ISSN 1392 – 124X INFORMACINĖS TECHNOLOGIJOS IR VALDYMAS, 2004, Nr. 2(31)

DIGITAL SIGNATURE SCHEME BASED ON ACTION OF INFINITE RING

Eligijus Sakalauskas, Tomas Burba

ASI Laboratory of Information Energetic Systems
Kaunas University of Technology, Lithuania

Abstract. An original digital signature scheme based on action of infinite ring on module is presented. It is assumed that the ring contains an infinite multiplicative monoid. The ring action is defined as monoid elements's action on the module element as an operator.

The signature scheme is based on particularly designed one–way functions (OWFs), using a postulated hard problem in monoid action level.

The investigation of signature scheme security against three kinds of attacks is presented. Referencing to the postulated OWFs, the proposed signature scheme has provable security property.

Key words: Digital signature scheme, one–way function, ring, monoid, group.

1. Indroduction

In recent time, there appeared two challenges in protection of cryptographic information:

1. Cryptosystem implementation in limited environments like PDA's, mobile phones and smart cards. RSA or ElGamal type algorithms based on integer factorization and discrete logarithms are not well suited for that because they require large integer modular arithmetic and therefore costly special co–processors.
2. The most worrisome threat appeared to integer factorization and discrete logarithm cryptosystems (including elliptic curve discrete logarithms) comes from quantum computers. (Shor, 1997) showed that if such machines could be built, integer factorization and discrete logarithms could be computed in polynomial time. The vulnerable ones are RSA and ElGamal cryptosystems.

According to our knowledge, the first signature scheme designed in infinite non-commutative groups appeared in (Ko *et al.*, 2002). This invention is based on an essential gap existing between the conjugacy decision problem (CDP) and conjugator search problem (CSP) in non–commutative group. This means that CSP is hard and CDP is feasible. The conjugation operation serves for signing and CDP provides a verification procedure. This scheme may be called a pure scheme based on group formalism, i.e. applying a group presentation level only. The motivation of this solution appears from the fact that traditional signature schemes require a compatible addition operation together with an existing single group multiplication operation or, in other words, with the conjugation operation. As it is clear, the group presentation level provides only one binary operation according to its definition.

Algebraic terms used in this study can be found in (van der Waerden, 1967).

We consider a group or monoid having an infinite number of elements we will call words. As usual, we reckon the word consists of some primitive elements called generators or atoms.

Similarly to (Ko *et al.*, 2002), our scheme also uses an infinite non-commutative group but only as an auxiliary system to construct a formal ring with elements acting as operators on a certain compatible module. Addition operation is defined for multiplicative group elements. So we obtain a new set with multiplication and addition operations and define it as a ring. Then instead of separately defined non-commutative group we have a non-commutative group in the ring as a subset. This group generates a multiplicative monoid in the ring applying all possible combinations of multiplication and addition operations with its elements. In general, each monoid element consists of sum of words, since the distributivity property takes place in the ring. So, each word is an element of generating group.

An infinite non-commutative group we consider as defined by finite set of generators and a relations (Magnus *et al*., 1966). In doing so both the group and the monoid have two level attributes: presentation level and action level. The same relations can be applied for every word included in ring element.

Finite set of generators and relations define the ring presentation level. The ring action level is a ring element action on the module as an operator. For an operator action on the module element the special binary operation is introduced. We treat an action operation as multiplicative operation having a distributivity property with respect to addition.

As was mentioned before, the introduced addition operation is formal, *i. e.* has no sense in the monoid presentation level, but has a concrete meaning in the ring action level. This means that the addition operation in the ring is compatible with an addition operation defined in the module. Then the module is said to be compatible with a ring (or monoid). The defined action operation is linked with multiplication in monoid and ring by mutual associativity property.

We introduce some problem called a Ring Action Problem (RAP) and reckon it as hard. The RAP in our case has the same sense as Monoid Action Problem (MAP). On this basis we will construct an One-Way Function (OWF) for creation of a signature scheme.

Historically, some attempts were made for a cryptographic primitives construction using more complex algebraic systems instead of traditional finite cyclic groups or finite fields during the last decade. The originator in this trend was (Sidelnikov *et al.*, 1993), where a proposition to use non-commutative groups and semigroups in session key agreement protocol is presented.

Some realization of key agreement protocol using (Sidelnikov, 1993) methodology with application of the semigroup action level could be found in (Sakalauskas and Burba, 2003). Some concrete construction of commutative sub-semigroup is proposed there.

Traditionally, the main problems for a cryptographic primitive's construction in the case of non-commutative groups is the word equivalence problem (word problem) and conjugator search problem (CSP), (Ko *et al*., 2000). The word problem must be solvable and the CSP must be intractable. Both these problems are considered in the non-commutative system presentation level, defining a finite set of generators and relations. For a cryptographic primitives design the OWF is constructed using the infeasible CSP as a core.

As usual, the solution of the word problem in groups is based on the normal (canonical) forms' construction (Dehornoy and Paris, 1999 / Ko *et al*., 2000). These normal forms, when used for cryptographic purposes, must reliably hide an information about the secret factors of the considered word. The unsolvability in general of the word problem for semigroups was proved by (Markov, 1947) and (Post, 1947). This means that there is no unique normal form for equivalent words in general semigroup. So the cryptographic primitives' construction in presentation level in general semigroups is problematic.

(Monico, 2002) has presented an example of cryptosystem based on finite semigroup action problem (SAP). It is a direct generalization of Diffie–Hellman key exchange algorithm using finite semigroup of matrices or matrix polynomials over a finite vector field. As a consequence the proposed SAP is a multi–dimensional generalization of traditional (one–dimensional) discrete logarithm problem (DLP) and is more hard. This cryptosystem is used for session key agreement protocol and ElGamal cryptosystem. According to the author, this cryptosystem requires further investigations and first of all the secure key length needs to be determined.

We think the action level introduction in complex algebraic systems serves to a word problem solution in this level much more easy than in the presentation level. Then there is no matter about the word problem complexity in presentation level. As a consequence, the CSP and other problems in group or monoid presentation level may be as hard as possible since we have no doubt about this complexity.

We present now some formal digital signature scheme based on the ring action on a module here. The postulated OWF is based on the RAP, which is treated as infeasible. To construct a signature, the word problem in semigroup presentation level is replaced by the word problem in action level, *i. e*. in the module where the word problem is reckoned feasible. Then we are able to choose the construction of monoid and ring as complex as possible taking no matter about the complexity of word problem solution in it.

Finally, we define some notations for signature creation and verification.

We denote the message space consisting of finite length binary strings by T. Let a signer Alice intends to sign some message $T_A \in T$ and to send it to a verifier Bob. As usual, Alice signs not a message T_A but some h–value m of the original message. Assume that there are two publicly available cryptographically secure h–functions (Menezes *et al.*, 1996), surjective function H and injective h. The data to be signed is expressed as $m = H(T_A)$.

Alice creates a signature S on value m and sends it to verifier Bob. Bob has a publicly available verification function Φ to verify the signature S on m.

Alice and Bob communicate through insecure and open communication channels and all the data published and transmitted are available to the active adversary Eve. All parties share information about the structure of ring $\mathtt{R}$, module $\mathtt{M}$, hash functions H and h, verification function Φ and public key of Alice. Eve can obtain, remove, forge and retransmit any message Alice sends to Bob.

In section 2 we present some basic concepts as preliminaries for signature scheme construction. We introduce a general infinite ring on the basis of infinite non-commutative Gaussian group acting on certain compatible module. The suitable OWF construction is presented.

We present a signature scheme in section 3.

Security analysis for three kinds of attacks is presented in section 4.

Section 5 is dedicated to some discussions on the presented signature scheme. Some considerations of security of this signature scheme are also presented there.

2. Preliminaries

The main definitions and notations used in this study are in (van der Waerden, 1967).

Let us consider some Gaussian group, presented by a finite set of generators and relations, and designated by the pair $(\mathbf{G}, \cdot)$ (Dehornoy and Paris, 1999). For elements of **G** we formally introduce an additive operation +. Assume that multiplication is distributive with respect to addition operation. We denote as **G'** the set of all available sums of elements in **G**. By combining the elements in $\mathbf{G} \cup \mathbf{G'}$ using a multiplication and addition operations we can obtain the new set **R**. Then **R** is a ring which can be denoted by the triplet $(\mathbf{R}, \cdot, +)$. The corresponding pair $(\mathbf{R}, \cdot)$ is a monoid which we denote as $\mathbf{G}_+$.

The monoid $\mathbf{G}_+$ is not a Gaussian monoid that is embedded in its group G of fractions in the sense of (Dehornoy and Paris, 1999). It is clear that $\mathbf{G} \subset \mathbf{G}_+$. The monoid $\mathbf{G}_+$ has the same set of generators and relations as group G which constitutes a monoid $\mathbf{G}_+$ presentation level. The monoid $\mathbf{G}_+$ has an unity element 1, such that for any $g \in \mathbf{G}_+$,

$$1 \cdot g = g \cdot 1 = 1 .$$

Accordingly the inverse element $\eta^{-1} \in$ G, satisfies the relations

$$\eta^{-1} \cdot \eta = \eta \cdot \eta^{-1} = 1 .$$

The set in R which has no multiplicative inverse elements we denote as $\mathbf{R} \setminus \mathbf{G}$.

We consider some module formally defined by the pair $(\mathbf{M}, +)$ over monoid $\mathbf{G}_+$ and at the same time over the ring **R**. As convenient the module is an additive abelian group.

Assume that there is an opportunity to define two mutually commutative subsets $\mathbf{R}_L$, $\mathbf{R}_R$ in $\mathbf{R} \setminus \mathbf{G}$. Then for any $s \in \mathbf{R}_L$ and $r \in \mathbf{R}_R$ the commutation property holds:

$$s \cdot r = r \cdot s.$$

We consider **R** as a ring of operators or multipliers acting on module **M**. Then as convenient **M** is called a module over the ring **R** or in other legal notation as **R**-module. For this action we introduce a new associative binary operation (function) $\circ: \mathbf{R} \times \mathbf{M} \to \mathbf{M}$. This means that for all $s \in \mathbf{S}$ and $m \in \mathbf{M}$ there exists $k \in \mathbf{M}$, such that

$$k = s \circ m .$$

The $\circ$ operation is a ring action operation on module.

We define the following order of the introduced associative operations $\cdot$, $\circ$ and + for $s, r \in$ R and $m, n \in$ M as illustrated by the following equation

$$s \cdot r \circ m + n = ((s \cdot r) \circ m) + n = (s \circ (r \circ m)) + n .$$

According to this and the associativity of operations applied, the following expressions are equivalent

$$(r \cdot s) \circ m = r \cdot s \circ m = r \circ (s \circ m) = r \circ s \circ m ;$$

Assume that the following distributive relations are valid for all $s, r \in \mathbf{R}$ and $m, n \in \mathbf{M}$

$$(r + s) \circ m = r \circ m + s \circ m ;$$

$$r \circ (m + n) = r \circ m + r \circ n .$$

For a signature scheme design the One-Way Function (OWF) construction is required. For that we restrict the $\circ$ to the domain $\mathbf{R} \setminus \mathbf{G}$. Then $\circ$ performs a mapping $\circ: \mathbf{R} \setminus \mathbf{G} \times \mathbf{M} \to \mathbf{M}$. Assume also that two mutually commutative subsets $\mathbf{R}_L$, $\mathbf{R}_R$ defined above are in $\mathbf{R} \setminus \mathbf{G}$.

So we postulate that this $\circ$ is the OWF. This also means that the corresponding Ring Action Problem (RAP) is hard, *i. e.* this means that neither having $a \in \mathbf{M}$ and $s \in \mathbf{R} \setminus \mathbf{G}$ we can not find $m \in \mathbf{M}$ and symmetrically nor having $a \in \mathbf{M}$ and $m \in \mathbf{M}$ we cannot find $s \in \mathbf{R} \setminus \mathbf{G}$ from the equation

$$a = s \circ m.$$

In the well known partial case of **S** being a cyclic group of prime order p and m being an integer, one can construct the OWF based on Discrete Logarithm Problem (DLP)

$$a = s \circ m = s^m \bmod p.$$

(Monico, 2002) has presented an example of cryptosystem based on the finite Semigroup Action Problem (SAP). It is a direct generalization of DLP, using finite semigroup of matrices or matrix polynomials over finite vector field. The proposed SAP is a multi–dimensional generalization of traditional (one-dimensional) DLP and is more hard.

The message space consisting of finite length binary strings we denote by T. Let Alice intends to sign some message $T_A \in T$ and send it to Bob. Assume that there are available two publicly known cryptographically secure h-functions (Menezes *et al.*, 1996) H and h , performing the following mappings

$$H: T \to \mathbf{M} ;$$

h: $\mathbf{M} \to \mathbf{R_R}$.

Function H is surjective and h is injective.

3. Signature creation and verification

3.1. Key generation. Alice chooses at random secret elements $\alpha \in \mathbf{R_L}$, $\eta \in \mathbf{G}$ and $x \in \mathbf{M}$. Then she calculates an element $a \in \mathbf{M}$ and $\rho \in \mathbf{R}$

$a = \eta \circ \alpha^2 \circ x$,

$\rho = \eta \cdot \alpha \cdot \eta^{-1}$.

Then the Private Key (PrK) and Public Key (PuK) are as follows:

PrK = (α , η, x) ; PuK = (a , ρ) .

3.2. Signature creation. Alice takes a message $T_A \in T$ to be signed, chooses at random $\xi \in \mathbf{R}$ and calculates h-values $m \in \mathbf{M}$ and $\mu \in \mathbf{R_R}$:

$m = H (T_A)$;

$\mu = h (\xi \circ m)$.

The secret signature key is ξ.

She calculates the following signature parameters

$\sigma = \eta \cdot \mu \cdot \eta^{-1}$;

$s = \sigma \circ (\eta \circ \alpha \circ x + m)$.

Alice forms the following signature for message T_A

$S = (\sigma , s)$.

3.3. Signature verification. After receiving message T_B and assuming that it is original, i.e. $T_B = T_A$, Bob calculates

$m_B = H (T_B)$.

Having signature's S components σ and s, and assuming that $m_B = m$, the verification function $\Phi = \Phi (m, \sigma, s)$ is TRUE if

$$\rho \circ s = \sigma \circ a + \rho \circ \sigma \circ m . \quad (V)$$

The validity of (V) follows from the equations

$$\begin{aligned} \rho \circ s &= \rho \circ (\sigma \cdot \eta \cdot \alpha \circ x + \sigma \circ m) = \\ &= \eta \cdot \alpha \cdot \eta^{-1} \cdot \eta \cdot \mu \cdot \eta^{-1} \cdot \alpha \circ x + \rho \circ \sigma \circ m = \\ &= \eta \cdot \alpha \cdot \mu \cdot \alpha \circ x + \rho \circ \sigma \circ m = \\ &= \eta \cdot \mu \cdot \alpha^2 \circ x + \rho \circ \sigma \circ m = \\ &= \eta \cdot \mu \cdot \eta^{-1} \cdot \eta \cdot \alpha^2 \circ x + \rho \circ \sigma \circ m = \\ &= \sigma \circ a + \rho \circ \sigma \circ m. \end{aligned}$$

In general, the condition presented here is sufficient for validity of verification function Φ. This is proved for three main kinds of attacks considered in the next section.

4. Security analysis

Assume that the active eavesdropper Eve can obtain, remove, forge and retransmit any message Alice sends to Bob. Any forgered data d we denote as d^F.

Consider security of signature scheme for three main attacks: data forgering on valid signature, signature repudiation on valid data and existential forgering.

4.1. Data forgering

Assume Eve replaces the original message T_A with forgered one T_A^F . Then she sends T_A^F to Bob. Bob having H calculates

$m^F = H(T_A^F)$,

and taking signature $S = (\sigma, s)$ verifies if $\rho \circ s$ is equal to $\sigma \circ q + \sigma \circ \rho \circ m^F$. Verification fails, because

$$\rho \circ s = \sigma \circ a + \sigma \circ \rho \circ m \neq \sigma \circ a + \sigma \circ \rho \circ m^F .$$

Another attempt is to try to find T_A^F for a valid m. But this is impossible because we assumed that h-function H is cryptographically secure.

So the invalid data can not be signed with a valid signature.

4.2. Signature repudiation.

Assume Alice intends to refuse recognition of his signature on some valid data. Then it follows that valid signature $S = (\sigma, s)$ can be forgered by Eve and she can sign the message m with forgered signature $S^F = (\sigma^F , s^F)$ instead. The verification procedure obtains that

$$\begin{aligned} \rho \circ s^F &= \rho \circ \sigma^F \circ \eta^F \circ \alpha^F \circ x + \rho \circ \sigma^F \circ m = \\ &= \eta \cdot \alpha \cdot \eta^{-1} \cdot \eta^F \cdot \mu^F \cdot \eta^{F-1} \cdot \eta^{F-1} \cdot \alpha^F \circ x^F + \rho \circ \sigma^F \circ m, \end{aligned}$$

where $\sigma^F = \eta^F \cdot \mu^F \cdot \eta^{F-1}$.

But $\eta^{-1} \cdot \eta^F \neq 1$ and $\alpha \cdot \alpha^F \neq \alpha^2$ and therefore

$\rho \circ s^F \neq \sigma^F \circ a + \rho \circ \sigma^F \circ m$

So this signature scheme ensures the non-repudiation property.

4.3. Existential forgering

An existential forgering is defined in (Goldwasser, 1988).

Assume Eve is trying to sign a forgered message T_A^F. Then she must to forge the parameters of PrK replacing them by α^F, η^F, x^F and perform the following calculations by choosing some $\xi^F \in \mathbf{S}$

$m^F = H (T_A^F)$

$\mu^F = h (\xi^F \circ x^F)$

$\sigma^F = \eta^F \cdot \mu^F \cdot \eta^{F-1}$

The forgered data must satisfy the equation (V)

$\rho \circ s^F = \sigma^F \circ a + \rho \circ \sigma^F \circ m^F$

Then Eve must determine s^F having m^F and σ^F which satisfy the last equation.

Let us formally write the equation

$$s^F = \rho^{-1} \circ (\sigma^F \circ a + \rho \circ \sigma^F \circ m^F),$$

taking in mind that $\rho^{-1} \circ \rho = 1$ and $1 \circ s^F = s^F$.

Then let also

$$\rho^{-1} = \eta \cdot \alpha^{-1} \cdot \eta^{-1} .$$

But according to definition of h function both μ and μ^F are in R_L, and R_L is a subset of $\mathbf{R} \setminus \mathbf{G}$. Hence μ^{F-1} does not exist and so does ρ^{-1}.

So Eve is not able to calculate forgered s^F, having m^F and σ^F.

5. Discussion

We have presented an abstract signature scheme based on the action of ring R on certain module M (R-module). We think that there is a possibility to construct such an algebraic structure using a Gaussian group as a construction material and to choose a module compatible to it. So the signature scheme is based on the three main constructions:

1. A certain ring R acting on module M as a ring of operators, defined above.

2. Commutative subsets $\mathbf{R_L}$, $\mathbf{R_R}$ in $\mathbf{R}$, defined above.

3.The OWF postulation based on the Ring Action Problem (RAP).

It is proved that our scheme is invulnerable against three main kinds of attacks investigated above. Referencing to postulated OWFs, this means that our scheme has a provable security property.

Proposed signature scheme does not require arithmetic calculations with large integers and so it could be more easily implemented in PDAs than RSA or ElGamal cryptosystems.

Finally, so far we have no any knowledge about quantum information algorithms capable to break a cryptosystem based on infinite non-commutative algebraic systems. The same, of course, is valid for our scheme as well. Therefore, we think that the signature scheme there presented requires further investigations as possible alternative to the traditional RSA and ElGamal signature schemes.

References

[1] **P. Dehornoy, L. Paris.** Gaussian groups and Garside groups: two generalizations of Artin groups. *Proc. London Math. Soc*. 79(3), 1999, 569 – 604.

[2] **S. Goldwasser, S. Micali, R. Rivest.** A digital signature scheme secure against adaptive chosen message attacks. *SIAM J. Comput*. 17, 1988, 281 – 308.

[3] **Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju–sung Kang, Choonsik Park.** New Public–key Cryptosystem Using Braid Groups. *Advances in Cryptology, Proc. Crypto* 2000, *LNCS* 1880, *Springer–Verlag,* 2000, 166–183.

[4] **Ki Hyoung Ko, Doo Ho Choi, Mi Sung Cho, Jang Won Lee.** New Signature Scheme Using Conjugacy Problem. *Department of Mathematics, KAIST, Daejeon*, 2002, *http://eprint/iacr.org.*

[5] **W. Magnus, A. Karrass, D. Solitar.** Combinatorial Group Theory. *Interscience Publishers, NY*, 1966.

[6] **A. Markov.** On the impossibility of certain algorithms in the theory of associative systems. *Dokl. Acad. Sci. URSS* 55, 1947, 583-586.

[7] **A. Menezes, P. van Oorschot and S. Vanstone.** Handbook of applied Cryptography. *CRC Press*, 1996.

[8] **C. Monico.** Semirings and Semigroup actions in Public-Key Cryptography. *Phd thesis, University of Notre Dame, May* 2002.

[9] **E. Sakalauskas, T. Burba.** Basic semigroup primitive for cryptographic Session Key Exchange Protocol (SKEP). *Information Technology and Control. ISSN* 1392-124X. 2003, *No*.3(28).

[10] **P. W. Shor.** Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput*., 26, 1997, 1484-1509.

[11] **V. Sidelnikov, M. Cherepnev, V. Yaschenko.** Systems of open distribution of keys on the basis of noncommutative semigroups. *Russian Acad. Sci. Dokl. Math*., 48(2), 1993, 566-567.

[12] **B. L. van der Waerden.** Algebra. *Springer-Verlag*, 1967.