A Rigorous Security Proof for the Enhanced Version of Password-Protected Secret Sharing Scheme

Shingo HASEGAWA¹, Shuji ISOBÉ¹, Jun-ya IWAZAKI¹,²,*, Eisuke KOIZUMI¹ and Hiroki SHIZUYA¹

¹Graduate School of Information Sciences, Tohoku University, Sendai 980-8576, Japan
²Presently, Graduate School of Medicine, Tohoku University, Sendai 980-8574, Japan

The password-protected secret sharing (PPSS, for short) and its security notion, called in this paper the PPSS-security, were proposed by Bagherzandi, Jarecki, Saxena and Lu. However, another security notion for PPSS schemes, the pparam-security was proposed by Hasegawa, Isobe, Iwazaki, Koizumi and Shizuya, because they pointed out an attack which can break the original protocol proposed by Bagherzandi et al. Hasegawa et al. also showed how to enhance the protocol, and proved that the enhanced one is pparam-secure. In this paper, we prove that the enhanced one is PPSS-secure as well.

KEYWORDS: password-protected secret sharing, twin ElGamal encryption, simulation-sound non-interactive zero knowledge

1. Introduction

Today a wide range of services are available via the Internet. Among those is a file-hosting service such as Google Drive, Dropbox and iCloud Drive. This service enables us to easily store and access documents or data files from mobile terminals as well as PC’s, and to share them with others. Although the file-hosting service is so popular in the Internet community, we should note that there is a latent risk that we would lose the files we have stored. For example, the server could be attacked by malware or be corrupted by some malicious attackers, and consequently the stored documents might be destroyed, erased, fabricated or stolen.

In order to safely store some secret documents or data distributedly in several servers via insecure networks such as the Internet, Bagherzandi et al. proposed a password-protected secret sharing (PPSS, for short) scheme [4] in 2011. Intuitively, a PPSS scheme consists of several parties: a user, n servers and initialization algorithm. For a pair (p, d) of a password p and a document d, the initialization first sets a public parameter and secret seeds, where the public parameter includes encryptions of p and d. Then the initialization sends the public parameter and the secret seeds to the user and the servers, respectively. Using the password p, the user interacts with the servers, and recovers the document d. A formal description of PPSS schemes will be given in Section 2.3. In [4], they proposed the protocol PPSS² which has the following three properties: (i) PPSS² is secure against the corruption of the coalition of servers of size less than the threshold, which means that one can obtain no useful information about the password and the document even though the adversary is allowed to adaptively interact with the servers and the user in impersonating manner. They showed that the protocol PPSS² is PPSS-secure [4].

In contrast, Hasegawa et al. [7] focused on the process of generating a public parameter, and proposed another security notion for PPSS schemes named the pparam-security (Definition 2.4). Intuitively, the pparam-security means that any public parameter does not include any clue to the stored document in a way that an adversary could recognize. Namely, no adversary could determine, on any given two documents and any public parameter, which document is stored in the public parameter, even though the adversary is allowed to adaptively interact with the servers and the user in impersonating manner. They showed that the protocol PPSS² is PPSS-secure [4].

In contrast, Hasegawa et al. [7] focused on the process of generating a public parameter, and proposed another security notion for PPSS schemes named the pparam-security (Definition 2.4). Intuitively, the pparam-security means that any public parameter does not include any clue to the stored document in a way that an adversary could recognize. Namely, no adversary could determine, on any given two documents and any public parameter, which document is stored in the public parameter, even though the adversary is allowed to adaptively receive the sample pairs of the public parameter and the stored document. The pparam-security means that the adversary could learn nothing from the sample pairs. In [7], they showed that the protocol PPSS² is not pparam-secure. Then they proposed an enhanced protocol ePPSS² (a.k.a. “Protocol 1” in this paper) of PPSS², and proved that the enhanced protocol is pparam-secure.

Received May 27, 2015; Accepted December 25, 2015; J-STAGE Advance published February 9, 2016
This work is supported in part by JSPS KAKENHI Grant Numbers 25870053 and 26330150.
*Corresponding author. E-mail: iwazaki@med.tohoku.ac.jp
It should be noted that these two security notions are independent in a sense that the pparam-security does not imply the PPSS-security in general and vice versa. As stated above, the protocol PPSS$_2$ is PPSS-secure but not pparam-secure. On the other hand, one can easily construct a protocol which is pparam-secure but not PPSS-secure (see Protocol 2 in Section 4). Hence, we should say that a PPSS scheme is preferable if it is both PPSS-secure and pparam-secure.

The purpose of this paper is to prove that the protocol $\epsilon$PPSS$_2$ is PPSS-secure. The proof is similar to that of Theorem 1 in [4] since $\epsilon$PPSS$_2$ is an enhanced protocol of PPSS$_2$. However, the latter proof lacks an estimate of a specific statistical distance which is a key to prove the PPSS-security, and the proof does not seem to be refined in this sense in a later version of the paper [3] (see Remark 6.1). We therefore supplement the proof in [4] and demonstrate that $\epsilon$PPSS$_2$ is rigorously PPSS-secure. The title of this paper comes from this fact.

In Section 2, we introduce notations and notions needed later. In Section 3, we recall the protocol $\epsilon$PPSS$_2$, and state our main result. Before proving the result, we give a protocol which is pparam-secure but not PPSS-secure in Section 4. We prove our result in Sections 5 and 6. Concluding remarks are given in Section 7.

2. Preliminary

Let $\Delta$ be a distribution over a finite set $A$. We write $x \in \Delta$ to denote that $x$ is chosen from $A$ according to the distribution $\Delta$. In particular, if $\Delta = U_A$, the uniform distribution over $A$, then we write $x \in A$ instead of $x \in U_A$. $N$ and $\mathbb{Z}$ denote the set of the natural numbers and the ring of the rational integers, respectively. For any $n \in N$, we use $\mathbb{Z}_n$ and $\mathbb{Z}_n^*$ to denote the residue ring $\mathbb{Z}/n\mathbb{Z}$ and its group of units, respectively. Let $1^k$ denote the string of $k$ ones. For any finite set $V$, $\#V$ denotes the cardinality of $V$. Let $\text{SS}_{n,a}$ be the Shamir $(t, n)$-threshold secret sharing scheme [8].

2.1 Cryptographic Assumptions

Let $Q$ be a safe prime, that is, $Q$ is a prime of the form $Q = 2q + 1$ for some prime $q$. We note that it is not shown that there are infinitely many safe primes. However, it is widely believed that the set of safe primes, or alternatively the set of Sophie Germain primes is not finite [1]. Throughout this paper, we assume that there are infinitely many safe primes.

We define the decisional Diffie-Hellman (DDH, for short) problem [2]. Let $Q = 2q + 1$ be a safe prime, and let $G_q$ denote the subgroup of $\mathbb{Z}_q^*$ of order $q$. We define

$$DH = \{(Q, g, g^a, g^b, g^{ab}) \mid g \text{ is a generator of } G_q, \text{ and } a, b \in \mathbb{Z}_q\},$$

and

$$\widehat{DH} = \{(Q, g, g^a, g^b, g^c) \mid g \text{ is a generator of } G_q, \text{ and } a, b, c \in \mathbb{Z}_q\}.$$

The DDH problem is to determine, for a tuple $w = (Q, g, g^a, g^b, g^c)$, whether or not $w \in DH$. Let $\text{Gen}$ be a probabilistic polynomial-time (PPT, for short) algorithm which works as follows: On input $1^k$, $\text{Gen}$ randomly chooses a safe prime $Q = 2q + 1$ of length $k + 2$ and a generator $g \in G_q$, and outputs a pair $(Q, g)$. For a probabilistic Turing machine $A$ called an adversary and a security parameter $k$, we define the advantage $\text{Adv}_{A}^{\text{DDH}}(k)$ as follows:

$$\text{Adv}_{A}^{\text{DDH}}(k) = |\Pr[A(Q, g, g^a, g^b, g^{ab}) = 1] - \Pr[A(Q, g, g^a, g^b, g^c) = 1]|,$$

where $(Q, g) = \text{Gen}(1^k)$ and $a, b, c \in \mathbb{Z}_q$. The probability is taken over the random tapes of $A$ and $\text{Gen}$, and the random choice of $a, b, c \in \mathbb{Z}_q$. The DDH problem is $(T_{\text{ddh}}, \varepsilon_{\text{ddh}})$-hard if $\text{Adv}_{A}^{\text{DDH}}(k) < \varepsilon_{\text{ddh}}$ holds for any $k$ and any adversary $A$ whose running time is at most $T_{\text{ddh}}$.

We next define the computational Diffie-Hellman problem [2]. Set

$$\text{CDH} = \{(Q, g, g^a, g^b) \mid g \text{ is a generator of } G_q, \text{ and } a, b \in \mathbb{Z}_q\}.$$

The CDH problem is to compute $\text{CDH}(w) = g^{ab}$ for a tuple $w = (Q, g, g^a, g^b) \in \text{CDH}$. The CDH problem is $(T_{\text{cdh}}, \varepsilon_{\text{cdh}})$-hard if

$$\Pr[M(Q, g^a, g^b) = g^{ab}] < \varepsilon_{\text{cdh}}$$

holds for any $k$ and any probabilistic Turing machine $M$ whose running time is at most $T_{\text{cdh}}$, where $(Q, g) = \text{Gen}(1^k)$ and $a, b \in \mathbb{Z}_q$. The probability is taken over the random tapes of $M$ and $\text{Gen}$, and the random choice of $a, b \in \mathbb{Z}_q$.

We state the relationship between the DDH and CDH problems.

Lemma 2.1. If the DDH problem is $(T_{\text{ddh}}, \varepsilon_{\text{ddh}})$-hard, then the CDH problem is $(T_{\text{ddh}}, \varepsilon_{\text{ddh}} + 2^{-k})$-hard.

Proof. Assume that the CDH problem is not $(T_{\text{ddh}}, \varepsilon_{\text{ddh}} + 2^{-k})$-hard. Then there exist a probabilistic Turing machine $M$ whose running time is at most $T_{\text{ddh}}$ such that

$$\Pr[M(Q, g^a, g^b) = g^{ab}] \geq \varepsilon_{\text{ddh}} + \frac{1}{2^k}.$$
holds for some $k_0$, where $(Q, g) \in \text{Gen}(1^k)$ and the probability is taken over the random tapes of $\mathcal{M}$ and Gen, and the random choice of $a, b \in \mathbb{Z}_q$. We now construct a probabilistic machine $\mathcal{A}$ as follows: On input $w = (Q, g, g_1, g_2, g_3)$.

1. Simulate $\mathcal{M}$ on input $(Q, g, g_1, g_2)$, and get an output $C$.
2. If $C = g_3$, then output 1, and halt. Otherwise, output 0, and halt.

We see that the running time of $\mathcal{A}$ is almost the same as that of $\mathcal{M}$. If $(Q, g) = \text{Gen}(1^k)$, then we have

$$\Pr_{w \in \text{DH}}[\mathcal{A}(w) = 1] = \Pr_{w \in \text{DH}}[\mathcal{M}(Q, g, g_1, g_2) = g_3] \geq \varepsilon_{\text{dbh}} + \frac{1}{2k_0}$$

and

$$\Pr_{w \in \text{DH}}[\mathcal{A}(w) = 1] = \Pr_{w \in \text{DH}}[\mathcal{M}(Q, g, g_1, g_2) = g_3] = \sum_{g \in \mathbb{G}_q} \Pr_{w \in \text{DH}}[\mathcal{M}(Q, g, g_1, g_2) = g_3 \land g_3 = g'] = \frac{1}{q} \sum_{g \in \mathbb{G}_q} \Pr_{w \in \text{DH}}[\mathcal{M}(Q, g, g_1, g_2) = g'] = \frac{1}{q}.$$  

Hence, we have

$$\text{Adv}_{\mathcal{A}}^{\text{DDH}}(k_0) \geq \left( \varepsilon_{\text{dbh}}(k_0) + \frac{1}{2k_0} \right) - \frac{1}{q} \geq \varepsilon_{\text{dbh}}(k_0).$$

This implies that the DDH problem is not $(T_{\text{dbh}}, \varepsilon_{\text{dbh}})$-hard, and the lemma follows. \qed

2.2 Simulation-Sound Non-Interactive Zero-Knowledge Proofs

A non-interactive proof system for a language $\mathcal{L}$ consists of two probabilistic polynomial-time algorithms $\mathcal{P}(\mathcal{L})$ and $\mathcal{V}(\mathcal{L})$:

- Prover $\mathcal{P}(\mathcal{L})$ produces a proof $\pi$ on input an instance $x$ and its witness $w$.
- Verifier $\mathcal{V}(\mathcal{L})$, on input an instance $x$ and a proof $\pi$, decides whether or not $\pi$ is a correct proof of the membership of $x \in \mathcal{L}$.

A proof $\pi$ is said to be valid if $\pi$ is correct. If $\pi$ is not correct, then $\pi$ is said to be invalid.

We give the definition of simulation-sound non-interactive zero-knowledge (SS-NIZK, for short) proof systems in the random oracle model [4]. We consider the following two games for a non-interactive proof system $(\mathcal{P}(\mathcal{L}), \mathcal{V}(\mathcal{L}))$ between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$:

Game ZK
1. $\mathcal{C}$ first chooses $\beta \in \{1,2\}$.
2. $\mathcal{A}$ is allowed to access a random oracle. If $\mathcal{A}$ queries any instance $\sigma$, then $\mathcal{C}$ answers a hash value $H(\sigma)$.
3. $\mathcal{A}$ is allowed to access a prover oracle. When $\mathcal{A}$ queries any pair $(x, w)$ of an instance $x$ and a witness $w$:
   a. if $\beta = 1$, then $\mathcal{C}$ answers a proof $\pi = \mathcal{P}(\mathcal{L})(x, w)$.
   b. if $\beta = 2$, then $\mathcal{C}$ answers a "simulated proof" $\pi = \delta(\mathcal{L})(x)$, where $\delta(\mathcal{L})$ is a probabilistic algorithm called simulator.
4. $\mathcal{A}$ sends $\tilde{\beta} \in \{1,2\}$ to $\mathcal{C}$.

In Game ZK, $\mathcal{A}$ is allowed to adaptively execute Steps (2) and (3) polynomially-many times in arbitrary order.

Game SS
1. $\mathcal{C}$ sets $S = \emptyset$.
2. $\mathcal{A}$ is allowed to access a random oracle. If $\mathcal{A}$ queries any instance $\sigma$, then $\mathcal{C}$ answers a hash value $H(\sigma)$.
3. $\mathcal{A}$ is allowed to access a simulator $\delta(\mathcal{L})$. If $\mathcal{A}$ queries any instance $x$, then $\mathcal{C}$ answers a simulated proof $\pi = \delta(\mathcal{L})(x)$, and sets $S = S \cup \{(x, \pi)\}$.
4. $\mathcal{A}$ sends a pair $(x^*, \pi^*)$ of an instance $x^*$ and a proof $\pi^*$ to $\mathcal{C}$.

In Game SS, $\mathcal{A}$ is allowed to adaptively execute Steps (2) and (3) polynomially-many times in arbitrary order.

We use the following notation. Let $\Pr[E_1]$ denote the probability that an event $E_1$ occurs, and let $\Pr[E_1|E_2]$ denote the conditional probability of $E_1$ occurrence of event $E_2$.

**Definition 2.2** ([4]). A proof system $(\mathcal{P}(\mathcal{L}), \mathcal{V}(\mathcal{L}))$ for a language $\mathcal{L}$ is $(T_S, q^q, q^H, \varepsilon_{\text{ZK}}, \varepsilon_{\text{SS}})$-SS-NIZK if there exists a simulator algorithm $\delta(\mathcal{L})$ whose running time is at most $T_S$ such that the following conditions hold for any adversary $\mathcal{A}$:

1. $(\mathcal{P}(\mathcal{L}), \mathcal{V}(\mathcal{L}))$ is a non-interactive proof system,
2. In each of Game ZK and Game SS, $\mathcal{A}$ is allowed to access a random oracle and a prover oracle (or a simulator $\delta(\mathcal{L})$) at most $q^q_H$ and $q^q_B$ times, respectively.
3. In Game ZK, the following inequality holds for any adversary $\mathcal{A}$:
   $$\left| \Pr[\tilde{\beta} = 1|\beta = 1] - \Pr[\tilde{\beta} = 1|\beta = 2] \right| \leq \varepsilon_{\text{ZK}}.$$
(4) In Step (4) of Game SS, the probability that $A$ outputs $(x^*, \pi^*)$ which satisfies the following conditions is at most $s_{SS}$: (i) $(x^*, \pi^*) \notin S$, (ii) $x^* \notin L$, and (iii) $\pi^*$ is valid.

2.3 Password-Protected Secret Sharing Schemes

We now introduce a formal description of PPSS schemes [4]. There are three sorts of participants in PPSS schemes: the initialization algorithm, the user algorithm and the algorithms for the servers. We formalize the setting for PPSS schemes in the following way.

Let $k$ denote a security parameter. A PPSS scheme involves a PPT algorithm $\text{Setup}$. This takes $1^k$ as an input, and outputs a setup parameter $\lambda \in \Lambda(k)$, where $\Lambda(k)$ is a finite set of all possible setup parameters with respect to the security parameter $k$. The setup parameter $\lambda$ specifies the following items:

- a set $PW_\lambda$ of all passwords;
- a set $Doc_\lambda$ of all documents;
- a set $Pub_\lambda$ of all public parameters;
- a set $Sec_\lambda$ of all secret seeds;
- a number $n$ of the servers; and
- a number $t$ with $0 < t \leq n$ for the $(t, n)$-threshold secret sharing that will be employed in the PPSS scheme.

We note that the numbers $n$ and $t$ are at most $\zeta(k)$ for some polynomial $\zeta$ since $\text{Setup}$ is a PPT algorithm.

For the PPSS scheme, the following three items are designated in addition to the algorithm $\text{Setup}$:

- $\text{Init}$: This is the initialization algorithm that takes a tuple $(\lambda, p, d)$ of a setup parameter $\lambda$, a password $p \in PW_\lambda$ and a secret document $d \in Doc_\lambda$ as an input, and outputs a pair (pub, sec) of a public parameter

$$\text{pub} = (\text{pub}_1, \text{pub}_2, \text{pub}_3) = (\text{pub}_1(\lambda), \text{pub}_2(\text{pub}_1(\lambda), p), \text{pub}_3(\text{pub}_1(\lambda), d)) \in \text{Pub}_\lambda$$

and a set $\text{sec} = \{\text{sec}_j\}_{j=1}^n$ of the seeds of the shares, where $\text{sec}_j \in \text{Sec}_\lambda$ denotes the seed stored with the $j$-th server.

We assume that $\text{Init}$ is a PPT algorithm.

- $\text{User}$ and $\text{Server} = \{\text{Server}_j\}_{j=1}^n$: The algorithms $\text{User}$ and $\text{Server}_j$, are PPT algorithms, and they are employed by the user and the $j$-th server, respectively. The user’s algorithm $\text{User}$ interacts with the server’s algorithm $\text{Server}_j$, for each $j$. At first, $\text{User}$ is given a tuple $(\lambda, p, \text{pub})$ of a setup parameter $\lambda$, a password $p \in PW_\lambda$ and a public parameter $\text{pub}$ as an input, and the algorithm $\text{Server}_j$ for each $j$ is given a tuple $(\lambda, \text{pub}, \text{sec}_j)$ of a setup parameter $\lambda$, a public parameter $\text{pub}$ and a seed $\text{sec}_j \in \text{Sec}_\lambda$. Interacting with the $n$ servers, $\text{User}$ eventually outputs either a document $d'$ or $\bot$, where $\bot$ denotes that $\text{User}$ has failed to recover the secret document $d$.

We write $\mathcal{P} = (\text{Setup}, \text{Init}, \text{User}, \text{Server})$ to denote a PPSS scheme. For a PPSS scheme $\mathcal{P}$ and $\tilde{p} \in PW_\lambda$, the output of $\text{User}$ are denoted by $\mathcal{P}(\tilde{p}, (\text{pub}, \{\text{sec}_j\}_{j=1}^n))$ on an input $(\lambda, \tilde{p}, \text{pub})$, where $\{\text{sec}_j\}_{j=1}^n = \text{Init}(p, d)$ for some $p \in PW_\lambda$ and $d \in Doc_\lambda$. A PPSS scheme $\mathcal{P}$ is valid if $\mathcal{P}(p, \text{Init}(\lambda, p, d)) = d$ holds for any $\lambda \in \Lambda(k)$, $p \in PW_\lambda$ and $d \in Doc_\lambda$. The PPSS schemes we consider in this paper are all valid.

2.4 A Security Notion for PPSS schemes: PPSS-security

We state the security of PPSS schemes defined in [4]. Let $\mathcal{P} = (\text{Setup}, \text{Init}, \text{User}, \text{Server})$ be a PPSS scheme. Then a PPSS adversarial game for $\mathcal{P}$ between an adversary $A$ and a challenger $C$ is defined as follows:

**Initialization phase**: $C$ first executes $\text{Setup}$ on input $1^k$, and gets a setup parameter $\lambda$. Then $C$ sends $\lambda$ to $A$. $A$ chooses two documents $d_1, d_2 \in Doc_\lambda$ and a subset $V' \subseteq [n] = \{1, \ldots, n\}$ with $\#V' = t < n$, and sends a tuple $(d_1, d_2, V')$ to $C$. $C$ chooses $\beta \in \{1, 2\}$ and $p \in PW_\lambda$. Then $C$ executes $\text{Init}$ on an input $(\lambda, p, d_\beta)$, and gets a tuple $(\text{pub}, \{\text{sec}_j\}_{j=1}^n)$. Finally, $C$ sends $(\text{pub}, \{\text{sec}_j\}_{j \in V'})$ to $A$.

**User’s query phase**: $A$ is allowed to interact with $C$. In each interaction, $A$ freely chooses the index $j$, and sits at the $j$-th server’s position. $C$ plays the role of the user who is given the tuple $(\lambda, p, \text{pub})$. $A$ and $C$ follow a single round of the scheme in each interaction. It should be noted that $A$ may deviate from the regular protocol according to his strategy, but $C$ strictly follows the protocol. $A$ may adaptively interact with $C$ in the manner.

**Server’s query phase**: $A$ is allowed to interact with $C$. In each interaction, $A$ sits at the server’s position and freely chooses a number $j \in [n] \setminus V'$. $C$ plays the role of $j$-th server given the pair $(\text{pub}, \text{sec}_j)$. $A$ and $C$ follow a single round of the scheme in each interaction. It should be noted that $A$ may deviate from the regular protocol according to his strategy, but $C$ strictly follows the protocol. $A$ may adaptively interact with $C$ in the manner.

**Challenge phase**: $A$ sends $\beta' \in \{1, 2\}$.

For $\beta = \{1, 2\}$, let $P(d_j; d_1, d_2)$ denote the probability that $A$ sends 1 in Challenge phase of the PPSS adversarial game under the following conditions: In Initialization phase,

1. $A$ chooses two documents $d_1$ and $d_2$, and
2. $C$ chooses $\beta$,

where the probability is taken over random tapes of $A$ and $C$.

**Definition 2.3 ([4])**. A PPSS scheme $\mathcal{P}$ is $(q_U, q_S, T, \varepsilon)$-PPSS-secure if for any security parameter $k$, any setup
A Rigorous Security Proof for the Enhanced Version of Password-Protected Secret Sharing Scheme

Parameter $\lambda \in \Lambda(k)$, any documents $d_1, d_2 \in \text{Doc}_1$, any subset $V' \subseteq [n]$ with $\#V' = t' < t$ and any adversary $\mathcal{A}$, the inequality

$$|P(d_1; d_1, d_2) - P(d_2; d_1, d_2)| \leq \left| q_\mathcal{S} \frac{t - t'}{t - t'} \right| \cdot \frac{1}{\#PW_\mathcal{A}} + \varepsilon$$

holds under the following conditions:
(1) $\mathcal{A}$ chooses the subset $V' \subseteq [n]$ in Initialization phase,
(2) the running time of the adversary $\mathcal{A}$ is at most $T$,
(3) $\mathcal{A}$ is allowed to enter User’s query phase at most $q_U$ times,
(4) $\mathcal{A}$ is allowed to enter Server’s query phase at most $q_S$ times.

2.5 Another security notion for PPSS schemes: $\text{pparam-security}$

We state another PPSS security notion called $\text{pparam-secure}$ [7]. A pparam-attack game for a PPSS scheme $\mathcal{P}$ between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ is as follows:

**Initialization phase:** $\mathcal{C}$ first executes Setup on input $1^k$, and gets a setup parameter $\lambda$. Then $\mathcal{C}$ sends $\lambda$ to $\mathcal{A}$. $\mathcal{A}$ chooses two documents $d_1, d_2 \in \text{Doc}_1$, and sends them to $\mathcal{C}$. $\mathcal{C}$ chooses $\beta \in \{1, 2\}$. Then $\mathcal{C}$ executes Init on an input $(\lambda, p, d_\beta)$, and gets a pair $(\text{pub}, \text{sec})$, where $\text{pub} = (\text{pub}_1, \text{pub}_2, \text{pub}_3)$. Finally, $\mathcal{C}$ sends the public parameter pair to $\mathcal{A}$.

**Attack phase:** $\mathcal{A}$ is allowed to interact with $\mathcal{C}$. In each interaction, $\mathcal{A}$ sends a public parameter $\text{pub}' = (\text{pub}_1', \text{pub}_2', \text{pub}_3') \in \text{Pub}_3$. $\mathcal{C}$ plays the role in computing the “inverse” of the initialization algorithm if $\text{pub}_1 = \text{pub}'_1$ and $\text{pub}_3 = \text{pub}'_3$. Then $\mathcal{C}$ returns a document $d \in \text{Doc}_1$, which satisfies $\text{Init}(\lambda, p, d) = (\text{pub}', \text{sec}')$ for some $p \in \text{PW}_\lambda$ and $\text{sec}' \in \text{Sec}_1$. Otherwise, $\mathcal{C}$ returns a special symbol $\perp$.

**Challenge phase:** $\mathcal{A}$ sends $\beta' \in \{1, 2\}$.

For $\beta = 1, 2$ and a security parameter $k$, let $P^{\beta}_{\text{pparam-attk}}(k)$ denote the probability that $\mathcal{A}$ sends $1$ in Challenge phase of the pparam-attack game under the condition that $\mathcal{C}$ chooses $\beta$ in Initialization phase, where the probability is taken over the random tapes of $\mathcal{A}$ and $\mathcal{C}$.

For a security parameter $k$ and an adversary $\mathcal{A}$, we define $\text{Adv}_{\mathcal{A}}(k)$ by

$$\text{Adv}_{\mathcal{A}}(k) = \left| P^{1}_{\text{pparam-attk}}(k) - P^{2}_{\text{pparam-attk}}(k) \right|.$$

**Definition 2.4** [7]. A PPSS scheme $\mathcal{P}$ is $(T, \varepsilon, \lambda)$-pparam-secure if for any security parameter $k$ and any adversary $\mathcal{A}$, $\text{Adv}_{\mathcal{A}}(k) < \varepsilon$ holds under the following conditions:
(1) $\mathcal{A}$ is allowed to enter Attack phase at most $q_\mathcal{A}$ times, and
(2) the running time of $\mathcal{A}$ is at most $T$.

It should be noted that the pparam-security is independent of the PPSS-security in a sense that the pparam-security does not imply the PPSS-security in general and vice versa. Indeed, the protocol PPSS$_2$ proposed in [4] is PPSS-secure [4], but not pparam-secure [7]. On the other hand, one can easily construct a protocol which is pparam-secure but not PPSS-secure. We give the protocol in Section 4. Hence, one prefers PPSS schemes which are both PPSS-secure and pparam-secure.

3. The protocol $\text{ePPSS}_2$ and Main Theorem

We depict a protocol $\text{ePPSS}_2$ in Protocol 1: the proof systems $(\mathcal{P}(\mathcal{L}_{\mathcal{S}_1}^{\text{pub}}), \mathcal{V}(\mathcal{L}_{\mathcal{S}_1}^{\text{pub}}))$ and $(\mathcal{P}(\mathcal{L}_{\mathcal{S}_2}^{\text{pub}}), \mathcal{V}(\mathcal{L}_{\mathcal{S}_2}^{\text{pub}}))$ are given in [4], and $(\mathcal{P}(\mathcal{L}_{\mathcal{S}_1}^{\text{pub}}), \mathcal{V}(\mathcal{L}_{\mathcal{S}_1}^{\text{pub}}))$ is given in [7]. [4] in [4], they stated that, for any given $q_\mathcal{P}$ and $q_\mathcal{H}$, these systems are $(T_\mathcal{S}, q_\mathcal{S} \epsilon_\text{SS}, \text{SS}-\text{NIZK})$, where $\epsilon_\text{SS} = \frac{q_\mathcal{P} q_\mathcal{H}}{q}$ and $T_\mathcal{S}$ is the same as the running time of the corresponding prover. The non-interactive proof system $(\mathcal{P}(\mathcal{L}_{\mathcal{E}}^{\text{pub}}), \mathcal{V}(\mathcal{L}_{\mathcal{E}}^{\text{pub}}))$ is similarly defined (see also [6]).

The protocol $\text{ePPSS}_2$ is the same as the protocol PPSS$_2$ except for the following three points:
(1) In Init, one constructs two pairs ($(g, y_1), x_1$) and ($(g, y_2), x_2$) of the public and secret keys, and generates two ElGamal encryptions $(u_{1, d}, v_{1, d})$ and $(u_{2, d}, v_{2, d})$ of the document $d$.
(2) In order to prove that $(u_{1, d}, v_{1, d})$ and $(u_{2, d}, v_{2, d})$ are encryptions of the same document $d$, a proof $\pi$ is added in the public parameter.
(3) The verification process of the proof $\pi$ is added in Step S1-1.

It was shown that $\text{ePPSS}_2$ is pparam-secure in [7]. Our main result is as follows:

**Theorem.** Assume that the following properties hold:

- the DDH problem is $(T_{\text{ddh}}, \epsilon_{\text{ddh}})$-hard,
- the proof systems $(\mathcal{P}(\mathcal{L}_{\mathcal{S}_1}^{\text{pub}}), \mathcal{V}(\mathcal{L}_{\mathcal{S}_1}^{\text{pub}}))$, $(\mathcal{P}(\mathcal{L}_{\mathcal{S}_2}^{\text{pub}}), \mathcal{V}(\mathcal{L}_{\mathcal{S}_2}^{\text{pub}}))$, and $(\mathcal{P}(\mathcal{L}_{\mathcal{S}_1}^{\text{pub}}), \mathcal{V}(\mathcal{L}_{\mathcal{S}_2}^{\text{pub}}))$ are $(T_{\mathcal{S}}, q_\mathcal{S}, \epsilon_{\text{SS}}, \text{SS}-\text{NIZK})$ and
- the proof system $(\mathcal{P}(\mathcal{L}_{\mathcal{E}}^{\text{pub}}), \mathcal{V}(\mathcal{L}_{\mathcal{E}}^{\text{pub}}))$ is $(T_{\mathcal{E}}, 1, \epsilon_{\text{SS}}, \text{SS}-\text{NIZK})$. 

...
The setup algorithm Setup:

1: Input $t^k$.
2: Run Gen on input $t^k$, and get a pair $(Q, g)$.
3: Choose natural numbers $t$ and $n$ with $t \leq n < T_{\text{Gen}}(k)$, where $T_{\text{Gen}}$ is a running time of Gen. Then output $\lambda = (q, g, t, n)$, where $q = (Q - 1)/2$.

The initialization algorithm Init:

11: Input a tuple $(\lambda, p, d)$, where $\lambda = (q, g, t, n)$ is a setup parameter output by Setup, $p \in \mathbb{Z}_q = \mathbb{P}W_d$ and $d \in \mathbb{G}_q = \mathbb{D}oc_i$.
12: Choose $x_1, x_2 \in \mathbb{Z}_q$, and compute $y_1 = g^{x_1}, y_2 = g^{x_2}, \{x_1\}_{j=1}^n = S_{\text{Set}}(x_1)$ and $\{x_2\}_{j=1}^n = S_{\text{Set}}(x_2)$.
13: Choose $h, \tilde{h}, \tilde{y}, \tilde{g} \in \mathbb{G}_q$ and $r_p, r_{1,d}, r_{2,d} \in \mathbb{Z}_q$.
14: Compute $u_p = g^\lambda, u_p = y_1^{r_p}, u_{1,d} = g^{x_1 r_p}, u_{2,d} = g^{x_2 r_p}, v_{1,d} = y_1^r d$ and $v_{2,d} = y_2^{r_p} d$.
15: Choose $r_{1,j}, r_{2,j} \in \mathbb{Z}_q$, and compute $y_{1,j} = g^{x_1 j r_p}$ and $y_{2,j} = g^{x_2 j r_p}$ for each $j \in \{n\}$.
16: Run $\mathcal{P}(\mathbb{L}_{\mathbb{S}_1}^{\text{pub}})$ on an input $((u_{1,d}, v_{1,d}, u_{2,d}, v_{2,d}), r_{1,d}, r_{2,d})$, and get a proof $\pi_1$.
17: Set $pub_j = (g, y_{1,j}, y_{2,j}, \{y_{1,j}\}_{j=1}^n, \{y_{2,j}\}_{j=1}^n, \tilde{h}, \tilde{y}, \tilde{g})$, $pub_j = (u_p, v_p)$, $pub_j = (u_{1,d}, v_{1,d}, u_{2,d}, v_{2,d})$ and $sec_j = (x_{1,j}, r_{1,j}, x_{2,j}, r_{2,j})$ for each $j \in \{n\}$, and output $(pub, sec) = ((pub_1, pub_2, pub_3, \pi, \{sec\}_{j=1}^n)$.

The interaction between the user algorithm User and the server algorithms Server$_1$, . . . , Server$_n$:

- User’s input is a tuple $(\lambda, pub, \tilde{p})$, where $\tilde{p} \in \mathbb{Z}_q = \mathbb{P}W_d$.
- For each $j$, Server$_j$’s input is a tuple $(\lambda, pub, sec_j)$.

U and $S_j$ are the same as those of PPSS$_2$.

S$_{1}$-1: If $\pi_1$ is invalid, then halt.
S$_{1}$-2: Choose $t_j \in \mathbb{Z}_q$, and compute $a_j = g^{x_1} b_j = u_p^\lambda$ and $\tilde{a}_j = (\tilde{g})^{x_1}$.
S$_{1}$-3: Run $\mathcal{P}(\mathbb{L}_{\mathbb{S}_1}^{\text{pub}})$ on an input $((a_j, b_j, \tilde{a}_j), t_j)$, and get a proof $\pi_{1,j}$.
S$_{1}$-4: Send a tuple $(a_j, b_j, \tilde{a}_j, \pi_{1,j})$ to User.

U$_{1}$-1: Choose a subset $V \subseteq \{n\}$ with $|V| = t$.
U$_{1}$-2: If $\pi_{1,j}$ is invalid for some $j \in V$, then halt.
U$_{1}$-3: Choose $r_p \in \mathbb{Z}_q$, and compute $w_p = g^{x_1 r_p}, v_p = y_1^{x_1 r_p}, \tilde{u}_p = (\tilde{g})^{x_1} r_p$ and $\tilde{v}_p = (\tilde{g})^{x_1} (\tilde{h})^{x_1}$.
U$_{1}$-4: Compute $e_j = (a_j)^{y_p}$ for each $j \in \{n\}$.
U$_{1}$-5: Compute $u = \prod_{e \in V(\{V\}, e_j)}^{x_2} j = \ell \mod q$.
U$_{1}$-6: Run $\mathcal{P}(\mathbb{L}_{\mathbb{S}_2}^{\text{pub}})$ on an input $((a_j, e_j, u_p, v_p, \tilde{u}_p, \tilde{v}_p, r_p, \tilde{p}), r_p, \tilde{p})$, and get a proof $\pi_{2,j}$.
U$_{1}$-7: Send a tuple $(V, u, e_j, u_p, v_p, \tilde{u}_p, \tilde{v}_p, \pi_{2,j})$ to Server$_j$ for each $j \in \{n\}$.

S$_{2}$-1: If $j \not\in V$ or $\pi_{2,j}$ is invalid, then halt.
S$_{2}$-2: Compute $w_j = (u_{1,d})^{y_j x_{1,j}},$ where

$$\lambda_j = \prod_{e \in V(\{j\})}^{x_2} j - \ell \mod q.$$

S$_{2}$-3: Compute $v_j = (v_p / v_{p,j})^{y_j}$.
S$_{2}$-4: Compute $z_j = v_j / w_j$.
S$_{2}$-5: Choose $r_{2,j} \in \mathbb{Z}_q$, and compute $u_{2,j} = g^{x_2}$ and $v_j = (u_p)^{y_j} z_j$.
S$_{2}$-6: Run $\mathcal{P}(\mathbb{L}_{\mathbb{S}_2}^{\text{pub}})$ on an input $((u_{2,j}, v_j, u_p, v_p, \tilde{u}_p, \tilde{v}_p, r_{2,j}, x_{1,j}, r_{1,j}))$, and get a proof $\pi_{3,j}$.
S$_{2}$-7: Send a tuple $((u_{2,j}, v_j, x_{1,j}), \pi_{3,j})$ to User.

U$_{2}$-1: If $\pi_{3,j}$ is invalid for some $j \in V$, then halt.
U$_{2}$-2: Compute $d' = v_1 d' \prod_{e \in V(\{V\})}^{x_2} j = \ell \mod q$, and output $d'$.

The languages $\mathbb{L}_{\mathbb{S}_1}^{\text{pub}}, \mathbb{L}_{\mathbb{S}_2}^{\text{pub}}$, $\mathbb{L}_{\mathbb{S}_2}^{\text{pub}}$, and $\mathbb{L}_{\mathbb{E}}^{\text{pub}}$ are defined as follows:

$$\mathbb{L}_{\mathbb{S}_1}^{\text{pub}} = \{(a_j, b_j, \tilde{a}_j) \in \mathbb{G}_q, \exists t_j \in \mathbb{Z}_q \text{ s.t. } (a_j, b_j, \tilde{a}_j) = (g^{x_1}(u_p)^{x_1} (\tilde{g})^{y_1})\}.$$

$$\mathbb{L}_{\mathbb{S}_2}^{\text{pub}} = \{(u_{2,j}, v_j, u_p, v_p, \tilde{u}_p, \tilde{v}_p) \in \mathbb{G}_q \mid \exists (r_{2,j}, \tilde{p}) \in \mathbb{Z}_q \text{ s.t. } (u_{2,j}, v_j, u_p, v_p, \tilde{u}_p, \tilde{v}_p) = (u_p)^{x_2} g^{x_2} y_j r_{2,j} (\tilde{g})^{y_2} (\tilde{h})^{x_2}\}$$

$$\mathbb{L}_{\mathbb{S}_2}^{\text{pub}} = \{(u_{2,j}, v_j, u_p, v_p, \tilde{u}_p, \tilde{v}_p) \in \mathbb{G}_q \mid \exists (r_{2,j}, t_j, x_j, r_j) \in \mathbb{Z}_q \text{ s.t. } (y_j, a_j, u_{2,j}, v_j) = (g^{x_2} y_{j} r_{2,j} g^{x_2} (u_p)^{x_1} (v_p / v_{p,j})^{y_j} (u_p)^{x_1})\}$$

and

$$\mathbb{L}_{\mathbb{E}}^{\text{pub}} = \{(u_{1,d}, v_{1,d}, u_{2,d}, v_{2,d}) \in \mathbb{G}_q \mid \exists (r_{1,d}, r_{2,d}) \in \mathbb{Z}_q \text{ s.t. } u_{1,d} = g^{x_1} u_{2,d} = g^{x_2}, v_{1,d} / v_{2,d} = y_1^{x_2} / y_2^{x_2}\}.$$
5. Proof of Main Theorem

Then the protocol ePPSS₂ is \((q_U, q_S, T, \varepsilon)\)-PPSS-secure, where \(\max \{nq_U, q_S\} \leq q^5_H, \)
\[ T \leq T_{\text{adh}} - 4T_S - q_U f^U - q_S f^S - f^I \]
for some polynomials \(f^U, f^S\) and \(f^I\) in \(n, t\) and \(k\), and
\[ \varepsilon \leq 8\varepsilon_{\text{ZK}} + (4nq_U q_S + 6nq_U - 4nq_S + 6q_S)\varepsilon_{\text{SS}} + (2q_U q_S + 3q_U + 2q_S + 7)\varepsilon_{\text{adh}} + q_U q_S \omega_1 + q_U \omega_2 + q_S \omega_3 + \omega_4, \]
where \(\omega_1, \omega_2, \omega_3\) and \(\omega_4\) are negligible in \(k\).

The proof of the theorem is given in Section 5.

4. A protocol which is pparam-secure but not PPSS-secure

As stated in the last of Section 2, the pparam-security is independent of the PPSS-security. In this section, we give a protocol which is pparam-secure but not PPSS-secure. The protocol is depicted in Protocol 2. We see that Protocol 2 is pparam-secure.

The setup algorithm Setup and Init are the same as those of ePPSS₂.

The interaction between the user algorithm User and the server algorithms Server₁, ..., Serverₙ:
- User’s input is a tuple \((λ, pub, p)\), where \(p \in \mathbb{Z}_q = PW_1\).
- For each \(j\), Serverᵢ’s input is a tuple \((λ, pub, \text{sec})\).

**U** and **S** are the same as those of PPSS₂.

**U1-1**: Choose a subset \(V ⊆ [n]\) with \(\#V = t\).

**U1-2**: Send \(V\) to **Server** for each \(j \in [n]\).

**S**₁: If \(π\) is invalid, then halt.

**S**₂: If \(j \in V\), then send the secret \(x_{1,j}\) to User. Otherwise, halt.

**U2-1**: Compute \(x'_i = Σ_{j | V \cap \{j\} ≠ \emptyset} A_j\), where \(A_j\) is defined in Step **S**₂-2 of the protocol ePPSS₂.

**U2-2**: Compute \(d' = v_{1,\ell}/(u_{1,\ell}v'_1), \) and output \(d'\).

Protocol 2. A protocol which is pparam-secure but not PPSS-secure

**Proposition 4.1.** Assume that the following properties hold:
- the protocol PPSS₂ is \((T, \varepsilon, 0)\)-pparam-secure, and
- the proof system \((\mathcal{P}(L_p^{\text{pub}}), \mathcal{V}(L_p^{\text{pub}}))\) is \((T_S, 1, q^2_H, \varepsilon_{\text{ZK}}, \varepsilon_{\text{SS}})-\text{SS-NIZK}\).

Then Protocol 2 is \((T', \varepsilon', q^2_H)\)-pparam-secure, where
\[ T' \leq T - T_S - q_A f_A, \quad q_A \leq q^S_H \quad \text{and} \quad \varepsilon' \leq 2\varepsilon + 6\varepsilon_{\text{SS}} \]
for some polynomial \(f_A\) in \(n, t\) and \(k\).

The proof of this proposition is the same as Theorem in [7]. On the other hand, Protocol 2 is not PPSS-secure.

**Proposition 4.2.** Protocol 2 is not PPSS-secure.

**Proof.** In the PPSS adversarial game for Protocol 2, assume that the adversary \(A\) receives the public parameter \(pub\) and the subset \(\{x_{1,j}\}_{j \in V}\) of secret seeds. Entering Server’s query phase at most \(t - t'\) times, \(A\) receives another subset \(\{x_{1,j}\}_{j \notin V_0}\) of secret seeds, where \(V_0\) is a subset of \([n]\) \(\setminus V\) with \(\#V_0 = t - t'\). Then, in time polynomial in the length of the setup parameter, computing \(x_1\) from the subset \(\{x_{1,j}\}_{j \notin V'}\) of secret seeds, \(A\) can recover the stored document. This implies that this protocol is not \((0, t - t', T, \varepsilon')\)-PPSS-secure, where \(T\) is the running time of \(A\) and \(\varepsilon'\) is any positive number which satisfies \(1 > 1/\#PW_1 + \varepsilon'\).

5. Proof of Main Theorem

We now give the proof of the theorem. We state several lemmas in order to prove the theorem. The proofs of the lemmas are given in Section 6.

We use the hybrid argument. Let \(A\) be a probabilistic machine followed by an adversary of the PPSS adversarial game for ePPSS₂. Assume that the running time of \(A\) is \(T\). Using the adversary \(A\), we define sequences of games \((\text{Game}(\mu, v))_{\mu, v}\) and \((\text{Game}(\mu, v, J))_{\mu, v, J}\). Let \((Q, g) = \text{Gen}(1^k)\). We first depict the game \text{Game}(0, 0) in Protocol 3. This game models the real PPSS adversarial game for ePPSS₂ with the exception that the real proofs constructed in ePPSS₂ are replaced by the simulated proofs and that Output phase is added. We convert the game \text{Game}(0, 0) so that the game does not depend on the document \(d\) and the password \(p\).
Initialization phase

I0: Set $C_V = C_S = C_f = 0$, $F = \text{false}$ and $\text{Upset} = \emptyset$.
I1: Choose $n, t \in \mathbb{N}$ with $t \geq n$, and send a tuple $(q, g, n, t)$ to $\mathcal{A}$, where $q = (Q - 1)/2$.
I2: If $\mathcal{A}$ sends two documents $d_1, d_2 \in \mathcal{Q}_q$ and a subset $\mathcal{V} \subseteq [n]$ with $|\mathcal{V}| = t' < t$, then choose $\beta \in \{1, 2\}$.
I3: Choose $x_1, x_2, y_1, y_2 \in \mathcal{Q}_q$, and compute $y_1 = g^{x_1^4}$, $y_2 = g^{x_2^4}$, $\{x_1, y_1\}_{j=1}^n = SS_{\mathcal{Q}_q}(x_1)$ and $\{x_2, y_2\}_{j=1}^n = SS_{\mathcal{Q}_q}(x_2)$.
I4: Choose $h, \hat{h}, \tilde{h}, \hat{\gamma}, \tilde{\gamma} \in \mathcal{Q}_q$ and $\mu_1, r_1, r_2, r_3 \in \mathcal{Q}_q$.
I5: Choose a password $p \in \mathcal{Q}_q$, and compute $u_p = g^{\gamma_p}$ and $v_p = \gamma_p^h \hat{h}^p$.
I6: Compute $(u_{i,j}, v_{i,d}) = (g^{r_{i,j}^2}, y_{i,j}^4 r_{i,j}^2 \hat{h}^2 \hat{\gamma}^2 d_p)$.
I7: Choose $r_{1,j}, r_{2,j} \in \mathcal{Q}_q$, and compute $y_{1,j} = g^{x_{1,j}^4} h^{r_{1,j}}$ and $y_{2,j} = g^{x_{2,j}^4} h^{r_{2,j}}$ for each $j \in [n]$.
I8: Run the simulator $\delta(\mathcal{L}_E^{\text{pub}})$ on an input $(u_{i,d}, v_{i,d}, u_{i,d}, v_{i,d}, \beta)$, and get a proof $\pi$.
I9: Set $\text{pub}_1 = (y, y_1, y_2, h, \{x_1, y_1\}_{j=1}^n, \{x_2, y_2\}_{j=1}^n, \hat{h}, \tilde{h}, \hat{\gamma}, \tilde{\gamma})$, $\text{pub}_2 = (u_p, v_p)$, $\text{pub}_3 = ((u_{i,j}, v_{i,d}), (u_{i,d}, v_{i,d}), \beta)$ and $\text{sec}_j = (x_{1,j}, r_{1,j}, x_{2,j}, r_{2,j})$ for each $j \in [n]$, and send $(\text{pub}, \text{sec}_\mathcal{V}) = (\text{pub}_1, \text{pub}_2, \text{pub}_3, \{\text{sec}_j\}_{j \in \mathcal{V}})$.

User’s query phase

If $\mathcal{A}$ enters User’s query phase with an $n$-tuple $\{(j, a_j, b_j, \tilde{a}_j, \pi_{1,j})\}_{j \in [n]}$, then execute the following procedure:
U1-0: Set $C_V = C_U + 1$.
U1-1: If $\pi_{1,j}$ is invalid for some $j \in [n]$, then halt.
U1-2: Choose a subset $V \subseteq [n]$ with $|V| = t$. 
U1-3: Choose $r_p \in \mathcal{Z}_q$, and compute $u_p = g^{r_p}$, $v_p = y_p^{r_p} h^{r_p}$, $\hat{u}_p = (\hat{\gamma})^{r_p}$ and $\hat{v}_p = \hat{\gamma}^{r_p}(\hat{h})^{r_p}$.
U1-4: Set $u_p(C_{\mathcal{V}}) = u_p$ and $\text{Upset} = \text{Upset} \cup \{u_p(C_{\mathcal{V}})\}$.
U1-5: Compute $e_j = (a_j)^{r_p}$ for each $j \in [n]$.
U1-6: Compute $\mathcal{U} = \prod_{(b_j/\mu_j) \in \mathcal{V}} (b_j/\mu_j)$.
U1-7: Run the simulator $\delta(\mathcal{L}_E^{\text{pub}})$ on an input tuple $(a_j, e_j, u_p, v_p, \hat{u}_p, \hat{v}_p, \pi_{2,j})$, and get a proof $\pi_{2,j}$ for each $j \in [n]$.
U1-8: Send $(V, u, e, u_p, v_p, \hat{u}_p, \hat{v}_p, \pi_{2,j})$ for each $j \in [n]$.
If $\mathcal{A}$ returns a tuple $\{(u_{i,j}, v_{i,j}, \pi_{3,j})\}_{j \in \mathcal{V}}$, then execute the following procedure:
U2-1: If $\pi_{2,j}$ is invalid for some $j \in V$, then halt.
U2-2: Compute $d' = v_{i,d}(\prod_{(b_j/\mu_j) \in \mathcal{V}} (b_j/\mu_j))$, and send $d'$ to $\mathcal{A}$.

Server’s query phase

If $\mathcal{A}$ enters Server’s query phase with an index $j \in [n] \setminus V$, then executes the following procedure:
S1-0: Set $C_S = C_S + 1$.
S1-1: If $\pi$ is invalid, then halt.
S1-2: Choose $t_j \in \mathcal{Z}_q$, and compute $a_j = g^{t_j}$, $b_j = u_j^\theta$ and $\tilde{a}_j = (\tilde{\gamma})^{t_j}$.
S1-3: Run the simulator $\delta(\mathcal{L}_S^{\text{pub}})$ on an input $(a_j, b_j, \tilde{a}_j)$ and get a proof $\pi_{1,j}$.
S1-4: Send a tuple $(j, a_j, b_j, \tilde{a}_j, \pi_{1,j})$.
If $\mathcal{A}$ returns a tuple $(V, u, e, u_p, v_p, \hat{u}_p, \hat{v}_p, \pi_{2,j})$, then execute the following procedure:
S2-1: If $\hat{v}_p(\hat{v}_p^{(\hat{v}_p^{d_p})} = \hat{h}^{r_p}$, then $\text{Idset} = \text{Idset} \cup \{j\}$. If $\text{Idset} \supseteq t - t'$, then set $F = \text{true}$.
S2-2: Compute $u_{i,d} = (u_{i,d})^{(d_j/\lambda_j)^{\hat{a}_j}}$, where $\lambda_j$ is defined in Step S2-2 of the protocol $\mathsf{ePPSS}_2$.
S2-3: Compute $v_{i,d} = (u_{i,d})^{(d_j/\lambda_j)^{\hat{a}_j}}$.
S2-4: Compute $u_{i,d} = (u_{i,d})^{(d_j/\lambda_j)^{\hat{a}_j}}$.
S2-5: Compute $z_j = v_{i,d}/u_{i,d}$.
S2-6: Choose $t_j \in \mathcal{Z}_q$, and compute $a_j = g^{t_j}$ and $v_j = (u_{i,d} v_{i,d}^{(d_j/\lambda_j)^{\hat{a}_j}}$.
S2-7: Run the simulator $\delta(\mathcal{L}_S^{\text{pub}})$ on an input $(u_{i,d}, v_{i,d}, a_j, v_j/v_{i,d}, u_{i,d}^{(d_j/\lambda_j)^{\hat{a}_j}})$, and get a proof $\pi_{3,j}$.
S2-8: Send $(u_{i,d}, v_{i,d}, \pi_{3,j})$.

Output phase

If $\mathcal{A}$ outputs 1, then set $\varphi = 1$. Otherwise, set $\varphi = 0$.

Protocol 3. Game(0, 0)

For $\beta = 1, 2$, we define the probabilistic machine $\mathcal{M}_{0,0}^\beta$ as follows: On input $w = (Q, g, g_1, g_2, g_3)$,
(i) Simulate Game(0, 0) by using $(Q, g)$, and choose $\beta$ in Step I2 of Initialization phase.
(ii) Output $\psi$ set in Output phase.
Let $E_{0,0,d_0}$ be the event that the adversary $\mathcal{A}$ outputs 1, and let $\psi_{0,0}$ be the output of $\mathcal{M}_{0,0}^0$.
We similarly define probabilistic machines $\mathcal{M}_{0,0}^\beta$ and $\mathcal{M}_{0,0}^{\beta, \text{new}}$, events $E_{\mu, \nu, d_0}$ and $E_{\mu, \nu, d, d_0}$, and outputs $\psi_{\mu, \nu}^\beta$ and $\psi_{\mu, \nu, d, d_0}^\beta$.
We set $p_{\mu, \nu}(d_0) = \mathbb{P}[E_{\mu, \nu, d_0}]$ and $p_{\mu, \nu, d, d_0}(d_0) = \mathbb{P}[E_{\mu, \nu, d, d_0}]$.
We note the following facts: in Game(0, 0),
1. In Initialization phase, the challenger queries $\delta(\mathcal{L}_E^{\text{pub}})$ one time in order to make a proof $\pi$.
2. When $\mathcal{A}$ enters User’s query phase,
   - $\mathcal{A}$ queries the random oracles at most $n$ and $t$ times in order to make proofs $(\pi_{1,j})_{j \in [n]}$ and $(\pi_{3,j})_{j \in \mathcal{V}}$, respectively.
A Rigorous Security Proof for the Enhanced Version of Password-Protected Secret Sharing Scheme 39

(3) When $A$ enters Server’s query phase,

- The challenger queries $S(\mathcal{L}_{U}^{\text{ph}})$ $n$ times in order to make proofs $\{\tau_{y_j}\}_{j\in[n]}$.

We also note that $q_{U,0}^0$ only depends on $Q$ and $g$, and is independent of $g_1$, $g_2$, and $g_3$. Hence, if the running times of the simulators $S(\mathcal{L}_{E}^{\text{ph}})$, $S(\mathcal{L}_{S_1}^{\text{ph}})$ and $S(\mathcal{L}_{S_2}^{\text{ph}})$ used in $\mathcal{M}_{0,0}^\beta(w)$ are at most $T_{\text{adh}}$ and $\max\{nq_{U},q_{S}\} \leq q_{P}^N, q_{H}^N$ holds, then we have

$$|P(d_1,d_2) - P(d_1,d_2) - p_{0,0}(d_2)| \leq 4\epsilon_{ZK}$$

for $\beta = 1, 2$. This implies that

$$|P(d_1,d_2) - P(d_2,d_2) - p_{0,0}(d_2)| \leq |p_{0,0}(d_1) - p_{0,0}(d_2)| + 8\epsilon_{ZK}. \quad (5.1)$$

(I) We define the sequence of games $\{\text{Game}(0,v)\}_{v=1}^{\epsilon_{SS}}$. In $\text{Game}(0,v)$, we replace Step U1-3 of $\text{Game}(0,0)$ by the following step:

**U1-3':** If $C_U \leq v$, then choose $\hat{v}_\beta \in \hat{G}_q$ and $r_{\beta} \in \hat{Z}_q$, and compute $u_\beta = g^{r_\beta}$, $v_\beta = y_\beta^r h^p$ and $\hat{u}_\beta = (\hat{g})^{r_\beta}$. Otherwise, choose $r_{\beta} \in \hat{Z}_q$, and compute $u_\beta = g^{r_\beta}$, $v_\beta = y_\beta^r h^p$, $\hat{u}_\beta = (\hat{g})^{r_\beta}$ and $\hat{v}_\beta = (\hat{g})^{r_\beta}(\hat{h})^p$.

**Lemma 5.1** (cf. Claim 5 [4]). If $T \leq T_{\text{adh}} - 4T_S - q_U f_1^U - q_S f_1^S - f_1^I$ holds for some polynomials $f_1^U$, $f_1^S$ and $f_1^I$ in $n$, $t$ and $k$, then

$$|p_{1,0,0}(d_2) - p_{1,0,v-1,0}(d_2)| \leq q_{U}(2n\epsilon_{SS} + \epsilon_{\text{adh}} + \hat{o}_1)$$

follows for $\beta \in \{1, 2\}$, where $\hat{o}_1$ is negligible in $k$.

(II) We define the sequence of games $\{\text{Game}(1,v,\xi)\}_{v=0}^{\epsilon_{SS}}$, where $v = 0, \ldots, q_U - 1$ and $\xi = 0, \ldots, q_S$. In $\text{Game}(1,v,\xi)$, we replace Step S2-5 of $\text{Game}(1,0,0) = \text{Game}(0,0)$ by the following step:

**S2-5':** If either of the following conditions (1) and (2) hold, then choose $z_j \in \hat{G}_q$.

1. $u_\beta \in \{u_{\beta}(1), \ldots, u_{\beta}(\min\{C_U, v\})\}$.
2. $C_U \leq v$, and $u_\beta = u_{\beta}(v + 1)$.

Otherwise, compute $z_j = v_j/w_j$.

We note that $\text{Game}(1,v,0) = \text{Game}(1,v-1,q_S)$ holds.

**Lemma 5.2** (cf. Claim 6 [4]). If $T \leq T_{\text{adh}} - 4T_S - q_U f_1^U - q_S f_1^S - f_1^I$ holds for some polynomials $f_1^U$, $f_1^S$ and $f_1^I$ in $n$, $t$ and $k$, then

$$|p_{1,0,0}(d_2) - p_{1,v-1,q}(d_2)| \leq q_{U}(2n\epsilon_{SS} + \epsilon_{\text{adh}} + \hat{o}_2)$$

follows for $\beta \in \{1, 2\}$, where $\hat{o}_2$ is negligible in $k$.

(III) We define the sequence of games $\{\text{Game}(2,v)\}_{v=0}^{\epsilon_{SS}}$. In $\text{Game}(2,v)$, we replace Steps 14 and S2-4 of $\text{Game}(2,0) = \text{Game}(1,q_U - 1, q_S)$ by the following steps, respectively:

**14':** Choose $h, \tilde{g}, \tilde{h}, \tilde{g} \in \hat{G}_q$ and $r_{\delta}, r_{d_1}, d_{2, d} \in \hat{Z}_q$, and compute $\tilde{v} = (\hat{g})^r$.

**S2-4':** If $C_S \leq v$ and $(\tilde{v}_\beta/\tilde{u}_\beta) \neq \tilde{h}^p$, then choose $v_j \in \hat{G}_q$. Otherwise, compute $v_j = (v_{\beta}/v_\beta)^y$.

**Lemma 5.3** (cf. Claim 7 [4]). If $T \leq T_{\text{adh}} - 4T_S - q_U f_1^U - q_S f_1^S - f_1^I$ holds for some polynomials $f_1^U$, $f_1^S$ and $f_1^I$ in $n$, $t$ and $k$, then

$$|p_{2,0,0}(d_2) - p_{2,v,q}(d_2)| \leq q_{S}(\epsilon_{\text{adh}} + 2\epsilon_{SS} + \hat{o}_3)$$

follows for $\beta \in \{1, 2\}$, where $\hat{o}_3$ is negligible in $k$.

Using Lemmas 5.1-5.3, we have

$$|p_{0,0}(d_1) - p_{0,0}(d_2)| \leq 4(nq_{U}q_{S} + nq_{U} - q_{S}q_{S} + 2q_{U}(q_{S} + 1)\epsilon_{\text{adh}} + q_{U}\hat{o}_1 + (q_{U} - 1)q_{S}\hat{o}_2 + q_{S}\hat{o}_3 + |p_{2,q_{S}}(d_1) - P_{2,q_{S}}(d_2)|). \quad (5.2)$$

(IV) We define the two games $\text{Game}(3,1)$ and $\text{Game}(3,2)$. In $\text{Game}(3,1)$, we replace Step 13 and Output phase of $\text{Game}(3,0) = \text{Game}(2,q_{S})$ by the following steps, respectively:

**13':** Choose $x_2 \in \hat{Z}_q$ and $y_1 \in \hat{G}_q$, and compute $y_2 = g^{x_2}$, $\{x_1\}_{j=1}^{v_{SS}} = SS_{\tau_{SS}}(0)$ and $\{x_2\}_{j=1}^{v_{SS}} = SS_{\tau_{SS}}(x_2)$.

**Output phase:** If $F$ = false and $A$’s output equals 1, then set $\varphi = 1$. Otherwise, set $\varphi = 0$.

In $\text{Game}(3,2)$, we replace Output phase of $\text{Game}(3,1)$ by the following procedure:

**Output phase:** If $F$ = true, then set $\varphi = 1$. Otherwise, set $\varphi = 0$.

For each $M_{0,0,0}^\beta$, let $F_{\mu,v,d_2}$ denote the event that $F$ = true holds. We write $p_{\mu,v}^{\beta}(d_2) = Pr[E_{\mu,v,d_2} \land F_{\mu,v,d_2}]$ and $p_{\mu,v}^{\beta}(d_2) = p_{\mu,v}(d_2) - p_{\mu,v}^{\beta}(d_2)$. Then we have
\begin{equation}
|p_{3,0}(d_1) - p_{3,0}(d_2)| \leq |p^f_{3,0}(d_1) - p^f_{3,0}(d_2)| + |p^f_{3,0}(d_1) - p^f_{3,0}(d_2)| + \max[\Pr[F_{3,0,d_1}], \Pr[F_{3,0,d_2}]].
\end{equation}

**Lemma 5.4** (cf. Claim 8 [4]). One has
\[\Pr[F_{3,0,d_1}] - \Pr[F_{3,2,d_1}] \leq \tilde{\alpha}_4\]
and
\[|p^f_{3,0}(d_1) - p^f_{3,0}(d_2)| \leq \tilde{\alpha}_4' + |p_{3,1}^f(d_1) - p_{3,1}^f(d_2)|,
\]
where \(\tilde{\alpha}_4\) and \(\tilde{\alpha}_4'\) are negligible in \(k\).

(V) We define the two games \textbf{Game}(4, 1) and \textbf{Game}(4, 2). In \textbf{Game}(4, 1) and \textbf{Game}(4, 2), we replace Step I6 of \textbf{Game}(3, 1) and \textbf{Game}(3, 2) by the following step, respectively:

\textbf{I6’}: Choose \((u_{1,d}, v_{1,d}) \in \mathbb{G}_q, \text{ and compute } (u_{2,d}, v_{2,d}) = (g^{f_{2,d}}, y^{f_{2,d}}_{2,d}).\)

**Lemma 5.5** (cf. Claim 9 [4]). If \(T \leq T_{\text{adh}} - 4TS - q_{4}f^U_{6} - q_{4}f^S_{6} - f_{4}^1\) holds for some polynomials \(f^U_{6}, f^S_{6}\) and \(f^1_{4}\) in \(n, t \text{ and } k\), then
\[|p^f_{3,1}(d_1) - p^f_{3,1}(d_2)| < \varepsilon_{\text{adh}}\]
and
\[\Pr[F_{3,2,d_1}] - \Pr[F_{4,2,d_1}] < \varepsilon_{\text{adh}}\]
follow for \(\beta \in \{1, 2\} \).

As we employ the twin-encryption version of the ElGamal encryption, which has not been involved in PPSS, we also need to replace the “second term” \((u_{2,d}, v_{2,d})\) by random values of \(\mathbb{G}_q^2\). So, we define the following games \textbf{Game}(4, 3) and \textbf{Game}(4, 4). In \textbf{Game}(4, 3) and \textbf{Game}(4, 4), we replace Step I6’ of \textbf{Game}(4, 1) and \textbf{Game}(4, 2) by the following step, respectively:

\textbf{I6”}: Choose \((u_{1,d}, v_{1,d}, u_{2,d}, v_{2,d}) \in \mathbb{G}_q\).

**Lemma 5.6.** If \(T \leq T_{\text{adh}} - 4TS - q_{4}f^U_{6} - q_{4}f^S_{6} - f_{4}^1\) holds for some polynomials \(f^U_{6}, f^S_{6}\) and \(f^1_{4}\) in \(n, t \text{ and } k\), then
\[|p^f_{3,1}(d_1) - p^f_{3,1}(d_2)| < \varepsilon_{\text{adh}}\]
and
\[\Pr[F_{4,2,d_1}] - \Pr[F_{4,4,d_1}] < \varepsilon_{\text{adh}}\]
follow for \(\beta \in \{1, 2\} \).

Since the values \(v_{1,d}\) and \(v_{2,d}\) are uniformly chosen in Step I6’’ of \textbf{Game}(4, 3), \(A\)'s output does not depend on the choice of \(\beta\) in Step I2 of the game. Hence, we see that \(p^f_{3,1}(d_1) = p^f_{3,1}(d_2)\). Using Lemmas 5.4–5.6, we have
\begin{equation}
|p^f_{3,1}(d_1) - p^f_{3,1}(d_2)| \leq 4\varepsilon_{\text{adh}} + \tilde{\alpha}_4.
\end{equation}

(IV) We define the sequence of games \(\langle \textbf{Game}(5, v) \rangle_{v \in \mathbb{G}_q^*}.\) In \textbf{Game}(5, v), we replace Step S(j-2)-4’ of \textbf{Game}(5, 0) = \textbf{Game}(4, 4) by the following step:

\textbf{S(j-2)-4’}: If \(C_S \leq v\) or \((\tilde{v}_\beta, \tilde{u}_\beta) \neq \tilde{h}_\beta\), then choose \(v_j \in \mathbb{G}_q\). Otherwise, compute \(v_j = (v_{p/v_{p,j})^y}.\)

**Lemma 5.7** (cf. Claim 10 [4]). If \(T \leq T_{\text{adh}} - 4TS - q_{4}f^U_{6} - q_{4}f^S_{6} - f_{4}^1\) holds for some polynomials \(f^U_{6}, f^S_{6}\) and \(f^1_{4}\) in \(n, t \text{ and } k\), then
\[\Pr[F_{5,0,d_1}] - \Pr[F_{5,0,d_2}] \leq q_{5}(2\varepsilon_{\text{adh}} + 2\varepsilon_{SS} + \tilde{\alpha}_7)\]
follows for \(\beta \in \{1, 2\} \), where \(\tilde{\alpha}_7\) is negligible in \(k\).

(VII) We define the sequence of games \(\langle \textbf{Game}(6, v) \rangle_{v \in \mathbb{G}_q^*} \). In \textbf{Game}(6, v), we replace Step U1-3’ of \textbf{Game}(6, 0) = \textbf{Game}(5, v) by the following step:

\textbf{U1-3’}: If \(C_U \leq v\), then choose \(\tilde{v}_\beta, \tilde{u}_\beta \in \mathbb{G}_q\) and \(r_{p} \in \mathbb{G}_q\) and compute \(u_{\beta} = g^{r_{p}}_{\beta} \text{ and } \tilde{u}_\beta = (\tilde{g})^{r_{p}} \text{. Otherwise, choose } \tilde{v}_\beta \in \mathbb{G}_q \text{ and } r_{p} \in \mathbb{G}_q, \text{ and compute } u_{\beta} = g^{r_{p}}_{\beta}, \text{ and } \tilde{u}_\beta = (\tilde{g})^{r_{p}} \).

**Lemma 5.8** (cf. Claim 11 [4]). If \(T \leq T_{\text{adh}} - 4TS - q_{4}f^U_{6} - q_{4}f^S_{6} - f_{4}^1\) holds for some polynomials \(f^U_{6}, f^S_{6}\) and \(f^1_{4}\) in \(n, t \text{ and } k\), then
\[\Pr[F_{6,0,d_1}] - \Pr[F_{6,0,d_2}] \leq q_U(4\varepsilon_{\text{adh}} + 2\varepsilon_{SS} + \tilde{\alpha}_8)\]
follows for \(\beta \in \{1, 2\} \), where \(\tilde{\alpha}_8\) is negligible in \(k\).
6. Proof of Lemmas

In this section, we prove Lemmas 5.1–5.9.

6.1 Proof of Lemma 5.1

We construct an intermediary machine $\tilde{M}_0^\beta$. On input $w = (Q, g, g_1, g_2, g_3)$, $\tilde{M}_0^\beta$ simulates $M_{0,\nu}^\beta$ except for the following steps:

**I4:** Choose $h, \tilde{h} \in_r G_q$ and $r_0, r_1, r_2, d \in_r Z_q$ and $r_0, r_1 \in_r Z_q^*$. Then set $\tilde{g} = g^{\nu_0}$, $\tilde{g} = g_1^{\nu_1}$ and $\tilde{g} = g_2$.

**U1-3′:** If $C_U = v$, then set $u_0 = g_1^{1/\nu_0}$, $v_0 = g_1^{1/\nu_0} h^\nu$, $\hat{u}_0 = g_1$ and $\hat{v}_0 = g_3^{1/\nu_0} (\tilde{h})^\beta$. Otherwise, execute Step U1-3′ of $M_{0,\nu}^\beta$.

**U1-5:** If $C_U = v$, then set $q_i \leftarrow (\tilde{g})^{1/(\nu r_0)}$ for each $j \in [n]$. Otherwise, execute Step U1-5 of $M_{0,\nu}^\beta$.

Let $\tilde{\varphi}_{0,\nu}^\beta$ be the outputs of $\tilde{M}_0^\beta$. Noting that $\varphi_{0,\nu}^\beta$ is independent of $g_1, g_2$ and $g_3$, we have

\[
|p_{0,\nu-1}(d) - p_{0,\nu}(d)| = \Pr_{\nu} [\varphi_{0,\nu-1}^\beta = 1] - \Pr_{\nu} [\varphi_{0,\nu}^\beta = 1] \leq \Pr_{\nu} [\varphi_{0,\nu-1}^\beta = 1] - \Pr_{\nu} [\varphi_{0,\nu-1}^\beta = 1] + \Pr_{\nu} [\varphi_{0,\nu-1}^\beta = 1] - \Pr_{\nu} [\varphi_{0,\nu-1}^\beta = 1] + \Pr_{\nu} [\varphi_{0,\nu-1}^\beta = 1] - \Pr_{\nu} [\varphi_{0,\nu-1}^\beta = 1].
\] (6.1)

For any $0 \leq v \leq q_U$, the running time of $\tilde{M}_0^\beta$ is at most $T_1 = T + 4T_S + q_U f_1^{U} + q_S f_1^{S} + f_1^{I}$ for some polynomials $f_1^{U}$, $f_1^{S}$ and $f_1^{I}$ in $n, t$ and $k$. So, if $T_1 \leq T_{\text{ddh}}$, then the second term on the right-hand side of (6.1) is at most $\varepsilon_{\text{ddh}}$.

We now estimate the first and the last terms on the right-hand side of (6.1). Let $E_{S_1,0}^{\nu_1}$ denote the event such that $A$ enters the $v$-th User’s query phase with a query $((i, a_0, b_{\nu_0} a_{\nu_0} \pi_1), j_{\nu_1}) \in S_1^{\nu_1}$ which satisfies the following two conditions for some $j_0 \in [n]$:

(i) $(a_0, b_{\nu_0}, \tilde{a}_{\nu_0}) \notin L_1^{\nu_1}$, and (ii) $\pi_1, j_0$ is a valid proof. Then we have

\[
\Pr_{\nu} [\varphi_{0,\nu}^\beta = 1] - \Pr_{\nu} [\varphi_{0,\nu}^\beta = 1] \leq \Pr_{\nu} [\varphi_{0,\nu-1}^\beta = 1] - E_{S_1,0}^{\nu_1} - \Pr [\varphi_{0,\nu-1}^\beta = 1] - E_{S_1,0}^{\nu_1} + \Pr [\varphi_{0,\nu-1}^\beta = 1] - E_{S_1,0}^{\nu_1} - \Pr [\varphi_{0,\nu-1}^\beta = 1].
\] (6.2)
Since \((P(\Sigma_{51}^f), \mathcal{V}(\Sigma_{51}^f))\) is \((T_5, q_{0,0}, q_{0,0}^f, \epsilon_{\text{ZK}}, \epsilon_{\text{SS}})\)-SS-NIZK, if the running time of \(\delta(\Sigma_{51}^f)\) used in \(M_{0,0}^\beta\) and \(\tilde{M}_{0,0}^\beta\) is at most \(T_5\), and \(\max\{nq_{0,0}, q_{0,0}^f\} \leq q_{0,0}^f\) holds, then we have

\[
\Pr_{w \in \mathcal{DH}} [\varphi_{0,0}^f = 1 \land E_{SS}_{51,0}^\beta] - \Pr_{w \in \mathcal{DH}} [\varphi_{0,0}^f = 1 \land \neg E_{SS}_{51,0}^\beta] \leq 1 - (1 - \epsilon_{SS})^n \leq n \epsilon_{SS}.
\]

By the similar argument, we have

\[
\Pr_{w \in \mathcal{DH}} [\varphi_{0,v}^f = 1] - \Pr_{w \in \mathcal{DH}} [\varphi_{0,v}^f = 1] \leq n \epsilon_{SS} + \Pr_{w \in \mathcal{DH}} [\varphi_{0,v}^f = 1 \land \neg \neg E_{SS}_{51,0}^\beta] - \Pr_{w \in \mathcal{DH}} [\varphi_{0,v}^f = 1 \land \neg E_{SS}_{51,0}^\beta]. \tag{6.3}
\]

In order to estimate other terms, we assume that the event \(E_{SS}_{51,0}^\beta\) does not occur.

(A) We first consider the last term on the right-hand side of (6.2). Let \(w \in \mathcal{DH}\). In the \(v\)-th User’s query phase of \(M_{0,0}^\beta\), if we set \(r_p = \alpha_1 / r_0\), where \(g_1 = g^{\alpha_1}\), then one has \(u_p = g^{r_p} v_p = g^{r_p} \hat{h}^{e_p}, \tilde{u}_p = (\hat{y})^{r_p} \tilde{v}_p = (\hat{y})^{r_p} (\tilde{h})^{e_p}\), where these are the same as the values obtained in the \(v\)-th User’s query phase of \(M_{0,0}^\beta\) with \(r_p = \alpha_1 / r_0\). Therefore, the only differences between \(M_{0,0}^\beta\) and \(\tilde{M}_{0,0}^\beta\) are the choices of \(\tilde{g}, \tilde{g}, \tilde{\gamma}\) and \(\tilde{\gamma}\) in Step 14 and that of \(u_p\) in Step 11-3 of the \(v\)-th User’s query phase. We define the following distribution over \(\mathcal{G}_q^2\):

\[
\Delta_{0,v}^1 = \{(g_0^{r_0}, g_1^{r_1}, g_2, g_3^{1/r_0}) \mid r_0, r_1 \in \mathbb{Z}_q^*, g_1, g_2 \in \mathcal{G}_q\}.
\]

The distribution \(\Delta_{0,v}^1\) is identical to the distribution of \((\tilde{g}, \tilde{g}, \tilde{\gamma}, \tilde{u}_p)\) constructed in \(\tilde{M}_{0,0}^\beta\). In addition, the distribution of \((\tilde{g}, \tilde{g}, \tilde{\gamma}, \tilde{u}_p)\) constructed in \(M_{0,0}^\beta\) is uniform over \(\mathcal{G}_q^4\). Hence, the last term on the right-hand side of (6.2) is bounded by the statistical distance between \(\Delta_{0,v}^1\) and \(U_{\mathcal{G}_q^4}\).

We see that the following statements hold:

For any \(\tilde{g}, \tilde{g}, u_p \in \mathcal{G}_q\), one has

\[
\Pr_{g \in \Delta_{0,v}^1} [g = (1, \tilde{g}, \tilde{\gamma}, u_p)] = 0.
\]

For any \(\tilde{g}, \tilde{g}, u_p \in \mathcal{G}_q \setminus \{1\}\) and \(\gamma \in \mathcal{G}_q\), one has

\[
\Pr_{g \in \Delta_{0,v}^1} [g = (\tilde{g}, 1, \tilde{\gamma}, u_p)] = \Pr_{g \in \Delta_{0,v}^1} [g = (\tilde{g}, \tilde{g}, \tilde{\gamma}, 1)] = 0, \quad \Pr_{g \in \Delta_{0,v}^1} [g = (\tilde{g}, 1, \tilde{\gamma}, 1)] = \frac{1}{q^2(q - 1)}
\]

and

\[
\Pr_{g \in \Delta_{0,v}^1} [g = (\tilde{g}, \tilde{g}, \tilde{\gamma}, u_p)] = \frac{1}{q^2(q - 1)^2}.
\]

So the statistical distance between \(\Delta_{0,v}^1\) and \(U_{\mathcal{G}_q^4}\) is given by \(2(3q^2 - 4q + 2)/q^3\). This value is negligible in the security parameter \(k\).

(B) We next consider the last term on the right-hand side of (6.3). Let \(w \in \mathcal{DH}\). Using the similar argument to (A), we see that the differences between \(M_{0,0}^\beta\) and \(\tilde{M}_{0,0}^\beta\) are the choices of \(\tilde{g}, \tilde{g}, \tilde{\gamma}\) and \(\tilde{\gamma}\) in Step 14 and those of \(u_p\) and \(\tilde{v}_p\) in Step 11-3 of the \(v\)-th User’s query phase. We define the following distribution over \(\mathcal{G}_q^2\) by

\[
\Delta_{0,v}^2 = \{(g_0^{r_0}, g_1^{r_1}, g_2, g_3^{1/r_0}) \mid r_0, r_1 \in \mathbb{Z}_q^*, g_1, g_2, g_3 \in \mathcal{G}_q\}.
\]

The distribution \(\Delta_{0,v}^2\) is identical to that of \((\tilde{g}, \tilde{g}, \tilde{\gamma}, \tilde{v}_p, \tilde{\gamma})\) constructed in \(\tilde{M}_{0,0}^\beta\). In addition, the distribution of \((\tilde{g}, \tilde{g}, \tilde{\gamma}, \tilde{v}_p, \tilde{\gamma})\) constructed in \(M_{0,0}^\beta\) is identical to \(U_{\mathcal{G}_q^4}\). The last term on the right-hand side of (6.3) is bounded by the statistical distance between \(\Delta_{0,v}^2\) and \(U_{\mathcal{G}_q^4}\).

We note that for any fixed \(r_0 \in \mathbb{Z}_q^*, p \in \mathbb{Z}_q\) and \(\hat{h} \in \mathcal{G}_q\), the distribution \(\{g_3^{1/r_0} \hat{h}^{e_p} \mid g_3 \in \mathcal{G}_q\}\) over \(\mathcal{G}_q\) is uniform. This implies that the statistical distance between \(\Delta_{0,v}^2\) and \(U_{\mathcal{G}_q^4}\) is less than the distance between \(\Delta_{0,v}^1\) and \(U_{\mathcal{G}_q^4}\).

Consequently, we have

\[
|p_{0,v-1}(d_p) - p_{0,v}(d_p)| \leq 2n\epsilon_{SS} + \epsilon_{\text{dh}} + \omega_1,
\]

where \(\omega_1\) is negligible in \(k\), and hence

\[
|p_{0,v}(d_p) - p_{0,0}(d_p)| \leq q_0(2n\epsilon_{SS} + \epsilon_{\text{dh}} + \omega_1)
\]

follows.

Remark 6.1. In the proof of Lemma 5.1, the construction of the machine \(\tilde{M}_{0,0}^\beta\), the estimation of the second term on the right-hand side of (6.1) and that of the first term on the right-hand side of (6.2) are the same as those in the proof of Claim 5 in [4]. On the other hand, in [4], the second term on the right-hand side of (6.2) and that of (6.3) are regarded to be zero without precise estimation. However, one has to estimate these terms precisely since the statistical distance between \(\Delta_{0,v}^1\) and \(U_{\mathcal{G}_q^4}\) and that between \(\Delta_{0,v}^2\) and \(U_{\mathcal{G}_q^4}\) are not necessarily zero as analyzed in (A) and (B) of our proof. The same applies in other lemmas.
6.2 Proof of Lemma 5.2

We construct an intermediary machine \( \tilde{\mathcal{M}}_{1,v,\xi}^\beta \). On input \( w = (Q, g, g_1, g_2, g_3) \), \( \tilde{\mathcal{M}}_{1,v,\xi}^\beta \) simulates \( \mathcal{M}_{1,v,\xi}^\beta \) except for the following steps:

14: Choose \( h, \tilde{h} \in \mathbb{G}_q \), \( r_p, r_{1,d}, r_{2,d}, r_0, \tilde{r} \in \mathbb{Z}_q \) and \( r_1 \in \mathbb{Z}_q^* \). Then set \( \tilde{g} = g^\tilde{h} \), \( \tilde{g} = g_{1}^\tilde{h} \) and \( \tilde{y} = \tilde{g}^r \).

1U-3': If \( C_U = v \), then choose \( \tilde{v}_p, \tilde{v}_2 \in \mathbb{G}_q \), and set \( \tilde{u}_p = g_1, \tilde{v}_p = g_1^r h^p \) and \( \tilde{u}_p = g_1^p \). Otherwise, execute Step 1U-3' of \( \mathcal{M}_{1,v,\xi}^\beta \).

1U-5: If \( C_U = v \), then set \( \tilde{g}_j = (\tilde{a}_j)^{1/|n|} \) for each \( j \in [n] \). Otherwise, execute Step 1U-5 of \( \mathcal{M}_{1,v,\xi}^\beta \).

S2-6: If \( C_S = \xi, C_U \geq v + 1 \) and \( u_p = u_p(v + 1) \) hold, then set \( u_{i_j} = g_2 \) and \( v_{i_j} = g_2 z_j \). Otherwise, execute Step S2-6 of \( \mathcal{M}_{1,v,\xi}^\beta \).

In each \( \mathcal{M}_{1,v,\xi}^\beta \) and \( \tilde{\mathcal{M}}_{1,v,\xi}^\beta \), let \( T_{p,\tilde{p}}^{\beta} \) denote the event that \( C_U \geq v + 1 \) and \( u_p = u_p(v + 1) \) hold in the \( \xi \)-th Server’s query phase.

Let \( \varphi_{1,\nu,\xi}^\beta \) be the output of \( \tilde{\mathcal{M}}_{1,v,\xi}^\beta \). Noting that \( \varphi_{1,\nu,\xi}^\beta \) is independent of \( g_1, g_2 \) and \( g_3 \), we have

\[
\left| p_{1,\nu,\xi-1}(d_p) - p_{1,\nu,\xi}(d_p) \right| \\
\leq \left| \Pr_{w \in \mathbb{DH}} [\varphi_{1,\nu,\xi-1}^\beta = 1] - \Pr_{w \in \mathbb{DH}} [\varphi_{1,\nu,\xi}^\beta = 1] \right| + \left| \Pr_{w \in \mathbb{DH}} [\varphi_{1,\nu,\xi}^\beta = 1] - \Pr_{w \in \mathbb{DH}} [\varphi_{1,\nu,\xi}^\beta = 1] \right|.
\]

We estimate the first and the last terms on the right-hand side of (6.4). Let \( \mathcal{E}_{SS}^{S_{T_1},d} \) denote the event defined as in the proof of the Lemma 5.1. If the running time of \( \mathcal{M}_{1,v,\xi-1} \) used in \( \mathcal{M}_{1,v,\xi}^\beta \) and \( \tilde{\mathcal{M}}_{1,v,\xi}^\beta \) is at most \( T_5 \) and \( \max\{nq_U, q_3\} \leq q'_1, q'_2 \) holds, then we have

\[
\left| \Pr_{w \in \mathbb{DH}} [\varphi_{1,\nu,\xi}^\beta = 1] - \Pr_{w \in \mathbb{DH}} [\varphi_{1,\nu,\xi}^\beta = 1] \right| \\
\leq 2n_{SS} + \left| \Pr_{w \in \mathbb{DH}} [\varphi_{1,\nu,\xi-1}^\beta = 1 \land \neg \mathcal{E}_{SS}^{S_{T_1},d}] - \Pr_{w \in \mathbb{DH}} [\varphi_{1,\nu,\xi}^\beta = 1 \land \neg \mathcal{E}_{SS}^{S_{T_1},d}] \right|.
\]

In order to estimate other terms, we assume that the event \( \mathcal{E}_{SS}^{S_{T_1},d} \) does not occur.

(A) We first consider the second term on the right-hand side of (6.5). Let \( w \in \mathbb{DH} \) in the \( v \)-th User’s query phase of \( \mathcal{M}_{1,v,\xi}^\beta \). If \( w_{i_j} = \alpha_1 \), where \( g_1 = g^\alpha_1 \), then one has \( u_0, v_p \neq \alpha \), \( u_{i_j} = g_2 \), \( v_{i_j} = g_2 z_j \); these values are the same as those obtained in the \( \xi \)-th Server’s query phase of \( \mathcal{M}_{1,v,\xi-1}^\beta \). We consider the \( \xi \)-th Server’s query phase of \( \mathcal{M}_{1,v,\xi}^\beta \):

- Assume that the event \( U_{p,\tilde{p}}^{\beta,\xi} \) occurs. If we set \( r_0 = \alpha_2 \), where \( g_2 = g^\alpha_2 \), then one has \( u_{i_j} = g_2 \) and \( v_{i_j} = u_p z_j \); these values are the same as those obtained in the \( \xi \)-th Server’s query phase of \( \mathcal{M}_{1,v,\xi}^\beta \) with \( r_0 = \alpha_2 \). In particular, \( g_2 \) is randomly chosen, and independent of the choices of \( \tilde{g}, \tilde{g}, \tilde{y} \) and \( u_{i_j} \).
- If the event \( U_{p,\tilde{p}}^{\beta,\xi} \) does not occur, then the \( \xi \)-th Server’s query phase of \( \mathcal{M}_{1,v,\xi}^\beta \) is the same as that of \( \mathcal{M}_{1,v,\xi-1}^\beta \). Hence, the differences between \( \mathcal{M}_{1,v,\xi-1}^\beta \) and \( \mathcal{M}_{1,v,\xi}^\beta \) are the choices of \( \tilde{g}, \tilde{g}, \tilde{y} \) and \( u_p \) in Step 14 and that of \( u_{i_j} \) in Step 1U-3'.

The distribution

\[
\Delta_{1,\nu,\xi}^\beta = \{(g_0^\alpha, g_{1}^\alpha, g_{2}^{\alpha,\xi}) : r_0, \tilde{r} \in \mathbb{Z}_q, r_1 \in \mathbb{Z}_q^* \},
\]

over \( \mathbb{G}_q^\alpha \) is identical to the distribution of \( (\tilde{g}, \tilde{g}, \tilde{y}, u_p) \) constructed in \( \tilde{\mathcal{M}}_{1,v,\xi}^\beta(w) \). In addition, the distribution of \( (\tilde{g}, \tilde{g}, \tilde{y}, u_p) \) constructed in \( \tilde{\mathcal{M}}_{1,v,\xi-1}^\beta(w) \) is uniform over \( \mathbb{G}_q^\alpha \). The second term on the right-hand side of (6.5) is bounded by the statistical distance between \( \Delta_{1,\nu,\xi}^\beta \) and \( U_{\mathbb{G}_q^\alpha}^\beta \). We define the following two distributions over \( \mathbb{G}_q^\alpha \):

\[
\tilde{\Delta}_{1,\nu,\xi}^\beta = \{(g_0^\alpha, g_{1}^\alpha) : r_0, \tilde{r} \in \mathbb{Z}_q\}
\]

and

\[
\tilde{\Delta}_{1,\nu,\xi}^\beta = \{(g_{1}^\alpha, g_{1}) : r_1 \in \mathbb{Z}_q^* \},
\]

for any \( \tilde{g}, \tilde{g}, \tilde{y}, u_p, u_{i_j} \in \mathbb{G}_q \backslash \{1\} \), we have

\[
\Pr_{g \in \tilde{\Delta}_{1,\nu,\xi}^\beta} [g = (1, \tilde{y})] = 0, \quad \Pr_{g \in \tilde{\Delta}_{1,\nu,\xi}^\beta} [g = (1, 1)] = \Pr_{g \in \Delta_{1,\nu,\xi}^\beta} [g = (1, 1)] = \frac{1}{q}.
\]
\[
\Pr_{g \in \Delta_{1,\nu}^\dagger} [g = (\bar{g}, 1)] = \Pr_{g \in \Delta_{1,\nu}^\dagger} [g = (\bar{g}, \bar{y})] = \frac{1}{q^2}, \quad \Pr_{g \in \Delta_{1,\nu}^\dagger} [g = (\bar{g}, u_p)] = \frac{1}{q(q-1)}
\]

and
\[
\Pr_{g \in \Delta_{1,\nu}^\dagger} [g = (1, u_p)] = \Pr_{g \in \Delta_{1,\nu}^\dagger} [g = (\bar{g}, 1)] = 0.
\]

Since \(\Delta_{1,\nu}^\dagger\) and \(\Delta_{1,\nu}^\ddagger\) are independent, the statistical distance between \(\Delta_{1,\nu}^\dagger\) and \(U_{G_q^\ddagger}\) is at most the sum of the distance between \(\Delta_{1,\nu}^\dagger\) and \(U_{G_q}\) and that between \(\Delta_{1,\nu}^\ddagger\) and \(U_{G_q}\). Hence, the statistical distance between \(\Delta_{1,\nu}^\dagger\) and \(U_{G_q^\ddagger}\) is at most \(6(q-1)/q^2\), which is negligible in \(k\).

**B** We next consider the last term on the right-hand side of (6.5). Let \(w \in \overline{D\bar{H}}\). We have
\[
\begin{aligned}
&\left| \Pr_{w \in \overline{D\bar{H}}} [\varphi_{1,\nu}^{\dagger} = 1 \land \neg E_{31,\nu}^{SS}] - \Pr_{w \in \overline{D\bar{H}}} [\varphi_{1,\nu}^{\ddagger} = 1 \land \neg E_{31,\nu}^{SS}] \right| \\
&\leq \left| \Pr_{w \in \overline{D\bar{H}}} [\varphi_{1,\nu}^{\dagger} = 1 \land \neg E_{31,\nu}^{SS} \land U_p^{\nu\ddagger}] - \Pr_{w \in \overline{D\bar{H}}} [\varphi_{1,\nu}^{\ddagger} = 1 \land \neg E_{31,\nu}^{SS} \land U_p^{\nu\ddagger}] \right| \\
&+ \left| \Pr_{w \in \overline{D\bar{H}}} [\varphi_{1,\nu}^{\dagger} = 1 \land \neg E_{31,\nu}^{SS} \land \neg U_p^{\nu\ddagger}] - \Pr_{w \in \overline{D\bar{H}}} [\varphi_{1,\nu}^{\ddagger} = 1 \land \neg E_{31,\nu}^{SS} \land \neg U_p^{\nu\ddagger}] \right|.
\end{aligned}
\] (6.6)

**B-1** In order to estimate the last term on the last-hand side of (6.5), we assume that the event \(U_p^{\nu\ddagger}\) does not occur. Then, by the similar argument to (A), the differences between \(\overline{\Delta}_{1,\nu}^\dagger\) and \(\overline{\Delta}_{1,\nu}^\ddagger\) are the choices of \(\tilde{g}, \tilde{g}\) and \(\bar{y}\) in Step 14, and that of \(u_p\) in Step 14 of the \(\nu\)-th User’s query phase. Hence, the last term on the right-hand side of (6.6) is at most the statistical distance between \(\overline{\Delta}_{1,\nu}^\dagger\) and \(U_{G_q^\ddagger}\) and is negligible in \(k\).

**B-2** In order to estimate the first term on the right-hand side of (6.6), we assume that the event \(U_p^{\nu\ddagger}\) occurs. The differences between \(\Delta_{1,\nu}^\dagger\) and \(\Delta_{1,\nu}^\ddagger\) are the choices of \(\tilde{g}, \tilde{g}\) and \(\bar{y}\) in Step 14, that of \(u_p\) in Step 14 of the \(\nu\)-th User’s query phase and those of \(z_j, u_q, v_q\) in Step 14 of the \(\xi\)-th Server’s query phase. Let \(Z\) be the distribution of \(z_j \in G_q^\ddagger\) computed in the \(\xi\)-th Server’s query phase of \(\Delta_{1,\nu}^\ddagger\). The distribution \(Z\) depends on \(g^n, g^1, g^2, g^3\) and \(g_1\), and is independent of \(g_2\) and \(g_3\).

The distribution
\[
\Delta_{1,\nu}^\ddagger = \{(g^n, g^1, g^{\nu\ddagger}, g_1, g_2, g_3 z_j) \mid r_0, \tilde{g} \in Z_q, r_1 \in Z_q, Z_q^\ddagger, g_1, g_2, g_3 \in G_q, z_j \in Z\}
\]
is identical to the distribution of \((\bar{g}, \bar{g}, \bar{y}, u_p, u_q, v_q)\) constructed in \(\Delta_{1,\nu}^\ddagger(w)\). Let \(m' = (m_1, m_2, m_3, m_4) \in G_q^3, m'' = (m_5, m_6) \in G_q^2\) and \(m = (m', m'')\). Then we have
\[
\Pr_{g \in \Delta_{1,\nu}^\ddagger} [g = m] = \Pr_{g \in \Delta_{1,\nu}^\dagger} [g'' = m'' \mid g' = m'] \Pr_{g \in \Delta_{1,\nu}^\dagger} [g' = m'],
\]
where we have set \(g = (g', g'')\). We note that
\[
\Pr_{g \in \Delta_{1,\nu}^\dagger} [g' = m'] = \Pr_{g \in \Delta_{1,\nu}^\dagger} [g' = m'].
\]
It follows that
\[
\Pr_{g \in \Delta_{1,\nu}^\dagger} [g'' = m'' \mid g' = m'] = \Pr_{g \in \Delta_{1,\nu}^\dagger} [g_3 z_j = m_6 \mid (g', g_2) = (m', m_5)] \Pr_{g \in \Delta_{1,\nu}^\dagger} [g_2 = m_5 \mid g' = m']
\]
\[
= \frac{1}{q} \sum_{m_6 \in G_q^2} \Pr_{g \in \Delta_{1,\nu}^\dagger} [z_j = m_6 m_0^{-1} \mid (g', g_2, g_3) = (m', m_5, m_6)] \Pr_{g \in \Delta_{1,\nu}^\dagger} [g_3 = m_0 \mid (g', g_2) = (m', m_5)]
\]
\[
= \frac{1}{q^2} \sum_{m_6 \in G_q^2} \Pr_{g \in \Delta_{1,\nu}^\dagger} [z_j = m_6 m_0^{-1} \mid (g', g_2, g_3) = (m', m_5, m_6)].
\]

Since \(m_0 m_0^{-1} \mid m_0 \in G_q^2\) for any \(m_6 \in G_q^2\), we have
\[
\Pr_{g \in \Delta_{1,\nu}^\dagger} [g'' = m'' \mid g' = m'] = \frac{1}{q^2}.
\]

The distribution
\[
\Delta_{1,\nu}^3 = \{(\bar{g}, \bar{g}, \bar{y}, g^{\nu\ddagger}, g^{\nu\ddagger}, g^{\nu\ddagger} z_j) \mid r_0, r_\tilde{g} \in Z_q, \tilde{g}, \tilde{g}, \bar{y}, z_j \in G_q\}
\]
is identical to that constructed in \(\Delta_{1,\nu}^\ddagger(w)\), and is uniform over \(G_q^6\). Since the first term on the right-hand side of (6.6) is bounded by the statistical distance between \(\Delta_{1,\nu}^\dagger\) and \(\Delta_{1,\nu}^3\), we have
where the last equation follows from the argument in (A). This value is negligible in $k$.

Note that, for any $0 \leq v \leq q_U - 1$ and $0 \leq \xi \leq \xi_S$, the running time of $\tilde{M}_{\eta,v}^\beta$ is at most $T_2 = T + 4T_S + q_U f_\xi^\beta + q_S f_\xi^\beta + f_\xi^1$ for some polynomials $f_\xi^1$, $f_\xi^2$, and $f_\xi^3$ in $n$, $t$, and $k$. So, if $T_2 \leq T_{\text{dbh}}$, then the second term on the right-hand side of (6.4) is at most $\varepsilon_{\text{dbh}}$. Consequently, we have

$$|p_{1,0,0}(d_{\beta}) - p_{1,q_{U} - 1,q_{U}}(d_{\beta})| \leq (q_U - 1)q_S(2n\varepsilon_{SS} + \varepsilon_{\text{dbh}} + \widetilde{\alpha}_2),$$

where $\widetilde{\alpha}_2$ is negligible in $k$.

### 6.3 Proof of Lemma 5.3

We construct an intermediary probabilistic machine $\tilde{M}_{\eta,v}^\beta$. On input $w = (Q, g, g_1, g_2, g_3)$, $\tilde{M}_{\eta,v}^\beta$ simulates $M_{\eta,v}^\beta$ except for the following steps:

14': Choose $g \in \sub{Z}_q$, $\tilde{x}, r_p, r_1,a_t,r_2,a_t',r_1 \in \sub{Z}_q$ and $v_0 \in \sub{Z}_{q_0}$, and set $h = g_2, \tilde{h} = g_3, \tilde{g} = \tilde{g}^\beta$ and $\tilde{g}^q = \tilde{g}$. \hspace{1cm} $S_{\eta,1-2}$: if $C_\eta = v$, then set $d_j = g_1, b_j = g_1^\beta$ and $\hat{d}_j = \hat{g}$. Otherwise, execute Step $S_{\eta,1-2}$ of $M_{\eta,v}^\beta$.

$S_{\eta,2-4'}$: if $C_\eta = \hat{v}$, then set

$$v_j = g_j \left( \frac{b_j}{e_j} \right)^{v_j - 1}.$$ 

Otherwise, execute Step $S_{\eta,2-4'}$ of $M_{\eta,v}^\beta$.

Noting that $\hat{\varphi}_{\eta,v}^\beta$ is independent of $g_1, g_2$ and $g_3$, we have

$$|p_{2,v-1}(d_{\beta}) - p_{2,v}(d_{\beta})| \leq \left| \Pr_{w \in \text{DH}} \left[ \hat{\varphi}_{\eta,v-1}^\beta = 1 \right] - \Pr_{w \in \text{DH}} \left[ \hat{\varphi}_{\eta,v}^\beta = 1 \right] + \right. \Pr_{w \in \text{DH}} \left[ \hat{\varphi}_{\eta,v}^\beta = 1 \right] - \Pr_{w \in \text{DH}} \left[ \hat{\varphi}_{\eta,v}^\beta = 1 \right] \right|$$

$$+ \Pr_{w \in \text{DH}} \left[ \hat{\varphi}_{\eta,v}^\beta = 1 \right] - \Pr_{w \in \text{DH}} \left[ \hat{\varphi}_{\eta,v}^\beta = 1 \right]. \quad (6.7)$$

We estimate the first and the last terms on the right-hand side of (6.7). Let $E_{SS}^{U_{\hat{v}_j}}$ denote the event such that $A$ enters the $v$-th Server’s query phase with a query $(V, u, e_j, u_p, v_j, u_\beta, \bar{u}_\beta, \tau_2, j)$ which satisfies the following two conditions: (i) $\pi_{2,j}$ is a valid proof, and (ii) $(a_j, e_j, u_p, v_j, u_\beta, \bar{u}_\beta, \tau_2, j) \notin U_{\hat{v}_j}$. Since $(\mathcal{P}(\hat{v}_j, (V, U_{\hat{v}_j})))$ is $(T_5, q_{\hat{v}_j}, \hat{q}_{\hat{v}_j}, \hat{q}_{\hat{2}}, \xi_{SS})$-SS-NIZK, if the running time of $\mathcal{P}(U_{\hat{v}_j})$ used in $M_{\eta,v-1}, \tilde{M}_{\eta,v}^\beta$ and $M_{\eta,v}^\beta$ is at most $T_5$, and $\max \{nu, q_S \} \leq \hat{q}_{\hat{v}_j}, \hat{q}_{\hat{2}}$ holds, then we have

$$\left| \Pr_{w \in \text{DH}} \left[ \hat{\varphi}_{\eta,v-1}^\beta = 1 \right] - \Pr_{w \in \text{DH}} \left[ \hat{\varphi}_{\eta,v}^\beta = 1 \right] + \Pr_{w \in \text{DH}} \left[ \hat{\varphi}_{\eta,v}^\beta = 1 \right] - \Pr_{w \in \text{DH}} \left[ \hat{\varphi}_{\eta,v}^\beta = 1 \right] \right|$$

$$\leq 2\varepsilon_{SS} + \left| \Pr_{w \in \text{DH}} \left[ \hat{\varphi}_{\eta,v-1}^\beta = 1 \right] - \Pr_{w \in \text{DH}} \left[ \hat{\varphi}_{\eta,v}^\beta = 1 \right] \right|$$

$$+ \Pr_{w \in \text{DH}} \left[ \hat{\varphi}_{\eta,v}^\beta = 1 \right] - \Pr_{w \in \text{DH}} \left[ \hat{\varphi}_{\eta,v}^\beta = 1 \right]. \quad (6.8)$$

In order to estimate other terms, we assume that the event $E_{SS}^{U_{\hat{v}_j}}$ does not occur.

(A) We first consider the second term on the right-hand side of (6.8). Let $w \in \text{DH}$. In the $v$-th Server’s query phase of $M_{\eta,v}^\beta$, if we set $t_j = \alpha_1$, where $g_1 = g^\alpha$, then one has $d_j = g^\alpha, b_j = u_\beta^\alpha, a_j = (\tilde{g})^\beta$ and $v_j = (u_\beta/v_\beta)^{\hat{v}}$: these values are the same as the values obtained in the $v$-th Server’s query phase of $M_{\eta,v-1}^\beta$ with $t_j = \alpha_1$. Hence, the differences between $M_{\eta,v-1}^\beta$ and $M_{\eta,v}^\beta$ is the choices of $h, \tilde{h}, \tilde{g}$ and $\tilde{g}$ in Step 14' and that of $a_j$ in Step $S_{\eta,1-2}$ of the $v$-th Server’s query phase. We define the distribution $\Delta_{\eta,v}^1$ over $\sub{Z}_q$ by

$$\Delta_{\eta,v}^1 = \{(g^\alpha, g^\alpha v_\beta, \tilde{g}^\beta, g^\alpha) \mid r_1, \alpha_1, \alpha_2 \in \sub{Z}_q, \ r_0 \in \sub{Z}_q \}.$$ 

The distribution $\Delta_{\eta,v}^1$ is identical to the distribution of $(h, \tilde{h}, \tilde{g}, a_j)$ constructed in $\tilde{M}_{\eta,v}^\beta(w)$. In addition, the distribution of $(h, \tilde{h}, \tilde{g}, a_j)$ constructed in $M_{\eta,v-1}^\beta(w)$ is identical to $U_{\sub{Z}_q}$. The second term on the right-hand side of (6.8) is bounded by the statistical distance between $\Delta_{\eta,v}^1$ and $U_{\sub{Z}_q}$. Since the distribution $\{(g^\alpha, r_1, r_2) \mid r_1, r_2 \in \sub{Z}_q \}$ is uniform, the statistical distance between $\Delta_{\eta,v}^1$ and $U_{\sub{Z}_q}$ is at most the distance between the distribution...
over $G_q^1$ and $U_{G_q^1}$. For any $h, h, a_j \in G_q \setminus \{1\}$, we have

$$\Pr_{g \in \Delta^1_{u,v}} [g = (h, h, a_j)] = \Pr_{g \in \Delta^1_{u,v}} [g = (h, h, 1)] = \Pr_{g \in \Delta^1_{u,v}} [g = (h, 1, a_j)] = 0,$$

and

$$\Pr_{g \in \Delta^1_{u,v}} [g = (h, 1, 1)] = \frac{1}{q^2(q-1)}.$$

Hence, the statistical distance between $\Delta^1_{u,v}$ and $U_{G_q^1}$ is at most $2(3q^2 - 5q + 2)/q^2$, which is negligible in $k$.

(B) We next consider the last term on the right-hand side of (6.8). Let $w \in DH$. We have

$$\Pr_{w \in DH} [\tilde{\psi}^\beta_{u,v} = 1 \land \neg E^{SS}_{U,v} \land I_v] - \Pr_{w \in DH} [\tilde{\psi}^\beta_{u,v} = 1 \land \neg E^{SS}_{U,v} \land I_v]$$

$$\leq \Pr_{w \in DH} [\tilde{\psi}^\beta_{u,v} = 1 \land \neg E^{SS}_{U,v} \land I_v] - \Pr_{w \in DH} \left[ \tilde{\psi}^\beta_{u,v} = 1 \land \neg E^{SS}_{U,v} \land \neg I_v \right] \bigg|_{\neg I_v}.$$

(B-1) In order to estimate the first term on the right-hand side of (6.9), we assume that the event $I_v$ occurs. In the $v$-th Server’s query phase of $M^0_{2,v}$, if we set $t_j = \alpha_1$, where $g_1 = g^{\alpha_1}$, then one has $a_j = g^e, b_j = u_p, \tilde{v}_p, v_j = (g^e)^{\beta}$ and

$$v_j = \frac{b_j}{e_j} = \frac{u_p g^{\beta}}{u_p^e g^{\beta}} = \left(\frac{v_p}{v_p}\right)^{\beta}.$$

This shows that these values are the same as the values obtained in the $v$-th Server’s query phase of $M^0_{2,v}$ with $t_j = \alpha_1$. Hence, the differences between $M^0_{2,v}$ and $M^0_{2,v}$ are the choices of $h, \tilde{h}$ and $\tilde{g}$ in Step 14 and that of $a_j$ in Step 5.2.2 of the $v$-th Server’s query phase. The distribution

$$\Delta^2_{u,v} = \{(g_2, g_3, g_4, g_5, g_6) \mid r_0 \in Z_q^*, r_1 \in Z_q^*, g_1, g_2, g_5 \in G_q^1\}$$

over $G_q^1$ is identical to the distribution of $(h, \tilde{h}, g, a_j)$ constructed in $M^0_{2,v}(w)$, and is uniform. Since the distribution of $(h, \tilde{h}, g, a_j)$ constructed in $M^0_{2,v}(w)$ is also uniform over $G_q^1$, we have

$$\Pr_{w \in DH} [\tilde{\psi}^\beta_{u,v} = 1 \land \neg E^{SS}_{U,v} \land I_v] = \Pr_{w \in DH} [\tilde{\psi}^\beta_{u,v} = 1 \land \neg E^{SS}_{U,v} \land \neg I_v].$$

(B-2) In order to estimate the last term on the right-hand side of (6.9), we assume that the event $I_v$ does not occur and that $A$ enters the $v$-th Server’s query phase with a query $(V, u, e_j, u_p, v_p, \tilde{v}_p, \tilde{w}_p, \pi_{2,v})$. The differences between $M^0_{2,v}$ and $M^0_{2,v}$ are the choices of $h, \tilde{h}$ and $\tilde{g}$ in Step 14 and, those of $a_j$ and $v_j$ in the $v$-th Server’s query phase.

We set $\delta_1 = x_1(r_p - r_q)$ and $\delta_2 = p - \tilde{p}$, where $u_p = \tilde{g}^{\beta}$ and $\tilde{v}_p(\tilde{w}_p)^{\beta} = \tilde{h}^{\beta}$. Then the value $v_j$ computed in the $v$-th Server’s query phase of $M^0_{2,v}(w)$ is equal to $g_1^{\delta_1} g_2^{\delta_2}$. Let $D_1$ and $D_2$ be the distributions of $\delta_1 \in Z_q^*$ and $\delta_2 \in Z_q^*$, respectively. The distributions $D_1$ and $D_2$ depend on $h, \tilde{h}, \tilde{g}$ and $a_j$.

The distribution

$$\Delta^2_{u,v} = \{(g_2, g_3, g_4, g_5, g_6) \mid r_0 \in Z_q^*, r_1 \in Z_q^*, g_1, g_2, g_5 \in G_q^1\}$$

is identical to the distribution of $(h, \tilde{h}, g, a_j, v_j)$ constructed in $M^0_{2,v}(w)$, and the distribution of $(h, \tilde{h}, g, a_j, v_j)$ constructed in $M^0_{2,v}(w)$ is uniform over $G_q^1$. The last term on the right-hand side of (6.9) is bounded by the statistical distance between $\Delta^2_{u,v}$ and $U_{G_q^1}$. We note that $\delta_2 \neq 0$ holds if the event $I_v$ does not occur. Hence, we have

$$\left| \Pr_{w \in DH} [\tilde{\psi}^\beta_{u,v} = 1 \land \neg E^{SS}_{U,v} \land I_v] - \Pr_{w \in DH} [\tilde{\psi}^\beta_{u,v} = 1 \land \neg E^{SS}_{U,v} \land \neg I_v] \right| \leq \sum_{m \in G_q^1} \left| \Pr_{g \in \Delta^2_{u,v}} [g = m \land \delta_2 \neq 0] - \Pr_{g \in U_{G_q^1}} [g = m \land \delta_2 \neq 0] \right|.$$
We write \( m = (m_1, m_2, m_3, m_4, m_5) = (m', m_5) \in \mathbb{Z}_q^5 \) and \( g = (g', g_5) \). For any \( m \in \mathbb{Z}_q^5 \), we have

\[
\Pr_{g \in U_{\mathbb{Z}_q^5}} [g = m \land \delta_2 \neq 0] = \frac{1}{q^5} \Pr_{g \in U_{\mathbb{Z}_q^5}} [g = m \land \delta_2 \neq 0 | g' = m']
\]

\[
= \frac{1}{q^4} \Pr_{g \in U_{\mathbb{Z}_q^5}} [g_5 = m_5 | \delta_2 \neq 0 \land g' = m'] \Pr_{g \in U_{\mathbb{Z}_q^5}} [\delta_2 \neq 0 | g' = m']
\]

\[
= \frac{1}{q^2} \Pr_{g \in U_{\mathbb{Z}_q^5}} [\delta_2 \neq 0 | g' = m'].
\]

Since the value \( \delta_2 \) depends on \( m' \), we have

\[
\Pr_{g \in U_{\mathbb{Z}_q^5}} [\delta_2 \neq 0 | g' = m'] = \Pr_{g \in U_{\mathbb{Z}_q^5}} [\delta_2 \neq 0 | g' = m'].
\]

We denote this value by \( D(m') \).

(i) When \( m_2 = m_4 = m_5 = 1 \), we have

\[
\Pr_{g \in U_{\mathbb{Z}_q^5}} [g = m \land \delta_2 \neq 0] = \frac{1}{q^4} \Pr_{g \in U_{\mathbb{Z}_q^5}} [g_5 = m_5 | \delta_2 \neq 0 \land g' = m'] D(m') = \frac{D(m')}{q^4}.
\]

(ii) When \( m_2 = m_4 = 1 \) and \( m_5 \neq 1 \), we have

\[
\Pr_{g \in U_{\mathbb{Z}_q^5}} [g = m \land \delta_2 \neq 0] = \frac{1}{q^4} \Pr_{g \in U_{\mathbb{Z}_q^5}} [g_5 = m_5 | \delta_2 \neq 0 \land g' = m'] D(m') = 0.
\]

(iii) When \( m_2 \neq 1 \) and \( m_4 = 1 \), we have

\[
\Pr_{g \in U_{\mathbb{Z}_q^5}} [g = m \land \delta_2 \neq 0] = \frac{1}{q^4} \Pr_{g \in U_{\mathbb{Z}_q^5}} [g_5^t = m_5 | \delta_2 \neq 0 \land g' = m'] D(m')
\]

\[
= \frac{1}{q^4} \sum_{t \neq 0} \Pr_{g \in U_{\mathbb{Z}_q^5}} [g_5^t = m_5 | \delta_2 = t_2 \land \delta_2 \neq 0 \land g' = m'] D(m')
\]

\[
= \frac{1}{q^4} \sum_{t \neq 0} \Pr_{g \in U_{\mathbb{Z}_q^5}} [g_5^t = m_5 | \delta_2 = t_2 \land \delta_2 \neq 0 \land g' = m'] \Pr_{g \in U_{\mathbb{Z}_q^5}} [\delta_2 = t_2 | \delta_2 \neq 0 \land g' = m'] D(m')
\]

\[
= \begin{cases} 
 0 & \text{if } m_5 = 1, \\
 \frac{D(m')}{q^4(q-1)} & \text{otherwise.}
\end{cases}
\]

(iv) When \( m_2 = 1 \) and \( m_4 \neq 1 \), we have

\[
\Pr_{g \in U_{\mathbb{Z}_q^5}} [g = m \land \delta_2 \neq 0] = \frac{1}{q^4} \Pr_{g \in U_{\mathbb{Z}_q^5}} [m_4^t = m_5 | \delta_2 \neq 0 \land g' = m'] D(m').
\]

Since, for fixed \( m_4 \neq 1 \), the function \( \mathbb{Z}_q \ni \delta_1 \mapsto m_4^t \in \mathbb{Z}_q \) is bijective, we have

\[
\frac{1}{q^4} \sum_{m_4 \in \mathbb{Z}_q} \Pr_{g \in U_{\mathbb{Z}_q^5}} [m_4^t = m_5 | \delta_2 \neq 0 \land g' = m'] D(m') = \frac{D(m')}{q^4}.
\]

(v) When \( m_2 \neq 1 \) and \( m_4 \neq 1 \), we have

\[
\Pr_{g \in U_{\mathbb{Z}_q^5}} [g = m \land \delta_2 \neq 0]
\]

\[
= \frac{1}{q^4} \sum_{\tau \neq 0, \delta \neq 0} \Pr_{g \in U_{\mathbb{Z}_q^5}} [m_4^\tau g_5^\delta = m_5 | \delta = \tau \land \delta_2 \neq 0 \land g' = m'] \Pr_{g \in U_{\mathbb{Z}_q^5}} [\delta = \tau \land \delta_2 \neq 0 \land g' = m'] D(m'),
\]

where \( \delta = (\delta_1, \delta_2) \) and \( \tau = (\tau_1, \tau_2) \). By the similar arguments to (iii) and (iv), we have

\[
\Pr_{g \in U_{\mathbb{Z}_q^5}} [m_4^\tau g_5^\delta = m_5 | \delta = \tau \land \delta_2 \neq 0 \land g' = m'] = \begin{cases} 
 0 & \text{if } m_4^\tau = m_5 \\
 \frac{1}{q-1} & \text{otherwise,}
\end{cases}
\]
and we see that
\[
\sum_{g \in \mathcal{G}_{\alpha}^t} \left( \Pr [g = m \land \delta_2 \neq 0] - \Pr [g = m \land \delta_2 \neq 0] \right) = \frac{D(m')}{q^2} \sum_{\tau_i \in \mathcal{I}_{\alpha}^t} \frac{1}{q - 1} \Pr [\delta_1 = \tau_1 \land \delta_2 \neq 0 \land g' = m'] - \frac{1}{q}.
\]

Since \(D(m') \leq 1\), we obtain
\[
\sum_{g \in \mathcal{G}_{\alpha}^t} \left( \Pr [g = m \land \delta_2 \neq 0] - \Pr [g = m \land \delta_2 \neq 0] \right) \leq \frac{2D(m')}{q^2 (q - 1)}.
\]

This value is negligible in \(k\).

Note that, for any \(0 \leq v \leq q_{ss}\), the running time of \(\tilde{M}_{\alpha,\nu}^\beta\) is at most \(T_3 = T + 4T_5 + q_{ss} f_n^0 + q_{ss} f_n^1 + f_n\) for some polynomials \(f_n^0, f_n^0\) and \(f_n\) in \(n, t\) and \(k\). So, if \(T_3 \leq T_{\text{adh}}\), then the second term on the right-hand side of (6.7) is at most \(\epsilon_{\text{adh}}\). Consequently, we have
\[
|p_{2,0}(d_0) - p_{2,0}(d_0)| \leq q_{ss}(\epsilon_{\text{adh}} + 2\epsilon_{SS} + \tilde{\alpha}_1),
\]
where \(\tilde{\alpha}_1\) is negligible in \(k\).

### 6.4 Proof of Lemma 5.4

The distribution of \(y_1\) constructed in \(\mathcal{M}_{\alpha,0}^\beta\) is identical to that constructed in \(\mathcal{M}_{\alpha,2}^\beta\). This implies that the distribution of \((g, y_1, y_2, h, \hat{g}, \hat{h}, \tilde{g}, \tilde{h}, pub_2, pub_3)\) constructed in \(\mathcal{M}_{\alpha,0}^\beta\) is identical to that constructed in \(\mathcal{M}_{\alpha,2}^\beta\).

We note the following two facts:

**F1** This fact is due to the property of the secret sharing \(SS_{\alpha,n}\). For any \(x, x' \in \mathbb{Z}_q\), we set \(\{x_j\}_{j=1}^n = SS_{\alpha,n}(x)\) and \(\{x_j'\}_{j=1}^n = SS_{\alpha,n}(x')\). Let \(t' < t\) and \(1 \leq j_1 < \cdots < j_t' \leq n\). Then, for any \(m_{j_1}, \ldots, m_{j_t'} \in \mathbb{Z}_q\), one has
\[
\Pr [x_{j_1}, \ldots, x_{j_t'}] = (m_{j_1}, \ldots, m_{j_t'}) = \Pr [x_{j_1}', \ldots, x_{j_t'}'] = (m_{j_1}, \ldots, m_{j_t'}) = \frac{1}{q^{t'}}.
\]

where the probability is taken over the random tape of \(SS_{\alpha,n}\). In particular, if \(t' < t - 1\), then for any \(j_0 \in [n] \setminus \{j_1, \ldots, j_t\}\) and \(m_{j_0} \in \mathbb{Z}_q\), one has
\[
\Pr [x_{j_0} = m_{j_0} \mid (x_{j_1}, \ldots, x_{j_t'})] = (m_{j_1}, \ldots, m_{j_t'}) = \Pr [x_{j_0}' = m_{j_0} \mid (x_{j_1}', \ldots, x_{j_t'})'] = (m_{j_1}, \ldots, m_{j_t'}) = \frac{1}{q^{t'}}.
\]

**F2** Let \(g\) and \(h\) be generators of \(\mathbb{G}_q\). Then for any \(x, x' \in \mathbb{Z}_q\) and \(y \in \mathbb{G}_q\), one has
\[
\Pr_{r \in \mathbb{Z}_q} [y = g^r h^r] = \Pr_{r \in \mathbb{Z}_q} [y = g^r h^r].
\]

Using these facts, we see that, for any subset \(V' \subseteq [n]\) with \(#V' < t\), under the condition that \(h \neq 1\), the distribution of \((\{y_{1,1}\}_{j=1}^n, \{y_{2,1}\}_{j=1}^n, \{sec_j\}_{j \in \mathcal{V}})\) constructed in \(\mathcal{M}_{\alpha,0}^\beta\) is identical to that constructed in \(\mathcal{M}_{\alpha,2}^\beta\). Namely, the distribution of \((pub, sec_\mathcal{V})\) constructed in \(\mathcal{M}_{\alpha,0}^\beta\) is also identical that constructed in \(\mathcal{M}_{\alpha,2}^\beta\).

Assume that \(h \neq 1\). We note that the only difference between \(\mathcal{M}_{\alpha,0}^\beta\) and \(\mathcal{M}_{\alpha,2}^\beta\) is the construction of the secret seeds \(\{x_{1,j}\}_{j=1}^n\). In User’s query phase, the challenger does not use the secret seeds in order to respond to the query. Hence, when \(A\) enters User’s query phase with a query \(\{(j, a_j, b_j, \tilde{a}_j, \pi_{1,j})\}_{j \in [n]}\) and the answer \((V, u\_e, e\_v, v\_m, u_g, \tilde{u}_g, \tilde{u}_g, \tilde{v}_g, \tilde{v}_g)\) constructed in \(\mathcal{M}_{\alpha,0}^\beta\) is identical to that constructed in \(\mathcal{M}_{\alpha,2}^\beta\).

In Server’s query phase, the answer \((u\_v, v\_m, \pi_{1,j})\) depends on the secret seed \(x_{1,j}\) although the answer \((j, a_j, b_j, \tilde{a}_j, \pi_{1,j})\) is independent of it. There are the following two cases to consider:

- **Assume that** \(\tilde{u}_g = (\tilde{u}_g)\) holds. Then the distribution of \((u\_g, v\_m)\) depends on the secret seed \(x_{1,j}\). However, if \(\#\text{Idset} < t - t'\), that is, \(F = \text{false}\), then the fact **F1** implies that the distribution of \(x_{1,j} \in \mathbb{Z}_q\) is uniform. Hence, under the condition that \(F = \text{false}\), the distribution of \((u\_g, v\_m)\) constructed in \(\mathcal{M}_{\alpha,0}^\beta\) is identical to that constructed in \(\mathcal{M}_{\alpha,2}^\beta\).

- **Assume that** \(\tilde{u}_g = (\tilde{u}_g)\) holds. Then the distribution of \((u\_g, v\_m)\) depends on the secret seed \(x_{1,j}\). However, if \(\#\text{Idset} < t - t'\), that is, \(F = \text{false}\), then the fact **F1** implies that the distribution of \(x_{1,j} \in \mathbb{Z}_q\) is uniform. Hence, under the condition that \(F = \text{false}\), the distribution of \((u\_g, v\_m)\) constructed in \(\mathcal{M}_{\alpha,0}^\beta\) is identical to that constructed in \(\mathcal{M}_{\alpha,2}^\beta\).

The same argument can be applied even when we replace \(\mathcal{M}_{\alpha,2}^\beta\) by \(\mathcal{M}_{\alpha,1}^\beta\). In summary, we see that \(\Pr [F_{3,0,\alpha,0} \wedge \alpha \neq 1] = \Pr [F_{3,2,\alpha,0} \wedge \alpha \neq 1] = p_{3,0}^{F_{3,0,\alpha,0} \wedge \alpha \neq 1}(d_0)\) and \(p_{3,2,\alpha,0}^{F_{3,0,\alpha,0} \wedge \alpha \neq 1}(d_0)\) where \(p_{3,2,\alpha,0}^{F_{3,0,\alpha,0} \wedge \alpha \neq 1}(d_0) = \Pr [E_{3,0,\alpha,0} \wedge \alpha \neq 1 • F_{3,2,\alpha,0} \wedge \alpha \neq 1] \) for \(v = 0, 1\). We have
\[
\Pr[F_{3,0,d_p}] \leq \left| \Pr[F_{3,0,d_	heta}] - \Pr[F_{3,2,d_p}] \right| + \Pr[F_{3,2,d_p}]
\]
\[
\leq \left| \Pr[F_{3,0,d_	heta} \wedge h \neq 1] - \Pr[F_{3,2,d_p} \wedge h \neq 1] \right| + \left| \Pr[F_{3,0,d_	heta} \wedge h = 1] - \Pr[F_{3,2,d_p} \wedge h = 1] \right| + \Pr[F_{3,2,d_p}]
\]
\[
\leq \frac{1}{q} + \Pr[F_{3,2,d_p}].
\]

The symmetric argument yields
\[
\Pr[F_{3,2,d_p}] \leq \frac{1}{q} + \Pr[F_{3,0,d_	heta}].
\]

Set \(p_{3,0}^{F,h=1}(d_p) = p_{3,0}^{F}(d_p) - p_{3,0}^{F,h=1}(d_p)\). Since \(p_{3,0}^{F,h=1}(d_p) \leq 1/q\), we have
\[
|p_{3,0}^{F}(d_1) - p_{3,0}^{F}(d_2)| \leq |p_{3,0}^{F}(d_1) - p_{3,0}^{F}(d_2)| + |p_{3,0}^{F}(d_1) - p_{3,0}^{F}(d_2)|
\]
\[
+ |p_{3,0}^{F}(d_1) - p_{3,0}^{F}(d_2)| \leq \frac{2}{q} + |p_{3,0}^{F}(d_1) - p_{3,0}^{F}(d_2)|,
\]
proving the lemma.

### 6.5 Proof of Lemmas 5.5 and 5.6

We first prove Lemma 5.5. We construct two intermediary machines \(\tilde{M}_{4,1}^\theta\) and \(\tilde{M}_{4,2}^\theta\). On input \(w = (Q, g, g_1, g_2, g_3)\), \(\tilde{M}_{4,1}^\theta\) and \(\tilde{M}_{4,2}^\theta\) simulate \(M_{4,1}^\theta\) and \(M_{4,2}^\theta\), respectively, except for the following steps:

**13'**: Set \(y_1 = g_1\). Then, choose \(x_2 \in Z_q\) and compute \(y_2 = g^{x_2}, \{x_1\}_j^{n_j} = SS_{x_1}^{n_j}(0)\) and \(\{x_2\}_j^{n_j} = SS_{x_2}^{n_j}(x_2)\).

**16'**: Set \(u_{1,d} = g_2\) and \(v_{1,d} = g_3d_p\), and compute \((u_{2,d}, v_{2,d}) = (g^{x_2}, g^{z_2}d_p)\).

**A** Let \(w \in DH\). In Step 16' of \(\tilde{M}_{4,1}^\theta\), if we set \(r_{1,d} = \alpha_2\), where \(g_2 = g^{x_2}\), then one has \(u_{1,d} = g^{x_2}\) and \(v_{1,d} = g^{z_2}d_p\): these values are the same as the values obtained in initialization phase of \(M_{4,1}^\theta\) with \(r_{1,d} = \alpha_2\). Hence, the differences between \(M_{4,1}^\theta\) and \(\tilde{M}_{4,1}^\theta\) are the choice of \(\alpha_2\) in Step 13' and that of \(u_{1,d}\) in Step 16'. The distribution \(\Delta_{4,1}^\theta = \{(g_1, g_2) \mid g_1, g_2 \in Z_q\}\) over \(\mathcal{G}_q\) is identical to the distribution of \((y_1, u_{1,d})\) constructed in \(M_{4,1}^\theta\). In particular, \(\Delta_{4,1}^\theta\) is uniform over \(\mathcal{G}_q\) and is identical to the distribution of \((y_1, u_{1,d})\) constructed in \(\tilde{M}_{4,1}^\theta\).

**B** Let \(w \in \tilde{DH}\). By the similar argument to (A), we see that the differences between \(\tilde{M}_{4,1}^\theta\) and \(M_{4,2}^\theta\) are the choice of \(y_1\) in Step 13' and those of \(u_{1,d}\) and \(v_{1,d}\) in Step 16'. The distribution \(\Delta_{4,1}^\theta = \{(g_1, g_2, g_3d_p) \mid g_1, g_2, g_3 \in Z_q\}\) over \(\mathcal{G}_q\) is identical to the distribution of \((y_1, u_{1,d}, v_{1,d})\) constructed in \(\tilde{M}_{4,1}^\theta\). The distribution \(\Delta_{4,1}^\theta\) is uniform, and is identical to the distribution of \((y_1, u_{1,d}, v_{1,d})\) constructed in \(M_{4,1}^\theta\).

Note that \(\varphi_{4,1}^\theta\) and \(\varphi_{4,2}^\theta\) are independent of \(g_1, g_2\) and \(g_3\). Since the maximum \(T_5\) of the running times of \(\tilde{M}_{4,1}^\theta\) and \(\tilde{M}_{4,2}^\theta\) is at most \(T + 4T_3 + qL_{s}f_0^U + qL_{s}f_1^U + f_2^U\) for some polynomials \(f_0^U, f_1^U\) and \(f_2^U\) in \(n, t\) and \(k\), if \(T_5 \leq T_{\text{dhd}}\), then we have
\[
|\Pr[F_{3,0,d_p}] - \Pr[F_{4,2,d_p}]| = \left| \Pr[w \in DH | \varphi_{4,2}^\theta = 1] - \Pr[w \in DH | \varphi_{4,2}^\theta = 1] \right| = \left| \Pr[w \in DH | \varphi_{4,1}^\theta = 1] - \Pr[w \in DH | \varphi_{4,1}^\theta = 1] \right| < \epsilon_{\text{dhd}}
\]
and
\[
|p_{3,0}^{F}(d_1) - p_{3,0}^{F}(d_2)| = \left| \Pr[w \in DH | \varphi_{4,1}^\theta = 1] - \Pr[w \in DH | \varphi_{4,1}^\theta = 1] \right| = \left| \Pr[w \in DH | \varphi_{4,1}^\theta = 1] - \Pr[w \in DH | \varphi_{4,1}^\theta = 1] \right| < \epsilon_{\text{dhd}}.
\]

We next prove Lemma 5.6. We construct two intermediary machines \(\tilde{M}_{5,1}^\theta\) and \(\tilde{M}_{5,4}^\theta\). On input \(w = (Q, g, g_1, g_2, g_3)\), \(\tilde{M}_{5,1}^\theta\) and \(\tilde{M}_{5,4}^\theta\) simulate \(M_{5,1}^\theta\) and \(M_{5,4}^\theta\), respectively, except for the following steps:

**13'**: Set \(y_2 = g_1\). Then, choose \(x_2 \in Z_q\) and compute \(y_2 = g^{x_2}, \{x_1\}_j^{n_j} = SS_{x_1}^{n_j}(0)\) and \(\{x_2\}_j^{n_j} = SS_{x_2}^{n_j}(x_2)\).

**16'**: Choose \(u_{1,d} = g_2\) and \(v_{1,d} = g_3d_p\), and set \(u_{2,d} = g_2\) and \(v_{2,d} = g_3d_p\).

Then, by using the similar argument to the proof of Lemma 5.5, we see that the lemma follows.

### 6.6 Proof of Lemma 5.7

We construct an intermediary machine \(\tilde{M}_{5,\nu}^\theta\). On input \(w = (Q, g, g_1, g_2, g_3)\), \(\tilde{M}_{5,\nu}^\theta\) simulates \(M_{5,\nu}^\theta\), except for the following steps:

**13'**: Set \(y_1 = g_2\). Then, choose \(x_2 \in Z_q\) and compute \(y_2 = g^{x_2}, \{x_1\}_j^{n_j} = SS_{x_1}^{n_j}(0)\) and \(\{x_2\}_j^{n_j} = SS_{x_2}^{n_j}(x_2)\).

**14'**: Choose \(y_p, r_1, r_2, r_3, \tilde{x}, r_1, r_2 \in Z_q\) and \(r_1, r_3 \in Z_q^*\), and set \(h = g^{r_1}, \tilde{h} = g^{r_1}, \tilde{h} = g^{r_1}\) and \(\tilde{g} = g^{r_2}\). Then, compute \(\tilde{y} = (g^{r_2})^{x_2} \) and \(\tilde{y} = (g^{r_2})^{x_2}\).

**S1-2** If \(C_5 = v\), then set \(a_j = g_1, b_j = g_1b_j\) and \(a_j = g_1b_j\). Otherwise, execute the Step S1-2 of \(M_{5,\nu}^\theta\).

**S2-4** If \(C_5 = v\) and \(v_y = (\tilde{a}_p)^{-r_1/r_1} (\tilde{a}_p)^{-1/r_1}\), then set
\[
v_y = g^{r_2} g^{r_1} \left( \frac{v_y}{(\tilde{a}_p)^{r_1}} \right) (\tilde{a}_p)^{-1/r_1}.\]
If $C_s = v$ and $\hat{v}_p/(\hat{u}_p)^{\gamma} \neq \hat{h}^\gamma$ hold, then choose $v_j \in \mathcal{G}_q$. Otherwise, execute Step $S_4'\text{-}4'$ of $\mathcal{M}_{\delta,v}^\epsilon$.

Noting that $\varphi_{\delta,v}^\epsilon$ is independent of $g_1$, $g_2$ and $g_3$, we have

$$\left| \Pr[F_{S,v-1,d_p}] - \Pr[F_{S,v,d_p}] \right| \\ \leq \left| \Pr_{\text{we DH}}[\varphi_{\delta,v-1}^\epsilon = 1] - \Pr_{\text{we DH}}[\varphi_{\delta,v}^\epsilon = 1] \right| + \Pr_{\text{we DH}}[\varphi_{\delta,v}^\epsilon = 1] - \Pr_{\text{we DH}}[\varphi_{\delta,v}^\epsilon = 1] \right| \\ + \left| \Pr_{\text{we DH}}[\varphi_{\delta,v}^\epsilon = 1] - \Pr_{\text{we DH}}[\varphi_{\delta,v}^\epsilon = 1] \right|. \quad (6.10)$$

We estimate the first and the last terms on the right-hand side of (6.10). Let $E_{U,v}^{SS}$ denote the event defined as in the proof of Lemma 5.3. If the running time of $\mathcal{M}(\mathcal{L}_U^{\text{pub}})$ used in $\mathcal{M}_{\delta,v-1}^\epsilon$, $\mathcal{M}_{\delta,v}$ and $\mathcal{M}_{\delta,v}^\epsilon$ is at most $T_3$, and $\max\{n_U, q_3\} \leq q''_U, q''_2$, then we have

$$\left| \Pr_{\text{we DH}}[\varphi_{\delta,v-1}^\epsilon = 1] - \Pr_{\text{we DH}}[\varphi_{\delta,v}^\epsilon = 1] \right| + \Pr_{\text{we DH}}[\varphi_{\delta,v}^\epsilon = 1] - \Pr_{\text{we DH}}[\varphi_{\delta,v}^\epsilon = 1] \right| \\ \leq 2\varepsilon_{SS} + \left| \Pr_{\text{we DH}}[\varphi_{\delta,v-1}^\epsilon = 1 \land \neg E_{U,v}^{SS}] - \Pr_{\text{we DH}}[\varphi_{\delta,v}^\epsilon = 1 \land \neg E_{U,v}^{SS}] \right| \\ + \left| \Pr_{\text{we DH}}[\varphi_{\delta,v}^\epsilon = 1 \land \neg E_{U,v}^{SS}] - \Pr_{\text{we DH}}[\varphi_{\delta,v}^\epsilon = 1 \land \neg E_{U,v}^{SS}] \right|. \quad (6.11)$$

In order to estimate other terms, we assume that the event $E_{U,v}^{SS}$ does not occur.

(A) We first consider the second term on the right-hand side of (6.11). Let $w \in \text{DH}$. We have

$$\left| \Pr_{\text{we DH}}[\varphi_{\delta,v-1}^\epsilon = 1 \land \neg E_{U,v}^{SS}] - \Pr_{\text{we DH}}[\varphi_{\delta,v}^\epsilon = 1 \land \neg E_{U,v}^{SS}] \right| \\ \leq \left| \Pr_{\text{we DH}}[\varphi_{\delta,v-1}^\epsilon = 1 \land \neg E_{U,v}^{SS} \land I_v] - \Pr_{\text{we DH}}[\varphi_{\delta,v}^\epsilon = 1 \land \neg E_{U,v}^{SS} \land I_v] \right| \\ + \left| \Pr_{\text{we DH}}[\varphi_{\delta,v}^\epsilon = 1 \land \neg E_{U,v}^{SS} \land \neg I_v] - \Pr_{\text{we DH}}[\varphi_{\delta,v}^\epsilon = 1 \land \neg E_{U,v}^{SS} \land \neg I_v] \right|. \quad (6.12)$$

where $I_v$ denotes the event defined as in the proof of Lemma 5.3.

(A-1) In order to estimate the first term on the right-hand side of (6.12), we assume that the event $I_v$ occurs. In the $v$-th Server's query phase of $\hat{M}_{\delta,v}^\epsilon$, if we set $t_j = \alpha_1$, where $g_1 = g^\epsilon$, then one has $a_j = g^\gamma$, $b_j = u_{\hat{p}r}$, $\hat{a}_j = (\hat{g})^\gamma$ and

$$v_j = g^\gamma_{\hat{p}} \hat{u}_r^{-1/r_2} = \left( \frac{\hat{u}_p^{\alpha_1} h_r^{\alpha_2}}{u_{\hat{p}r}^{\alpha_1} h_r^{\alpha_2}} \right)^{t_j} \hat{h}_r^{\gamma}. \frac{\hat{h}_r^{\gamma}}{h_r^{\gamma}}. \hat{h}_r^{\gamma}$$

This shows that these values are the same as the values obtained in the $v$-th Server's query phase of $\hat{M}_{\delta,v-1}^\epsilon$ with $t_j = \alpha_1$. Hence, the differences between $\hat{M}_{\delta,v-1}^\epsilon$ and $\hat{M}_{\delta,v}^\epsilon$ are the choice of $y_1$ in Step $S_4'$, those of $h$, $\hat{g}$, $\hat{h}$ and $\hat{g}$ in Step $S_4'$ and that of $a_j$ in Step $S_4'\text{-}2'$ in the $v$-th Server's query phase. We define the distribution $\Delta_{\delta,v}^\epsilon$ over $\mathcal{G}_q$ by

$$\Delta_{\delta,v}^\epsilon = \{(g^\gamma_{\hat{p}}, g^\epsilon_{\hat{a}t_1}, g^\epsilon_{\hat{d}t_2}, g^\epsilon_{\hat{r}t_3}) \mid r_0, r_2, \alpha_1, \alpha_2 \in \mathbb{Z}_q, r_1, r_3 \in \mathbb{Z}_q^*\}.$$ 

The distribution $\Delta_{\delta,v}^\epsilon$ is identical to the distribution of $(y_1, h, \hat{g}, \hat{h}, \hat{g}, a_1)$ constructed in $\hat{M}_{\delta,v-1}^\epsilon(w)$. In addition, the distribution of $(y_1, h, \hat{g}, \hat{h}, \hat{g}, a_1)$ constructed in $\hat{M}_{\delta,v-1}^\epsilon(w)$ is uniform over $\mathcal{G}_q$. The first term on the right-hand side of (6.12) is bounded by the statistical distance between $\Delta_{\delta,v}^\epsilon$ and $U_{\mathcal{G}_q}$. Since the distribution $\{(g^\gamma_{\hat{p}}, g^\epsilon_{\hat{a}t_1}, g^\epsilon_{\hat{d}t_2}, g^\epsilon_{\hat{r}t_3}) \mid r_0, r_2, \alpha_1, \alpha_2 \in \mathbb{Z}_q, r_1, r_3 \in \mathbb{Z}_q^*\}$ over $\mathcal{G}_q$ is uniform, the statistical distance between $\Delta_{\delta,v}^\epsilon$ and $U_{\mathcal{G}_q}$ is less than the distance between the distribution $\Delta_{\delta,v}^\epsilon$ and $U_{\mathcal{G}_q}$. For any $\hat{g} \in \mathcal{G}_q \setminus \{1\}$ and $\hat{h}, a_1 \in \mathcal{G}_q$, we have

$$\Pr_{\hat{g}, a_1 \in \mathcal{G}_q} \{ g = (1, \hat{g}, \hat{h}, a_1) \} = 0.$$ 

For any $y_1, \hat{g}, \hat{h}, a_1 \in \mathcal{G}_q \setminus \{1\}$, we have

$$\Pr_{\hat{g}, a_1 \in \mathcal{G}_q} \{ g = (y_1, \hat{h}, a_1) \} = \Pr_{\hat{g}, a_1 \in \mathcal{G}_q} \{ g = (y_1, 1, a_1) \} \Pr_{\hat{g}, a_1 \in \mathcal{G}_q} \{ g = (y_1, 1, 1) \} \Pr_{\hat{g}, a_1 \in \mathcal{G}_q} \{ g = (y_1, \hat{g}, 1) \} \Pr_{\hat{g}, a_1 \in \mathcal{G}_q} \{ g = (y_1, \hat{g}, \hat{h}) \} \Pr_{\hat{g}, a_1 \in \mathcal{G}_q} \{ g = (1, 1, a_1) \} \Pr_{\hat{g}, a_1 \in \mathcal{G}_q} \{ g = (1, 1, 1) \} = 0,$$
\[
\Pr_{g \in \Delta_{x}} [g = (y_1, 1, 1)] = \Pr_{g \in \Delta_{x}} [g = (1, 1, 1, 1)] = \frac{1}{q^2}, \quad \Pr_{g \in \Delta_{x}} [g = (1, 1, \hat{h}, a)] = \frac{1}{q^4(q-1)}
\]

and

\[
\Pr_{g \in \Delta_{x}} [g = (y_1, \hat{g}, a)] = \frac{1}{q^4(q-1)^2}.
\]

Hence, the statistical distance between \(\Delta_{x}\) and \(U_{G_q}^{\alpha}\) is at most \(2(q-1)/(4q^2 - 3q + 2)/q^4\), which is negligible in \(k\).

(A-2) In order to estimate the last term on the right-hand side of (6.12), we assume that the event \(I_v\) does not occur. Then, the value \(v_1\) is uniformly chosen in the \(v\)-th Server’s query phase of both \(M_{x,v-1}^\alpha\) and \(M_{x,v}^\alpha\). Hence, the differences between \(M_{x,v-1}^\beta\) and \(M_{x,v}^\beta\) are the same as the case where \(I_v\) occurs, and we have

\[
\begin{align*}
\Pr_{w \in \mathcal{DH}} [\varphi_{x,v-1}^\beta = 1 \land \neg E_{U,v}^{SS}] - \Pr_{w \in \mathcal{DH}} [\varphi_{x,v}^\beta = 1 \land \neg E_{U,v}^{SS}] &\leq \frac{4(q-1)(4q^2 - 3q + 2)}{q^4}.
\end{align*}
\]

This value is negligible in \(k\).

(B) We next consider the last term on the right-hand side of (6.11). Let \(w \in \overline{\mathcal{DH}}\). We have

\[
\begin{align*}
\Pr_{w \in \mathcal{DH}} [\varphi_{x,v}^\beta = 1 \land \neg E_{U,v}^{SS}] - \Pr_{w \in \mathcal{DH}} [\varphi_{x,v}^\beta = 1 \land \neg E_{U,v}^{SS}] &\leq \Pr_{w \in \mathcal{DH}} [\varphi_{x,v}^\beta = 1 \land \neg E_{U,v}^{SS} \land I_v] - \Pr_{w \in \mathcal{DH}} [\varphi_{x,v}^\beta = 1 \land \neg E_{U,v}^{SS} \land I_v]
\end{align*}
\]

\[
\frac{4(q-1)(4q^2 - 3q + 2)}{q^4}.
\]

(B-1) In order to estimate the last term on the right-hand side of (6.13), we assume that the event \(I_v\) does not occur. Then the differences between \(M_{x,v}^\beta\) and \(M_{x,v}^\alpha\) are the same as the case of (A-2). The distribution

\[
\Delta_{x,v}^\beta = \{(g_2, g_3^o, g_4^o, g_1^o, g_1) \mid r_0, r_2, r_2, r_1, r_3 \in \mathbb{Z}_q, g_1, g_2, g_3 \in \mathbb{G}_q\}
\]

over \(G_q^\alpha\) is identical to the distribution of \((y_1, h, \hat{g}, \hat{h}, \hat{g}, a_1)\) constructed in \(M_{x,v}^\alpha(w)\). In addition, the distribution of \((y_1, h, \hat{g}, \hat{h}, \hat{g}, a_1)\) constructed in \(M_{x,v}^\alpha(w)\) is uniform over \(G_q^\alpha\). The last term on the right-hand side of (6.13) is bounded by the statistical distance between \(\Delta_{x,v}^\beta\) and \(U_{G_q}^{\alpha}\). Since the distribution

\[
\{(g_2, g_3^o, g_4^o, g_1^o) \mid r_0, r_2, r_2, r_1, r_3 \in \mathbb{Z}_q, g_1, g_2, g_3 \in \mathbb{G}_q\}
\]

over \(G_q^\alpha\) is uniform, the statistical distance between \(\Delta_{x,v}^\beta\) and \(U_{G_q}^{\alpha}\) is less than the distance between \(U_{G_q}^{\alpha}\) and \(\Delta_{x,v}^\beta\) defined in the proof of Lemma 5.2. Hence, the statistical distance between \(\Delta_{x,v}^\beta\) and \(U_{G_q}^{\alpha}\) is at most \(4(q-1)/q^4\), which is negligible in \(k\).

(B-2) In order to estimate the first term on the right-hand side of (6.13), we assume that the event \(I_v\) occurs. Let \(R_v\) denote the event such that \(A\) enters the \(v\)-th Server’s query phase with a query \((V, u, e, j, u_p, \hat{u}_p, \hat{v}_p, \pi_{2,j})\) which satisfies the following two conditions: (i) \(u_p = u_p\) and (ii) \(\pi_{2,j}\) is a valid proof. We have

\[
\begin{align*}
\Pr_{w \in \mathcal{DH}} [\varphi_{x,v}^\beta = 1 \land \neg E_{U,v}^{SS} \land I_v] - \Pr_{w \in \mathcal{DH}} [\varphi_{x,v}^\beta = 1 \land \neg E_{U,v}^{SS} \land I_v]
\end{align*}
\]

\[
\frac{4(q-1)(4q^2 - 3q + 2)}{q^4}.
\]

(1) In order to estimate the last term on the right-hand side of (6.14), we assume that the event \(R_v\) does not occur. The differences between \(M_{x,v}^\beta\) and \(M_{x,v}^\alpha\) are the choice of \(y_1\) in Step 13, those of \(h, \hat{g}, \hat{h}\) and \(\hat{g}\) in Step 14, and those of \(a_j\) and \(v_j\) in the \(v\)-th Server’s query phase.

If \(\pi_{2,j}\) is invalid, then the value \(v_j\) is not computed in the \(v\)-th Server’s query phase. So the differences between \(M_{x,v}^\beta\) and \(M_{x,v}^\alpha\) are the same as the case of (B-1).

Assume that \(\pi_{2,j}\) is valid. We set \(\delta = \bar{r}_p - \bar{r}_p\), where \(u_p = g^\delta\). Then the value \(v_j\) computed in the \(v\)-th Server’s query phase of \(M_{x,v}^\beta\) is equal to \(\bar{g}_5\). Let \(D\) be the distribution of \(\delta \in \mathbb{Z}_q\). The distribution \(D\) depends on \(y_1, h, \hat{g}, \hat{h}, \hat{g}\) and \(a_j\). The distribution
\[ \Delta^3_{S,v} = \{(g_2, g^n, g^p, g_1, g^q, g_{1, g_3}) | r_1, r_2 \in \mathbb{Z}_s, \: r_0, r_2 \in \mathbb{Z}_t, \: g_1, g_2, g_3 \in \mathbb{G}_q, \: \delta \in \mathbb{D} \} \]

is identical to the distribution of \((y_1, h, \hat{g}, h, \hat{g}, a_j, v_j)\) constructed in \(M^7_{S,v}(w)\), and the distribution of \((y_1, h, \hat{g}, h, \hat{g}, a_j, v_j)\) constructed in \(M^7_{S,v}(w)\) is uniform over \(\mathbb{G}_q^7\). The last term on the right-hand side of (6.14) is bounded by the statistical distance between \(\Delta^3_{S,v}\) and \(U_{G_q^7}\). We note that if \(\delta \neq 0\) if \(\pi_{2, f}\) is valid. Hence, we have

\[
\frac{4(q-1)}{q^2} + \sum_{m \in \mathbb{G}_q^7} \Pr_{g \in U_{G_q^7}} [g = m \land \delta \neq 0] - \Pr_{g \in U_{G_q^7}} [g = m \land \delta \neq 0].
\]

We write \(m = (m_1, \ldots, m_6, m_7) = (m', m_7) \in \mathbb{G}_q^7\) and \(g = (g', g_7)\). For any \(m \in \mathbb{G}_q^7\), we have

\[
\Pr_{g \in U_{G_q^7}} [g = m \land \delta \neq 0] = \frac{1}{q^6} \Pr_{g \in U_{G_q^7}} [g = m_1 \land \delta \neq 0 | g' = m']
\]

\[
= \frac{1}{q^6} \Pr_{g \in U_{G_q^7}} [g_7 = m_7 | \delta \neq 0 \land g' = m'] \Pr_{g \in U_{G_q^7}} [\delta \neq 0 | g' = m']
\]

\[
= \frac{1}{q^6} \Pr_{g \in U_{G_q^7}} [\delta \neq 0 | g' = m'].
\]

Since the value \(\delta\) depends on \(m'\), we have

\[
\Pr_{g \in U_{G_q^7}} [\delta \neq 0 | g' = m'] = \Pr_{g \in \Delta^3_{S,v}} [\delta \neq 0 | g' = m'].
\]

We denote this value by \(D(m')\).

(i) When \(m_3 = m_4 = m_6 = m_7 = 1\), we have

\[
\Pr_{g \in \Delta^3_{S,v}} [g = m \land \delta \neq 0] = \frac{1}{q^7} \Pr_{g \in \Delta^3_{S,v}} [g_7 = m_7 | \delta \neq 0 \land g' = m'] = \frac{1}{q^7} \Pr_{g \in \Delta^3_{S,v}} [\delta = 1 | \delta \neq 0 \land g' = m']D(m') = \frac{D(m')}{q^7}.
\]

(ii) When \(m_3 = m_7 = 1\) and \(m_4, m_6 \neq 1\), we have

\[
\Pr_{g \in \Delta^3_{S,v}} [g = m \land \delta \neq 0] = \frac{1}{q^7} \Pr_{g \in \Delta^3_{S,v}} [g_7 = m_7 | \delta \neq 0 \land g' = m'] = \frac{1}{q^7} \Pr_{g \in \Delta^3_{S,v}} [\delta = 1 | \delta \neq 0 \land g' = m']D(m') = \frac{D(m')}{q^7(q-1)}.
\]

(iii) When \(m_3 = m_6 = 1\) and \(m_4, m_7 \neq 1\), we have

\[
\Pr_{g \in \Delta^3_{S,v}} [g = m \land \delta \neq 0] = \frac{1}{q^7} \Pr_{g \in \Delta^3_{S,v}} [g_7 = m_7 | \delta \neq 0 \land g' = m'] = \frac{1}{q^7(q-1)} \Pr_{g \in \Delta^3_{S,v}} [\delta = 1 | \delta \neq 0 \land g' = m']D(m') = \frac{D(m')}{q^7(q-1)}.
\]

(iv) When \(m_3, m_4, m_6, m_7 \neq 1\), by the similar argument to (iii), we have

\[
\Pr_{g \in \Delta^3_{S,v}} [g = m \land \delta \neq 0] = \frac{1}{q^7(q-1)} \Pr_{g \in \Delta^3_{S,v}} [g_7 = m_7 | \delta \neq 0 \land g' = m']D(m') = \frac{1}{q^7(q-1)} \Pr_{g \in \Delta^3_{S,v}} [\delta = 1 | \delta \neq 0 \land g' = m']D(m') = \frac{D(m')}{q^7(q-1)^2}.
\]

If \(m\) does not apply to any cases above, then \(\Pr_{g \in \Delta^3_{S,v}} [g = m \land \delta \neq 0] = 0\) follows. Since \(D(m') \leq 1\), we obtain

\[
\sum_{m \in \mathbb{G}_q^7} \Pr_{g \in \Delta^3_{S,v}} [g = m \land \delta \neq 0] - \Pr_{g \in U_{G_q^7}} [g = m \land \delta \neq 0] \leq \frac{8q^3 - 16q^2 + 16q - 8}{q^4},
\]

which is negligible in \(k\).
(2) In order to estimate the first term on the right-hand side of (6.14), we assume that \( R_i \) occurs. Using the machines \( M_{5,v}^\beta \) and \( \tilde{M}_{5,v}^\beta \), we construct new machines \( N_{5,v}^\beta \) and \( \tilde{N}_{5,v}^\beta \) which solve the CDH problem. On input \((Q,g,g_1,g_2)\), \( N_{5,v}^\beta \) works as follows:

1. \( \text{Choose } a_1, a_2, a_3 \in \mathbb{Z}_q \) and simulate \( M_{5,v}^\beta \) on input \( w = (Q,g,g^{a_1},g^{a_2},g^{a_3}) \) except for the following steps:
   - \( 1^3' \): Choose \( x_1, x_2 \in \mathbb{Z}_q \) and compute \( y_1 = g^{a_1}, y_2 = g^{a_2}, \{x_1, y_1\}^{a_3} = SS_{/x_1}(0) \) and \( \{x_2, y_2\}^{a_3} = SS_{/x_2}(2) \).
   - \( 1^4' \): Choose \( z \in \mathbb{Z}_q \), \( h, h', \tilde{g}, \tilde{g}' \in \mathbb{G}_q \), and \( r_1, r_2, d \in \mathbb{Z}_q \), and set \( \tilde{g} = g_1 \). Then compute \( \tilde{g} = (\tilde{g})^d \).
   - \( 1^5 \): Choose a password \( p \in \mathbb{Z}_q \), and simulate \( \tilde{g}^{h} \).

(2) When \( A \) enters the \( v \)-th Server's query phase with a query \((V, w, e, j, u_p, v_p, \hat{u}_p, \hat{v}_p, \pi_{2,j})\),

- if \( u_p \neq u_y \) and \( \pi_{2,j} \) is valid, then output \( \hat{u}_p \) and halt.
- Otherwise, output \( z \in \mathbb{G}_q \), and halt.

We note that if the event \( E_{U,v}^{SS} \land R_i \) occurs in \( N_{5,v}^\beta \), then \( \hat{u} = CDH(Q, g, g_1, g_2) \) follows. In addition, we see that the probability that the event \( E_{U,v}^{SS} \land R_i \) occurs in \( N_{5,v}^\beta \) is equal to that in \( M_{5,v}^\beta \) by the construction of \( N_{5,v}^\beta \). If the running time of \( N_{5,v}^\beta \) is less than \( T_{\text{ddh}} \), then by Lemma 2.1, we have

\[
\Pr_{w \in \mathbb{DH}}[M_{5,v}^\beta(w) = 1 \land E_{U,v}^{SS} \land I_v \land R_i] \leq \Pr_{w \in \mathbb{DH}}[M_{5,v}^\beta(Q,g,g_1,g_2) = CDH(Q,g,g_1,g_2)] < 2^{-\frac{1}{2}} \cdot \varepsilon_{\text{ddh}} + \frac{1}{2
\}

We next construct the machine \( \tilde{N}_{5,v}^\beta \), \( \tilde{M}_{5,v}^\beta \) works as follows: On input \((Q,g,g_1,g_2)\),

1. \( \text{Choose } a_1, a_2 \in \mathbb{Z}_q \), and simulate \( M_{5,v}^\beta \) on input \( w = (Q,g,g^{a_1},g^{a_2},g) \) except for the following steps:
   - \( 1^5 \): Choose a password \( p \in \mathbb{Z}_q \), and simulate \( \tilde{g}^{h} \).

(2) When \( A \) enters the \( v \)-th Server's query phase with a query \((V, w, e, j, u_p, v_p, \hat{u}_p, \hat{v}_p, \pi_{2,j})\),

- if \( u_p \neq u_y \) and \( \pi_{2,j} \) is valid, then output \( \hat{u}_p \) and halt.
- Otherwise, output \( z \in \mathbb{G}_q \), and halt.

If the event \( E_{U,v}^{SS} \land R_i \) occurs in \( \tilde{N}_{5,v}^\beta \), then \( \hat{u} = CDH(Q,g,g_1,g_2) \) follows. In addition, we see that the probability that the event \( E_{U,v}^{SS} \land R_i \) occurs in \( \tilde{N}_{5,v}^\beta \) is equal to that in \( \tilde{M}_{5,v}^\beta \) by the construction of \( \tilde{N}_{5,v}^\beta \). Hence, if the running time of \( \tilde{N}_{5,v}^\beta \) is less than \( T_{\text{ddh}} \), then by Lemma 2.1, we have

\[
\Pr_{w \in \mathbb{DH}}[\tilde{M}_{5,v}^\beta(w) = 1 \land E_{U,v}^{SS} \land I_v \land R_i] \leq \Pr_{w \in \mathbb{DH}}[\tilde{M}_{5,v}^\beta(Q,g,g_1,g_2) = CDH(Q,g,g_1,g_2)] < 2^{-\frac{1}{2}} \cdot \varepsilon_{\text{ddh}} + \frac{1}{2
\}

Note that the maximum \( T_7 \) of the running time of machines \( \{M_{5,v}^\beta, \tilde{M}_{5,v}^\beta, \tilde{N}_{5,v}^\beta, \tilde{N}_{5,v}^\beta, \tilde{N}_{5,v}^\beta, \tilde{N}_{5,v}^\beta\} \) is at most \( T_7 = 4T_3 + qT_3 + qT_3 + T_3 \) for some polynomials \( T_3, T_3, T_3, T_3 \) in \( n, r, t, k \) and \( k \). So, if \( T_7 \leq T_{\text{ddh}} \), then second term on the right-hand side of (6.10) is at most \( T_{\text{ddh}} \). Consequently, we have

\[
\Pr[F_{5,0,\alpha}] - \Pr[F_{5,0,\alpha}] \leq qg(2\varepsilon_{\text{ddh}} + 2\varepsilon_{\text{ss}} + \alpha_1),
\]

where \( \alpha_1 \) is negligible in \( k \).

7.1 Proof of Lemma 5.8

We construct an intermediary machine \( \tilde{N}_{5,v}^\beta \). On input \( w = (Q,g,g_1,g_2,g_3) \), \( \tilde{N}_{5,v}^\beta \) simulates \( \tilde{M}_{5,v}^\beta \) except for the following steps:

1. \( \text{Set } y_1 = g_2 \). Then, choose \( x_2 \in \mathbb{Z}_q \), and compute \( y_2 = g^{a_2}, \{x_1, y_1\}^{a_3} = SS_{/x_1}(0) \) and \( \{x_2, y_2\}^{a_3} = SS_{/x_2}(2) \).
   - \( 1^4' \): Choose \( \tilde{g}^{a_1}, \tilde{g}^{a_2}, \tilde{g}^{a_3} \in \mathbb{G}_q \), and set \( \tilde{g} = g^{a_1} \) and \( \tilde{g} = g^{a_2} \). Then, compute \( \tilde{g} = (\tilde{g})^{a_3} \).
   - \( 1^3' \): Set \( C_U = v \), then set \( e_j = (\tilde{g})^{a_3} \) for each \( j \in [n] \). Otherwise, execute Step 1.3' of \( M_{5,v}^\beta \).

Noting that \( \psi_{5,v}^\beta \) is independent of \( g_1 \), \( g_2 \) and \( g_3 \), we have

\[
\left| \Pr_{w \in \mathbb{DH}}[F_{\psi_{5,v}^\beta}] = - \Pr[F_{\psi_{5,v}^\beta}] \right| 
\leq \left| \Pr_{w \in \mathbb{DH}}[\psi_{5,v}^\beta] = 1 \right| - \left| \Pr_{w \in \mathbb{DH}}[\psi_{5,v}^\beta] = 1 \right| 
+ \left| \Pr_{w \in \mathbb{DH}}[\psi_{5,v}^\beta] = 1 \right| - \left| \Pr_{w \in \mathbb{DH}}[\psi_{5,v}^\beta] = 1 \right| 
\]

We estimate the first and the last terms on the right-hand side of (6.15). Let \( E_{U,v}^{SS} \) denote the event defined as in the proof of Lemma 5.1. If the running time of \( A(L_{5,v}^{\psi_{5,v}^\beta}) \) used in \( M_{5,v}^\beta \) and \( \tilde{M}_{5,v}^\beta \) is at most \( T_5 \), and \( \max\{nu, q_3 \} \leq q_3 T_{\text{ddh}} \), then we have

\[
\text{(6.15)}
\]
that the differences between

\[ V_{\alpha_{\nu}} = 1 - \mathbb{E}_{\text{SS}} \]

are identical to the distribution of \( V_{\alpha_{\nu}} \). Hence, we have

\[ \frac{V_{\alpha_{\nu}}}{\nu_{\text{SS}}} \]

in order to estimate other terms, we assume that the event \( \mathbb{E}_{\text{SS}} \) does not occur.

(A) We first consider the second term on the right-hand side of (6.16). Let \( w \in \text{DH} \). Using the similar argument to (A) of the proof of Lemma 5.1, we see that the differences between \( M_{\alpha_{\nu}} \) and \( M_{\alpha_{\nu}} \) are the choice of \( y_1 \) in Step 13', those of \( \tilde{y}_1 \) and \( \tilde{y} \) in Step 14' and that of \( u_\rho \) in Step 13'' of the \( \nu \)-th User’s query phase. The distribution

\[ \Delta_{\alpha_{\nu}} = \{(g_1, g_2, g_3, g_4, g_5) \mid r_1, r_2, r_3, r_4, r_5 \in \mathbb{Z}_{q^r}, g_1, g_2, g_3, g_4, g_5 \in \mathbb{Z}_{q^r} \} \]

over \( \mathbb{G}_{\nu} \) is identical to the distribution of \( \{(y_1, \tilde{y}_1, \tilde{y}, u_\rho) \} \) constructed in \( M_{\alpha_{\nu}}(w) \), and the distribution

\[ \Delta_{\alpha_{\nu}} = \{(y_1, \tilde{y}_1, \tilde{y}, u_\rho) \} \]

over \( \mathbb{G}_{\nu} \) is identical to the distribution of \( \{(y_1, \tilde{y}_1, \tilde{y}, u_\rho) \} \) constructed in \( M_{\alpha_{\nu}}(w) \). The second term on the right-hand side of (6.16) is bounded by the statistical distance between \( \Delta_{\alpha_{\nu}} \) and \( \Delta_{\alpha_{\nu}} \). Note that the distribution \( \{(g_2, g_3, g_4, g_5) \mid r_2, r_3, r_4, r_5 \in \mathbb{Z}_{q^r}, g_1, g_2, g_3, g_4, g_5 \in \mathbb{Z}_{q^r} \} \) is uniform over \( \mathbb{G}_{\nu} \). So, the statistical distance between \( \Delta_{\alpha_{\nu}} \) and \( \Delta_{\alpha_{\nu}} \) is less than the distance between \( U_{\alpha_{\nu}} \) and \( \Delta_{\alpha_{\nu}} \) defined in the proof of Lemma 5.2. Hence, the statistical distance between \( \Delta_{\alpha_{\nu}} \) and \( U_{\alpha_{\nu}} \) is at most \( 4q_{\nu}^2 \), which is negligible in \( k \).

(B) We next consider the last term on the right-hand side of (6.16). Let \( w \in \overline{\text{DH}} \). By the similar argument to (A), we see that the differences between \( M_{\alpha_{\nu}} \) and \( M_{\alpha_{\nu}} \) are the choice of \( y_1 \) in Step 13', those of \( \tilde{y}_1 \) and \( \tilde{y} \) in Step 14' and that of \( u_\rho \) and \( v_\rho \) in Step 13'' of the \( \nu \)-th User’s query phase. The distribution

\[ \Delta_{\alpha_{\nu}} = \{(g_2, g_3, g_4, g_5, g_6) \mid r_2, r_3, r_4, r_5, r_6 \in \mathbb{Z}_{q^r}, g_1, g_2, g_3, g_4, g_5, g_6 \in \mathbb{Z}_{q^r} \} \]

over \( \mathbb{G}_{\nu} \) is identical to the distribution of \( \{(y_1, \tilde{y}_1, \tilde{y}, u_\rho, v_\rho) \} \) constructed in \( M_{\alpha_{\nu}}(w) \), and the distribution

\[ \Delta_{\alpha_{\nu}} = \{(y_1, \tilde{y}_1, \tilde{y}, u_\rho, v_\rho) \} \]

over \( \mathbb{G}_{\nu} \) is identical to the distribution of \( \{(y_1, \tilde{y}_1, \tilde{y}, u_\rho, v_\rho) \} \) constructed in \( M_{\alpha_{\nu}}(w) \). The last term on the right-hand side of (6.16) is bounded by the statistical distance between \( \Delta_{\alpha_{\nu}} \) and \( \Delta_{\alpha_{\nu}} \). Note that for any fixed \( p \in \mathbb{Z}_{q^r} \) and \( h \in \mathbb{G}_{\nu} \) the distribution \( \{(h, h) \mid g_4, g_5, g_6 \in \mathbb{Z}_{q^r} \} \) is uniform. So, by the same argument as above, the statistical distance between \( \Delta_{\alpha_{\nu}} \) and \( \Delta_{\alpha_{\nu}} \) is less than the distance between \( U_{\alpha_{\nu}} \) and \( U_{\alpha_{\nu}} \).

Note that, for any \( 0 \leq \nu \leq q_{\nu} \), the running time of \( M_{\alpha_{\nu}} \) is at most \( T_8 = T + 4T_5 + q_{\nu} \) for some polynomials \( f_1, f_2 \) and \( f_3 \) in \( n, t \) and \( k \). So, if \( T_8 \leq T_{\text{adh}} \), then the second term on the right-hand side of (6.15) is at most \( \varepsilon_{\text{adh}} \). Hence, we have

\[ \frac{V_{\alpha_{\nu}}}{\nu_{\text{SS}}} \leq \varepsilon_{\text{adh}} + 2ne_{\text{SS}} + \varepsilon_{\text{adh}}, \]

where \( \varepsilon_{\text{adh}} \) is negligible in \( k \).

6.8 Proof of Lemma 5.9

We construct an intermediary machine \( M_{\rho_0} \). On input \( w = (Q_1, g_1, g_2, g_3, \ldots) \), \( M_{\rho_0} \) simulates \( M_{\rho_0} \) except for the following steps:

13': Set \( y_1 = g_1 \). Then, choose \( x_2 \in \mathbb{Z}_{q^r} \) and compute \( y_2 = g^{x_2}, \{x_{1,j}\}_{j=1}^n = \text{SS}_{\rho_0}(0) \) and \( \{x_{2,j}\}_{j=1}^n = \text{SS}_{\rho_0}(0) \).

15': Choose \( p \in \mathbb{Z}_{q^r} \) and set \( u_\rho = g_2 + v_\rho \).

(A) Let \( w \in \text{DH} \). Using the similar argument to (A) of the proof of Lemma 5.5, we see that the differences between \( M_{\rho_0} \) and \( M_{\rho_0} \) are the choice of \( y_1 \) in Step 13' and that of \( u_\rho \) in Step 15'. The distribution \( \Delta_{\rho_0} = \{(g_1, g_2) \mid g_1, g_2 \in \mathbb{G}_{\nu} \} \) is identical to the distribution of \( (y_1, u_\rho) \) constructed in \( M_{\rho_0}(w) \). The distribution \( \Delta_{\rho_0} \) is uniform over \( \mathbb{G}_{\nu} \), and is identical to the distribution of \( (y_1, u_\rho) \) constructed in \( M_{\rho_0}(w) \).

(B) Let \( w \in \overline{\text{DH}} \). By the similar argument to (A), we see that the differences between \( M_{\rho_0} \) and \( M_{\rho_1} \) are the choice of \( y_1 \) in Step 13' and those of \( u_\rho \) and \( v_\rho \) in Step 15'. For any fixed \( p \in \mathbb{Z}_{q^r} \) and \( h \in \mathbb{G}_{\nu} \), the distribution \( \Delta_{\rho_1} = \{(g_1, g_2, g_3, g_4, g_5, g_6) \mid g_1, g_2, g_3, g_4, g_5, g_6 \in \mathbb{G}_{\nu} \} \) is identical to the distribution of \( (y_1, u_\rho, v_\rho) \) constructed in \( M_{\rho_1}(w) \). The distribution \( \Delta_{\rho_1} \) is uniform, and is identical to that constructed in \( M_{\rho_1}(w) \).

Since the running time of \( M_{\rho_0} \) is at most \( T_9 = T + 4T_5 + q_{\nu}f_1 + q_{\nu}f_2 + q_{\nu}f_3 \) for some polynomials \( f_1, f_2, f_3 \) in \( n, t \) and \( k \), if \( T_9 \leq T_{\text{adh}} \), then we have
\[ | \text{Pr}[F_{7,0,d_j}] - \text{Pr}[F_{7,1,d_j}] | = \left| \text{Pr}_{w \in \text{DH}} [ \psi_{7,0}^a = 1] - \text{Pr}_{w \in \text{DH}} [ \psi_{7,1}^a = 1] \right| = \left| \text{Pr}_{w \in \text{DH}} [ \psi_{7,0}^a = 1] - \text{Pr}_{w \in \text{DH}} [ \psi_{7,1}^a = 1] \right| < \epsilon_{\text{DH}}. \]

7. Concluding Remarks

We have studied the PPSS scheme PPSS\textsubscript{2} proposed in [4], and pointed out that PPSS\textsubscript{2} can be broken by an attack based on public parameters, and the proof of PPSS-security leaves room for refinement. The former difficulty was resolved in [7], where they introduced another security notion for PPSS schemes, called pparam-secure, showed how to enhance the protocol, and proved that the enhanced protocol is pparam-secure. We have investigated the latter point in this paper. Namely, we have made the proof of PPSS-security rigorous, and proved that ePPSS\textsubscript{2} is PPSS-secure as well as pparam-secure.

Acknowledgments

The authors would like to thank anonymous reviewers for their comments and suggestions to improve the readability of manuscript.

REFERENCES

[1] Agrawal, M., Kayal, N. and Saxena, N., “PRIMES is in P,” Ann. of Math. (2), 160: 781–793 (2004).
[2] Boneh, D., “The Decision Diffie-Hellman Problem,” Algorithmic Number Theory, LNCS, 1423: 48–63 (1998).
[3] Bagherzandi, A., Jarecki, S., Lu, Y. and Saxena, N., Password-Protected Secret Sharing, preprint (2011).
[4] Bagherzandi, A., Jarecki, S., Saxena, N. and Lu, Y., “Password-Protected Secret Sharing,” Proc. CCS’11, 433–444 (2011).
[5] ElGamal, T., “A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,” IEEE Trans. on Inform. Theory, 31: 469–472 (1985).
[6] Fouque, P. A., and Pointcheval, D., “Threshold Cryptosystems Secure against Chosen-Ciphertext Attacks,” ASIACRYPT’01, LNCS, 2248: 352–368 (2001).
[7] Hasegawa, S., Isobe, S., Iwazaki, J., Koizumi, E. and Shizuya, H., “A Strengthened Security Notion for Password-Protected Secret Sharing Schemes,” IEICE Trans. Fundamentals, 98-A: 203–212 (2015).
[8] Shamir, A., “How to Share a Secret,” Commun. ACM, 22: 612–613 (1979).