KDM-CCA Security of the Cramer-Shoup Cryptosystem, Revisited

Jinyong Chang[1,2] and Rui Xue[1]
[1]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Minzhuang Road 89#, Beijing, China*
[2]*Department of Mathematics, Changzhi University, Changzhi, China*

Keywords: Key-dependent Message Security, CCA Security, DDH Assumption, Public Key Encryption.

Abstract: An encryption scheme is key-dependent message chosen plaintext attack (KDM-CPA) secure means that it is secure even if an adversary obtains encryptions of messages that depend on the secret key. However, there are not many schemes that are KDM-CPA secure, let alone key-dependent message chosen ciphertext attack (KDM-CCA) secure. So far, only two general constructions, due to Camenisch, Chandran, and Shoup (Eurocrypt 2009), and Hofheinz (Eurocrypt 2013), are known to be KDM-CCA secure in the standard model. Another scheme, a concrete implementation, was recently proposed by Qin, Liu and Huang (ACISP 2013), where a KDM-CCA secure scheme was obtained from the classic Cramer-Shoup (CS) cryptosystem w.r.t. a new family of functions. In this paper, we revisit the KDM-CCA security of the CS-scheme and prove that, in two-user case, the CS-scheme achieves KDM-CCA security w.r.t. richer ensembles, which covers the result of Qin et al.. In addition, we present another proof about the result in (QLH13) by extending our approach used in two-user case to n-user case, which achieves a tighter reduction to the decisional Diffie-Hellman (DDH) assumption.

1 INTRODUCTION

Secure encryption is the most basic task in cryptography, and significant works have gone into defining and attaining it. Many commonly accepted definitions for secure encryption (GM84; RS91; RALS11) assume that the plaintext messages to be encrypted cannot depend on the secret decryption keys themselves. Over the last few years, it was observed that in some situations the plaintext messages do depend on the secret keys. Such situations may arise in hard-disk encryption (BHHO08), computational soundness results in formal methods (BRS02), or specific protocols (CL01). Security in this more demanding setting was termed KDM-CPA security (BRS02).[1]

KDM-CPA security does not follow from standard security (CGH12), and there are indications that KDM-CPA security (at least in its most general form) cannot be proven using standard techniques (BHHI10). For this reason, KDM-CPA security has also received much attention in other settings, including symmetric key encryption(BPS08), identity-based encryption (GHV12).

[1]A specific notion, called circular security, was defined by Camenisch and Lysyanskaya in (CL01).

In this paper, we mainly focus on the KDM security in public key encryption (PKE) setting. Therefore, firstly, let us recall the classic definition of KDM-CPA security w.r.t. an efficiently computable function ensemble $\mathcal{F}$, proposed by Black et al. in (BRS02). In particular, an adversary is given n public keys $pk_1, \cdots, pk_n$ and can access an oracle O that upon receiving a query (i, f), where f is a function in $\mathcal{F}$, and $i \in [n]$ is an index, returns an encryption of $f(sk_1, \cdots, sk_n)$ under the public key pk_i. Then the scheme is KDM-CPA secure w.r.t. $\mathcal{F}$ if the adversary cannot distinguish between the oracle O and an oracle O' that always returns an encryption of (say) the (same length) all-zero string.

When considering an active adversary, we require a stronger form of KDM-CPA security, namely, KDM-CCA security. In short, KDM-CCA security requires the scheme is secure against an adversary who has access to an additional decryption oracle. Naturally, to avoid a trivial notion, the adversary is not allowed to submit any of those given from encryption oracle to its decryption oracle.

So far, only two general constructions, due to Camenisch et al. (CCS09) and Hofheinz (H13), are known to be KDM-CCA secure in the standard

Chang J. and Xue R..
KDM-CCA Security of the Cramer-Shoup Cryptosystem, Revisited.
DOI: 10.5220/0005048802990306
In *Proceedings of the 11th International Conference on Security and Cryptography* (SECRYPT-2014), pages 299-306
ISBN: 978-989-758-045-1

model. In particular, Camenisch et al. showed that a variation of the Naor-Yung paradigm (NY90) allows one to obtain KDM-CCA security from any KDM-CPA secure encryption scheme. In 2013, Hofheinz constructed a KDM-CCA secure scheme with compact ciphertexts w.r.t. selector functions $(f_i(sk_1,\cdots,sk_n)=sk_i)$ using a new but intricate tool named lossy algebraic filters. However, none of them are competitive with current KDM-free but CCA-secure schemes in terms of parameters and efficiency.

Temporarily putting the efficiency aside, we also observe that, up to now, the existing KDM-CCA (even KDM-CPA) secure schemes are usually limited to affine functions with some individual exceptions such as (BHHI10; BGK11). Therefore, how to achieve more KDM security beyond the affine functions has become an open problem.

Recently, in the excellent work of (QLH13), Qin et al. proved that the tailored CS-scheme is KDM-CCA secure w.r.t. a new function ensemble $\mathcal{F}$ (we call QLH-ensemble) which covers some affine functions, as well as other functions that are not contained in the affine ensemble. Morever, compared to other KDM-CCA secure proposals, Qin et al.'s scheme is the most practical and efficient one due to the efficiency of CS-scheme.

Then the following question arises naturally: *Can we find other ensembles and prove that the CS-scheme is also KDM-CCA secure w.r.t. these ensembles?*

Our Motivation and Contribution. The argument of this paper is motivated by those of (QLH13). We revisit Qin et al.'s proof, and find that they defined a specific ensemble (i.e. QLH-ensemble) and reduced the KDM-CCA security w.r.t. QLH-ensemble to the CCA security of the CS-scheme and, hence, (indirectly) to the DDH assumption. In particular, in the hybrid argument, assume that there exists a KDM-CCA adversary $\mathcal{A}$ who has the "ability" to distinguish the distributions of following ciphertexts:

$$C' = \big(\cdots, \mathrm{Enc}(pk_{i_{\ell-1}}, f_{i_{\ell-1}}), \mathrm{Enc}(pk_{i_\ell}, f_{i_\ell}), \mathrm{Enc}(pk_{i_{\ell+1}}, 0^{|f_{i_{\ell+1}}|}), \cdots\big),$$

and

$$C'' = \big(\cdots, \mathrm{Enc}(pk_{i_{\ell-1}}, f_{i_{\ell-1}}), \mathrm{Enc}(pk_{i_\ell}, 0^{|f_{i_\ell}|}), \mathrm{Enc}(pk_{i_{\ell+1}}, 0^{|f_{i_{\ell+1}}|}), \cdots\big),$$

where f_{i_j} is the jth function queried by $\mathcal{A}$. Then they constructed an adversary $\mathcal{A}'$ who implements a chosen-ciphertext attack on the CS-scheme using $\mathcal{A}$ as a subroutine. Then our idea is that whether we can directly reduce the KDM-CCA security to the DDH assumption and hence obtain KDM-CCA security w.r.t. much richer ensembles. As a result, we show that, in the two-user case, this conjecture is true.

On the other hand, in the original proof presented by Qin et al., the simulator $\mathcal{A}'$ has to embed his public key pk^* (obtained from his challenger) into the public keys $pk_1,\cdots,pk_n$ that will be given to $\mathcal{A}$. Therefore, he chooses randomly $i^* \in [n]$ and embeds pk^* into the i^*th position. He also "hopes" $\mathcal{A}$ will query the encryption of f_{i_ℓ} under the public key pk_{i^*} so that he can embed his challenge ciphertext. However, the probability of $i^* = i_\ell$ equals $1/n$. In other words, $\mathcal{A}'$ has only the probability of $1/n$ to successfully embed his challenge. This results in their reduction to DDH assumption much looser. Then, when extending the technique used in two-user case to n-user case, we also obtain a new proof of the result in (QLH13) with a tighter reduction.

2 PRELIMINARIES

2.1 Decisional Diffie-Hellman (DDH) Assumption

Let $\mathbb{G}$ be a group of prime order q and g be a random generator. We let $\mathcal{P}_{\mathrm{DDH}}$ be the distribution (g, g^x, g^y, g^{xy}) in $\mathbb{G}^4$ where x, y are uniform in $\mathbb{Z}_q$. Let $\mathcal{R}_{\mathrm{DDH}}$ be the distribution (g, g^x, g^y, g^z) in $\mathbb{G}^4$, where x, y, z are uniform in $\mathbb{Z}_q$.

Definition 1 (DDH Assumption)**.** *We say the decisional Diffie-Hellman problem is hard over group $\mathbb{G}$ if, for any probabilistic polynomial time (PPT) distinguisher $\mathcal{D}$, there exists a negligible function* $\mathrm{negl}(\lambda)$ *such that*

$$\mathrm{Adv}^{\mathrm{DDH}}_{\mathbb{G},\mathcal{D}}(\lambda) := |\Pr[r \xleftarrow{\$} \mathcal{P}_{\mathrm{DDH}} : \mathcal{D}(r)=1] - \Pr[r \xleftarrow{\$} \mathcal{R}_{\mathrm{DDH}} : \mathcal{D}(r)=1]| \le \mathrm{negl}(\lambda).$$

Remark. *Let p be a strong prime with $p = 2q+1$, where q is also a prime. If we let $\mathbb{QR}_p$ be the subgroup of quadratic residues in $\mathbb{Z}_p^*$, then it is a cyclic group with order q. It is widely believed that the DDH assumption over $\mathbb{QR}_p$ holds (CS02).*

2.2 Target Collision-Resistant (TCR) Hash Functions

A family of hash functions $\mathcal{H} = \{H : D \to R\}$ is called a TCR family, if for any PPT $\mathcal{A}$, $\mathrm{Adv}^{\mathrm{TCR}}_{\mathcal{H},\mathcal{A}}(\lambda)$ is negli-

gible, where

$$\mathrm{Adv}^{\mathrm{TCR}}_{\mathcal{H},\mathcal{A}}(\lambda) := \Pr[x \xleftarrow{\$} D, H \xleftarrow{\$} \mathcal{H}, y \leftarrow \mathcal{A}(x,H) : x \neq y \wedge H(x) = H(y)].$$

2.3 KDM-CCA Security

Now, we recall the formal definition of KDM-CCA security of a public key encryption scheme $\mathcal{PKE} = (\mathrm{Pars}, \mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ proposed by Camenisch et al. (CCS09). Let $\mathcal{K}$ be the space of secret keys of $\mathcal{PKE}$. For $n = n(\lambda)$, let $\mathcal{F} = \{f : \mathcal{K}^n \to \mathcal{M}\}$ be a set of functions. We define the following experiment between a challenger and an adversary $\mathcal{A}$.

$\mathrm{Exp}^{\text{KDM-CCA}}_{\mathcal{PKE},\mathcal{A}}(\lambda, b)$:

1. **Initialization Phase:** The challenger runs $\mathrm{Pars}(1^\lambda)$ to generate a public parameter pp and then runs $\mathrm{Gen}(pp)$ n times to generate n key-pairs (pk_i, sk_i), $i \in [n]$. It sends pp and the public keys pk_i, $i \in [n]$ to $\mathcal{A}$. The challenger also initializes a list $\mathrm{CL} := \emptyset$ to an empty list.
2. **Query Phase:** $\mathcal{A}$ may adaptively query the challenger for two types of operations.
   - **Encryption Queries:** The adversary selects $(i, f) \in [n] \times \mathcal{F}$ and submits it to the challenger. The challenger computes $c = \mathrm{Enc}(pp, pk_i, m)$, where m depends on the value of b. If $b = 0$, then $m = 0^{|f(sk_1, \cdots, sk_n)|}$, else $m = f(sk_1, \cdots, sk_n)$. Then it appends (i, c) to CL. Finally, the challenger sends c to the adversary.
   - **Decryption Queries:** The adversary submits a ciphertext c together with an index $i \in [n]$ to the challenger. If $(i, c) \in \mathrm{CL}$, the challenger returns $\perp$; otherwise returns the output of $\mathrm{Dec}(pp, sk_i, c)$.
3. **Guess Phase:** The adversary outputs a bit $b' \in \{0,1\}$. Then the experiment also outputs b'.

Definition 2 (KDM-CCA)**.** *A public key encryption scheme $\mathcal{PKE}$ is* KDM-CCA *secure w.r.t. $\mathcal{F}$ if for any PPT adversary $\mathcal{A}$, the advantage*

$$\mathrm{Adv}^{\text{KDM-CCA}}_{\mathcal{PKE},\mathcal{A}}(\lambda) := \left|\Pr[\mathrm{Exp}^{\text{KDM-CCA}}_{\mathcal{PKE},\mathcal{A}}(\lambda, 0) = 1] - \Pr[\mathrm{Exp}^{\text{KDM-CCA}}_{\mathcal{PKE},\mathcal{A}}(\lambda, 1) = 1]\right|$$

is negligible.

2.4 New Function Ensembles

In this subsection, we propose a series of function ensembles which will be used for the KDM-CCA security of the CS-scheme in later sections. Let q be a prime. Let S be a finite set contained in $\mathbb{Z}_q^6$ which, in fact, will be corresponding to the secret key space of CS-scheme. For any *nonzero* elements a_1, a_2, a_3 in $\mathbb{Z}_q$, we define an ensemble $\mathcal{F}^{q,n}_{a_1,a_2,a_3}$ over S^n. Formally, let $sk_i = (x_{i1}, x_{i2}, y_{i1}, y_{i2}, z_{i1}, z_{i2}) \in S$, for $1 \leq i \leq n$. Each function $f \in \mathcal{F}^{q,n}_{a_1,a_2,a_3}$ can be expressed as

$$f(sk_1, \cdots, sk_n) = \sum_{t_1,t_2,t_3} \alpha_{t_1,t_2,t_3} \prod_{i>j, i,j \in [n], s_1,s_2,s_3 \in \{1,2\}} [(x_{i,s_1} + a_1 x_{j,s_1})^{b_{i,j,t_1}} \cdot (y_{i,s_2} + a_2 y_{j,s_2})^{b_{i,j,t_2}} \cdot (z_{i,s_3} + a_3 z_{j,s_3})^{b_{i,j,t_3}}] \pmod q,$$

where $\alpha_{t_1,t_2,t_3} \in \mathbb{Z}_q$, b_{i,j,t_1}, b_{i,j,t_2} and $b_{i,j,t_3} \in \mathbb{N}$.

Now, we present two special cases in order to illustrate that our new function ensembles are properly larger.

Case 1: For $k \in \{1,2\}$, the functions $x_{2k} + a_1 x_{1k}, x_{3k} + a_1 x_{2k}, \cdots, x_{nk} + a_1 x_{n-1,k}$, (similarly, $y_{2k} + a_2 y_{1k}, y_{3k} + a_2 y_{2k}, \cdots, y_{nk} + a_2 y_{n-1,k}$, $z_{2k} + a_3 z_{1k}, z_{3k} + a_3 z_{2k}, \cdots, z_{nk} + a_3 z_{n-1,k}$) are all contained in $\mathcal{F}^{n,q}_{a_1,a_2,a_3}$.

It is clear that a PKE achieving KDM security w.r.t. this ensemble has the so-called "all-or-nothing" sharing property. Thus, it can also be used to discourage delegation of credentials in an anonymous credential system proposed by Camenisch and Lysyanskaya in (CL01).

On the other hand, if $a_1 = a_2 = a_3 = -1$, then the ensemble $F^{n,q}_{-1,-1,-1}$ essentially equals to the QLH-ensemble (see Appendix). Therefore, our following result, which states that the "tailored" Cramer-Shoup scheme is KDM-CCA secure w.r.t. the series of ensembles, completely covers that of (QLH13) when the number of users equals 2.

Case 2: When either the degrees b_{i,j,t_1}, b_{i,j,t_2}, or b_{i,j,t_3} is higher than 1, the new ensembles naturally contain a great many of functions that do not belong to the affine function ensemble.

3 THE TAILORED CS-SCHEME

Note that the message space of CS-scheme is $\mathbb{G}$ of order (prime) q, whereas the secret key space is $\mathbb{Z}_q^6$. Therefore, we have to tailor the traditional CS-scheme (i.e. encode the elements of $\mathbb{Z}_q$ into elements of $\mathbb{G}$). In particular, we assume that there exist an efficient injective encoding $encode : \mathbb{Z}_q \to \mathbb{G}$ and a decoding $decode : \mathbb{G} \to \mathbb{Z}_q$ such that $decode(encode(x)) = x$ for all $x \in \mathbb{Z}_q$ (CS02).

Now, we recall the tailored CS-scheme $\mathcal{TCS} = (\mathrm{Pars}, \mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ as follows (QLH13).

- **Public Parameters Generation** $\mathrm{Pars}(1^\lambda)$**:** Generate a group $\mathbb{G}$ with order q, where q is a λ-bits prime. Choose $g_1, g_2 \xleftarrow{\$} \mathbb{G}$ and $H \xleftarrow{\$} \mathcal{H}$, where $\mathcal{H}$

is a TCR family from $\mathbb{G}^3 \to \mathbb{Z}_q$. Output the public parameter $pp = (\mathbb{G}, q, g_1, g_2, H)$.

- **Key Generation** $\mathrm{Gen}(pp)$**:** Randomly choose elements $x_1, x_2, y_1, y_2, z_1, z_2$ from $\mathbb{Z}_q$ and compute $c = g_1^{x_1} g_2^{x_2}, d = g_1^{y_1} g_2^{y_2}, h = g_1^{z_1} g_2^{z_2}$. Output the public/private keys pair $(pk, sk) = \big((c,d,h),(x_1,x_2,y_1,y_2,z_1,z_2)\big)$.
- **Encryption** $\mathrm{Enc}(pp, pk, m)$**:** To encrypt a message $m \in \mathbb{Z}_q$, one chooses $r \in \mathbb{Z}_q$ at random. Then compute

$$u_1 = g_1^r, u_2 = g_2^r, e = h^r \cdot encode(m), v = c^r d^{r\alpha},$$

where $\alpha = H(u_1, u_2, e)$. Output the ciphertext $C = (u_1, u_2, e, v)$.
- **Decryption** $\mathrm{Dec}(pp, sk, C)$**:** Given a ciphertext $C = (u_1, u_2, e, v)$, one runs as follows. Compute $\alpha = H(u_1, u_2, e)$, and check whether $u_1^{x_1+y_1\alpha} u_2^{x_2+y_2\alpha} = v$. If not, output $\perp$ and halt; else, output $m = decode(e/u_1^{z_1} u_2^{z_2})$.

The correctness of the scheme can be verified easily.

About its security, we have the following theorem.

Theorem 1 ((CS02; QLH13))**.** *If $\mathcal{H}$ is a family of TCR hash functions and the DDH assumption holds in $\mathbb{QR}_p$, then the tailored CS-scheme $\mathcal{TCS}$ is CCA secure. More precisely, for any PPT adversary $\mathcal{A}$, we have*

$$\mathrm{Adv}^{\mathrm{CCA}}_{\mathcal{TCS},\mathcal{A}}(\lambda) \le 2 \cdot (\mathrm{Adv}^{\mathrm{DDH}}_{\mathbb{QR}_p,\mathcal{B}_1}(\lambda) + \mathrm{Adv}^{\mathrm{TCR}}_{\mathcal{H},\mathcal{B}_2}(\lambda) + \frac{(Q_d+4)}{q}),$$

where $\mathcal{B}_1$, $\mathcal{B}_2$ are DDH-distinguisher and TCR-adversary, respectively, and Q_d is the number of $\mathcal{A}$'s decryption queries.

4 SECURITY PROOF

4.1 KDM-CCA Security (2-User Case)

Now we turn to the KDM-CCA security of the tailored CS-scheme w.r.t. the ensembles we proposed. We will note that it is instructive to treat the two-user case. Therefore, firstly, we specially restate the ensembles $\mathcal{F}^{q,n}_{a_1,a_2,a_3}$ in two-user case (i.e. $\mathcal{F}^{q,2}_{a_1,a_2,a_3}$) in order to make our proof easy to understand. Actually, each function $f \in \mathcal{F}^{q,n}_{a_1,a_2,a_3}$ can also be considered as a multivariate polynomial with the following six arguments

$$x_{21} + a_1 x_{11}, x_{22} + a_1 x_{12}, y_{21} + a_2 y_{11}, y_{22} + a_2 y_{12}, z_{21} + a_3 z_{11}, z_{22} + a_3 z_{12}.$$

Theorem 2. *Let $n = 2$ and p be a safe prime number with $p = 2q+1$. For any nonzero elements $a_1, a_2, a_3 \in \mathbb{Z}_q$, if $\mathcal{H}$ is a family of TCR hash functions, and the DDH assumption holds in $\mathbb{QR}_p$, then the tailored CS-scheme $\mathcal{TCS}$ described in Section 3 achieves KDM-CCA security w.r.t. the ensemble $\mathcal{F}^{q,2}_{a_1,a_2,a_3}$. More precisely, for any PPT adversary $\mathcal{A}$, there exist a DDH-distinguisher $\mathcal{B}$ and a TCR-adversary $\mathcal{B}_1$, such that*

$$\mathrm{Adv}^{\text{KDM-CCA}}_{\mathcal{TCS},\mathcal{A}}(\lambda) \le Q \cdot (\mathrm{Adv}^{\mathrm{DDH}}_{\mathbb{QR}_p,\mathcal{B}}(\lambda) + \mathrm{Adv}^{\mathrm{TCR}}_{\mathcal{H},\mathcal{B}_1}(\lambda) + \frac{Q_d}{q - Q_d}),$$

assuming that $\mathcal{A}$ makes at most Q queries to the encryption oracle and Q_d queries to the decryption oracle.

Proof. Let $\mathcal{A}$ be any PPT adversary who implements a key-dependent message chosen ciphertexts attack on the tailored CS-scheme $\mathcal{TCS}$. Let Q denote the number of queries to the encryption oracle and Q_d the number of queries to the decryption oracle. We will proceed in a sequence of games, each of which is a modification of the previous one. Let X_i be the output of $\mathcal{A}$ in Game_i.

Game$_0$: This game is the KDM-CCA security experiment for $b = 0$. Therefore, we have

$$\Pr[X_0 = 1] = \Pr[\mathrm{Exp}^{\text{KDM-CCA}}_{\mathcal{TCS},\mathcal{A}}(\lambda, 0) = 1].$$

Game$_\ell$ ($\ell = 1, \cdots Q$): This game is the same as $\mathrm{Game}_{\ell-1}$ except that the challenger responds the kth encryption query (i_k, f_k) with

$$C_k = \begin{cases} \mathrm{Enc}(pp, pk_{i_k}, f_k(sk_1, sk_2)), & k = 1, 2, \cdots, \ell; \\ \mathrm{Enc}(pp, pk_{i_k}, 0^{|f_k(sk_1,sk_2)|}), & k = \ell+1, \cdots, Q. \end{cases}$$

Obviously, Game_Q is the KDM-CCA security experiment for $b = 1$ and

$$\Pr[X_Q = 1] = \Pr[\mathrm{Exp}^{\text{KDM-CCA}}_{\mathcal{TCS},\mathcal{A}}(\lambda, 1) = 1].$$

Thus,

$$\begin{aligned} \mathrm{Adv}^{\text{KDM-CCA}}_{\mathcal{TCS},\mathcal{A}}(\lambda) &= |\Pr[\mathrm{Exp}^{\text{KDM-CCA}}_{\mathcal{TCS},\mathcal{A}}(\lambda, 0) = 1] \\ &\quad - \Pr[\mathrm{Exp}^{\text{KDM-CCA}}_{\mathcal{TCS},\mathcal{A}}(\lambda, 1) = 1]| \\ &= |\Pr[X_0 = 1] - \Pr[X_Q = 1]| \\ &\le \sum_{\ell=1}^{Q} \big|\Pr[X_{\ell-1} = 1] - \Pr[X_\ell = 1]\big|. \end{aligned}$$

Next, we claim that, for any $\ell \in [Q]$, there exist two suitable adversaries $\mathcal{B}$ and $\mathcal{B}_1$, who attack on the DDH assumption and the TCR-security of $\mathcal{H}$, respectively, such that

$$\big|\Pr[X_{\ell-1} = 1] - \Pr[X_\ell = 1]\big| \le \mathrm{Adv}^{\mathrm{DDH}}_{\mathbb{QR}_p,\mathcal{B}}(\lambda) + \mathrm{Adv}^{\mathrm{TCR}}_{\mathcal{H},\mathcal{B}_1}(\lambda) + \frac{Q_d}{q - Q_d}.$$

Then we have

$$\mathrm{Adv}^{\text{KDM-CCA}}_{\mathcal{TCS},\mathcal{A}}(\lambda) \le Q \cdot \big(\mathrm{Adv}^{\text{DDH}}_{\mathbb{QR}_p,\mathcal{B}}(\lambda) + \mathrm{Adv}^{\text{TCR}}_{\mathcal{H},\mathcal{B}_1}(\lambda) + \frac{Q_d}{q-Q_d}\big).$$

Therefore, the KDM-CCA security of the tailored CS-scheme $\mathcal{TCS}$ follows.

Finally, we turn to prove the above claim. In particular, for $\ell \in [Q]$, we construct an adversary $\mathcal{B}$ who attacks on the DDH assumption over $\mathbb{G}(=\mathbb{QR}_p)$ using $\mathcal{A}$ as a subroutine.

In particular, when given $(\mathbb{G},q)$ and a tuple (g_1,g_2,u_1,u_2) coming from either the distribution $\mathcal{P}_{\text{DDH}}$ or $\mathcal{R}_{\text{DDH}}$, $\mathcal{B}$ randomly and independently chooses

$$x_{11},x_{12},y_{11},y_{12},z_{11},z_{12},x_{21},x_{22},y_{21},y_{22},z_{21},z_{22} \in \mathbb{Z}_q,$$

and computes

$$c_1 = g_1^{x_{11}} g_2^{x_{12}}, d_1 = g_1^{y_{11}} g_2^{y_{12}}, h_1 = g_1^{z_{11}} g_2^{z_{12}},$$
$$c_2 = g_1^{x_{21}} g_2^{x_{22}}, d_2 = g_1^{y_{21}} g_2^{y_{22}}, h_2 = g_1^{z_{21}} g_2^{z_{22}}.$$

Then pick $H \xleftarrow{\$} \mathcal{H}$. Give $pp = (\mathbb{G},q,g_1,g_2,H)$, $pk_1 = (c_1,d_1,h_1)$, and $pk_2 = (c_2,d_2,h_2)$ to $\mathcal{A}$. Note that $\mathcal{B}$ knows the two secret keys $sk_1 = (x_{11},x_{12},y_{11},y_{12},z_{11},z_{12})$, $sk_2 = (x_{21},x_{22},y_{21},y_{22},z_{21},z_{22})$. Therefore, he can compute all the functions f of the secret keys and answer all decryption queries from $\mathcal{A}$ as in the actual decryption algorithms.

Next, we describe how to answer encryption queries from $\mathcal{A}$. For the kth encryption queries (i_k,f_k) (without loss of generality, we assume that $i_\ell = 1$), $\mathcal{B}$ works as follows. Choose $b \xleftarrow{\$} \{0,1\}$.

- For $k \in \{1,\cdots,\ell-1\}$, compute $C_k = \mathrm{Enc}(pp, pk_{i_k}, f_k(sk_1,sk_2))$ and return it to $\mathcal{A}$.
- For $k = \ell$, compute

  $$e_\ell = u_1^{z_{11}} u_2^{z_{12}} \cdot encode(m_b),$$

  and

  $$v_\ell = u_1^{x_{11}+y_{11}\alpha_\ell} u_2^{x_{12}+y_{12}\alpha_\ell},$$

  where $\alpha_\ell = H(u_1,u_2,e_\ell)$, and

  $$m_b = \begin{cases} 0^{|f_\ell(sk_1,sk_2)|}, & \text{if } b=0; \\ f_\ell(sk_1,sk_2), & \text{if } b=1. \end{cases}$$

  Let $C_\ell = (u_1,u_2,e_\ell,v_\ell)$ and return it to $\mathcal{A}$.
- For $k \in \{\ell+1,\cdots,Q\}$, compute $C_k = \mathrm{Enc}(pp, pk_{i_k}, 0^{|f_k(sk_1,sk_2)|})$ and return it to $\mathcal{A}$.

Finally, $\mathcal{B}$ stores $(i_1,C_1),\cdots,(i_Q,C_Q)$ in the ciphertext list CL. That completes the description of $\mathcal{B}$.

Obviously, when the input (g_1,g_2,u_1,u_2) of $\mathcal{B}$ comes from $\mathcal{P}_{\text{DDH}}$, the output of the encryption oracle is a legitimate ciphertext and $\mathcal{B}$ successfully simulates $\mathrm{Game}_{\ell-1}$ (when $b=0$) or Game_ℓ (when $b=1$) for $\mathcal{A}$.

Next, we analyze $\mathcal{A}$'s view when $\mathcal{B}$'s input (g_1,g_2,u_1,u_2) comes from $\mathcal{R}_{\text{DDH}}$. Let $u_1 = g_1^{r_1}$ and $u_2 = g_2^{r_2} := g_1^{\omega r_2}$. We may assume that $r_1 \neq r_2$, since this occurs except with negligible probability. In the following, we call $(u_1',u_2',e',v') \in \mathbb{G}^4$ a *valid ciphertext* if and only if $\log_{g_1} u_1' = \log_{g_2} u_2'$. Then the fact that $\mathcal{A}$'s view is essentially independent of the bit b follows immediately from the following two claims.

Claim 1. *If the decryption oracle rejects all invalid ciphertexts during the attack, then the distribution of the hidden bit b is independent of the adversary's view.*

Proof of Claim 1. Consider the point $\mathbf{Q} = (z_{11},z_{12}) \in \mathbb{Z}_q^2$. If the decryption oracle rejects all invalid ciphertexts during the whole attack, then the adversary $\mathcal{A}$'s view consists of the public parameter $pp = (\mathbb{G},q,g_1,g_2,H)$, the public keys pk_1,pk_2, the valid ciphertexts submitted to the decryption oracle and the answers from it, and the answers from encryption oracle. In order to make our analysis clarity, we divide it into the following three phases. In short, $\mathcal{A}$ may obtain "more information" in the latter phase than the former one.

- At the beginning of the attack, the adversary's view only consists of the public parameter $pp = (\mathbb{G},q,g_1,g_2,H)$ and the public keys pk_1,pk_2. Now, $\mathcal{A}$ can learn the following equations from pk_1,pk_2:

  $$\begin{cases} z_{11} + \omega z_{12} = \log_{g_1} h_1, \\ z_{21} + \omega z_{22} = \log_{g_1} h_2, \end{cases} \quad (1)$$

  in which only one equation is related to $\mathbf{Q}$:

  $$z_{11} + \omega z_{12} = \log_{g_1} h_1. \quad (2)$$

  Therefore, $\mathbf{Q}$ is a random point on the line (2).
- Next, we consider that the adversary $\mathcal{A}$'s view consists of the valid ciphertexts submitted to the decryption oracle and the answers from it, except for pp, pk_1, and pk_2. Since the decryption oracle only answer valid ciphertexts (u_1',u_2',e',v'), $\mathcal{A}$ only obtains the following equation that is linearly dependent on (2):

  $$r' z_{11} + r' \omega z_{12} = r' \log_{g_1} h_1.$$

  Hence, $\mathbf{Q}$ remains a random point on the line (2).

- Finally, we inject the outputs $(u_{11}, u_{12}, e_1, v_1), \cdots, (u_{Q1}, u_{Q2}, e_Q, v_Q)$ of $\mathcal{B}$'s encryption answers into $\mathcal{A}$'s view, where

$$\begin{aligned} e_1 &= \varepsilon_1 \cdot encode(f_1(sk_1, sk_2)), \\ &\vdots \\ e_{\ell-1} &= \varepsilon_{\ell-1} \cdot encode(f_{\ell-1}(sk_1, sk_2)), \\ e_\ell &= \varepsilon_\ell \cdot encode(m_b), \\ e_{\ell+1} &= \varepsilon_{\ell+1} \cdot encode(0^{|f_{\ell+1}(sk_1, sk_2)|}), \\ &\vdots \\ e_Q &= \varepsilon_Q \cdot encode(0^{|f_Q(sk_1, sk_2)|}), \end{aligned}$$

for $\varepsilon_j = u_{j1}^{z_{ij}1} u_{j2}^{z_{ij}2}$, $j \in [Q]\backslash\{\ell\}$; $\varepsilon_\ell = u_1^{z11} u_2^{z12}$, and

$$m_b = \begin{cases} 0^{|f_\ell(sk_1, sk_2)|}, & \text{if } b = 0; \\ f_\ell(sk_1, sk_2), & \text{if } b = 1. \end{cases}$$

Note that the items $v_1, \cdots, v_Q$ is independent of $\mathbf{Q}$ although they have relations to the secret keys sk_1, sk_2. Therefore, $\mathcal{A}$ can obtain (at most) the following equations from $e_1, \cdots, e_Q$:

$$\begin{cases} f_1(sk_1, sk_2) := a_1, \\ \quad\vdots \\ f_Q(sk_1, sk_2) := a_Q. \end{cases} \tag{3}$$

According to the definition of the ensemble $\mathcal{F}^{q,2}_{a_1,a_2,a_3}$, we know that the adversary can learn at most the following two equations from (3):[2]

$$\begin{cases} z_{21} + a_3 z_{11} := a_{11}, \\ z_{22} + a_3 z_{12} := a_{22}. \end{cases} \tag{4}$$

Putting (1) and (4) together, $\mathcal{A}$ can distill

$$\begin{cases} z_{11} + \omega z_{12} = \log_{g_1} h_1, \\ z_{21} + \omega z_{22} = \log_{g_1} h_2, \\ z_{21} + a_3 z_{11} = a_{11}, \\ z_{22} + a_3 z_{12} = a_{22}. \end{cases} \tag{5}$$

We can easily know that the coefficient matrix of (5) equals 3.
In addition, from $\varepsilon_\ell = u_1^{z11} u_2^{z22}$, we have

$$r_1 z_{11} + \omega r_2 z_{12} = \log_{g_1} \varepsilon_\ell. \tag{6}$$

Therefore, $\mathcal{A}$ obtains a new system of equations composed by (5) and (6). Let $\mathbf{A}_1$ be the coefficient matrix of the new system. Obviously, the rank of $\mathbf{A}_1$ equals 4 since $r_1 \neq r_2$.

Hence, the conditional distribution of ε_ℓ, conditioning on everything in the adversary's view other than e_ℓ, is uniform. It follows that b is independent of the adversary's view. □

[2]We still ignore the equations including x_{ij}, y_{ij}, for $i, j \in \{1,2\}$, since they are independent of the point $\mathbf{Q}$.

Claim 2. *The decryption oracle will reject all invalid ciphertexts, except with negligible probability.*

Proof of Claim 2. Now, we analyze the distribution of $\mathbf{P}_i = (x_{i1}, x_{i2}, y_{i1}, y_{i2}) \in \mathbb{Z}_q^4$, for $i = 1, 2$, conditioned on the adversary's view. Without loss of generality, we only consider the point $\mathbf{P}_1$. As in the proof of Claim 1, at the beginning of the attack, the adversary's view consists of the public parameter $pp = (\mathbb{G}, q, g_1, g_2, H)$ and the public keys $pk_1 = (c_1, d_1, h_1)$, and $pk_2 = (c_2, d_2, h_2)$. Hence, the adversary $\mathcal{A}$ learns the following system:[3]

$$\begin{cases} x_{11} + \omega x_{12} = \log_{g_1} c_1, \\ y_{11} + \omega y_{12} = \log_{g_1} d_1, \\ x_{21} + \omega x_{22} = \log_{g_1} c_2, \\ y_{21} + \omega y_{22} = \log_{g_1} d_2. \end{cases} \tag{7}$$

After receiving the challenge ciphertexts $(u_{11}, u_{12}, e_1, v_1), \cdots, (u_{Q1}, u_{Q2}, e_Q, v_Q)$ that are encrypted under the public keys $pk_{i_1}, \cdots, pk_{i_Q}$, respectively, $\mathcal{A}$ can also get (at most) the following equations from $e_1, \cdots, e_Q$:

$$\begin{cases} f_1(sk_1, sk_2) = a_1, \\ \quad\vdots \\ f_Q(sk_1, sk_2) = a_Q. \end{cases} \tag{8}$$

Getting rid of the equations from the system (8) that are independent of $\mathbf{P}_1$, the adversary can distill (in worst case) the equations:

$$\begin{cases} x_{21} + a_1 x_{11} := a_{11}, \\ x_{22} + a_1 x_{12} := a_{12}, \\ y_{21} + a_2 y_{11} := a_{21}, \\ y_{22} + a_2 y_{12} := a_{22}. \end{cases} \tag{9}$$

In addition, he can also obtain (note that $i_\ell = 1$)

$$\begin{cases} r'_1 x_{i_1 1} + \omega r'_1 x_{i_1 2} + \alpha_1 r'_1 y_{i_1 1} + \alpha_1 \omega r'_1 y_{i_1 2} = \log_{g_1} v_1, \\ \quad\vdots \\ r'_{\ell-1} x_{i_{\ell-1} 1} + \omega r'_{\ell-1} x_{i_{\ell-1} 2} + \alpha_{\ell-1} r'_{\ell-1} y_{i_{\ell-1} 1} \\ \qquad + \alpha_{\ell-1} \omega r'_{\ell-1} y_{i_{\ell-1} 2} = \log_{g_1} v_{\ell-1}, \\ r_1 x_{11} + \omega r_2 x_{12} + \alpha_\ell r_1 y_{11} + \alpha_\ell \omega r_2 y_{12} = \log_{g_1} v_\ell, \\ r'_{\ell+1} x_{i_{\ell+1} 1} + \omega r'_{\ell+1} x_{i_{\ell+1} 2} + \alpha_{\ell+1} r'_{\ell+1} y_{i_{\ell+1} 1} \\ \qquad + \alpha_{\ell+1} \omega r'_{\ell+1} y_{i_{\ell+1} 2} = \log_{g_1} v_{\ell+1}, \\ \quad\vdots \\ r'_Q x_{i_Q 1} + \omega r'_Q x_{i_Q 2} + \alpha_Q r'_Q y_{i_Q 1} \\ \qquad + \alpha_Q \omega r'_Q y_{i_Q 2} = \log_{g_1} v_Q. \end{cases} \tag{10}$$

from $v_1, \cdots, v_Q$, in which r'_j, for $j \in [Q]\backslash\{\ell\}$, is the randomness of the jth encryption. Since the equations in (10) are linear combinations of those in (7), except for

$$r_1 x_{11} + \omega r_2 x_{12} + \alpha r_1 y_{11} + \alpha\omega r_2 y_{12} = \log_{g_1} v_\ell.$$

[3]We also ignore the equations including z_{ij}, $i, j \in \{1,2\}$ since they are independent of $\mathbf{P}_1$.

Combining all the equations listed in (7), (9), and (10) that are "useful" for $\mathcal{A}$ to fix the point $\mathbf{P}_1$, we have

$$\begin{cases} x_{11}+\omega x_{12}=\log_{g_1} c_1, \\ y_{11}+\omega y_{12}=\log_{g_1} d_1, \\ x_{21}+\omega x_{22}=\log_{g_1} c_2, \\ y_{21}+\omega y_{22}=\log_{g_1} d_2, \\ x_{21}+a_1 x_{11}:=a_{11}, \\ x_{22}+a_1 x_{12}:=a_{12}, \\ y_{21}+a_2 y_{11}:=a_{21}, \\ y_{22}+a_2 y_{12}:=a_{22}, \\ r_1 x_{11}+\omega r_2 x_{12}+\alpha r_1 y_{11}+\alpha\omega r_2 y_{12}=\log_{g_1} v_\ell. \end{cases} \tag{11}$$

It can be easily verified that the rank of coefficient matrix of (11) equals 7.

Now assume that $\mathcal{A}$ submits an *invalid* ciphertext $C^* := (u_{11}^*, u_{12}^*, e_1^*, v_1^*) \neq (u_{11}, u_{12}, e_1, v_1)$, where $u_{11}^* = g_1^{r_1^*}, u_{12}^* = g_2^{r_2^*}$, and $r_1^* \neq r_2^*$. Let $\alpha^* = H(u_{11}^*, u_{12}^*, e_1^*)$. We consider the following three cases.

- $(u_{11}^*, u_{12}^*, e_1^*) = (u_{11}, u_{12}, e_1)$. Then $\alpha = \alpha^*$. But $v_1^* \neq v_1$ implies that C^* will certainly be rejected.
- $(u_{11}^*, u_{12}^*, e_1^*) \neq (u_{11}, u_{12}, e_1)$ and $\alpha^* = \alpha$. Then a straightforward reduction to the TCR-property of H implies that this case occurs with negligible probability. That is, if we denote F be the event that $(u_{11}^*, u_{12}^*, e_1^*) \neq (u_{11}, u_{12}, e_1)$ and $\alpha^* = \alpha$, then we can easily construct an adversary $\mathcal{B}_1$ satisfying
$$\Pr[F] \leq \mathrm{Adv}^{\mathrm{TCR}}_{\mathcal{H},\mathcal{B}_1}(\lambda).$$
- $(u_{11}^*, u_{12}^*, e_1^*) \neq (u_{11}, u_{12}, e_1)$ and $\alpha^* \neq \alpha$. In this case, the decryption oracle will reject unless $u_{11}^{* x_{11}+y_{11}\alpha^*} u_{12}^{* x_{12}+y_{12}\alpha^*} = v_1^*$, i.e.
$$r_1^* x_{11} + \omega r_2^* x_{12} + \alpha^* r_1^* y_{11} + \alpha^* \omega r_2^* y_{12} = \log_{g_1} v_1^*. \tag{12}$$
Then the coefficient matrix of the new system formed by adding this equation into the system (11) has rank of 8. Therefore, different values of v_1^* give different solutions for $(x_{11}, x_{12}, y_{11}, y_{12})$. It follows that the adversary guesses $(x_{11}, x_{12}, y_{11}, y_{12})$ correctly with probability at most $1/q$. Hence, the first invalid ciphertext C^* is accepted with probability at most $1/q$. Similarly, the ith invalid ciphertext is accepted with probability at most $1/(q-i+1) \leq 1/(q-Q_d)$, where Q_d is the total number of decryption queries. By the union bound, we know that the decryption oracle rejects the ciphertext C^*, except with (at most) negligible probability $Q_d/(q-Q_d)$.

□

Combining the conclusions of Claim 1 with that of Claim 2 completes the proof of the theorem. □

4.2 KDM-CCA Security with a Tighter Reduction (n-User Case)

In this subsection, we present a new proof of Qin et al.'s result in (QLH13), which has the benefit that our new proof achieves a tighter reduction to the DDH assumption than that of (QLH13). From a technology perspective, we simply and straightly reduce the KDM-CCA security of $\mathcal{TCS}$ to the DDH assumption, using a similar analysis as in Theorem 2, instead of Qin et al.'s approach that reduce the KDM security to CCA security of the CS-scheme. Formally, we have

Theorem 3. *Let p be a safe prime number with $p = 2q+1$ and n be a polynomial of λ. If $\mathcal{H}$ is a family of TCR hash functions, and the DDH assumption holds in $\mathbb{QR}_p$, then the tailored CS-scheme $\mathcal{TCS}$ described in Section 3 achieves KDM-CCA security w.r.t. the QLH-ensemble (i.e. $\mathcal{F}^{q,n}_{-1,-1,-1}$). More precisely, for any PPT adversary $\mathcal{A}$, there exist a DDH-distinguisher $\mathcal{B}$ and a TCR-adversary $\mathcal{B}_1$, such that*

$$\mathrm{Adv}^{\text{KDM-CCA}}_{\mathcal{TCS},\mathcal{A}}(\lambda) \leq Q \cdot \big(\mathrm{Adv}^{\mathrm{DDH}}_{\mathbb{QR}_p,\mathcal{B}}(\lambda) + \mathrm{Adv}^{\mathrm{TCR}}_{\mathcal{H},\mathcal{B}_1}(\lambda) + \frac{Q_d}{q-Q_d}\big),$$

assuming that $\mathcal{A}$ makes at most Q queries to the encryption oracle and Q_d queries to the decryption oracle.

Since the main idea is completely analogous to that of Theorem 2, we omit it here.

5 CONCLUSIONS

In this paper, we introduced a series of new function ensembles and, in the two-user case, proved that the tailored CS-scheme achieves the KDM-CCA security w.r.t. the ensembles, which completely covers the result in (QLH13). As Qin et al. said in (QLH13), though the new function ensembles do not cover all the affine functions, it suffices for some applications like the anonymous credential systems. Moreover, in n-user case, we also give a new proof of the result in (QLH13), which achieves a tighter reduction to the DDH assumption.

ACKNOWLEDGEMENTS

The authors are grateful to anonymous reviewers for many invaluable comments and suggestions. This work is supported by National Natural Science Foundation of China (No.61170280), the Strategic Priority

Research Program of Chinese Academy of Sciences (No.XDA06010701), and the Foundation of Institute of Information Engineering for Cryptography.

REFERENCES

Backes, M., Pfitzmann, B., Scedrov, A. (2008). Key-dependent message security under active attacks - BRSIM/UC-soundness of dolev-yao-style encryption with key cycles. *Journal of Computer Security*. Vol. 16(5), pp. 497-530.

Barak, B., Haitner, I., Hofheinz, D., Ishai, Y. (2010). Bounded key-dependent message security. In *EUROCRYPT'10*. LNCS, vol. 6110, pp. 423-444. Springer, Heidelberg.

Black, J., Rogaway, P., Shrimpton, T. (2002). Encryption-scheme security in the presence of key-dependent messages. In *SAC'02*. LNCS, vol. 2595, pp. 62-75. Springer, Heidelberg.

Boneh, D., Halevi, S., Hamburg, M., Ostrovsky, R. (2008). Circular-secure encryption from decision Diffie-Hellman. In *CRYPTO'08*. LNCS, vol. 5157, pp. 108-125. Springer, Heidelberg.

Brakerski, Z., Goldwasser, S., Kalai, Y.T. (2011). Black-box circular-secure encryption beyond affine functions. In *TCC'11*. LNCS, vol. 6597, pp. 201-218. Springer, Heidelberg.

Camenisch, J., Chandran, N., Shoup, V. (2009). A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks. In *EUROCRYPT'09*. LNCS, vol. 5479, pp. 351-368. Springer, Heidelberg.

Camenisch, J., Lysyanskaya, A. (2001). An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *EUROCRYPT'01*. LNCS, vol. 2045, pp. 93-118. Springer, Heidelberg.

Cash, D., Green, M. and Hohenberger, S. (2012). New definitions and separations for circular security. In *PKC'12*. LNCS, vol. 7293, pp. 540-557. Springer, Heidelberg.

Cramer, R., Shoup, V. (2002). Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In *EUROCRYPT'02*. LNCS, vol. 2332, pp. 45-64. Springer, Heidelberg.

Galindo, D., Herranz, J., Villar, J. (2012). Identity-based encryption with master keydependent message security and leakage-resilience. In *ESORICS'12*. LNCS, vol. 7459, pp. 627-642. Springer, Heidelberg.

Goldwasser, S., Micali, S. (1984). Probabilistic encryption. *J. Comput. Syst. Science*. Vol. 28(2), pp. 270-299.

Hofheinz, D. (2013). Circular chosen-ciphertext security with compact ciphertexts. In *EUROCRYPT'13*. LNCS, vol. 7881, pp. 520-536. Springer, Heidelberg.

Naor, M., Yung, M. (1990). Public-key cryptosystems provably secure against chosen ciphertext attacks. In *STOC'90*. pp. 427-437. ACM.

Qin, B., Liu, S., Huang, Z. (2013). Key-dependent message chosen-ciphertext security of the Cramer-Shoup cryptosystem. In *ACISP'13*. LNCS, vol. 7959, pp. 136-151. Springer, Heidelberg.

Rackoff, C., Simon, D. (1992). Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *CRYPTO'91*. LNCS, vol. 576, pp. 433-444. Springer, Heidelberg.

Roman, R., Alcaraz Tello, C., Lopez, J., Sklavos, N. (2011). Key management systems for sensor networks in the context of the Internet of things. *Computers & Electrical Engineering*. Vol. 37(2), pp. 147-159.

APPENDIX (QLH-Ensemble)

Let q be a prime number and $\mathcal{X}$ be a subset of $\mathbb{Z}_q$. Then the QLH-function ensemble is a family of functions $\mathcal{F}_{q,n} := \{f : \mathcal{X}^n \to \mathbb{Z}_N\}$ and each function $f \in \mathcal{F}_{q,n}$ is defined as

$$f(x_1, \cdots, x_n) = \sum_t \alpha_t \prod_{i \neq j, i, j \in [n]} (x_i - x_j)^{a_{i,j,t}} \bmod q,$$

where $\alpha_t \in \mathbb{Z}_q$ and $a_{i,j,t} \in \mathbb{N}$.

Specific to the tailored CS-scheme, we can represent functions from the QLH-ensemble as

$$f(sk_1, \cdots, sk_n) = \sum_{t_1,t_2,t_3} \alpha_{t_1,t_2,t_3} \prod_{i>j,i,j \in [n], s_1,s_2,s_3 \in \{1,2\}} [(x_{i,s_1} - x_{j,s_1})^{b_{i,j,t_1}} \cdot (y_{i,s_1} - y_{j,s_1})^{b_{i,j,t_2}} \cdot (z_{i,s_1} - z_{j,s_1})^{b_{i,j,t_3}}] \pmod q,$$

where $sk_i = (x_{i1}, x_{i2}, y_{i1}, y_{i2}, z_{i1}, z_{i2})$ is the secret key for the ith user, $\alpha_{t_1,t_2,t_3} \in \mathbb{Z}_q$, b_{i,j,t_1}, b_{i,j,t_2} and $b_{i,j,t_3} \in \mathbb{N}$.