KEY AGREEMENT PROTOCOL (KAP) BASED ON MATRIX POWER FUNCTION*

Eligijus Sakalauskas, Narimantas Listopadskis, Povilas Tvarijonas

Abstract: The key agreement protocol (KAP) is constructed using matrix power functions. These functions are based on matrix ring action on some matrix set. Matrix power functions have some indications as being a one-way function since they are linked with certain generalized satisfiability problems which are potentially NP-Complete. A working example of KAP with guaranteed brute force attack prevention is presented for certain algebraic structures. The main advantage of proposed KAP is considerable fast computations and avoidance of arithmetic operations with long integers.

Keywords: key agreement protocol, matrix power function, one-way function (OWF).

ACM Classification Keywords: E.3 Data encryption, F.2.1 Numerical Algorithms and Problems.

Conference: The paper is selected from Sixth International Conference on Information Research and Applications – i.Tech 2008, Varna, Bulgaria, June-July 2008

Introduction

After the sound Diffie-Hellman key agreement protocol (KAP) some attempts have been made to construct this protocol using hard problems in infinite non-commutative groups. The ideas were based on either conjugator search problems or decomposition problems (double co-set problems) which were reckoned as potentially hard problems for construction of one-way functions (OWF). One of the first ideas appeared in [Sidelnikov et. al., 1993]. From this time main attempts were directed to the suitable platform group or semigroup selection.

In 1999, first algorithms appeared using braid groups as a platform groups. In [Anshel et. al., 1999] the KAP was based on both simultaneous multiple conjugator search problem and so–called membership problem. Authors pointed out that the realization of proposed algorithm could be perspective using braid groups. In [Ko et. al., 1999] the multiple conjugator search problem in braid groups was used.

But nevertheless, it was pointed out [Shpilrain and Ushakov, 2004], that using conjugator search problem in braid groups is unnecessary and insufficient condition for KAP security. Moreover, authors noticed that the main problem for construction of cryptographic primitives in infinite non-commutative groups is to reliably hide the factors in the group word. In some groups the hiding procedure can take almost the same resources as to reveal these factors. Hence, one of the directions of investigations in this field is to combine together at least two hard problems in infinite non-commutative groups [Shpilrain and Ushakov, 2005].

The papers presented above can be interpreted as an investigation direction based on hard problems in infinite non-commutative group presentation level, i.e. using the group combinatorial theory [Magnus et. al., 1966]. This approach is also named symbolic computation.

The cryptographic application of group or semigroup action in finite dimensional vector spaces or, more generally, in some module is presented in [Monico, 2002]. This action is related with multidimensional generalization of classical modular exponent in cyclic group. This generalization pretends to be an OWF with higher complexity when compared with one based on classical exponent function in cyclic group related with discrete logarithm problem (DLP).

The idea to use non-commutative infinite group (e.g. braid group) representation was also used for construction of the other kind of OWFs as a background of both digital signature scheme and key agreement protocol [Sakalauskas, 2005], [Sakalauskas et. al., 2005]. The (semi)group representation level allows us to hide the

* Work is partially supported by the Lithuanian State Science and Studies Foundation

factors in the publicly available group word in a very natural way. However, the original hard problems, such as conjugator search or decomposition problems in (semi)group presentation level are considerably weakened when they are transferred to the representation level. Therefore in this case these problems must be considerably strengthened by simultaneously adding other additional hard problems.

The construction of KAP presented there is based on some matrix semiring $\mathcal{R}$ action on matrix set $\mathcal{M}$. The set $\mathcal{M}$ is not specified as a closed set with respect to some internal operation. Both $\mathcal{R}$ and $\mathcal{M}$ are defined over two different algebraic structures. $\mathcal{R}$ is defined over some commutative semiring $\mathcal{S}$ and $\mathcal{M}$ over some finite semigroup $\mathcal{T}$. The KAP is constructed using two external action operations of $\mathcal{R}$ on $\mathcal{M}$. These operations are named matrix power functions and were used for matrix power S-box construction [Sakalauskas and Luksys, 2007]. In some sense they are linked with well–known decomposition problem in infinite non-commutative (semi)groups [Shpilrain and Ushakov, 2005], but in contrary they are based on external action operation. The functions so defined have some indications as being one-way functions (OWF).

Matrix power functions

The classical definitions and notations in this section can be found in [Van der Waerden, 1967] and [Birkhoff and Bartee, 1974]. Let $\mathcal{R}$ be a matrix semiring consisting of m-dimensional square matrices with entries in some commutative semiring $\mathcal{S}$, i.e. $\mathcal{R}$ is a matrix semiring over $\mathcal{S}$. The elements of $\mathcal{R}$ we call a set of operators and denote them by X, Y, Z, and etc. The matrix edition and multiplication in $\mathcal{R}$ are defined in a convenient way, so since $\mathcal{S}$ is commutative, the matrix multiplication satisfies the associative law. We assume that these operators (matrices) are acting on some set of m-dimensional square matrices denoted by $\mathcal{M}$ over some finite semigroup $\mathcal{T}$. Hence we defined some action of matrix ring $\mathcal{R}$ on a set of matrices in $\mathcal{M}$. More precisely this action is the action of elements of $\mathcal{R}$ on elements of $\mathcal{M}$ in a particular way, i.e. for any $X\in\mathcal{R}$ there exists some action function f_X: $\mathcal{M}\to\mathcal{M}$. Then for all $Q\in\mathcal{M}$ and all $X\in\mathcal{R}$ there exist some A in $\mathcal{M}$, such that $f_X(Q)=A$. Hence we assumed that set $\mathcal{M}$ is closed under the action of $\mathcal{R}$. According to classical definition, the action function corresponds to the left composition function $f_X(\ )$ which arguments are in $\mathcal{M}$. Then for any such function $f_X(\ )$ the corresponding left action operation can be defined, which we denote by $\triangleright$: $\mathcal{R}\times\mathcal{M}\to\mathcal{M}$ and

$$f_X(Q)=X\triangleright Q=A \qquad (1)$$

Alternatively, assume that for any left composition function $f_X(\ )$ on $\mathcal{M}$ there exists right composition function $(\ )f_X$. Analogously to the action of left compositions functions we can define the corresponding right action operation which we denote by $\triangleleft$: $\mathcal{M}\times\mathcal{R}\to\mathcal{M}$. Then for any $Y\in\mathcal{R}$ there exists some $B\in\mathcal{M}$ satisfying equation

$$(Q)f_Y=Q\triangleleft Y=B. \qquad (2)$$

Definition 1. Functions $f_X(\ )$, $(\ )f_Y$ and the corresponding action operations $\triangleright$, $\triangleleft$ are bi-associative, if

$$(X\triangleright Q)\triangleleft Y=X\triangleright(Q\triangleleft Y). \qquad (3)$$

Further action operations $\triangleright$, $\triangleleft$ we interpret as functions. These functions are defined in abstract algebraic structures. For KAP construction we present below a more concrete realization of these functions.

Using matrix notation we write matrices as sets of their elements, i.e. $X=\{x_{ij}\}$, $Q=\{q_{jk}\}$, $Y=\{y_{ki}\}$, $A=\{a_{ik}\}$ and $B=\{b_{ji}\}$. Since matrices are of the m-th order then the indexes are $i,j,k\in\{1\ldots, m\}$.

To define the left action function $\triangleright$ of X on Q yielding the matrix A, we write the following formula relating the elements of these matrices

$$a_{ik}=\prod_{j=1}^{m} q_{jk}^{x_{ij}} \qquad (4)$$

Analogously, the result of right action operation $\triangleleft$ of matrix Y on Q is the matrix B which entries satisfies the following equations

$$b_{ji} = \prod_{k=1}^{m} q_{jk}^{y_{ki}} . \quad (5)$$

These functions were introduced in [Sakalauskas and Luksys, 2007] for the matrix power S-box construction.

To illustrate action of functions $\triangleright$ and $\triangleleft$ let us assume that matrices A, B, X, Q and Y are of the 2-nd order, i.e. having two rows and two columns. Then m=2 and (4), (5) can be rewritten in the form

$$A = X \triangleright Q = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \triangleright \begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix} = \begin{pmatrix} q_{11}^{x_{11}} q_{21}^{x_{12}} & q_{12}^{x_{11}} q_{22}^{x_{12}} \\ q_{11}^{x_{21}} q_{21}^{x_{22}} & q_{12}^{x_{21}} q_{22}^{x_{22}} \end{pmatrix}, \quad (6)$$

$$B = Q \triangleleft Y = \begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix} \triangleleft \begin{pmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{pmatrix} = \begin{pmatrix} q_{11}^{y_{11}} q_{12}^{y_{21}} & q_{11}^{y_{12}} q_{12}^{y_{22}} \\ q_{21}^{y_{11}} q_{22}^{y_{21}} & q_{21}^{y_{12}} q_{22}^{y_{22}} \end{pmatrix}. \quad (7)$$

As we see functions $\triangleright$ and $\triangleleft$ can be interpreted as left and right matrix power operations. Then using the analogy to the power (exponent) function defined in certain algebraic structures (say, in a ring of integers $\mathcal{Z}_n$) the action operations can be rewritten in the form reflecting the left and right matrix power operations

$$X \triangleright Q = {}^{X}Q = A, \quad (8)$$

$$Q \triangleleft Y = Q^{Y} = B. \quad (9)$$

Definition 2. Functions $\triangleright$ and $\triangleleft$ we define as left and right matrix power functions, correspondingly.

These functions are properly defined if powering operations of q_{jk} by the elements of x_{ij} and y_{ki} have a sensible meaning. In the most simple (but practically significant) case the semiring $\mathcal{S}$ can be assumed as being a semiring of natural numbers $\mathcal{N}$={1, 2, 3 …}, i.e. $\mathcal{S}$= $\mathcal{N}$. Then the variables x_{ij} and y_{ki} are natural numbers and the elements of matrices A and B denoted by $\{a_{ik}\}$ and $\{b_{ik}\}$ in (4) and (5) can be calculated by powering the elements q_{jk} in finite semigroup $\mathcal{T}$ by natural numbers x_{ik} and y_{ik} using the multiplication operation defined in $\mathcal{T}$.

The following theorem can be formulated for functions $\triangleright$ and $\triangleleft$.

Theorem 1. If Z=XY, where X, Y and Z are in $\mathcal{M}$, then

$$Z \triangleright Q = (XY) \triangleright Q = X \triangleright (Y \triangleright Q) = X \triangleright Y \triangleright Q. \quad (10)$$

$$Q \triangleleft Z = Q \triangleleft (XY) = Q \triangleleft (X \triangleleft Y) = Q \triangleleft X \triangleleft Y. \quad (11)$$

▼ Proof. The proof directly follows from the (4), (5) and the rule of convenient matrix multiplication in $\mathcal{R}$. ▲

Theorem 2. . If $\mathcal{S}$=$\mathcal{N}$, then functions $\triangleright$ and $\triangleleft$ are bi-associative.

▼ Proof. Since the elements of matrices X and Y are the natural numbers in $\mathcal{N}$, then for all $q_i \in \mathcal{T}$ and $x_i, y_k \in \mathcal{N}$, the following exponentiation rules in $\mathcal{T}$ are valid $\left(q_j^{x_i}\right)^{y_k} = \left(q_j^{y_k}\right)^{x_i} = q_j^{x_i y_k} = q_j^{y_k x_i}$ and $q_j^{x_i} q_j^{y_k} = q_j^{x_i + y_k}$.

Using association law of matrix multiplication in $\mathcal{R}$ and (4), (5), and applying direct calculations we find that $(X \triangleright Q) \triangleleft Y = X \triangleright (Q \triangleleft Y) = D$, where $D=\{d_{ij}\}$ is the matrix in $\mathcal{M}$. ▲

Key agreement protocol

Using a combination of functions $\triangleright$ and $\triangleleft$ we construct the key agreement protocol (KAP). It is based on the conjecture that these functions are one-way functions (OWFs). Let us define two subsets of commuting matrices $\mathcal{R}_L$ and $\mathcal{R}_R$ in $\mathcal{R}$. This means that for all $X, U \in \mathcal{R}_L$ and $Y, V \in \mathcal{R}_R$

$$XU = UX, \quad (12)$$

$$YV = VY. \quad (13)$$

Then we propose the following KAP.

1. Parties agree on publicly available matrix Q in $\mathcal{M}$ and two subsets $\mathcal{R}_L$ and $\mathcal{R}_R$ in $\mathcal{R}$.

Alice chooses at random the secret matrix X in $\mathcal{R}_L$ and Y in $\mathcal{R}_R$, respectively, calculates matrix A and sends it to Bob, where

$$A=X \triangleright Q \triangleleft Y. \quad (14)$$

2. Bob chooses at random the secret matrix U in $\mathcal{R}_L$ and V in $\mathcal{R}_R$ respectively, calculates matrix B and sends it to Alice, where

$$B=U \triangleright Q \triangleleft V. \quad (15)$$

3. Both parties compute the following common secret key K:

$$K=X \triangleright B \triangleleft Y= X \triangleright U \triangleright Q \triangleright V \triangleleft Y=U \triangleright X \triangleright Q \triangleright Y \triangleleft V=U \triangleright A \triangleleft V. \quad (16)$$

The last identities are valid since Theorems 1, 2 and equations (12), (13) hold.

The proposed KAP is some generalization of well known Diffie-Hellman protocol. Indeed, if all matrices are numbers in Galois field GF(p) then according to (4), (5), and (16) we can write

$$X \triangleright Q \triangleleft Z= {}^{X}Q^{Y}=Q^{XY}=K, \quad (17)$$

where K is a Diffie-Hellman secret key.

To compromise the secret key K one must find any matrices X, Y in (14) and U, V in (15) for given instances Q, A and Q, B correspondingly. Let us consider the case to find any matrices X, Y in (14). Let the elements of X, Y, Q and A are $\{x_{ij}\}$, $\{y_{ij}\}$, $\{q_{jk}\}$ and $\{a_{ik}\}$ correspondingly. For more clarity the matrix equation (14) we write in a form of the system of equations for the matrices of 2-nd order, i.e. for m=2:

$$\begin{cases} q_{11}^{x_{11}y_{11}} & q_{21}^{x_{12}y_{11}} & q_{12}^{x_{11}y_{21}} & q_{22}^{x_{12}y_{21}} & = & a_{11} \\ q_{11}^{x_{11}y_{12}} & q_{21}^{x_{12}y_{12}} & q_{12}^{x_{11}y_{22}} & q_{22}^{x_{12}y_{12}} & = & a_{12} \\ q_{11}^{x_{21}y_{11}} & q_{21}^{x_{22}y_{11}} & q_{12}^{x_{21}y_{21}} & q_{22}^{x_{22}y_{21}} & = & a_{21} \\ q_{11}^{x_{21}y_{12}} & q_{21}^{x_{22}y_{12}} & q_{12}^{x_{21}y_{22}} & q_{22}^{x_{22}y_{22}} & = & a_{22} \end{cases} \quad (18)$$

At the first sight it seems that the problem to find any $X=\{x_{ij}\}$, $Y=\{y_{ij}\}$ is some matrix generalization of discrete logarithm problem (DLP). But nevertheless the solution of DLP is not a sufficient condition to find X and Y even in the case when $\mathcal{T}$ is a group of Galois field GF(p). If we choose some matrix Y in $\mathcal{R}_R$ and will try to find X by solving (14), there is no guarantee that obtained matrix X will be in $\mathcal{R}_L$. Hence the compromising of K is related with the solution of matrix equation (15). This equation for m=2 is presented in (18).

Without proof we declare that the security of proposed KAP relies on the complexity of certain generalized satisfiability problem which conveniently is denoted by SAT(S), [Shaefer, 1978]. According to Shaefer Dichotomy theorem the SAT(S) problem is either P or NP-Complete, [Garey and Johnson, 1979]. The first alternative is rather a very rare exception since the conditions of SAT(S) problem to be in class P occurs in a very special predetermined cases, [Shaefer, 1978]. Hence the key K compromisation with a very big certainty corresponds to the solution of NP-Complete problem.

In contrary to the classical Diffie-Hellman protocol, we think that one of advantages of there proposed protocol is the avoidance of performing arithmetic operations with big integers and faster computations.

Implementation

The concrete realization of KAP requires defining both the matrix semiring $\mathcal{R}$ over commutative semiring $\mathcal{S}$ and the set of matrices $\mathcal{M}$ over the semigroup $\mathcal{T}$. As it was denoted above, we can choose $\mathcal{S}=\mathcal{N}$, when $\mathcal{T}$ was assumed to be finite semigroup. The most known types of $\mathcal{T}$ can be either a semigroup Z_n^* of ring of integers $\mathcal{Z}_n$, or the group $\mathcal{F}^*$ of some Galois (finite) field $\mathcal{F}$, or a group of Elliptic Curve points in some finite field $\mathcal{F}$.

In any case when $\mathcal{T}$ is a semigroup neither matrix multiplication nor addition are defined in $\mathcal{M}$. Hence we have specified $\mathcal{M}$ as a set without any internal operations. As an example we can choose $\mathcal{T}$=GF(251).

We think that essential security parameters in our construction are the order of matrices m and the logarithm of cardinality of $\mathcal{T}$, which we denote by $N=\lceil \log_2 n \rceil$. When $\mathcal{T}$=GF(251), $N=\lceil \log_2 n \rceil=\lceil \log_2 251 \rceil=8$. Let the other security parameter m=32. Then we have the matrix Q in $\mathcal{M}$ of order 32 with elements in GF(251). In this case the matrices X and Y are represented by $k = mxmxN$=32x32x8=8192 bits.

Bibliography

[Anshel et. al., 1999], I. Anshel, M. Anshel and D. Goldfeld, An algebraic method for public-key cryptography, Math. Res. Lett. 6, 1999, pp. 287-291.

[Birkhoff and Bartee, 1974], G. Birkhoff and C. Bartee, Modern applied algebra, McGraw-Hill, 1974.

[Garey and Johnson, 1979], M. Garey and D. Johnson, Computers and intractability: a guide to theory of NP-Completeness. H.Freeman, New York, 1979.

[Ko et. al., 1999], K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang and C. Park, New public-key cryptosystem using braid groups, Advances in cryptology, Advances in Cryptology, Proc. Crypto 2000, LNCS 1880, Springer–Verlag 2000, pp. 166-183.

[Magnus et. al., 1966], W. Magnus, A. Karrass and D. Solitar, Combinatorial Group Theory, Interscience Publishers, NY, 1966.

[Monico, 2002], C. Monico, Semirings and Semigroup actions in Public–Key Cryptography, Phd. thesis, University of Notre Dame, May 2002, pp. 1-78.

[Sakalauskas, 2005], E. Sakalauskas, One Digital Signature Scheme in Semimodule over Semiring, Informatica, ISSN: 0868-4952, Vol. 16, No. 3, 2005, pp. 383-394.

[Sakalauskas et. al., 2007], E. Sakalauskas, P. Tvarijonas and A. Raulynaitis, Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problems in Group Representation Level, Informatica, Vol. 18, No. 1, 2007, pp. 115-124.

[Sakalauskas and Luksys, 2007], E. Sakalauskas and K. Lukšys, Matrix Power S-Box Construction,*Cryptology . ePrint Archive: Report*, no. 214 (2007), http://eprint.iacr.org/2007/214.

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

[Shaefer, 1978], T. J. Shaefer, The Complexity of Satisfiability Problems, *Proceedings of the 10th Annual Symposium on Theory and Computing*, 1978, pp. 216-226.

[Shpilrain and Ushakov, 2004], V. Shpilrain and A. Ushakov, The conjugacy search problem in public key cryptography: unnecessary and insufficient, Available at: http://eprint.iacr.org/2004/321, 2004.

[Shpilrain and Ushakov, 2005], V. Shpilrain and A. Ushakov, A new key exchange protocol based on the decomposition problem, Available at: http://eprint.iacr.org/2005/447, 2005.

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

Authors' Information

Eligijus Sakalauskas – Assoc. prof., Department of Applied Mathematics, Kaunas University of Technology, Studentu str. 50-324a, Kaunas, LT-51368, Lithuania, e-mail Eligijus.Sakalauskas@ktu.lt

Narimantas Listopadskis – Assoc. prof., Department of Applied Mathematics, Kaunas University of Technology, Studentu str. 50-324a, Kaunas, LT-51368, Lithuania, e-mail Narimantas.Listopadskis@ktu.lt

Povilas Tvarijonas – Lector, Department of Applied Mathematics, Kaunas University of Technology, Studentu str. 50-324a, Kaunas, LT-51368, Lithuania, e-mail Povilas.Tvarijonas@ktu.lt