Biuletyn WAT
Vol. LX, Nr 3, 2011

New symmetric cryptosystem

ZBIGNIEW JELONEK

Polish Academy of Sciences, Institute of Mathematics,
Śniadeckich 8, 00-956 Warsaw, Poland;
email: najelone@cyf-kr.edu.pl

Abstract. In this note we show how to use some simple algebraic concepts in symmetric cryptography. For a given number $n \geqslant 2$ let $M \subset \mathbb{Z}^n$ be a free submodule of rank n of prime index $[\mathbb{Z}^n : M] = p$. To code the information we use the algebraic structure of the quotient module $\mathbb{Z}^n/M$. The (private) key is composed from the prime number p and some vectors $v_1, \dots v_n; w \in \mathbb{Z}^n$.
Keywords: symmetric cryptosystem, private key, quotient module, linear algebra

1. Introduction

The aim of this note is to sketch the idea of a new symmetric cryptosystem, which is intend for fast code of information. There are several well-known such cryptosystems as AES, DES – see [2]. However, mathematicians still try to find some new systems – see e.g. [1]. In this note we use properties of torsion modules and linear algebra to sketch a quite new cryptosystem. The main property of this system is that each time we code the same information in a different way. We begin with the following well-known fact:

Theorem 1.1. *Let $M = \mathbb{Z}^n$ be a free $\mathbb{Z}-$ modul of rank n. Let W be a subdmodule of M such that, the modul M/W is torsion. Then, $W \cong \mathbb{Z}^n$ and if vectors $\mathbf{w_i} = (w_{i1}, ..., w_{in}),\ i = 1, ..., n$ generate W then,*

$$\#M/W = |det[w_{ij}]|.$$

This theorem suggests how we can construct a large cyclic group G of a prime order. Indeed, for a given n (we can take e.g., $n = 10$) it is enough to find a $n \times n$ matrix $\mathbb{A}$ with integral coefficients, whose discriminant is a large prime number and then to take as a submodule W the $\mathbb{Z}^n$ module generated by columns of the matrix $\mathbb{A}$. Now put

$$G = \mathbb{Z}^n / W.$$

The following Lemma explains how to find such a matrix $\mathbb{A}$:

Lemma 1.2. *Let* $p = 1 + \sum_{i=1}^n a_i b_i$. *Then*

$$\det \begin{bmatrix} 1 + a_1 b_1 & a_1 b_2 & \dots & a_1 b_n \\ a_2 b_1 & 1 + a_2 b_2 & \dots & a_2 b_n \\ \vdots & \vdots & \ddots & \vdots \\ a_n b_1 & a_n b_2 & \dots & 1 + a_n b_n \end{bmatrix} = p.$$

Proof Note, that $[a_i b_j] = [a_1, \dots, a_n][b_1, \dots, b_n]^T$. In particular, the matrix $[a_i b_j]$ has a rank less or equal to one. Hence

$$\det \begin{bmatrix} \lambda + a_1 b_1 & a_1 b_2 & \dots & a_1 b_n \\ a_2 b_1 & \lambda + a_2 b_2 & \dots & a_2 b_n \\ \vdots & \vdots & \ddots & \vdots \\ a_n b_1 & a_n b_2 & \dots & \lambda + a_n b_n \end{bmatrix} = \lambda^n + \lambda^{n-1} \big(\sum_{i=1}^n a_i b_i \big),$$

because all other coefficients of this polynomial disappear as sums of higher minors. Now, it is enough to put above $\lambda = 1$. $\square$

Assume now, that we have a matrix $\mathbb{A}$ with determinant p. Let W be a subspace of $\mathbb{Z}^n$ generated by columns $\boldsymbol{w}_1, \dots, \boldsymbol{w}_n$ of the matrix $\mathbb{A}$. Take $G = \mathbb{Z}^n / W$. The elements of G are equivalence classes of vectors from $\mathbb{Z}^n$. The following algorithm checks whether two given vectors are in the same class:

INPUT: vectors $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}^n$, $\boldsymbol{w}_1, \dots, \boldsymbol{w}_n$
1) solve a linear system

$$\boldsymbol{a} - \boldsymbol{b} = \sum_{i=1}^n x_i \boldsymbol{w}_i,$$

2) if all $x_i \in \mathbb{Z}$ then $q := true$, else $q := false$.
OUTPUT: $q := \{\boldsymbol{a} = \boldsymbol{b}\}$

The next algorithm is the algorithm to find a special generator of G, namely such a vector $\boldsymbol{w} = (w_1, \ldots, w_n)$, that

1) $\boldsymbol{w}$ generates G,
2)

$$\det \begin{bmatrix} w_1 & w_{2,1} & \ldots & w_{n,1} \\ w_2 & w_{2,2} & \ldots & w_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ w_n & w_{2,n} & \ldots & w_{n,n} \end{bmatrix} \neq 0 \bmod p. \qquad *)$$

INPUT: vectors $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n$
1) choose randomly $\boldsymbol{w} = (w_1, \ldots, w_n)$, where $|w_i| < p$.
2) if $\boldsymbol{w} = \mathbf{0}$ in G, then go back to 1)
3) if

$$\det \begin{bmatrix} w_1 & w_{2,1} & \ldots & w_{n,1} \\ w_2 & w_{2,2} & \ldots & w_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ w_n & w_{2,n} & \ldots & w_{n,n} \end{bmatrix} = 0 \bmod p$$

then, change vectors $\boldsymbol{w}_i$ in a cyclic way:

$$\boldsymbol{w}_1 \to \boldsymbol{w}_2, \boldsymbol{w}_2 \to \boldsymbol{w}_2, \ldots, \boldsymbol{w}_n \to \boldsymbol{w}_1$$

and go back to 3).

OUTPUT: vector $\boldsymbol{w}$ which generates the group G and satisfies the condition $*$) and (maybe) a new (renumbered) system of vectors $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n$.

To build a new cryptosystem we need also the algorithm of masking. In the sequel we need a following notation:

Definition 1.3. For a vector $\boldsymbol{w} = (w_1, \ldots, w_n) \in \mathbb{Z}^n$ we denote

$$\boldsymbol{w} \bmod p = (w_1 \bmod p, \ldots, w_n \bmod p) \in \mathbb{Z}^n.$$

Remark 1.4. Note, that the vector $\boldsymbol{w}$ is in the same equivalence class as the vector $\boldsymbol{w}$ mod p.

Now, we show how to mask a given vector without changing the equivalence class of this vector:

INPUT: vectors $\boldsymbol{w}, \boldsymbol{w}_1, \ldots, \boldsymbol{w}_n$
1) for $i = 1, \ldots, n$ choose randomly integers x_i: $0 < |x_i| < p$
2) $\boldsymbol{w}_1 := \boldsymbol{w} + \sum_{i=1}^{n} x_i \boldsymbol{w}_i$
3) $\boldsymbol{w}' = \boldsymbol{w}_1 \bmod p$
OUTPUT: vector $\boldsymbol{w}'$ – the masked vector $\boldsymbol{w}$.

2. Cryptosystem

Our cryptosystem is symmetric with private key. Assume a situation, where two people called Y and X want to communicate via an insecure channel in a secure manner.

Their private key are the number p and the vectors $\boldsymbol{w}_i = (w_{i,1}, \ldots, w_{i,n})$ and vector $\boldsymbol{w} = (w_1, ..., w_n)$ constructed above. These data we have to send to Y in a some secure way (for example we can use the method based on elliptic curves). Assume now that X and also Y have the group G constructed as in section one. We can send a secret message q (we assume that this message is a natural number $q \in (0, p)$) in the following way:

INPUT: vector $\boldsymbol{w}$ – a special generator of G, vectors $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n$
1) Y computes $\boldsymbol{Q} = q\boldsymbol{w}$
2) Y masks vector $\boldsymbol{Q}$ and send the masked vector $\boldsymbol{Q}' = (q'_1, \ldots, q'_n)$ to X
OUTPUT: the coded message $\boldsymbol{Q}'$

To recover the message q we use the following algorithm:

INPUT: the coded message $\boldsymbol{Q}'$
1) X computes determinants

$$\alpha := \det \begin{bmatrix} w_1 & w_{2,1} & \cdots & w_{n,1} \\ w_2 & w_{2,2} & \cdots & w_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ w_n & w_{2,n} & \cdots & w_{n,n} \end{bmatrix}$$

and

$$\beta := \det \begin{bmatrix} q'_1 & w_{2,1} & \cdots & w_{n,1} \\ q'_2 & w_{2,2} & \cdots & w_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ q'_n & w_{2,n} & \cdots & w_{n,n} \end{bmatrix}.$$

2) Now X recovers q using formula:

$$q := \alpha^{-1}\beta \bmod p.$$

OUTPUT: the original message q.

To see that indeed $q = \alpha^{-1}\beta \bmod p$, note that we have a system of equation:

$$\mathbf{Q}' - q\boldsymbol{w} = \sum_{i=1}^{n} x_i \boldsymbol{w}_i, \quad x_i \in \mathbb{Z}.$$

Using the Cramer rules we get that

$$(\beta - q\alpha)/p = x_1 \in \mathbb{Z},$$

i.e.;

$$\beta = q\alpha \bmod p$$

and finally since $\alpha \neq 0 \bmod p$ we have:

$$q := \alpha^{-1}\beta \bmod p.$$

Remark 2.1. The optimal number n (the dimension of $\mathbb{Z}$) we should determine using tests of our system.

3. Implementation for $n = 2$

Here, we give a more detailed implementation of our algorithm in the special case $n = 2$.

1) **Construction of the private key**
   a) choose the prime number p,
   b) choose the number $a \in (0, p)$ (the base of M are vectors $(0, p)$ and $(1, a)$),
   c) choose numbers $(w_1, w_2) \in (0, p)^2$ until $w_1 - w_2 a \neq 0 \bmod p$ (the vector (w_1, w_2) is a generator of the group $\mathbb{Z}^2/M$),
   d) put $\alpha = w_1 - w_2 a \bmod p$.
2) **Coding of the message $q \in (0, p)$ by vector $s = (s_1, s_2)$:**
   a) choose $x \in (0, p)$,
   b) put $(s_1, s_2) := (q(w_1, w_2) + x(a, 1)) \bmod p$.

3) **Recovering** q
   a) put $\beta = s_1 - s_2 a \bmod p$,
   b) then $q = \beta\alpha^{-1} \bmod p$.

This paper is supported by the research project 0 R00 0043 07, 2009–2011.

Received February 07 2011; Revised May 2011.

REFERENCES

[1] C. Elsner, *KronCrypt – A new symetric cryptosystem based on Kronecker Approximation Theorem*, preprint, Leibniz Universität Hannover, 2005.
[2] W. Stallings, *Cryptography and Network Security, Principles and Practices*, Prentice Hall, NJ, 2003.

Z. JELONEK

Nowy kryptosystem symetryczny

Streszczenie. W tej pracy stosujemy pewne proste algebraiczne koncepcje, by zbudować nowy kryptosystem symetryczny. Dla danej liczby naturalnej $n \geqslant 2$ niech $M \subset \mathbb{Z}^n$ będzie podmodułem wolnym rzędu n i indeksu pierwszego $[\mathbb{Z}^n : M] = p$. Informacje kodujemy, wykorzystując algebraiczną strukturę modułu ilorazowego $\mathbb{Z}^n/M$. Klucz (prywatny) składa się z liczby pierwszej p i pewnych wektorów $v_1, ...v_n$; $w \in \mathbb{Z}^n$.
Słowa kluczowe: wzorzec biometryczny, bezpieczeństwo danych, tożsamość cyfrowa, kryptologia, podpis cyfrowy, informatyka kryminalistyczna