Computer Science Journal of Moldova, vol.**23**, no.3(69), 2015

Probability on groups and an application to cryptography *

Sidoine Djimnaibeye, Daniel Tieudjo†, Norbert Youmbi

Abstract

In her thesis, Mosina introduced the concept of *mean-set of random (graph-) group-variables* and generalized Strong Law of Large Numbers (SLLN) to (graphs) groups, which she used for cryptanalysis of authentication schemes. This attack called the *mean-set attack* is presented here. It allows to break the Sibert authentication scheme on braid groups without solving the underlined difficult problem. We propose an amelioration to this attack and its implementation on the platform CRAG. We carry some experiments and we present the results. These results are discussed and they confirm those obtained by Mosina and Ushakov with a considerable gain of time.

Keywords: Braid group, Authentication protocol, Probability on groups, Mean-set attack, CRAG.

2010 Mathematics Subject Classification: primary 20F36, 60B15, secondary 14G50.

1 Introduction

During these last years, several cryptosystems among which the authentication schemes based on difficult problems in braid groups were proposed. Indeed, Sibert and *al.* [21] presented authentication schemes based on the conjugacy problem, the Diffie-Helmann-type conjugacy problem, the root problem; in [3], Dehornoy designed an authentication scheme using the shifted conjugacy problem; Lal and Chaturvedi

*This work was completed at Saint Francis University (Loretto, PA, USA) during the second author's visit thanks to the Fulbright Program. Saint Francis University and the Fulbright Scholar Program are gratefully acknowledged.

proposed in [8] two authentication schemes presumably based on the difficulty of the root problem; Shpilrain and Ushakov also offered in [20] an authentication scheme whose security is based on the hardness of the twisted conjugacy search problem, etc. The security of these authentication schemes relies on the difficulty to solve the underlined algorithmic problems. So, the robustness of these schemes is ensured by their resistance to the known cryptanalysis methods. Several methods to attack the authentication schemes were suggested in the literature [5, 6, 9, 10, 11, 23]. Mostly, these methods try to solve the difficult problem used to design the scheme.

In 2009 in her thesis, Natalia Mosina presented a new probabilistic approach to prove the vulnerability of the authentication protocols on the braid groups [14, 15, 16] without solving the underlying problem. So, given a group G with a probability measure induced by random G-variables, Mosina defined the mean-set of random G-elements. She stated and proved the Strong Law of Large Numbers (SLLN) on G, and gave an algorithm to compute the mean-set of a sequence of independent and identically distributed (i.i.d.) random G-variables. Using these tools, she developed an approach called *mean-set attack* that breaks the Sibert and *al.* authentication scheme, without solving the difficult problem used to design the protocol. She then implemented the attack and carried some experiments on the n-string braid group B_n with the software package CRAG. In her approach, Mosina considered the relative frequency as the probability distribution on the group B_n. However in [21], Sibert and *al.* suggested the use of the uniform law to generate the braids and the bits in the authentication protocol.

In this work, we present the Mosina's probabilistic approach and a restricted form which uses the uniform law. We derive a simplified mean-set attack algorithm that we implement on CRAG. We perform a series of experiments and discuss the results obtained. We see that they confirm those obtained by Mosina with a considerable gain of time.

2 Probability on groups

2.1 Mean set of a random G-variable

Let $G = \langle X \rangle$ be the group generated by a non empty set X. Let $C_G(X)$ be the Cayley graph associated to G. Let $(\Omega, \mathcal{F}, P)$ be a probability space and $\xi : \Omega \to G$ a random G-variable.

- A *probability distribution* is a function $\mu : G \to [0,1]$ on ξ such that:

$$\mu(g) = \mu_\xi(g) = P(\{\omega \in \Omega \mid \xi(\omega) = g\}, g \in G);$$

- The *weight function* is the function $M_\xi : G \to \mathbb{R}$ defined by

$$M_\xi(g) = \sum_{s \in G} d^2(g,s)\mu(s),$$

  where $d(g,s)$ is the distance between g and s in the Cayley graph $C_G(X)$ of G.

- The domain $domain(M)$ of the weight function M is defined by:

$$domain(M) = \left\{ g \in G \mid \sum_{s \in G} d^2(g,s)\mu(s) < \infty \right\}.$$

The weight function M_ξ is *totally defined* if for all vertices $g \in G$, $M_\xi(g) < \infty$ i.e. $domain(M) = G$.

Definition 2.1. *Let ξ be a random G-variable such that $M_\xi(\cdot)$ is totally defined. The set $\mathbb{E}(\xi)$ of vertices $g \in G$ having the smallest value of M_ξ i.e.*

$$\mathbb{E}(\xi) = \{g \in G : M_\xi(g) \leq M_\xi(u), \forall u \in G\}$$

is called mean-set of ξ.

Since $d(a,b) = d(ga, gb)$ for all a, b, $g \in G$ we have:

Proposition 2.1 (Shift Property)**.** Let $G = \langle X \rangle$ be the group generated by a non empty set X and let $g \in G$. Suppose $(\Omega, \mathcal{F}, P)$ is a probability space and let $\xi : \Omega \to G$ be a random G-variable on Ω. Then ξ_g defined by $\xi_g(\omega) = g\xi(\omega)$ is a random G-variable and we have $\mathbb{E}(\xi_g) = g\mathbb{E}(\xi)$.

2.2 The Strong Law of Large Numbers (SLLN)

Definition 2.2. *Let $\xi_1, \ldots, \xi_n$ be a sequence of i.i.d. random G-variables with $\xi_i : \Omega \to G$ defined on a probability space $(\Omega, \mathcal{F}, P)$.*

- *The relative frequency*

$$\mu_n(g) = \mu_n(g, \omega) = \frac{|\{i \mid \xi_i(\omega) = g, 1 \leq i \leq n\}|}{n}$$

  is the probability with which g occurs in the random sample $\xi_1, \ldots, \xi_n$. μ_n defines a probability distribution on G.

- *The sampling weight function is the function $M_n : G \to \mathbb{R}$ defined by*

$$M_n(g) = \sum_{s \in G} d^2(g, s)\mu_n(s),$$

  where $d(g, s)$ is the distance between g and s in the Cayley graph $C_G(X)$ of G.

- *The sample mean-set of $\xi_1, \ldots, \xi_n$ is the set $\mathbb{S}_n$ defined by*

$$\mathbb{S}_n = \mathbb{S}(\xi_1, \ldots, \xi_n) = \{g \in G : M_n(g) \leq M_n(u), \forall u \in G\}.$$

We now state the SLLN generalized to graphs and groups which shows the convergence of the sample mean-set $\mathbb{S}_n$ to the mean-set $\mathbb{E}(\xi)$ when $n \to \infty$.

Theorem 2.1. *Let $G = \langle X \rangle$ be the group generated by a non empty set X, where its associated Cayley graph $C_G(X)$ is connected and locally finite. Let $\{\xi_i\}_{i=1}^{\infty}$ be a sequence of i.i.d. random G-variables. If the*

weight function $M_{\xi_1}(\cdot)$ *is totally defined and* $\mathbb{E}(\xi_1) = \{g\}$ *for some vertex* $g \in G$*, then*

$$\lim_{n\to\infty} \mathbb{S}(\xi_1, \ldots, \xi_n) = \mathbb{E}(\xi_1)$$

with probability 1*.*

For more details, see [14, 15].

Let $G = \langle X \rangle$ be a group and $G_1 = \{g_1, \ldots, g_n\}$ be a subset of group G with cardinality n. In [16], the following polynomial algorithm to compute the mean-set of G_1 is described.

Algorithm 2.1. ***Computation of the mean-set in a group***
INPUT: *the group* G *by its set* X *of generators and a subset* $G_1 = \{g_1, ..., g_n\}$ *of* G*.*
OUTPUT: *An element* g *of* G *having the smallest weight function.*
COMPUTATIONS:

A. Choose a random element $g \in G$ *according to some probability measure* μ *on* G*.*

B. If for every $x \in X^{\pm 1}, M_n(g) \leq M_n(gx)$*, then output* g*.*

C. Otherwise put $g \leftarrow gx$*, where* $x \in X^{\pm 1}$ *is an element minimizing the value of* $M_n(gx)$ *and go to step B.*

The computation of $\mathbb{S}_n$, the mean-set of the sample G_1, poses some problems:

- The computation of the set $\{M(g) : g \in G\}$ requires at least $O(|G_1|^2)$ elementary operations. This computation is practically impossible when n is too large;
- The computation of the distance function $d(\cdot, \cdot)$ is difficult in some groups like the braid groups.

However, Algorithm 2.1 presented above allows to solve the first problem. Indeed, it is a direct descent heuristic algorithm and it computes the sample mean-set since the weight function M_n comes from a sequence of random elements of G_1. The second problem is the computation of the distance between two elements in G. An approximation of the computation of the distance is described in [12]. Although it does not guarantee an optimal solution, this approximation sometimes has been used in a series of attacks.

3 Cryptanalysis of the authentication protocol

We now present the probabilistic approach used by Mosina to attack an authentication protocol in the braid groups [16].

3.1 The Sibert and *al.* authentication protocol

The authentication is a procedure that permits the user to convince the interlocutor of its identity. So, it involves two parties: the Prover (user) and the Verifier (interlocutor). The Prover provides the purported identity to the Verifier, and then both the Prover and the Verifier should corroborate and act simultaneously such that the Verifier should be convinced of the identity of the Prover. Only the Prover knows the secret value corresponding to his public one, and it is the proper use of this secret value which allows to convince the Verifier of its identity.

For $n \geq 2$, the n-string braid group denoted B_n is the group with the following presentation:

$$B_n = \left\langle \sigma_1, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{c} \sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } |i-j| \geq 2 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \text{ for } |i-j| = 1 \end{array} \right\rangle. \qquad (1)$$

We present the Sibert and *al.* authentication protocol. The security level of this protocol is parametered by the size of the used braids and by the rank of the group B_n.

Protocol 3.1. *Let n be an integer, let b be a braid in B_n and let h be a hash function. b is written on its normal form or handle reduction form.*

Phase I. Keys generation
Private key: *Alice chooses a secret braid* $s \in B_n$
Public key: *Alice publishes* $(b, b^{'})$ *with* $b' = h(s^{-1}bs)$
Phase II. Authentication phase*: repeat* k *times*
Engagement: *Alice choses a random braid* r *and sends* $x = h(r^{-1}b'r)$ *to Bob;*
Challenge: *Bob sends a random bit* ϵ *to Alice;*
Answer:

- *If* $\epsilon = 0$*, Alice sends* $y = r$ *to Bob and Bob checks if* $x = h(y^{-1}b'y)$;
- *If* $\epsilon = 1$*, Alice sends* $y = h(sr)$ *to Bob and Bob checks if* $x = h(y^{-1}by)$.

3.2 Mean-set attack

In this section we present the mean-set attack on the protocol 3.1 described above (see also [16] or [14]).

3.2.1 Principle

If observe the Sibert and *al.* protocol 3.1, wee see that the Prover sends to the Verifier sequence of two types of random elements: r and sr, where r is a randomly generated element and s is the secret of the Prover. An Intruder (Eve) can intercept and arrange the answers of the challenges in a table similar to Table 1.

We obtain two sets R_0 and R_1 of elements, corresponding to $\epsilon = 0$ and $\epsilon = 1$ respectively. $R_0 = \{r_{i_1}, \ldots, r_{i_l}\}$ and $R_1 = \{sr_{j_1}, \ldots, sr_{j_t}\}$, where all the elements r_i $(i = 1, \ldots, k = l+t)$ are distributed according to a probability law μ. The objective of Eve is to retrieve the secret s using the intercepted sequences R_0 and R_1.

Suppose $G = \mathbb{Z}$. In this case, we write $R_1 = \{s+r_{j_1}, \ldots, s+r_{j_t}\}$, and we can compute the empirical average $\overline{r_0} = \frac{1}{l}\sum_{m=1}^{l} r_{i_m}$ of elements of $R_0 \subset \mathbb{Z}$ and the empirical average $\overline{r_1} = \frac{1}{t}\sum_{p=1}^{t}(s+r_{j_p}) = s+\frac{1}{t}\sum_{p=1}^{t} r_{j_p}$ of elements of $R_1 \subset \mathbb{Z}$. By the SLLN (Section 2.2, Theorem 2.1), if the

Table 1. Principle of the mean-set attack

Tour	Challenge	Answers type # 1	Answers type # 2
1	$\epsilon = 1$	–	sr_1
2	$\epsilon = 0$	r_2	–
3	$\epsilon = 0$	r_3	–
4	$\epsilon = 1$	–	sr_4
5	$\epsilon = 0$	r_5	–
...	...	...	...
k	$\epsilon = 0$	r_l	–

sequence R_0 is too large, then $\overline{r_0}$ tends to the mathematical expectation $\mathbb{E}(\mu)$ of the distribution μ in $\mathbb{Z}$. Similarly, if the sequence R_1 is too large, then $\overline{r_1}$ tends to $s + \mathbb{E}(\mu)$. Hence, by subtracting the limit of $\overline{r_0}$ to the limit of $\overline{r_1}$ we obtain an approximation of the secret s.

So, in this case, where $G = \mathbb{Z}$, we can compute the secret thanks to the following three properties:

(AV1) (SLLN for real-valued random variables): If $\{\xi_i\}_{i=1}^{\infty}$ is a sequence of real i.i.d. random variables and if $\mathbb{E}(\xi_1) < \infty$, then

$$\frac{1}{n}\sum_{i=1}^{n} \xi_i \to \mathbb{E}(\xi_1)$$

with probability 1 when $n \to \infty$.

(AV2) (Shift Property): For all real random variable ξ, we have

$$\mathbb{E}(c + \xi) = c + \mathbb{E}(\xi),$$

where c is a constant.

(AV3) (Efficient computation): The average $\frac{1}{n}\sum_{i=1}^{n} \xi_i$ is efficiently computable.

Now, this method can be generalized to some infinite groups where these three properties (AV1), (AV2) and (AV3) are defined similarly and are satisfied. Indeed let G be an infinite group.

- For a random G-variable $\xi : \Omega \to G$, define a set $\mathbb{E}(\xi) \subseteq G$ called *mean-set*;
- For a set of n random G-variables $\xi_1, \ldots, \xi_n$, define a set $\mathbb{S}_n = \mathbb{S}(\xi_1, \ldots, \xi_n) \subseteq G$ called the *sample mean-set* of $\xi_1, \ldots, \xi_n$.

Hence, we have the shift property $\mathbb{E}(s\xi) = s\mathbb{E}(\xi)$ and a generalization of the SLLN for groups in the sense that $\mathbb{S}(\xi_1, \ldots, \xi_n)$ converges to $\mathbb{E}(\xi_1)$ when $n \to \infty$, with probability 1. Moreover, suppose that the sample mean-set $\mathbb{S}(\xi_1, \ldots, \xi_n)$ is efficiently computable. Then Eve can form the sets $\mathbb{S}(sr_{j_1}, \ldots, sr_{j_{n-k}})$ and $\mathbb{S}(r_{i_1}, \ldots, r_{i_k})$ and compute

$$\mathbb{S}(sr_{j_1}, \ldots, sr_{j_{n-k}}) \cdot [\mathbb{S}(r_{i_1}, \ldots, r_{i_k})]^{-1},$$

which contains s with high probability when n is sufficiently large.

Below is the algorithm of the mean-set attack designed by Mosina.

3.2.2 Attack algorithm

Algorithm 3.1. The mean-set attack Algorithm
INPUT: *the Prover public key* (t, w) *and the sequences* R_0 *and* R_1;
OUTPUT: *an element* z *such that* $t = zwz^{-1}$ *or 'Failure'.*
COMPUTATION:

A. *Apply Algorithm 2.1 to* R_0 *and get* g_0.

B. *Apply Algorithm 2.1 to* R_1 *and get* g_1.

C. *If* $g_1 g_0^{-1}$ *satisfies* $t = (g_1 g_0^{-1})^{-1} w (g_1 g_0^{-1})$, *then retrieve* $g_1 g_0^{-1}$. *Otherwise output Failure.*

4 An amelioration of the mean-set attack

As mentioned by Sibert and *al.* in [21], we now consider the uniform law as the probability distribution used to generate r and ϵ in the protocol 3.1. We need to redefine the parameters of Section 2.2 for this restriction.

- Taking a sample S of k elements in B_n, the probability for an element to appear more than once in S is negligeable (since the probability distribution is uniform and $|B_n| = \infty$); we then have the *relative frequency*

$$\mu_k(g) = \mu_k(g, \omega) = \frac{1}{k},$$

  where $g \in S$.

- *The sample weight* is

$$M_k(g) = \frac{1}{k} \sum_{i \in S} d^2(g, i),$$

  where $d(\cdot, \cdot)$ is the distance function in B_n.

- *The sample mean-set* is

$$\mathbb{S}_k = \mathbb{S}(\xi_1, \ldots, \xi_k) =$$

$$= \{g \in B_n : \sum_{i \in S} d^2(g, i) \leq \sum_{i \in S} d^2(u, i), \quad \forall u \in B_n\}.$$

The SLLN is then stated as follows:

Theorem 4.1. *Let B_n be the n-string braid group and let $\{\xi_i\}_{i=1}^{\infty}$ be a sequence of i.i.d. random B_n-variables. If $M_{\xi_1}(\cdot)$ is totally defined and $\mathbb{E}(\xi_1) = \{g\}$ for an element $g \in B_n$, then*

$$\lim_{k \to \infty} \mathbb{S}_k = \mathbb{E}(\xi_1) = \{g\}.$$

Proof. Similar to the proof of theorem 2.1 which can be seen in [14, 15]. □

Now take a sequence of sample elements in B_n. We can approximate the mean-set of random B_n-variables. We experiment Mosina's algorithm 3.1 on CRAG by varying (n) the number of strings, (L) the length of the secret keys and (k) the number of elements in the sample. The results are presented in Tables 2–3.

T.T represents the ratio for obtaining the trivial braid e as element of the mean-set (on 100 tests).

$$T.T = \frac{|\{g_i | short(g_i) = e\}|}{100}$$

with g_i the element of the mean-set for the i-th test and $short(g_i)$ is the shortest normal or reduced element representing g_i.

DLMoy represents the average length of the braids when the element of the mean-set is different from the trivial braid.

$$DLmoy = \frac{1}{100 - TT * 100} \sum_{g \in S} l_X(g),$$

where S is the set of the elements which are different from the trivial braid and $l_X(g)$ represents the length of the element g with respect to X.

Table 2. Experimental results of the approximation of the mean-set of a random B_5-variable

L\k	20		40		80		160	
	T.T	**DLMoy**	**T.T**	**DLMoy**	**T.T**	**DLMoy**	**T.T**	**DLMoy**
10	65%	1,08	92%	1	100%	0	100%	0
20	45%	1,66	88%	1,8	96%	1	100%	0
30	45%	3,3	60%	1,7	89%	1,45	98%	1
40	21%	5,87	48%	5,11	64%	3,5	89%	8
50	14%	13,03	29%	6,7	71%	6,06	88%	5

An analysis of these results shows that the element of the mean-set of a random B_n-variable is either the trivial braid or either a braid which is very closed to the trivial braid (see that $DLMoy$ tends to 0

Table 3. Experimental results of the approximation of the mean-set of a random B_{10}-variable

L\k	20		40		80		160	
	T.T	**DLMoy**	**T.T**	**DLMoy**	**T.T**	**DLMoy**	**T.T**	**DLMoy**
10	85%	1,33	97%	1	100%	0	100%	0
20	49%	1,29	92%	0,99	100%	0	100%	0
30	46%	1,59	93%	1,01	100%	0	100%	0
40	31%	1,42	88%	1,66	97%	1	100%	0
50	29%	2,8	74%	1,8	98%	1	100%	0

when $T.T$ tends to 100). Hence we can deduce the following proposition:

Proposition 4.1. *Let B_n be the n-string braid group and let $g \in B_n$. Let $(\Omega, \mathcal{F}, P)$ be a probability space and let $\{\xi_i^g\}_{i=1}^{\infty}$ be a sample of random B_n-variables. Then for the random B_n-variable ξ_i^g defined by $\xi_i^g(\omega) = g\xi_i(\omega)$, we have*

$$\lim_{k\to\infty} \mathbb{S}_k(\xi_1^g, ...\xi_k^g) = g \lim_{k\to\infty} \mathbb{S}_k(\xi_1, ...\xi_k) = g.$$

This proposition means that $\lim_{n\to\infty} \mathbb{S}(\xi_1, \ldots, \xi_n) = \mathbb{E}(\xi_1) = e$, where e is the trivial braid in B_n. We then pose the following conjecture:

Conjecture 4.1. *Let B_n be the n-string braid group. Let $(\Omega, \mathcal{F}, P)$ be a probability space and let $\xi : \Omega \to B_n$ a random B_n-variable. Then $\mathbb{E}(\xi) = \{g\}$, where the normal form short(g) of g is such that short$(g) = e$, the trivial braid in B_n.*

Thus, from the set R_1 defined in Section 3.2.1, one can compute the set

$$\mathbb{S}(sr_{j_1}, \ldots, sr_{j_k})$$

which contains element s with a very high probability when k is large.

We can then rewrite the attack Algorithm 3.1 as follows.

Algorithm 4.1. The revisited mean-set attack Algorithm
INPUT: *the Prover public key* (t, w) *and a sequence* R_1
OUTPUT: *an element* g *such that* $t = gwg^{-1}$ *or 'Failure'*
COMPUTATION:

A. Apply Algorithm 2.1 to R_1 *and get* g.

B. If g *satisfies* $t = g^{-1}wg$, *then retrieve* g. *Else Failure.*

The experimental results, implemented on CRAG with this revisited mean-set attack Algorithm 4.1, are presented in Tables 4–6. Here, we vary n the number of strings, the length L of the words and the number k of tours in the algorithm (or elements in the sample).

Table 4. Experimental results of the attack Algorithm 4.1 in B_5

L\k	**20**	**40**	**80**	**160**
10	66%	95%	100%	100%
20	55%,	85%,	95%	100%
30	13%	38%	67%,	100%

Table 5. Experimental results of the attack Algorithm 4.1 in B_{10}

L\k	**20**	**40**	**80**	**160**
10	73%	99%	100%	100%
20	60%,	95%,	100%	100%
30	45%	90%	100%,	100%

Table 6. Experimental results of the attack Algorithm 4.1 in B_{20}

L\k	**20**	**40**	**80**	**160**
10	94%	100%	100%	100%
20	89%,	100%,	100%	100%
30	65%	97%	100%,	100%

On these tables, we see that the rate of success increases when the values of k increase. The length of the key influences the rate of success. Also, the success rate increases with the rank (number of

strings) of the group . These results, as those on Tables 2 and 3, confirm Mosina and Ushakov's obtained in [16]. Moreover we obtain a slight rise of the success rate, compared to Mosina. Furthermore, we gain in computation time since we need to compute only the mean-set of the set R_1, instead of computing for R_0 and R_1. Note that the computation of the mean-set is timely significant when k and L are large.

Acknowledgement

This work was completed at Saint Francis University (Loretto, PA, USA) during the second author's visit thanks to the Fulbright Program. Saint Francis University and the Fulbright Scholar Program are gratefully acknowledged.

References

[1] CRyptography And Groups (CRAG) C++ Library, available at http://www.acc.stevens.edu/downloads.php.

[2] P. Dehornoy. *Efficient solutions to the braid isotopy problem*, Disc. Appl. Math., Volume 156 Issue 16, September, (2008) 3091–3112, (online: http://www.arxiv.org/abs/math.GR/0703666).

[3] P. Dehornoy. *Using shifted conjugacy in braid-based cryptography*, Contemp. Math. 418 (2006) 65–73.

[4] W. Diffie, M.E. Hellman. *New directions of cryptography*, IEEE Transactions on Information theory, **22** (1976) 644–654.

[5] A. Groch, D. Hofheinz, R. Steinwandt. *A practical attack on the root problem in braid groups*, Contemp. Math. **418** (2006) 121–131.

[6] D. Hofheinz, R. Steinwandt. *A practical attack on some braid group based cryptographic primitives*, PKC 2003; Springer Lect. Notes in Comp. Sci. **2567** (2002) 187–198.

[7] C. Kassel, V. Turaev. *Braid groups*, Springer, 2007.

[8] S. Lal, A. Chaturvedi. *Authentication schemes using braid groups*, preprint (2005) (online: http://arxiv.org/pdf/cs.CR/0507066).

[9] J. Longrigg, A. Ushakov. *A Practical Attack on a Certain Braid Group Based Shifted Conjugacy Authentication Protocol*, Groups-Complexity-Cryptology, Vol. 1, No. 2 (2009) 275-286.

[10] S. Maffre. *Reduction of conjugacy problem in braid groups, using two Garside structures*, WCC 2005, 214–224.

[11] A. G. Miasnikov, V. Shpilrain, A. Ushakov *A practical attack on some braid group based cryptographic protocols*. Advances in Cryptology – CRYPTO 2005, Lecture Notes in Computer Science 3621, pp. 86–96. Springer, Berlin, 2005.

[12] A. G. Miasnikov, V. Shpilrain, A. Ushakov. *Random Subgroups of Braid Groups: An Approach to Cryptanalysis of a Braid Group Based Cryptographic Protocol*. Advances in Cryptology – PKC 2006, Lecture Notes in Computer Science 3958, pp. 302–314. Springer, Berlin, 2006.

[13] A. G. Miasnikov, V. Shpilrain, A. Ushakov. *Group-based Cryptography*, Advanced Courses in Mathematics - CRM Barcelona. Birkhäuser Basel, 2008.

[14] N. Mosina. *Probability on graphs and groups: theory and applications*, Ph.D. thesis, Columbia University, 2009. Available at http://www.math.columbia.edu/ thaddeus/theses/2009/mosina.pdf.

[15] N. Mosina, A. Ushakov. *Strong law of large numbers on graphs and groups*, Groups Complexity Cryptology, Vol. 3 Issue 1 (2011) 67–103.

[16] N. Mosina, A. Ushakov. *Mean-set attack: cryptanalysis of Sibert and al. authentication protocol*, J. Math. Cryp. 4, (2010) 149–174.

[17] R.L Rivest, A. Shamir, L.M Adleman. *A method for obtaining digital signatures and public-key cryptosystems*, Communication of ACM, **21** (1978) 120–126.

[18] C.E. Shannon. *Communication theory of secrecy systems*, Bell System Technical Journal, **28** (1949) 656–715.

[19] P.W. Shor. *Polynomial-time algorithm for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comp. **26**(5) (1997) 1484–1509.

[20] V. Shpilrain, A. Ushakov. *An authentication scheme based on the twisted conjugacy problem*, Applied Cryptography and Network Security, Lecture Notes in Computer Science Volume 5037, (2008) 366–372.

[21] H. Sibert, P. Dehornoy, M. Girault. *Entity authentication schemes using braid word reduction*, Proc. Internat. Workshop on Coding and Cryptography, 153–164, Versailles, 2003 OR Discrete applied Mathematics 154, (2006), 420–436.

[22] M.R. Spiegel. *Probabilits et statistique*. Neuvime tirage, MC Graw-Hill, Paris (1992).

[23] B. Tsaban. *On an authentication scheme based on the root problem in the braid group*, arXiv:cs/0509059 v2, (2007)

[24] M. Welschenbach. *Cryptography in C and C++* , Second Edition, 2005.

Sidoine Djimnaibeye, Daniel Tieudjo,
Norbert Youmbi

Received May 20, 2015

Sidoine Djimnaibeye, Daniel Tieudjo
Department of Mathematics and computer science
The University of Ngaoundere
P.O. Box 454 Ngaoundere – Cameroon
E–mail: dosiusher@yahoo.fr, tieudjo@yahoo.com

Norbert Youmbi
School of Science, Department of Mathematics
Saint Francis University
117 Evergreen Dr, Loretto PA, 15940 USA
E–mail: NYoumbi@francis.edu