ID-Based Group Password-Authenticated Key Exchange

Xun Yi[1], Raylin Tso[2], and Eiji Okamoto[2]

[1]School of Engineering and Science
Victoria University, Melbourne, Victoria 8001, Australia

[2] Department of Risk Engineering
University of Tsukuba, Tsukuba, Ibaraki, 305-8573, Japan

Abstract—Password-authenticated key exchange (PAKE) protocols are designed to be secure even when the secret key used for authentication is a human-memorable password. In this paper, we consider PAKE protocols in the group scenario, in which a group of clients, each of them shares a password with an "honest but curious" server, intend to establish a common secret key (i.e., a group key) with the help of the server. In this setting, the key established is known to the clients only and no one else, including the server. Each client needs to remember passwords only while the server keeps passwords in addition to private keys related to his identity. Towards our goal, we present a compiler that transforms any group key exchange (KE) protocol secure against a passive eavesdropping to a group PAKE which is secure against an active adversary who controls all communication in the network. This compiler is built on any group KE protocol (e.g., the Burmester-Desmedt protocol), any identity-based encryption (IBE) scheme (e.g., Gentry's scheme), and any identity-based signature (IBS) scheme (e.g., Paterson-Schuldt scheme). It adds only two rounds and $O(1)$ communication (per client) to the original group KE protocol. As long as the underlying group KE protocol, IBE scheme and an IBS scheme have provably security without random oracles, a group PAKE constructed by our compiler can be proven to be secure without random oracles.

Keywords: Group key agreement, protocol compiler, password-authenticated key exchange, common reference model.

1 Introduction

Popularity of group-oriented applications and protocols is currently on the increase and, as a result, group communication is taking place in many different settings, from network layer multicasting to application layer tele- and video-conferencing. Securing group communication makes demands of protocols for group authenticated key exchange (AKE), which allows a group of users communicating over an insecure public network to establish a common secret key (i.e., a group key) and furthermore to be guaranteed that they are indeed sharing this key with each other.

Protocols for 2-party AKE has been extensively investigated in [36, 15, 37, 13, 11, 32, 33, 34]. A number of works have considered extending the 2-party Diffie-Hellman protocol [36] to the multi-party setting [43, 57, 29, 58, 10, 50, 51]. Among them, the works of Ingemarsson et al. [43], Burmester and Desmedt [29], and Steiner et al. [58] may be the most well-known. They are merely key exchange (KE) protocols, intended to be secure against a passive adversary only.

However, AKE protocols aim to be secure against more powerful adversaries, who - in addition to eavesdropping - control all communication in the network. A number of initial protocols for group AKE were suggested in [44, 19, 7, 8, 59]. But none of these works have rigorous security proofs in a well-defined model.

Bresson et al. [22, 23, 24] were the first to define a formal model of security for group AKE and give the first provably secure protocols for this setting. Their model was built on the earlier work of Bellare and Rogaway in the two-party setting [12, 13, 11] and their protocols were based on the work of Steiner et al. [58], which requires $O(n)$ rounds to establish a key among n users, and therefore not scalable. A constant-round group AKE with a security proof in the random oracle model was given in [20], but it was shown to be insecure in [56]. Katz and Yung [48] were the first to give scalable protocol for group AKE along with a rigorous proof of security in the standard model. They also presented the first efficient compiler that transforms any group KE protocols secure against a passive eavesdropping to authenticated protocols by signing message flows. Their compiler adds only one round to the original protocol. However, this compiler requires each user to have a pair of public and private keys for digital signature. The (high-entropy) private key is not human-memorable and needs additional cryptographic devices to store it.

Bellovin and Merritt [14] were the first to consider AKE based on (low-entropy) password only and introduced a series of so-called "encrypted key exchange" (EKE) protocols for two-party AKE. A password-based AKE (i.e., PAKE) has to be immune to the dictionary attack, in which an adversary exhaustively tries all possible passwords from a dictionary in order to determine the correct one. Even though these attacks are not very effective in the case of high-entropy keys, they can be very damaging when the secret key is a password since the attacker has a non-negligible chance of winning. Dictionary attacks are usually divided into two categories: offline and online dictionary attacks. Formal models of security for two-party PAKE were firstly given independently by Bellare, Pointcheval and Rogaway [11], and Boyko, MacKenzie, Patel and Swaminathan [21] in 2000. Since then, protocols for two-party PAKE have been continuously proposed and proven to be secure in either the random oracle model (e.g.,[26, 27, 3, 4, 5]) or the standard model (e.g., [40, 46, 45]).

Bresson et al. [25, 28] were the first to adapt a group KE protocol to the password-based scenario. As the original protocol, the first group PAKE protocol was not scalable and practical for large groups. In addition, their security proof required ideal models. Recently, a number of constant-round group PAKE have been proposed in the literature by Abdalla et al. [2, 6], by Bohli et al. [16], and by Kim, Lee and Lee [49]. All of these constructions are built on the Burmester-Desmedt protocol [29, 31] and are rather efficient. Among them, the works of Abdalla et al. [6] and Bohli et al. [16] enjoy security proofs in the standard model.

Most of existing group PAKE protocols assume that users of a group share the same password, e.g., [25, 28, 2, 6]. In the scenarios where a user wants to participate in many groups, the number of passwords that he would need to remember would be linear in the number of possible groups. In order to limit the number of passwords that each user has to remember, a couple of group PAKE protocols assume that each user shares a password only with a server, which helps users of a group with establishment of a common secret key (i.e., a group key), e.g., [3, 4, 52]. The server is assumed to behave in an "honest but curious" manner. By the knowledge of passwords, the server may attempt to learn the group key. The setting with different passwords seems to be more practical in the real world than the setting with the same password.

More recently, Abdalla et al. [1] presented a protocol compiler that transforms any two-party

AKE into a group AKE with two more rounds of communication. Their idea is inspired by the construction of Burmester and Desmedt [29], where the trick of constructing a group key from pairwise agreed keys among users of a group was firstly introduced. In particular, applying this compiler to a two-party PAKE protocol yields a group PAKE protocol. The primary motivation of this compiler was the two-party setting. As implied in [48, 47], a compiler tailored from the group setting scales better than the compiler from two-party setting. This leads a question, is there any protocol compiler that transforms any group KE protocol directly to a group PAKE protocol?

Contribution. To the best of our knowledge, there has not yet been any protocol compiler that can transform any group KE protocol directly into a group PAKE protocol at present. In this paper, we present such a compiler on the basis of the "state-of-the-art" identity-based cryptosystem, a public-key cryptosystem in which an arbitrary string (e.g., user identity) can be used as the public key.

Our compiler employs any group KE protocol secure against passive eavesdropping, any IBE with chosen-ciphertext security and any IBS with existential unforgeability. We assume that clients of a group, each of them shares a password with an "honest but curious" server, intend to establish a common secret key (i.e., a group key) with the help of the server, where the key established is known to the clients only and no one else, including the server. For more details of the "honest but curious" server, we can refer to the work of Abdalla et al. in [3].

The **basic idea** of our compiler is that users of a group firstly run the group KE protocol to establish a group key without any help of the server, and then the server helps users of the group with mutual authentication and key confirmation by the shared password (protected with the IBE scheme), and finally each user authenticates the server, along with partnered users and the established key during the group KE, by the IBS scheme.

To analyze the security of our compiler, we put forth a formal model of security for ID-based PAKE in the group setting, by embedding Boneh et al.'s ID-based model [17][18] into the group PAKE model given by Bresson et al. in [25, 28] and improved by Abdalla et al. [1].

Our model assumes that all users and servers refer to the common public parameters including the public key of a private key generator (commonly used in ID-based model). Thus, our model is between the Halevi-Krawczyk model [42] (where each user needs to keep the public key of each server or to authenticate it with the public key of a certificate authority) and the Katz-Ostrovsky-Yung model [48] (where all users and servers refer the common public parameters only). Different from the Halevi-Krawczyk model, our model is ID-based, where the public key of a server is its identity (which is meaningful) and public key authentication is unnecessary. Thus, the Public Key Infrastructure (PKI) is not needed in our model. Similar to the Katz-Ostrovsky-Yung model, our model includes the public key of a private key generator in the common public parameters. Although the Katz-Ostrovsky-Yung model assumes that the public parameter generator uses random numbers as the public key of Cramer-Shoup cryptosystem [35], it can, in fact, chooses the private key at first and then computes the public key without being detected. Furthermore, provided with the public key in the common public parameters, if the corresponding private key is compromised, both the Katz-Ostrovsky-Yung protocol and our protocol have to reset.

We provide a rigorous proof of security for our compiler. Our compiler does not rely on the random oracle model as long as the underlying primitives themselves do not rely on it. By using Burmester-Desmedt group KE protocol [29], Gentry IBE scheme [39], Paterson-Schuldt IBS scheme [54], our compiler can construct a group PAKE with provably security in the standard

model.

Organization. In Section 2, we introduce a new model for ID-based group PAKE. In Section 3, we describe the underlying cryptographic primitives to build our group PAKE. Then, in Section 4, we present a new ID-based group PAKE compiler. After that, in Section 5, the brief security proof for our protocol is given. We conclude this paper in Section 6. In addition, the detail security proof is provided in Appendix.

2 Definitions

A formal model of security for group PAKE was firstly given by Bresson et al. in [25, 26] (based on Bellare et al.'s formal model for 2-party PAKE [12]), and improved by Abdalla et al. in [1]. Boneh and Franklin were the first to define chosen ciphertext security for IBE under chosen identity attack [17, 18]. In this section, we put forward a new model of security for ID-based group PAKE, on the basis of definitions given by Bresson et al., Abdalla et al. and Boneh et al.

Participants, Initialization and Passwords. An ID-based group PAKE protocol involves three kinds of participants: (1) A set of clients (denoted as Client); (2) A set of servers (denoted as Server), which behave in an honest but curious manner; (3) A Private Key Generator (PKG), which generates public parameters and corresponding private keys for servers, and behaves in an honest but curious manner as well. We assume that $\mathsf{ClientServerPair}$ is the set of pairs of the client and the server, who share a password. In addition, $\mathsf{User} = \mathsf{Client} \bigcup \mathsf{Server}$ and $\mathsf{Client} \bigcap \mathsf{Server} = \emptyset$.

Prior to any execution of the protocol, we assume that an initialization phase occurs. During initialization, PKG generates public parameters for the protocol, which are available to all participants, and issues private keys for each server. For any pair $(A, S) \in \mathsf{ClientServerPair}$, the client A and the server S are assumed to share the same password pw_A^S. We assume that the client A chooses pw_A^S independently and uniformly at random from a "dictionary" $\mathcal{D} = \{\mathsf{pw}_1, \mathsf{pw}_2, \cdots, \mathsf{pw}_N\}$ of size N, where N is a fixed constant which is independent of the security parameter. The password pw_A^S is then stored at the server S for authentication.

After initialization, a server can be still added to the system as long as it obtains its private key related to its identity from PKG. A client can join the system once he shares his password with a server.

Execution of the Protocol. In the real world, a protocol determines how users behave in response to input from their environments. In the formal model, these inputs are provided by the adversary. Each user is assumed to be able to execute the protocol multiple times (possibly concurrently) with different partners. This is modeled by allowing each user to have unlimited number of instances with which to execute the protocol. We denote instance i of user U as U^i. A given instance may be used only once. The adversary is given oracle access to these different instances. Furthermore, each instance maintains (local) state which is updated during the course of the experiment. In particular, each instance U^i has associated with it the following variables, initialized as NULL or FALSE (as appropriate) during the initialization phase.

- sid_U^i and pid_U^i are variables (initialized as NULL) denoting the session identity and partner identity for an instance, respectively. The session identity sid_U^i is simply a way to keep track of the different executions of a particular user U. The partner identity pid_U^i is the

set of users with whom U^i believes it is interacting to establish a session key (including U itself).

- acc_U^i and term_U^i are boolean variables (initialized as FLASE) denoting whether a given instance has been accepted or terminated, respectively. Termination means that the given instance has done receiving and sending messages, acceptance indicates successful termination. In our case, acceptance means that the instance is sure that a group key has been established, thus, when an instance U^i accepts, sid_U^i and pid_U^i are no longer NULL.

- used_U^i is a boolean variable (initialized as FLASE) denoting whether an instance has begun executing the protocol. This is a formalism which will ensure each instance is used only once.

- state_U^i (initialized as NULL) records any state necessary for execution of the protocol by a user instance U^i.

- sk_A^i is a variable (initialized as NULL) denoting the session key for a client instance A^i. Computation of the session key is, of course, the ultimate goal of the protocol. When A^i accepts (i.e., $\mathsf{acc}_A^i = \mathsf{TRUE}$), sk_A^i is no longer NULL.

The adversary $\mathcal{A}$ is assumed to have complete control over all communications in the network and the adversary's interaction with the users (more specifically, with various instances) or PKG is modeled via access to oracles which we describe now. The state of an instance may be updated during an oracle call, and the oracle's output may depend upon the relevant instance. The oracle types are as follows:

- $\mathsf{Execute}(A_1^{i_1}, A_2^{i_2}, \cdots, A_n^{i_n}, S^j)$ – If $A_\ell^{i_\ell}$ and S^j have not yet been used (where $A_\ell \in \mathsf{Client}$, $S \in \mathsf{Server}$, $(A_\ell, S) \in \mathsf{ClientServerPair}$, $\ell = 1, 2, \cdots, n$), this oracle executes the protocol among these instances and outputs the transcript of this execution. This oracle call represents passive eavesdropping of a protocol execution. In addition to the transcript, the adversary receives the values of sid, pid, acc, and term for all instances, at each step of protocol execution.

- $\mathsf{Send}(U^i, M)$ – This sends message M to instance U^i. Assuming $\mathsf{term}_U^i = \mathsf{FALSE}$, this instance runs according to the protocol specification, updating state as appropriate. The output of U^i (i.e., the message sent by the instance) is given to the adversary, who receives the updated values of $\mathsf{sid}_U^i, \mathsf{pid}_U^i, \mathsf{acc}_U^i$, and term_U^i. This oracle call models the active attack to a protocol.

- $\mathsf{KeyGen}(\mathsf{PKG}, S)$ – This sends the identity of the server S to PKG, which generates private keys $\mathsf{d_S}$ corresponding to S and forwards it to the adversary. This oracle models possible compromising of a server due to, for example, hacking into the server. This implies that all passwords stored in the server are disclosed.

- $\mathsf{Corrupt}(A)$ – This query allows the adversary to learn the passwords of the client A, which models the possibility of subverting a client by, for example, witnessing a user type in his password, or installing a "Trojan horse" on his machine. This implies that all passwords held by A are disclosed.

- $\mathsf{Reveal}(A^i)$ – This outputs the current value of session key sk_A^i for a client instance if $\mathsf{acc}_A^i = \mathsf{TRUE}$. This oracle call models possible leakage of session keys due to, for example, improper erasure of session keys after use, or cryptanalysis.

- $\mathsf{Test}(A^i)$ – This oracle does not model any real-world capability of the adversary, but is instead used to define security of the session key of client instance A^i. If $\mathsf{acc}_A^i = \mathsf{TRUE}$ and $\mathsf{sk}_A^i \neq \mathsf{NULL}$, a random bit b is generated. If $b = 0$, the adversary is given sk_A^i, and if $b = 1$ the adversary is given a random session key. The adversary is allowed a single Test query, at any time during its execution.

A passive adversary is given access to the Execute, KeyGen, Reveal, Corrupt, and Test oracles, while an active adversary is additionally given access to the Send oracles. We assume that all servers behave in a honest but curious manner. We can imagine a server as a passive adversary who have already queried a KeyGen oracle to retrieve the server's private keys and all passwords stored in it. In addition, we assume that all servers have no access to any form of Send oracles. In the definition of Execute and Send oracles, we reasonably require that $A_1, A_2, \cdots, A_n$ share different passwords with the same server S.

Partnering. We say that client instances A^i and B^j are partnered if there exists a server instance S^k associated with A^i and B^j such that (1) $\mathsf{pid}_A^i = \mathsf{pid}_B^j = \mathsf{pid}_S^k$ and (2) $\mathsf{sid}_A^i = \mathsf{sid}_B^j = \mathsf{sid}_S^k$. The notion of partnering will be fundamental in defining both correctness and security.

Correctness. To be viable, a key exchange protocol must satisfy the following notion of correctness: if A^i and B^j are partnered and $\mathsf{acc}_A^i = \mathsf{acc}_B^j = \mathsf{TRUE}$, then it must be the case that $\mathsf{sk}_A^i = \mathsf{sk}_B^j \neq \mathsf{NULL}$ (i.e., they conclude with the same session key).

Freshness. Informally, the adversary succeeds if it can guess the bit b used by a Test oracle. Before formally defining the adversary's success, we must first define a notion of freshness. A client instance A^i is fresh unless one of the following is true at the conclusion of the experiment, namely, at some point,

- The adversary queried $\mathsf{Reveal}(A^i)$ or $\mathsf{Reveal}(B^j)$ with the client instances A^i and B^j being partnered.

- The adversary queried $\mathsf{KeyGen}(\mathsf{PKG}, S)$ where the server instance $S \in \mathsf{pid}_A^i$, before a query of the form $\mathsf{Send}(U^\ell, M)$, where $U \in \mathsf{pid}_A^i$, has taken place, for some message M (or identities).

- The adversary queried $\mathsf{Corrupt}(A)$ or $\mathsf{Corrupt}(B)$ with the client instance A^i and B^j being partnered, before a query of the form $\mathsf{Send}(U^\ell, M)$, where $U \in \mathsf{pid}_A^i$, has taken place, for some message M (or identities).

Note that a client instance is fresh to a server or PKG adversary as long as the first event did not happen, because the server or PKG adversary has no access to any Send oracles and the last two events always happen.

The adversary is thought to succeed only if its Test query is made to a fresh instance. Note that this is necessary for any reasonable definition of security, otherwise, the adversary could always succeed, e.g., submitting a Test query for an instance for which it had already submitted a Reveal query. In addition, a server instance S^j is fresh if any client instance A^i such that $(A, S) \in \mathsf{ClientServerPair}$, $\mathsf{sid}_A^i = \mathsf{sid}_S^j$, and $\mathsf{pid}_A^i = \mathsf{pid}_S^j$, is fresh.

Advantage of the adversary. We say an adversary $\mathcal{A}$ succeeds if it makes a single query $\mathsf{Test}(A^i)$ to a fresh client instance A^i, with $\mathsf{acc}^i_A = \mathsf{TRUE}$ at the time of this query, and outputs a single bit b' with $b' = b$ (recall that b is the bit chosen by the Test oracle). We denote this event by Succ. The advantage of adversary $\mathcal{A}$ in attacking protocol P is a function in the security parameter k, defined as

$$\mathsf{Adv}^P_{\mathcal{A}}(k) = 2 \cdot \mathsf{Pr}^P_{\mathcal{A}}[\mathsf{Succ}] - 1$$

where the probability is taken over the random coins used by the adversary and the random coins used during the course of the experiment (including the initialization phase). It remains to define what we mean by a secure protocol. Note that a probabilistic polynomial-time (PPT) adversary can always succeed by trying all passwords one-by-one in an online impersonation attack. This is possible since the size of the password dictionary is constant. Informally, a protocol is secure if this is the best an adversary can do. Formally, an instance U^i represents an online attack if both the following are true at the time of the Test query: (1) at some point, the adversary queried $\mathsf{Send}(U^i, *)$, and (2) at some point, the adversary queried $\mathsf{Reveal}(A^j)$ or $\mathsf{Test}(A^j)$, where the client instance $A^j \in \mathsf{pid}^i_U$. In particular, instances with which the adversary interacts via $\mathsf{Execute}$, KeyGen, Reveal and $\mathsf{Corrupt}$ queries are not counted as online attacks. The number of online attacks represents a bound on the number of passwords the adversary could have tested in an online fashion.

Definition 1. Protocol P is a secure protocol for password-authenticated key exchange if, for all dictionary size N and for all PPT adversaries $\mathcal{A}$ making at most $Q(k)$ online attacks, there exists a negligible function $\varepsilon(\cdot)$ such that

$$\mathsf{Adv}^P_{\mathcal{A}}(k) \leq Q(k)/N + \varepsilon(k)$$

The above definition ensures that the adversary can (essentially) do no better than guess a single password during each online attack. Calls to the $\mathsf{Execute}$, KeyGen, Reveal and $\mathsf{Corrupt}$ oracles, which are not included in $Q(k)$, are of no help to the adversary in breaking the security of the protocol. This means the passive attacks and offline dictionary attacks are of no use.

Forward secrecy. We follow the definition of forward secrecy from [47, 1] and consider the weak corrupt model of [12], in which corrupting a client means retrieving his passwords, while asking KeyGen query on a server means retrieving its private keys and all passwords stored in it. Forward secrecy is then achieved if such queries do not give the adversary any information about previous agreed session keys. In addition, we follow the definition of freshness from [1]. The adversary is allowed to ask the Test query on a client instance, where he has known (1) the passwords of the client or any of his partners by $\mathsf{Corrupt}$ query; or (2) the private key of the server and all password stored in it by KeyGen query, however, he has not asked any Send query to the instance of the client or any of his partners. In this sense, the above definition of security implies forward secrecy.

Key privacy with respect to the server. The notion of key privacy respect to the server was introduced in [3] to capture the idea where the session key shared between two instances should only be known to these two instances and no one else, including the server, who behaves in an honest but curious manner. In our model, the server can be imagined as a passive adversary who has already queried a KeyGen oracle to retrieve the server's private keys and all passwords stored in it. On the basis of the above definition for forward secrecy, key privacy with respect to the server is implied in forward secrecy.

3 Cryptographic Building Blocks

3.1 Group Key Exchange

A group key exchange (KE) protocols allow users of a group communicating over an insecure public network to establish a common secret key (i.e., a group key), where the shared secret key is derived by two or more users as a function of the information contributed by, or associated with, each of these, (ideally) such that no user can predetermine the resulting key. They are intended to be secure against the passive adversary only. A passive adversary is given access to the Execute, Reveal, and Test oracles as defined in Section 2. In the definition of Execute oracle, we reasonably require that different executions yield different group session keys.

We say a passive adversary $\mathcal{A}$ succeeds if it makes a single query $\mathsf{Test}(A^i)$ to a fresh instance A^i (i.e., no Reveal oracle is queried to A^i and his partnered instances), and outputs a single bit b' with $b' = b$ (recall that b is the bit chosen by the Test oracle). We denote this event by Succ. The advantage of a passive adversary $\mathcal{A}$ in attacking a group KE protocol P is a function in the security parameter k, defined as $\mathsf{Adv}^P_{\mathcal{A}}(k) = 2 \cdot \mathsf{Pr}^P_{\mathcal{A}}[\mathsf{Succ}] - 1$.

A group KE protocol P is secure against passive eavesdropping if no polynomial bounded adversary $\mathcal{A}$ has a non-negligible advantage in attacking it.

The group KE protocols proposed by Ingemarsson et al. [43], Burmester and Desmedt [29], and Steiner et al. [58] may be the most well-known. Among them, Burmester-Desmedt protocol has been shown to be secure against passive eavesdropping in the standard model by Katz and Yung [48].

3.2 Identity-Based Encryption

An identity-based encryption (IBE) scheme is specified by four randomized algorithms: Setup, Extract, Encrypt, Decrypt as follows.

- Setup: On input a security parameter k, it returns params (public system parameters) and master-key (known only to the "Private Key Generator").
- Extract: On inputs params, master-key and a public identity $\mathsf{ID} \in \{0,1\}^*$, it returns a private key d.
- Encrypt: On inputs params, ID, and a message $M \in \mathcal{M}$ (the plaintext space), it returns a ciphertext $C \in \mathcal{C}$ (the ciphertext space).
- Decryption: On inputs params, $C \in \mathcal{C}$, and a private key d, it returns $M \in \mathcal{M}$.

Chosen ciphertext security is the standard acceptable notion of security for a public key encryption scheme. An IBE scheme is semantically secure against the adaptive chosen ciphertext attack if no polynomial bounded adversary $\mathcal{A}$ has a non-negligible advantage against the challenger in the following game:

- *Initialize*: The challenger runs the Setup algorithm, gives params to the adversary, but keeps the master-key to itself.
- *Phase* 1: The adversary adaptively asks a number of different queries $q_1, q_2, \cdots, q_m$, where q_i is either $\mathsf{Extract}(\mathsf{ID}_i)$ or $\mathsf{Decrypt}(\mathsf{ID}_i, C_i)$.

- *Challenge*: Once the adversary decides that Phase 1 is over, it outputs a pair of equal length plaintexts (M_0, M_1) and an identity ID on which it wishes to be challenged, where ID must not appear in Phase 1. The challenger picks a random bit $b \in \{0, 1\}$ and sends $C = \mathsf{Encrypt}(\mathsf{ID}, M_b)$ as the challenge to the adversary.

- *Phase* 2: The adversary issues more queries $q_{m+1}, q_{m+2}, \cdots, q_n$ adaptively as in Phase 1, except that the adversary may not request a private key for ID or the decryption of (ID, C).

- *Guess*: Finally, the adversary outputs a guess $b' \in \{0, 1\}$ and wins the game if $b' = b$.

We define the adversary $\mathcal{A}$'s advantage in attacking the IBE scheme as a function of the security parameter k, $\mathsf{Adv}^E_{\mathcal{A}}(k) = |\mathsf{Pr}^E_{\mathcal{A}}[b' = b] - 1/2|$, where the probability is over the random bits used by the challenger and the adversary. The most efficient identity-based encryption schemes are currently based on bilinear pairings on elliptic curves, such as the Weil or Tate pairings. Boneh and Franklin [17, 18] were the first to give an IBE scheme from Weil pairing and prove it to be adaptive chosen-ciphertext security in the random oracle model. More recently, several new IBE schemes from pairing (e.g., [60][39]) were proposed and proven to be adaptive chosen-ciphertext security in the standard model. A common feature of the latest IBE schemes is that the plaintext space is a cyclic group of prime order.

3.3 Identity-Based Signature

An identity-based signature (IBS) scheme can be described by four algorithms $\mathsf{Setup}, \mathsf{Extract}$, $\mathsf{Sign}, \mathsf{Verify}$ as follows.

- Setup: On input a security parameter k, it returns params (public system parameters) and $\mathsf{master\text{-}key}$ (known only to the "Private Key Generator").

- $\mathsf{Extract}$: Given $\mathsf{params}, \mathsf{master\text{-}key}$ and a public identity $\mathsf{ID} \in \{0, 1\}^*$, it returns a private key d_{ID}.

- Sign: Given a message M, $\mathsf{params}, \mathsf{ID}$ and a private key d_{ID}, it generates a signature σ of the user (with identity ID) on M.

- Verify: Given a signature σ, a message M, and $\mathsf{params}, \mathsf{ID}$, it outputs accept if σ is a valid signature of the user (with identity ID) on M, and outputs reject otherwise.

An IBS scheme is existential unforgeability under the chosen message attack [41] if no polynomial bounded adversary $\mathcal{A}$ has a non-negligible advantage against the challenger in the following game:

- *Initialize*: The challenger runs the Setup algorithm, gives params to the adversary, but keeps the $\mathsf{master\text{-}key}$ to itself.

- *Queries*: The adversary adaptively asks a number of different queries $q_1, q_2, \cdots, q_m$, where q_i is either $\mathsf{Extract}(\mathsf{ID}_i)$ or $\mathsf{Sign}(\mathsf{ID}_i, M)$.

- *Forgery*: Once the adversary decides that queries are over, it outputs a message M', an identity ID' and a string σ'. The adversary succeeds (denoted as Succ) if $\mathsf{Verify}(\mathsf{ID}', M', \sigma') = 1$, where ID' cannot appear in $\mathsf{Extract}$ queries and (ID', M') cannot appear in Sign queries.

We define the adversary $\mathcal{A}$'s advantage in attacking the IBS scheme as a function of the security parameter k, $\mathsf{Adv}^S_{\mathcal{A}}(k) = \mathsf{Pr}^S_{\mathcal{A}}[\mathsf{Succ}]$, where the probability is over the random bits used by the challenger and the adversary.

A generic approach to construct IBS schemes is to use an ordinary (i.e., non-identity-based) signature scheme and simply attach a certificate containing the public key of the signer to the signature [38]. An IBS scheme with provable security in the standard model was given by Paterson and Schuldt in [54].

3.4 Decisonal Squaring Diffie-Hellman Problem

The computational squaring Diffie-Hellman (CSDH) problem in a cyclic group G with a prime order q and a generator g is: Given g, g^a where a is randomly chosen from $\mathbb{Z}_q^*$, determine g^{a^2}. The problem is as hard as Diffie-Hellman problem [53, 30, 9].

The decisional squaring Diffie-Hellman (DSDH) problem in a cyclic group G with a prime order q and a generator g is to distinguish between two distributions (g, g^a, g^{a^2}) (dentoed as $b = 0$) and (g, g^a, z) (denoted as $b = 1$), where a is randomly chosen from $\mathbb{Z}_q^*$ and z is randomly chosen from G. This problem is not harder than the decisional DH problem, but we believe that this problem can still be hard, that is, we can assume that the advantage of any PPT algorithm $\mathcal{A}$ that outputs $b \in \{0, 1\}$ in solving the DSDH problem is negligible, namely,

$$|Pr[\mathcal{A}(g, g^a, g^{a^2}) = 0] - Pr[\mathcal{A}(g, g^a, z) = 0]|$$

is negligible, where the probability is over the random choice of a in $\mathbb{Z}_q^*$ and z in G, and the random bits consumed by $\mathcal{A}$.

4 An Efficient Compiler for Group PAKE

4.1 Description of the Compiler

In this section, we present an efficient compiler transforming any group KE protocol P to a group PAKE protocol P'.

Following the communication model given in [3], we assume that arbitrary point-to-point connections among clients and servers to be available. The network is non-private and fully asynchronous, that is, the adversary may delay, eavesdrop, insert and delete message at will.

Given a group KE protocol P, our compiler constructs a group PAKE protocol P' as shown in Fig. 1, in which n clients $A_1, A_2, \cdots, A_n$ (in lexicographic order) wish to establish a common authenticated secret key (i.e., a group key) with the help of a server S. A completely formal specification of the group PAKE protocol will appear in Section 5, where we give a brief proof of security for the protocol in the security model described in Section 2.

We present the protocol by describing initialization and execution. The cryptographic building blocks of our protocol include a group KE protocol, an IBE scheme and an IBS scheme. We let k be the security parameter given to the setup algorithm.

Initialization. Given a security parameter $k \in \mathbb{Z}^*$, the initialization includes:

Parameter Generation: On input k, (1) PKG runs Setup^P of the group KE protocol P to generate system parameters, denoted as params^P; (2) PKG runs Setup^E of the IBE scheme to generate public system parameters for the IBE scheme, denoted as params^E, and the secret $\mathsf{master\text{-}key}^E$

for itself; (3) PKG runs Setup^S of the IBS scheme to generate public system parameters for the IBS scheme, denoted as params^S, and the secret $\mathsf{master\text{-}key}^S$ for itself; In addition, PKG chooses a large cyclic group G with a prime order q and a generator g, and a hash function $H : \{0,1\}^* \to \mathcal{M}$ (where $\mathcal{M}$ is the plaintext space of IBE), from a collision-resistant hash family. The public system parameters for the protocol P' is $\mathsf{params} = \{H, G, q, g\} \bigcup \mathsf{params}^P \bigcup \mathsf{params}^E \bigcup \mathsf{params}^S$ and the secret ($\mathsf{master\text{-}key}^E$, $\mathsf{master\text{-}key}^S$) is known only to PKG.

Round 0 (Group Key Exchange (P))

Clients $A_\ell, \ell = 1, 2, \cdots, n$

$\mathsf{pid}_{A_\ell} \leftarrow (A_1, A_2, \cdots, A_n)$

$(\mathsf{sk}^P_{A_1}, \mathsf{sk}^P_{A_2}, \cdots, \mathsf{sk}^P_{A_n}) \leftarrow \mathsf{Execute}^P(A_1, A_2, \cdots, A_n)$

Round 1 (Client Authentication)

Client $A_\ell, \ell \in \{1, 2, \cdots, n\}$, $\mathsf{pid}_{A_\ell} \leftarrow \mathsf{pid}_{A_\ell} \cup \{S\}$, $\mathsf{sid}_{A_\ell} \leftarrow g^{\mathsf{sk}^P_{A_\ell}}$

$\mathsf{Auth}_\ell \leftarrow \mathsf{E}_{\mathsf{ID_S}}[H(\mathsf{sid}_{A_\ell}|\mathsf{pid}_{A_\ell}|\mathsf{pw}^S_{A_\ell})]$

$\{S\} \leftarrow \mathsf{msg}_{A_\ell} = A_\ell|\mathsf{sid}_{A_\ell}|\mathsf{Auth}_\ell$

Server S, $\mathsf{pid}_S \leftarrow (A_1, A_2, \cdots, A_n, S)$, $\mathsf{sid}_S \leftarrow \mathsf{sid}_{A_1}$

If $\exists \ell$ such that $\mathsf{D}_{\mathsf{d_S}}[\mathsf{Auth}_\ell] \neq H(\mathsf{sid}_S|\mathsf{pid}_S|\mathsf{pw}^S_{A_\ell})$, then return $\perp$

Round 2 (Server Authentication)

Server S

$\mathsf{Auth}_S \leftarrow \mathsf{S}_{\mathsf{d'_S}}[\mathsf{pid}_S|\mathsf{sid}_S]$

$\{A_1, A_2, \cdots, A_n\} \leftarrow \mathsf{msg}_S = S|\mathsf{Auth}_S$

Client $A_\ell, \ell = 1, 2, \cdots, n$

If $\mathsf{V}_{\mathsf{ID_S}}[\mathsf{pid}_{A_\ell}|\mathsf{sid}_{A_\ell}, \mathsf{Auth}_S] \neq 1$, then return $\perp$

Else $\mathsf{accept} \leftarrow \mathsf{TRUE}, \mathsf{sk}^{P'}_{A_\ell} \leftarrow g^{(\mathsf{sk}^P_{A_\ell})^2}$

Fig. 1. ID-based group PAKE protocol P'

Key Generation: On input the identity ID_S of a server $S \in \mathsf{Server}$, params, and ($\mathsf{master\text{-}key}^E$, $\mathsf{master\text{-}key}^S$), PKE runs $\mathsf{Extract}^E$ of the IBE scheme and sets the decryption key of S to be $\mathsf{d_S}$, and runs $\mathsf{Extract}^S$ of the IBS scheme and sets the signing key of S to be $\mathsf{d'_S}$.

Password Generation: On input $(A, S) \in \mathsf{ClientServerPair}$, a string pw^S_A, the password, is uniformly drawn by the client A from the dictionary $\mathsf{Password} = \{\mathsf{pw}_1, \mathsf{pw}_2, \cdots, \mathsf{pw}_N\}$, and then store it in the server S.

Protocol Execution. For a group of clients $A_1, A_2, \cdots, A_n$ (in lexicographic order), where there exists a server S such that $(A_\ell, S) \in \mathsf{ClientServerPair}$, when A_ℓ (having password $\mathsf{pw}^S_{A_\ell}$) ($\ell = 1, 2, \cdots, n$) agree to establish a common authenticated secret key (i.e., a group key) via S, they firstly run the group KE protocol P and each client A_ℓ computes the initial group key $\mathsf{sk}^P_{A_\ell}$. Note that the clients may not be authentic and the initial group key derived by different clients in the same session may not be equal. Mutual authentication and key confirmation run as follows.

Each client A_ℓ compute $\mathsf{sid}_{A_\ell} = g^{\mathsf{sk}^P_{A_\ell}}$ and an IBE encryption of $H(\mathsf{sid}_{A_\ell}|\mathsf{pid}_{A_\ell}|\mathsf{pw}^S_{A_\ell})$ based on the identity ID_S of the server, denoted as Auth_ℓ. Then $\mathsf{msg}_{A_\ell} = A_\ell|\mathsf{sid}_{A_\ell}|\mathsf{Auth}_\ell$ is submitted to the server S.

Upon receiving the messages msg_{A_ℓ} ($\ell = 1, 2, \cdots, n$), the server S lets $\mathsf{sid}_S = \mathsf{sid}_{A_1}$ and decrypts the ciphertexts with its decryption key $\mathsf{d_S}$, and verifies whether

$$\mathsf{D}_{\mathsf{d_S}}[\mathsf{Auth}_\ell] = H(\mathsf{sid}_S|\mathsf{pid}_S|\mathsf{pw}^S_{A_\ell}) \tag{1}$$

If equation (1) holds for $\ell = 1, 2, \cdots, n$, the server S uses its signing key $\mathsf{d'_S}$ to generate a signature $\mathsf{Auth}_S = \mathsf{S}_{\mathsf{d'_S}}[\mathsf{pid}_S|\mathsf{sid}_S]$, and then broadcasts $\mathsf{msg}_S = S|\mathsf{Auth}_S$.

Upon receiving $\mathsf{msg_S}$, each client A_ℓ checks if

$$\mathsf{V}_{\mathsf{ID_S}}[\mathsf{pid}_{A_\ell}|\mathsf{sid}_{A_\ell}, \mathsf{Auth}_S] = 1 \tag{2}$$

If equation (2) holds, A_ℓ computes $g^{(\mathsf{sk}^P_{A_\ell})^2}$ and accepts it as the authenticated group key $\mathsf{sk}^{P'}_{A_\ell}$.

4.2 Correctness, Explicit Authentication, Trust Model and Efficiency

Correctness. In the case where two clients A_i and A_j are partnered with $\mathsf{acc}_{A_i} = \mathsf{acc}_{A_j} = \mathsf{TRUE}$, the signature of the server on $\mathsf{pid}_{A_i}|\mathsf{sid}_{A_i} = \mathsf{pid}_{A_j}|\mathsf{sid}_{A_j} = \mathsf{pid}_S|\mathsf{sid}_S$ ensures that $\mathsf{pid}_{A_i} = \mathsf{pid}_{A_j}$ and $\mathsf{sid}_{A_i} = \mathsf{sid}_{A_j}$. Therefore, $g^{\mathsf{sk}^P_{A_i}} = g^{\mathsf{sk}^P_{A_j}}$ and further $\mathsf{sk}^P_{A_i} = \mathsf{sk}^P_{A_j} (mod\ q)$. This means, $g^{(\mathsf{sk}^P_{A_i})^2} = g^{(\mathsf{sk}^P_{A_j})^2}$, that is, $\mathsf{sk}^{P'}_{A_i} = \mathsf{sk}^{P'}_{A_j}$. Thus, our protocol meets correctness.

Explicit authentication. By verifying equation (1) which involves the password $\mathsf{pw}^S_{A_\ell}$, the partner identity pid_S and the initial group key $\mathsf{sk}^P_{A_\ell}$ for $\ell = 1, 2, \cdots, n$, the server S can make sure the authenticity of each client A_ℓ and the initial group key. By verifying equation (2) which involves the signature of the server, each client A_ℓ is convinced of the authenticity of the server S, other partners and the initial group key. If both equations (1) and (2) hold, all clients are legitimate, the initial group key is genuine and thus the final group key $g^{(\mathsf{sk}^P_{A_\ell})^2}$ is authentic. This shows that the group PAKE protocol P' achieves explicit authentication, that is, each client knows that its intended partners have successfully computed a matching session key (i.e, a group key).

Trust model. The protocol compiler for group PAKE given by Abdalla et al. [1] is applicable where each user of the group is honest. If two adjacent users are dishonest, they can conspire to include one (or several) impersonating attacker(s) between them, while other users are unaware of this attack. Our compiler assumes that there exist "honest but curious" servers, which are trusted to authenticate users of the group, but may perform passive attacks on the protocol to retrieve the group key. In terms of trust management, we believe that our compiler is more practical than Abdalla et al.'s compiler.

Efficiency consideration. The efficiency of our group PAKE protocol depends on performance of the underlying group KE protocol, IBE and IBS schemes. Only two rounds are added to the original group KE protocol P. In these two rounds, each client sends out one message and receives one message only. This compiler adds only $O(1)$ communication (per client) to the original group KE protocol. If our compiler employs Burmester-Desmedt group key exchange protocol, our group PAKE protocol has 4 rounds only. The communication cost of each client is $O(2n)$ bits, where n is the number of clients. If Abdalla et al.'s compiler employs KOY 2-PAKE protocol [46] and constructs the commitment scheme with Cramer-Shoup public key encryption

scheme [35], their group PAKE protocol has 5 rounds. The communication cost of each user is $O(6n)$ bits. In this sense, we believe that our compiler is more efficient than Abdalla et al.'s compiler. Note that we take into account cryptographic blocks with provably security in the standard model only.

5 Proof of Security

We follow the methods of the security proofs given in [48, 46] to prove the security of our compiler without random oracles. First of all, we provide a formal specification of the group PAKE protocol by specifying the initialization phase and the oracles to which the adversary has access, as shown in Fig. 2−4.

During the initialization phase for security parameter k, algorithm $\mathsf{Initialize}$ generates $\mathsf{params} = \{G, q, g, H\} \bigcup \mathsf{params}^P \bigcup \mathsf{params}^E \bigcup \mathsf{params}^S$ and the secret $(\mathsf{master\text{-}key}^E, \mathsf{master\text{-}key}^S)$ at first. Furthermore, the sets Client, Server, $\mathsf{ClientServerPair}$ are determined. Passwords for clients are chosen at random, and then stored at corresponding servers.

$\mathsf{Initialize}(1^k)$
$(\mathsf{params}^{P,E,S}, \mathsf{master\text{-}key}^{E,S}) \xleftarrow{R} \mathsf{Setup}^{P,E,S}(1^k)$
$(\mathsf{Client}, \mathsf{Server}, \mathsf{ClientServerPair}) \xleftarrow{R} \mathsf{UserGen}(1^k), (G, q, g) \xleftarrow{R} \mathsf{GGen}(1^k), H \xleftarrow{R} \mathsf{CRHF}(1^k)$
For each $i \in \{1, 2, \cdots\}$ and each $U \in \mathsf{User}$
$\mathsf{acc}_U^i \leftarrow \mathsf{term}_U^i \leftarrow \mathsf{used}_U^i \leftarrow \mathsf{FALSE}, \mathsf{sid}_U^i \leftarrow \mathsf{pid}_U^i \leftarrow \mathsf{sk}_U^i \leftarrow \mathsf{NULL}$
For each $S \in \mathsf{Server}$, $\mathsf{d_S}, \mathsf{d'_S} \leftarrow \mathsf{Extract}^{E,S}(\mathsf{ID}_S, \mathsf{params}^{E,S}, \mathsf{master\text{-}key}^{E,S})$
For each $(A, S) \in \mathsf{ClientServerPair}, \mathsf{pw}_A^S \xleftarrow{R} \{\mathsf{pw}_1, \mathsf{pw}_2, \cdots, \mathsf{pw}_N\}$
Return $\mathsf{Client}, \mathsf{Server}, \mathsf{ClientServerPair}, G, q, g, H, \mathsf{params}^{P,E,S}$

Fig. 2. Specification of the initialize

$\mathsf{Execute}(A_1^{i_1}, \cdots, A_n^{i_n}, S^j)$, where $A_\ell \in \mathsf{Client}, S \in \mathsf{Server}$
If $(\exists \ell$ such that $(A_\ell, S) \notin \mathsf{ClientServerPair} \vee \mathsf{used}_{A_\ell}^{i_\ell}) \vee \mathsf{used}_S^j$, return $\perp$
$\mathsf{used}_{A_\ell}^{i_\ell} \leftarrow \mathsf{used}_S^j \leftarrow \mathsf{TRUE}, \mathsf{pid}_{A_\ell}^{i_\ell} \leftarrow \mathsf{pid}_S^j \leftarrow \{A_1, \cdots, A_n, S\}, \ell = 1, 2, \cdots, n$
$(\mathsf{sk}_{A_1}^P, \mathsf{sk}_{A_2}^P, \cdots, \mathsf{sk}_{A_n}^P) \leftarrow \mathsf{Execute}^P(A_1^{i_1}, A_2^{i_2}, \cdots, A_n^{i_n})$
$\mathsf{sid}_{A_\ell}^{i_\ell} \leftarrow g^{\mathsf{sk}_{A_\ell}^P}, \mathsf{Auth}_\ell \leftarrow \mathsf{E}_{\mathsf{ID_S}}[H(\mathsf{sid}_{A_\ell}^{i_\ell} | \mathsf{pid}_{A_\ell}^{i_\ell} | \mathsf{pw}_{A_\ell}^S)], \mathsf{msg}_{A_\ell} \leftarrow A_\ell | \mathsf{sid}_{A_\ell}^{i_\ell} | \mathsf{Auth}_\ell, \ell = 1, 2, \cdots, n$
$\mathsf{sid}_S^j \leftarrow \mathsf{sid}_{A_1}^{i_1}, \mathsf{Auth}_S \leftarrow \mathsf{S}_{\mathsf{d'_S}}[\mathsf{pid}_S^j | \mathsf{sid}_S^j], \mathsf{msg}_S \leftarrow S | \mathsf{Auth}_S$
$\mathsf{acc}_{A_\ell}^{i_\ell} \leftarrow \mathsf{term}_{A_\ell}^{i_\ell} \leftarrow \mathsf{acc}_S^j \leftarrow \mathsf{term}_S^j \leftarrow \mathsf{TRUE}, \mathsf{sk}_{A_\ell}^{i_\ell} \leftarrow g^{(\mathsf{sk}_{A_\ell}^P)^2}, \ell = 1, 2, \cdots, n$
Return $\mathsf{status}_{A_1}^{i_1}, \cdots, \mathsf{status}_{A_n}^{i_n}, \mathsf{status}_S^j$

$\mathsf{KeyGen}(\mathsf{PKG}, S)$
Return $\mathsf{d_S}, \mathsf{d'_S}$ and pw_A^S for any A

$\mathsf{Corrupt}(A)$
Return pw_A^S for any S

$\mathsf{Reveal}(A^i)$
Return sk_A^i

$\mathsf{Test}(A^i)$
$b \xleftarrow{R} \{0, 1\}, \mathsf{sk'} \xleftarrow{R} \Omega$. If $b = 1$ return $\mathsf{sk'}$ else return sk_A^i

Fig. 3. Specification of the Execute, KeyGen, Corrupt, Reveal, Test oracles

$\mathsf{Send}_0(A_\ell^{i_\ell}, (A_1^{i_1}, \cdots, A_n^{i_n}))$

If $\mathsf{used}_{A_\ell}^{i_\ell}$, return $\perp$

$\mathsf{used}_{A_\ell}^{i_\ell} \leftarrow \mathsf{TRUE}$

. . . . . .

$\mathsf{Send}'_0(A_\ell^{i_\ell}, S^j)$

If $\neg\mathsf{used}_{A_\ell}^{i_\ell} \vee (A_\ell, S) \notin \mathsf{ClientServerPair} \vee \mathsf{term}_{A_\ell}^{i_\ell}$, return $\perp$

$\mathsf{pid}_{A_\ell}^{i_\ell} \leftarrow \{A_1, \cdots, A_n, S\}, \mathsf{sid}_{A_\ell}^{i_\ell} \leftarrow g^{\mathsf{sk}_{A_\ell}^P}, \mathsf{Auth}_\ell \leftarrow \mathsf{E}_{\mathsf{ID}_\mathsf{S}}[H(\mathsf{sid}_{A_\ell}^{i_\ell}|\mathsf{pid}_{A_\ell}^{i_\ell}|\mathsf{pw}_{A_\ell}^S)]$

$\mathsf{MsgOut} \leftarrow A_\ell|\mathsf{sid}_{A_\ell}^{i_\ell}|\mathsf{Auth}_\ell, \mathsf{state}_{A_\ell}^{i_\ell} \leftarrow (\mathsf{pid}_{A_\ell}^{i_\ell}, \mathsf{sk}_{A_\ell}^P, \mathsf{MsgOut})$

Return $\mathsf{status}_{A_\ell}^{i_\ell}$

$\mathsf{Send}'_1(S^j, (A_\ell^{i_\ell}|\mathsf{sid}_{A_\ell}^{i_\ell}|\mathsf{Auth}_\ell)_{\ell=1,2,\cdots,n})$

If ($\exists\ell$ such that $(A_\ell, S) \notin \mathsf{ClientServerPair}$) $\vee\ \mathsf{used}_S^j$, return $\perp$

$\mathsf{used}_S^j \leftarrow \mathsf{TRUE}, \mathsf{pid}_S^j \leftarrow \{A_1, A_2, \cdots, A_n, S\}, \mathsf{sid}_S^j \leftarrow \mathsf{sid}_{A_1}^{i_1}$

If $\exists\ell$ such that $\mathsf{D}_{\mathsf{d}_\mathsf{S}}[\mathsf{Auth}_\ell] \neq H(\mathsf{sid}_S^j|\mathsf{pid}_S^j|\mathsf{pw}_{A_\ell}^S)$, reject and return status_S^j

$\mathsf{Auth}_S \leftarrow \mathsf{S}_{\mathsf{d}'_\mathsf{S}}[\mathsf{pid}_S^j|\mathsf{sid}_S^j], \mathsf{acc}_S^j \leftarrow \mathsf{term}_S^j \leftarrow \mathsf{TRUE}, \mathsf{MsgOut} \leftarrow S|\mathsf{Auth}_S$

Return status_S^j

$\mathsf{Send}'_2(A_\ell^{i_\ell}, S^j|\mathsf{Auth}_S)$

$\mathsf{state}_{A_\ell}^{i_\ell} \leftarrow (\mathsf{pid}_{A_\ell}^{i_\ell}, \mathsf{sk}_{A_\ell}^P, \mathsf{FirstMsgOut})$

If $\neg\mathsf{used}_{A_\ell}^{i_\ell} \vee \mathsf{term}_{A_\ell}^{i_\ell} \vee (S \notin \mathsf{pid}_{A_\ell}^{i_\ell})$, return $\perp$

If $\mathsf{V}_{\mathsf{ID}_\mathsf{S}}[\mathsf{pid}_{A_\ell}^{i_\ell}|\mathsf{sid}_{A_\ell}^{i_\ell}, \mathsf{Auth}_S] \neq 1$, reject and return $\mathsf{status}_{A_\ell}^{i_\ell}$

$\mathsf{acc}_{A_\ell}^{i_\ell} \leftarrow \mathsf{term}_{A_\ell}^{i_\ell} \leftarrow \mathsf{TRUE}, \mathsf{sk}_{A_\ell}^{i_\ell} \leftarrow g^{(\mathsf{sk}_{A_\ell}^P)^2}$

Return $\mathsf{status}_{A_\ell}^{i_\ell}$

Fig. 4. Specification of the Send oracles

The description of the Execute oracle matches the high-level protocol described in Fig. 1, but additional details (for example, the updating of state information) are included. We let status_U^i denote the vector of values $(\mathsf{sid}_U^i, \mathsf{pid}_U^i, \mathsf{acc}_U^i, \mathsf{term}_U^i)$ associated with instance U^i. Given an adversary $\mathcal{A}$, we imagine a simulator that runs the protocol for $\mathcal{A}$. More preciously, the simulator begins by running algorithm $\mathsf{Initialize}(1^k)$ (which includes choosing passwords for clients) and giving the public output of the algorithm to $\mathcal{A}$. When $\mathcal{A}$ queries an oracle, the simulator also responds by executing the appropriate algorithm. The simulator also records all state information defined during the course of the experiment.

In particular, when the adversary completes its execution and outputs a bit b', the simulator can tell whether the adversary succeeds by checking whether (1) a single Test query was made, for some client instance U^i; (2) acc_U^i was true at the time of Test query; (3) instance U^i is fresh; and (4) $b' = b$. Success of the adversary is denoted by event Succ. For any experiment P' we define

$$\mathsf{Adv}_\mathcal{A}^{P'}(k) = 2 \cdot \mathsf{Pr}_\mathcal{A}^{P'}[\mathsf{Succ}] - 1$$

Based on the model described in Section 2, we have

Theorem 1. Assume that (1) the group KE protocol is secure against passive eavesdropping; (2) the IBE scheme is secure against the chosen-ciphertext attack; (3) the IBS scheme is existential unforgeability under the chosen-message attack; (4) the decisional squaring Diffie-Hellman (DSDH) problem is hard over a cyclic group G with a prime order q and a generator g; (5) CRHF is a collision-resistant hash family; then the protocol P' described in Fig. 1 is a secure group PAKE protocol.

The detail proof of Theorem 1 is provided in Appendix.

6 Conclusion

In this paper, we present an efficient compiler to transform any group KE protocol to a group PAKE protocol from identity-based cryptosystem. In addition, we provide a rigorous proof of security for our compiler. As long as our group PAKE protocol is built on a group KE protocol, and IBE and IBS schemes with provable security without random oracles, it can be proven to be secure without random oracles.

References

[1] M. Abdalla, J. M. Bohli, M. I. G. Vasco, R. Steinwandt. (Password) authenticated key establishment: From 2-party to group. In *Proc. TCC'07*, pages 499-514, 2007.

[2] M. Abdalla, E. Bresson, O. Chevassut, and D. Pointcheval. Password-based group key exchange in a constant number of rounds. In *Proc. PKC'06*, pages 427-442, 2006.

[3] M. Abdalla, P. A. Fouque, and D. Pointcheval. Password-based authenticated key exchange in the three-party setting. In *Proc. PKC'05*, pages 65-84, Jan. 2005.

[4] M. Abdalla, P. A. Fouque, and D. Pointcheval. Password-based authenticated key exchange in the three-party setting. *IEE Proceedings in Information Security*, 153(1): 27-39, Mar. 2006.

[5] M. Abdalla and D. Pointcheval. Simple password-based encrypted key exchange protocols. In *Proc. CT-RSA 2005*, pages 191 - 208, Feb. 2005.

[6] M. Abdalla and D. Pointcheval. A scalable password-based group key exchange in the standard model. In *Proc. Asiacrypt'06*, pages 332-347, 2006.

[7] G. Ateniese, M. Steiner, and G. Tsudik. Authenticated group key agreement and friends. In *Proc. CCS'98*, pages 17-26, 1998.

[8] G. Ateniese, M. Steiner, and G. Tsudik. New multi-party authentication services and key agreement protocol. *IEEE Journal on Selected Areas in Communications*, (18)4: 628-639, 2000.

[9] F. Bao, R. H. Deng and H. Zhu. Variations of Diffie-Hellman problem. In *Proc. ICICS'03*, pages 301-312, 2003.

[10] C. Becker and U. Wille. Communication complexity of group key distribution. In *Proc. CCS'98*, pages 1-6, 1998.

[11] M. Bellare, R. Canetti, and H. Krawczyk. A modular approach to the design and analysis of authentication and key exchange protocol. In *Proc. 30th Annual ACM Symposium on Theory of Computing*, pages 419-428, 1998.

[12] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In *Proc. Eurocrypt'00*, pages 139-155, May 2000.

[13] M. Bellare and P. Rogaway. Entity authentication and key distribution. In *Proc. Crypto'93*, pages 232-249, 1993.

[14] S. M. Bellovin and M. Merritt. Encrypted key exchange: Password-based protocol secure against dictionary attack. In *Proc. 1992 IEEE Symposium on Research in Security and Privacy*, pages 72-84, May 1992.

[15] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, and M. Yung. Systematic design of two-party authentication protocols. *IEEE Journal on Selected Areas in Communications*, 11(5): 679-693, 1993.

[16] J. M. Bohli, M. I. G. Vasco, and R. Steinwandt. Password-authenticated constant-round group key establishment with a common reference string. Cryptology ePrint Archive, Report 2006/214, 2006. http://eprint.iacr.org/.

[17] D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. In *Proc. Crypto'01*, pages 213-229, 2001.

[18] D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. *SIAM Journal of Computing*, 32(3):586-615, 2003.

[19] C. Boyd. On key agreement and conference key agreement. In *Proc. ACISP'97*, pages 294-302, 1997.

[20] C. Boyd and J. M. G. Nieto. Round-optimal contributory conference key agreement. In *Proc. PKC'03*, pages 161-174, 2003.

[21] V. Boyko, P. Mackenzie, and S. Patel. Provably secure password-authenticated key exchange using Diffie-Hellman. In *Proc. Eurocrypt'00*, pages 156-171, May 2000.

[22] E. Bresson, O. Chevassut, and D. Pointcheval. Provably authenticated group Diffie-Hellman key exchange - the dynamic case. In *Proc. Asiacrypt'01*, pages 290-309, 2001.

[23] E. Bresson, O. Chevassut, D. Pointcheval, and J. J. Quisquater. Provably authenticated group Diffie-Hellman key exchange. In *Proc. CCS'01*, pages 255-264, 2001.

[24] E. Bresson, O. Chevassut, and D. Pointcheval. Dynamic group Diffie-Hellman key exchange under standard assumptions. In *Proc. Eurocrypt'02*, pages 321-336, 2002.

[25] E. Bresson, O. Chevassut, and D. Pointcheval. Group Diffie-Hellman key exchange secure against dictionary attack. In *Proc. Asiacrypt'02*, pages 497-514, 2002.

[26] E. Bresson, O. Chevassut, and D. Pointcheval. Security proofs for an efficient password-based key exchange. In *Proc. CCS'03*, pages 241-250, 2003.

[27] E. Bresson, O. Chevassut, and D. Pointcheval. New security results on encrypted key exchange. In *Proc. PKC'04*, pages 145-158, 2004.

[28] E. Bresson, O. Chevassut, and D. Pointcheval. A security solution for IEEE 802.11s ad-hoc mode: password-authentication and group-Diffie-Hellman key exchange. *International Journal of Wireless and Mobile Computing*, 2(1): 4-13, 2007.

[29] M. Burmester and Y. Desmedt. A secure and efficient conference key distribution system. In *Proc. Eurocrypt'94*, pages 275-286, 1995.

[30] M. Burmester, Y. Desmedt, J. Seberry. Equitable key escrow with limited time span. In *Proc. Asiacrypt'98*, pages 380-391, 1998.

[31] M. Burmester and Y. Desmedt. A secure and scalable group key exchange system. *Information Processing Letters*, 94(3): 137-143, 2005.

[32] R. Canetti and H. Krawczyk. Key-exchange protocols and their use for building secure channels. In *Proc. Eurocrypt'01*, pages 453-474, 2001.

[33] R. Canetti and H. Krawczyk. Universally composable notions of key exchange and secure channels. In *Proc. Eurocrypt'02*, pages 337-351, 2002.

[34] R. Canetti and H. Krawczyk. Security analysis of IKE's signature-based key-exchange protocol. In *Proc. Crypto'02*, pages 143-161, 2002.

[35] R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *Proc. Crypto'98*, pages 13-25, 1998.

[36] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 32(2): 644-654, 1976.

[37] W. Diffie, P. van Oorschot and M. Wiener. Authentication and authenticated key exchange. *Designs, Codes, and Cryptography*, 2(2): 107-125, 1992.

[38] D. Galindo, J. Herranz and E. Kiltz. On the generic construction of identity-based signatures with additional properties. In *Proc. Asiacrypt'06*, pages 178-193, 2006.

[39] C. Gentry. Practical identity-based encryption without random oracle. In *Proc. Eurocrypt'06*, pages 445-464, 2006.

[40] O. Goldreich and Y. Lindell. Session-key generation using human passwords only. In *Proc. Crypto'01*, pages 408-432, 2001.

[41] S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen-message attack. *SIAM J. Computing*, 17(2): 281-308, 1988.

[42] S. Halevi and H. Krawczyk. Public-key cryptography and password protocols. *ACM Transactions on Information and System Security*, 2(3):230–268, 1999.

[43] I. Ingemarsson, D. T. Tang, and C. K. Wong. A conference key distribution system. *IEEE Transactions on Information Theory*, 28(5): 714-720, 1982.

[44] M. Just and S. Vaudenay. Authenticated multi-party key agreement. In *Proc. Asiacrypt'96*, pages 36-49, 1996.

[45] S. Jiang and G. Gong. Password based key exchange with mutual authentication. In *Proc. Selected Areas in Cryptography'04*, pages 267-279, 2004.

[46] J. Katz, R. Ostrovsky, and M. Yung. Efficient password-authenticated key exchange using human-memorable passwords. In *Proc. Eurocrypt'01*, pages 457-494, 2001.

[47] J. Katz, R. Ostrovsky, and M. Yung. Forward secrecy in password-only key exchange protocols. In *Proc. 3rd International Conference on Security in Communication Networks (SCN'03)*, pages 29-44, 2003.

[48] J. Katz and M. Yung. Scalable protocols for authenticated group key exchange. In *Proc. Crypt0'03*, pages 110-125, 2003.

[49] H. J. Kim, S. M. Lee, and D. H. Lee. Constant-round authenticated group key exchange for dynamic groups. In *Proc. Asiacrypt'04*, pages 245-259, 2004.

[50] Y. Kim, A. Perig, and G. Tsudik. Simper and fault-tolerant key agreement for dynamic collaborative groups. In *Proc. CCS'00*, pages 235-244, 2000.

[51] Y. Kim, A. Perrig, and G. Tsudik. Communication-efficient group key agreement. In *Proc. IFIP TC11 16th Annual Working Conference on Information Security (IFIP/SEC)*, pages 229-244, 2001.

[52] J. O. Kown, I. R. Jeong, K. Sakurai and D. H. Lee. Password-authenticated multi-party key exchange with different passwords. Cryptology ePrint Archive, Report 2006/476, http://eprint.iacr.org.

[53] U. M. Maurer and S. Wolf, Diffie-Hellman oracles. In *Proc. Crypto'96*, pages 268-282, 1996.

[54] K. G. Paterson and J. C. N. Schuldt. Efficient identity-based signatures secure in the standard model. In *Proc. ACISP'06*, pages 207-222, 2006.

[55] S. Patel. Number-theoretic attack on secure password scheme. In *Proc. IEEE Symposium on Research in Security and Privacy*, pages 236-247, 1997.

[56] K. R. Choo, C. Boyd, and Y. Hitchcock. Errors in computational complexity proofs for protocols. In *Proc. Asiacrypt'05*, pages 624-643, 2005.

[57] D. Steer, L. Strawczynski, W. Diffie and M. Wiener. A secure audio teleconference system. In *Proc. Crypto'98*, pages 520-528, 1998.

[58] M. Steiner, G. Tsudik, and M. Widner. Key agreement in dynamic peer groups. *IEEE Transactions on Parallel and Distributed Systems*, 11(8): 769-780, 2000.

[59] W. G. Tzeng. A practical and secure fault-tolerant conference key agreement protocol. In *Proc. PKC'00*, pages 1-13, 2000.

[60] B. Waters. Efficient identity-based encryption without random oracles. In *Proc. Eurocrypt'05*, pages 114-127, 2005.

Appendix: Proof of Theorem 1

We begin with some terminology that will be used throughout the proof. A given message is called oracle-generated if it was output by the simulator in response to some oracle query. The message is said to be adversarially-generated otherwise. **An adversarially-generated message must not be the same as any oracle-generated message.**

We refer to the real execution of the experiment, as described above, as P'_0. We will introduce a sequence of transformations to the experiment P'_0 and bound the effect of each transformation on the adversary's advantage. We then bound the adversary's advantage in the final experiment. This immediately yields a bound on the adversary's advantage in the original experiment.

Experiment P'_1: In this experiment, the simulator interacts with the adversary as before except that the adversary does not succeed, and the experiment is aborted, if any of the following occur:

1. At any point during the experiment, an oracle-generated message (e.g., msg_{A_ℓ} or msg_S) is repeated.

2. At any point during the experiment, a collision occurs in the hash function H (regardless of whether this is due to a direct action of the adversary, or whether this occurs during the course of the simulator's response to an oracle query).

It is immediate that events 1 occurs with only negligible probability, event 2 occurs with negligible probability assuming CRHF as a collision-resistant hash family. Put everything together, we are able to see that

Claim 1. If CRHF is a collision-resistant hash family, $|\mathsf{Adv}_{\mathcal{A}}^{P'_0}(k) - \mathsf{Adv}_{\mathcal{A}}^{P'_1}(k)|$ is negligible.

Experiment P'_2: In this experiment, the simulator interacts with the adversary $\mathcal{A}$ as in experiment P'_1 except that the adversary's queries to $\mathsf{Execute}$ oracles are handled differently: for any $\mathsf{Execute}(A_1^{i_1}, \cdots, A_n^{i_n}, S^j)$ oracle where the adversary has not queried $\mathsf{Reveal}(A_\ell^{i_\ell})$ $(\ell = 1, 2, \cdots, n)$ in the end of experiment P'_1, the initial group key $\mathsf{sk}_{A_\ell}^P$ $(\ell = 1, 2, \cdots, n)$ established during the group key exchange protocol P are replaced with a random value from an appropriate set.

The difference between the current experiment and the previous one is bounded by the probability that an adversary breaks the security of the group key exchange protocol P. More precisely, we have

Claim 2. If the group key exchange protocol P is secure against passive eavesdropping, $|\mathsf{Adv}_{\mathcal{A}}^{P'_1}(k) - \mathsf{Adv}_{\mathcal{A}}^{P'_2}(k)|$ is negligible.

Assume that there are m such $\mathsf{Execute}$ queries in the end of experiment P'_1, the claim is proved by m sub-experiments $P_2'^{(1)}, \cdots, P_2'^{(m)} = P'_2$, in each of which only one such $\mathsf{Execute}$ is handled differently. Let $P_2'^{(0)} = P'_1$, we only need to prove $|\mathsf{Adv}_{\mathcal{A}}^{P_2'^{(t-1)}}(k) - \mathsf{Adv}_{\mathcal{A}}^{P_2'^{(t)}}(k)|$ (where $1 \leq t \leq m$) to be negligible.

If $|\mathsf{Adv}_{\mathcal{A}}^{P_2'^{(t-1)}}(k) - \mathsf{Adv}_{\mathcal{A}}^{P_2'^{(t)}}(k)|$ is non-negligible, where $P_2'^{(t)}$ is for $\mathsf{Execute}(A_1^{i_1}, \cdots, A_n^{i_n}, S^j)$, we show that the simulator can use $\mathcal{A}$ as a subroutine to perform the passive attack to the GKE protocol P as follows.

Given the parameters params^P of a GKE protocol P, the simulator runs the initialization protocol as shown in Fig. 2, expect that params^P is not generated. To respond to those $\mathsf{Execute}$ queries with Reveal asked by the adversary $\mathcal{A}$, the simulator queries $\mathsf{Execute}^P$ and Reveal^P to the protocol P at first. When $\mathcal{A}$ asks $\mathsf{Execute}(A_1^{i_1}, \cdots, A_n^{i_n}, S^j)$ query, the simulator queries $\mathsf{Execute}^P(A_1^{i_1}, \cdots, A_n^{i_n})$ and then $\mathsf{Test}^P(A_1^{i_1})$ to the protocol P. Suppose that $\mathsf{Test}^P(A_1^{i_1}) = \mathsf{sk}_b$ where $b \in \{0, 1\}$, sk_0 is the group key while sk_1 is a random value from Ω. Let $\mathsf{sk}_{A_\ell}^P = \mathsf{sk}_b$ $(\ell = 1, 2, \cdots, n)$, the simulator constructs $\mathsf{Execute}(A_1^{i_1}, \cdots, A_n^{i_n}, S^j)$ accordingly (i.e., letting $\mathsf{sid}_{A_\ell}^{i_\ell} = g^{h(\mathsf{sk}_b)}$) and responds to $\mathcal{A}$.

When $b = 0$, the distribution of adversary's view in the current experiment and $P_2'^{(t-1)}$ are identical, and thus the adversary has the same $\mathsf{Adv}_{\mathcal{A}}^{P_2'^{(t-1)}}(k)$. If $b = 1$, the distribution of adversary's view in the current experiment and $P_2'^{(t)}$ are identical, and thus the adversary has the same $\mathsf{Adv}_{\mathcal{A}}^{P_2'^{(t)}}(k)$. If $|\mathsf{Adv}_{\mathcal{A}}^{P_2'^{(t-1)}}(k) - \mathsf{Adv}_{\mathcal{A}}^{P_2'^{(t)}}(k)|$ is non-negligible, the simulator can decide when $b = 0$ or $b = 1$ with a non-negligible advantage, and thus win the game against the protocol P.

Since the GKE protocol P is assumed to be secure against the passive attack, $|\mathsf{Adv}_{\mathcal{A}}^{P_2'^{(t-1)}}(k) - \mathsf{Adv}_{\mathcal{A}}^{P_2'^{(t)}}(k)|$ must be negligible and Claim 2 is true.

Experiment P_3': In this experiment, the simulator interacts with the adversary $\mathcal{A}$ as in experiment P_2' except that the adversary's queries to $\mathsf{Execute}$ oracles are handled differently: for any $\mathsf{Execute}(A_1^{i_1}, \cdots, A_n^{i_n}, S^j)$ oracle where the adversary has not queried $\mathsf{Reveal}(A_\ell^{i_\ell})$ $(\ell = 1, 2, \cdots, n)$ in the end of experiment P_2', the final group key $\mathsf{sk}_{A_\ell}^{i_\ell}$ $(\ell = 1, 2, \cdots, n)$ are replaced with a random value from G.

The difference between the current experiment and the previous one is bounded by the probability to solve the decisional squaring Diffie-Hellman (DSDH) problem over a cyclic group G with a prime order q and a generator g. More precisely, we have

Claim 3. If the decisional squaring Diffie-Hellman (DSDH) problem is hard over (G, q, g), $|\mathsf{Adv}_{\mathcal{A}}^{P_2'}(k) - \mathsf{Adv}_{\mathcal{A}}^{P_3'}(k)|$ is negligible.

If the above difference is non-negligible, we show that the simulator can use $\mathcal{A}$ as a subroutine to solve the DSDH problem with non-negligible probability as follows.

Given a DSDH problem (g, g^a, Z), where a is randomly chosen from $\mathbb{Z}_q^*$ and Z is either g^{a^2} (denoted as $b = 0$) or a random element z from G (denoted as $b = 1$), the simulator (without knowledge of a and b) runs the initialization protocol as shown in Fig. 2, except that (G, q, g) is not generated. To respond to $\mathsf{Execute}(A_1^{i_1}, \cdots, A_n^{i_n}, S^j)$ query where the adversary $\mathcal{A}$ has not queried $\mathsf{Reveal}(A_\ell^{i_\ell})$ $(\ell = 1, 2, \cdots, n)$, the simulator chooses a random number $r \in \mathbb{Z}_q^*$ and lets $\mathsf{sid}_{A_\ell}^{i_\ell} = (g^a)^r$ and $\mathsf{sk}_{A_\ell}^{i_\ell} = Z^{r^2}$ $(\ell = 1, 2, \cdots, n)$. Because all initial group keys have been replaced with random values in experiment P_2', when $b = 0$, the distribution of adversary's view in the current experiment and P_2' are identical, and thus the adversary has the same $\mathsf{Adv}_{\mathcal{A}}^{P_2'}(k)$; when $b = 1$, the distribution of adversary's view in the current experiment and P_3' are identical, and thus the adversary has the same $\mathsf{Adv}_{\mathcal{A}}^{P_3'}(k)$.

If $|\mathsf{Adv}_{\mathcal{A}}^{P_2'}(k) - \mathsf{Adv}_{\mathcal{A}}^{P_3'}(k)|$ is non-negligible, the simulator can decide when $b = 0$ or $b = 1$ with a non-negligible advantage, and thus solve the DSDH problem. Therefore, the above difference must be negligible and the claim is true.

In experiment P_3', the adversary's probability of correctly guessing the bit b used by the Test oracle is exactly $1/2$ if the Test query is made to a fresh client instance A^i invoked by an $\mathsf{Execute}$ oracle, where the freshness only requires that the adversary has not queried $\mathsf{Reveal}(A^i)$ or $\mathsf{Reveal}(B^j)$ with the client instances A^i and B^j being partnered. This is so because the final group keys for such instances in P_3' are chosen at random from G, and hence there is no way to distinguish whether the Test oracle outputs a random group key or the "actual" group key (which is just a random element, anyway).

Note that an adversary is allowed to ask the above Test oracle even if he has queried KeyGen or $\mathsf{Corrupt}$ oracles, but the probability of correctly guessing the bit b is $1/2$, too. Therefore, a server adversary never succeed in the game.

The remainder of the proof concentrates on the instances invoked by Send oracles.

Experiment P_4': In this experiment, we modify the simulator's responses to Send_1' and Send_2' queries.

Before describing this change we introduce some terminology. The simulator first runs the protocol initialization as shown in Fig. 2. For a query $\mathsf{Send}_1'(S^j, (\mathsf{msg}_{A_1}, \cdots, \mathsf{msg}_{A_n}))$, where

$(\mathsf{msg}_{A_1}, \cdots, \mathsf{msg}_{A_n})$ is adversarially-generated, if equation (1) holds for $\ell = 1, 2, \cdots, n$, then $(\mathsf{msg}_{A_1}, \cdots, \mathsf{msg}_{A_n})$ is said to be valid. Otherwise, $(\mathsf{msg}_{A_1}, \cdots, \mathsf{msg}_{A_n})$ is said to be invalid. Similarly, for a query $\mathsf{Send}'_2(A^{i_\ell}_\ell, \mathsf{msg}_S)$ where msg_S is adversarially-generated, if equation (2) holds, then msg_S is said to be valid. Otherwise, msg_S is said to be invalid. Informally, valid messages use correct passwords or signing keys while invalid messages do not.

Given this terminology, we continue with our description of experiment P'_4. When the adversary makes oracle queries $\mathsf{Send}'_1(S^j, (\mathsf{msg}_{A_1}, \cdots, \mathsf{msg}_{A_n}))$, the simulator examines $(\mathsf{msg}_{A_1}, \cdots, \mathsf{msg}_{A_n})$. If it is adversarially-generated and valid, the query is answered as in experiment P'_4 except that acc^j_S is assigned the special value ∇. In any other case, (i.e., $(\mathsf{msg}_{A_1}, \cdots, \mathsf{msg}_{A_n})$ is oracle-generated, or adversarially-generated but invalid), the query is answered exactly as in experiment P'_4. When the adversary makes oracle queries $\mathsf{Send}'_2(A^{i_\ell}_\ell, \mathsf{msg}_S)$, the simulator examines msg_S. If msg_S is adversarially-generated and valid, the query is answered as in experiment P'_3 except that $\mathsf{acc}^{i_\ell}_{A_\ell}$ is assigned the special value ∇. In any other case, (i.e., msg_S is oracle-generated, or adversarially-generated but invalid), the query is answered exactly as in experiment P'_3.

Finally, the definition of the adversary's success in P'_4 is changed. If the adversary ever queries Send'_1 or Send'_2 with $\mathsf{acc}^j_S = \nabla$ or $\mathsf{acc}^{i_\ell}_{A_\ell} = \nabla$, the simulator halts and the adversary succeeds. Otherwise the adversary's success is determined as in experiment P'_3.

The distribution on the adversary's view in experiments P'_3 and P'_4 are identical up to the point when the adversary queries Send'_1 or Send'_2 with $\mathsf{acc}^j_S = \nabla$ or $\mathsf{acc}^{i_\ell}_{A_\ell} = \nabla$. If such a query is never made, the distributions on the view are identical. Therefore, we have

Claim 4. $\mathsf{Adv}^{P'_3}_{\mathcal{A}}(k) \leq \mathsf{Adv}^{P'_4}_{\mathcal{A}}(k)$.

In experiment P'_4, the adversary $\mathcal{A}$ succeeds if one of the following occurs: (1) the adversary queries $\mathsf{Send}'_1(S^j, (\mathsf{msg}_{A_1}, \cdots, \mathsf{msg}_{A_n}))$ for adversarially-generated and valid $(\mathsf{msg}_{A_1}, \cdots, \mathsf{msg}_{A_n})$, that is, $\mathsf{acc}^j_S = \nabla$ (let Succ_1 denote this event); (2) the adversary queries $\mathsf{Send}'_2(A^{i_\ell}_\ell, \mathsf{msg}_S)$ for adversarially-generated and valid msg_S, that is, $\mathsf{acc}^{i_\ell}_{A_\ell} = \nabla$ (let Succ_2 denote this event); (3) neither Succ_1 nor Succ_2 happens, the adversary wins the game by a Test query to a fresh client instance A^i.

In the last event, if the fresh client instance A^i is invoked by Send oracles, the messages in these Send oracles have to be oracle-generated. In this case, the group of these Send oracles form an $\mathsf{Execute}$ oracle, where the final group key sk^i_A can be replaced by a random value from G on the basis of Claims 1 to 3.

To evaluate $\mathsf{Pr}^{P'_4}_{\mathcal{A}}[\mathsf{Succ}_2]$, we do the following experiment.

Experiment P'_5. Given the parameters (params^S) of IBS, the simulator responds to all oracle queries as in experiment P'_4 except that it begins by running a modified initialization as follows.

$\mathsf{Initialize}'(1^k, \mathsf{params}^S)$–
$(\mathsf{params}^{P,E}, \mathsf{master\text{-}key}^E) \xleftarrow{R} \mathsf{Setup}^{P,E}(1^k), (G, q, g) \xleftarrow{R} \mathsf{GGen}(1^k), H \xleftarrow{R} \mathsf{CRHF}(1^k)$
$(\mathsf{Client}, \mathsf{Server}, \mathsf{ClientServerPair}) \xleftarrow{R} \mathsf{UserGen}(1^k)$
For each $S \in \mathsf{Server}$, $\mathsf{d_S} \leftarrow \mathsf{Extract}^E(\mathsf{ID}_S, \mathsf{params}^E, \mathsf{master\text{-}key}^E)$
For each $(A, S) \in \mathsf{ClientServerPair}$, $\mathsf{pw}^S_A \xleftarrow{R} \{\mathsf{pw}_1, \mathsf{pw}_2, \cdots, \mathsf{pw}_N\} \subset \mathbb{Z}^*_p$
Return $\mathsf{Client}, \mathsf{Server}, \mathsf{ClientServerPair}, G, q, g, h, H, \mathsf{params}^{P,E,S}$

The distribution of the adversary's view on experiments P'_4 and P'_5 are identical.

Claim 5. If the IBS has existential unforgeability under chosen-message attack, then $\mathsf{Pr}_{\mathcal{A}}^{P'_5}[\mathsf{Succ}_2]$ is negligible.

If $\mathsf{Pr}_{\mathcal{A}}^{P'_5}[\mathsf{Succ}_2]$ is non-negligible, the simulator can use the adversary $\mathcal{A}$ to construct a forger $\mathcal{A}'$ attacking the IBS scheme as follows.

For KeyGen queries asked by the adversary $\mathcal{A}$, the simulator has the adversary $\mathcal{A}'$ to query the challenger of the IBS scheme. Each time the simulator responds to Send'_1 query asked by $\mathcal{A}$, it checks if the messages are valid or not (note that it knows the decryption key $\mathsf{d_S}$ and passwords). For oracle-generated Send'_1 query, the simulator has $\mathcal{A}'$ to query the signing oracle $\mathsf{S}_{\mathsf{d}'_\mathsf{S}}$ of the IBS scheme on the message $\mathsf{pid}_S^j|\mathsf{sid}_S^j$ and returns the signature Auth_S. In addition, the simulator responds to all other oracles as in P'_4.

In case that the adversary $\mathcal{A}$ queried $\mathsf{Send}'_2(A_\ell^{i_\ell}, \mathsf{msg}_S)$ to a fresh client instance $A_\ell^{i_\ell}$ for adversarially-generated and valid msg_S (that is, $\mathsf{acc}_{A_\ell}^{i_\ell} = \nabla$), the adversary $\mathcal{A}'$ uses it to forge a signature of the signer S on the message msg_S. The freshness of $A_\ell^{i_\ell}$ ensures that the adversary has not queried $\mathsf{KeyGen}(\mathsf{PKG}, S)$ before $\mathsf{Send}'_2(A_\ell^{i_\ell}, \mathsf{msg}_S)$ oracle query.

If $\mathsf{Pr}_{\mathcal{A}}^{P'_5}[\mathsf{Succ}_2]$ is non-negligible, the advantage of the forger $\mathcal{A}'$ attacking the IBS scheme is non-negligible. It is in contradiction with the assumption that the IBS scheme has existential unforgeability. Therefore, $\mathsf{Pr}_{\mathcal{A}}^{P'_5}[\mathsf{Succ}_2]$ must be negligible and the claim follows.

To evaluate $\mathsf{Pr}_{\mathcal{A}}^{P'_5}[\mathsf{Succ}_1]$, we do the following experiment.

Experiment P'_6: In this experiment, the simulator interacts with the adversary $\mathcal{A}$ as in experiment P'_5 except that the adversary's queries to $\mathsf{Execute}$ and Send'_0 oracles are handled differently: for $\mathsf{Execute}(A_1^{i_1}, \cdots, A_n^{i_n}, S^j)$ and $\mathsf{Send}'_0(A_\ell^{i_\ell}, S^j)$ oracles where the adversary has not queried $\mathsf{KeyGen}(\mathsf{PKG}, S)$, Auth_ℓ is computed as $\mathsf{E}_{\mathsf{ID}_S}[H(\mathsf{sid}_{A_\ell}^{i_\ell}|\mathsf{pid}_{A_\ell}^{i_\ell}|\mathsf{pw}')]$ where pw' is randomly chosen from $\mathsf{Z}_p^* - \mathsf{Password}$ (i.e., it is not a valid password). The following bounds the effect this transformation can have on the adversary's advantage.

Claim 6. If the IBE scheme is secure against the chosen-ciphertext attack, $|\mathsf{Adv}_{\mathcal{A}}^{P'_5}(k) - \mathsf{Adv}_{\mathcal{A}}^{P'_6}(k)|$ is negligible.

Assume that there are m pairs of client instance $A_\lambda^{i_\lambda}$ and server instance S^j in experiment P'_5, where (1) $\mathsf{sid}_{A_\lambda}^{i_\lambda} = \mathsf{sid}_S^j$ and (2) the adversary has not queried $\mathsf{KeyGen}(\mathsf{PKG}, S)$. The claim is proved by m sub-experiments $P_6^{\prime(1)}, \cdots, P_6^{\prime(m)} = P'_6$, each of them corresponds to a pair of $(A_\lambda^{i_\lambda}, S^j)$. In the sub-experiment for $(A_\lambda^{i_\lambda}, S^j)$, only $\mathsf{Execute}$ and Send'_0 related to $A_\lambda^{i_\lambda}$ and S^j are handled differently. Let $P_6^{\prime(0)} = P'_5$, we only need to prove $|\mathsf{Adv}_{\mathcal{A}}^{P_6^{\prime(t-1)}}(k) - \mathsf{Adv}_{\mathcal{A}}^{P_6^{\prime(t)}}(k)|$ (where $1 \le t \le m$) to be negligible.

If $|\mathsf{Adv}_{\mathcal{A}}^{P_6^{\prime(t-1)}}(k) - \mathsf{Adv}_{\mathcal{A}}^{P_6^{\prime(t)}}(k)|$ is non-negligible, where $P_6^{\prime(t)}$ is the sub-experiment for $(A_\lambda^{i_\lambda}, S^j)$, we show that the simulator can use $\mathcal{A}$ as a subroutine to perform the chosen-ciphertext attack to the IBE as follows.

Given public parameters params^E for an instance of the IBE scheme, the simulator begins by running a modified initialization protocol as follows.

$\mathsf{Initialize}''(1^k, \mathsf{params}^E)$–

$(\mathsf{params}^{P,S}, \mathsf{master\text{-}key}^S) \xleftarrow{R} \mathsf{Setup}^{P,S}(1^k), (G, q, g) \xleftarrow{R} \mathsf{GGen}(1^k), H \xleftarrow{R} \mathsf{CRHF}(1^k)$

$(\mathsf{Client}, \mathsf{Server}, \mathsf{ClientServerPair}) \xleftarrow{R} \mathsf{UserGen}(1^k)$,

For each $S \in \mathsf{Server}$, $\mathsf{d}'_\mathsf{S} \leftarrow \mathsf{Extract}^S(\mathsf{ID}_S, \mathsf{params}^S, \mathsf{master\text{-}key}^S)$

For each $(A, S) \in \mathsf{ClientServerPair}$, $\mathsf{pw}_A^S \xleftarrow{R} \{\mathsf{pw}_1, \mathsf{pw}_2, \cdots, \mathsf{pw}_N\} \subset \mathbb{Z}_p^*$
Return $\mathsf{Client}, \mathsf{Server}, \mathsf{ClientServerPair}, G, q, g, h, H, \mathsf{params}^{P,E,S}$

Let $M_0 = H(\mathsf{sid}_{A_\lambda}^{i_\lambda} | \mathsf{pid}_{A_\lambda}^{i_\lambda} | \mathsf{pw}_{A_\lambda}^S)$ and $M_1 = H(\mathsf{sid}_{A_\lambda}^{i_\lambda} | \mathsf{pid}_{A_\lambda}^{i_\lambda} | \mathsf{pw}')$. Assume that the simulator wishes to challenge the two equal length plaintexts (M_0, M_1) and the identity ID_S. Given the ciphertext $C = \mathsf{E}_{\mathsf{ID}_\mathsf{S}}(M_b)$ where $b \in \{0, 1\}$ is unknown, the simulator responds all of the adversary's queries as in experiment $P_6^{(t-1)}$ except from $\mathsf{Execute}$ and Send_0' queries related to $A_\lambda^{i_\lambda}$ and S^j as shown in Fig. 5 and Fig. 6, respectively.

$\mathsf{Execute}(A_1^{i_1}, \cdots, A_n^{i_n}, S^j)$
If $(\exists \ell$ such that $(A_\ell, S) \notin \mathsf{ClientServerPair} \vee \mathsf{used}_{A_\ell}^{i_\ell}) \vee \mathsf{used}_S^j$, return $\perp$
$\mathsf{used}_{A_\ell}^{i_\ell} \leftarrow \mathsf{used}_S^j \leftarrow \mathsf{TRUE}, \mathsf{pid}_{A_\ell}^{i_\ell} \leftarrow \mathsf{pid}_S^j \leftarrow \{A_1, \cdots, A_n, S\}, \ell = 1, 2, \cdots, n$
$(\mathsf{sk}_{A_1}^P, \mathsf{sk}_{A_2}^P, \cdots, \mathsf{sk}_{A_n}^P) \leftarrow \mathsf{Execute}^P(A_1^{i_1}, A_2^{i_2}, \cdots, A_n^{i_n})$
$\mathsf{sid}_{A_\ell}^{i_\ell} \xleftarrow{R} G, \mathsf{Auth}_\ell \leftarrow \begin{cases} C & (\ell = \lambda) \\ \mathsf{E}_{\mathsf{ID}}[H(\mathsf{sid}_{A_\ell}^{i_\ell} | \mathsf{pid}_{A_\ell}^{i_\ell} | \mathsf{pw}_{A_\ell}^S)] & (\ell \neq \lambda) \end{cases} \mathsf{msg}_{A_\ell} \leftarrow A_\ell | \mathsf{sid}_{A_\ell}^{i_\ell} | \mathsf{Auth}_\ell$
$\mathsf{sid}_S^j \leftarrow \mathsf{sid}_{A_1}^{i_1}, \mathsf{Auth}_S \leftarrow \mathsf{S}_{\mathsf{d}_\mathsf{S}'}[\mathsf{pid}_S^j | \mathsf{sid}_S^j], \mathsf{msg}_S \leftarrow S | \mathsf{Auth}_S$
$\mathsf{acc}_{A_\ell}^{i_\ell} \leftarrow \mathsf{term}_{A_\ell}^{i_\ell} \leftarrow \mathsf{acc}_S^j \leftarrow \mathsf{term}_S^j \leftarrow \mathsf{TRUE}, \mathsf{sk}_{A_\ell}^{i_\ell} \xleftarrow{R} G, \ell = 1, 2, \cdots, n$
Return $\mathsf{status}_{A_1}^{i_1}, \cdots, \mathsf{status}_{A_n}^{i_n}, \mathsf{status}_S^j$

Fig. 5. The modified $\mathsf{Execute}$ oracle for proof of Claim 6

$\mathsf{Send}_0'(A_\ell^{i_\ell}, S^j)$
If $\neg \mathsf{used}_{A_\ell}^{i_\ell} \vee (A_\ell, S) \notin \mathsf{ClientServerPair} \vee \mathsf{term}_{A_\ell}^{i_\ell} \vee (S \notin \mathsf{pid}_{A_\ell}^{i_\ell})$, return $\perp$
$\mathsf{pid}_{A_\ell}^{i_\ell} \leftarrow \{A_1, \cdots, A_n, S\}$
$\mathsf{sid}_{A_\ell}^{i_\ell} \leftarrow g^{\mathsf{sk}_{A_\ell}^P}, \mathsf{Auth}_\ell \leftarrow \begin{cases} C & (\ell = \lambda) \\ \mathsf{E}_{\mathsf{ID}}[H(\mathsf{sid}_{A_\ell}^{i_\ell} | \mathsf{pid}_{A_\ell}^{i_\ell} | \mathsf{pw}_{A_\ell}^S)] & (\ell \neq \lambda) \end{cases}$
$\mathsf{MsgOut} \leftarrow A_\ell | \mathsf{sid}_{A_\ell}^{i_\ell} | \mathsf{Auth}_\ell, \mathsf{state}_{A_\ell}^i \leftarrow (\mathsf{pid}_{A_\ell}^{i_\ell}, \mathsf{sk}_{A_\ell}^P, \mathsf{MsgOut})$
Return $\mathsf{status}_{A_\ell}^{i_\ell}$

$\mathsf{Send}_1'(S^j, (A_\ell^{i_\ell} | \mathsf{sid}_{A_\ell}^{i_\ell} | \mathsf{Auth}_\ell)_{\ell=1,2,\cdots,n})$
If $(\exists \ell$ such that $(A_\ell, S) \notin \mathsf{ClientServerPair}) \vee \mathsf{used}_S^j$, return $\perp$
$\mathsf{used}_S^j \leftarrow \mathsf{TRUE}, \mathsf{pid}_S^j \leftarrow \{A_1, A_2, \cdots, A_n, S\}, \mathsf{sid}_S^j \leftarrow \mathsf{sid}_{A_1}^{i_1}$
If MsgIn is adversarially-generated
  If $\forall \ell, \mathsf{D}_{\mathsf{d}_\mathsf{S}}[\mathsf{Auth}_\ell] = H(\mathsf{sid}_S^j | \mathsf{pid}_S^j | \mathsf{pw}_{A_\ell}^S)$, then $\mathsf{acc}_S^j \leftarrow \nabla$
Else $\mathsf{acc}_S^j \leftarrow \mathsf{term}_S^j \leftarrow \mathsf{TRUE}, \mathsf{Auth}_S \leftarrow \mathsf{S}_{\mathsf{d}_\mathsf{S}'}[\mathsf{pid}_S^j | \mathsf{sid}_S^j], \mathsf{MsgOut} \leftarrow S | \mathsf{Auth}_S$
Return status_S^j

$\mathsf{Send}_2'(A_\ell^{i_\ell}, S^j | \mathsf{Auth}_S)$
$\mathsf{state}_{A_\ell}^{i_\ell} \leftarrow (\mathsf{pid}_{A_\ell}^{i_\ell}, \mathsf{sk}_{A_\ell}^P, \mathsf{FirstMsgOut})$
If $\neg \mathsf{used}_{A_\ell}^{i_\ell} \vee \mathsf{term}_{A_\ell}^{i_\ell} \vee (S \notin \mathsf{pid}_{A_\ell}^{i_\ell})$, return $\perp$
If MsgIn is adversarially-generated
  If $\mathsf{V}_{\mathsf{ID}_\mathsf{S}}[\mathsf{pid}_{A_\ell}^{i_\ell} | \mathsf{sid}_{A_\ell}^{i_\ell}, \mathsf{Auth}_S] = 1$, then $\mathsf{acc}_S^j \leftarrow \nabla$
Else $\mathsf{acc}_{A_\ell}^{i_\ell} \leftarrow \mathsf{term}_{A_\ell}^{i_\ell} \leftarrow \mathsf{TRUE}, \mathsf{sk}_{A_\ell}^{i_\ell} \leftarrow g^{(\mathsf{sk}_{A_\ell}^P)^2}$
Return $\mathsf{status}_{A_\ell}^{i_\ell}$

Fig. 6. The modified Send oracles for the proof of Claim 6

Note that an adversarially-generated message which contains $A_\ell | \mathsf{sid}_{A_\ell}^{i_\ell} | C$ in $\mathsf{Send}_1'(S^j, *)$ query, where $\ell \neq \lambda$ or $\ell = \lambda$ but $\mathsf{sid}_{A_\ell}^{i_\ell} \neq \mathsf{sid}_S^j$, is invalid. The decryption of C is either

$H(\mathsf{sid}^{i_\lambda}_{A_\lambda}|\mathsf{pid}^{i_\lambda}_{A_\lambda}|\mathsf{pw}^{S}_{A_\lambda})$ or $H(\mathsf{sid}^{i_\lambda}_{A_\lambda}|\mathsf{pid}^{i_\lambda}_{A_\lambda}|\mathsf{pw}')$. Because different sessions have different sid, different clients use different passwords, and H is a collision-resistant hash function, we have both $H(\mathsf{sid}^{i_\lambda}_{A_\lambda}|\mathsf{pid}^{i_\lambda}_{A_\lambda}|\mathsf{pw}^{S}_{A_\lambda}) \neq H(\mathsf{sid}^{i_\ell}_{A_\ell}|\mathsf{pid}^{i_\ell}_{A_\ell}|\mathsf{pw}^{S}_{A_\ell})$ and $H(\mathsf{sid}^{i_\lambda}_{A_\lambda}|\mathsf{pid}^{i_\lambda}_{A_\lambda}|\mathsf{pw}') \neq H(\mathsf{sid}^{i_\ell}_{A_\ell}|\mathsf{pid}^{i_\ell}_{A_\ell}|\mathsf{pw}^{S}_{A_\ell})$ for the above message, which means equation (1) does not hold for ℓ. Although the simulator cannot query the decryption of C, it can respond to all kinds of Send'_1 queries involving C properly.

When $b = 0$, the distribution of adversary's view in the current experiment and $P_6'^{(t-1)}$ are identical, and thus the adversary has the same $\mathsf{Adv}_{\mathcal{A}}^{P_6'^{(t-1)}}(k)$. If $b = 1$, the distribution of adversary's view in the current experiment and $P_6'^{(t)}$ are identical, and thus the adversary has the same $\mathsf{Adv}_{\mathcal{A}}^{P_6'^{(t)}}(k)$. If $|\mathsf{Adv}_{\mathcal{A}}^{P_6'^{(t-1)}}(k) - \mathsf{Adv}_{\mathcal{A}}^{P_6'^{(t)}}(k)|$ is non-negligible, the simulator can decide when $b = 0$ or $b = 1$ with a non-negligible advantage.

Since the IBE is assumed to be secure against the chosen-ciphertext attack, $|\mathsf{Adv}_{\mathcal{A}}^{P_6'^{(t-1)}}(k) - \mathsf{Adv}_{\mathcal{A}}^{P_6'^{(t)}}(k)|$ must be negligible and Claim 2 is true.

Now let us consider an adversarially-generated $\mathsf{Send}'_1(S^j, (A_\ell^{i_\ell}|\mathsf{sid}^{i_\ell}_{A_\ell}|\mathsf{Auth}_\ell)_{1,2,\cdots,n})$ query to a fresh server instance S^j. The freshness of S^j implies that the adversary has not queried $\mathsf{KeyGen}(\mathsf{PKG}, S)$ oracle and any $\mathsf{Corrupt}(A_\ell)$ $(\ell = 1, 2, \cdots, n)$. In experiment P_6', all messages which are dependent of $\mathsf{pw}^S_{A_\ell}$ $(\ell = 1, 2, \cdots, n)$ have been replaced by those which are independent of these passwords. Therefore, the adversary's view is independent of the passwords $\mathsf{pw}^S_{A_\ell}$ $(\ell = 1, 2, \cdots, n)$ chosen by the simulator. In order to win the game, the adversary has to try all passwords one-by-one in an online impersonation attack. The probability that Succ_1 occurs is at most $Q(k)/N$, where $Q(k)$ is the number of online attacks made by the adversary $\mathcal{A}$.

In experiment P_6', the adversary succeeds if either Succ_1 or Succ_2 occurs, or else by guessing the value of b used by the Test oracle. However, if neither Succ_1 nor Succ_2 occurs and the adversary queries $\mathsf{Test}(A^i)$ where A^i is fresh and $\mathsf{acc}^i_U = \mathsf{TRUE}$, then sk^i_A is randomly-distributed in G independent of the adversary's view. Thus, the adversary's probability of success when neither Succ_1 nor Succ_2 occurs is $1/2$. The preceding discussion implies that

$$Pr_{\mathcal{A}}^{P_6'}[\mathsf{Succ}] \leq Q(k)/N + 1/2 \cdot (1 - Q(k)/N)$$

and thus the adversary's advantage in experiment P_6' is at most $Q(k)/N$. The sequence of claims proved above show that

$$\mathsf{Adv}_{\mathcal{A}}^{P_0'}[\mathsf{Succ}] \leq \mathsf{Adv}_{\mathcal{A}}^{P_6'}(k) + \varepsilon(k)$$

for some negligible function $\varepsilon(\cdot)$ and therefore the adversary's advantage in P_0' (i.e., the original protocol) is at most $Q(k)/N$ plus some negligible quantity. This complete the proof of the theorem.