FORMALIZED MATHEMATICS
Volume 7, Number 2, 1998
University 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`.

The articles [11], [2], [4], [5], [6], [3], [10], [14], [8], [1], [7], [15], [12], [13], and [9] 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 tuples of n and *Boolean*.

Next we state several propositions:

(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 $k_1 \mathrm{mod} n = k_2 \mathrm{mod} n$ and $k_1 \leqslant k_2$ there exists a natural number t such that $k_2 - k_1 = n \cdot t$.

ISSN 1426–2630

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

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

(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 the n-th power of $2 \neq 1$.

2. Basic Operators of IDEA Cryptograms

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

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

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

(Def. 2) For every i such that $i \in \mathrm{Seg}\, n$ holds $\pi_i(x \oplus y) = \pi_i x \oplus \pi_i y$.

The following propositions are true:

(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 tuples of n and *Boolean*. Let us observe 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) $i <$ the n-th power of 2.

The following proposition is true

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

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

(Def. 4) $\mathrm{ADD\_MOD}(i, j, n) = (i + j) \bmod (\text{the } n\text{-th power of } 2)$.

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 by:

(Def. 5) $\mathrm{NEG\_N}(i, n) = (\text{the } n\text{-th power of } 2) - i$.

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

(Def. 6) NEG_MOD(i,n) = NEG_N(i,n) mod (the n-th power of 2).

We now state several propositions:

(12) For all n, i such that i is expressible by n holds ADD_MOD$(i,$ NEG_MOD$(i,n),n) = 0$.

(13) For all n, i, j holds ADD_MOD(i,j,n) = ADD_MOD(j,i,n).

(14) For all n, i such that i is expressible by n holds ADD_MOD$(0,i,n) = i$.

(15) For all n, i, j, k holds ADD_MOD(ADD_MOD$(i,j,n),k,n)$ = ADD_MOD$(i,$ ADD_MOD$(j,k,n),n)$.

(16) For all n, i, j holds ADD_MOD(i,j,n) is expressible by n.

(17) For all n, i such that i is expressible by n holds NEG_MOD(i,n) is expressible by n.

Let us consider n and let i be a natural number. The functor ChangeVal_1(i,n) yields a natural number and is defined by:

(Def. 7) $\text{ChangeVal\_1}(i,n) = \begin{cases} \text{the } n\text{-th power of 2}, & \text{if } i = 0, \\ i, & \text{otherwise.} \end{cases}$

We now state two propositions:

(18) For all n, i such that i is expressible by n holds ChangeVal_1$(i,n) \leqslant$ the n-th power of 2 and 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 ChangeVal_1(a_1,n) = ChangeVal_1(a_2,n). Then $a_1 = a_2$.

Let us consider n and let i be a natural number. The functor ChangeVal_2(i,n) yields a natural number and is defined as follows:

(Def. 8) $\text{ChangeVal\_2}(i,n) = \begin{cases} 0, & \text{if } i = \text{the } n\text{-th power of 2}, \\ i, & \text{otherwise.} \end{cases}$

We now state two propositions:

(20) For all n, i such that i is expressible by n holds 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 ChangeVal_2(a_1,n) = ChangeVal_2(a_2,n) holds $a_1 = a_2$.

Let us consider n and let i, j be natural numbers. The functor MUL_MOD(i,j,n) yields a natural number and is defined as follows:

(Def. 9) MUL_MOD(i,j,n) = ChangeVal_2(ChangeVal_1$(i,n)\cdot$ ChangeVal_1(j,n) mod ((the n-th power of 2)+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 (the n-th power of 2)+1 is prime. The functor INV_MOD(i,n) yielding a natural number is defined as follows:

(Def. 10) MUL_MOD$(i,$ INV_MOD$(i,n),n) = 1$ and INV_MOD(i,n) is expressible by n.

The following propositions are true:

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

(23) For all n, i such that i is expressible by n holds $\mathrm{MUL\_MOD}(1, i, n) = i$.

(24) Let given n, i, j, k. Suppose that

(i) (the n-th power of 2)+1 is prime,

(ii) i is expressible by n,

(iii) j is expressible by n, and

(iv) 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) For all n, i, j holds $\mathrm{MUL\_MOD}(i, j, n)$ 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 $\mathrm{IDEAoperationA}(m, k, n)$ yielding a finite sequence of elements of $\mathbb{N}$ 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 $\mathrm{IDEAoperationB}(m, k, n)$ yielding a finite sequence of elements of $\mathbb{N}$ is defined by the conditions (Def. 12).

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

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

$(m(1))) \oplus (n\text{-BinarySequence}(m(3)))), k(5), n), \text{MUL\_MOD}(\text{ADD\_MOD}$ $(\text{MUL\_MOD}(\text{Absval}((n\text{-BinarySequence}$ $(m(1)))\oplus(n\text{-BinarySequence}(m(3)))), k(5), n), \text{Absval}((n\text{-BinarySequence}(m$ $(2))) \oplus (n\text{-BinarySequence}(m(4)))), n), k(6), n), n))))$ and if $i = 3$, then $(\text{IDEAoperationB}(m, k, n))(i) = \text{Absval}((n\text{-BinarySequence}(m(3))) \oplus$ $(n\text{-BinarySequence}(\text{MUL\_MOD}(\text{ADD\_MOD}(\text{MUL\_MOD}(\text{Absval}$ $((n\text{-BinarySequence}(m(1)))\oplus(n\text{-BinarySequence}(m(3)))), k(5), n), \text{Absval}$ $((n\text{-BinarySequence}(m(2))) \oplus (n\text{-BinarySequence}(m(4)))), n), k(6), n))))$ and if $i = 4$, then $(\text{IDEAoperationB}(m, k, n))(i) =$ $\text{Absval}((n\text{-BinarySequence}(m(4))) \oplus (n\text{-BinarySequence}$ $(\text{ADD\_MOD}(\text{MUL\_MOD}(\text{Absval}((n\text{-BinarySequence}(m(1)))\oplus$ $(n\text{-BinarySequence}(m(3)))), k(5), n), \text{MUL\_MOD}(\text{ADD\_MOD}(\text{MUL\_MOD}$ $(\text{Absval}((n\text{-BinarySequence}(m(1)))\oplus(n\text{-BinarySequence}(m(3)))), k(5), n),$ $\text{Absval}((n\text{-BinarySequence}(m(2)))\oplus(n\text{-BinarySequence}(m(4)))), n), k(6),$ $n), n))))$ and if $i \neq 1$ and $i \neq 2$ and $i \neq 3$ and $i \neq 4$, then $(\text{IDEAoperationB}(m, k, n))(i) = m(i)$.

Let m be a finite sequence of elements of $\mathbb{N}$. The functor $\text{IDEAoperationC}\, m$ yields a finite sequence of elements of $\mathbb{N}$ and is defined as follows:

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

The following propositions are true:

(27) Let given n, m, k. Suppose $\text{len}\, m \geqslant 4$. Then
- (i) $(\text{IDEAoperationA}(m, k, n))(1)$ is expressible by n,
- (ii) $(\text{IDEAoperationA}(m, k, n))(2)$ is expressible by n,
- (iii) $(\text{IDEAoperationA}(m, k, n))(3)$ is expressible by n, and
- (iv) $(\text{IDEAoperationA}(m, k, n))(4)$ is expressible by n.

(28) Let n be a non empty natural number and given m, k. Suppose $\text{len}\, m \geqslant 4$. Then
- (i) $(\text{IDEAoperationB}(m, k, n))(1)$ is expressible by n,
- (ii) $(\text{IDEAoperationB}(m, k, n))(2)$ is expressible by n,
- (iii) $(\text{IDEAoperationB}(m, k, n))(3)$ is expressible by n, and
- (iv) $(\text{IDEAoperationB}(m, k, n))(4)$ is expressible by n.

(29) Let given m. Suppose that
- (i) $\text{len}\, m \geqslant 4$,
- (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) $(\text{IDEAoperationC}\, m)(1)$ is expressible by n,

(vii) (IDEAoperationC m)(2) is expressible by n,
(viii) (IDEAoperationC m)(3) is expressible by n, and
(ix) (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
(i) (the n-th power of 2)+1 is prime,
(ii) $\operatorname{len} m \geqslant 4$,
(iii) $m(1)$ is expressible by n,
(iv) $m(2)$ is expressible by n,
(v) $m(3)$ is expressible by n,
(vi) $m(4)$ is expressible by n,
(vii) $k_1(1)$ is expressible by n,
(viii) $k_1(2)$ is expressible by n,
(ix) $k_1(3)$ is expressible by n,
(x) $k_1(4)$ is expressible by n,
(xi) $k_2(1) = \mathrm{INV\_MOD}(k_1(1), n)$,
(xii) $k_2(2) = \mathrm{NEG\_MOD}(k_1(2), n)$,
(xiii) $k_2(3) = \mathrm{NEG\_MOD}(k_1(3), n)$, and
(xiv) $k_2(4) = \mathrm{INV\_MOD}(k_1(4), n)$.
Then IDEAoperationA(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
(i) (the n-th power of 2)+1 is prime,
(ii) $\operatorname{len} m \geqslant 4$,
(iii) $m(1)$ is expressible by n,
(iv) $m(2)$ is expressible by n,
(v) $m(3)$ is expressible by n,
(vi) $m(4)$ is expressible by n,
(vii) $k_1(1)$ is expressible by n,
(viii) $k_1(2)$ is expressible by n,
(ix) $k_1(3)$ is expressible by n,
(x) $k_1(4)$ is expressible by n,
(xi) $k_2(1) = \mathrm{INV\_MOD}(k_1(1), n)$,
(xii) $k_2(2) = \mathrm{NEG\_MOD}(k_1(3), n)$,
(xiii) $k_2(3) = \mathrm{NEG\_MOD}(k_1(2), n)$, and
(xiv) $k_2(4) = \mathrm{INV\_MOD}(k_1(4), n)$.
Then IDEAoperationA(IDEAoperationC IDEAoperationA (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
(i) (the n-th power of 2)+1 is prime,
(ii) $\operatorname{len} m \geqslant 4$,
(iii) $m(1)$ is expressible by n,
(iv) $m(2)$ is expressible by n,

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

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

(vii) $k_1(5)$ is expressible by n,

(viii) $k_1(6)$ is expressible by n,

(ix) $k_2(5) = k_1(5)$, and

(x) $k_2(6) = k_1(6)$.

Then IDEAoperationB(IDEAoperationB(m, k_1, n), k_2, n) $= m$.

(33) For every m such that len $m \geqslant 4$ holds IDEAoperationC IDEAoperationC $m = m$.

4. Sequences of IDEA Cryptogram's Operations

The set MESSAGES is defined by:

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

Let us mention that MESSAGES is non empty.

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

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

Let n be a non empty natural number and let us consider k. The functor IDEA_P(k, n) yielding a function from MESSAGES into MESSAGES is defined as follows:

(Def. 15) For every m holds (IDEA_P(k, n))(m) = IDEAoperationA (IDEAoperationC IDEAoperationB(m, k, n), k, n).

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

(Def. 16) For every m holds (IDEA_Q(k, n))(m) = IDEAoperationB (IDEAoperationA(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 IDEA_P_F(K_1, n, r) yielding a finite sequence is defined as follows:

(Def. 17) len IDEA_P_F(K_1, n, r) $= r$ and for every i such that $i \in$ dom IDEA_P_F(K_1, n, r) holds (IDEA_P_F(K_1, n, r))(i) = IDEA_P(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 $l_1 \times 6$. One can verify that 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 $\mathrm{IDEA\_Q\_F}(K_1, n, r)$ yielding a finite sequence is defined as follows:

(Def. 18) $\mathrm{len}\,\mathrm{IDEA\_Q\_F}(K_1, n, r) = r$ and for every i such that $i \in \mathrm{dom}\,\mathrm{IDEA\_Q\_F}(K_1, n, r)$ 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 $l_1 \times 6$. Observe 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 as follows:

(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 $\mathrm{IDEA\_PE}(k, n)$ yielding a function from MESSAGES into MESSAGES 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 $\mathrm{IDEA\_QE}(k, n)$ yielding a function from MESSAGES into MESSAGES is defined by:

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

We now state a number of propositions:

(34) Let n be a non empty natural number and given m, k_1, k_2. Suppose that

- (i) (the n-th power of 2)+1 is prime,
- (ii) $\mathrm{len}\, m \geqslant 4$,
- (iii) $m(1)$ is expressible by n,
- (iv) $m(2)$ is expressible by n,
- (v) $m(3)$ is expressible by n,
- (vi) $m(4)$ is expressible by n,
- (vii) $k_1(1)$ is expressible by n,
- (viii) $k_1(2)$ is expressible by n,
- (ix) $k_1(3)$ is expressible by n,
- (x) $k_1(4)$ is expressible by n,
- (xi) $k_1(5)$ is expressible by n,
- (xii) $k_1(6)$ is expressible by n,
- (xiii) $k_2(1) = \mathrm{INV\_MOD}(k_1(1), n)$,

(xiv) $k_2(2) = \mathrm{NEG\_MOD}(k_1(3), n)$,
(xv) $k_2(3) = \mathrm{NEG\_MOD}(k_1(2), n)$,
(xvi) $k_2(4) = \mathrm{INV\_MOD}(k_1(4), n)$,
(xvii) $k_2(5) = k_1(5)$, and
(xviii) $k_2(6) = k_1(6)$.

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

(i) (the n-th power of 2)+1 is prime,
(ii) $\mathrm{len}\, m \geqslant 4$,
(iii) $m(1)$ is expressible by n,
(iv) $m(2)$ is expressible by n,
(v) $m(3)$ is expressible by n,
(vi) $m(4)$ is expressible by n,
(vii) $k_1(1)$ is expressible by n,
(viii) $k_1(2)$ is expressible by n,
(ix) $k_1(3)$ is expressible by n,
(x) $k_1(4)$ is expressible by n,
(xi) $k_2(1) = \mathrm{INV\_MOD}(k_1(1), n)$,
(xii) $k_2(2) = \mathrm{NEG\_MOD}(k_1(2), n)$,
(xiii) $k_2(3) = \mathrm{NEG\_MOD}(k_1(3), n)$, and
(xiv) $k_2(4) = \mathrm{INV\_MOD}(k_1(4), n)$.

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

(i) (the n-th power of 2)+1 is prime,
(ii) $\mathrm{len}\, m \geqslant 4$,
(iii) $m(1)$ is expressible by n,
(iv) $m(2)$ is expressible by n,
(v) $m(3)$ is expressible by n,
(vi) $m(4)$ is expressible by n,
(vii) $k_1(1)$ is expressible by n,
(viii) $k_1(2)$ is expressible by n,
(ix) $k_1(3)$ is expressible by n,
(x) $k_1(4)$ is expressible by n,
(xi) $k_1(5)$ is expressible by n,
(xii) $k_1(6)$ is expressible by n,
(xiii) $k_2(1) = \mathrm{INV\_MOD}(k_1(1), n)$,
(xiv) $k_2(2) = \mathrm{NEG\_MOD}(k_1(2), n)$,
(xv) $k_2(3) = \mathrm{NEG\_MOD}(k_1(3), n)$,
(xvi) $k_2(4) = \mathrm{INV\_MOD}(k_1(4), n)$,
(xvii) $k_2(5) = k_1(5)$, and
(xviii) $k_2(6) = k_1(6)$.

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 $M = (\mathrm{IDEA\_P}(k, n))(m)$ and $\mathrm{len}\, m \geqslant 4$. Then

- (i) $\mathrm{len}\, M \geqslant 4$,
- (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 $\mathrm{rng}\, \mathrm{compose}_{\mathrm{MESSAGES}}\, \mathrm{IDEA\_P\_F}(K_1, n, r) \subseteq \mathrm{MESSAGES}$ and $\mathrm{dom}\, \mathrm{compose}_{\mathrm{MESSAGES}}\, \mathrm{IDEA\_P\_F}(K_1, n, r) = \mathrm{MESSAGES}$.

(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 $\mathrm{rng}\, \mathrm{compose}_{\mathrm{MESSAGES}}\, \mathrm{IDEA\_Q\_F}(K_1, n, r) \subseteq \mathrm{MESSAGES}$ and $\mathrm{dom}\, \mathrm{compose}_{\mathrm{MESSAGES}}\, \mathrm{IDEA\_Q\_F}(K_1, n, r) = \mathrm{MESSAGES}$.

(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 $\operatorname{len} m \geqslant 4$, then $\operatorname{len} M \geqslant 4$.

(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) $\operatorname{len} m \geqslant 4$,
(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) $\operatorname{len} M \geqslant 4$,
(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

One can prove the following 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

(i) $l_1 \geqslant r$,
(ii) (the n-th power of 2)+1 is prime,
(iii) $\operatorname{len} m \geqslant 4$,
(iv) $m(1)$ is expressible by n,
(v) $m(2)$ is expressible by n,
(vi) $m(3)$ is expressible by n,
(vii) $m(4)$ is expressible by n, and
(viii) for every natural number i such that $i \leqslant r$ holds $(K_2)_{i,1}$ is expressible by n and $(K_2)_{i,2}$ is expressible by n and $(K_2)_{i,3}$ is expressible by n and $(K_2)_{i,4}$ is expressible by n and $(K_2)_{i,5}$ is expressible by n and $(K_2)_{i,6}$ is expressible by n and $(K_3)_{i,1}$ is expressible by n and $(K_3)_{i,2}$ is expressible by n and $(K_3)_{i,3}$ is expressible by n and $(K_3)_{i,4}$ is expressible by n and $(K_3)_{i,5}$ is expressible by n and $(K_3)_{i,6}$ is expressible by n and $(K_3)_{i,1} = \text{INV\_MOD}((K_2)_{i,1}, n)$ and $(K_3)_{i,2} = \text{NEG\_MOD}((K_2)_{i,3}, n)$ and $(K_3)_{i,3} =$

NEG_MOD($(K_2)_{i,2}, n$) and $(K_3)_{i,4}$ = INV_MOD($(K_2)_{i,4}, n$) and $(K_2)_{i,5} = (K_3)_{i,5}$ and $(K_2)_{i,6} = (K_3)_{i,6}$.

Then $(\mathrm{compose}_{\mathrm{MESSAGES}}((\mathrm{IDEA\_P\_F}(K_2, n, r))^\frown\mathrm{IDEA\_Q\_F}(K_3, n, r)))(m) = m$.

(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

(i) $l_1 \geqslant r$,

(ii) (the n-th power of 2)+1 is prime,

(iii) $\mathrm{len}\, m \geqslant 4$,

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

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

(vi) $m(3)$ is expressible by n,

(vii) $m(4)$ is expressible by n,

(viii) for every natural number i such that $i \leqslant r$ holds $(K_2)_{i,1}$ is expressible by n and $(K_2)_{i,2}$ is expressible by n and $(K_2)_{i,3}$ is expressible by n and $(K_2)_{i,4}$ is expressible by n and $(K_2)_{i,5}$ is expressible by n and $(K_2)_{i,6}$ is expressible by n and $(K_3)_{i,1}$ is expressible by n and $(K_3)_{i,2}$ is expressible by n and $(K_3)_{i,3}$ is expressible by n and $(K_3)_{i,4}$ is expressible by n and $(K_3)_{i,5}$ is expressible by n and $(K_3)_{i,6}$ is expressible by n and $(K_3)_{i,1}$ = INV_MOD($(K_2)_{i,1}, n$) and $(K_3)_{i,2}$ = NEG_MOD($(K_2)_{i,3}, n$) and $(K_3)_{i,3}$ = NEG_MOD($(K_2)_{i,2}, n$) and $(K_3)_{i,4}$ = INV_MOD($(K_2)_{i,4}, n$) and $(K_2)_{i,5} = (K_3)_{i,5}$ and $(K_2)_{i,6} = (K_3)_{i,6}$,

(ix) $k_3(1)$ is expressible by n,

(x) $k_3(2)$ is expressible by n,

(xi) $k_3(3)$ is expressible by n,

(xii) $k_3(4)$ is expressible by n,

(xiii) $k_4(1)$ = INV_MOD($k_3(1), n$),

(xiv) $k_4(2)$ = NEG_MOD($k_3(2), n$),

(xv) $k_4(3)$ = NEG_MOD($k_3(3), n$),

(xvi) $k_4(4)$ = INV_MOD($k_3(4), n$),

(xvii) $k_5(1)$ is expressible by n,

(xviii) $k_5(2)$ is expressible by n,

(xix) $k_5(3)$ is expressible by n,

(xx) $k_5(4)$ is expressible by n,

(xxi) $k_5(5)$ is expressible by n,

(xxii) $k_5(6)$ is expressible by n,

(xxiii) $k_6(1)$ = INV_MOD($k_5(1), n$),

(xxiv) $k_6(2)$ = NEG_MOD($k_5(2), n$),

(xxv) $k_6(3)$ = NEG_MOD($k_5(3), n$),

(xxvi) $k_6(4)$ = INV_MOD($k_5(4), n$),

(xxvii) $k_6(5) = k_5(5)$, and

(xxviii) $k_6(6) = k_5(6)$.

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. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[3] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.

[4] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[5] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[6] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[7] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

[8] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.

[9] Andrzej Kondracki. The chinese remainder theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.

[10] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

[11] Robert Milewski. Binary arithmetics. Binary sequences. *Formalized Mathematics*, 7(**1**):23–26, 1998.

[12] Konrad Raczkowski and Andrzej Nędzusiak. Serieses. *Formalized Mathematics*, 2(**4**):449–452, 1991.

[13] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[14] Edmund Woronowicz. Many–argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.

[15] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Received September 7, 1998