RIST

Information Processing at the Digital Age

VOL22. N.2(2018) 31-38

On public key cryptosystems based on Thue Monoid Morphism Interpretation (TMMI)

Nacer Ghadbane *

Laboratory of Pure and Applied Mathematics , Department of Mathematics, University of M'sila, Algeria

Submitted 11/01/2019, Accepted 17/03/219

Abstract

The asymmetric encryption methods are based on difficult problems in mathematics.
Let Σ^* be the free monoid over a finite alphabet Σ and R a binary relation on Σ^*. The pair (Σ, R) is called a Thue system. The congruence generated by R is defined as follows:

- $xuy \leftrightarrow_R xvy$, whenever $x, y \in \Sigma^*$and uRv or vRu.
- $w \leftrightarrow_R{}^* w'$, whenever $u_0, u_1, \dots, u_n \in \Sigma^*$with, $u_0 = w, u_i \leftrightarrow_R u_{i+1}, \forall 0 \leq i \leq n-1, u_n = w'$.

The word problem for R on Σ^* is then following : given two words $w_1, w_2 \in \Sigma^*$, do we have $w_1 \leftrightarrow_R{}^* w_2$? [7]
In this paper we investigate on a public key cryptosystems based on the difficult word problem in free monoid, introduced by Wagner and Magyarik in 1985. It's well known that the word problem is undecidable in general, meaning that there is no algorithm to solve it. We introduce some cryptosystems based on the Thue Monoid Morphism Interpresentation where the word problem is decidable in linear time.

keywords : Free monoid, Thue system, Finitely presented monoids, Word problem in monoid, Public key cryptography.

* Corresponding author. Tel.: 078-122-4013; fax: +0-000-000-0000 .
E-mail address: *nacer.ghadbane@yahoo.com*

1. Introduction

Let Σ^* be the free monoid over a finite alphabet Σ and R a binary relation on Σ^*. The congruence generated by R is defined as follows:

- $xuy \leftrightarrow_R xvy$, whenever $x, y \in \Sigma^*$and uRv or vRu.
- $w \leftrightarrow_R{}^* w'$, whenever $u_0, u_1, \ldots, u_n \in \Sigma^*$with, $u_0 = w, u_i \leftrightarrow_R u_{i+1}, \forall 0 \le i \le n-1, u_n = w'$.

A presentation by generators and relations of a monoid M is a pair (Σ, R) such that M is isomorphic to the quotient of Σ^* by the congruence noted $\leftrightarrow_R{}^*$ generated by R , i.e, $M \cong \Sigma^*/\leftrightarrow_R{}^*$.

The word problem for R on Σ^* is then following : given two words $w_1, w_2 \in \Sigma^*$, do we have $w_1 \leftrightarrow_R{}^* w_2$. The word problem as introduced by Max Dehn in 1911 [7], in the 1950′ s, Novikov and Boon independently showed that there are finite monoid presentations whose word problem is undecidable.

A number of public key cryptosystems based on combinatorial group theory have been proposed since the early 1980s.

The first proposal to use nonabelian groups in public key cryptography is due to Wagner and Magyarik [10] in 1985. The cryptosystem are based on the hardness of the word problem for finitely presented monoids. The importance of Wagner and Magyarik's scheme lies in its novelty, which commenced an interplay between cryptography and combinatorial monoid theory.

The remainder of this paper is organized as follows. In Section 2, we begin with some elementary material concerning of finitely presented monoids and Public key cryptography. In Section 3, we investigate the public-key cryptosystems based on Thue Monoid Morphism Interpretation (TMMI). In Section 4, we give the security of TMMI protocol. Finally, we draw our conclusions in Section 5.

2. Preliminaries

A monoid $(M,\cdot)$ consists of a set M together with a binary operation "$\cdot$" on M such that

(i) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in M$. (associativity)

(ii) There existes an identity $1_M \in M$such that $a \cdot 1_M = 1_M \cdot a = a$ for all $a \in M$.

We formally define an alphabet as a non-empty finite set. A word over an alphabet Σ is a finite sequence of symbols of Σ. Although one writes a sequence as $(\sigma_1, \sigma_2, \ldots, \sigma_n)$, in the present context, we prefer to write it as $\sigma_1\sigma_2, \ldots \sigma_n$. The set of all words on the alphabet Σ is denoted by $\Sigma^*$and is equipped with the associative operation defined by the concatenation of two sequences. The concatenation of two sequences $\alpha_1\alpha_2..\alpha_n$ and $\beta_1\beta_2..\beta_m$ is the sequence $\alpha_1\alpha_2..\alpha_n\,\beta_1\beta_2..\beta_m$.

The concatenation is an associative operation. The string consisting of zero letters is called the empty word, written ε. Thus, $\varepsilon, \alpha, \beta, \alpha\alpha\beta\alpha, \alpha\alpha\alpha\beta\alpha$ are words over the alphabet $\{\alpha, \beta\}$. Thus the set Σ^* of words is equipped with the structure of a monoid. The monoid Σ^* is called the free monoid on Σ. The length of a word w, denoted $|w|$, is the number of letters in w when each letter is counted as many times as it occurs. Again by definition, $|\varepsilon| = 0$. For example $|\alpha\alpha\beta\alpha| = 4$ and $|\alpha\alpha\alpha\beta\alpha| = 5$. Let w be a word over an alphabet Σ. For $\sigma \in \Sigma$, the number of occurrences of σ in w shall be denoted by $|w|_\sigma$. For example $|\alpha\alpha\beta\alpha|_\beta = 1$ and $|\alpha\alpha\alpha\beta\alpha|_\alpha = 4$.

A mapping $h: \Sigma^* \to \Delta^*$, where Σ and Δ are alphabets, satisfying the condition

$$h(uv) = h(u)h(v), \text{ for all words } u \text{ and } v \text{ in } \Sigma^*, \text{ is called a morphism.}$$

Define a morphism h, it suffices to list all the words $h(\sigma)$, where a ranges over all the (finitely many) letters of Σ. If M is a monoid, then any mapping $f: \Sigma \to M$ extends to a unique morphism $f: \Sigma^* \to M$. For

instance, if M is the additive monoid $\mathbb{N}$, and f is defined by $f(\sigma) = 1$ for each $\sigma \in \Sigma$, then $f(u)$ is the length $|u|$ of the word u.

A binary relation on Σ^* is a subset $R \subseteq \Sigma^* \times \Sigma^*$. If $(x, y) \in R$, we say that x is related to y by R, denoted xRy. The inverse relation of R is the binary reation $R^{-1} \subseteq \Sigma^* \times \Sigma^*$defined by $yR^{-1}x \Leftrightarrow (x, y) \in R$.

The relation I_{Σ^*} ={(x,x),$x \in \Sigma^*$ } is called the identity relation. The relation $(\Sigma^*)^2$ is called the complete relation.

Let $R \subseteq \Sigma^* \times \Sigma^*$ and $S \subseteq \Sigma^* \times \Sigma^*$ are binary relations. The composition of R and S is a binary relation $S \circ R \subseteq \Sigma^* \times \Sigma^*$ defined by: $x(S \circ R)z \Leftrightarrow \exists y \in \Sigma^*$ such that xRy and ySz.

A binary relation R on a set Σ^* is said to be

· reflexive if xRx for all x in Σ^*;

· symmetric if xRy implies yRx;

· transitive if xRy and yRz imply xRz.

The relation R is called an equivalence relation if it is reflexive, symmetric, and transitive. And in this case, if xRy, we say that x and y are equivalent.

Let R be a relation on a set Σ^*. The reflexive closure of R is the smallest reflexive relation R^r on Σ^* that contains R, that is,

▸ $R \subseteq R^r$;

▸ if R' is a reflexive relation on Σ^* and $R \subseteq R'$, then $R^r \subseteq R'$.

The symmetric closure of R is the smallest symmetric relation R^s on Σ^* that contains R, that is,

▸ $R \subseteq R^s$;

▸ if R' is a symmetric relation on $\Sigma^*$and $R \subseteq R'$, then $R^s \subseteq R'$.

The transitive closure of R is the smallest transitive relation R^t on Σ^* that contains R, that is,

▸ $R \subseteq R^t$;

▸ if R' is a transitive relation on $\Sigma^*$and $R \subseteq R'$, then $R^t \subseteq R'$.

Let R be a relation on a set Σ^*. Then

· $R^r = R \cup I_{\Sigma^*}$.

· $R^s = R \cup R^{-1}$.

· $R^t = \bigcup_{k=1}^{k=+\infty} R^k$.

A congruence on a monoid M is an equivalence relation $\equiv$ on M compatible with the operation of M, i.e,

for all $m, m' \in M, u, v \in M, m \equiv m' \Rightarrow umv \equiv um'v$.

If $h: \Sigma^* \to \Delta^*$ is a morphism of monoids, Then $Ker\ h$ is a congruence defined by:

$$\forall u, v \in \Sigma^*: u\ Ker f\ v \Leftrightarrow f(u) = f(v).$$

Let L be a language over Σ, the syntactic congruence of L denoted by $\equiv_L$ is defined by:

$$u \equiv_L v \Leftrightarrow (\forall x, y \in \Sigma^*: xuy \in L \Leftrightarrow xvy \in L).$$

The quotient of Σ^* by $\equiv_L$ is, by definition, the syntactic monoid of L denoted $M(L)$, i.e., $M(L) = \Sigma^*/\equiv_L$

A Thue system is a pair (Σ, R) where Σ is an alphabet and R is a non-empty finite binary on Σ^*, we write $xuy \longrightarrow_R xvy$ whenever $x, y \in \Sigma^*$ and $(u, v) \in R$. We write $\lambda \longrightarrow_R{}^* \mu$ if there exists a words $\lambda_0, \lambda_1, \ldots, \lambda_n \in \Sigma^*$ such that, $\lambda_0 = \lambda$, $\lambda_i \longrightarrow_R \lambda_{i+1}, \forall 0 \leq i \leq n-1$ and $\lambda_n = \mu$.

If $n = o$, we get $\lambda = \mu$, and if $n = 1$, we get $\lambda \longrightarrow_R \mu$. $\longrightarrow_R{}^*$ is the reflexive transitive closure of $\longrightarrow_R$.

The congruence generated by R is defined as follows:

▸ $xuy \leftrightarrow_R xvy$ whenever $x, y \in \Sigma^*$, and uRv or vRv;

▸ $\lambda \leftrightarrow_R{}^* \mu$ whenever $\lambda = \lambda_0 \leftrightarrow_R \lambda_1 \leftrightarrow_R \ldots \leftrightarrow_R \lambda_n = \mu$.

$\leftrightarrow_R{}^*$ is the reflexive symmetric transitive closure of $\leftrightarrow_R$. The congruence class of $w \in \Sigma^*$ with respect to $\leftrightarrow_R{}^*$ is $[w]_{\leftrightarrow_R{}^*}=\{x \in \Sigma^*: x \leftrightarrow_R{}^* w\}$. A monoid M is finitely generated if it is isomorphic to a monoid of the form $\Sigma^*/\leftrightarrow_R{}^*$. In this case, we also say that M is finitely generated by Σ , If in addition to Σ also R is finite, then M is a finitely presented monoid.

The word problem for R on Σ^* is then following : given two words $w_1, w_2 \in \Sigma^*$, do we have $w_1 \leftrightarrow_R{}^* w_2$? The word problem as introduced by Max Dehn in 1911, in the 1950's, Novikov and Boon independently showed that there are finite monoid presentations whose word problem is undecidable.

Public-Key cryptography, also called asymmetric cryptography, was invented by Diffie And Hellman more than forty years ago. In Public-Key cryptography, a user U has a pair of related keys (pK,sK): the key pK is public and should be available to everyone, while the key sK must be kept secret by U. The fact that sK is kept secret by a single entity creates an asymmetry, hence the name asymmetric cryptography.

Wagner and Magyarik build the TMMI protocol, the idea is transform a system of Thue (Σ, R) for which the word problem is undecidable in a Thue system (Σ, S) for which the word problem is decidable in linear time.

Public-Key (pK): a finitely presented monoid (Σ,R), and two words w_0,w_1 of Σ^*, with w_0, w_1 are not equivalent with respect to $\leftrightarrow_R{}^*$.

Secret-key (sK): a set of relations $S \subseteq \Sigma^* \times \Sigma^*$, rendering the word problem in $\Sigma^*/\leftrightarrow_S{}^*$ easy, with the property that $\forall u, v \in \Sigma^*, u \leftrightarrow_R{}^* v \Rightarrow u \leftrightarrow_S{}^* v$.

and satisfying also w_0, w_1 are not equivalent with respect to $\leftrightarrow_S{}^*$.

Encryption: to encrypt $b \in \{0,1\}$, choose a word $w \in \Sigma^*$ with $w \leftrightarrow_R{}^* w_b$.

Decryption: solve the easy word problem in $\Sigma^*/\leftrightarrow_S{}^*$ to find b such that $w \leftrightarrow_S{}^* w_b$ [10].

3. Results

In the following proposition we give a condition on the relation of a Thue system to show that the congruence generated by this relation is included in the congruence associated a morphism of monoids. Also we use this included to present the public-key cryptosystems based on the Thue Monoid Morphism Interpretation (TMMI).

Proposition 1: Let $f: \Sigma^* \to M$ be a monoids morphism and R is a binary relation on a set Σ^* suth that, for all $(r, s) \in R, f(r) = f(s)$. Then $\leftrightarrow_R{}^* \subseteq Kerf$.

Proof: If $f: \Sigma^* \to M$ is a morphism of monoids, Then $Ker\ f$ is a congruence defined by: $\forall u, v \in \Sigma^*: u\ Kerf\ v \Leftrightarrow f(u) = f(v)$. Since for all $(r, s) \in R, f(r) = f(s)$, we have $R \subseteq Kerf$, then $\leftrightarrow_R{}^* \subseteq Kerf$.

Proposition 2: Public-Key (pK): a finitely presented monoid (Σ,R), and two words w_0,w_1 of Σ^*, with w_0, w_1 are not equivalent with respect to $\leftrightarrow_R{}^*$.

Secret-key (sK): a morphism of monoids $f: \Sigma^* \to M$ and the word problem in $\Sigma^*/Kerf$ is easy, with the property that $\forall u, v \in \Sigma^*, u \leftrightarrow_R{}^* v \Rightarrow$ u $Kerf$ v and satisfying also w_0,w_1 are not equivalent with respect to $Kerf$.

Encryption: to encrypt $b \in \{0,1\}$, choose a word $w \in \Sigma^*$ with w$\leftrightarrow_R{}^* w_b$.
Decryption: solve the easy word problem in $\Sigma^*/Kerf$ to find b such that w $Kerf w_b$.

Example 1: Consider the morphism of monoids $f:\{\alpha,\beta\}^* \to (\mathbb{Z},+)$ defined by:

$$f(\alpha) = 1, f(\beta) = -1, f(\varepsilon) = 0.$$

And then, $\forall w \in \{\alpha,\beta\}^*$ we have $f(w) = |w|_\alpha - |w|_\beta$.
Let $\Sigma = \{\alpha,\beta\}$, $R = \{(\alpha\beta\alpha\beta\alpha, \alpha\alpha\beta), (\alpha\beta,\varepsilon)\}$, we have $f(\alpha\beta\alpha\beta\alpha) = |\alpha\beta\alpha\beta\alpha|_\alpha$ -$|\alpha\beta\alpha\beta\alpha|_\beta$=3-2=1,
$f(\alpha\alpha\beta) = |\alpha\alpha\beta|_\alpha$-$|\alpha\alpha\beta|_\beta = 2-1 = 1$. And $f(\alpha\beta) = |\alpha\beta|_\alpha$-$|\alpha\beta|_\beta = 1-1 = 0$,
$f(\varepsilon) = |\varepsilon|_\alpha$-$|\varepsilon|_\beta = 0-0 = 0$. Then for all $(r,s) \in R, f(r) = f(s)$.
Consequently $\leftrightarrow_R{}^* \subseteq Kerf$.
Public-Key (pK): a finitely presented monoid (Σ,R), where $\Sigma = \{\alpha,\beta\}$, $R = \{(\alpha\beta\alpha\beta\alpha, \alpha\alpha\beta), (\alpha\beta,\varepsilon)\}$. Let $w_0 = \alpha\alpha\beta\alpha\beta\alpha$ and $w_1 = \beta\alpha\beta\alpha\beta\alpha$, w_0, w_1 are not equivalent with respect to $\leftrightarrow_R{}^*$, because $\alpha\alpha\beta\alpha\beta\alpha \leftrightarrow_R{}^* \alpha\alpha$ and $\beta\alpha\beta\alpha\beta\alpha \leftrightarrow_R{}^* \beta\alpha$. (Σ, R, w_0, w_1) constitute a public-key.
Secret key (sK): the morphism of monoids $f:\{\alpha,\beta\}^* \to (\mathbb{Z},+)$ defined by:
$f(\alpha) = 1, f(\beta) = -1, f(\varepsilon) = 0$ and $\leftrightarrow_S{}^*$, $=Kerf$, i.e., $\leftrightarrow_s{}^*$, is the congruence associated a morphism of monoids f. We have w_0, w_1 are not equivalent with respect to $Kerf$ becouse $f(w_0) = 2$ and
$f(w_1) = 0, f(w_0) \neq f(w_0)$.
Encryption: for encrypt a bit $b \in \{0,1\}$, Alice chooses a word c of $\{\alpha,\beta\}^*$ in the equivalence class of w_b with respect to $\leftrightarrow_R{}^*$,, i. e, $c \in [w_b]_{\leftrightarrow_R{}^*}$ where $[w_b]_{\leftrightarrow_R{}^*}$ denotes the equivalence class of w_b with respect to $\leftrightarrow_R{}^*$ and then sent to Bob. for example Alice chooses a word $c = \alpha\beta\alpha\beta\beta\alpha\beta\alpha\beta\alpha$,

we have $[c]_{\leftrightarrow_R{}^*} = [w_1]_{\leftrightarrow_R{}^*} = [\beta\alpha]_{\leftrightarrow_R{}^*}$.

Decryption: upon receipt of a word c$\in \{\alpha,\beta\}^*$ a Bob, since $c \leftrightarrow_R{}^* w_b$ and according to the result $\leftrightarrow_R{}^* \subseteq Kerf$, we have $c\ Kerf\ w_b$, then the message is decrypted 1.

In the following proposition we give a condition on the relation of a Thue system to show that the congruence generated by this relation is included in the syntactic congruence class of any word modulo the congruence associated a morphism of monoids. Also we use this included to present the public key cryptosystems based on the Thue Monoid Morphism Interpretation (TMMI).

Proposition 3: Let $f: \Sigma^* \to M$ be a monoids morphism and R is a binary relation on a set Σ^*suth that for all $(r,s) \in R, f(r) = f(s)$. Then for all $w \in \Sigma^*$, the congruence generated by R is included in the syntactic congruence of the equivalence class of w modulo Ker f .i.e,

$$\forall u, v \in \Sigma^*, u \leftrightarrow_R{}^* v \Rightarrow u \equiv_{[w]_{Ker}} v.$$

Proof: Since for all $(r,s) \in R, f(r) = f(s)$, we have $R \subseteq Ker$ f, then $\leftrightarrow_R{}^* \subseteq Ker\ f$. Now we show that $\leftrightarrow_R{}^* \subseteq \equiv_{[w]_{Ker}}$, let $(u,v) \in \Sigma^* \times \Sigma^*$suth that $u \leftrightarrow_R{}^* v$, we check that $u \equiv_{[w]_{Ker}} v$, i.e,

for all $(x,y) \in \Sigma^* \times \Sigma^*, xuy \in [w]_{Ker} \Leftrightarrow xvy \in [w]_{Ker}$

We have $xuy \in [w]_{Ker} \Leftrightarrow xuy \in \bigcup_{i\in I}[c_i]_{\leftrightarrow_R{}^*}$, because $\leftrightarrow_R{}^* \subseteq Ker\ f$. Then $\exists i_0 \in I$ suth that

$xuy \in [c_{i_0}]_{\leftrightarrow_R{}^*}$, then $xuy \leftrightarrow_R{}^* c_{i_0}$. Furthermore $u \leftrightarrow_R{}^* v$ implies that $xuy \leftrightarrow_R{}^* xvy$.

We have $xuy \leftrightarrow_R{}^* c_{i_0}$ and $xuy \leftrightarrow_R{}^* xvy$ implies $xuy \leftrightarrow_R{}^* c_{i_0}$, then $xvy \in [w]_{Ker}$.

A similar argument shows that if $xvy \in [w]_{Ker}$ then $xuy \in [w]_{Ker}$. Finally $\leftrightarrow_R{}^* \subseteq \equiv_{[w]_{Ker}}$.

Example 2: Let $\Sigma = \{\alpha, \beta\}$, $R = \{(\alpha\beta, \beta\alpha)\}$ and $f : \{\alpha, \beta\}^* \longrightarrow \mathbb{N}, f(u) = |u|$.

We have $\Sigma^*/\leftrightarrow_R{}^* = \{[\beta^m\alpha^n]_{\leftrightarrow_R{}^*}, (m,n) \in \mathbb{N} \times \mathbb{N}\}$ and for all $w \in \{\alpha, \beta\}^*$, $[w]_{Ker} = \{x \in \{\alpha, \beta\}^* : |x| = |w|\}$. Now we show that $\leftrightarrow_R{}^* \subseteq \equiv_{[w]_{Ker}}$, let $(u, v) \in \Sigma^* \times \Sigma^*$ such that $u \leftrightarrow_R{}^* v$,

then there exists $(p, q) \in \mathbb{N} \times \mathbb{N}$: u $\leftrightarrow_R{}^* \beta^p\alpha^q$ and v $\leftrightarrow_R{}^* \beta^p\alpha^q$, there ($|u|_\alpha = |v|_\alpha = q$ and $|u|_\beta = |v|_\beta = q$), we check that $u \equiv_{[w]_{Ker}} v$, i.e, for all $(x, y) \in \Sigma^* \times \Sigma^*, xuy \in [w]_{Ker} \Leftrightarrow xvy \in [w]_{Ker}$.

Let $(x, y) \in \Sigma^* \times \Sigma^*$, we have $xuy \in [w]_{Ker} \Leftrightarrow |xuy| = |w| \Leftrightarrow |xvy| = |w| \Leftrightarrow xvy \in [w]_{Ker}$, because ($|u|_\alpha = |v|_\alpha = q$ and $|u|_\beta = |v|_\beta = q$). Finally $\leftrightarrow_R{}^* \subseteq \equiv_{[w]_{Ker}}$.

Proposition 4: Public Key (pK): a finitely presented monoid (Σ,R), and two words w_0,w_1 of Σ^*, with w_0, w_1 are not equivalent with respect to $\leftrightarrow_R{}^*$.

Secret key (sK): let $w \in \Sigma^*$ and to $\leftrightarrow_S{}^* = \equiv_{[w]_{Ker}}$, i.e., $\leftrightarrow_S{}^*$ is the syntactic congruence class of word w with respect to the congruence associated a morphism of monoids. The word problem in $\Sigma^*/\equiv_{[w]_{Ker}}$ is easy, with the property that $\forall u, v \in \Sigma^*, u \leftrightarrow_R{}^* . v \Rightarrow u \equiv_{[w]_{Ker}} v$.

and satisfying also w_0,w_1 are not equivalent with respect to $\equiv_{[w]_{Ker}}$.

Encryption: to encrypt $b \in \{0,1\}$, choose a word $w \in \Sigma^*$ with w$\leftrightarrow_R{}^* w_b$.
Decryption: solve the easy word problem in $\Sigma^*/\equiv_{[w]_{Ker}}$ to find b such that $w \equiv_{[w]_{Ker}} w_b$.

Example 3: Public Key (pK): a finitely presented monoid (Σ, R), where $\Sigma = \{\alpha, \beta\}$, $R = \{(\alpha\beta, \beta\alpha)\}$. We have $\Sigma^*/\leftrightarrow_R{}^* = \{[\beta^m\alpha^n]_{\leftrightarrow_R{}^*}, (m,n) \in \mathbb{N} \times \mathbb{N}\}$. Le $w_0 = \alpha\alpha\beta\beta\beta\beta$ and $w_1 = \beta\beta\alpha\alpha\alpha$, w_0, w_1 are not equivalent with respect to $\leftrightarrow_R{}^*$, because ($|w_0|_\alpha = 2 \neq |w_1|_\alpha = = 3$ and ($|w_0|_\beta = 4 \neq |w_1|_\beta = 2$).

(Σ,R,w_0,w_1) constitute a public key.

Secret key (sK): let $w = \alpha^5\beta^5 \in \{\alpha, \beta\}^*$, $f : \{\alpha, \beta\}^* \longrightarrow \mathbb{N}, f(u) = |u|$. and $\leftrightarrow_S{}^* = \equiv_{[\alpha^5\beta^5]_{Ker}}$, i.e., $\leftrightarrow_S{}^*$ is the syntactic congruence class of word $\alpha^5\beta^5$ with respect to the congruence associated f.

We have $[\alpha^5\beta^5]_{Ker} = \{x \in \{\alpha, \beta\}^* : |x| = |\alpha^5\beta^5| = 10\}$ and

$$u \equiv_{[\alpha^5\beta^5]_{Ker}} v \Leftrightarrow \forall (x, y) \in \{\alpha, \beta\}^* \times \{\alpha, \beta\}^* : |xuy| = 10 \Leftrightarrow |xvy| = 10.$$

The word problem in $\{\alpha, \beta\}^*/\equiv_{[\alpha^5\beta^5]_{Ker}}$ is easy, with the property that

$$\forall u, v \in \Sigma^*, u \leftrightarrow_R{}^* . v \Rightarrow u \equiv_{[\alpha^5\beta^5]_{Ker}} v.$$

We have w_0,w_1 are not equivalent with respect to $\equiv_{[\alpha^5\beta^5]_{Ker}}$ becouse si $x = \alpha\alpha$ and $y = \beta\beta$ then $|xw_0y| = 10$ and $|xw_1y| = 9$.

Encryption: for encrypt a bit $b \in \{0,1\}$, Alice chooses a word c of $\{\alpha, \beta\}^*$ in the equivalence class of w_b with respect to $\leftrightarrow_R{}^*$,, i. e, $c \in [w_b]_{\leftrightarrow_R{}^*}$ where $[w_b]_{\leftrightarrow_R{}^*}$ denotes the equivalence class of w_b with respect to $\leftrightarrow_R{}^*$ and then sent to Bob. for example Alice chooses a word $c = \alpha\beta\beta\alpha\beta\beta$,

we have $[c]_{\leftrightarrow_R{}^*} = [w_0]_{\leftrightarrow_R{}^*} = [\beta^4\alpha^2]_{\leftrightarrow_R{}^*}$.

Decryption: upon receipt of a word c$\in \{\alpha, \beta\}^*$ a Bob, since $c \leftrightarrow_R{}^* w_b$ and according to the result $\leftrightarrow_R{}^* \subseteq \equiv_{[\alpha^5\beta^5]_{Ker}}$, we have $c \equiv_{[\alpha^5\beta^5]_{Ker}} w_0$, then the message is decrypted 0.

Security of TMMI protocol

An attack against TMMI does not allow to find exactly the Secret-Key. We will get rather a key that is equivalent to it in the following direction:

We say that (Σ, S') is an equivalent key to the Secret key (Σ, S) if any message encrypted with the Public Key (Σ, R, w_0, w_1) can be decrypted with (Σ, S'). This is the case for example if (Σ, S') checks the following three conditions:

1. The word problem in $\Sigma^*/\leftrightarrow_S{}'{}^*$ is easy.
2. $\forall u, v \in \Sigma^*, (u \leftrightarrow_R{}^* v) \Longrightarrow (u \leftrightarrow_S{}'{}^* v)$.
3. w_0, w_1 are not equivalent with respect to$\leftrightarrow_S{}'{}^*$.

Now we recall some keys that are equivalent to the Secret key (Σ,S).

1. if $\leftrightarrow_S{}'{}^* \subseteq \leftrightarrow_S{}^*$, then (Σ, S') is an equivalent key to the Secret key (Σ, S).
2. if $S' \subseteq \Sigma^* \times \Sigma^*$, such that $\leftrightarrow_S{}'{}^* = \leftrightarrow_S{}^*$, then (Σ, S') is an equivalent key to the Secret key (Σ, S).

4. Conclusion

In this work, based on the hardness of the word problem for finitely presented monoids, we investigate the public key cryptosystems based on Thue Monoid Morphism Interpretation (TMMI). First, we give a conditions on the relation of a rewrite system to show that the congruence generated by this relation is included in the congruence associated a morphism of monoids, and the congruence generated by this relation is included in the syntactic congruence class of any word modulo the congruence associated a morphism of monoids. Also we use these includeds to present the public key cryptosystems based on the Thue Monoid Morphism Interpretation (TMMI).

References

W. Diffie, M. E. Hellman, "New Direction in Cryptography," IEEE Trans, on Inform Theory, 22(6), P. 644-665, (1976).
N. Ghadbane, D. Mihoubi, "Some attacks of an encryption system based on the word problem in a monoid", Internaional journal of applied Mathematical Research, Vol. 5, No.4, pp. 158-161, (2016).

N. Ghadbane, D. Mihoubi, "Presentation of monoids by generators and relations", Global and Stochastic Analysis, Vol. 3, No.2, pp. 61-73, (2016).
Y. Lafont, "Réécritue et problème du mot," Gazette des Mathématiciens, Laboratoire de Mathématiques Discrètes de Luminy, Marseille, France, (2009).
M. Gonzàlez, R. Steinwandt, "A reaction attak on a public key cryptosystem based on the word problem", Applicable Algebra in Engineering, Communication and Computing, Vol. 14, pp. 335-340, (2004).
H. Phan, P. Guillot," Preuves de sécurité des schémas cryptographiques," université Paris 8, (2013).
E. Post, "Recursive unthenlvability of a problem of Thue,", Journal of Symbolic Logic, 12(1):1-11, (1947).
S. Qiao, W. Han, Y. Li and L. Jiao, "Construction of Extended Multivariante Public Key Cryptosystems," International Journal of Network Security, Vol. 18, No.1, pp. 60-67, (2016).
H. Rosen, "Cryptography Theory and Practice," Third Edition, Chapman and Hall/CRC, (2006).
N. R. Wagner, M. R. Magyarik. A Public Key Cryptosystem Based on the Word Problem. Proceedings of CRYPTO'84, LNCS 196, Springer-Verlag, pp. 19-36, (1985).
A. Salomaa, S. Yu, "On a public key cryptosystem based on iterated morphisms and substitutions", Theoretical Computer Science, Vol. 48, pp. 283-296, (1986).