum authenticated key exchange from supersingular isogenies. IACR Cryptology ePrint Archive 2018, 267 (2018). http://eprint.iacr.org/2018/267
16. Manulis, M., Suzuki, K., Ustaoglu, B.: Modeling leakage of ephemeral secrets in tripartite/group key exchange. IEICE Trans. **96**–**A**(1), 101–110 (2013)
17. National Institute of Standards and Technology: Post-Quantum crypto standardization: Call for Proposals Announcement, December 2016. http://csrc.nist.gov/groups/ST/post-quantum-crypto/cfp-announce-dec2016.html
18. Rostovtsev, A., Stolbunov, A.: Public-key cryptosystem based on isogenies. IACR Cryptology ePrint Archive 2006, 145 (2006). http://eprint.iacr.org/2006/145
19. Suzuki, K., Yoneyama, K.: Exposure-resilient one-round tripartite key exchange without random oracles. In: ACNS 2013, pp. 458–474 (2013)
20. Xu, X., Xue, H., Wang, K., Tian, S., Liang, B., Yu, W.: Strongly secure authenticated key exchange from supersingular isogeny. IACR Cryptology ePrint Archive 2018, 760 (2018). http://eprint.iacr.org/2018/760