Introduction

Nowadays the Internet has expanded and encompasses not only regular PCs, but also a large number of small devices ranging from PDAs and cell phones to appliances and network sensors. Conventionally these systems are called embedded systems. In this connection information security becomes a very important issue [1]. Symmetric cryptography achieves information confidentiality goals. However it requires pre-distribution of secret keys, which can be done with the help of public-key cryptography. Traditional key agreement protocols (KAP) requires a significant amount of computation [2], but in restricted computational environment we are limited in computational power and memory size.

In this paper we propose a new KAP based on NP-complete problem and hence having a property of provable security. Proposed KAP can be used in low-cost systems and it should work efficiently even on 8-bit microprocessors with no dedicated cryptographic coprocessors. We also compare the realization of our KAP with classical KAPs.

Key agreement protocols

KAPs are one of the basic cryptographic protocols. KAP allows two or more parties negotiate a common secret key using insecure communications. First KAP was presented by [3] which caused a rapid development of asymmetric cryptography. Its realization in restricted computational environments is time consuming since it requires arithmetical operations with big integers.

In 1985 [4, 5] independently suggested elliptic curve cryptography. Based on that elliptic curve Diffie-Hellman (ECDH) KAP was developed. Because of the smaller key size its realization is significantly faster then that of original Diffie-Hellman (DH) protocol.

In 1993 new ideas appeared in asymmetric cryptography [6] – using known hard computational problems in infinite non-commutative groups instead of hard number theory problems such as discrete logarithm or integer factorization problems. These ideas were realized in [7, 8, 9].

Nevertheless, [10] showed that conjugator search problem in braid groups does not produce sufficient security level. Moreover, authors noticed that the main problem for construction of cryptographic primitives in infinite non-commutative groups is to reliably hide the factors in group word.

The idea to use non-commutative infinite group (e.g. braid group) representation was also used to construct other candidate one-way function as a background of both digital signature scheme and key agreement protocol [11, 12]. The (semi)group representation level allows us to avoid a significant problem of hiding the factors in the publicly available group word when using its presentation level. Since this problem is solved in a very natural way. However, the original hard problems, such as conjugator search or decomposition problems in (semi)group presentation level are weakened when they are transformed into the representation level. Therefore using representation level these problems must be considerably strengthened by simultaneously adding the other additional hard problems. One of solution is to use matrix power function (MPF) [12].

The idea of this article is to create a new KAP based on the centralizer’s application in braid groups presentation level, Burau representation and MPF and having effective realization in 8-bits microprocessors. KAP based on braid groups as platform groups in presentation level using centralizers is also presented in [9].

Proposed KAP is using matrix power function which is some matrix (semi)group $S$ action on a matrix set $M$. The set $M$ is not specified as a closed set with respect to
some internal operation. Both \( S \) and \( M \) are defined over two different algebraic structures. \( S \) is defined over some finite field \( F \) and \( M \) over some finite non-cyclic group \( G \). We will show that inversion of so defined MPF has some indications to be NP-complete. Hence the security of presented KAP relies on the complexity conjectured of NP-complete problem and its realization is based on the candidate one-way function (OWF).

**Mathematical background**

We consider general Artin braid group [13] as our infinite non-commutative group. Given an integer \( n \geq 2 \), the braid group on \( n \) strands, \( B_n \), is defined by following presentation

\[
B_n = \left\{ e, \sigma_1, \ldots, \sigma_{n-1} \mid \sigma_i \sigma_j = \sigma_j \sigma_i \; \text{if} \; j \geq 2, \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}, 1 \leq i \leq n-2 \right\}.
\]  

(1)

Given a group \( B_n \), the centralizer of an element \( x \in B_n \) is the subgroup of \( B_n \) consisting of all elements which commute with \( x \). We denote \( C(x) = \{ \gamma_1, \ldots, \gamma_k \} \) the know set of generators of the centralizer of an element \( x \). An algorithm how to compute a generating set for the centralizer of an element in braid group and more generally in Garside group is presented by [14]. We claim that all elements satisfy equation

\[
a_{ij} = \prod_{k=1}^{m} q_{ij}^{x_k}.
\]  

(4)

These left and right actions are called matrix power functions. To illustrate them let us assume that matrices \( A, B, Q, X \) and \( Y \) are of the 2-nd order. Then \( m = 2 \) and (3), (4) can be can be written:

\[
A = X^Q = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}, \quad B = Y^Q = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}.
\]  

(5)

Matrix power function is explained in more detail by [16, 17]. There is also shown that following equations are correct:

\[
X^Y Q = (X^Y) Q = X^{(Y Q)},
\]  

(7)

\[
Q^{XY} = Q^{(XY)} = (Q^X)^Y,
\]  

(8)

\[
X^Q Y = (X^Q)^Y = X^{(Q^Y)}.
\]  

(9)

**Proposed protocol**

Now we propose the following key agreement protocol for two parties – Alice and Bob.

1. Parties agree on publicly available braid group \( B_n \) order \( n \), prime number \( p \), modulo \( m \) of the group \( G \), element \( t \in S \) and matrix \( Q \in M \) of the \((n-1)\)-th order;

2. Alice randomly generates braid group word \( x \in B_n \). After calculating \( C(x) \), \( X = \rho(x) \) and \( C(X) = \rho(C(x)) \) she stores \( X \) as her private key and makes \( C(X) \) publicly available as her public key;

3. Bob randomly generates braid group word \( y \in B_n \). After calculating \( C(Y) \), \( Y = \rho(y) \) and \( C(Y) = \rho(C(Y)) \) he stores \( Y \) as his private key and makes \( C(Y) \) publicly available as his public key;

4. Alice randomly generates matrix \( V \in C(Y) \), calculates \( K_a \) and sends it to Bob

\[
K_a = V^{\top} Q^Y;
\]  

(10)

5. Bob randomly generates matrix \( U \in C(X) \), calculates \( K_b \) and sends it to Alice

\[
K_b = U^{\top} Q^Y;
\]  

(11)

6. Since matrices \( X, U \) and \( Y, V \) are commuting, both parties compute common secret key \( K \)

\[
K = \begin{pmatrix} X^{\top} \\ Y^{\top} \end{pmatrix} = \begin{pmatrix} U^{\top} Q^{XY} \end{pmatrix} = \begin{pmatrix} U^{XY} Q^{YY} \end{pmatrix} = \begin{pmatrix} U^{XY} \end{pmatrix} = K_a.
\]  

(12)
Preliminary security analysis

To compromise the secret key $K$ one must find any matrices $X, V$ in (10) or $U, Y$ in (11) for given instances $Q$, $K_a$ and $Q_b$ correspondingly. Let us consider the case of finding any matrices $X, V$ in (10). Let the elements of $X, V, Q$ and $K_a$ be $\{x_{ij}\}, \{y_{ij}\}, \{q_{ij}\}$ and $\{a_{ij}\}$ correspondingly. For more clarity the matrix equation (10) we will write in a form of system of equations for the matrices of 2-nd order, i.e. when $n=3$:

$$
\begin{align*}
q_{11}^{x_1^{11}11} \cdot q_{21}^{x_1^{21}11} \cdot q_{12}^{x_1^{12}21} \cdot q_{22}^{x_1^{22}21} &= a_{11}, \\
q_{11}^{x_1^{11}11} \cdot q_{21}^{x_1^{21}12} \cdot q_{12}^{x_1^{12}22} \cdot q_{22}^{x_1^{22}22} &= a_{12}, \\
q_{11}^{x_2^{11}11} \cdot q_{21}^{x_2^{11}21} \cdot q_{12}^{x_2^{12}21} \cdot q_{22}^{x_2^{22}21} &= a_{21}, \\
q_{11}^{x_2^{11}12} \cdot q_{21}^{x_2^{21}21} \cdot q_{12}^{x_2^{12}22} \cdot q_{22}^{x_2^{22}22} &= a_{22}.
\end{align*}
$$

(13)

At the first sight it seems that the problem of finding any $X = \{x_{ij}\}$ and $V = \{y_{ij}\}$ can be performed by applying a discrete logarithm function to all equations in (13). This is known as discrete logarithm problem (DLP). If it is the case then due to Fermat’s theorem we obtain a system of multivariate quadratic (MQ) equations over the ring. As it is known [18, 19] the solution of MQ system is an algorithm of order $\frac{n^4}{3}$ and field $Z_7$ variables of 8 bits are more than enough.

Further investigations are required to determine the length of braid words used in 1-st step of the protocol. We consider the protocol’s implementation in ordinary 8-bits microprocessor.

Implementing the protocol for operations in group $Z_{21}^*$ and field $Z_7$ variables of 8 bits are more than enough.

Conclusions

In this paper we present new KAP using matrix power function which is some matrix (semi)group $S$ action on a matrix set $M$. We showed that inversion of so defined
MPF has some indications to be NP-complete. Hence the security of presented KAP relies on the complexity conjectured of NP-complete problem.

The comparison results with known KAPs are presented and show a considerable computational time reduction in about 100 times compared to DH and ECDH. It shows that our KAP can be effectively realized in low-cost restricted computational environments such as microprocessors and embedded systems, e.g. in 8-bits microcontrollers.

References


Received 2011 06 07
Accepted after revision 2011 10 10


Key agreement protocol (KAP) using Burau braid groups representation and matrix power function (MPF) is presented. MPF is based on matrix semigroup action on some matrix set. All matrices are defined over finite field or ring. These functions pretend to be one-way functions since they are linked with multivariate quadratic (MQ) problems over some field. It is known that MQ problems are NP-complete over any field. We show that our KAP can be effectively realized in low-cost restricted computational environments such as microprocessors and embedded systems, e.g. in 8-bits microcontrollers.