Survey on Lattice-based Key Exchange and Multi-party Key Exchange

Chapter 1. Introduction

The need for a key exchange protocol over an insecure channel is raised to prevent unauthorized access or accidental disclosure of the information while transmission process between entities over a network. Communicating between two entities on a public network needs to be secure to prevent any attacks to read transmitted messages. Secure transmission means encrypting the message with an encryption key and then sending it from one entity to another. The problem is how to share the key between two entities securely. For that, we use key exchange protocols which identifies each entity to another, create and distribute the key among them securely.

Key exchange protocols can be categorized into two categories: key transport protocols and key agreement protocols. In key transport protocols, the session key is first created by one of communicating entities and then transmitted securely to the other. In other hands, the key agreement protocol relies on some information from the both parties to derive the session key from. So, key transport protocol is more centralized protocol and key agreement protocol is more decentralized protocol.

On the other hand, as the quantum computer becomes realistic in the near future, constructing protocols using post-quantum cryptography against quantum computing attack is currently one of challenging issues in cryptography. Indeed, the security of all public key algorithms based on classical hard problems will no longer be assured as soon as an adequate quantum computer exists. It is clear that the effort to develop quantum-resistant technologies is intensifying. In the US, the National Security Agency (NSA) planned to transition from its Suite B cryptographic tools to quantum-resistant algorithms. The National Institute of Standards and Technology (NIST) requested to submit post-quantum cryptographic algorithms for standards.

In this paper, we survey on the lattice-based key exchange protocols (AKE) with quantum resistance and other key exchange protocols with multi-party setting.

The rest of this paper is structured as follows. First, we review the definition of key exchange, authenticated key exchange, and password-based authenticated key exchange protocols in Chapter 2. Then, we present the previous lattice-based key exchange protocols and multi-party key exchange protocols in Chapter 3 and 4, respectively. Then, we deal with the quantum key exchange protocols with the quantum computation in Chapter 5 and finally, we give a conclusion and future work in Chapter 6.

Chapter 2. Key Exchange and Authenticated Key Exchange

A key exchange protocol is a cryptographic primitive to establish the mutual session key for communication between two entities over an insecure channel. One of the first key exchange protocols appeared is called Diffie-Hellman key exchange by Diffie and Hellman. The purpose of Diffie-Hellman protocol is to enable two entities to securely exchange a session key which can then be used for next transmission. The idea of Diffie-Hellman protocol is to calculate a session key by communicating entities based on public parameters that are shared in the initial phase. Diffie-Hellman's security is based on the difficulty of discrete logarithm problem. However, the protocol can only be used for exchanging secret data without authenticating two parties. Thus, original Diffie-Hellman protocol is vulnerable to man-in-the-middle attacks.

One possible solution is to use digital signatures during the key exchange processing to provide authentication. An authenticated key exchange protocol is a key exchange protocol with authentication process to prevent attacks like the man-in-the-middle attack by providing mutual authentication between two entities.

Password-based Authenticated Key Exchange (PAKE) protocol assumes a more realistic scenario where secret keys are not uniformly distributed over a large space with a high-entropy, but chosen from a human-memorable set with a low-entropy. Passwords are normally easier to remember for users than cryptographically secure keys. Though, in the scenario that a user communicates with more than one user, he/she needs to remember all passwords between them. Thus, in this paper, we consider a three-party PAKE (3PAKE) protocol where user only shares a password with a trusted third party, e.g. a server.

PAKE protocol is beneficial for its simple use but is always vulnerable against the so-called dictionary attacks. In dictionary attacks, the adversary tries all possible combination of secret keys in a small set of values like dictionary, to break the security of a scheme. This attack is not very effective in the case of high-entropy keys but it becomes very damaging when the secret key is a password with low-entropy since the attacker has a non-negligible chance of finding the valid secret key.

Dictionary attacks are divided into two types: online and off-line dictionary attacks. To address this problem, several protocols are designed to be secure even when the secret key is a password. The goal of these protocols is to restrict the adversaries' success to on-line guessing attacks and prevent off-line dictionary attacks. The security of these systems relies on a policy invalidating or blocking the use of a password if a certain number of failed attempts has occurred.

In PAKE protocols, they are generally listed into two types as balanced PAKE and augmented PAKE. A balanced protocol assumes two party use the same password to authenticate a shared key for communication. This is generic for any communication, including client-server and client-client. On the other hand, an augmented one is more suitable to the client-server case, in which the server does not store password-equivalent data. This means that an attacker that stole the server data still cannot impersonate as the client unless they first perform a brute force search for the password.

The 3PAKE protocols are divided into two categories as implicit server authentication and explicit server authentication. A 3PAKE protocol with implicit server authentication can only have mutual authentication between two users, i.e., the server does not authenticate a user while executing the protocol. In contrast, a 3PAKE protocol with explicit server authentication must have mutual authentication between a server and users. Thus, a 3PAKE protocol with explicit server authentication normally has more complicated than the one with implicit server authentication

We consider the key exchange protocols from two perspectives: cost/efficiency and security. Cost/efficiency considers both processing and communication costs. Security means the protocol resistance to known attacks such as a key compromise impersonation attack, an ephemeral key compromise attack, a dictionary attack, etc.

Chapter 3. Previous Lattice-based Key Exchange

[DXL12] suggested the first lattice-based key exchange protocol in 2012. Following this research, numerous work studied key exchange and authenticated key exchange protocols based on Learning with Errors (LWE) problem and its variant.

[Pei14] gave efficient and practical lattice-based protocols for key transport and authenticated key exchange that are suitable as "drop-in" replacement for current Internet standards. [BCNS15] designed the more efficient protocol to be implemented in the TLS protocol and [NewHope] protocol improved the performance this protocol with higher security level.

[Frodo] protocol was suggested to remove the risk to have more structure in the hardness problem, ring structure in the case of lattice-based key exchange protocols. It was designed to rest its security on LWE problem instead of ring-LWE problem.

[ZZD+15] designed an authenticated key exchange based on lattice similar to the well-known HMQV protocol. [Kyber] protocol is yet another authenticated key exchange protocol recently proposed by Bos et al. This protocol is based on a variant of LWE problem called Module-LWE to enhance the performance and proves the security with the Quantum-accessible Random Oracle Model (QaROM) instead of classical Random Oracle Model (ROM).

There are only a small number of PAKE protocols based on lattice at the time of this research. One of these lattice-based PAKE protocols is that of Katz and Vaikuntanathan [KV09]. This protocol is proven secure in the standard model security, but it is not so efficient due to its Common Reference String (CRS)-based design. Recently, Zhang and Yu [ZY17] suggested a new CRS-based PAKE framework from public key encryption with associated approximate smooth projective hashing. But CRS-based protocols use complicated cryptographic tools to achieve standard-model security while ROM-based protocols have very simple and elegant designs. Compared to those CRS-based protocols like [KV09, ZY17], Ding et al.'s [DAL+17] suggested more efficient PAKE protocol based on ROM.

For more than two entities setting, Xu et al. [XHCC17] proposed the first lattice-based 3PAKE protocol with explicit server authentication, extending Ding et al.'s RLWE-PAK protocol and Choi et al. [CAK18] proposed the lattice-based 3PAKE protocol with implicit server authentication.

Chapter 4. Known Multi-party Key Exchange Protocol from Classical Setting

4-1. Three-party Key Exchange

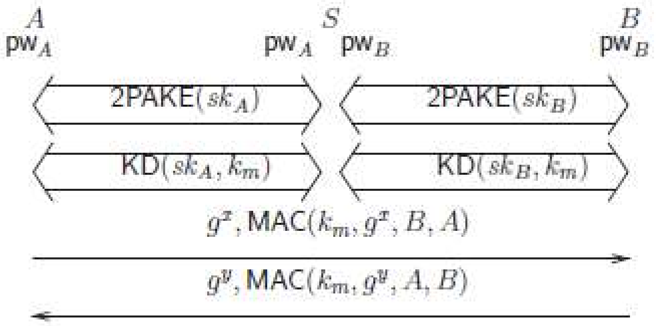
[Jou00] introduced a one-round three-party protocol for tripartite Diffie-Hellman using Weil and Tate pairings on elliptic curves. This protocol uses bilinear maps and the security is based on Decision Tate Diffie-Hellman (DTDH) problem: Given (P, aP, bP, cP) a quadruplet of elements from $\mathbb{G}_1$ and $\hat{t}(P,P)^d$ an element of $\mathbb{G}_2$ for random $a, b, c,$ and d, decide whether $d = abc$.

Figure. Relation between complexity assumptions

$$\begin{tikzcd}
 & & \mathrm{CDH}_{\mathbb{G}_1} \arrow[rr] \arrow[dr] & & \mathrm{DL}_{\mathbb{G}_1} \arrow[d] & \\
\mathrm{DTDH} \arrow[r] \arrow[dr] & \mathrm{TDH} \arrow[ur] \arrow[dr] & \mathrm{GTI} \arrow[r] & \mathrm{FTI} \arrow[r] & \mathrm{DL}_{\mathbb{G}_2} \arrow[r, leftrightarrow] & \mathrm{DL}_{\mathbb{G}_1} \text{ or } \mathrm{GTI} \\
 & \mathrm{DDH}_{\mathbb{G}_2} \arrow[r] & \mathrm{CDH}_{\mathbb{G}_2} \arrow[ur] & & &
\end{tikzcd}$$

Then, [AP03] proposes 4 kinds of three-party authenticated key exchange protocols in the random oracle model. The protocol is based on Bilinear DH (BDH) problem in random oracle model. This protocol assumes the attacker is both passive and active to provide perfect forward secrecy, implicit authentication, security against unknown key-share and key compromise impersonation attack, and session key security. But, this paper totally broken by [SW07] paper.

[AFP05] extends two-party PAKE protocol to three-party PAKE protocol in a natural generic construction, and prove the security using Real-OR-Random (ROR) model. Assuming that the adversary can perform both passive and active attacks, the security is given based on Decisional DH (DDH) problem with the TTP server.



[LC07] suggested S-3PAKE (simple three password-based key exchange) protocol based on Chosen-basis Computational DH (CCDH) problem. They show the security against on-line/off-line guessing attacks, replay attack and the protocol satisfies perfect forward secrecy and session key security. But, S-3PAKE protocol is broken by [CK08] paper. It demonstrates weakness of S-3PAKE protocol against impersonation attacks and man-in-the-middle attack. Then, they suggest its countermeasures.

[LH10] constructs two three-party authenticated key exchange such as implicit and explicit server authentication, with random oracle model. Compared to EKE (Encrypted Key Exchange) protocol [AP05] and S-3PAKE protocol [LC07], this protocol is more secure and efficient since it does not require server public keys. The security is based on DDH problem.

Protocol		Server auth.	Exponentiation	Mul/Div	Resistance	
					Undetectable online guessing	Offline guessing
S-3PAKE	Alice	Implicit	3	2	Insecure	Insecure
	Bob		3	2		
	Server		4	4		
S-IA-3PAKE	Alice	Implicit	3	3	Insecure	Secure
	Bob		3	3		
	Server		2	6		
LHL-3PAKE	Alice	explicit	3	0	Secure	Secure
	Bob		3	0		
	Server		4	0		
S-EA-3PAKE	Alice	explicit	3	3	Secure	Secure

[Shi12] proposes a round-optimal identity-based authenticated key agreement protocol with security proof using random oracle model. They consider fault detection and tolerance in the protocol. This protocol is secure against unknown key-share attack and key compromise impersonation attack. The security proof is based on BDH problem and Collusion Attack Algorithm with k-Traitor (k-CAA) problem. But, they did not consider insider attack in their original protocol and the attack is assumed to be passive.

4-2. Group Key Exchange

A group key exchange (GKE) protocol is a group key establishment protocol in which a shared secret is derived from two or more parties as a function of the information contributed by each of these. In GKE protocol, every group member has to interact in order to computer the group key and no entity can predetermine the resulting value. GKE protocol does not require the existence of secure channels between its participants since no secure transfer takes place during the processing.

In the paradigm of provable security, Bresson et al. [BCPQ01] suggested the first security model for GKE protocols with two major security notions. The first notion is authenticated key exchange (AKE) security which requires the indistinguishability of computed group keys from random keys and the second notion is mutual authentication (MA) security which means that two parties authenticates bilaterally.

[BCPQ01] defines a security model for cryptographic problems and AKE with implicit authentication in static setting. There are four types of queries for attackers: send, reveal, corrupt, and test queries. Then, [BCP01] provides the formal security model for dynamic-case authenticated group key exchange protocol and define AKE precisely with implicit authentication. The protocol is constructed as dynamic group DH protocol and the security is based on Group Computational DH (G-CDH) problem. The attack model is active where the attacker can setup, remove, join, send, reveal, corrupt, and test queries, however, the model does not capture "more serious" attacks yet.

[BCP02] defines a protocol for authenticated dynamic group DH with formal proofs. In this model, the attacker can generate concurrent membership changes (strong corruption). The security is based on Group DDH and Multi DDH, existence of PRF family in the standard model and it guarantees forward secrecy and implicit authentication.

[STW96] extends two-party Diffie-Hellman key exchange to group communications with three natural multi-party cases. The protocol has no a priori ordering of group members and no synchronization as well. Then, [STW98] proposes a protocol that considers the problem of key agreement in a group setting with highly-dynamic group member population. It supports dynamic group operations like adding and deleting group members. They consider two types of group key exchange protocols as centralized one and contributory one. [STW00] identifies requirements for initial key agreement (IKA) and auxiliary key agreement (AKA) operations and develops CLIQUE protocol. The security is based on n-party DDH. The protocol is easy to implement on dynamic groups but hard to manage when the number of group members is too large.

[AST00] studies the problem of authenticated group key exchange (AGKE) protocols in dynamic peer group with the emphasis on efficient and provably secure. They consider malicious insider seeking to alter the group membership by excluding some members. It satisfies key authentication, perfect forward secrecy, resistance to known-key attacks, key confirmation, and key integrity.

[KPT00] proposes the group key agreement by blending binary key trees with Diffie-Hellman key exchange, considering self-stabilization and fault-tolerance. This protocol is dynamic and the attacker model is passive guaranteeing group key secrecy, forward secrecy (not PFS), backward secrecy, and key independence. The security is based on DDH problem.

[KY03] proposes the first scalable protocol for AGKE in the standard model and presents a scalable compiler that transforms any GKE to be secure. The adversary is assumed to have full control over all communication in the network. Provable security is given based on DDH problem and static model. Protocol runs in a constant number of rounds and it only requires O(1) communication, 3 modular exponentiations, and O(n) signature verifications for each user.

[BC04] proposes a new constant-round group key exchange protocol that provides efficiency and privacy. It is secure based on DDH problem when the attacker has full control of the network.

[BD05] extends Diffie-Hellman protocol in a natural, scalable way without group manager, using the assumption of CDH and DDH problems. It has two rounds and the number of modular exponentiations per user is constant.

[CHL04] constructs scalable and 2-round protocols ID-authenticated GKA from well-known Burmester-Desmedt scheme [BD94]. The protocol has a group manager and it broadcasts but still, this protocol is a kind of contributory key agreement with forward secrecy and implicit authentication. The security is based on CDH and Decisional Bilinear DH (DBDH).

[KPT04] constructs Tree-based Group Diffie-Hellman (TGDH) key management solution which is a decentralized scheme with key trees. The protocol is dynamic and contributory. The protocol runs assuming PKI, perfectly balanced tree and there are five initial operations: join, leave, merge, partition, and key refresh. It provides fault-tolerance and robustness.

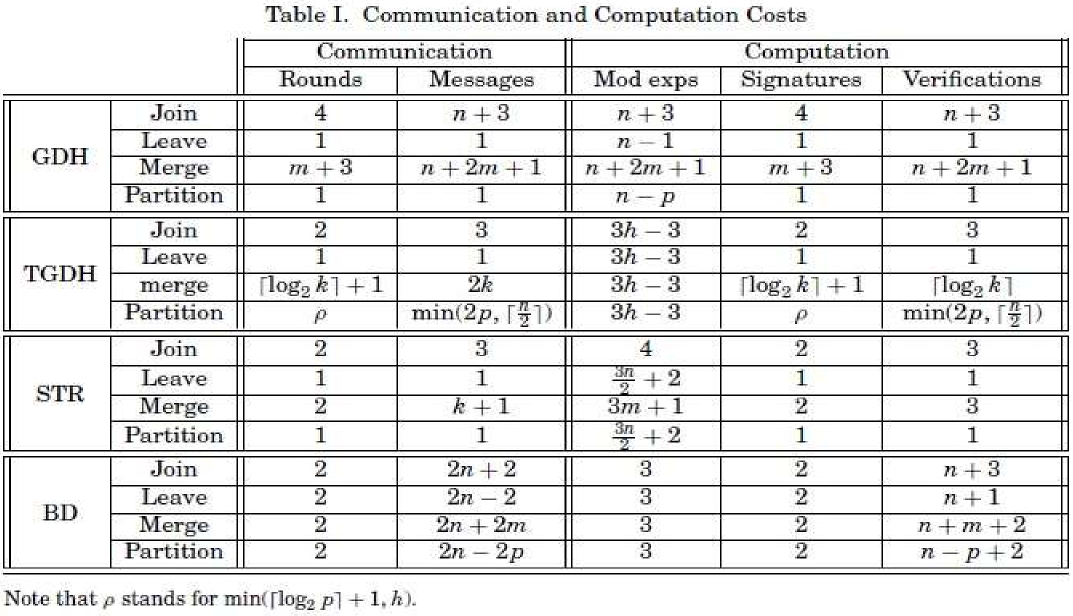


Table I. Communication and Computation Costs

		Communication		Computation		
		Rounds	Messages	Mod exps	Signatures	Verifications
GDH	Join	4	$n+3$	$n+3$	4	$n+3$
	Leave	1	1	$n-1$	1	1
	Merge	$m+3$	$n+2m+1$	$n+2m+1$	$m+3$	$n+2m+1$
	Partition	1	1	$n-p$	1	1
TGDH	Join	2	3	$3h-3$	2	3
	Leave	1	1	$3h-3$	1	1
	merge	$\lceil\log_2 k\rceil+1$	$2k$	$3h-3$	$\lceil\log_2 k\rceil+1$	$\lceil\log_2 k\rceil$
	Partition	ρ	$\min(2p, \lceil\frac{n}{2}\rceil)$	$3h-3$	ρ	$\min(2p, \lceil\frac{n}{2}\rceil)$
STR	Join	2	3	4	2	3
	Leave	1	1	$\frac{3n}{2}+2$	1	1
	Merge	2	$k+1$	$3m+1$	2	3
	Partition	1	1	$\frac{3n}{2}+2$	1	1
BD	Join	2	$2n+2$	3	2	$n+3$
	Leave	2	$2n-2$	3	2	$n+1$
	Merge	2	$2n+2m$	3	2	$n+m+2$
	Partition	2	$2n-2p$	3	2	$n-p+2$

Note that ρ stands for $\min(\lceil\log_2 p\rceil+1, h)$.

[DB08] constructs a protocol which is a variant of Burmester-Desmedt (BD) group key agreement protocol. It uses the ring structure for participants and detect the presence of the corrupted ring member. The security is based on DDH problem in the standard model and it guarantees the forward secrecy. But, it does not consider malicious insider attacks.

[ZWD+15] constructs round-efficient, sender-unrestricted, member-dynamic, and provably secure key escrow freeness identity-based authenticated asymmetric group key agreement (IBAAGKA) protocol. Their protocol is dynamic 1-round protocol and any user can access the encryption key. There exists a group manager in the protocol and the security of proposed scheme is given based on CDH problem and k-bilinear DH Exponent (k-BDHE) problem.

[TYM+16] constructs one-round attribute-based key exchange (OAKE) protocol in the multi-party setting using novel hybrid signcryption scheme and the generic multilinear maps. They construct this hybrid signcryption scheme from key-policy attribute-based encryption scheme and identity-based signature scheme. The security is based on k-multilinear DDH problem and CDH problem and it achieves the session key security for OAKE and existential unforgeability for hybrid signcryption scheme.

[YLL+17] proposes a new model for stAGKE to formulate security properties in particular for resistance to the leakage attacks on ephemeral key, without random oracles. It also suggests the new protocol built in a simple tree structure for efficiency in member join protocol execution.

4-3. MPKE from Indistinguishability Obfuscation

Indistinguishability obfuscation (iO) requires that given any two equivalent circuits C0 and C1 of similar size, the obfuscations of C0 and C1 should be computationally indistinguishable, while both circuit operates the same functionality. iO becomes the tremendous notion, powerful enough to give rise to almost any known cryptographic object.

[BZ17] shows how to use iO to build multi-party KE protocol in the standard model. It has no trusted setup and the size of published value is independent of the total number of users. In the processing, it runs a certain public obfuscated program on public values along with their secret seed and program outputs the group key. The protocol is secure in a semi-static model using punctured PRF technique by Sahai and Waters [SW] and full power of the constrained PRF by Boneh and Waters [BW]. Weaker security notion called static security can be achieved using only point-wise punctured PRF. It is necessary to fix an a priori bound on the number of participants as well as the number of corrupted parties.

After this work, several work on KE protocols using iO are suggested. Zhandry [Zha] suggested KE protocol from the weaker notion called witness PRF than iO and from extractable weak PRF, he shrink the size of the parameters.

Ananth et al. [] suggested that differing-inputs obfuscation (stronger notion of obfuscation) can shrink the parameter size of KE in [BZ17] paper.

[KRS15] gives how to shrink the parameter size of NIKE using standard iO, as well as other tools like fully homomorphic encryption. It is the first non-interactive key exchange protocol which supports an unbounded number of parties and have a security proof that does not rely on knowledge assumption. In the protocol, any party can derive a shared secret key for a group of which it is a member and parameters do not grow with the number of parties.

[KRS15] benefits from iO-friendly hashing called somewhere statistically binding (SSB) hash and parties can hash down an unbounded number of public values using some accumulator. The static security is proved.

Garg et al. [] shrinks the sizes using only iO and one-way functions and Hoffheinz et al. [] gives a strong adaptive notion in ROM.

Rao [Rao] suggests adaptively-secure one from new primitive called obliviously patchable puncturable PRFs but this is interactive assumption. It uses punctured PRF for static notion, and constrained PRF for circuit predicates to achieve semi-static notion

[XHZ15] presents the first one-round password-based GKE protocol in the common random string model and a new approach for two-round protocol without common random string. It is the first PAKE protocol without any trusted setup. As a building block, they use iO and Burmester-Desmedt protocol.

4-4. Other MPKE

[AG00] constructs a password-based multi-party key agreement protocol in ad hoc network. It uses unicast-based method and has log n rounds for whole processing. It has no TTP or PKI. Unicast means that one-to-one transmission from one point in the network to another point; that is, one sender and one receiver, each identified by a network address. This protocol guarantees forward secrecy and fault tolerance.

[JV96] examines KE protocols providing (1) key authentication, (2) key confirmation, and (3) forward secrecy. It provides the generalization of Burmester-Desmedt (BD) model for multi-party key agreement. It requires a trusted center for creating public key certificate for each user, but this can be done off-line, and the center is not required to maintain the secrecy of any information of any users. So, the protocol does not require the aid of an on-line or TTP when each entity has a copy of other public key a priori. The paper checks the security against active attacks and middleperson attacks

[BDS03] extends Joux's Protocol to Multi Party Key Agreement as unauthenticated one and authenticated one. Unauthenticated one uses ternary trees based on bilinear maps and authenticated one uses ternary trees based on pubic identities and key generation center. Security analysis is done against passive adversaries and the security is proven by reduction: when two or three underlying protocols are secure, multi-party version is also secure. The security is based on Decisional Hash Bilinear DH (DHBDH) problem. It guarantees implicit key authentication, known session key security, perfect forward secrecy, no key-compromise impersonation attack, no unknown key-share attack, and no key control. They also provides how to deal with the dynamic membership in their full paper.

[LLL04] suggests (n+1) different types of one round authenticated MPKE from multilinear forms and check their security for known session key security, perfect forward secrecy, no key-compromise impersonation, no unknown key-share, and no key control. The security is based on multilinear DH problem.

[SZH+17] constructs block-design-based key agreement protocol that supports multi-party and flexible, without TTP. The security is based on BDH problem assuming both passive and active attacker. It guarantees security for no key compromise impersonation attack, known session key security, and perfect forward security.

Chapter 5. Known Multi-party Key Exchange from Quantum Setting

Quantum key agreement (QKA) protocol is the key establishment technique whereby a classical shared secret key is derived by two or more specified entities fairly based on quantum mechanics principles. Theoretically, unconditional security is obtained from QKA by quantum mechanics principles. [ZZX04] proposed the first QKA protocol, which used the quantum teleportation technique to generate a secret key over public channels but it turns out it is not a fair QKA. Then, [CH10] proposed a QKA protocol based on the BB84 protocol using the technique of delayed measurement and the authenticated classical channel, but only two entities were involved.

For multi-party setting, [SZ13] suggests the first multi-party QKA protocol based on the correlation between Bell states and Bell measurements. The proposed protocols have lots of advantages such as fairness, efficiency, and security. Also, it is feasible to implement them with the present techniques but this protocol is not secure in the sense that the key can be totally determined by a dishonest participant alone.

[LGHW13] suggests the first secure multi-party QKA protocol using single particles. This protocol is secure against both outside and inside attacks. The proposed protocol satisfies two conditions: (1) outside eavesdroppers cannot gain the generated key without introducing any error and (2) the generated key cannot be determined by any non-trivial subset of the participants.

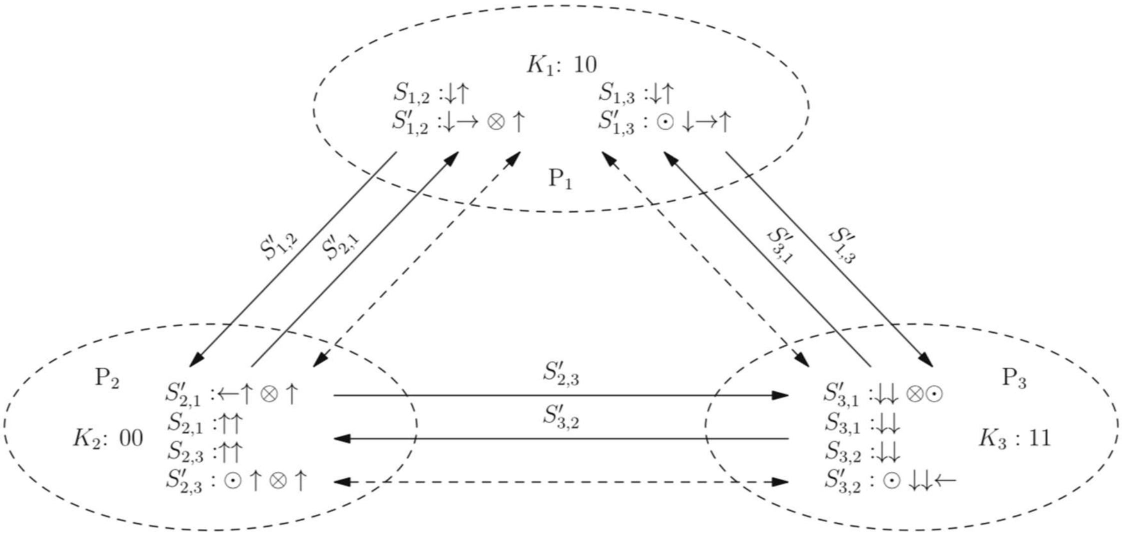


Fig. 1 The process of 3-party QKA protocol when $n = 2$ and $k = 1$. ↓ and ↑ represent the encoding states $|0\rangle$ and $|1\rangle$. ⊙, ⊗, →, ← represent the decoy states $|+\rangle$, $|-\rangle$, $|+y\rangle$, $|-y\rangle$. The *dashed arrows* represent the classical information exchange in detection stage

But particle efficiency of [LGHW13] is only 1/{(k+1)N(N-1)}. Then, [SZW+13] improves the efficiency to 1/{(k+1)N} and privacy.

[XWGQ14] multi-party QKA using Greenberger-Horne-Zeilinger (GHZ) states with better efficiency compared to the efficiency of [LGHW13]. The distributor of the GHZ states needs only one quantum communication with the other two parties, respectively, and everyone performs single-particle measurements simply. a. It is secure against outside attacks (measure-resend attack, intercept-replace attack, entangle-measure attack) and participant attacks.

[YML13] constructs three-party QKA with two-qubit entangled states, which can resist against both outsider and insider attacks. It is based on the idea of quantum dense coding on the four EPR pairs. The security of this protocol is considered under the condition of ideal quantum channels. Since noise cannot be disregarded in a practical transmission process, the success probability of quantum communication would be decreased in a noisy channel.

[SYW16] is a multi-party QKA extending the two-party QKA protocol with four-qubit cluster state. The qubit efficiency is improved as 1/N where N is the number of the participants by using the dense coding method. It is secure against both participant and outside attacks.

[SHW16] is a secure multi-party QKA based on commutative encryption. It is secure against both outsider and participant attacks but it cannot resist collusion attacks and it is not secure against insider attack [ME17]

[SZW+16] gives a multi-party QKA using maximally entangled six-qubit states, resistant to both outsider and insider attacks. The proposed protocol allows participants to share a secret key and preserves the following advantages. First, the outcome of the protocol is influenced by all parties. Second, it is fairness. And third, outside eavesdroppers cannot gain the generated key without introducing any error. [SSW17] is based on [SZW+16] and proposes a multi-party QKA resistant to collusion attacks, that is, the protocol resists t participants collaborating to predetermine the final key.

Chapter 6. Conclusion

In this paper, we survey lattice-based key exchange protocols and multi-party key exchange protocols in the literature. Key exchange protocol is the very important tool for secure communication in an insecure channel and it must be secure against all known attacks including quantum computing attacks.

As a future work, we investigate a possible way to build multi-party key exchange protocols with quantum resistance. One possible solution is that we use lattice-based key exchange protocol with two entities as a building block and construct some tree-like structure. We will consider all possible cryptographic ingredients like functional encryption, homomorphic encryption, and blockchain techniques.

References

[ABG+13] Prabhanjan Ananth, et al. "Differing-inputs obfuscation and applications." IACR Cryptology ePrint Archive, 2013/689, 2013.

[ADPS16][NewHope] Erdem Alkim, et al. "Post-quantum key exchange-a new hope." USENIX Security Symposium 2016, 2016.

[AFP05] Michel Abdalla, Pierre-Alain Fouque, and David Pointcheval. "Password-based authenticated key exchange in the three-party setting." International Workshop on Public Key Cryptography, pp. 65-84, 2005.

[AG00] N. Asokan and Philip Ginzboorg. "Key agreement in ad hoc networks." Computer Communications, 23(17), pp. 1627-1637, 2000.

[AP03] Sattam S. Al-Riyami and Kenneth G. Paterson. "Tripartite authenticated key agreement protocols from pairings." IMA International Conference on Cryptography and Coding, pp. 332-359, 2003.

[AP05] Michel Abdalla and David Pointcheval. "Simple password-based encrypted key exchange protocols." Cryptographers' track at the RSA conference, pp. 191-208, 2005.

[AST00] Giuseppe Ateniese, Michael Steiner, and Gene Tsudik. "New multiparty authentication services and key agreement protocols." IEEE Journal on Selected Areas in Communications, 18(4), pp. 628-639, 2000.

[BC04] Emmanuel Bresson and Dario Catalano. "Constant round authenticated group key agreement via distributed computation." International Workshop on Public Key Cryptography, pp. 115-129, 2004.

[BCD+16][Frodo] Joppe W. Bos, et al. "Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE." 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 1006-1018. 2016.

[BCNS15] Joppe W Bos, et al. "Post-quantum key exchange for the tls protocol from the ring learning with errors problem." 2015 IEEE Symposium on Security and Privacy (S&P), pp. 553-570, 2015.

[BCP01] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval.. "Provably authenticated group Diffie-Hellman key exchange – the dynamic case." ASIACRYPT 2001, pp. 290-309, 2001.

[BCP02] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. "Dynamic group Diffie-Hellman key exchange under standard assumptions." EUROCRYPT 2002, pp. 321-336, 2002.

[BCPQ01] Emmanuel Bresson, et al. "Provably authenticated group Diffie-Hellman key exchange." The 8th ACM Conference on Computer and Communications Security, pp. 255-264, 2001.

[BD94] Mike Burmester and Yvo Desmedt, "A secure and efficient conference key distribution system," EUROCRYPT 1994, pp. 275-286, 1994.

[BD05] Mike Burmester and Yvo Desmedt. "A secure and scalable group key exchange system." Information Processing Letters, 94(3), pp. 137-143, 2005.

[BDK+17][Kyber] Joppe W Bos, et al. "CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM." IACR Cryptology ePrint Archive, 2017/634, 2017.

[BDS03] Rana Barua, Ratna Dutta, and Palash Sarkar. "Extending Joux's protocol to multi party key agreement." International Conference on Cryptology in India – INDOCRYPT 2003, pp. 205-217, 2003.

[BW13] Dan Boneh and Brent Waters. "Constrained pseudorandom functions and their applications." ASIACRYPT 2013, pp. 280-300, 2013.

[BZ17] Dan Boneh and Mark Zhandry. "Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation." Algorithmica, 79(4), pp. 1233-1285, 2017.

[CAK18] Rakyong Choi, Hyeongcheol An, and Kwangjo Kim, "AtLast: Another Three-party Lattice-based PAKE Scheme", 2018 Symposium on Cryptography and Information Security, Session 2B1-3, 2018.

[CH10] Song-Kong Chong and Tzonelih Hwang. "Quantum key agreement protocol based on BB84." Optics Communications, 283(6), pp. 1192-1195, 2010.

[CHL04] Kyu Young Choi, Jung Yeon Hwang, and Dong Hoon Lee. "Efficient ID-based group key agreement with bilinear maps." International Workshop on Public Key Cryptography, pp. 130-144, 2004.

[CK08] Hao-Rung Chung and Wei-Chi Ku. "Three weaknesses in a simple three-party key exchange protocol." Information Sciences, 178(1), pp. 220-229, 2008.

[DAL+17] Jintai Ding, et al. "Provably secure password authenticated key exchange based on RLWE for the post-quantum world. Cryptographers' Track at the RSA Conference, pp. 183-204, 2017.

[DB08] Ratna Dutta and Rana Barua. "Provably secure constant round contributory group key agreement in dynamic setting." IEEE Transactions on Information Theory, 54(5), pp. 2007-2025, 2008.

[DXL12] Jintai Ding, Xiang Xie, and Xiaodong Lin. "A simple provably secure key exchange scheme based on the learning with errors problem. IACR Cryptology ePrint Archive, 2012/688, 2012.

[GPSZ17] Sanjam Garg, et al. "Breaking the sub-exponential barrier in obfustopia." EUROCRYPT 2017, pp. 156-181, 2017.

[HJK+16] Dennis Hofheinz, et al. "How to generate and use universal samplers." ASIACRYPT 2016, pp. 715-744, 2016.

[Jou00] Antoine Joux. "A one round protocol for tripartite Diffie-Hellman." International Algorithmic Number Theory Symposium, pp. 385-393, 2000.

[JV96] Mike Just and Serge Vaudenay. "Authenticated multi-party key agreement." ASIACRYPT 1996, pp. 36-49, 1996.

[KPT00] Yongdae Kim, Adrian Perrig, and Gene Tsudik. "Simple and fault-tolerant key agreement for dynamic collaborative groups." The 7th ACM Conference on Computer and Communications Security, pp. 235-244, 2000.

[KPT04] Yongdae Kim, Adrian Perrig, and Gene Tsudik. "Tree-based group key agreement." ACM Transactions on Information and System Security (TISSEC), 7(1), pp. 60-96, 2004.

[KRS15] Dakshita Khurana, Vanishree Rao, and Amit Sahai. "Multi-party key exchange for unbounded parties from indistinguishability obfuscation." ASIACRYPT 2015, pp. 52-75, 2015.

[KV09] Jonathan Katz and Vinod Vaikuntanathan. "Smooth projective hashing and password-based authenticated key exchange from lattices." ASIACRYPT 2009, pp. 636-652, 2009.

[KY03] Jonathan Katz and Moti Yung. "Scalable protocols for authenticated group key exchange." CRYPTO 2003, pp. 110-125, 2003.

[LC07] Rongxing Lu and Zhenfu Cao. "Simple three-party key exchange protocol." Computers & Security, 26(1), pp. 94-97, 2007.

[LGHW13] Bin Liu, et al. "Multiparty quantum key agreement with single particles." Quantum Information Processing, 12(4), pp. 1797-1805, 2013.

[LH10] Tian-Fu Lee and Tzonelih Hwang. "Simple password-based three-party authenticated key exchange without server public keys." Information Sciences, 180(9), pp. 1702-1714, 2010.

[LLL04] Young-Ran Lee, Hyang-Sook Lee, and Ho-Kyu Lee. "Multi-party authenticated key agreement protocols from multi-linear forms." Applied Mathematics and Computation, 159(2), pp. 317-331, 2004.

[ME17] Razieh Mohajer and Ziba Eslami. "Cryptanalysis of a multiparty quantum key agreement protocol based on commutative encryption." Quantum Information Processing, 16:197, 2017.

[Pei14] Chris Peikert. "Lattice cryptography for the internet." International Workshop on Post-Quantum Cryptography, pp. 197-219, 2014.

[Rao14] Vanishree Rao. "Adaptive Multiparty Non-interactive Key Exchange without Setup in the Standard Model." IACR Cryptology ePrint Archive 2014/910, 2014.

[Shi12] Kyung-Ah Shim. "A round-optimal three-party id-based authenticated key agreement protocol." Information Sciences, 186(1), pp. 239-248, 2012.

[SHW16] Zhiwei Sun, Jiwu Huang, and Ping Wang. "Efficient multiparty quantum key agreement protocol based on commutative encryption." Quantum Information Processing, 15(5), pp. 2101-2111, 2016.

[STW96] Michael Steiner, Gene Tsudik, and Michael Waidner. "Diffie-Hellman key distribution extended to group communication." The 3rd ACM Conference on Computer and Communications Security, pp. 31-37, 1996.

[STW98] Michael Steiner, Gene Tsudik, and Michael Waidner. "CLIQUES: A new approach to group key agreement." 18th International Conference on Distributed Computing Systems, pp. 380-387, 1998.

[STW00] Michael Steiner, Gene Tsudik, and Michael Waidner. "Key agreement in dynamic peer groups." IEEE Transactions on Parallel and Distributed Systems, 11(8), pp. 769-780, 2000.

[SW14] Amit Sahai and Brent Waters. "How to use indistinguishability obfuscation: deniable encryption, and more." The forty-sixth Annual ACM Symposium on Theory of Computing, pp. 475-484, 2014.

[SYW16] Zhiwei Sun, Jianping Yu, and Ping Wang. "Efficient multi-party quantum key agreement by cluster states." Quantum Information Processing, 15(1), pp. 373-384, 2016.

[SZ13] Run-Hua Shi and Hong Zhong. "Multi-party quantum key agreement with bell states and bell measurements." Quantum Information Processing, 12(2), pp. 921-932, 2013.

[SZH+17] Jian Shen, et al. "Block design-based key agreement for group data sharing in cloud computing." IEEE Transactions on Dependable and Secure Computing, (1), pp. 1-15, 2017.

[SZW+13] Zhiwei Sun, et al. "Improvements on "multiparty quantum key agreement with single particles"." Quantum Information Processing, 12(11), pp. 3411-3420, 2013.

[SZW+16] Zhiwei Sun, et al. "Multi-party quantum key agreement by an entangled six-qubit state." International Journal of Theoretical Physics, 55(3), pp. 1920-1929, 2016.

[TYM+16] Yangguang Tian, et al. "One-round attribute-based key exchange in the multi-party setting." International Conference on Provable Security, pp. 227-243, 2016.

[WSS17] Ping Wang, Zhiwei Sun, and Xiaoqiang Sun. "Multi-party quantum key agreement protocol secure against collusion attacks." Quantum Information Processing 16.7, 170, 2017.

[XHCC17] Dongqing Xu, et al. "Provably secure three-party password authenticated key exchange protocol based on ring learning with error." IACR Cryptology ePrint Archive, 2017/360, 2017.

[XHZ15] Jing Xu, Xue-Xian Hu, and Zhen-Feng Zhang. "Round-optimal password-based group key exchange protocols in the standard model." International Conference on Applied Cryptography and Network Security, pp. 42-61, 2015.

[XWGQ14] Guang-Bao Xu, et al. "Novel multiparty quantum key agreement protocol with GHZ states."

Quantum Information Processing, 13(12), pp. 2587-2594, 2014.

[YLL+17] Zheng Yang, et al. "A new strong security model for stateful authenticated group key exchange." International Journal of Information Security, pp. 1-18, 2017.

[YML13] Xun-Ru Yin, Wen-Ping Ma, and Wei-Yan Liu. "Three-party quantum key agreement with two-photon entanglement." International Journal of Theoretical Physics, 52(11), pp. 3915-3921, 2013.

[Zha16] Mark Zhandry. "How to avoid obfuscation using witness PRFs." Theory of Cryptography Conference, pp. 421-448, 2016.

[ZWDF+15] Lei Zhang, et al. "Round-efficient and sender-unrestricted dynamic group key agreement protocol for secure group communications." IEEE Transactions on Information Forensics and Security, 10(11), pp. 2352-2364, 2015.

[ZY17] Jiang Zhang and Yu Yu. "Two-round PAKE from approximate SPH and instantiations from lattices." ASIACRYPT 2017, pp. 37-67, 2017.

[ZZD+15] Jiang Zhang, et al. "Authenticated key exchange from ideal lattices." EUROCRYPT 2015, pp. 719-751, 2015.

[ZZX04] Nanrun Zhou, Guihua Zeng, and Jin Xiong. "Quantum key agreement protocol. Electronics Letters, 40(18), pp. 1149-1150, 2004.