<table>
<thead>
<tr>
<th>Authors</th>
<th>Y. KOBAYASHI, N. YANAI, K. YONEYAMA, T. NISHIDE, G. HANAOKA, K. KIM, E. OKAMOTO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Journal</td>
<td>IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences</td>
</tr>
<tr>
<td>Volume</td>
<td>E100.A</td>
</tr>
<tr>
<td>Issue/Number</td>
<td>12/2991-3006</td>
</tr>
<tr>
<td>Year</td>
<td>2017</td>
</tr>
<tr>
<td>Copyright</td>
<td>© 2017 The Institute of Electronics, Information and Communication Engineers</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2241/00150563">http://hdl.handle.net/2241/00150563</a></td>
</tr>
<tr>
<td>DOI</td>
<td>10.1587/transfun.E100.A.2991</td>
</tr>
</tbody>
</table>

The page contains a table with the following columns:

- **著者** (Authors)
- **タイトル** (Title)
- **掲載誌** (Journal)
- **巻号** (Volume)
- **号及びページ** (Issue/Number)
- **発行年** (Year)
- **著作権** (Copyright)
- **URL** (URL)
- **DOI** (DOI)

The table summarizes the publication details, including the authors, journal, volume, issue, page range, year, copyright, URL, and DOI.
Provably Secure Gateway Threshold Password-Based Authenticated Key Exchange Secure against Undetectable On-Line Dictionary Attack**

Yukou KOYAYASHI†*, Nonmember, Naoto YANAI†††, Kazuki YONEYAMA††††, Takashi NISHIDE††*†, Members, Goichiro HANAOKA†††††, Nonmember, Kwangjo KIM††††††, Member, and Eiji OKAMOTO††††††, Fellow

SUMMARY By using Password-based Authenticated Key Exchange (PAKE), a server can authenticate a user who has only the same password shared with the server in advance and establish a session key with the user simultaneously. However, in the real applications, we may have a situation where a user needs to share a session key with server A, but the authentication needs to be done by a different server B that shares the password with the user. Further, to achieve higher security on the server side, it may be required to make PAKE tolerant of a server breach by having multiple authentication servers. To deal with such a situation, Abdalla et al. proposed a variant of PAKE called Gateway Threshold PAKE (GTPAKE) where a gateway corresponds to the aforementioned server A being an online service provider and also a potential adversary that may try to guess the passwords. However, the schemes of Abdalla et al. turned out to be vulnerable to Undetectable On-line Dictionary Attack (UDonDA). In this paper, we propose the first GTPAKE provably secure against UDonDA, and in the security analysis, we prove that our GTPAKE is secure even if an adversary breaks into parts of multiple authentication servers.

key words: password-based authenticated key exchange, threshold cryptography

1. Introduction

1.1 Background

Password-based authenticated key exchange (PAKE) [3]–[6], [13], [15] is a two-party protocol by which a user and an authentication server can establish a cryptographic key that is computationally hard to guess by sharing only the same human-memorable password in advance. PAKE can be useful because it does not assume a public-key infrastructure that requires the user to bring a device storing public-key related data. PAKE will also fit in well with computational environments where simple and secure ubiquitous access is needed.

Although PAKE is useful, there exist situations where (two-party) PAKE cannot be deployed as is. For instance, in the case of a global roaming service, a user (who is located abroad) may receive the service from an external server (called a gateway which can be considered as a service provider) by establishing a session key with the server, but in PAKE, it is assumed that the authentication server is the service provider at the same time. Hence, traditional PAKE will not function in such a context because the gateway is different from the authentication server. Furthermore, as the European Network and Information Security Agency (ENISA) [10] pointed out the potential threat of malicious servers, it is desirable to take into consideration the existence of malicious authentication servers to achieve high security. However, traditional PAKE will not be sufficient because only a single authentication server is supposed to be involved. Even if the server is trusted, software vulnerabilities can lead to a leakage of important data as shown by Heartbleed in April 2014 [11] where the vulnerability of OpenSSL can cause a leakage of the passwords stored in servers. Therefore, traditional PAKE cannot cope with such a threat.

To tackle those problems, Abdalla et al. proposed Gateway PAKE (GPAKE) [1] by introducing an entity called a gateway into PAKE and Gateway Threshold PAKE (GT-PAKE) [1] by further having multiple authentication servers. However, as shown in [8], these schemes of Abdalla et al. turn out to be vulnerable to Undetectable On-line Dictionary Attack (UDonDA) in which an adversary mounts a password guessing attack in the on-line transaction and the attack cannot be detected by the authentication servers [9]. Although, in [2], it is mentioned that these protocols can be modified such that the authentication server can detect on-line dictionary attacks, the details of how it can be done and the security proof were not described. In the schemes of Abdalla et al., the authentication server responds and sends a message without authenticating the user, so the adversary can make on-line attempts to guess the password repeatedly. Due to the low entropy of the password, that attack becomes devastating. Hence, it is needed to propose a new GTPAKE scheme that overcomes UDonDA.

Copyright © 2017 The Institute of Electronics, Information and Communication Engineers
Table 1  Comparison of the existing GPAKE and GTPAKE schemes.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>User</th>
<th>Gateway</th>
<th>Server</th>
<th>Message</th>
<th>Assumption</th>
<th>Model</th>
<th>Threshold</th>
<th>UDonDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPAKE [1]</td>
<td>2e</td>
<td>2e</td>
<td>2e</td>
<td>4</td>
<td>PCDDH</td>
<td>ROM</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>GTPAKE [1]</td>
<td>2e</td>
<td>2e</td>
<td>(13n + 18)e</td>
<td>3n + 4</td>
<td>PCDDH</td>
<td>ROM</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>GPAKE [18]</td>
<td>3e</td>
<td>2e</td>
<td>2e</td>
<td>6</td>
<td>DDH</td>
<td>ROM</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>GPAKE [20]</td>
<td>5e + E</td>
<td>2e</td>
<td>5e + E</td>
<td>6</td>
<td>DDH</td>
<td>Standard</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>GPAKE [19]</td>
<td>3e</td>
<td>2e</td>
<td>2e</td>
<td>9</td>
<td>CDH</td>
<td>ROM</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>Our GTPAKE</td>
<td>6e</td>
<td>2e</td>
<td>(2n^2 + 19n + 11)e</td>
<td>4n + 11</td>
<td>DDH</td>
<td>ROM</td>
<td>YES</td>
<td>YES</td>
</tr>
</tbody>
</table>

The computational costs for the user, gateway, and authentication server are estimated in the User, Gateway, and Server columns, respectively. Especially, the computational costs of [20] here are the ones recalculated by us. We use modular exponentiation denoted as “e” because modular exponentiation is the most expensive computation and “E” means the cost of a public key encryption. For the sake of simplicity, n authentication servers participate in the authentication phase. In the Message column, the number of communications is shown and we evaluate a broadcast to all authentication servers as n communication costs. In the Assumption column, the hardness assumption is shown. In the Model column, the random oracle model or the standard model is shown. In the Threshold column, it is shown whether the protocol tolerates the corruption of authentication servers. In the UDonDA column, it is shown whether the protocol can detect malicious login attempts for guessing the passwords of users.

1.2 Contribution

We propose new GTPAKE which has resistance of UDonDA and the corruption of authentication servers. We adapt the security model of GPAKE [1], [18] to that of GTPAKE and prove the security of our GTPAKE under standard assumptions in the random oracle model. The proposed scheme has the stronger security against a malicious gateway or authentication servers compared with existing schemes, and a global roaming service used for users regardless of places and devices is expected to be one of its applications.

A naive extension of GPAKE where the communication process is not changed and the process of authentication servers is adapted to the threshold secret sharing does not lead to GTPAKE. Even if the password is encrypted and the secret key for encrypting the password is shared among the authentication servers, the password itself needs to be decrypted to compare the registered password with the login password, which means the leakage of password to an adversary corrupting authentication servers. To overcome this problem, in the authentication process, the servers decrypt the encrypted password partially and authenticate a user simultaneously without revealing the password itself.

We compare the proposed scheme with other existing GPAKE and GTPAKE schemes\(^1\). As shown in Table 1, the computation and communication costs of our protocol are not better than those of GTPAKE [1]. However, Szydllo shows that the Chosen-basis Decisional Diffie-Hellman (CDDH) assumption on which the schemes of Abdalla et al. are based is already vulnerable to some attacks [17]. The security of our scheme is proven in the random oracle model with the DDH assumption. Similarly to GTPAKE of Abdalla et al., our scheme tolerates the corruption of some authentication servers. Furthermore, while the schemes of Abdalla et al. are vulnerable to UDonDA, our scheme is invulnerable to this attack, although our proof similar to [18] is given in the non-concurrent setting, which assumes that a new session does not begin until the previous session is finished.

The organization of the paper is as follows. In Sect. 2, we introduce some background to understand this paper. In Sect. 3, we define the security model of GTPAKE. In Sect. 4, we describe the construction of our scheme. In Sect. 5, we prove the security of the proposed scheme. In Sect. 6, we make final remarks. Finally, we explain the reason why the proposed scheme needs a commitment scheme in Appendix A and the bound related to the birthday problem in Appendix B.

2. Preliminaries

We show the notation and security assumptions used in this paper.

2.1 Notation

We use the following notation throughout this paper. We denote by \( \mathbb{Z}_q \) the set \( \{0, 1, \ldots, q - 1\} \).\(^{1}\) \( x \leftarrow A \) represents that \( x \) is chosen uniformly at random from set \( A \). Let \( g \) be a generator of the subgroup \( \mathcal{G} \) of order \( p \) over \( \mathbb{Z}_q \) and \( a \parallel b \) be the concatenation of elements \( a \) and \( b \), which is able to be divided into its original elements. We denote by \( [0, 1]^k \) the set of all binary strings of length \( k \). Especially, \( [0, 1]^\ast \) means the set of all binary strings of arbitrary length. The function \( \text{negl} \) is negligible if and only if, for every positive integer \( c \), there exists an integer \( N \) such that \( \text{negl}(x) < 1/x^c \) for any \( x > N \).

We represent a user as \( U \in \mathcal{U} \), a gateway as \( G \in \mathcal{G} \), and the \( i \)-th authentication server as \( S_i \in \mathcal{S} \) for \( i = 1, \ldots, n \) where \( \mathcal{U} \), \( \mathcal{G} \), and \( \mathcal{S} \) are the sets of all users, gateways, and authentication servers, respectively, and \( n \) is the number of all authentication servers. Especially, we denote by \( P \) any participant in the set of all participants \( \mathcal{P} \) (= \( \mathcal{U} \cup \mathcal{G} \cup \mathcal{S} \)). We call one representative of the authentication servers that communicates with a gateway a combiner \( C \in \mathcal{S} \). We set \( t \) (\( < n/2 + 1 \)) as the threshold value which is the minimum number of servers required to authenticate users.

\(^{1}\)In the comparison here, we focus only on schemes with security proofs, and the discussion of schemes without security proofs can be found in [18].
2.2 Security Assumptions

The following security assumptions are well-known.

**Definition 1:** (Computational Diffie-Hellman (CDH) Assumption). We define the Computational Diffie-Hellman (CDH) problem as the problem of computing $g^{ab}$ from given $(g, g^a, g^b)$ where $g$ is a generator chosen at random from group $\mathbb{G}$ and $(a, b) \leftarrow \mathbb{Z}_q^2$. We say that the CDH assumption holds in $\mathbb{G}$ if the advantage in solving the CDH problem defined as $\text{Adv}_{\mathcal{A}}(\kappa) = \Pr[\mathcal{A}(g, g^a, g^b) = g^{ab}]$ is negligible for any probabilistic polynomial time algorithm $\mathcal{A}$ with respect to the security parameter $\kappa$.

**Definition 2:** (Decisional Diffie-Hellman (DDH) Assumption). We define the Decisional Diffie-Hellman (DDH) problem as the problem of distinguishing the distribution of $(g, g^a, g^b, g^{ab})$ and $(g, g^a', g^b', g'^{ab})$ where $g$ is a generator chosen at random from group $\mathbb{G}$ and $(a, b, c) \leftarrow \mathbb{Z}_q^3$. We say that the DDH assumption holds in $\mathbb{G}$ if the advantage in solving the DDH problem defined as $\text{Adv}_{\mathcal{A}}(\kappa) = \Pr[\mathcal{A}(g, g^a, g^b, g^{ab}) = 1] - \Pr[\mathcal{A}(g, g^a', g^b', g'^{ab}) = 1]$ is negligible for any probabilistic polynomial time algorithm $\mathcal{A}$ with respect to the security parameter $\kappa$.

2.3 Building Block

We use the non-interactive zero-knowledge proof of equality of discrete logarithm as the building block in a similar manner to GTPAKE of Abdalla et al. [1]. We describe the proof system between a prover and a verifier as follows.

Two generators $(g_1, g_2)$ over a group $\mathbb{G}$ are given and let $\text{EDLog}_{(g_1, g_2)}$ be the language pairs $(x_1, x_2) \in \mathbb{G}^2$ where there exists a random number $x \in \mathbb{Z}_q$ such that $x_1 = g_1^x$ and $x_2 = g_2^x$. The prover chooses $y \leftarrow \mathbb{Z}_q$ and computes $y_1 = g_1^y$ and $y_2 = g_2^y$. After computing $c = H_0(q \parallel g_1 \parallel g_2 \parallel x_1 \parallel x_2 \parallel y_1 \parallel y_2)$ where $H_0$ is a hash function mapping $\{0,1\}^* \rightarrow \mathbb{Z}_q$, the prover computes $z = xc + y \mod q$ and sends $(c, z)$ to the verifier. The verifier checks the equation $c = H_0(q \parallel g_1 \parallel g_2 \parallel x_1 \parallel x_2 \parallel g_1^x/x_1^2 \parallel g_2^x/x_2^2)$. 

3. Security Model

We describe the system model and security definitions of GTPAKE.

As Fig. 1 shows the communication model of GTPAKE, the user as the client connects to a gateway playing the role of the service provider. The gateway has a role of forwarding the message to one of the authentication servers named the combiner. Here the authentication servers play the role of authentication service provider. The combiner communicates with other servers to authenticate the user. Although the communication channel between the user and the gateway is insecure and under the control of an adversary, the channel between the gateway and the combiner is authenticated and the channel between the authentication servers is secure.

When an authentication process for a user (say, User A) is being processed, another login attempt from the same user (i.e., User A) is suspended until the preceding authentication process is finished. We assume a static adversary that corrupts the set of less than the threshold authentication servers before the protocol is executed.

3.1 System Model

The proposed scheme consists of the following three sub-protocols.

- **Init.** Given the security parameter and the setup parameters, the public parameters $\text{params}$ are output$^{11}$. 
- **Regi.** The user registers his password with the authentication servers. If all authentication servers cannot register the password successfully, then outputs the error symbol $\bot$. 
- **Auth.** The more than or equal to the threshold servers authenticate a user. If the user and gateway can establish the same session key while passing authentication successfully, then outputs a session key $sk$, otherwise outputs $\bot$.

3.2 Security Requirements

We describe the security requirements for GTPAKE. The technical details of reflecting these requirements are given in Definitions 4 and 6.

3.2.1 Existing Security Requirements

The security requirements for not only GPAKE but also GTPAKE are as follows (due to Wei et al. [18]).

- **Known-Key Security (KS).** The adversary cannot distinguish a real session key from a random session key even if the adversary obtains other session keys. 
- **Forward Secrecy (FS).** The established session key before the adversary obtains the static keys of the user including passwords are still indistinguishable from a random session key.

$^{11}$To establish an authenticated or secure channel, both parties (i.e., the gateway and combiner, the combiner and authentication server, and pairs of authentication servers) have a common static key.

$^{11}$Although we assume a trusted dealer distributing some parameters for simplicity, the authentication servers themselves can publish parameters by using the technique of the distributed key generation [12].
• **Resistance to Basic Impersonation (BI).** The adversary cannot impersonate a legitimate user unless the adversary obtains the password of the user.

• **Resistance to Off-line Dictionary Attack (orrDA).** The adversary cannot guess a password by verifying its guess in the off-line manner.

• **Resistance to Undetectable On-line Dictionary Attack (UDonDA).** The adversary cannot guess a password by verifying its guess in the on-line manner without being detected by uncorrupted participants.

3.2.2 Modified Security Requirements

We adapt the security requirements of GPAKE to that for the threshold setting. Unlike the single server setting where the adversary does not corrupt the authentication server in GPAKE, we take an active adversary corrupting less than threshold authentication servers into consideration in GTPAKE.

• **Resistance to leakage of internal information to servers (LIS).** An adversary cannot distinguish a real session key from a random session key and cannot guess the password even if the adversary obtains internal information of some authentication servers.

3.3 Oracles

We show the necessary oracles to define a stronger security model than that of GTPAKE [1]. To distinguish the session between participants, the ℓ-th instance for participant \( P \) is denoted by \( P^{(\ell)} \). Let \( U^{(\ell)}, G^{(\ell)}, C^{(\ell)}, \) and \( S_i^{(\ell)} \) be instances of a user, gateway, combiner, and \( i \)-th authentication server, respectively. The instance represents the state of a participant in a session during the progress of the protocol.

3.3.1 Existing Oracles [18]

The oracles used in the existing GPAKE are as follows.

- **Execute** \((U^{(\ell)}, G^{(\ell)}, C^{(\ell)})\). This query models passive attacks. The output of this query consists of the message exchanged during the execution in the protocol among \( U^{(\ell)}, G^{(\ell)}, \) and \( C^{(\ell)} \).

- **SendUser** \((U^{(\ell)}, m)\). This query models active attacks against a user instance \( U^{(\ell)} \). The output of this query consists of the message the user instance \( U^{(\ell)} \) would generate on receipt of message \( m \).

- **SendGateway** \((G^{(\ell)}, m)\). This query models active attacks against a gateway instance \( G^{(\ell)} \). The output of this query consists of the message the gateway instance \( G^{(\ell)} \) would generate on receipt of message \( m \).

- **SendServer** \((C^{(\ell)}, m)\). This query models active attacks against a combiner instance \( C^{(\ell)} \). The output of this query consists of the message the combiner instance \( C^{(\ell)} \) would generate on receipt of message \( m \).

- **SessionKeyReveal** \((P^{(\ell)})\). This query models leakage of session keys related to information of passwords. If the session key for the instance of participant \( P^{(\ell)} \) is not defined, then return 1. Otherwise, return the session key for \( P^{(\ell)} \).

- **StaticKeyReveal** \((P)\). This query models leakage of the static secrets of participant \( P \). If \( P \) is a user, then return the password. If \( P \) is a gateway, then return secret keys for authenticated channels. If \( P \) is an authentication server, then return the encrypted passwords for all users, the share of a secret key, the published parameters for all authentication servers, and other secret keys for authenticated and secure channels.

- **EstablishParty** \((U, pw_U)\). This query models that an adversary registers a password \( pw_U \) on behalf of a user \( U \). The users against whom the adversary has not ask this query are called honest.

- **Test** \((P^{(\ell)})\). This query models the indistinguishability of the session key of \( P^{(\ell)} \). At the beginning of the experiment the challenge bit \( b \) is chosen from \( \{0, 1\} \). If the session key for \( P^{(\ell)} \) is not defined, then return 1. Otherwise, return session key of \( P^{(\ell)} \) if \( b = 1 \) or a random key of the same size if \( b = 0 \). The adversary can ask this query only once at any time during the experiment.

- **TestPassword** \((U, pw_U)\). This query models the secrecy of the password held by an honest user \( U \). If the guessed password \( pw'_U \) equals the registered password \( pw_U \) of the user \( U \), then return 1. Otherwise, return 0. The adversary can ask this query only once at any time during the experiment.

3.3.2 Added Oracles

We add a new oracle to adapt the single server setting to the threshold setting where an adversary can obtain internal information of authentication servers by corruption.

- **Corrupt** \((S_i)\). This query models intrusion into the authentication server. By asking the query at the beginning of the protocol, the adversary can take full control of the authentication server \( S_i \).

3.4 Security Definitions

We describe the security definitions of GTPAKE. The defi-
nitions here are similar to those of GPAKE [1], [18], but the method of dealing with authentication servers is different. The Session ID (SID) is provided when the protocol is first initiated to determine the session uniquely. The Partner ID (PID) is taken to be an identifier of the instance intended to establish a session key.

**Definition 3: (Partnering [1]).** A user $U^{(i)}$ and gateway $G^{(j)}$ are partnered if the following conditions hold.

1. $U^{(i)}$ and $G^{(j)}$ exist.
2. $U^{(i)}$ and $G^{(j)}$ have the same SID.
3. The PID of $U^{(i)}$ is $G^{(j)}$ and the PID of $G^{(j)}$ is $U^{(i)}$.
4. No other instances have the same PID of $U^{(i)}$ or $G^{(j)}$.

3.4.1 Session Key Security

For the security of session keys, an adversary can ask the Test oracle once against a *fresh* participant. In the following definition, the adversary is restricted such that the adversary cannot ask queries that break the security of the protocol trivially.

**Definition 4: (Freshness in Session Key Security).** A user $U^{(i)}$ and partnered gateway $G^{(j)}$ are *fresh* if the user is honest and none of the following conditions hold.

1. The adversary asks $\text{SessionKeyReveal}(U^{(i)})$ or $\text{SessionKeyReveal}(G^{(j)})$.
2. The adversary asks $\text{EphemeralKeyReveal}(U^{(i)})$ or $\text{EphemeralKeyReveal}(G^{(j)})$.
3. The adversary asks $\text{SendServer}(C^{(k)}, m)$ and either queries.
   a. $\text{StaticKeyReveal}(G)$.
   b. $\text{StaticKeyReveal}(C)$.
4. The adversary asks $\text{SendUser}(U^{(i)}, m)$ or $\text{SendGateway}(G^{(j)}, m)$ and either queries.
   a. $\text{StaticKeyReveal}(U)$.
   b. $\text{EphemeralKeyReveal}(U^{(i)})$ in any instance $\ell$.
   c. $\text{Corrupt}(S_j)$ for more than or equal to $t$ authentication servers.

To model the attacks which the adversary can mount through the game in the security of session keys, an adversary is allowed to ask the Execute, SendUser, SendGateway, SendServer, SessionKeyReveal, StaticKeyReveal, EphemeralKeyReveal, Corrupt, EstablishParty, and Test oracles. The list of participants is given to the adversary at the beginning of the experiment. In this situation, we define $\text{Succ}^{\text{aks}}$ as the event where an adversary succeeds in guessing a challenge bit $b$ in the Test oracle.

(1) Capturing the security properties of session keys

As described in the condition 1 of Definition 4, KS is reflected by allowing an adversary to obtain session keys in non-target sessions. As described in the condition 2, LIS is reflected by allowing an adversary to obtain the ephemeral and static keys or intermediate results calculated by some authentication servers and by prohibiting the adversary from obtaining the ephemeral keys of users and gateways in the target session. As described in the condition 3, FS is reflected by allowing an adversary to obtain static keys of the users and by prohibiting the adversary from obtaining the static keys of partnered gateways and the combiner. As described in the condition 4, BI is reflected by allowing an adversary to ask queries in non-target sessions and by prohibiting the adversary from obtaining the password of the target user.

**Definition 5: ((T, R)-Session Key Security).** In GPAKE protocol $\mathcal{L}$, the advantage of adversary $\mathcal{A}$ for $(T, R)$-session key security is defined as

$$\text{Adv}^{\text{aks}}_{\mathcal{L}, \mathcal{D}}(\mathcal{A}) = |\Pr[\text{Succ}^{\text{aks}}] - 1/2|,$$

where the password is chosen at random from dictionary $\mathcal{D}$ of size $|\mathcal{D}|$. The maximum advantage among all adversaries that expend at most $T$ time and $R$ resources is defined as

$$\text{Adv}^{\text{aks}}_{\mathcal{L}, \mathcal{D}}(T, R) = \max_{\mathcal{A}} \text{Adv}^{\text{aks}}_{\mathcal{L}, \mathcal{D}}(\mathcal{A}).$$

The $(T, R)$-session key security meets the equation $\text{Adv}^{\text{aks}}_{\mathcal{L}, \mathcal{D}}(T, R) \leq q_{\text{send}}/|\mathcal{D}| + \text{negl}(\kappa)$ for any probabilistic polynomial time adversaries where $q_{\text{send}}(< |\mathcal{D}|)$ is the number of queries to the SendUser and SendServer oracles and $\kappa$ is a security parameter.

3.4.2 Password Protection Security

For the security of passwords, an adversary can ask the TestPassword oracle once against a *fresh* password. In the following definition, the adversary is restricted such that the adversary cannot ask queries that break the security of the protocol trivially.

**Definition 6: (Freshness in Password Protection Security).** The password of a user $U$ is *fresh* if the user is honest and the adversary does not ask the following queries.

1. $\text{StaticKeyReveal}(U)$.
2. $\text{EphemeralKeyReveal}(U^{(i)})$ in any instance $\ell$.
3. $\text{Corrupt}(S_j)$ for more than or equal to $t$ authentication servers.

To model the attacks which the adversary can mount through the game in the security of passwords, an adversary is allowed to ask the SendUser, SendServer, SessionKeyReveal, StaticKeyReveal, EphemeralKeyReveal, Corrupt, EstablishParty, and TestPassword oracles. The list of participants is given to the adversary at the beginning of the experiment. In this situation, we define $\text{Succ}^{\text{pps}}$ as the event where an adversary succeeds in guessing the password $pw_U$ in the TestPassword oracle.

(1) Capturing the security properties of passwords

As described in Definition 6, UDOSDA is reflected by allowing an adversary to ask the SendUser and SendServer oracles until the number of incorrect login attempts exceeds...
a predetermined limit. Also orrDA is reflected by allowing an adversary to obtain internal information such as the ephemeral and static keys of non-target users and a set of less than the threshold corrupted authentication servers. The corrupted combiner can disturb the communication between a user and honest authentication servers, but successful disturbance is not considered as the success of breaking the security of passwords.

**Definition 7:** ($\mathcal{T}, \mathcal{R}$)-Password Protection Security. In GTPAKE protocol $L$, the advantage of adversary $\mathcal{A}$ for ($\mathcal{T}, \mathcal{R}$)-password protection security is defined as

$$
Adv^{\text{ppS}}_{L, \mathcal{D}}(\mathcal{A}) = \Pr[\text{Succ}^{\text{ppS}}],
$$

where the password is chosen at random from dictionary $\mathcal{D}$ of size $|\mathcal{D}|$. The maximum advantage among all adversaries that expend at most $\mathcal{T}$ time and $\mathcal{R}$ resources is defined as

$$
Adv^{\text{ppS}}_{L, \mathcal{D}}(\mathcal{T}, \mathcal{R}) = \max_{\mathcal{A}}\{Adv^{\text{ppS}}_{L, \mathcal{D}}(\mathcal{A})\}.
$$

The ($\mathcal{T}, \mathcal{R}$)-password protection security meets the equation $Adv^{\text{ppS}}_{L, \mathcal{D}}(\mathcal{T}, \mathcal{R}) \leq (q_{\text{send}} + 1)/|\mathcal{D}| + \text{negl}(\kappa)$ for any probabilistic polynomial time adversaries where $q_{\text{send}} (< |\mathcal{D}|)$ is the number of queries to the SendUser and SendServer oracles and $\kappa$ is a security parameter.

4. Our Scheme

4.1 How to Construct GTPAKE

We describe the problems and give an intuitive explanation of our construction. As described in Sect. 1.2, it is difficult to convert GPAKE of Wei et al. (which is secure against UDonDA) into GTPAKE. In fact, the naive extension of GPAKE of Wei et al. is the insecure scheme described in Appendix A. In addition, it seems difficult to make GTPAKE of Abdalla et al. secure against UDonDA. In the schemes of Abdalla et al., it is impossible for an authentication server to terminate the protocol when an incorrect login attempt is made because the message made by an honest user is indistinguishable from that by the adversary. In the proposed scheme, it is possible for authentication servers to compute the result while keeping the password itself secret by realizing decryption and randomization simultaneously. We also use zero knowledge proofs in communication among authentication servers to prevent an adversary from showing incorrect shares.

4.2 Overview of Our Scheme

We describe the flow of our proposed scheme. First, a trusted dealer generates some public system parameters such as the public key $pk$ of the authentication servers. Second, a user registers the ElGamal ciphertext $(PW \cdot pk^e, q')$ with the hash value $PW$ of his password $pw$ and a random number $v$. Third, the user sends $g'/PW$ to the authentication servers via a gateway where $r$ is a random number. After a random number $w$ is generated while hiding the random number among the authentication servers, the combiner sends $g''$ to the user. The user and authentication servers verify the validity of $H(g''^w)$ with each other where $H$ is a hash function. The user sends $g''$ to the gateway where $x$ is a random number. The gateway sends $g''$ to the user where $y$ is a random number. Finally, the session key $H(g''^y)$ is established between the user and the gateway.

4.3 Construction

We show our proposed scheme based on the system model defined in Sect. 3.1. A perspective of the proposed scheme is shown in Fig. 2.

First, we describe the following sub-protocol of initialization. If the number of authentication servers is modified, this sub-protocol is executed again.

**Init.** Let $p$ be a $k$-bit prime where $k$ is the given security parameter and $q$ be a large prime dividing $p - 1$. Let us denote a generator of subgroup $\mathbb{G}$ of order $q$ over $\mathbb{Z}_p$ by $g$.

The hash functions $H_0 : \{0, 1\}^* \rightarrow \mathbb{Z}_q$, $H_1 : \{0, 1\}^* \rightarrow \mathbb{G}$, and $H_2 : \{0, 1\}^* \rightarrow \{0, 1\}^*$ are chosen.

A trusted dealer computes the parameters as follows.

The trusted dealer computes another random generator $h (# g)$ and the public key $pk = g^e$ of a secret key $s \leftarrow \mathbb{Z}_q$ for the ElGamal encryption.

The trusted dealer chooses $a_k \leftarrow \mathbb{Z}_q$ for $k = 1, \ldots, t - 1$ where $t$ is the given threshold value and generates the polynomial $f(z) = s + a_1z + \cdots + a_{t-1}z^{t-1} \mod q$.

The trusted dealer sends a share $s_i = f(i) \mod q$ to each authentication server $S_i$ via a secure channel and publishes $g^e \mod p$ among the authentication servers.

Finally, the public system parameters $\text{params} = (p, q, \mathbb{G}, g, h, pk, H_0, H_1, H_2, H_3)$ are output.

Second, we describe the following sub-protocol of registration.

**Regi.** A new user chooses a password $pw_U$ at random from a dictionary $\mathcal{D}$ and computes $PW_U = H_1(U || pw_U)$ by using his identification $U$.

After generating the ElGamal ciphertext $\text{Enc}(pw_U) = (PW_U \cdot pk^e \mod p, g'^e \mod p)$ where $v \leftarrow \mathbb{Z}_q$, the user sends $(U, \text{Enc}(pw_U))$ to the authentication servers.

This information is stored in all authentication servers as the ciphertext of the password for the user $U$.

If any problems occur, then the error symbol $\perp$ is output.

Third, we describe the following sub-protocol of authentication composed of twelve steps.

**Auth.** If a processing request has come in the invalid order, the incorrect login attempt is counted and the session is rejected. After the counter of incorrect login attempts exceeds the predetermined limit, a processing request from the user
is rejected.

**Step 1.** A user $U$ computes $PW_U = H_1(U \parallel pw_U)$ by using his password $pw_U$.

$U$ chooses $r \leftarrow \mathbb{Z}_q$ and computes $R = g^r$ and $R^* = R / PW_U$.

$U$ sends $(U, R^*)$ to a gateway $G$.

**Step 2.** The gateway $G$ sends $(U, G, R^*)$ to a combiner $C$.

**Step 3.** The combiner $C$ publishes $(U, G, C, R^*)$ to all authentication servers.

The authentication server $S_i$ generates two polynomials $g_i(z) = b_{i,0} + b_{i,1} z + \cdots + b_{i,t-1} z^{t-1} \mod q$ and $g'_i(z) = b'_{i,0} + b'_{i,1} z + \cdots + b'_{i,t-1} z^{t-1} \mod q$ where $(b_{i,k}, b'_{i,k}) \leftarrow \mathbb{Z}_q$ for $k = 0, \ldots, t - 1$.

$S_i$ broadcasts $B_{i,k} = g_{i,k} h_{i,k}^p \mod p$ for $k = 0, \ldots, t - 1$ and sends $w_{i,j} = g_i(j) \mod q$, $w'_{i,j} = g'_i(j) \mod q$ to $S_j$ for $j = 1, \ldots, n$.

If the confirmation does not hold for index $i$, $S_j$ publishes a complaint against $S_i$.

An authentication server receiving more than or equal to the threshold $t$ complaints is marked as disqualified.

$S_j$ publishing the complaint against $S_i$'s values $(w_{i,j}, w'_{i,j})$ satisfying the confirmation is also marked as disqualified.

The set $L$ is defined as the subscript set of more than or equal to the threshold qualified authentication servers.

$S_j$ whose index is included in $L$ computes as follows.

$S_j$ computes $w_i = \sum_{j \in L} w_{i,j}$ and broadcasts $A_{ik} = g_{ik}^h$ for $k = 0, \ldots, t - 1$.

$S_j$ checks the equation $g_{ik}^h = \prod_{k=0}^{t-1}(A_{ik})^h$ for $i \in L$.

If the confirmation does not hold for index $i$, $S_j$ publishes a complaint.

Otherwise, $S_i$ computes $W = \prod_{i \in L} A_{i,0}$.

Using the encrypted password $Enc(pw_U) = (E_1, E_2) = (PW_U \cdot pk^e, g^h)$, $S_i$ broadcasts $F_1,i = (E_1 \cdot R^*)^\alpha$, $F_2,i = E_2^\beta$, and proofs $EDLog_{E_i,R_i}(F_1,i, \prod_{j \in L} \prod_{k \in [1]} (A_{ik})^h)$,

$EDLog_{E_i,R_i}(F_2,i, \prod_{j \in L} \prod_{k \in [1]} (A_{ik})^h)$.

After checking the proofs, $S_i$ checks the validity of $S_j$ by sending $(U, C, W)$ to $G$.

**Step 4.** The gateway $G$ chooses $y \leftarrow \mathbb{Z}_q$ and computes $Y = g^y$.

$G$ sends $(C, Y, W)$ to $U$.

**Step 5.** The user $U$ chooses $(x, d) \leftarrow \mathbb{Z}_q^2$.

$U$ computes $X = g^x$, $K_1 = W^r$, $\alpha = H_2(U \parallel G \parallel C \parallel X \parallel Y \parallel R^* \parallel W \parallel K_1)$, and the commitment $Com = g^h\text{rand}$.

$U$ sends $(U, X, Com)$ to $G$.

**Step 6.** The gateway $G$ sends $(U, X, Y, Com)$ to $C$.

**Step 7.** The combiner $C$ broadcasts $(U, X, Y, Com)$ among $S_i$ whose index is included in the set $L$.

$S_i$ computes $F_1 = \prod_{i \in L} F_{1,i}^{\lambda_{L,i,j}}$, and $F_2 = \prod_{i \in L} F_{2,i}^{\lambda_{L,i,j}}$ where $\lambda_{L,i,j} = \prod_{k \in L \setminus i \setminus j} (j - k)$ is the Lagrange coefficient.

$S_i$ broadcasts $T_{2,i} = F_2^\beta$ and the proof $EDLog_{E_i,R_i}(T_{2,i}, g^h)$.

After checking the proof, $S_i$ computes $K_1 = F_1 / \prod_{i \in L} T_{2,i}$.

$S_i$ computes $\alpha' = H_2(U \parallel G \parallel C \parallel X \parallel Y \parallel R^* \parallel W \parallel K_1)$.

$C$ sends $(U, \alpha')$ to $G$.

1The reason why our scheme uses a commitment scheme here (although it seems unnecessary) is explained in Appendix A. Without this commitment, it enables a malicious gateway to guess a password by combining subtle on-line and off-line dictionary attacks. We believe this shows the complexity that arises in considering the extension (i.e., GTPAKE) of traditional PAKE where more than two parties are involved.
Step 8. The gateway $G$ computes $K_2 = X^\alpha$ and an authenticator $Auth' = H_3(U || G || C || X || Y || R' || W || K_2)$. $G$ sends $(\alpha', Auth')$ to $U$.

Step 9. The user $U$ checks the validity of $\alpha'$ by using $\alpha$. $U$ computes $K_2 = Y^\alpha$ and checks the validity of $Auth'$ by using $K_2$.

If one of the two confirmations is false, $U$ increments the counter of incorrect login attempts for $G$, reject is output, and this sub-protocol is terminated. Otherwise, $U$ computes the session key $sk = H_3(U || G || C || X || Y || R' || W || K_2)$ and sends $(U, d)$ to $G$.

Step 10. The gateway $G$ sends $(U, d)$ to $C$.

Step 11. The combiner $C$ broadcasts $(U, d)$ among $S_i$ whose index is included in the set $L$.

$S_i$ checks the validity of $Com$ by using $d$ and $\alpha'$.

If one of the confirmations is false, $S_i$ increments the counter of incorrect login attempts for $U$, reject is output, and $C$ sends $(U, failure)$ to $G$ where $failure$ means that the authentication process failed. Otherwise, $C$ sends $(U, success)$ to $G$ where $success$ means that the authentication process succeeded.

Step 12. The gateway $G$ computes the session key $sk = H_3(U || G || C || X || Y || R' || W || K_2)$ and $sk$ is output if $success$ is received. Otherwise (i.e., $failure$ is received), the session is rejected.

5. Security Analysis

5.1 Session Key Security

We prove the security of the session key in the proposed scheme under the CDH assumption in the random oracle model.

**Theorem 1:** ($(T, R)$-Session Key Security). Let $\mathcal{L}$ be our GTPAKE scheme and $\mathcal{A}$ be a probabilistic polynomial time adversary that corrupts at most $(t - 1)(< n/2)$ authentication servers in advance. Then the advantage of $\mathcal{A}$ for the session key security in $\mathcal{L}$ with at most $T$ time and $R$ resources is

$$\text{Adv}^\text{sk}_{\mathcal{L}(\cdot), \mathcal{A}}(\mathcal{L}) \leq \frac{q_{H_0}^2 + q_{H_1}^2 + (q_{exe} + q_{send})^2}{2^q} + \frac{q_{H_0} + q_{H_1}}{2^{\kappa + 1}} \cdot \text{Adv}^\text{sk}^{\text{auth}}(\kappa) + \frac{q_{H_0} + q_{H_1}}{2^2} \frac{q_{exe} + q_{send} + q_{sent}}{|D|},$$

where $q_{H_0}, q_{H_1}, q_{H_2},$, and $q_{H_3}$ are the number of hash queries to the oracles $H_0, H_1, H_2,$ and $H_3$, respectively, $q_{exe}$ is the number of queries to the Execute oracle, $q_{send}$ is the number of queries to the SendUser, SendGateway, and SendServer oracles. $q_{send}$ and $q_{sent}$ are the number of queries to the SendServer and SendUser oracles, respectively, i.e., the equation $q_{send} + q_{sent} \leq q_{send}$ holds, and $|D|$ is the size of the dictionary $D$.

**Proof 1:** We define $\text{Succ}^\text{sk} n$ in Game $n$ as $\text{Succ}^\text{sk} n$.

**Game 0.** This experiment corresponds to a real attack by the adversary in the random oracle model. By Definition 5, and we have

$$\text{Adv}_{\mathcal{L}(\cdot), \mathcal{A}}(\mathcal{L}) = |\text{Pr}[\text{Succ}^\text{sk} n] - 1/2|.$$

**Game 1.** In this experiment, we simulate the hash functions and the oracle defined in Sect. 3.3. We simulate the random oracles $H_0, H_1, H_2,$ and $H_3$ by maintaining hash lists $\Lambda_0, \Lambda_1, \Lambda_2,$ and $\Lambda_3$ as follows.

- On a hash query $H_0(m)$, if there already exists a record $(m, r)$, then we return $r$; otherwise, we choose $r \leftarrow Z_q$, add the record $(m, r)$ in the hash list $\Lambda_0$, and return $r$.
- On a hash query $H_1(m)$, if there already exists a record $(m, r)$, then we return $r$; otherwise, we choose $r \leftarrow G$, add the record $(m, r)$ in the hash list $\Lambda_1$, and return $r$.
- On a hash query $H_2(m)$ (resp. $H_3(m)$), if there already exists a record $(m, r)$, then we return $r$; otherwise, we choose $r \leftarrow \{0, 1\}^t$, add the record $(m, r)$ in the hash list $\Lambda_2$ (resp. $\Lambda_3$) and return $r$.

For the simulations in the later games, we also prepare the hash functions $H_2$ and $H_3$ by maintaining hash lists $\Lambda_2'$ and $\Lambda_3'$.

The Execute, SendUser, SendGateway, SendServer, SessionKeyReveal, StaticKeyReveal, Ephemer- alKeyReveal, EstablishParty, Corrupt, and Test oracles can be simulated as follows.

- On a query $\text{SendUser}(U^{(i)}, *)$, we proceed as follows. If a query $\text{StaticKeyReveal}(U)$, $\text{EphemeralKeyReveal}(U^{(i)})$ in any instance $i$, or $\text{Corrupt}(S_i)$ for more than or equal to $t$ authentication servers has been asked by the adversary, then do nothing. If the processing request has come in the invalid order or the counter of incorrect login attempts exceeds the predetermined limit, we increment the counter of incorrect login attempts and do not reply.

1. On a query $\text{SendUser}(U^{(i)}$, start), we proceed as follows.

   - $PW_U = H_1(U || pw_U)$; $r \leftarrow Z_q$;
   - $R = g^r$; $R' = R/PW_U$; then return $(U, R')$.
2. On a query $\text{SendUser}(U^{(i)}, (G, C, Y, W))$, we proceed as follows.

   - $(x, d) \leftarrow Z_q^2$; $X = g^x$; $K_1 = W^r$;
   - $\alpha = H_2(U || G || C || X || Y || R' || W || K_1)$;
   - $Com = g^\alpha h^d$; then return $(U, X, Com)$.
3. On a query $\text{SendUser}(U^{(i)}, (\alpha', \text{Auth}'))$, we proceed as follows.
- We check the validity of $\alpha'$; $K_2 = Y^\alpha$;
- We check the validity of Auth';
- If one of the two confirmations is false, we increment the counter of incorrect login attempts for $G$ and return abort;
- Otherwise, $sk = H_3(U || G || C || X || Y || R^* || W || K_2)$;
- then return $(U, d)$;

- On a query $\text{SendServer}(C^{(k)}, *)$, we proceed as follows.

  If a query $\text{StaticKeyReveal}(G)$ or $\text{StaticKeyReveal}(C)$ has been asked by the adversary, then do nothing. If the processing request has come in the invalid order or the counter of incorrect login attempts exceeds the predetermined limit, we increment the counter of incorrect login attempts and do not reply. In the following queries, the adversary does the process on behalf of the corrupted authentication server $S_j$.

1. On a query $\text{SendServer}(C^{(k)}, (U, G, R^*))$, we proceed as follows.

   The uncorrupted authentication server $S_j$ broadcasts $B_{j,k} = g^{\beta_j}h^{\beta_j}$ and sends $w_{j,i} = g(t(j))$, $w'_{j,i} = g'(j)$ secretly to the authentication server $S_j$ corrupted by the adversary;
   - $S_j$ checks the validity of $w_{j,i}$, $w'_{j,i}$ by using $B_{j,k}$;
   - $S_j$ computes the share $w_i = \sum_{j \in L} w_{j,i}$ and broadcasts $A_{j,k} = g^{\beta_j}$;
   - $S_j$ checks the validity of $A_{j,k}$ by using $w_{j,i}$;
   - $S_j$ broadcasts $F_{1,i} = (E_1 \cdot R^*)^\alpha_i$, $F_{2,i} = E_{2,i}$ and proofs;
   - $S_j$ checks the proofs and computes $W = \prod_{j \in L} A_{i,j}$ then return $(U, C, W)$;

2. On a query $\text{SendServer}(C^{(k)}, (U, X, Y, \text{Com}))$, we proceed as follows.

   The uncorrupted authentication server $S_j$ computes $F_1 = \prod_{i \neq L} F_{1,i}^{\alpha_i}$ and $F_2 = \prod_{i \neq L} F_{2,i}^{\beta_i}$;
   - $S_j$ broadcasts $T_{2,i} = F_{2,i}$ and the proof;
   - $S_j$ checks the proof and computes $K_1 = F_1 / \prod_{L \neq i} F_{1,i}^{\alpha_i}$;
   - $S_j$ computes $\alpha' = H_2(U || G || C || X || Y || R^* || W || K_1)$;
   - then return $(U, \alpha')$;

3. On a query $\text{SendServer}(C^{(k)}, (U, d))$, we proceed as follows.

   The uncorrupted authentication server $S_j$ checks the validity of Com;
   - If one of the confirmations is false, we increment the counter of incorrect login attempts for $U$ and return (U, failure);
   - Otherwise, return $(U, success)$;

- On a query $\text{SendGateway}(G^{(j)}, *)$, we proceed as follows.

   If a query $\text{StaticKeyReveal}(U)$, $\text{EphemeralKeyReveal}(U^{(f)})$ in any instance $\ell$, or $\text{Corrupt}(S_j)$ for more than or equal to $t$ authentication servers has been asked by the adversary, then do nothing. If the processing request has come in the invalid order, then do not reply.

   1. On a query $\text{SendGateway}(G^{(j)}, (U, R^*))$, then return $(U, G, R^*)$;

   2. On a query $\text{SendGateway}(G^{(j)}, (U, C, W))$, $y \leftarrow Z_q; Y = C^y$;
      - then return $(G, C, Y, W)$;

   3. On a query $\text{SendGateway}(G^{(j)}, (U, X, \text{Com}))$, then return $(U, X, Y, Com)$;

   4. On a query $\text{SendGateway}(G^{(j)}, (U, \alpha'))$, $K_2 = X^q$;
      - $\text{Auth}' = H_2(U || G || C || X || Y || R^* || W || K_2)$;
      - then return $(\alpha', \text{Auth}')$;

   5. On a query $\text{SendGateway}(G^{(j)}, (U, d))$, then return $(U, d)$;

   6. On a query $\text{SendGateway}(G^{(j)}, (U, success/failure))$, we proceed as follows.
      - If success is received, $sk = H_3(U || G || C || X || Y || R^* || W || K_2)$;
      - If failure is received, then do nothing;

- On a query $\text{Execute}(U^{(i)}, G^{(j)}, C^{(k)})$, we proceed as follows.

   $(U, R^*) \leftarrow \text{SendUser}(U^{(i)}, \text{start});$
   $(U, G, R^*) \leftarrow \text{SendGateway}(G^{(j)}, (U, R^*));$
   $(U, C, W) \leftarrow \text{SendServer}(C^{(k)}, (U, G, R^*));$
   $(G, C, Y, W) \leftarrow \text{SendGateway}(G^{(j)}, (U, C, W));$
   $(U, X, \text{Com}) \leftarrow \text{SendUser}(U^{(i)}, (G, C, Y, W));$
   $(U, X, Y, \text{Com}) \leftarrow \text{SendGateway}(G^{(j)}, (U, X, \text{Com}));$
   $(U, \alpha') \leftarrow \text{SendServer}(C^{(k)}, (U, X, Y, \text{Com}));$
   $(\alpha', \text{Auth}') \leftarrow \text{SendGateway}(G^{(j)}, (U, \alpha'));
   $(U, d) \leftarrow \text{SendUser}(U^{(i)}, (\alpha', \text{Auth}'));$
   $(U, d) \leftarrow \text{SendGateway}(G^{(j)}, (U, d));$
   $(\text{success/failure}) \leftarrow \text{SendServer}(C^{(k)}, (U, d));$
   $\text{SendGateway}(G^{(j)}, (U, \text{success/failure}))$;
   - then return $(U, G, C, X, Y, R^*, W, \alpha, \alpha', \text{Auth}, \text{Auth}', Com, d, \text{success/failure})$;

- On a query $\text{SessionKeyReveal}(p^{(i)})$, we proceed as follows.

   If the session key $sk$ is defined for the user or gateway instance $p^{(i)}$ then return $sk$, else return $\perp$;

- On a query $\text{StaticKeyReveal}(P)$, we proceed as follows.

   If $P$ is a user $U$, then return the registered password $pw$;
   If $P$ is a gateway $G$, then return the secret key for the authenticated channels between the gateway and authentication servers;
   If $P$ is an authentication server $S_j$, then return the encrypted password $\text{Enc}(pw) = (PW \cdot \beta^{\nu} \cdot q^\nu)$ for all users, the share $s_i$ of the secret key for $P$, the published parameter $q^\nu$ for all authentication servers, and other secret keys for the authenticated channels between the authentication server and a gateway and secure channels among authentication servers;
• On a query \text{EphemeralKeyReveal}(p(C)) we proceed as follows.
  
  If there are already the ephemeral keys generated by the instance \( p(C) \), then return the ephemeral keys, else return \( \bot \).

• On a query \text{Corrupt}(S_i), we proceed as follows.
  
  We return all information obtained by the authentication server \( S_i \) such as static keys, ephemeral keys, and all the intermediate values of the computation in \( S_i \).

• On a query \text{EstablishParty}(U, pw_i), we proceed as follows.
  
  If there is already a user \( U \), then do nothing, else establish a new user \( U \) with the password \( pw_i \);

• On a query \text{Test}(U_i), we proceed as follows.
  
  \( sk \leftarrow \text{SessionKeyReveal}(p(C)) \);

  If \( sk = \bot \), then return \( \bot \), else \( b \leftarrow \{0, 1\} \);

  If \( b = 1 \) (resp. \( b = 0 \)), \( sk' = sk \) (resp. \( sk' \leftarrow \{0, 1\}^* \)), then return \( sk' \).


This experiment is perfectly indistinguishable from the previous experiment, and we have

\[
\Pr[\text{Succ}_{1}^{sk}] = \Pr[\text{Succ}_{0}^{sk}].
\]

\textbf{Game 2.} Wehalt this experiment when a collision on the outputs of the hash oracles and the transcripts occurs. We set the number of queries to the hash oracle \( H_i \) as \( q_H \) for \( i = 0, 1, 2, 3 \), that to the \text{Execute} oracle as \( q_{exe} \) and that to the \text{SendUser}, \text{SendGateway}, and \text{SendServer} oracles as \( q_{send} \). By using the bound described in Appendix B (i.e., the value \( n \) corresponds to \( q \) or \( 2^q \) and the value \( m \) corresponds to \( q_H, q_H, q_H, q_H, q_{exe} + q_{send} \)), we have

\[
\frac{q_H^2 + q_H^2 + (q_{exe} + q_{send})^2}{2q} + \frac{q_H^2 + q_H^2}{2^{2e+1}}.
\]

\textbf{Game 3.} We change the simulation of queries to the \text{Execute} oracle, especially queries to the \text{SendUser} and \text{SendGateway} oracles on a test session. When a query \text{SendGateway}(G_0, (U, \alpha')) or \text{SendUser}(U_i, (\alpha', \text{Auth}')) is asked, we compute the authenticator \text{Auth}' and the session key \( sk \) as \( H'_1(U \parallel G \parallel C \parallel X \parallel Y \parallel R' \parallel W) \) and \( H'_2(U \parallel G \parallel C \parallel X \parallel Y \parallel R' \parallel W) \) by using the private hash oracles \( H'_1 \) and \( H'_2 \), respectively. The difference between this experiment and the previous one is indistinguishable unless the adversary asks the query \( (U \parallel G \parallel C \parallel X \parallel Y \parallel R' \parallel W) \) to the hash function \( H_2 \) or \( H_3 \). The difference of the following probabilities is negligible as long as the CDH assumption holds, and we have

\[
\frac{\Pr[\text{Succ}_{1}^{sk}] - \Pr[\text{Succ}_{0}^{sk}]}{q_{exe} \cdot (q_H + q_H) \cdot \text{Adv}_{H}(\kappa)}.
\]

To evaluate the probability of this event, we construct an algorithm to solve the CDH problem. The algorithm obtains the CDH tuple \( (M, N) \) and chooses the session \( (U, G) \). We set \( X = M^a \cdot g^b \) for a query \text{SendUser}(U, (G, C, Y, W)) and \( Y = N^a \cdot g^b \) for a query \text{SendGateway}(G, (U, C, W)) where \( (u_1, u_2, u_3, u_4) \leftarrow \mathbb{Z}_q^4 \).

We compute \( \alpha \) and \text{Auth}' as \( H_2(U \parallel G \parallel C \parallel X \parallel Y \parallel R' \parallel W) \) and \( sk \) as \( H_3(U \parallel G \parallel C \parallel X \parallel Y \parallel R' \parallel W) \) for queries \text{SendUser}(U, (G, C, Y, W)), \text{SendUser}(U, (\alpha', \text{Auth}')), \text{SendGateway}(G, (U, C, W)), and \text{SendGateway}(G, (U, success/failure)). All other queries are handled in the same way as the previous game. The simulator picks a test session with the probability \( 1/q_{exe} \). Although the simulator cannot obtain the ephemeral keys of a user and a gateway by Definition 4, the simulator can simulate queries to all oracles without log \( q \) and log \( y \).

If the adversary asks the query \( (U \parallel G \parallel C \parallel X \parallel Y \parallel R' \parallel W) \) to the hash function \( H_2 \) or \( H_3 \) in the session \( (U, G, G') \), we can compute \( K_2 = \text{CDH}(M^a \cdot g^b, N^a \cdot g^b) = \text{CDH}(M^a, N^a) \cdot \text{CDH}(M^a, g^b) \cdot \text{CDH}(g^a, N^a) \cdot \text{CDH}(g^a, g^b) = \text{CDH}(M, N^a) \cdot M^a \cdot N^a \cdot g^b \) from hash lists \( \Lambda_2 \) and \( \Lambda_3 \) where CDH is a function to return \( g^\beta \) from \( (g^\gamma, g^\delta) \) in terms of the generator \( g \) in the same way as in [7]. In this way, we can extract the value \( \text{CDH}(M, N) \) from the given tuple \( (M, N) \).

In Game 3, the Diffie-Hellman key \( K_2 \) is random and independent from any other ephemeral and static keys such as passwords. In this situation, only three bits distinguish a session key from a random key are left as follows.

\textbf{Case 1.} The adversary asks the query \( (U \parallel G \parallel C \parallel X \parallel Y \parallel R' \parallel W) \) to the hash function \( H_2 \) or \( H_3 \).

The probability that Case 1 occurs is \( (q_H + q_H)/2^e \).

\textbf{Case 2.} The adversary asks the \text{SendGateway} or \text{SendServer} oracle except for the \text{SendGateway}(G, m) and successfully shares the session key with \( G \).

In order for the adversary to share the session key with the gateway, the adversary needs to convince the gateway by sending valid commitments \( Com \) and \( d \) to the combiner and giving \( Succ \) to the gateway. Also we note that an authenticated channel is established between the gateway and combiner in our security model. Therefore, even if the adversary tries to send \( Com \) and \( d \) to the combiner directly (i.e., not via the gateway) or to send \( Succ \) to the gateway directly (i.e., not via the combiner), this attack fails because the adversary is not allowed to obtain the static key for establishing the authenticated channel by Definition 4. Thus, the adversary has no choice but to do active attacks to authentication servers via the gateway through queries to the \text{SendServer} oracle. Therefore, the probability that the adversary successfully gives \( Succ \) to the gateway without communicating with the gateway and combiner is negligible. However, the adversary cannot obtain information of passwords unless active attacks are done as Theorem 2, and thus, the probability that Case 2 occurs is at most \( q_{send}/|\mathcal{D}| \) where \( q_{send} \) is the number of queries to the \text{SendServer} oracle.

\textbf{Case 3.} The adversary asks the \text{SendUser} oracle except for \text{SendUser}(U_i, m) and successfully shares the session key with \( U \).

The adversary needs to send valid authenticators \( \alpha' \) and \text{Auth}' to impersonate \( G \) to \( U \). However, the adversary cannot obtain information of passwords unless active attacks
are done as Theorem 2. According to Definition 4, the adversary is not allowed to obtain static keys and ephemeral keys of the user and corrupt more than or equal to $t$ authentication servers. The probability that Case 3 occurs is at most $q_{sendu}/|D|$ where $q_{sendu}$ is the number of queries to the SendUser oracle.

As a result, the probability that the adversary succeeds in guessing the challenge bit $b$ at random, we have

$$\text{Pr[Succ}_{3}^{\text{skis}}] = \frac{1}{2} + \frac{q_{H_h} + q_{H_1}}{2^t} + \frac{q_{sendu} + q_{sendu}}{|D|}.$$\hfill $\square$

5.2 Password Protection Security

We prove the security of the password in the proposed scheme under the DDH assumption in the random oracle model.

Theorem 2: ((T, R)-Password Protection Security). Let $\mathcal{L}$ be our GTPAKE scheme and $\mathcal{A}$ be a probabilistic polynomial time adversary that corrupts at most $(t-1)/n$ authentication servers in advance. Then the advantage of $\mathcal{A}$ for the password protection security in $\mathcal{L}$ with at most $T$ time and $R$ resources is

$$\text{Adv}_{\mathcal{L}}^{\text{pps}}(\mathcal{A}) \leq \frac{q_{H_h}^2 + q_{H_1}^2 + (q_{exe} + q_{sendu})^2}{2q} + \frac{q_{H_h}^2 + q_{H_1}^2}{2^{t+1}} + (q_{exe} + 1) \cdot \text{Adv}_{\mathcal{A}}^{\text{ddh}}(\kappa) + \frac{q_{sendu} + q_{sendu} + 1}{|D|},$$

where $q_{H_h}, q_{H_1}, q_{exe}$ and $q_{sendu}$ are the number of queries to the oracles $H_h, H_1, H_2, H_1$, respectively, $q_{exe}$ is the number of queries to the Execute oracle, $q_{sendu}$ is the number of queries to the SendUser, SendGateway, and SendServer oracles, $q_{send}$ and $q_{sendu}$ are the number of queries to the SendServer and SendUser oracles, respectively, i.e., the equation $q_{sendu} + q_{send} \leq q_{sendu}$ holds, and $|D|$ is the size of the dictionary $D$.

Proof 2: We define $\text{Succ}_{\text{pps}}^{\text{skis}}$ in Game $n$ as $\text{Succ}_{\kappa}^{\text{pps}}$.

Game 0. This experiment corresponds to a real attack by the adversary in the random oracle model. By Definition 7, and we have

$$\text{Adv}_{\mathcal{L}}^{\text{pps}}(\mathcal{A}) = \text{Pr}[\text{Succ}_{0}^{\text{pps}}].$$

Game 1. As the proof in Sect. 5.1, we can simulate the functions $H_i$ for $i = 0, 1, 2, 3$, the Execute, SendUser, SendGateway, SendServer, SessionKeyReveal, StaticKeyReveal, EphemeralKeyReveal, EstablishParty, and Corrupt oracles. We simulate the TestPassword oracle as follows.

- On a query TestPassword$(U, pw_U^t)$, we proceed as follows.
  - $pw_U' \leftarrow \text{StaticKeyReveal}(U)$;
  - If $pw_U' = pw_U$, then return 1, else return 0;

This experiment is perfectly indistinguishable from the previous experiment, and we have

$$\text{Pr}[\text{Succ}_{1}^{\text{pps}}] = \text{Pr}[\text{Succ}_{0}^{\text{pps}}].$$

Game 2. We halt this experiment when a collision on the outputs of the hash oracles and the transcripts occurs. By using the bound described in Appendix B (i.e., the value $n$ corresponds to $q$ or $2^n$ and the value $m$ corresponds to $q_{H_h}, q_{H_1}, q_{H_2}, q_{exe}$ or $(q_{exe} + q_{sendu})$), we have

$$\frac{\text{Pr}[\text{Succ}_{2}^{\text{pps}}] - \text{Pr}[\text{Succ}_{1}^{\text{pps}}]}{2q} + \frac{q_{H_h}^2 + q_{H_1}^2}{2} \leq \frac{|D|}{2^{t+1}}.$$

Game 3. We change the simulation of the queries to the SendServer oracle for all sessions and the Corrupt oracle for authentication servers. When a query SendServer$(C^{skis}, (U, X, Y, Com))$ or Corrupt$(S_i)$ is asked, we replace the secret part needed to decrypt the stored ElGamal ciphertext of the password with a random element for honest users. The difference between this experiment and the previous one is the stored passwords which are not generated by EstablishParty. The difference of the following probabilities is negligible as long as the DDH assumption holds, and we have

$$\text{Pr}[\text{Succ}_{3}^{\text{pps}}] - \text{Pr}[\text{Succ}_{2}^{\text{pps}}] \leq \text{Adv}_{\mathcal{A}}^{\text{ddh}}(\kappa).$$

We suppose that we have a successful distinguisher between Games 2 and 3, we construct an algorithm to solve the DDH problem to prove the above.

The simulator needs to change the process done by uncorrupted authentication servers to be consistent with the intended values. We assume w.l.o.g. that $S_n$ is in the set of uncorrupted authentication servers in the well-defined set $L$. The simulator controls the other uncorrupted authentication servers as usual.

First, we deal with the simulation about the public key in the sub-protocol of setup Init. In this proposed model, the trusted dealer computes a secret key $s$, the public key $pk = g^s$, and the corresponding share $g^{s_a}$. Given $g^s$ without knowing $s$, the simulator needs to publish $g^{s_a}$ as a trusted dealer such that $g^s$ is the ElGamal public key. Using the DDH triple $(M, N, Z)$, the corresponding share for $S_n$ is set as $g^{s_a} = M^{\lambda_{L,s}} \cdot \prod_{i \in \{L,s\}}(g^{s_a})^{\lambda_{L,i}}$ where $\lambda_{L,s} = \prod_{j \in \{L,s\}}(l-k)/(l-k)$ is the Lagrange coefficient. Due to the honest majority setting, the simulator can compute all the share $s_j$ of the secret key $s$.

To simplify the system, we assume that the trusted dealer distributes the shares of the secret key corresponding to the ElGamal public key. We can construct the proposed scheme without the trusted dealer by producing some parameters among the authentication servers. In this case, we can simulate the public key by hitting the intended value similar to the distributed key generation technique [12].

Second, we deal with the simulation about the stored passwords in the sub-protocol of registration Regi. Since all
users register the encrypted passwords by sending the encrypted passwords to the authentication servers, the simulator knows all the passwords for honest users. When a query \text{Corrupt}(S_i) is asked, we embed the DDH triple into all encrypted passwords. The simulator returns \((PW_{i1} \cdot Z_{u1}^i, N_{w1})\) where \(v_i \leftarrow Z_q\) for all honest users and \((PW_{i2} \cdot pk_i', g_{i2}')\) for the other users. Other internal information is given to the adversary as usual.

Third, we deal with the simulation about a partial decryption in the sub-protocol of authentication \text{Auth}. We need to simulate the uncorrupted authentication servers for \text{SendServer}(C^{(k)}, (U, X, Y, Com)). The share \(T_{2,n}\) for \(U_i\) can be computed as \(Z_{w1}^{i \cdot X_i} \cdot \prod_{j \in (U_i \setminus \{i\})} N_{w1}^{i \cdot X_i} \cdot L_{w1}^{i \cdot X_i} \) without \(s_n\). Other parameters generated from the uncorrupted servers can be simulated similarly to the authentication process.

To detect malicious authentication servers that publish incorrect shares, the non-active zero-knowledge proof of equality of discrete logarithm is used in our scheme. In the random oracle model, the simulator can simulate this proof without knowing the secret keys. The simulator chooses \((c, z) \leftarrow Z_q^2\) and sends \((c, z)\) as the proof. The hash oracle \(H_0\) returns \(c\) from the hash list \(A_0\) if the adversary asks the query \((q_1, g_{i1}, u_{i1}, u_{i2}, g'_{i1}, g'_{i2}, u_{i2}')\).

Therefore, the simulator assigns \((pk, g', CDH(pk, g'))\) for the given DDH triple \((M, N, Z)\). The simulator is able to solve the DDH problem by using the difference of success probability that an adversary guesses the registered password of one honest user through the \text{TestPassword} oracle because all the encrypted passwords for all honest users include the DDH triple. In the case of \(Z = CDH(M, N)\), the environment for the distinguisher corresponds to Game 2. In the case of \(Z \neq CDH(M, N)\), the environment for the distinguisher corresponds to Game 3. If the distinguisher decides that the distinguisher interacted with Game 2, the algorithm outputs 1, otherwise 0.

**Game 4.** We change the simulation of queries to the \text{Execute} oracle, especially the \text{SendUser} and \text{SendServer} oracles on a test session. When a query \text{SendUser}(U^{(i)}, start), \text{SendServer}(U^{(i)}, (G, C, Y, W)), or \text{SendServer}(C^{(k)}, (U, G, R')) is asked, we replace the Diffie-Hellman key in the authenticators \(\alpha\) and \(\alpha'\) with random elements. The difference of the following probabilities between this experiment and the previous one is negligible as long as the DDH assumption holds, and we have

\[
|\text{Pr}[\text{Succ}_{\text{ppp}}^4] - \text{Pr}[\text{Succ}_{\text{pp}}^3]| \leq q_{exe} \cdot \text{Adv}_{\text{DH}}(k).
\]

To evaluate the probability of this event, we construct an algorithm to solve the DDH problem. The algorithm obtains the DDH triple \((M, N, Z)\) and chooses the session \((U^{(i)}, C^{(k)})\). The distinguisher picks a test session with the probability \(1/q_{exe}\). We show the simulation of the \text{SendUser} and \text{SendServer} oracles without ephemeral keys \(log_q R\) and \(\log_q Y\) as follows.

We set \(R = M^a\) for a query \text{SendUser}(U^{(i)}, start) and \(K_1 = Z^{u_1}\) for a query \text{SendServer}(U^{(i)}, (G, C, Y, W)) where \((u_1, u_2) \leftarrow Z_q^2\). When a query \text{SendServer}(C^{(k)}, (U, G, R')) is asked, we need to simulate the process of honest authentication servers sending and receiving information privately and publicly for corrupted parties. The simulator knows all the shares \(u_{i,j}, w_{i,j}\), the coefficients \(b_{i,k}, b'_{i,k}\), and the public values \(B_i\) due to the honest majority setting. We assume w.l.o.g. that \(S_n\) is in the set of uncorrupted authentication servers in the well-defined set \(L\). We change the simulation of queries to the \text{Auth} oracle, especially the \text{TestPassword} oracle, especially the \text{TestPassword} oracle.

Because all the encrypted passwords for all honest users in-
asked, we compute $R^*$ as $g^r$ where $r^* \leftarrow \mathbb{Z}_q$ without using the password $pw_{W^r}$. $R^*$ has been simulated, but $W$ has been generated by the adversary trying to impersonate a combiner to a user. To succeed in passing the verification done by the adversary trying to impersonate a combiner, the password $pw_{W^r}$ is used, which is computed by at most one password in the non-concurrent setting. Then the success probability with at most $T$ time and $R$ resources is at most $q_{send}/|D|$ where $q_{send}$ is the number of queries to the $SendUser$ oracle, we have

$$|\Pr[Succ_{pp}^6] - \Pr[Succ_{pp}^5]| \leq q_{send}/|D|.$$ 

In this game, information of the password obtained via the $SendUser$ and $SendServer$ oracles is not used in sessions, so the adversary cannot do much better than guessing the password at random. Finally, the adversary guesses the password through the $TestPassword$ oracle once, we have

$$\Pr[Succ_{pp}^6] = 1/|D|. \quad \Box$$ 

6. Concluding Remarks

We proposed new GTPAKE which has resistance of UDOnDA and the corruption of authentication servers. We proved the security of our GTPAKE under standard assumptions in the random oracle model. The proposed scheme has the stronger security against a malicious provider compared with existing schemes, and a global roaming service used for users regardless of places and devices is expected to be one of its applications. Our scheme is an instantiation of GTPAKE, and the generic construction of GPAKE and GTPAKE is left as future work.

Acknowledgements

We would like to thank anonymous reviewers and Shin-Akarui-Angou-Benyou-Kai for their valuable comments. This work was supported in part by JSPS KAKENHI Grant Number 17K00178, Institute for Information and & communications Technology Promotion (IITP) grant (2017-0-00555), and National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2015R1A-2A2A01006812).

References


Appendix A: Security Analysis of the Scheme without Commitments

A.1 Construction

We mention the insecure construction to explain the reason why the proposed scheme needs a commitment scheme, although it seems unnecessary. We describe the following sub-protocol of setup and registration in this scheme are the same as those of the proposed scheme in Sect.4.3. A perspective of the insecure scheme is shown in Fig. A-1.
Auth. If a processing request has come in the invalid order, the incorrect login attempt is counted and the session is rejected. After the counter of incorrect login attempts exceeds the predetermined limit, a processing request from the user is rejected.

Step 1. A user $U$ computes $PW_U = H_3(U \parallel pw_U)$ by using his password $pw_U$. $U$ chooses $r \leftarrow \mathbb{Z}_q$ and computes $R = g^r$ and $R^* = R/PW_U$. $U$ sends $(U, R^*)$ to a gateway $G$.

Step 2. The gateway $G$ sends $(U, G, R^*)$ to a combiner $C$.

Step 3. The combiner $C$ publishes $(U, G, R^*)$ to all authentication servers. The authentication server $S_i$ generates two polynomials $g_i(z) = b_{i0} + b_{i1} z + \cdots + b_{i,t-1} z^{t-1} \mod q$ and $g'_i(z) = b'_{i0} + b'_{i1} z + \cdots + b'_{i,t-1} z^{t-1} \mod q$ where $(b_{i,j}, b'_{i,j}) \leftarrow \mathbb{Z}_q^2$ for $k = 0, \ldots, t - 1$. $S_i$ broadcasts $B_{i,j} = g^{b_{i,j}} h_k^{b'_{i,j}} \mod p$ for $k = 0, \ldots, t - 1$ and sends $w_{i,j} = g_i(j) \mod q, w'_{i,j} = g'_i(j) \mod q$ to $S_j$ for $j = 1, \ldots, n$. $S_j$ checks the equation $g^{w_{i,j}} h^{w'_{i,j}} = \prod_{k=0}^{t-1} (B_{i,k})^{\lambda}$ for $i = 1, \ldots, n$. If the confirmation does not hold for index $i$, $S_j$ publishes a complaint against $S_i$. An authentication server receiving more than or equal to the threshold $t$ complaints is marked as disqualified. $S_i$ publishing the complaint against $S_j$’s values $(w_{i,j}, w'_{i,j})$ satisfying the confirmation is also marked as disqualified.

The set $L$ is defined as the subscript set of more than or equal to the threshold qualified authentication servers. $S_i$ whose index is included in $L$ computes as follows.

$S_i$ computes $w_i = \sum_{j \in L} w_{i,j}$ and broadcasts $A_{i,k} = g^{b_{i,k}}$ for $k = 0, \ldots, t - 1$. $S_j$ checks the equation $g^{w_{i,j}} h^{w'_{i,j}} = \prod_{k=0}^{t-1} (A_{i,k})^{\lambda}$ for $i \in L$. If the confirmation does not hold for index $i$, $S_j$ publishes a complaint.

Otherwise, $S_i$ computes $W = \prod_{i \in L} A_{i,0}$. Using the encrypted password $Enc(pw_U) = (E_1, E_2) = (PW_U \cdot pk^e, g^a)$, $S_i$ broadcasts $F_{1,i} = (E_1 \cdot R^*)^a, F_{2,i} = E_2^a$ and proofs $EDLog_{(E; R^*)} (F_{1,i}, \prod_{i \in L} \prod_{j \in L} \prod_{k \in L} (A_{i,k})^{\lambda})$, $EDLog_{(E; R^*)} (F_{2,i}, \prod_{i \in L} \prod_{j \in L} \prod_{k \in L} (A_{i,k})^{\lambda})$. After $S_i$ checks the proofs, $C$ sends $(U, C, W)$ to $G$.

Step 4. The gateway $G$ chooses $y \leftarrow \mathbb{Z}_q$ and computes $Y = g^y$. $G$ sends $(G, C, Y, W)$ to $U$.

Step 5. The user $U$ chooses $x \leftarrow \mathbb{Z}_q$ and computes $X = g^x, K_1 = W^x$, and $\alpha = H_2(U \parallel G \parallel C \parallel X \parallel Y \parallel R^* \parallel W \parallel K_1)$. $U$ sends $(U, x, \alpha)$ to $G$.

Step 6. The gateway $G$ sends $(U, X, Y, \alpha) \rightarrow C$.

Step 7. The combiner $C$ broadcasts $(U, X, Y, \alpha)$ among $S_i$ whose index is included in the set $L$. $S_i$ computes $F_1 = \prod_{i \in L} F_{1,i}^{\lambda_{j,i}}$ and $F_2 = \prod_{i \in L} F_{2,i}^{\lambda_{j,i}}$ where $\lambda_{j,i} = \prod_{k \in L} \prod_{i \in L} (i-k)/(j-k)$ is the Lagrange coefficient. $S_i$ broadcasts $T_{2,i} = F_2^a$ and the proof $EDLog_{(E; Y)} (F_{2,i}, \prod_{i \in L} \prod_{j \in L} (A_{i,j})^{\lambda})$. After checking the proof, $S_i$ computes $K_1 = F_1 / \prod_{i \in L} T_{2,i}^{\lambda_{j,i}}$. $S_j$ checks the validity of $\alpha$ using $K_1$. If the confirmation is false, $S_i$ increments the counter of incorrect login attempts for $U$, reject is output, and this sub-protocol is terminated.

Otherwise, $C$ computes $\beta' = H_2(U \parallel G \parallel C \parallel X \parallel Y \parallel R^* \parallel W \parallel K_1)$ and sends $(\beta', Auth') \rightarrow U$.

Step 8. The gateway $G$ computes $K_2 = X^\beta$, an authenticator $Auth' = H_2(U \parallel G \parallel C \parallel X \parallel Y \parallel R^* \parallel W \parallel K_2)$ and the session key $sk = H_3(U \parallel G \parallel C \parallel X \parallel Y \parallel R^* \parallel W \parallel K_2)$. $G$ sends $(\beta', Auth') \rightarrow U$. 

Fig. A-1 Overview of the insecure scheme.
Step 9. The user \( U \) checks the validity of \( \beta' \) by using \( K_1 \). \( U \) computes \( K_2 = Y' \) and checks the validity of \( \text{Auth}' \) by using \( K_2 \). If one of the two confirmations is false, \( U \) increments the counter of incorrect login attempts for \( G \) and \( \text{reject} \) is output. Otherwise, \( U \) computes the session key \( sk = H_3(U \parallel G \parallel C \parallel X \parallel Y \parallel R' \parallel W \parallel K_2) \) and \( sk \) is output.

A.2 Attack against Password Protection Security

We describe the following method for an adversary acting as a malicious gateway to guess the password of a target user by a combination of the on-line and off-line dictionary attacks in the scheme described in Sect. A.1. To avoid this attack, the proposed scheme in Sect. 4.3 uses a commitment scheme that can hide the calculated intermediate results among the authentication servers.

1. The active adversary interacts with a target user \( U \) once as below where instances of a user, a malicious gateway, and a combiner are \( U^{(i)} \), \( G^{(i,j)} \), and \( C^{(k)} \) respectively. We note that this attack in the on-line manner is detected by the honest authentication servers correctly because the value generated by the adversary at random does not pass the verification with overwhelming probability. However, we also note that this attack is quite powerful in the sense that this only one probe makes the whole password guessing attack possible.

   a. The adversary (i.e., the malicious gateway \( G' \)) obtains \( R' \) in the message \( (U, R') \) from \( U \).
   b. The adversary chooses the random numbers \( (y, w') \leftarrow Z_n^{*2} \) and computes \( Y = g^y, W' = g^{w'} \). The adversary sends \( (G', C, Y, W') \) to \( U \) and obtains \( \alpha' \) in the response message \( (U, X, \alpha') \) from \( U \).

2. The passive adversary guesses the password \( pw_U \) in the off-line manner by using the obtained data as below.

   a. The adversary chooses the password \( pw'_U \) from the dictionary \( D \) and computes \( R' = R' \cdot H_1(U \parallel pw'_U) \).
   b. The adversary checks whether \( H_2(U \parallel G' \parallel C \parallel X \parallel Y' \parallel R' \parallel W' \parallel (R')^{w''} \) equals the hash value \( \alpha' \).
   c. The adversary repeats Steps (a) and (b) until the password satisfying the equation in (b) (that is the correct password) is detected.

Appendix B: The Bound Related to the Birthday Problem

We explain how to derive the bound of the probability of the collision on the outputs of the hash function used in the proof of Theorems 1 and 2. This probability is widely discussed as the birthday problem [14], which asks for the probability that at least one pair in a set of \( m \) people will have the same birthday. We compute the probability \( p(n, m) \) that there is at least one collision in the set of \( m \) hash values computed from hash function \( H \) which outputs \( n \) kinds of hash values as below.

When the first value is chosen, the probability of no collision is 1. When the second value is chosen, the probability of no collision is \( 1 - 1/n \). When the third value is chosen, the probability of no collision is \( 1 - 2/n \). Similarly, when the \( m \)-th value is chosen, the probability of no collision is \( 1 - (m - 1)/n \). The probability that at least one collision happens is

\[
p(n, m) = 1 - (1 - 1/n)(1 - 2/n) \cdots (1 - (m - 1)/n).
\]

By using a first-order approximation for \( e^x \) where \( e \) is Napier’s constant and \( |x| \ll 1 \), we have \( e^x \approx (1 + x) \). Thus when the equation \( m \ll n \) holds,

\[
p(n, m) \approx 1 - e^{-1/n} \cdot e^{-2/n} \cdots e^{-(m-1)/n} \\
= 1 - e^{-(1+2+\cdots+(m-1))/n} \\
= 1 - e^{-m(m-1)/2n} \\
\approx 1 - (1 - m(m - 1)/2n) \\
= m(m - 1)/2n \\
< m^2/2n.
\]
Kazuki Yoneyama received the B.E., M.E. and Ph.D. degrees from the University of Electro-Communications, Tokyo, Japan, in 2004, 2006 and 2008, respectively. He was a researcher of NTT Secure Platform Laboratories from 2009 to 2015. He is presently engaged in research on cryptography at the Ibaraki University, since 2015. He is a member of the International Association for Cryptologic Research (IACR), IPSJ and JSIAM.

Takashi Nishide received B.S. degree from the University of Tokyo in 1997, M.S. degree from the University of Southern California in 2003, and Dr.Eng. degree from the University of Electro-Communications in 2008. From 1997 to 2009, he had worked at Hitachi Software Engineering Co., Ltd. developing security products. From 2009 to 2013, he had been an assistant professor at Kyushu University and from 2013 he is an associate professor at University of Tsukuba. His research is in the areas of cryptography and information security.

Goichiro Hanaoka Graduated from the Department of Engineering, The University of Tokyo in 1997. Received Ph.D. degree from The University of Tokyo in 2002. Joined AIST in 2005. Currently, Leader, Advanced Cryptosystems Research Group, Information Technology Research Institute, AIST. Engages in the R&Ds for encryption and information security technologies including the efficient design and security evaluation of public key cryptosystem. Received the Wilkes Award (2007), British Computer Society; Best Paper Award (2008), The Institute of Electronics, Information and Communication Engineers; Innovative Paper Award (2012, 2014), Symposium on Cryptography and Information Security (SCI); Award of Telecommunication Advancement Foundation (2005); 20th Anniversary Award (2005), SCIS; Best Paper Award (2006), SCIS; Encouragement Award (2000), Symposium on Information Theory and its Applications (SITA); and others.

Kwangjo Kim received the B.S. and M.S. degrees of Electronic Engineering in Yonsei University, Korea in 1980 and 1983, respectively and Ph.D. of Div. of Electrical and Computer Engineering in Yokohama National University, Japan in 1991. He has served board member of International Association for Cryptologic Research (IACR) from 2000 to 2004, chairperson of Asiacrypt Steering Committee from 2005 to 2008 and President of Korea Institute of Information Security and Cryptography (KIISC) in 2009. Also he was a visiting professor in MIT (2005), UCSD (2005), KUSTAR, UAE (2012) and an education specialist in ITB, Indonesia (2013). He is currently a professor at School of Computing in KAIST, Korea, Korea Representative to IFIP TC-11 and Honorable President of KIISC. His research interests include the theory of cryptography and information security and its application. He is members of IEICE, IEEE, IACR and ACM. He is a Fellow of the IACR.

Eiji Okamoto received his B.S., M.S. and Ph.D. degrees in electronics engineering from the Tokyo Institute of Technology in 1973, 1975 and 1978, respectively. He worked and studied communication theory and cryptography for NEC central research laboratories since 1978. In 1991 he became a professor at Japan Advanced Institute of Science and Technology, then at Toho University. Now he is a professor at Faculty of Engineering, Information and Systems, University of Tsukuba. His research interests are cryptography and information security. He is members of IEEE and ACM.