Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2014, Article ID 630607, 10 pages
http://dx.doi.org/10.1155/2014/630607

Research Article

Conjugacy Systems Based on Nonabelian Factorization Problems and Their Applications in Cryptography

Lize Gu and Shihui Zheng

Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Correspondence should be addressed to Shihui Zheng; shihuizh@gmail.com

Received 2 February 2014; Accepted 6 April 2014; Published 28 April 2014

Academic Editor: Javier Oliver

Copyright © 2014 L. Gu and S. Zheng. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

To resist known quantum algorithm attacks, several nonabelian algebraic structures mounted upon the stage of modern cryptography. Recently, Baba et al. proposed an important analogy from the integer factorization problem to the factorization problem over nonabelian groups. In this paper, we propose several conjugated problems related to the factorization problem over nonabelian groups and then present three constructions of cryptographic primitives based on these newly introduced conjugacy systems: encryption, signature, and signcryption. Sample implementations of our proposal as well as the related performance analysis are also presented.

1. Introduction

Background and Motivation. Although the idea of encryption has made it to the world thousands of years ago, the concept of public key cryptography (PKC) came to us no more than half of a century. To secure communications over insecure channels, the core idea of PKC is to exert a heavy burden, that is, computational cost in general, on eavesdroppers but meanwhile keep the additional workload of legitimate users as light as possible [1]. This idea is always instantiated by certain challenging problems for which the legitimate users know at least one feasible solution, while it is infeasible to find a solution even if the attackers exhaust all available resources. Along this roadmap, the well-known Diffie-Hellman key exchange protocol [2] as well as many public key cryptosystems, such as RSA [3], ElGamal [4], and ECC [5, 6], manifests their great success during the past four decades. However, considering that the famous problem $P \overset{?}{=} NP$ remained open up to now, all these cryptographic protocols/schemes relay their security on assumptions of the intractability of certain problems, say integer factorization problem (IFP), discrete logarithm problem over finite fields (DLP), or elliptic curves (ECDLP).

Intractability assumptions of certain cryptographic problems themselves never mean the security of real systems. Instead, they must be embedded in implementing certain cryptographic primitives. In fact, security is a composite concept and it can be divided into several different properties. Among them, confidentiality, authenticity, and integrity attract a lot of attention in the community of PKC. Although the primitive of encryption is mainly intended to keep confidentiality, when an encryption scheme achieves indistinguishability against adaptive chosen ciphertext attacks (IND-CCA2), the integrity of the ciphertexts is also granted. Similarly, the primitive of signature maintains the authenticity and integrity, simultaneously. Another cryptographic primitive, signcryption, is a data security technology by which confidentiality is protected and authenticity is achieved seamlessly at the same time [7–9]. The primitive of signcryption, invented in 1996 but firstly disclosed to the public at CRYPTO 1997 [7, 8], is now an international standard for data protection (ISO/IEC 29150, Dec 2011). Up-to-date, many constructions of signcryption were proposed, based on the intractability assumptions of IFP [10, 11] or DLP/ECDLP [12, 13]. Some constructions further utilize the bilinear pairing to enhance the functionalities and performance [14, 15], but the security of these constructions was also rooted in the intractability assumption of ECDLP. Unfortunately, IFP and DLP as well as ECDLP could be efficiently solved by Shor's quantum algorithms [16, 17] and its extensions [18]. Thus, there is an urgent requirement to develop new signcryption schemes that have the potential capability to resist Shor-like quantum attacks. Although two lattice-based signcryption schemes were claimed recently [19, 20] to have the advantages in resisting known quantum algorithm attacks, the parameter size of these constructions is considerably large. Therefore, more efficient designs are expected.

Contribution. In this paper, we made efforts from two aspects. At first, we define several conjugated problems related to the factorization problem over nonabelian groups and we name these problems as conjugacy systems. Next, we explore the usefulness of these conjugacy systems via presenting three constructions of cryptographic primitives: encryption, signature, and signcryption. In addition, sample implementations of our proposal as well as related performance analysis are presented.

Related Work. Our work belongs to the line of the so-called noncommutative cryptography that has become noticeable recently [21]. Considering that Shor's quantum algorithm and its extension work well over some *commutative* groups, such as the multiplication group $\mathbb{Z}_n^*$, the multiplication group $\mathbb{F}_q^*$, and the addition group over elliptic curves on finite field $\mathbb{F}_q$, and we have already known efficient quantum algorithms for hidden group problems (HSP) over all *commutative* groups, a lot of attempts on developing cryptosystems are based on *noncommutative* algebraic structures. During the past decade, braid groups [9, 22, 23], inner automorphism groups [24, 25], Thompson's groups [26], linear groups and classical modular groups [27, 28], random covers and logarithmic signatures [29], and so forth have already mounted upon the stage of modern cryptography. However, this area is considerably immature and at present there are no practical, both in efficiency and security, noncommutative cryptosystems [9]. In particular, finding a secure nonabelian analogy of cryptosystems based on IFP remains open [21] until recently. In 2011, Baba et al. proposed a nonabelian factorization problem and presented associated cryptosystems [30]. Although BKT's constructions failed to achieve semantic security, the insight embedded in the nonabelian factorization problem opens a new avenue for developing practical nonabelian cryptography [31]. In 2012, Gu et al. [31] proposed an IND-CCA2 secure encryption scheme based on BKT's idea. Moreover, they gave the first arguments on resisting Shor's quantum algorithm attacks based on noncommutativity (see Remark 11).

Roadmap. The remaining content is organized as follows. In Section 2, we at first recall the definition of nonabelian factorization problem and related extensions, then define some new cryptographic problems (referred to as conjugacy systems), and finally present analysis on the hardness of these problems; in Section 3, we present new constructions on encryption, signature, andsigncryption based on the newly introduced conjugacy systems; in Section 4, we discuss the possible implementation platforms and related performance; finally, concluded remarks are given in Section 5.

2. Conjugacy Systems Based on Nonabelian Factorization Problems

Most public key cryptosystems are based on certain intractability assumptions and thus finding new intractable assumptions is an interesting cryptographic practice. In this section, we will at first review the so-called nonabelian factorization problem that was firstly formulated in [30] and then introduce some new cryptographic problems by coupling related problems with conjugate operations. This idea is in fact enlightened by braid cryptosystems [23] and the CSP-based constructions [32] where conjugacy related problems play center roles. For abbreviation, we refer to these problems as conjugacy systems.

2.1. Nonabelian Factorization Problem and New Cryptographic Problems

Definition 1 (factorization problem, FP [30, 31]). Let G be any nonabelian finite group with identity e. Let $g, h \in G$ be two random elements so that $\langle g\rangle \cap \langle h\rangle = \{e\}$. The factorization problem with respect to G, g, h, denoted by $\mathrm{FP}_{g,h}^{G}$, is to split the given product $g^x h^y \in G$ into a pair $(g^x, h^y) \in G^2$, where x and y are arbitrary integers picked at random.

Definition 2 (computational Diffie-Hellman problem, CDH [30, 31]). Let G be any nonabelian finite group with identity e. Let $g, h \in G$ be two random elements so that $\langle g\rangle \cap \langle h\rangle = \{e\}$. The computational Diffie-Hellman (CDH) problem with respect to G, g, h, denoted by $\mathrm{CDH}_{g,h}^{G}$, is to recover $g^{a+c}h^{b+d}$ from the given pair $(g^a h^b, g^c h^d) \in G^2$, where a, b, c, d are arbitrary integers picked at random.

Definition 3 (decisional Diffie-Hellman problem, DDH [31]). Let G be any nonabelian finite group with identity e. Let $g, h \in G$ be two random elements so that $\langle g\rangle \cap \langle h\rangle = \{e\}$. The decisional Diffie-Hellman (DDH) problem with respect to G, g, h, denoted by $\mathrm{DDH}_{g,h}^{G}$, is to distinguish the distribution

$$\mathscr{D}_0 \triangleq \left\{\left(g^a h^b, g^c h^d, g^z h^y\right) : a, b, c, d, z, y \in_R \mathbb{Z}\right\} \quad (1)$$

and the distribution

$$\mathscr{D}_1 \triangleq \left\{\left(g^a h^b, g^c h^d, g^{a+c} h^{b+d}\right) : a, b, c, d \in_R \mathbb{Z}\right\}. \quad (2)$$

Definition 4 (gap computational Diffie-Hellman problem, Gap-CDH [31]). Let G be any nonabelian finite group with identity e. Let $g, h \in G$ be two random elements so that $\langle g\rangle \cap \langle h\rangle = \{e\}$. The gap computational Diffie-Hellman (Gap-CDH) problem (In [31], this problem is called gap Diffie-Hellman (Gap-DH) problem) with respect to G, g, h, denoted by Gap-$\mathrm{CDH}_{g,h}^{G}$, is to solve the $\mathrm{CDH}_{g,h}^{G}$ problem given access to an oracle that solves the $\mathrm{DDH}_{g,h}^{G}$ problem.

Definition 5 (subgroup conjugator searching problem, SCSP). Let G be any nonabelian finite group with identity e. Let $g, h \in G$ be two random elements so that $\langle g\rangle \cap \langle h\rangle = \{e\}$. The subgroup conjugator searching problem (SCSP) with respect to G, g, h, denoted by $\mathrm{SCSP}_{g,h}^{G}$, is to recover g^{x} from the given pair $(h^{y}, g^{x}h^{y}g^{-x}) \in G^{2}$, where x, y are arbitrary integers picked at random.

Definition 6 (subgroup conjugacy deciding problem, SCDP). Let G be any nonabelian finite group with identity e. Let $g, h \in G$ be two random elements so that $\langle g\rangle \cap \langle h\rangle = \{e\}$. The subgroup conjugacy deciding problem (SCDP) with respect to G, g, h, denoted by $\mathrm{SCDP}_{g,h}^{G}$, is to distinguish the distribution

$$\mathscr{D}_2 \triangleq \left\{\left(h^{b}, g^{a}h^{b}g^{c}\right) : a, b, c \in_R \mathbb{Z}\right\} \tag{3}$$

and the distribution

$$\mathscr{D}_3 \triangleq \left\{\left(h^{b}, g^{a}h^{b}g^{-a}\right) : a, b \in_R \mathbb{Z}\right\}. \tag{4}$$

Definition 7 (conjugated computational Diffie-Hellman problem, CCDH). Let G be any nonabelian finite group with identity e. Let $g, h \in G$ be two random elements so that $\langle g\rangle \cap \langle h\rangle = \{e\}$. The conjugated computational Diffie-Hellman (CCDH) problem with respect to G, g, h, denoted by $\mathrm{CCDH}_{g,h}^{G}$, is to recover $g^{a+c}h^{b}g^{-a-c}$ from the given triple

$$\left(h^{b}, g^{a}h^{b}g^{-a}, g^{c}h^{b}g^{-c}\right) \in G^{3}, \tag{5}$$

where a, b, c, d are arbitrary integers picked at random.

Definition 8 (conjugated decisional Diffie-Hellman problem, CDDH). Let G be any nonabelian finite group with identity e. Let $g, h \in G$ be two random elements so that $\langle g\rangle \cap \langle h\rangle = \{e\}$. The conjugated decisional Diffie-Hellman (CDDH) problem with respect to G, g, h, denoted by $\mathrm{CDDH}_{g,h}^{G}$, is to distinguish the distribution

$$\mathscr{D}_4 \triangleq \left\{\left(h^{b}, g^{a}h^{b}g^{-a}, g^{c}h^{b}g^{-c}, g^{d}h^{b}g^{-d}\right)\right\}, \tag{6}$$

(where $a, b, c, d \in_R \mathbb{Z}$ are drawn at random) and the distribution

$$\mathscr{D}_5 \triangleq \left\{\left(h^{b}, g^{a}h^{b}g^{-a}, g^{c}h^{b}g^{-c}, g^{a+c}h^{b}g^{-a-c}\right)\right\}, \tag{7}$$

(where $a, b, c \in_R \mathbb{Z}$ are drawn at random).

Definition 9 (gap conjugated computational Diffie-Hellman problem, Gap-CCDH). Let G be any nonabelian finite group with identity e. Let $g, h \in G$ be two random elements so that $\langle g\rangle \cap \langle h\rangle = \{e\}$. The gap conjugated computational Diffie-Hellman (Gap-CCDH) problem with respect to G, g, h, denoted by $\text{Gap-CCDH}_{g,h}^{G}$, is to solve the $\mathrm{CCDH}_{g,h}^{G}$ problem, given access to an oracle that solves the $\mathrm{CDDH}_{g,h}^{G}$ problem.

2.2. Hardness Assumptions. Firstly, we should notice that the condition $\langle g\rangle \cap \langle h\rangle = \{e\}$ implies that the FP problem is well-defined in the sense that the solution is unique for any given FP instance. In addition, if G is abelian and the orders of g and h are coprime and known, then the FP problem can be reduced to the discrete logarithm problem in G according to [30]. However, if the orders of g and h have common factors or are kept unrevealed or G is nonabelian, then the FP problem seems much hard. In this case, the naive method of trying all different pairs (x, y) is apparently infeasible if the orders of g and h are large enough. Therefore, we would like to introduce the meta-assumptions as follows:

(i) (G, e) is a nonabelian finite group, where e is the identity;

(ii) the orders of g and h are large enough;

(iii) $gh \neq hg$ and $\langle g\rangle \cap \langle h\rangle = \{e\}$.

And then, based on this meta-assumption, our first hardness assumption states that the FP $_{g,h}^{G}$ problem is intractable.

Secondly, both the $\mathrm{DDH}_{g,h}^{G}$ problem and the $\text{Gap-DH}_{g,h}^{G}$ problem are no harder than the $\mathrm{CDH}_{g,h}^{G}$ problem. But as far as we know, there is no better solution for the $\mathrm{DDH}_{g,h}^{G}$ problem and $\text{Gap-CDH}_{g,h}^{G}$ problem other than solving the $\mathrm{CDH}_{g,h}^{G}$ problem. (Note that if g and h commute (i.e., $gh = hg$), although the $\mathrm{FP}_{g,h}^{G}$ problem is still meaningful, but the $\mathrm{CDH}_{g,h}^{G}$ problem, the $\mathrm{DDH}_{g,h}^{G}$ problem, and the $\text{Gap-DH}_{g,h}^{G}$ problem become trivial, thus, the meta-assumption of noncommutativity of g and h is one of the crucial factors.) Therefore, our 2nd, 3rd, and 4th hardness assumptions state the intractabilities of the $\mathrm{CDH}_{g,h}^{G}$ problem, the $\mathrm{DDH}_{g,h}^{G}$ problem, and the $\text{Gap-DH}_{g,h}^{G}$ problem, respectively.

Thirdly, the SCDP problem might be *tractable* for certain nonabelian groups, say matrix groups, considering that the trace of the matrix $g^{a}h^{b}g^{-a}$ is the same as the trace of h^{b}. However, even for matrix groups, it seems that both the CCDH problem and the CDDH problem are still intractable, since we have not found an easier way for solving them than using the naive method of enumerating all possible entries. Intuitively, it is hard to solve the CDDH problem without solving the SCSP problem when G is modeled as a generic semigroup model. In 2005, Maurer [33] proved that the discrete logarithm problem (DLP) and the corresponding decisional Diffie-Hellman (DDH) problem are polynomially equivalent in a generic cyclic group. By an analogical manner, we speculate that the SCSP problem and the CDDH problem in a generic noncommutative semigroup are polynomially equivalent. Furthermore, we do not know a better solution for the $\mathrm{CDDH}_{g,h}^{G}$ problem and $\text{Gap-CCDH}_{g,h}^{G}$ problem other than solving the $\mathrm{CCDH}_{g,h}^{G}$ problem. Therefore, our 5th, 6rd, 7th, and 8th hardness assumptions state the intractabilities of the $\mathrm{SCSP}_{g,h}^{G}$ problem, the $\mathrm{CCDH}_{g,h}^{G}$ problem, the $\mathrm{CDDH}_{g,h}^{G}$, and the $\text{Gap-CCDH}_{g,h}^{G}$ problem, respectively. Note that in this paper, we do not assume that $\mathrm{SCDP}_{g,h}^{G}$ problem is hard. At present, we have no idea on whether (gap) conjugated computational (resp., decisional) Diffie-Hellman problem is harder than (gap) computational (resp., decisional) Diffie-Hellman problem or vice versa.

Finally, a solution to the $\mathrm{FP}_{g,h}^{G}$ problem would imply a solution to all above problems [30]. In addition, h^b is not required to be invertible in all above definitions; thus it is possible to instantiate these problems over nonabelian semigroups (see Figure 1).

Remark 10 (SCSP versus CSP). Note that the subgroup conjugator searching problem (SCSP) and the subgroup conjugacy deciding problem (SCDP) introduced in this paper are in general at least as hard as the conjugator searching problem (CSP) and the conjugacy deciding problem (CDP) given in [21] in the sense that SCSP and SCDP further require the potential conjugator g^x coming from a specified subgroup $\langle g\rangle \subset G$.

Remark 11 (quantum attack resistant). Note that in [31], we give detailed analysis of the core role of noncommutativity on resisting Shor's quantum algorithm attacks. To make this paper self-contained, we briefly recall some points. We know that the main part of Shor's quantum algorithm is a quantum algorithm to solve the order-finding problem over the abelian group $\mathbb{Z}_n^*$ [16, 17]. Now, suppose that a quantum algorithm to solve the order-finding problem over the underlying group G is at hand and we have already worked out g's order a and h's order b. However, the following lifting reductions are blocked by noncommutativity:

$$\begin{aligned}(g^x h^y)^a &\neq g^{x\cdot a} h^{y\cdot a} = e\cdot h^{y\cdot a} = h^{y\cdot a},\\ (g^x h^y)^b &\neq g^{x\cdot b} h^{y\cdot b} = g^{x\cdot b}\cdot e = g^{x\cdot b}.\end{aligned} \tag{8}$$

The above two inequalities are very important in our arguments. Without them, one can reduce the $\mathrm{FP}_{g,h}^{G}$ problem to the DLP problems over the cyclic groups $\langle g\rangle$ and $\langle h\rangle$, which are quantumly tractable by using Shor's algorithm [31]. In this sense, we can see that BKT's method pins down the true meaning of noncommutativity for resisting Shor's quantum algorithm attacks (see Section 7.1 of [31] for more details).

3. Cryptographic Applications

Let us proceed to demonstrate the usefulness of the conjugacy systems defined above. Suppose that G is a nonabelian group. At first, the common setting on the public parameters of the proposed schemes are given by a quintuple $\langle \mathfrak{D}, g, h, H_1, H_2\rangle$, where

(i) $\mathfrak{D}$ is a description of G. Without loss of generality, we assume the length of $\mathfrak{D}$ is bounded by $\mathcal{O}(\log|G|)$ for finite G. When G is infinite but admits a finite presentation, say $G = \langle X \mid R\rangle$, then the description of $\mathfrak{D}$ is given by the description of X and R.

(ii) $g, h \in G$ are two fixed elements that are picked at random so that

  (a) g and h do not commute; that is, $gh \neq hg$;

  (b) $\langle g\rangle \cap \langle h\rangle = \{e\}$;

  (c) the order of g is large enough. Typically, we assume that the order of g is no less than the system security parameter k that will be specified later.

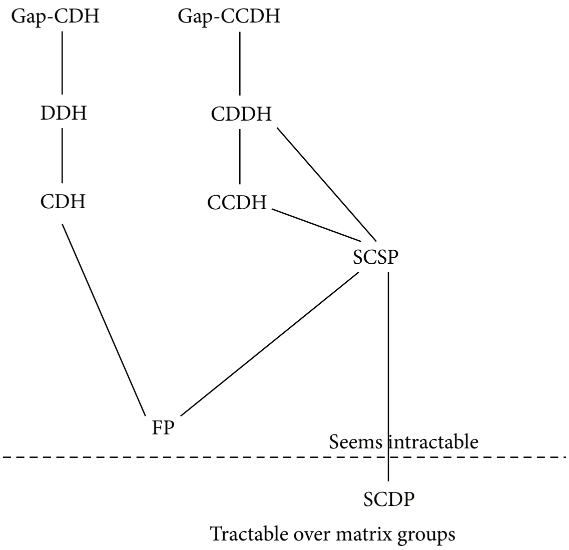

FIGURE 1: Cryptographic problems over nonabelian semigroups.

(iii) $H_1 : G \rightarrow G^2$ and $H_2 : G^2 \rightarrow G$ are two cryptographic hash functions that are modeled as random oracles.

3.1. Encryption with IND-CPA Security. Now, as a warming-up, an Elgamal-like encryption scheme, denoted by V_1, is described as follows.

(i) $\mathrm{KeyGen}(1^k)$: this is the key generation algorithm that takes, as input, the system security parameter 1^k, picks an integer $s \in \{0,1\}^k$ at random and calculates $x = g^s h g^{-s} \in G$, and finally outputs $(g^s, x) \in G^2$ as the private/public key pair.

(ii) $\mathrm{Enc}(x; m)$: this is the encryption algorithm that takes as inputs the public key $x \in G$ and the message $m \in G$ and performs the following steps:

  (a) pick $t \in \{0,1\}^k$ at random,

  (b) compute $c_1 = g^t h g^{-t}$ and $c_2 = m g^t x g^{-t}$,

  (c) output (c_1, c_2).

(iii) $\mathrm{Dec}(g^s; c_1, c_2)$: this is the decryption algorithm that takes as inputs the private key $g^s \in G$ and the ciphertext pair $(c_1, c_2) \in G^2$ and then outputs the intended message $m = c_2(g^s c_1 g^{-s})^{-1}$.

Correctness. The correctness of the scheme is granted by the following calculation:

$$\begin{aligned} c_2\left(g^s c_1 g^{-s}\right)^{-1} &= mg^t xg^{-t}\left(g^s g^t hg^{-t} g^{-s}\right)^{-1} \\ &= mg^t xg^{-t}\left(g^t g^s hg^{-s} g^{-t}\right)^{-1} \\ &= m\left(g^t xg^{-t}\right)\left(g^t xg^{-t}\right)^{-1} \\ &= m. \end{aligned} \tag{9}$$

Security. The security of the above encryption scheme is essentially similar to the security of the well-known Elgamal encryption scheme [4]. That is, it is indistinguishable against chosen plaintext attack (IND-CPA) under the assumption of the intractability of the $\text{CDDH}_{g,h}^{G}$ problem. One can also find similar proofs from either [9] or [32]. In addition, since neither H_1 nor H_2 are used in this scheme, it is secure in the standard model. By using two random oracles H_1 and H_2, one can easily convert it into an IND-CCA2 secure encryption scheme according to the well-known FO transformation theorem [34] (see the proof of Theorem 14).

3.2. Signature with the Lowest Security. Next, let us describe a signature scheme, denoted by V_2, that can be viewed as a simplified variant of the noncommutative signature scheme given in [35].

(i) KeyGen(1^k): it is the same as in Section 3.1.

(ii) Sign($g^s; m$): this is the signing algorithm that takes as inputs the private key $g^s \in G$ and the message $m \in G$ and performs the following steps:

(a) pick $t \in \{0, 1\}^k$ at random,

(b) compute $u = g^t hg^{-t}$, $v = H_2(m, u)$, and $w = H_2(u, v)g^{-t}g^s$,

(c) output the signature $\sigma = (u, w) \in G^2$.

(iii) Verify($x; m, \sigma$): this is the verifying algorithm that takes as inputs the public key $x \in G$ and the message-signature pair (m, σ) and then performs the following steps:

(a) parse σ into $(u, w) \in G^2$,

(b) compute $v = H_2(m, u)$ and verify whether the following equality holds

$$wuw^{-1} \overset{?}{=} H_2(u, v)\, xH_2(u, v)^{-1}, \tag{10}$$

(c) if so, accept this signature; otherwise, reject it.

Correctness. The correctness of the scheme is granted by the following calculation:

$$\begin{aligned} wuw^{-1} &= H_2(u, v)\, g^{-t} g^s \left(g^t hg^{-t}\right) g^{-s} g^t H_2(u, v)^{-1} \\ &= H_2(u, v)\left(g^{-s} hg^s\right) H_2(u, v)^{-1} \\ &= H_2(u, v)\, xH_2(u, v)^{-1}. \end{aligned} \tag{11}$$

Security. On one hand, under the assumptions of the intractability of the $\text{SCSP}_{g,h}^{G}$ problem and H_2 being a random oracle, this signature scheme merely achieves unforgeability against no message attacks (UF-NMA)—this is the lowest security level for a signature scheme where adversaries are merely given the public key and asked to output a successful forgery. The arguments are similar to the security analysis given in [35]. On the other hand, taking this scheme as a building block, we can design a signcryption scheme that achieves existential unforgeability against external adaptively chosen message attack (see the next subsection).

3.3. Signcryption with IND-CCA2 Security. Based on the encryption scheme V_1 and the signature scheme V_2, let us proceed to present a signcryption scheme, denoted by V_3.

(i) KeyGen(1^k): it the same as in Section 3.1.

(ii) SignCrypt($g^s, y; m$): this is the signcryption algorithm that takes as inputs the sender's private key $g^s \in G$, the receiver's public key $y \in G$, and the message $m \in G$ and performs the following steps:

(a) pick $t \in \{0, 1\}^k$ at random,

(b) compute

$$\begin{aligned} c_1 &= g^t hg^{-t}, \\ \tau &= H_2(m, c_1), \\ \sigma &= \tau c_1 g^s g^{-t}, \\ \gamma &= H_1\left(g^t yg^{-t}\right), \\ c_2 &= (m \parallel \sigma) \oplus \gamma, \end{aligned} \tag{12}$$

where operator "⊕" should be viewed as XOR operation over bit-strings that are encoding results of a pair in G^2,

(c) output (c_1, c_2).

(iii) UnSignCrypt ($g^r, x; c_1, c_2$): this is the unsigncryption algorithm that takes as inputs the receiver's private key $g^r \in G$, the sender's public key $x \in G$, and the ciphertext pair (c_1, c_2) and performs the following steps:

(a) compute $m' \parallel \sigma' = c_2 \oplus H_1(g^r c_1 g^{-r})$,

(b) let $\tau' = H_2(m', c_1)$,

(c) output m' if $\sigma' c_1 \sigma'^{-1} = (\tau' c_1)x(\tau' c_1)^{-1}$ and $\perp$ otherwise.

Remark 12. The above signcryption scheme inherits the same framework from [9]. However, the construction given here is featured by the following differences.

(i) Different platforms with different security bases. In [9], the platform is the braid group B_n and the underlying intractability assumption is the conjugator searching problem (CSP), while in this paper, the platform could be any nonabelian group and the underlying intractability assumption is the subgroup conjugator searching problem (SCSP) that is based on the intractability assumption of the nonabelian factorization problem. In general, we think the SCSP problem is at least as hard as the CSP problem (see Remark 10). In particular, based on nonabelian factorization related problems, noncommutativity plays a core role in resisting Shor's quantum algorithm attacks.

(ii) Different settings with different trade-off in computational/storage cost. As suggested in [9], with the braid group B_{50}, we need about 4 Kbits to represent a braid with canonical length $\ell \leq 10$. This is a bit inefficient in storage. Therefore, instead of keeping a braid as the private key, we merely use a positive integer $s \in \{0,1\}^k$ to indicate the private key. Considering that the braid exponentiation can be finished very efficiently, the real private key $a^s \in B_{50}$ can be reconstructed whenever it is required. However in this paper, our proposal could be instantiated over arbitrary nonabelian groups only if the related intractability assumptions remain reasonable. Thus, we directly use $g^s \in G$ as the private key. To deploy our proposal in real systems, the engineers are responsible for making proper trade-off choice between the storage cost and the computational cost.

Correctness. The correctness of the above scheme is given by the following theorem.

Theorem 13. *The proposed signcryption is consistent.*

Proof. Suppose the sender and the receiver perform honestly and their inputs are well formed. That is, $x = g^s h g^{-s}$ and $y = g^r h g^{-r}$. Then, since

$$\begin{aligned} g^r c_1 g^{-r} &= g^r g^t h g^{-t} g^{-r} \\ &= g^t g^r h g^{-r} g^{-t} \\ &= g^t y g^{-t}, \\ m' \parallel \sigma' &= c_2 \oplus H_1\left(g^r c_1 g^{-r}\right) \\ &= (m \parallel \sigma) \oplus H_1\left(g^t y g^{-t}\right) \oplus H_1\left(g^t y g^{-t}\right) \\ &= m \parallel \sigma, \\ \tau' &= H_2\left(m', c_1\right) = H_2\left(m, c_1\right) = \tau, \\ \sigma &= \tau c_1 g^s g^{-t}, \end{aligned} \tag{13}$$

we have that

$$\begin{aligned} \sigma' c_1 \sigma'^{-1} &= \sigma\left(g^t h g^{-t}\right)\sigma^{-1} \\ &= \left(\tau c_1 g^s g^{-t}\right)\left(g^t h g^{-t}\right)\left(\tau c_1 g^s g^{-t}\right)^{-1} \\ &= \left(\tau' c_1\right)\left(g^s h g^{-s}\right)\left(\tau' c_1\right)^{-1} \\ &= \left(\tau' c_1\right) x \left(\tau' c_1\right)^{-1}. \end{aligned} \tag{14}$$

Then, $m' = m$ will be output correctly. □

Security. As for a signcryption scheme, the security includes two aspects: indistinguishability and unforgeability.

Theorem 14. *Suppose that H_1 and H_2 are random oracles. The proposed signcryption is indistinguishable against adaptive chosen ciphertext attack (IND-CCA2) assuming that the $\mathrm{CDDH}_{g,h}^{G}$ problem is intractable.*

Proof (sketch of the proof). The proof threads are similar to what is given in [9]. At first, we can apply the well-known Fujisaki-Okamoto transformation theorem [34] to conclude the IND-CCA2 security of the following encryption scheme, denoted by V_4.

(i) KeyGen(1^k): it is the same as in Section 3.1.

(ii) Enc$'(y; m)$: this is the encryption algorithm that takes as inputs the receiver's public key y and a message $m \in G$ and then performs the following steps:

  (a) pick $u \in G$ at random,
  (b) let $(c_1, c_2) \leftarrow \mathrm{Enc}(y; u)$, where Enc is the encryption algorithm in Section 3.1,
  (c) let $c_3 = m \oplus H_1(u)$ and $c_4 = H_2(m, u)$,
  (d) output (c_1, c_2, c_3, c_4).

(iii) Dec$'(g^r; c_1, c_2, c_3, c_4)$: this is the decryption algorithm that takes as inputs the receiver's private key $g^r \in G$ and the ciphertext quadruple (c_1, c_2, c_3, c_4) and then performs the following steps:

  (a) let $u' \leftarrow \mathrm{Dec}(g^r; c_1, c_2)$, where Dec is the decryption algorithm in Section 3.1,
  (b) let $m' \leftarrow c_3 \oplus H_1(u')$,
  (c) output m' if $c_4 = H_2(m', u')$ and $\perp$ otherwise.

Apparently, V_4 is an FO-like variant of V_1 and its security is enhanced to IND-CCA2 assuming that both H_1 and H_2 are random oracles [34].

Now, let us show that, with the same random oracles, if there exists a probabilistic polynomial time adversary $\mathscr{A}$ that can break the IND-CCA2 security of the proposed signcryption scheme V_3, then there also exists another probabilistic polynomial time adversary $\mathscr{B}$ that can break the IND-CCA2 security of V_4.

In fact, since $\mathscr{B}$ controls the response of the random oracles H_1 and H_2, it can break the IND-CCA2 security of V_4 easily: whenever seeing a ciphertext (c_1, c_2, c_3, c_4), it can retrieve the message m and random salt u by looking up the response list of H_2 under the reasonable assumption that the probability for different pair (m', u') with same hash value with the pair (m, u) is negligible. The thing left is to show *how* $\mathscr{B}$, without knowing the receiver's private key $g^r \in G$, *can simulate* the response on decryption queries for $\mathscr{A}$ by a perfect manner.

Whenever $\mathscr{A}$ invokes an unsigncryption query by submitting a signcryption pair (c_1, c_2), $\mathscr{B}$ responds as follows.

(1) Lookup $(*, c_1, *)$ in H_2-list, where $*$ indicates a wildcard that can be matched with arbitrary inputs. If there is no matched triple, $\mathscr{B}$ sends $\perp$ to $\mathscr{A}$ as the response.

(2) For each matched triple (m_i, c_1, τ_i), $\mathscr{B}$ performs the following steps:

(a) for each (u, γ) in H_1 list, do the following steps:

(i) extract a possible σ_i according to the following formula:

$$c_2 = (m_i \mid\mid \sigma_i) \oplus \gamma, \tag{15}$$

(ii) test whether the equality

$$\sigma_i c_1 \sigma_i^{-1} \overset{?}{=} (\tau_i c_1)\, x (\tau_i c_1)^{-1} \tag{16}$$

holds. If so, reply $\mathscr{A}$ with m_i and end the response; otherwise, continue.

(3) If up to now $\mathscr{B}$ has no output response to $\mathscr{A}$ yet, then $\mathscr{B}$ sends $\perp$ to $\mathscr{A}$ as the response and then end the response.

Finally, without accessing hash queries on random oracles H_1 and H_2, $\mathscr{A}$'s probability for submitting a valid signcryption pair (c_1, c_2) is negligible. Thus, whenever $\mathscr{A}$ invokes hash queries on H_1 and H_2 for forming a valid signcryption pair, related materials are recorded, and $\mathscr{B}$ can retrieve them and finally send $\mathscr{A}$ a perfect response. □

Theorem 15. *Suppose that H_1 and H_2 are random oracles. The proposed signcryption scheme is existential unforgeable against external adaptive chosen message attacks (EUF-ext-CMA) assuming that the SCSP$^G_{g,h}$ problem is intractable.*

Proof. Here, the term "external" means that the forger is neither the singer, nor the intended receiver. Let us show that whenever an external attacker $\mathscr{A}$ outputs a successful forgery, then this must mean a contrary against the UF-NMA security of the signature scheme V_2 given in Section 3.2. At first, without invoking any query, $\mathscr{A}$'s successful forgery itself means an attack against the UF-NMA security. Next, suppose that $\mathscr{A}$ invokes many polynomial signcryption queries or unsigncryption queries. Let us show that the responses for these queries have no help to $\mathscr{A}$ for making a forged signcryption.

Suppose $\mathscr{A}$ invokes a signcryption query on some message m and receives a pair (c_1, c_2) as the response. After then, $\mathscr{A}$ invokes a random oracle query on H_2 with inputs m and c_1 and then he/she obtains τ. Now, $\mathscr{A}$ still has no means to obtain a valid signature from (m, c_1, c_2, τ) since both $g^s g^{-t}$ and γ remain unknown. Suppose $\mathscr{A}$ can get γ via invoking a random oracle query on H_1 with input $g^t y g^{-t}$. Then, its query input gives a solution to the SCSP instance $(c_1 = g^t h g^{-t}, y = g^r h g^{-r})$. This is a contrary to the assumption of the intractability of the SCSP problem.

Now, suppose $\mathscr{A}$ invokes an unsigncryption query on some signcryption pair (c_1, c_2). Similar to the response of $\mathscr{B}$ given in the proof of Theorem 14, $\mathscr{A}$ gets either a symbol $\perp$ or a message m_i. In the former case, $\mathscr{A}$'s query is invalid and rejected. In the latter case, $\mathscr{A}$'s query is valid and there exists a matched entry γ in H_1 list. This in turn implies that there exists a matched entry $g^t y g^{-t}$ in H_1 list. However, this is impossible since it again means a solution to the SCSP instance $(c_1 = g^t h g^{-t}, y = g^r h g^{-r})$.

This concludes the theorem. □

Remark 16. To proof the unforgeability of a signature scheme, it is reasonable to exclude the signer from forgeries. But just as what was done in [9], the so-called external attacker model enables us to further exclude the intended receiver from the forgeries. Unlike the primitive authenticated encryption, the authenticity embedded in the primitive of signcryption is unidirectional to some extent. That is, it seems that there is no reason for an intended receiver to forge a signature on behalf of some signer and then encrypt the signature for himself/herself, except for planting false evidence against some senders. Otherwise, an existentially unforgeable signature scheme, such as the noncommutative signature scheme in [36], should be embedded therein.

4. Sample Implementations and Performance Evaluation

In [30], the authors suggested to consider the intractability assumption of the FP$^G_{g,h}$ problem over three kinds of platforms:

(1) $\mathbf{GL}_n(\mathbb{F}_q)$, that is, the general linear group over finite field,

(2) $\mathbf{UT}_n(\mathbb{F}_q)$, that is, the nonabelian subgroup of $\mathbf{GL}_n(\mathbb{F}_q)$ consisting of unitriangular matrices,

(3) braids set $B_n(l)$, that is, the set of braids in the braid group B_n with l canonical factors.

At first, a braid $B_n(l)$ can be represented by a bit string of size $\lceil \ln \log n \rceil$ [23] and the complexities of the braid operations such as multiplication, inversion, and canonical form computation are bounded by $\mathscr{O}(l^2 n \log n)$ in the sense of bit operations [9]. Thus, if we follow Maffre's suggestions by setting $n = 50$ and $l = 10$ [37], then the number of bit operations for implementing these braid operations is proportional to 2^{15} and the sizes of the system parameters, the private key, the public key, and the ciphertexts are 5650 bits, 80 bits, 2822 bits, and 8466 bits, respectively. More detailed evaluation on the performance of braid-based cryptosystems can be found either in [36] or in [9].

Next, let us pay attention to $\mathbf{GL}_n(\mathbb{F}_q)$ and $\mathbf{UT}_n(\mathbb{F}_q)$. In particular, we mainly focus on two aspects: the time complexity of exponentiation and the related parameter sizes. Since the classical techniques for matrix multiplication/inversion in $\mathbf{GL}_n(\mathbb{F}_q)$ (resp., $\mathbf{UT}_n(\mathbb{F}_q)$) take about n^3 (resp., $n(n+1)(n+2)/6$) $\mathbb{F}_q$-operations, while each $\mathbb{F}_q$-operation needs $\mathcal{O}(\log^2 q)$ bit operations [38], thus by employing the idea of "square-multiply," the time complexity of calculating an exponentiation g^s with $s \in_R \{0,1\}^k$ in both $\mathbf{GL}_n(\mathbb{F}_q)$ and $\mathbf{UT}_n(\mathbb{F}_q)$ is $\mathcal{O}(n^3 k \log^2 q)$ in sense of bit operations. To represent a matrix in $\mathbf{GL}_n(\mathbb{F}_q)$ (resp., $\mathbf{UT}_n(\mathbb{F}_q)$), we need n^2 (resp., $n(n-1)/2$) $\mathbb{F}_q$-elements, while each $\mathbb{F}_q$-element occupies exactly $\log q$ bits. In practice, n need not to be too large. Typically, we set $n = 4$ and then collect our analysis in Table 1. From this table, we can see that the computational/storage cost of cryptosystems over $\mathbf{UT}_n(\mathbb{F}_q)$ is about merely $1/3$ times of those over $\mathbf{GL}_n(\mathbb{F}_q)$ when $n = 4$. (Note that since both the encryption scheme V_1 and the signature scheme V_2 are embedded into the signcryption scheme V_3, we merely present performance analysis on V_3.)

5. Conclusion

The booming of quantum algorithm casts distrust on many public key cryptosystems based on integer factorization problem, discrete logarithm, and other assumed intractable problems over certain abelian groups. Some breakthrough in developing new public key cryptography based on nonabelian algebraic structures has been made during the past decade. In particular, Baba et al. made the first step toward construct cryptographic schemes based on nonabelian factorization problems. In this paper, we at first present several conjugacy systems based on the factorization problem over nonabelian groups and then present new construction of encryption, signature, and signcryption based on the newly introduced cryptographic intractable assumptions. Some possible implementation platforms and the related performance analysis are also given. Two possible future perspectives are to investigate more efficient platforms for implementing our proposal and to investigate possible reductions from the hardness of the related conjugated problems to the hardness of the underlying problems.

Appendix

Existential Forgery on the Noncommutative Signature Scheme in [35]

In 2012, Kahrobaei and Koupparis [35] introduced a noncommutative digital signature scheme, denoted by KK12 for short. In KK12, a highly smooth composite number n was introduced and the authors claimed it is necessary to use the exponent n for resisting existential forgery. The KK12 signature scheme can be summarized as follows.

(i) KeyGen: the private key is a pair (s, n) with $s \in_R G$ and $n = \prod_{k=1}^{l} p_k^{e_k}$ (where p_k are prime and $e_k \in \mathbb{N}$) while the public key is set to $x = g^{ns}$. (For arbitrary $s \in G$ and $n \in \mathbb{N}$, g^s and g^n represent $s^{-1}gs \in G$ and $\underbrace{g \cdots g}_{n \text{ times}} \in G$, resp. In addition, although neither ns nor sn is well-defined, we have that $g^{ns} = s^{-1}g^n s = (g^s)^n = g^{sn}$ holds without any ambiguity.)

(ii) Sign: to sign a given message m, the signer with private key (s, n) performs the following steps:

(a) pick $t \in G$ at random and a random factorization of $n = n_i n_j$,

(b) compute

$$y = g^{n_j t}, h = H(m, y), \alpha = t^{-1} shy, \tag{A.1}$$

(c) output the signature $\sigma = (y, \alpha, n_j)$.

(iii) Verify: $y^{n_j \alpha} \overset{?}{=} x^{hy}$ where $h = H(m, y)$.

Unfortunately, we find that this is not true and the newly introduced exponent n did not bring to bear upon existential forgery. In fact, the authors [35] had already realized this problem and suggested to let the signer keep a public list that contains all n_js, that is, random factors of n, he/she has used thus far. But we think this solution is impractical; this would make the signature verification process very inefficient, since one has to check the freshness of n_j.This needs to go through all existing n_js from the list.

Now, let us proceed to describe our cryptanalysis on KK12. Upon obtaining a valid signature triple $\sigma = (y, \alpha, n_j)$ on message m, by reusing the exponent n_j, our existential forgery $\sigma' = (y', \alpha', n_j)$ on arbitrary message m' is formed as follows:

$$y' = y^{t'}, \quad h' = H(m', y'), \quad \alpha' = t'^{-1} \alpha y^{-1} h^{-1} h' y', \tag{A.2}$$

where $t' \in G$ is picked at random and $h = H(m, y)$. The left thing is to show that this forgery can pass the verification. In fact, we have

$$\begin{aligned} \alpha' &= t'^{-1} \alpha y^{-1} \widehat{h}^{-1} h' y' \\ &= t'^{-1} \left(t^{-1} shy\right) y^{-1} \widehat{h}^{-1} h' y' \\ &= \left(tt'\right)^{-1} sh' y', \\ y' &= y^{t'} \\ &= t'^{-1} \left(t^{-1} g^{n_i} t\right) t' \\ &= g^{n_i tt'}. \end{aligned} \tag{A.3}$$

Thus,

$$y'^{n_j \alpha'} = \left(g^{n_i tt'}\right)^{n_j \alpha'} = g^{ntt'(tt')^{-1} sh' y'} = (g^{ns})^{h' y'} = x^{h' y'}. \tag{A.4}$$

That is, the above existential forgery attack is successful.

Table 1: Performance of signcryption scheme V_3 ($n = 4$).

Platforms	Operations* and complexities†			Parameters and sizes‡		
	KeyGen	SignCrypt	UnSignCrypt	pk§	sk	Ciphertext
G	$1e + 2m + 1i$	$1e + 7m + 1i$	$7m + 3i$	$\log \lvert G \rvert$	$\log \lvert G \rvert$	$2 \log \lvert G \rvert$
$\mathbf{GL}_n(\mathbb{F}_q)$	$\sim 64k\log^2 q$		$\sim 640\log^2 q$	$\sim 16\log q$	$\sim 16\log q$	$\sim 32\log q$
$\mathbf{UT}_n(\mathbb{F}_q)$	$\sim 20k\log^2 q$		$\sim 200\log^2 q$	$\sim 6\log q$	$\sim 6\log q$	$\sim 12\log q$
$B_{50}(10)$	$\sim 2^{15}$			5730	2822	8466

* $e/m/i$: exponentiation/multiplication/inversion in the nonabelian group G.

†In the sense of bit operations.

‡In the sense of bit length.

§Including system parameters shared by all users.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work is partially supported by the National Natural Science Foundation of China (NSFC) (no. 61121061, 61370194) and the Fundamental Research Funds for the Central Universities (no. BUPT2012RC0219). Finally, the authors would like to thank the anonymous referees for their very careful and instructive comments.

References

[1] R. C. Merkle, "Secure communications over insecure channels," *Communications of the ACM*, vol. 21, no. 4, pp. 294–299, 1978.

[2] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[3] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the Association for Computing Machinery*, vol. 21, no. 2, pp. 120–126, 1978.

[4] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[5] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology (CRYPTO '85)*, vol. 218 of *Lecture Notes in Computer Science*, pp. 417–426, Springer, Berlin, Germany, 1986.

[6] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[7] A. Dent and Y. Zheng, *Practical Signcryption*, Information Security and Cryptography, Springer, Berlin, Germany, 2010, http://www.signcryption.org/.

[8] Y. Zheng, "Digital signcryption or how to achieve Cost(Signature & Encryption) ≪ Cost(Signature) + Cost(Encryption)," in *Advances in Cryptology—Crypto '97*, vol. 1294 of *Lecture Notes in Computer Science*, pp. 165–179, Springer, Berlin, Germany, 1997.

[9] L. Gu, Y. Pan, M. Dong, and K. Ota, "Noncommutative lightweight signcryption for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 818917, 10 pages, 2013.

[10] R. Steinfeld and Y. Zheng, "A signcryption scheme based on integer factorization," in *Information Security Workshop—ISW '00*, vol. 1975 of *Lecture Notes in Computer Science*, pp. 308–322, Springer, Berlin, Germany, 2000.

[11] J. Malone-Lee and W. Mao, "Two birds one stone: signcryption using RSA," in *Cryptographers' Track at the RSA Conference—CT-RSA '03*, vol. 2612 of *Lecture Notes in Computer Science*, pp. 211–225, Springer, Berlin, Germany, 2003.

[12] Y. Zheng and H. Imai, "How to construct efficient signcryption schemes on elliptic curves," *Information Processing Letters*, vol. 68, no. 5, pp. 227–233, 1998.

[13] M. Toorani and A. A. B. Shirazi, "A directly public verifiable signcryption scheme based on elliptic curves," in *Proceedings of the IEEE Symposium on Computers and Communications (ISCC '09)*, pp. 713–716, Sousse, Tunisia, July 2009.

[14] L. Zhang and T. Mo, "A signcryption scheme for WEP in WLAN based on bilinear pairings," in *Proceedings of the International Conference on Computer Application and System Modeling (ICCASM '10)*, vol. 8, pp. 126–130, IEEE Computer Society, Taiyuan, China, October 2010.

[15] J. Zhang, Y. Yang, and X. Niu, "A novel identity-based multi-signcryption scheme," *International Journal of Distributed Sensor Networks*, vol. 1, no. 5, pp. 28–28, 2009.

[16] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS '94)*, pp. 124–134, IEEE Computer Society, Santa Fe, NM, USA, November 1994.

[17] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[18] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," *Quantum Information & Computation*, vol. 3, no. 4, pp. 317–344, 2003.

[19] F. Li, F. Muhaya, M. Khan, and T. Takagi, "Lattice-based signcryption," *Concurrency and Computation: Practice and Experience*, vol. 25, no. 14, pp. 2112–2122, 2013.

[20] F. Wang, Y. Hu, and C. Wang, "Post-quantum secure hybrid signcryption from lattice assumption," *Applied Mathematics & Information Sciences*, vol. 6, no. 1, pp. 23–28, 2012.

[21] A. Myasnikov, V. Shpilrain, and A. Ushakov, *Non-Commutative Cryptography and Complexity of Group-Theoretic Problems*, vol. 177 of *Mathematical Surveys and Monographs*, American Mathematical Society, Providence, RI, USA, 2011.

[22] I. Anshel, M. Anshel, and D. Goldfeld, "An algebraic method for public-key cryptography," *Mathematical Research Letters*, vol. 6, no. 3-4, pp. 287–291, 1999.

[23] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J.-s. Kang, and C. Park, "New public-key cryptosystem using braid groups," in *Advances in Cryptology (CRYPTO '00)*, M. Bellare, Ed., vol. 1880 of *Lecture Notes in Computer Science*, pp. 166–183, Springer, Berlin, Germany, 2000.

[24] S. H. Paeng, K. C. Ha, J. H. Kim, S. Chee, and C. Park, "New public key cryptosystem using finite nonabelian groups," in *Advances in Cryptology (CRYPTO '01)*, vol. 2139 of *Lecture Notes in Computer Science*, pp. 470–485, Springer, Berlin, Germany, 2001.

[25] A. Mahalanobis, "A simple generalization of the ElGamal cryptosystem to non-abelian groups," *Communications in Algebra*, vol. 36, no. 10, pp. 3878–3889, 2008.

[26] V. Shpilrain and A. Ushakov, "Thompson's group and public key cryptography," in *Applied Cryptography and Network Security (ACNS '05)*, vol. 3531 of *Lecture Notes in Computer Science*, pp. 151–163, Springer, Berlin, Germany, 2005.

[27] G. Baumslag, B. Fine, and X. Xu, "A proposed public key cryptosystem using the modular group," in *Combinatorial Group Theory, Discrete Groups, and Number Theory*, vol. 421 of *Contemporary Mathematics*, pp. 35–44, American Mathematical Society, Providence, RI, USA, 2006.

[28] G. Baumslag, B. Fine, and X. Xu, "Cryptosystems using linear groups," *Applicable Algebra in Engineering, Communication and Computing*, vol. 17, no. 3-4, pp. 205–217, 2006.

[29] S. S. Magliveras, D. R. Stinson, and T. van Trung, "New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups," *Journal of Cryptology*, vol. 15, no. 4, pp. 285–297, 2002.

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

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

[32] L. Wang, L. Wang, Z. Cao, E. Okamoto, and J. Shao, "New constructions of public-key encryption schemes from conjugacy search problems," in *Information Security and Cryptology (Inscrypt '10)*, vol. 6584 of *Lecture Notes in Computer Science*, pp. 1–17, Springer, Berlin, Germany, 2011.

[33] U. Maurer, "Abstract models of computation in cryptography," in *Cryptography and Coding*, N. P. Smart, Ed., vol. 3796 of *Lecture Notes in Computer Science*, pp. 1–12, Springer, Heidelberg, Germany, 2005.

[34] E. Fujisaki and T. Okamoto, "How to enhance the security of public key encryption at minimum cost," in *Public Key Cryptography (PKC '99)*, vol. 1560 of *Lecture Notes in Computer Science*, pp. 53–68, Springer, Berlin, Germany, 1999.

[35] D. Kahrobaei and C. Koupparis, "Non-commutative digital signatures," *Groups Complexity Cryptology*, vol. 4, no. 2, pp. 377–384, 2012.

[36] L. Wang, L. Wang, Z. Cao, Y. Yang, and X. Niu, "Conjugate adjoining problem in braid groups and new design of braid-based signatures," *Science China—Information Sciences*, vol. 53, no. 3, pp. 524–536, 2010.

[37] S. Maffre, "A weak key test for braid based cryptography," *Designs, Codes and Cryptography*, vol. 39, no. 3, pp. 347–373, 2006.

[38] A. J. Menezes and Y.-H. Wu, "The discrete logarithm problem in GL (n, q)," *Ars Combinatoria*, vol. 47, pp. 23–32, 1997.