Novel Constructions of Cramer-Shoup Like Cryptosystems Based on Index Exchangeable Family

Jing Li
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications
Beijing 100876, P.R. China
lijingbeiyou@163.com

Licheng Wang
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications
Beijing 100876, P.R. China
wanglc@bupt.edu.cn

Zonghua Zhang
Institut Mines-Télécom/ TELECOM Lille, and CNRS UMR 5157 SAMOVAR Lab
zonghua.zhang@telecom-lille.fr

Xinxin Niu
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications
Beijing 100876, P.R. China
xxniu@bupt.edu.cn

ABSTRACT

The Cramer-Shoup cryptosystem has attracted much attention from the research community, mainly due to its efficiency in encryption/decryption, as well as the provable reductions of security against adaptively chosen ciphertext attacks in the standard model. At TCC 2005, Vasco et al. proposed a method for building Cramer-Shoup like cryptosystem over non-abelian groups and raised an open problem for finding a secure instantiation. Based on this work, we present another general framework for constructing Cramer-Shoup like cryptosystems. We firstly propose the concept of index exchangeable family (IEF) and an abstract construction of Cramer-Shoup like encryption scheme over IEF. The concrete instantiations of IEF are then derived from some reasonable hardness assumptions over abelian groups as well as non-abelian groups, respectively. These instantiations ultimately lead to simple yet efficient constructions of Cramer-Shoup like cryptosystems, including new non-abelian analogies that can be potential solutions to Vasco et al.'s open problem. Moreover, we propose a secure outsourcing method for the encryption of the non-abelian analog based on the factorization problem over non-commutative groups. The experiments clearly indicate that the computational cost of our outsourcing scheme can be significantly reduced thanks to the load sharing with cloud datacenter servers.

ASIA CCS '16, May 30-June 03, 2016, Xi'an, China

DOI: http://dx.doi.org/10.1145/2897845.2897920

Keywords

Cramer-Shoup like encryption; provable security in the standard model; index exchangeable family; non-abelian groups; outsourcing encryption

1. INTRODUCTION

The standard notion of security for public key encryption (PKE), i.e., indistinguishability against chosen ciphertext attacks (IND-CCA), was introduced in [17], where the adversary is allowed to make queries to the decryption oracle at any time, while the decryption query on the challenge ciphertext is not permitted. After then, IND-CCA secure PKE schemes based on non-interactive zero-knowledge (NIZK) proof of knowledge were proposed [6, 14], which however are inefficient in both performance and security reductions. In 1993, Zheng and Seberry gave immunizing public key cryptosystems against chosen ciphertext attacks [22, 23]. Subsequently, based on Zheng's method, Bellare and Rogaway designed IND-CCA secure PKEs in random oracle models (ROM) [3]. At CRYPTO 1998, Cramer and Shoup constructed an efficient PKE scheme that is not only provably IND-CCA secure in the standard model, but also very efficient in terms of security reductions [4]. Four years later, Cramer and Shoup [5] further proposed a general framework for building secure PKEs by using the so-called universal projective hash family which was shown implementable based on either subset membership problems or language membership problems from a general class of group theoretic perspectives.

Meanwhile, many cryptographers pay effort to the design of cryptography based on non-abelian algebraic structures, such as braid group [11], Thompson group [20], Suzuki 2-group [13, 12]. At TCC 2005, Vasco et al. presented a new approach to building Cramer-Shoup like PKEs from group theoretic perspectives, in which the concept of automorphism group system is used to construct universal pro-

jective hash families [21]. But they failed in finding a secure instantiation based on reasonable non-abelian intractability assumptions. Recently, Kahrobael and Anshel proposed a non-abelian construction of Cramer-Shoup like PKE scheme by using matrices of group ring [10]. However, we find that ciphertexts of their scheme are malleable and thus cannot resistant to adaptively chosen ciphertext attacks. Therefore, it is interesting to develop a new tool to build Cramer-Shoup like PKEs based on non-abelian groups.

We firstly define the concept of index exchangeable family (IEF) and propose IEF's security requirements for cryptographic applications. Then, based on IEF, an efficient framework for constructing Cramer-Shoup like encryption is proposed, and the IND-CCA security reduction is presented. After that, we give three concrete instantiations of IEF: the first is based on the hardness assumptions of decisional Diffie-Hellman problem over finite fields, resulting in the original Cramer-Shoup encryption scheme. The second and the third are respectively based on the hardness assumptions of decisional conjugacy problem and decisional group factorization problem over certain non-abelian groups, contributing to the potential solutions towards Vasco et al.'s open problem. Furthermore, we propose a secure outsourcing technique for the third instantiation, where the encryptor only needs to keep its transformation key that can be hidden by a random slot. The scheme significantly saves the computational cost by taking advantage of the computational resource from cloud servers.

2. PRELIMINARIES

In this section, we recall some mathematic backgrounds on computational group theory, mainly focusing on the materials that are related to our following cryptographic applications. Considering for resisting all kinds of exhaustive attacks as well as the well-known birthday attacks, the involved groups are in general assumed to be very large, say with orders no less than 2^{160} or sometimes infinite. Thus, it is impossible to enumerate all elements of the involved groups. Instead, we always specify a group G by its presentations. In particular, for a given, possibly non-abelian, group G, we use $\langle g\rangle$ denotes the cyclic subgroup of G generated by $g \in G$.

Our main concern is related to the following computational and the decisional problems over non-abelian groups:

- Conjugacy Search Problem (CSP) [11, 10, 15]: Given a non-abelian group G and two conjugate elements $g, h \in G$, the objective is to find $g_0 \in G$ such that $g_0^{-1} g g_0 = h$.
- Group Factorization Problem (GFP) [1, 8, 9]: Given a non-abelian group G and three elements $g, h, g_0 \in G$ with $gh \neq hg$, the objective is to find $g_1 \in \langle g\rangle$ and $g_2 \in \langle h\rangle$ such that $g_1 g_2 = g_0$, provided that there is at least one solution.

The corresponding computational Diffie-Hellman like versions of above problems are given below:

- Computational Diffie-Hellman Conjugacy Problem (CDH-CP): Given a non-abelian group G and a quadruple $(g, h, g_1 = h^x g h^{-x}, g_2 = h^y g h^{-y})$ for some unknown $x, y \in Z$, where $gh \neq hg$, the objective is to compute $g_3 = h^{x+y} g h^{-x-y}$.
- Computational Diffie-Hellman Factorization Problem (CDH-FP): Given a non-abelian group G and a quadruple $(g, h, g_1 = g^{x_1} h^{y_1}, g_2 = g^{x_2} h^{y_2})$ for some unknown $x_1, x_2, y_1, y_2 \in Z$, where $gh \neq hg$, the objective is to compute $g_3 = g^{x_1+x_2} h^{y_1+y_2}$.

Similarly, the corresponding decisional Diffie-Hellman like versions are given below:

- Decisional Diffie-Hellman Conjugacy Problem (DDH-CP): Given a non-abelian group G and a quintuple $(g, h, g_1 = h^x g h^{-x}, g_2 = h^y g h^{-y}, g_3 = h^z g h^{-z})$ for some unknown $x, y, z \in Z$, where $gh \neq hg$, the objective is to decide whether $g_3 = h^{x+y} g h^{-x-y}$ or not.
- Decisional Diffie-Hellman Factorization Problem (DDH-FP): Given a non-abelian group G and a quintuple $(g, h, g_1 = g^{x_1} h^{y_1}, g_2 = g^{x_2} h^{y_2}, g_3 = g^{x_3} h^{y_3})$ for some unknown $x_1, x_2, x_3, y_1, y_2, y_3 \in Z$, where $gh \neq hg$, the objective is to decide whether $g_3 = g^{x_1+x_2} h^{y_1+y_2}$ or not.

Apparently, the average hardness relationships among the above problems are

$$\text{CSP} \preceq \text{CDH-CP} \preceq \text{DDH-CSP}$$

and

$$\text{GFP} \preceq \text{CDH-FP} \preceq \text{DDH-GFP},$$

where symbol "$\preceq$" means "as least as hard as". At present, we do not know whether the CSP (resp. CDH-CP or DDH-CP) problem is harder or easier than the GFP (resp. CDH-FP or DDH-FP) problem. On one hand, from the perspective of computational group theory, there are no known efficient algorithms, except for exhaustive search, for all above problems if we regard G as a generic group[1]. On the other hand, the non-commutativity of G is necessary for maintaining the hardness of the CSP, CDH-CP and DDH-CP problems. In fact according to the analysis presented in [8, 9], we know that the non-commutativity in the above definitions plays core roles in resisting the well-known Shor's quantum algorithm attacks [19]. As for the GFP, CDH-FP and DDH-FP problems, although the underlying group G is not required to be non-abelian, the existing cryptographic constructions based on these problems also employ the so-called Sandwich transformation technique [13, 12] that is meaningless if the underlying group is abelian. Therefore, if without explicit statement, groups mentioned in this paper are in general non-abelian.

3. NEW FRAMEWORK OF CRAMER-SHOUP LIKE ENCRYPTION

3.1 Index Exchangeable Family

Definition 1. (Index Exchangeable Family, IEF) Let G be a group and $\Omega = \{\varphi_{K_i}\}$ be a collection of maps indexed by $\mathcal{K}$, where each $\varphi_{K_i}\colon G \to G$ (for $K_i \in \mathcal{K}$) maps G to itself.

[1]In a generic group model, the adversary is only given access to a randomly chosen encoding of a group, instead of efficient encodings. Up to now, the GFP is still hard for most non-abelian groups such as Suzuki 2-Groups and $GL_n(R)$, etc. The most efficient algorithm of solving GFP is subexponential for group $SL_2(F_{2^m})$ [16].

We say that Ω is an index exchangeable family (IEF) on any $g \in G$, denoted by $\Omega^{ie}_{\mathcal{K}}(g)$, if

$$\varphi_{K_i}(\varphi_{K_j}(g)) = \varphi_{K_j}(\varphi_{K_i}(g))$$

holds for $\forall K_i, K_j \in \mathcal{K}$. Furthermore,if Ω is an IEF on every $g \in G$, we call Ω an IEF over G, denoted by $\Omega^{ie}_{\mathcal{K}}(G)$.

As for cryptographic applications, we propose the following basic security requirements for the above defined IEF $\Omega^{ie}_{\mathcal{K}}(g)$: [2]

- Onewayness of map index (OMI): Given a pair $(g, \varphi_{K_i}(g)) \in G^2$, it is hard to derive $K_i \in \mathcal{K}$. (Note that this implies that $\mathcal{K}$ should be large enough; otherwise, one can easily get K_i with non-negligible probability by guessing.)

- Onewayness of map composition (OMC): Given a triple $(g, \varphi_{K_i}(g), \varphi_{K_j}(g)) \in G^3$, it is hard to compute $g_0 \in G$ such that $g_0 = \varphi_{K_i}(\varphi_{K_j}(g))$, where $K_i, K_j \in \mathcal{K}$.

- Confidentiality of map composition (CMC): Given a quadruple $(g, g_0, \varphi_{K_i}(g), \varphi_{K_j}(g)) \in G^4$, it is hard to decide whether or not $g_0 = \varphi_{K_i}(\varphi_{K_j}(g))$, where $K_i, K_j \in \mathcal{K}$.

Apparently, a Diffie-Hellman like key exchange protocol can be immediately obtained by using an $\Omega^{ie}_{\mathcal{K}}(g)$ with CMC property, in which $K_i, K_j \in \mathcal{K}$ are viewed as temporary keys of two parties and then $\varphi_{K_j}(\varphi_{K_i}(g))$ is their shared session key. One can also do this by using an $\Omega^{ie}_{\mathcal{K}}(g)$ with merely OMI property, plus a universal hash function that is used as the key deriving function. Similarly, an Elgamal like encryption scheme can also be derived based on an $\Omega^{ie}_{\mathcal{K}}(g)$ with CMC property.

3.2 Cramer-Shoup Encryption Scheme From Index Exchangeable Families

Now, let us propose a Cramer-Shoup like encryption scheme based on index exchangeable families.

Key Generation**:** Let λ be the system security parameter. Suppose that G is a finite group with order $|G| = 2^{\Theta(\lambda)}$ and $\Omega^{ie}_{\mathcal{K}}(g)$ is an associated index exchangeable family for any $g \in G$ and index set $\mathcal{K}$. Let $H : G^3 \to \mathcal{K}$ and $H_0 : G \to \{0,1\}^\lambda$ be cryptographic hash functions. Randomly choose $K_1, K_2, K_3, K_4 \in \mathcal{K}$ and compute

$$g_1 = \varphi_{K_1}(g_0),\ b = \varphi_{K_2}(g_0),\ c = \varphi_{K_3}(g_1),\ d = \varphi_{K_4}(g_1).$$

Then, the public key is $\mathbf{pk} = (G, \mathcal{K}, g_0, g_1, b, c, d, H, H_0)$ and the secret key is $\mathbf{sk} = (K_2, K_3, K_4)$.

Encryption**:** To encrypt a message $m \in \{0,1\}^\lambda$, one chooses $K_5 \in \mathcal{K}$ at random and then outputs a ciphertext as:

$$C = (u, v, e, w) = (\varphi_{K_5}(g_0),\ \ \varphi_{K_5}(g_1),$$

$$H_0(\varphi_{K_5}(b)\varphi_{K_5}(c)) \oplus m,\ \ \varphi_{K_5}(d)\varphi_\alpha(\varphi_{K_5}(b))),$$

where $\alpha = H(u, v, e) \in \mathcal{K}$.

[2]We will see that for cryptographic applications, we merely need a $\Omega^{ie}_{\mathcal{K}}(g)$ for some $g \in G$, instead of $\Omega^{ie}_{\mathcal{K}}(G)$.

Decryption**:** Upon receiving a ciphertext $C = (u, v, e, w)$, the receiver knowing the secret key $\mathbf{sk}$ at first checks whether the equation

$$w = \varphi_{K_4}(v) \cdot \varphi_\alpha(\varphi_{K_2}(u)) \quad (1)$$

holds, where $\alpha = H(u, v, e)$. If so, he/she computes the message

$$m = H_0(\varphi_{K_2}(u) \cdot \varphi_{K_3}(v)) \oplus e; \quad (2)$$

otherwise, he/she outputs $\perp$, for indicating that C is an invalid ciphertext.

Consistency. To prove the correctness of the above scheme, one only needs to notice the following equalities:

$$\begin{aligned} w &= \varphi_{K_5}(d) \cdot \varphi_\alpha(\varphi_{K_5}(b)) \\ &= \varphi_{K_5}(\varphi_{K_4}(g_1)) \cdot \varphi_\alpha(\varphi_{K_5}(\varphi_{K_2}(g_0))) \\ &= \varphi_{K_4}(\varphi_{K_5}(g_1)) \cdot \varphi_\alpha(\varphi_{K_2}(\varphi_{K_5}(g_0))) \\ &= \varphi_{K_4}(v) \cdot \varphi_\alpha(\varphi_{K_2}(u)), \\ e &= H_0(\varphi_{K_5}(b)\varphi_{K_5}(c)) \oplus m \\ &= H_0(\varphi_{K_5}(\varphi_{K_2}(g_0))\varphi_{K_5}(\varphi_{K_3}(g_1))) \oplus m \\ &= H_0(\varphi_{K_2}(\varphi_{K_5}(g_0))\varphi_{K_3}(\varphi_{K_5}(g_1))) \oplus m \\ &= H_0(\varphi_{K_2}(u)\varphi_{K_3}(v)) \oplus m. \end{aligned}$$

Remark 1. The above framework is different from the original construction in [4], especially for key generation. Actually, based on the algorithm of decryption of the Cramer-Shoup scheme, the multiplication homomorphism of exponential function is used in verification equation. However, in non-abelian algebraic structure, the functions of IEF sometimes cannot provide this homomorphism as $\varphi_{K_i}(g_1 g_2) \neq \varphi_{K_i}(g_1)\varphi_{K_i}(g_2)$. Besides, H_0 is employed for enhancing the security. Particularly, the OMI assumption is required in the security proof.

3.3 Security

The following theorems capture the security of the proposed scheme.

Theorem 1. The encryption scheme is semantic secure against adaptively chosen ciphertext attacks (IND-CCA) in the standard model, assuming that the associated index exchangeable family $\Omega^{ie}_{\mathcal{K}}(g_0)$ satisfies the property of CMC.

Proof. (Sketch of the proof.) Suppose there is an adversary $\mathcal{A}$ that can break the IND-CCA security of the above scheme with non-negligible probability. Now, let us construct a simulator $\mathcal{S}$ that can break the CMC property of the associated IEF $\Omega^{ie}_{\mathcal{K}}(g_0)$ with non-negligible probability, too.

Suppose that $\mathcal{S}$ is given the CMC challenge, i.e. a quadruple

$$(g_0,\ g_1 = \varphi_{K_1}(g_0),\ g_2 = \varphi_{K_5}(g_0),\ g_3) \in G^4,$$

and its purpose is to decide whether $g_3 = \varphi_{K_1}(\varphi_{K_5}(g_0))$ or not. The simulator will invokes $\mathcal{A}$ in executing the following IND-CCA game:

Setup**:** The simulator randomly chooses $K_2, K_3, K_4 \in \mathcal{K}$, and computes

$$b = \varphi_{K_2}(g_0),\ c = \varphi_{K_3}(g_1),\ d = \varphi_{K_4}(g_1).$$

Then, the simulator $\mathcal{S}$ sends the public key $\mathbf{pk} = (G, \mathcal{K}, g_0, g_1, b, c, d, H, H_0)$ to the adversary $\mathcal{A}$, while

keeps the secret key $\mathbf{sk} = (K_2, K_3, K_4)$ only known to himself/herself.

Phase 1**:** Now, the adversary $\mathcal{A}$ can invoke decryption queries at his/her will, and the simulator produces the response accordingly by using the secret key $\mathbf{sk}$.

Challenge**:** The adversary $\mathcal{A}$ submits two equal-length challenge messages $m_0, m_1 \in G$ to the simulator $\mathcal{S}$. Then, $\mathcal{S}$ flips a fair coin $\beta \in \{0,1\}$, and then replies $\mathcal{A}$ with the challenge ciphertext that is computed as below:

$$C^* = (u^*, v^*, e^*, w^*) = (g_2,\ g_3,$$

$$H_0(\varphi_{K_2}(g_2)\varphi_{K_3}(g_3)) \oplus m_\beta,\ \varphi_{K_4}(g_3) \cdot \varphi_{\alpha^*}(\varphi_{K_2}(g_2))),$$

where $\alpha^* = H(u^*, v^*, e^*)$.

Phase 2**:** Now, the adversary $\mathcal{A}$ will continue to invoke decryption queries at his/her will, except that the decryption query on the challenge ciphertext C^* is not allowed. In response, the simulator, by using the secret key $\mathbf{sk}$, will check the validity of the ciphertexts and then output the corresponding messages or $\perp$.

Guess**:** Finally, the adversary $\mathcal{A}$ outputs $\beta' \in \{0,1\}$ as a guess on β. Now, if $\beta' = \beta$, the simulator $\mathcal{S}$ answers his/her CMC challenge with 1 for indicating $g_3 = \varphi_{K_1}(\varphi_{K_5}(g_0))$; otherwise, $\mathcal{S}$ simply answers his/her CMC challenge at random.

Now, let us consider $\mathcal{S}$'s advantage for making correct decision on his/her CMC challenge. Apparently, if g_3 is random, then C^* is also random and gives no information about the simulator's choice of β. Thus in this case, both A and S have no any advantage in making correct decisions. On the other hand, if $g_3 = \varphi_{K_1}(\varphi_{K_5}(g_0))$, then the challenge ciphertext C^* is well formed under the public key $\mathbf{pk}$. Thus in this case, whenever the adversary $\mathcal{A}$ has non-negligible advantage in making correct guess on β, the simulator $\mathcal{S}$ has non-negligible advantage in making correct decision on his/her CMC challenge. This concludes the theorem. □

In the following theorem, we illustrate that the bit β is independent from the adversary's view.

Theorem 2. Any information of the challenged message won't be revealed in Phase 2.

Proof. Suppose the adversary invokes decryption query on the ciphertext $C = (u, v, e, w) \neq (u^*, v^*, e^*, w^*)$ after Challenge phase. We discuss by the following three cases.

Case 1: $(u, v, e) = (u^*, v^*, e^*)$.

In this case, the hash values are the same, but $w \neq w^*$ implies that the decryption query will be rejected.

Case 2: $(u, v, e) \neq (u^*, v^*, e^*)$ and $\alpha = \alpha^*$.

If this happens with non-negligible probability, then it is a contradictory for the collision-resistant property of the hash function H.

Case 3: $(u, v, e) \neq (u^*, v^*, e^*)$ and $\alpha \neq \alpha^*$.

(1) When $u = u^*$ and $v = v^*$, then $e \neq e^*$. The adversary fails to construct w such that $w = \varphi_{K_4}(v^*) \cdot \varphi_\alpha(\varphi_{K_2}(u^*))$ since $\varphi_{K_4}(v^*)$ and $\varphi_{K_2}(u^*)$ are unknown. That is, such a query will be rejected.

(2) When $u \neq u^*$ or $v \neq v^*$, baesd on the collision-resistance of H_0, $H_0(\varphi_{K_2}(u)\varphi_{K_3}(v))$ is random and independent from $H_0(\varphi_{K_2}(u^*)\varphi_{K_3}(v^*))$. In this case, even if C can pass the verification equation (1), the replied message is unrelated to the challenged message.

This concludes the theorem. □

Note that in the above reduction on the confidentiality of ciphertext, the simulator $\mathcal{S}$ is allowed to possess the secret key $\mathbf{sk}$ during his/her whole interactive process with the adversary $\mathcal{A}$. This idea is directly inherited from the original Cramer-Shoup cryptosystem [4]. Therefore, to establish the fully confidence on the security of the above scheme, we need to further show the confidential of the secret key against chosen ciphertext attacks.

Actually, after a polynomial number of queries of ciphertexts to the decryption oracle, the adversary can get the following equations about secret key K_2, K_3 from decryption algorithms:

$$\begin{cases} e_1 \oplus m_1 = H_0(\varphi_{K_2}(u_1)\varphi_{K_3}(v_1)) \\ \cdots \\ e_i \oplus m_i = H_0(\varphi_{K_2}(u_i)\varphi_{K_3}(v_i)) \end{cases}$$

Meanwhile, $\mathcal{A}$ also obtains the equations about secret key about K_2, K_3, K_4 from verification equations:

$$\begin{cases} w_1 = \varphi_{K_4}(v_1) \cdot \varphi_\alpha(\varphi_{K_2}(u_1)) \\ \cdots \\ w_i = \varphi_{K_4}(v_i) \cdot \varphi_\alpha(\varphi_{K_2}(u_i)) \end{cases}$$

Here, $u_i, v_i, e_i, w_i, m_i, \alpha$ are known to the adversary $\mathcal{A}$. Then, the security of secret key is based on the GFP and the OMI.

4. INSTANTIATIONS

In this section, we give some concrete instantiations of the so-called index exchangeable families. The corresponding schemes can be obtained based on these IEFs.

4.1 Instantiations of IEFs

- **IEF based on DDH problem.** Let $G = \langle g \rangle$ be a cyclic group with order of λ. Let us define the index-set as

  $$\mathcal{K} = \{K_i = x_i :\ x_i \in Z_\lambda\}.$$

  Meanwhile, for each $K_i \in \mathcal{K}$, the map $\varphi_{K_i} : G \to G$ is defined as

  $$\varphi_{K_i}(g) = g^{x_i}.$$

  It is easy to see that

  $$\varphi_{K_i}(\varphi_{K_j}(g)) = (g^{x_j})^{x_i} = \varphi_{K_j}(\varphi_{K_i}(g)).$$

  Thus, we indeed get an index exchangeable family $\Omega^{ie}_{\mathcal{K}}(g)$. It is a very straight observation that $\Omega^{ie}_{\mathcal{K}}(g)$ meets the property of CMC, under the intractability assumption of DDH problem over G.

- **IEF based on DDH-CP problem.** Let G be a non-abelian group. For any pair $(g, h) \in G^2$ satisfying $gh \neq hg$ and $\langle g \rangle \cap \langle h \rangle = \{1_G\}$, let us define the index-set as

  $$\mathcal{K} = \{K_i = h^{x_i} :\ x_i \in Z_\lambda\},$$

where λ is the order of the subgroup $\langle h\rangle$. Meanwhile, for each $K_i \in \mathcal{K}$, the map $\varphi_{K_i} : G \to G$ is defined as

$$\varphi_{K_i}(g) = h^{x_i} g h^{-x_i}.$$

It can be proved that

$$\varphi_{K_i}(\varphi_{K_j}(g)) = h^{(x_i+x_j)} g h^{-(x_i+x_j)} = \varphi_{K_j}(\varphi_{K_i}(g)).$$

That is, we get an index exchangeable family $\Omega^{ie}_{\mathcal{K}}(g)$, and apparently, under the intractability assumption of DDH-CP problem over G, $\Omega^{ie}_{\mathcal{K}}(g)$ satisfies the property of CMC.

- **IEF based on DDH-FP problem.** Let G be a non-abelian group. For any pair $(g, h) \in G^2$ satisfying $gh \neq hg$ and $\langle g\rangle \cap \langle h\rangle = \{1_G\}$, define the index-set as

  $$\mathcal{K} = \{K_i = (g^{x_i}, h^{y_i}) : g, h \in G, x_i \in Z_\lambda, y_i \in Z_\delta\},$$

  where λ, δ are orders of subgroups $\langle g\rangle$ and $\langle h\rangle$, respectively. Then, for each index $(g^{x_i}, h^{y_i}) \in \mathcal{K}$, let us define the map $\varphi_{K_i} : G \to G$ as

  $$\varphi_{K_i}(g_0) = g^{x_i} g_0 h^{y_i}$$

  for a fixed $g_0 \in G$. It can be proved that

  $$\varphi_{K_i}(\varphi_{K_j}(g_0)) = g^{x_i+x_j} g_0 h^{y_i+y_j} = \varphi_{K_j}(\varphi_{K_i}(g_0)).$$

That is, we get an index exchangeable family $\Omega^{ie}_{\mathcal{K}}(g_0)$. Similarly, we see that under the hard assumption of DDH-FP problem over G, $\Omega^{ie}_{\mathcal{K}}(g_0)$ satisfies the property of CMC.

Remark 2. In practice, it still works if we replace Z_λ and Z_δ with integers set Z or natural numbers set $\mathbb{N}$ directly in all above instantiations. By doing so, explicit specification on the index set $\mathcal{K}$ is no longer necessary.

4.2 Outsourcing technique based on non-abelian analog

In this section, we propose an efficient outsourcing technique for the encryption of the non-abelian analog based on the factorization problem.

Key Generation**:** Suppose that λ is the system secure parameter, G is a non-abelian group with order of $2^{\Theta(\lambda)}$, and the pair $(g, h) \in G^2$ meets the conditions $gh \neq hg$. Let $H : G^3 \to \{0,1\}^\lambda \times \{0,1\}^\lambda$ and $H_0 : G \to \{0,1\}^\lambda$ be secure cryptographic hash functions. Randomly choose 8 large [3] integers $x_i, y_i \in Z$ $(i = 1, 2, 3, 4)$ and compute

$$g_1 = g^{x_1} h^{y_1},\ b = g^{x_2} h^{y_2},\ c = g^{x_3} g_1 h^{y_3},\ d = g^{x_4} g_1 h^{y_4}.$$

Then, set the public key $\mathbf{pk} = (g, h, g_1, b, c, d, H, H_0)$ and the secret key $\mathbf{sk} = (x_2, y_2, x_3, y_3, x_4, y_4)$.

Pre − processing**:** The encryptor randomly chooses $t, \bar{t} \in \mathbb{Z}$ and computes his/her transformation key $g^t, h^{\bar{t}}$.

Encryption**:** The encryption algorithm is divided into the following steps:

Stage 1. To encrypt a message $m \in G$, the user randomly chooses two large integers $x_5, y_5 \in Z$, then computes $x_5 - t, y_5 - \bar{t}$ and sends $(g, h, x_5 - t, y_5 - \bar{t})$ as the outsourcing parameters to cloud server.

Stage 2. The cloud server returns $g^{x_5-t}, h^{y_5-\bar{t}}$ to user.

Stage 3. The user computes $g^{x_5} = g^{x_5-t} g^t, h^{y_5} = h^{y_5-\bar{t}} h^{\bar{t}}$ and then outputs the partial-ciphertext as

$$C_0 = (u, v, e) = (g^{x_5} h^{y_5}, g^{x_5} g_1 h^{y_5},$$

$$H_0(g^{x_5} b h^{y_5} g^{x_5} c h^{y_5}) \oplus m),$$

and $(\alpha_1, \alpha_2) = H(u, v, e)$. Then the user sends $\alpha_1 - t, \alpha_2 - \bar{t}$ to the cloud server.

Stage 4. The cloud server returns $g^{\alpha_1-t}, h^{\alpha_2-\bar{t}}$ to user.

Stage 5. The user computes $g^{\alpha_1}, h^{\alpha_2}$ and then outputs $C = (u, v, e, w)$ for $w = g^{x_5} d h^{y_5} \cdot g^{\alpha_1}(g^{x_5} b h^{y_5}) h^{\alpha_2}$.

Decryption**:** Upon receiving a ciphertext $C = (u, v, e, w)$, if the equation

$$w = g^{x_4} v h^{y_4} \cdot g^{\alpha_1} g^{x_2} u h^{y_2} h^{\alpha_2}$$

holds for $(\alpha_1, \alpha_2) = H(u, v, e)$, then the receiver decrypts the message as

$$m = H_0(g^{x_2} u h^{y_2} \cdot g^{x_3} v h^{y_3}) \oplus e;$$

Otherwise, he/she outputs $\perp$.

The security analysis is given as below.

Security of transformation key: Any adversary $\mathcal{A}$ wants to compute the transformation key $g^t, h^{\bar{t}}$, but it can only obtain $g^t h^{\bar{t}} = g^{t-x_5} u h^{\bar{t}-y_5}$. Based on the GFP, $\mathcal{A}$ fails to derive $g^t, h^{\bar{t}}$ by the factoring method. Meanwhile, $t, \bar{t}$ are secure relying on the DLP.

Security of encryption-random numbers: The adversary can gets $x_5 - t, y_5 - \bar{t}$, where x_5, y_5 are blinded by $t, \bar{t}$. Then the security of encryption-random numbers x_5, y_5 is based on the privacy of $t, \bar{t}$.

4.3 Performance analysis

In the above outsourced scheme, the encryptor only has to carry its transformation key then eliminates exponential operation for encryption. Thus, the computational cost of encryption can be largely reduced. Now we will present the efficiency by comparing the outsourced encryption algorithm with the non-outsourced scheme. Table 1 shows the computational cost of multiplication (MUL) and exponential (EXP) operations. Note that, the user requires two EXPs in Pre-processing before encryption.

Table 1: Computational cost for encryption

Schemes	MUL	EXP
Outsourced Scheme	16	4
Non-outsourced Scheme	20	0

Fig. 1 is obtained based on a 2×2 matrix group over Z_p. We measured the running time of the two schemes with 80-bit secure parameter (here we only consider the exhaustive attack) by using Maple 18 on a 64-bit machine of 1.70GHz. The figure clearly indicates that the outsourcing method saves significant computational cost for Cramer-Shoup like encryption over non-abelian group.

[3]Here, the adjective "large" indicates that x_i, y_i should be large enough for resisting exhaustive attacks. In practice, it is safe to sample them uniformly and randomly from the interval $[2^\lambda, 2^{\lambda+1}]$.

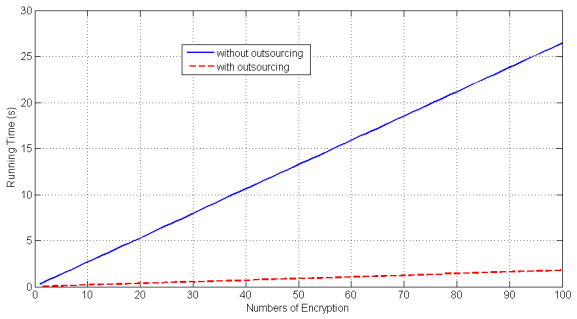

Figure 1: The comparison of encryption efficiency

5. CONCLUSION

Inspired by the seminal work of Diffie-Hellman's key agreement protocol, we introduced the concept of index exchangeable family (IEF) and proposed another general framework for constructing Cramer-Shoup like cryptosystems. We further showed that IEF can be instantiated based on the reasonable hardness assumptions originating from number theory and computational group theory. In particular, our instantiations can be considered as potential solutions to Vasco et al.'s open problem of finding non-abelian analogies of Cramer-Shoup cryptosystem. In addition, we proposed a secure outsourcing method for the encryption of the non-abelian analog based on the factorization problem over non-abelian groups. We demonstrated that the scheme can significantly reduce the computational cost thanks to using the cloud servers.

6. ACKNOWLEDGEMENTS

This work was supported by the National Natural Science Foundation of China (NSFC) (Nos. 61370194, 61411146001, 61502048).

7. REFERENCES

[1] S. Baba, S. Kotyada, R. Teja. A non-abelian factorization problem and an associated cryptosystem. Cryptology ePrint Archive: Report 2011/048.

[2] E. Begelfor, S.D. Miller, R. Venkatesan. Non-Abelian Analogs of Lattice Rounding. Cryptology ePrint Archive: Report 2015/024.

[3] M. Bellare, P. Rogaway. Random oracles are practical: a paradigm for designing efficient protocols. CCS 1993, pp. 62-73. ACM press, 1993.

[4] R. Cramer, V. Shoup. A practical public key cryptosystem secure against adaptive chosen ciphertext attacks. CRYPTO 1998, pp. 13-25. Springer, 1998.

[5] R. Cramer, V. Shoup. Universal Hash Proofs and a Paradiam for Adaptive Chosen Ciphertext Secure Public-Key Encryption. EUROCRYPT 2002, pp. 45-64. Springer, 2002.

[6] D. Dolev, C. Dwork, M. Naor. Non-malleable cryptography. STOC 1991, 542-552. ACM Press, 1991.

[7] Goyal V, Pandey O, Sahai A, Waters B.: Attribute-Based encryption for fine-grained access control of encrypted data. In: ACM conference on Computer and Communications Security (ACM CCS). pp. 89-98, 2006.

[8] L. Gu, L. Wang, K. Ota, M. Dong, Z. Cao, Y. Yang. New public key cryptosystems based on non-abelian factorization problems. Security and Communication Networks, vol. 6, no. 7, pp. 912-922, 2013.

[9] L. Gu, S. Zheng. Conjugacy Systems Based on Nonabelian Factorization Problems and Their Applications in Cryptography. Journal of Applied Mathematics, Volume 2014 (2014), Article ID 630607, http://dx.doi.org/10.1155/2014/630607

[10] D. Kahrobael, M. Anshel. Decision and search in non-abelian cramer shoup public key cryptosystem. Groups Complexity Cryptology, vol. 1(2), pp. 217-225, 2009. CoRR abs/1309.4519 (2013).

[11] K. H. Ko and S. J. Lee and J. H. Cheon and J. W. Han and J. Kang and C. Park. New public-key cryptosystem using braid groups. CRYPTO 2000, LNCS 1880, pp. 166–183. Springer, 2000.

[12] W. Lempken, S.S. Magliveras, T. Trung, W. Wei. A public key cryptosystem based on non-abelian finite groups. Journal of Cryptology 22(1), pp. 62-74, 2009.

[13] S.S. Magliveras, D.R. Stinson, T. Trung. New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups. Journal of Cryptology 15(4), pp. 285-297, 2002.

[14] M. Naor, M. Yung. Public-Key Cryptosystems Provably Secure against Chosen Ciphertext Attacks. STOC 1990, pp. 427-437. ACM press, 1990.

[15] A.G. Myasnikov, V. Shpilrain and A. Ushakov, Non-commutative Cryptography and Complexity of Group-theoretic Problems, Amer. Math. Soc. Surveys and Monographs, 2011.

[16] Christophe Petit. Towards factoring in $SL(2, F_{2^n})$. Design Codes Cryptography, 71(3), pp. 409-431, 2014.

[17] C. Rackoff, D. Simon. Noninteractive zero-knowledge proof of knowledge and chosen ciphertext attack. CRYPTO 1991, pp. 433-444. Springer, 1991.

[18] Martin Rötteler. Quantum algorithms: A survey of some recent results. Inform, Forsch. Entwickl, 21(2006): 3–20.

[19] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithme on a quantum computer. SIAM Journal on Computing, pp. 1484-1509, 1997.

[20] V. Shpilrain and A. Ushakov. Thompson's group and public key cryptography. ACNS 2005, LNCS 3531, pp. 151–164. Springer, 2005.

[21] M.I.G. Vasco, C. Martinez, R. Steinwandt, J. Villar. A new Cramer-Shoup like methodology for group based on provably secure encryption schemes. TCC 2005, LNCS 3378, pp. 495-509. Springer, 2005.

[22] Y. Zheng, J. Seberry. Practical approachs to attaining security against adaptively chosen ciphertext attacks. CRYPTO 1992, LNCS 740, pp. 292-304. Springer, 1992.

[23] Y. Zheng and J. Seberry. Immunizing public key cryptosystems against chosen ciphertext attacks. Special Issue on Secure Communications, IEEE Journal on Selected Areas on Communicastions, vol. 11(5), pp. 715-724, 1993.