M a t h e m a t i c a
B a l k a n i c a

New Series Vol. 24, 2010, Fasc.3-4

Cryptographic Primitives with Quasigroup Transformations

Aleksandra Mileva

The intention of this research is to justify deployment of quasigroups in cryptography, especially with new quasigroup based cryptographic hash function NaSHA as a runner in the First round of the ongoing NIST SHA-3 competition. We present new method for fast generation of huge quasigroup operations, based on the so-called extended Feistel networks and modification of the Sade's diagonal method. We give new design of quasigroup based family of cryptographic hash functions - NaSHA, which deploy the new method and with a novel approach - different quasigroups for every application of component quasigroup transformations in every iteration of the compression function and, much more, the used quasigroups are functions of the processed message block.

AMS Subj. Classification: Primary 20*N*05, Secondary 94*A*60

Key Words: cryptographic hash function, NaSHA, quasigroup transformations

1. Introduction

This thesis is the final result of four years of research done in the Institute of Informatics at "Ss Cyril and Methodius" University in Republic of Macedonia. In the following sequel we give the motivation and our research goals.

The most known constructions of the cryptographic primitives, error detecting and error correcting codes use structures from the associative algebra as groups, rings and fields. Two eminent specialists on quasigroups, J. Dénes and A. D. Keedwell [2], once proclaimed the advent of a new era in cryptology, consisting in the application of non-associative algebraic systems as quasigroups and neo-fields. The quasigroups and their combinatorial equivalent Latin squares are very suitable for this aim, because of their structure, their features, their big number and because they lead to particular simple and yet efficient primitives. Nevertheless, at present, very few researchers use these tools and cryptographic community still hesitate about them.

On October 9, 2007 NIST announced the request for candidate algorithm nominations for a new cryptographic SHA-3 hash algorithm family. The reason were Wang′s differential attacks [4, 3] on SHA-1 from 2005. The last standard -

SHA-2 hash functions are in the same general family of hash functions as SHA-1. They could potentially be attacked with similar techniques, but they are much stronger than SHA-1.

With this thesis we wanted to justify deployment of quasigroups in cryptography, especially with new quasigroup based cryptographic hash function as a runner in the NIST SHA-3 competition. Several questions were raised, as: (1) What kind of quasigroups are suitable for cryptographic purposes? (2) How to generate and how to compute fast operation of huge quasigroups? (3) What kind of features have huge quasigroups obtained by new construction method? (4) Do some old or new quasigroup transformations exist that can use quasigroups obtained by new method? (5) Design of cryptographic primitives with quasigroup transformations.

In the following sections we will present, without proofs, some of the main results of this thesis.

2. How to choose a quasigroup?

In a quasigroup based cryptography you can find that different authors are seeking quasigroups with different properties. One needs $CI-$quasigroups, the other needs multivariate quadratic quasigroups, the third needs quasigroups with less possible structure, the fourth needs exponential quasigroups, the fifth needs orthogonal quasigroups etc. Some cryptographic primitives need special kind of quasigroups. There are special cryptosystems build on some particular subsets of quasigroups. Our interest is to find what properties should have a quasigroup in order to be used as a non-linear building block in cryptographic primitives and to be able to contribute to the defence against linear and differential attacks. When we try to find quasigroups suitable for cryptography in this sense, we started from shapeless quasigroups, defined by Gligoroski et al. [6].

Definition 1. [6] *A quasigroup $(Q,*)$ of order r is said to be* **shapeless** *iff it is non-idempotent, non-commutative, non-associative, it does not have neither left nor right unit, it does not contain proper sub-quasigroups, and there is no $k < 2r$ for which identities of the kinds are satisfied:*

$$\underbrace{x(...*(x}_{k}*y)) = y,\ y = ((y*\underbrace{x)*...)*x}_{k} \tag{2.1}$$

Shapeless quasigroups are a good choice, but sometimes even a quasigroup with some structure is preferable (when the structure does not affect the security). In other cases quasigroups with additional restriction to the structure may be needed, for example, not to be either semisymmetric or Stein quasigroup or Schroeder quasigroup, etc. Most often quasigroups are used for creating quasigroup transformations, and for them, usually it is enough a quasigroup

to be shapeless. Some quasigroup transformations, like $\mathcal{A}$ and $\mathcal{RA}$, even defined by linear quasigroups [5], can produce non-linear Boolean functions [11]. Some quasigroup transformations, like E transformation, preserve linearity of the used quasigroup [11]. At the end, it is important the quasigroup string transformations to be non-linear Boolean functions without any linear component Boolean function, without nontrivial difference propagations with prop ratio 1 and restriction weight of 0 and with every nonzero output selection vector correlated to more than one input selection vector.

3. **Fast generation of huge quasigroup operations**

We introduced the so called extended Feistel networks (which are Feistel networks with additional properties) as orthomorphisms to define huge quasigroups [8]. A Feistel network [15] takes any function and transforms it into a bijection, so it is a commonly used technique for creating a non-linear cryptographic function. Using a Feistel network for creating a huge quasigroup is not a novel approach. Kristen [14] presents several different constructions using one or two Feistel networks and isotopies of quasigroups. Complete mappings, introduced by Mann [13] (the equivalent concept of orthomorphism was introduced explicitly in [12]), are also useful for creation of huge quasigroups. In [14] complete mappings with non-affine functions represented by Cayley tables or with affine functions represented by binary transformations, are used for that aim. The main disadvantages of the previously mentioned constructions are the lack of efficiency in one case and the lack of security in the other case. Namely, the Cayley table representations need a lot of memory, and also the affine functions do not have good cryptographic properties.

Our approach uses the extended Feistel networks as orthomorphisms, to generate huge quasigroups of order $R = 2^{s2^t}$. We only need to store small permutations of order 2^s, $s = 4, 8, 16$. We use the generalization of Sade's diagonal method [10] to the complete mappings and the orthomorphisms, given by the following Theorem. For the Abelian group $(\mathbb{Z}_2^n, \oplus_n)$ they are equivalent with Sade's diagonal method.

Theorem 1. *Let ϕ be a complete mapping of the admissible group $(G, +)$ and let θ be an orthomorphism associated to ϕ. Define an operations $\circ$ and $\bullet$ on G by:*

$$x \circ y = \phi(y - x) + y \tag{3.1}$$

$$x \bullet y = \theta(x - y) + y \tag{3.2}$$

where $x, y \in G$. Then $(G, \circ)$ and $(G, \bullet)$ are quasigroups.

Definition 2. *Let $(G,+)$ be an Abelian group, let $f : G \to G$ be a mapping and let $a, b, c \in G$ are constants. The* **extended Feistel network** *$F_{a,b,c} : G^2 \to G^2$ created by f is defined for every $l, r \in G$ by*

$$F_{a,b,c}(l,r) = (r + a, l + b + f(r + c)).$$

The extended Feistel network $F_{a,b,c}$ is a bijection with inverse

$$F^{-1}_{a,b,c}(l,r) = (r - b - f(l + c - a), l - a).$$

One of the main results of this thesis, that we will frequently use, is the following one.

Theorem 2. *Let $(G,+)$ be an Abelian group and $a, b, c \in G$. If $F_{a,b,c} : G^2 \to G^2$ is an extended Feistel network created by a bijection $f : G \to G$, then $F_{a,b,c}$ is an orthomorphism of the group $(G^2,+)$.*

In the sequel we will consider only extended Feistel networks of the Abelian groups $(\mathbb{Z}_2^n, \oplus_n)$.

Proposition 3.1. *Let $a, b, c \in \mathbb{Z}_2^k$ and let $F_{a,b,c} : \mathbb{Z}_2^{2k} \to \mathbb{Z}_2^{2k}$ be an extended Feistel network of the group $(\mathbb{Z}_2^{2k}, \oplus_{2k})$ created by a mapping $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$. Then $F_{a,b,c}$ is affine iff f is affine.*

Proposition 3.2. *Let $f, g : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ be bijections, $a, b, c, a', b', c' \in \mathbb{Z}_2^k$ and let $F_{a,b,c}, F_{a',b',c'} : \mathbb{Z}_2^{2k} \to \mathbb{Z}_2^{2k}$ be extended Feistel networks of the group $(\mathbb{Z}_2^{2k}, \oplus_{2k})$, created by f and g respectfully. Then the composite function $F_{a,b,c} \circ F_{a',b',c'}$ is a complete mapping and orthomorphism on $\mathbb{Z}_2^{2k}$ too.*

Corollary 1. *If $F_{a,b,c}$ is an extended Feistel network of the group $(\mathbb{Z}_2^{2k}, \oplus_{2k})$ created by bijection f, then $F^2_{a,b,c}$ is a complete mapping and orthomorphism too.*

The following Theorem shows us that extended Feistel network $F_{a,b,c}$ has the same algebraic degree as its starting bijection f.

Theorem 3. *Let $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ be a bijection of algebraic degree $deg(f) \geq 1$ and let $F_{a,b,c} : \mathbb{Z}_2^{2k} \to \mathbb{Z}_2^{2k}$ be an extended Feistel network of the group $(\mathbb{Z}_2^{2k}, \oplus_{2k})$, created by f. Then $deg(F_{a,b,c}) = deg(f)$.*

Here is a method for definition of huge quasigroups from small bijection.

Algorithm (Creation of extended Feistel network of order 2^{2^r})
Step 1 Take a suitable non-affine bijection of desired algebraic degree $f : \mathbb{Z}_2^{2^t} \to \mathbb{Z}_2^{2^t}$ where $t < r$ is a small positive integer ($t = 2, 3, 4$). Let $f' = f$ and $k = t$.
Step 2 Create Extended Feistel network $F_{a,b,c} : \mathbb{Z}_2^{2^{k+1}} \to \mathbb{Z}_2^{2^{k+1}}$ for some $a, b, c \in \mathbb{Z}_2^{2^k}$ using f' as starting bijection. Let $f' = F_{a,b,c}$ and $k = k + 1$.

Step 3 If $k < r$, go to step 2 else output the f'.

In applications one needs effectively constructed quasigroups of order 2^{256}, 2^{512},2^{1024},.... A huge quasigroup of order 2^{2^r} can now be designed as it follows. Take a suitable non-affine bijection of desired algebraic degree $f : \mathbb{Z}_2{}^{2^t} \to \mathbb{Z}_2{}^{2^t}$, where $t < r$ is a small positive integer ($t = 2, 3, 4$). We use the previous algorithm and we obtain F as the output extended Feistel network of order 2^{2^r}. Define a quasigroup operation $\circ$ on the set $\mathbb{Z}_2{}^{2^r}$ by 3.2, i.e.,

$$x \circ y = F(x \oplus y) \oplus y, \text{ for every } x, y \in \mathbb{Z}_2{}^{2^r}.$$

Note that we need only $r - t$ iterations for getting F and a small amount of memory for storing the bijection f. Hence, the complexity of our algorithm for construction of quasigroups of order 2^{2^r} is $\mathcal{O}(\texttt{log}(\texttt{log}\ r))$.

Example 1. We use a starting bijection $f : \mathbb{Z}_2^4 \to \mathbb{Z}_2^4$. So, $t = 2$. We choose constants $(a^{(i)}, b^{(i)}, c^{(i)}) = (i, 0, 0) \in \mathbb{Z}_2{}^{2^{t+i}}$, $i = 1, 2, \ldots, 7$. Now we can construct the following orthomorphisms, where $l_i, r_i \in \mathbb{Z}_2^i$, $i = 4, 8, 16, \ldots$:

$F^{(1)}_{1,0,0} : \mathbb{Z}_2^8 \to \mathbb{Z}_2^8$ as $F^{(1)}_{1,0,0}(l_4, r_4) = ((r_4 \oplus_4 1), (l_4 \oplus_4 f(r_4)))$,

$F^{(2)}_{2,0,0} : \mathbb{Z}_2^{16} \to \mathbb{Z}_2^{16}$ as $F^{(2)}_{2,0,0}(l_8, r_8) = ((r_8 \oplus_8 2), (l_8 \oplus_8 F^{(1)}_{1,0,0}(r_8)))$,

$F^{(3)}_{3,0,0} : \mathbb{Z}_2^{32} \to \mathbb{Z}_2^{32}$ as $F^{(3)}_{3,0,0}(l_{16}, r_{16}) = ((r_{16} \oplus_{16} 3), (l_{16} \oplus_{16} F^{(2)}_{2,0,0}(r_{16})))$,

$F^{(4)}_{4,0,0} : \mathbb{Z}_2^{64} \to \mathbb{Z}_2^{64}$ as $F^{(4)}_{4,0,0}(l_{32}, r_{32}) = ((r_{32} \oplus_{32} 4), (l_{32} \oplus_{32} F^{(3)}_{3,0,0}(r_{32})))$,

$F^{(5)}_{5,0,0} : \mathbb{Z}_2^{128} \to \mathbb{Z}_2^{128}$ as $F^{(5)}_{5,0,0}(l_{64}, r_{64}) = ((r_{64} \oplus_{64} 5), (l_{64} \oplus_{64} F^{(4)}_{4,0,0}(r_{64})))$,

$F^{(6)}_{6,0,0} : \mathbb{Z}_2^{256} \to \mathbb{Z}_2^{256}$ as $F^{(6)}_{6,0,0}(l_{128}, r_{128}) = ((r_{128} \oplus_{128} 6), (l_{128} \oplus_{128} F^{(5)}_{5,0,0}(r_{128})))$,

$F^{(7)}_{7,0,0} : \mathbb{Z}_2^{512} \to \mathbb{Z}_2^{512}$ as $F^{(7)}_{7,0,0}(l_{256}, r_{256}) = ((r_{256} \oplus_{256} 7), (l_{256} \oplus_{256} F^{(6)}_{6,0,0}(r_{256})))$.

So we need $7 = 9 - 2$ iterations for getting $F^{(7)}_{7,0,0} : \mathbb{Z}_2^{512} \to \mathbb{Z}_2^{512}$.

Further on in this section we consider the algebraic properties of the quasigroups obtained by the above mentioned algorithm. For that aim we take a somewhat simplified situation when $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ is a bijection and $F_{a,b,c} : \mathbb{Z}_2^{2k} \to \mathbb{Z}_2^{2k}$ is an extended Feistel network created by f. We denote by $(Q, \circ)$ the quasigroup on the set $Q = \mathbb{Z}_2^{2k}$ derived by the orthomorphism $F_{a,b,c}$.

Proposition 3.3. *The quasigroup $(Q, \circ)$ is non-idempotent iff $f(c) \neq b$ or $a \neq 0$.*

Proposition 3.4. *The equality*

$$(x \circ y) \circ (y \circ x) = x \tag{3.3}$$

is an identity in $(Q, \circ)$, i.e. $(Q, \circ)$ is a Schroeder quasigroup.

Corollary 2. *The quasigroup $(Q, \circ)$ is non-commutative and, much more, no different elements of Q commutes.*

Proposition 3.5. *The quasigroup $(Q, \circ)$ has neither left nor right unit.*

Proposition 3.6. *If $a \neq 0$, or $f(c) \neq b$, or $\phi \circ F_{a,b,c}(x) \neq F_{a,b,c} \circ \phi(x)$ for some $x \neq 0 \in Q$, then the quasigroup $(Q, \circ)$ is non-associative.*

Proposition 3.7. *a) The identity*

$$y = (\underbrace{(y \circ x) \circ \dots) \circ x}_{l}$$

holds true in $(Q, \circ)$ iff $F^l_{a,b,c} = I$.

b) The identity

$$\underbrace{x \circ (\cdots \circ (x}_{l} \circ y)) = y$$

holds true in $(Q, \circ)$ iff $\phi^l = I$, where $\phi = I \oplus_{2k} F_{a,b,c}$.

Regarding the subquasigroups of the quasigroup $(Q, \circ)$, we notice the following property, where $< A >$ denotes the subquasigroup generated by the subset A of Q.

Proposition 3.8. $< 0 >=< \{\theta^i(0) |\ i = 1, 2, \dots\} >$.

Proposition 3.9. *The quasigroup $(Q, \bullet)$, created by an affine orthomorphism θ of a group $(\mathbb{Z}_2^n, \oplus_n)$ is totally anti-symmetric (TA-quasigroup).*

So, even affine extended Feistel network can find some application also, for example, for creating TA-quasigroups that can be used for the definition of the check digit systems, where the early typing errors have to be recognized.

4. Cryptographic hash function NaSHA

We use the quasigroup transformation $\mathcal{MT}$ for definition of a new family of hash functions NaSHA-(m, k, r) [7]. The parameters m, k and r denote the length of the output hash result (the message digest), the complexity of $\mathcal{MT}$ and the order 2^{2^r} of used quasigroup respectively, so k is a positive even integer and m and r are positive integers. We showed that, the transformation $\mathcal{MT} : Q^t \to Q^t$ can be considered as a one-way function when $Q = \mathbb{Z}_{2^n}$ is enough big.

NaSHA-(m,k,r) hash algorithm

Input: A positive even integer k and positive integers m and r such that $m > 2^r$, and an input message M.

Output: A hash value NaSHA-$(m,k,r)(M)$ of m bits.

1. Denote by n the smallest integer such that $m \leq 2^n$.
   (For example, n=8 for m=224 and n=9 for m=384.)
2. Pad the message M, so that the length of the padded message M' is a multiple of 2^{n+1}, $|M'| = 2^{n+1}N$ for some N.
   Separate M' in N 2^{n+1}-bit blocks, $M' = M_1||M_2||\ldots||M_N,\ |M_i| = 2^{n+1}$.
3. Initialize the initial value H_0, which is a 2^{n+1}-bit word.
4. The first message block M_1 and the initial value H_0 separate to $q = 2^{n-r+1}$ 2^r-bits words:
   $M_1 = S_1||S_3||S_5||\ldots||S_{2q-3}||S_{2q-1}$,
   $H_0 = S_2||S_4||S_6||\ldots||S_{2q-2}||S_{2q}$, ($|S_i| = 2^r$) and form the word
   $S^{(0)} = S_1||S_2||S_3||S_4||\ldots||S_{2q-3}||S_{2q-2}||S_{2q-1}||S_{2q}$.
5. Choose leaders l_i as functions that depend on $S_1, S_2, S_3, \ldots, S_{2q}$ and a suitable linear transformation $LinTr_{2^{n+2}}$.
6. Choose two quasigroups $(\{0,1\}^{2^r}, *_1)$ and $(\{0,1\}^{2^r}, *_2)$ (one for $\mathcal{A}$ and one for $\mathcal{RA}$ transformation) and compute the string of bits $S^{(N-1)}$ as follows:
   for $i = 1$ to $N-1$ do
   $A_1||A_2||A_3||\ldots||A_{2q} \leftarrow \mathcal{MT}(LinTr^{2q}_{2^{n+2}}(S^{(i-1)}))$
   $B_1||B_2||B_3||\ldots||B_{q-1}||B_q \leftarrow M_{i+1}$,
   $S^{(i)} := B_1||A_2||B_2||A_4||\ldots||B_{q-1}||A_{2q-2}||B_q||A_{2q}$,
   end
7. Choose two quasigroups $(\{0,1\}^{2^r}, *_1)$ and $(\{0,1\}^{2^r}, *_2)$ and compute $\mathcal{MT}(LinTr^{2q}_{2^{n+2}}(S^{(N-1)})) := A_1||A_2||A_3||\ldots||A_{2q}$. Then
   NaSHA-$(m,k,r)(M) = A_4||A_8||\ldots||A_{2q-4}||A_{2q}$ (`mod` 2^m).

We give a complete implementation of NaSHA-$(m,2,6)$ algorithm where $m \in \{224, 256, 384, 512\}$ in [7]. It supports internal state sizes of 1024 and 2048 bits, and arbitrary output sizes between 125 and 512 bits. The used quasigroups of order $2^{2^6} = 2^{64}$ are constructed by extended Feistel networks, because they allow to insert tunable parameters in their definition. We used that feature to obtain the novel design: different quasigroups for every application of component quasigroup transformations in every iteration of the compression function and, much more, the used quasigroups are functions of the processed message block. This implementation has been accepted as a 1^{st} Round candidate in the SHA-3 competition of The American National Institute of Standards and Technology, NIST, but did not pass to the 2^{nd} Round. Some improvements are given in [9]. We obtain performance of up to 23.06 cycles per byte on an Intel Core 2 Duo in 64-bit mode.

In the implementation, as a starting bijection $f : \mathbb{Z}_2^8 \to \mathbb{Z}_2^8$ we use an improved AES S-box with the APA structure from Cui and Cao [1]. From the starting bijection f we define three extended Feistel networks F_{a_1,b_1,c_1}, F_{a_2,b_2,c_2},

$F_{a_3,b_3,c_3} : \mathbb{Z}_2^{16} \to \mathbb{Z}_2^{16}$ by

$$F_{a_i,b_i,c_i}(l_8||r_8) = (r_8 \oplus a_i)||(l_8 \oplus b_i \oplus f(r_8 \oplus c_i)),$$

where l_8 and r_8 are 8-bit variables, and $a_i,\ b_i,\ c_i$ are 8-bit words that are defined before each application of $\mathcal{MT}$. Denote by f' the bijection $F_{a_1,b_1,c_1} \circ F_{a_2,b_2,c_2} \circ F_{a_3,b_3,c_3} : \mathbb{Z}_2^{16} \to \mathbb{Z}_2^{16}$.

By using the bijection f' we define a quasigroup operation on $\mathbb{Z}_2^{64}$ which is going to be used for the additive string transformation $\mathcal{A}$ as follows. Create the Feistel networks $F_{\alpha_1,\beta_1,\gamma_1} : \mathbb{Z}_2^{32} \to \mathbb{Z}_2^{32}$ and $F_{A_1,B_1,C_1} : \mathbb{Z}_2^{64} \to \mathbb{Z}_2^{64}$ by

$$F_{\alpha_1,\beta_1,\gamma_1}(l_{16}||r_{16}) = (r_{16} \oplus \alpha_1)||(l_{16} \oplus \beta_1 \oplus f'(r_{16} \oplus \gamma_1)),$$

$$F_{A_1,B_1,C_1}(l_{32}||r_{32}) = (r_{32} \oplus A_1)||(l_{32} \oplus B_1 \oplus F_{\alpha_1,\beta_1,\gamma_1}(r_{32} \oplus C_1)),$$

where l_{16}, r_{16} are 16-bit variables, $\alpha_1, \beta_1, \gamma_1$ are 16-bit words, l_{32}, r_{32} are 32-bit variables and A_1, B_1, C_1 are 32-bit words. The constant words will be defined latter. The function F_{A_1,B_1,C_1} is an orthomorphism (complete mapping) in the group $(\mathbb{Z}_2^{64}, \oplus)$, and then the operation defined by

$$x *_{a_1,b_1,c_1,a_2,b_2,c_2,a_3,b_3,c_3,\alpha_1,\beta_1,\gamma_1,A_1,B_1,C_1} y = F_{A_1,B_1,C_1}(x \oplus y) \oplus y$$

is a quasigroup operation in $\mathbb{Z}_2^{64}$.

By using the bijection f' we define also a quasigroup operation in $\mathbb{Z}_2^{64}$ which is going to be used for the reverse additive string transformation $\mathcal{RA}$ as follows. Create the Feistel networks $F_{\alpha_2,\beta_2,\gamma_2} : \mathbb{Z}_2^{32} \to \mathbb{Z}_2^{32}$ and $F_{A_2,B_2,C_2} : \mathbb{Z}_2^{64} \to \mathbb{Z}_2^{64}$ by

$$F_{\alpha_2,\beta_2,\gamma_2}(l_{16}||r_{16}) = (r_{16} \oplus \alpha_2)||(l_{16} \oplus \beta_2 \oplus f'(r_{16} \oplus \gamma_2)),$$

$$F_{A_2,B_2,C_2}(l_{32}||r_{32}) = (r_{32} \oplus A_2)||(l_{32} \oplus B_2 \oplus F_{\alpha_2,\beta_2,\gamma_2}(r_{32} \oplus C_2)),$$

where l_{16}, r_{16} are 16-bit variables, $\alpha_2, \beta_2, \gamma_2$ are 16-bit words, l_{32}, r_{32} are 32-bit variables and A_2, B_2, C_2 are 32-bit words. The constant words will be defined later. The function F_{A_2,B_2,C_2} is an orthomorphism (complete mapping) in the group $(\mathbb{Z}_2^{64}, \oplus)$, and then the operation defined by

$$x *_{a_1,b_1,c_1,a_2,b_2,c_2,a_3,b_3,c_3,\alpha_2,\beta_2,\gamma_2,A_2,B_2,C_2} y = F_{A_2,B_2,C_2}(x \oplus y) \oplus y$$

is a quasigroup operation in $\mathbb{Z}_2^{64}$.

Before every computation $\mathcal{MT}(S_1||S_2||S_3||\dots||S_{2q-1}||S_{2q})$, where S_i are 64-bit words, we define the 64-bit leaders l_1 of $\mathcal{RA}$ and l_2 of $\mathcal{A}$, the 8-bit words $a_1, b_1, c_1,\ a_2, b_2, c_2,\ a_3, b_3, c_3$, the 16-bit words $\alpha_1, \beta_1, \gamma_1, \alpha_2, \beta_2,\ \gamma_2$ and the 32-bit words $A_1, B_1,\ C_1,\ A_2, B_2, C_2$.

For $m = 224$ and 256, necessary definitions are:

$$l_1 = S_1 + S_2, \quad l_2 = S_3 + S_4,$$

$$a_1||b_1||c_1||a_2||b_2||c_2||a_3||b_3 = S_5 + S_6, \quad c_3 = a_1$$

$$\alpha_1||\beta_1||\gamma_1||\alpha_2 = S_7 + S_8, \quad \beta_2||\gamma_2 = (S_9 + S_{10})(\mathtt{mod}\ 2^{32}),$$

$$A_1||B_1 = S_{11} + S_{12}, \quad C_1||A_2 = S_{13} + S_{14}, \quad B_2||C_2 = S_{15} + S_{16}.$$

For $m = 384$ and 512, necessary definitions are (this is improved version, suggested in [9]):

$$l_1 = S_1 + S_2 + S_{28} + S_{30}, \quad l_2 = S_3 + S_4 + S_{29} + S_{31},$$
$$a_1||b_1||c_1||a_2||b_2||c_2||a_3||b_3 = S_5 + S_6 + S_{17} + S_{18}, \quad c_3 = a_1$$
$$\alpha_1||\beta_1||\gamma_1||\alpha_2 = S_7 + S_8 + S_{19} + S_{20},$$
$$\beta_2||\gamma_2 = (S_9 + S_{10} + S_{21} + S_{22})(\mathtt{mod}\ 2^{32}),$$
$$A_1||B_1 = S_{11} + S_{12} + S_{23} + S_{27}, \quad C_1||A_2 = S_{13} + S_{14} + S_{24} + S_{26},$$
$$B_2||C_2 = S_{15} + S_{16} + S_{25} + S_{32}.$$

Here, the addition + is modulo 2^{64}.

The linear transformations are given as follows. Denote by $LinTr_{512}$ and by $LinTr_{256}$ the transformations of the sets $\{0,1\}^{2028}$ and $\{0,1\}^{1024}$ respectively, defined by

$$LinTr_{512}(S_1||S_2||\dots||S_{31}||S_{32}) = (S_7 \oplus S_{15} \oplus S_{25} \oplus S_{32})||S_1||S_2||\dots||S_{31},$$
$$LinTr_{256}(S_1||S_2||\dots||S_{15}||S_{16}) = (S_4 \oplus S_7 \oplus S_{10} \oplus S_{16})||S_1||S_2||\dots||S_{15},$$

where S_i are 64-bits words, $\oplus$ denotes the operation XOR on 64-bits words, and the operation $||$ denotes the concatenation of words.

For more information about NaSHA, see [7].

5. Future work

In the future we plan an examination of quasigroups produced by Extended Feistel networks of other Abelian groups. Also we plan to use them in the design of quasigroup based block cipher.

References

[1] L. Cui, Y. Cao, A new S-box structure named Affine-Power-Affine, *International Journal of Innovative Computing, Information and Control,* **3**(3), 2007, 751–759

[2] J. Dénes, D. Keedwell, Some applications of non-associative algebraic systems in cryptology, *Pure Mathematics and Applications*, **12**(2), 2001, 147–195

[3] X. Wang, Y. L. Yin, H. Yu, Finding Collisions in the Full SHA-1, *Advances in Cryptology - CRYPTO 2005, LNCS 3621*, 2005, 17–36

[4] X. Wang, H. Yu, Y. L. Yin, Efficient Collision Search Attacks on SHA-0, *Advances in Cryptology - CRYPTO 2005, LNCS 3621*, 2005, 1–16

[5] D. Gligoroski, V. Dimitrova, S. Markovski, *Quasigroups as Boolean Functions, Their Equation Systems and Gröbner Bases, Gröbner Bases, Coding, and Cryptography*, Springer 2009, 415–420

[6] D. Gligoroski, S. Markovski, L. Kocarev, Edon-$\mathcal{R}$, an Infinite Family of Cryptographic Hash Functions, *The Second NIST Cryptographic Hash Workshop, UCSB, Santa Barbara, CA,* 2006, 275–285
[7] S. Markovski, A. Mileva, *NaSHA*, Submission to NIST, 2008
[8] S. Markovski, A. Mileva, Generating huge quasigroups from small non-linear bijections via extended Feistel function, *Quasigroups and Related Systems*, **17**, 2009, 91–106
[9] S. Markovski, A. Mileva, NaSHA - cryptographic hash functions, *NIST The First SHA-3 Candidate Conference, 25-28 February 2009, Leuven, Belgium*
[10] A. Sade, Groupoides automorphes par le groupe cyclique, *Canadian Journal of Mathematics*, **9**(3), 1957, 321–335
[11] A. Mileva, Analysis of some Quasigroup transformations as Boolean Functions, *MASSEE International Congress on Mathematics MICOM 2009, 16-20 September, Ohrid*
[12] D. M. Johnson, A. L. Dulmage, N. S. Mendelsohn, Orthomorphisms of groups and orthogonal latin squares I, *Canad. J. Math.*, **13**, 1961, 356–372
[13] H. B. Mann, The construction of orthogonal Latin squares, *The Annals of Mathematical Statistics*,**13**, 1942, 418–423
[14] K. A. Meyer, *A new message authentication code based on the non-associativity of quasigroups*, PhD thesis, Iowa State University, 2006
[15] H. Feistel, Cryptography and computer privacy, *Scientific American*, **228** (No. 5), 1973, 15–23

Faculty of Computer Science
and Information Technology,
University "Goce Delcev",
Štip, Republic of Macedonia

E-Mail: aleksandra.mileva@ugd.edu.mk