ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

QUANTUM KEY DISTRIBUTION PROTOCOLS-A SECURED THREE-PARTY AUTHENTICATION ON COMMUNICATION NETWORKS

Mahalakshmi,pgscholar
A.Ramya, Assistant Professsor
Dept of CSE
Indra Ganesan College of Engg

ABSTRACT

Quantum key Distribution Protocols (QKDPs) to safeguard security in large networks, ushering in new directions in classical cryptography and quantum cryptography. Two three-party QKDPs, one with implicit user authentication and the other with explicit mutual authentication, are proposed to demonstrate the merits of the new combination, which include Security against such attacks as man-in-the-middle, eavesdropping and Replay attacks, Efficiency is improved as the proposed protocols contain the fewest number of communication rounds among existing QKDPs, Two parties can share and use a long-term secret (repeatedly).This work also presents a new primitive called the Unbiased-Chosen Basis (UCB) assumption which is used to prove the security of the proposed schemes. Quantum key distribution is a creation of secret keys from quantum mechanical correlations and is an example of how physical methods can be used to solve problems in classical information theory.

Index Terms— Communication security, key management, identity-based cryptography, asymmetric group key agreement.

I. INTRODUCTION

SECURE group communication is usually required in modern collaborative and distributed applications such as multi-party interactive computations, peer-to-peer file sharing and distributed social networks. A popular approach to secure group communications is to exploit group key agreement (GKA). Conventional GKA protocols allow a group of members to interact over an open network to establish a common secret key; thereafter, the group members can securely exchange messages using this shared key. This implies that, when a sender wants to send a secret message to a group of receivers, the sender has to first join the receivers to form a group and run a GKA protocol. This is inefficient since the sender may change frequently. We call this limitation of conventional GKA *sender restriction*. Further, with the standard round notion, the best-known GKA protocols require two or more rounds to establish a secret key.

Due to the above two limitations of conventional GKA protocols, they are ill-suited to scenarios like the following ones. *Scenario 1*. Two (or more) combat units would like to securely communicate with each other to coordinate their actions in different battlefields; any member of one unit may wish to report to the other unit. *Scenario 2*. A group of users in different time zones would like to discuss some sensitive topics via an untrusted third party, e.g., a social network service provider (such as Facebook). If conventional GKA is used in Scenario 1, each member of one unit has to first run the GKA protocol with the members of the other unit in a different battlefield. This is almost prohibitive given the poor communication environment in battle scenarios.

In Scenario 2, if a GKA protocol with two or more rounds is used, all users have to stay online to finish the protocol before they can receive any encrypted contents. This is difficult for users in different time zones. Motivated by the above observations, Wu *et al.* [20] introduced the notion of asymmetric group key agreement (AGKA) and proposed a concrete *one-round* AGKA protocol. Unlike conventional GKA, AGKA allows the members to negotiate a common group encryption key while holding different decryption keys. Any user may access the group encryption key and securely encrypt to the group members. Thus, AGKA is *sender-unrestricted*.

The original AGKA notion and the instantiated protocol were only intended for static groups and were only secure against passive attackers who just eavesdrop the open communications. In the real world, most group communication environments are dynamic, meaning that users can join or leave a group frequently. Further, security against passive attackers is not sufficient because realistic attackers may fully control open networks and launch powerful active attacks such as member impersonation, communication tampering, replay of early protocol transcripts, etc. [14], [16]. To resist active attacks, an authenticated AGKA protocol [21] for static groups has been proposed in the identity-based cryptosystem (IBC) setting [1]. In this IBC setting, a key generation center (KGC) is employed to generate the long-term private keys for the group members. With these private keys, the members can then securely establish a secure broadcast channel among them. The authenticated AGKA protocol in [21] achieves partial forward secrecy. That is, if only one or some specific group members' private keys are compromised, the secrets exchanged before the compromise stay unknown to the attacker. However, if all the group members' private keys are leaked, then the previously established secrets will be exposed to the attacker and the protocol is no longer secure. In practice, we do not know which members might be compromised after the protocol is deployed; in the worst case, all the members and even the KGC would be compromised. Obviously, since the KGC knows all the long-term private keys of the group members, it can always read the secrets. This is known as the key escrow problem. This observation motivates us to investigate authenticated AGKA protocols with stronger active security.

A. Problem Statement

The problem is how can the sender do this in an environment with the following constraints:

1) A fully trusted dealer to generate keys for the group members is not available;
2) It is hard to estimate who will send encrypted messages to the group members;
3) The system is key escrow free;
4) The group is dynamic, that is, a user may join or leave the group.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

It is worth noticing that broadcast encryption [9] may also perform a similar function to AGKA. However, in a broadcast encryption system, a trusted dealer is usually required to maintain the group. Even though some broadcast encryption systems are free from trusted dealers, they cannot offer forward secrecy and/or key escrow freeness [12].

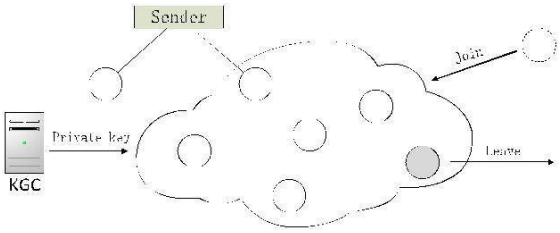

Fig. 1. Network model.

• Setup: The same as the BM.Setup in Section IV-C, except that an additional cryptographic hash function $H_5 : G_2 \longrightarrow \{0, 1\}^{l0}$ is chosen, where l_0 defines the bit-length of plaintexts. The system's parameter list is $\Upsilon = (q, G_1, G_2, e\hat{}, g, g_{pub}, H_1 \sim H_5, l_0)$.

- Extract: Each entity may request at most N private keys. Suppose the identity of an entity is I D_i new private key. Generally, a user will not join and leave the group with the same isid frequently. Therefore, N does not need to be large in most cases.
- Agreement: Assume the group size is n and the group manager is the t-th participant in the group. This protocol runs as follows.

TABLE I

MESSAGES REQUIRED BY THE *i* -th USER IN THE GROUP

$z_{1,i}$	ID_1, t_1, r_1, u_1
$z_{2,i}$	ID_2, t_2, r_2, u_2
$z_{3,i}$	ID_3, t_3, r_3, u_3
⋮	⋮
$z_{n,i}$	ID_n, t_n, r_n, u_n

- BM.Setup: On input a security parameter _, KGC chooses q, g, G_1, G_2, $e\hat{} : G_1 \times G_1 \longrightarrow G_2$ as defined in Section II-C; chooses $\kappa \in Z^*_q$ as the *master-secret* and sets $g_{pub} = g^{\kappa}$; chooses hash functions $H_1, H_2, H_3 : \{0, 1\}^* \longrightarrow G_1, H_4 : \{0, 1\}^* \longrightarrow Z^*_q$. The system parameter list is $\Upsilon = (q, G_1, G_2, e\hat{}, g, g_{pub}, H_1 \sim H_4)$.

TABLE II

MESSAGES RECEIVED BY THE GROUP MANAGER

∅	$z_{1,2}$	$z_{1,3}$	⋯	$z_{1,n}$	ID_1, t_1, r_1, u_1
$z_{2,1}$	∅	$z_{2,3}$	⋯	$z_{2,n}$	ID_2, t_2, r_2, u_2
$z_{3,1}$	$z_{3,2}$	∅	⋯	$z_{3,n}$	ID_3, t_3, r_3, u_3
⋮	⋮	⋮	⋱	⋮	⋮
$z_{n,1}$	$z_{n,2}$	$z_{n,3}$	⋯	∅	ID_n, t_n, r_n, u_n

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

Proof: Let C be a challenger and A be an adversary who can break the proposed protocol. Assume that, in each session, the group of participants is of size at most k.

C is given$(g, h, g_1, \ldots, g_k, g_{k+2}, \ldots, g_{2k})$ of the k-BDHE problem, where $g_i = g^{\alpha^i}$, $i \in \{1, \ldots, k, k+2, \ldots, 2k\}$. We show how C can use A to solve the k-BDHE problem.
In the sequel, only costly operations are considered and the operations that can be pre-computed are omitted.

Table III compares our dynamic protocol with the other protocols regarding transmission cost, where P_1, P_2, P_{ID}, P_m, P_{sig}, ι denote the binary length of an element in G_1, G_2, an identity, a message, an identity-based signature and the index of a user's private key, respectively. The table shows

TABLE III

TRANSMISSION OVERHEAD

Protocols	Agreement/Join/Leave	Ciphertext	Security
AGKA in [20]	$nP_1 + P_2$/static/static	$2P_1 + P_2$	unauthenticated
AGKA in [21], [23]	$nP_1 + P_{sig} + P_{ID}$/static/static	$2P_1 + P_m$	PFS
AGKA in [24]	$(n+1)P_1 + P_{ID}$/static/static	$2P_1 + P_m$	KEF§
Proposed protocol	$(n+1)P_1 + P_{ID} + \iota$	$2P_1 + P_m$	KEF

§: The formal security proof is not provided.

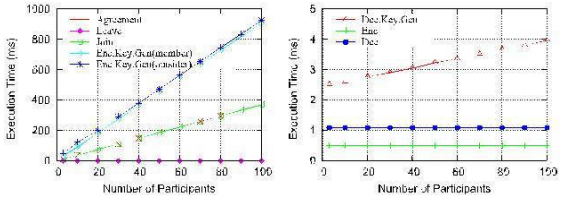

Fig. 2. Average execution time.

From this figure, we can see that the time costs for a outsider and a group member to generate a group encryption key are almost the same if pre-computation is not considered and higher than those of other stages. They grow linearly as the number of participants grows. However, the time costs are still not high. When the group size is 100, they are less than 1 second. We note that the efficiency of the Enc.Key.Gen stage will not significantly affect the efficiency

CONCLUSION

We have defined the security model for dynamicIBAAGKA protocols, in which an attacker is allowed to learn the master secret of the KGC. A one-round dynamic IBAAGKA protocol is proposed and proven secure in our model under the k-BDHE assumption. It offers secrecy and known-key security, and it does not suffer from the key
escrow problem. Therefore, not even the KGC can decrypt the ciphertexts sent to a group.

REFERENCES

[1] M. H. Au, J. K. Liu,W. Susilo, and J. Zhou, "Realizing fully secure unrestricted
ID-based ring signature in the standard model based on HIBE,"*IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1909–1922,
Dec. 2013.
[2] M. Bellare and P. Rogaway, "Entity authentication and key
distribution," in *Proc. 13th Annu. Int. Cryptol. Conf. (CRYPTO)*, 1994,pp. 232–249.
[3] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *Proc. 24th Annu.*
Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT), 2005,pp. 440–456.
[4] D. Boneh and A. Silverberg, "Applications of multilinear forms to cryptography," *Contemp. Math.*, vol. 324, no. 1, pp. 71–90,2002.
[5] M. Burmester and Y. Desmedt, "A secure and efficient conference key distribution system," in *Proc. Workshop Theory Appl. Cryptograph.*
Techn. (EUROCRYPT), 1995, pp. 275–286.
[6] L. Chen and C. Kudla, "Identity based authenticated key agreement protocols from pairings," in *Proc. 16th IEEE Comput. Security Found.Workshop (CSFW)*, Jun./Jul. 2003, pp. 219–233.
[7] L. Chen, Z. Cheng, and N. P. Smart, "Identity-based key agreement protocols from pairings," *Int. J. Inf. Security*, vol. 6, no. 4, pp. 213–241,2007.
[8] K. Y. Choi, J. Y. Hwang, and D. H. Lee, "Efficient ID-based group key agreement with bilinear maps," in *Proc. 7th Int. Workshop Theory Pract.Public Key Cryptography (PKC)*, 2004, pp. 130–144.
[9] A. Fiat and M. Naor, "Broadcast encryption," in *Proc. 13th Annu. Int.Cryptol. Conf. (CRYPTO)*, 1994, pp. 480–491.
[10] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," in *Proc. 19th Annu. Int. Cryptol.Conf. (CRYPTO)*, 1999, pp. 537–554.[11] S. Garg, C. Gentry, and S. Halevi, "Candidate multilinear maps
from ideal lattices and applications," in *Proc. 32nd Annu. Int.Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, 2013,pp. 1–17.
[12] C. Gentry and B. Waters, "Adaptive security in broadcast encryptionsystems (with short ciphertexts)," in *Proc. 28th Annu. Int. Conf. Theory*
Appl. Cryptograph. Techn. (EUROCRYPT), 2009, pp. 171–188.
[13] I. Ingemarsson, D. Tang, and C. K. Wong, "A conference key distribution system," *IEEE Trans. Inf. Theory*, vol. 28, no. 5, pp. 714–720,Sep. 1982.
[14] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement
over wireless fading channels," *IEEE Trans. Inf. Forensics Security*,vol. 7, no. 2, pp. 480–490, Apr. 2012.
[15] X. Lv, H. Li, and B. Wang, "Authenticated asymmetric group key
agreement based on certificateless cryptosystem," *Int.*