

Homomorphic Secret-Sharing with Certified Deletion

Nikhil Pappu[†]

[†]Portland State University
nikpappu@pdx.edu

October 16, 2024

Abstract

Contents

1	Preliminaries	3
2	HSS with Certified Deletion	3
2.1	HSS-CD Syntax	3
2.2	Additive HSS-CD Syntax	4
2.3	Security Definitions	4
3	Impossibility Results	5
4	Feasibility Results	6
4.1	FHE-CD based Construction	6
4.2	Spooky-Encryption based Construction with Entangled Shares	8
5	HSS and FSS with Weak Certified-Deletion	8

1 Preliminaries

2 HSS with Certified Deletion

Unless otherwise specified, we will consider the following kind of HSS schemes by default:

- Are 2-out-of-2 secret-sharing schemes.
- Allow evaluation for a single secret.

An HSS scheme with certified deletion must have the following syntax and correctness requirements:

2.1 HSS-CD Syntax

A scheme satisfying the HSS-CD syntax for a PPT circuit family \mathcal{C} is a tuple of 5 algorithms $\text{HSS-CD} = (\text{Share}, \text{Eval}, \text{Del}, \text{Vrfy}, \text{Rec})$ with the following properties:

Syntax:

$\text{Share}(s) \rightarrow (sh_0^0, vk_0), (sh_1^0, vk_1)$: The sharing algorithm outputs quantum (possibly-entangled) secret-shares sh_0^0, sh_1^0 encoding an input secret s . It also outputs the corresponding classical verification keys vk_0, vk_1 .

$\text{Eval}(C_j, i, sh_i^{j-1}) \rightarrow sh_i^j$: The evaluation algorithm takes the description of a PPT computable circuit C_j , an index $i \in \{0, 1\}$, and an input share sh_i^{j-1} . It outputs a possibly-altered output share sh_i^j .

$\text{Del}(i, sh_i^j) \rightarrow \text{cert}_i$: The deletion algorithm takes an index $i \in \{0, 1\}$, a corresponding share sh_i^j , and produces a deletion certificate cert_i .

$\text{Vrfy}(i, vk_i, \text{cert}_i) \rightarrow \top / \perp$: The verification algorithm takes an index $i \in \{0, 1\}$, the corresponding verification key vk_i and a certificate cert_i . It outputs \top or \perp .

$\text{Rec}(sh_0^q, sh_1^q) \rightarrow (d_1, \dots, d_q)$: The reconstruction algorithm takes two evaluated input shares sh_0^q, sh_1^q and outputs a q -tuple (d_1, \dots, d_q) .

Evaluation Correctness: $\forall q = \text{poly}(\lambda)$ and $\forall (C_1, \dots, C_q) \in \mathcal{C}^q$, the following condition holds:

$$\Pr \left[(d_1, \dots, d_q) = (C_1(s), \dots, C_q(s)) : \begin{array}{l} (sh_0^0, vk_0), (sh_1^0, vk_1) \leftarrow \text{Share}(s) \\ \forall i, j \in \{0, 1\} \times [q] : sh_i^j \leftarrow \text{Eval}(C_j, i, sh_i^{j-1}) \\ (d_1, \dots, d_q) \leftarrow \text{Rec}(sh_0^q, sh_1^q) \end{array} \right] \geq 1 - \text{negl}(\lambda)$$

Deletion Correctness: The following condition holds for all $i \in \{0, 1\}$, $q = \text{poly}(\lambda)$ and $(C_1, \dots, C_q) \in \mathcal{C}^q$:

$$\Pr \left[\text{Vrfy}(i, vk_i, \text{cert}_i) \rightarrow \top : \begin{array}{l} (sh_0^0, vk_0), (sh_1^0, vk_1) \leftarrow \text{Share}(s) \\ \forall j \in [q] : sh_i^j \leftarrow \text{Eval}(C_j, i, sh_i^{j-1}) \\ \text{cert}_i \leftarrow \text{Del}(i, sh_i^q) \end{array} \right] \geq 1 - \text{negl}(\lambda)$$

Compactness: The following condition holds for all $i \in \{0, 1\}$, $q = \text{poly}(\lambda)$ and $(C_1, \dots, C_q) \in \mathcal{C}^q$, where l_q denotes the output length of the circuit C_q :

$$\left[|sh_i^q| - |sh_i^{q-1}| = \text{poly}(1^\lambda, l_q) : \begin{array}{l} (sh_0^0, vk_0), (sh_1^0, vk_1) \leftarrow \text{Share}(s) \\ \forall j \in [q] : sh_i^j \leftarrow \text{Eval}(C_j, i, sh_i^{j-1}) \end{array} \right]$$

2.2 Additive HSS-CD Syntax

A scheme satisfying the additive HSS-CD syntax for a PPT circuit family \mathcal{C} is a tuple of 4 algorithms $\text{HSS-CD} = (\text{Share}, \text{Eval}, \text{Del}, \text{Vrfy})$ with the following properties:

Syntax:

$\text{Share}(s) \rightarrow (sh_0^0, vk_0), (sh_1^0, vk_1)$: The sharing algorithm outputs quantum (possibly-entangled) secret-shares sh_0^0, sh_1^0 encoding an input secret s . It also outputs the corresponding classical verification keys vk_0, vk_1 .

$\text{Eval}(C_j, i, (sh_i^{j-1}, sh_i^{j-1})) \rightarrow (sh_i^j, sh_i^j)$: The evaluation algorithm takes the description of a PPT computable circuit C_j , an index $i \in \{0, 1\}$, a quantum input share sh_i^{j-1} , and a classical input share sh_i^{j-1} where $sh_i^0 = \perp$. It outputs a quantum output share sh_i^j and a classical output share sh_i^j .

$\text{Del}(i, sh_i^j) \rightarrow \text{cert}_i$: The deletion algorithm takes an index $i \in \{0, 1\}$, a corresponding quantum share sh_i^j , and produces a deletion certificate cert_i .

$\text{Vrfy}(i, vk_i, \text{cert}_i) \rightarrow \top / \perp$: The verification algorithm takes an index $i \in \{0, 1\}$, the corresponding verification key vk_i and a certificate cert_i . It outputs \top or \perp .

Evaluation Correctness: The following condition holds for all $q = \text{poly}(\lambda)$ and $(C_1, \dots, C_q) \in \mathcal{C}^q$:

$$\Pr \left[sh_0^q \oplus sh_1^q = C_1(s) \parallel \dots \parallel C_q(s) : \begin{array}{l} (sh_0^0, vk_0), (sh_1^0, vk_1) \leftarrow \text{Share}(s) \\ \forall i, j \in \{0, 1\} \times [q] : (sh_i^j, sh_i^j) \leftarrow \text{Eval}(C_j, i, (sh_i^{j-1}, sh_i^{j-1})) \end{array} \right] \geq 1 - \text{negl}(\lambda)$$

In the case of additive HSS-CD, we will consider the following weaker deletion guarantee:

Delete-before-Eval Correctness: The following condition holds for all $i \in \{0, 1\}$:

$$\Pr \left[\text{Vrfy}(i, vk_i, \text{cert}_i) \rightarrow \top : \begin{array}{l} (sh_0^0, vk_0), (sh_1^0, vk_1) \leftarrow \text{Share}(s) \\ \text{cert}_i \leftarrow \text{Del}(i, sh_i^0) \end{array} \right] \geq 1 - \text{negl}(\lambda)$$

2.3 Security Definitions

Statistical/Computational Deletion Security wrt Share j : The following security notion is defined wrt a non-local quantum adversary $(\mathcal{A}_0, \mathcal{A}_1)$:

$\text{Expt}_{\text{HSS-CD}, (\mathcal{A}_0, \mathcal{A}_1)}^{\text{del}}(1^\lambda, j, b)$:

1. \mathcal{A}_0 sends $(s_0, s_1) \in \{0, 1\}^\lambda$ to the challenger.
2. The challenger runs $(sh_0^0, vk_0), (sh_1^0, vk_1) \leftarrow \text{Share}(s_b)$ and sends each sh_i^0 to party P_i .
3. \mathcal{A}_j sends (cert_j, R_j) and \mathcal{A}_{1-j} sends R_{1-j} where R_0, R_1 are some registers.
4. If $\text{Vrfy}(j, vk_j, \text{cert}_j) = \top$, then output (R_1, R_2) .

Statistical Deletion Security wrt Share j holds if the following holds:

$$TD\left(\text{Expt}_{\text{HSS-CD}, (\mathcal{A}_0, \mathcal{A}_1)}^{\text{del}}(1^\lambda, j, 0), \text{Expt}_{\text{HSS-CD}, (\mathcal{A}_0, \mathcal{A}_1)}^{\text{del}}(1^\lambda, j, 1)\right) \leq \text{negl}(\lambda)$$

Computational Deletion Security wrt Share j holds if the following holds for all QPT \mathcal{A} :

$$\left| \Pr \left[\mathcal{A}\left(\text{Expt}_{\text{HSS-CD}, (\mathcal{A}_0, \mathcal{A}_1)}^{\text{del}}(1^\lambda, j, 0)\right) = 1 \right] - \Pr \left[\mathcal{A}\left(\text{Expt}_{\text{HSS-CD}, (\mathcal{A}_0, \mathcal{A}_1)}^{\text{del}}(1^\lambda, j, 1)\right) = 1 \right] \right| \leq \text{negl}(\lambda)$$

Statistical/Computational Double-Deletion Security: The following security notion is defined wrt a non-local quantum adversary $(\mathcal{A}_0, \mathcal{A}_1)$:

$\text{Exp}_{\text{HSS-CD}, (\mathcal{A}_0, \mathcal{A}_1)}^{\text{del-2}}(1^\lambda, b)$:

- 1.
2. \mathcal{A}_0 sends $(s_0, s_1) \in \{0, 1\}^\lambda$ to the challenger. The challenger runs $(sh_0^0, vk_0), (sh_1^0, vk_1) \leftarrow \text{Share}(s_b)$ and sends each sh_i^0 to party P_i .
3. \mathcal{A}_0 sends (cert_0, R_0) and \mathcal{A}_1 sends (cert_1, R_1) where R_0, R_1 are some registers.
4. If $\text{Vrfy}(0, vk_0, \text{cert}_0) = \text{Vrfy}(1, vk_1, \text{cert}_1) = \top$, then output (R_0, R_1) .

Statistical Double-Deletion Security holds if the following holds:

$$TD\left(\text{Exp}_{\text{HSS-CD}, (\mathcal{A}_0, \mathcal{A}_1)}^{\text{del-2}}(1^\lambda, 0), \text{Exp}_{\text{HSS-CD}, (\mathcal{A}_0, \mathcal{A}_1)}^{\text{del-2}}(1^\lambda, 1)\right) \leq \text{negl}(\lambda)$$

Computational Double-Deletion Security holds if the following holds for all QPT \mathcal{A} :

$$\left| \Pr \left[\mathcal{A} \left(\text{Exp}_{\text{HSS-CD}, (\mathcal{A}_0, \mathcal{A}_1)}^{\text{del-2}}(1^\lambda, 0) \right) = 1 \right] - \Pr \left[\mathcal{A} \left(\text{Exp}_{\text{HSS-CD}, (\mathcal{A}_0, \mathcal{A}_1)}^{\text{del-2}}(1^\lambda, 1) \right) = 1 \right] \right| \leq \text{negl}(\lambda)$$

Hereafter, we will use *stat* to denote statistical security and *comp* to denote computational security.

Definition 2.1 ((Additive) (X, Y)-HSS-CD scheme for \mathcal{C}). An (Additive) (X, Y)-HSS-CD scheme for \mathcal{C} , where $X, Y \in \{\text{stat}, \text{comp}\}^2$ is a scheme that satisfies the (Additive) HSS-CD syntax for \mathcal{C} , the X deletion security for share 0, and the Y deletion security for share 1.

Definition 2.2 ((Additive) (X)-HSS-CD scheme). An (Additive) (X)-HSS-CD scheme for \mathcal{C} where $X \in \{\text{stat}, \text{comp}\}$ is a scheme satisfying the (Additive) HSS-CD syntax for \mathcal{C} and the X double-deletion security.

Remark 2.3. Observe that a (stat, comp)-HSS-CD scheme for \mathcal{C} is also a (stat)-HSS-CD scheme for \mathcal{C} . Likewise, a (comp, comp)-HSS-CD scheme for \mathcal{C} is also a (comp)-HSS-CD scheme for \mathcal{C} .

3 Impossibility Results

Lemma 3.1. Any (stat, stat)-HSS-CD scheme for \mathcal{C} is also an information-theoretic HSS scheme for \mathcal{C} .

Proof. Suppose there exists a (stat, stat)-HSS-CD scheme that does not satisfy information-theoretic secrecy. Then, there exists an unbounded adversary \mathcal{D} that receives some share sh_i^0 and distinguishes between the secrets s_0, s_1 . Then, there exists an adversary $(\mathcal{A}_0, \mathcal{A}_1)$ in the statistical security wrt share 1 — i game that works as follows. \mathcal{A}_{1-i} honestly deletes its share and outputs a dummy register while \mathcal{A}_i outputs a register containing its share sh_i^0 . In the second-stage, the distinguisher \mathcal{D} is run on sh_i^0 to tell apart the secrets s_0, s_1 . \square

The following theorem shows that the classical impossibility result regarding information-theoretic HSS by [BGI⁺18] also applies to the setting of quantum shares.

Theorem 3.2. TBD.

Theorem 3.3. There does not exist an Additive (comp)-HSS-CD scheme HSS-CD for any PPT circuit class \mathcal{C} , given that $\text{HSS-CD.Share}(s)$ outputs shares sh_0, sh_1 that are not entangled with each other.

Proof. In fact, we will prove that this holds even for a weaker notion of evaluation correctness, where \mathcal{Eval} supports only a single evaluation. Specifically, for shares (sh_0, sh_1) output by $\mathcal{Share}(s)$, $\mathcal{Eval}(i, C, sh_i)$ outputs y_i such that $y_0 \oplus y_1 = C(s)$. The argument is as follows:

Let $(|\psi_0\rangle, vk_0), (|\psi_1\rangle, vk_1)$ be some pure state output by $\mathcal{Share}(s)$, where $|\psi_0\rangle, |\psi_1\rangle$ are not entangled with each other. Wlog, let $\{\Pi_0, \mathbb{I} - \Pi_0\}$ be the projective measurement equivalent of $\mathcal{Eval}(0, C, |\psi_0\rangle)$, i.e., Π_0 corresponds to $y_0 = 0$ and $\mathbb{I} - \Pi_0$ corresponds to $y_0 = 1$. Let Y_0 denote the random variable of the output y_0 . Likewise, consider the projective measurement $\{\Pi_1, \mathbb{I} - \Pi_1\}$ equivalent of $\mathcal{Eval}(1, C, |\psi_1\rangle)$ and let Y_1 be the corresponding output random variable. Notice that for every outcome y_0 of Y_0 , there is a single outcome y_1 of Y_1 that satisfies $y_1 = C(s) \oplus y_0$. Let \tilde{Y}_0 be the random variable for \tilde{y}_0 sampled as $\tilde{y}_0 = C(s) \oplus y_1 : y_1 \leftarrow Y_1$. By the evaluation correctness requirement, we require that $\Pr[Y_0 = \tilde{Y}_0] \geq 1 - \text{negl}(\lambda)$. Since Y_0 and \tilde{Y}_0 are independent random variables, this is only possible if there exists y_0^* such that $\Pr[Y_0 = y_0^*] \geq 1 - \text{negl}(\lambda)$ and $\Pr[\tilde{Y}_0 = y_0^*] \geq 1 - \text{negl}(\lambda)$. In other words, the measurement $\{\Pi_0, \mathbb{I} - \Pi_0\}$ either accepts the state $|\psi_0\rangle$ with probability $1 - \text{negl}(\lambda)$ or rejects it with probability $1 - \text{negl}(\lambda)$. Consequently, by the gentle measurement lemma, the leftover state is close in trace distance to the state $|\psi_0\rangle$. As a result, it can be certifiably deleted after obtaining y_0 . By a similar argument, y_1 can be obtained in the same way. Since this holds for every possible pure state output by $\mathcal{Share}(s)$, it also holds for arbitrary mixed states. As a result, the adversary can efficiently compute $y_0 \oplus y_1 = C(s)$ in the second-stage, breaking the computational double-deletion security. Since this security notion is the weakest one, this also rules out the other notions. \square

4 Feasibility Results

4.1 FHE-CD based Construction

We construct a (stat, comp)-HSS-CD scheme $\text{HSS-CD} = \text{HSS-CD}(\mathcal{Share}, \mathcal{Eval}, \mathcal{Del}, \mathcal{Vrfy}, \mathcal{Rec})$ using the following building blocks.

- Fully Homomorphic Encryption with Certified Deletion (FHE-CD) scheme $\text{FHE-CD} = \text{FHE-CD}(\text{Setup}, \mathcal{Enc}, \mathcal{Dec}, \mathcal{Eval}, \mathcal{Del}, \mathcal{Vrfy})$.
- Secret Sharing with Certified Deletion (SS-CD) scheme $\text{SS-CD} = \text{SS-CD}(\mathcal{Share}, \mathcal{Rec}, \mathcal{Del}, \mathcal{Vrfy})$.

The construction is as follows.

$\text{HSS-CD}.\mathcal{Share}(s)$:

1. Generate $(pk, sk) \leftarrow \text{FHE-CD}.\text{Setup}(1^\lambda)$.
2. Compute $(fhecd.ct^0, fhecd.vk) \leftarrow \text{FHE-CD}.\mathcal{Enc}(s)$.
3. Compute $(sscd.sh, sscd.csh), sscd.vk \leftarrow \text{SS-CD}.\mathcal{Share}(sk)$.
4. Set $sh_0^0 := (fhecd.pk, fhecd.ct^0, sscd.csh)$ and $vk_0 := fhecd.vk$.
5. Set $sh_1^0 := sscd.sh$ and $vk_1 := sscd.vk$.
6. Output $(sh_0^0, vk_0), (sh_1^0, vk_1)$.

$\text{HSS-CD}.\mathcal{Eval}(C_j, i, sh_i^{j-1})$: If $i = 1$, set $sh_1^j := sh_1^{j-1}$. Else, execute the following:

1. Parse sh_0^{j-1} as $(fhecd.pk, fhecd.ct^{j-1}, sscd.csh)$.
2. Compute $fhecd.ct^j \leftarrow \text{FHE-CD}.\mathcal{Eval}(fhecd.pk, C_j, fhecd.ct^{j-1})$.
3. Set $sh_0^j := (fhecd.pk, fhecd.ct^j, sscd.csh)$.

4. Output sh_i^j .

HSS-CD.Del(i, sh_i^j):

1. If $i = 0$, execute the following:
 - (i) Parse sh_0^j as $(fhecd.pk, fhecd.ct^j, sscd.csh)$.
 - (ii) Compute and output $cert_0 \leftarrow \text{FHE-CD.Del}(fhecd.ct^j)$.
2. If $i = 1$, execute the following:
 - (i) Parse sh_1^j as $sscd.sh$.
 - (ii) Compute and output $cert_1 \leftarrow \text{SS-CD.Del}(sscd.sh)$.

HSS-CD.Vrfy($i, vk_i, cert_i$):

1. If $i = 0$, output $ans_0 \leftarrow \text{FHE-CD.Vrfy}(vk_0, cert_0)$.
2. If $i = 1$, output $ans_0 \leftarrow \text{SS-CD.Vrfy}(vk_1, cert_1)$.

HSS-CD.Rec(sh_0^q, sh_1^q):

1. Parse sh_0^q as $(fhecd.pk, fhecd.ct^q, sscd.csh)$.
2. Parse sh_1^q as $sscd.sh$.
3. Compute $sk \leftarrow \text{SS-CD.Dec}(sscd.sh, sscd.csh)$.
4. Compute and output $(d_1, \dots, d_q) \leftarrow \text{FHE-CD.Dec}(sk, fhecd.ct^q)$.

Theorem 4.1. *There exists a (stat, comp)-HSS-CD scheme assuming the existence of a fully homomorphic encryption scheme with certified deletion (FHE-CD), and a secret-sharing scheme with certified deletion (SS-CD).*

Proof. We will prove that the construction HSS-CD is a (stat, comp)-HSS-CD scheme. First, we will assume that $(\mathcal{A}_0, \mathcal{A}_1)$ is a non-local adversary that breaks the statistical deletion security of share 0. We will use this adversary to break the certified deletion security of the FHE-CD scheme FHE-CD. Consider a QPT reduction \mathcal{R} that runs as follows in the FHE-CD game:

Execution of $\mathcal{R}^{(\mathcal{A}_0, \mathcal{A}_1)}$ in $\text{Exp}_{\text{FHE-CD}, \mathcal{R}}^{\text{fhe-cd}}(1^\lambda, b)$:

1. \mathcal{A}_0 sends $(s_0, s_1) \in \{0, 1\}^\lambda$ to \mathcal{R} , which \mathcal{R} forwards to the challenger.
2. The challenger samples $(pk, sk) \leftarrow \text{Setup}(1^\lambda)$ and sends pk to \mathcal{R} .
3. The challenger encrypts s_b as $ct \leftarrow \text{Enc}(pk, s_b)$ and sends ct to \mathcal{R} .
4. \mathcal{R} computes $sh_0^0 := (pk, ct, sscd.csh)$, where $sscd.csh \leftarrow \text{SS-CD.Sim}(1^\lambda)$.
5. \mathcal{R} runs \mathcal{A}_0 on input sh_0^0 . If \mathcal{A}_0 outputs $(cert_0, R_0)$, \mathcal{R} sends $cert_0$ to the challenger.
6. The challenger computes $ans \leftarrow \text{Vrfy}(vk, cert_0)$. If $ans = \top$, it sends sk to \mathcal{R} . Else, it outputs \perp .
7. \mathcal{R} computes $sscd.sh$ conditioned on $(sscd.sh, sscd.sh)$ encoding sk .
8. \mathcal{R} sends $sh_1^0 := sscd.sh$ to \mathcal{A}_1 . If \mathcal{A}_1 outputs R_1 , send (R_0, R_1) to the challenger.

We will now argue that if $(\mathcal{A}_0, \mathcal{A}_1)$ break statistical security wrt share 0, then \mathcal{R} breaks the certified-deletion security of FHE-CD. Observe that the view of \mathcal{A}_0 in the reduction is identically distributed to its view in $\text{Expt}_{\text{HSS-CD}, (\mathcal{A}_0, \mathcal{A}_1)}^{\text{del}}(1^\lambda, 0, b)$. Now, notice that if $\text{HSS-CD.Vrfy}(0, vk_0, cert_0)$ passes, then $\text{FHE-CD.Vrfy}(vk, cert_0)$ also passes. Consequently, \mathcal{R} receives the secret key sk . By the information-theoretic secrecy of the scheme SS-CD, the view of \mathcal{A}_1 is identically distributed to that in the original experiment. As a result, (R_0, R_1) are identically distributed to that of the HSS-CD game. By assumption, there exists an unbounded algorithm that can use (R_0, R_1) to guess b with non-negligible probability. This breaks the certified-deletion security of FHE-CD.

Next, we will assume that $(\mathcal{A}_0, \mathcal{A}_1)$ is a non-local adversary that breaks the computational deletion security of share 1. We will use this adversary to break the certified deletion security of the SS-CD scheme SS-CD. Consider a non-local reduction $(\mathcal{R}_0, \mathcal{R}_1)$ that runs as follows:

Execution of $(\mathcal{R}_0, \mathcal{R}_1)$ in $\text{Exp}_{\text{SS-CD}, (\mathcal{R}_0, \mathcal{R}_1)}^{\text{ss-cd}}(1^\lambda, b)$:

1. \mathcal{R}_0 samples $(\text{pk}, \text{sk}) \leftarrow \text{FHE-CD.Setup}(1^\lambda)$. It sets $s_0 := 0^\lambda$ and $s_1 := \text{sk}$ and sends (s_0, s_1) to the challenger.
2. The challenger computes $(sh, \text{csh}, \text{vk}) \leftarrow \text{Share}(s_b)$. It sends csh to \mathcal{R}_0 and sh to \mathcal{R}_1 .
3. \mathcal{R}_0 runs \mathcal{A}_0 . \mathcal{A}_0 sends (s'_0, s'_1) to \mathcal{R}_0 .
4. \mathcal{R}_0 sends $(\text{pk}, ct, \text{csh})$ to \mathcal{A}_0 , where $ct \leftarrow \text{FHE-CD.Enc}(\text{pk}, s'_c)$ and $c \leftarrow \{0, 1\}$.
5. \mathcal{A}_0 sends R'_0 to \mathcal{R}_0 . \mathcal{R}_0 sets $R_0 := (R'_0, c)$ and sends it to the challenger.
6. \mathcal{R}_1 runs \mathcal{A}_1 on input sh . If \mathcal{A}_1 outputs (cert_1, R'_1) , then \mathcal{R}_1 sets $R_1 := R'_1$ and sends it to the challenger.
7. The challenger computes $\text{ans} = \text{Vrfy}(\text{vk}, \text{cert}_1)$. If $\text{ans} = \top$, it outputs (R_0, R_1) .

Consider now the experiment $\text{Exp}_{\text{SS-CD}, (\mathcal{R}_0, \mathcal{R}_1)}^{\text{ss-cd}}(1^\lambda, 0)$. Notice that if there exists a QPT algorithm \mathcal{A} that obtains the registers (R'_0, R'_1) and outputs $c' = c$ with probability $\frac{1}{2} + \text{non-negl}(\lambda)$, then the security of FHE-CD is broken. This is because a reduction can obtain an FHE-CD ciphertext and simulate the view of $\mathcal{A}_0, \mathcal{A}_1$ as needed, because knowledge of sk is not required.

By assumption, there exists a QPT algorithm \mathcal{A} that obtains (R'_0, R'_1) and outputs $c' = c$ with probability $\frac{1}{2} + \text{non-negl}(\lambda)$ in the experiment $\text{Exp}_{\text{SS-CD}, (\mathcal{R}_0, \mathcal{R}_1)}^{\text{ss-cd}}(1^\lambda, 1)$.

Now, consider an algorithm \mathcal{R} that obtains $(R_0 = (c, R'_0), R_1 = R'_1)$. It runs \mathcal{A} on (R'_0, R'_1) and checks if the value c' equals c or not. If it is, then \mathcal{R} outputs $b' = 1$, otherwise it outputs $b' = 0$. Consequently, \mathcal{R} outputs $b' = b$ with probability $\frac{1}{2} + \text{non-negl}(\lambda)$, breaking the security of the scheme SS-CD. This gives us a contradiction. \square

4.2 Spooky-Encryption based Construction with Entangled Shares

5 HSS and FSS with Weak Certified-Deletion

References

- [BGI⁺18] Elette Boyle, Niv Gilboa, Yuval Ishai, Huijia Lin, and Stefano Tessaro. Foundations of homomorphic secret sharing. In Anna R. Karlin, editor, *ITCS 2018*, volume 94, pages 21:1–21:21. LIPIcs, January 2018. (Cited on page 5.)