Interdisciplinary Information Sciences Vol. 22, No. 1 (2016) 31–55
©Graduate School of Information Sciences, Tohoku University
ISSN 1340-9050 print/1347-6157 online
DOI 10.4036/iis.2015.R.04

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

Shingo HASEGAWA[1], Shuji ISOBE[1], Jun-ya IWAZAKI[1,2,*], Eisuke KOIZUMI[1] and Hiroki SHIZUYA[1]

[1]*Graduate School of Information Sciences, Tohoku University, Sendai 980-8576, Japan*
[2]*Presently, 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 PPSS_2 which has the following three properties: (**i**) PPSS_2 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 if some servers are corrupted, (**ii**) the user can be authenticated with a single password by all the servers, and (**iii**) there is no useful information about the password and the document in the interaction.

We now see more on the security notion for PPSS schemes formulated in [4]. They focused on the interaction between the user and the servers, and defined a security notion which we call the PPSS-security (Definition 2.3). A PPSS protocol is PPSS-secure if no polynomial time 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 PPSS_2 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 PPSS_2 is not pparam-secure. Then they proposed an enhanced protocol ePPSS_2 (a.k.a. "Protocol 1" in this paper) of PPSS_2, 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 ePPSS_2 is PPSS-secure. The proof is similar to that of Theorem 1 in [4] since ePPSS_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 ePPSS_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 ePPSS_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 Δ 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 Δ. In particular, if $\Delta = U_A$, the uniform distribution over A, then we write $x \in_r A$ instead of $x \in U_A$. $\mathbb{N}$ and $\mathbb{Z}$ denote the set of the natural numbers and the ring of the rational integers, respectively. For any $n \in \mathbb{N}$, 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 $\mathsf{SS}_{t,n}$ 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 $\mathbb{G}_q$ denote the subgroup of $\mathbb{Z}_Q^*$ of order q. We define

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

and

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

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

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

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

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

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

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

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

holds for any k and any probabilistic Turing machine $\mathcal{M}$ whose running time is at most T_{cdh}, where $(Q, g) = \mathsf{Gen}(1^k)$ and $a, b \in \mathbb{Z}_q$. 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 state the relationship between the DDH and CDH problems.

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

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

$$\Pr[\mathcal{M}(Q, g, g^a, g^b) = g^{ab}] \geq \varepsilon_{\mathrm{ddh}} + \frac{1}{2^{k_0}}$$

holds for some k_0, where $(Q, g) = \mathsf{Gen}(1^{k_0})$ 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 $(Q, g) = \mathsf{Gen}(1^{k_0})$, then we have

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

and

$$\begin{aligned}\Pr_{w\in \widetilde{\mathrm{DH}}}[\mathcal{A}(w) = 1] &= \Pr_{w\in \widetilde{\mathrm{DH}}}[\mathcal{M}(Q, g, g_1, g_2) = g_3] = \sum_{g'\in\mathbb{G}_q} \Pr_{w\in \widetilde{\mathrm{DH}}}[\mathcal{M}(Q, g, g_1, g_2) = g_3 \wedge g_3 = g'] \\ &= \sum_{g'\in\mathbb{G}_q} \Pr_{w\in \widetilde{\mathrm{DH}}}[\mathcal{M}(Q, g, g_1, g_2) = g_3 \mid g_3 = g'] \Pr_{w\in \widetilde{\mathrm{DH}}}[g_3 = g'] = \frac{1}{q} \sum_{g'\in\mathbb{G}_q} \Pr_{w\in \widetilde{\mathrm{DH}}}[\mathcal{M}(Q, g, g_1, g_2) = g'] = \frac{1}{q}.\end{aligned}$$

Hence, we have

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

This implies that the DDH problem is not $(T_{\mathrm{ddh}}, \varepsilon_{\mathrm{ddh}})$-hard, and the lemma follows. □

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

A proof π is said to be valid if π is correct. If π is not correct, then π 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 $\beta \in_r \{1, 2\}$.

(2) $\mathcal{A}$ is allowed to access a random oracle. If $\mathcal{A}$ queries any instance σ, 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" $\pi = \mathcal{S}(\mathcal{L})(x)$, where $\mathcal{S}(\mathcal{L})$ 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 σ, then $\mathcal{C}$ answers a hash value $H(\sigma)$.

(3) $\mathcal{A}$ is allowed to access a simulator $\mathcal{S}(\mathcal{L})$. If $\mathcal{A}$ queries any instance x, then $\mathcal{C}$ answers a simulated proof $\pi = \mathcal{S}(\mathcal{L})(x)$, and sets $S = S \cup \{(x, \pi)\}$.

(4) $\mathcal{A}$ sends a pair (x^*, π^*) of an instance x^* and a proof π^* 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 $(T_S, q_P^S, q_H^S, \varepsilon_{\mathrm{ZK}}, \varepsilon_{\mathrm{SS}})$-SS-NIZK if there exists a simulator algorithm $\mathcal{S}(\mathcal{L})$ 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 $\mathcal{S}(\mathcal{L})$) at most q_H^S and q_P^S times, respectively.

(3) In **Game ZK**, the following inequality holds for any adversary $\mathcal{A}$:

$$|\Pr[\tilde{\beta} = 1|\beta = 1] - \Pr[\tilde{\beta} = 1|\beta = 2]| < \varepsilon_{\mathrm{ZK}}.$$

(4) In Step (4) of **Game SS**, the probability that $\mathcal{A}$ outputs (x^*, π^*) which satisfies the following conditions is at most $\varepsilon_{\mathrm{SS}}$: **(i)** $(x^*, \pi^*) \notin S$, **(ii)** $x^* \notin \mathcal{L}$, and **(iii)** π^* 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 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 λ specifies the following items:

- a set PW_λ of all passwords;
- a set Doc_λ of all documents;
- a set Pub_λ of all public parameters;
- a set Sec_λ 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 ζ since Setup is a PPT algorithm.

For the PPSS scheme, the following three items are designated in addition to the algorithm Setup:

- Init: This is the initialization algorithm that takes a tuple (λ, p, d) of a setup parameter λ, a password $p \in \mathsf{PW}_\lambda$ and a secret document $d \in \mathsf{Doc}_\lambda$ as an input, and outputs a pair (pub, sec) of a public parameter
$$\mathrm{pub} = (\mathrm{pub}_1, \mathrm{pub}_2, \mathrm{pub}_3) = (\mathrm{pub}_1(\lambda), \mathrm{pub}_2(\mathrm{pub}_1(\lambda), p), \mathrm{pub}_3(\mathrm{pub}_1(\lambda), d)) \in \mathsf{Pub}_\lambda$$
and a set $\mathrm{sec} = \{\mathrm{sec}_j\}_{j=1}^n$ of the seeds of the shares, where $\mathrm{sec}_j \in \mathsf{Sec}_\lambda$ denotes the seed stored with the j-th server. We assume that Init is a PPT algorithm.
- User and $\mathsf{Server} = \{\mathsf{Server}_j\}_{j=1}^n$: The algorithms User and Server_j are PPT algorithms, and they are employed by the user and the j-th server, respectively. The user's algorithm User interacts with the server's algorithm Server_j for each j. At first, User is given a tuple $(\lambda, p, \mathrm{pub})$ of a setup parameter λ, a password $p \in \mathsf{PW}_\lambda$ and a public parameter pub as an input, and the algorithm Server_j for each j is given a tuple $(\lambda, \mathrm{pub}, \mathrm{sec}_j)$ of a setup parameter λ, a public parameter pub and a seed $\mathrm{sec}_j \in \mathsf{Sec}_\lambda$. Interacting with the n servers, User eventually outputs either a document d' or $\perp$, where $\perp$ denotes that User has failed to recover the secret document d.

We write $\mathcal{P} = (\mathsf{Setup}, \mathsf{Init}, \mathsf{User}, \mathsf{Server})$ to denote a PPSS scheme. For a PPSS scheme $\mathcal{P}$ and $\tilde{p} \in \mathsf{PW}_\lambda$, the output of User is denoted by $\mathcal{P}(\tilde{p}, (\mathrm{pub}, \{\mathrm{sec}_j\}_{j=1}^n))$ on an input $(\lambda, \tilde{p}, \mathrm{pub})$, where $(\mathrm{pub}, \{\mathrm{sec}_j\}_{j=1}^n) = \mathsf{Init}(p, d)$ for some $p \in \mathsf{PW}_\lambda$ and $d \in \mathsf{Doc}_\lambda$. A PPSS scheme $\mathcal{P}$ is valid if $\mathcal{P}(p, \mathsf{Init}(\lambda, p, d)) = d$ holds for any $\lambda \in \Lambda(k)$, $p \in \mathsf{PW}_\lambda$ and $d \in \mathsf{Doc}_\lambda$. 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 $\mathcal{P} = (\mathsf{Setup}, \mathsf{Init}, \mathsf{User}, \mathsf{Server})$ be a PPSS scheme. Then a PPSS adversarial game for $\mathcal{P}$ between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ is defined as follows:

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

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

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

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

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

(1) $\mathcal{A}$ chooses two documents d_1 and d_2, and
(2) $\mathcal{C}$ chooses β,

where the probability is taken over random tapes of $\mathcal{A}$ and $\mathcal{C}$.

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

$$|P(d_1; d_1, d_2) - P(d_2; d_1, d_2)| \leq \left\lfloor \frac{q_S}{t - t'} \right\rfloor \cdot \frac{1}{\#\mathsf{PW}_\lambda} + \varepsilon$$

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, and
(4) $\mathcal{A}$ is allowed to enter Server's query phase at most q_S times.

2.5 Another security notion for PPSS schemes: pparam-security

We state another PPSS security notion called 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 λ. Then $\mathcal{C}$ sends λ to $\mathcal{A}$. $\mathcal{A}$ chooses two documents $d_1, d_2 \in \mathsf{Doc}_\lambda$, and sends them to $\mathcal{C}$. $\mathcal{C}$ chooses $\beta \in_r \{1, 2\}$. Then $\mathcal{C}$ executes Init on an input (λ, p, d_β), and gets a pair $(\mathrm{pub}, \mathrm{sec})$, where $\mathrm{pub} = (\mathrm{pub}_1, \mathrm{pub}_2, \mathrm{pub}_3)$. Finally, $\mathcal{C}$ sends the public parameter pub to $\mathcal{A}$.

Attack phase: $\mathcal{A}$ is allowed to interact with $\mathcal{C}$. In each interaction, $\mathcal{A}$ sends a public parameter $\mathrm{pub}' = (\mathrm{pub}'_1, \mathrm{pub}'_2, \mathrm{pub}'_3) \in \mathsf{Pub}_\lambda$ to $\mathcal{C}$. $\mathcal{C}$ plays the role in computing the "inverse" of the initialization algorithm if $\mathrm{pub}_1 = \mathrm{pub}'_1$ and $\mathrm{pub}_3 \neq \mathrm{pub}'_3$. Then $\mathcal{C}$ returns a document $d \in \mathsf{Doc}_\lambda$ which satisfies $\mathsf{Init}(\lambda, p, d) = (\mathrm{pub}', \mathrm{sec}')$ for some $p \in \mathsf{PW}_\lambda$ and $\mathrm{sec}' \in \mathsf{Sec}_\lambda$. 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 $P^{\beta}_{\text{pparam-atk}}(k)$ denote the probability that $\mathcal{A}$ sends 1 in Challenge phase of the pparam-attack game under the condition that $\mathcal{C}$ chooses β 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 $\mathrm{Adv}_{\mathcal{A}}(k)$ by

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

Definition 2.4 ([7]). A PPSS scheme $\mathcal{P}$ is (T, ε, q_A)-pparam-secure if for any security parameter k and any adversary $\mathcal{A}$, $\mathrm{Adv}_{\mathcal{A}}(k) < \varepsilon$ holds under the following conditions:

(1) $\mathcal{A}$ is allowed to enter Attack phase at most q_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 ePPSS_2 and Main Theorem

We depict a protocol ePPSS_2, in Protocol 1: the proof systems $(\mathcal{P}(\mathcal{L}^{\mathrm{pub}}_{S1}), \mathcal{V}(\mathcal{L}^{\mathrm{pub}}_{S1}))$ and $(\mathcal{P}(\mathcal{L}^{\mathrm{pub}}_{U}), \mathcal{V}(\mathcal{L}^{\mathrm{pub}}_{U}))$ are given in [4], and $(\mathcal{P}(\mathcal{L}^{\mathrm{pub}}_{S2}), \mathcal{V}(\mathcal{L}^{\mathrm{pub}}_{S2}))$ is given in [7]. In [4], they stated that, for any given q^S_P and q^S_H, these systems are $(T_S, q^S_P, q^S_H, \varepsilon_{\mathrm{ZK}}, \varepsilon_{\mathrm{SS}})$-SS-NIZK, where $\varepsilon_{\mathrm{ZK}} = q^S_P q^S_H / q$, $\varepsilon_{\mathrm{SS}} = q^S_H / q$ and T_S is the same as the running time of the corresponding prover. The non-interactive proof system $(\mathcal{P}(\mathcal{L}^{\mathrm{pub}}_{E}), \mathcal{V}(\mathcal{L}^{\mathrm{pub}}_{E}))$ is similarly defined (see also [6]).

The protocol 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 π is added in the public parameter.
(3) The verification process of the proof π is added in Step $\mathbf{S_j 1\text{-}1}$.

It was shown that ePPSS_2 is pparam-secure in [7]. Our main result is as follows:

Theorem. *Assume that the following properties hold:*

- *the* DDH *problem is* $(T_{\mathrm{ddh}}, \varepsilon_{\mathrm{ddh}})$*-hard,*
- *the proof systems* $(\mathcal{P}(\mathcal{L}^{\mathrm{pub}}_{S1}), \mathcal{V}(\mathcal{L}^{\mathrm{pub}}_{S1}))$, $(\mathcal{P}(\mathcal{L}^{\mathrm{pub}}_{U}), \mathcal{V}(\mathcal{L}^{\mathrm{pub}}_{U}))$ *and* $(\mathcal{P}(\mathcal{L}^{\mathrm{pub},j}_{S2}), \mathcal{V}(\mathcal{L}^{\mathrm{pub},j}_{S2}))$ *are* $(T_S, q^S_P, q^S_H, \varepsilon_{\mathrm{SS}}, \varepsilon_{\mathrm{ZK}})$*-SS-NIZK, and*
- *the proof system* $(\mathcal{P}(\mathcal{L}^{\mathrm{pub}}_{E}), \mathcal{V}(\mathcal{L}^{\mathrm{pub}}_{E}))$ *is* $(T_S, 1, q^S_H, \varepsilon_{\mathrm{SS}}, \varepsilon_{\mathrm{ZK}})$*-SS-NIZK.*

The setup algorithm Setup:

1: Input 1^k.

2: Run Gen on input 1^k, and get a pair (Q, g).

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

The initialization algorithm Init:

I1: Input a tuple (λ, p, d), where $\lambda = (q, g, t, n)$ is a setup parameter output by Setup, $p \in \mathbb{Z}_q = \mathsf{PW}_\lambda$ and $d \in \mathbb{G}_q = \mathsf{Doc}_\lambda$.

I2: Choose $x_1, x_2 \in_r \mathbb{Z}_q$, and compute $y_1 = g^{x_1}$, $y_2 = g^{x_2}$, $\{x_{1,j}\}_{j=1}^n = \mathsf{SS}_{t,n}(x_1)$ and $\{x_{2,j}\}_{j=1}^n = \mathsf{SS}_{t,n}(x_2)$.

I3: Choose $h, \hat{g}, \hat{h}, \hat{y}, \bar{g} \in_r \mathbb{G}_q$ and $r_p, r_{1,d}, r_{2,d} \in_r \mathbb{Z}_q$.

I4: Compute $u_p = g^{r_p}$, $v_p = y_1^{r_p} h^p$, $u_{1,d} = g^{r_{1,d}}$, $u_{2,d} = g^{r_{2,d}}$, $v_{1,d} = y_1^{r_{1,d}} d$ and $v_{2,d} = y_2^{r_{2,d}} d$.

I5: Choose $r_{1,j}, r_{2,j} \in_r \mathbb{Z}_q$, and compute $y_{1,j} = g^{x_{1,j}} h^{r_{1,j}}$ and $y_{2,j} = g^{x_{2,j}} h^{r_{2,j}}$ for each $j \in [n]$.

I6: Run $\mathcal{P}(\mathcal{L}_E^{\text{pub}})$ 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 π.

I7: Set $\text{pub}_1 = (g, y_1, y_2, h, \{y_{1,j}\}_{j=1}^n, \{y_{2,j}\}_{j=1}^n, \hat{g}, \hat{h}, \hat{y}, \bar{g})$, $\text{pub}_2 = (u_p, v_p)$, $\text{pub}_3 = (u_{1,d}, v_{1,d}, u_{2,d}, v_{2,d})$ and $\text{sec}_j = (x_{1,j}, r_{1,j}, x_{2,j}, r_{2,j})$ for each $j \in [n]$, and output $(\text{pub}, \text{sec}) = ((\text{pub}_1, \text{pub}_2, \text{pub}_3, \pi), \{\text{sec}_j\}_{j=1}^n)$.

The interaction between the user algorithm User and the server algorithms $\mathsf{Server}_1, \ldots, \mathsf{Server}_n$:

- User's input is a tuple $(\lambda, \text{pub}, \tilde{p})$, where $\tilde{p} \in \mathbb{Z}_q = \mathsf{PW}_\lambda$.
- For each j, Server_j's input is a tuple $(\lambda, \text{pub}, \text{sec}_j)$.

U and $\mathbf{S_j}$ are the same as those of PPSS_2.

$\mathbf{S_j}$**1-1:** If π is invalid, then halt.

$\mathbf{S_j}$**1-2:** Choose $t_j \in_r \mathbb{Z}_q$, and compute $a_j = g^{t_j}$, $b_j = u_p^{t_j}$ and $\bar{a}_j = (\bar{g})^{t_j}$.

$\mathbf{S_j}$**1-3:** Run $\mathcal{P}(\mathcal{L}_{S1}^{\text{pub}})$ on an input $((a_j, b_j, \bar{a}_j), t_j)$, and get a proof $\pi_{1,j}$.

$\mathbf{S_j}$**1-4:** Send a tuple $(a_j, b_j, \bar{a}_j, \pi_{1,j})$ to User.

U1-1: Choose a subset $V \subseteq [n]$ with $\#V = t$.

U1-2: If $\pi_{1,j}$ is invalid for some $j \in V$, then halt.

U1-3: Choose $r_{\tilde{p}} \in_r \mathbb{Z}_q$, and compute $u_{\tilde{p}} = g^{r_{\tilde{p}}}$, $v_{\tilde{p}} = y_1^{r_{\tilde{p}}} h^{\tilde{p}}$, $\hat{u}_{\tilde{p}} = (\hat{g})^{r_{\tilde{p}}}$ and $\hat{v}_{\tilde{p}} = (\hat{y})^{r_{\tilde{p}}} (\hat{h})^{\tilde{p}}$.

U1-4: Compute $e_j = (a_j)^{r_{\tilde{p}}}$ for each $j \in [n]$.

U1-5: Compute $u = \prod_{j \in V} (b_j / e_j)$.

U1-6: Run $\mathcal{P}(\mathcal{L}_U^{\text{pub}})$ on an input $((a_j, e_j, u_{\tilde{p}}, v_{\tilde{p}}, \hat{u}_{\tilde{p}}, \hat{v}_{\tilde{p}}), r_{\tilde{p}}, \tilde{p})$, and get a proof $\pi_{2,j}$.

U1-7: Send a tuple $(V, u, e_j, u_{\tilde{p}}, v_{\tilde{p}}, \hat{u}_{\tilde{p}}, \hat{v}_{\tilde{p}}, \pi_{2,j})$ to Server_j for each $j \in [n]$.

$\mathbf{S_j}$**2-1:** If $j \notin V$ or $\pi_{2,j}$ is invalid, then halt.

$\mathbf{S_j}$**2-2:** Compute $w_j = (u_{1,d} u)^{\lambda_j x_{1,j}}$, where

$$\lambda_j = \prod_{\ell \in V \setminus \{j\}} \frac{-\ell}{j - \ell} \bmod q.$$

$\mathbf{S_j}$**2-3:** Compute $v_j = (v_p / v_{\tilde{p}})^{t_j}$.

$\mathbf{S_j}$**2-4:** Compute $z_j = v_j / w_j$.

$\mathbf{S_j}$**2-5:** Choose $r_{z_j} \in \mathbb{Z}_q$, and compute $u_{z_j} = g^{r_{z_j}}$ and $v_{z_j} = (u_{\tilde{p}})^{r_{z_j}} z_j$.

$\mathbf{S_j}$**2-6:** Run $\mathcal{P}(\mathcal{L}_{S2}^{\text{pub},j})$ on an input $((u_{z_j}, v_{z_j}, u_{\tilde{p}}, a_j, v_p / v_{\tilde{p}}, (u_{1,d} u)^{\lambda_j}), r_{z_j}, t_j, x_{1,j}, r_{1,j})$, and get a proof $\pi_{3,j}$.

$\mathbf{S_j}$**2-7:** Send a tuple $((u_{z_j}, v_{z_j}), \pi_{3,j})$ to User.

U2-1: If $\pi_{3,j}$ is invalid for some $j \in V$, then halt.

U2-2: Compute $d' = v_{1,d} (\prod_{j \in V} v_{z_j} / (\prod_{j \in V} u_{z_j})^{r_{\tilde{p}}})$, and output d'.

The languages $\mathcal{L}_{S1}^{\text{pub}}$, $\mathcal{L}_U^{\text{pub}}$, $\mathcal{L}_{S2}^{\text{pub},j}$ and $\mathcal{L}_E^{\text{pub}}$ are defined as follows:

$$\mathcal{L}_{S1}^{\text{pub}} = \{(a_j, b_j, \bar{a}_j) \in \mathbb{G}_q^3 \mid \exists t_j \in \mathbb{Z}_q \text{ s.t. } (a_j, b_j, \bar{a}_j) = (g^{t_j}, (u_p)^{t_j}, (\bar{g})^{t_j})\},$$

$$\mathcal{L}_U^{\text{pub}} = \{(a_j, e_j, u_{\tilde{p}}, v_{\tilde{p}}, \hat{u}_{\tilde{p}}, \hat{v}_{\tilde{p}}) \in \mathbb{G}_q^6 \mid \exists (r_{\tilde{p}}, \tilde{p}) \in \mathbb{Z}_q^2 \text{ s.t. } (e_j, u_{\tilde{p}}, v_{\tilde{p}}, \hat{u}_{\tilde{p}}, \hat{v}_{\tilde{p}}) = (a_j^{r_{\tilde{p}}}, g^{r_{\tilde{p}}}, y^{r_{\tilde{p}}} h^{\tilde{p}}, (\hat{g})^{r_{\tilde{p}}}, (\hat{y})^{r_{\tilde{p}}} (\hat{h}^{\tilde{p}})\},$$

$$\begin{aligned} \mathcal{L}_{S2}^{\text{pub},j} = \{&(u_{z_j}, v_{z_j}, u_{\tilde{p}}, a_j, v_p / v_{\tilde{p}}, (u_d u)^{\lambda_j}) \in \mathbb{G}_q^6 \mid \exists (r_{z_j}, t_j, x_j, r_j) \in \mathbb{Z}_q^4 \\ &\text{s.t. } (y_j, a_j, u_{z_j}, v_{z_j}) = (g^{x_j} h^{r_j}, g^{t_j}, g^{r_{z_j}}, (u_{\tilde{p}})^{r_{z_j}} (v_p / v_{\tilde{p}})^{t_j} (u_d u)^{-\lambda_j x_j})\} \end{aligned}$$

and

$$\mathcal{L}_E^{\text{pub}} = \{(u_{1,d}, v_{1,d}, u_{2,d}, v_{2,d}) \in \mathbb{G}_q^4 \mid \exists (r_{1,d}, r_{2,d}) \in \mathbb{Z}_q^2 \text{ s.t. } u_{1,d} = g^{r_{1,d}}, u_{2,d} = g^{r_{2,d}}, v_{1,d} / v_{2,d} = y_1^{r_{1,d}} / y_2^{r_{2,d}}\}.$$

Protocol 1. The protocol ePPSS_2

Then the protocol ePPSS_2 *is* $(q_U, q_S, T, \varepsilon)$*-PPSS-secure, where* $\max\{nq_U, q_S\} \leq q_P^S, q_H^S$,

$$T \leq T_{\mathrm{ddh}} - 4T_S - q_U f^U - q_S f^S - f^I$$

for some polynomials f^U, f^S *and* f^I *in* n, t *and* k, *and*

$$\varepsilon \leq 8\varepsilon_{\mathrm{ZK}} + (4nq_Uq_S + 6nq_U - 4nq_S + 6q_S)\varepsilon_{\mathrm{SS}} + (2q_Uq_S + 3q_U + 2q_S + 7)\varepsilon_{\mathrm{ddh}} + q_Uq_S\omega_1 + q_U\omega_2 + q_S\omega_3 + \omega_4,$$

where ω_1, ω_2, ω_3 *and* ω_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 ePPSS_2.
The interaction between the user algorithm User and the server algorithms $\mathsf{Server}_1, \ldots, \mathsf{Server}_n$:

- User's input is a tuple $(\lambda, \mathrm{pub}, \tilde{p})$, where $\tilde{p} \in \mathbb{Z}_q = \mathsf{PW}_\lambda$.
- For each j, Server_j's input is a tuple $(\lambda, \mathrm{pub}, \mathrm{sec}_j)$.

U and $\mathbf{S_j}$ are the same as those of PPSS_2.
U1-1: Choose a subset $V \subseteq [n]$ with $\#V = t$.
U1-2: Send V to Server_j for each $j \in [n]$.

$\mathbf{S_j1}$**:** If π is invalid, then halt.
$\mathbf{S_j2}$**:** If $j \in V$, then send the secret $x_{1,j}$ to User. Otherwise, halt.

U2-1: Compute $x'_1 = \Sigma_{j \in V} x_{1,j}\lambda_j$, where λ_j is defined in Step $\mathbf{S_j2\text{-}2}$ of the protocol ePPSS_2.
U2-2: Compute $d' = v_{1,d}/(u_{1,d})^{x'_1}$, 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* PPSS_2 *is* $(T, \varepsilon, 0)$*-pparam-secure, and*
- *the proof system* $(\mathcal{P}(\mathcal{L}_E^{\mathrm{pub}}), \mathcal{V}(\mathcal{L}_E^{\mathrm{pub}}))$ *is* $(T_S, 1, q_H^S, \varepsilon_{\mathrm{ZK}}, \varepsilon_{\mathrm{SS}})$*-SS-NIZK.*

Then Protocol 2 is (T', ε', q_A)*-pparam-secure, where*

$$T' \leq T - T_S - q_A f_A, \ q_A \leq q_H^S \quad \text{and} \quad \varepsilon' \leq 2\varepsilon + 6\varepsilon_{\mathrm{SS}}$$

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 $\mathcal{A}$ 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, $\mathcal{A}$ receives another subset $\{x_{1,j}\}_{j \in V_0}$ 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 $\{x_{1,j}\}_{V_0 \cup V'}$ of secret seeds, $\mathcal{A}$ 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 $\mathcal{A}$ and ε' is any positive number which satisfies $1 > 1/\#\mathsf{PW}_\lambda + \varepsilon'$. □

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 $\mathcal{A}$ be a probabilistic machine followed by an adversary of the PPSS adversarial game for ePPSS_2. Assume that the running time of $\mathcal{A}$ is T. Using the adversary $\mathcal{A}$, we define sequences of games $\{\mathbf{Game}(\mu, \nu)\}_{\mu,\nu}$ and $\{\mathbf{Game}(\mu, \nu, \xi)\}_{\mu,\nu,\xi}$. Let $(Q, g) = \mathsf{Gen}(1^k)$. We first depict the game $\mathbf{Game}(0, 0)$ in Protocol 3. This game models the real PPSS adversarial game for ePPSS_2 with the exception that the real proofs constructed in ePPSS_2 are replaced by the simulated proofs and that Output phase is added. We convert the game $\mathbf{Game}(0, 0)$ so that the game does not depend on the document d and the password p.

Initialization phase

I0: Set $C_U = C_S = C_F = 0$, $\mathrm{F} = \text{false}$ and $\text{Upset} = \text{Idset} = \emptyset$.

I1: Choose $n, t \in \mathbb{N}$ with $n \geq t$, and send a tuple (q, g, n, t) to $\mathcal{A}$, where $q = (Q-1)/2$.

I2: If $\mathcal{A}$ sends two documents $d_1, d_2 \in \mathbb{G}_q$ and a subset $V' \subseteq [n]$ with $\#V' = t' < t$, then choose $\beta \in_r \{1, 2\}$.

I3: Choose $x_1, x_2 \in_r \mathbb{Z}_q$, and compute $y_1 = g^{x_1}$, $y_2 = g^{x_2}$, $\{x_{1,j}\}_{j=1}^{n} = \mathsf{SS}_{t,n}(x_1)$ and $\{x_{2,j}\}_{j=1}^{n} = \mathsf{SS}_{t,n}(x_2)$.

I4: Choose $h, \hat{g}, \hat{h}, \hat{y}, \bar{g} \in_r \mathbb{G}_q$ and $r_p, r_{1,d}, r_{2,d} \in_r \mathbb{Z}_q$.

I5: Choose a password $p \in_r \mathbb{Z}_q$, and compute $u_p = g^{r_p}$ and $v_p = y_1^{r_p} h^p$.

I6: Compute $(u_{1,d}, v_{1,d}) = (g^{r_{1,d}}, y_1^{r_{1,d}} d_\beta)$ and $(u_{2,d}, v_{2,d}) = (g^{r_{2,d}}, y_2^{r_{2,d}} d_\beta)$.

I7: Choose $r_{1,j}, r_{2,j} \in_r \mathbb{Z}_q$, and compute $y_{1,j} = g^{x_{1,j}} h^{r_{1,j}}$ and $y_{2,j} = g^{x_{2,j}} h^{r_{2,j}}$ for each $j \in [n]$.

I8: Run the simulator $\mathcal{S}(\mathcal{L}_E^{\mathrm{pub}})$ on an input $(u_{1,d}, v_{1,d}, u_{2,d}, v_{2,d})$, and get a proof π.

I9: Set $\mathrm{pub}_1 = (g, y_1, y_2, h, \{y_{1,j}\}_{j=1}^{n}, \{y_{2,j}\}_{j=1}^{n}, \hat{g}, \hat{h}, \hat{y}, \bar{g})$, $\mathrm{pub}_2 = (u_p, v_p)$, $\mathrm{pub}_3 = ((u_{1,d}, v_{1,d}), (u_{2,d}, v_{2,d}), \pi)$ and $\mathrm{sec}_j = (x_{1,j}, r_{1,j}, x_{2,j}, r_{2,j})$ for each $j \in [n]$, and send $(\mathrm{pub}, \mathrm{sec}_{V'}) = ((\mathrm{pub}_1, \mathrm{pub}_2, \mathrm{pub}_3), \{\mathrm{sec}_j\}_{j \in V'})$.

User's query phase

If $\mathcal{A}$ enters User's query phase with n-tuple $\{(j, a_j, b_j, \bar{a}_j, \pi_{1,j})\}_{j \in [n]}$, then execute the following procedure:

U1-0: Set $C_U = C_U + 1$.

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 $r_{\tilde{p}} \in_r \mathbb{Z}_q$, and compute $u_{\tilde{p}} = g^{r_{\tilde{p}}}$, $v_{\tilde{p}} = y_1^{r_{\tilde{p}}} h^p$, $\hat{u}_{\tilde{p}} = (\hat{g})^{r_{\tilde{p}}}$ and $\hat{v}_{\tilde{p}} = (\hat{y})^{r_{\tilde{p}}} (\hat{h})^p$.

U1-4: Set $u_{\tilde{p}}(C_U) = u_{\tilde{p}}$ and $\text{Upset} = \text{Upset} \cup \{u_{\tilde{p}}(C_U)\}$.

U1-5: Compute $e_j = (a_j)^{r_{\tilde{p}}}$ for each $j \in [n]$.

U1-6: Compute $u = \prod_{j \in V} (b_j / e_j)$.

U1-7: Run the simulator $\mathcal{S}(\mathcal{L}_U^{\mathrm{pub}})$ on an input tuple $(a_j, e_j, u_{\tilde{p}}, v_{\tilde{p}}, \hat{u}_{\tilde{p}}, \hat{v}_{\tilde{p}})$, and get a proof $\pi_{2,j}$ for each $j \in [n]$.

U1-8: Send $(V, u, e_j, u_{\tilde{p}}, v_{\tilde{p}}, \hat{u}_{\tilde{p}}, \hat{v}_{\tilde{p}}, \pi_{2,j})$ for each $j \in [n]$.

If $\mathcal{A}$ returns a tuple $\{(u_{z_j}, v_{z_j}, \pi_{3,j})\}_{j \in V}$, then execute the following procedure:

U2-1: If $\pi_{3,j}$ is invalid for some $j \in V$, then halt.

U2-2: Compute $d' = v_{1,d} (\prod_{j \in V} v_{z_j} / (\prod_{j \in V} u_{z_j})^{r_{\tilde{p}}})$, 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:

S$_\mathbf{j}$1-0: Set $C_S = C_S + 1$.

S$_\mathbf{j}$1-1: If π is invalid, then halt.

S$_\mathbf{j}$1-2: Choose $t_j \in_r \mathbb{Z}_q$, and compute $a_j = g^{t_j}$, $b_j = u_p^{t_j}$ and $\bar{a}_j = (\bar{g})^{t_j}$.

S$_\mathbf{j}$1-3: Run the simulator $\mathcal{S}(\mathcal{L}_{S1}^{\mathrm{pub}})$ on an input $(a_j, b_j, \bar{a}_j)$ and get a proof $\pi_{1,j}$.

S$_\mathbf{j}$1-4: Send a tuple $(j, a_j, b_j, \bar{a}_j, \pi_{1,j})$.

If $\mathcal{A}$ returns a tuple $(V, u, e_j, u_{\tilde{p}}, v_{\tilde{p}}, \hat{u}_{\tilde{p}}, \hat{v}_{\tilde{p}}, \pi_{2,j})$, then execute the following procedure:

S$_\mathbf{j}$2-1: If $j \notin V$ or $\pi_{2,j}$ is invalid, then halt.

S$_\mathbf{j}$2-2: If $\hat{v}_{\tilde{p}} / (\hat{u}_{\tilde{p}})^{\hat{x}} = \hat{h}^p$, then $\text{Idset} = \text{Idset} \cup \{j\}$. If $\#\text{Idset} \geq t - t'$, then set $\mathrm{F} = \text{true}$.

S$_\mathbf{j}$2-3: Compute $w_j = (u_{1,d} u)^{\lambda_j x_{1,j}}$, where λ_j is defined in Step **S$_\mathbf{j}$2-2** of the protocol ePPSS_2.

S$_\mathbf{j}$2-4: Compute $v_j = (v_p / v_{\tilde{p}})^{t_j}$.

S$_\mathbf{j}$2-5: Compute $z_j = v_j / w_j$.

S$_\mathbf{j}$2-6: Choose $r_{z_j} \in \mathbb{Z}_q$, and compute $u_{z_j} = g^{r_{z_j}}$ and $v_{z_j} = (u_{\tilde{p}})^{r_{z_j}} z_j$.

S$_\mathbf{j}$2-7: Run the simulator $\mathcal{S}(\mathcal{L}_{S2}^{\mathrm{pub},j})$ on an input $(u_{z_j}, v_{z_j}, u_{\tilde{p}}, a_j, v_p / v_{\tilde{p}}, (u_{1,d} u)^{\lambda_j})$, and get a proof $\pi_{3,j}$.

S$_\mathbf{j}$2-8: Send $(u_{z_j}, v_{z_j}, \pi_{3,j})$.

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 β in Step **I2** of Initialization phase.

(ii) Output ψ set in Output phase.

Let $E_{0,0,d_\beta}$ be the event that the adversary $\mathcal{A}$ outputs 1, and let $\varphi_{0,0}^{\beta}$ be the output of $\mathcal{M}_{0,0}^{\beta}$.

We similarly define probabilistic machines $\mathcal{M}_{\mu,\nu}^{\beta}$ and $\mathcal{M}_{\mu,\nu,\xi}^{\beta}$, events E_{μ,ν,d_β} and E_{μ,ν,ξ,d_β}, and outputs $\varphi_{\mu,\nu}^{\beta}$ and $\varphi_{\mu,\nu,\xi}^{\beta}$. We set $p_{\mu,\nu}(d_\beta) = \Pr[E_{\mu,\nu,d_\beta}]$ and $p_{\mu,\nu,\xi}(d_\beta) = \Pr[E_{\mu,\nu,\xi,d_\beta}]$.

We note the following facts: in **Game**$(0, 0)$,

(1) in Initialization phase, the challenger queries $\mathcal{S}(\mathcal{L}_E^{\mathrm{pub}})$ one time in order to make a proof π.

(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 $\{\pi_{3,j}\}_{j \in V}$, respectively.

- the challenger queries $\mathcal{S}(\mathcal{L}_U^{\mathrm{pub}})$ n times in order to make proofs $\{\pi_{2,j}\}_{j\in[n]}$.

(3) When $\mathcal{A}$ enters Server's query phase,

- $\mathcal{A}$ queries the random oracles at most one time in order to make a proof $\pi_{2,j}$.
- the challenger queries $\mathcal{S}(\mathcal{L}_{S1}^{\mathrm{pub}})$ and $\mathcal{S}(\mathcal{L}_{S2}^{\mathrm{pub},j})$ one time in order to make proofs $\pi_{1,j}$ and $\pi_{3,j}$, respectively.

We also note that $\varphi_{0,0}^{\beta}$ 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 $\mathcal{S}(\mathcal{L}_E^{\mathrm{pub}})$, $\mathcal{S}(\mathcal{L}_{S1}^{\mathrm{pub}})$, $\mathcal{S}(\mathcal{L}_U^{\mathrm{pub}})$ and $\mathcal{S}(\mathcal{L}_{S2}^{\mathrm{pub},j})$ used in $\mathcal{M}_{0,0}^{\beta}(w)$ are at most T_S and $\max\{nq_U, q_S\} \le q_P^S, q_H^S$ holds, then we have

$$|P(d_\beta; d_1, d_2) - p_{0,0}(d_\beta)| \le 4\varepsilon_{\mathrm{ZK}}$$

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

$$|P(d_1; d_1, d_2) - P(d_2; d_1, d_2)| \le |p_{0,0}(d_1) - p_{0,0}(d_2)| + 8\varepsilon_{\mathrm{ZK}}. \tag{5.1}$$

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

U1-3′: If $C_U \le \nu$, then choose $\hat{v}_{\tilde{p}} \in_r \mathbb{G}_q$ and $r_{\tilde{p}} \in_r \mathbb{Z}_q$, and compute $u_{\tilde{p}} = g^{r_{\tilde{p}}}$, $v_{\tilde{p}} = y_1^{r_{\tilde{p}}} h^p$ and $\hat{u}_{\tilde{p}} = (\hat{g})^{r_{\tilde{p}}}$. Otherwise, choose $r_{\tilde{p}} \in_r \mathbb{Z}_q$, and compute $u_{\tilde{p}} = g^{r_{\tilde{p}}}$, $v_{\tilde{p}} = y_1^{r_{\tilde{p}}} h^p$, $\hat{u}_{\tilde{p}} = (\hat{g})^{r_{\tilde{p}}}$ and $\hat{v}_{\tilde{p}} = (\hat{y})^{r_{\tilde{p}}} (\hat{h})^p$.

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

$$|p_{0,0}(d_\beta) - p_{0,q_U}(d_\beta)| \le q_U(2n\varepsilon_{\mathrm{SS}} + \varepsilon_{\mathrm{ddh}} + \widetilde{\omega}_1)$$

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

(II) We define the sequence of games $\{\mathbf{Game}(1,\nu,\xi)\}$, where $\nu = 0, \dots, q_U - 1$ and $\xi = 0, \dots, q_S$. In $\mathbf{Game}(1,\nu,\xi)$, we replace Step **S$_\mathbf{j}$2-5** of $\mathbf{Game}(1,0,0) = \mathbf{Game}(0,q_U)$ by the following step:

S$_\mathbf{j}$2-5′: If either of the following conditions (1) and (2) hold, then choose $z_j \in_r \mathbb{G}_q$.

(1) $u_{\tilde{p}} \in \{u_{\tilde{p}}(1), \dots, u_{\tilde{p}}(\min\{C_U, \nu\})\}$.

(2) $C_S \le \xi$, $C_U \ge \nu + 1$ and $u_{\tilde{p}} = u_{\tilde{p}}(\nu + 1)$.

Otherwise, compute $z_j = v_j / w_j$.

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

Lemma 5.2 (cf. Claim 6 [4]). *If $T \le T_{\mathrm{ddh}} - 4T_S - q_U f_2^U - q_S f_2^S - f_2^I$ holds for some polynomials f_2^U, f_2^S and f_2^I in n, t and k, then*

$$|p_{1,0,0}(d_\beta) - p_{1,q_U-1,q_S}(d_\beta)| \le (q_U - 1)q_S(2n\varepsilon_{\mathrm{SS}} + \varepsilon_{\mathrm{ddh}} + \widetilde{\omega}_2)$$

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

(III) We define the sequence of games $\{\mathbf{Game}(2,\nu)\}_{\nu=0}^{q_S}$. In $\mathbf{Game}(2,\nu)$, we replace Steps **I4** and **S$_\mathbf{j}$2-4** of $\mathbf{Game}(2,0) = \mathbf{Game}(1,q_U-1,q_S)$ by the following steps, respectively:

I4′: Choose $h, \hat{g}, \hat{h}, \bar{g} \in_r \mathbb{G}_q$ and $\hat{x}, r_p, r_{1,d}, r_{2,d} \in_r \mathbb{Z}_q$, and compute $\hat{y} = (\hat{g})^{\hat{x}}$.
S$_\mathbf{j}$2-4′: If $C_S \le \nu$ and $(\hat{v}_{\tilde{p}} / \hat{u}_{\tilde{p}}^{\hat{x}}) \ne \hat{h}^p$, then choose $v_j \in_r \mathbb{G}_q$. Otherwise, compute $v_j = (v_p / v_{\tilde{p}})^{t_j}$.

Lemma 5.3 (cf. Claim 7 [4]). *If $T \le T_{\mathrm{ddh}} - 4T_S - q_U f_3^U - q_S f_3^S - f_3^I$ holds for some polynomials f_3^U, f_3^S and f_3^I in n, t and k, then*

$$|p_{2,0}(d_\beta) - p_{2,q_S}(d_\beta)| \le q_S(\varepsilon_{\mathrm{ddh}} + 2\varepsilon_{\mathrm{SS}} + \widetilde{\omega}_3)$$

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

Using Lemmas 5.1–5.3, we have

$$\begin{aligned} &|p_{0,0}(d_1) - p_{0,0}(d_2)| \\ &\quad \le 4(nq_Uq_S + nq_U - nq_S + q_S)\varepsilon_{\mathrm{SS}} + 2q_U(q_S+1)\varepsilon_{\mathrm{ddh}} + q_U\widetilde{\omega}_1 + (q_U - 1)q_S\widetilde{\omega}_2 + q_S\widetilde{\omega}_3 + |p_{2,q_S}(d_1) - P_{2,q_S}(d_2)|. \end{aligned} \tag{5.2}$$

(IV) We define the two games $\mathbf{Game}(3,1)$ and $\mathbf{Game}(3,2)$. In $\mathbf{Game}(3,1)$, we replace Step **I3** and Output phase of $\mathbf{Game}(3,0) = \mathbf{Game}(2,q_S)$ by the following steps, respectively:

I3′: Choose $x_2 \in_r \mathbb{Z}_q$ and $y_1 \in_r \mathbb{G}_q$, and compute $y_2 = g^{x_2}$, $\{x_{1,j}\}_{j=1}^n = \mathsf{SS}_{t,n}(0)$ and $\{x_{2,j}\}_{j=1}^n = \mathsf{SS}_{t,n}(x_2)$.
Output phase: If F = false and $\mathcal{A}$'s output equals 1, then set $\varphi = 1$. Otherwise, set $\varphi = 0$.

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

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

For each $\mathcal{M}_{\mu,\nu}^{\beta}$, let F_{μ,ν,d_β} denote the event that F = true holds. We write $p_{\mu,\nu}^F(d_\beta) = \Pr[E_{\mu,\nu,d_\beta} \wedge F_{\mu,\nu,d_\beta}]$ and $p_{\mu,\nu}^{\neg F}(d_\beta) = p_{\mu,\nu}(d_\beta) - p_{\mu,\nu}^F(d_\beta)$. Then we have

$$|p_{3,0}(d_1) - p_{3,0}(d_2)| \le |p^{F}_{3,0}(d_1) - p^{F}_{3,0}(d_2)| + |p^{\neg F}_{3,0}(d_1) - p^{\neg F}_{3,0}(d_2)| + \max\{\Pr[F_{3,0,d_1}], \Pr[F_{3,0,d_2}]\}. \tag{5.3}$$

Lemma 5.4 (cf. Claim 8 [4]). *One has*

$$|\Pr[F_{3,0,d_\beta}] - \Pr[F_{3,2,d_\beta}]| \le \widetilde{\omega_4}$$

and

$$\left|p^{\neg F}_{3,0}(d_1) - p^{\neg F}_{3,0}(d_2)\right| \le \widetilde{\omega_4}' + \left|p^{\neg F}_{3,1}(d_1) - p^{\neg F}_{3,1}(d_2)\right|,$$

where $\widetilde{\omega_4}$ *and* $\widetilde{\omega_4}'$ *are negligible in* k.

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

I6′: Choose $u_{1,d}, v_{1,d} \in_r \mathbb{G}_q$, and compute $(u_{2,d}, v_{2,d}) = (g^{r_{2,d}}, y_2^{r_{2,d}} d_\beta)$.

Lemma 5.5 (cf. Claim 9 [4]). *If* $T \le T_{\mathrm{ddh}} - 4T_S - q_U f^U_5 - q_S f^S_5 - f^I_5$ *holds for some polynomials* f^U_5, f^S_5 *and* f^I_5 *in* n, t *and* k, *then*

$$|p^{\neg F}_{3,1}(d_\beta) - p^{\neg F}_{4,1}(d_\beta)| < \varepsilon_{\mathrm{ddh}}$$

and

$$|\Pr[F_{3,2,d_\beta}] - \Pr[F_{4,2,d_\beta}]| < \varepsilon_{\mathrm{ddh}}$$

follow for $\beta \in \{1,2\}$.

As we employ the twin-encryption version of the ElGamal encryption, which has not been involved in PPSS_2, 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 **Game**$(4,3)$ and **Game**$(4,4)$. In **Game**$(4,3)$ and **Game**$(4,4)$, we replace Step **I6′** of **Game**$(4,1)$ and **Game**$(4,2)$ by the following step, respectively:

I6″: Choose $u_{1,d}, v_{1,d}, u_{2,d}, v_{2,d} \in_r \mathbb{G}_q$.

Lemma 5.6. *If* $T \le T_{\mathrm{ddh}} - 4T_S - q_U f^U_6 - q_S f^S_6 - f^I_6$ *holds for some polynomials* f^U_6, f^S_6 *and* f^I_6 *in* n, t *and* k, *then*

$$|p^{\neg F}_{4,1}(d_\beta) - p^{\neg F}_{4,3}(d_\beta)| < \varepsilon_{\mathrm{ddh}}$$

and

$$|\Pr[F_{4,2,d_\beta}] - \Pr[F_{4,4,d_\beta}]| < \varepsilon_{\mathrm{ddh}}$$

follow for $\beta \in \{1,2\}$.

Since the values $v_{1,d}$ and $v_{2,d}$ are uniformly chosen in Step **I6″** of **Game**$(4,3)$, $\mathcal{A}$'s output does not depend on the choice of β in Step **I2** of the game. Hence, we see that $p^{\neg F}_{4,3}(d_1) = p^{\neg F}_{4,3}(d_2)$. Using Lemmas 5.4–5.6, we have

$$|p^{\neg F}_{3,0}(d_1) - p^{\neg F}_{3,0}(d_2)| \le 4\varepsilon_{\mathrm{ddh}} + \widetilde{\omega_4}. \tag{5.4}$$

(VI) We define the sequence of games $\{\mathbf{Game}(5,\nu)\}_{\nu=0}^{q_S}$. In **Game**$(5,\nu)$, we replace Step **S$_\mathbf{j}$2-4′** of **Game**$(5,0) =$ **Game**$(4,4)$ by the following step:

S$_\mathbf{j}$2-4″: If $C_S \le \nu$ or $(\hat{v}_{\tilde{p}}/\hat{u}_{\tilde{p}}) \ne \hat{h}^p$, then choose $v_j \in_r \mathbb{G}_q$. Otherwise, compute $v_j = (v_p/v_{\tilde{p}})^{t_j}$.

Lemma 5.7 (cf. Claim 10 [4]). *If* $T \le T_{\mathrm{ddh}} - 4T_S - q_U f^U_7 - q_S f^S_7 - f^I_7$ *holds for some polynomials* f^U_7, f^S_7 *and* f^I_7 *in* n, t *and* k, *then*

$$|\Pr[F_{5,0,d_\beta}] - \Pr[F_{5,q_S,d_\beta}]| \le q_S(2\varepsilon_{\mathrm{ddh}} + 2\varepsilon_{\mathrm{SS}} + \widetilde{\omega_7})$$

follows for $\beta \in \{1,2\}$, *where* $\widetilde{\omega_7}$ *is negligible in* k.

(VII) We define the sequence of games $\{\mathbf{Game}(6,\nu)\}_{\nu=0}^{q_U}$. In **Game**$(6,\nu)$, we replace Step **U1-3′** of **Game**$(6,0) =$ **Game**$(5,q_U)$ by the following step:

U1-3″: If $C_U \le \nu$, then choose $\hat{v}_{\tilde{p}}, v_{\tilde{p}} \in_r \mathbb{G}_q$ and $r_{\tilde{p}} \in_r \mathbb{Z}_q$, and compute $u_{\tilde{p}} = g_1^{r_{\tilde{p}}}$ and $\hat{u}_{\tilde{p}} = (\hat{g})^{r_{\tilde{p}}}$. Otherwise, choose $\hat{v}_{\tilde{p}} \in_r \mathbb{G}_q$ and $r_{\tilde{p}} \in_r \mathbb{Z}_q$, and compute $u_{\tilde{p}} = g^{r_{\tilde{p}}}$, $v_{\tilde{p}} = y_1^{r_{\tilde{p}}} h^{\tilde{p}}$ and $\hat{u}_{\tilde{p}} = (\hat{g})^{r_{\tilde{p}}}$.

Lemma 5.8 (cf. Claim 11 [4]). *If* $T \le T_{\mathrm{ddh}} - 4T_S - q_U f^U_8 - q_S f^S_8 - f^I_8$ *holds for some polynomials* f^U_8, f^S_8 *and* f^I_8 *in* n, t *and* k, *then*

$$|\Pr[F_{6,0,d_\beta}] - \Pr[F_{6,q_U,d_\beta}]| \le q_U(\varepsilon_{\mathrm{ddh}} + 2n\varepsilon_{\mathrm{SS}} + \widetilde{\omega_8})$$

follows for $\beta \in \{1,2\}$, *where* $\widetilde{\omega_8}$ *is negligible in* k.

(VIII) We define the game **Game**$(7,1)$. In **Game**$(7,1)$, we replace Step **I5** of **Game**$(7,0)=$ **Game**$(6,q_U)$ by the following step:

I5′: Choose $p \in_r \mathbb{Z}_q$ and $u_p, v_p \in_r \mathbb{G}_q$.

Lemma 5.9 (cf. Claim 12 [4]). *If $T \le T_{\mathrm{ddh}} - 4T_S - q_U f_9^U - q_S f_9^S - f_9^I$ holds for some polynomials f_9^U, f_9^S and f_9^I in n, t and k, then*

$$|\Pr[F_{7,0,d_\beta}] - \Pr[F_{7,1,d_\beta}]| < \varepsilon_{\mathrm{ddh}}$$

follows for $\beta \in \{1,2\}$.

For $\beta \in \{1,2\}$, using Lemmas 5.4–5.9, we have

$$\Pr[F_{3,0,d_\beta}] \le \Pr[F_{7,1,d_\beta}] + (2q_S + q_U + 3)\varepsilon_{\mathrm{ddh}} + 2(nq_U + q_S)\varepsilon_{\mathrm{SS}} + \widetilde{\omega}_4 + q_S\widetilde{\omega}_7 + q_U\widetilde{\omega}_8. \tag{5.5}$$

The values v_p, $v_{\tilde{p}}$ and $\hat{v}_{\tilde{p}}$ constructed in Steps **I5′** and **U1-3″** of **Game**$(7,1)$ are independent of the choice of p in Step **I5′**. Hence, for $\beta \in \{1,2\}$, we have

$$\Pr[F_{7,1,d_\beta}] \le \left\lfloor \frac{q_S}{t-t'} \right\rfloor \cdot \frac{1}{\#\mathsf{PW}_\lambda}. \tag{5.6}$$

Hence, if $T \le T_{\mathrm{ddh}} - 4T_S - q_U f^U - q_S f^S - f^I$ holds for some polynomials f^U, f^S and f^I in n, t and k, then, by the inequalities (5.1)–(5.6), we obtain

$$\begin{aligned}|P(d_1;d_1,d_2) - P(d_2;d_1,d_2)| \le{}& \left\lfloor \frac{q_S}{t-t'} \right\rfloor \cdot \frac{1}{\#\mathsf{PW}_\lambda} + 8\varepsilon_{\mathrm{ZK}} + (4nq_Uq_S + 6nq_U - 4nq_S + 6q_S)\varepsilon_{\mathrm{SS}} \\ &+ (2q_Uq_S + 3q_U + 2q_S + 7)\varepsilon_{\mathrm{ddh}} + q_Uq_S\omega_1 + q_U\omega_2 + q_S\omega_3 + \omega_4,\end{aligned}$$

where ω_1, ω_2, ω_3 and ω_4 are negligible in k. This completes the proof of the theorem.

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 $\widetilde{\mathcal{M}}_{0,\nu}^{\beta}$. On input $w = (Q, g, g_1, g_2, g_3)$, $\widetilde{\mathcal{M}}_{0,\nu}^{\beta}$ simulates $\mathcal{M}_{0,\nu}^{\beta}$ except for the following steps:

I4: Choose $h, \hat{h} \in_r \mathbb{G}_q$, $r_p, r_{1,d}, r_{2,d} \in_r \mathbb{Z}_q$ and $r_0, r_1 \in_r \mathbb{Z}_q^*$. Then set $\hat{g} = g^{r_0}$, $\bar{g} = g_1^{r_1}$ and $\hat{y} = g_2$.
U1-3′: If $C_U = \nu$, then set $u_{\tilde{p}} = g_1^{1/r_0}$, $v_{\tilde{p}} = g_1^{x_1/r_0}h^p$, $\hat{u}_{\tilde{p}} = g_1$ and $\hat{v}_{\tilde{p}} = g_3^{1/r_0}(\hat{h})^p$. Otherwise, execute Step **U1-3′** of $\mathcal{M}_{0,\nu}^{\beta}$.
U1-5: if $C_U = \nu$, then set $e_j = (\bar{a}_j)^{1/(r_0r_1)}$ for each $j \in [n]$. Otherwise, execute Step **U1-5** of $\mathcal{M}_{0,\nu}^{\beta}$.

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

$$\begin{aligned}\left|p_{0,\nu-1}(d_\beta) - p_{0,\nu}(d_\beta)\right| &= \left| \Pr_{w\in\mathrm{DH}}[\varphi_{0,\nu-1}^{\beta} = 1] - \underset{\widetilde{w\in\mathrm{DH}}}{\Pr}[\varphi_{0,\nu}^{\beta} = 1] \right| \\ &\le \left| \Pr_{w\in\mathrm{DH}}[\varphi_{0,\nu-1}^{\beta} = 1] - \Pr_{w\in\mathrm{DH}}[\widetilde{\varphi}_{0,\nu}^{\beta} = 1] \right| + \left| \Pr_{w\in\mathrm{DH}}[\widetilde{\varphi}_{0,\nu}^{\beta} = 1] - \underset{\widetilde{w\in\mathrm{DH}}}{\Pr}[\widetilde{\varphi}_{0,\nu}^{\beta} = 1] \right| \\ &\quad + \left| \underset{\widetilde{w\in\mathrm{DH}}}{\Pr}[\widetilde{\varphi}_{0,\nu}^{\beta} = 1] - \underset{\widetilde{w\in\mathrm{DH}}}{\Pr}[\varphi_{0,\nu}^{\beta} = 1] \right|.\end{aligned} \tag{6.1}$$

For any $0 \le \nu \le q_U$, the running time of $\widetilde{\mathcal{M}}_{0,\nu}^{\beta}$ 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 $T_1 \le T_{\mathrm{ddh}}$, then the second term on the right-hand side of (6.1) is at most $\varepsilon_{\mathrm{ddh}}$.

We now estimate the first and the last terms on the right-hand side of (6.1). Let $E_{S1,\nu}^{\mathrm{SS}}$ denote the event such that $\mathcal{A}$ enters the ν-th User's query phase with a query $\{(j, a_j, b_j, \bar{a}_j, \pi_{1,j})\}_{j\in[n]}$ which satisfies the following two conditions for some $j_0 \in [n]$: (**i**) $(a_{j_0}, b_{j_0}, \bar{a}_{j_0}) \notin \mathcal{L}_{S1}^{\mathrm{pub}}$, and (**ii**) π_{1,j_0} is a valid proof. Then we have

$$\begin{aligned}&\left| \Pr_{w\in\mathrm{DH}}[\varphi_{0,\nu-1}^{\beta} = 1] - \Pr_{w\in\mathrm{DH}}[\widetilde{\varphi}_{0,\nu}^{\beta} = 1] \right| \\ &\le \left| \Pr_{w\in\mathrm{DH}}[\varphi_{0,\nu-1}^{\beta} = 1 \wedge E_{S1,\nu}^{\mathrm{SS}}] - \Pr_{w\in\mathrm{DH}}[\widetilde{\varphi}_{0,\nu}^{\beta} = 1 \wedge E_{S1,\nu}^{\mathrm{SS}}] \right| \\ &\quad + \left| \Pr_{w\in\mathrm{DH}}[\varphi_{0,\nu-1}^{\beta} = 1 \wedge \neg E_{S1,\nu}^{\mathrm{SS}}] - \Pr_{w\in\mathrm{DH}}[\widetilde{\varphi}_{0,\nu}^{\beta} = 1 \wedge \neg E_{S1,\nu}^{\mathrm{SS}}] \right|.\end{aligned} \tag{6.2}$$

Since $(\mathcal{P}(\mathcal{L}_{S1}^{\mathrm{pub}}), \mathcal{V}(\mathcal{L}_{S1}^{\mathrm{pub}}))$ is $(T_S, q_P^S, q_H^S, \varepsilon_{\mathrm{ZK}}, \varepsilon_{\mathrm{SS}})$-SS-NIZK, if the running time of $\mathcal{S}(\mathcal{L}_{S1}^{\mathrm{pub}})$ used in $\mathcal{M}_{0,\nu-1}^{\beta}$ and $\widetilde{\mathcal{M}}_{0,\nu}^{\beta}$ is at most T_S, and $\max\{nq_U, q_S\} \leq q_H^S, q_P^S$ holds, then we have

$$\left|\Pr_{w\in\mathrm{DH}}[\varphi_{0,\nu-1}^{\beta} = 1 \wedge E_{S1,\nu}^{\mathrm{SS}}] - \Pr_{w\in\mathrm{DH}}[\widetilde{\varphi}_{0,\nu}^{\beta} = 1 \wedge E_{S1,\nu}^{\mathrm{SS}}]\right| \leq 1 - (1-\varepsilon_{\mathrm{SS}})^n \leq n\varepsilon_{\mathrm{SS}}.$$

By the similar argument, we have

$$\left|\Pr_{w\in\widetilde{\mathrm{DH}}}[\widetilde{\varphi}_{0,\nu}^{\beta} = 1] - \Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi_{0,\nu}^{\beta} = 1]\right| \leq n\varepsilon_{\mathrm{SS}} + \left|\Pr_{w\in\widetilde{\mathrm{DH}}}[\widetilde{\varphi}_{0,\nu}^{\beta} = 1 \wedge \neg E_{S1,\nu}^{\mathrm{SS}}] - \Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi_{0,\nu}^{\beta} = 1 \wedge \neg E_{S1,\nu}^{\mathrm{SS}}]\right|. \tag{6.3}$$

In order to estimate other terms, we assume that the event $E_{S1,\nu}^{\mathrm{SS}}$ does not occur.

(A) We first consider the last term on the right-hand side of (6.2). Let $w \in \mathrm{DH}$. In the ν-th User's query phase of $\widetilde{\mathcal{M}}_{0,\nu}^{\beta}$, if we set $r_{\tilde{p}} = \alpha_1/r_0$, where $g_1 = g^{\alpha_1}$, then one has $u_{\tilde{p}} = g^{r_{\tilde{p}}}$, $v_{\tilde{p}} = y_1^{r_{\tilde{p}}} h^p$, $\hat{u}_{\tilde{p}} = (\hat{g})^{r_{\tilde{p}}}$, $\hat{v}_{\tilde{p}} = (\hat{y})^{r_{\tilde{p}}}(\hat{h})^p$ and $e_j = (a_j)^{r_{\tilde{p}}}$: these values are the same as the values obtained in the ν-th User's query phase of $\mathcal{M}_{0,\nu-1}^{\beta}$ with $r_{\tilde{p}} = \alpha_1/r_0$. Therefore, the only differences between $\mathcal{M}_{0,\nu-1}^{\beta}$ and $\widetilde{\mathcal{M}}_{0,\nu}^{\beta}$ are the choices of $\hat{g}$, $\bar{g}$ and $\hat{y}$ in Step **I4** and that of $u_{\tilde{p}}$ in Step **U1-3′** of the ν-th User's query phase. We define the following distribution over $\mathbb{G}_q^4$:

$$\Delta_{0,\nu}^1 = \{(g^{r_0}, g_1^{r_1}, g_2, g_1^{1/r_0}) \mid r_0, r_1 \in_r \mathbb{Z}_q^*,\ g_1, g_2 \in_r \mathbb{G}_q\}.$$

The distribution $\Delta_{0,\nu}^1$ is identical to the distribution of $(\hat{g}, \bar{g}, \hat{y}, u_{\tilde{p}})$ constructed in $\widetilde{\mathcal{M}}_{0,\nu}^{\beta}(w)$. In addition, the distribution of $(\hat{g}, \bar{g}, \hat{y}, u_{\tilde{p}})$ constructed in $\mathcal{M}_{0,\nu-1}^{\beta}(w)$ is uniform over $\mathbb{G}_q^4$. Hence, the last term on the right-hand side of (6.2) is bounded by the statistical distance between $\Delta_{0,\nu}^1$ and $U_{\mathbb{G}_q^4}$.

We see that the following statements hold:

For any $\bar{g}, \hat{y}, u_{\tilde{p}} \in \mathbb{G}_q$, one has

$$\Pr_{\boldsymbol{g}\in\Delta_{0,\nu}^1}[\boldsymbol{g} = (1, \bar{g}, \hat{y}, u_{\tilde{p}})] = 0.$$

For any $\hat{g}, \bar{g}, u_{\tilde{p}} \in \mathbb{G}_q \setminus \{1\}$ and $\hat{y} \in \mathbb{G}_q$, one has

$$\Pr_{\boldsymbol{g}\in\Delta_{0,\nu}^1}[\boldsymbol{g} = (\hat{g}, 1, \hat{y}, u_{\tilde{p}})] = \Pr_{\boldsymbol{g}\in\Delta_{0,\nu}^1}[\boldsymbol{g} = (\hat{g}, \bar{g}, \hat{y}, 1)] = 0, \quad \Pr_{\boldsymbol{g}\in\Delta_{0,\nu}^1}[\boldsymbol{g} = (\hat{g}, 1, \hat{y}, 1)] = \frac{1}{q^2(q-1)}$$

and

$$\Pr_{\boldsymbol{g}\in\Delta_{0,\nu}^1}[\boldsymbol{g} = (\hat{g}, \bar{g}, \hat{y}, u_{\tilde{p}})] = \frac{1}{q^2(q-1)^2}.$$

So the statistical distance between $\Delta_{0,\nu}^1$ and $U_{\mathbb{G}_q^4}$ 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 $w \in \widetilde{\mathrm{DH}}$. Using the similar argument to (A), we see that the differences between $\widetilde{\mathcal{M}}_{0,\nu}^{\beta}$ and $\mathcal{M}_{0,\nu}^{\beta}$ are the choices of $\hat{g}$, $\bar{g}$ and $\hat{y}$ in Step **I4** and those of $u_{\tilde{p}}$ and $\hat{v}_{\tilde{p}}$ in Step **U1-3′** of the ν-th User's query phase. We define the distribution $\Delta_{0,\nu}^2$ over $\mathbb{G}_q^5$ by

$$\Delta_{0,\nu}^2 = \{(g^{r_0}, g_1^{r_1}, g_2, g_1^{1/r_0}, g_3^{1/r_0}\hat{h}^p) \mid r_0, r_1 \in_r \mathbb{Z}_q^*,\ g_1, g_2, g_3 \in_r \mathbb{G}_q\}.$$

The distribution $\Delta_{0,\nu}^2$ is identical to that of $(\hat{g}, \bar{g}, \hat{y}, u_{\tilde{p}}, \hat{v}_{\tilde{p}})$ constructed in $\widetilde{\mathcal{M}}_{0,\nu}^{\beta}(w)$. In addition, the distribution of $(\hat{g}, \bar{g}, \hat{y}, u_{\tilde{p}}, \hat{v}_{\tilde{p}})$ constructed in $\mathcal{M}_{0,\nu}^{\beta}(w)$ is identical to $U_{\mathbb{G}_q^5}$. The last term on the right-hand side of (6.3) is bounded by the statistical distance between $\Delta_{0,\nu}^2$ and $U_{\mathbb{G}_q^5}$. We note that for any fixed $r_0 \in \mathbb{Z}_q^*$, $p \in \mathbb{Z}_q$ and $\hat{h} \in \mathbb{G}_q$, the distribution $\{g_3^{1/r_0}\hat{h}^p \mid g_3 \in_r \mathbb{G}_q\}$ over $\mathbb{G}_q$ is uniform. This implies that the statistical distance between $\Delta_{0,\nu}^2$ and $U_{\mathbb{G}_q^5}$ is less than the distance between $\Delta_{0,\nu}^1$ and $U_{\mathbb{G}_q^4}$.

Consequently, we have

$$\left|p_{0,\nu-1}(d_\beta) - p_{0,\nu}(d_\beta)\right| \leq 2n\varepsilon_{\mathrm{SS}} + \varepsilon_{\mathrm{ddh}} + \widetilde{\omega}_1,$$

where ω_1 is negligible in k, and hence

$$\left|p_{0,0}(d_\beta) - p_{0,q_U}(d_\beta)\right| \leq q_U(2n\varepsilon_{\mathrm{SS}} + \varepsilon_{\mathrm{ddh}} + \widetilde{\omega}_1)$$

follows.

Remark 6.1. In the proof of Lemma 5.1, the construction of the machine $\widetilde{\mathcal{M}}_{0,\nu}^{\beta}$, 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 $\Delta_{0,\nu}^1$ and $U_{\mathbb{G}_q}^4$ and that between $\Delta_{0,\nu}^2$ and $U_{\mathbb{G}_q}^5$ 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 $\widetilde{\mathcal{M}}^{\beta}_{1,\nu,\xi}$. On input $w = (Q, g, g_1, g_2, g_3)$, $\widetilde{\mathcal{M}}^{\beta}_{1,\nu,\xi}$ simulates $\mathcal{M}^{\beta}_{1,\nu,\xi-1}$ except for the following steps:

I4: Choose $h, \hat{h} \in_r \mathbb{G}_q$, $r_p, r_{1,d}, r_{2,d}, r_0, \hat{x} \in_r \mathbb{Z}_q$ and $r_1 \in_r \mathbb{Z}_q^*$. Then set $\hat{g} = g^{r_0}$, $\bar{g} = g_1^{r_1}$ and $\hat{y} = \hat{g}^{\hat{x}}$.
U1-3′: if $C_U = \nu$, then choose $\hat{v}_{\tilde{p}} \in_r \mathbb{G}_q$, and set $u_{\tilde{p}} = g_1$, $v_{\tilde{p}} = g_1^{x_1} h^p$ and $\hat{u}_{\tilde{p}} = g_1^{r_0}$. Otherwise, execute Step **U1-3′** of $\mathcal{M}^{\beta}_{1,\nu,\xi-1}$.
U1-5: if $C_U = \nu$, then set $e_j = (\bar{a}_j)^{1/r_1}$ for each $j \in [n]$. Otherwise, execute Step **U1-5** of $\mathcal{M}^{\beta}_{1,\nu,\xi-1}$.
S$_\mathbf{j}$2-6: if $C_S = \xi$, $C_U \geq \nu + 1$ and $u_{\tilde{p}} = u_{\tilde{p}}(\nu + 1)$ hold, then set $u_{z_j} = g_2$ and $v_{z_j} = g_3 z_j$. Otherwise, execute Step **S$_\mathbf{j}$2-6** of $\mathcal{M}^{\beta}_{1,\nu,\xi-1}$.

In each $\mathcal{M}^{\beta}_{1,\nu,\xi}$ and $\widetilde{\mathcal{M}}^{\beta}_{1,\nu,\xi}$, let $U_p^{\nu,\xi}$ denote the event that $C_U \geq \nu + 1$ and $u_{\tilde{p}} = u_{\tilde{p}}(\nu + 1)$ hold in the ξ-th Server's query phase.

Let $\widetilde{\varphi}^{\beta}_{\mu,\nu,\xi}$ be the output of $\widetilde{\mathcal{M}}^{\beta}_{\mu,\nu,\xi}$. Noting that $\varphi^{\beta}_{1,\nu,\xi}$ is independent of g_1, g_2 and g_3, we have

$$\begin{aligned}
&|p_{1,\nu,\xi-1}(d_\beta) - p_{1,\nu,\xi}(d_\beta)| \\
&\leq \left| \underset{w\in\mathrm{DH}}{\Pr}[\varphi^{\beta}_{1,\nu,\xi-1} = 1] - \underset{w\in\mathrm{DH}}{\Pr}[\widetilde{\varphi}^{\beta}_{1,\nu,\xi} = 1] \right| + \left| \underset{w\in\mathrm{DH}}{\Pr}[\widetilde{\varphi}^{\beta}_{1,\nu,\xi} = 1] - \underset{w\in\widetilde{\mathrm{DH}}}{\Pr}[\widetilde{\varphi}^{\beta}_{1,\nu,\xi} = 1] \right| \\
&\quad + \left| \underset{w\in\widetilde{\mathrm{DH}}}{\Pr}[\widetilde{\varphi}^{\beta}_{1,\nu,\xi} = 1] - \underset{w\in\widetilde{\mathrm{DH}}}{\Pr}[\varphi^{\beta}_{1,\nu,\xi} = 1] \right|. \qquad (6.4)
\end{aligned}$$

We estimate the first and the last terms on the right-hand side of (6.4). Let $E^{\mathrm{SS}}_{S1,\nu}$ denote the event defined as in the proof of the Lemma 5.1. If the running time of $\mathcal{S}(\mathcal{L}^{\mathrm{pub}}_{S1})$ used in $\mathcal{M}^{\beta}_{1,\nu,\xi-1}$, $\widetilde{\mathcal{M}}^{\beta}_{1,\nu,\xi}$ and $\mathcal{M}^{\beta}_{1,\nu,\xi}$ is at most T_S, and $\max\{nq_U, q_S\} \leq q_H^S, q_P^S$ holds, then we have

$$\begin{aligned}
&\left| \underset{w\in\mathrm{DH}}{\Pr}[\varphi^{\beta}_{1,\nu,\xi-1} = 1] - \underset{w\in\mathrm{DH}}{\Pr}[\widetilde{\varphi}^{\beta}_{1,\nu,\xi} = 1] \right| + \left| \underset{w\in\widetilde{\mathrm{DH}}}{\Pr}[\widetilde{\varphi}^{\beta}_{1,\nu,\xi} = 1] - \underset{w\in\widetilde{\mathrm{DH}}}{\Pr}[\varphi^{\beta}_{1,\nu,\xi} = 1] \right| \\
&\leq 2n\varepsilon_{\mathrm{SS}} + \left| \underset{w\in\mathrm{DH}}{\Pr}[\varphi^{\beta}_{1,\nu,\xi-1} = 1 \wedge \neg E^{\mathrm{SS}}_{S1,\nu}] - \underset{w\in\mathrm{DH}}{\Pr}[\widetilde{\varphi}^{\beta}_{1,\nu,\xi} = 1 \wedge \neg E^{\mathrm{SS}}_{S1,\nu}] \right| \\
&\quad + \left| \underset{w\in\widetilde{\mathrm{DH}}}{\Pr}[\widetilde{\varphi}^{\beta}_{1,\nu,\xi} = 1 \wedge \neg E^{\mathrm{SS}}_{S1,\nu}] - \underset{w\in\widetilde{\mathrm{DH}}}{\Pr}[\varphi^{\beta}_{1,\nu,\xi} = 1 \wedge \neg E^{\mathrm{SS}}_{S1,\nu}] \right|. \qquad (6.5)
\end{aligned}$$

In order to estimate other terms, we assume that the event $E^{\mathrm{SS}}_{S1,\nu}$ does not occur.

(A) We first consider the second term on the right-hand side of (6.5). Let $w \in \mathrm{DH}$. In the ν-th User's query phase of $\widetilde{\mathcal{M}}^{\beta}_{1,\nu,\xi}$, if we set $r_{\tilde{p}} = \alpha_1$, where $g_1 = g^{\alpha_1}$, then one has $u_{\tilde{p}} = g^{r_{\tilde{p}}}$, $v_{\tilde{p}} = y_1^{r_{\tilde{p}}} h^p$, $\hat{u}_{\tilde{p}} = (\hat{g})^{r_{\tilde{p}}}$, $\hat{v}_{\tilde{p}} \in_r \mathbb{G}_q$ and $e_j = (a_j)^{r_{\tilde{p}}}$: these values are the same as the values obtained in the ν-th Server's query phase of $\mathcal{M}^{\beta}_{1,\nu,\xi-1}$. We consider the ξ-th Server's query phase of $\widetilde{\mathcal{M}}^{\beta}_{1,\nu,\xi}$.

- Assume that the event $U_p^{\nu,\xi}$ occurs. If we set $r_{z_j} = \alpha_2$, where $g_2 = g^{\alpha_2}$, then one has $u_{z_j} = g^{r_{z_j}}$ and $v_{z_j} = u_{\tilde{p}}^{r_{z_j}} z_j$: these values are the same as the values obtained in the ξ-th Server's query phase of $\mathcal{M}^{\beta}_{1,\nu,\xi-1}$ with $r_{z_j} = \alpha_2$. In particular, g_2 is randomly chosen, and is independent of the choices of $\hat{g}$, $\bar{g}$, $\hat{y}$ and $u_{\tilde{p}}$.
- If the event $U_p^{\nu,\xi}$ does not occur, then the ξ-th Server's query phase of $\widetilde{\mathcal{M}}^{\beta}_{1,\nu,\xi}$ is the same as that of $\mathcal{M}^{\beta}_{1,\nu,\xi-1}$.

Hence, the differences between $\mathcal{M}^{\beta}_{1,\nu,\xi-1}$ and $\widetilde{\mathcal{M}}^{\beta}_{1,\nu,\xi}$ are the choices of $\hat{g}$, $\bar{g}$ and $\hat{y}$ in Step **I4** and that of $u_{\tilde{p}}$ in Step **U1-3′**. The distribution

$$\Delta^1_{1,\nu,\xi} = \{(g^{r_0}, g_1^{r_1}, g^{r_0\hat{x}}, g_1) \mid r_0, \hat{x} \in_r \mathbb{Z}_q,\ r_1 \in_r \mathbb{Z}_q^*,\ g_1 \in_r \mathbb{G}_q\}$$

over $\mathbb{G}_q^4$ is identical to the distribution of $(\hat{g}, \bar{g}, \hat{y}, u_{\tilde{p}})$ constructed in $\widetilde{\mathcal{M}}^{\beta}_{1,\nu,\xi}(w)$. In addition, the distribution of $(\hat{g}, \bar{g}, \hat{y}, u_{\tilde{p}})$ constructed in $\mathcal{M}^{\beta}_{1,\nu,\xi-1}(w)$ is uniform over $\mathbb{G}_q^4$. The second term on the right-hand side of (6.5) is bounded by the statistical distance between $\Delta^1_{1,\nu,\xi}$ and $U_{\mathbb{G}_q^4}$. We define the following two distributions over $\mathbb{G}_q^2$:

$$\bar{\Delta}^1_{1,\nu,\xi} = \{(g^{r_0}, g^{r_0\hat{x}}) \mid r_0, \hat{x} \in_r \mathbb{Z}_q\}$$

and

$$\widetilde{\Delta}^1_{1,\nu,\xi} = \{(g_1^{r_1}, g_1) \mid r_1 \in_r \mathbb{Z}_q^*,\ g_1 \in_r \mathbb{G}_q\}.$$

For any $\hat{g}, \bar{g}, \hat{y}, u_{\tilde{p}}, u_{z_j} \in \mathbb{G}_q \setminus \{1\}$, we have

$$\underset{\boldsymbol{g}\in\bar{\Delta}^1_{1,\nu,\xi}}{\Pr}[\boldsymbol{g} = (1, \hat{y})] = 0, \qquad \underset{\boldsymbol{g}\in\bar{\Delta}^1_{1,\nu,\xi}}{\Pr}[\boldsymbol{g} = (1, 1)] = \underset{\boldsymbol{g}\in\tilde{\Delta}^1_{1,\nu,\xi}}{\Pr}[\boldsymbol{g} = (1, 1)] = \frac{1}{q},$$

$$\Pr_{\boldsymbol{g}\in\bar{\Delta}^1_{1,\nu,\xi}}[\boldsymbol{g}=(\hat{g},1)]=\Pr_{\boldsymbol{g}\in\bar{\Delta}^1_{1,\nu,\xi}}[\boldsymbol{g}=(\hat{g},\hat{y})]=\frac{1}{q^2},\quad \Pr_{\boldsymbol{g}\in\tilde{\Delta}^1_{1,\nu,\xi}}[\boldsymbol{g}=(\bar{g},u_{\tilde{p}})]=\frac{1}{q(q-1)}$$

and

$$\Pr_{\boldsymbol{g}\in\tilde{\Delta}^1_{1,\nu,\xi}}[\boldsymbol{g}=(1,u_{\tilde{p}})]=\Pr_{\boldsymbol{g}\in\tilde{\Delta}^1_{1,\nu,\xi}}[\boldsymbol{g}=(\bar{g},1)]=0.$$

Since $\bar{\Delta}^1_{1,\nu,\xi}$ and $\tilde{\Delta}^1_{1,\nu,\xi}$ are independent, the statistical distance between $\Delta^1_{1,\nu,\xi}$ and $U_{\mathbb{G}_q^4}$ is at most the sum of the distance between $\bar{\Delta}^1_{1,\nu,\xi}$ and $U_{\mathbb{G}_q^2}$ and that between $\tilde{\Delta}^1_{1,\nu,\xi}$ and $U_{\mathbb{G}_q^2}$. Hence, the statistical distance between $\Delta^1_{1,\nu,\xi}$ and $U_{\mathbb{G}_q^4}$ 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 $w\in\widetilde{\mathrm{DH}}$. We have

$$\begin{aligned}&\left|\Pr_{w\in\widetilde{\mathrm{DH}}}[\widetilde{\varphi}^{\beta}_{1,\nu,\xi}=1\wedge\neg E^{\mathrm{SS}}_{S1,\nu}]-\Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi^{\beta}_{1,\nu,\xi}=1\wedge\neg E^{\mathrm{SS}}_{S1,\nu}]\right|\\&\le\left|\Pr_{w\in\widetilde{\mathrm{DH}}}[\widetilde{\varphi}^{\beta}_{1,\nu,\xi}=1\wedge\neg E^{\mathrm{SS}}_{S1,\nu}\wedge U_p^{\nu,\xi}]-\Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi^{\beta}_{1,\nu,\xi}=1\wedge\neg E^{\mathrm{SS}}_{S1,\nu}\wedge U_p^{\nu,\xi}]\right|\\&\quad+\left|\Pr_{w\in\widetilde{\mathrm{DH}}}[\widetilde{\varphi}^{\beta}_{1,\nu,\xi}=1\wedge\neg E^{\mathrm{SS}}_{S1,\nu}\wedge\neg U_p^{\nu,\xi}]-\Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi^{\beta}_{1,\nu,\xi}=1\wedge\neg E^{\mathrm{SS}}_{S1,\nu}\wedge\neg U_p^{\nu,\xi}]\right|.\end{aligned}\tag{6.6}$$

(B-1) In order to estimate the last term on the last-hand side of (6.6), we assume that the event $U_p^{\nu,\xi}$ does not occur. Then, by the similar argument to (A), the differences between $\widetilde{\mathcal{M}}^{\beta}_{1,\nu,\xi}$ and $\mathcal{M}^{\beta}_{1,\nu,\xi}$ are the choices of $\hat{g}$, $\bar{g}$ and $\hat{y}$ in Step **I4** and that of $u_{\tilde{p}}$ in Step **U1-3′** of the ν-th User's query phase. Hence, the last term on the right-hand side of (6.6) is at most the statistical distance between $\Delta^1_{1,\nu,\xi}$ and $U_{\mathbb{G}_q^4}$, 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 $U_p^{\nu,\xi}$ occurs. The differences between $\widetilde{\mathcal{M}}^{\beta}_{1,\nu,\xi}$ and $\mathcal{M}^{\beta}_{1,\nu,\xi}$ are the choices of $\hat{g}$, $\bar{g}$ and $\hat{y}$ in Step **I4**, that of $u_{\tilde{p}}$ in Step **U1-3′** of the ν-th User's query phase and those of z_j, u_{z_j} and v_{z_j} of the ξ-th Server's query phase. Let Z be the distribution of $z_j\in\mathbb{G}_q$ computed in the ξ-th Server's query phase of $\widetilde{\mathcal{M}}^{\beta}_{1,\nu,\xi}$. The distribution Z depends on g^{r_0}, $g_1^{r_1}$, $g^{r_0\hat{x}}$ and g_1, and is independent of g_2 and g_3.

The distribution

$$\Delta^2_{1,\nu,\xi}=\{(g^{r_0},g_1^{r_1},g^{r_0\hat{x}},g_1,g_2,g_3z_j)\mid r_0,\hat{x}\in_r\mathbb{Z}_q,\ r_1\in_r\mathbb{Z}_q^*,\ g_1,g_2,g_3\in_r\mathbb{G}_q,\ z_j\in Z\}$$

is identical to the distribution of $(\hat{g},\bar{g},\hat{y},u_{\tilde{p}},u_{z_j},v_{z_j})$ constructed in $\widetilde{\mathcal{M}}^{\beta}_{1,\nu,\xi}(w)$. Let $m'=(m_1,m_2,m_3,m_4)\in\mathbb{G}_q^4$, $m''=(m_5,m_6)\in\mathbb{G}_q^2$ and $m=(m',m'')$. Then we have

$$\Pr_{\boldsymbol{g}\in\Delta^2_{1,\nu,\xi}}[\boldsymbol{g}=m]=\Pr_{\boldsymbol{g}\in\Delta^2_{1,\nu,\xi}}[\boldsymbol{g}''=m''\mid\boldsymbol{g}'=m']\Pr_{\boldsymbol{g}\in\Delta^2_{1,\nu,\xi}}[\boldsymbol{g}'=m'],$$

where we have set $\boldsymbol{g}=(\boldsymbol{g}',\boldsymbol{g}'')$. We note that

$$\Pr_{\boldsymbol{g}\in\Delta^1_{1,\nu,\xi}}[\boldsymbol{g}'=m']=\Pr_{\boldsymbol{g}\in\Delta^2_{1,\nu,\xi}}[\boldsymbol{g}'=m'].$$

It follows that

$$\begin{aligned}\Pr_{\boldsymbol{g}\in\Delta^2_{1,\nu,\xi}}[\boldsymbol{g}''=m''\mid\boldsymbol{g}'=m']&=\Pr_{\boldsymbol{g}\in\Delta^2_{1,\nu,\xi}}[g_3z_j=m_6\mid(\boldsymbol{g}',g_2)=(m',m_5)]\Pr_{\boldsymbol{g}\in\Delta^2_{1,\nu,\xi}}[g_2=m_5\mid\boldsymbol{g}'=m']\\&=\frac{1}{q}\sum_{m_0\in\mathbb{G}_q}\Pr_{\boldsymbol{g}\in\Delta^2_{1,\nu,\xi}}[z_j=m_6m_0^{-1}\mid(\boldsymbol{g}',g_2,g_3)=(m',m_5,m_0)]\Pr_{\boldsymbol{g}\in\Delta^2_{1,\nu,\xi}}[g_3=m_0\mid(\boldsymbol{g}',g_2)=(m',m_5)]\\&=\frac{1}{q^2}\sum_{m_0\in\mathbb{G}_q}\Pr_{\boldsymbol{g}\in\Delta^2_{1,\nu,\xi}}[z_j=m_6m_0^{-1}\mid(\boldsymbol{g}',g_2,g_3)=(m',m_5,m_0)].\end{aligned}$$

Since $\{m_6m_0^{-1}\mid m_0\in\mathbb{G}_q\}=\mathbb{G}_q$ for any $m_6\in\mathbb{G}_q$, we have

$$\Pr_{\boldsymbol{g}\in\Delta^2_{1,\nu,\xi}}[\boldsymbol{g}''=m''\mid\boldsymbol{g}'=m']=\frac{1}{q^2}.$$

The distribution

$$\Delta^3_{1,\nu,\xi}=\{(\hat{g},\bar{g},\hat{y},g^{r_{\tilde{p}}},g^{r_{z_j}},g^{r_{\tilde{p}}r_{z_j}}z_j)\mid r_{\tilde{p}},r_{z_j}\in_r\mathbb{Z}_q,\ \hat{g},\bar{g},\hat{y},z_j\in_r\mathbb{G}_q\}$$

is identical to that constructed in $\mathcal{M}^{\beta}_{1,\nu,\xi}(w)$, and is uniform over $\mathbb{G}_q^6$. Since the first term on the right-hand side of (6.6) is bounded by the statistical distance between $\Delta^2_{1,\nu,\xi}$ and $\Delta^3_{1,\nu,\xi}$, we have

$$\begin{aligned}
&\left| \underset{w\in\mathrm{DH}}{\underset{\sim}{\Pr}}[\widetilde{\varphi}^{\beta}_{1,\nu,\xi} = 1 \wedge \neg E^{\mathrm{SS}}_{S1,\nu} \wedge U^{\nu,\xi}_{p}] - \underset{w\in\mathrm{DH}}{\underset{\sim}{\Pr}}[\varphi^{\beta}_{1,\nu,\xi} = 1 \wedge \neg E^{\mathrm{SS}}_{S1,\nu} \wedge U^{\nu,\xi}_{p}] \right| \\
&\quad \le \sum_{m\in\mathbb{G}_q^6} \left| \Pr_{\boldsymbol{g}\in\Delta^2_{1,\nu,\xi}}[\boldsymbol{g} = m] - \Pr_{\boldsymbol{g}\in\Delta^3_{1,\nu,\xi}}[\boldsymbol{g} = m] \right| = \sum_{m''\in\mathbb{G}_q^2} \frac{1}{q^2} \sum_{m'\in\mathbb{G}_q^4} \left| \Pr_{\boldsymbol{g}\in\Delta^2_{1,\nu,\xi}}[\boldsymbol{g}' = m'] - \frac{1}{q^4} \right| = \frac{6(q-1)}{q^2},
\end{aligned}$$

where the last equation follows from the argument in (A). This value is negligible in k.

Note that, for any $0 \le \nu \le q_U - 1$ and $0 \le \xi \le q_S$, the running time of $\widetilde{\mathcal{M}}^{\beta}_{1,\nu,\xi}$ is at most $T_2 = T + 4T_S + q_U f_2^U + q_S f_2^S + f_2^I$ for some polynomials f_2^U, f_2^S and f_2^I in n, t and k. So, if $T_2 \le T_{\mathrm{ddh}}$, then the second term on the right-hand side of (6.4) is at most $\varepsilon_{\mathrm{ddh}}$. Consequently, we have

$$|p_{1,0,0}(d_\beta) - p_{1,q_U-1,q_S}(d_\beta)| \le (q_U - 1)q_S(2n\varepsilon_{\mathrm{SS}} + \varepsilon_{\mathrm{ddh}} + \widetilde{\omega}_2),$$

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

6.3 Proof of Lemma 5.3

We construct an intermediary probabilistic machine $\widetilde{\mathcal{M}}^{\beta}_{2,\nu}$. On input $w = (Q, g, g_1, g_2, g_3)$, $\widetilde{\mathcal{M}}^{\beta}_{2,\nu}$ simulates $\mathcal{M}^{\beta}_{2,\nu}$ except for the following steps:

I4′: Choose $\hat{g} \in_r \mathbb{G}_q$, $\hat{x}, r_p, r_{1,d}, r_{2,d}, r_1 \in_r \mathbb{Z}_q$ and $r_0 \in_r \mathbb{Z}_q^*$, and set $h = g_2$, $\hat{h} = g_3^{r_0}$, $\hat{y} = \hat{g}^{\hat{x}}$ and $\bar{g} = g^{r_1}$.
S$_\mathbf{j}$1-2: if $C_S = \nu$, then set $a_j = g_1$, $b_j = g_1^{r_p}$ and $\bar{a}_j = g_1^{r_1}$. Otherwise, execute Step **S$_\mathbf{j}$1-2** of $\mathcal{M}^{\beta}_{2,\nu}$.
S$_\mathbf{j}$2-4′: if $C_S = \nu$, then set

$$v_j = \left(\frac{b_j}{e_j}\right)^{x_1} g_3^{p} \left(\frac{\hat{v}_{\tilde{p}}}{(\hat{u}_{\tilde{p}})^{\hat{x}}}\right)^{-1/r_0}.$$

Otherwise, execute Step **S$_\mathbf{j}$2-4′** of $\mathcal{M}^{\beta}_{2,\nu}$.

Noting that $\varphi^{\beta}_{2,\nu}$ is independent of g_1, g_2 and g_3, we have

$$\begin{aligned}
&|p_{2,\nu-1}(d_\beta) - p_{2,\nu}(d_\beta)| \\
&\le \left| \Pr_{w\in\mathrm{DH}}[\varphi^{\beta}_{2,\nu-1} = 1] - \Pr_{w\in\mathrm{DH}}[\widetilde{\varphi}^{\beta}_{2,\nu} = 1] \right| + \left| \Pr_{w\in\mathrm{DH}}[\widetilde{\varphi}^{\beta}_{2,\nu} = 1] - \underset{w\in\mathrm{DH}}{\underset{\sim}{\Pr}}[\widetilde{\varphi}^{\beta}_{2,\nu} = 1] \right| \\
&+ \left| \underset{w\in\mathrm{DH}}{\underset{\sim}{\Pr}}[\widetilde{\varphi}^{\beta}_{2,\nu} = 1] - \underset{w\in\mathrm{DH}}{\underset{\sim}{\Pr}}[\varphi^{\beta}_{2,\nu} = 1] \right|.
\end{aligned} \tag{6.7}$$

We estimate the first and the last terms on the right-hand side of (6.7). Let $E^{\mathrm{SS}}_{U,\nu}$ denote the event such that $\mathcal{A}$ enters the ν-th Server's query phase with a query $(V, u, e_j, u_{\tilde{p}}, v_{\tilde{p}}, \hat{u}_{\tilde{p}}, \hat{v}_{\tilde{p}}, \pi_{2,j})$ which satisfies the following two conditions: (**i**) $\pi_{2,j}$ is a valid proof, and (**ii**) $(a_j, e_j, u_{\tilde{p}}, v_{\tilde{p}}, \hat{u}_{\tilde{p}}, \hat{v}_{\tilde{p}}) \notin \mathcal{L}^{\mathrm{pub}}_{U}$. Since $(\mathcal{P}(\mathcal{L}^{\mathrm{pub}}_{U}), \mathcal{V}(\mathcal{L}^{\mathrm{pub}}_{U}))$ is $(T_S, q_P^S, q_H^S, \varepsilon_{\mathrm{ZK}}, \varepsilon_{\mathrm{SS}})$-SS-NIZK, if the running time of $\mathcal{S}(\mathcal{L}^{\mathrm{pub}}_{U})$ used in $\mathcal{M}^{\beta}_{2,\nu-1}$, $\mathcal{M}^{\beta}_{2,\nu}$ and $\widetilde{\mathcal{M}}^{\beta}_{2,\nu}$ is at most T_S, and $\max\{nq_U, q_S\} \le q_H^S, q_P^S$ holds, then we have

$$\begin{aligned}
&\left| \Pr_{w\in\mathrm{DH}}[\varphi^{\beta}_{2,\nu-1} = 1] - \Pr_{w\in\mathrm{DH}}[\widetilde{\varphi}^{\beta}_{2,\nu} = 1] \right| + \left| \underset{w\in\mathrm{DH}}{\underset{\sim}{\Pr}}[\widetilde{\varphi}^{\beta}_{2,\nu} = 1] - \underset{w\in\mathrm{DH}}{\underset{\sim}{\Pr}}[\varphi^{\beta}_{2,\nu} = 1] \right| \\
&\le 2\varepsilon_{\mathrm{SS}} + \left| \Pr_{w\in\mathrm{DH}}[\varphi^{\beta}_{2,\nu-1} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu}] - \Pr_{w\in\mathrm{DH}}[\widetilde{\varphi}^{\beta}_{2,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu}] \right| \\
&+ \left| \underset{w\in\mathrm{DH}}{\underset{\sim}{\Pr}}[\widetilde{\varphi}^{\beta}_{2,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu}] - \underset{w\in\mathrm{DH}}{\underset{\sim}{\Pr}}[\varphi^{\beta}_{2,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu}] \right|.
\end{aligned} \tag{6.8}$$

In order to estimate other terms, we assume that the event $E^{\mathrm{SS}}_{U,\nu}$ does not occur.

(**A**) We first consider the second term on the right-hand side of (6.8). Let $w \in \mathrm{DH}$. In the ν-th Server's query phase of $\widetilde{\mathcal{M}}^{\beta}_{2,\nu}$, if we set $t_j = \alpha_1$, where $g_1 = g^{\alpha_1}$, then one has $a_j = g^{t_j}$, $b_j = u_p^{t_j}$, $\bar{a}_j = (\bar{g})^{t_j}$ and $v_j = (v_p/v_{\tilde{p}})^{t_j}$: these values are the same as the values obtained in the ν-th Server's query phase of $\mathcal{M}^{\beta}_{2,\nu-1}$ with $t_j = \alpha_1$. Hence, the differences between $\mathcal{M}^{\beta}_{2,\nu-1}$ and $\widetilde{\mathcal{M}}^{\beta}_{2,\nu}$ is the choices of h, $\hat{h}$ and $\bar{g}$ in Step **I4′** and that of a_j in Step **S$_\mathbf{j}$1-2** of the ν-th Server's query phase. We define the distribution $\Delta^1_{2,\nu}$ over $\mathbb{G}_q^4$ by

$$\Delta^1_{2,\nu} = \{(g^{\alpha_2}, g^{\alpha_1\alpha_2 r_0}, g^{r_1}, g^{\alpha_1}) \mid r_1, \alpha_1, \alpha_2 \in_r \mathbb{Z}_q,\ r_0 \in_r \mathbb{Z}_q^*\}.$$

The distribution $\Delta^1_{2,\nu}$ is identical to the distribution of $(h, \hat{h}, \bar{g}, a_j)$ constructed in $\widetilde{\mathcal{M}}^{\beta}_{2,\nu}(w)$. In addition, the distribution of $(h, \hat{h}, \bar{g}, a_j)$ constructed in $\mathcal{M}^{\beta}_{2,\nu-1}(w)$ is identical to $U_{\mathbb{G}_q^4}$. The second term on teh right-hand side of (6.8) is bounded by the statistical distance between $\Delta^1_{2,\nu}$ and $U_{\mathbb{G}_q^4}$. Since the distribution $\{g^{r_1} \mid r_1 \in_r \mathbb{Z}_q\}$ over $\mathbb{G}_q$ is uniform, the statistical distance between $\Delta^1_{2,\nu}$ and $U_{\mathbb{G}_q^4}$ is at most the distance between the distribution

$$\bar{\Delta}^1_{2,\nu} = \{(g^{\alpha_2}, g^{\alpha_1\alpha_2 r_0}, g^{\alpha_1}) \mid \alpha_1, \alpha_2 \in_r \mathbb{Z}_q,\ r_0 \in_r \mathbb{Z}_q^*\}$$

over $\mathbb{G}_q^3$ and $U_{\mathbb{G}_q^3}$. For any $h, \hat{h}, a_j \in \mathbb{G}_q \setminus \{1\}$, we have

$$\Pr_{\boldsymbol{g}\in\bar{\Delta}^1_{2,\nu}}[\boldsymbol{g} = (1, \hat{h}, a_j)] = \Pr_{\boldsymbol{g}\in\bar{\Delta}^1_{2,\nu}}[\boldsymbol{g} = (1, \hat{h}, 1)] = \Pr_{\boldsymbol{g}\in\bar{\Delta}^1_{2,\nu}}[\boldsymbol{g} = (h, \hat{h}, 1)] = \Pr_{\boldsymbol{g}\in\bar{\Delta}^1_{2,\nu}}[\boldsymbol{g} = (h, 1, a_j)] = 0,$$

$$\Pr_{\boldsymbol{g}\in\bar{\Delta}^1_{2,\nu}}[\boldsymbol{g} = (h, \hat{h}, a_j)] = \frac{1}{q^2(q-1)}$$

and

$$\Pr_{\boldsymbol{g}\in\bar{\Delta}^1_{2,\nu}}[\boldsymbol{g} = (h, 1, 1)] = \Pr_{\boldsymbol{g}\in\bar{\Delta}^1_{2,\nu}}[\boldsymbol{g} = (1, 1, a_j)] = \Pr_{\boldsymbol{g}\in\bar{\Delta}^1_{2,\nu}}[\boldsymbol{g} = (1, 1, 1)] = \frac{1}{q^2}.$$

Hence, the statistical distance between $\Delta^1_{2,\nu}$ and $U_{\mathbb{G}_q^4}$ is at most $2(3q^2 - 5q + 2)/q^3$, which is negligible in k.

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

$$\begin{aligned}
&\left| \Pr_{w\in\widetilde{\mathrm{DH}}}[\widetilde{\varphi}^{\beta}_{2,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu}] - \Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi^{\beta}_{2,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu}] \right| \\
&\quad \le \left| \Pr_{w\in\widetilde{\mathrm{DH}}}[\widetilde{\varphi}^{\beta}_{2,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu} \wedge I_\nu] - \Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi^{\beta}_{2,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu} \wedge I_\nu] \right| \\
&\quad\quad + \left| \Pr_{w\in\widetilde{\mathrm{DH}}}[\widetilde{\varphi}^{\beta}_{2,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu} \wedge \neg I_\nu] - \Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi^{\beta}_{2,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu} \wedge \neg I_\nu] \right|,
\end{aligned} \tag{6.9}$$

where I_ν denotes the event such that $\mathcal{A}$ enters the ν-th Server's query phase with a query $(V, u, e_j, u_{\tilde{p}}, v_{\tilde{p}}, \hat{u}_{\tilde{p}}, \hat{v}_{\tilde{p}}, \pi_{2,j})$ which satisfies $\hat{v}_{\tilde{p}}/(\hat{u}_{\tilde{p}})^{\hat{x}} = \hat{h}^p$.

(B-1) In order to estimate the first term on the right-hand side of (6.9), we assume that the event I_ν occurs. In the ν-th Server's query phase of $\widetilde{\mathcal{M}}^{\beta}_{2,\nu}$, if we set $t_j = \alpha_1$, where $g_1 = g^{\alpha_1}$, then one has $a_j = g^{t_j}$, $b_j = u_p^{t_j}$, $\bar{a}_j = (\bar{g})^{t_j}$ and

$$v_j = \frac{b_j^{x_1}}{e_j^{x_1}} = \frac{u_p^{t_j x_1} h^{p t_j}}{u_{\tilde{p}}^{t_j x_1} h^{p t_j}} = \left(\frac{v_p}{v_{\tilde{p}}}\right)^{t_j}.$$

This shows that these values are the same as the values obtained in the ν-th Server's query phase of $\mathcal{M}^{\beta}_{2,\nu}$ with $t_j = \alpha_1$. Hence, the differences between $\widetilde{\mathcal{M}}^{\beta}_{2,\nu}$ and $\mathcal{M}^{\beta}_{2,\nu}$ are the choices of h, $\hat{h}$ and $\bar{g}$ in Step **I4′** and that of a_j in Step **Sj1-2** of the ν-th Server's query phase. The distribution

$$\Delta^2_{2,\nu} = \{(g_2, g_3^{r_0}, g^{r_1}, g_1) \mid r_0 \in_r \mathbb{Z}_q^*,\ r_1 \in \mathbb{Z}_q,\ g_1, g_2, g_3 \in_r \mathbb{G}_q\}$$

over $\mathbb{G}_q^4$ is identical to the distribution of $(h, \hat{h}, \bar{g}, a_j)$ constructed in $\widetilde{\mathcal{M}}^{\beta}_{2,\nu}(w)$, and is uniform. Since the distribution of $(h, \hat{h}, \bar{g}, a_j)$ constructed in $\mathcal{M}^{\beta}_{2,\nu}(w)$ is also uniform over $\mathbb{G}_q^4$, we have

$$\Pr_{w\in\widetilde{\mathrm{DH}}}[\widetilde{\varphi}^{\beta}_{2,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu} \wedge I_\nu] = \Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi^{\beta}_{2,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu} \wedge I_\nu].$$

(B-2) In order to estimate the last term on the right-hand side of (6.9), we assume that the event I_ν does not occur and that $\mathcal{A}$ enters the ν-th Server's query phase with a query $(V, u, e_j, u_{\tilde{p}}, v_{\tilde{p}}, \hat{u}_{\tilde{p}}, \hat{v}_{\tilde{p}}, \pi_{2,j})$. The differences between $\widetilde{\mathcal{M}}^{\beta}_{2,\nu}$ and $\mathcal{M}^{\beta}_{2,\nu}$ are the choices of h, $\hat{h}$ and $\bar{g}$ in Step **I4′**, and those of a_j and v_j in the ν-th Server's query phase.

We set $\delta_1 = x_1(r_p - r_{\tilde{p}})$ and $\delta_2 = p - \tilde{p}$, where $u_{\tilde{p}} = g^{r_{\tilde{p}}}$ and $\hat{v}_{\tilde{p}}/(\hat{u}_{\tilde{p}})^{\hat{x}} = \hat{h}^{\tilde{p}}$. Then the value v_j computed in the ν-th Server's query phase of $\widetilde{\mathcal{M}}^{\beta}_{2,\nu}$ is equal to $g_1^{\delta_1} g_3^{\delta_2}$. Let D_1 and D_2 be the distributions of $\delta_1 \in \mathbb{Z}_q$ and $\delta_2 \in \mathbb{Z}_q$, respectively. The distributions D_1 and D_2 depend on h, $\hat{h}$, $\bar{g}$ and a_j.

The distribution

$$\Delta^3_{2,\nu} = \{(g_2, g_3^{r_0}, g^{r_1}, g_1, g_1^{\delta_1} g_3^{\delta_2}) \mid g_1, g_2, g_3 \in_r \mathbb{G}_q,\ r_0 \in_r \mathbb{Z}_q^*,\ r_1 \in_r \mathbb{Z}_q\ \delta_1 \in D_1,\ \delta_2 \in D_2\}$$

is identical to the distribution of $(h, \hat{h}, \bar{g}, a_j, v_j)$ constructed in $\widetilde{\mathcal{M}}^{\beta}_{2,\nu}(w)$, and the distribution of $(h, \hat{h}, \bar{g}, a_j, v_j)$ constructed in $\mathcal{M}^{\beta}_{2,\nu}(w)$ is uniform over $\mathbb{G}_q^5$. The last term on the right-hand side of (6.9) is bounded by the statistical distance between $\Delta^3_{2,\nu}$ and $U_{\mathbb{G}_q^5}$. We note that $\delta_2 \neq 0$ holds if the event I_ν does not occur. Hence, we have

$$\begin{aligned}
&\left| \Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi^{\beta}_{2,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu} \wedge \neg I_\nu] - \Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi^{\beta}_{2,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu} \wedge \neg I_\nu] \right| \\
&\quad \le \sum_{m\in\mathbb{G}_q^5} \left| \Pr_{\boldsymbol{g}\in\Delta^3_{2,\nu}}[\boldsymbol{g} = m \wedge \delta_2 \neq 0] - \Pr_{\boldsymbol{g}\in U_{\mathbb{G}_q^5}}[\boldsymbol{g} = m \wedge \delta_2 \neq 0] \right|.
\end{aligned}$$

We write $m = (m_1, m_2, m_3, m_4, m_5) = (m', m_5) \in \mathbb{G}_q^5$ and $\boldsymbol{g} = (\boldsymbol{g}', \boldsymbol{g}_5)$. For any $m \in \mathbb{G}_q^5$, we have

$$\begin{aligned}\Pr_{\boldsymbol{g}\in U_{\mathbb{G}_q^5}}[\boldsymbol{g} = m \wedge \delta_2 \neq 0] &= \frac{1}{q^4} \Pr_{\boldsymbol{g}\in U_{\mathbb{G}_q^5}}[\boldsymbol{g} = m \wedge \delta_2 \neq 0 \mid \boldsymbol{g}' = m'] \\ &= \frac{1}{q^4} \Pr_{\boldsymbol{g}\in U_{\mathbb{G}_q^5}}[\boldsymbol{g}_5 = m_5 \mid \delta_2 \neq 0 \wedge \boldsymbol{g}' = m'] \Pr_{\boldsymbol{g}\in U_{\mathbb{G}_q^5}}[\delta_2 \neq 0 \mid \boldsymbol{g}' = m'] \\ &= \frac{1}{q^5} \Pr_{\boldsymbol{g}\in U_{\mathbb{G}_q^5}}[\delta_2 \neq 0 \mid \boldsymbol{g}' = m'].\end{aligned}$$

Since the value δ_2 depends on m', we have

$$\Pr_{\boldsymbol{g}\in U_{\mathbb{G}_q^5}}[\delta_2 \neq 0 \mid \boldsymbol{g}' = m'] = \Pr_{\boldsymbol{g}\in\Delta_{2,\nu}^3}[\delta_2 \neq 0 \mid \boldsymbol{g}' = m'].$$

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

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

$$\begin{aligned}\Pr_{\boldsymbol{g}\in\Delta_{2,\nu}^3}[\boldsymbol{g} = m \wedge \delta_2 \neq 0] &= \frac{1}{q^4} \Pr_{\boldsymbol{g}\in\Delta_{2,\nu}^3}[\boldsymbol{g}_5 = 1 \wedge \delta_2 \neq 0 \mid \boldsymbol{g}' = m'] \\ &= \frac{1}{q^4} \Pr_{\boldsymbol{g}\in\Delta_{2,\nu}^3}[1^{\delta_1+\delta_2} = 1 \mid \delta_2 \neq 0 \wedge \boldsymbol{g}' = m'] D(m') = \frac{D(m')}{q^4}.\end{aligned}$$

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

$$\Pr_{\boldsymbol{g}\in\Delta_{2,\nu}^3}[\boldsymbol{g} = m \wedge \delta_2 \neq 0] = \frac{1}{q^4} \Pr_{\boldsymbol{g}\in\Delta_{2,\nu}^3}[1^{\delta_1+\delta_2} = m_5 \mid \delta_2 \neq 0 \wedge \boldsymbol{g}' = m'] D(m') = 0.$$

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

$$\begin{aligned}\Pr_{\boldsymbol{g}\in\Delta_{2,\nu}^3}[\boldsymbol{g} = m \wedge \delta_2 \neq 0] &= \frac{1}{q^4} \Pr_{\boldsymbol{g}\in\Delta_{2,\nu}^3}[\boldsymbol{g}_3^{\delta_2} = m_5 \mid \delta_2 \neq 0 \wedge \boldsymbol{g}' = m'] D(m') \\ &= \frac{1}{q^4} \sum_{\tau_2 \neq 0} \Pr_{\boldsymbol{g}\in\Delta_{2,\nu}^3}[\boldsymbol{g}_3^{\delta_2} = m_5 \wedge \delta_2 = \tau_2 \mid \delta_2 \neq 0 \wedge \boldsymbol{g}' = m'] D(m') \\ &= \frac{1}{q^4} \sum_{\tau_2 \neq 0} \Pr_{\boldsymbol{g}\in\Delta_{2,\nu}^3}[\boldsymbol{g}_3^{\delta_2} = m_5 \mid \delta_2 = \tau_2 \wedge \delta_2 \neq 0 \wedge \boldsymbol{g}' = m'] \Pr_{\boldsymbol{g}\in\Delta_{2,\nu}^3}[\delta_2 = \tau_2 \mid \delta_2 \neq 0 \wedge \boldsymbol{g}' = m'] D(m') \\ &= \begin{cases} 0 & \text{if } m_5 = 1, \\ \dfrac{D(m')}{q^4(q-1)} & \text{otherwise.} \end{cases}\end{aligned}$$

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

$$\Pr_{\boldsymbol{g}\in\Delta_{2,\nu}^3}[\boldsymbol{g} = m \wedge \delta_2 \neq 0] = \frac{1}{q^4} \Pr_{\boldsymbol{g}\in\Delta_{2,\nu}^3}[m_4^{\delta_1} = m_5 \mid \delta_2 \neq 0 \wedge \boldsymbol{g}' = m'] D(m').$$

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

$$\frac{1}{q^4} \sum_{m_5 \in \mathbb{G}_q} \Pr_{\boldsymbol{g}\in\Delta_{2,\nu}^3}[m_4^{\delta_1} = m_5 \mid \delta_2 \neq 0 \wedge \boldsymbol{g}' = m'] D(m') = \frac{D(m')}{q^4}.$$

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

$$\begin{aligned}&\Pr_{\boldsymbol{g}\in\Delta_{2,\nu}^3}[\boldsymbol{g} = m \wedge \delta_2 \neq 0] \\ &= \frac{1}{q^4} \sum_{\tau \in \mathbb{Z}_q \times \mathbb{Z}_q^*} \Pr_{\boldsymbol{g}\in\Delta_{2,\nu}^3}[m_4^{\tau_1} \boldsymbol{g}_3^{\tau_2} = m_5 \mid \delta = \tau \wedge \delta_2 \neq 0 \wedge \boldsymbol{g}' = m'] \Pr_{\boldsymbol{g}\in\Delta_{2,\nu}^3}[\delta = \tau \wedge \delta_2 \neq 0 \wedge \boldsymbol{g}' = m'] D(m'),\end{aligned}$$

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

$$\Pr_{\boldsymbol{g}\in\Delta_{2,\nu}^3}[m_4^{\tau_1} \boldsymbol{g}_3^{\tau_2} = m_5 \mid \delta = \tau \wedge \delta_2 \neq 0 \wedge \boldsymbol{g}' = m'] = \begin{cases} 0 & \text{if } m_4^{\tau_1} = m_5 \\ \dfrac{1}{q-1} & \text{otherwise,} \end{cases}$$

and we see that

$$\begin{aligned}
&\sum_{m_5 \in \mathbb{G}_q} \left| \Pr_{\boldsymbol{g} \in \Delta^3_{2,\nu}} [\boldsymbol{g} = m \wedge \delta_2 \neq 0] - \Pr_{\boldsymbol{g} \in U_{\mathbb{G}_q^5}} [\boldsymbol{g} = m \wedge \delta_2 \neq 0] \right| \\
&= \frac{D(m')}{q^4} \sum_{\tau_1 \in \mathbb{Z}_q} \left| \frac{1}{q-1} \Pr_{\boldsymbol{g} \in \Delta^3_{2,\nu}} [\delta_1 \neq \tau_1 \mid \delta_2 \neq 0 \wedge \boldsymbol{g}' = m'] - \frac{1}{q} \right| \\
&= \frac{D(m')}{q^4(q-1)} \sum_{\tau_1 \in \mathbb{Z}_q} \left| \frac{1}{q} - \Pr_{\boldsymbol{g} \in \Delta^3_{2,\nu}} [\delta_1 = \tau_1 \mid \delta_2 \neq 0 \wedge \boldsymbol{g}' = m'] \right| \leq \frac{2D(m')}{q^4(q-1)}.
\end{aligned}$$

Since $D(m') \leq 1$, we obtain

$$\sum_{m \in \mathbb{G}_q^5} \left| \Pr_{\boldsymbol{g} \in \Delta^3_{2,\nu}} [\boldsymbol{g} = m \wedge \delta_2 \neq 0] - \Pr_{\boldsymbol{g} \in U_{\mathbb{G}_q^5}} [\boldsymbol{g} = m \wedge \delta_2 \neq 0] \right| \leq \frac{4q^2 - 1}{q^3}.$$

This value is negligible in k.

Note that, for any $0 \leq \nu \leq q_S$, the running time of $\widetilde{\mathcal{M}}^{\beta}_{2,\nu}$ is at most $T_3 = T + 4T_S + q_U f_3^U + q_S f_3^S + f_3^I$ for some polynomials f_3^U, f_3^S and f_3^I in n, t and k. So, if $T_3 \leq T_{\mathrm{ddh}}$, then the second term on the right-hand side of (6.7) is at most $\varepsilon_{\mathrm{ddh}}$. Consequently, we have

$$|p_{2,0}(d_\beta) - p_{2,q_S}(d_\beta)| \leq q_S(\varepsilon_{\mathrm{ddh}} + 2\varepsilon_{\mathrm{SS}} + \widetilde{\omega}_3),$$

where $\widetilde{\omega}_3$ is negligible in k.

6.4 Proof of Lemma 5.4

The distribution of y_1 constructed in $\mathcal{M}^{\beta}_{3,0}$ is identical to that constructed in $\mathcal{M}^{\beta}_{3,2}$. This implies that the distribution of $(g, y_1, y_2, h, \hat{g}, \hat{h}, \hat{y}, \bar{g}, \mathrm{pub}_2, \mathrm{pub}_3)$ constructed in $\mathcal{M}^{\beta}_{3,0}$ is identical to that constructed in $\mathcal{M}^{\beta}_{3,2}$.

We note the following two facts:

F1 This fact is due to the property of the secret sharing $\mathsf{SS}_{t,n}$. For any $x, x' \in \mathbb{Z}_q$, we set $\{x_j\}_{j=1}^n = \mathsf{SS}_{t,n}(x)$ and $\{x'_j\}_{j=1}^n = \mathsf{SS}_{t,n}(x')$. 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 $\mathsf{SS}_{t,n}$. 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

$$\Pr[x_{j_0} = m_{j_0} \mid (x_{j_1}, \ldots, x_{j_{t'}}) = (m_{j_1}, \ldots, m_{j_{t'}})] = \Pr[x'_{j_0} = m_{j_0} \mid (x'_{j_1}, \ldots, x'_{j_{t'}}) = (m_{j_1}, \ldots, m_{j_{t'}})] = \frac{1}{q}.$$

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

$$\Pr_{r \in_r \mathbb{Z}_q} [y = g^x h^r] = \Pr_{r \in_r \mathbb{Z}_q} [y = g^{x'} h^r].$$

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 $(\{y_{1,j}\}_{j=1}^n, \{y_{2,j}\}_{j=1}^n, \{\mathrm{sec}_j\}_{j \in V'})$ constructed in $\mathcal{M}^{\beta}_{3,0}$ is identical to that constructed in $\mathcal{M}^{\beta}_{3,2}$. Namely, the distribution of $(\mathrm{pub}, \mathrm{sec}_{V'})$ constructed in $\mathcal{M}^{\beta}_{3,0}$ is also identical that constructed in $\mathcal{M}^{\beta}_{3,2}$.

Assume that $h \neq 1$. We note that the only difference between $\mathcal{M}^{\beta}_{3,0}$ and $\mathcal{M}^{\beta}_{3,2}$ 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 $\mathcal{A}$ enters User's query phase with a query $\{(j, a_j, b_j, \bar{a}_j, \pi_{1,j})\}_{j \in [n]}$, the distribution of the answer $(V, u, e_j, u_{\tilde{p}}, v_{\tilde{p}}, \hat{u}_{\tilde{p}}, \hat{v}_{\tilde{p}}, \pi_{2,j})$ constructed in $\mathcal{M}^{\beta}_{3,0}$ is identical to that constructed in $\mathcal{M}^{\beta}_{3,2}$.

In Server's query phase, the answer $(u_{z_j}, v_{z_j}, \pi_{3,j})$ depends on the secret seed $x_{1,j}$ although the answer $(j, a_j, b_j, \bar{a}_j, \pi_{1,j})$ is independent of it. There are the following two cases to consider:

- Assume that $\hat{v}_{\tilde{p}}/(\hat{u}_{\tilde{p}})^{\hat{x}} \neq \hat{h}^p$. Then v_j is randomly chosen in Step **S$_j$2-4**. So we may regard that in Step **S$_j$2-5**, the value z_j is uniformly chosen from $\mathbb{G}_q$. Hence, the distribution of (u_{z_j}, v_{z_j}) constructed in $\mathcal{M}^{\beta}_{3,0}$ is identical to that constructed in $\mathcal{M}^{\beta}_{3,2}$.
- Assume that $\hat{v}_{\tilde{p}}/(\hat{u}_{\tilde{p}})^{\hat{x}} = \hat{h}^p$ holds. Then the distribution of (u_{z_j}, v_{z_j}) depends on the secret seed $x_{1,j}$. However, if $\#\mathrm{Idset} < t - t'$, that is, $\mathrm{F} = \mathrm{false}$, then the fact **F1** implies that the distribution of $x_{1,j} \in \mathbb{Z}_q$ is uniform. Hence, under the condition that $\mathrm{F} = \mathrm{false}$, the distribution of (u_{z_j}, v_{z_j}) constructed in $\mathcal{M}^{\beta}_{3,0}$ is identical to that constructed in $\mathcal{M}^{\beta}_{3,2}$.

The same argument can be applied even when we replace $\mathcal{M}^{\beta}_{3,2}$ by $\mathcal{M}^{\beta}_{3,1}$. In summary, we see that $\Pr[F_{3,0,d_\beta} \wedge h \neq 1] = \Pr[F_{3,2,d_\beta} \wedge h \neq 1]$ and $p_{3,0}^{\neg F \wedge h \neq 1}(d_\beta) = p_{3,1}^{\neg F \wedge h \neq 1}(d_\beta)$, where $p_{3,\nu}^{\neg F \wedge h \neq 1}(d_\beta) = \Pr[E_{3,\nu,d_\beta} \wedge \neg F_{3,\nu,d_\beta} \wedge h \neq 1]$ for $\nu = 0, 1$. We have

$$\begin{aligned}\Pr[F_{3,0,d_\beta}] &\le \left|\Pr[F_{3,0,d_\beta}] - \Pr[F_{3,2,d_\beta}]\right| + \Pr[F_{3,2,d_\beta}]\\ &\le \left|\Pr[F_{3,0,d_\beta} \wedge h \neq 1] - \Pr[F_{3,2,d_\beta} \wedge h \neq 1]\right| + \left|\Pr[F_{3,0,d_\beta} \wedge h = 1] - \Pr[F_{3,2,d_\beta} \wedge h = 1]\right| + \Pr[F_{3,2,d_\beta}]\\ &\le \frac{1}{q} + \Pr[F_{3,2,d_\beta}].\end{aligned}$$

The symmetric argument yields

$$\Pr[F_{3,2,d_\beta}] \le \frac{1}{q} + \Pr[F_{3,0,d_\beta}].$$

Set $p_{3,\nu}^{\neg F\wedge h=1}(d_\beta) = p_{3,\nu}^{\neg F}(d_\beta) - p_{3,\nu}^{\neg F\wedge h\neq 1}(d_\beta)$. Since $p_{3,\nu}^{\neg F\wedge h=1}(d_\beta) \le 1/q$, we have

$$\begin{aligned}\left|p_{3,0}^{\neg F}(d_1) - p_{3,0}^{\neg F}(d_2)\right| &\le \left|p_{3,0}^{\neg F}(d_1) - p_{3,1}^{\neg F}(d_1)\right| + \left|p_{3,1}^{\neg F}(d_1) - p_{3,1}^{\neg F}(d_2)\right|\\ &+ \left|p_{3,1}^{\neg F}(d_2) - p_{3,0}^{\neg F}(d_2)\right| \le \frac{2}{q} + \left|p_{3,1}^{\neg F}(d_1) - p_{3,1}^{\neg F}(d_2)\right|,\end{aligned}$$

proving the lemma.

6.5 Proof of Lemmas 5.5 and 5.6

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

I3′: Set $y_1 = g_1$. Then, choose $x_2 \in_r \mathbb{Z}_q$, and compute $y_2 = g^{x_2}$, $\{x_{1,j}\}_{j=1}^{n} = \mathsf{SS}_{t,n}(0)$ and $\{x_{2,j}\}_{j=1}^{n} = \mathsf{SS}_{t,n}(x_2)$.
I6′: Set $u_{1,d} = g_2$ and $v_{1,d} = g_3 d_\beta$, and compute $(u_{2,d}, v_{2,d}) = (g^{r_{2,d}}, y_2^{r_{2,d}} d_\beta)$.

(A) Let $w \in \mathrm{DH}$. In Step **I6′** of $\widetilde{\mathcal{M}}_{4,\nu}^{\beta}$, if we set $r_{1,d} = \alpha_2$, where $g_2 = g^{\alpha_2}$, then one has $u_{1,d} = g^{r_{1,d}}$ and $v_{1,d} = y_1^{r_{1,d}} d_\beta$: these values are the same as the values obtained in Initialization phase of $\mathcal{M}_{3,\nu}^{\beta}$ with $r_{1,d} = \alpha_2$. Hence, the differences between $\mathcal{M}_{3,\nu}^{\beta}$ and $\widetilde{\mathcal{M}}_{4,\nu}^{\beta}$ are the choice of y_1 in Step **I3′** and that of $u_{1,d}$ in Step **I6′**. The distribution $\Delta_{4,\nu}^{1} = \{(g_1, g_2) \mid g_1, g_2 \in_r \mathbb{G}_q\}$ over $\mathbb{G}_q^2$ is identical to the distribution of $(y_1, u_{1,d})$ constructed in $\widetilde{\mathcal{M}}_{4,\nu}^{\beta}(w)$. In particular, $\Delta_{4,\nu}^{1}$ is uniform over $\mathbb{G}_q^2$, and is identical to the distribution of $(y_1, u_{1,d})$ constructed in $\mathcal{M}_{4,\nu}^{\beta}(w)$.

(B) Let $w \in \widetilde{\mathrm{DH}}$. By the similar argument to (A), we see that the differences between $\widetilde{\mathcal{M}}_{4,\nu}^{\beta}$ and $\mathcal{M}_{4,\nu}^{\beta}$ are the choice of y_1 in Step **I3′** and those of $u_{1,d}$ and $v_{1,d}$ in Step **I6′**. The distribution $\Delta_{4,\nu}^{2} = \{(g_1, g_2, g_3 d_\beta) \mid g_1, g_2, g_3 \in_r \mathbb{G}_q\}$ over $\mathbb{G}_q^3$ is identical to the distribution of $(y_1, u_{1,d}, v_{1,d})$ constructed in $\widetilde{\mathcal{M}}_{4,\nu}^{\beta}(w)$. The distribution $\Delta_{4,\nu}^{2}$ is uniform, and is identical to the distribution of $(y_1, u_{1,d}, v_{1,d})$ constructed in $\mathcal{M}_{4,\nu}^{\beta}(w)$.

Note that $\varphi_{3,\nu}^{\beta}$ and $\varphi_{4,\nu}^{\beta}$ are independent of g_1, g_2 and g_3. Since the maximum T_5 of the running times of $\widetilde{\mathcal{M}}_{4,1}^{\beta}$ and $\widetilde{\mathcal{M}}_{4,2}^{\beta}$ is at most $T + 4T_S + q_U f_5^U + q_S f_5^S + f_5^I$ for some polynomials f_5^U, f_5^S and f_5^I in n, t and k, if $T_5 \le T_{\mathrm{ddh}}$, then we have

$$|\Pr[F_{3,2,d_\beta}] - \Pr[F_{4,2,d_\beta}]| = \left|\Pr_{w\in\mathrm{DH}}[\varphi_{3,2}^{\beta} = 1] - \Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi_{4,2}^{\beta} = 1]\right| = \left|\Pr_{w\in\mathrm{DH}}[\widetilde{\varphi}_{3,2}^{\beta} = 1] - \Pr_{w\in\widetilde{\mathrm{DH}}}[\widetilde{\varphi}_{4,2}^{\beta} = 1]\right| < \varepsilon_{\mathrm{ddh}}$$

and

$$|p_{3,1}^{\neg F}(d_\beta) - p_{4,1}^{\neg F}(d_\beta)| = \left|\Pr_{w\in\mathrm{DH}}[\varphi_{3,1}^{\beta} = 1] - \Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi_{4,1}^{\beta} = 1]\right| = \left|\Pr_{w\in\mathrm{DH}}[\widetilde{\varphi}_{3,1}^{\beta} = 1] - \Pr_{w\in\widetilde{\mathrm{DH}}}[\widetilde{\varphi}_{4,1}^{\beta} = 1]\right| < \varepsilon_{\mathrm{ddh}}.$$

We next prove Lemma 5.6. We construct two intermediary machines $\widetilde{\mathcal{M}}_{4,3}^{\beta}$ and $\widetilde{\mathcal{M}}_{4,4}^{\beta}$. On input $w = (Q, g, g_1, g_2, g_3)$, $\widetilde{\mathcal{M}}_{4,3}^{\beta}$ and $\widetilde{\mathcal{M}}_{4,4}^{\beta}$ simulate $\mathcal{M}_{4,3}^{\beta}$ and $\mathcal{M}_{4,4}^{\beta}$, resptectively, except for the following steps:

I3′: Set $y_2 = g_1$. Then, choose $x_2 \in_r \mathbb{Z}_q$ and $y_1 \in_r \mathbb{G}_q$, and compute $\{x_{1,j}\}_{j=1}^{n} = \mathsf{SS}_{t,n}(0)$ and $\{x_{2,j}\}_{j=1}^{n} = \mathsf{SS}_{t,n}(x_2)$.
I6″: Choose $u_{1,d}, v_{1,d} \in_r \mathbb{G}_q$, and set $u_{2,d} = g_2$ and $v_{2,d} = g_3 d_\beta$.

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 $\widetilde{\mathcal{M}}_{5,\nu}^{\beta}$. On input $w = (Q, g, g_1, g_2, g_3)$, $\widetilde{\mathcal{M}}_{5,\nu}^{\beta}$ simulates $\mathcal{M}_{5,\nu}^{\beta}$ except for the following steps:

I3′: Set $y_1 = g_2$. Then, choose $x_2 \in_r \mathbb{Z}_q$, and compute $y_2 = g^{x_2}$, $\{x_{1,j}\}_{j=1}^{n} = \mathsf{SS}_{t,n}(0)$ and $\{x_{2,j}\}_{j=1}^{n} = \mathsf{SS}_{t,n}(x_2)$.
I4′: Choose $r_p, r_{1,d}, r_{2,d}, \hat{x}, r_0, r_2 \in_r \mathbb{Z}_q$ and $r_1, r_3 \in_r \mathbb{Z}_q^*$, and set $h = g^{r_0}$, $\hat{g} = g_3^{r_3}$, $\hat{h} = g_1^{r_1}$ and $\bar{g} = g^{r_2}$. Then, compute $\hat{y} = (\hat{g})^{\hat{x}}$.
S$_\mathbf{j}$1-2: If $C_S = \nu$, then set $a_j = g_1$, $b_j = g_1^{r_p}$ and $\bar{a}_j = g_1^{r_2}$. Otherwise, execute the Step **S$_\mathbf{j}$1-2** of $\mathcal{M}_{5,\nu}^{\beta}$.
S$_\mathbf{j}$2-4″: If $C_S = \nu$ and $\hat{v}_{\tilde{p}}/(\hat{u}_{\tilde{p}})^{\hat{x}} = \hat{h}^{p}$ hold, then set

$$v_j = g_3^{r_p} g_1^{p r_0} \left(\frac{\hat{v}_{\tilde{p}}}{(\hat{u}_{\tilde{p}})^{\hat{x}}}\right)^{-r_0/r_1} (\hat{u}_{\tilde{p}})^{-1/r_3}.$$

If $C_S = \nu$ and $\hat{v}_{\tilde{p}}/(\hat{u}_{\tilde{p}})^{\hat{x}} \neq \hat{h}^p$ hold, then choose $v_j \in_r \mathbb{G}_q$. Otherwise, execute Step **S** $\mathbf{S_j 2\text{-}4''}$ of $\mathcal{M}^{\beta}_{5,\nu}$.
Noting that $\varphi^{\beta}_{5,\nu}$ is independent of g_1, g_2 and g_3, we have

$$
\begin{aligned}
&|\Pr[F_{5,\nu-1,d_\beta}] - \Pr[F_{5,\nu,d_\beta}]| \\
&\quad \leq \left| \underset{w\in\mathrm{DH}}{\Pr}[\varphi^{\beta}_{5,\nu-1} = 1] - \underset{w\in\mathrm{DH}}{\Pr}[\widetilde{\varphi}^{\beta}_{5,\nu} = 1] \right| + \left| \underset{w\in\mathrm{DH}}{\Pr}[\widetilde{\varphi}^{\beta}_{5,\nu} = 1] - \underset{w\in\widetilde{\mathrm{DH}}}{\Pr}[\widetilde{\varphi}^{\beta}_{5,\nu} = 1] \right| \\
&\quad\quad + \left| \underset{w\in\widetilde{\mathrm{DH}}}{\Pr}[\widetilde{\varphi}^{\beta}_{5,\nu} = 1] - \underset{w\in\widetilde{\mathrm{DH}}}{\Pr}[\varphi^{\beta}_{5,\nu} = 1] \right|. \qquad (6.10)
\end{aligned}
$$

We estimate the first and the last terms on the right-hand side of (6.10). Let $E^{\mathrm{SS}}_{U,\nu}$ denote the event defined as in the proof of Lemma 5.3. If the running time of $\mathcal{S}(\mathcal{L}^{\mathrm{pub}}_U)$ used in $\mathcal{M}^{\beta}_{5,\nu-1}$, $\widetilde{\mathcal{M}}^{\beta}_{5,\nu}$ and $\mathcal{M}^{\beta}_{5,\nu}$ is at most T_S, and $\max\{nq_U, q_S\} \leq q^S_H, q^S_P$ holds, then we have

$$
\begin{aligned}
&\left| \underset{w\in\mathrm{DH}}{\Pr}[\varphi^{\beta}_{5,\nu-1} = 1] - \underset{w\in\mathrm{DH}}{\Pr}[\widetilde{\varphi}^{\beta}_{5,\nu} = 1] \right| + \left| \underset{w\in\widetilde{\mathrm{DH}}}{\Pr}[\widetilde{\varphi}^{\beta}_{5,\nu} = 1] - \underset{w\in\widetilde{\mathrm{DH}}}{\Pr}[\varphi^{\beta}_{5,\nu} = 1] \right| \\
&\quad \leq 2\varepsilon_{\mathrm{SS}} + \left| \underset{w\in\mathrm{DH}}{\Pr}[\varphi^{\beta}_{5,\nu-1} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu}] - \underset{w\in\mathrm{DH}}{\Pr}[\widetilde{\varphi}^{\beta}_{5,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu}] \right| \\
&\quad\quad + \left| \underset{w\in\widetilde{\mathrm{DH}}}{\Pr}[\widetilde{\varphi}^{\beta}_{5,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu}] - \underset{w\in\widetilde{\mathrm{DH}}}{\Pr}[\varphi^{\beta}_{5,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu}] \right|. \qquad (6.11)
\end{aligned}
$$

In order to estimate other terms, we assume that the event $E^{\mathrm{SS}}_{U,\nu}$ does not occur.

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

$$
\begin{aligned}
&\left| \underset{w\in\mathrm{DH}}{\Pr}[\varphi^{\beta}_{5,\nu-1} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu}] - \underset{w\in\mathrm{DH}}{\Pr}[\widetilde{\varphi}^{\beta}_{5,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu}] \right| \\
&\quad \leq \left| \underset{w\in\mathrm{DH}}{\Pr}[\varphi^{\beta}_{5,\nu-1} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu} \wedge I_\nu] - \underset{w\in\mathrm{DH}}{\Pr}[\widetilde{\varphi}^{\beta}_{5,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu} \wedge I_\nu] \right| \\
&\quad\quad + \left| \underset{w\in\mathrm{DH}}{\Pr}[\varphi^{\beta}_{5,\nu-1} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu} \wedge \neg I_\nu] - \underset{w\in\mathrm{DH}}{\Pr}[\widetilde{\varphi}^{\beta}_{5,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu} \wedge \neg I_\nu] \right|, \qquad (6.12)
\end{aligned}
$$

where I_ν 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_ν occurs. In the ν-th Server's query phase of $\widetilde{\mathcal{M}}^{\beta}_{5,\nu}$, if we set $t_j = \alpha_1$, where $g_1 = g^{\alpha_1}$, then one has $a_j = g^{t_j}$, $b_j = u_p^{t_j}$, $\bar{a}_j = (\bar{g})^{t_j}$ and

$$
v_j = g_3^{r_p} \hat{u}_{\tilde{p}}^{-1/r_3} = \frac{u_p^{t_j x_1} h^{p t_j}}{u_{\tilde{p}}^{t_j x_1} h^{p t_j}} = \left(\frac{v_p}{v_{\tilde{p}}} \right)^{t_j}.
$$

This shows that these values are the same as the values obtained in the ν-th Server's query phase of $\mathcal{M}^{\beta}_{5,\nu-1}$ with $t_j = \alpha_1$. Hence, the differences between $\mathcal{M}^{\beta}_{5,\nu-1}$ and $\widetilde{\mathcal{M}}^{\beta}_{5,\nu}$ are the choice of y_1 in Step **I3′**, those of h, $\hat{g}$, $\hat{h}$ and $\bar{g}$ in Step **I4** and that of a_j in Step $\mathbf{S_j 1\text{-}2}$ in the ν-th Server's query phase. We define the distribution $\Delta^1_{5,\nu}$ over $\mathbb{G}_q^6$ by

$$
\Delta^1_{5,\nu} = \{(g^{\alpha_2}, g^{r_0}, g^{\alpha_1\alpha_2 r_3}, g^{\alpha_1 r_1}, g^{r_2}, g^{\alpha_1}) \mid r_0, r_2, \alpha_1, \alpha_2 \in_r \mathbb{Z}_q,\ r_1, r_3 \in_r \mathbb{Z}_q^*\}.
$$

The distribution $\Delta^1_{5,\nu}$ is identical to the distribution of $(y_1, h, \hat{g}, \hat{h}, \bar{g}, a_j)$ constructed in $\widetilde{\mathcal{M}}^{\beta}_{5,\nu}(w)$. In addition, the distribution of $(y_1, h, \hat{g}, \hat{h}, \bar{g}, a_j)$ constructed in $\mathcal{M}^{\beta}_{5,\nu-1}(w)$ is uniform over $\mathbb{G}_q^6$. The first term on the right-hand side of (6.12) is bounded by the statistical distance between $\Delta^1_{5,\nu}$ and $U_{\mathbb{G}_q^6}$. Since the distribution $\{(g^{r_0}, g^{r_2}) \mid r_0, r_2 \in_r \mathbb{Z}_q\}$ over $\mathbb{G}_q^2$ is uniform, the statistical distance between $\Delta^1_{5,\nu}$ and $U_{\mathbb{G}_q^6}$ is less than the distance between the distribution

$$
\bar{\Delta}^1_{5,\nu} = \{(g^{\alpha_2}, g^{\alpha_1\alpha_2 r_3}, g^{\alpha_1 r_1}, g^{\alpha_1}) | \alpha_1, \alpha_2 \in_r \mathbb{Z}_q,\ r_1, r_3 \in_r \mathbb{Z}_q^*\}
$$

over $\mathbb{G}_q^4$ and $U_{\mathbb{G}_q^4}$. For any $\hat{g} \in \mathbb{G}_q \setminus \{1\}$ and $\hat{h}, a_j \in \mathbb{G}_q$, we have

$$
\underset{\boldsymbol{g}\in\bar{\Delta}^1_{5,\nu}}{\Pr}[\boldsymbol{g} = (1, \hat{g}, \hat{h}, a_j)] = 0.
$$

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

$$
\begin{aligned}
&\underset{\boldsymbol{g}\in\bar{\Delta}^1_{5,\nu}}{\Pr}[\boldsymbol{g} = (y_1, 1, \hat{h}, a_j)] = \underset{\boldsymbol{g}\in\bar{\Delta}^1_{5,\nu}}{\Pr}[\boldsymbol{g} = (y_1, 1, 1, a_j)] = \underset{\boldsymbol{g}\in\bar{\Delta}^1_{5,\nu}}{\Pr}[\boldsymbol{g} = (y_1, 1, \hat{h}, 1)] = \underset{\boldsymbol{g}\in\bar{\Delta}^1_{5,\nu}}{\Pr}[\boldsymbol{g} = (y_1, \hat{g}, 1, a_j)] \\
&\quad = \underset{\boldsymbol{g}\in\bar{\Delta}^1_{5,\nu}}{\Pr}[\boldsymbol{g} = (y_1, \hat{g}, \hat{h}, 1)] = \underset{\boldsymbol{g}\in\bar{\Delta}^1_{5,\nu}}{\Pr}[\boldsymbol{g} = (y_1, \hat{g}, 1, 1)] = \underset{\boldsymbol{g}\in\bar{\Delta}^1_{5,\nu}}{\Pr}[\boldsymbol{g} = (1, 1, \hat{h}, 1)] = \underset{\boldsymbol{g}\in\bar{\Delta}^1_{5,\nu}}{\Pr}[\boldsymbol{g} = (1, 1, 1, a_j)] = 0,
\end{aligned}
$$

$$\Pr_{\boldsymbol{g}\in\bar{\Delta}^1_{5,\nu}}[\boldsymbol{g}=(y_1,1,1,1)]=\Pr_{\boldsymbol{g}\in\bar{\Delta}^1_{5,\nu}}[\boldsymbol{g}=(1,1,1,1)]=\frac{1}{q^2},\quad \Pr_{\boldsymbol{g}\in\bar{\Delta}^1_{5,\nu}}[\boldsymbol{g}=(1,1,\hat{h},a_j)]=\frac{1}{q^2(q-1)}$$

and

$$\Pr_{\boldsymbol{g}\in\bar{\Delta}^1_{5,\nu}}[\boldsymbol{g}=(y_1,\hat{g},\hat{h},a_j)]=\frac{1}{q^2(q-1)^2}.$$

Hence, the statistical distance between $\Delta^1_{5,\nu}$ and $U_{\mathbb{G}_q^6}$ 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_ν does not occur. Then, the value v_j is uniformly chosen in the ν-th Server's query phase of both $\mathcal{M}^\beta_{5,\nu-1}$ and $\widetilde{\mathcal{M}}^\beta_{5,\nu}$. Hence, the differences between $\mathcal{M}^\beta_{5,\nu-1}$ and $\widetilde{\mathcal{M}}^\beta_{5,\nu}$ are the same as the case where I_ν occurs, and we have

$$\left|\Pr_{w\in\mathrm{DH}}[\varphi^\beta_{5,\nu-1}=1\wedge\neg E^{\mathrm{SS}}_{U,\nu}]-\Pr_{w\in\mathrm{DH}}[\widetilde{\varphi}^\beta_{5,\nu}=1\wedge\neg E^{\mathrm{SS}}_{U,\nu}]\right|\le\frac{4(q-1)(4q^2-3q+2)}{q^4}.$$

This value is negligible in k.

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

$$\begin{aligned}&\left|\Pr_{w\in\widetilde{\mathrm{DH}}}[\widetilde{\varphi}^\beta_{5,\nu}=1\wedge\neg E^{\mathrm{SS}}_{U,\nu}]-\Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi^\beta_{5,\nu}=1\wedge\neg E^{\mathrm{SS}}_{U,\nu}]\right|\\&\le\left|\Pr_{w\in\widetilde{\mathrm{DH}}}[\widetilde{\varphi}^\beta_{5,\nu}=1\wedge\neg E^{\mathrm{SS}}_{U,\nu}\wedge I_\nu]-\Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi^\beta_{5,\nu}=1\wedge\neg E^{\mathrm{SS}}_{U,\nu}\wedge I_\nu]\right|\\&+\left|\Pr_{w\in\widetilde{\mathrm{DH}}}[\widetilde{\varphi}^\beta_{5,\nu}=1\wedge\neg E^{\mathrm{SS}}_{U,\nu}\wedge\neg I_\nu]-\Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi^\beta_{5,\nu}=1\wedge\neg E^{\mathrm{SS}}_{U,\nu}\wedge\neg I_\nu]\right|.\end{aligned}\tag{6.13}$$

(B-1) In order to estimate the last term on the right-hand side of (6.13), we assume that the event I_ν does not occur. Then the differences between $\widetilde{\mathcal{M}}^\beta_{5,\nu}$ and $\mathcal{M}^\beta_{5,\nu}$ are the same as the case of **(A-2)**. The distribution

$$\Delta^2_{5,\nu}=\{(g_2,g^{r_0},g_3^{r_3},g_1^{r_1},g^{r_2},g_1)\mid r_0,r_2\in_r\mathbb{Z}_q,\ r_1,r_3\in_r\mathbb{Z}_q^*,\ g_1,g_2,g_3\in_r\mathbb{G}_q\}$$

over $\mathbb{G}_q^6$ is identical to the distribution of $(y_1,h,\hat{g},\hat{h},\bar{g},a_j)$ constructed in $\widetilde{\mathcal{M}}^\beta_{5,\nu}(w)$. In addition, the distribution of $(y_1,h,\hat{g},\hat{h},\bar{g},a_j)$ constructed in $\mathcal{M}^\beta_{5,\nu}(w)$ is uniform over $\mathbb{G}_q^6$. The last term on the right-hand side of (6.13) is bounded by the statistical distance between $\Delta^2_{5,\nu}$ and $U_{\mathbb{G}_q^6}$. Since the distribution

$$\{(g_2,g^{r_0},g_3^{r_3},g^{r_2})\mid r_0,r_2\in_r\mathbb{Z}_q,\ r_3\in_r\mathbb{Z}_q^*,\ g_2,g_3\in_r\mathbb{G}_q\}$$

over $\mathbb{G}_q^4$ is uniform, the statistical distance between $\Delta^2_{5,\nu}$ and $U_{\mathbb{G}_q^6}$ is less than the distance between $U_{\mathbb{G}_q^2}$ and $\widetilde{\Delta}^1_{1,\nu,\xi}$ defined in the proof of Lemma 5.2. Hence, the statistical distance between $\Delta^2_{5,\nu}$ and $U_{\mathbb{G}_q^6}$ is at most $4(q-1)/q^2$, 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_ν occurs. Let R_ν denote the event such that $\mathcal{A}$ enters the ν-th Server's query phase with a query $(V,u,e_j,u_{\tilde{p}},v_{\tilde{p}},\hat{u}_{\tilde{p}},\hat{v}_{\tilde{p}},\pi_{2,j})$ which satisfies the following two conditions: **(i)** $u_{\tilde{p}}=u_p$ and **(ii)** $\pi_{2,j}$ is a valid proof. We have

$$\begin{aligned}&\left|\Pr_{w\in\widetilde{\mathrm{DH}}}[\widetilde{\varphi}^\beta_{5,\nu}=1\wedge\neg E^{\mathrm{SS}}_{U,\nu}\wedge I_\nu]-\Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi^\beta_{5,\nu}=1\wedge\neg E^{\mathrm{SS}}_{U,\nu}\wedge I_\nu]\right|\\&\le\left|\Pr_{w\in\widetilde{\mathrm{DH}}}[\widetilde{\varphi}^\beta_{5,\nu}=1\wedge\neg E^{\mathrm{SS}}_{U,\nu}\wedge I_\nu\wedge R_\nu]-\Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi^\beta_{5,\nu}=1\wedge\neg E^{\mathrm{SS}}_{U,\nu}\wedge I_\nu\wedge R_\nu]\right|\\&+\left|\Pr_{w\in\widetilde{\mathrm{DH}}}[\widetilde{\varphi}^\beta_{5,\nu}=1\wedge\neg E^{\mathrm{SS}}_{U,\nu}\wedge I_\nu\wedge\neg R_\nu]-\Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi^\beta_{5,\nu}=1\wedge\neg E^{\mathrm{SS}}_{U,\nu}\wedge I_\nu\wedge\neg R_\nu]\right|.\end{aligned}\tag{6.14}$$

(1) In order to estimate the last term on the right-hand side of (6.14), we assume that the event R_ν does not occur. The differences between $\widetilde{\mathcal{M}}^\beta_{5,\nu}$ and $\mathcal{M}^\beta_{5,\nu}$ are the choice of y_1 in Step **I3′**, those of h, $\hat{g}$, $\hat{h}$ and $\bar{g}$ in Step **I4**, and those of a_j and v_j in the ν-th Server's query phase.

If $\pi_{2,j}$ is invalid, then the value v_j is not computed in the ν-th Server's query phase. So the differences between $\widetilde{\mathcal{M}}^\beta_{5,\nu}$ and $\mathcal{M}^\beta_{5,\nu}$ are the same as the case of **(B-1)**.

Assume that $\pi_{2,j}$ is valid. We set $\delta=r_p-\tilde{r}_p$, where $u_{\tilde{p}}=g^{r_{\tilde{p}}}$. Then the value v_j computed in the ν-th Server's query phase of $\widetilde{\mathcal{M}}^\beta_{5,\nu}$ is equal to g_3^δ. Let D be the distribution of $\delta\in\mathbb{Z}_q$. The distribution D depends on y_1, h, $\hat{g}$, $\hat{h}$, $\bar{g}$ and a_j. The distribution

$$\Delta^3_{5,\nu} = \{(g_2, g^{r_0}, g_3^{r_3}, g_1^{r_1}, g^{r_2}, g_1, g_3^{\delta}) \mid r_1, r_3 \in_r \mathbb{Z}_q^*,\ r_0, r_2 \in_r \mathbb{Z}_q,\ g_1, g_2, g_3 \in_r \mathbb{G}_q,\ \delta \in D\}$$

is identical to the distribution of $(y_1, h, \hat{g}, \hat{h}, \bar{g}, a_j, v_j)$ constructed in $\widetilde{\mathcal{M}}^{\beta}_{5,\nu}(w)$, and the distribution of $(y_1, h, \hat{g}, \hat{h}, \bar{g}, a_j, v_j)$ constructed in $\mathcal{M}^{\beta}_{5,\nu}(w)$ 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 $\Delta^3_{5,\nu}$ and $U_{\mathbb{G}_q^7}$. We note that $\delta \neq 0$ if $\pi_{2,j}$ is valid. Hence, we have

$$\begin{aligned}
&\left| \underset{w\in\mathrm{DH}}{\underset{\sim}{\Pr}}[\widetilde{\varphi}^{\beta}_{5,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu} \wedge I_\nu \wedge \neg R_\nu] - \underset{w\in\mathrm{DH}}{\underset{\sim}{\Pr}}[\varphi^{\beta}_{5,\nu} = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu} \wedge I_\nu \wedge \neg R_\nu] \right| \\
&\qquad \le \frac{4(q-1)}{q^2} + \sum_{m\in\mathbb{G}_q^7} \left| \Pr_{g\in\Delta^3_{5,\nu}}[\boldsymbol{g} = m \wedge \delta \neq 0] - \Pr_{g\in U_{\mathbb{G}_q^7}}[\boldsymbol{g} = m \wedge \delta \neq 0] \right|.
\end{aligned}$$

We write $m = (m_1, \ldots, m_6, m_7) = (m', m_7) \in \mathbb{G}_q^7$ and $\boldsymbol{g} = (\boldsymbol{g}', \boldsymbol{g}_7)$. For any $m \in \mathbb{G}_q^7$, we have

$$\begin{aligned}
\Pr_{g\in U_{\mathbb{G}_q^7}}[\boldsymbol{g} = m \wedge \delta \neq 0] &= \frac{1}{q^6} \Pr_{g\in U_{\mathbb{G}_q^7}}[\boldsymbol{g} = m \wedge \delta \neq 0 \mid \boldsymbol{g}' = m'] \\
&= \frac{1}{q^6} \Pr_{g\in U_{\mathbb{G}_q^7}}[\boldsymbol{g}_7 = m_7 \mid \delta \neq 0 \wedge \boldsymbol{g}' = m'] \Pr_{g\in U_{\mathbb{G}_q^7}}[\delta \neq 0 \mid \boldsymbol{g}' = m'] \\
&= \frac{1}{q^7} \Pr_{g\in U_{\mathbb{G}_q^7}}[\delta \neq 0 \mid \boldsymbol{g}' = m'].
\end{aligned}$$

Since the value δ depends on m', we have

$$\Pr_{g\in U_{\mathbb{G}_q^7}}[\delta \neq 0 \mid \boldsymbol{g}' = m'] = \Pr_{g\in\Delta^3_{5,\nu}}[\delta \neq 0 \mid \boldsymbol{g}' = m'].$$

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

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

$$\Pr_{g\in\Delta^3_{5,\nu}}[\boldsymbol{g} = m \wedge \delta \neq 0] = \frac{1}{q^5} \Pr_{g\in\Delta^3_{5,\nu}}[\boldsymbol{g}_7 = 1 \wedge \delta \neq 0 \mid \boldsymbol{g}' = m'] = \frac{1}{q^5} \Pr_{g\in\Delta^3_{5,\nu}}[1^{\delta} = 1 \mid \delta \neq 0 \wedge \boldsymbol{g}' = m'] D(m') = \frac{D(m')}{q^5}.$$

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

$$\Pr_{g\in\Delta^3_{5,\nu}}[\boldsymbol{g} = m \wedge \delta \neq 0] = \frac{1}{q^5(q-1)} \Pr_{g\in\Delta^3_{5,\nu}}[1^{\delta} = 1 \mid \delta \neq 0 \wedge \boldsymbol{g}' = m'] D(m') = \frac{D(m')}{q^5(q-1)}.$$

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

$$\begin{aligned}
\Pr_{g\in\Delta^3_{5,\nu}}[\boldsymbol{g} = m \wedge \delta \neq 0] &= \frac{1}{q^5} \Pr_{g\in\Delta^3_{5,\nu}}[g_3^{\delta} = m_7 \mid \delta \neq 0 \wedge \boldsymbol{g}' = m'] D(m') \\
&= \frac{1}{q^5} \sum_{\tau\neq 0} \Pr_{g\in\Delta^3_{5,\nu}}[g_3^{\delta} = m_7 \mid \delta = \tau \wedge \delta \neq 0 \wedge \boldsymbol{g}' = m'] \Pr_{g\in\Delta^3_{5,\nu}}[\delta = \tau \mid \delta \neq 0 \wedge \boldsymbol{g}' = m'] D(m') \\
&= \frac{D(m')}{q^5(q-1)}.
\end{aligned}$$

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

$$\begin{aligned}
\Pr_{g\in\Delta^3_{5,\nu}}[\boldsymbol{g} = m \wedge \delta \neq 0] &= \frac{1}{q^5(q-1)} \Pr_{g\in\Delta^3_{5,\nu}}[g_3^{\delta} = m_7 \mid \delta \neq 0 \wedge \boldsymbol{g}' = m'] D(m') \\
&= \frac{1}{q^5(q-1)} \sum_{\tau\in\mathbb{Z}_q} \Pr_{g\in\Delta^3_{5,\nu}}[g_3^{\delta} = m_7 \mid \delta = \tau \wedge \delta \neq 0 \wedge \boldsymbol{g}' = m'] \Pr_{g\in\Delta^3_{5,\nu}}[\delta = \tau \mid \delta \neq 0 \wedge \boldsymbol{g}' = m'] D(m') \\
&= \frac{D(m')}{q^5(q-1)^2}.
\end{aligned}$$

If m does not apply to any cases above, then $\Pr_{g\in\Delta^3_{5,\nu}}[\boldsymbol{g} = m \wedge \delta \neq 0] = 0$ follows. Since $D(m') \le 1$, we obtain

$$\sum_{m\in\mathbb{G}_q^7} \left| \Pr_{g\in\Delta^3_{5,\nu}}[\boldsymbol{g} = m \wedge \delta \neq 0] - \Pr_{g\in U_{\mathbb{G}_q^7}}[\boldsymbol{g} = m \wedge \delta \neq 0] \right| \le \frac{8q^3 - 16q^2 + 16q - 8}{q^4},$$

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_ν occurs. Using the machines $\mathcal{M}^{\beta}_{5,\nu}$ and $\widetilde{\mathcal{M}}^{\beta}_{5,\nu}$, we construct new machines $\mathcal{N}^{\beta}_{5,\nu}$ and $\widetilde{\mathcal{N}}^{\beta}_{5,\nu}$ which solve the CDH problem. On input (Q, g, g_1, g_2), $\mathcal{N}^{\beta}_{5,\nu}$ works as follows:

(1) Choose $\alpha_1, \alpha_2, \alpha_3 \in_r \mathbb{Z}_q$, and simulate $\mathcal{M}^{\beta}_{5,\nu}$ on input $w = (Q, g, g^{\alpha_1}, g^{\alpha_2}, g^{\alpha_3})$ except for the following steps:

I3′: Choose $x_1, x_2 \in_r \mathbb{Z}_q$, and compute $y_1 = g^{x_1}$, $y_2 = g^{x_2}$, $\{x_{1,j}\}_{j=1}^{n} = \mathsf{SS}_{t,n}(0)$ and $\{x_{2,j}\}_{j=1}^{n} = \mathsf{SS}_{t,n}(x_2)$.

I4′: Choose $\hat{x} \in_r \mathbb{Z}_q$, $h, \hat{h}, \bar{g} \in_r \mathbb{G}_q$ and $r_{1,d}, r_{2,d} \in_r \mathbb{Z}_q$, and set $\hat{g} = g_1$. Then compute $\hat{y} = (\hat{g})^{\hat{x}}$.

I5: Choose a password $p \in_r \mathbb{Z}_q$, and set $u_p = g_2$ and $v_p = g_2^{x_1} h^p$.

(2) When $\mathcal{A}$ enters the ν-th Server's query phase with a query $(V, u, e_j, u_{\tilde{p}}, v_{\tilde{p}}, \hat{u}_{\tilde{p}}, \hat{v}_{\tilde{p}}, \pi_{2,j})$,

- if $u_p = u_{\tilde{p}}$ and $\pi_{2,j}$ is valid, then output $\hat{u}_{\tilde{p}}$, and halt.
- Otherwise, output $z \in_r \mathbb{G}_q$, and halt.

We note that if the event $\neg E^{\mathrm{SS}}_{U,\nu} \wedge R_\nu$ occurs in $\mathcal{N}^{\beta}_{5,\nu}$, then $\hat{u}_{\tilde{p}} = \mathsf{CDH}(Q, g, g_1, g_2)$ follows. In addition, we see that the probability that the event $\neg E^{\mathrm{SS}}_{U,\nu} \wedge R_\nu$ occurs in $\mathcal{N}^{\beta}_{5,\nu}$ is equal to that in $\mathcal{M}^{\beta}_{5,\nu}$ by the construction of $\mathcal{N}^{\beta}_{5,\nu}$. If the running time of $\mathcal{N}^{\beta}_{5,\nu}$ is less than T_{ddh}, then by Lemma 2.1, we have

$$\Pr_{w \in \widetilde{\mathrm{DH}}}[\mathcal{M}^{\beta}_{5,\nu}(w) = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu} \wedge I_\nu \wedge R_\nu] \le \Pr_{w \in \widetilde{\mathrm{DH}}}[\neg E^{\mathrm{SS}}_{U,\nu} \wedge R_\nu] \le \Pr[\mathcal{N}^{\beta}_{5,\nu}(Q, g, g_1, g_2) = \mathsf{CDH}(Q, g, g_1, g_2)] < \varepsilon_{\mathrm{ddh}} + \frac{1}{2^k}.$$

We next construct the machine $\widetilde{\mathcal{N}}^{\beta}_{5,\nu}$. $\widetilde{\mathcal{N}}^{\beta}_{5,\nu}$ works as follows: On input (Q, g, g_1, g_2),

(1) Choose $\alpha_1, \alpha_2 \in_r \mathbb{Z}_q$, and simulate $\widetilde{\mathcal{M}}^{\beta}_{5,\nu}$ on input $w = (Q, g, g^{\alpha_1}, g^{\alpha_2}, g_1)$ except for the following steps:

I5: Choose a password $p \in_r \mathbb{Z}_q$, and set $u_p = g_2$ and $v_p = g_2^{\alpha_2} h^p$.

$\mathbf{S_j}$1-2: if $C_S = \nu$, then set $a_j = g^{\alpha_1}$, $b_j = g_2^{\alpha_1}$ and $\bar{a}_j = \bar{g}^{\alpha_1}$. Otherwise, choose $t_j \in_r \mathbb{Z}_q$, and compute $a_j = g^{t_j}$, $b_j = u_p^{t_j}$ and $\bar{a}_j = (\bar{g})^{t_j}$.

(2) When $\mathcal{A}$ enters the ν-th Server's query phase with a query $(V, u, e_j, u_{\tilde{p}}, v_{\tilde{p}}, \hat{u}_{\tilde{p}}, \hat{v}_{\tilde{p}}, \pi_{2,j})$,

- if $u_p = u_{\tilde{p}}$ and $\pi_{2,j}$ is valid, then output $(\hat{u}_{\tilde{p}})^{1/r_3}$, and halt, where r_3 is chosen in Step **I4** of $\widetilde{\mathcal{M}}^{\beta}_{5,\nu}$.
- Otherwise, output $z \in_r \mathbb{G}_q$, and halt.

If the event $\neg E^{\mathrm{SS}}_{U,\nu} \wedge R_\nu$ occurs in $\widetilde{\mathcal{N}}^{\beta}_{5,\nu}$, then $(\hat{u}_{\tilde{p}})^{1/r_3} = \mathsf{CDH}(Q, g, g_1, g_2)$ follows. In addition, the probability that the event $\neg E^{\mathrm{SS}}_{U,\nu} \wedge R_\nu$ occurs in $\widetilde{\mathcal{N}}^{\beta}_{5,\nu}$ is equal to that in $\widetilde{\mathcal{M}}^{\beta}_{5,\nu}$ by the construction of $\widetilde{\mathcal{N}}^{\beta}_{5,\nu}$. Hence, if the running time of $\widetilde{\mathcal{N}}^{\beta}_{5,\nu}$ is less than T_{ddh}, then, by Lemma 2.1, we have

$$\Pr_{w \in \widetilde{\mathrm{DH}}}[\widetilde{\mathcal{M}}^{\beta}_{5,\nu}(w) = 1 \wedge \neg E^{\mathrm{SS}}_{U,\nu} \wedge I_\nu \wedge R_\nu] \le \Pr_{w \in \widetilde{\mathrm{DH}}}[\neg E^{\mathrm{SS}}_{U,\nu} \wedge R_\nu] \le \Pr[\widetilde{\mathcal{N}}^{\beta}_{5,\nu}(Q, g, g_1, g_2) = \mathsf{CDH}(Q, g, g_1, g_2)] < \varepsilon_{\mathrm{ddh}} + \frac{1}{2^k}.$$

Note that the maximum T_7 of the running times of machines $\{\mathcal{M}^{\beta}_{5,\nu}, \widetilde{\mathcal{M}}^{\beta}_{5,\nu}, \mathcal{N}^{\beta}_{5,\nu}, \widetilde{\mathcal{N}}^{\beta}_{5,\nu}\}_{\nu=0}^{q_S}$ is at most $T_7 = T + 4T_S + q_U f_7^U + q_S f_7^S + f_7^I$ for some polynomials f_7^U, f_7^S and f_7^I in n, t and k. So, if $T_7 \le T_{\mathrm{ddh}}$, then second term on the right-hand side of (6.10) is at most $\varepsilon_{\mathrm{ddh}}$. Consequently, we have

$$|\Pr[F_{5,0,d_\beta}] - \Pr[F_{5,q_S,d_\beta}]| \le q_S(2\varepsilon_{\mathrm{ddh}} + 2\varepsilon_{\mathrm{SS}} + \widetilde{\omega}_7),$$

where $\widetilde{\omega}_7$ is negligible in k.

6.7 Proof of Lemma 5.8

We construct an intermediary machine $\widetilde{\mathcal{M}}^{\beta}_{6,\nu}$. On input $w = (Q, g, g_1, g_2, g_3)$, $\widetilde{\mathcal{M}}^{\beta}_{6,\nu}$ simulates $\mathcal{M}^{\beta}_{6,\nu}$ except for the following steps:

I3′: Set $y_1 = g_2$. Then, choose $x_2 \in_r \mathbb{Z}_q$, and compute $y_2 = g^{x_2}$, $\{x_{1,j}\}_{j=1}^{n} = \mathsf{SS}_{t,n}(0)$ and $\{x_{2,j}\}_{j=1}^{n} = \mathsf{SS}_{t,n}(x_2)$.

I4′: Choose $r_p, r_{1,d}, r_{2,d}, \hat{x}, r_0 \in_r \mathbb{Z}_q$, $r_1 \in_r \mathbb{Z}_q^*$ and $h, \hat{h} \in_r \mathbb{G}_q$, and set $\hat{g} = g^{r_0}$ and $\bar{g} = g_1^{r_1}$. Then, compute $\hat{y} = (\hat{g})^{\hat{x}}$.

U1-3″: If $C_U = \nu$, then choose $\hat{v}_{\tilde{p}} \in_r \mathbb{G}_q$, and set $u_{\tilde{p}} = g_1$, $\hat{u}_{\tilde{p}} = g_1^{r_0}$ and $v_{\tilde{p}} = g_3 h^p$. Otherwise, execute Step **U1-3″** of $\mathcal{M}^{\beta}_{6,\nu}$.

U1-5: if $C_U = \nu$, then set $e_j = (\bar{a}_j)^{1/r_1}$ for each $j \in [n]$. Otherwise, execute Step **U1-5** of $\mathcal{M}^{\beta}_{6,\nu}$.

Noting that $\varphi^{\beta}_{6,\nu}$ is independent of g_1, g_2 and g_3, we have

$$\begin{aligned}
&|\Pr[F_{6,\nu-1,d_\beta}] - \Pr[F_{6,\nu,d_\beta}]| \\
&\le \left| \Pr_{w \in \mathrm{DH}}[\varphi^{\beta}_{6,\nu-1} = 1] - \Pr_{w \in \mathrm{DH}}[\widetilde{\varphi}^{\beta}_{6,\nu} = 1] \right| + \left| \Pr_{w \in \mathrm{DH}}[\widetilde{\varphi}^{\beta}_{6,\nu} = 1] - \Pr_{w \in \widetilde{\mathrm{DH}}}[\widetilde{\varphi}^{\beta}_{6,\nu} = 1] \right| \\
&\quad + \left| \Pr_{w \in \widetilde{\mathrm{DH}}}[\widetilde{\varphi}^{\beta}_{6,\nu} = 1] - \Pr_{w \in \widetilde{\mathrm{DH}}}[\varphi^{\beta}_{6,\nu} = 1] \right|. \qquad (6.15)
\end{aligned}$$

We estimate the first and the last terms on the right-hand side of (6.15). Let $E^{\mathrm{SS}}_{S1,\nu}$ denote the event defined as in the proof of Lemma 5.1. If the running time of $\mathcal{S}(\mathcal{L}^{\mathrm{pub}}_{S1})$ used in $\mathcal{M}^{\beta}_{6,\nu-1}$, $\mathcal{M}^{\beta}_{6,\nu}$ and $\widetilde{\mathcal{M}}^{\beta}_{6,\nu}$ is at most T_S, and $\max\{nq_U, q_S\} \le q_H^S, q_P^S$ holds, then we have

$$\begin{aligned}
&\left|\Pr_{w\in \mathrm{DH}}[\varphi^{\beta}_{6,\nu-1}=1]-\Pr_{w\in \mathrm{DH}}[\widetilde{\varphi}^{\beta}_{6,\nu}=1]\right|+\left|\Pr_{w\in \widetilde{\mathrm{DH}}}[\widetilde{\varphi}^{\beta}_{6,\nu}=1]-\Pr_{w\in \widetilde{\mathrm{DH}}}[\varphi^{\beta}_{6,\nu}=1]\right|\\
&\quad\le 2n\varepsilon_{\mathrm{SS}}+\left|\Pr_{w\in \mathrm{DH}}[\varphi^{\beta}_{6,\nu-1}=1\wedge\neg E^{\mathrm{SS}}_{S1,\nu}]-\Pr_{w\in \mathrm{DH}}[\widetilde{\varphi}^{\beta}_{6,\nu}=1\wedge\neg E^{\mathrm{SS}}_{S1,\nu}]\right|\\
&\qquad+\left|\Pr_{w\in \widetilde{\mathrm{DH}}}[\widetilde{\varphi}^{\beta}_{6,\nu}=1\wedge\neg E^{\mathrm{SS}}_{S1,\nu}]-\Pr_{w\in \widetilde{\mathrm{DH}}}[\varphi^{\beta}_{6,\nu}=1\wedge\neg E^{\mathrm{SS}}_{S1,\nu}]\right|. \qquad (6.16)
\end{aligned}$$

In order to estimate other terms, we assume that the event $E^{\mathrm{SS}}_{S1,\nu}$ does not occur.

(A) We first consider the second term on the right-hand side of (6.16). Let $w \in \mathrm{DH}$. Using the similar argument to (A) of the proof of Lemma 5.1, we see that the differences between $\mathcal{M}^{\beta}_{6,\nu-1}$ and $\widetilde{\mathcal{M}}^{\beta}_{6,\nu}$ are the choice of y_1 in Step **I3′**, those of $\hat{g}$, $\bar{g}$ and $\hat{y}$ in Step **I4′** and that of $u_{\tilde{p}}$ in Step **U1-3″** of the ν-th User's query phase. The distribution

$$\Delta^1_{6,\nu}=\{(g_2,g^{r_0},g_1^{r_1},g^{r_0\hat{x}},g_1)\mid r_0,\hat{x}\in_r\mathbb{Z}_q,\ r_1\in_r\mathbb{Z}_q^*,\ g_1,g_2\in_r\mathbb{G}_q\}$$

over $\mathbb{G}_q^5$ is identical to the distribution of $(y_1,\hat{g},\bar{g},\hat{y},u_{\tilde{p}})$ constructed in $\widetilde{\mathcal{M}}^{\beta}_{6,\nu}(w)$, and the distribution

$$\bar{\Delta}^1_{6,\nu}=\{(y_1,\hat{g},\bar{g},\hat{g}^{\hat{x}},g^{r_{\tilde{p}}})\mid \hat{x},r_{\tilde{p}}\in_r\mathbb{Z}_q,\ y_1,\hat{g},\bar{g}\in_r\mathbb{G}_q\}$$

over $\mathbb{G}_q^5$ is identical to the distribution of $(y_1,\hat{g},\bar{g},\hat{y},u_{\tilde{p}})$ constructed in $\mathcal{M}^{\beta}_{6,\nu-1}(w)$. The second term on the right-hand side of (6.16) is bounded by the statistical distance between $\Delta^1_{6,\nu}$ and $\bar{\Delta}^1_{6,\nu}$. Note that the distribution $\{(g_2,g^{r_0},g^{r_0\hat{x}})\mid r_0,\hat{x}\in_r\mathbb{Z}_q,\ g_2\in_r\mathbb{G}_q\}$ over $\mathbb{G}_q^3$ is identical to the distribution $\{(y_1,\hat{g},\hat{g}^{\hat{x}})\mid y_1,\hat{g}\in_r\mathbb{G}_q,\ \hat{x}\in_r\mathbb{Z}_q\}$ over $\mathbb{G}_q^3$. So, the statistical distance between $\Delta^1_{6,\nu}$ and $\bar{\Delta}^1_{6,\nu}$ is less than the distance between $U_{\mathbb{G}_q^2}$ and $\widetilde{\Delta}^1_{1,\nu,\xi}$ defined in the proof of Lemma 5.2. Hence, the statistical distance between $\widetilde{\Delta}^1_{6,\nu}$ and $U_{\mathbb{G}_q^2}$ is at most $4(q-1)/q^2$, which is negligible in k.

(B) We next consider the last term on the right-hand side of (6.16). Let $w\in\widetilde{\mathrm{DH}}$. By the similar argument to (A), we see that the differences between $\widetilde{\mathcal{M}}^{\beta}_{6,\nu}$ and $\mathcal{M}^{\beta}_{6,\nu}$ are the choice of y_1 in Step **I3′**, those of $\hat{g}$, $\bar{g}$ and $\hat{y}$ in Step **I4′** and those of $u_{\tilde{p}}$ and $v_{\tilde{p}}$ in Step **U1-3″** of the ν-th User's query phase. The distribution

$$\Delta^2_{6,\nu}=\{(g_2,g^{r_0},g_1^{r_1},g^{r_0\hat{x}},g_1,g_3h^p)\mid r_0,\hat{x},p\in_r\mathbb{Z}_q,\ r_1\in_r\mathbb{Z}_q^*,\ g_1,g_2,g_3,h\in_r\mathbb{G}_q\}$$

over $\mathbb{G}_q^6$ is identical to the distribution of $(y_1,\hat{g},\bar{g},\hat{y},u_{\tilde{p}},v_{\tilde{p}})$ constructed in $\widetilde{\mathcal{M}}^{\beta}_{6,\nu}(w)$, and the distribution

$$\widetilde{\Delta}^2_{6,\nu}=\{(y_1,\hat{g},\bar{g},\hat{g}^{\hat{x}},g^{r_{\tilde{p}}},v_{\tilde{p}})\mid \hat{x},r_{\tilde{p}}\in_r\mathbb{Z}_q,\ y_1,\hat{g},\bar{g},\hat{y},v_{\tilde{p}}\in_r\mathbb{G}_q\}$$

over $\mathbb{G}_q^6$ is identical to the distribution of $(y_1,\hat{g},\bar{g},\hat{y},u_{\tilde{p}},v_{\tilde{p}})$ constructed in $\mathcal{M}^{\beta}_{6,\nu}(w)$. The last term on the right-hand side of (6.16) is bounded by the statistical distance between $\Delta^2_{6,\nu}$ and $\tilde{\Delta}^2_{6\nu}$. Note that for any fixed $p\in\mathbb{Z}_q$ and $h\in\mathbb{G}_q$ the distribution $\{g_3h^p\mid g_3\in_r\mathbb{G}_q\}$ over $\mathbb{G}_q$ is uniform. So, by the same argument as above, the statistical distance between $\Delta^2_{6,\nu}$ and $\widetilde{\Delta}^2_{6,\nu}$ is less than the distance between $\widetilde{\Delta}^1_{6,\nu}$ and $U_{\mathbb{G}_q^2}$.

Note that, for any $0\le\nu\le q_U$, the running time of $\widetilde{\mathcal{M}}^{\beta}_{6,\nu}$ is at most $T_8=T+4T_S+q_Uf_8^U+q_Sf_8^S+f_8^I$ for some polynomials f_8^U, f_8^S and f_8^I in n, t and k. So, if $T_8\le T_{\mathrm{ddh}}$, then the second term on the right-hand side of (6.15) is at most $\varepsilon_{\mathrm{ddh}}$. Hence, we have

$$|\Pr[F_{6,0,d_\beta}]-\Pr[F_{6,q_U,d_\beta}]|\le q_U(\varepsilon_{\mathrm{ddh}}+2n\varepsilon_{\mathrm{SS}}+\widetilde{\omega}_8),$$

where $\widetilde{\omega}_8$ is negligible in k.

6.8 Proof of Lemma 5.9

We construct an intermediary machine $\widetilde{\mathcal{M}}^{\beta}_{7,0}$. On input $w=(Q,g,g_1,g_2,g_3)$, $\widetilde{\mathcal{M}}^{\beta}_{7,0}$ simulates $\mathcal{M}^{\beta}_{7,0}$ except for the following steps:

I3′: Set $y_1=g_1$. Then, choose $x_2\in_r\mathbb{Z}_q$, and compute $y_2=g^{x_2}$, $\{x_{1,j}\}_{j=1}^n=\mathsf{SS}_{t,n}(0)$ and $\{x_{2,j}\}_{j=1}^n=\mathsf{SS}_{t,n}(x_2)$.
I5′: Choose $p\in_r\mathbb{Z}_q$, and set $u_p=g_2$ and $v_p=g_3h^p$.

(A) Let $w\in\mathrm{DH}$. Using the similar argument to (A) of the proof of Lemma 5.5, we see that the differences between $\mathcal{M}^{\beta}_{7,0}$ and $\widetilde{\mathcal{M}}^{\beta}_{7,0}$ are the choice of y_1 in Step **I3′** and that of u_p in Step **I5′**. The distribution $\Delta^1_{7,0}=\{(g_1,g_2)\mid g_1,g_2\in_r\mathbb{G}_q\}$ is identical to the distribution of (y_1,u_p) constructed in $\widetilde{\mathcal{M}}^{\beta}_{7,0}(w)$. The distribution $\Delta^1_{7,0}$ is uniform over $\mathbb{G}_q^2$, and is identical to the distribution of (y_1,u_p) constructed in $\mathcal{M}^{\beta}_{7,0}(w)$.

(B) Let $w\in\widetilde{\mathrm{DH}}$. By the similar argument to (A), we see that the differences between $\widetilde{\mathcal{M}}^{\beta}_{7,0}$ and $\mathcal{M}^{\beta}_{7,1}$ are the choice of y_1 in Step **I3′** and those of u_p and v_p in Step **I5′**. For any fixed $p\in\mathbb{Z}_q$ and $h\in\mathbb{G}_q$ the distribution $\Delta^2_{7,0}=\{(g_1,g_2,g_3h^p)\mid g_1,g_2,g_3,h\in_r\mathbb{G}_q,\ p\in_r\mathbb{Z}_p\}$ over $\mathbb{G}_q^3$ is identical to the distribution of (y_1,u_p,v_p) constructed in $\widetilde{\mathcal{M}}^{\beta}_{7,0}(w)$. The distribution $\Delta^2_{7,0}$ is uniform, and is identical to that constructed in $\mathcal{M}^{\beta}_{7,1}(w)$.

Since the running time of $\widetilde{\mathcal{M}}^{\beta}_{7,0}$ is at most $T_9=T+4T_S+q_Uf_9^U+q_Sf_9^S+f_9^I$ for some polynomials f_9^U, f_9^S and f_9^I in n, t and k, if $T_9\le T_{\mathrm{ddh}}$, then we have

$$|\Pr[F_{7,0,d_\beta}] - \Pr[F_{7,1,d_\beta}]| = \left|\Pr_{w\in\mathrm{DH}}[\varphi^{\beta}_{7,0} = 1] - \Pr_{w\in\widetilde{\mathrm{DH}}}[\varphi^{\beta}_{7,1} = 1]\right| = \left|\Pr_{w\in\mathrm{DH}}[\widetilde{\varphi}^{\beta}_{7,0} = 1] - \Pr_{w\in\widetilde{\mathrm{DH}}}[\widetilde{\varphi}^{\beta}_{7,1} = 1]\right| < \varepsilon_{\mathrm{ddh}}.$$

7. Concluding Remarks

We have studied the PPSS scheme PPSS_2 proposed in [4], and pointed out that PPSS_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_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).