JOURNAL OF FORMALIZED MATHEMATICS
Volume 10, Released 1998, Published 2003
Inst. of Computer Science, Univ. of Białystok

Algebraic Group on Fixed-length Bit Integer and its Adaptation to IDEA Cryptography

Yasushi Fuwa
Shinshu University
Nagano

Yoshinori Fujisawa
Shinshu University
Nagano

Summary. In this article, an algebraic group on fixed-length bit integer is constructed and its adaptation to IDEA cryptography is discussed. In the first section, we present some selected theorems on integers. In the continuous section, we construct an algebraic group on fixed-length integer. In the third section, operations of IDEA Cryptograms are defined and some theorems on these operations are proved. In the fourth section, we define sequences of IDEA Cryptogram's operations and discuss their nature. Finally, we make a model of IDEA Cryptogram and prove that the ciphertext that is encrypted by IDEA encryption algorithm can be decrypted by the IDEA decryption algorithm.

MML Identifier: IDEA_1.

WWW: http://mizar.org/JFM/Vol10/idea_1.html

The articles [17], [21], [18], [19], [12], [1], [23], [22], [5], [10], [13], [7], [6], [2], [4], [16], [8], [3], [9], [20], [15], [14], and [11] provide the notation and terminology for this paper.

1. Some Selected Theorems on Integers

We adopt the following rules: i, j, k, n are natural numbers and x, y, z are n-tuples of *Boolean*.

The following propositions are true:

(1) For all i, j, k such that j is prime and $i < j$ and $k < j$ and $i \neq 0$ there exists a natural number a such that $a \cdot i \bmod j = k$ and $a < j$.

(2) For all natural numbers n, k_1, k_2 such that $n \neq 0$ and $k_1 \bmod n = k_2 \bmod n$ and $k_1 \leq k_2$ there exists a natural number t such that $k_2 - k_1 = n \cdot t$.

(3) For all natural numbers a, b holds $a - b \leq a$.

(4) For all natural numbers b_1, b_2, c such that $b_2 \leq c$ holds $b_2 - b_1 \leq c$.

(5) For all natural numbers a, b, c such that $0 < a$ and $0 < b$ and $a < c$ and $b < c$ and c is prime holds $a \cdot b \bmod c \neq 0$.

(6) For every non empty natural number n holds $2^n \neq 1$.

2. Basic Operators of IDEA Cryptograms

Let us consider n. The functor $\mathrm{ZERO}\,n$ yielding a n-tuple of *Boolean* is defined by:

(Def. 1) $\mathrm{ZERO}\,n = n \mapsto \mathit{false}$.

Let us consider n and let x, y be n-tuples of *Boolean*. The functor $x \oplus y$ yielding a n-tuple of *Boolean* is defined as follows:

(Def. 2) For every i such that $i \in \operatorname{Seg} n$ holds $(x \oplus y)_i = x_i \oplus y_i$.

One can prove the following propositions:

(7) For all n, x holds $x \oplus x = \mathrm{ZERO}\, n$.

(8) For all n, x, y holds $x \oplus y = y \oplus x$.

Let us consider n and let x, y be n-tuples of *Boolean*. Let us notice that the functor $x \oplus y$ is commutative.

One can prove the following propositions:

(9) For all n, x holds $\mathrm{ZERO}\, n \oplus x = x$.

(10) For all n, x, y, z holds $(x \oplus y) \oplus z = x \oplus (y \oplus z)$.

Let us consider n and let i be a natural number. We say that i is expressible by n if and only if:

(Def. 3) $i < 2^n$.

One can prove the following proposition

(11) For every n holds n-BinarySequence$(0) = \mathrm{ZERO}\, n$.

Let us consider n and let i, j be natural numbers. The functor $\mathrm{ADD\_MOD}(i, j, n)$ yielding a natural number is defined by:

(Def. 4) $\mathrm{ADD\_MOD}(i, j, n) = (i + j) \bmod 2^n$.

Let us consider n and let i be a natural number. Let us assume that i is expressible by n. The functor $\mathrm{NEG\_N}(i, n)$ yielding a natural number is defined as follows:

(Def. 5) $\mathrm{NEG\_N}(i, n) = 2^n - i$.

Let us consider n and let i be a natural number. The functor $\mathrm{NEG\_MOD}(i, n)$ yields a natural number and is defined as follows:

(Def. 6) $\mathrm{NEG\_MOD}(i, n) = \mathrm{NEG\_N}(i, n) \bmod 2^n$.

Next we state several propositions:

(12) If i is expressible by n, then $\mathrm{ADD\_MOD}(i, \mathrm{NEG\_MOD}(i, n), n) = 0$.

(13) $\mathrm{ADD\_MOD}(i, j, n) = \mathrm{ADD\_MOD}(j, i, n)$.

(14) If i is expressible by n, then $\mathrm{ADD\_MOD}(0, i, n) = i$.

(15) $\mathrm{ADD\_MOD}(\mathrm{ADD\_MOD}(i, j, n), k, n) = \mathrm{ADD\_MOD}(i, \mathrm{ADD\_MOD}(j, k, n), n)$.

(16) $\mathrm{ADD\_MOD}(i, j, n)$ is expressible by n.

(17) $\mathrm{NEG\_MOD}(i, n)$ is expressible by n.

Let n, i be natural numbers. The functor $\mathrm{ChangeVal\_1}(i, n)$ yields a natural number and is defined as follows:

(Def. 7) $\mathrm{ChangeVal\_1}(i, n) = \begin{cases} 2^n, & \text{if } i = 0, \\ i, & \text{otherwise.} \end{cases}$

Next we state two propositions:

(18) If i is expressible by n, then $\mathrm{ChangeVal\_1}(i, n) \leq 2^n$ and $\mathrm{ChangeVal\_1}(i, n) > 0$.

(19) Let n, a_1, a_2 be natural numbers. Suppose a_1 is expressible by n and a_2 is expressible by n and $\mathrm{ChangeVal\_1}(a_1,n) = \mathrm{ChangeVal\_1}(a_2,n)$. Then $a_1 = a_2$.

Let us consider n and let i be a natural number. The functor $\mathrm{ChangeVal\_2}(i,n)$ yields a natural number and is defined by:

(Def. 8) $\mathrm{ChangeVal\_2}(i,n) = \begin{cases} 0, \text{ if } i = 2^n, \\ i, \text{ otherwise.} \end{cases}$

The following two propositions are true:

(20) If i is expressible by n, then $\mathrm{ChangeVal\_2}(i,n)$ is expressible by n.

(21) For all natural numbers n, a_1, a_2 such that $a_1 \neq 0$ and $a_2 \neq 0$ and $\mathrm{ChangeVal\_2}(a_1,n) = \mathrm{ChangeVal\_2}(a_2,n)$ holds $a_1 = a_2$.

Let us consider n and let i, j be natural numbers. The functor $\mathrm{MUL\_MOD}(i,j,n)$ yields a natural number and is defined by:

(Def. 9) $\mathrm{MUL\_MOD}(i,j,n) = \mathrm{ChangeVal\_2}(\mathrm{ChangeVal\_1}(i,n) \cdot \mathrm{ChangeVal\_1}(j,n) \bmod (2^n+1), n)$.

Let n be a non empty natural number and let i be a natural number. Let us assume that i is expressible by n and 2^n+1 is prime. The functor $\mathrm{INV\_MOD}(i,n)$ yielding a natural number is defined as follows:

(Def. 10) $\mathrm{MUL\_MOD}(i, \mathrm{INV\_MOD}(i,n), n) = 1$ and $\mathrm{INV\_MOD}(i,n)$ is expressible by n.

We now state several propositions:

(22) $\mathrm{MUL\_MOD}(i,j,n) = \mathrm{MUL\_MOD}(j,i,n)$.

(23) If i is expressible by n, then $\mathrm{MUL\_MOD}(1,i,n) = i$.

(24) Suppose 2^n+1 is prime and i is expressible by n and j is expressible by n and k is expressible by n. Then $\mathrm{MUL\_MOD}(\mathrm{MUL\_MOD}(i,j,n),k,n) = \mathrm{MUL\_MOD}(i, \mathrm{MUL\_MOD}(j,k,n), n)$.

(25) $\mathrm{MUL\_MOD}(i,j,n)$ is expressible by n.

(26) If $\mathrm{ChangeVal\_2}(i,n) = 1$, then $i = 1$.

3. Operations of IDEA Cryptograms

Let us consider n and let m, k be finite sequences of elements of $\mathbb{N}$. The functor $\mathrm{IDEAoperationA}(m,k,n)$ yields a finite sequence of elements of $\mathbb{N}$ and is defined by the conditions (Def. 11).

(Def. 11)(i) $\mathrm{len}\,\mathrm{IDEAoperationA}(m,k,n) = \mathrm{len}\,m$, and

(ii) for every natural number i such that $i \in \mathrm{dom}\,m$ holds if $i = 1$, then $(\mathrm{IDEAoperationA}(m,k,n))(i) = \mathrm{MUL\_MOD}(m(1),k(1),n)$ and if $i = 2$, then $(\mathrm{IDEAoperationA}(m,k,n))(i) = \mathrm{ADD\_MOD}(m(2),k(2),n)$ and if $i = 3$, then $(\mathrm{IDEAoperationA}(m,k,n))(i) = \mathrm{ADD\_MOD}(m(3),k(3),n)$ and if $i = 4$, then $(\mathrm{IDEAoperationA}(m,k,n))(i) = \mathrm{MUL\_MOD}(m(4),k(4),n)$ and if $i \neq 1$ and $i \neq 2$ and $i \neq 3$ and $i \neq 4$, then $(\mathrm{IDEAoperationA}(m,k,n))(i) = m(i)$.

In the sequel m, k, k_1, k_2 denote finite sequences of elements of $\mathbb{N}$.

Let n be a non empty natural number and let m, k be finite sequences of elements of $\mathbb{N}$. The functor $\mathrm{IDEAoperationB}(m,k,n)$ yields a finite sequence of elements of $\mathbb{N}$ and is defined by the conditions (Def. 12).

(Def. 12)(i) $\operatorname{len}\mathrm{IDEAoperationB}(m,k,n) = \operatorname{len}m$, and

(ii) for every natural number i such that $i \in \operatorname{dom}m$ holds if $i = 1$, then $(\mathrm{IDEAoperationB}(m,k,n))(i) = \mathrm{Absval}((n\text{-BinarySequence}(m(1))) \oplus (n\text{-BinarySequence}(\mathrm{MUL\_MOD}(\mathrm{ADD\_MOD}(\mathrm{MUL\_MOD}(\mathrm{Absval}((n\text{-BinarySequence}(m(1))) \oplus (n\text{-BinarySequence}(m(3)))),k(5),n),\mathrm{Absval}((n\text{-BinarySequence}(m(2))) \oplus (n\text{-BinarySequence}(m(4)))),n),k(6),n))))$ and if $i = 2$, then $(\mathrm{IDEAoperationB}(m,k,n))(i) = \mathrm{Absval}((n\text{-BinarySequence}(m(2))) \oplus (n\text{-BinarySequence}(\mathrm{ADD\_MOD}(\mathrm{MUL\_MOD}(\mathrm{Absval}((n\text{-BinarySequence}(m(1))) \oplus (n\text{-BinarySequence}(m(3)))),k(5),n),\mathrm{MUL\_MOD}(\mathrm{ADD\_MOD}(\mathrm{MUL\_MOD}(\mathrm{Absval}((n\text{-BinarySequence}(m(1))) \oplus (n\text{-BinarySequence}(m(3)))),k(5),n),\mathrm{Absval}((n\text{-BinarySequence}(m(2))) \oplus (n\text{-BinarySequence}(m(4)))),n),k(6),n),n))))$ and if $i = 3$, then $(\mathrm{IDEAoperationB}(m,k,n))(i) = \mathrm{Absval}((n\text{-BinarySequence}(m(3))) \oplus (n\text{-BinarySequence}(\mathrm{MUL\_MOD}(\mathrm{ADD\_MOD}(\mathrm{MUL\_MOD}(\mathrm{Absval}((n\text{-BinarySequence}(m(1))) \oplus (n\text{-BinarySequence}(m(3)))),k(5),n),\mathrm{Absval}((n\text{-BinarySequence}(m(2))) \oplus (n\text{-BinarySequence}(m(4)))),n),k(6),n))))$ and if $i = 4$, then $(\mathrm{IDEAoperationB}(m,k,n))(i) = \mathrm{Absval}((n\text{-BinarySequence}(m(4))) \oplus (n\text{-BinarySequence}(\mathrm{ADD\_MOD}(\mathrm{MUL\_MOD}(\mathrm{Absval}((n\text{-BinarySequence}(m(1))) \oplus (n\text{-BinarySequence}(m(3)))),k(5),n),\mathrm{MUL\_MOD}(\mathrm{ADD\_MOD}(\mathrm{MUL\_MOD}(\mathrm{Absval}((n\text{-BinarySequence}(m(1))) \oplus (n\text{-BinarySequence}(m(3)))),k(5),n),\mathrm{Absval}((n\text{-BinarySequence}(m(2))) \oplus (n\text{-BinarySequence}(m(4)))),n),k(6),n),n))))$ and if $i \neq 1$ and $i \neq 2$ and $i \neq 3$ and $i \neq 4$, then $(\mathrm{IDEAoperationB}(m,k,n))(i) = m(i)$.

Let m be a finite sequence of elements of $\mathbb{N}$. The functor $\mathrm{IDEAoperationC}\,m$ yielding a finite sequence of elements of $\mathbb{N}$ is defined by:

(Def. 13) $\operatorname{len}\mathrm{IDEAoperationC}\,m = \operatorname{len}m$ and for every natural number i such that $i \in \operatorname{dom}m$ holds $(\mathrm{IDEAoperationC}\,m)(i) = (i = 2 \rightarrow m(3),(i = 3 \rightarrow m(2),m(i)))$.

One can prove the following propositions:

(27) Suppose $\operatorname{len}m \geq 4$. Then

(i) $(\mathrm{IDEAoperationA}(m,k,n))(1)$ is expressible by n,

(ii) $(\mathrm{IDEAoperationA}(m,k,n))(2)$ is expressible by n,

(iii) $(\mathrm{IDEAoperationA}(m,k,n))(3)$ is expressible by n, and

(iv) $(\mathrm{IDEAoperationA}(m,k,n))(4)$ is expressible by n.

(28) Let n be a non empty natural number. Suppose $\operatorname{len}m \geq 4$. Then

(i) $(\mathrm{IDEAoperationB}(m,k,n))(1)$ is expressible by n,

(ii) $(\mathrm{IDEAoperationB}(m,k,n))(2)$ is expressible by n,

(iii) $(\mathrm{IDEAoperationB}(m,k,n))(3)$ is expressible by n, and

(iv) $(\mathrm{IDEAoperationB}(m,k,n))(4)$ is expressible by n.

(29) Suppose that

(i) $\operatorname{len}m \geq 4$,

(ii) $m(1)$ is expressible by n,

(iii) $m(2)$ is expressible by n,

(iv) $m(3)$ is expressible by n, and

(v) $m(4)$ is expressible by n.

Then

(vi) $(\mathrm{IDEAoperationC}\,m)(1)$ is expressible by n,

(vii) $(\mathrm{IDEAoperationC}\,m)(2)$ is expressible by n,

(viii) $(\mathrm{IDEAoperationC}\,m)(3)$ is expressible by n, and

(ix) $(\mathrm{IDEAoperationC}\,m)(4)$ is expressible by n.

(30) Let n be a non empty natural number and given m, k_1, k_2. Suppose that $2^n + 1$ is prime and $\operatorname{len}m \geq 4$ and $m(1)$ is expressible by n and $m(2)$ is expressible by n and $m(3)$ is expressible by n and $m(4)$ is expressible by n and $k_1(1)$ is expressible by n and $k_1(2)$ is expressible by n and $k_1(3)$ is expressible by n and $k_1(4)$ is expressible by n and $k_2(1) = \mathrm{INV\_MOD}(k_1(1),n)$ and $k_2(2) = \mathrm{NEG\_MOD}(k_1(2),n)$ and $k_2(3) = \mathrm{NEG\_MOD}(k_1(3),n)$ and $k_2(4) = \mathrm{INV\_MOD}(k_1(4),n)$. Then $\mathrm{IDEAoperationA}(\mathrm{IDEAoperationA}(m,k_1,n),k_2,n) = m$.

(31) Let n be a non empty natural number and given m, k_1, k_2. Suppose that $2^n + 1$ is prime and $\operatorname{len} m \geq 4$ and $m(1)$ is expressible by n and $m(2)$ is expressible by n and $m(3)$ is expressible by n and $m(4)$ is expressible by n and $k_1(1)$ is expressible by n and $k_1(2)$ is expressible by n and $k_1(3)$ is expressible by n and $k_1(4)$ is expressible by n and $k_2(1) = \mathrm{INV\_MOD}(k_1(1), n)$ and $k_2(2) = \mathrm{NEG\_MOD}(k_1(3), n)$ and $k_2(3) = \mathrm{NEG\_MOD}(k_1(2), n)$ and $k_2(4) = \mathrm{INV\_MOD}(k_1(4), n)$. Then $\mathrm{IDEAoperationA}(\mathrm{IDEAoperationC}\,\mathrm{IDEAoperationA}(\mathrm{IDEAoperationC}\,m, k_1, n), k_2, n) = m$.

(32) Let n be a non empty natural number and given m, k_1, k_2. Suppose that $2^n + 1$ is prime and $\operatorname{len} m \geq 4$ and $m(1)$ is expressible by n and $m(2)$ is expressible by n and $m(3)$ is expressible by n and $m(4)$ is expressible by n and $k_1(5)$ is expressible by n and $k_1(6)$ is expressible by n and $k_2(5) = k_1(5)$ and $k_2(6) = k_1(6)$. Then $\mathrm{IDEAoperationB}(\mathrm{IDEAoperationB}(m, k_1, n), k_2, n) = m$.

(33) For every m such that $\operatorname{len} m \geq 4$ holds $\mathrm{IDEAoperationC}\,\mathrm{IDEAoperationC}\,m = m$.

4. Sequences of IDEA Cryptogram's Operations

The set MESSAGES is defined as follows:

(Def. 14) $\mathrm{MESSAGES} = \mathbb{N}^*$.

Let us note that MESSAGES is non empty.

Let us observe that every element of MESSAGES is function-like and relation-like.

Let us mention that every element of MESSAGES is finite sequence-like.

Let n be a non empty natural number and let us consider k. The functor $\mathrm{IDEA\_P}(k, n)$ yields a function from MESSAGES into MESSAGES and is defined as follows:

(Def. 15) For every m holds $(\mathrm{IDEA\_P}(k, n))(m) = \mathrm{IDEAoperationA}(\mathrm{IDEAoperationC}\,\mathrm{IDEAoperationB}(m, k, n), k, n)$.

Let n be a non empty natural number and let us consider k. The functor $\mathrm{IDEA\_Q}(k, n)$ yields a function from MESSAGES into MESSAGES and is defined as follows:

(Def. 16) For every m holds $(\mathrm{IDEA\_Q}(k, n))(m) = \mathrm{IDEAoperationB}(\mathrm{IDEAoperationA}(\mathrm{IDEAoperationC}\,m, k, n), k, n)$.

Let r, l_1 be natural numbers, let n be a non empty natural number, and let K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$. The functor $\mathrm{IDEA\_P\_F}(K_1, n, r)$ yields a finite sequence and is defined by:

(Def. 17) $\operatorname{len} \mathrm{IDEA\_P\_F}(K_1, n, r) = r$ and for every i such that $i \in \operatorname{dom} \mathrm{IDEA\_P\_F}(K_1, n, r)$ holds $(\mathrm{IDEA\_P\_F}(K_1, n, r))(i) = \mathrm{IDEA\_P}(\mathrm{Line}(K_1, i), n)$.

Let r, l_1 be natural numbers, let n be a non empty natural number, and let K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$. Observe that $\mathrm{IDEA\_P\_F}(K_1, n, r)$ is function yielding.

Let r, l_1 be natural numbers, let n be a non empty natural number, and let K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$. The functor $\mathrm{IDEA\_Q\_F}(K_1, n, r)$ yields a finite sequence and is defined by:

(Def. 18) $\operatorname{len} \mathrm{IDEA\_Q\_F}(K_1, n, r) = r$ and for every i such that $i \in \operatorname{dom} \mathrm{IDEA\_Q\_F}(K_1, n, r)$ holds $(\mathrm{IDEA\_Q\_F}(K_1, n, r))(i) = \mathrm{IDEA\_Q}(\mathrm{Line}(K_1, (r -' i) + 1), n)$.

Let r, l_1 be natural numbers, let n be a non empty natural number, and let K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$. One can check that $\mathrm{IDEA\_Q\_F}(K_1, n, r)$ is function yielding.

Let us consider k, n. The functor $\mathrm{IDEA\_PS}(k, n)$ yields a function from MESSAGES into MESSAGES and is defined as follows:

(Def. 19) For every m holds $(\mathrm{IDEA\_PS}(k, n))(m) = \mathrm{IDEAoperationA}(m, k, n)$.

Let us consider k, n. The functor $\mathrm{IDEA\_QS}(k, n)$ yields a function from MESSAGES into MESSAGES and is defined by:

(Def. 20) For every m holds $(\mathrm{IDEA\_QS}(k, n))(m) = \mathrm{IDEAoperationA}(m, k, n)$.

Let n be a non empty natural number and let us consider k. The functor IDEA_PE(k,n) yields a function from MESSAGES into MESSAGES and is defined by:

(Def. 21) For every m holds $(\mathrm{IDEA\_PE}(k,n))(m) = \mathrm{IDEAoperationA}(\mathrm{IDEAoperationB}(m,k,n),k,n)$.

Let n be a non empty natural number and let us consider k. The functor IDEA_QE(k,n) yields a function from MESSAGES into MESSAGES and is defined by:

(Def. 22) For every m holds $(\mathrm{IDEA\_QE}(k,n))(m) = \mathrm{IDEAoperationB}(\mathrm{IDEAoperationA}(m,k,n),k,n)$.

One can prove the following propositions:

(34) Let n be a non empty natural number and given m, k_1, k_2. Suppose that 2^n+1 is prime and $\mathrm{len}\, m \geq 4$ and $m(1)$ is expressible by n and $m(2)$ is expressible by n and $m(3)$ is expressible by n and $m(4)$ is expressible by n and $k_1(1)$ is expressible by n and $k_1(2)$ is expressible by n and $k_1(3)$ is expressible by n and $k_1(4)$ is expressible by n and $k_1(5)$ is expressible by n and $k_1(6)$ is expressible by n and $k_2(1) = \mathrm{INV\_MOD}(k_1(1),n)$ and $k_2(2) = \mathrm{NEG\_MOD}(k_1(3),n)$ and $k_2(3) = \mathrm{NEG\_MOD}(k_1(2),n)$ and $k_2(4) = \mathrm{INV\_MOD}(k_1(4),n)$ and $k_2(5) = k_1(5)$ and $k_2(6) = k_1(6)$. Then $(\mathrm{IDEA\_Q}(k_2,n) \cdot \mathrm{IDEA\_P}(k_1,n))(m) = m$.

(35) Let n be a non empty natural number and given m, k_1, k_2. Suppose that 2^n+1 is prime and $\mathrm{len}\, m \geq 4$ and $m(1)$ is expressible by n and $m(2)$ is expressible by n and $m(3)$ is expressible by n and $m(4)$ is expressible by n and $k_1(1)$ is expressible by n and $k_1(2)$ is expressible by n and $k_1(3)$ is expressible by n and $k_1(4)$ is expressible by n and $k_2(1) = \mathrm{INV\_MOD}(k_1(1),n)$ and $k_2(2) = \mathrm{NEG\_MOD}(k_1(2),n)$ and $k_2(3) = \mathrm{NEG\_MOD}(k_1(3),n)$ and $k_2(4) = \mathrm{INV\_MOD}(k_1(4),n)$. Then $(\mathrm{IDEA\_QS}(k_2,n) \cdot \mathrm{IDEA\_PS}(k_1,n))(m) = m$.

(36) Let n be a non empty natural number and given m, k_1, k_2. Suppose that 2^n+1 is prime and $\mathrm{len}\, m \geq 4$ and $m(1)$ is expressible by n and $m(2)$ is expressible by n and $m(3)$ is expressible by n and $m(4)$ is expressible by n and $k_1(1)$ is expressible by n and $k_1(2)$ is expressible by n and $k_1(3)$ is expressible by n and $k_1(4)$ is expressible by n and $k_1(5)$ is expressible by n and $k_1(6)$ is expressible by n and $k_2(1) = \mathrm{INV\_MOD}(k_1(1),n)$ and $k_2(2) = \mathrm{NEG\_MOD}(k_1(2),n)$ and $k_2(3) = \mathrm{NEG\_MOD}(k_1(3),n)$ and $k_2(4) = \mathrm{INV\_MOD}(k_1(4),n)$ and $k_2(5) = k_1(5)$ and $k_2(6) = k_1(6)$. Then $(\mathrm{IDEA\_QE}(k_2,n) \cdot \mathrm{IDEA\_PE}(k_1,n))(m) = m$.

(37) Let n be a non empty natural number, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, and k be a natural number. Then $\mathrm{IDEA\_P\_F}(K_1,n,k+1) = (\mathrm{IDEA\_P\_F}(K_1,n,k)) \frown \langle \mathrm{IDEA\_P}(\mathrm{Line}(K_1,k+1),n) \rangle$.

(38) Let n be a non empty natural number, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, and k be a natural number. Then $\mathrm{IDEA\_Q\_F}(K_1,n,k+1) = \langle \mathrm{IDEA\_Q}(\mathrm{Line}(K_1,k+1),n) \rangle \frown \mathrm{IDEA\_Q\_F}(K_1,n,k)$.

(39) Let n be a non empty natural number, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, and k be a natural number. Then $\mathrm{IDEA\_P\_F}(K_1,n,k)$ is a composable finite sequence.

(40) Let n be a non empty natural number, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, and k be a natural number. Then $\mathrm{IDEA\_Q\_F}(K_1,n,k)$ is a composable finite sequence.

(41) Let n be a non empty natural number, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, and k be a natural number. If $k \neq 0$, then $\mathrm{IDEA\_P\_F}(K_1,n,k)$ is a composable sequence from MESSAGES into MESSAGES.

(42) Let n be a non empty natural number, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, and k be a natural number. If $k \neq 0$, then $\mathrm{IDEA\_Q\_F}(K_1,n,k)$ is a composable sequence from MESSAGES into MESSAGES.

(43) Let n be a non empty natural number, M be a finite sequence of elements of $\mathbb{N}$, and given m, k. Suppose $M = (\text{IDEA\_P}(k,n))(m)$ and $\text{len}\, m \geq 4$. Then

(i) $\text{len}\, M \geq 4$,

(ii) $M(1)$ is expressible by n,

(iii) $M(2)$ is expressible by n,

(iv) $M(3)$ is expressible by n, and

(v) $M(4)$ is expressible by n.

(44) Let n be a non empty natural number, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, and r be a natural number. Then $\text{rng}\, \text{compose}_{\text{MESSAGES}}\, \text{IDEA\_P\_F}(K_1,n,r) \subseteq \text{MESSAGES}$ and $\text{dom}\, \text{compose}_{\text{MESSAGES}}\, \text{IDEA\_P\_F}(K_1,n,r) = \text{MESSAGES}$.

(45) Let n be a non empty natural number, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, and r be a natural number. Then $\text{rng}\, \text{compose}_{\text{MESSAGES}}\, \text{IDEA\_Q\_F}(K_1,n,r) \subseteq \text{MESSAGES}$ and $\text{dom}\, \text{compose}_{\text{MESSAGES}}\, \text{IDEA\_Q\_F}(K_1,n,r) = \text{MESSAGES}$.

(46) Let n be a non empty natural number, m be a finite sequence of elements of $\mathbb{N}$, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, r be a natural number, and M be a finite sequence of elements of $\mathbb{N}$. If $M = (\text{compose}_{\text{MESSAGES}}\, \text{IDEA\_P\_F}(K_1,n,r))(m)$ and $\text{len}\, m \geq 4$, then $\text{len}\, M \geq 4$.

(47) Let n be a non empty natural number, l_1 be a natural number, K_1 be a matrix over $\mathbb{N}$ of dimension $l_1 \times 6$, r be a natural number, M be a finite sequence of elements of $\mathbb{N}$, and given m. Suppose that

(i) $M = (\text{compose}_{\text{MESSAGES}}\, \text{IDEA\_P\_F}(K_1,n,r))(m)$,

(ii) $\text{len}\, m \geq 4$,

(iii) $m(1)$ is expressible by n,

(iv) $m(2)$ is expressible by n,

(v) $m(3)$ is expressible by n, and

(vi) $m(4)$ is expressible by n.

Then

(vii) $\text{len}\, M \geq 4$,

(viii) $M(1)$ is expressible by n,

(ix) $M(2)$ is expressible by n,

(x) $M(3)$ is expressible by n, and

(xi) $M(4)$ is expressible by n.

5. Modeling of IDEA Cryptogram

We now state two propositions:

(48) Let n be a non empty natural number, l_1 be a natural number, K_2, K_3 be matrices over $\mathbb{N}$ of dimension $l_1 \times 6$, r be a natural number, and given m. Suppose that $l_1 \geq r$ and $2^n + 1$ is prime and $\text{len}\, m \geq 4$ and $m(1)$ is expressible by n and $m(2)$ is expressible by n and $m(3)$ is expressible by n and $m(4)$ is expressible by n and for every natural number i such that $i \leq r$ holds $K_2 \circ (i,1)$ is expressible by n and $K_2 \circ (i,2)$ is expressible by n and $K_2 \circ (i,3)$ is expressible by n and $K_2 \circ (i,4)$ is expressible by n and $K_2 \circ (i,5)$ is expressible by n and $K_2 \circ (i,6)$ is expressible by n and $K_3 \circ (i,1)$ is expressible by n and $K_3 \circ (i,2)$ is expressible by n and $K_3 \circ (i,3)$ is expressible by n and $K_3 \circ (i,4)$ is expressible by n and $K_3 \circ (i,5)$ is expressible by n and $K_3 \circ (i,6)$ is expressible by n and $K_3 \circ (i,1) = \text{INV\_MOD}(K_2 \circ (i,1),n)$ and $K_3 \circ (i,2) = \text{NEG\_MOD}(K_2 \circ (i,3),n)$ and $K_3 \circ (i,3) = \text{NEG\_MOD}(K_2 \circ (i,2),n)$ and $K_3 \circ (i,4) = \text{INV\_MOD}(K_2 \circ (i,4),n)$ and $K_2 \circ (i,5) = K_3 \circ (i,5)$ and $K_2 \circ (i,6) = K_3 \circ (i,6)$. Then $(\text{compose}_{\text{MESSAGES}}((\text{IDEA\_P\_F}(K_2,n,r)) ^\frown \text{IDEA\_Q\_F}(K_3,n,r)))(m) = m$.

(49) Let n be a non empty natural number, l_1 be a natural number, K_2, K_3 be matrices over $\mathbb{N}$ of dimension $l_1 \times 6$, r be a natural number, k_3, k_4, k_5, k_6 be finite sequences of elements of $\mathbb{N}$, and given m. Suppose that $l_1 \geq r$ and 2^n+1 is prime and $\operatorname{len} m \geq 4$ and $m(1)$ is expressible by n and $m(2)$ is expressible by n and $m(3)$ is expressible by n and $m(4)$ is expressible by n and for every natural number i such that $i \leq r$ holds $K_2 \circ (i,1)$ is expressible by n and $K_2 \circ (i,2)$ is expressible by n and $K_2 \circ (i,3)$ is expressible by n and $K_2 \circ (i,4)$ is expressible by n and $K_2 \circ (i,5)$ is expressible by n and $K_2 \circ (i,6)$ is expressible by n and $K_3 \circ (i,1)$ is expressible by n and $K_3 \circ (i,2)$ is expressible by n and $K_3 \circ (i,3)$ is expressible by n and $K_3 \circ (i,4)$ is expressible by n and $K_3 \circ (i,5)$ is expressible by n and $K_3 \circ (i,6)$ is expressible by n and $K_3 \circ (i,1) = \mathrm{INV\_MOD}(K_2 \circ (i,1),n)$ and $K_3 \circ (i,2) = \mathrm{NEG\_MOD}(K_2 \circ (i,3),n)$ and $K_3 \circ (i,3) = \mathrm{NEG\_MOD}(K_2 \circ (i,2),n)$ and $K_3 \circ (i,4) = \mathrm{INV\_MOD}(K_2 \circ (i,4),n)$ and $K_2 \circ (i,5) = K_3 \circ (i,5)$ and $K_2 \circ (i,6) = K_3 \circ (i,6)$ and $k_3(1)$ is expressible by n and $k_3(2)$ is expressible by n and $k_3(3)$ is expressible by n and $k_3(4)$ is expressible by n and $k_4(1) = \mathrm{INV\_MOD}(k_3(1),n)$ and $k_4(2) = \mathrm{NEG\_MOD}(k_3(2),n)$ and $k_4(3) = \mathrm{NEG\_MOD}(k_3(3),n)$ and $k_4(4) = \mathrm{INV\_MOD}(k_3(4),n)$ and $k_5(1)$ is expressible by n and $k_5(2)$ is expressible by n and $k_5(3)$ is expressible by n and $k_5(4)$ is expressible by n and $k_5(5)$ is expressible by n and $k_5(6)$ is expressible by n and $k_6(1) = \mathrm{INV\_MOD}(k_5(1),n)$ and $k_6(2) = \mathrm{NEG\_MOD}(k_5(2),n)$ and $k_6(3) = \mathrm{NEG\_MOD}(k_5(3),n)$ and $k_6(4) = \mathrm{INV\_MOD}(k_5(4),n)$ and $k_6(5) = k_5(5)$ and $k_6(6) = k_5(6)$. Then $(\mathrm{IDEA\_QS}(k_4,n) \cdot (\mathrm{compose}_{\mathrm{MESSAGES}}\,\mathrm{IDEA\_Q\_F}(K_3,n,r) \cdot (\mathrm{IDEA\_QE}(k_6,n) \cdot (\mathrm{IDEA\_PE}(k_5,n) \cdot (\mathrm{compose}_{\mathrm{MESSAGES}}\,\mathrm{IDEA\_P\_F}(K_2,n,r) \cdot \mathrm{IDEA\_PS}(k_3,n))))))(m) = m$.

REFERENCES

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/nat_1.html.

[2] Grzegorz Bancerek. Curried and uncurried functions. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/funct_5.html.

[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/finseq_1.html.

[4] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Journal of Formalized Mathematics*, 8, 1996. http://mizar.org/JFM/Vol8/funct_7.html.

[5] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_1.html.

[6] Czesław Byliński. Functions from a set to a set. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_2.html.

[7] Czesław Byliński. Partial functions. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/partfun1.html.

[8] Czesław Byliński. A classical first order language. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/cqc_lang.html.

[9] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/finseq_2.html.

[10] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Journal of Formalized Mathematics*, 3, 1991. http://mizar.org/JFM/Vol3/matrix_1.html.

[11] Andrzej Kondracki. The Chinese Remainder Theorem. *Journal of Formalized Mathematics*, 9, 1997. http://mizar.org/JFM/Vol9/wsierp_1.html.

[12] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/int_2.html.

[13] Beata Madras. Product of family of universal algebras. *Journal of Formalized Mathematics*, 5, 1993. http://mizar.org/JFM/Vol5/pralg_1.html.

[14] Robert Milewski. Binary arithmetics. Binary sequences. *Journal of Formalized Mathematics*, 10, 1998. http://mizar.org/JFM/Vol10/binari_3.html.

[15] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Journal of Formalized Mathematics*, 5, 1993. http://mizar.org/JFM/Vol5/binarith.html.

[16] Konrad Raczkowski and Andrzej Nędzusiak. Series. *Journal of Formalized Mathematics*, 3, 1991. http://mizar.org/JFM/Vol3/series_1.html.

[17] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. http://mizar.org/JFM/Axiomatics/tarski.html.

[18] Andrzej Trybulec. Subsets of real numbers. *Journal of Formalized Mathematics*, Addenda, 2003. `http://mizar.org/JFM/Addenda/numbers.html`.

[19] Michał J. Trybulec. Integers. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/int_1.html`.

[20] Wojciech A. Trybulec. Pigeon hole principle. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/finseq_4.html`.

[21] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/subset_1.html`.

[22] Edmund Woronowicz. Relations and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/relat_1.html`.

[23] Edmund Woronowicz. Many-argument relations. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/margrel1.html`.

Received September 7, 1998

Published January 2, 2004