Cryptanalysis of the Vesta-2M Stream Cipher

Marina Pudovkina

maripa@online.ru

Moscow Engineering Physics Institute (Technical University)
Department of Cryptology and Discrete Mathematics

Abstract. In this paper the security of the stream cipher Vesta-2M is investigated. Cryptanalytic algorithm is developed for a known plaintext attack where only a small segment of plaintext is assumed to be known. The complexity the attack is estimated the time of searching through the square root of all possible initial states.

Keywords. Cryptanalysis. Stream Cipher. Vesta-2M.

1 Introduction

Any keystream generators for practical stream cipher applications can generally be represented as an autonomous finite-state machine whose initial state and possibly next-state and output functions as well are secret key dependent. Many keystream generators proposed in the literature consist of possibly clocked linear feedback shift registers (LFSR) that are combined by a function without or with memory. On of these generators, known as Vesta-2M, has been publicized and described in [1]. Vesta-2M is widely used in commercial products in Russia [3].

In this paper the security of Vesta-2M is investigated. Cryptanalytic algorithm is developed for a known plaintext attack where only a small segment of plaintext is assumed to be known. The complexity the attack is estimated the time of searching through the square root of all possible initial states. However, this still poses no threat to Vesta-2M in practical applications.

The paper is organized as follows. In section 2 we give a description of Vesta-2M. In section 3 we discuss an attack on a simplified version of Vesta-2M. Section 4 describes attacks on the full Vesta-2M. We conclude in section 5.

2 Description of Vesta-2M

Details of Vesta-2M are given in Figure 1.

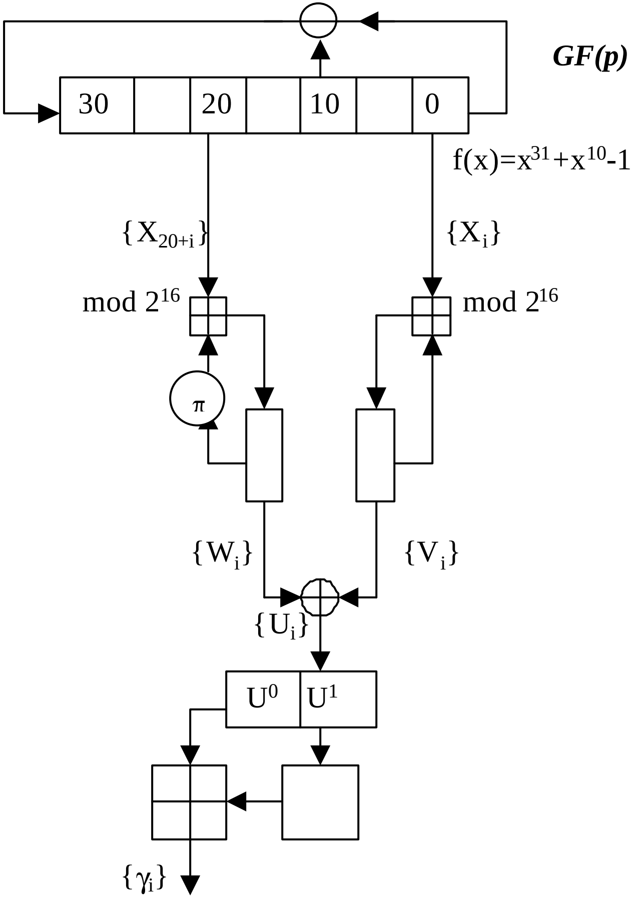
Let p be a prime number of the order 2^{15} and $\left\{x_i\right\}_{i=0}^{\infty}$ be a linear recurrent sequence satisfying

$$X_{31+i}=X_i-X_{i+10}\,(\text{mod p}) \qquad (1)$$

The characteristic polynomial of this sequence is

$$f(\text{x})=\text{x}^{31}+\text{x}^{10}-1 \qquad (2)$$

Fig.1. Vesta –2M



Calculate W_i, V_i, i=1, 2…, as follows:

$$W_i= \pi(W_{i-1})+X_{i-1+20} \pmod{2^{16}} \tag{3}$$

$$V_i= V_{i-1}+X_{i-1} \pmod{2^{16}}. \tag{4}$$

Let $\pi\in S_{2^{16}}$ be a permutation of bits of a binary representation of numbers W_i in the inverse order, i.e. 0 ↔ 15,..., 7 ↔ 8.

Compute

$$U_i = W_i\oplus V_i, \tag{6}$$

Here, $\oplus$ is exclusive-Or (XOR) operation.

Represent U_i as follows

$$U_i = U_i^{(0)} + 2^8\cdot U_i^{(1)}, \tag{7}$$

Compute the output sequence γ_i, i=1,2,3,..., as follows:

$$\gamma_i \equiv U_i^{(0)} + U_{i-1}^{(1)} \pmod{2^8} = U_i^{(0)}+U_{i-1}^{(1)}-\sigma_i\cdot 2^8, \tag{8}$$

where i=1,2,3,..., and $\sigma_i\in\{0,1\}$ is a carry bit.

A key of Vesta-2M consists of values $X_0, X_1,\dots, X_{30}$ and U_0, W_0, V_0.

3 Attack on Vesta-2M without the permutation.

In this section we describe a known plaintext attack on Vesta-2M without permutation π. We begin with definitions. Here and the rest of the paper we keep to them.

Let $\{ z_i^{(15)},\ldots,z_i^{(7)}, z_i^{(6)},\ldots, z^{(0)}\}$ be a binary representation of Z, where $Z=X_i$, p, V_i, U_i, W_i.
Let $\delta_i^v(j)$ be a carry bit in j bit of $V_i = V_{i-1}+X_i \pmod{2^{16}}$ and $\delta_i^w(j)$ be a carry bit in j bit of $W_i = \pi(W_{i-1})+X_{i-1+20} \pmod{2^{16}}$.
Let

$$\delta_i^p(j) = \begin{cases} 1, & \text{if } (X_i+p\cdot\xi_{i+31}) \pmod{2^{j-1}} < X_{i+10} \pmod{2^{j-1}} \\ 0, & \text{if } (X_i+p\cdot\xi_{i+31}) \pmod{2^{j-1}} \geq X_{i+10} \pmod{2^{j-1}} \end{cases}$$

Then X_{i+31} is represented as follows

$$X_{i+31}= X_i- X_{i+10}+p\cdot\xi_{i+31}.$$

Let

$$\xi_{i+31} = \begin{cases} 1, & \text{if } X_i \leq X_{i+10} \\ 0, & \text{if } X_i > X_{i+10} \end{cases}$$

Let $\delta_{i+31}^x(j)$ be a carry bit in j bit of $X_i + p\cdot\xi_{i+31} \pmod{2^{16}}$.

The attack is based on following propositions.

Proposition 1
If we know $X_0 \pmod{2^8}$, $X_1 \pmod{2^8}$,……, $X_{30} \pmod{2^8}$ and $V_0 \pmod{2^8}$, $U_0 \pmod{2^8}$, $W_0 \pmod{2^8}$, then

$$U_{i-1}^{(1)}= \gamma_i-U_i^{(0)} \pmod{2^8},$$

where i=1...29.
Proof.
From (3), (4) and (5) we get

$$W_i= W_{i-1}+X_{i+20} \pmod{2^8},$$
$$V_i= V_{i-1}+X_i \pmod{2^8},$$
$$U_i^{(0)} =(W_i \bmod 2^8)\oplus V_i(\bmod 2^8).$$

From (8) we have

$$U_{i-1}^{(1)}= \gamma_i-U_i^{(0)} \pmod{2^8}. \qquad (9)$$

where i=1…29.

Proposition 2
$U_i^{(0)} =(W_0+X_0+X_1+\ldots+ X_{i-1}+X_i \pmod{2^8}) \oplus (V_0+ X_0+X_1+\ldots+ X_{i-1}+X_i \pmod{2^8})$.
Proof.
Really, from (3), (4) and (5) we obtain
$U_i^{(0)}= W_i\oplus V_i =(W_{i-1}+ X_i \pmod{2^8}) \oplus (V_{i-1}+ X_{i+20} \pmod{2^8})=\ldots=(W_0+ X_0+ X_1+\ldots+ X_{i-1}+ X_i(\bmod 2^8)) \oplus (V_0+X_0+X_1+\ldots+ X_{i-1}+X_i \pmod{2^8})$.

Proposition 3

$u_i^{(j)} = (v_0^{(j)} \oplus x_0^{(j)} \oplus x_1^{(j)} \oplus x_2^{(j)} \oplus \ldots \oplus x_{i-1}^{(j)} \oplus \delta_1^v(j) \oplus \delta_2^v(j) \ldots \oplus \delta_{i-1}^v(j) \oplus \delta_i^v(j)) \oplus (w_0^{(j)} \oplus x_{20}^{(j)} \oplus x_{21}^{(j)} \oplus x_{22}^{(j)} \oplus \ldots \oplus x_{i+19}^{(j)} \oplus \delta_1^w(j) \oplus \delta_2^w(j) \ldots \oplus \delta_{i-1}^w(j) \oplus \delta_i^w(j))$

Proof.

From (3), (4) and (5) we have

$u_i^{(j)} = v_i^{(j)} \oplus w_i^{(j)} = (v_{i-1}^{(j)} \oplus x_{i-1}^{(j)} \oplus \delta_i^v(j)) \oplus (w_{i-1}^{(j)} \oplus x_{i+19}^{(j)} \oplus \delta_i^w(j)) = (v_{i-2}^{(j)} \oplus x_{i-1}^{(j)} \oplus \delta_i^v(j) \oplus \delta_{i-1}^v(j)) \oplus (w_{i-2}^{(j)} \oplus x_{i+19}^{(j)} \oplus \delta_i^w(j) \oplus \delta_{i-1}^w(j)) = \ldots = (v_0^{(j)} \oplus x_0^{(j)} \oplus x_1^{(j)} \oplus x_2^{(j)} \oplus \ldots \oplus x_{i-1}^{(j)} \oplus \delta_1^v(j) \oplus \delta_2^v(j) \ldots \oplus \delta_{i-1}^v(j) \oplus \delta_i^v(j)) \oplus (w_0^{(j)} \oplus x_{20}^{(j)} \oplus x_{21}^{(j)} \oplus x_{22}^{(j)} \oplus \ldots \oplus x_{i+19}^{(j)} \oplus \delta_1^w(j) \oplus \delta_2^w(j) \ldots \oplus \delta_{i-1}^w(j) \oplus \delta_i^w(j))$.

Proposition 4

$u_i^{(j)} = u_1^{(j)} \oplus u_2^{(j)} \oplus \ldots \oplus u_{i-2}^{(j)} \oplus u_{i-1}^{(j)} \oplus \delta_i^v(j) \oplus \delta_{i-1}^v(j) \oplus \ldots \delta_2^v(j) \oplus \delta_1^v(j) \oplus \delta_i^w(j) \oplus \delta_{i-1}^w(j) \oplus \ldots \oplus \delta_2^w(j) \oplus \delta_1^w(j) \oplus x_{i-1}^{(j)} \oplus x_{i+19}^{(j)}$ (10)

Proof.

From (3), (4) and (5) we obtain

$u_i^{(j)} = v_i^{(j)} \oplus w_i^{(j)} = (v_{i-1}^{(j)} \oplus x_{i-1}^{(j)} \oplus \delta_i^v(j)) \oplus (w_{i-1}^{(j)} \oplus x_{i+19}^{(j)} \oplus \delta_i^w(j)) = u_{i-1}^{(j)} \oplus \delta_i^v(j) \oplus \delta_{i-1}^v(j) \oplus \delta_i^w(j) \oplus \delta_{i-1}^w(j) \oplus x_{i-1}^{(j)} \oplus x_{i+19}^{(j)} = \ldots = u_1^{(j)} \oplus u_2^{(j)} \oplus \ldots \oplus u_{i-2}^{(j)} \oplus u_{i-1}^{(j)} \oplus \delta_i^v(j) \oplus \delta_{i-1}^v(j) \oplus \ldots \delta_2^v(j) \oplus \delta_1^v(j) \oplus \delta_i^w(j) \oplus \delta_{i-1}^w(j) \oplus \ldots \oplus \delta_2^w(j) \oplus \delta_1^w(j) \oplus x_{i-1}^{(j)} \oplus x_{i+19}^{(j)}$.

Remark 1

Let $C_i^{(j)} = u_1^{(j)} \oplus u_2^{(j)} \oplus \ldots \oplus u_{i-2}^{(j)} \oplus u_{i-1}^{(j)} \oplus \delta_i^v(j) \oplus \delta_{i-1}^v(j) \oplus \ldots \delta_2^v(j) \oplus \delta_1^v(j) \oplus \delta_i^w(j) \oplus \delta_{i-1}^w(j) \oplus \ldots \oplus \delta_2^w(j) \oplus \delta_1^w(j) \oplus u_i^{(j)}$.

Then we can rewrite (10) as follows

$$x_{i-1}^{(j)} \oplus x_{i+19}^{(j)} = C_i^{(j)}. \qquad (11)$$

Proposition 5

If we know $\{x_0^{(j-1)}, \ldots, x_0^{(0)}\}$, $\{x_1^{(j-1)}, \ldots, x_1^{(0)}\}$, $\{x_2^{(j-1)}, \ldots, x_2^{(0)}\}, \ldots, \{x_{30}^{(j-1)}, \ldots, x_{30}^{(0)}\}$, then we can determine $x_{i+31}^{(j)}$ by

$$x_{i+31}^{(j)} = x_i^{(j)} \oplus x_{i+10}^{(j)} \oplus \delta_{i+31}^p(j) \oplus \xi_{i+31} \cdot (\delta_{i+31}^x(j) \oplus p^{(j)}).$$

Proof.

Note that $(X_i + p \cdot \xi_{i+31})^{(j)} = x_i^{(j)} \oplus \delta_{i+31}^x(j) \oplus \xi_{i+31} \cdot p^{(j)} = x_i^{(j)} \oplus \xi_{i+31} \cdot (\delta_{i+31}^x(j) \oplus p^{(j)})$.

If $(X_i + p \cdot \xi_{i+31}) \pmod{2^{j-1}} < X_{i+10} \pmod{2^{j-1}}$, then

$$x_{i+31}^{(j)} = x_i^{(j)} \oplus x_{i+10}^{(j)} \oplus 1 \oplus \xi_{i+31} \cdot (\delta_{i+31}^x(j) \oplus p^{(j)}).$$

If $(X_i + p \cdot \xi_{i+31}) \pmod{2^{j-1}} \geq X_{i+10} \pmod{2^{j-1}}$, then

$$x_{i+31}^{(j)} = x_i^{(j)} \oplus x_{i+10}^{(j)} \oplus \xi_{i+31} \cdot (\delta_{i+31}^x(j) \oplus p^{(j)}).$$

Therefore,

$$x_{i+31}^{(j)} = x_i^{(j)} \oplus x_{i+10}^{(j)} \oplus \delta_{i+31}^p(j) \oplus \xi_{i+31} \cdot (\delta_{i+31}^x(j) \oplus p^{(j)}).$$

Remark 2

If we know $\{x_0^{(j-1)}, \ldots, x_0^{(0)}\}$, $\{x_1^{(j-1)}, \ldots, x_1^{(0)}\}$, $\{x_2^{(j-1)}, \ldots, x_2^{(0)}\}, \ldots, \{x_{30}^{(j-1)}, \ldots, x_{30}^{(0)}\}$ and $V_0, W_0, \xi_{31}, \xi_{32}, \ldots, \xi_{50}$, then we can compute $\{C_i^{(k)}\}$, where k=1.. j, i=0..50, and $\{\delta_i^x(j)\}$, $\{\delta_i^p(j)\}$.

Theorem 1

If we know $\{x_0^{(j-1)},\ldots, x_0^{(0)}\}$, $\{x_1^{(j-1)},\ldots, x_1^{(0)}\}$, $\{x_2^{(j-1)},\ldots, x_2^{(0)}\},\ldots,$ $\{ x_{30}^{(j-1)},\ldots, x_{30}^{(0)}\}$, $\xi_{31}, \xi_{32},\ldots, \xi_{50}$ and V_0, W_0, then we can determine $\{x_{30}^{(j)},\ldots, x_0^{(j)} \}$ from the following system of linear equations.

$$
\begin{array}{l}
x_{20}^{(j)} \oplus x_0^{(j)}= C_1^{(j)} \\
x_{21}^{(j)} \oplus x_1^{(j)}= C_2^{(j)} \\
x_{22}^{(j)} \oplus x_2^{(j)}= C_3^{(j)} \\
\ldots\ldots\ldots\ldots\ldots\ldots \\
x_{20+i}^{(j)} \oplus x_i^{(j)}= C_{i+1}^{(j)}, \text{ when } i<31 \\
\ldots\ldots\ldots\ldots\ldots\ldots \\
x_{30}^{(j)} \oplus x_{10}^{(j)}= C_{11}^{(j)} \\
x_0^{(j)}\oplus x_{10}^{(j)}\oplus x_{11}^{(j)}= C_{12}^{(j)} \oplus\delta_{31}^{p}(j)\oplus\xi_{31}\cdot(\delta_{31}^{x} (j)\oplus p^{(j)}) \\
x_1^{(j)}\oplus x_{11}^{(j)}\oplus x_{12}^{(j)}= C_{13}^{(j)} \oplus\delta_{32}^{p}(j) \oplus\xi_{32}\cdot(\delta_{32}^{X}(j)\oplus p^{(j)}) \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
x_{i-31}^{(j)}\oplus x_{i-21}^{(j)}\oplus x_{i-20}^{(j)}= C_{i+1}^{(j)} \oplus\delta_i^{p}(j)\oplus\xi_i\cdot(\delta_i^{X} (j)\oplus p^{(j)}), \text{ when } 30<i<51 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
x_{19}^{(j)}\oplus x_{29}^{(j)}\oplus x_{30}^{(j)}= C_{51}^{(j)} \oplus\delta_{50}^{p}(j)\oplus\xi_{50}\cdot(\delta_{50}^{X}(j)\oplus p^{(j)})
\end{array}
\qquad (12)
$$

The proof is followed from proposition 4, proposition 5, remark 1 and remark 2.

Attack on Vesta-2M without π.

The method of recovering of a key consists of the following stages.
For these values we do.

1. Guess $\{x_0^{(7)}, x_0^{(6)},\ldots, x_0^{(0)}\}$, $\{x_1^{(7)}, x_1^{(6)},\ldots, x_1^{(0)}\},\ldots,$ $\{x_{30}^{(7)}, x_{30}^{(6)},\ldots, x_{30}^{(0)}\}$.
2. Guess V_0, W_0.
3. Guess $\xi_{31}, \xi_{32},\ldots, \xi_{50}$.

Let j=8.

a) Using proposition 1, we determine$\{ U_i^{(1)}\}$, i=1…52.
b) Using proposition 4, remark 1 and remark 2 we determine $\{C_i^{(j)}\}$ and $\{\delta_i^{x} (j)\}$ i=1..52.
c) $\{x_{30}^{(j)},\ldots, x_0^{(j)}\}$ are determined from (12).
d) If j<15 then j=j+1.
e) We execute untwisting of the cryptosystem on necessary length of an output sequence for exclusion of false variants of the key.

Let us estimate the complexity of the method.
In the describing attack we guess $X_0 \pmod{2^8}$, $X_1 \pmod{2^8},\ldots,$ $X_{30} \pmod{2^8}$ and V_0, U_0, W_0.
We may assume that the probability distributions of V_0, U_0, W_0, $X_1 \pmod{2^8}$, …, $W_{30} \pmod{2^8}$ are uniform.
Therefore,
$P\{V_0=V_0^{(cor)},\ W_0=W_0^{(cor)},\ U_0=U_0^{(cor)},\ \{\xi_{31},\ \xi_{32},\ldots,\ \xi_{50}\},\ \{x_0^{(7)},\ldots,x_0^{(0)}\}=\ X_0^{(cor)} \pmod{2^8},\ \ldots,$ $\{x_{30}^{(7)},\ldots,x_{30}^{(0)}\}= X_{30}^{(cor)} \pmod{2^8}\}= 1/2^{16\cdot 3}\cdot 1/2^{p'\cdot 31}\cdot 1/2^{20} \approx 1/2^{276}$.
Thus, the complexity of this attack is approximately 2^{276}. Note that the complexity of the brute force attack is equal to 2^{543}.

4 A Known Plaintext Attack on the Vesta-2M Stream Cipher

In this section we describe the method of recovering of a key of full Vesta-2M. The attack is based on following propositions.

Proposition 6
If we know W_i (mod 2^9) and W_{i+1} (mod 2^9), then we can determine X_{i+20}(mod 2^8).
Proof.
Really, from (3) we obtain $W_{i+1}= \pi(W_i)+X_{i+20}$ (mod 2^{16}).
Then $W_{i+1}= \pi(W_i)+X_{i+20}$ (mod 2^8). Therefore,

$$X_{i+20}(\text{mod } 2^8)=W_{i+1}-\pi(W_i) \ (\text{mod } 2^8).$$

Proposition 7
If we know W_0(mod 2^9), W_1(mod 2^9),…, W_{31}(mod 2^9) and the bits ξ_{31}, ξ_{32},…, ξ_{50}, then we can determine X_0(mod 2^8), X_1(mod 2^8) ,…, X_{30}(mod 2^8).
Proof.
Really, from proposition 6 we get X_{20}(mod 2^8), X_{21}(mod 2^8).., X_{30}(mod 2^8), X_{31}(mod 2^8), X_{32}(mod 2^8), … X_{50}(mod 2^8).
Note that $X_{i+31}= X_i- X_{i+10}+p\cdot\xi_{i+31}$, then X_{i+31}(mod 2^8)=($X_i- X_{i+10}+p\cdot\xi_{i+31}$)(mod 2^8).
Therefore,
(X_i) (mod 2^8)=$X_{i+31}+X_{i+10}$ -$p\cdot\xi_{i+31}$ (mod 2^8).
This means that
$x_i^{(j)} = x_{i+31}^{(j)} \oplus x_{i+10}^{(j)} \oplus \delta_{i+31}^{p}(j) \oplus \xi_{i+31}\cdot(\delta_{i+31}^{x}(j) \oplus p^{(j)})$, where j=0…8.
We obtain
(X_{19}) (mod 2^8)=$X_{29}+X_{50}$ -$p\cdot\xi_{50}$ (mod 2^8)
(X_{18}) (mod 2^8)=$X_{28}+X_{49}$ -$p\cdot\xi_{49}$ (mod 2^8)
(X_{17}) (mod 2^8)=$X_{27}+X_{48}$ -$p\cdot\xi_{48}$ (mod 2^8)
(X_{16}) (mod 2^8)=$X_{26}+X_{47}$ -$p\cdot\xi_{47}$ (mod 2^8)
(X_{15}) (mod 2^8)=$X_{25}+X_{46}$ -$p\cdot\xi_{46}$ (mod 2^8)
(X_{14}) (mod 2^8)=$X_{24}+X_{45}$ -$p\cdot\xi_{45}$ (mod 2^8)
(X_{13}) (mod 2^8)=$X_{23}+X_{44}$ -$p\cdot\xi_{44}$ (mod 2^8)
(X_{12}) (mod 2^8)=$X_{22}+X_{43}$ -$p\cdot\xi_{43}$ (mod 2^8)
……………………………………………
(X_3) (mod 2^8)=$X_{13}+X_{34}$ -$p\cdot\xi_{34}$ (mod 2^8)
(X_2) (mod 2^8)=$X_{12}+X_{33}$ -$p\cdot\xi_{33}$ (mod 2^8)
(X_1) (mod 2^8)=$X_{11}+X_{32}$ -$p\cdot\xi_{32}$ (mod 2^8)
(X_0) (mod 2^8)=$X_{10}+X_{31}$ -$p\cdot\xi_{31}$ (mod 2^8)

Consequently, we determine X_0(mod 2^8), X_1(mod 2^8) ,…, X_{30}(mod 2^8).

Proposition 8
If we know X_0(mod 2^8), X_1(mod 2^8), X_2(mod 2^8),.., X_{30}(mod 2^8), V_0(mod 2^8), U_0(mod 2^8) and W_0(mod 2^9), W_1(mod 2^9),…, W_{31}(mod 2^9), then we can determine by

$$U_{i-1}^{(1)}= \gamma_i-U_i^{(0)} \ (\text{mod } 2^8),$$

where i=1...31.

Proof.
Note that we know X_0(mod 2^8), X_1(mod 2^8), X_2(mod 2^8),.., X_{30}(mod 2^8), V_0(mod 2^8), W_0(mod 2^8).
From (3), (4) and (5) we get

$$W_{i+1}= \pi(W_i)+X_{i+20} \text{ (mod } 2^8)$$
$$V_{i+1}= V_i+X_i \text{ (mod } 2^8)= (V_0+ X_0+X_1+\ldots.+ X_{i-1}+X_i \text{ (mod } 2^8))$$
$$U_i^{(0)} =(W_i \bmod 2^8)\oplus V_i(\text{mod } 2^8)$$

From (8) we obtain

$$U_{i-1}^{(1)}= \gamma_i-U_i^{(0)} \text{ (mod } 2^8),$$

where i=1...31.

Proposition 9
If we know X_0(mod 2^j), X_1(mod 2^j), X_2(mod 2^j),.., X_{30}(mod 2^j), V_0(mod 2^j), U_0(mod 2^j) and W_0(mod 2^j), W_1(mod 2^j),…, W_{31}(mod 2^j), then we can determine W_0(mod 2^{j+1}), W_1(mod 2^{j+1}) , …, W_{30}(mod 2^{j+1}).
Proof.
Really, from

$$w_{i+1}^{(j)} =w_i^{(j+1)} \oplus x_{i+20}^{(j)}\oplus \delta_{i+1}^{w}(j).$$

we get

$$w_i^{(j+1)} = w_{i+1}^{(j)} \oplus x_{i+20}^{(j)}\oplus \delta_{i+1}^{w}(j),$$

where i=0..29.

Proposition 10
If we know X_0(mod 2^j), X_1(mod 2^j), X_2(mod 2^j),.., X_{30}(mod 2^j) and U_0(mod 2^j) W_0(mod 2^{j+1}), W_1(mod 2^{j+1}),…,W_{31}(mod 2^{j+1}), V_0(mod 2^{j+1}), then we can determine X_0(mod 2^{j+1}), X_1(mod 2^{j+1}),…, X_{30}(mod 2^{j+1}).
Proof.
Note that from proposition 8 we get $u_i^{(j+1)} = v_i^{(j+1)} \oplus w_i^{(j+1)}$ then $v_i^{(j+1)} = u_i^{(j+1)} \oplus w_i^{(j+1)}$.
From
$v_i^{(j+1)} = v_{i-1}^{(j+1)} \oplus x_{i-1}^{(j+1)}\oplus\delta_i^{v} (j+1)=(v_0^{(j+1)} \oplus x_0^{(j+1)}\oplus x_1^{(j+1)} \oplus x_2^{(j+1)} \oplus\ldots.\oplus x_{i-1}^{(j+1)}\oplus\delta_1^{v} (j+1)\oplus \delta_2^{v} (j+1)\ldots \oplus\delta_{i-1}^{v} (j+1) \oplus\delta_i^{v} (j+1))$
we obtain
$X_0^{(j+1)} = v_0^{(j+1)} \oplus v_1^{(j+1)} \oplus\delta_1^{v} (j+1)$
$X_1^{(j+1)} = v_1^{(j+1)} \oplus v_2^{(j+1)} \oplus\delta_2^{v} (j+1)$
$X_2^{(j+1)} = v_2^{(j+1)} \oplus v_3^{(j+1)} \oplus\delta_3^{v} (j+1)$
…………………………………
$x_{i-1}^{(j+1)} = v_{i-1}^{(j+1)} \oplus v_i^{(j+1)} \oplus\delta_i^{v} (j+1)$
………………………………….
$X_{29}^{(j+1)} = v_{29}^{(j+1)} \oplus v_{30}^{(j+1)} \oplus\delta_{30}^{v} (j+1)$
$X_{30}^{(j+1)} = v_{30}^{(j+1)} \oplus v_{31}^{(j+1)} \oplus\delta_{31}^{v} (j+1)$
Therefore, we determine X_0(mod 2^{j+1}), X_1(mod 2^{j+1}),…, X_{30}(mod 2^{j+1}).

Attack on Vesta-2M

The method of recovering of the key consists of the following stages.

1. We guess W_0 (mod 2^9), W_1(mod 2^9),…,W_{30}(mod 2^9).
2. We guess V_0, U_0, W_{31}.
3. We guess ξ_{31}, ξ_{32},…, ξ_{50}.

For these values we do.

a) Using proposition 7, we calculate X_0(mod 2^8), X_1(mod 2^8) ,…, X_{30}(mod 2^8)
b) Using proposition 8, we calculate { $U_i^{(1)}$}, where i=1..31.
   Let j=9.
c) Using proposition 9, we determine values of the bits {$w_{30}^{(j+1)}$,…, $w_0^{(j+1)}$}.
d) Using proposition 10, we determine values of the bits {$x_{30}^{(j+1)}$,…, $x_0^{(j+1)}$}.
e) If j<15 then j=j+1.
f) We execute untwisting of the cryptosystem on necessary length of an output sequence for exclusion of false variants of the key.

Let us estimate the complexity of the method.
In the describing attack we guess W_0 (mod 2^9), W_1(mod 2^9),…, W_{30}(mod 2^9) and V_0, U_0, W_{31}.
We may assume that the probability distributions of V_0, U_0, W_{31}, W_1(mod 2^9), …, W_{30}(mod 2^9) are uniform.
Therefore,
$P\{V_0=V_0^{(cor)},\ W_{31}=W_{31}^{(cor)},\ U_0=U_0^{(cor)},\ \{\xi_{31}, \xi_{32},\dots, \xi_{50}\}, \{w_0^{(8)},\dots, w_0^{(0)}\}= W_0^{(cor)}(\mathrm{mod}\ 2^9), \dots, \{w_{30}^{(8)},\dots,w_{30}^{(0)}\}= W_{30}^{(cor)}(\mathrm{mod}\ 2^9)\ \} = 1/2^{16\cdot 2+8}\cdot 1/2^{9\cdot 31}\cdot 1/2^{20}\approx 1/2^{339}$.
Thus, the complexity of this attack is approximately 2^{338}. Note that the complexity of the brute force attack is equal to 2^{543}.

5 Conclusion

We have demonstrated several cryptanalytic algorithms on the Vesta-2M stream cipher. The algorithms try to deduce the initial state in a known plaintext attack. The algorithms find the correct initial state using only a small segment of known plaintext. We demonstrated the importance of the permutation π in Vesta-2M and described the attack based on linear approximations.

The complexities of the attacks were approximated to be less than time of searching through the square root of all possible initial states. However, Vesta-2M remains a secure cipher for practical applications.

References

[1] OCT 51-06-98 An algorithm of encoding of data.

[2] OCT 51-08-98 An algorithm of forming the identifier of access to data.

[3] http:\\www.lancrypto.com\main.html

[4] Schneier B., Applied Cryptography .Second edition, 1996.

[5] Rueppel R.A. “Analysis and Design of Stream Ciphers” Springer-Verlag Communications and Control Engineering Series, 1986.

[6] Varfolomeev A.A., Zhukov A.E., Pudovkina M., "Analysis of Stream Ciphers ", Moscow, 2000.