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 [8], we begin to formally define the properties we wanted for the cryptographic protocols and prove 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 rerandomizable. This property can be formally defined as resistant to Replayable Chosen-Ciphertext Attack(RCCA). Some work on construct more complex cryptographic system like mix network proposed by Golle *el. al.* [4] RCCA encryption scheme are required in such schemes. However, the previous constructions [4] are suffered from the Chosen-Chipertext attack or based on some non standard assumptions [7] or not very efficient [3]. The aim of my internship is to construct and prove efficient encryption scheme which are suitable for the above schemes. The one of 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 based on the standard assumptions in the practical point of view.

Proposed Contributions

The contributions of my internship are the following: We first give an efficient instantiation of the general controlled-malleable encryption scheme proposed by [3] which ciphertext has $93\mathbb{G}$ elements.

Then we use another approach to get a very efficient computational RCCA encryption in which the the ciphertext size is only $39\mathbb{G} + 20\hat{\mathbb{G}}$ elements. As a sub-result, we also have constructed a public verifiable structure-preserving CCA encryption which is more efficient than the existing construction $16\mathbb{G} + 11\hat{\mathbb{G}}$ against $321\mathbb{G}$ [2].

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 RCCA scheme, the re-randomization is computational. A natural open question is can we have RCCA scheme which rerandomization which is statistical unlinkable.

2 Preliminaries

In this section, we 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 the rest of this work, a negligible function $\varepsilon(\lambda)$ is a positive function which is asymptoticaly smaller than $2^{-\lambda}$.

In cryptography, one of the most studied assumption is Diffie-Hellman assumption. In this work, we consider a slightly stronger variant of DDH assumption Symmetric external Diffie-Hellman(SXDH).

Definition 1. *Decisional Diffie-Hellman(DDH) For a security parameter λ, we say a group $\mathbb{G}$ of prime order $p > 2^\lambda$ verifies the Diffie-Hellman assumption, if given a group generator $g \in \mathbb{G}$ and two triples of group elements (g^a, g^b, g^{ab}) and (g^a, g^b, g^c) in which (a, b, c) are random values generated randomly $(a, b, c) \leftarrow \mathbb{Z}_p^3$, we define the advantage of an adversary $\mathcal{A}$ against the DDH problem by:*

$$adv(\mathcal{A}) = |\Pr(\mathcal{A}(g, g^a, g^b, g^{ab}) = 1) = \Pr(\mathcal{A}(g, g^a, g^b, g^c) = 1)| < \varepsilon(\lambda).$$

where $\varepsilon(\lambda)$ is a negligible function of the security parameter λ.

Definition 2. *Symmetric external Diffie-Hellman(SXDH) For a security parameter λ and for a asymmetric pairing group setting, three groups of prime order $p > 2^\lambda$: $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$ and the pairing $e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T$. If there is no adversary with non-negligible advantage against the DDH problem both on the group $\mathbb{G}$ and $\hat{\mathbb{G}}$, then we say that the group triple $(\mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T)$ verifies the SXDH assumption.*

We also introduce Double Pairing assumption which can be applied by the SXDH assumption

Definition 3. *Double Pairing(DP) Given a asymmetric pairing setting $(\mathbb{G}, \hat{G}, \mathbb{G}_T, e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T)$. Given two random non-zero generators $(g_z, g_r) \in \mathbb{G}$,*

$$\Pr[(z, r) \leftarrow \mathcal{A} | (z, r) \in \hat{\mathbb{G}}^2 \wedge e(g_z, z) \cdot e(g_r, r) = 1] \in negl(\lambda)$$

For the simplicity of the description of the algorithm, we also use symmetric pairing setting, in which the DDH and SXDH assumption are not verified, we introduce the DLIN assumption

Definition 4. *Decisional Linear(DLIN) For a security parameter λ, we say a group $\mathbb{G}$ of prime order $p > 2^\lambda$ verifies the Decisional Linear assumption, if given three group generators $(f, g, h) \in \mathbb{G}^3$ and two triples of group elements (f^a, g^b, h^{a+b}) and (f^a, g^b, h^c) in which (a, b, c) are random values generated randomly $(a, b, c) \leftarrow \mathbb{Z}_p^3$, we define the advantage of an adversary $\mathcal{A}$ against the DLIN problem by:*

$$adv(\mathcal{A}) = |\Pr(\mathcal{A}(f, g, h, f^a, g^b, h^{a+b}) = 1) = \Pr(\mathcal{A}(f, g, h, f^a, g^b, h^c) = 1)| < \varepsilon(\lambda).$$

where $\varepsilon(\lambda)$ is a negligible function of the security parameter λ.

2.2 Building Blocks

Definition 5. *Linearly Homomorphic Structure Preserving Signature based on SXDH assumption [5]*

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

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

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

$$z = \prod_{i=1}^{k} m_i^{\hat{\chi}_i} \qquad\qquad r = \prod_{i=1}^{k} m_i^{\hat{\gamma}_i}$$

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* $\mathsf{vk} = (\hat{g}_1, \ldots, \hat{g}_k)$
2. *Verify the pairing equation:*

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

Definition 6. *A LHSPS for the message vectors of size k is strongly unforgeable if no PPT(probabilistic polynomial Turing machine) adversary has non-negligible advantage in the following game:*

Init phase: *The challenger use* Setup *and* KeyGen *to generate the public parameters* PP*, verification key* VK *and signing key*SK*. Then send* PP *and* VK *to the challenger.*

Signing queries: *The adversary has access of a signing oracle, he can require a polynomial number of messages* $\{\vec{M}_i\}_{i=1}^q$ *to sign.*

Challenge phase: *The adversary outputs a message and signature pair* $(\vec{M}^*, \sigma^*)$.

$$adv(\mathcal{A}) = \Pr[LHSPS.\mathsf{Verify}(\mathsf{VK}, \vec{M}^*, \sigma) = \mathsf{True} \wedge \vec{M}^* \notin Span(\{\vec{M}_i\}_{i=1}^q)]$$

The following theorem is proved in [6].

Theorem 1. *The previous constructed LHSPS is strongly unforgeable.*

In the construction of the structure preserving publicly verifiable encryption scheme, we also need a trapdoor commitment proposed by Abe *el. al.* [1].

***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, $\vec{M}$, open)** :

1. Parse $\vec{M}$ 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:

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

Definition 7. *Chosen-Message Target Collision Resistance This property of a Trapdoor Commitment scheme TC is defined by the winning probability of the adversary against the following security game:*

Init phase: *The challenger generate the public parmeters* $\mathsf{PP}_{TC} \leftarrow TC.\mathsf{Setup}$.

Query phase: *The adversary has oracle access of the commitment algorithm* Commit. *For each query of message m, the challenger compute* $(\mathsf{com}, \mathsf{open}) \leftarrow TC.\mathsf{Commit}(m)$. *Record them in the hash table Q. and outputs* $(\mathsf{com}, \mathsf{open})$ *to the adversary.*

Challenge phase: *The adversary outputs message-commitment triple* $(m^*, \mathsf{com}^*, \mathsf{open}^*)$.

The advantage of the adversary is defined by the following probability:

$$\Pr[(m^*, \mathsf{com}^*, \mathsf{open}^*) \leftarrow \mathcal{A} | \mathsf{com}^* \in Q \wedge (\mathsf{com}^*, m^*) \notin Q \wedge TC.\mathsf{Verify}(\vec{ck}, \mathsf{com}^*, m^*, \mathsf{open}^*) = \mathsf{True}].$$

The following theorem is proved in [1].

Theorem 2. *The previous Trapdoor Commitment scheme is Chosen-Massage Target Collision Resistant.*

2.3 Security Notions

An public key encryption scheme is a quadruple of algorithms $\mathcal{E} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$.

Definition 8. *CCA-2 The CCA-2 security of the public key encryption is defined by the wining probability of the adversary in the following game:*

Init phase *: We generate the public parameter w.r.t. the secure parameter* λ. *The Challenger use* KeyGen *algorithm to generate a pair of public key* pk *and secrect key* sk*, then give the public key to the adversary.*

Quary phase 1 *: The adversary has the oracle access to the decryption oracle, he can decrypt polynomialy many ciphertext by the decryption oracle.*

Challenge phase *: The adversary choose two message* (m_0, m_1)*, then submits them to the challenger. The challenger choose randomly a bit* $b \in \{0, 1\}$*, then encrypts the message* m_b *using the public encryption key* pk *and return the result ciphertext* c_b *to the adversary.*

Quary phase 2 *: The adversary has the oracle access to the decryption oracle expect that he can not require the oracle to decrypt the ciphertext c_b.*

Gussing phase *: The adversary output a bit b'.*

The encryption scheme $\mathcal{E}$ is CCA-2 secure iff $adv(\mathcal{A}) = |\Pr(b = b') - \frac{1}{2}| < negl(\lambda)$ where $negl(\lambda)$ is a negligible function w.r.t. λ.

We also define the Replayable-CCA encryption scheme(RCCA)

Definition 9. *RCCA The RCCA security of the public key encryption is defined by the wining probability of the adversary in the following game:*

Init phase *: We generate the public parameter w.r.t. the secure parameter λ. The Challenger use* KeyGen *algorithm to generate a pair of public key* pk *and secrect key* sk*, then give the public key to the adversary.*

Query phase 1 *: The adversary has the oracle access to the decryption oracle, he can decrypt polynomialy many ciphertext by the decryption oracle.*

Challenge phase *: The adversary choose two message (m_0, m_1), then submits them to the challenger. The challenger choose randomly a bit $b \in \{0, 1\}$, then encrypts the message m_b using the public encryption key* pk *and return the result ciphertext c_b to the adversary.*

Query phase 2 *: The adversary has the oracle access to the decryption oracle expect that when the oracle receive a ciphertext, if the result of the decryption is equal to m_0 or m_1, then the oracle returns Replay.*

Guessing phase *: The adversary output a bit b'.*

The encryption scheme $\mathcal{E}$ is CCA-2 secure iff $adv(\mathcal{A}) = |\Pr(b = b') - \frac{1}{2}| < negl(\lambda)$ where $negl(\lambda)$ is a negligible function w.r.t. λ.

We also define the unlinkability of the RCCA encryption scheme which is first proposed by Prabhakaran *el. al.* [7].

Definition 10. *Unlinkability Let RCCA encryption be the following four algorithm* (Setup, KeyGen, Enc, Dec, ReRan
The unlinkability of RCCA encrypton scheme is defined by the wining probability of the adversary in the following game:

Init phase *: We generate the public parameter w.r.t. the secure parameter λ. The Challenger use* KeyGen *algorithm to generate a pair of public key* pk *and secrect key* sk*, then give the public key to the adversary.*

Query phase 1 *: The adversary has the oracle access to the decryption oracle, he can decrypt polynomialy many ciphertext by the decryption oracle.*

Challenge phase *: The adversary choose outputs a ciphertext C, then submits it to the challenger. If $\mathsf{Dec}(C) \neq \perp$, the challenger choose randomly a bit $b \in \{0, 1\}$, Then if $b = 0$, the challenger outputs $\mathsf{Enc}(\mathsf{Dec}(C))$, otherwise he outputs $\mathsf{ReRandom}(C)$.*

Query phase 2 *: The adversary has again the oracle access to the decryption oracle, he can decrypt polynomialy many ciphertext by the decryption oracle.*

Guessing phase *: The adversary output a bit b'.*

The RCCA scheme is computational(resp. statistical) unlinkable if all PPT(resp. omnipotent) adversary has negligible advantage against the previous game.

3 Efficient instantiation of the re-randomization encryption of generic construction [3]

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

***RCCA*1.Setup(λ):** 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 $\{\chi_i, \gamma_i, \delta_i\}_{i=1}^3, \zeta, \rho, \phi \xleftarrow{R} \mathbb{Z}_p$, 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. $\mathsf{PK} = (d, \mathsf{pk}_{enc}, \mathsf{vk}_{sig}, \sigma_{crs})$.
8. $\mathsf{SK} = (x, y)$

***RCCA*1.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

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

***RCCA*1.Dec(PK, SK, $\vec{C}$)** :

1. Parse $\vec{C}$ as $(C_1, C_2, C_3), \vec{C}_H, \vec{C}_{d^b}, \vec{C}_M, \{\vec{C}_{R_1}\}_{i=1}^2, \{\vec{C}_{D_i}\}_{i=1}^3, \{\vec{C}_{S_i}\}_{i=1}^2, \{\vec{C}_{\Sigma_i}\}_{i=1}^3, \{\vec{C}_{\Delta_i}\}_{i=1}^3, \vec{C}_F, \vec{C}_G, \vec{\pi})$.
2. Parse SK as (x, y)
3. Verify that all proofs are correct.
4. If any proof fails then return $\perp$. otherwise return $C_3/(C_1 \cdot C_2)$

***RCCA*1.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 $\vec{C}' = (C'_1, C'_2, C'_3)$.

The detailed proof elements are in the appendix A. With this instantiation, the ciphertext of the RCCA encryption scheme has 93 group elements.

4 Using the trapdoor commitment scheme to construct 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
$$C_1 = g_1^\theta \qquad C_2 = g_2^\theta$$
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(PK, $\vec{C}$, 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

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

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

5 Combine Structure Perserving Public Encryption scheme with LHSPS and Groth-Sahai proof

***RCCA2*.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 $(\rho_u, \rho'_u) \xleftarrow{R} \mathbb{Z}_p^2$ 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 $\vec{u}_2 = (\vec{u}_1)^{\rho_u} = (\hat{g}^{\rho_u}, \hat{h}^{\rho'_u}) \in \hat{\mathbb{G}}^2$. Note that $\vec{u}_1$ and $\vec{u}_2$ are linearly independent with overwhelming probability.
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$(\mathsf{PP}_{GS}) = (\vec{g}_r, \vec{g}_s)$.
11. We output the public parameters $\mathsf{PP} = (g_1, g_2, \mathsf{PP}_{TC}, \vec{\mathsf{ck}}, \mathsf{PP}_{GS})$.
12. $\mathsf{SK} = (x_1, x_2)$
13. $\mathsf{PK} = (\vec{u}_1, \vec{u}_2, X)$

***RCCA2*.Enc($\mathsf{PP}, M, \mathsf{PK}$)** :

1. Generate the LHSPS signature keys $(\mathsf{SSK}, \mathsf{SVK}) \leftarrow LHSPS.\mathsf{KeyGen}(\mathsf{PP})$ with $\mathsf{SSK} = (\{\chi_i, \gamma_i\}_{i=1}^3) \in \mathbb{Z}_p^8$ and $\mathsf{SVK} = (\{\mathsf{SVK}_i\}_{i=1}^4) = (\{\hat{g}_i\}_{i=1}^4) \in \hat{\mathbb{G}}^4$.

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,

$$(\mathsf{com}, \mathsf{open}) \leftarrow TC.\mathsf{Commit}(\mathsf{PP}_{TC}, \vec{ck}, \mathsf{SVK}) \in \hat{\mathbb{G}} \times (\mathbb{G}^7 \times \hat{\mathbb{G}}^2)$$

4. Construct the proof vector $\vec{u}_{\mathsf{com}} = \vec{u}_2 \cdot (1, \mathsf{com})$.
5. 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}.
6. Generate $(r, s) \xleftarrow{R} \mathbb{Z}_p$. Compute $\vec{C}_{\theta} = \vec{u}_{\mathsf{com}}^{\theta} \cdot (\vec{u}_1)^r$ and $\vec{C}_1 = \vec{u}_{\mathsf{com}} \cdot (\vec{u}_1)^s$.
7. Note that we have the commitment of com is $\vec{C}_{\mathsf{com}} = (1, \mathsf{com}) \cdot \vec{g}_r^{r_{\mathsf{com}}} \cdot \vec{g}_s^{s_{\mathsf{com}}}$.
8. Using $\vec{C}_{\theta}$ to get two GS proofs $(\vec{\pi}_{\theta}, \vec{\pi}_1)$:

$$\begin{aligned}
\vec{\pi}_{\theta} &= (\vec{\pi}_{\theta,1}, \vec{\pi}_{\theta,2}) \\
&= ((\pi_{\theta,1,1}, \pi_{\theta,1,2}, \pi_{\theta,1,3}), (\pi_{\theta,2,1}, \pi_{\theta,2,2}, \pi_{\theta,2,3})) \\
&= ((g_1^r, C_1^{r_{\mathsf{com}}}, C_1^{s_{\mathsf{com}}}), (g_2^r, C_2^{r_{\mathsf{com}}}, C_2^{s_{\mathsf{com}}})) \\
\vec{\pi}_1 &= (\pi_{1,1,1}, \pi_{1,1,2}) \\
&= ((\pi_{1,1,1}, \pi_{1,1,2}, \pi_{1,1,3}), (\pi_{1,2,1}, \pi_{1,2,2}, \pi_{1,2,3})) \\
&= ((g_1^s, g_1^{r_{\mathsf{com}}}, g_1^{s_{\mathsf{com}}}), (g_2^s, g_2^{r_{\mathsf{com}}}, g_2^{s_{\mathsf{com}}}))
\end{aligned}$$

of

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

which verifies:

$$\begin{aligned}
E(g_1, \vec{C}_{\theta}) &= E(C_1, \vec{u}_2) \cdot E(C_1, \boxed{\vec{C}_{\mathsf{com}}}) \cdot E(\pi_{\theta,1,1}, \vec{u}_1) \cdot E(\pi_{\theta,1,2}, \vec{g}_r) \cdot E(\pi_{\theta,1,3}, \vec{g}_s) \\
E(g_2, \vec{C}_{\theta}) &= E(C_2, \vec{u}_2) \cdot E(C_2, \boxed{\vec{C}_{\mathsf{com}}}) \cdot E(\pi_{\theta,2,1}, \vec{u}_1) \cdot E(\pi_{\theta,2,2}, \vec{g}_r) \cdot E(\pi_{\theta,2,3}, \vec{g}_s) \\
E(g_1, \vec{C}_1) &= E(g_1, \vec{u}_2) \cdot E(g_1, \boxed{\vec{C}_{\mathsf{com}}}) \cdot E(\pi_{1,1,1}, \vec{u}_1) \cdot E(\pi_{1,1,2}, \vec{g}_r) \cdot E(\pi_{1,1,3}, \vec{g}_s) \\
E(g_2, \vec{C}_1) &= E(g_2, \vec{u}_2) \cdot E(g_2, \boxed{\vec{C}_{\mathsf{com}}}) \cdot E(\pi_{1,2,1}, \vec{u}_1) \cdot E(\pi_{1,2,2}, \vec{g}_r) \cdot E(\pi_{1,2,3}, \vec{g}_s)
\end{aligned}$$

9. We also compute the signature $\vec{\sigma}_1 = (z_1, r_1)$ of the vector (g, X, g_1, g_2) and the signature $\vec{\sigma}_m = (z_m, r_m)$ of the vector $(1, C_0, C_1, C_2)$.
10. Generate the proof $(\vec{\pi}_{\mathsf{com}}, \vec{\pi}_{\vec{\sigma}_1}, \vec{\pi}_{\vec{\sigma}_m})$ of the following equations:

$$\begin{aligned}
TC.\mathsf{Verify}(\mathsf{ck}, \mathsf{com}, \mathsf{SVK}, \mathsf{open}) &= \mathsf{True} \\
LHSPS.\mathsf{Verify}(\mathsf{SVK}, (g, X, g_1, g_2), \vec{\sigma}_1) &= \mathsf{True} \\
LHSPS.\mathsf{Verify}(\mathsf{SVK}, (1, C_0, C_1, C_2), \vec{\sigma}_m) &= \mathsf{True}
\end{aligned}$$

More explicitly, We parse open as $(D, g_z, g_1, g_2, g_3, g_4, \mathsf{ovk}_{POS}, \hat{Z}, \hat{R}) \in \mathbb{G}^7 \times \hat{\mathbb{G}}^2$, then we have $\vec{C}_{\mathsf{open}} \in \mathbb{G}^{14} \times \hat{\mathbb{G}}^4$, then we proof the following equations:

$$e(g, \boxed{\hat{C}}) = e(\boxed{D}, \hat{g}) \prod_{i=1}^{4} e(\boxed{\mathsf{SVK}_i}, \boxed{\hat{X}_i}) \cdot e(\boxed{g_z}, \boxed{\hat{X}_5}) \cdot e(\boxed{\mathsf{ovk}_{POS}}, \boxed{\hat{X}_6})$$

$$e(\boxed{\mathsf{ovk}_{POS}}, \hat{g}) = e(\boxed{g_z}, \boxed{\hat{Z}}) \cdot e(g, \boxed{\hat{R}}) \cdot \prod_{i=1}^{4} e(\boxed{g_i}, \boxed{\mathsf{SVK}_i})$$

Then we have $\pi_{\mathsf{com}} \in \mathbb{G}^2 \times \hat{\mathbb{G}}^2$.

11. Then we prove the following equations:

$$e(z_1, \hat{g}_z) \cdot e(r_1, \hat{g}_r) = e(g, \boxed{\mathsf{SVK}_1}) \cdot e(X, \boxed{\mathsf{SVK}_2}) \cdot e(g_0, \boxed{\mathsf{SVK}_3}) \cdot e(g_1, \boxed{\mathsf{SVK}_4}) \quad (2)$$

$$e(z_m, \hat{g}_z) \cdot e(r_m, \hat{g}_r) = e(1, \boxed{\mathsf{SVK}_1}) \cdot e(C_0, \boxed{\mathsf{SVK}_2}) \cdot e(C_1, \boxed{\mathsf{SVK}_3}) \cdot e(C_2, \boxed{\mathsf{SVK}_4}) \quad (3)$$

Thus we have $(\vec{\pi}_{\vec{\sigma}_1}, \vec{\pi}_{\vec{\sigma}_m}) \in \mathbb{G}^2 \times \mathbb{G}^2$

12. Output the ciphertext

$$\vec{C} = (C_0, C_1, C_2, \vec{C}_\theta, \vec{\pi}_\theta, \vec{\pi}_1, \vec{\sigma}_1, \vec{\sigma}_m, \vec{C}_{\mathsf{SVK}}, \vec{C}_{\mathsf{com}}, \vec{C}_1, \vec{C}_{\mathsf{open}}, \vec{\pi}_{\mathsf{com}}, \vec{\pi}_{\vec{\sigma}_1}, \vec{\pi}_{\vec{\sigma}_m}, \vec{\pi}_\theta) \in \mathbb{G}^{39} \times \hat{\mathbb{G}}^{20}$$

***RCCA2*.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 $\vec{C} = (C_0, C_1, C_2, \vec{C}_\theta, \vec{\pi}, \vec{\sigma}_1, \vec{\sigma}_m, \vec{C}_{\mathsf{SVK}}, \vec{C}_{\mathsf{com}}, \vec{C}_{\mathsf{open}}, \vec{\pi}_{\mathsf{com}}, \vec{\pi}_{\vec{\sigma}_1}, \vec{\pi}_{\vec{\sigma}_m})$.
3. Verify that $\vec{\pi}_{\vec{\sigma}_1}$ is a valid Groth-Sahai proof w.r.t. the commitments $(\vec{C}_{\mathsf{SVK}})$ for the equation 2.
4. Verify that $\vec{\pi}_{\vec{\sigma}_m}$ is a valid Groth-Sahai proof w.r.t. the commitments $(\vec{C}_{\mathsf{SVK}})$ for the equation 3.
5. If any of the verification fails then halt and return $\perp$, otherwise, output $C_0/(C_1^{x_1} \cdot C_2^{x_2})$.

***RCCA2*.ReRandom** :

1. We choose randomly a value $r' \xleftarrow{R} \mathbb{Z}_p$.
2. We update $\vec{C}$ by $\vec{C}' = (C_1 \cdot f^{r'}, C_2 \cdot g^{r'}, C_3 \cdot h^{r'})$.
3. Compute the new signature $\vec{\sigma}'_m = \vec{\sigma}_m \cdot \vec{\sigma}_1^{r'}$
4. Compute the new proof $\vec{\pi}'_{\vec{\sigma}_m} = \vec{\pi}_{\vec{\sigma}_m} \cdot \vec{\pi}_{\vec{\sigma}_1}^{r'}$
5. Update the commitment $\vec{C}'_\theta = \vec{C}_\theta \cdot \vec{C}_1^{r'}$. We also update the proof $\vec{\pi}'_\theta = \vec{\pi}_\theta \cdot \vec{\pi}_1^{r'}$.
6. Then we randomize all the commitments and GS proofs.

Theorem 4. *$RCCA2$ scheme is secure against RCCA security under SXDH assumption.*

Proof. This will be a game based proof. From the first game which is the definition of the RCCA security game to the last game, in which the adversary can trivially not have any advantage. In the i-th game, we define the advantage of the adversary by S_i.

Game 0 **:** This is the real game, the adversary is against the RCCA security game. We give the adversary the public key PK of the encryption scheme which contains the proof vectors $(\vec{u}_1, \vec{u}_2)$ which verifies:

$$\vec{u}_1 = (\hat{g}, \hat{h}) \in \hat{\mathbb{G}}^2$$
$$\vec{u}_2 = (\hat{g}^{\rho_u}, \hat{h}^{\rho'_u}) \in \hat{\mathbb{G}}^2$$

The adversary has the access to the decryption oracle.

Then during the challenge phase, the adversary choose two messages $(m_0, m_1) \in \mathbb{G}^2$ submits to the Challenger and obtains a challenge ciphertext

$$\vec{C}^* = (C_0^*, C_1^*, C_2^*, \vec{C}_\theta^*, \vec{\pi}_\theta^*, \vec{\pi}_1^*, \vec{\sigma}_1^*, \vec{\sigma}_m^*, \vec{C}_{\mathsf{SVK}}^*, \vec{C}_{\mathsf{com}}^*, \vec{C}_1^*, \vec{C}_{\mathsf{open}}^*, \vec{\pi}_{\mathsf{com}}^*, \vec{\pi}_{\vec{\sigma}_1}^*, \vec{\pi}_{\vec{\sigma}_m}^*, \vec{\pi}_\theta^*)$$

especially we have:

$$C_0^* = m_b \cdot X^{\theta^*} \qquad C_1^* = g_1^{\theta^*} \qquad C_2^* = g_2^{\theta^*}.$$

The adversary has the access to the decryption oracle expect the ciphertext $\vec{C}$ corresponded to the ciphertext m_0 or m_1.

At the end, the adversary outputs a bit b', it's advantage against the RCCA security game is defined by the wining probability of $S_0 = |\Pr[b' = b] - \frac{1}{2}|$.

Game 1 **:** In this game, the challenger generate the signing key and verification key pair and the commitment com^* of the signature's verification key at the beginning of the game. Since this does not change the view of the adversary then we have $S_0 = S_1$.

Game 2 **:** In the KeyGen algorithm, we modify the generation of the public key. Instead of generate $(\vec{u}_1, \vec{u}_2)$ as in the Game 0, we define:

$$\vec{u}_1 = (\hat{g}, \hat{h}) \in \hat{\mathbb{G}}^2$$
$$\vec{u}_2 = (\hat{g}^{\rho_u}, \hat{h}^{\rho'_u}) \cdot (1, (\mathsf{com}^*)^{-1}) \in \hat{\mathbb{G}}^2$$

Since $\vec{u}_2$ always distributed uniformly over $\hat{\mathbb{G}}^2$, this change does not affect the view of the adversary. Thus we have $S_2 = S_1$.

Game 3 **:** In this game, we change the public parameter PP_{GS} of the underlying Groth-Sahai proof system to the perfect binding setting. Due to the witness indistinguishable property, we have $|S_3 - S_2| \leq adv_{\mathcal{B}}^{wit-IND}(\lambda)$.

Game 4 **:** In this game, we define a failure event F_4: the ciphertext submitted by the adversary to the decryption oracle during the first query phase(before the challenge phase) contains the commitment $\vec{C}_{\mathsf{com}}$ which verifies $\mathsf{com} = \mathsf{com}^*$.

If the event F_4 happens, then the experiment halts and outputs a random bit. Since com^* is chosen uniformly in the space $\hat{\mathbb{G}}$, and remains independent from the adversary's view until the challenge phase, then we have $|S_4 - S_3| \leq \Pr[F_4] \leq q_D/p$ where q_D represents the number of decryption queries before the challenge phase p is the order of the group $\hat{\mathbb{G}}$.

Game 5 **:** In this game, we modify the decryption oracle during the second query phase, let us denote the event F_5: the ciphertext submitted by the adversary to the decryption oracle during the second query phase contains the commitments $(\vec{C}_{\mathsf{com}}, \vec{C}_{\mathsf{open}})$ which verifies $\mathsf{com} = \mathsf{com}^*$ but $\mathsf{open} \neq \mathsf{open}^*$.

The experiment halts if F_5 occurs and outputs a random bit. Thus we have $|S_5 - S_4| \leq \Pr[F_5]$.

And if F_5 occurs, we can easily construct an adversary $\mathcal{B}$ of the target collision-resistance of the underlying structure-preserving trapdoor commitment TC which contradicts the Double Pairing assumption.

Thus we have $|S_5 - S_4| \leq \Pr[F_2] \leq adv_{\mathcal{B}}^{TCR-CR}(\lambda) \leq adv_{\mathcal{B}}^{DP}(\lambda)$.

Game 6 **:** We modify again the decryption oracle during the second query phase. During the second query phase, the ciphertext submitted by the adversary contains $(\vec{C}_{\mathsf{com}}, \vec{C}_{\mathsf{open}})$ such that $\mathsf{com} = \mathsf{com}^*$ and $\mathsf{open} = \mathsf{open}^*$ but (C_0, C_1, C_2) does not verify that $(C_0/C_0^*, C_1/C_1^*, C_2/C_2^*) \in Span((X, g_1, g_2))$ and pass all other verification, we denote this event F_6. If F_6 occurs, the experiment halts and outputs a random bit. Thus we have $|S_6 - S_5| \leq \Pr[F_6]$. The event F_6 is contradict the strong unforgeability of the underlying LHSPS signature(The GS proof is in the perfect binding setting, if F_6 occurs, we can extract a signature which is not in the subspace $Span((g, C_0, C_1, C_2), (a, X, g_1, g_2)))$. Thus we have $|S_6 - S_5| \leq adv_{\mathcal{B}}^{SUF-OTLHS}(\lambda) \leq adv_{\mathcal{B}}^{DP}(\lambda)$.

Game 7 **:** In this game, we modify the distribution of the public keys. We compute the public keys $(\vec{u}_1, \vec{u}_2)$ in the following way:

$$\vec{u}_1 = (\hat{g}, \hat{h}) \in \hat{\mathbb{G}}^2$$
$$\vec{u}_1 = (\hat{g}^{\rho_u}, \hat{h}^{\rho_u}) \cdot (1, \mathsf{com}^{-1}) \in \hat{\mathbb{G}}^2$$

Since the Challenger does not use ρ_u or ρ'_u in the security game, thus an adversary who can make difference between Game 6 and Game 7, is an adversary agains the DDH assumption in $\hat{\mathbb{G}}$. Thus we have $|S_6 - S_5| \leq adv_{\mathcal{B}}^{DDH}(\lambda)$.

Game 8 **:** In this game, instead of generate the proof $(\vec{\pi}_{\theta^*,1,1}, \vec{\pi}_{\theta^*,2,1})$ using the witness θ^*, we generate a random value $r \xleftarrow{R} \mathbb{Z}_p^*$ and generate $(\vec{C}_{\theta^*}, \vec{\pi}_{\theta^*,1,1}, \vec{\pi}_{\theta^*,2,1})$ as following:

$$\vec{C}_{\theta^*} = \vec{u}_1^r \qquad \vec{\pi}_{\theta^*,1,1} = g_1^r \cdot C_1^{*-\rho_u} \qquad \vec{\pi}_{\theta^*,2,1} = g_2^r \cdot C_2^{*-\rho_u}$$

Notice that even the proof elements are generated without using the witness $\theta^* = log_{g_1}(C_1^*) = log_{g_2}(C_2^*)$. The distribution of the proof is remain the same as in the original proof. In fact, let us define $\tilde{r} = r - \rho_u \cdot \theta^*$, we have:

$$\vec{C}_{\theta}^* = \vec{u}_{\mathsf{com}}^{\theta^*} \cdot \vec{u}_1^{\tilde{r}} \qquad \vec{\pi}_{\theta^*,1,1} = g_1^{\tilde{r}} \qquad \vec{\pi}_{\theta^*,2,1} = g_2^{\tilde{r}}$$

Thus we have $S_8 = S_7$.

Game 9 **:** In this game, we modify the ciphertext generation in the challenge phase. Instead of compute the ciphertext using the public key (X, g_1, g_2), we generate it with the secret key (x_1, x_2):

$$C_1^* = g_1^{\theta^*} \qquad C_2^* = g_2^{\theta^*} \qquad C_0 = M_b \cdot C_1^{*x_1} \cdot C_2^{*x_2}$$

Since the ciphertext remains exactly the same as in the Game 8. Thus this modification does not change the view of the adversary, which means $S_9 = S_8$.

Game 10 **:** In this game, we modify again the ciphertext generation in the challenge phase. Recall that since the Game 8, we don't use anymore θ^* to generate $(\vec{C}_{\theta^*}, \vec{\pi}_{\theta^*,1,1}, \vec{\pi}_{\theta^*,2,1})$, then we generate two random values $(\theta_1, \theta_2) \xleftarrow{R} \mathbb{Z}_p^2$ and compute the ciphertext as following:

$$C_1 = g_1^{\theta_1} \qquad C_2 = g_2^{\theta_2} \qquad C_0 = m_b \cdot C_1^{x_1} \cdot C_2^{x_2}$$

As we don't use anymore θ_1 nor θ_2 in the whole game, we can easily construct a reduction from an adversary who can make difference between Game 10 and Game 9 to an adversary against the DDH assumption. Thus we have $|S_{10} - S_9| \leq adv_{\mathcal{B}}^{DDH}(\lambda)$.

Notice that in the final game, the ciphertext component is as follows:

$$C_1 = g_1^{\theta^*} \qquad C_2 = g_2^{\theta^*+\theta'} \qquad C_0 = m_b \cdot X_1^{\theta^*} \cdot g_2^{x_2 \cdot \theta'}$$

As x_2 is completely independent of the adversary's view, C_0 can be seen as a one-time pad of the message m_b. Thus the adversary does not have any information about the bit b. Then we have $S_{10} = 0$.

For summary, we have

$$\begin{aligned} adv_{\mathcal{A}}^{RCCA}(\lambda) &= S_0 \\ &\leq S_{10} + 2 \cdot adv_{\mathcal{B}}^{DDH}(\lambda) + 2 \cdot adv_{\mathcal{B}}^{DP}(\lambda) + q_D/p + adv_{\mathcal{B}}^{wit-IND}(\lambda) \\ &= 2 \cdot adv_{\mathcal{B}}^{DDH}(\lambda) + 2 \cdot adv_{\mathcal{B}}^{DP}(\lambda) + q_D/p + adv_{\mathcal{B}}^{wit-IND}(\lambda) \in negl(\lambda) \end{aligned}$$

□

6 Conclusion

During this internship, we explore many aspect of security proof of the cryptographic protocols and we have constructed and improved several existing rerandomizable encryption scheme. However, there are many questions left open. Can we construct efficient protocol for larger family of homomorphic encryption scheme.

References

[1] Masayuki Abe et al. "Fully Structure-Preserving Signatures and Shrinking Commitments". In: *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II*. Ed. by Elisabeth Oswald and Marc Fischlin. Vol. 9057. Lecture Notes in Computer Science. Springer, 2015, pp. 35–65. ISBN: 978-3-662-46802-9. DOI: 10.1007/978-3-662-46803-6_2. URL: http://dx.doi.org/10.1007/978-3-662-46803-6_2.

[2] Masayuki Abe et al. “Tagged One-Time Signatures: Tight Security and Optimal Tag Size”. In: *Public-Key Cryptography - PKC 2013 - 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, February 26 - March 1, 2013. Proceedings*. Ed. by Kaoru Kurosawa and Goichiro Hanaoka. Vol. 7778. Lecture Notes in Computer Science. Springer, 2013, pp. 312–331. ISBN: 978-3-642-36361-0. DOI: 10.1007/978-3-642-36362-7_20. URL: http://dx.doi.org/10.1007/978-3-642-36362-7_20.

[3] 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.

[4] Philippe Golle et al. “Universal Re-encryption for Mixnets”. In: *Topics in Cryptology - CT-RSA 2004, The Cryptographers’ Track at the RSA Conference 2004, San Francisco, CA, USA, February 23-27, 2004, Proceedings*. Ed. by Tatsuaki Okamoto. Vol. 2964. Lecture Notes in Computer Science. Springer, 2004, pp. 163–178. ISBN: 3-540-20996-4. DOI: 10.1007/978-3-540-24660-2_14. URL: http://dx.doi.org/10.1007/978-3-540-24660-2_14.

[5] Benoît Libert et al. “Linearly Homomorphic Structure-Preserving Signatures and Their Applications”. In: *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II*. Ed. by Ran Canetti and Juan A. Garay. Vol. 8043. Lecture Notes in Computer Science. Springer, 2013, pp. 289–307. ISBN: 978-3-642-40083-4. DOI: 10.1007/978-3-642-40084-1_17. URL: http://dx.doi.org/10.1007/978-3-642-40084-1_17.

[6] Benoît Libert et al. “Linearly homomorphic structure-preserving signatures and their applications”. In: *Des. Codes Cryptography* 77.2-3 (2015), pp. 441–477. DOI: 10.1007/s10623-015-0079-1. URL: http://dx.doi.org/10.1007/s10623-015-0079-1.

[7] Manoj Prabhakaran and Mike Rosulek. “Rerandomizable RCCA Encryption”. In: *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*. Ed. by Alfred Menezes. Vol. 4622. Lecture Notes in Computer Science. Springer, 2007, pp. 517–534. ISBN: 978-3-540-74142-8. DOI: 10.1007/978-3-540-74143-5_29. URL: http://dx.doi.org/10.1007/978-3-540-74143-5_29.

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

Appendices

A Details of the rerandomization algorithm of RCCA encryption by Chase *el. al.*[3]

A.1 Construction

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:

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

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

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

A.2 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) $\tilde{\pi}_3^{6,12} = \pi_3^{7,13} \cdot \pi_{15,3}^{\theta'_2} \cdot d^{t_{\Delta'_2}} \cdot f^{-t_{R'_2}} \cdot \beta^{-\tilde{t}_{d^b}} \cdot h_z^{-\tilde{t}_{\Sigma_1}} \cdot h_u^{-\tilde{t}_{\Sigma_3}} \cdot \prod_{i=1}^{3} h_i^{-\tilde{t}_{D_i}}$