INFORMATICA, 2005, Vol. 16, No. 3, 383–394

One Digital Signature Scheme in Semimodule over Semiring

Eligijus SAKALAUSKAS
Kaunas University of Technology, Department of Applied Mathematics
Studentų 50, 51368 Kaunas, Lithuania
e-mail: esakal@asi.lt

Received: September 2004

Abstract. A modernization of signature scheme published in (Sakalauskas, 2004) is presented. This scheme differs from the prototype by its structure and uses a more general algebraic systems. It has a higher security and shorter key length and is also more computationally effective.

The introduced new algebraic structures, semiring and semimodule, are mutually compatible algebraic systems. The semiring is a set of operators acting in a semimodule as endomorphisms. There is postulated that action operation has a one-way function (OWF) property. The compatibility of both algebraic structures' means that the action operation has right and left distributivity property with respect to the additive operation defined in semimodule and semiring.

Two other essential OWFs are defined. The latter are based on known constructions and have a greater complexity than other recognized hard problems such as conjugator search problem in noncommutative groups, for example.

Key words: digital signature scheme, one-way function, Gaussian group, semiring action problem.

1. Introduction

We would like to present there a modernization of signature scheme appeared in (Sakalauskas, 2004). In the previously published paper we used a two-stage scheme: the encryption of message's H – function by the signer's private key and the authentication of this encryption using signature parameters and a public key.

In current paper we propose the one stage signing instead of using two stages and so we reduce the key length used and achieve more effective computations. We also reformulate the basic hard problems for One Way Functions' (OWFs) construction and performe some generalization of used algebraic systems. These modifications increase the security of obtained signature scheme.

The designed scheme is based on some generalization of previously used vector space to the semimodule and requires introduction of a semiring (instead of a monoid) being a semiring of operators acting in this semimodule. The semiring and semimodule are compatible in the sense that the operators in semiring are treated as endomorphisms in semimodule. So the action operation could be treated as multiplication and is right distributive with respect to the addition operation defined in semimodule. The addition operation in semiring is the same as defined in semimodule and is introduced formally. It has sense only in the context of semiring action in the semimodule. So this addition operation has also a left and right distribution property.

The main concepts and problem survey of proposed scheme could be found in (Sakalauskas, 2004).

The new construction of algebraic structures are presented in Section 2.

Signature creation and verification is described in Section 3.

Section 4 provides a proof of signature security for three kinds of attacks: private key compromitation, signature + data forgering and data forgering causing a repudiation possibility.

A brief analysis on the designed scheme is presented in Section 5. Referencing to this analysis the designed signature scheme could be compared with other known signature schemes as in (Sakalauskas, 2004).

2. Construction of Algebraic Structures

The main definitions used in this section could be found in (van der Waerden, 1967).

We consider some semimodule $(M, +)$ over semiring $(R, \cdot, +)$. The semiring R is treated as a set of operators acting in semimodule M.

According to the definition (van der Waerden, 1967), module is an additive Abelian group over some set of operators. It is a generalization of vector space. Instead of a module we consider its generalization, i.e., semimodule M which is an additive Abelian semigroup. In our case we do not require for the semimodule to have an inverse element $(-m)$ for any $m \in M$ but we assume there exists a zero element 0 such that $m + 0 = 0 + m = m$. So the semimodule M is an additive Abelian monoid.

The semiring means that $(R, \cdot, +)$ is a semigroup with respect to both addition and multiplication and the distributive law holds. More precisely we consider a semiring which is a non-commutative monoid with respect to multiplication, and an Abelian semigroup with respect to addition. Then $(R, \cdot)$ has an unity element 1. Analogously to the definition of semimodule M we assume that $(R, +)$ has no inverse elements and has a zero element 0. So $(R, +)$ could be treated as a semimodule in the semiring, i.e., an internal Abelian additive monoid, while $(M, +)$ is an external semimodule over the semiring R.

We define now an action of semiring R on semimodule M. R is a semiring of endomorphisms acting in M. This means that for any $\mu \in$ R there exists a mapping μ: $M \rightarrow M$. The action operation we denote as *. Then for any $\mu \in R,\ m \in M$ there exists $n \in M$ such that

$$\mu * m = n.$$

In the semiring we consider some subset $J \subset R$ with elements having its multiplicative inverses. This means that for any $\alpha \in J$ there exists α^{-1} such that

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

Let us define the structure of J in R more precisely. According to (Sakalauskas, 2004) consider some infinite non-commutative group G presented by finite set of atoms and relations (Magnus *et al.*, 1966) and let $J = G$. Assume, for example, this group is Gaussian group $(G, \cdot)$ (Dehornoy and Paris, 1999). For all $\alpha, \beta \in G$ we can formally introduce an addition operation + having in mind that $(\alpha + \beta)$ is the element belonging to the semiring R. In this case G could be treated as a generator of R (Kurosh, 1974). Then J is a multiplicative group G in R.

Recall that the elements of G are called words and words consist of products of atoms or their inverses. Then the variety of products and sums of words are the elements of R. For example assume the set of atoms is $\{\ \alpha_1, \alpha_2, ..., \alpha_n\} \subset G$. Then any word w in G can be expressed as

$$w = \alpha_i^{\pm 1} \cdot \alpha_j^{\pm 1} \cdot ... \cdot \alpha_k^{\pm 1}.$$

Due to distributivity condition in R any composition of elements using $\cdot$ and + operations can be expressed by sums of words. For example, if $w_1, w_2, w_3 \in R$, then

$$w_1 \cdot (w_2 + w_3) = w_1 \cdot w_2 + w_1 \cdot w_3 = w_{12} + w_{13}; w_{12}, w_{13} \in G.$$

The relations defined in G are not valid for the arbitrary elements of R but only for the words in G. So if $w_4 = w_1 \cdot (w_2 + w_3)$ then relations of G does not hold for w_4 but they hold for each of w_1, w_2, w_3 separately if they all are words in G, i.e., they consist of atoms.

For any word $w_0 \in G$ one can define its equivalency class $[w_0]$ consisting of elements, which were obtained by applying any relation in G to element w_0. This is called equivalence transformations in G. As usual these transformations for certain groups can be used for words' equivalence problem solution (Ko, *et al.*, 2000, Dehornoy and Paris, 1999).

According to the considerations above the subset J we can treat both as a group G generating R, or as a subset in R having inverse elements. Especially J consist of such elements which are not composed of sums + of other semiring elements. Then the complement of J in R consists of elements composed of sums + and having no inverses. This complement set we denote by $R \backslash J$.

Further the elements of J we call words and the elements of $R \backslash J$ we call terms. Recall that a term consists of at least one formal addition of words. The sense of addition operation in R will be explained below.

We formulate now two essentially hard problems, which according to (Rabi and Sherman, 1993) could be treated as one-way functions (OWF).

P1. Multiple Factors' search problem (**MFSP**).

Having $\rho \in R \backslash J$, find words $\alpha, \beta \in$ J and term $\eta \in R \backslash J$ satisfying equation

$$\rho_0 = \alpha \cdot \eta \cdot \beta, \tag{P1}$$

where ρ is equivalent to the unknown ρ_0 in the sense of relations, defined in J, i.e., $\rho \in [\rho_0]$.

For example, in the case when $J = G$ and G is a Gaussian group, the factors α, β and η can be efficiently hidden using equivalence transformations for words. One kind of these transformations is a Dehornoy normal form (Dehornoy and Paris, 1999). The other one could be random atoms' mixing transformations proposed in (Sakalauskas, 2004). When G is a Braid group, then the left weighted canonical form transformation could be applied (Ko *et al.*, 2000).

For example, MFSP is evidently infeasible in sufficiently large index Braid group B (Ko *et al.*, 2000), when left weighted canonical form is applied. This problem is much more complicated than conjugator search problem (CSP) which is widely recognized as infeasible. In the case when R is generated by B, the left weighted canonical form transformation must be applied to the words presented in element ρ_0.

P2. Operator and Operand search problem (**OOSP**).

Having $a \in M$, find $\rho \in R\backslash J$ and $x \in M$ from the equation

$$a = \rho * x. \tag{P2}$$

A good example might be the problem expressed by the well known relation

$$a = \rho * x = x^{\rho} \bmod p,$$

where x, ρ are natural numbers (x must be a generator of cyclic group of order p) and p is a prime. In this example according to our definition x and ρ are unknown and require to be determined. Evidently this problem is much more hard than the corresponding Discrete Logarithm Problem.

The problems (P1), (P2) are called essential, because they are very natural and easy realizable in a wide variety of known examples of algebraic systems.

Both MFSP and OOSP can be treated as OWFs and they are used for our scheme construction.

Beside the essential OWFs defined above we define now two operation-related OWFs. It is required to redefine the operation * and to introduce a new operation which we denote as $\oplus$.

Redefine action operation * as the mapping * : $R\backslash J \times M \to M.$

P3. * Operand Search Problem **(*OSP**).

For given ρ and b it is infeasible to find m from the equation

$$\rho * m = b.$$

Having in mind that $\rho \in R\backslash J$, the inverse element ρ^{-1} does not exist and therefore it is impossible to find m from the equation

$$\rho^{-1} * \rho * m = m = \rho^{-1} * b.$$

We have assumed that R is a semiring of endomorphisms of semimodule M. More exactly a fixed endomorphism corresponding to $\rho \in R\backslash J$ may be expressed as a mapping $\rho *$: $M \to M$. Then, according to any morphism definition, operation * satisfies the right distributivity condition with respect to operation + in M

$$\rho * (m + n) = \rho * m + \rho * n,$$

where $m, n \in M$.

To provide a sense for operation + in R we define a left distributivity property in the form

$$(\rho + \sigma) * m = \rho * m + \sigma * m,$$

where $\rho, \sigma \in R, m \in M$.

Then it is clear that regardless of whether the element $(\rho + \sigma)$ has no meaning in the generating group G, it has a sense, considering that $(\rho + \sigma)$ is an operator in M due to right distributivity property.

Let us introduce the second additive operation in M, related with any $\rho \in R$ and denoted by $\oplus$.

$$m \oplus n = \rho * m + \rho * n.$$

For convenience, we fix a certain operation $\oplus$ for a particular $\rho \in R$.

P4. $\oplus$ Operand Search Problem **(**$\oplus$**OSP**).

PROPOSITION 1. If * is OWF then $\oplus$ is OWF.

Proof. We show that for given $n, b \in M$ it is hard to find m from the equation
$m \oplus n = b$.

This equation can be rewritten in the form
$\rho * (m + n) = b$.

According to P3 it is infeasible to find $m + n$ for given ρ, b. This implies that it is infeasible to find m.

It is clear from the definition that $\oplus$ is a right distributive as well.

We have constructed two operations-based OWFs denoted as *OSP and $\oplus$OSP, required for signature scheme design.

Define now the order of operations $\cdot, *$ and + for our construction. Both $\cdot$ and * are distributive with respect to addition +. For any $\rho \in R$ and $m \in M$ the term $\rho \cdot m$ has no sense. The following identities take place for any $\rho, \sigma \in R$ and $m, n \in M$

$$\begin{aligned}
\rho * m + \sigma * n &= (\rho * m) + (\sigma * n),\\
\rho \cdot \sigma * (m + n) &= (\rho \cdot \sigma) * (m + n)\\
&= \rho * \sigma * (m + n)\\
&= \rho * \sigma * m + \rho * \sigma * n\\
&= \rho \cdot \sigma * m + \rho \cdot \sigma * n.
\end{aligned}$$

The same equations are valid when $\oplus$ is used instead +.

Similarly to (Sakalauskas, 2004) we define two mutually commutative subsets $R_L, R_R \subset R\backslash J$, so that

$$\sigma \cdot \rho = \rho \cdot \sigma,$$

when $\sigma \in R_L, \rho \in R_R$.

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 mappings

$$H\colon\ T \to M;$$
$$h\colon\ M \to R_L.$$

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 semiring R, semimodule 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.

3. Signature Creation and Verification

3.1. *Key Generation*

Alice chooses at random $\alpha, \beta \in J,\ \eta \in R_R$ and $x \in M$.

Then she calculates

$$\rho = \alpha \cdot \eta \cdot \beta^{-1},$$
$$\rho' = \beta \cdot \eta \cdot \alpha^{-1},$$
$$a = \rho' * x.$$

The Alice's Private Key (PrK) and Public Key (PuK) are as follows:

$$PrK = (\alpha, \beta, x); \quad PuK = (\rho, a).$$

Parameters η and ρ' are temporary and are not required for further applications.

3.2. *Signature Creation*

Alice takes a message $T_A \in T$ to be signed and chooses at random $\xi \in R_L$, commuting with element η. She calculates the following elements:

$$\begin{aligned}
&m = H(T_A),\\
&\mu = h(\xi * m),\\
&\sigma = \alpha \cdot \mu \cdot \beta^{-1},\\
&\sigma' = \beta \cdot \mu \cdot \alpha^{-1},\\
&\zeta' = \alpha \cdot \xi \cdot \beta^{-1},\\
&\zeta = \beta \cdot \xi \cdot \alpha^{-1},\\
&s = \sigma' * (x \oplus \zeta' * m).
\end{aligned}$$

Secret signature key is ξ. The signature S parameters are

$$S = (s, \sigma, \zeta).$$

Alice sends S and T_A to Bob.

3.3. *Signature Verification*

Assume Bob receives from Alice message T_B which he reckons to be original, i.e., $T_B = T_A$. Then Bob calculates H-value

$$m_B = H(T_B).$$

Having S, Bob calculates semimodule element $\rho*$ s $\in M$, having access to the Alice's PuK.

The signature S on H-value m_B is accepted if the verification function $\Phi = \Phi(m_B, s, \sigma, \zeta)$ is TRUE. The validity verification function Φ is defined by the equation

$$\rho * s = \sigma * (a \oplus \zeta * \rho * m). \tag{V}$$

The proof of verification condition (V) follows from the expressions

$$\begin{aligned}
\rho * s &= \rho * \sigma' * x \oplus \rho * \sigma' * \zeta' * m\\
&= \alpha \cdot \eta \cdot \beta^{-1} \cdot \beta \cdot \mu \cdot \alpha^{-1} * x \oplus \alpha \cdot \eta \cdot \beta^{-1} \cdot \beta \cdot \mu \cdot \alpha^{-1} \cdot \alpha \cdot \xi \cdot \beta^{-1} * m\\
&= \alpha \cdot \eta \cdot \mu \cdot \alpha^{-1} * x \oplus \alpha \cdot \eta \cdot \mu \cdot \xi \cdot \beta^{-1} * m\\
&= \alpha \cdot \mu \cdot \eta \cdot \alpha^{-1} * x \oplus \alpha \cdot \mu \cdot \xi \cdot \eta \cdot \beta^{-1} * m\\
&= \alpha \cdot \mu \cdot \beta^{-1} \cdot \beta \cdot \eta \cdot \alpha^{-1} * x \oplus \alpha \cdot \mu \cdot \beta^{-1} \cdot \beta \cdot \xi \cdot \alpha^{-1} \cdot \alpha \cdot \eta \cdot \beta^{-1} * m\\
&= \sigma * a \oplus \sigma * \zeta * \rho * m\\
&= \sigma * (a \oplus \zeta * \rho * m).
\end{aligned}$$

The proof is based on the identities $\eta \cdot \mu = \mu \cdot \eta, \eta \cdot \xi = \xi \cdot \eta, \alpha^{-1} \cdot \alpha = 1, \beta^{-1} \cdot \beta = 1$, distributivity property and relations defined between * and $\cdot$ from above.

4. Security Analysis

Assume that the active eavesdropper Eve can obtain, remove, forge and retransmit any message Alice sends to Bob. Eve has access to the Alice's PuK and knows the hash functions H and h. Any forged data d we denote as d^F.

The presented signature scheme is based on two essentially hard problems, MFSP and OOSP, and on two postulated hard problems *OSP and $\oplus$OSP. The proof of security of designed signature scheme against the PrK compromitation, signature + data forgering and data forgering is presented. The latter case guarantees the non-repudiation property.

We postulate that three kind of attacks here considered cover the most of other possible attacks. So we postulate that our signature scheme has a provable security property (Cramer and Shoup, 1998).

4.1. *PrK Compromitation*

Instance: PuK = (ρ, a).
Objective: find PrK = (α, β, x).

To solve this problem Eve must solve two hard problems simultaneously: MFSP and OOSP.

$$\rho = \alpha \cdot \eta \cdot \beta^{-1},$$
$$a = \rho' * x.$$

It is hard to believe if there will be any other algorithms for determination of α, β, η and x, except the total search in a sufficiently complicated semiring and semimodule. As for a semiring it is required that the subset J would have effective equivalence transformations which reliably hide multiplicative factors in the word. This condition is easily satisfied in the most useful algebraic systems, as was mentioned above.

4.2. *Signature + Data Forgering*

This kind of forgering is performed by active eavesdropper trying to sign a forged message T^F and to replace a signature S by forged one S^F expecting that the verification procedure will not fail.

We assume that Eve can not guess the actual α, β, x and μ. So instead of these she can choose the forged ones α^F, β^F, x^F and μ^F.

Let Eve has a message T^F and is trying to sign it and send to Bob instead and on behalf of Alice. She calculates a H-value of T^F

$$m^F = H(T^F).$$

Eve can not guess σ' and ζ'. Then she must choose forgered ones σ'^F and ζ'^F of the form

$$\sigma'^F = \beta^F \cdot \mu^F \cdot \alpha^{F-1},$$

$$\zeta'^F = \alpha^F \cdot \xi^F \cdot \beta^{F-1}.$$

Eve's signature parameter s^F is of the form

$$s^F = \sigma'^F * (x^F \oplus \zeta' * m^F).$$

Then she replaces σ with σ^F and ζ with ζ^F of the form

$$\sigma^F = \alpha^F \cdot \mu^F \cdot \beta^{F-1},$$
$$\zeta^F = \beta^F \cdot \xi^F \cdot \alpha^{F-1}.$$

Eve sends the forged signature $S^F = (s^F, \sigma^F, \zeta^F)$ and a message T^F to Bob.

Bob takes an Alice's PuK components ρ and a and verifies

$$\begin{aligned}\rho * s^F &= \rho * \sigma'^F * (x^F \oplus \zeta' * m^F)\\ &= \alpha \cdot \eta \cdot \beta^{-1} \cdot \beta^{F-1} \cdot \mu^F \cdot \alpha^F * x^F \oplus \alpha \cdot \eta \cdot \beta^{-1} \cdot \beta^F \cdot \mu^F \cdot \alpha^{F-1}\\ &\quad \cdot \alpha^F \cdot \xi^F \cdot \beta^{F-1} * m^F\\ &\neq \sigma^F * (a \oplus \zeta^F * \rho * m^F),\end{aligned}$$

since $\beta^{-1} \cdot \beta^{F-1} \neq 1$.

This kind of forgering could be named existential forgering (Goldwasser *et al.*, 1998).

4.3. *Data Forgering (Non-Repudiation)*

Assume Eve is trying to supply Bob with a forgered message T^F signed with a valid Alice's signature S. If this opportunity takes place then, on the other hand, Alice can refuse to recognize her signature under the same unfavor circumstances.

Then it follows that with a valid signature $S = (\sigma, s, \zeta)$ a forgered message T^F can be signed. The H-value $m^F = H(T^F)$ must satisfy the verification condition (V) which we rewrite in the form

$$\sigma * \zeta * \rho * m^F \oplus \sigma * a = \rho * s.$$

But according to $\oplus$OSP it is infeasible to find m_1, expressed by equation $m_1 = \sigma * \zeta * \rho * m^F$, because $\oplus$OSP is hard.

Moreover it is hard to find m^F from m_1, because Eve must sequentially solve three hard *OSPs.

Even if m^F is found, there is impossible to construct a sensible disinformation message T^F such that

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

due to our assumption that H-function is cryptographically secure.

So we proved that the forgered message could not be signed with a valid signature and hence the signature has non-repudiation property.

5. Discussion

The quality of signature scheme depends on the quality of *OWF and $\oplus$OWF. This quality depends on the concrete realization of R and M and requires further investigations.

One of possible realizations of R could be found by constructing a semiring R using a Gaussian group G as a generator. Having also some prototype of vector space (Sakalauskas, 2004), we can generalize it to the semimodule M.

It is natural to assume that essential OWFs based on MFSP and OOSP are secure. It is evident that essential OWFs easily satisfy security requirements when, for example, some member of Gaussian groups' family is used.

The main advantages of presented scheme are the following:

1 It has fewer components in PrK and PuK. Moreover the length of ρ in current scheme is shorter, because it is not composed of quadratic factors as it is in the previous scheme. Hence the key length is shorter.

2 There is no requirement for elements of M to have their inverses. This increases the signature scheme security because the expression

$$\sigma * \zeta * \rho * m = \rho * s - \sigma * a,$$

is meaningless due to insensibility of – operation.

3 The secret signature key ξ is less restricted than in previous scheme, where according to the current notations it is required that $\xi \in R_{L1}$, where $R_{L1} \subset R_L$. In this scheme $\xi \in R_L$. This also increases security of modernized scheme, since R_L is not splitted into smaller parts.

4 The modernized scheme is more effective computationally, because it is required to calculate two H-functions instead of three.

In (Sakalauskas, 2004) the qualitative analysis of previous signature scheme and the comparison of performance figures with other known schemes is done. We can affirmate that the performance of modernized scheme is no worse than the scheme proposed earlier (Sakalauskas, 2004).

References

Cramer, R., V. Shoup (1988). A public key cryptosystem provably secure against adaptive choosen ciphertext attack. *Advances in Cryptology – Crypto' 98*. pp. 13–25.

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

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

Ki Hyoung, Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, Choonsik Park (2000). New public-key cryptosystem using braid groups. *Advances in Cryptology, Proc. Crypto 2000*, LNCS **1880**, Springer-Verlag. pp. 166–183.

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

Kurosh, A. (1974). *General Algebra*. Moscow, Nauka (in Russian).

Magnus, W., A. Karrass, D. Solitar (1966). *Combinatorial Group Theory*. Interscience Publishers, NY.

Menezes, A., P. van Oorschot, S. Vanstone (1996). *Handbook of Applied Cryptography*. CRC Press.

Rabi, M., A. Sherman (1993). *Associative One-Way Function: A New Paradigm for Secret Key Agreement and Digital Signatures*. Univ. of Maryland. Comp. Sci. Dep.

Sakalauskas, E. (2004). New digital signature scheme in Gaussian monoid, *Informatica*. **15**(2), 251–270.

van der Waerden, B.L. (1967). *Algebra*. Springer-Verlag.

E. Sakalauskas received PhD degree from Kaunas Polytechnical Institute in 1983. Currently he is a head of Laboratory of Information and Energetic Systems, senior reseacher in Institute of Defence Technology and assist. prof. in Department of Applied Mathematics in Kaunas University of Technology. The scope of scientific interests is a system theory, identification and cryptography. In recent time his research interests are focused mainly in the cryptography. There were achieved some results in the following fields: one way function construction based on the hard problems in infinite noncommutative groups, digital signature schemes, key exchange protocols and pseudorandom number generation. In this field are published 7 papers. E. Sakalauskas has published over 31 scientific papers in all and 8 of them are published in journals included in ISI Master Journal List Catalog.

Viena skaitmeninio parašo schema realizuota semimodulyje virš semižiedo

Eligijus SAKALAUSKAS

Pateikta skaitmeninio parašo schemos modernizacija, publikuotos (Sakalauskas, 2004). Ši schema skiriasi nuo savo prototipo savo struktūra ir naudoja bendresnes algebrines sistemas. Ji pasižymi didesniu saugumu, turi trumpesnius raktų ilgius ir yra algoritmiškai efektyvesnė.

Įvedamos naujos algebrinės strukturos semimodulis ir semižiedas, kurios yra tarpusavyje suderintos algebrinės sistemos. Semižiedas yra operatorių aibė, kurie veikia semomodulyje kaip endomorfizmai. Postuluojama, kad veikimo operacija turi vienkryptės funkcijos (VKF) savybę. Algebrinių sistemų suderinamumas reiškia, kad veikimo operacija yra didtributyvi iš kairės ir dešinės modulyje ir žiede apibrežtos adityvinės operacijos atžvigiu.

Dvi kitos natūralios VKF yra apibrežtos, kurios yra paremtos žinomomis konstrukcijomis ir turi didesnį sudėtingumą nei kitos pripažintos sunkios problemos, tokios kaip pvz. jungtinuko suradimo problema nekomutatyvinėse grupėse.