A known plaintext attack on the ISAAC keystream generator

Marina Pudovkina

maripa@online.ru

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

Abstract. Stream ciphers are often used in applications where high speed and low delay are a requirement. The ISAAC keystream generator is a fast software-oriented encryption algorithm. In this papers the security of the ISAAC keystream generator is investigated. Cryptanalytic algorithm is developed for a known plaintext attack where only a small segment of plaintext is assumed to be known.

Keywords. ISAAC. Keystream generator. Cryptanalysis.

1 Introduction

Stream ciphers are an important class of encryption algorithms. They encrypt individual characters of a plaintext message one at a time, using an encryption transformation, which varies with time. By contrast, block ciphers tend to simultaneously encrypt groups of characters of a plaintext message using a fixed encryption transformation. Stream ciphers are generally faster than block ciphers in hardware, and have less complex hardware circuitry.

There is a vast body of theoretical knowledge on stream ciphers, and various design principles for stream ciphers have been proposed and extensively analyzed. The most of stream ciphers proposed in open literature are based on LFSRs (linear feedback shift registers).

For software implementation, a few keystream generators have been designed which are not based on shift registers. One of these generators is ISAAC. The ISAAC (Indirection, Shift, Accumulate, Add, and Count) keystream generator was introduced in [1] by R. Jenkins as a fast software-oriented encryption algorithm.

The aim of this paper is to derive some cryptanalytic algorithm that find the correct initial state of the ISAAC stream cipher using only a small segment of output stream, and to give precise estimates for the complexity of the attack. Our results are intrinsic to the design principles of ISAAC and are independent of the size of the key.

The paper is organized as follows. In section 2 we give a general description of ISAAC. In section 3 we discuss some properties of ISAAC. Section 4 describes attack on ISAAC. We conclude in section 5.

2 Description of ISAAC

ISAAC is in fact a family of algorithms indexed by parameter m, which is a positive integer. The internal state of ISAAC at time t consists of a table $S_t = \{s_t[0],\ldots,s_t[m-1]\}$ of $m=2^n$ K-bit words and of two K-bit words a_t and i_t. Let z_t denote the output K-bit word of ISAAC at time t. Let initially $i_0 = a_0 = 0$. $K=2n+\Delta$, $\Delta>0$. The key of ISAAC is the initial table S_0.

Jenkins takes m=256, n=8, K=32, p0=13, p1=6, p2=2, p3=16, $\theta_1=\theta_2=2$.
Let $\theta_1,\theta_2<n$.

$$G(a_{t-1}, t, p(t))= \begin{cases} ((a_{t-1}<<p0) \oplus a_{t-1}) & \text{if } t=0 \pmod 4. \\ ((a_{t-1}>>p1) \oplus a_{t-1}) & \text{if } t=1 \pmod 4. \\ ((a_{t-1}<<p2) \oplus a_{t-1}) & \text{if } t=2 \pmod 4. \\ ((a_{t-1}>>p3) \oplus a_{t-1}) & \text{if } t=3 \pmod 4. \end{cases}$$

where >> and << indicate rotation to the right and left, and

$$p(t)= \begin{cases} p0 & \text{if } t=0 \pmod 4. \\ p1 & \text{if } t=1 \pmod 4. \\ p2 & \text{if } t=2 \pmod 4. \\ p3 & \text{if } t=3 \pmod 4. \end{cases}$$

The next-state function F
a) $i_t= i_{t-1}+1 \pmod m$.
b) $a_t= (G(a_{t-1}, t, p(t))+ s_t[(t+ m/2)(\text{mod } m)]) \pmod{2^K}$.
c) $s_t[i_t]= (s_{t-1}[(s_{t-1}[i_t]>>\theta_1) \pmod m]+a_t+ z_{t-1}) \pmod{2^K}$.

The output function f
Output: $z_t=(s_t[(s_t[i_t]>>(n+\theta_2))(\text{mod } m)]+s_{t-1}[i_t]) \pmod{2^K}$.

3 Properties of ISAAC

In this section we describe some properties of ISAAC that are used in the description of our attack. We will assume that the output sequence $z_1, z_2,\ldots, z_{m+1}$ is known.
Let $a_t=(a_{t,K-1}, a_{t,K-2},\ldots,a_{t,i},\ldots, a_{t,1}, a_{t,0})$ be a binary representation of $a_t \in \boldsymbol{Z_K}$, $\{a_{t,j}\} \in \boldsymbol{Z_2}$.

Proposition 1
1. The transformation
$F_{<<}(a,p)=((a<<p) \oplus a)= (a_{K-1}\oplus a_{K-p-1}, a_{K-2}\oplus a_{K-p-2},\ldots, a_{p+i} \oplus a_i,\ldots, a_p\oplus a_0, a_{p-1} , a_{p-2},\ldots, a_1, a_0)$.
2. The transformation
$F_{>>}(a,p)=((a>>p) \oplus a)=(a_{K-1} , a_{K-2},\ldots, a_p, a_{K-1}\oplus a_{K-p-1}, a_{K-2}\oplus a_{K-p-2},\ldots, a_{p+i} \oplus a_i,\ldots, a_p\oplus a_0)$.
Proof
Note that

$$(a<<p)= (a_{K-p-1}, a_{K-p-2},\ldots,a_i,\ldots, a_1, a_0,0,\ldots,0).$$

Thus,
$F_{<<}(a,p)=((a<<p)\oplus a)= (a_{K-1}\oplus a_{K-p-1}, a_{K-2}\oplus a_{K-p-2},\ldots, a_{p+i} \oplus a_i,\ldots, a_p\oplus a_0, a_{p-1} , a_{p-2},\ldots, a_1, a_0)$.
Note that $(a>>p)= (0,\ldots, 0, a_{K-1}, a_{K-2},\ldots, a_{p+1}, a_p)$.
Therefore,
$F_{>>}(a,p)=((a>>p)\oplus a)= (a_{K-1} , a_{K-2},\ldots, a_p, a_{K-1}\oplus a_{K-p-1}, a_{K-2}\oplus a_{K-p-2},\ldots, a_{p+i} \oplus a_i,\ldots, a_p\oplus a_0)$
The proposition is proved.

Denote by $q_t=s_t[s_t[i_t] >>(n+\theta_2) \pmod m]) \pmod m$ and $\alpha_t= (s_{t-1}[t]>> \theta_1) \pmod m$, t=1,2…..

In propositions given below we will assume that j_t, α_t are known.

Proposition 2
If we know $s_m[0] \pmod{2^\beta}$, $s_1[1] \pmod{2^\beta}$,…, $s_{m-1}[m-1] \pmod{2^\beta}$ and $z_1, z_2, \ldots, z_{m+1}$, then $s_0[0] \pmod{2^\beta}$, $s_0[1] \pmod{2^\beta}$,…, $s_0[m-1] \pmod{2^\beta}$, can be found for t=m, m-1, m-2,…, 2, 1 as follows.
If j_t=0, m-1,…,t+1, then

$$s_0[t](\mathrm{mod}\ 2^\beta) = (z_t(\mathrm{mod}\ 2^\beta) - s_0[j_t](\mathrm{mod}\ 2^\beta))(\mathrm{mod}\ 2^\beta).$$

If $0<j_t<t+1$, then

$$s_0[t](\mathrm{mod}\ 2^\beta) = (z_t(\mathrm{mod}\ 2^\beta) - s_{j_t}[j_t](\mathrm{mod}\ 2^\beta))(\mathrm{mod}\ 2^\beta),$$

Proof.
Note that

$$z_t(\mathrm{mod}\ 2^\beta)=(s_t[j_t] \pmod{2^\beta}+s_{t-1}[i_t] \pmod{2^\beta}) \pmod{2^\beta},$$
$$(s_m[j_m] \pmod{2^\beta}+ s_0[0] \pmod{2^\beta}) \pmod{2^\beta}= z_m(\mathrm{mod}\ 2^\beta),$$

and

$$s_m[j_m] = s_{j_m}[j_m].$$

Then

$$s_0[0](\mathrm{mod}\ 2^\beta) = (z_m(\mathrm{mod}\ 2^\beta) - s_{j_m}[j_m](\mathrm{mod}\ 2^\beta))(\mathrm{mod}\ 2^\beta).$$

Let us consider t=m-1. If j_m=0 (mod m), then we get

$$s_0[m-1](\mathrm{mod}\ 2^\beta) = (z_{m-1}(\mathrm{mod}\ 2^\beta) - s_0[0](\mathrm{mod}\ 2^\beta))(\mathrm{mod}\ 2^\beta).$$

If $0<j_{m-1}<m$, then

$$s_0[m-1](\mathrm{mod}\ 2^\beta) = (z_{m-1}(\mathrm{mod}\ 2^\beta) - s_{j_{m-1}}[j_{m-1}](\mathrm{mod}\ 2^\beta))(\mathrm{mod}\ 2^\beta).$$

Now we consider t=m-2…1. Assume that $s_0[0] \pmod{2^\beta}$, $s_0[m-1] \pmod{2^\beta}$,…, $s_0[t+1] \pmod{2^\beta}$ have been determined. Then for j_m=0, m-1,…,t+1 we have

$$s_0[t](\mathrm{mod}\ 2^\beta) = (z_t(\mathrm{mod}\ 2^\beta) - s_0[j_t](\mathrm{mod}\ 2^\beta))(\mathrm{mod}\ 2^\beta).$$

If $0<j_t<t+1$, then we obtain

$$s_0[t](\mathrm{mod}\ 2^\beta) = (z_t(\mathrm{mod}\ 2^\beta) - s_{j_t}[j_t](\mathrm{mod}\ 2^\beta))(\mathrm{mod}\ 2^\beta).$$

The proposition is proved.

Proposition 3
If we know $s_m[0](\mathrm{mod}\ 2^\beta)$, $s_1[1](\mathrm{mod}\ 2^\beta)$,…,$s_{m-1}[m-1](\mathrm{mod}\ 2^\beta)$ and $z_1, z_2, \ldots, z_{m+1}$, then $a_1(\mathrm{mod}\ 2^\beta)$, $a_2(\mathrm{mod}\ 2^\beta)$,…., $a_{m+1}(\mathrm{mod}\ 2^\beta)$, can be found as follows.
If $j_t>t$, then

$$a_t(\mathrm{mod}\ 2^\beta)=(s_t[t] \pmod{2^\beta}- s_0[\alpha_t](\mathrm{mod}\ 2^\beta) - z_{t-1} \pmod{2^\beta}) \pmod{2^\beta}.$$

If $t \geq j_t$, then

$$a_t(\mathrm{mod}\ 2^\beta) = (s_t[t](\mathrm{mod}\ 2^\beta) - s_{\alpha_t}[\alpha_t](\mathrm{mod}\ 2^\beta) - z_{t-1}(\mathrm{mod}\ 2^\beta))(\mathrm{mod}2^\beta),$$

where t=1…m+1.
Proof.
Note that for t=1, 2, …. we have

$$s_t[i_t]= s_{t-1}[\alpha_t]+a_t+z_{t-1} \pmod{2^K}.$$

Whence,

$$a_t(\mathrm{mod}\ 2^\beta)=(s_t[i_t] \pmod{2^\beta}- s_{t-1}[\alpha_t](\mathrm{mod}\ 2^\beta) - z_{t-1} \pmod{2^\beta}) \pmod{2^\beta}.$$

Using proposition 2 we can find $s_0[0] \pmod{2^\beta}$, $s_0[1] \pmod{2^\beta}$,…, $s_0[m-1] \pmod{2^\beta}$.
Let us remark that for any t, d if d>t, then $s_t[d]= s_0[d]$ and if t≥d, then $s_t[d]= s_d[d]$.
This implies that if α_t>t, then we get

$$a_t \pmod{2^\beta} = (s_t[t] \pmod{2^\beta} - s_0[\alpha_t] \pmod{2^\beta} - z_{t-1} \pmod{2^\beta}) \pmod{2^\beta},$$

if t≥α_t, then

$$a_t \pmod{2^\beta} = (s_t[t] \pmod{2^\beta} - s_{\alpha_t}[\alpha_t] \pmod{2^\beta} - z_{t-1} \pmod{2^\beta}) \pmod{2^\beta}.$$

The proposition is proved.

Let q be the smallest number of p1, p3, i.e. q=min(p1, p3).

Proposition 4
Let τ≥2n+θ2. If we know $a_1 \pmod{2^\tau}$, $a_2 \pmod{2^\tau}$,…,$a_i \pmod{2^\tau}$,…,$a_m \pmod{2^\tau}$ è $s_2[2+m/2] \pmod{2^\tau}$, $s_4[4+m/2] \pmod{2^\tau}$,…., $s_{2i}[(m/2+2i) \pmod m] \pmod{2^\tau}$,…,$s_m[m] \pmod{2^\tau}$, then $a_1 \pmod{2^{\tau+q}}$, $a_3 \pmod{2^{\tau+q}}$,…, $a_{2i+1} \pmod{2^{\tau+q}}$,…. $a_{m-1} \pmod{2^{\tau+q}}$ can be determined as follows.

$$a_{t,q-1+\tau} = b_{t+1,\tau-1} \oplus a_{t,\tau-1},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_{t,q+\tau-j} = b_{t+1,\tau-j} \oplus a_{t,\tau-j},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_{t,\tau} = b_{t+1,\tau-q} \oplus a_{t,\tau-q}.$$

where t=1 (mod 2), $b_{t+1}=(a_{t+1} \pmod{2^\tau} - s_{t+1}[t+1+m/2] \pmod{2^\tau}) \pmod{2^\tau}$.
Proof.
By proposition 1
$F_{>>}(a,p)=((a>>p) \oplus a)=(a_{K-1}, a_{K-2},\ldots, a_p, a_{K-1} \oplus a_{K-p-1}, a_{K-2} \oplus a_{K-p-2},\ldots, a_{p+i} \oplus a_i,\ldots, a_p \oplus a_0)$.
From

$$a_t \pmod{2^\tau} = (F_{<<}(a_{t-1},p(t)) \pmod{2^\tau} + s_t[t+m/2] \pmod{2^\tau}) \pmod{2^\tau},$$

where t=0 (mod 2), it follows that

$$F_{>>}(a_{t-1},p(t)) \pmod{2^\tau} = b_t = (a_t \pmod{2^\tau} - s_t[t+m/2] \pmod{2^\tau}) \pmod{2^\tau}.$$

Hence,

$$b_{t,\tau-1} = a_{t-1,p(t)-1+\tau} \oplus a_{t-1,\tau-1}, \ldots, b_{t,\tau-p(t)} = a_{t-1,\tau} \oplus a_{t-1,\tau-p(t)}.$$

Thus, we have found unknown p(t) bits

$$a_{t-1,p(t)-1+\tau} = b_{t,\tau-1} \oplus a_{t-1,\tau-1},$$
$$\ldots\ldots$$
$$a_{t-1,\tau} = b_{t,\tau-p(t)} \oplus a_{t-1,\tau-p(t)}.$$

Therefore, we have computed $a_1 \pmod{2^{\tau+p1}}$, $a_3 \pmod{2^{\tau+p3}}$,…, $a_{4i+1} \pmod{2^{\tau+p1}}$, $a_{4i+3} \pmod{2^{\tau+p3}}$,…,$a_{m-1} \pmod{2^{\tau+p3}}$. This shows that $a_1 \pmod{2^{\tau+q}}$,…, $a_{2i+1} \pmod{2^{\tau+q}}$,…. $a_{m-1} \pmod{2^{\tau+q}}$ are found.
The proposition is proved.

Let $\sigma_t^a(j)$ be a carry bit in j^{th}-bit of the sum $(G(a_{t-1}, t, p(t)) + s_t[(t+m/2) \pmod m]) \pmod{2^K}$, $\sigma_t^z(j)$ be a carry bit in j^{th}-bit of the sum $(s_t[(s_t[t]>>(n+\theta_2)) \pmod m] + s_{t-1}[t]) \pmod{2^K}$ and $\sigma_t^s(j)$ be a carry bit in j^{th}-bit of the sum $(s_{t-1}[(s_{t-1}[t]>>\theta_1) \pmod m] + a_t + z_{t-1}) \pmod{2^K}$.

Let

$$\delta(t,k)=\begin{cases}0 & \text{if } t>k\\ t & \text{if } t\le k\end{cases}$$

and

$$\rho(t,k)=\begin{cases}0 & \text{if } t>k\\ 1 & \text{if } t\le k\end{cases}.$$

Proposition 5

If $j<p(t)$, then

$$a_{2i+1,j}=a_{2i,j}\oplus s_{\delta(2i+1,2i+1+m/2),j}[2i+1+m/2]\oplus \sigma_{2i^{a}+1}(j).$$

If $j\ge p(t)$, then

$$a_{2i+1,j}=a_{2i,j}\oplus a_{2i,j-p(2i+1)}\oplus s_{\delta(2i+1,2i+1+m/2),j}[2i+1+m/2]\oplus \sigma_{2i^{a}+1}(j).$$

This proposition can easily be proved if note that

$$a_t(\mathrm{mod}\ 2^j)=(G(a_{t-1},t,p(t))\ (\mathrm{mod}\ 2^j)+s_t[(t+m/2)(\mathrm{mod}\ m)]\ (\mathrm{mod}\ 2^j))\ (\mathrm{mod}\ 2^j)$$

and j^{th}-bit of $G(a_{2i},t,p(2i+1))$ is

$$G(a_{2i},t,p(2i+1))_j=\begin{cases}a_{2i,j} & \text{if } j<p(t),\\ a_{2i,j}\oplus a_{2i,j-p(2i+1)} & \text{if } j\ge p(t).\end{cases}$$

Proposition 6

If we know $s_t[t]\ (\mathrm{mod}\ 2^{j-1})$, $s_0[t]\ (\mathrm{mod}\ 2^{j-1})$, α_t, $j_t(\mathrm{mod}\ 2^{j-1})$, $z_{t-1}(\mathrm{mod}\ 2^{j-1})$, $a_{t-1}(\mathrm{mod}\ 2^{j-1})$, then $\sigma_t^{s}(j)$, $\sigma_t^{z}(j)$ and $\sigma_{2i^{a}+1}(j)$ can be computed as follows.

$$\sigma_t^{s}(j)=\begin{cases}1 & \text{if } (s_{\delta(t,\acute{a}_t)}[\alpha_t](\mathrm{mod}\ 2^{j-1})+z_{t-1}(\mathrm{mod}\ 2^{j-1})+a_{t,j-1}(\mathrm{mod}\ 2^{j-1}))\ (\mathrm{mod}\ 2^{j+1})\ge 2^j,\\ 0 & \text{otherwise.}\end{cases}$$

$$\sigma_t^{z}(j)=\begin{cases}1 & \text{if } (s_{\delta(t,j_t),j-1}[j_t]\ (\mathrm{mod}\ 2^{j-1})+s_{0,j-1}[t]\ (\mathrm{mod}\ 2^{j-1}))\ (\mathrm{mod}\ 2^{j+1})\ge 2^j,\\ 0 & \text{otherwise.}\end{cases}$$

If $j<p(t)$ and $t=1\ (\mathrm{mod}\ 2)$, then

$$\sigma_{2i^{a}+1}(j)=\begin{cases}1 & \text{if } (a_{2i}(\mathrm{mod}\ 2^{j-1})+s_{2i+1}[2i+1+m/2](\mathrm{mod}\ 2^{j-1}))\ (\mathrm{mod}\ 2^{j+1})\ge 2^j,\\ 0 & \text{otherwise.}\end{cases}$$

If $j\ge p(t)$ and $t=1\ (\mathrm{mod}\ 2)$, then

$$\sigma_t^{a}(j)=\begin{cases}1, & \text{if } \sum_{k=p(t)}^{j-1}(a_{t-1,k}\oplus a_{t-1-p(t),k})\cdot 2^k+a_{t-1}(\mathrm{mod}\ 2^{p(t)-1})+s_{\delta(t,t+m/2),j}[t+m/2]\ (\mathrm{mod}\ 2^{j-1}))\ (\mathrm{mod}\ 2^{j+1})\ge 2^j\\ 0, & \text{otherwise.}\end{cases}$$

Proof.

Note that $\sigma_t^{s}(j)$, $\sigma_t^{a}(j)$ and $\sigma_t^{z}(j)$ are equal to 1 if and only if $(G(a_{t-1},t,p(t))+s_t[(t+m/2)(\mathrm{mod}\ m)])\ (\mathrm{mod}\ 2^{j+1})\ge 2^j$, $(s_t[(s_t[t]>>(n+\theta_2))(\mathrm{mod}\ m)]+s_{t-1}[t])\ (\mathrm{mod}\ 2^{j+1})\ge 2^j$, $(s_{t-1}[(s_{t-1}[t]>>\theta_1)\ (\mathrm{mod}\ m)]+a_t+z_{t-1})\ (\mathrm{mod}\ 2^{j+1})\ge 2^j$.

Thus,

$$\sigma_t^{a}(j)=\begin{cases}1 & \text{if } (G(a_{t-1},t,p(t))\ (\mathrm{mod}\ 2^{j-1})+s_t[t+m/2](\mathrm{mod}\ 2^{j-1}))\ (\mathrm{mod}\ 2^{j+1})\ge 2^j,\\ 0 & \text{otherwise.}\end{cases}$$

and

$$G(a_{t-1}, t, p(t)) \pmod{2^{j-1}} = \begin{cases} a_{2i} \pmod{2^{j-1}} & \text{if } j<p(t), \\ \sum_{k=p(t)}^{j-1} (a_{t-1,k} \oplus a_{t-1-p(t),k}) \cdot 2^k + a_{t-1} \pmod{2^{p(t)-1}} & \text{otherwise.} \end{cases}$$

By the above notes we obtain the proof of the proposition.

Theorem 1

If we know α_t, j_t, $a_{2i+1} \pmod{2^j}$, $a_{2i} \pmod{2^{j-1}}$, $\sigma_t^s(j)$, $\sigma_t^a(j)$, $\sigma_t^z(j)$, $z_{t,j}$, $t=1,\ldots,m$, $i=0\ldots m/2-1$ and $j \geq \max(p(1), p(3))$, then $s_{t,j}[t]$, $s_{0,j}[t]$, $t=1,\ldots,m$, can be found by solving the following system of equations.

$$s_{0,j}[0] \oplus s_{\delta(m, j_m),j}[j_m] = z_{m,j} \oplus \sigma_m^z(j),$$
$$s_{0,j}[1] \oplus s_{\delta(1, j_1),j}[j_1] = z_{1,j} \oplus \sigma_1^z(j),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s_{0,j}[t] \oplus s_{\delta(t, j_t),j}[j_t] = z_{t,j} \oplus \sigma_t^z(j),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s_{0,j}[1+m/2] = a_{1,j} \oplus \sigma_1^a(j),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s_{0,j}[t] \oplus s_{\delta(t, j_t),j}[j_t] = z_{t,j} \oplus \sigma_t^z(j),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s_{0,j}[m-1] \oplus s_{\delta(m-1, j_{m-1}),j}[j_{m-1}] = z_{m-1,j} \oplus \sigma_{m-1}^z(j),$$
$$s_{1,j}[1] \oplus s_{\delta(1, \alpha_1),j}[\alpha_1] = a_{1,j} \oplus \sigma_1^s(j),$$
$$s_{2,j}[2] \oplus s_{\delta(2, \alpha_2),j}[\alpha_2] \oplus s_{0,j}[3+m/2] = z_{1,j} \oplus a_{3,j} \oplus a_{2,j-p(3)} \oplus \sigma_3^a(j) \oplus \sigma_2^s(j),$$
$$s_{3,j}[3] \oplus s_{\delta(3, \alpha_3),j}[\alpha_3] = z_{2,j} \oplus a_{3,j} \oplus \sigma_3^s(j),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$
$$s_{2i,j}[2i] \oplus s_{\delta(2i+1,2i+1+m/2),j}[2i+1+m/2] \oplus s_{\delta(2i, \alpha_{2i}),j}[\alpha_{2i}] = z_{2i-1,j} \oplus a_{2i+1,j} \oplus a_{2i,j-p(2i+1)} \oplus \sigma_{2i+1}^a(j) \oplus \sigma_{2i}^s(j),$$
$$s_{2i+1,j}[2i+1] \oplus s_{\delta(2i+1, \alpha_{2i+1}),j}[\alpha_{2i+1}] = z_{2i,j} \oplus a_{2i+1,j} \oplus \sigma_{2i+1}^s(j),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s_{m-2,j}[m-2] \oplus s_{\delta(m-2, \alpha_{m-2}),j}[\alpha_{m-2}] = z_{m-3,j} \oplus a_{m-2,j} \oplus \sigma_{m-2}^s(j),$$
$$s_{m-1,j}[m-1] \oplus s_{\delta(m-1,m/2-1),j}[m/2-1] \oplus s_{\delta(m-1, \alpha_{m-1}),j}[\alpha_{m-1}] = z_{m,j} \oplus a_{m-1,j} \oplus a_{m-2,j-p(3)} \oplus \sigma_{m-1}^a(j) \oplus \sigma_{m-1}^s(j),$$
$$s_{m,j}[m] \oplus s_{\delta(m, \alpha_m),j}[\alpha_m] = z_{m-1,j} \oplus a_{m,j} \oplus \sigma_m^s(j).$$

$a_{2i,j}$, $i=0\ldots m/2$ can be found as follows

$$a_{2i,j} = a_{2i+1,j} \oplus a_{2i,j-p(2i+1)} \oplus s_{\delta(2i+1,2i+1+m/2),j}[2i+1+m/2] \oplus \sigma_{2i+1}^a(j).$$

Proof

Consider j^{th}-bit of

$$a_t = (G(a_{t-1}, t, p(t)) + s_t[(t+m/2) \pmod m]) \pmod{2^K}, \quad t=1 \pmod 2$$
$$s_t[t] = (s_{t-1}[\alpha_t] + a_t + z_{t-1}) \pmod{2^K}, \quad t=1\ldots m.$$
$$z_t = (s_t[j_t] + s_0[t]) \pmod{2^K}, \quad t=1\ldots m.$$

Thus, we obtain the following system of equations.

$$a_{1,j} = s_{0,j}[1+m/2] \oplus \sigma_1^a(j),$$
$$s_{1,j}[1] = s_{\delta(1, \alpha_1),j}[\alpha_1] \oplus a_{1,j} \oplus \sigma_1^s(j),$$

$$z_{1,j}= s_{\delta(1,\, j_1),j}[j_1]\oplus s_{0,j}[1]\oplus \sigma_1^{z}(j),$$
$$s_{2,j}[2]= s_{\delta(2,\, \alpha_2),j}[\alpha_2]\oplus z_{1,j}\oplus a_{2,j} \oplus\sigma_2^{s}(j),$$
$$z_{2,j}= s_{\delta(2,\, j_2),j}[j_2]\oplus s_{0,j}[2]\oplus \sigma_2^{z}(j),$$
$$a_{3,j}=a_{2,j}\oplus a_{2,j-p(3)}\oplus s_{0,j}[3+m/2]\oplus\sigma_3^{a}(j),$$
$$s_{3,j}[3]= s_{\delta(3,\, \alpha_3),j}[\alpha_3]\oplus z_{2,j}\oplus a_{3,j} \oplus\sigma_3^{s}(j),$$
$$z_{3,j}= s_{\delta(3,\, j_3),j}[j_3]\oplus s_{0,j}[3]\oplus \sigma_3^{z}(j),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \qquad (2)$$
$$s_{2i,j}[2i]= s_{\delta(2i,\, \alpha_{2i}),j}[\alpha_{2i}]\oplus z_{2i-1,j}\oplus a_{2i,j} \oplus\sigma_{2i}^{s}(j),$$
$$z_{2i,j}= s_{\delta(2i,\, j_{2i}),j}[j_{2i}]\oplus s_{0,j}[2i]\oplus \sigma_{2i}^{z}(j),$$
$$a_{2i+1,j}=a_{2i,j}\oplus a_{2i,j-p(2i+1)}\oplus s_{\delta(2i+1,2i+1+m/2),j}[2i+1+m/2]\oplus\sigma_{2i+1}^{a}(j),$$
$$s_{2i+1,j}[2i+1]= s_{\delta(2i+1,\, \alpha_{2i+1}),j}[\alpha_{2i+1}]\oplus z_{2i,j}\oplus a_{2i+1,j} \oplus\sigma_{2i+1}^{s}(j),$$
$$z_{2i+1,j}= s_{\delta(2i+1,\, j_{2i+1}),j}[j_{2i+1}]\oplus s_{0,j}[2i+1]\oplus \sigma_{2i+1}^{z}(j),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s_{m-2,j}[m-2]= s_{\delta(m-2,\, \alpha_{m-2}),j}[\alpha_{m-2}]\oplus z_{m-3,j}\oplus a_{m-2,j} \oplus\sigma_{m-2}^{s}(j),$$
$$z_{m-2,j}= s_{\delta(m-2,\, j_{m-2}),j}[j_{m-2}]\oplus s_{0,j}[m-2]\oplus \sigma_{m-2}^{z}(j),$$
$$a_{m-1,j}=a_{m-2,j}\oplus a_{m-2,j-p(m-1)}\oplus s_{\delta(m-1,m/2-1),j}[m/2-1]\oplus\sigma_{m-1}^{a}(j),$$
$$s_{m-1,j}[m-1]= s_{\delta(m-1,\, \alpha_{m-1}),j}[\alpha_{m-1}]\oplus z_{m,j}\oplus a_{m-1,j} \oplus\sigma_{m-1}^{s}(j),$$
$$z_{m-1,j}= s_{\delta(m-1,\, j_{m-1}),j}[j_{m-1}]\oplus s_{0,j}[m-1]\oplus \sigma_{m-1}^{z}(j),$$
$$s_{m,j}[m]= s_{\delta(m,\, \alpha_m),j}[\alpha_m]\oplus z_{m-1,j}\oplus a_{m,j} \oplus\sigma_m^{s}(j),$$
$$z_{m,j}= s_{\delta(m,\, j_m),j}[j_m]\oplus s_{0,j}[0]\oplus \sigma_m^{z}(j).$$

Note that $s_{t,j}[t]$, $s_{0,j}[t]$, $a_{2i,j}$, $t=1,\ldots, m$, $i=0\ldots m/2$, are unknown and the number of unknown values in (2) is $5m/2$.

By proposition 6 we have

$$a_{2i,j} = a_{2i+1,j} \oplus a_{2i,j-p(2i+1)}\oplus s_{\delta(2i+1,2i+1+m/2),j}[2i+1+m/2]\oplus\sigma_{2i+1}^{a}(j),$$

where $i=1\ldots m/2-1$. If we replace $a_{2i,j}$ by $a_{2i+1,j} \oplus a_{2i,j-p(2i+1)}\oplus s_{\delta(2i+1,2i+1+m/2),j}[2i+1+m/2]\oplus\sigma_{2i+1}^{a}(j)$ in (2), we get

$$a_{1,j}=s_{0,j}[1+m/2]\oplus\sigma_1^{a}(j),$$
$$s_{1,j}[1]= s_{\delta(1,\, \alpha_1),j}[\alpha_1]\oplus a_{1,j} \oplus\sigma_1^{s}(j),$$
$$z_{1,j}= s_{\delta(1,\, j_1),j}[j_1]\oplus s_{0,j}[1]\oplus \sigma_1^{z}(j),$$
$$s_{2,j}[2]= s_{\delta(2,\, \alpha_2),j}[\alpha_2]\oplus z_{1,j}\oplus a_{3,j} \oplus a_{2,j-p(3)}\oplus s_{0,j}[3+m/2]\oplus\sigma_3^{a}(j) \oplus\sigma_2^{s}(j),$$
$$z_{2,j}= s_{\delta(2,\, j_2),j}[j_2]\oplus s_{0,j}[2]\oplus \sigma_2^{z}(j),$$
$$s_{3,j}[3]= s_{\delta(3,\, \alpha_3),j}[\alpha_3]\oplus z_{2,j}\oplus a_{3,j} \oplus\sigma_3^{s}(j),$$
$$z_{3,j}= s_{\delta(3,\, j_3),j}[j_3]\oplus s_{0,j}[3]\oplus \sigma_3^{z}(j),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \qquad (3)$$
$$s_{2i,j}[2i]= s_{\delta(2i,\, \alpha_{2i}),j}[\alpha_{2i}]\oplus z_{2i-1,j}\oplus a_{2i+1,j} \oplus a_{2i,j-p(2i+1)}\oplus s_{\delta(2i+1,2i+1+m/2),j}[2i+1+m/2]\oplus\sigma_{2i+1}^{a}(j)\oplus\sigma_{2i}^{s}(j),$$
$$z_{2i,j}= s_{\delta(2i,\, j_{2i}),j}[j_{2i}]\oplus s_{0,j}[2i]\oplus \sigma_{2i}^{z}(j),$$
$$s_{2i+1,j}[2i+1]= s_{\delta(2i+1,\, \alpha_{2i+1}),j}[\alpha_{2i+1}]\oplus z_{2i,j}\oplus a_{2i+1,j} \oplus\sigma_{2i+1}^{s}(j),$$
$$z_{2i+1,j}= s_{\delta(2i+1,\, j_{2i+1}),j}[j_{2i+1}]\oplus s_{0,j}[2i+1]\oplus \sigma_{2i+1}^{z}(j),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$s_{m-2,j}[m-2]= s_{\delta(m-2,\,\alpha_{m-2}),j}[\alpha_{m-2}]\oplus z_{m-3,j}\oplus a_{m-2,j}\oplus\sigma_m{}^{s}{}_{-2}(j),$$
$$z_{m-2,j}= s_{\delta(m-2,\,j_{m-2}),j}[j_{m-2}]\oplus s_{0,j}[m-2]\oplus \sigma_m{}^{z}{}_{-2}(j),$$
$$s_{m-1,j}[m-1]= s_{\delta(m-1,\,\alpha_{m-1}),j}[\alpha_{m-1}]\oplus z_{m,j}\oplus a_{m-1,j}\oplus a_{m-2,j\,-\,p(3)}\oplus s_{\delta(m-1,m/2-1),j}[m/2-1]\oplus\sigma_m{}^{a}{}_{-1}(j)\oplus\sigma_m{}^{s}{}_{-1}(j),$$
$$z_{m-1,j}= s_{\delta(m-1,\,j_{m-1}),j}[j_{m-1}]\oplus s_{0,j}[m-1]\oplus \sigma_m{}^{z}{}_{-1}(j),$$
$$s_{m,j}[m]= s_{\delta(m,\,\alpha_m),j}[\alpha_m]\oplus z_{m-1,j}\oplus a_{m,j}\oplus\sigma_m{}^{s}(j),$$
$$z_{m,j}= s_{\delta(m,\,j_m),j}[j_m]\oplus s_{0,j}[0]\oplus \sigma_m{}^{z}(j),$$

We stress that the number of equations and the number of unknown values in (3) are 2m. If we rewrite (3) such that unknown elements in the equations are on the left, and known values on the right, then we have

$$s_{0,j}[0]\oplus s_{\delta(m,\,j_m),j}[j_m] = z_{m,j}\oplus\sigma_m{}^{z}(j),$$
$$s_{0,j}[1]\oplus s_{\delta(1,\,j_1),j}[j_1]= z_{1,j}\oplus \sigma_1{}^{z}(j),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s_{0,j}[t]\oplus s_{\delta(t,\,j_t),j}[j_t]=z_{t,j}\oplus \sigma_t{}^{z}(j),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s_{0,j}[1+m/2]= a_{1,j}\oplus\sigma_1{}^{a}(j),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s_{0,j}[t]\oplus s_{\delta(t,\,j_t),j}[j_t]=z_{t,j}\oplus \sigma_t{}^{z}(j),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s_{0,j}[m-1]\oplus s_{\delta(m-1,\,j_{m-1}),j}[j_{m-1}]= z_{m-1,j}\oplus \sigma_m{}^{z}{}_{-1}(j),$$
$$s_{1,j}[1]\oplus s_{\delta(1,\,\alpha_1),j}[\alpha_1] = a_{1,j}\oplus\sigma_1{}^{s}(j),$$
$$s_{2,j}[2]\oplus s_{\delta(2,\,\alpha_2),j}[\alpha_2]\oplus s_{0,j}[3+m/2]= z_{1,j}\oplus a_{3,j}\oplus a_{2,j\,-\,p(3)}\oplus\sigma_3{}^{a}(j)\oplus\sigma_2{}^{s}(j),$$
$$s_{3,j}[3]\oplus s_{\delta(3,\,\alpha_3),j}[\alpha_3] = z_{2,j}\oplus a_{3,j}\oplus\sigma_3{}^{s}(j),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$
$$s_{2i,j}[2i]\oplus s_{\delta(2i+1,2i+1+m/2),j}[2i+1+m/2]\oplus s_{\delta(2i,\,\alpha_{2i}),j}[\alpha_{2i}]=z_{2i-1,j}\oplus a_{2i+1,j}\oplus a_{2i,j\,-\,p(2i+1)}\oplus\sigma_{2i}{}^{a}{}_{+1}(j)\oplus\sigma_{2i}{}^{s}(j),$$
$$s_{2i+1,j}[2i+1]\oplus s_{\delta(2i+1,\,\alpha_{2i+1}),j}[\alpha_{2i+1}] = z_{2i,j}\oplus a_{2i+1,j}\oplus\sigma_{2i}{}^{s}{}_{+1}(j),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s_{m-2,j}[m-2]\oplus s_{\delta(m-2,\,\alpha_{m-2}),j}[\alpha_{m-2}]= z_{m-3,j}\oplus a_{m-2,j}\oplus\sigma_m{}^{s}{}_{-2}(j),$$
$$s_{m-1,j}[m-1]\oplus s_{\delta(m-1,m/2-1),j}[m/2-1]\oplus s_{\delta(m-1,\,\alpha_{m-1}),j}[\alpha_{m-1}]= z_{m,j}\oplus a_{m-1,j}\oplus a_{m-2,j\,-\,p(3)}\oplus\sigma_m{}^{a}{}_{-1}(j)\oplus\sigma_m{}^{s}{}_{-1}(j),$$
$$s_{m,j}[m]\oplus s_{\delta(m,\,\alpha_m),j}[\alpha_m] = z_{m-1,j}\oplus a_{m,j}\oplus\sigma_m{}^{s}(j),$$

The theorem is proved.

4 Attack on ISAAC

In this section we describe a known plaintext attack on the ISAAC keystream generator.

First let us carry out an estimation of the unicity distance D_{ISAAC} of ISAAC. Recall that the unicity distance is the number of keystream symbols that need to be observed in a known plaintext attack before the key can be uniquely determined.

Note that the number of various states of the ISAAC is equal to $m \cdot 2^K \cdot 2^{Km}$. Then we get that $(2^K)^{D_{ISAAC}} = m \cdot 2^{K+Km}$. Therefore, $D_{ISAAC} \approx m+2$.
Let us denote with mark "*" guessed elements of S_t^* and elements of the output sequence $\{z_i^*\}$ produced on the guessed initial state.

The method consists of four steps.
Step 1. Guess $s_m[0] \pmod{2^{2n+\theta 2}}, \ldots, s_t[t] \pmod{2^{2n+\theta 2}}, \ldots, s_{m-1}[m-1] \pmod{2^{2n+\theta 2}}$.

Step 2
Let $\beta = 2n+\theta 2$.

1. Use proposition 2 to compute $s_0[t]$, $t=0,1,\ldots,m-1$.
2. Use proposition 3 to compute $a_t \pmod{2^{2n+\theta 2}}$, $t=1\ldots m+1$.
3. Let $\tau=\beta$. Use proposition 4 to compute $a_{2j+1} \pmod{2^{\tau+q}}$, $j=0\ldots m/2-1$.
4. To find $s_m[0] \pmod{2^{\tau+q}}$, $s_1[1] \pmod{2^{\tau+q}}, \ldots, s_{m-1}[m-1] \pmod{2^{\tau+q}}$, $s_0[0] \pmod{2^{\tau+q}}$, $s_0[1] \pmod{2^{\tau+q}}, \ldots, s_0[m-1] \pmod{2^{\tau+q}}$, $a_{2i} \pmod{2^{\tau+q}}$, $i=0\ldots m/2$, we do the following.
   a) Let $j=\tau+1$.
   b) While $j \le \tau+q$ do.
   Use theorem 1 to compute $s_m[0] \pmod{2^j}, \ldots, s_{m-1}[m-1] \pmod{2^j}$, $s_0[0] \pmod{2^j}, \ldots, s_0[m-1] \pmod{2^j}$, $a_{2i} \pmod{2^j}$, $i=0\ldots m/2$. Take $j=j+1$.

Step 3
Let $\tau=2n+\theta 2+q$.
While $\tau<K$.

1. Use proposition 4 to compute $a_{2j+1} \pmod{2^{\tau+q}}$, $j=0\ldots m/2-1$.
2. To find $s_m[0] \pmod{2^{\tau+q}}$, $s_1[1] \pmod{2^{\tau+q}}, \ldots, s_{m-1}[m-1] \pmod{2^{\tau+q}}$, $s_0[0] \pmod{2^{\tau+q}}$, $s_0[1] \pmod{2^{\tau+q}}, \ldots, s_0[m-1] \pmod{2^{\tau+q}}$, $a_{2i} \pmod{2^{\tau+q}}$, $i=0\ldots m/2$, we do the following.
   a) Let $j=\tau+1$.
   b) While $j \le \tau+q$ do.
   Use to theorem 1 to compute $s_m[0] \pmod{2^j}, \ldots, s_{m-1}[m-1] \pmod{2^j}$, $s_0[0] \pmod{2^j}, \ldots, s_0[m-1] \pmod{2^j}$, $a_{2i} \pmod{2^j}$, $i=0\ldots m/2$. Take $j=j+1$.

Step 4
Compute the first $L = D_{ISAAC}$ of elements of the output sequence $z_1^*, z_2^*, \ldots z_L^*$. If $z_1^* = z_1$, $z_2^* = z_2, \ldots z_L^* = z_L$ then we have found the correct initial state of the cryptosystem, otherwise return to step 1.

Let us estimate the complexity of the method.
We may assume that the probability
$P\{s_0^*[0] \pmod{2^{(2n+\theta 2)}} = s_0[0] \pmod{2^{(2n+\theta 2)}}, \ldots, s_0^*[m-1] \pmod{2^{(2n+\theta 2)}} = s_0[m-1] \pmod{2^{(2n+\theta 2)}}\} = 1/2^{(2n+\theta 2)m}$.
Then the average of guessed elements is equal to $2^{(2n+\theta 2)m-1}$. The complexity of a solution of systems of equations at steps 2, 3 can be estimated $(K-2n-\theta 2)\cdot(2m)/3$.

Therefore, the complexity of the method is equal to $T_{met} = 2^{(2n+\theta 2)m-1} \cdot (K-2n-\theta 2)\cdot(2m)/3$. Note that the complexity of the brute force attack is equal to $T_{br} = 2^{K \cdot m-1}$.
For $m=256$, $n=8$, $K=32$, $p0=13$, $p1=6$, $p2=2$, $p3=16$, $\theta_1=\theta_2=2$, we get $T_{met} = 4.67 \cdot 10^{1240}$, $T_{br} = 5.91 \cdot 10^{2446}$.

5 Conclusion

We have described cryptanalytic algorithm on the ISAAC stream cipher. The algorithm tries to deduce the initial state in a known plaintext attack.

The described method depends on difference K-2n. If K-2n-θ2≥2n, then the complexity of the attack is approximated to be less than time of searching through the square root of all possible initial states. For values used in the cryptosystem we get the complexity $T_{met} = 4.67 \cdot 10^{1240}$. ISAAC remains a secure cipher for practical applications.

References.

[1] R.J. Jenkins, "ISAAC", Fast Software Encryption –Cambridge 1996, vol. 1039, D. Gollmann ed., Springer-Verlag.

[2] R. J. Jenkins " ISAAC" http://ourworld.compuserve.com/homepages/ bob_jenkins/isaac.htm

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

[4] Pudovkina M. "A Cycle Structure of the Alleged RC4 Keystream Generator". Journal of "Security of information technologies", Moscow, 4, 2000.