Abstract—Password-authenticated key exchange (PAKE) is where a client and a server, who share a password, authenticate each other and meanwhile establish a cryptographic key by exchange of messages. In this setting, all the passwords necessary to authenticate clients are stored in a single server. If the server is compromised, due to, for example, hacking or even insider attack, passwords stored in the server are all disclosed. In this paper, we consider a scenario where two servers cooperate to authenticate a client and if one server is compromised, the attacker still cannot pretend to be the client with the information from the compromised server. Current solutions for two-server PAKE are either symmetric in the sense that two peer servers equally contribute to the authentication or asymmetric in the sense that one server authenticates the client with the help of another server. This paper presents a symmetric solution for two-server PAKE, where the client can establish different cryptographic keys with the two servers, respectively. Our protocol runs in parallel and is more efficient than existing symmetric two-server PAKE protocol, and even more efficient than existing asymmetric two-server PAKE protocols in terms of parallel computation.

Index Terms—Password-authenticated key exchange, dictionary attack, Diffie-Hellman key exchange, ElGamal encryption

1 INTRODUCTION

TODAY, passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines and so on. A computer user may require passwords for many purposes: logging in to computer accounts, retrieving e-mail from servers, accessing programs, databases, networks, web sites, and even reading the morning newspaper online.

Earlier password-based authentication systems transmitted a cryptographic hash of the password over a public channel which makes the hash value accessible to an attacker. When this is done, and it is very common, the attacker can work offline, rapidly testing possible passwords against the true password’s hash value. Studies have consistently shown that a large fraction of user-chosen passwords are readily guessed automatically. For example, according to Bruce Schneier, examining data from a 2006 phishing attack, 55 percent of MySpace passwords would be crackable in 8 hours using a commercially available Password Recovery Toolkit capable of testing 200,000 passwords per second in 2006 [26].

Recent research advances in password-based authentication have allowed a client and a server mutually to authenticate with a password and meanwhile to establish a cryptographic key for secure communications after authentication. In general, current solutions for password-based authentication follow two models.

The first model, called PKI-based model, assumes that the client keeps the server’s public key in addition to a password with the server. In this setting, the client can send the password to the server by public key encryption. Gong et al. [15], [22] were the first to present this kind of authentication protocols with heuristic resistant to offline dictionary attacks, and Halevi and Krawczyk [16] were the first to provide formal definitions and rigorous proofs of security for PKI-based model.

The second model is called password-only model. Bellovin and Merritt [4] were the first to consider authentication based on password only, and introduced a set of so-called “encrypted key exchange” protocols, where the password is used as a secret key to encrypt random numbers for key exchange purpose. Formal models of security for the password-only authentication were first given independently by Bellare et al. [3] and Boyko et al. [8]. Katz et al. [19] were the first to give a password-only authentication protocol which is both practical and provably secure under standard cryptographic assumption.

Based on the identity-based encryption technique [5], [6], Yi et al. [32], [33], [34] suggested an identity-based model where the client needs to remember the password only while the server keeps the password in addition to private keys related to its identity. In this setting, the client can encrypt the password based on the identity of the server. This model is between the PKI-based and the password-only models.

Typical protocols for password-based authentication assume a single server stores all the passwords necessary to authenticate clients. If the server is compromised, due to, for example, hacking, or installing a “Trojan horse,” or even insider attack, user passwords stored in the server are
disclosed. To address this issue, two-server password-based authentication protocols were introduced in [9], [20], [29], [30], [31], and [18], where two servers cooperate to authenticate a client on the basis of password and if one server is compromised, the attacker still cannot pretend to be the client with the information from the compromised server.

Current solutions for two-server PAKE are either symmetric in the sense that two peer servers equally contribute to the authentication, such as [20], or asymmetric in the sense that one server authenticates the client with the help of another server, such as [30], [18]. A symmetric two-server PAKE protocol, for example, Katz et al.’s protocol [20], can run in parallel and establishes secret session keys between the client and two servers, respectively. In case one of the two servers shuts down due to the denial-of-service attack, another server can continue to provide services to authenticated clients. In terms of parallel computation and reliable service, a symmetric protocol is superior to an asymmetric protocol. So far, only Katz et al.’s two-server PAKE protocol [20] has been symmetric. But their protocol is not efficient for practical use. An asymmetric two-server PAKE protocol runs in series and only the front-end server and the client need to establish a secret session key. Current asymmetric protocols, for example, Yang et al.’s protocol [30], [31] and Jin et al.’s protocol [18], need two servers to exchange messages for several times in series. These asymmetric designs are less efficient than a symmetric design which allows two servers to compute in parallel.

In this paper, we propose a new symmetric solution for two-server PAKE. In all existing two-server PAKE protocols, two servers are provided random password shares $pw_1$ and $pw_2$ subject to $pw_1 + pw_2 = pw$. In our protocol, we provide one server $S_1$ with an encryption of the password $E(g_{p_1}^{pw_1}, pk_2)$, and another server $S_2$ with an encryption of the password $E(g_{p_1}^{pw_2}, pk_1)$, where $pk_1$ and $pk_2$ are the encryption keys of $S_1$ and $S_2$, respectively. In addition, two servers are provided random password shares $b_1$ and $b_2$ subject to $b_1 \oplus b_2 = H(pw)$, where $H$ is a hash function. Like [20], [31], [18], the password $pw$ is secret unless the two servers collude.

Although we use the concept of public key cryptosystem, our protocol follows the password-only model. The encryption and decryption key pairs for the two servers are generated by the client and delivered to the servers through different secure channels during the client registration, as the client in any two-server PAKE protocol sends two halves of the password to the two servers in secret, respectively. In fact, a server should not know the encryption key of another server and is restricted to operate on the encryption of the password on the basis of the homomorphic properties of ElGamal encryption scheme. For example, given $E(g_2^{pw}, pk_2)$, $S_1$ can construct $E(Ag_{p_1}^{pw}, pk_2)$ and $E(g_2^{pw}, pk_2)$ for any group element $A$ and integer $a$ without the knowledge of the encryption key $pk_2$.

Security analysis has shown that our protocol is secure against both passive and active attacks in case that one server is compromised. Performance analysis has shown that our protocol is more efficient than existing symmetric and asymmetric two-server PAKE protocols in terms of parallel computation.

Our protocol can be applied in distributed systems where multiple servers exist. For example, Microsoft active directory domain service (AD DS) is the foundation for distributed networks built on Windows server operating systems that use domain controllers. AD DS provides structured and hierarchical data storage for objects in a network such as users, computers, printers, and services. AD DS also provides support for locating and working with these objects. For a large enterprise running its own domain, there must be two AD DS domain controllers, for fault-tolerance purpose. To authenticate a user on a network, the user usually needs to provide his/her identification and password to one AD DS domain controller. Based on our two-server PAKE protocol, we can split the user’s password into two parts and store them, respectively, on the two AD DS domain controllers, which can then cooperate to authenticate the user. Even if one domain controller is compromised, the system can still work. In this way, we can achieve more secure AD DS.

The remainder of this paper is organized as follows: We introduce related works in Section 2, and two cryptographic building blocks of our protocol, Diffie-Hellman key exchange protocol and ElGamal encryption scheme, in Section 3, and describe our two-server PAKE protocol in Section 4. Security and performance analysis of our protocol is done in Sections 5 and 6, respectively, and Conclusions are drawn in the last section.

2 RELATED WORKS

In a single-server PAKE protocol, if the server is compromised, user passwords stored in the server are all disclosed. To address this issue, in 2000, Ford and Kaliski [13] proposed the first threshold PAKE protocol in the PKI-based model, in which $n$ servers cooperate to authenticate a client. Their protocol remains secure as long as $n - 1$ or fewer servers are compromised. Subsequently, in 2001, Joblon [17] removed the requirement for PKI and suggested a protocol with the similar property in the password-only model. Both the threshold PAKE protocols were not shown to be secure formally. In 2002, MacKenzie et al. [24] gave a protocol in the PKI-based setting, which requires only $t$ out of $n$ servers to cooperate to authenticate a client and is secure as long as $t - 1$ or fewer servers are compromised. They were the first to provide a formal security proof for their threshold PAKE protocol in the random oracle model. In 2003, Di Raimondo and Gennaro [11] proposed a protocol in the password-only setting, which requires less than $1/3$ of the servers to be compromised, with a formal security proof in the standard model.

In 2003, Brainard et al. [9] developed the first two-server protocol in the PKI-based setting. Their protocol and its variant [27] assume a secure channel between the client and the server(s), which would be in practice implemented using public key techniques such as SSL. In 2005, Katz et al. [20] proposed the first two-server password-only authenticated key exchange protocol with a proof of security in the standard model. Their protocol extended and built upon the Katz-Ostrovsky-Yung PAKE protocol [19], called KOY protocol for brevity. In their protocol, a client $C$ randomly chooses a password $pw$, and two servers $A$ and $B$ are
provided random password shares $pw_1$ and $pw_2$ subject to $pw_1 + pw_2 = pw$. At high level, their protocol can be viewed as two executions of the KOY protocol, one between the client $C$ and the server $A$, using the server $B$ to assist with the authentication, and one between the client $C$ and the server $B$, using the server $A$ to assist with the authentication. The assistance of the other server is necessary since the password is split between two servers. In the end of their protocol, each server and the client agree on a secret session key. Katz et al.'s protocol [20] is symmetric where two servers equally contribute to the client authentication and key exchange. For their basic protocol secure against a passive adversary, each party performs roughly twice the amount of work as the KOY protocol. For the protocol secure against active adversaries, the work of the client remains the same but the work of the servers increases by a factor of roughly 2-4. The advantage of Katz et al.'s protocols is the protocol structure which supports two servers to compute in parallel, but its disadvantage is ineffectiveness for practical use.

Built on Brainard et al.'s work [9], in 2005, Yang et al. [29] suggested an asymmetric setting, where a front-end server, called service server (SS), interacts with the client, while a back-end server, called control server (CS), helps SS with the authentication, and only SS and the client agree on a secret session key in the end. They proposed a PKI-based asymmetric two-server PAKE protocol in [29] in 2005 and several asymmetric password-only two-server PAKE protocols in [30] and [31] in 2006. In their password-only protocol [30], [31], the client initiates a request, and SS responds with $B = B_1B_2$, where $B_1 = g_1^{\alpha_1}g_2^{\beta_1}$ and $B_2 = g_1^{\alpha_2}g_2^{\beta_2}$ are generated by SS and CS on the basis of their random password shares $\pi_1$ and $\pi_2$, respectively. The advantage of Jin et al.'s protocol is that it can be used as follows:

1. Alice and Bob agree on a cyclic group $\mathbb{G}$ of large prime order $q$ with a generator $g$.
2. Alice randomly chooses an integer $a$ from $\mathbb{Z}_q^*$ and computes $X = g^a$, while Bob randomly chooses an integer $b$ from $\mathbb{Z}_q^*$ and computes $Y = g^b$. Then Alice and Bob exchange $X$ and $Y$.
3. Alice computes the secret key $k_1 = Y^a = g^{ab}$, while Bob computes the secret key $k_2 = X^b = g^{ab}$.

It is obvious that $k_1 = k_2$ and thus Alice and Bob have agreed on the same secret key, by which the subsequent communications between them can be protected.

Diffie-Hellman key exchange protocol is secure against any passive adversary, who cannot interact with Alice and Bob, attempting to determine the secret key solely based upon observed data. The security is built on the well-known computational Diffie-Hellman (CDH) and decisional Diffie-Hellman (DDH) assumptions as follows:

**CDH assumption.** Consider a cyclic group $\mathbb{G}$ of large prime order $q$ with a generator $g$. The CDH assumption states that, given $(\mathbb{G}, g, g^a, g^b)$ for randomly chosen $a, b$ from $\mathbb{Z}_q^*$, it is computationally intractable to compute the value $g^{ab}$.

**DDH assumption.** Consider a cyclic group $\mathbb{G}$ of large prime order $q$ with a generator $g$. The DDH assumption states that, given $(\mathbb{G}, g, g^a, g^b, g^c)$ for randomly chosen $a, b, c$ from $\mathbb{Z}_q^*$, the value $g^{ab}$ looks like a random element in $\mathbb{G}$. This intuitive notion is formally stated by saying that no
probabilistic polynomial time (PPT) algorithm can distinguish the following two probability distributions with a probability more than 1/2 plus a nonnegligible value:

- \((g^a, g^b, g^c),\) where \(a\) and \(b\) are randomly and independently chosen from \(\mathbb{Z}_q^*\).
- \((g^a, g^b, g^c),\) where \(a, b, c\) are randomly and independently chosen from \(\mathbb{Z}_q^*\).

### 3.2 ElGamal Encryption Scheme

The ElGamal encryption scheme was invented by ElGamal in 1985 [12] on the basis of Diffie-Hellman key exchange protocol. It consists of key generation, encryption, and decryption algorithms as follows:

1. **Key generation.** On input a security parameter \(k\), it publishes a cyclic group \(\mathbb{G}\) of large prime order \(q\) with a generator \(g\). Then it chooses a decryption key \(x\) randomly from \(\mathbb{Z}_q^*\) and computes an encryption key \(y = g^x\).

2. **Encryption.** On inputs a message \(m \in \mathbb{G}\) and the encryption key \(y\), it chooses an integer \(r\) randomly from \(\mathbb{Z}_q^*\) and outputs a ciphertext \(C = E(m, y) = (A, B) = (g^r, m \cdot g^r)\).

3. **Decryption.** On inputs a ciphertext \((A, B)\), and the decryption key \(x\), it outputs the plaintext \(m = D(C, x) = B^x / A^x\).

ElGamal encryption scheme is a probabilistic encryption scheme. If encrypting the same message with ElGamal encryption scheme several times, it will, in general, yield different ciphertexts. Tsiounis and Yung [28] proved ElGamal encryption scheme to be semantically secure under the DDH assumption. ElGamal encryption scheme has useful homomorphic properties as follows:

- Given an encryption of \(m, E(m, y) = (A, B)\), one can compute \(A \cdot B^\gamma \in \mathbb{G}\) for any \(\gamma \in \mathbb{G}\), an encryption of \(\gamma m\), and one can also compute \((A^\alpha, B^\alpha) = E(m^\alpha, y)\) for any \(\alpha \in \mathbb{Z}_q^*\), an encryption of \(m^\alpha\).

- Given encryptions of \(m_1\) and \(m_2\), \(E(m_1, y) = (A_1, B_1)\) and \(E(m_2, y) = (A_2, B_2)\), one can compute \((A_1A_2, B_1B_2) = E(m_1m_2, y)\), an encryption of \(m_1m_2\).

### 4 Two-Server Password-Only Authentication and Key Exchange

#### 4.1 Our Model

In our system, there exist two servers \(S_1\) and \(S_2\) and a group of clients. The two servers cooperate to authenticate clients and provide services to authenticated clients. Prior to authentication, each client \(C\) chooses a password \(pw_C\) and generates the password authentication information \(Auth_C^{(1)}\) and \(Auth_C^{(2)}\) for \(S_1\) and \(S_2\), respectively, such that nobody can determine the password \(pw_C\) from \(Auth_C^{(1)}\) or \(Auth_C^{(2)}\) unless \(S_1\) and \(S_2\) collude. The client sends \(Auth_C^{(1)}\) and \(Auth_C^{(2)}\) to \(S_1\) and \(S_2\), respectively, through different secure channels during the client registration. After that, the client remembers the password only, and the two servers keep the password authentication information. Like all existing solutions for two-server PAKE, we assume the two servers never collude to reveal the password of the client.

When the two servers cooperate to authenticate a client \(C\), we assume that the client \(C\) can broadcast a message to both of \(S_1\) and \(S_2\) simultaneously, but stress that we do not assume a broadcast channel and, in particular, an attacker can deliver different messages to the two servers or refuse to deliver a message to a server. In our protocol, the client and the two servers communicate through a public channel which may be eavesdropped, delayed, replayed, and even tampered by an attacker.

Our protocol is symmetric if two peer servers equally contribute to the authentication in terms of computation and communication.

**Definition 1.** Our protocol is correct if each server establishes a secret session key with the client in the end.

An adversary in our system is either passive or active. We consider both online dictionary attack, where an attacker attempts to login repeatedly, trying each possible password, and offline dictionary attack, where an adversary derives information about the password from observed transcripts of log sessions. The online dictionary attack cannot be prevented by cryptographic means but can be easily detected and suspended once the authentication fails several times.

We assume that an adversary can compromise one server only and obtain all information stored in the server. A passive adversary is able to monitor the communications among the client and two servers. An active adversary is able to pretend to be both one server and the client to communicate with the honest server or pretend to be both two servers to communicate with the legal client, deviate in an arbitrary way from the actions prescribed by the protocol.

In our protocol, the adversary attempts to learn the secret session key established between the client and the honest server. In an active attack, an adversary can learn the secret session key between the client and the honest server if the adversary can determine the password of the client.

In general, we say that our protocol is secure if no adversary can succeed in any passive and active attacks in case that one server is compromised. We will define when an adversary succeeds in a passive attack or an active attack later in Section 5.

#### 4.2 Our Protocol

Our protocol runs in three phases—initialization, registration, and authentication.

##### 4.2.1 Initialization

The two peer servers \(S_1\) and \(S_2\) jointly choose a cyclic group \(\mathbb{G}\) of large prime order \(q\) with a generator \(g\) and a secure hash function \(H : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*\) which maps a message of arbitrary length into an \(\ell\)-bit integer, where \(\ell = \log_2 q\). Next, \(S_1\) randomly chooses an integer \(s_1\) from \(\mathbb{Z}_q^*\) and \(S_2\) randomly chooses an integer \(s_2\) from \(\mathbb{Z}_q^*\), and \(S_1\) and \(S_2\) exchange \(g^{s_1}\) and \(g^{s_2}\). After that, \(S_1\) and \(S_2\) jointly publish public system parameters \(\mathbb{G}, q, g, g_1, g_2, H\), where \(g_2 = g^{s_2}\).

**Remark.** In most of existing two-server PAKE protocols such as [30], [31], [18], it is assumed or implied that the
discrete logarithm of \( g_2 \) to the base \( g_1 \) is unknown to anyone. Otherwise, their protocols are insecure. Our initialization can ensure that nobody is able to know the discrete logarithm of \( g_2 \) to the base \( g_1 \) unless the two servers collude. It is well known that the discrete logarithm problem is hard, and our model assumes that the two servers never collude.

### 4.2.2 Registration

Prior to authentication, each client \( C \) is required to register both \( S_1 \) and \( S_2 \) through different secure channels. First of all, the client \( C \) generates decryption and encryption key pairs \( (x_i, y_i) \) where \( y_i = g_1^{x_i} \) for the server \( S_i \) \((i = 1, 2)\) using the public parameters published by the two servers. Next, the client \( C \) chooses a password \( pw_C \) and encrypts the password using the encryption key \( y_i \), i.e., \( E(g_2^{pw_C}, y_i) = (A_i, B_i) = (g_1^{a_i}, g_2^{pw_C} y_i) \) \((i = 1, 2)\) where \( a_i \) is randomly chosen from \( \mathbb{Z}_q^* \) according to ElGamal encryption. Then, the client \( C \) randomly chooses \( b_1 \) from \( \mathbb{Z}_q^* \) and lets \( b_2 = H(pw_C) \oplus b_1 \), where \( \oplus \) stands for exclusive OR of two \( t \)-bit blocks. At last, the client \( C \) delivers the password authentication information \( Auth^{(1)}_C = \{x_1, a_1, b_1, (A_2, B_2)\} \) to \( S_1 \) through a secure channel, and the password authentication information \( Auth^{(2)}_C = \{x_2, a_2, b_2, E(g_2^{pw_C}, y_1)\} \) to \( S_2 \) through another secure channel. After that, the client \( C \) remembers the password \( pw_C \) only. The detailed process of registration is depicted in Fig. 1.

**Remark.** The two secure channels are necessary for all two-server PAKE protocols, where a password is split into two parts, which are securely distributed to the two servers, respectively, during registration. Although we refer to the concept of public key cryptosystem, the encryption key of one server should be unknown to another server and the client needs to remember a password only after registration.

### 4.2.3 Authentication and Key Exchange

Assume that the two servers \( S_1 \) and \( S_2 \) have received the password authentication information of a client \( C \) during the registration, there are five steps for the two servers \( S_1 \) and \( S_2 \) to authenticate the client \( C \) and establish secret session keys with the client \( C \) in terms of parallel computation.

- **Step 1.** The client \( C \) randomly chooses an integer \( r \) from \( \mathbb{Z}_q^* \) computes \( R = g_1^{a_1} g_2^{x_1} \) and then broadcasts a request message \( M_1 = \{C, Req, R\} \) to the two servers \( S_1 \) and \( S_2 \).

- **Step 2.** On receiving \( M_1 \), the server \( S_1 \) randomly chooses an integer \( r_1 \) from \( \mathbb{Z}_q^* \) and computes

\[
A_1' = A_1^r, \quad B_1' = (R \cdot B_2)^{r_1}.
\]

The server \( S_2 \) randomly chooses an integer \( r_2 \) from \( \mathbb{Z}_q^* \) and computes

\[
A_2' = A_2^r, \quad B_2' = (R \cdot B_1)^{r_2}.
\]

Then, \( S_1 \) and \( S_2 \) exchange \( M_2 = (A_1', B_1') \) and \( M_3 = (A_2', B_2') \).

- **Step 3.** On receiving \( (A_1', B_1') \), the server \( S_1 \) randomly chooses an integer \( r_1' \) from \( \mathbb{Z}_q^* \) computes

\[
R_1 = A_1'^{a_1 r_1'}, \quad K_1 = (B_1'/A_1' r_1')^{r_1'}, \quad h_1 = H(K_1, 0) \oplus b_1,
\]

and replies \( M_4 = \{S_1, R_1, h_1\} \) to the client \( C \).

On receiving \( (A_2', B_2') \), the server \( S_2 \) randomly chooses an integer \( r_2' \) from \( \mathbb{Z}_q^* \) computes

\[
R_2 = A_2'^{a_2 r_2'}, \quad K_2 = (B_2'/A_2' r_2')^{r_2'}, \quad h_2 = H(K_2, 0) \oplus b_2,
\]

and replies \( M_5 = \{S_2, R_2, h_2\} \) to the client \( C \).

- **Step 4.** After receiving \( M_4 \) and \( M_5 \), the client \( C \) computes

\[
K_1' = R_1^r, \quad K_2' = R_2^r,
\]

and checks if

\[
H(K_1', 0) \oplus H(K_2', 0) \oplus h_1 \oplus h_2 = H(pw_C).
\]

If so, the two servers \( S_1 \) and \( S_2 \) are authentic. The client \( C \) computes

\[
h_1' = H(K_1', 1) \oplus H(K_1', 0) \oplus h_1, \quad h_2' = H(K_2', 1) \oplus H(K_2', 0) \oplus h_2,
\]

and then broadcasts \( M_6 = \{h_1', h_2'\} \). At last, the client \( C \) sets the secret session keys with \( S_1 \) and \( S_2 \) as \( SK_1' = H(K_1', 2) \) and \( SK_2' = H(K_2', 2) \), respectively.

---

**Fig. 1. Registration of our protocol.**

\[
\begin{align*}
&x_1, x_2, a_1, a_2, b_1, b_2, E : \mathbb{Z}_q^* \\
y_1 \leftarrow g_1^{x_1}, \ y_2 \leftarrow g_1^{x_2} \\
&\quad (A_1, B_1) \leftarrow (g_1^{a_1}, g_2^{pw_C} y_1^{a_1}) \\
&\quad (A_2, B_2) \leftarrow (g_1^{a_2}, g_2^{pw_C} y_2^{a_2}) \\
&\quad b_2 \leftarrow H(pw_C) \oplus b_1 \\
&\quad Auth^{(1)}_C = \{x_1, a_1, b_1, (A_2, B_2)\} \\
&\quad Auth^{(2)}_C = \{x_2, a_2, b_2, (A_1, B_1)\} \\
&\quad \text{Secure Channel 1} \\
&\quad \text{Server } S_1 \\
&\quad \text{Secure Channel 2} \\
&\quad \text{Server } S_2
\end{align*}
\]
Proof. Since $R = g_1^x g_2^{pywC}$, $A_1 = g_1^{y_1}, B_1 = g_2^{pwC} y_1^{y_1}, A_1' = A_1^r, B_1' = (RB_1)^{y_1}$, we have

$$A_1' = (g_1^{y_1})^{r_1} = g_1^{r_1 y_1},$$

$$B_1' = (g_1^x g_2^{pwC} y_1^{y_1})^{r_1} = g_1^{r_1 y_1} y_1^{r_1 y_1}.$$

We can see $(A_1', B_1')$ is an ElGamal encryption of $g_1^{r_1}$ by the encryption key $y_1$ of the server $S_1$.

Because $y_1 = g_1^{r_1}$, we have

$$K_1 = (B_1' / A_1'^{r_1})^{r_1} = (g_1^{r_1} y_1^{r_1} / (g_1^{r_1})^{r_1})^{r_1} = (g_1^{r_1} y_1^{r_1} / y_1^{r_1})^{r_1} = g_1^{r_1 r_1}.$$  

In addition,

$$R_1 = A_1'^{r_1} r_1^{r_1} = (g_1^{r_1})^{r_1} r_1^{r_1} = g_1^{r_1 r_1}.$$  

Therefore, $K_1 = K_1$. By the symmetric property, we can prove $K_1' = K_2$ in the same way.

Because $h_1 = H(K_1, 0) \oplus b_1, h_2 = H(K_2, 0) \oplus b_2$, we have

$$H(K_1', 0) \oplus h_1 \oplus h_2 = H(K_1', 0) \oplus H(K_2', 0) \oplus H(K_1, 0) \oplus b_1 \oplus H(K_2, 0) \oplus b_2 = b_1 \oplus b_2 = H(pwC),$$  

In view of this, the client $C$ accepts the messages $M_4$ and $M_5$, broadcasts $h_1' = H(K_1', 1) \oplus h_1$, $h_2' = H(K_2', 1) \oplus H(K_2', 0) \oplus h_2$ to two servers $S_1$ and $S_2$, and computes two secret session keys $SK_1' = H(K_1', 2)$ and $SK_2' = H(K_2', 2)$.
At last, because $H(K_1, 1) \oplus b_1 = H(K_1, 1) \oplus (H(K_1, 0) \oplus b_1) = h'_1$, the server $S_1$ accepts the message $M_6$ and computes the secret session key $SK_1 = H(K_1, 2)$. It is obvious that $SK_1 = SK'_1$ because $K_1 = K'_1$. In the same way, we can prove that $SK_2 = SK'_2$. \qed

\section{Security of Our Protocol}

In this section, we will provide security proof of our protocol against the passive attack and the active attack, respectively.

\subsection{Security against Passive Attack}

Since our protocol is symmetric, we only consider the passive attack, where the passive adversary $A$, who has compromised the server $S_2$ and is able to play the role of $S_2$ and monitor all communications between $S_1$ and $C$, attempts to learn the secret session key established between the server $S_1$ and the client $C$.

The hash function is for authentication purpose instead of key exchange purpose. To simplify the security analysis, we treat $K_1$ instead of $SK_1 = H(K_1, 2)$ as the secret session key derived by the server $S_1$ for the client $C$, and treat $K'_1$ instead of $SK'_1 = H(K'_1, 2)$ as the secret session key derived by the client $C$ for the server $S_1$, and ignore the communication of hash values in our protocol. Like [3], [19], [20], [21], we define the security of our protocol with a game, where after establishing a secret session key $K_1(K'_1)$, the adversary $A$ is provided with either $K_1(K'_1)$ or a random element in $G$ with equally probability to guess. $A$ wins the game if $A$ can guess correctly.

\begin{definition}
Our protocol (without communication of hash values) is secure against the passive attack if no PPT adversary can win the above game with a probability more than $1/2$ plus a nonnegligible value.
\end{definition}

\begin{theorem}
Under the DDH assumption, our protocol (without communication of hash values) is secure against the passive attack.
\end{theorem}

\begin{proof}
If our protocol is insecure against the passive attack, i.e., the passive adversary $A$ can win the above game with a probability more than $1/2$ plus a nonnegligible value, we can use $A$ as a subroutine to solve the DDH problem as follows:

Suppose that we challenge a DDH problem $(g^a, g^b, Z)$ where $Z$ is either $g^c$ or a random element in $G$ with equal probability. First of all, we run the initialization and the registration for the client $C$ and forward the pairs $(a, b, A, B) = \{a_1, a_2, b_1, A_1, B_1\}$ to the adversary $A$. Under the DDH assumption, the ElGamal encryption scheme is semantically secure [12] and thus $A$ is unable to distinguish an encryption of $g^{ap_{sc}}$ from the encryption of $g^{a}g^{p_{sc}}Z$ under the encryption key $(g^a)^{x_1}$ without knowledge of the decryption key $x_1$. With reference to Fig. 2, we let the client $C$ broadcast $R = g^{al_2}g^{p_{sc}}$ to $S_1$ and $S_2$ (played by the passive adversary $A$), which follow the protocol and exchange $\{c_1, B'_1\}$ and $\{c_2, B'_2\}$. In $S_1$, we let $R = (A_1)^{x_1} = (g^{al_1})^{x_1}$, $K_1 = B'_1/A_1^{x_1} = Z^{x_1}$, where $r_2$ is randomly chosen by $A$, and then $S_1$ replies $C$ with $\{R_1\}$. In $S_2$, the passive adversary $A$ computes $R_2 = (A'_2)^{x_1} = (g_{a_2})^{x_2}$, $K_2 = (B'_2/A'_2)^{x_1} = (g^{a_2})^{x_2}$ with knowledge of $(x_2, a_2)$, where $r_1, r'_1$ are randomly chosen by $S_1$ and $A$, respectively, and then $A$ replies $C$ with $\{R_2\}$. After the client $C$ receives $R_1$ and $R_2$, we let $K'_1 = Z^{x_1}$.

In this experiment, the exchanged messages are available to $A$. When $Z = g^{a_1}$, this experiment is exactly the same as our protocol in the view of $A$.

Next, $A$ is provided $K_1(K'_1)$ or a random element in $G$ with equal probability. If $A$ guesses correctly, we conclude $Z = g^{a_1}$. Otherwise, we conclude $Z$ is a random element in $G$. Since $A$ can win the game with a probability more than $1/2$ plus a nonnegligible value, we can distinguish $g^{a_1}$ from a random element in $G$ in the DDH problem with a probability more than $1/2$ plus a nonnegligible value. This contradicts with the DDH assumption. Therefore, our protocol is secure against the passive attack and the theorem is proved. \qed

\subsection{Security against Active Attack}

We first consider the active attack to the honest server, where an active adversary $A$, who has compromised $S_2$ and pretend to be the server $S_2$ and the client $C$ to communicate with the server $S_1$, attempts to learn the secret session key $K_1$ derived by $S_1$ for $C$. Like our security analysis on the passive attack, we ignore the communication of hash values. We define the security of our protocol with a game, where after the server $S_1$ computes $K_1$, the adversary $A$ is provided with either $K_1$ or a random element in $G$ with equally probability to guess. $A$ wins the game if $A$ can guess correctly.

\begin{definition}
Our protocol is secure against the active attack to the honest server if no PPT adversary can win the above game with a probability more than $Q/N + 1/2$ plus a nonnegligible value, where $N$ is the size of the dictionary $D$ from which the password is randomly chosen and $Q$ is the number of queries that the adversary can try.
\end{definition}

\begin{definition}
Our protocol is secure against the active attack to the honest server if no PPT adversary can win the above game with a probability more than $Q/N + 1/2$ plus a nonnegligible value, where $N$ is the size of the dictionary $D$ from which the password is randomly chosen and $Q$ is the number of queries that the adversary can try.
\end{definition}

To prove the security of our protocol against the active attack, we need two variants of the DDH assumption as follows:

\begin{itemize}
  \item \textit{vDDH1 assumption.} Consider a cyclic group $G$ of large prime order $q$ with a generator $g$. The vDDH1 assumption states that, given $(G, g, g^a, g^{a_1})$ for randomly chosen $a, b$ from $\mathbb{Z}_q$, no PPT algorithm can distinguish $g^a$ from a random element in $G$ with a probability more than $1/2$ plus a nonnegligible value.
  \item \textit{vDDH2 assumption.} [7]: Consider a cyclic group $G$ of large prime order $q$ with a generator $g$. The vDDH2 assumption states that, given $(G, g, h, g^{a_1})$ for randomly chosen $a$ from $\mathbb{Z}_q$ and $h$ from $G$, no PPT algorithm can distinguish $h^a$ from a random element in $G$ with a probability more than $1/2$ plus a nonnegligible value.
\end{itemize}

\begin{remark}
The vDDH2 assumption has been used in [30] and [18] to prove the security of their protocols.
\end{remark}

\begin{theorem}
Under the DDH, vDDH1, and vDDH2 assumptions, our protocol (without communication of hash values) is secure against the active attack to the honest server.
\end{theorem}
Proof. We provide a sketch of security proof in Section 1 of our supplementary material, which can be found on the Computer Society Digital Library at http://doi.ieeecomputersociety.org/10.1109/TPDS.2012.282.

Next, we consider the active attack to the client C, where an active adversary A, who has compromised the server S2 and pretends to be the servers S1 and S2 to communicate with the client C, attempts to learn the secret session key $K'_1$ derived by C for S1 after C accepts the messages $M_1$ and $M_2$. Because the client authenticates the messages $M_1$ and $M_2$ by hash function $H$, we will take in account the communication of hash values in this security analysis. We define the security of our protocol with a game, where after accepting the messages $M_1$ and $M_2$, the client C computes $K'_1$, and the adversary A is provided with either the secret session key $SK'_1 = H(K'_1, 2)$ or an random element with equally probability to guess. A wins the game if A can guess correctly.

Definition 4. Our protocol is secure against the active attack to the client C if no PPT adversary can win the above game with a probability more than $Q/N$ plus a nonnegligible value, where $N$ is the size of the dictionary D from which the password is randomly chosen and $Q$ is the number of queries that the adversary can try.

Theorem 4. Under the DDH, vDDH1, and vDDH2 assumptions, our protocol (with communications of hash values) is secure against the active attack to the client if the hash function $H$ is one-way and collision-free.

Remark. A hash function $H$ is said to be one-way if given a hash value $h$, it is computationally infeasible to find some input $x$ such that $H(x) = h$. If, given a message $x$, it is computationally infeasible to find a message $y$ not equal to $x$ such that $H(x) = H(y)$ then $H$ is said to be a weakly collision-free hash function. A strongly collision-free hash function $H$ is one for which it is computationally infeasible to find any two messages $x$ and $y$ such that $H(x) = H(y)$.

Proof. We provide a sketch of security proof in Section 2 of our online supplementary material.

Our protocol provides explicit authentication in the sense that each party know that other parties have established their secret session keys correctly if the message authentication by the party succeeds. If the client C accepts the messages $M_1$ and $M_2$, the client C is confirmed that the servers S1 and S2 will compute their secret session keys with the client C correctly. If the server S1 accepts the message $M_0$, the server S1 is confirmed that the client C has computed the same secret session key $SK'_1$, and the client C and the server S2 have established their secret session key correctly.

6 PERFORMANCE ANALYSIS

In this section, we analyze the performance of our protocol and compare our protocol with existing protocols for two-server password-only authentication and key exchange.

<table>
<thead>
<tr>
<th>Participants</th>
<th>KMTG Protocol</th>
<th>Our Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>comm. &gt; 15L</td>
<td>comm. 3L + 4L</td>
</tr>
<tr>
<td></td>
<td>comp. &gt; 20</td>
<td>comp. 4</td>
</tr>
<tr>
<td></td>
<td>rounds 3</td>
<td>rounds 4</td>
</tr>
<tr>
<td>Server</td>
<td>comm. &gt; 19L</td>
<td>comm. 6L + 3L</td>
</tr>
<tr>
<td></td>
<td>comp. &gt; 26</td>
<td>comp. 5</td>
</tr>
<tr>
<td></td>
<td>rounds 5</td>
<td>rounds 4</td>
</tr>
</tbody>
</table>

With reference to Fig. 2, we can see that both servers in our protocol equally contribute to authentication and key exchange and have the same communication and computation complexity. We only need to analyze the performance of one server.

As far as the server S1 is concerned, it receives $M_1$ from the client C, exchanges $M_2, M_3$ with the server S2, replies $M_4$ to C, and receives $M_5$ from C. The total communication complexity for S1 is $6L + 3q$, where $L$ is the size of a group element in $G$ and $q$ is the size of the hash value, i.e., $\log_2 q$. The total computation complexity for S1 is five exponentiations in $G$.

The client C broadcasts $M_1$ to S1 and S2, receives $M_4$ and $M_5$ from S1 and S2, respectively, and broadcasts $M_6$ to S1 and S2. The total communication complexity for C is $3L + 4q$, almost half of the communication complexity for S1. The total computation complexity is four exponentiation.

In terms of parallel computation, our protocol has four communication rounds only. The client C broadcasts $M_1$ to the two servers S1 and S2 in the first round; S1 and S2 exchange $M_2$ and $M_3$ in the second round; S1 and S2 both reply C with $M_4$ and $M_5$ in the third round; C broadcasts $M_6$ in the last round. The client C is involved in three communication rounds.

A naive solution for two-server password-only authentication and key exchange can be implemented by running two parallel password-authenticated key exchange (PAKE) sessions between the client and both servers, respectively. At the end, both servers confirm to each other the outcome of the authentication process. This solution can be constructed with any existing efficient two-party PAKE protocol, like [1], [2], but is impractical because the client is required to remember two passwords, a different one for each server.

To the best of our knowledge, Katz et al.’s protocol [20], called the KMTG protocol for brevity, is the only existing symmetric protocol for two-server password-only authentication and key exchange. The performance comparison of our protocol with the KMTG protocol is shown in Table 1. From Table 1, we can see that our protocol is much more efficient than the KMTG protocol in both the client and the server sides.

The performance comparison of our protocol with Jin et al.’s protocol [18], called the JWX protocol for brevity, and Yang et al.’s protocol [30], called the YDB protocol for brevity, is shown in Table 2.

From Table 2, we can see that 1) our protocol in the client side is more efficient than both the YDB protocol and the JWX protocol; 2) our protocol in one of two servers is more efficient than both the YDB protocol and the JWX protocol in the SS; but 3) our protocol in another server is slightly
TABLE 2
Performance Comparison of Our Protocol with YDB and JWX Protocols

<table>
<thead>
<tr>
<th>Participants</th>
<th>YDB Protocol</th>
<th>JWX Protocol</th>
<th>Our Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client C</td>
<td>(6L + 2\ell) bits</td>
<td>(6L + 3\ell) bits</td>
<td>(6L + 4\ell) bits</td>
</tr>
<tr>
<td></td>
<td>comp. 5</td>
<td>comp. 6</td>
<td>comp. 4</td>
</tr>
<tr>
<td></td>
<td>rounds 6</td>
<td>rounds 3</td>
<td>rounds 4</td>
</tr>
<tr>
<td>Server (S_1) (SS)</td>
<td>(8L + 3\ell) bits</td>
<td>(11L + 3\ell) bits</td>
<td>(6L + 3\ell) bits</td>
</tr>
<tr>
<td></td>
<td>comp. 6</td>
<td>comp. 8</td>
<td>comp. 5</td>
</tr>
<tr>
<td></td>
<td>rounds 10</td>
<td>rounds 6</td>
<td>rounds 4</td>
</tr>
<tr>
<td>Server (S_2) (CS)</td>
<td>(4L + 3\ell) bits</td>
<td>(5L + 3\ell) bits</td>
<td>(6L + 3\ell) bits</td>
</tr>
<tr>
<td></td>
<td>comp. 3</td>
<td>comp. 4</td>
<td>comp. 5</td>
</tr>
<tr>
<td></td>
<td>rounds 4</td>
<td>rounds 3</td>
<td>rounds 4</td>
</tr>
<tr>
<td>Total</td>
<td>(8L + 3\ell) bits</td>
<td>(11L + 3\ell) bits</td>
<td>(6L + 3\ell) bits</td>
</tr>
<tr>
<td>(Server Side)</td>
<td>comp. 9</td>
<td>comp. 12</td>
<td>comp. 5</td>
</tr>
<tr>
<td></td>
<td>rounds 10</td>
<td>rounds 6</td>
<td>rounds 4</td>
</tr>
</tbody>
</table>

less efficient than the YDB protocol and the JWX protocol in the CS.

Note that the YDB protocol and the JWX protocol are asymmetric, where only the front-end server and the client agree on a secret session key in the end. Our protocol is symmetric, where the client agrees on two different secret keys with the two servers in the end, respectively. In addition, the YDB protocol and the JWX protocol run in series, while our protocol runs in parallel.

In terms of parallel computation, our symmetric protocol has a feature that the total running time in the two-server side is equal to the total running time of one server, i.e., transmitting \(6L + 3\ell\) bits and computing five modular exponentiations in four rounds. However, in the asymmetric YDB protocol and the asymmetric JWX protocol, the total running time in the two-server side is equal to the sum of two servers’ running time, i.e., transmitting \(8L + 3\ell\) bits and computing nine modular exponentiations in 10 rounds in the YDB protocol, and transmitting \(11L + 3\ell\) bits and computing 12 modular exponentiations in six rounds in the JWX protocol. Even if the precomputation is allowed, the two servers in the YDB protocol or the JWX protocol still need to compute seven modular exponentiations in series. Therefore, our protocol is even more efficient than the asymmetric YDB protocol and the asymmetric JWX protocol in terms of the total running time.

Our protocol need more storage to keep the password authentication information in the two servers than the YDB protocol and the JWX protocol. Because of rapidly declining data storage costs, the difference in storage costs between our protocol and the YDB and JWX protocols is not significant.

7 Conclusion
In this paper, we have presented a symmetric protocol for two-server password-only authentication and key exchange. Security analysis has shown that our protocol is secure against passive and active attacks in case that one of the two servers is compromised. Performance analysis has shown that our protocol is more efficient than existing symmetric and asymmetric two-server PAKE protocols.

Acknowledgments
The authors would like to appreciate valuable comments from blind reviewers. These comments are really helpful for us to improve this paper. This work was done during his visit to Division of Mathematical Sciences, the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore, and partially supported by the Singapore National Research Foundation Competitive Research Program grant NRF-CRP2-2007-03. This work was partially supported by the Singapore National Research Foundation Competitive Research Program grant NRF-CRP2-2007-03.

References


