Journal of Information Hiding and Multimedia Signal Processing ©2017 ISSN 2073-4212
Ubiquitous International Volume **8**, Number **4**, July **2017**

Simple and Universal Construction for Round-Optimal Password Authenticated Key Exchange towards Quantum-Resistant

Hongfeng Zhu and Shuai Geng

Software College
Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 - China
zhuhongfeng1978@163.com; 1036103490@qq.com

Received February, 2015; revised April, 2017

Abstract. *Since quantum computers came on the scene, the world has changed greatly, especially related to cryptography. Public key cryptosystem, particularly RSA cryptosystem cant resist the quantum computers attack, so some quantum-resistant schemes have been proposed mainly based on quantum key distribution (QKD) method or new resistance to quantum algorithms. Recently, Jonathan et al (2013) presents two password-based authenticated key exchange (PAKE) protocols which make the communication reduce to one-round. At the same time Jonathans protocols achieve the mutual authentication and agreement the session key by constructing smooth projective hash functions. However Jonathans two protocols are subjected to quantum attacks, and there are so many time-consuming arithmetics just only for achieving a smooth projective hash function in Jonathans two protocols. Based on these motivations, this paper firstly proposes a provably secure and flexible one-round PAKE scheme based on elliptic curve isogenies. Compared with Jonathans two protocols, the results show that our one-round PAKE scheme can not only refrain from consuming modular exponential computing and scalar multiplication, but is also robust to resist quantum attacks. Finally we give the provable security of our scheme.*

Keywords: Authentication, Key exchange, Elliptic curve isogenies, Quantum-resistant, One-round communication

1. **Introduction.** Advances in quantum computers pose great threats on the currently used public key cryptographic algorithms such as RSA and ECC [**1, 2**]. So people hope to find having properties of public-key cryptography just like quantum cryptographic protocol [**3**], and we called them Quantum Public-key Cryptography (QPKC). The related research can mainly be divided into two kinds:

(1) Quantum physics-based methodology. Quantum cryptography, which began with Wiesners idea [**4**] almost 40 years ago, has reached the stage of commercial key distribution devices now. Origin of quantum key distribution in its oldest form is belonged to Bennett and Brassard [**6**] in 1984. The most popular method is No-Cloning Theorem which means a user cannot copy a qubit if he/she does not know the polarization basis of the qubit [**7**]. Based on No-Cloning Theorem, many quantum key distribution protocols (QKDPs) appeared. QKDPs employ quantum mechanisms to distribute session keys and public discussions to check for eavesdroppers and verify the correctness of a session key. However, public discussions require additional communication rounds between a sender and receiver and cost precious qubits. The other method is multipartite entanglement

which can design kinds of secure protocols, such as [**10**].The security of this kind method can be guaranteed by principle of quantum physics which can achieve perfect secrecy if not considering social engineering attacks and some flaws about designing protocol, but its hard to control the quantum key, lack of flexibility, narrow application recently and so on.

(2) Computational complexity-based methodology. This kind method aims to find hard problems under the quantum computation and according to these hard problems to structure the Public-key Cryptography and security protocol. These schemes are very flexible which can be imagined a bridge between electronic computer and quantum computer. There are two kinds of popular methods, called Multivariate Quadratic Polynomials (MQ problem) and lattice-based schemes. The former is a promising problem in cryptography. The associated decision problem is known to be NP-complete [**11**], and a random instance of the MQ problem is widely believed to be intractable. In contrast to factorization or a discrete logarithm problem, there is no known polynomialtime quantum algorithm to solve the MQ problem. The latter is based on an average-case problem which is as hard as worst-case problems, and some of them [**12**] are secure under active attack even if repeated in parallel.

Authenticated key exchange (AKE) protocols enable two parties to generate a shared, cryptographically strong key while communicating over an insecure network under the complete control of an adversary. Then because of owning the property which can allow users only to remember a password to bootstrap the weak (e.g., short password) shared secret into a (much longer) cryptographic key, password-based authenticated key exchange (PAKE) protocols become very popular at present [**16,17**].

However, all above-mentioned user-friendly authenticated key agreement schemes cant resist quantum computers attack. The chief aim of this paper is to design a practical PAKE protocol towards quantum-resistant for convenience of customers. To the best of our knowledge, no one-round PAKE protocol based on elliptic curve isogenies has been proposed, yet. Generally speaking, a one-round PAKA protocol with elliptic curve isogenies should achieve the following requirements: (1) It should allow two users establish a secure session key over an insecure communication channel with the public and the shared passwords. (2) The protocol should be based on elliptic curve isogenies that can resist quantum attack on algorithm level. (3) The protocol should be able to resist all known attacks on protocol level, such as password guessing attacks, impersonation attacks, man-in-the-middle attacks, etc. (4) The protocol should achieve some well-known properties, such as perfect forward secrecy, no timestamp, and execution efficiency.

In this paper, based on elliptic curve isogenies, we propose a new one-round password-authenticated key agreement protocol which achieves the above requirements. The rest of the paper is organized as follows: We outline preliminaries in Section 2. Next, an elliptic curve isogenies-based one-round PAKE protocol is described in Section 3. Then, the security analysis and efficiency analysis are given in Section 4 and Section 5. This paper is finally concluded in Section 6.

2. **Preliminaries.**

2.1. **Isogenies [19, 23].**

Definition 2.1. *An isogeny φ is a nontrivial (non-constant) rational map (such as: $\varphi(x,y) = (\frac{f_1(x,y)}{g_1(x,y)}, \frac{f_2(x,y)}{g_2(x,y)})$) of an Elliptic Curve onto another Elliptic Curve that is also a group homomorphism (satisfying $\varphi(\infty) = \infty$, equivalently $\varphi(P+Q) = \varphi(P) + \varphi(Q)$).*

The degree of an isogeny is its degree as an algebraic map. The endomorphism ring End(E) is the set of isogenies from $E(\bar{F})$ to itself, together with the constant homomorphism. This set forms a ring under pointwise addition and composition. If $\varphi : E \to E'$ is an isogeny, then φ is surjective. Meaning that for a point P' in $E'(\bar{K})$ there exists a point P in $E(\bar{K})$ such that $\varphi(P)$ is P'.

Definition 2.2. *Let $\varphi : E \to E'$ be an isogeny, and let $r_1(x)$ be the x-coordinate map. If the derivative of the x-coordinate map $r_1'(x)$ is not 0 then φ is separable.*

Definition 2.3. *An elliptic curve is called supersingular if $E[p] = \{\infty\}$, where $p = char.(E)$.*

Proposition 1 E/F_q,$q = p^r$.Let $a = q + 1 - \#E(F_q) \to E$ is supersingular if and only if $a \equiv 0(modp) \Leftrightarrow E(F_q) \equiv 1(modp)$

Two curves E and E' are isogenous over F_q if and only if $\#E = \#E'$.

2.2. Hard problems of elliptic curve isogenies-based[25, 22].

Arithmetic generation About any fixed choice of $l_A^{e_A}$ and $l_B^{e_B}$,it is easy to found random values of f and $p = l_A^{e_A} l_B^{e_B} \cdot f \pm 1$, where p is prime. For elliptic curve isogenies-based computation is also easy according to literatures.

Complexity Assumptions

Supersingular Isogeny (SSI) problem. Let $\phi_A : E_0 \to E_A$ be an isogeny whose kernel is $\langle [m_A]P_A + [n_A]Q_A \rangle$ where m_A and n_A are chosen at random from $Z/\ell_A^{e_A}Z$ and not both divisible by ℓ_A . Given E_A and the values $\phi_A(P_B), \phi_A(Q_B),$, find a generator R_A of $\langle [m_A]P_A + [n_A]Q_A \rangle$. Given a generator $R_A = [m_A]P_A + [n_A]Q_A$, it's easy to solve for (m_A, n_A) , since E_0 has smooth order and thus extended discrete logarithms are esay in E_0 .

Supersingular Computational Diffie-Hellman (SSCDH) problem. Let $\phi_A : E_0 \to E_A$ be an isogeny whose kernel is $\langle [m_A]P_A + [n_A]Q_A \rangle$, and Let $\phi_B : E_0 \to E_B$ $\phi_A : E_0 \to E_A$ $\langle [m_B]P_B + [n_B]Q_B \rangle$, where m_A and n_A (respectively m_B , n_B) are chosen at random from $Z/\ell_A^{e_A}Z$ (respectively $Z/\ell_B^{e_B}Z$) and not both divisible by ℓ_A (respectively ℓ_B) Given the curves E_A , E_B and the points $\phi_A(P_B)$,$\phi_A(Q_B)$,$\phi_B(P_A)$,$\phi_B(Q_A)$,find the j-invariant of $E_0/\langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B \rangle$

Supersingular Decision Diffie-Hellman (SSDDH) problem. Given a tupe sampled with probability 1/2 from one of the following two distributions:

— $(E_A, E_B,\ \phi_A(P_B)$,$\phi_A(Q_B)$,$\phi_B(P_A)$,$\phi_B(Q_A)$,$E_{AB})$,where E_A , E_B , $\phi_A(P_B)$,$\phi_A(Q_B)$, $\phi_B(P_A)$, $\phi_B(Q_A)$,E_{AB} are as in the *SSCDH* problem and $E_{AB} \cong E_0/\ \langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B \rangle$,

— $(E_A, E_B,\ \phi_A(P_B)$,$\phi_A(Q_B)$,$\phi_B(P_A)$,$\phi_B(Q_A)$,$E_C)$,where E_A ,E_B , $\phi_A(P_B)$,$\phi_A(Q_B)$,$\phi_B(P_A)$, $\phi_B(Q_A)$ are as in the *SSCDH* problem and $E_{AB} \cong E_0/\ \langle [m_A']P_A + [n_A']Q_A, [m_B']P_B + [n_B']Q_B \rangle$, where m_A',n_A' (respectively m_B',n_B') are chosen at random from $Z/\ell_A^{e_A}Z$ (respectively $Z/\ell_B^{e_B}Z$) and not both divisible by ℓ_A (respectively ℓ_B), determine from which distribution the triple is sampled.

3. The Proposed Isogenies-based Scheme.

3.1. Notations.

The notation used hereafter is shown in **Table 1**.

3.2. One-Round Instance with Elliptic Curve Isogenies-based. (1) Instance set up

In this phase, any party can choose public information E_0,$(P_A$,$Q_A)$=$E_0[l_A^{e_A}]$,$(P_B$,$Q_B)$ = $E_0[l_B^{e_B}]$based on elliptic curve isogenies, a secure one-way quantum hash function H_Q against quantum attack. Additionally, Alice shares passwords *PW* with Bob; users Alice

Table 1. Notations

Symbol	Definition
ID_A , ID_B	Identity information of the Alice, Bob and Server
$\|\|$	Means that two adjacent messages are concatenated
H_Q [9]	a secure one-way quantum hash function which can resist quantum computing
SK	Session Key
E_0,(P_A,Q_A),(P_B,Q_B)	Public information
(m_A,n_A) (m_B,n_B)	Temporary number of Alice and Bob chosen based on the bases
K	A field
$\overline{K}$	A fixed algebraic closure of K
E	A fixed elliptic curve given by the Weierstrass model with coefficients in K
$E(K)$, $E(\overline{K})$	The set of pairs (x, y) satisfying the Weierstrass equation of E where x and y are taken in K or $\overline{K}$ respectively
φ	An isogeny from E to another elliptic curve E'
pw	Shared by Alice and Bob
l_A,l_B	Small primes
f_1,f_2,f_3	Cofactors
e_A,e_B	Positive integer

and Bob choose their identities ID_A and ID_B , respectively. No Pre-distribution means that public/private key pair has no use for each party, and anyone can produce the public information, that is to say, any two parties only have shared password which make them to achieve the one round-optimal password authenticated key exchange based on the public and setting information. The kind of one-round instance can not only refrain from distributing the public/private key pair to each party, but is also robust to resist various attacks and achieves quantum-resistant.

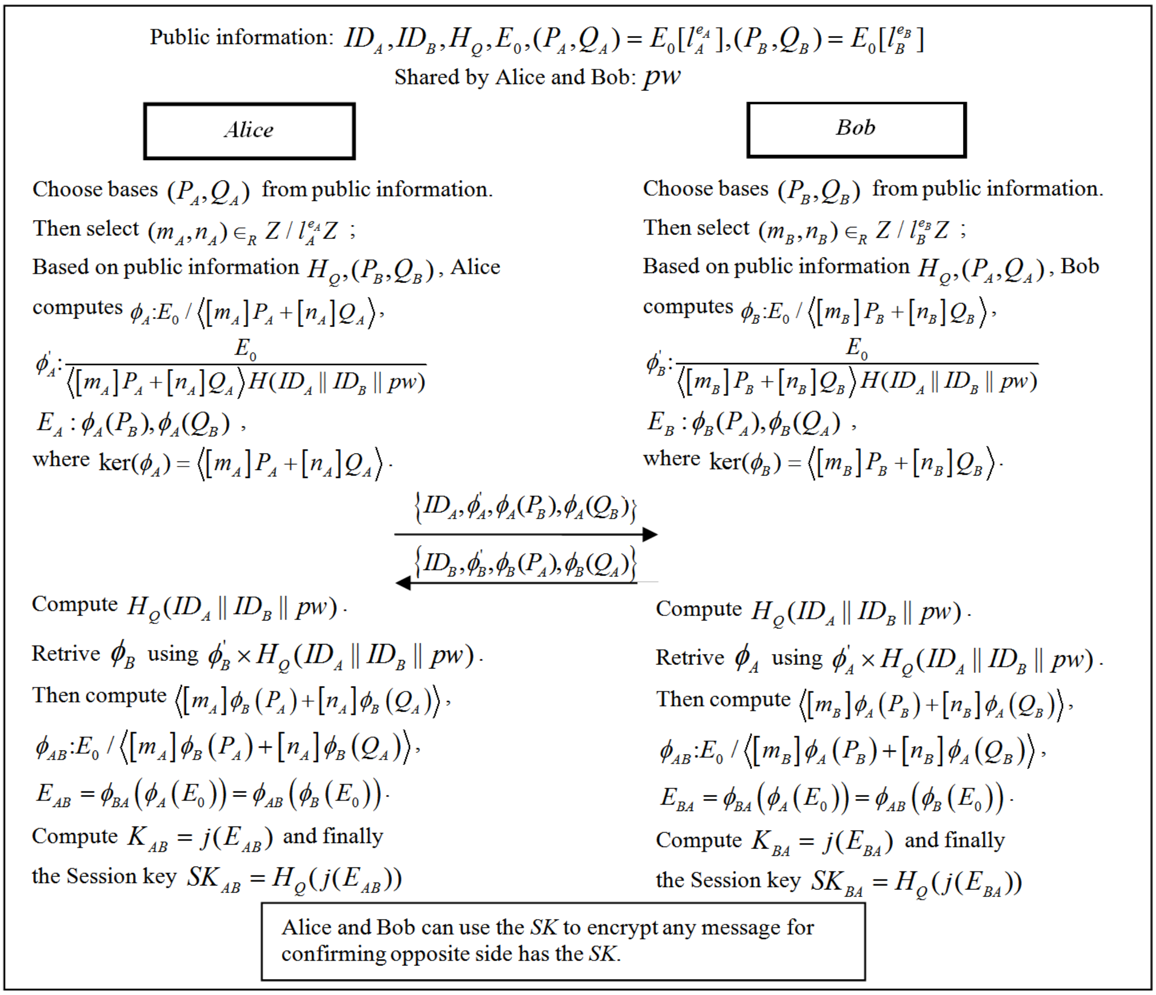
(2) One-Round Instance

One-Round Exchange. The one-round instance used hereafter is shown in **Fig.1**.Alice chooses bases $(P_A$,$Q_A)$ from the public information and selects a pair of random nonces $(m_A, n_A) \in {}_R Z/l_A^{e_A} Z$ Based on the public information H_Q,$(P_B$,$Q_B)$,Alice computes $\phi_A : E_0/\langle [m_A]P_A + [n_A]Q_A\rangle$,$\phi_A^{'} : E_0/\{\langle [m_A]P_A + [n_A]Q_A\rangle H_Q(ID_A||ID_B||pw)\}$,$E_A : \phi_A(P_B)$, $\phi_A(Q_B)$, where $ker(\phi_A) = \langle [m_A]P_A + [n_A]Q_A\rangle$.Finally Alice sends the message $\{ID_A$, $\phi_A(P_B), \phi_A(Q_B)\}$to Bob.

For Bob: Choose bases (P_B, Q_B) from the public information and select a pair of random nonces $(m_B, n_B) \in {}_R Z/l_B^{e_B} Z$Based on the public informationH_Q,$(P_A$,$Q_A)$, Bob computes $\phi_B : E_0/\langle [m_B]P_B + [n_B]Q_B\rangle$,$\phi_B^{'} : E_0/\{\langle [m_B]P_B + [n_B]Q_B\rangle H_Q(ID_B||ID_B||pw)\}$,$E_B : \phi_B(P_A), \phi_B(Q_A)$, where $ker(\phi_B) = \langle [m_B]P_B + [n_B]Q_B\rangle$.Finally Bob sends the message $\{ID_A, \phi_A(P_B), \phi_A(Q_B)\}$to Alice.

Local Computation and Get the Session Key. First of all, because E_{AB} or E_{BA} has the same j-invariant, Alice and Bob can compute the same j-invariant based on E_{AB} or E_{BA} by executing the proposed scheme.

For Bob: After receiving the message $\{ID_A, \phi_A^{'}\phi_A(P_B), \phi_A(Q_B)\}$from Alice, Bob will authenticate Alice and then compute the session key: Bob will compute $H_Q(ID_A||ID_B||pw)$ using the shared password PW with Alice, and then Bob can recover the information $\phi_B : E_0/\langle [m_B]P_B + [n_B]Q_B\rangle$ ($\phi_B = \phi_B^{'} \times H_Q(ID_A||ID_B||pw)$).Next based on ϕ_B Bob computes the information $\phi_{AB} : \langle [m_B]\phi_A(P_B) + [n_B]\phi_A(Q_B)\rangle$ and $E_{AB} = \phi_{BA}(\phi_A(E_0)) = \phi_{AB}(\phi_B(E_0))$.Bob computes $K_{AB} = j(E_{BA})$ and finally the session key $SK_{AB} = H_Q(j(E_{BA}))$. Because $\phi_A(P_B), \phi_A(Q_B)$ are two values and $\phi_B^{'}$ is kernel of another elliptic



Public information: $ID_A, ID_B, H_Q, E_0, (P_A, Q_A) = E_0[l_A^{e_A}], (P_B, Q_B) = E_0[l_B^{e_B}]$

Shared by Alice and Bob: pw

Alice

Choose bases (P_A, Q_A) from public information.
Then select $(m_A, n_A) \in_R Z / l_A^{e_A} Z$;
Based on public information $H_Q, (P_B, Q_B)$, Alice
computes $\phi_A{:}E_0 / \langle [m_A]P_A + [n_A]Q_A \rangle$,

$\phi_A^{'}{:}\dfrac{E_0}{\langle [m_A]P_A + [n_A]Q_A \rangle H(ID_A \| ID_B \| pw)}$

$E_A : \phi_A(P_B), \phi_A(Q_B)$,
where $\ker(\phi_A) = \langle [m_A]P_A + [n_A]Q_A \rangle$.

Bob

Choose bases (P_B, Q_B) from public information.
Then select $(m_B, n_B) \in_R Z / l_B^{e_B} Z$;
Based on public information $H_Q, (P_A, Q_A)$, Bob
computes $\phi_B{:}E_0 / \langle [m_B]P_B + [n_B]Q_B \rangle$,

$\phi_B^{'}{:}\dfrac{E_0}{\langle [m_B]P_B + [n_B]Q_B \rangle H(ID_A \| ID_B \| pw)}$

$E_B : \phi_B(P_A), \phi_B(Q_A)$,
where $\ker(\phi_B) = \langle [m_B]P_B + [n_B]Q_B \rangle$.

$$\xrightarrow{\{ID_A, \phi_A^{'}, \phi_A(P_B), \phi_A(Q_B)\}}$$

$$\xleftarrow{\{ID_B, \phi_B^{'}, \phi_B(P_A), \phi_B(Q_A)\}}$$

Compute $H_Q(ID_A \| ID_B \| pw)$.
Retrive ϕ_B using $\phi_B^{'} \times H_Q(ID_A \| ID_B \| pw)$.
Then compute $\langle [m_A]\phi_B(P_A) + [n_A]\phi_B(Q_A) \rangle$,
$\phi_{AB}{:}E_0 / \langle [m_A]\phi_B(P_A) + [n_A]\phi_B(Q_A) \rangle$,
$E_{AB} = \phi_{BA}(\phi_A(E_0)) = \phi_{AB}(\phi_B(E_0))$.
Compute $K_{AB} = j(E_{AB})$ and finally
the Session key $SK_{AB} = H_Q(j(E_{AB}))$

Compute $H_Q(ID_A \| ID_B \| pw)$.
Retrive ϕ_A using $\phi_A^{'} \times H_Q(ID_A \| ID_B \| pw)$.
Then compute $\langle [m_B]\phi_A(P_B) + [n_B]\phi_A(Q_B) \rangle$,
$\phi_{AB}{:}E_0 / \langle [m_B]\phi_A(P_B) + [n_B]\phi_A(Q_B) \rangle$,
$E_{BA} = \phi_{BA}(\phi_A(E_0)) = \phi_{AB}(\phi_B(E_0))$.
Compute $K_{BA} = j(E_{BA})$ and finally
the Session key $SK_{BA} = H_Q(j(E_{BA}))$

Alice and Bob can use the *SK* to encrypt any message for confirming opposite side has the *SK*.

FIGURE 1. Authentication and key agreement phase.

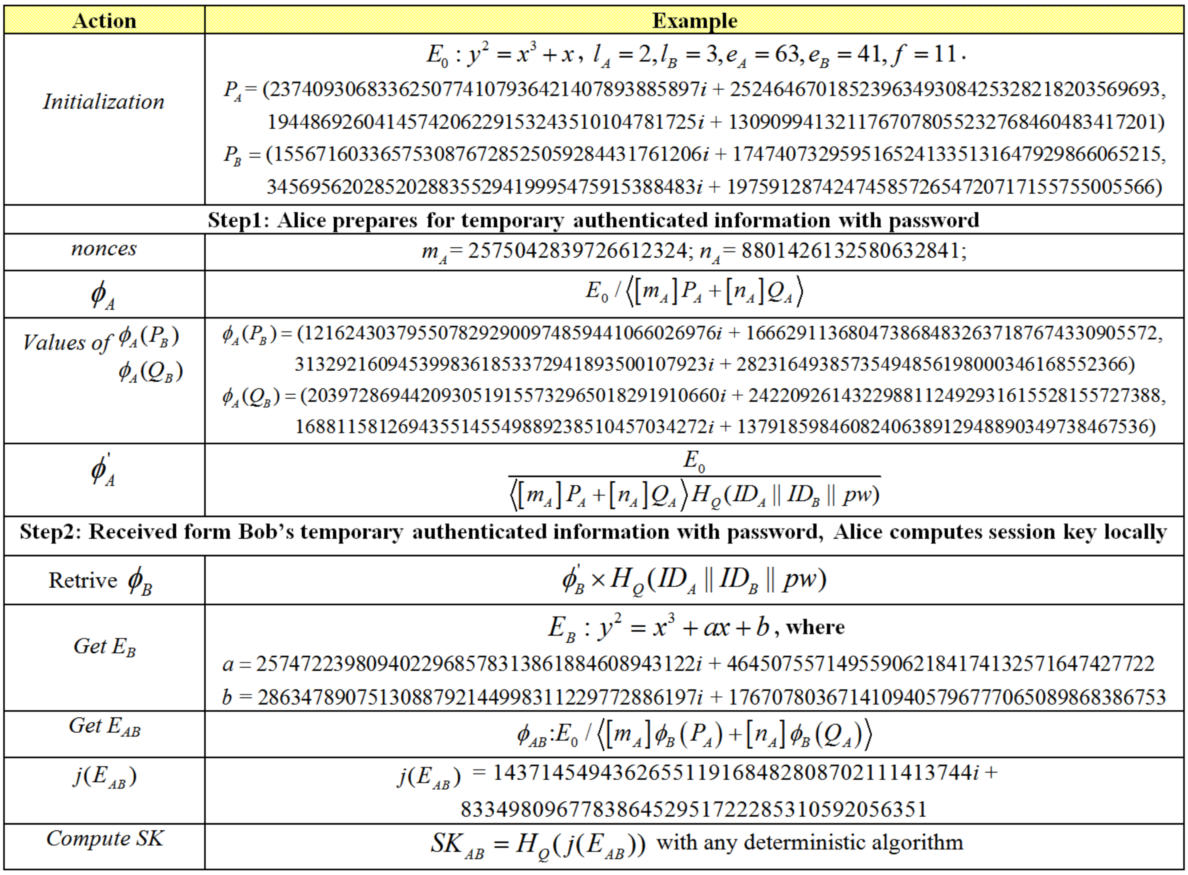
curve, only known the information $\phi_A(P_B), \phi_A(Q_B), \phi_B^{'}$ is hard to recover $\phi_B^{'}$ and E_B. Consequences of above-mentioned, an attacker cant get $\phi_B^{'}$ and E_B and E_{AB} , and then cant get the SK.

For Alice: Do the same way to get the $SK_{AB} = H_Q(j(E_{AB}))$. Alice and Bob can use the SK to encrypt any message for confirming opposite side has the SK. An example is shown in **Table 2**.

4. **Security Consideration.** Assume there are three secure components, including the three problems SSI, $SSCDH$ and $SSDDH$ cannot be solved in polynomial-time by quantum computers, a secure one-way quantum hash function and a secure symmetric encryption which both can resist quantum computers attack. We also prove that our proposed scheme achieves the security and efficiency goals. The analysis of our Quantum resistant scheme will be illustrated in **Appendix A**, and the provable security of our scheme will be illustrated in textbf Appendix B.

5. **Efficiency Analysis.** After all, our proposed protocol is the first practical one-round scheme which is based on elliptic curve isogenies towards quantum-resistant. To the best of our knowledge, no elliptic curve isogenies-based practical one-round password-authenticated key exchange protocol without using a timestamp has been proposed, so there is no literatures to contrast and we sum up our proposed protocol as show in **Table**

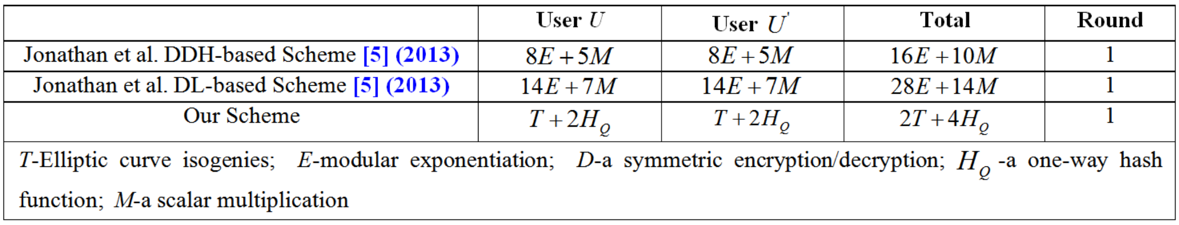
Table 2. An example with values from the view of Alice



Action	Example
Initialization	$E_0 : y^2 = x^3 + x$, $l_A = 2, l_B = 3, e_A = 63, e_B = 41, f = 11$. P_A= (23740930683362507741079364214078938858897i + 25246467018523963493084253282182035669693, 1944869260414574206229153243510104781725i + 1309099413211767078055232768460483417201) P_B = (1556716033657530876728525059284431761206i + 17474073295951652413351316479298660665215, 3456956202852028835529419995475915388483i + 1975912874247458572654720717155755005566)
Step1: Alice prepares for temporary authenticated information with password	
nonces	m_A= 2575042839726612324; n_A= 8801426132580632841;
ϕ_A	$E_0 / \langle [m_A]P_A + [n_A]Q_A \rangle$
Values of $\phi_A(P_B)$ $\phi_A(Q_B)$	$\phi_A(P_B)$ = (1216243037955078292900974859441066026976i + 1666291136804738684832637187674330905572, 3132921609453998361853372941893500107923i + 2823164938573549485619800034616855236 6) $\phi_A(Q_B)$ = (2039728694420930519155732965018291910660i + 2422092614322988112492931615528155727388, 1688115812694355145549889238510457034272i + 1379185984608240638912948890349738467536)
$\phi_A^{'}$	$\dfrac{E_0}{\langle [m_A]P_A + [n_A]Q_A \rangle H_Q(ID_A \parallel ID_B \parallel pw)}$
Step2: Received form Bob's temporary authenticated information with password, Alice computes session key locally	
Retrive ϕ_B	$\phi_B^{'} \times H_Q(ID_A \parallel ID_B \parallel pw)$
Get E_B	$E_B : y^2 = x^3 + ax + b$, **where** a = 2574722398094022968578313861884608943122i + 4645075571495590621841741325716474277 22 b = 2863478907513088792144998311229772886197i + 1767078036714109405796777065089868386753
Get E_{AB}	ϕ_{AB}:$E_0 / \langle [m_A]\phi_B(P_A) + [n_A]\phi_B(Q_A) \rangle$
$j(E_{AB})$	$j(E_{AB})$ = 1437145494362655119168482808702111413744i + 8334980967783864529517222853105920563 51
Compute SK	$SK_{AB} = H_Q(j(E_{AB}))$ with any deterministic algorithm

3 (Efficiency). Our protocol is reasonably efficient. The efficiency is measured by the following two aspects which are communication cost and computation cost.

Table 3. Efficiency comparison of one-round authentication and key exchange



	User U	User $U^{'}$	Total	Round
Jonathan et al. DDH-based Scheme [5] (2013)	$8E + 5M$	$8E + 5M$	$16E + 10M$	1
Jonathan et al. DL-based Scheme [5] (2013)	$14E + 7M$	$14E + 7M$	$28E + 14M$	1
Our Scheme	$T + 2H_Q$	$T + 2H_Q$	$2T + 4H_Q$	1
T-Elliptic curve isogenies; E-modular exponentiation; D-a symmetric encryption/decryption; H_Q -a one-way hash function; M-a scalar multiplication				

6. **Conclusions.** The paper put forward a new framework to improve the efficiency about the problems of password authenticated key exchange. In the new framework, we give one round-optimal instance: based on elliptic curve isogenies which can resist quantum attack and without pre-distribution for each party, that is to say, no pre-distribute public/private key pair to each party, any two parties only have shared password can make them to achieve the one round-optimal password authenticated key exchange based on the public and setting information. On the basis of assuming all secrets can be stored securely and the password has already been assigned, our proposed scheme has satisfactory security, efficiency and functionality. Next, we will extend the proposed protocols in three aspects: (1) From the strength of the security level, we will bring in the smart card or biometric. (2) From the view of functionality, we will research the fairness or entanglement and so

on. (3) From the perspective of complex, diversified algorithms, especially for quantum security, are our interests. Acknowledgement. This work is supported by the Liaoning Provincial Natural Science Foundation of China (Grant No. 201602680).

REFERENCES

[1] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J Comput*, vol. 6, pp. 14841509, 1997.

[2] L. K. Grover, A fast quantum mechanical algorithm for database search,*[c]. Proc. 28th Annual ACM symposium on theory of computing(STOC), New York, ACM*, pp. 212-219, 1996.

[3] W. Chen, Z. F. Han, X. F. Mo , et al., Active phase compensation of quantum key distribution system, *J. Chinese Sci Bull*, vol. 53, pp. 1310-1314, 2008.

[4] S. Wiesner, Conjugate coding*J. ACM Sigact News* , vol. 15, no. 1, pp. 7888, 1983.

[5] C. C. Lai, H. C. Huang and C. C. Tsai, Jonathan Katz, Vinod Vaikuntanathan. Round-Optimal Password-Based Authenticated Key Exchange.*J. Cryptol.*, vol. 26, pp. 714743, 2013.

[6] Bennett, C.H., Brassard, G.: Quantum cryptography, public-key distribution and coin tossing. In, *Proceedings IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore,* pp. 175179. IEEE, New York 1984.

[7] W.K. Wootters and W.H. Zurek, A Single Quantum Cannot Be Cloned, *Nature,* vol. 299, pp. 802-803, 1992.

[8] R. H. Shi, H.ng Zhong, Multiparty quantum secret sharing with the pure entangled two-photon states. *Quantum Inf Process* , vol. 11, pp. 161-169, 2012. DOI 10.1007/s11128-011-0239-9.

[9] D.Li, J. Zhang, F. Z. Guo, et al., Discrete-time interacting quantum walks and quantum hash schemes. *Quantum Inf Process* , vol. 12, pp.1501 1513, 2013.

[10] S. Bose, V. Vedral, P.L. Knight, A multiparticle generalization of entanglement swapping, *J. Phys. Rev.* , vol. A 57, pp. 822 1998.

[11] J. Patarin, L. Goubin, Trapdoor One-Way Permutations and Multivariate Polynominals. *In, Han, Y., Okamoto, T., Qing, S. (eds.) ICICS 1997. LNCS*, vol. 1334, pp. 356368. Springer, Heidelberg (1997)

[12] V. Lyubashevsky, Fiat-Shamir with Aborts, Applications to Lattice and Factoring-Based Signatures. I*n, Matsui, M. (ed.) ASIACRYPT 2009. LNCS,* vol. 5912, pp. 598616., Springer, Heidelberg (2009).

[13] A. Childs, D. Jao, and V. Soukharev, Constructing elliptic curve isogenies in quantum subexponential time, 2010. http://arxiv.org/abs/1012.4019/.

[14] O. Billet , Robshaw, T. Peyrin, On building hash functions from multivariate quadratic equations. *In, Proceedings of ACISP 2007, LNCS, vol. 4586, Berlin, Springer-Verlag, 2007,* pp. 82-95.

[15] Ran Canetti and Hugo Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. In Birgit Ptzmann, editor, EUROCRYPT, volume 2045 of *Lecture Notes in Computer Science*, pp. 453-474. Springer, 2001.

[16] T. H. liu, Q. Wang, H. F. Zhu, A Multi-function Password Mutual Authentication Key Agreement Scheme with privacy preserving, *Journal of information hiding and multimedia signal processing.* vol. 5, no. 2, 2014.

[17] Ho. Wang, H. Zhang, J. X. Li and X. Chen , A(3,3) visual cryptography scheme for authentication. *Journal of Shenyang Normal University (Natural Science Edition)*, vol. 31, no. 101(03), pp. 397-400, 2013.

[18] G. Jacob, A. Murugan, DNA based Cryptography, An Overview and Analysis. *Int. J. Emerg. Sci.,* no. 3, no. 1, pp. 36-42, March 2013.

[19] J. H. Silverman, The arithmetic of elliptic curves, *vol. 106 of Graduate Texts in Mathematics.* SpringerVerlag, New York, 1992. Corrected reprint of the 1986 original.

[20] Anton Stolbunov. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves, *J. Adv. Math. Commun.*, vol. 4, no. 2, pp. 215-235, 2010.

[21] D. Steven Galbraith and A. Stolbunov, Improved algorithm for the isogeny problem for ordinary elliptic curves, 2011. http://arxiv.org/abs/1105.6331/.

[22] E. Teske, The pohlig-hellman method generalized for group structure computation, *Journal of Symbolic Computation*, vol.27, no. 6, pp. 521-534, 1999.

[23] D. Steven Galbraith, Constructing isogenies between elliptic curves over finite fields, *LMS J. Comput. Math.*, vol. 2, pp. 118-138 , 1999.

[24] S. D. Galbraith, Florian Hess, and Nigel P. Smart, *Extending the GHS Weil descent attack. In Advances in cryptology-EUROCRYPT 2002 (Amsterdam), volume 2332 of Lecture Notes in Comput. Sci.*, pp. 29-44. Springer, Berlin, 2002.

[25] D. Jao and L. De Feo, Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies, *Post-Quantum Cryptography Lecture Notes in Computer Science*, vol. 7071/2011, pp. 19-34, 2011.

Appendix A. The analysis of our Quantum resistant scheme

definition A. It encompasses all the ways in which can resist quantum computer attack, including quantum cryptography [**8**], DNA cryptography [**18**] and resistance to quantum algorithms [**25**], and we called them Post-Quantum Cryptography or Quantum Resistant Cryptography

Theorem A.*The proposed protocol can resist quantum computer attack.*

Proof. Our proposed protocol is composed of three parts, elliptic curve isogenies in Public Key Cryptosystem, a secure one-way hash function and a pair of secure symmetric encryption/decryption which all can resist quantum computer attack. **(a) Elliptic curve isogenies algorithm.**The Shor algorithm [**1**] is the greatest threat which can attack most public key Cryptosystem, such as RSA, Diffie-Hellman, ELGamal and ECC. Theory indicates that 256 bits elliptic curve cryptography can be decoded by 1024 bits quantum computer, and 1024 bits RSA cryptography can be cracked by 2048 bits quantum computer easily. However, our protocol adopts elliptic curve isogenies in public key Cryptosystem which can resist quantum computers, even for quantum computers attack that still requires fully exponential time [**21**]. Recently, Stolbunov [**20**] proposed a Diffie-Hellman type system based on the difficulty of computing isogenies between ordinary elliptic curves, with the stated aim of obtaining quantum-resistant cryptographic protocols. The fastest known (classical) probabilistic algorithm for solving this problem is the algorithm of Galbraith and Stolbunov [**21**], based on the algorithm of Galbraith, Hess, and Smart [**24**]. This algorithm is exponential, with a worst-case running time of $(O\sqrt[4]{x})$. However, on a quantum computer, recent work of Childs et al. [**13**] has shown that the private keys in Stolbunov's system can be recovered in subexponential time. Moreover, even if we only consider classical attacks in assessing security levels, Stolbunov's scheme requires 229 seconds (even with pre-computation) to perform a single key exchange operation at the 128-bit security level on a desktop PC [**20**]**.(b) A pair of secure symmetric algorithm.**Anyway, Grover algorithm [**2**] is the general method which can reduce the key length to half for symmetric cryptography. So we can double the key length and adopt a secure symmetric algorithm that is enough.**(c) A secure one-way hash function.**Until now many multivariate hash functions can resist quantum computers attack, such as [**14**] and so on.

Appendix B. The provable security of our scheme

We recall the definition of session-key security in the authenticated-links adversarial model of Canetti and Krawczyk [**15**]. The basic descriptions are shown in **Table 4**.

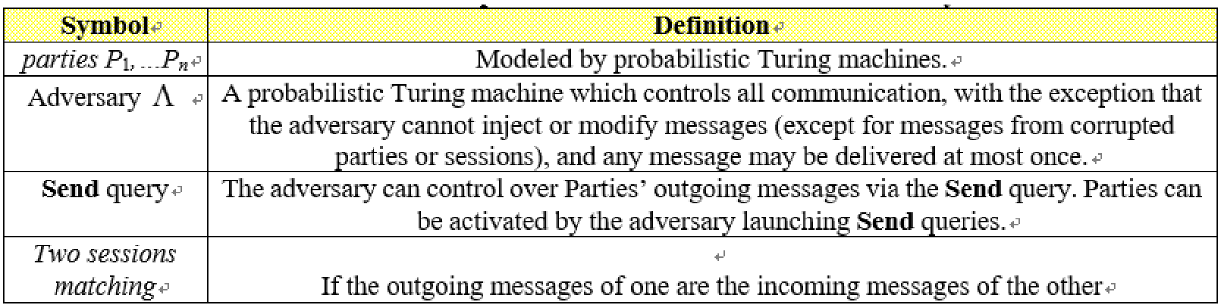
We allow the adversary access to the queries **SessionStateReveal, SessionKeyReveal,**and **Corrupt**.

(1)**SessionStateReveal(s)**: This query allows the adversary to obtain the contents of the session state, including any secret information. s means no further output.

(2)**SessionKeyReveal(s)**: This query enables the adversary to obtain the session key for the specified session s, so long as s holds a session key.

(3)**Corrupt(Pi)**: This query allows the adversary to take over the party P_i including long-lived keys and any session-specific information in P_i 's memory. A corrupted party produces no further output.

Table 4. Descriptions the model of Canetti and Krawczyk



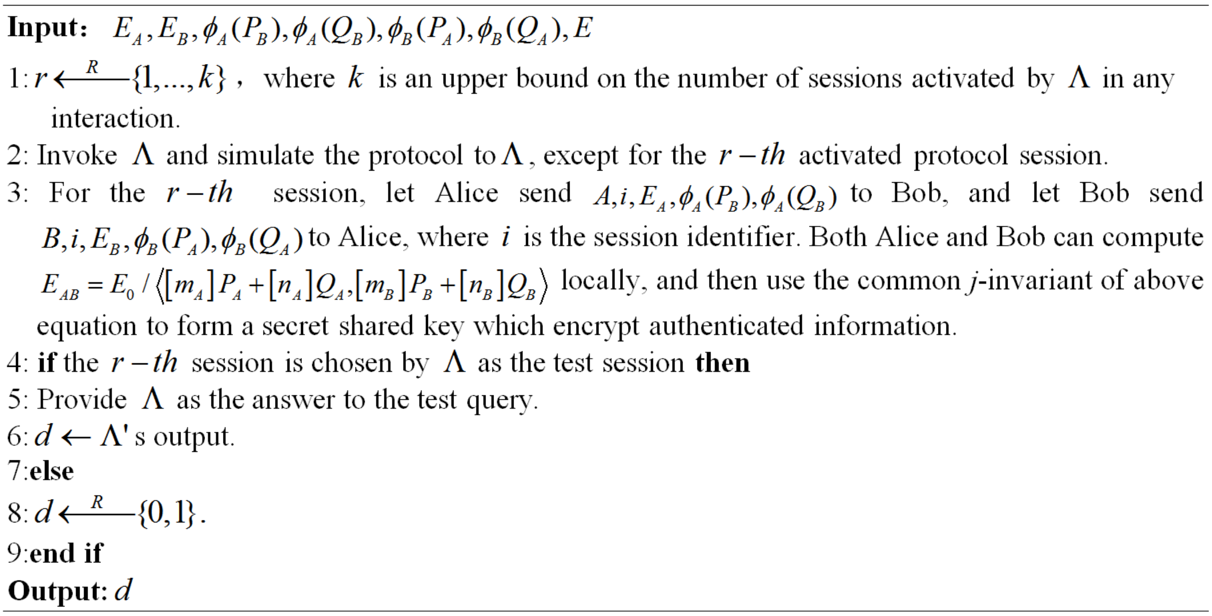
Symbol	**Definition**
parties $P_1, \ldots P_n$	Modeled by probabilistic Turing machines.
Adversary Λ	A probabilistic Turing machine which controls all communication, with the exception that the adversary cannot inject or modify messages (except for messages from corrupted parties or sessions), and any message may be delivered at most once.
Send query	The adversary can control over Parties' outgoing messages via the **Send** query. Parties can be activated by the adversary launching **Send** queries.
Two sessions matching	If the outgoing messages of one are the incoming messages of the other

(3)**Test(s)**: This query allows the adversary to be issued at any stage to a completed, fresh, unexpired session **s**. A bit b is then picked randomly. If $b = 0$, the test oracle reveals the session key, and if $b = 1$, it generates a random value in the key space. The adversary Λ can then continue to issue queries as desired, with the exception that it cannot expose the test session. At any point, the adversary can try to guess b.Let $GoodGuess^{\Lambda}(k)$ be the event that the adversary Λ correctly guesses b, and we define the advantage of adversary Λ as $Advantage^{\Lambda}(k) = max\{0, |Pr[GoodGuess^{\Lambda}(k)] - \frac{1}{2}|\}$, where k is a security parameter.

A session **s** is locally exposed with : if the adversary has issued **SessionStateReveal(s), SessionKeyReveal(s), Corrupt(Pi)** before s is expired.

Definition B.1. A key exchange protocol Π in security parameter k is said to be session-key secure in the adversarial model of Canetti and Krawczyk if for any polynomial-time adversary Λ,

Algorithm 1 SSDDH distinguisher



```
Input: $E_A, E_B, \phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A), E$
$r \xleftarrow{R} \{1, \ldots, k\}$ , where $k$ is an upper bound on the number of sessions activated by $\Lambda$ in any interaction.
Invoke $\Lambda$ and simulate the protocol to $\Lambda$, except for the $r-th$ activated protocol session.
For the $r-th$ session, let Alice send $A, i, E_A, \phi_A(P_B), \phi_A(Q_B)$ to Bob, and let Bob send $B, i, E_B, \phi_B(P_A), \phi_B(Q_A)$ to Alice, where $i$ is the session identifier. Both Alice and Bob can compute $E_{AB} = E_0 / \langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B \rangle$ locally, and then use the common $j$-invariant of above equation to form a secret shared key which encrypt authenticated information.
if the $r-th$ session is chosen by $\Lambda$ as the test session then
    Provide $\Lambda$ as the answer to the test query.
    $d \leftarrow \Lambda$'s output.
else
    $d \xleftarrow{R} \{0,1\}$.
end if
Output: $d$
```

(1) If two uncorrupted parties have completed matching sessions, these sessions produce the same key as output;

(2) $Advantage^{\Lambda}(k)$ is negligible.

Theorem B.1. *Under the SSDDH assumption, using the Algorithm 1 to compute session key is session-key secure in the adversarial model of Canetti and Krawczyk* [**15**]

Proof. The proof is based on the proof given by Refs. [**25,15**]. There are two uncorrupted parties in matching sessions output the same session key, and thus the first part of **Definition B.1** is satisfied. To show that the second part of the definition is satisfied, assume that there is a polynomial-time adversary Λ with a non-negligible advantage εin standard model. We claim that Algorithm 1 forms a polynomial-time distinguisher for SSDDH having non-negligible advantage. **Probability analysis.** It is clear that Algorithm 1 runs in polynomial time and has non-negligible advantage. There are two cases where the r-th session is chosen by Λ as the test session: (1) If the r-th session is not the test session, then Algorithm 1 outputs a random bit, and thus its advantage in solving the SSDDH is 0. (2) If the r-th session is the test session, then Λ will succeed with advantage ε , since the simulated protocol provided to Λ is indistinguishable from the real protocol. The latter case occurs with probability $1/k$, so the overall advantage of the SSDDH distinguisher is ε/k, which is non-negligible.