Universally Composable Attribute-based Group Key Exchange

Zenghui Zhao, Yunfang Hao

School of Intelligence Science and Information Engineering

Xi'an Peihua University, Xi’an, China

296883619@qq.com

Keywords: attribute-based group key exchange, universal composability, random oracle, encapsulation policy attribute-based key encapsulation mechanism, ACK property

Abstract: Several protocols implementing attribute-based group key exchange, which allows users with certain set of attributes to establish a session key, have been proposed in recent years. However, attacks on attribute-based group key exchange in current research have been considered only in stand-alone fashion. Thus these protocols may be vulnerable when run with other protocol sessions concurrently. We treat the security of attribute-based group key exchange in the universal composability framework to ensure that a protocol remains secure when run with arbitrary protocol sessions concurrently. More specifically, we define an ideal functionality for attribute-based group key exchange first, then propose a two-round protocol based on a primitive called encapsulation policy attribute-based key encapsulation mechanism. In addition, a complete security proof of our protocol in the universal composability framework under random oracle model is given.

1. Introduction

Recently, much attention has been attracted by attribute based cryptography (ABC). In ABC, an identity is a set of descriptive attributes instead of a single identity string. Attribute based encryption (ABE) has significant advantage over the traditional PKC primitives as it achieves flexible one to many encryption. Thus ABE provides means for decentralized access control in large and dynamic networks and ubiquitous computing environments without the need of administrating large access control policies. Additionally, ABC achieves better identity privacy preserving since members do not necessarily have to know the identity of the other members with whom they communicate with.

In spite of the advantage of ABE, it is much more convenient and efficient using symmetric-key encryption with a key obtained in a group key exchange (GKE) protocol than using ABE to implement secure group communication in popular group-oriented applications and protocols. To efficiently secure group communication in ABC, we consider a scenario where participants in a GKE aim at obtaining a common session key with partners having certain attributes. In such a scenario, only members whose attributes satisfy the given policy can participate in the GKE without disclosing their identities. Such a GKE protocol is called an attribute-based group key exchange (AB-GKE) protocol.

2. Preliminaries

In this section, we give a brief overview of EP-AB-KEM introduced in the UC framework, and ACK property in this section [1].

2.1 Encapsulation Policy Attribute-based Key Encapsulation Mechanism (EP-AB-KEM)

The EP-AB-KEM introduced by Gorantla et al. and used by our protocol follows the framework of ciphertext policy attribute based encryption (CP-ABE).

An EP-AB-KEM consists of five probabilistic polynomial time algorithm listed below.

(1) Setup: inputs system security parameter and attribute universe description, then outputs system public parameters PK and system master key MK.

(2) Encapsulation: inputs the system master key and a policy A over a set of attributes with the attribute universe U, outputs encapsulation C and a symmetric key SK. Only the user with attributes satisfying A can recover SK from C.

(3) KeyGen: inputs the system master key MK, system public parameters and a set of attributes S, outputs a private key pk for S.

(4) Decapsulation: inputs system public parameters, an encapsulation C, and a private key pk, if pk is the private key of a user with attributes satisfying a policy specified in the computation of encapsulation C outputs a symmetric key SK else outputs an error symbol $\perp$.

(5) Delegate: inputs system public parameters, a private key pk corresponding to a set of attributes S, and a set S*$\subseteq$S, outputs another private key pk* for S*. Delegate is an optional algorithm.

The security of EP-AB-KEM is a semantic security which ensures that any probabilistic polynomial time adversary can not distinguish the symmetric key SK generated in encapsulation algorithm and a random value in the probability distribution of the symmetric key. We refer to for more detail.

2.2 Universally Composable Framework

Canetti introduced the UC framework to design and analyze the security of cryptographic primitives and protocols [2]. In the UC framework, entities involved in the real execution of a protocol are a number of players, an adversary, and in addition an entity called the environment which represents everything outside of the protocol. In the ideal process of UC framework an ideal functionality of the protocol is defined and an adversary in the ideal process is introduced. Essentially, the ideal functionality is a trusted party that produces the desired functionality of the given protocol. Furthermore, the players in ideal process are replaced by dummy players, who do not communicate with each other but transfer messages between the ideal functionality and the environment.

Security is defined from the environment’s point of view such that no environment can distinguish the execution of the real protocol and a simulation in the ideal process. More precisely, a protocol securely realizes an ideal functionality if for any real execution adversary, there exists an ideal process adversary such that no environment, on any input, can distinguish whether it is interacting with the real execution adversary and players running the protocol, or with the ideal process adversary and the ideal functionality. We refer to for more detail.

2.3 ACK Property

The ACK property is first introduced by Canetti and Krawczyk to implement UC security of two-party key exchange protocols [3], and is generalized to group key exchange in [4]. Roughly speaking, a GKE protocol has the ACK property if by the time the first player outputs a session key and no player in the session is corrupted, the internal states of all players in the session can be simulated given the session key and messages exchanged among these players.

Consider an interaction among an environment machine, an adversary, a GKE protocol π, and an algorithm I. π runs with and; further more, has not corrupted any player when the first player output a session key. Then I is given the session key and messages exchanged among these players, and generates “simulated” internal state for each player in the protocol. Next, the internal state of each player is replaced with the “simulated” internal state for this player, and the interaction of and with π continues. I is called a good internal state simulator if no probabilistic polynomial time can distinguish between the above interaction with π and I and an interaction with π in the real execution.

Definition 1. (ACK property) Let π be a GKE protocol. π is said to have ACK property if there exists a good internal state simulator for π.

2.4 Divisible Computational Diffie-Hellman Problem and Divisible Computational Diffie-Hellman Assumption

Divisible computational Diffie-Hellman (DCDH) problem is a variation of CDH problem. Let q be a large prime number, G be a cyclic additive group of order q, and P be a generator of G.

DCDH problem: On input P, aP, and bP, where a,b∈Zq*, outputs (a/b)P.

DCDH assumption: There is no probabilistic polynomial time Turing machine solves the DCDH problem with non- negligible probability.

3. Universally Composable Attribute-based GKE

To formally define the notion of UC security for attribute-based group key exchange, we present an ideal functionality$\mathcal{F}_{\mathcal{AB}\text{-}\mathcal{GKE}}$ as follows.

Unlike traditional group key exchange functionality, $\mathcal{F}_{\mathcal{AB}\text{-}\mathcal{GKE}}$ checks whether attributes satisfies policy or not for each tuple (sid, number, policy, attributes, new-session). This ensures that only players whose attributes satisfy a given policy can participate in the protocol session. Furthermore, each player only knows the number of players in the session other than the identities of the players in initialization stage, so that the identity privacy is achieved.

Though our ideal functionality only handles a single protocol session, it is easy to use universal composition with joint state to obtain the mufti-session extension which handles multiple sessions of the protocol [5]. In addition, focusing on single-session protocols simplifies the definitions and the analysis.

Forward secrecy is the notion that corruption of a player should not reveal previous session keys generated by the player. To model forward secrecy, the adversary is not given the session key on corruption of a party if the key has already been delivered to the player in $\mathcal{F}_{\mathcal{AB}\text{-}\mathcal{GKE}}$.

4. Universally Composable secure AB-GKE protocol

This section shows our attribute-based group key exchange protocol followed with the security proof of the protocol. Our protocol is obtained by enhancing Gorantla et al.'s protocol and is composed of two rounds. Each player sends a message to all other players in each round. Our basic strategy is ensuring ACK property by adding a new round of message sending. The new message of each player contains an ephemeral key which is used to ensure the ACK property. Additionally, in order to prevent impersonation attack in the new round of message sending, each player add an "blind" ephemeral value in first message and prove himself a valid player in the protocol by combining this value in the second message.

Since identities of players keep undiscovered in AB-GKE, impersonation-resilient in AB-GKE only guarantees each player participates in the second round of message sending is indeed a player participates in the first round of message sending and each participant in the first round indeed participates in the second round of message sending.

4.1 Notations

The notations in the protocol are listed below.

k: system security parameter.

q: a large prime of k bits.

G1,G2: two groups of prime order q. G1 is an additive group.

e:G1×G1→G2: a bilinear map.

P: a generator of the group G1.

f1: {0, 1}*→G1 is a secure hash function that models a random oracle.

f2: {0, 1}*→Zq* is a collision-resistant hash function.

PK : the system public parameters of the EP-AB-KEM in the protocol.

A : the description of a policy.

pki : the private key of a player Ui in the EP-AB-KEM.

(Ci, SKi): the encapsulation pair obtained in encapsulation algorithm run by a player Ui.

4.2 Protocol Description

Let U={U1, U2,…，Un} be the set of players who wish to establish a group key. Before the protocol, the Setup algorithm of an EKP-AB-KEM is executed, and the KeyGen algorithm is executed for each player in the protocol, so that each Ui∈U obtains a private key pki for the EKP-AB-KEM. Unlike the protocol of Gorantla et al. ACK property by using of eki and αP and by erasing internal state before finishing round 2.

Before accepting the group key, each player Ui checks that whether the players who send messages in round 2 are indeed the players who send messages in round 1 and whether the ephemeral key held by other players are valid, so that any uncorrupted players in the same protocol session output the same group session key. Note that we do not take into account the case that the adversary who is a valid player in the protocol impersonates another valid player from the beginning, because identity privacy in ABC makes it impossible for a player to verify the identity of another player in a protocol session. All we can do is to guarantee the players who send messages in round 2 are indeed the players who send messages in round 1. Therefore we also assume broadcast messages sent by all players in round 1 are received by all players without being modified.

5. Conclusions

We focus on secure AB-GKE protocol in UC framework in this paper. After presenting an ideal functionality of AB-GKE in UC framework, we propose a two-round AB-GKE which securely realizes the functionality. Our protocol is constructed from any secure EP-AB-KEM scheme follows the framework of CP-ABE. According to the security analysis, our protocol is universally composable.

References

[1] M. Choudary Gorantla, Colin Boyd, and Juan Manuel Gonzalez Nieto. Attribute-based Authenticated Key Exchange. Proceedings of ACISP 2012, Sydney, Australia, July 2012.

[2] R. Canetti. Universally Composable Security: A New Paradigm for Cryptographic Protocols. Manuscript dated Jan. 28, 2013

[3] R. Canetti and H. Krawczyk. Universally Composable Notions of Key Exchange and Secure Channels. Proceedings of Eurocrypt 2012, Amsterdam, Holland, April 2012ol. 2332: 337–351.

[4] J. Katz, J. Shin. Modeling insider attacks on group key-exchange protocols. Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS’05), Alexandria, USA, 2014:180–189.

[5] R. Canetti and T. Rabin. Universal Composition with Joint State. Proceedings of Crypto 2013, LNCS, Vol. 2729, Springer-Verlag: 2013, 265–281.