On the conjugacy search problem and left conjugacy closed loops

Juha Partala and Tapio Seppänen

Department of Electrical and Information Engineering
University of Oulu, Finland
Tel.: +358-8-5532536, Fax: +358-8-5532612,
Juha Partala, juha.partala@ee.oulu.fi,
Tapio Seppänen, tapio.seppanen@ee.oulu.fi

Abstract. The conjugacy search problem (CSP) is used as a primitive in several braid group based public key encryption schemes. It has been pointed out that, in braid groups, it unlikely provides adequate security. Therefore, new structures need to be found. In this paper, we give a formulation of the CSP for left conjugacy closed loops. In order to construct a generalization of the Anshel-Anshel-Goldfeld key establishment method, we also define a partial conjugacy search problem PCSP and show it to be equivalent to the CSP, if the underlying structure is a group. We also study closer the PCSP in a class of conjugacy closed loops of order p^2, where p is a prime.

Keywords: Conjugacy search, Conjugacy problem, Non-associative, Cryptography, Key exchange

Published in: Partala J. & Seppänen T. (2008), On the conjugacy search problem and left conjugacy closed loops, Applicable Algebra in Engineering, Communication and Computing 19(4): 311-322. The original publication is available at www.springerlink.com. DOI: 10.1007/s00200-008-0066-0

1 Introduction

Non-associative structures, such as quasigroups and loops, have not been extensively used in cryptographic applications. Some applications can be found, for example, in [12, 14, 15]. Modern public key cryptography is based on hard number theoretic problems as well as the structural theory of groups. Similar structural theory has not been available for the generalized, non-associative, case. As pointed out in [16], there probably are not any interesting structural results about the class of all loops. One has to restrict the study into a specific class. Recently, many interesting results have been obtained for the subclass of conjugacy closed loops. The potential of such loops for cryptography has been suggested by Drápal in his doctoral thesis. Especially recent results concerning constructions of such loops [6–8] provide tools for an instantiation of a key exchange protocol as well as a cryptosystem. The purpose of this paper is to generalize the conjugacy search problem for left conjugacy closed loops and to start a study of its hardness and suitability for key exchange protocols and public key encryption.

Recently, there has been great progress in solving the CSP in braid groups [10], and it has become a prevalent opinion in the scientific community that it unlikely offers adequate security for practical encryption [21, 23]. Therefore, it makes sense to search for different types of structures with potentially harder CSPs. By generalizing the CSP into non-associative structures, we get a broader class of candidates for the underlying structure. We can also show that in some sense the CSP is harder, if a non-associative structure is used.

In this paper, we replay the definition of left conjugacy closed loops and give cryptographically relevant results related to them. We also give references to methods of constructing these loops. Hopefully these can be used for further research on this topic. In order to generalize the key establishment method of Anshel, Anshel and Goldfeld [2] to left conjugacy closed loops, we define a partial version of the CSP, PCSP. We show it to be equivalent to CSP, if the underlying structure is a group. We also asses the hardness of the PCSP in conjugacy closed loops of order p^2, where p is a prime, and show that solving it is equivalent to solving a quadratic equation of n variables $u_1, u_2, \ldots, u_n$ of type

$$bp(u_1^2 + u_2^2 + \cdots + u_n^2 - b(u_1 + u_2 + \cdots + u_n)) + b = c,$$

where $u_1, u_2, \ldots, u_n, b, c \in \mathbb{Z}_{p^2}$.

2 Conjugacy closed loops

Let Q be a non-empty set and $\cdot$ a binary operation on Q. Then $(Q, \cdot)$ is a *quasigroup*, if and only if for every ordered pair $(a, b) \in Q^2$ equations

$$x \cdot a = b, \qquad a \cdot y = b \tag{1}$$

have unique solutions $x, y \in Q$. These solutions are often expressed as $x = b/a$ and $y = a \backslash b$. An equivalent definition is sometimes given using *translation mappings*. These are functions $L_a, R_a : Q \to Q$, where $a \in Q$, $L_a(x) = a \cdot x$ and $R_a(x) = x \cdot a$. It is easily seen that $(Q, \cdot)$ is a quasigroup if and only if the translation mappings L_a and R_a are bijections for every $a \in Q$.

Usually the application of a function f to an element x is denoted as xf. In the following, the same convention [20, 16] is used. In this case, function compositions are worked out from left to right. That is, for example, $xL_aL_b = L_b(L_a(x))$. A loop is a quasigroup which has an identity element e satisfying $e \cdot a = a \cdot e = a$ for every element a of the quasigroup.

Example 1. Let $Q = \{1, 2, 3, 4, 5\}$, and let $*$ be given by

*	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	5	1	2	4
4	4	3	5	1	2
5	5	4	3	2	1

Clearly translation mappings are bijections and $(Q,*)$ is a quasigroup. In addition, 1 is the identity element and $(Q,*)$ is a loop. It is not associative since

$$3*(2*2) = 3*1 = 3 \neq (3*2)*2 = 5*2 = 4.\square$$

Left and right translations are permutations on Q and they generate a subgroup of $\mathrm{Sym}(Q)$. The group generated by left translations,

$$\mathscr{L} = \langle L_a : a \in Q \rangle,$$

is called *the left multiplication group*. Similarly, the group generated by right translations is denoted by $\mathscr{R}$ and is called *the right multiplication group*. Together they generate the multiplication group of Q.

If G is a group, then $xL_bL_a = a(bx) = (ab)x = xL_{ab}$ and $\{L_a : a \in G\}$ is closed under composition. Using the left regular representation of G, it is seen that $G \cong \mathscr{L}$. If Q is a non-associative loop, then $\{L_a : a \in Q\}$ is not closed under composition. A similar law can be formulated using conjugation. A loop Q is *left conjugacy closed* (LCC), if and only if

$$L_x^{-1}L_yL_x = L_{(xy)/x}$$

for every $x,y \in Q$. The property is called *the left conjugacy law* and it asserts that the set of left translations is closed under conjugation. An identical identity can be formulated for right translations with $R_x^{-1}R_yR_x = R_{x\backslash(yx)}$ for every $x,y \in Q$. In this case the loop is called right conjugacy closed (RCC). If the loop satisfies both of these properties, then it is called conjugacy closed (CC).

Example 2. The multiplication table of the only non-group CC-loop of order 6 [16].

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	1	5	6	4
3	3	1	2	6	4	5
4	4	6	5	2	1	3
5	5	4	6	3	2	1
6	6	5	4	1	3	2

The following easy theorem is useful to us.

Theorem 1. *Let Q be a left conjugacy closed loop. Let also α be a composition of left translations and $L_g \in \mathscr{L}$. Then $\alpha^{-1}L_g\alpha = L_c$ for some $c \in Q$.*

Proof. Let

$$\alpha = L_{a_1}L_{a_2}\cdots L_{a_n},$$

where $a_i \in Q$, for every $0 \leq i \leq n$. We proceed with induction on n. Since Q is left conjugacy closed,

$$L_{a_1}^{-1}L_gL_{a_1} = L_{(a_1g)/a_1},$$

and the claim is true for $n = 1$. Suppose that the claim is true for $n \leq k-1$, and let $\beta = L_{a_1}L_{a_2}\cdots L_{a_{k-1}}$ and $\alpha = \beta L_{a_k} = L_{a_1}L_{a_2}\cdots L_{a_k}$. Now,

$$\beta^{-1}L_g\beta = L_d$$

for some $d \in Q$, and

$$\alpha^{-1}L_g\alpha = (\beta L_{a_k})^{-1}L_g(\beta L_{a_k}) = L_{a_k}^{-1}\beta^{-1}L_g\beta L_{a_k} = L_{a_k}^{-1}L_dL_{a_k} = L_{(a_kd)/a_k},$$

which proves our claim. □

In [6, 8] the authors construct left conjugacy closed loops from an abelian group G using a zero preserving and right additive mapping b. Let $(G,+)$ and $(R,+)$ be abelian groups and $b : G \times G \to R$. The subgroup

$$\mathrm{Rad}\,(b) = \{u \in G : b(x+u,y) = b(x,y) = b(x,u+y) \text{ for every } x,y \in G\}$$

is called *the radical* of b. Mapping b is called zero preserving if $b(x,0) = b(0,x) = 0$ for every $x \in G$. If $b(x,y+z) = b(x,y) + b(x,z)$ for all $x,y,z \in G$, then b is called additive on the right. Similarily, b is additive on the left, if $b(x+y,z) = b(x,z) + b(y,z)$ for all $x,y,z \in G$. If b is both left and right additive, then it is called biadditive. The construction is based on the following theorem [6, 8].

Theorem 2. *Let G be an abelian group with a subgroup R. Let $b : G \times G \to R$ be a zero preserving mapping with* $\mathrm{Rad}\,(b) \geq R$ *that is additive on the right. Then*

$$x \cdot y = x + y + b(x,y)$$

defines on G a left conjugacy closed loop.

The loop induced by G and b in this way is denoted by $G[b] = G[b(x,y)]$. In [6] it is also shown that, if b is biadditive, then the loop is a group. It is conjugacy closed, if and only if

$$b(x+y,z) - b(x,z) - b(y,z) = b(x+z,y) - b(x,y) - b(z,y)$$

for all $x,y,z \in G$. It is also pointed out in [7], that b can be induced by a triadditive mapping $f : G \times G \times G \to G$ with

$$f(x,y,z) = b(x+y,z) - b(x,z) - b(y,z) \tag{2}$$

for every $x,y,z \in G$. If f is symmetric, then Q is a CC-loop. The following theorem is a reformulation of a part of lemma 6.3 in [7].

Theorem 3. *Let V be a finite vector space over a prime field F with $|F| \geq 3$, and let $f : V \times V \times V \to F$ be a trilinear form with $f(u,v,w) = f(v,u,w)$ for all $u,v,w \in V$. Then*

$$b(u,v) = \frac{1}{2}f(u,u,v)$$

is zero preserving, right linear, and satisfies

$$f(u,v,w) = b(u+v,w) - b(u,w) - b(v,w).$$

This theorem allows us to construct CC-loops $V(b)$ from a vector space V over a prime field using a symmetric trilinear form f.

3 The conjugacy search problem

Assume that G is a group and $b,c \in G$ are conjugate. The conjugacy search problem (CSP) is to find an element a such that

$$a^{-1}ba = c. \tag{3}$$

This problem has been mainly utilized as a cryptographic primitive in braid group based systems as suggested in [2, 1] and in [13]. Unfortunately, there are several successful attacks on these systems on braid groups [18, 17, 5, 11].

If Q is a loop, then in general $a^{-1}(ba) \neq (a^{-1}b)a$, but we can formulate the same problem in the left multiplication group. In this case, given conjugates $\beta,\gamma \in \mathscr{L}$, the problem is to find an element $\alpha \in \mathscr{L}$, such that

$$\alpha^{-1}\beta\alpha = \gamma.$$

It should be noted that α,β,γ are not necessarily left translations, since they can be arbitrary permutations from the left multiplication group $\mathscr{L}$.

We will restrict ourselves to the case where Q is left conjugacy closed, $\beta = L_b, \gamma = L_c$ and $\alpha = L_{u_1}L_{u_2}\cdots L_{u_n}$ is a composition of left translation as in theorem 1. In this case, the problem is to find $\alpha \in \mathscr{L}$ such that

$$\alpha^{-1}L_b\alpha = L_c,$$

given $b,c \in Q$. We shall denote this restricted version of the CSP by PCSP. Our definition is useful in the sense that L_b and L_c can be represented by single loop elements $b,c \in Q$ and α can be represented as an ordered n-tuple of loop elements $(u_1,u_2,\ldots,u_n)$.

Theorem 4. *If G is a group, then the PCSP is equivalent to the CSP.*

Proof. Suppose that we have an instance of PCSP,

$$\alpha^{-1}\beta\alpha = \gamma,$$

in the left multiplication group of a group G. Now, $\mathscr{L}$ is isomorphic to G by the left regular representation. Let φ denote this isomorphism $\mathscr{L} \to G$. Now, for every $\alpha,\beta,\gamma \in \mathscr{L}$, there are $a,b,c \in G$ such that $\varphi(\alpha) = a, \varphi(\beta) = b$ and $\varphi(\gamma) = c$, and

$$\alpha^{-1}\beta\alpha = \gamma$$

in $\mathscr{L}$, if and only if

$$a^{-1}ba = c$$

in G.

Conversely, suppose that we have an instance of CSP, $a^{-1}ba = c$, in G. By the isomorphism φ^{-1}, there is an instance of CSP, $\alpha^{-1}\beta\alpha = \gamma$, in $\mathscr{L}$. It remains to be shown that α,β,γ are of the right type. Now, since G is associative, the set of left translations is closed under composition. That is,

$$\mathscr{L} = \{L_g : g \in G\}.$$

Therefore, $\alpha = L_u, \beta = L_v, \gamma = L_w$ for some $u,v,w \in G$. □

If Q is a non-associative loop, then the set of left translations cannot be closed under composition. That is, there exists at least one element of $\mathscr{L}$ that is not a left translation. This means that, as sets, $\{L_a : a \in Q\} \subsetneq \mathscr{L}$, whereas $\{L_a : a \in G\} = \mathscr{L}$, if G is a group. That is, if Q is non-associative, we have a greater number of candidates for the solution of PCSP. In this sense the PCSP is harder, if a non-associative loop is used.

In order to construct a secure key negotiation scheme, the restricted conjugacy search problem has to be hard in the left multiplication group of the particular loop. We know that there are loops in which, to the best of our knowledge, the problem cannot be solved in polynomial time. For example, the braid groups are loops in which the best known bound for time complexity is exponential [9]. However, there are conjectures on polynomial bounds as well as results that suggest that braid based cryptographic protocols are insecure [10]. Our motivation is to find different and more secure structures. Especially we would be interested in finding non-associative loops that give us a completely differently structured PCSP that renders ultra summit set based algorithms inapplicable.

If the constructions of theorems 2 and 3 are used, the essential part in the generation of a hard PCSP is the mapping b (or f). It characterizes the conjugation operation, as the loop is constructed from an abelian group G, in which it does not even make sense to speak of conjugation. In terms of these constructions, it suffices to study different functions b, and the PCSP they generate on $\mathscr{L}$. Basically, this amounts to finding such functions that the corresponding conjugacy equations on G are hard to solve.

As the PCSP has not been previously studied in non-associative structures, it seems sensible to start our investigation from the simplest odd order CC-loops: namely those that have simple G, R and b. The loops in the following section are constructed from the cyclic group $\mathbb{Z}_p$ and have an order of p^2, where p is a prime.

3.1 PCSP in conjugacy closed loops of order p^2

Let p be a prime. There are, up to isomorphism, exactly three non-associative conjugacy closed loops of order p^2 [16]. Using the construction in theorem 2, the authors in [6] obtain the following formulas for these loops:

$$\begin{aligned} (x,y)\cdot(u,v) &= (x+y, u+v+x^2y), \\ x\cdot y &= x+y+px^2y, \\ x\cdot y &= x+y+\kappa px^2y, \end{aligned} \tag{4}$$

where $\kappa \in \mathbb{Z}_p$ is a nonsquare. We will study closer the loop with the second identity, and shall denote it by Q. In this case, for the construction in theorem 2, we choose $G = \mathbb{Z}_p$, $R = G$ and $b(x,y) = px^2y$. Now, b satisfies

$$b(x+y,z) - b(x,z) - b(y,z) = b(x+z,y) - b(x,y) - b(z,y)$$

for all $x, y, z \in \mathbb{Z}_p$ and the resulting loop is conjugacy closed.

A left translation L_a is given by

$$xL_a = ax = a + x + pa^2x, \tag{5}$$

and its inverse is

$$yL_a^{-1} = a\backslash y = (y-a)(1+pa^2)^{-1}, \tag{6}$$

where the computations are done modulo p^2.

Let $\alpha = L_a$, and let $b \in Q$. Now,

$$\alpha^{-1} L_b \alpha = L_a^{-1} L_b L_a = L_{(ab)/a}.$$

By observing that

$$0L_a^{-1} L_b L_a = 0L_{(ab)/a} = (ab)/a \cdot 0 = (ab)/a,$$

and using (5) and (6), we get that

$$(ab)/a = (pa^2 - pba + 1)b. \tag{7}$$

The problem of solving the PCSP for a single left translation is equivalent to finding a given b and $(pa^2 - pba + 1)b$ in $\mathbb{Z}_{p^2}$. Suppose now, that α comprises of n left translations. Then, we can show that the following theorem holds:

Theorem 5. *Let*

$$\alpha = L_{u_1} L_{u_2} \cdots L_{u_n},$$

where $n \geq 1$, and $u_i \in \mathbb{Z}_{p^2}$ for all $1 \leq i \leq n$. Then

$$c = 0\alpha^{-1} L_b \alpha = bp(u_1^2 + u_2^2 + \cdots + u_n^2 - b(u_1 + u_2 + \cdots + u_n)) + b. \tag{8}$$

Proof. We proceed with induction on n. The case $n = 1$ is true according to (7). Suppose that the claim is true for $n \leq k-1$. That is,

$$(L_{u_1} L_{u_2} \cdots L_{u_{k-1}})^{-1} L_b (L_{u_1} L_{u_2} \cdots L_{u_{k-1}}) = L_d,$$

where

$$d = bp(u_1^2 + u_2^2 + \cdots + u_{k-1}^2 - b(u_1 + u_2 + \cdots + u_{k-1})) + b.$$

Now

$$0L_{u_k}^{-1} L_d L_{u_k} = (u_k d)/u_k = (pu_k^2 - pdu_k + 1)b$$

by (7). Substituting for d and simplifying,

$$(u_k d)/u_k = bp(u_1^2 + u_2^2 + \cdots + u_k^2 - b(u_1 + u_2 + \cdots + u_k)) + b. \square$$

It is easily seen, that solving the PCSP is equivalent to finding n and solving (8) for $u_1, u_2, \ldots, u_n$ knowing b and $c = 0\alpha^{-1} L_b \alpha$. We cannot easily see a method of figuring out n for (8) simply from b and c.

4 Generalization of the Anshel-Anshel-Goldfeld key establishment method

In [2] the authors suggest a construction of a group based two-party key establishment method using the conjugacy search problem. The method has been instantiated using braid groups [1]. Let us assume that there are two principals, A and B, who wish to communicate with each other. Let A be the initiator. The construction can be generally described, ignoring security notions, as follows.

Let G be a group and

$$S_A = \langle a_1, a_2, \ldots, a_s \rangle, \quad S_B = \langle b_1, b_2, \ldots, b_t \rangle$$

be two publicly assigned subgroups. Users A and B choose secret elements $a \in S_A$ and $b \in S_B$, respectively, by multiplying a finite number of generators. A computes and transmits elements

$$a^{-1}b_1a, a^{-1}b_2a, \ldots, a^{-1}b_ta$$

to B. B computes and replies with elements

$$b^{-1}a_1b, b^{-1}a_2b, \ldots, b^{-1}a_sb.$$

Now, A and B can obtain $b^{-1}ab$ and $a^{-1}ba$, respectively, and the common secret key is

$$k_{AB} = a^{-1}b^{-1}ab = [a,b],$$

which is the commutator of a and b.

We shall give a simple general construction of the Anshel-Anshel-Goldfeld scheme in a left conjugacy closed loop using $\mathscr{L}$. If the loop is a group G, then the construction is identical to the one given by Anshel et al. This is again easily seen due to the isomorphism between G and $\mathscr{L}$. In this view, the construction can be regarded as a generalization of the CSP based construction of [2] to left conjugacy closed loops.

Let us assume that we have a left conjugacy closed loop Q with a hard conjugacy search problem on the left multiplication group $\mathscr{L}$ of Q. Let

$$\mathscr{L}_A = \langle L_{a_1}, L_{a_2}, \ldots, L_{a_s} \rangle, \quad \mathscr{L}_B = \langle L_{b_1}, L_{b_2}, \ldots, L_{b_t} \rangle$$

be publicly chosen subgroups of $\mathscr{L}$. Now A and B choose, respectively, elements $\alpha \in \mathscr{L}_A$ and $\beta \in \mathscr{L}_B$ by multiplying a finite number of generators. A computes

$$\alpha^{-1}L_{b_1}\alpha, \alpha^{-1}L_{b_2}\alpha, \ldots, \alpha^{-1}L_{b_t}\alpha$$

and transmits them to B. According to theorem 1, these are left translations for every b_i and can be represented by some loop elements $c_1, c_2, \ldots, c_t \in Q$. Similarily, B computes

$$\beta^{-1}L_{a_1}\beta, \beta^{-1}L_{a_2}\beta, \ldots, \beta^{-1}L_{a_s}\beta$$

and replies with the representing elements. The common secret key is

$$K_{AB} = \alpha^{-1}\beta^{-1}\alpha\beta = [\alpha,\beta].$$

If the underlying structure is a group G, the secret key is always a left translation with an element $g \in G$. That is, the principals are in possession of a shared secret element g. This is not the case with a non-associative left conjugacy closed loop, because the set of left translations is not closed under composition. Instead, A and B now hold a shared secret bijection on Q which cannot be deduced by the adversary provided that the PCSP is hard on $\mathscr{L}$.

Basically we are applying the Anshel-Anshel-Goldfeld protocol with a restricted version of the CSP in the group $\mathscr{L}$. It would be possible to apply the original protocol with CSP by forgetting Q and working with a group $G \cong \mathscr{L}$. However, representation of the elements would be complex as $\mathscr{L}$ is a group of permutations. By restricting ourselves to PCSP, we can select the representing elements $a_1, a_2, \ldots, a_s$ and $b_1, b_2, \ldots, b_t$ of the left translations from Q instead of arbitrary permutations from $\mathscr{L}$.

In [22], the authors have studied the conjugacy search problem and its usage in key exchange protocols. In the case of the Anshel-Anshel-Goldfeld protocol, it is not sufficient for the adversary to solve the (P)CSP in order to get the common key. Using the notation of this section, the adversary would also have to find an expression for the mappings α, β as a word in $L_{a_1}, L_{a_2}, \ldots, L_{a_s}$ and $L_{b_1} L_{b_2}, \ldots, L_{b_t}$. In a particular loop, this could be a hard problem in itself. One could also study such conjugacy closed loops Q that have a left multiplication group that can be generated with only a few elements. If, for example,

$$\mathscr{L} = \langle L_{a_1}, L_{a_2}, \ldots, L_{a_s} \rangle$$

and $s \in \mathbb{N}$ is relatively small, then no subgroups $\mathscr{L}_A$ and $\mathscr{L}_B$ need to be chosen.

For practical encryption, issues like parallel protocol execution, authentication and malicious insiders need to be addressed. Cryptographic protocols based on non-commutative group theory have not been constructed under an established cryptographic framework of provable security [3]. The field seems to be currently under investigation and several promising constructions for non-abelian groups have appeared [3, 4]. These constructions can be extended for left conjugacy closed loops as $\mathscr{L}$ is a non-abelian group. These hopefully allow constructions of provably secure key-agreement protocols and IND-CCA provably secure cryptosystems.

It is emphasized that research is needed to find suitable loops. The crucial point is the conjugacy search problem. In the case of a conjugacy closed loop of order p^2, the following observations can be made. Suppose that the adversary knows the elements $b_1, b_2, \ldots, b_t$, and the corresponding elements $c_1, c_2, \ldots, c_t$, where

$$L_{c_i} = \alpha^{-1} L_{b_i} \alpha.$$

Then, in order to find α – that is, to solve the system of restricted conjugacy equations – the adversary has to solve a system of t quadratic equations of type (8) in $\mathbb{Z}_{p^2}$ with an unknown n. In general, the problem of solving systems of multivariate quadratic equations over finite fields is known to be NP-complete [19]. Of course, $\mathbb{Z}_{p^2}$ is not a field and in our case the equations are all of a specific type. Nevertheless, we cannot easily see a method of figuring out n only by observing the values of $c_i, i = 1, 2, ..., t$. If the adversary does not know such a method, then she has to solve the systems of equations for $n \geq 1$ until the right n and thus the right α are found. In this case, time complexity of such a procedure is exponential in the size of $\mathscr{L}_A$.

If the loop is constructed from an abelian group that does not constitute a field, then the adversary would have to solve a set of equations in the corresponding $\mathbb{Z}$-module without the additional field axioms. This could enable complicated loops to be more useful compared to the one in section 3.1 in terms of the hardness of the PCSP. Even if the loops of order p^2 are not satisfactory in terms of hardness of the PCSP, they hopefully pave way for more sophisticated structures.

References

1. Anshel, I., Anshel, M., Fisher, B., Goldfeld, D.: New key agreement protocols in braid group cryptography. In: Topics in cryptology—CT-RSA 2001 (San Francisco, CA), *Lecture Notes in Comput. Sci.*, vol. 2020, pp. 13–27. Springer, Berlin (2001)
2. Anshel, I., Anshel, M., Goldfeld, D.: An algebraic method for public-key cryptography. Math. Res. Lett. **6**(3-4), 287–291 (1999)
3. Bohli, J.M., Glas, B., Steinwandt, R.: Towards provably secure group key agreement building on group theory. In: Progress in Cryptology—VIETCRYPT 2006, *Lecture Notes in Comput. Sci.*, vol. 4341, pp. 322–336. Springer (2006)
4. Bohli, J.M., Vasco, M.I.G., Steinwandt, R.: Secure group key establishment revisited. Int. J. Inf. Secur. **6**(4), 243–254 (2007). DOI http://dx.doi.org/10.1007/s10207-007-0018-x
5. Cheon, J.H., Jun, B.: A polynomial time algorithm for the braid Diffie-Hellman conjugacy problem. In: Advances in cryptology—CRYPTO 2003, *Lecture Notes in Comput. Sci.*, vol. 2729, pp. 212–225. Springer, Berlin (2003)
6. Csörgő, P., Drápal, A.: Left conjugacy closed loops of nilpotency class two. Results Math. **47**(3-4), 242–265 (2005)
7. Csörgő, P., Drápal, A.: On left conjugacy closed loops in which the left multiplication group is normal. Abh. Math. Sem. Univ. Hamburg **76**, 17–34 (2006)
8. Drápal, A.: On extraspecial left conjugacy closed loops. J. Algebra **302**(2), 771–792 (2006)
9. Gebhardt, V.: A new approach to the conjugacy problem in Garside groups. J. Algebra **292**(1), 282–302 (2005)
10. Gebhardt, V.: Conjugacy search in braid groups: from a braid-based cryptography point of view. Appl. Algebra Engrg. Comm. Comput. **17**(3-4), 219–238 (2006)
11. Hofheinz, D., Steinwandt, R.: A practical attack on some braid group based cryptographic primitives. In: Public key cryptography—PKC 2003, *Lecture Notes in Comput. Sci.*, vol. 2567, pp. 187–198. Springer, Berlin (2002)
12. Keedwell, A.D.: Construction, properties and applications of finite neofields. Comment. Math. Univ. Carolin. **41**(2), 283–297 (2000). Loops'99 (Prague)
13. Ko, K.H., Lee, S.J., Cheon, J.H., Han, J.W., Kang, J.s., Park, C.: New public-key cryptosystem using braid groups. In: Advances in cryptology—CRYPTO 2000 (Santa Barbara, CA), *Lecture Notes in Comput. Sci.*, vol. 1880, pp. 166–183. Springer, Berlin (2000)
14. Kościelny, C.: NLPN sequences over GF(q). Quasigroups Related Systems **4**, 89–102 (1999) (1997)
15. Kościelny, C.: Generating quasigroups for cryptographic applications. Int. J. Appl. Math. Comput. Sci. **12**(4), 559–569 (2002)
16. Kunen, K.: The structure of conjugacy closed loops. Trans. Amer. Math. Soc. **352**(6), 2889–2911 (2000)
17. Lee, E., Park, J.H.: Cryptanalysis of the public-key encryption based on braid groups. In: Advances in cryptology—EUROCRYPT 2003, *Lecture Notes in Comput. Sci.*, vol. 2656, pp. 477–490. Springer, Berlin (2003)

18. Lee, S.J., Lee, E.: Potential weaknesses of the commutator key agreement protocol based on braid groups. In: Advances in cryptology—EUROCRYPT 2002 (Amsterdam), *Lecture Notes in Comput. Sci.*, vol. 2332, pp. 14–28. Springer, Berlin (2002)
19. Patarin, J., Goubin, L.: Trapdoor one-way permutations and multivariate polynomials. In: International Conference on Information Security and Cryptology, *Lecture Notes in Comput. Sci.*, vol. 1334, pp. 356–368. Springer, Berlin (1997)
20. Pflugfelder, H.O.: Quasigroups and loops: introduction, *Sigma Series in Pure Mathematics*, vol. 7. Heldermann Verlag, Berlin (1990)
21. Shpilrain, V.: Assessing security of some group based cryptosystems. In: Group theory, statistics, and cryptography, *Contemp. Math.*, vol. 360, pp. 167–177. Amer. Math. Soc., Providence, RI (2004)
22. Shpilrain, V., Ushakov, A.: The conjugacy search problem in public key cryptography: unnecessary and insufficient. Appl. Algebra Engrg. Comm. Comput. **17**(3-4), 285–289 (2006)
23. Shpilrain, V., Zapata, G.: Combinatorial group theory and public key cryptography. Appl. Algebra Engrg. Comm. Comput. **17**(3-4), 291–302 (2006)