Efficient RCCA encryption scheme and structure-perserving publicly verifiable encryption scheme

Qian Chen Supervisors: Benoît Libert, Fabien Laguillaumie Aric Lip ENS Lyon

20 Auguest 2016

1 Introduction

General Context

For the simple needs of communicate safely and privately, cryptography is very important in our current life. Start with Shanon in 1949 in his paper Communication theory of secrecy systems [5], we begin to formally define the properties we wanted for the cryptographic protocols and proof these properties based on some hardness assumptions or complexity assumptions. As one of most useful cryptographic protocol, the encryption scheme is widely used in the construction or more complex cryptographic system. Thus we are motivated to define the most adapted security notion for the encryption scheme. From the very basic One-Wayness Chosen-Plaintext Attack(OW-CPA) to the most secure Indistinguishable Chosen-Ciphertext Attack(IND-CCA) model.

One of the most important property of the encryption scheme is the malleability, which means with a valid ciphertext we can produce another ciphertext of a plaintext which is related to the original one without knowing it. This property necessarily produce some information leakages, thus it is forbidden by the most secure definition(IND-CCA). But recently, these properties are seen to be a potentially useful feature that can be exploited.

Problem studied

My internship focused on the encryption scheme which only allowed to be re-randomizable. This property can be formally defined as resist of Replayeable Chosen-Ciphertext Attack(RCCA). In some recent work of constructing more advanced cryptographic protocols like receipt-free voting system [3] and reverse firewall [4], RCCA encryption scheme are required in such schemes, The first application requires a weak re-randomization RCCA encryption scheme, and the second application requires a strong re-randomization RCCA encryption scheme. The aim of my internship is to construct and prove efficient encryption scheme which are suitable for the above schemes. The main motivation is that the previous works on constructing such scheme are more or less not efficient. We try to improve there efficiency to get some usable protocol in the practical point of view.

Proposed Contributions

The contributions of my internship are the following: the construction and proof of a efficient weak RCCA encryption which is adapted to the receipt-free voting system, efficient instantiation of the

general controlled-malleable encryption scheme proposed by [2]. Then we use another approach to get a very efficient strong RCCA encryption in which the the ciphertext size is only . As a sub-result, we also have constructed a public verifiable structure-preserving CCA encryption which is more efficient than the existing construction.

Arguments Supporting Their Validity

For the validity of our construction, every construction has been proven for the security model with standard complexity assumptions which are well studied and general believed. And we also give their efficiency by counting their ciphertext size and compare with existing schemes to show that we achieve efficiency improvement.

Summary and Future Work

During my internship, I have proposed several efficiency improvements for the construction of the cryptographic scheme, This contribution can be considered as improvement both in the efficiency and the construction of the new scheme with some practical properties for the further construction of more complex cryptographic system.

However, several questions are left open. We especially studied the re-randomizable encryption scheme, which is a subset of homomorphic encryption scheme, can we use the similar idea of the efficiency improvement for a wider class of homomorphic encryption scheme. And, even in our strong RCCA scheme, the re-randomization is computational. A natural open question is can we achieve strong RCCA scheme which re-randomization is statistical.

2 Preliminaries

In this section, we first briefly present some standard computation assumptions, we will use in this report. Then we present the security model and proprieties we want achieve we also give some building blocks.

2.1 Assumptions

In cryptography, one of the most studied assumption is Diffie-Hellman assumption.

2.2 Bulding Blocks

Definition 1. *Linearly Homomorphic Structure Preserving Signature based on SXDH assumption*

***LHSPS*.Setup(1^λ)** *:*

1. *We generate a bilinear group system* $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T, e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T)$.
2. *Choose random group generators* $(\hat{g}_z, \hat{g}_r) \xleftarrow{R} \hat{\mathbb{G}}^2$.
3. *Choose random group generator* $g \xleftarrow{R} \mathbb{G}$.
4. *Output* $\mathsf{PP} = (\hat{g}_z, \hat{g}_r, g)$.

***LHSPS*.KeyGen(PP)** *:*

1. *Generate* $(\{\hat{\chi}_i, \hat{\gamma}_i\}_{i=1}^k, \hat{\zeta}, \hat{\rho}) \xleftarrow{R} \mathbb{Z}_p^{2k+2}$.
2. *Compute for* $i \in \{1, \ldots, k\}$, $\hat{g}_i \leftarrow \hat{g}_z^{\hat{\chi}_i} \hat{g}_r^{\hat{\gamma}_i}$ *and* $\hat{a} \leftarrow \hat{g}_z^{\hat{\zeta}} \hat{g}_r^{\hat{\rho}}$.
3. *Output* $\mathsf{vk} = (\{\hat{g}_i\}_{i=1}^k, \hat{a}) \in \hat{\mathbb{G}}^{k+1}$ *and* $\mathsf{sk} = (\{\hat{\chi}_i, \hat{\gamma}_i\}_{i=1}^k, \hat{\zeta}, \hat{\rho}) \in \mathbb{Z}_p^{2k+2}$.

***LHSPS*.Sign(sk, $\{m_1, \ldots, m_k\}$)** *: where* $(m_1, \ldots, m_k) \in \mathbb{G}^k$

1. *Parse* sk *with* $(\{\hat{\chi}_i, \hat{\gamma}_i\}_{i=1}^k, \hat{\zeta}, \hat{\rho})$.
2. *Compute*

$$z = g^{\hat{\zeta}} \cdot \prod_{i=1}^{k} m_i^{-\hat{\chi}_i} \qquad\qquad r = g^{\hat{\rho}} \cdot \prod_{i=1}^{k} m_i^{-\hat{\gamma}_i}$$

3. *Output the signature* $\sigma = (z, r)$

***LHSPS*.Verify(vk, σ, $\{m_1, \ldots, m_k\}$)** *:*

1. *Parse the signature* σ *with* $\sigma = (z, r)$ *and the verification key* vk *with* $\mathsf{vk} = (\hat{g}_1, \ldots, \hat{g}_k, \hat{a})$
2. *Verify the pairing equation:*

$$e(g, \hat{a}) = e(z, \hat{g}_z) \cdot e(r, \hat{g}_r) \cdot \prod_{i=1}^{k} e(m_i, \hat{g}_i)$$

3 From tag-based encryption to the weak RCCA encryption scheme

In this section, we first give an instantiation of weak CCA tag-based encryption based on SXDH assumption, then combined with a linearly homomorphic signature scheme, we can construct a partially randomizable RCCA encryption scheme.

3.1 Tag based-encryption

In this section, we first describe a tag based-encryption which is selective-ID CCA1 tag-based encryption scheme. The construction of this scheme is proposed by Cash *el. al.* [1] in the form of an public key encryption scheme.

$\mathsf{Setup}(1^\lambda)$:

1. Choose a group $\mathbb{G}$ of prime order p in which the DDH problem is hard and choose randomly a group generator $g \xleftarrow{R} \mathbb{G}$.
2. Generate three random values $(x_1, \tilde{x}_1, x_2) \xleftarrow{R} \mathbb{Z}_p^3$.
3. Compute $X_1 \leftarrow g^{x_1}$, $\tilde{X}_1 \leftarrow g^{\tilde{x}_1}$.
4. Set $\mathsf{PP} \leftarrow (g, \mathbb{G})$
5. Compute $\mathsf{PK} \leftarrow (X_1, \tilde{X}_1, X_2)$ and $\mathsf{SK} \leftarrow (x_1, \tilde{x}_1, x_2)$

$\mathsf{Enc}(\mathsf{PP}, \mathsf{PK}, m, \tau)$: where $m \in \mathbb{G}$ and $\tau \in \mathbb{Z}_p$

1. Generate a random value $r \xleftarrow{R} \mathbb{Z}_p$.
2. Compute

$$R = g^r, \qquad Z = (X_1^\tau \tilde{X}_1)^r \qquad C = X_2^r \cdot m \tag{1}$$

3. Output the cipher-text $\vec{C} = (R, Z, C) \in \mathbb{G}^3$.

$\mathsf{Dec}(\mathsf{PP}, \mathsf{SK}, \vec{C}, \tau)$: where $\vec{C} \in \mathbb{G}^3$

1. Parse $\vec{C}$ as (R, Z, C) and SK as $(x_1, \tilde{x}_1, x_2)$.
2. Verify that if $Y^{x_1\tau + \tilde{x}_1} = Z$.
3. If not reject, otherwise, compute:

$$m = C/R^{x_2} \tag{2}$$

4. Output the message m.

3.2 Combine the tag-based encryption with the Linearly Homomorphic Structure-Preserving Signature(LHSPS)

In this section, we follow the general idea of construction CCA2 security encryption from a selective-tag based CCA1 encryption scheme. To achieve the partially randomization property, we use the LHSPS in the construction of our public key encryption scheme.

We present our construction for the partially randomizable encryption scheme as following:

$RCCA1.\mathsf{Setup}(1^\lambda)$:

1. Generate the public parameters for the LHSPS scheme $\mathsf{PP}_{LHSPS} \leftarrow LHSPS.\mathsf{Setup}(1^\lambda, \ell = 4)$. Where ℓ presents the length of the message will be signed.
2. Generate the public parameters for the tag-based encryption scheme $\mathsf{PP}_{TBE} \leftarrow TBE.\mathsf{Setup}(1^\lambda)$.
3. Generate a collision resistant hash function $H : \hat{\mathbb{G}}^4 \rightarrow \mathbb{Z}_p$.
4. Output the public parameter $\mathsf{PP} \leftarrow (\mathsf{PP}_{LHSPS}, \mathsf{PP}_{TBE})$

$RCCA1.\mathsf{KeyGen}(\mathsf{PP})$:

1. Parse PP as $(\mathsf{PP}_{LHSPS}, \mathsf{PP}_{TBE})$.
2. Using PP_{TBE} to generate the public keys and secret keys $(\mathsf{PK}, \mathsf{SK}) \leftarrow TBE.\mathsf{KeyGen}(\mathsf{PP}_{TBE})$ of the underlying tag-based encryption scheme.

$RCCA1.\mathsf{KeyGen}(\mathsf{PP})$:

1. Generate the signing key-verification key pair for the underlying signature scheme

$$(\mathsf{SSK}, \mathsf{SVK}) \leftarrow LHSPS.\mathsf{KeyGen}(\mathsf{PP}_{LHSPS}) \in (\mathbb{Z}_p^8 \times \mathbb{G}^4).$$

2. Hash the verification key of the underlying signature scheme $\tau \leftarrow H(\mathsf{SVK})$.
3. Generate the encryption of the message m of the underlying tag-based encryption scheme $\vec{C} \leftarrow TBE.\mathsf{Enc}()$

4 Efficient instantiation of the re-randomization encryption of generic construction [2]

For the simplicity, we choose the symmetric setting of the bilinear group and our construction is based on the DLIN assumption.

***Setup*($\boldsymbol{\lambda}$):** This algorithm generates the public and secret keys of our RCCA encryption scheme.

1. Pick bilinear group $(\mathbb{G}, \mathbb{G}_T)$ of prime order p and the bilinear map e on this pair of groups with generators $(f, g, h) \xleftarrow{R} \mathbb{G}^3$ which verify $f^x = g^y = h$.
2. Choose a random group generator $d \in \mathbb{G}$.
3. Choose $g_1, g_2 \xleftarrow{R} \mathbb{G}$ and set $\vec{g}_1 = (g_1, 1, g) \in \mathbb{G}^3$, $\vec{g}_2 = (1, g_2, g) \in \mathbb{G}^3$ and $\vec{g}_3 \xleftarrow{R} \mathbb{G}^3$.
4. Set up the keys for the underlying encryption scheme $\mathsf{pk}_{enc} = (f, g, h)$ and $\mathsf{sk}_{enc} = (x, y)$.
5. Choose four random group generators (g_z, g_r, h_z, h_u) and twelve random exponents $\{\chi_i, \gamma_i, \delta_i\}_{i=1}^3, \zeta, \rho, \phi \leftarrow \mathbb{Z}_p$, then compute $(g_i, h_i) = (g_z^{\chi_i} g_r^{\gamma_i}, h_z^{\chi_i} h_u^{\delta_i})$ for $i \in \{1, 2, 3\}$ and $(\alpha, \beta) = (g_z^{\zeta} g_r^{\rho}, h_z^{\zeta} h_u^{\phi})$
6. Set up the keys for the underlying signature scheme

$$\mathsf{vk}_{sig} = (g_z, h_z, g_r, h_u, \{g_i, h_i\}_{i=1}^3, \alpha, \beta)$$

and

$$\mathsf{sk}_{sig} = (\mathsf{vk}_{sig}, \zeta, \rho, \phi, \{\chi_i, \gamma_i, \delta_i\}_{i=1}^3).$$

7. $\mathsf{PK} = (d, \mathsf{pk}_{enc}, \mathsf{vk}_{sig}, \sigma_{crs})$

***Enc*(PK, *m*):** This algorithm takes as input a message and the public key of the underlying encryption scheme, outputs the corresponded ciphertext of our RCCA encryption scheme.

1. Choose two random exponents $(\theta_1, \theta_2) \xleftarrow{R} \mathbb{Z}_p$ and compute $\vec{r} = (\theta_1, \theta_2)$.
2. Compute the ciphertext $\vec{C} = (C_1, C_2, C_3)$:

$$C_1 = f^{\theta_1} \qquad C_2 = g^{\theta_2} \qquad C_3 = m \cdot h^{\theta_1+\theta_2}$$

3. Recall that we want prove the knowledge of the witness $\vec{w} = (m, \vec{r}, \vec{D}, \vec{S}, \vec{\sigma})$ which verifies that

$$Enc_{BBS}(pk_{enc}, m; \vec{r}) = \vec{C} \vee (\vec{C} = ReRand(\vec{D}; \vec{S}) \wedge Verify(vk_{sig}, \vec{D}) = \mathsf{True})$$

4. Define the bit $b = 1$ and a Groth-Sahai commitment $\vec{C}_b = (1, 1, d^b) \cdot \vec{g}_1^{r_b} \cdot \vec{g}_2^{s_b} \cdot \vec{g}_3^{t_b}$ and also a $NIWI$ proof $\pi_b \in \mathbb{G}^6$ of the pairing product equation

$$e(d, \boxed{d^b}) = e(\boxed{d^b}, \boxed{d^b}) \tag{1}$$

which ensures that $b \in \{0, 1\}$.

5. We first prove the left side of the OR statement, we generate commitments $(\vec{C}_{R_1}, \vec{C}_{R_2})$ of the variables $(R_1 = d^{\theta_1 b}, R_2 = d^{\theta_2 b})$ and $\vec{C}_M$ commitment of $M = m^b$ and commitments $\{\vec{C}_{\Delta_i}\}_{i=1}^3$ of the variables $\{\Delta_i = C_i^b\}_{i=1}^3$. Recall that $\{C_i\}_{i=1}^3$, $\{R_1, R_2\}$ and $\{\Delta_i\}_{i=1}^3$ verify the following equations:

$$e(C_i, \boxed{d^b}) = e(\boxed{\Delta_i}, d) \qquad \forall i \in \{1, 2, 3\} \tag{2,3,4}$$

$$e(\boxed{\Delta_1}, d) = e(f, \boxed{R_1}) \tag{5}$$

$$e(\boxed{\Delta_2}, d) = e(g, \boxed{R_2}) \tag{6}$$

$$e(\boxed{\Delta_3}, d) \cdot e(\boxed{M}, d^{-1}) = e(\boxed{R_1}, h) \cdot e(\boxed{R_2}, h) \tag{7}$$

6. Then we prove the right side of the OR statement:
   (a) The *ReRand* component: define $(D_1, D_2, D_3) = (1_{\mathbb{G}}, 1_{\mathbb{G}}, 1_{\mathbb{G}})$ and $(S_1, S_2) = (1_{\mathbb{G}}, 1_{\mathbb{G}})$.
   (b) Remind that actually these variables are of the following forms in the security proof, but in the case $b = 1$ they all become $1_{\mathbb{G}}$.

$$(D_1, D_2, D_3) = (f^{(\theta_1+\theta_1')\cdot(1-b)}, g^{(\theta_2+\theta_2')\cdot(1-b)}, m^{1-b} \cdot h^{(\theta_1+\theta_1'+\theta_2+\theta_2')\cdot(1-b)})$$

   and

$$(S_1, S_2) = (d^{\theta_1'\cdot(1-b)}, d^{\theta_2'\cdot(1-b)})$$

   (c) Then compute the commitments $\{\vec{C}_{D_i}\}_{i=1}^3$ of $\{D_i\}_{i=1}^3$ and $(\vec{C}_{S_1}, \vec{C}_{S_2})$ commitments of S_1, S_2.

(d) And also compute the proofs of following equations:

$$e(C_1/\boxed{\Delta_1}, d) = e(\boxed{D_1}, d) \cdot e(f^{-1}, \boxed{S_1}) \tag{8}$$

$$e(C_2/\boxed{\Delta_2}, d) = e(\boxed{D_2}, d) \cdot e(g^{-1}, \boxed{S_2}) \tag{9}$$

$$e(C_3/\boxed{\Delta_3}, d) = e(\boxed{D_3}, d) \cdot e(\boxed{S_1}, h^{-1}) \cdot e(\boxed{S_2}, h^{-1}) \tag{10}$$

(e) Then the signature component (Remind that $b = 1$): define

$$\vec{\sigma} = (\Sigma_1, \Sigma_2, \Sigma_3) = (z^{1-b}, r^{1-b}, u^{1-b}) = (1_{\mathbb{G}}, 1_{\mathbb{G}}, 1_{\mathbb{G}}),$$

then compute their commitments $(\vec{C}_{\Sigma_1}, \vec{C}_{\Sigma_2}, \vec{C}_{\Sigma_3})$.

(f) We generate the proof of the following linear pairing equations:

$$e(\alpha, d/\boxed{d^b}) = e(g_z, \boxed{\Sigma_1}) \cdot e(g_r, \boxed{\Sigma_2}) \cdot \prod_{i=1}^{3} e(g_i, \boxed{D_i}) \tag{11}$$

$$e(\beta, d/\boxed{d^b}) = e(h_z, \boxed{\Sigma_1}) \cdot e(h_u, \boxed{\Sigma_3}) \cdot \prod_{i=1}^{3} e(h_i, \boxed{D_i}) \tag{12}$$

7. To allow the re-randomization of the ciphertext, we need to compute the commitments $\vec{C}_F$, $\vec{C}_G$ to the variables :

$$H = h^b \qquad F = f^b, \qquad G = g^b$$

and their corresponding proofs:

$$e(\boxed{d^b}, h) = e(\boxed{H}, d) \qquad e(\boxed{F}, d) = e(f, \boxed{d^b}) \qquad e(\boxed{G}, d) = e(g, \boxed{d^b}) \qquad (13,\ 14,\ 15)$$

8. We put all these proofs together to get $\vec{\pi}$.
9. The ciphertext of the RCCA-scheme is

$$(\vec{C} = (C_1, C_2, C_3), \vec{C}_H, \vec{C}_{d^b}, \vec{C}_M, \{\vec{C}_{R_1}\}_{i=1}^{2}, \{\vec{C}_{D_i}\}_{i=1}^{3}, \{\vec{C}_{S_i}\}_{i=1}^{2}, \{\vec{C}_{\Sigma_i}\}_{i=1}^{3}, \{\vec{C}_{\Delta_i}\}_{i=1}^{3}, \vec{C}_F, \vec{C}_G, \vec{\pi})$$

***ReRandom*(PK, C):** This algorithm takes as input the public key and the ciphertext $C = (C_1, C_2, C_3)$, then outputs a re-randomized new ciphertext $C' = (C'_1, C'_2, C'_3)$ and the new ciphertext is unlinkable to the original one.

In this algorithm, for the variable X, we denote its commitment by $\vec{C}_X = (1, 1, X) \cdot \vec{g}_1^{r_X} \cdot \vec{g}_2^{s_X} \cdot \vec{g}_3^{t_X}$ its new commitment from the first stage by $\vec{C}'_X = \vec{C}_X \cdot \vec{g}_1^{r'_X} \cdot \vec{g}_2^{s'_X} \cdot \vec{g}_3^{t'_X}$ and denote the new randomness introduced in the second step by $(\tilde{r}_X, \tilde{s}_X, \tilde{t}_X)$.

For the randomization, we will proceed in two stages. Firstly we sample two random values $(\theta'_1, \theta'_2) \leftarrow \mathbb{Z}_p$. The new variables are $C'_1 = C_1 \cdot f^{\theta'_1}$, $C'_2 = C_2 \cdot g^{\theta'_2}$ and $C'_3 = C_3 \cdot h^{\theta'_1 + \theta'_2}$. Then using the proof of the equations $(13, 14, 15)$, to update the new proofs corresponding the new ciphertext $\vec{C}' = (C'_1, C'_2, C'_3)$.

For the second stage, we randomize all the commitments and the GS proofs without changing the ciphertext part $\vec{C}' = (C'_1, C'_2, C'_3)$.

First Stage : Rerandomize the ciphertext and update the proofs.

1. To update the proofs we need the old proof elements of the equations $(13, 14, 15)$. We first explicit the proofs elements for these equations:
   (a) Equation 13:
   $e(\boxed{d^b}, h) = e(\boxed{H}, d)$:
   The Verification equation is: $E(\vec{C}_b, \iota(h)) = E(\vec{C}_H, d) \cdot E(\iota(\pi_{13,1}), \vec{g}_1) \cdot E(\iota(\pi_{13,2}), \vec{g}_2) \cdot E(\iota(\pi_{13,3}), \vec{g}_3)$
   with
   $\pi_{13,1} = h^{r_{d^b}} \cdot d^{-r_H}$
   $\pi_{13,2} = h^{s_{d^b}} \cdot d^{-s_H}$
   $\pi_{13,3} = h^{t_{d^b}} \cdot d^{-t_H}$
   (b) Equation 14:
   $e(\boxed{F}, d) = e(f, \boxed{d^b})$
   The Verification equation is: $E(\vec{C}_F, \iota(d)) = E(\iota(f), \vec{C}_{d^b}) \cdot E(\iota(\pi_{14,1}), \vec{g}_1) \cdot E(\iota(\pi_{14,2}), \vec{g}_2) \cdot E(\iota(\pi_{14,3}), \vec{g}_3)$
   with
   $\pi_{14,1} = d^{r_F} \cdot f^{-r_{d^b}}$
   $\pi_{14,2} = d^{s_F} \cdot f^{-s_{d^b}}$
   $\pi_{14,3} = d^{t_F} \cdot f^{-t_{d^b}}$
   (c) Equation 15:
   $e(\boxed{G}, d) = e(g, \boxed{d^b})$
   The Verification equation is: $E(\vec{C}_G, \iota(d)) = E(\iota(g), \vec{C}_{d^b}) \cdot E(\iota(\pi_{15,1}), \vec{g}_1) \cdot E(\iota(\pi_{15,2}), \vec{g}_2) \cdot E(\iota(\pi_{15,3}), \vec{g}_3)$
   with
   $\pi_{15,1} = d^{r_G} \cdot g^{-r_{d^b}}$
   $\pi_{15,1} = d^{s_G} \cdot g^{-s_{d^b}}$
   $\pi_{15,1} = d^{t_G} \cdot g^{-t_{d^b}}$
2. We generate two new random values (θ'_1, θ'_2), and compute the new ciphertext vector $\vec{C}' = (C'_1, C'_2, C'_3) = (C_1 \cdot f^{\theta'_1}, C_2 \cdot g^{\theta'_2}, C_3 \cdot h^{\theta'_1+\theta'_2})$. We compute the new commitments, then update the proofs for the equation $(2, 3, 4, 5, 6, 7, 8, 9, 10)$. Update the commitments:
   (a) $\vec{C}'_{\Delta_1} = \vec{C}_{\Delta_1} \cdot \vec{C}_F^{\theta'_1}$
   (b) $\vec{C}'_{\Delta_2} = \vec{C}_{\Delta_2} \cdot \vec{C}_G^{\theta'_2}$
   (c) $\vec{C}'_{\Delta_3} = \vec{C}_{\Delta_3} \cdot \vec{C}_H^{\theta'_1+\theta'_2}$
   (d) $\vec{C}'_{R_1} = \vec{C}_{R_1} \cdot \vec{C}_{d^b}^{\theta'_1}$
   (e) $\vec{C}'_{R_2} = \vec{C}_{R_2} \cdot \vec{C}_{d^b}^{\theta'_2}$
   (f) $\vec{C}'_{S_1} = \vec{C}_{S_1} \cdot \vec{C}_{d^b}^{\theta'_1}$
   (g) $\vec{C}'_{S_2} = \vec{C}_{S_2} \cdot \vec{C}_{d^b}^{\theta'_2}$

(a) Equation 2:

$e(\boxed{\Delta_1}, d) = e(C_1, \boxed{d^b})$:

The Verification equation is: $E(\vec{C}_{\Delta_1}, \iota(d)) = E(\iota(C_1), \vec{C}_{d^b}) \cdot E(\iota(\pi_{2,1}), \vec{g}_1) \cdot E(\iota(\pi_{2,2}), \vec{g}_2) \cdot E(\iota(\pi_{2,3}), \vec{g}_3)$

with

$\pi_{2,1} = d^{r_{\Delta_1}} \cdot C_1^{-r_{d^b}}$

$\pi_{2,2} = d^{s_{\Delta_1}} \cdot C_1^{-s_{d^b}}$

$\pi_{2,3} = d^{t_{\Delta_1}} \cdot C_1^{-t_{d^b}}$

The new proofs of the equations are:

$\pi'_{2,1} = d^{r_{\Delta_1}+r'_{\Delta_1}} \cdot C_1^{-r_{d^b}} \cdot f^{-r_{d^b} \cdot \theta'_1}$

$\pi'_{2,2} = d^{s_{\Delta_1}+s'_{\Delta_1}} \cdot C_1^{-s_{d^b}} \cdot f^{-s_{d^b} \cdot \theta'_1}$

$\pi'_{2,3} = d^{t_{\Delta_1}+t'_{\Delta_1}} \cdot C_1^{-t_{d^b}} \cdot f^{-t_{d^b} \cdot \theta'_1}$

Using the proof $\vec{\pi}_{14}$, we can update the proof elements:

$\pi'_{2,1} = \pi_{2,1} \cdot \pi_{14,1}^{\theta'_1}$

$\pi'_{2,2} = \pi_{2,2} \cdot \pi_{14,2}^{\theta'_1}$

$\pi'_{2,3} = \pi_{2,3} \cdot \pi_{14,3}^{\theta'_1}$

(b) Equation 3:

$e(\boxed{\Delta_2}, d) = e(C_2, \boxed{d^b})$:

The Verification equation is: $E(\vec{C}_{\Delta_2}, \iota(d)) = E(\iota(C_2), \vec{C}_{d^b}) \cdot E(\iota(\pi_{3,1}), \vec{g}_1) \cdot E(\iota(\pi_{3,2}), \vec{g}_2) \cdot E(\iota(\pi_{3,3}), \vec{g}_3)$

with

$\pi_{3,1} = d^{r_{\Delta_2}} \cdot C_2^{-r_{d^b}}$

$\pi_{3,2} = d^{s_{\Delta_2}} \cdot C_2^{-s_{d^b}}$

$\pi_{3,3} = d^{t_{\Delta_2}} \cdot C_2^{-t_{d^b}}$

The new proofs of the equations are:

$\pi'_{3,1} = d^{r_{\Delta_2}+r'_{\Delta_2}} \cdot C_2^{-r_{d^b}} \cdot g^{-r_{d^b} \cdot \theta'_2}$

$\pi'_{3,2} = d^{s_{\Delta_2}+s'_{\Delta_2}} \cdot C_2^{-s_{d^b}} \cdot g^{-s_{d^b} \cdot \theta'_2}$

$\pi'_{3,3} = d^{t_{\Delta_2}+t'_{\Delta_2}} \cdot C_2^{-t_{d^b}} \cdot g^{-t_{d^b} \cdot \theta'_2}$

Using the proof $\vec{\pi}_{15}$, we can update the proof elements:

$\pi'_{3,1} = \pi_{3,1} \cdot \pi_{15,1}^{\theta'_2}$

$\pi'_{3,2} = \pi_{3,2} \cdot \pi_{15,2}^{\theta'_2}$

$\pi'_{3,3} = \pi_{3,3} \cdot \pi_{15,3}^{\theta'_2}$

(c) Equation 4:

$e(\boxed{\Delta_3}, d) = e(C_3, \boxed{d^b})$:

The Verification equation is: $E(\vec{C}_{\Delta_3}, \iota(d)) = E(\iota(C_3), \vec{C}_{d^b}) \cdot E(\iota(\pi_{4,1}), \vec{g}_1) \cdot E(\iota(\pi_{4,2}), \vec{g}_2) \cdot E(\iota(\pi_{4,3}), \vec{g}_3)$

with

$\pi_{4,1} = d^{r_{\Delta_3}} \cdot C_3^{-r_{d^b}}$

$\pi_{4,2} = d^{s_{\Delta_3}} \cdot C_3^{-s_{d^b}}$

$\pi_{4,3} = d^{t_{\Delta_3}} \cdot C_3^{-t_{d^b}}$

The new proofs of the equations are:

$\pi'_{4,1} = d^{r_{\Delta_3}+r'_{\Delta_3}} \cdot C_3^{-r_{d^b}} \cdot h^{-r_{d^b}\cdot(\theta'_1+\theta'_2)}$

$\pi'_{4,2} = d^{s_{\Delta_3}+s'_{\Delta_3}} \cdot C_3^{-s_{d^b}} \cdot h^{-s_{d^b}\cdot(\theta'_1+\theta'_2)}$

$\pi'_{4,3} = d^{t_{\Delta_3}+t'_{\Delta_3}} \cdot C_3^{-t_{d^b}} \cdot h^{-t_{d^b}\cdot(\theta'_1+\theta'_2)}$

Using the proof $\vec{\pi}_{13}$, we can update the proof elements:

$\pi'_{4,1} = \pi_{4,1} \cdot \pi_{13,1}^{-(\theta'_1+\theta'_2)}$

$\pi'_{4,2} = \pi_{4,1} \cdot \pi_{13,2}^{-(\theta'_1+\theta'_2)}$

$\pi'_{4,3} = \pi_{4,1} \cdot \pi_{13,3}^{-(\theta'_1+\theta'_2)}$

(d) Equation 5:

$e(\boxed{\Delta_1}, d) = e(f, \boxed{R_1})$:

The Verification equation is: $E(\vec{C}_{\Delta_1}, \iota(d)) = E(\iota(f), \vec{C}_{R_1}) \cdot E(\iota(\pi_{5,1}), \vec{g}_1) \cdot E(\iota(\pi_{5,2}), \vec{g}_2) \cdot E(\iota(\pi_{5,3}), \vec{g}_3)$

with

$\pi_{5,1} = d^{r_{\Delta_1}} \cdot f^{-r_{R_1}}$

$\pi_{5,2} = d^{s_{\Delta_1}} \cdot f^{-s_{R_1}}$

$\pi_{5,3} = d^{t_{\Delta_1}} \cdot f^{-t_{R_1}}$

Using the proof $\vec{\pi}_{14}$ we can update the proof elements:

$\pi'_{5,1} = \pi_{5,1} \cdot \pi_{14,1}^{\theta'_1}$

$\pi'_{5,2} = \pi_{5,2} \cdot \pi_{14,2}^{\theta'_1}$

$\pi'_{5,3} = \pi_{5,3} \cdot \pi_{14,3}^{\theta'_1}$

(e) Equation 6:

$e(\boxed{\Delta_2}, d) = e(f, \boxed{R_2})$:

The Verification equation is: $E(\vec{C}_{\Delta_2}, \iota(h)) = E(\iota(f), \vec{C}_{R_2}) \cdot E(\iota(\pi_{6,1}), \vec{g}_1) \cdot E(\iota(\pi_{6,2}), \vec{g}_2) \cdot E(\iota(\pi_{6,3}), \vec{g}_3)$

with

$\pi_{6,1} = d^{r_{\Delta_2}} \cdot f^{-r_{R_2}}$

$\pi_{6,2} = d^{s_{\Delta_2}} \cdot f^{-s_{R_2}}$

$\pi_{6,3} = d^{t_{\Delta_2}} \cdot f^{-t_{R_2}}$

Using the proof $\vec{\pi}_{15}$ we can update the proof elements:

$\pi'_{6,1} = \pi_{6,1} \cdot d^{r'_{\Delta_2}} \cdot f^{-r'_{R_2}} = \pi_{7,1} \cdot \pi_{15,1}^{\theta'_2}$

$\pi'_{6,2} = \pi_{6,2} \cdot d^{s'_{\Delta_2}} \cdot f^{-s'_{R_2}} = \pi_{7,2} \cdot \pi_{15,2}^{\theta'_2}$

$\pi'_{6,3} = \pi_{6,3} \cdot d^{t'_{\Delta_2}} \cdot f^{-t'_{R_2}} = \pi_{7,3} \cdot \pi_{15,3}^{\theta'_2}$

(f) Equation 7:

$e(\boxed{\Delta_3}, d) \cdot e(\boxed{M}, d^{-1}) = e(\boxed{R_1}, h) \cdot e(\boxed{R_2}, h)$:

The Verification equation is: $E(\vec{C}_{\Delta_3}, \iota(d)) \cdot E(\vec{C}_M, \iota(d^{-1})) = E(\vec{C}_{R_1}, \iota(h)) \cdot E(\vec{C}_{R_2}, \iota(h)) \cdot E(\iota(\pi_{7,1}), \vec{g}_1) \cdot E(\iota(\pi_{7,2}), \vec{g}_2) \cdot E(\iota(\pi_{7,3}), \vec{g}_3)$
with

$\pi_{7,1} = d^{r_{\Delta_3}} \cdot d^{-r_M} \cdot h^{-r_{R_1}} \cdot h^{-r_{R_2}}$

$\pi_{7,2} = d^{s_{\Delta_3}} \cdot d^{-s_M} \cdot h^{-s_{R_1}} \cdot h^{-s_{R_2}}$

$\pi_{7,3} = d^{t_{\Delta_3}} \cdot d^{-t_M} \cdot h^{-t_{R_1}} \cdot h^{-t_{R_2}}$

Using the proof $\vec{\pi}_{13}$ we can update the proof elements:

$\pi'_{7,1} = \pi_{7,1} \cdot d^{r'_{\Delta_3}} \cdot h^{-r'_{R_1}} \cdot h^{-r'_{R_2}} = \pi_{7,1} \cdot \pi_{13,1}^{-(\theta'_1+\theta'_2)}$

$\pi'_{7,2} = \pi_{7,2} \cdot d^{s'_{\Delta_3}} \cdot h^{-s'_{R_1}} \cdot h^{-s'_{R_2}} = \pi_{7,2} \cdot \pi_{13,2}^{-(\theta'_1+\theta'_2)}$

$\pi'_{7,3} = \pi_{7,3} \cdot d^{t'_{\Delta_3}} \cdot h^{-t'_{R_1}} \cdot h^{-t'_{R_2}} = \pi_{7,3} \cdot \pi_{13,3}^{-(\theta'_1+\theta'_2)}$

(g) Equation 8:
$e(C_1/\boxed{\Delta_1}, d) = e(\boxed{D_1}, d) \cdot e(f^{-1}, \boxed{S_1})$
The Verification equation is: $E(\iota(C_1)/\vec{C}_{\Delta_1}, \iota(d)) = E(\vec{C}_{D_1}, \iota(d)) \cdot E(\iota(f^{-1}), \vec{C}_{S_1}) \cdot E(\iota(\pi_{8,1}), \vec{g}_1) \cdot E(\iota(\pi_{8,2}), \vec{g}_2) \cdot E(\iota(\pi_{8,3}), \vec{g}_3)$
with

$\pi_{8,1} = d^{-r_{\Delta_1}} \cdot d^{-r_{D_1}} \cdot f^{r_{S_1}}$

$\pi_{8,2} = d^{-s_{\Delta_1}} \cdot d^{-s_{D_1}} \cdot f^{s_{S_1}}$

$\pi_{8,3} = d^{-t_{\Delta_1}} \cdot d^{-t_{D_1}} \cdot f^{t_{S_1}}$

Using the proof $\vec{\pi}_{14}$ we can update the proof elements:

$\pi'_{8,1} = \pi_{8,1} \cdot d^{-r'_{\Delta_1}} \cdot f^{r'_{S_1}} = \pi_{8,1} \cdot \pi_{14,1}^{-\theta'_1}$

$\pi'_{8,2} = \pi_{8,2} \cdot d^{-s'_{\Delta_1}} \cdot f^{s'_{S_1}} = \pi_{8,2} \cdot \pi_{14,2}^{-\theta'_1}$

$\pi'_{8,3} = \pi_{8,3} \cdot d^{-t'_{\Delta_1}} \cdot f^{t'_{S_1}} = \pi_{8,3} \cdot \pi_{14,3}^{-\theta'_1}$

(h) Equation 9:
$e(C_2/\boxed{\Delta_2}, d) = e(\boxed{D_2}, d) \cdot e(g^{-1}, \boxed{S_2})$
The Verification equation is: $E(\iota(C_2)/\vec{C}_{\Delta_2}, \iota(d)) = E(\vec{C}_{D_2}, \iota(d)) \cdot E(\iota(g^{-1}), \vec{C}_{S_2}) \cdot E(\iota(\pi_{9,1}), \vec{g}_1) \cdot E(\iota(\pi_{9,2}), \vec{g}_2) \cdot E(\iota(\pi_{9,3}), \vec{g}_3)$
with

$\pi_{9,1} = d^{-r_{\Delta_2}} \cdot d^{-r_{D_2}} \cdot g^{r_{S_2}}$

$\pi_{9,2} = d^{-s_{\Delta_2}} \cdot d^{-s_{D_2}} \cdot g^{s_{S_2}}$

$\pi_{9,3} = d^{-t_{\Delta_2}} \cdot d^{-t_{D_2}} \cdot g^{t_{S_2}}$

Using the proof $\vec{\pi}_{15}$ we can update the proof elements:

$\pi'_{9,1} = \pi_{9,1} \cdot d^{-r'_{\Delta_2}} \cdot f^{-r'_{S_2}} = \pi_{9,1} \cdot \pi_{15,1}^{-\theta'_2}$

$\pi'_{9,2} = \pi_{9,2} \cdot d^{-s'_{\Delta_2}} \cdot f^{-s'_{S_2}} = \pi_{9,2} \cdot \pi_{15,2}^{-\theta'_2}$

$\pi'_{9,3} = \pi_{9,3} \cdot d^{-t'_{\Delta_2}} \cdot f^{-t'_{S_2}} = \pi_{9,3} \cdot \pi_{15,3}^{-\theta'_2}$

(i) Equation 10:
$e(C_3/\boxed{\Delta_3}, d) = e(\boxed{D_3}, d) \cdot e(\boxed{S_1}, h^{-1}) \cdot e(\boxed{S_2}, h^{-1})$
The Verification equation is: $E(\iota(C_3/\vec{C}_{\Delta_3}), \iota(d)) = E(\vec{C}_{D_3}, \iota(d)) \cdot E(\iota(h^{-1}), \vec{C}_{S_1}) \cdot E(\iota(h^{-1}), \vec{C}_{S_2}) \cdot E(\iota(\pi_{10,1}), \vec{g}_1) \cdot E(\iota(\pi_{10,2}), \vec{g}_2) \cdot E(\iota(\pi_{10,3}), \vec{g}_3)$
with

$$\pi_{10,1} = d^{-r_{\Delta_3}} \cdot d^{-r_{D_3}} \cdot h^{r_{S_1}} \cdot h^{r_{S_2}}$$
$$\pi_{10,2} = d^{-s_{\Delta_3}} \cdot d^{-s_{D_3}} \cdot h^{s_{S_1}} \cdot h^{s_{S_2}}$$
$$\pi_{10,3} = d^{-t_{\Delta_3}} \cdot d^{-t_{D_3}} \cdot h^{t_{S_1}} \cdot h^{t_{S_2}}$$

Using the proof $\vec{\pi}_{13}$ we can update the proof elements:

$$\pi'_{10,1} = \pi_{10,1} \cdot d^{-r'_{\Delta_3}} \cdot h^{r'_{S_1}} \cdot h^{r'_{S_2}} = \pi_{10,1} \cdot \pi_{13,1}^{\theta'_1+\theta'_2}$$
$$\pi'_{10,2} = \pi_{10,1} \cdot d^{-s'_{\Delta_3}} \cdot h^{s'_{S_1}} \cdot h^{s'_{S_2}} = \pi_{10,2} \cdot \pi_{13,2}^{\theta'_1+\theta'_2}$$
$$\pi'_{10,3} = \pi_{10,1} \cdot d^{-t'_{\Delta_3}} \cdot h^{t'_{S_1}} \cdot h^{t'_{S_2}} = \pi_{10,3} \cdot \pi_{13,3}^{\theta'_1+\theta'_2}$$

Second Stage : Rerandomize the commitments and the proofs.

For each commitment $\vec{C}_X$ or $\vec{C}'_X$, we randomize it with $\tilde{vec}C_X = \vec{C}_X \cdot g_1^{r_X} \cdot g_2^{s_X} \cdot g_3^{t_X}$.

1. The proof of the quadratic equation: $e(d, \boxed{d^b}) = e(\boxed{d^b}, \boxed{d^b})$
   The Verification equation is: $E(\iota(d), \vec{C}_{d^b}) = E(\vec{C}_{d^b}, \vec{C}_{d^b}) \cdot E(\vec{\pi}_{1,1}, \vec{g}_1) \cdot E(\vec{\pi}_{1,2}, \vec{g}_2) \cdot E(\vec{\pi_{1,3}}, \vec{g}_3)$
   with

$$\vec{\pi}_{1,1} = \iota(d^b)^{2r_{d^b}} \cdot (\vec{g}_1^{r_{d^b}} \cdot \vec{g}_2^{s_{d^b}} \cdot \vec{g}_3^{t_{d^b}})^{r_{d^b}} \cdot \iota(d^{-1})^{r_{d^b}}$$
$$\vec{\pi}_{1,2} = \iota(d^b)^{2s_{d^b}} \cdot (\vec{g}_1^{r_{d^b}} \cdot \vec{g}_2^{s_{d^b}} \cdot \vec{g}_3^{t_{d^b}})^{s_{d^b}} \cdot \iota(d^{-1})^{s_{d^b}}$$
$$\vec{\pi}_{1,3} = \iota(d^b)^{2t_{d^b}} \cdot (\vec{g}_1^{r_{d^b}} \cdot \vec{g}_2^{s_{d^b}} \cdot \vec{g}_3^{t_{d^b}})^{t_{d^b}} \cdot \iota(d^{-1})^{t_{d^b}}$$

   The new proofs of the new equations can be generated as:

$$\tilde{\vec{\pi}}_{1,1} = \vec{\pi}_{1,1} \cdot \vec{C}_{d^b}^{2\tilde{r}_{d^b}} \cdot (\vec{g}_1^{\tilde{r}_{d^b}} \cdot \vec{g}_2^{\tilde{s}_{d^b}} \cdot \vec{g}_3^{\tilde{t}_{d^b}})^{\tilde{r}_{d^b}} \cdot \iota(d^{-1})^{\tilde{r}_{d^b}}$$
$$\tilde{\vec{\pi}}_{1,2} = \vec{\pi}_{1,2} \cdot \vec{C}_{d^b}^{2\tilde{s}_{d^b}} \cdot (\vec{g}_1^{\tilde{r}_{d^b}} \cdot \vec{g}_2^{\tilde{s}_{d^b}} \cdot \vec{g}_3^{\tilde{t}_{d^b}})^{\tilde{s}_{d^b}} \cdot \iota(d^{-1})^{\tilde{s}_{d^b}}$$
$$\tilde{\vec{\pi}}_{1,3} = \vec{\pi}_{1,3} \cdot \vec{C}_{d^b}^{2\tilde{t}_{d^b}} \cdot (\vec{g}_1^{\tilde{r}_{d^b}} \cdot \vec{g}_2^{\tilde{s}_{d^b}} \cdot \vec{g}_3^{\tilde{t}_{d^b}})^{\tilde{t}_{d^b}} \cdot \iota(d^{-1})^{\tilde{t}_{d^b}}$$

2. Equation 2:
   $e(\boxed{\Delta'_1}, d) = e(C'_1, \boxed{d^b})$:
   The Verification equation is: $E(\vec{C}_{\Delta'_1}, \iota(d)) = E(\iota(C'_1), \vec{C}_{d^b}) \cdot E(\iota(\pi_{2,1}), \vec{g}_1) \cdot E(\iota(\pi_{2,2}), \vec{g}_2) \cdot E(\iota(\pi_{2,3}), \vec{g}_3)$
   with

$$\pi_{2,1} = d^{r_{\Delta'_1}} \cdot C_1'^{-r_{d^b}}$$
$$\pi_{2,2} = d^{s_{\Delta'_1}} \cdot C_1'^{-s_{d^b}}$$
$$\pi_{2,3} = d^{t_{\Delta'_1}} \cdot C_1'^{-t_{d^b}}$$

   The new proofs of the equations are:

$$\tilde{\pi}_{2,1} = \pi'_{2,1} \cdot d^{\tilde{r}_{\Delta'_1}} \cdot C_1'^{-\tilde{r}_{d^b}}$$
$$\tilde{\pi}_{2,2} = \pi'_{2,2} \cdot d^{\tilde{s}_{\Delta'_1}} \cdot C_1'^{-\tilde{s}_{d^b}}$$
$$\tilde{\pi}_{2,3} = \pi'_{2,3} \cdot d^{\tilde{t}_{\Delta'_1}} \cdot C_1'^{-\tilde{t}_{d^b}}$$

3. Equation 3:
   $e(\boxed{\Delta'_2}, d) = e(C'_2, \boxed{d^b})$:
   The Verification equation is: $E(\vec{C}'_{\Delta_2}, \iota(d)) = E(\iota(C'_2), \vec{C}_{d^b}) \cdot E(\iota(\pi_{4,1}), \vec{g}_1) \cdot E(\iota(\pi_{4,2}), \vec{g}_2) \cdot E(\iota(\pi_{4,3}), \vec{g}_3)$
   with

$\pi_{3,1} = d^{r_{\Delta'_2}} \cdot C_2'^{-r_{d^b}}$

$\pi_{3,2} = d^{s_{\Delta'_2}} \cdot C_2'^{-s_{d^b}}$

$\pi_{3,3} = d^{t_{\Delta'_2}} \cdot C_2'^{-t_{d^b}}$

The new proofs of the equations are:

$\tilde{\pi}_{3,1} = \pi'_{3,1} \cdot d^{\tilde{r}_{\Delta'_2}} \cdot C_2'^{-\tilde{r}_{d^b}}$

$\tilde{\pi}_{3,2} = \pi'_{3,2} \cdot d^{\tilde{s}_{\Delta'_2}} \cdot C_2'^{-\tilde{s}_{d^b}}$

$\tilde{\pi}_{3,3} = \pi'_{3,2} \cdot d^{\tilde{t}_{\Delta'_2}} \cdot C_2'^{-\tilde{t}_{d^b}}$

4. Equation 4:
   $e(\boxed{\Delta'_3}, d) = e(C'_3, \boxed{d^b})$:
   The Verification equation is: $E(\vec{C}_{\Delta'_3}, \iota(d)) = E(\iota(C'_3), \vec{C}_{d^b}) \cdot E(\iota(\pi_{5,1}), \vec{g}_1) \cdot E(\iota(\pi_{5,2}), \vec{g}_2) \cdot E(\iota(\pi_{5,3}), \vec{g}_3)$
   with

$\pi_{4,1} = d^{r_{\Delta'_3}} \cdot C_3'^{-r_{d^b}}$

$\pi_{4,2} = d^{s_{\Delta'_3}} \cdot C_3'^{-s_{d^b}}$

$\pi_{4,3} = d^{t_{\Delta'_3}} \cdot C_3'^{-t_{d^b}}$

The new proofs of the equations are:

$\tilde{\pi}_{4,1} = \pi'_{4,1} \cdot d^{\tilde{r}_{\Delta'_3}} \cdot C_3'^{-\tilde{r}_{d^b}}$

$\tilde{\pi}_{4,2} = \pi'_{4,1} \cdot d^{\tilde{s}_{\Delta'_3}} \cdot C_3'^{-\tilde{s}_{d^b}}$

$\tilde{\pi}_{4,3} = \pi'_{4,1} \cdot d^{\tilde{t}_{\Delta'_3}} \cdot C_3'^{-\tilde{t}_{d^b}}$

5. $e(\boxed{\Delta_1}, d) = e(f, \boxed{R_1})$:
   The Verification equation is: $E(\vec{C}_{\Delta'_1}, \iota(d)) = E(\iota(f), \vec{C}_{R'_1}) \cdot E(\iota(\pi_{5,1}), \vec{g}_1) \cdot E(\iota(\pi_{5,2}), \vec{g}_2) \cdot E(\iota(\pi_{5,3}), \vec{g}_3)$
   with

$\pi_{5,1} = d^{r_{\Delta'_1}} \cdot f^{-r_{R'_1}}$

$\pi_{5,2} = d^{s_{\Delta'_1}} \cdot f^{-s_{R'_1}}$

$\pi_{5,3} = d^{t_{\Delta'_1}} \cdot f^{-t_{R'_1}}$

The new proofs of the equations are:

$\tilde{\pi}_{5,1} = \pi'_{5,1} \cdot d^{\tilde{r}_{\Delta'_1}} \cdot f^{-\tilde{r}_{R'_1}}$

$\tilde{\pi}_{5,2} = \pi'_{5,2} \cdot d^{\tilde{s}_{\Delta'_1}} \cdot f^{-\tilde{s}_{R'_1}}$

$\tilde{\pi}_{5,3} = \pi'_{5,3} \cdot d^{\tilde{t}_{\Delta'_1}} \cdot f^{-\tilde{t}_{R'_1}}$

6. $e(\boxed{\Delta'_2}, d) = e(f, \boxed{R'_2})$:
   The Verification equation is: $E(\vec{C}_{\Delta'_2}, \iota(h)) = E(\iota(f), \vec{C}_{R'_2}) \cdot E(\iota(\pi_{6,1}), \vec{g}_1) \cdot E(\iota(\pi_{6,2}), \vec{g}_2) \cdot E(\iota(\pi_{6,3}), \vec{g}_3)$
   with

$\pi_{6,1} = d^{r_{\Delta'_2}} \cdot f^{-r_{R'_2}}$

$\pi_{6,2} = d^{s_{\Delta'_2}} \cdot f^{-s_{R'_2}}$

$\pi_{6,3} = d^{t_{\Delta'_2}} \cdot f^{-t_{R'_2}}$

The new proofs of the equations are:

$\tilde{\pi}_{6,1} = \pi'_{6,1} \cdot d^{\tilde{r}_{\Delta'_2}} \cdot f^{-\tilde{r}_{R'_2}}$

$\tilde{\pi}_{6,2} = \pi'_{6,2} \cdot d^{\tilde{s}_{\Delta'_2}} \cdot f^{-\tilde{s}_{R'_2}}$

$\tilde{\pi}_{6,3} = \pi'_{6,3} \cdot d^{\tilde{t}_{\Delta'_2}} \cdot f^{-\tilde{t}_{R'_2}}$

7. $e(\boxed{\Delta'_3}, d) \cdot e(\boxed{M}, d^{-1}) = e(\boxed{R'_1}, h) \cdot e(\boxed{R'_2}, h)$:

The Verification equation is: $E(\vec{C}_{\Delta'_3}, \iota(d)) \cdot E(\vec{C}_M, \iota(d^{-1})) = E(\vec{C}_{R'_1}, \iota(h)) \cdot E(\vec{C}_{R'_2}, \iota(h)) \cdot E(\iota(\pi_{7,1}), \vec{g}_1) \cdot E(\iota(\pi_{7,2}), \vec{g}_2) \cdot E(\iota(\pi_{7,3}), \vec{g}_3)$

with

$\pi_{7,1} = d^{r_{\Delta'_3}} \cdot d^{-r_M} \cdot h^{-r_{R'_1}} \cdot h^{-r_{R'_2}}$

$\pi_{7,2} = d^{s_{\Delta'_3}} \cdot d^{-s_M} \cdot h^{-s_{R'_1}} \cdot h^{-s_{R'_2}}$

$\pi_{7,3} = d^{t_{\Delta'_3}} \cdot d^{-t_M} \cdot h^{-t_{R'_1}} \cdot h^{-t_{R'_2}}$

The new proofs of the equations are:

$\tilde{\pi}_{7,1} = \pi'_{7,1} \cdot d^{\tilde{r}_{\Delta'_3}} \cdot d^{-\tilde{r}_M} \cdot h^{-\tilde{r}_{R'_1}} \cdot h^{-\tilde{r}_{R'_2}}$

$\tilde{\pi}_{7,2} = \pi'_{7,2} \cdot d^{\tilde{s}_{\Delta'_3}} \cdot d^{-\tilde{s}_M} \cdot h^{-\tilde{s}_{R'_1}} \cdot h^{-\tilde{s}_{R'_2}}$

$\tilde{\pi}_{7,3} = \pi'_{7,3} \cdot d^{\tilde{t}_{\Delta'_3}} \cdot d^{-\tilde{t}_M} \cdot h^{-\tilde{t}_{R'_1}} \cdot h^{-\tilde{t}_{R'_2}}$

8. $e(C'_1/\boxed{\Delta'_1}, d) = e(\boxed{D_1}, d) \cdot e(f^{-1}, \boxed{S'_1})$

The Verification equation is: $E(\iota(C'_1)/\vec{C}_{\Delta'_1}, \iota(d)) = E(\vec{C}_{D_1}, \iota(d)) \cdot E(\iota(f^{-1}), \vec{C}_{S'_1}) \cdot E(\iota(\pi_{8,1}), \vec{g}_1) \cdot E(\iota(\pi_{8,2}), \vec{g}_2) \cdot E(\iota(\pi_{8,3}), \vec{g}_3)$

with

$\pi_{8,1} = d^{-r_{\Delta'_1}} \cdot d^{-r_{D_1}} \cdot f^{r_{S'_1}}$

$\pi_{8,2} = d^{-s_{\Delta'_1}} \cdot d^{-s_{D_1}} \cdot f^{s_{S'_1}}$

$\pi_{8,3} = d^{-t_{\Delta'_1}} \cdot d^{-t_{D_1}} \cdot f^{t_{S'_1}}$

The new proofs of the equations are:

$\tilde{\pi}_{8,1} = \pi'_{8,1} \cdot d^{-\tilde{r}_{\Delta'_1}} \cdot d^{-\tilde{r}_{D_1}} \cdot f^{\tilde{r}_{S'_1}}$

$\tilde{\pi}_{8,2} = \pi'_{8,2} \cdot d^{-\tilde{s}_{\Delta'_1}} \cdot d^{-\tilde{s}_{D_1}} \cdot f^{\tilde{s}_{S'_1}}$

$\tilde{\pi}_{8,3} = \pi'_{8,3} \cdot d^{-\tilde{t}_{\Delta'_1}} \cdot d^{-\tilde{t}_{D_1}} \cdot f^{\tilde{t}_{S'_1}}$

9. $e(C'_2/\boxed{\Delta'_2}, d) = e(\boxed{D_2}, d) \cdot e(g^{-1}, \boxed{S'_2})$

The Verification equation is: $E(\iota(C'_2)/\vec{C}_{\Delta'_2}, \iota(d)) = E(\vec{C}_{D_2}, \iota(d)) \cdot E(\iota(g^{-1}), \vec{C}_{S'_2}) \cdot E(\iota(\pi_{9,1}), \vec{g}_1) \cdot E(\iota(\pi_{9,2}), \vec{g}_2) \cdot E(\iota(\pi_{9,3}), \vec{g}_3)$

with

$\pi_{9,1} = d^{-r_{\Delta'_2}} \cdot d^{-r_{D_2}} \cdot g^{r_{S'_2}}$

$\pi_{9,2} = d^{-s_{\Delta'_2}} \cdot d^{-s_{D_2}} \cdot g^{s_{S'_2}}$

$\pi_{9,3} = d^{-t_{\Delta'_2}} \cdot d^{-t_{D_2}} \cdot g^{t_{S'_2}}$

The new proofs of the equations are:

$\tilde{\pi}_{9,1} = \pi'_{9,1} \cdot d^{-\tilde{r}_{\Delta'_2}} \cdot d^{-\tilde{r}_{D_2}} \cdot g^{-\tilde{r}_{S'_2}}$

$\tilde{\pi}_{9,2} = \pi'_{9,2} \cdot d^{-\tilde{s}_{\Delta'_2}} \cdot d^{-\tilde{s}_{D_2}} \cdot g^{-\tilde{s}_{S'_2}}$

$\tilde{\pi}_{9,3} = \pi'_{9,3} \cdot d^{-\tilde{t}_{\Delta'_2}} \cdot d^{-\tilde{t}_{D_2}} \cdot g^{-\tilde{t}_{S'_2}}$

10. $e(C'_3/\boxed{\Delta'_3}, d) = e(\boxed{D_3}, d) \cdot e(\boxed{S'_1}, h^{-1}) \cdot e(\boxed{S'_2}, h^{-1})$
    The Verification equation is: $E(\iota(C'_3/\vec{C}_{\Delta'_3}), \iota(d)) = E(\vec{C}_{D_3}, \iota(d)) \cdot E(\iota(h^{-1}), \vec{C}_{S'_1}) \cdot E(\iota(h^{-1}), \vec{C}_{S'_2}) \cdot E(\iota(\pi_{10,1}), \vec{g}_1) \cdot E(\iota(\pi_{10,2}), \vec{g}_2) \cdot E(\iota(\pi_{10,3}), \vec{g}_3)$
    with

$\pi_{10,1} = d^{-r_{\Delta'_3}} \cdot d^{-r_{D_3}} \cdot h^{r_{S'_1}} \cdot h^{r_{S'_2}}$

$\pi_{10,2} = d^{-s_{\Delta'_3}} \cdot d^{-s_{D_3}} \cdot h^{s_{S'_1}} \cdot h^{s_{S'_2}}$

$\pi_{10,3} = d^{-t_{\Delta'_3}} \cdot d^{-t_{D_3}} \cdot h^{t_{S'_1}} \cdot h^{t_{S'_2}}$

    The new proofs of the equations are:

$\tilde{\pi}_{10,1} = \pi'_{10,1} \cdot d^{-\tilde{r}_{\Delta'_3}} \cdot d^{-\tilde{r}_{D_3}} \cdot h^{\tilde{r}_{S'_1}} \cdot h^{\tilde{r}_{S'_2}}$

$\tilde{\pi}_{10,2} = \pi'_{10,1} \cdot d^{-\tilde{s}_{\Delta'_3}} \cdot d^{-\tilde{s}_{D_3}} \cdot h^{\tilde{s}_{S'_1}} \cdot h^{\tilde{s}_{S'_2}}$

$\tilde{\pi}_{10,3} = \pi'_{10,1} \cdot d^{-\tilde{t}_{\Delta'_3}} \cdot d^{-\tilde{t}_{D_3}} \cdot h^{\tilde{t}_{S'_1}} \cdot h^{\tilde{t}_{S'_2}}$

11. $e(\alpha, d/\boxed{d^b}) = e(g_z, \boxed{\Sigma_1}) \cdot e(g_r, \boxed{\Sigma_2}) \cdot \prod_{i=1}^{3} e(g_i, \boxed{D_i})$
    The Verification equation is: $E(\iota(a), \iota(h)/\vec{C}_b) = E(\iota(g_z), \vec{C}_{\Sigma_1}) \cdot E(\iota(g_r), \vec{C}_{\Sigma_2}) \cdot \prod_{i=1}^{3} E(\iota(g_i)), \vec{C}_{D_i} \cdot E(\iota(\pi_{12,1}), \vec{g}_1) \cdot E(\iota(\pi_{12,2}), \vec{g}_2) \cdot E(\iota(\pi_{12,3}), \vec{g}_3)$
    with

$\pi_{12,1} = \alpha^{-r_{d^b}} \cdot g_z^{-r_{\Sigma_1}} \cdot g_r^{-r_{\Sigma_2}} \cdot \prod_{i=1}^{3} g_i^{-r_{D_i}}$

$\pi_{12,2} = \alpha^{-s_{d^b}} \cdot g_z^{-s_{\Sigma_1}} \cdot g_r^{-s_{\Sigma_2}} \cdot \prod_{i=1}^{3} g_i^{-s_{D_i}}$

$\pi_{12,3} = \alpha^{-t_{d^b}} \cdot g_z^{-t_{\Sigma_1}} \cdot g_r^{-t_{\Sigma_2}} \cdot \prod_{i=1}^{3} g_i^{-t_{D_i}}$

    The new proofs of the equations are:

$\tilde{\pi}_{12,1} = \pi_{12,1} \cdot \alpha^{-\tilde{r}_{d^b}} \cdot g_z^{-\tilde{r}_{\Sigma_1}} \cdot g_r^{-\tilde{r}_{\Sigma_2}} \cdot \prod_{i=1}^{3} g_i^{-\tilde{r}_{D_i}}$

$\tilde{\pi}_{12,2} = \pi_{12,2} \cdot \alpha^{-\tilde{s}_{d^b}} \cdot g_z^{-\tilde{s}_{\Sigma_1}} \cdot g_r^{-\tilde{s}_{\Sigma_2}} \cdot \prod_{i=1}^{3} g_i^{-\tilde{s}_{D_i}}$

$\tilde{\pi}_{12,3} = \pi_{12,3} \cdot \alpha^{-\tilde{t}_{d^b}} \cdot g_z^{-\tilde{t}_{\Sigma_1}} \cdot g_r^{-\tilde{t}_{\Sigma_2}} \cdot \prod_{i=1}^{3} g_i^{-\tilde{t}_{D_i}}$

12. $e(\beta, d/\boxed{d^b}) = e(h_z, \boxed{\Sigma_1}) \cdot e(h_u, \boxed{\Sigma_3}) \cdot \prod_{i=1}^{3} e(h_i, \boxed{D_i})$
    The Verification equation is: $E(\iota(b), \iota(h)/\vec{C}_b) = E(\iota(h_z), \vec{C}_{\Sigma_1}) \cdot E(\iota(h_u), \vec{C}_{\Sigma_3}) \cdot \prod_{i=1}^{3} E(\iota(h_i)), \vec{C}_{D_i} \cdot E(\iota(\pi_{13,1}), \vec{g}_1) \cdot E(\iota(\pi_{13,2}), \vec{g}_2) \cdot E(\iota(\pi_{13,3}), \vec{g}_3)$
    with

$\pi_{13,1} = \beta^{-r_{d^b}} \cdot h_z^{-r_{\Sigma_1}} \cdot h_u^{-r_{\Sigma_3}} \cdot \prod_{i=1}^{3} h_i^{-r_{D_i}}$

$\pi_{13,2} = \beta^{-s_{d^b}} \cdot h_z^{-s_{\Sigma_1}} \cdot h_u^{-s_{\Sigma_3}} \cdot \prod_{i=1}^{3} h_i^{-s_{D_i}}$

$\pi_{13,3} = \beta^{-t_{d^b}} \cdot h_z^{-t_{\Sigma_1}} \cdot h_u^{-t_{\Sigma_3}} \cdot \prod_{i=1}^{3} h_i^{-t_{D_i}}$

    The new proofs of the equations are:

$\tilde{\pi}_{13,1} = \pi_{13,1} \cdot \beta^{-\tilde{r}_{d^b}} \cdot h_z^{-\tilde{r}_{\Sigma_1}} \cdot h_u^{-\tilde{r}_{\Sigma_3}} \cdot \prod_{i=1}^{3} h_i^{-\tilde{r}_{D_i}}$

$\tilde{\pi}_{13,2} = \pi_{13,1} \cdot \beta^{-\tilde{s}_{d^b}} \cdot h_z^{-\tilde{s}_{\Sigma_1}} \cdot h_u^{-\tilde{s}_{\Sigma_3}} \cdot \prod_{i=1}^{3} h_i^{-\tilde{s}_{D_i}}$

$\tilde{\pi}_{13,3} = \pi_{13,1} \cdot \beta^{-\tilde{t}_{d^b}} \cdot h_z^{-\tilde{t}_{\Sigma_1}} \cdot h_u^{-\tilde{t}_{\Sigma_3}} \cdot \prod_{i=1}^{3} h_i^{-\tilde{t}_{D_i}}$

13. $e(\boxed{d^b}, h) = e(\boxed{h^b}, d)$:
The Verification equation is: $E(\vec{C}_b, \iota(h)) = E(\vec{C}_{h^b}, d) \cdot E(\iota(\pi_{13,1}), \vec{g}_1) \cdot E(\iota(\pi_{13,2}), \vec{g}_2) \cdot E(\iota(\pi_{13,3}), \vec{g}_3)$
with

$\pi_{13,1} = h^{r_{d^b}} \cdot d^{-r_{h^b}}$

$\pi_{13,2} = h^{s_{d^b}} \cdot d^{-s_{h^b}}$

$\pi_{13,3} = h^{t_{d^b}} \cdot d^{-t_{h^b}}$

We can rerandomize this proof using the following formulas:

$\tilde{\pi}_{13,1} = h^{r_{d^b}+\tilde{r}_{d^b}} \cdot d^{r_{h^b}+\tilde{r}_{h^b}} = \pi_{13,1} \cdot h^{\tilde{r}_{d^b}} \cdot d^{\tilde{r}_{h^b}}$

$\tilde{\pi}_{13,2} = h^{s_{d^b}+\tilde{s}_{d^b}} \cdot d^{s_{h^b}+\tilde{s}_{h^b}} = \pi_{13,2} \cdot h^{\tilde{s}_{d^b}} \cdot d^{\tilde{s}_{h^b}}$

$\tilde{\pi}_{13,3} = h^{t_{d^b}+\tilde{t}_{d^b}} \cdot d^{t_{h^b}+\tilde{t}_{h^b}} = \pi_{13,3} \cdot h^{\tilde{t}_{d^b}} \cdot d^{\tilde{t}_{h^b}}$

14. $e(\boxed{F}, d) = e(f, \boxed{d^b})$
The Verification equation is: $E(\vec{C}_F, \iota(d)) = E(\iota(f), \vec{C}_{d^b}) \cdot E(\iota(\pi_{14,1}), \vec{g}_1) \cdot E(\iota(\pi_{14,2}), \vec{g}_2) \cdot E(\iota(\pi_{14,3}), \vec{g}_3)$
with

$\pi_{14,1} = d^{r_F} \cdot f^{-r_{d^b}}$

$\pi_{14,2} = d^{s_F} \cdot f^{-s_{d^b}}$

$\pi_{14,3} = d^{t_F} \cdot f^{-t_{d^b}}$

The new proofs of the equations are:

$\tilde{\pi}_{14,1} = \tilde{\pi}_{14,1} \cdot d^{\tilde{r}_F} \cdot f^{-\tilde{r}_{d^b}}$

$\tilde{\pi}_{14,2} = \tilde{\pi}_{14,2} \cdot d^{\tilde{s}_F} \cdot f^{-\tilde{s}_{d^b}}$

$\tilde{\pi}_{14,3} = \tilde{\pi}_{14,3} \cdot d^{\tilde{t}_F} \cdot f^{-\tilde{t}_{d^b}}$

15. $e(\boxed{G}, d) = e(g, \boxed{d^b})$
The Verification equation is: $E(\vec{C}_G, \iota(d)) = E(\iota(g), \vec{C}_{d^b}) \cdot E(\iota(\pi_{15,1}), \vec{g}_1) \cdot E(\iota(\pi_{15,2}), \vec{g}_2) \cdot E(\iota(\pi_{15,3}), \vec{g}_3)$
with

$\pi_{15,1} = d^{r_G} \cdot g^{-r_{d^b}}$

$\pi_{15,1} = d^{s_G} \cdot g^{-s_{d^b}}$

$\pi_{15,1} = d^{t_G} \cdot g^{-t_{d^b}}$

The new proofs of the equations are:

$\tilde{\pi}_{15,1} = \pi_{15,1} \cdot d^{\tilde{r}_G} \cdot g^{-\tilde{r}_{d^b}}$

$\tilde{\pi}_{15,1} = \pi_{15,1} \cdot d^{\tilde{s}_G} \cdot g^{-\tilde{s}_{d^b}}$

$\tilde{\pi}_{15,1} = \pi_{15,1} \cdot d^{\tilde{t}_G} \cdot g^{-\tilde{t}_{d^b}}$

5 Efficiency

From the efficiency point of view, there are in total 108 group elements.

For the efficientcy reason, we can replace

- $(\vec{\pi}_3, \vec{\pi}_9)$ by $(\vec{\pi}_3 \cdot \vec{\pi}_9)$

- $(\vec{\pi}_4, \vec{\pi}_{10})$ by $(\vec{\pi}_4 \cdot \vec{\pi}_{10})$
- $(\vec{\pi}_5, \vec{\pi}_{11})$ by $(\vec{\pi}_5 \cdot \vec{\pi}_{11})$
- $(\vec{\pi}_6, \vec{\pi}_{12})$ by $(\vec{\pi}_6 \cdot \vec{\pi}_{12})$
- $(\vec{\pi}_7, \vec{\pi}_{13})$ by $(\vec{\pi}_7 \cdot \vec{\pi}_{13})$

Thus we can reduce the number of group elements down to $108 - 5 \cdot 3 = 93$.

$\tilde{\vec{\pi}}^{2,8}$:

(a) $\tilde{\pi}_1^{2,8} = \pi_1^{2,8} \cdot \pi_{14,1}^{\theta'_1} \cdot d^{\tilde{r}_{\Delta'_1}} \cdot C_1^{\prime -\tilde{r}_{d^b}} \cdot \pi_{14,1}^{-\theta'_1} \cdot d^{-\tilde{r}_{\Delta'_1}} \cdot d^{-\tilde{r}_{D_1}} \cdot f^{\tilde{r}_{S'_1}} = \pi_1^{2,8} \cdot C_1^{\prime -\tilde{r}_{d^b}} \cdot d^{-\tilde{r}_{D_1}}$

(b) $\tilde{\pi}_2^{2,8} = \pi_2^{2,8} \cdot \pi_{14,2}^{\theta'_1} \cdot d^{\tilde{s}_{\Delta'_1}} \cdot C_1^{\prime -\tilde{s}_{d^b}} \cdot \pi_{14,2}^{-\theta'_1} \cdot d^{-\tilde{s}_{\Delta'_1}} \cdot d^{-\tilde{s}_{D_1}} \cdot f^{\tilde{s}_{S'_1}} = \pi_2^{2,8} \cdot C_1^{\prime -\tilde{s}_{d^b}} \cdot d^{-\tilde{s}_{D_1}}$

(c) $\tilde{\pi}_3^{2,8} = \pi_3^{2,8} \cdot \pi_{14,3}^{\theta'_1} \cdot d^{\tilde{t}_{\Delta'_1}} \cdot C_1^{\prime -\tilde{t}_{d^b}} \cdot \pi_{14,3}^{-\theta'_1} \cdot d^{-\tilde{t}_{\Delta'_1}} \cdot d^{-\tilde{t}_{D_1}} \cdot f^{\tilde{t}_{S'_1}} = \pi_3^{2,8} \cdot C_1^{\prime -\tilde{t}_{d^b}} \cdot d^{-\tilde{t}_{D_1}}$

$\tilde{\vec{\pi}}^{3,9}$:

(a) $\tilde{\pi}_1^{3,9} = \pi_1^{3,9} \cdot \pi_{15,1}^{\theta'_2} \cdot d^{\tilde{r}_{\Delta'_2}} \cdot C_2^{\prime -\tilde{r}_{d^b}} \cdot \pi_{15,1}^{-\theta'_2} \cdot d^{-\tilde{r}_{\Delta'_2}} \cdot d^{-\tilde{r}_{D_2}} \cdot g^{-\tilde{r}_{S'_2}} = \pi_1^{3,9} \cdot C_2^{-\tilde{r}_{d^b}} \cdot d^{-\tilde{r}_{D_2}} \cdot g^{-\tilde{r}_{S'_2}}$

(b) $\tilde{\pi}_2^{3,9} = \pi_2^{3,9} \cdot \pi_{15,2}^{\theta'_2} \cdot d^{\tilde{s}_{\Delta'_2}} \cdot C_2^{\prime -\tilde{s}_{d^b}} \cdot \pi_{15,2}^{-\theta'_2} \cdot d^{-\tilde{s}_{\Delta'_2}} \cdot d^{-\tilde{s}_{D_2}} \cdot g^{-\tilde{s}_{S'_2}} = \pi_2^{3,9} \cdot C_2^{-\tilde{r}_{d^b}} \cdot d^{-\tilde{s}_{D_2}} \cdot g^{-\tilde{s}_{S'_2}}$

(c) $\tilde{\pi}_3^{3,9} = \pi_3^{3,9} \cdot \pi_{15,3}^{\theta'_2} \cdot d^{\tilde{t}_{\Delta'_2}} \cdot C_2^{\prime -\tilde{t}_{d^b}} \cdot \pi_{15,3}^{-\theta'_2} \cdot d^{-\tilde{t}_{\Delta'_2}} \cdot d^{-\tilde{t}_{D_2}} \cdot g^{-\tilde{t}_{S'_2}} = \pi_3^{3,9} \cdot C_2^{-\tilde{r}_{d^b}} \cdot d^{-\tilde{t}_{D_2}} \cdot g^{-\tilde{t}_{S'_2}}$

$\tilde{\vec{\pi}}^{4,10}$:

(a) $\tilde{\pi}_1^{4,10} = \pi_1^{4,10} \cdot \pi_{13,1}^{-(\theta'_1+\theta'_2)} \cdot d^{\tilde{r}_{\Delta'_3}} \cdot C_3^{\prime -\tilde{r}_{d^b}} \cdot \pi_{13,1}^{\theta'_1+\theta'_2} \cdot d^{-\tilde{r}_{\Delta'_3}} \cdot d^{-\tilde{r}_{D_3}} \cdot h^{\tilde{r}_{S'_1}} \cdot h^{\tilde{r}'_{S_2}} = \pi_1^{5,11} \cdot C_3^{-\tilde{r}_{d^b}} \cdot d^{-\tilde{r}_{D_3}} \cdot h^{\tilde{r}_{S'_1}} \cdot h^{\tilde{r}'_{S_2}}$

(b) $\tilde{\pi}_2^{4,10} = \pi_2^{4,10} \cdot \pi_{13,2}^{-(\theta'_1+\theta'_2)} \cdot d^{\tilde{s}_{\Delta'_3}} \cdot C_3^{\prime -\tilde{s}_{d^b}} \cdot \pi_{13,2}^{\theta'_1+\theta'_2} \cdot d^{-\tilde{s}_{\Delta'_3}} \cdot d^{-\tilde{s}_{D_3}} \cdot h^{\tilde{s}_{S'_1}} \cdot h^{\tilde{s}'_{S_2}} = \pi_2^{5,11} \cdot C_3^{-\tilde{s}_{d^b}} \cdot d^{-\tilde{s}_{D_3}} \cdot h^{\tilde{s}_{S'_1}} \cdot h^{\tilde{s}'_{S_2}}$

(c) $\tilde{\pi}_3^{4,10} = \pi_3^{4,10} \cdot \pi_{13,3}^{-(\theta'_1+\theta'_2)} \cdot d^{\tilde{t}_{\Delta'_3}} \cdot C_3^{\prime -\tilde{t}_{d^b}} \cdot \pi_{13,3}^{\theta'_1+\theta'_2} \cdot d^{-\tilde{t}_{\Delta'_3}} \cdot d^{-\tilde{t}_{D_3}} \cdot h^{\tilde{t}_{S'_1}} \cdot h^{\tilde{t}'_{S_2}} = \pi_3^{5,11} \cdot C_3^{-\tilde{t}_{d^b}} \cdot d^{-\tilde{t}_{D_3}} \cdot h^{\tilde{t}_{S'_1}} \cdot h^{\tilde{t}'_{S_2}}$

$\tilde{\vec{\pi}}^{5,11}$:

(a) $\tilde{\pi}_1^{5,11} = \pi_1^{5,12} \cdot \pi_{14,1}^{\theta'_1} \cdot d^{r_{\Delta'_1}} \cdot f^{-r'_{R_1}} \cdot \alpha^{-\tilde{r}_{d^b}} \cdot g_z^{-\tilde{r}_{\Sigma_1}} \cdot g_r^{-\tilde{r}_{\Sigma_2}} \cdot \prod_{i=1}^{3} g_i^{-\tilde{r}_{D_i}}$

(b) $\tilde{\pi}_2^{5,11} = \pi_2^{5,12} \cdot \pi_{14,2}^{\theta'_1} \cdot d^{s_{\Delta'_1}} \cdot f^{-s'_{R_1}} \cdot \alpha^{-\tilde{s}_{d^b}} \cdot g_z^{-\tilde{s}_{\Sigma_1}} \cdot g_r^{-\tilde{s}_{\Sigma_2}} \cdot \prod_{i=1}^{3} g_i^{-\tilde{s}_{D_i}}$

(c) $\tilde{\pi}_3^{5,11} = \pi_3^{5,12} \cdot \pi_{14,3}^{\theta'_1} \cdot d^{t_{\Delta'_1}} \cdot f^{-t'_{R_1}} \cdot \alpha^{-\tilde{t}_{d^b}} \cdot g_z^{-\tilde{t}_{\Sigma_1}} \cdot g_r^{-\tilde{t}_{\Sigma_2}} \cdot \prod_{i=1}^{3} g_i^{-\tilde{t}_{D_i}}$

$\tilde{\vec{\pi}}^{6,12}$:

(a) $\tilde{\pi}_1^{6,12} = \pi_1^{7,13} \cdot \pi_{15,1}^{\theta'_2} \cdot d^{r_{\Delta'_2}} \cdot f^{-r_{R'_2}} \cdot \beta^{-\tilde{r}_{d^b}} \cdot h_z^{-\tilde{r}_{\Sigma_1}} \cdot h_u^{-\tilde{r}_{\Sigma_3}} \cdot \prod_{i=1}^{3} h_i^{-\tilde{r}_{D_i}}$

(b) $\tilde{\pi}_2^{6,12} = \pi_2^{7,13} \cdot \pi_{15,2}^{\theta'_2} \cdot d^{s_{\Delta'_2}} \cdot f^{-s_{R'_2}} \cdot \beta^{-\tilde{s}_{d^b}} \cdot h_z^{-\tilde{s}_{\Sigma_1}} \cdot h_u^{-\tilde{s}_{\Sigma_3}} \cdot \prod_{i=1}^{3} h_i^{-\tilde{s}_{D_i}}$

(c) $\tilde{\pi}_3^{6,12} = \pi_3^{7,13} \cdot \pi_{15,3}^{\theta'_2} \cdot d^{t_{\Delta'_2}} \cdot f^{-t_{R'_2}} \cdot \beta^{-\tilde{t}_{d^b}} \cdot h_z^{-\tilde{t}_{\Sigma_1}} \cdot h_u^{-\tilde{t}_{\Sigma_3}} \cdot \prod_{i=1}^{3} h_i^{-\tilde{t}_{D_i}}$

6 Construction of Structure Perserving Public Encryption scheme

7 Instantiation of the trapdoor commitment scheme

***TC*.Setup($1^\lambda, \ell$)** : Generate the public parameters for the trapdoor commitment scheme for security parameter λ and message vector length ℓ.

1. Choose a random prime $p < 2^\lambda$.
2. Generate a asymmetric pairing groups $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$ of prime order p and a pairing function $e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T$.
3. Generate the group generators $(g, \hat{g}) \in \mathbb{G} \times \hat{\mathbb{G}}$.
4. $\mathsf{PP} = (p, \mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T, e, g, \hat{g}, \ell)$.

***TC*.KeyGen(PP)** :

1. For $i = 1, \ldots, \ell + 2$, generate random values $\rho_i \xleftarrow{R} \mathbb{Z}_p^*$, then compute $\hat{X}_i \leftarrow \hat{g}^{\rho_i}$.
2. Set $\mathsf{ck} \leftarrow \{\hat{X}_i\}_{i=1}^{\ell+2}$ and $tk \leftarrow \{\rho_i\}_i^{\ell+2}$.

***TC*.Commit(PP, ck, $\vec{M}$)** : where $\vec{\hat{M}} = (\hat{M}_1, \ldots, \hat{M}_\ell) \in \hat{\mathbb{G}}^\ell$.

1. Choose a random value $w_z \in \mathbb{Z}_p^*$ then compute $g_z = g^{w_z}$.
2. For $i = 1, \ldots, \ell$, generate random values $\chi_i \xleftarrow{R} \mathbb{Z}_p$ and compute $g_i = g^{\chi_i}$.
3. Set $\mathsf{vk}_{pots} \leftarrow (g_z, g_1, \ldots, g_\ell) \in \mathbb{G}^{\ell+1}$ and $\mathsf{sk}_{pots} \leftarrow (w_z, \chi_1, \ldots, \chi_\ell)$.
4. Choose randomly $a \xleftarrow{R} \mathbb{Z}_p$, then set $\mathsf{ovk}_{pots} = A = g^a$ and $\mathsf{osk}_{pots} = a$.
5. Using the signing key sk_{pots} to generate signatures of the message $\vec{\hat{M}}$ w.r.t. to the one-time signature's secret key osk_{pots}:
   (a) Generate random value $\zeta_1 \in \mathbb{Z}_p$
   (b) Compute the signature $(\hat{Z}, \hat{R}) \in \hat{\mathbb{G}}^2$ for $\vec{\hat{M}}$:

$$\hat{Z} = \hat{g}^{\zeta_1} \qquad\qquad \hat{R} = \hat{g}^{a-\zeta_1 w_z} \prod_{i=1}^{\ell} \hat{M}_i^{\chi_i}$$

6. We use the commitment key to generate the commitment for the message.
   (a) Set $(m_1, \ldots, m_{\ell+2}) \leftarrow (\chi_1, \ldots, \chi_\ell, w_z, a)$
   (b) Parse $\vec{\mathsf{ck}}$ as $(\hat{X}_1, \ldots, \hat{X}_{\ell+2})$.
   (c) Generate a random value $\zeta_2 \leftarrow \mathbb{Z}_p^*$ and compute:

$$\hat{C} = \hat{g}^{\zeta_2} \prod_{i=1}^{\ell+2} \hat{X}_i^{m_i} \qquad\qquad D = g^{\zeta_2}$$

7. We set the commitment as $\mathsf{com} = \hat{C}$ and $\mathsf{open} = (D, g_z, g_1, \ldots, g_\ell, \mathsf{ovk}_{pots} = g^a, \hat{Z}, \hat{R}) \in \mathbb{G}^{\ell+3} \times \hat{\mathbb{G}}^2$.

***TC*.Verify(ck, com, $\vec{\hat{M}}$, open)** :

1. Parse $\vec{\hat{M}}$ with $(\hat{M}_1, \ldots, \hat{M}_\ell)$ and open with $(D, g_z, g_1, \ldots, g_\ell, \mathsf{ovk}_{pots} = g^a, \hat{Z}, \hat{R})$.
2. Set $\vec{N} = (N_1, \ldots, N_{\ell+2}) = (g_1, \ldots, g_\ell, g_z, \mathsf{ovk}_{pots})$
3. Using $\mathsf{ovk}_{pots} = A \in \mathbb{G}$, verify the following equations:

$$e(g, \hat{C}) = e(D, \hat{g}) \prod_{i=1}^{\ell+2} e(N_i, \hat{X}_i) \qquad e(A, \hat{g}) = e(g_z, \hat{Z}) \cdot e(g, \hat{R}) \cdot \prod_{i=1}^{\ell} e(g_i, \hat{M}_i)$$

8 Using the trapdoor commitment scheme to construct more efficient structure preserving publicly verifiable CCA-2 encryption scheme

In this section, we use the previous trapdoor commitment scheme to commit the verification key, as they are constructed to verify so called CMTCR (Chosen-Message Target Collision Resistant) property, this will leads us to a wanted CCA-2 encryption scheme.

***SPCCA*.KeyGen(1^λ)** :

1. Choose a asymmetric pairing group system $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$, groups of prime order $p > 2^\lambda$.
2. Set PP as $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$.
3. Choose also group generators $g_1, g_2 \xleftarrow{R} \mathbb{G}$ and random values $x_1, x_2 \xleftarrow{R} \mathbb{Z}_p$.
4. Generate group generator $\hat{g} \xleftarrow{R} \hat{\mathbb{G}}$
5. Set $X = g_1^{x_1} g_2^{x_2}$.
6. Choose random values $\rho_u, \rho'_u \xleftarrow{R} \mathbb{Z}_p$ and random group generators $(\hat{g}, \hat{h}) \xleftarrow{R} \hat{\mathbb{G}}^2$.
7. Set $(\vec{u}_1, \vec{u}_2)$ as $\vec{u}_1 = (\hat{g}, \hat{h}) \in \hat{\mathbb{G}}^2$ and $\vec{u}_2 = (\hat{g}^{\rho_u}, \hat{h}^{\rho'_u}) \in \hat{\mathbb{G}}^2$. Note that $\vec{u}_1$ and $\vec{u}_2$ are linearly independent with overwhelming probability.
8. Set $\mathsf{PP}_{TC} = (\mathsf{PP}, g_1, \hat{g}, \ell = 6)$.
9. Generate the commitment key $\vec{\mathsf{ck}} \in \hat{\mathbb{G}}^8$ and $\vec{\mathsf{tk}} \in \mathbb{Z}_p^8$
10. Define $\mathsf{SK} = (x_1, x_2)$ and $\mathsf{PK} = (g_1, g_2, \vec{u}_1, \vec{u}_2, X, \mathsf{PP}_{TC}, \vec{\mathsf{ck}})$

***SPCCA*.Enc(M, PK)** :

1. Generate the one-time signature keys $(\mathsf{SSK}, \mathsf{SVK}) \leftarrow OT1.\mathsf{KeyGen}(\mathsf{PP})$ with $\mathsf{SSK} = (\{\chi_i, \gamma_i\}_{i=1}^5, \zeta, \rho) \in \mathbb{Z}_p^{12}$ and $\mathsf{SVK} = (\{\hat{g}_i\}_{i=1}^5, \hat{A}) \in \hat{\mathbb{G}}^6$.
2. Choose $\theta \xleftarrow{R} \mathbb{Z}_p$ and compute

$$C_0 = M \cdot X^\theta, \qquad C_1 = g_1^\theta, \qquad C_2 = g_2^\theta.$$

3. Generate a commitment to $\mathsf{SVK} = (\{\hat{g}_i\}_{i=1}^5, \hat{a})$ and let

$$(\mathsf{com}, \mathsf{open}) \leftarrow TC.\mathsf{Commit}(\mathsf{PP}_{TC}, \vec{ck}, \mathsf{SVK}) \in \hat{\mathbb{G}} \times (\mathbb{G}^9 \times \hat{\mathbb{G}}^2)$$

be the resulting commitment/decommitment pair.

4. Define vector $\vec{u}_{\mathsf{com}} = \vec{u}_2 \cdot (1, \mathsf{com})$ and the Groth-Sahai CRS $\mathbf{u}_{\mathsf{com}} = (\vec{u}_{\mathsf{com}}, \vec{u}_1)$.
5. Pick $r \xleftarrow{R} \mathbb{Z}_p$. Compute $\vec{C}_\theta = \vec{u}_{\mathsf{com}}^{\theta} \cdot (\vec{u}_1)^r$.
6. Using the randomness of the commitment $\vec{C}_\theta$, generate proof elements $\vec{\pi} = (\pi_1, \pi_2) = (g_1^r, g_2^r) \in \mathbb{G}^2$ showing that the committed $\theta \in \mathbb{Z}_p$ satisfies the multi-exponentiation equations
$$C_1 = g_1^{\theta} \qquad\qquad C_2 = g_2^{\theta}$$
7. Output the ciphertext
$$\vec{C} = (\mathsf{SVK}, \mathsf{com}, \mathsf{open}, C_0, C_1, C_2, \vec{C}_\theta, \vec{\pi}, \vec{\sigma}) \in \mathbb{G}^{16} \times \hat{\mathbb{G}}^{11}$$
in which $\vec{\sigma} = OT1.\mathsf{Sign}(\mathsf{SSK}, (C_0, C_1, C_2, \pi_1, \pi_2)) \in \mathbb{G}^2$.
Notice that we don't sign the commitments because in the Groth-Sahai proof system and in this very special case, there is only one valid commitment for given proofs.

***SPCCA*.Dec($\mathsf{PK}, \vec{C}, \mathsf{SK}$)** :

1. Parse PK with $(\vec{g}_1, \vec{g}_2, X, \mathsf{PP}_{TC}, \mathsf{ck})$ and SK with (x_1, x_2).
2. Parse $\vec{C}$ with $(\mathsf{SVK}, \mathsf{com}, \mathsf{open}, C_0, C_1, C_2, \vec{C}_\theta, \vec{\pi}, \vec{\sigma})$.
3. Verify the signature is valid $OT1.\mathsf{Verify}(\mathsf{PP}, (C_0, C_1, C_2, \pi_1, \pi_2), \sigma) = \mathsf{True}$.
4. Using the commitment verification algorithm to verify that $TC.\mathsf{Verify}(\mathsf{ck}, \mathsf{com}, \mathsf{SVK}, \mathsf{open}) = \mathsf{True}$
5. Verify that $\vec{\pi} = (\pi_1, \pi_2)$ is a valid Groth-Sahai proof w.r.t. $(C_1, C_2, \vec{C}_\theta, \mathsf{com})$. Namely, it should satisfy
$$\begin{aligned} E(g_1, \vec{C}_\theta) &= E(C_1, \vec{u}_{\mathsf{com}}) \cdot E(\pi_1, \vec{u}_1) \\ E(g_2, \vec{C}_\theta) &= E(C_2, \vec{u}_{\mathsf{com}}) \cdot E(\pi_2, \vec{u}_1) \end{aligned} \tag{3}$$
6. If any of the verification fails then halt and return $\perp$, otherwise, output $M = C_0/(C_1^{x_1} \cdot C_2^{x_2})$.

Theorem 1. *The scheme provides IND-CCA2 security under the SXDH assumption.*

Proof. The proof proceeds with a sequence of games that begins with the real game and ends with a game where no advantage is left to the adversary. In each game, we call W_i the event that the experiment outputs 1.

Game 0**:** This is the real game. The adversary is given the public key PK which contains vectors $(\vec{u}_1, \vec{u}_2)$ such that
$$\begin{aligned} \vec{u}_1 &= (\hat{g}, \hat{h}) \in \hat{\mathbb{G}}^2 \\ \vec{u}_2 &= (\hat{g}^{\rho_u}, \hat{h}^{\rho'_u}) \in \hat{\mathbb{G}}^2, \end{aligned} \tag{4}$$
where $\hat{g}, \hat{h} \xleftarrow{R} \hat{\mathbb{G}}$, $\rho_u, \rho'_u \xleftarrow{R} \mathbb{Z}_p$. In the challenge phase, it chooses two messages $M_0, M_1 \in \mathbb{G}$ and obtains a challenge ciphertexts
$$\vec{C}^\star = (\mathsf{SVK}^\star, \mathsf{com}^\star, \mathsf{open}^\star, C_0^\star, C_1^\star, C_2^\star, \vec{C}_\theta^\star, \vec{\pi}^\star, \vec{\sigma}^\star)$$

where

$$C_0^\star = M_\beta \cdot X^{\theta^\star}, \qquad C_1^\star = g_1^{\theta^\star}, \qquad C_2^\star = g_2^{\theta^\star},$$

for some random bit $\beta \xleftarrow{R} \{0,1\}$, and

$$\begin{aligned}
\mathsf{com}^\star &= \hat{C}^\star = \hat{g}^{\zeta_2^\star} \cdot \prod_{i=1}^{\ell} \hat{X}_i^{\chi_i^\star} \cdot \hat{X}_{\ell+1}^{w_z^\star} \cdot \hat{X}_{\ell+2}^{a^\star} \\
\mathsf{open}^\star &= (D^\star, g_z^\star, g_1^\star, \ldots, g_\ell^\star, A^\star, \hat{Z}^\star, \hat{R}^\star) \\
&= (g^{\zeta_2^\star},\ g^{w_z^\star},\ g^{\chi_1^\star},\ \ldots,\ g^{\chi_\ell^\star},\ g^{\chi_z^\star},\ g^{a^\star},\ \hat{g}^{\zeta_1^\star},\ \hat{g}^{a^\star - \zeta_1^\star w_z^\star} \cdot \prod_{i=1}^{6} \hat{M}_i^{\star\ \chi_i^\star}), \\
\vec{C}_\theta^\star &= \vec{u}_{\mathsf{com}^\star}^{\theta^\star} \cdot (\vec{u}_1)^{r^\star} \\
\vec{\pi}^\star &= (\pi_1^\star, \pi_2^\star) = (g_1^{r^\star}, g_2^{r^\star})
\end{aligned}$$

with $(\hat{M}_1^\star, \ldots, \hat{M}_\ell^\star) = (\hat{g}_1^\star, \ldots, \hat{g}_5^\star, \hat{A}^\star)$ and $\vec{u}_{\mathsf{com}^\star} = \vec{u}_2 \cdot (1, \mathsf{com}^\star)$. The adversary's decryption queries are always faithfully answered by the challenger. When the adversary halts, it outputs $\beta' \in \{0,1\}$ and wins if $\beta' = \beta$. In this case, the experiment outputs 1. Otherwise, it outputs 0. The adversary's advantage is thus $|\Pr[W_0] - 1/2|$.

Game 1**:** In this game, we modify the generation of the public key and define

$$\begin{aligned}
\vec{u}_1 &= (\hat{g}, \hat{h}) \in \hat{\mathbb{G}}^2 \\
\vec{u}_2 &= (\hat{g}^{\rho_u}, \hat{h}^{\rho'_u}) \cdot (1, \hat{C}^{\star\ -1}) \in \hat{\mathbb{G}}^2.
\end{aligned} \tag{5}$$

instead of computing $(\vec{u}_1, \vec{u}_2)$ as in (4) (note that we may assume w.l.o.g. that $\mathsf{SVK}^\star$ and $\mathsf{com}^\star = \hat{C}^\star$ are generated at the outset of the game). However, this modification does not affect the adversary's view since $\vec{u}_2$ remains uniformly distributed over $\hat{\mathbb{G}}^2$. We have $\Pr[W_1] = \Pr[W_0]$.

Game 2**:** This game is like Game 1 with the difference that, if the adversary makes a pre-challenge decryption query $\vec{C} = (\mathsf{SVK}, \mathsf{com}, \mathsf{open}, C_0, C_1, C_2, \vec{C}_\theta, \vec{\pi}, \vec{\sigma})$ such that $\mathsf{com} = \mathsf{com}^\star$, the expermiment halts and outputs a random bit. Since Game 2 is identical to Game 1 until this event F_2 occurs, we have $|\Pr[W_2] - \Pr[W_1]| \leq \Pr[F_2]$. Moreover, since $\mathsf{com}^\star$ was chosen uniformly in $\hat{\mathbb{G}}$ and remains independent of $\mathcal{A}$'s view until the challenge phase, we have $|\Pr[W_2] - \Pr[W_1]| \leq \Pr[F_2] \leq q_D/p$.

Game 3**:** This game is like Game 2 but we modify the decryption oracle. Namely, if the adversary makes a post-challenge decryption query for a valid ciphertext

$$\vec{C} = (\mathsf{SVK}, \mathsf{com}, \mathsf{open}, C_0, C_1, C_2, \vec{C}_\theta, \vec{\pi}, \vec{\sigma})$$

such that $\mathsf{com} = \mathsf{com}^\star$ but $\mathsf{open} \neq \mathsf{open}^\star$, the experiment halts and outputs a random bit. If we call F_3 the latter event, we have $|\Pr[W_3] - \Pr[W_2]| \leq \Pr[F_3]$. Moreover, event F_3 clearly implies an adversary $\mathcal{B}$ against the target collision-resistance of the structure-preserving trapdoor commitment in Section 7, which contradicts the Double Pairing assumption. Hence, we have $|\Pr[W_3] - \Pr[W_2]| \leq \mathbf{Adv}_{\mathcal{B}}^{\mathsf{TCR\text{-}CR}}(\lambda) \leq \mathbf{Adv}_{\mathcal{B}}^{\mathrm{DP}}(\lambda)$.

Game 4**:** We modify again the decryption oracle. After the phase, if the adversary queries the decryption of a ciphertext $\vec{C} = (\mathsf{SVK}, \mathsf{com}, \mathsf{open}, C_0, C_1, C_2, \vec{C}_\theta, \vec{\pi}, \vec{\sigma})$ such that $(\mathsf{com}, \mathsf{open}) = (\mathsf{com}^\star, \mathsf{open}^\star)$ but $(C_0, C_1, C_2, \pi_1, \pi_2) \neq (C_0^\star, C_1^\star, C_2^\star, \pi_1^\star, \pi_2^\star)$, the experiment halts and outputs a random bit. If we call F_4 this event, we have the inequality $|\Pr[W_4] - \Pr[W_3]| \leq \Pr[F_4]$ since Game 4 is identical to Game 3 until F_4 occurs. Moreover, F_4 would contradict the strong unforgeability of the one-time structure-preserving signature and thus the DP assumption. This implies $|\Pr[W_4] - \Pr[W_3]| \leq \mathbf{Adv}_{\mathcal{B}}^{\mathsf{SUF\text{-}OTS}}(\lambda) \leq \mathbf{Adv}_{\mathcal{B}}^{\mathrm{DP}}(\lambda)$.

Game 5**:** We introduce yet another modification in the decryption oracle. We let the decryption oracle reject all ciphertexts $\vec{C} = (\mathsf{SVK}, \mathsf{com}, \mathsf{open}, C_0, C_1, C_2, \vec{C}_\theta, \vec{\pi}, \vec{\sigma})$ such that

$$(\mathsf{com}, \mathsf{open}) = (\mathsf{com}^\star, \mathsf{open}^\star) \quad \wedge \quad (C_0, C_1, C_2, \pi_1, \pi_2) = (C_0^\star, C_1^\star, C_2^\star, \pi_1^\star, \pi_2^\star) \quad \wedge \quad \vec{C}_\theta \neq \vec{C}_\theta^\star. \tag{6}$$

Let F_5 be the event that the decryption oracle rejects a ciphertext that would not have been rejected in Game 4. We argue that $\Pr[W_5] = \Pr[W_4]$ since Game 5 is identical to Game 4 until event F_5 occurs and we have $\Pr[F_5] = 0$. Indeed, for a given $(C_1^\star, C_2^\star, \pi_1^\star, \pi_2^\star) \in \mathbb{G}^4$, there exists only one commitment $\vec{C}_\theta^\star \in \hat{\mathbb{G}}^2$ that satisfies the equalities (3). This follows from the fact that, since $(C_1^\star, C_2^\star, \pi_1^\star, \pi_2^\star) = (g_1^{\theta^\star}, g_2^{\theta^\star}, g_1^{r^\star}, g_2^{r^\star})$, relations (3) can be written

$$\begin{aligned} E(g_1, \vec{C}_\theta^\star) &= E(g_1^{\theta^\star}, \vec{u}_{\mathsf{com}}) \cdot E(g_1^{r^\star}, \vec{u}_1) = E(g_1, \vec{u}_{\mathsf{com}}^{\theta^\star}) \cdot E(g_1, \vec{u}_1^{r^\star}) \\ E(g_2, \vec{C}_\theta^\star) &= E(g_2^{\theta^\star}, \vec{u}_{\mathsf{com}}) \cdot E(g_2^{r^\star}, \vec{u}_1) = E(g_2, \vec{u}_{\mathsf{com}}^{\theta^\star}) \cdot E(g_2, \vec{u}_1^{r^\star}) \end{aligned}$$

which uniquely determines the only commitment $\vec{C}_\theta^\star = \vec{u}_{\mathsf{com}}^{\theta^\star} \cdot \vec{u}_1^{r^\star} \in \hat{\mathbb{G}}^2$ that satisfies (3). This shows that $\Pr[F_5] = 0$, as claimed.

Game 6**:** In this game, we modify the distribution of the public key. Namely, instead of generating the vectors $(\vec{u}_1, \vec{u}_2)$ as in (5), we set

$$\begin{aligned} \vec{u}_1 &= (\hat{g}, \hat{h}) \in \hat{\mathbb{G}}^2 \\ \vec{u}_2 &= (\hat{g}^{\rho_u}, \hat{h}^{\rho_u}) \cdot (1, \hat{C}^{\star\ -1}) \in \hat{\mathbb{G}}^2. \end{aligned} \tag{7}$$

Said otherwise, $\vec{u}_2$ is now the product of two terms, the first one of which lives in the one-dimensional subspace spanned by $\vec{u}_1$. Under the DDH assumption in $\hat{\mathbb{G}}$, this modified distribution of PK should have not noticeable impact on the adversary's behavior. A straightforward reduction shows that $|\Pr[W_6] - \Pr[W_5]| \leq \mathbf{Adv}_{\mathcal{B}}^{\mathrm{DDH}}(\lambda)$. Note that, although the vectors $(\vec{u}_{\mathsf{com}^\star}, \vec{u}_1) \in \hat{\mathbb{G}}^2$ are no longer linearly independent, $\vec{C}_\theta^\star = \vec{u}_1^{\rho_u \cdot \theta^\star + r^\star}$ remains the only commitment that satisfies the verification equations for a given tuple $(C_1^\star, C_2^\star, \pi_1^\star, \pi_2^\star)$.

Game 7**:** In this game, we modify the challenge ciphertext and replace the NIZK proof $\vec{\pi}^\star = (\pi_1^\star, \pi_2^\star) \in \mathbb{G}^2$ by a simulated proof which is produced using $\rho_u \in \mathbb{Z}_p$ as a simulation trapdoor. Namely, $(\vec{C}_\theta^\star, \vec{\pi}^\star)$ is obtained by picking $r \xleftarrow{R} \mathbb{Z}_p$ and computing

$$\vec{C}_\theta^\star = \vec{u}_1^r, \qquad \pi_1^\star = g_1^r \cdot C_1^{\star -\rho_u}, \qquad \pi_2^\star = g_2^r \cdot C_2^{\star -\rho_u}$$

Observe that, although $(\vec{C}_\theta^\star, \pi_1^\star, \pi_2^\star)$ are generated without using the witness $\theta^\star = \log_{g_1}(C_1^\star) = \log_{g_2}(C_2^\star)$, the NIZK property of GS proofs ensures that their distribution remains exactly as in Game 6: indeed, if we define $\tilde{r} = r - \rho_u \cdot \theta^\star$, we have

$$\vec{C}_\theta^\star = \vec{u}_{\mathsf{com}^\star}^{\theta^\star} \cdot \vec{u}_1^{\tilde{r}}, \qquad \pi_1^\star = g_1^{\tilde{r}}, \qquad \pi_2^\star = g_2^{\tilde{r}},$$

which implies $\Pr[W_7] = \Pr[W_6]$.

Game 8**:** We modify the generation of the challenge ciphertext, which is generated using the private key $\mathsf{SK} = (x_1, x_2)$ instead of the public key: Namely, the challenger computes

$$C_1^\star = g_1^{\theta^\star}, \qquad C_2^\star = g_2^{\theta^\star}, \qquad C_0^\star = M_\beta \cdot C_1^{\star x_1} \cdot C_2^{\star x_2},$$

while $(\vec{C}_\theta^\star, \pi_1^\star, \pi_2^\star)$ are computed using the NIZK simulation trapdoor $\rho_u \in \mathbb{Z}_p$ as in Game 7. This modification does not affect the adversary's view since the ciphertext retains exactly the same distribution as in Game 7. We have $\Pr[W_8] = \Pr[W_7]$.

Game 9**:** We modify again the distribution of the challenge ciphertext which is obtained as

$$C_1^\star = g_1^{\theta_1^\star}, \qquad C_2^\star = g_2^{\theta_2^\star}, \qquad C_0^\star = M_\beta \cdot C_1^{\star x_1} \cdot C_2^{\star x_2},$$

for random and independent $\theta_1^\star, \theta_2^\star \stackrel{R}{\leftarrow} \mathbb{Z}_p$, while the NIZK proof $(\vec{C}_\theta^\star, \pi_1^\star, \pi_2^\star)$ is simulated using $\rho_u \in \mathbb{Z}_p$ as in Game 8. Since the witness $\theta^\star \in \mathbb{Z}_p$ was not used anymore in Game 8, a straightforward reduction shows that any noticeable change in $\mathcal{A}$'s output distribution implies a DDH distinguisher in $\mathbb{G}$. We have $|\Pr[W_9] - \Pr[W_8]| \leq \mathbf{Adv}^{\mathrm{DDH}}_{\mathcal{B},\mathbb{G}}(\lambda)$.

We remark that, although we now have $\log_{g_1}(C_1^\star) \neq \log_{g_2}(C_2^\star)$ with overwhelming probability, the signed ciphertext components $(C_1^\star, C_2^\star, \pi_1^\star, \pi_2^\star)$ still uniquely determine $\vec{C}_\theta^\star \in \hat{\mathbb{G}}^2$ as the only commitment that satisfies the verification equations of $(\vec{C}_\theta^\star, \pi_1^\star, \pi_2^\star)$: indeed, the equalities

$$\begin{aligned} E(g_1, \vec{C}_\theta^\star) &= E(C_1^\star, \vec{u}_{\mathsf{com}^\star}) \cdot E(\pi_1^\star, \vec{u}_1) \\ E(g_2, \vec{C}_\theta^\star) &= E(C_2^\star, \vec{u}_{\mathsf{com}^\star}) \cdot E(\pi_2^\star, \vec{u}_1) \end{aligned}$$

can be written

$$\begin{aligned} E(g_1, \vec{C}_\theta^\star) &= E(C_1^\star, \vec{u}_1^{\rho_u}) \cdot E(g_1^r \cdot C_1^{\star -\rho_u}, \vec{u}_1) = E(g_1^r, \vec{u}_1) \\ E(g_2, \vec{C}_\theta^\star) &= E(C_2^\star, \vec{u}_1^{\rho_u}) \cdot E(g_2^r \cdot C_2^{\star -\rho_u}, \vec{u}_1) = E(g_2^r, \vec{u}_1), \end{aligned}$$

which implies that $\vec{C}_\theta^\star = \vec{u}_1^r$ is the only commitment satisfying (3). Hence, at any step of the sequence of games, $\vec{C}_\theta^\star$ is always uniquely determined by $(C_1^\star, C_2^\star, \pi_1^\star, \pi_2^\star)$ and does not have to be signed.

In the final game, it is easy to see that $\Pr[W_9] = 1/2$ since the challenge ciphertext does not carry any information about $\beta \in \{0, 1\}$. Indeed, we have

$$C_1^\star = g_1^{\theta_1^\star}, \qquad C_2^\star = g_2^{\theta_1^\star + \theta_1'}, \qquad C_0^\star = M_\beta \cdot X^{\theta_1^\star} \cdot {g_2}^{\theta_1' \cdot x_2},$$

for some random $\theta_1' \in_R \mathbb{Z}_p$, which implies that the term ${g_2}^{\theta_1' \cdot x_2}$ perfectly hides M_β in the expression of $C_0^\star$. This follows from the fact that $x_2 \in \mathbb{Z}_p$ is perfectly independent of the adversary's view. Indeed, the public key leaves $x_2 \in \mathbb{Z}_p$ completely undetermined as it only reveals $X = g_1^{x_1} g_2^{x_2}$. During the game, decryption queries are guaranteed not to reveal anything about x_2 since all NIZK proofs $(\vec{C}_\theta, \pi_1, \pi_2)$ take place on Groth-Sahai CRSes $(\vec{u}_{\mathsf{com}}, \vec{u}_1)$ which are perfectly sound (as they span the

entire vector space $\hat{\mathbb{G}}^2$) whenever $\mathsf{com} \neq \mathsf{com}^\star$. This implies that, although the adversary can see a simulated NIZK proof $(\vec{C}_\theta^\star, \pi_1^\star, \pi_2^\star)$ for a false statement in the challenge phase, it remains unable to trick the decryption oracle into accepting a ciphertext $\vec{C} = (\mathsf{SVK}, \mathsf{com}, \mathsf{open}, C_0, C_1, C_2, \vec{C}_\theta, \vec{\pi}, \vec{\sigma})$ such that $\log_{g_1}(C_1) \neq \log_{g_2}(C_2)$. As a consequence, the adversary does not learn anything about x_2 from responses of the decryption oracle.

□

9 Combine Structure Perserving Public Encryption scheme with LHSPS

***RCCA*3.KeyGen(1^λ)** :

1. Choose a asymmetric pairing group system $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$, groups of prime order $p > 2^\lambda$.
2. Set PP as $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$.
3. Choose also group generators $g_1, g_2 \xleftarrow{R} \mathbb{G}$ and random values $x_1, x_2 \xleftarrow{R} \mathbb{Z}_p$.
4. Generate group generator $\hat{g} \xleftarrow{R} \hat{\mathbb{G}}$
5. Set $X = g_1^{x_1} g_2^{x_2}$.
6. Generate random values ρ_u and random group generators $(\hat{g}, \hat{h}) \xleftarrow{R} \hat{\mathbb{G}}^2$.
7. Set $(\vec{u}_1, \vec{u}_2)$ as $\vec{u}_1 = (\hat{g}, \hat{h}) \in \hat{\mathbb{G}}^2$ and $\vec{u}_2 = (\vec{u}_1)^{\rho_u} = (\hat{g}^{\rho_u}, \hat{h}^{\rho_u}) \in \hat{\mathbb{G}}^2$.
8. $\mathsf{PP}_{TC} = (\mathsf{PP}, g_1, \hat{g}, \ell = 6)$.
9. Generate the commitment key $\vec{\mathsf{ck}} \in \hat{\mathbb{G}}^8$ and $\vec{\mathsf{tk}} \in \mathbb{Z}_p^8$.
10. Generate a pair of Groth-Sahai commitment parameters(PP_{GS}).
11. $\mathsf{SK} = (x_1, x_2)$
12. $\mathsf{PK} = (g_1, g_2, \vec{u}_1, \vec{u}_2, X, \mathsf{PP}_{TC}, \vec{\mathsf{ck}}, \mathsf{PP}_{GS})$

***RCCA*3.Enc(M, PK)** :

1. Generate the LHSPS signature keys $(\mathsf{SSK}, \mathsf{SVK}) \leftarrow LHSPS.\mathsf{KeyGen}(\mathsf{PP})$ with $\mathsf{SSK} = (\{\chi_i, \gamma_i\}_{i=1}^5) \in \mathbb{Z}_p^{10}$ and $\mathsf{SVK} = (\{\mathsf{SVK}_i\}_{i=1}^5) = (\{\hat{g}_i\}_{i=1}^5) \in \hat{\mathbb{G}}^5$.
2. Choose $\theta \xleftarrow{R} \mathbb{Z}_p$ and compute

$$C_0 = M \cdot X^\theta, \qquad C_1 = g_1^\theta, \qquad C_2 = g_2^\theta.$$

3. Generate commitment and open of the verification key SVK,

$$(\mathsf{com}, \mathsf{open}) \leftarrow TC.\mathsf{Commit}(\mathsf{PP}_{TC}, \vec{ck}, \mathsf{SVK}) \in \hat{\mathbb{G}} \times (\mathbb{G}^9 \times \hat{\mathbb{G}}^2)$$

4. Construct the proof vector $\vec{u}_{\mathsf{com}} = \vec{u}_2 \cdot (1, \mathsf{com})$.
5. Generate $r \xleftarrow{R} \mathbb{Z}_p$. Compute $\vec{C}_\theta = \vec{u}_{\mathsf{com}}^\theta \cdot (\vec{u}_1)^r$.
6. Using $\vec{C}_\theta$ to get two GS proofs $\vec{\pi}$ of

$$C_1 = g_1^\theta \qquad C_2 = g_2^\theta$$

7. Generate the commitment $\vec{C}_{\mathsf{SVK}}, \vec{C}_{\mathsf{com}}, \vec{C}_{\mathsf{open}}$ of $\mathsf{SVK}, \mathsf{com}, \mathsf{open}$ with respect to PP_{GS}.
8. Generate the proof $(\vec{\pi}_{\mathsf{com}}, \vec{\pi}_{proof})$ of the following equations:

   $$TC.\mathsf{Verify}(\mathsf{ck}, \mathsf{com}, \mathsf{SVK}, \mathsf{open}) = \mathsf{True} \quad GS.\mathsf{Verify}(\vec{\pi}, \{\vec{C}_{theta}\}, \{\vec{u_1}, \vec{u_2} \cdot (1, \mathsf{com})\}) = \mathsf{True}$$

   More explicitly, We parse open as $(D, g_z, g_1, \ldots, g_5, \mathsf{ovk}_{POS}, \hat{Z}, \hat{R}) \in \mathbb{G}^8 \times \hat{\mathbb{G}}^2$, then we have $\vec{C}_{\mathsf{open}} \in \mathbb{G}^{16} \cdot \hat{\mathbb{G}}^4$, then we proof the following equations:

   $$e(g, \hat{C}) = e(D, \hat{g}) \prod_{i=1}^{5} e(\mathsf{SVK}_i, \hat{X}_i) \cdot e(g_z, \hat{X}_6) \cdot e(\mathsf{ovk}_{POS}, \hat{X}_7) \quad e(\mathsf{ovk}_{POS}, \hat{g}) = e(g_z, \hat{Z}) \cdot e(g, \hat{R}) \cdot \prod_{i=1}^{\ell} e(g_i, \mathsf{S}$$

   Then we have $\pi_{\mathsf{com}} \in \mathbb{G}^2 \times \hat{G}^2$.
   We Parse $\vec{\pi}$ with (π_1, π_2), the we generate the GS proof for the following equations:

   $$E(g_1, \vec{C}_\theta) = E(C_1, \vec{u}_2) \cdot E(C_1, (1, \mathsf{com})) \cdot E(\pi_1, \vec{u}_1)$$
   $$E(g_2, \vec{C}_\theta) = E(C_2, \vec{u}_2) \cdot E(C_2, (1, \mathsf{com})) \cdot E(\pi_2, \vec{u}_1)$$

   Thus we have $\vec{\pi}_{proof} \in \mathbb{G}^4$.
9. Output the ciphertext

   $$\vec{C} = (C_0, C_1, C_2, \vec{C}_\theta, \vec{\pi}, \vec{\sigma}, \vec{\sigma_{r_1}}, \vec{\sigma_{r_2}}, \vec{C}_{\mathsf{SVK}}, \vec{C}_{\mathsf{com}}, \vec{C}_{\mathsf{open}}, \vec{\pi}_{\mathsf{com}}, \vec{\pi}_{proof}) \in \mathbb{G}^{42} \times \hat{\mathbb{G}}^{23}$$

   in which $\vec{\sigma} = LSHSPS.\mathsf{Sign}(\mathsf{SSK}, (C_0, C_1, C_2, \vec{\pi})) \in \mathbb{G}^2$, $\vec{\sigma_r} = LHSPS.\mathsf{Sign}(\mathsf{SSK}, (X, g_1, g_2, 1, 1))$ and $\vec{\sigma_r} = LHSPS.\mathsf{Sign}(\mathsf{SSK}, (1, 1, 1, g_1, g_2))$. Notice that we don't sign the commitments because in the Groth-Sahai proof system and in this very special case, there is only one valid commitment for given proofs.

***RCCA*3.Dec($\mathsf{PK}, \vec{C}, \mathsf{SK}$)** :

1. Parse PK with $(\vec{g}_1, \vec{g}_2, X, \mathsf{PP}_{TC}, \mathsf{ck})$ and SK with (x_1, x_2).
2. Parse $\vec{C}$ with $(\mathsf{SVK}, \mathsf{com}, \mathsf{open}, C_0, C_1, C_2, \vec{C}_\theta, \vec{\pi}, \vec{\sigma})$.
3. Verify the signature is valid $LHSPS.\mathsf{Verify}(\mathsf{PP}, (C_0, C_1, C_2, \vec{\pi}), \sigma) = \mathsf{True}$.
4. Using the commitment verification algorithm to verify that $TC.\mathsf{Verify}(\mathsf{ck}, \mathsf{com}, \mathsf{SVK}, \mathsf{open}) = \mathsf{True}$
5. Verify that $\vec{\pi}$ is a valid Groth-Sahai proof w.r.t. $(C_1, C_2, \vec{C}_\theta, \mathsf{com})$.
6. If any of the verification fails then halt and return $\perp$, otherwise, output $C_0/(C_1^{x_1} \cdot C_2^{x_2})$.

References

[1] David Cash, Eike Kiltz, and Victor Shoup. "The Twin Diffie-Hellman Problem and Applications". In: *J. Cryptology* 22.4 (2009), pp. 470–504. DOI: 10.1007/s00145-009-9041-6. URL: http://dx.doi.org/10.1007/s00145-009-9041-6.

[2] Melissa Chase et al. “Malleable Proof Systems and Applications”. In: *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*. Ed. by David Pointcheval and Thomas Johansson. Vol. 7237. Lecture Notes in Computer Science. Springer, 2012, pp. 281–300. ISBN: 978-3-642-29010-7. DOI: 10.1007/978-3-642-29011-4_18. URL: http://dx.doi.org/10.1007/978-3-642-29011-4_18.

[3] Véronique Cortier, Georg Fuchsbauer, and David Galindo. *BeleniosRF: A Strongly Receipt-Free Electronic Voting Scheme*. Cryptology ePrint Archive, Report 2015/629. http://eprint.iacr.org/2015/629. 2015.

[4] Yevgeniy Dodis, Ilya Mironov, and Noah Stephens-Davidowitz. “Message Transmission with Reverse Firewalls - Secure Communication on Corrupted Machines”. In: *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*. Ed. by Matthew Robshaw and Jonathan Katz. Vol. 9814. Lecture Notes in Computer Science. Springer, 2016, pp. 341–372. ISBN: 978-3-662-53017-7. DOI: 10.1007/978-3-662-53018-4_13. URL: http://dx.doi.org/10.1007/978-3-662-53018-4_13.

[5] C. Shannon. “Communication Theory of Secrecy Systems”. In: *Bell System Technical Journal, Vol 28, pp. 656–715* (1949).