An analysis and an improvement of iterative fast correlation attacks

Michel Mitton
SGDN/DCSSI/SDS/Crypto. Lab.
51, boulevard de La Tour-Maubourg
75700 Paris-07 SP, France

November 26, 2004

Abstract

We analyse asymptotically performances and convergence of fast iterative correlation attacks for the cryptanalysis of stream ciphers using linear feedback shift registers as autonomous stages. Finally, we describe and analyse an improvement for this class of cryptanalytical algorithms.

Keywords

Stream ciphers, fast correlation attacks, asymptotic analysis, algorithmics, linear feedback shift registers, cryptanalysis.

1 Introduction

Stream ciphers are a special class of encryption algorithms. They encrypt plaintext bits one at a time, contrary to the block ciphers which encrypt blocks of plaintext bits. A *synchronous stream cipher* is a stream cipher where the ciphertext is produced by bitwise adding the plaintext bits with a stream of bits, named the *keystream*, produced by the stream cipher independently of the plaintext and depending only of the secret key and of one initialization vector.

A large number of stream ciphers use autonomous *Linear Feedback Shift Registers* (LFSR) as components, the initialization of these LFRSs being related to the secret key and the initialization vector. The most popular academic stream ciphers use some LFSRs combined through one or several nonlinear Boolean functions for building the keystream. Many variations exist where the registers are irregulary clocked or multiplexed.

Synchronous stream ciphers using LFSRs are the main target of fast correlation attacks.

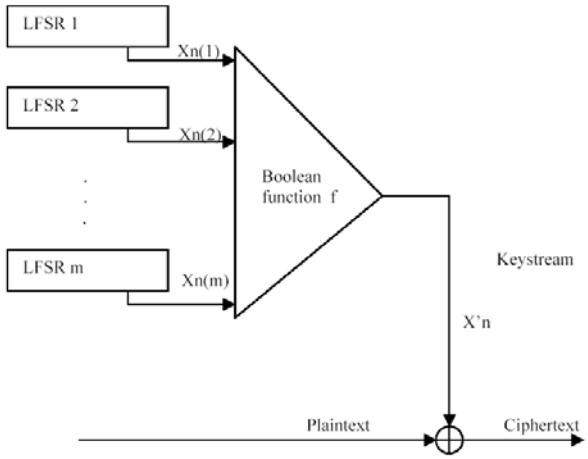

Figure 1: m LFSRs combined by a nonlinear Boolean function

Among the different kinds of attacks against stream ciphers, correlation attacks are one of the most important [9, 10]. They require the existence of correlations between linear combination of internal and output bits of keystream. These correlations need to be good enough for the attack to be succesful. A fundamental fact is that correlations always exist [9]. When nonlinear Boolean functions are used as internal components of stream cipher, correlations can be found by analyzing the Walsh-Fourier spectrum of these functions, but generally, the main method to find these correlations is by statistical analysis. Once a correlation is found, it can be written as a probability:

$$p = \Pr(x_n^{'} = x_n(i_1) \oplus x_n(i_2) \oplus ... \oplus x_n(i_m)) \neq 0.5$$

where $x_n^{'}$ is the n-th bit of keystream and $x_n(i_j)$ is the n-th output bit of the LFSR i_j. The keystream can thus be considered as a noisy version of the corresponding linear combination of output bits of one or more LFSR of stream cipher. The quality of the correlation is mesured by the parameter $\varepsilon = 1 - 2p$. Without loss of generality, and if necessary after complementation of the sequence $(x_n^{'})_{n\geq 1}$, we suppose in the sequel $\varepsilon \in [-1, 0]$. If ε is close to -1, the correlation is very good and the stream cipher is not very strong. On the contrary, if ε is close to 0, the linear combinaison of LFSR's output is very noisy and the correlation attacks will probably be inefficient. Since the LFSR output is produced by linear relations, we can always write the sum of output bits $x_n(i_1) \oplus x_n(i_2) \oplus ... \oplus x_n(i_m)$ as the output of one only larger LFSR. Without loss of generality, the stream cipher can be represented as in Fig. 2, where this sum is remplaced by x_i output of one only register, and the Boolean function by a BSC (binary symmetric channel), i.e. by a channel introducing noise on x_i with probability $1 - p$.

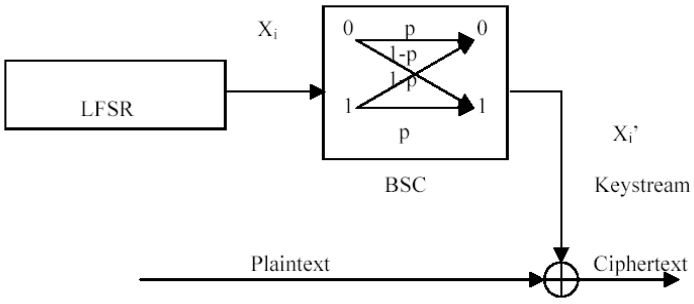

Figure 2: Equivalent schema where the keystream x'_i is correlated with the output $x_i : \Pr(x'_i = x_i) \neq 0.5$

Fast correlation attacks [1, 2, 3, 4, 5, 6, 7] are improvements of basic correlation attack [10] which essentially consists in mounting an hypothesis statistical test in an exhaustive key search procedure. In this article, we present a new asymptotic analysis of iterative fast correlation attacks and a new improvement of these algorithms.

2 Fast correlation attacks

Fast correlation attacks are usually studied in the binary symmetric channel model of Fig. 2. In this model, we consider the keystream as a noisy version of the output of some LFSR. The cryptanalysis then becomes a decoding problem: given a noisy output, find the exact output of the registers or reconstruct the initialization of these registers.

The common point of all the fast correlation attacks is the use of parity-check equations, i.e. linear relations beween register output bits x_i. Once found, these relations are evaluated on the noisy bits $x_i^{'}$. This evaluation give us a family of estimation on each bit of output register which helps to reconstruct the exact sequence of the LFSR.

Fast correlation attacks are divided into iterative and one-pass algorithms. In iterative algorithms, the parity-checks are used to modify the sequence $x_i^{'}$ and to obtain a new noisyless sequence which converges towards the sequence x_i [1, 5]. In one-pass algorithms, the parity-checks values enable us to directly compute the correct value of a small number of LFSR output x_i from the sequence $(x_i^{'})_{i\geq 1}$ [2, 3, 4, 5, 6, 7].

Our paper investigates the iterative algorithms but it's clear that the probabilist analysis developped here is also adapted to one-pass algorithms.

3 Notation and problems

In the sequel, we use the following notations:

$x \oplus y$ represents the addition modulo 2 (XOR) of two binary variables x, y. $(\mathbf{Z}/\mathbf{2Z}, \oplus, .)$ represents the finite field of characteristic 2 denoted $\mathbf{F}_2$.

We suppose known the noisy sequence $(x'_n)_{1 \leq n \leq L}$ where $x'_n = x_n \oplus e_n$, and $(x_n)_{1 \leq n \leq L}$ the sequence generated by a LFSR of length r, of transition matrix T, and initialization vector R.

$(e_n)_{1 \leq n \leq L}$ is a sequence of realization of independent and identically distributed Bernoulli random variables (iid), of parameter $q = 1 - p = \Pr(e_n = 1) = \frac{1}{2}(1 + \varepsilon)$ with $-1 < \varepsilon < 0$.

$|a|$ denotes the absolute value of the real number a.

$P(X) = \det(T \oplus XI_r) \in \mathbf{F}_2[X]$ representents the characteristic polynomial of the LFSR. This polynomial is, unless explicit hypothesis, supposed primitive in the ring $\mathbf{F}_2[X]$.

For $Q(X), R(X) \in \mathbf{F}_2[X]$, we denote $Q(X)|R(X)$ when $Q(X)$ divides $R(X)$.

$H(p) = -p \log_2(p) - (1-p) \log_2(1-p)$ is the binary entropy of the distribution probability of a Bernoulli random variable X such that $\Pr(X = 1) = p$.

The isomorphism between two isomorphic fields K and K' will be denoted $K \approxeq K'$.

The problem of the estimation of R is the basic problem of fast correlation attacks. Another problem is the estimation of the length L necessary to solve this basic problem.

4 Basic algorithm for fast correlation attacks

4.1 An estimation problem

Let $X, E_1, ..., E_m$ be $m + 1$ independent Bernoulli random variables such that $p_0 = 1 - q_0 = \Pr(X = 0)$ and $p_i = 1 - q_i = \Pr(E_i = 0)$ for $i = 1, ..., m$.

We consider the new Bernoulli random variables $Y_i = X \oplus E_i$, $1 \leq i \leq m$, and we want to compute $Q = \Pr(X = 1 | Y_1 = y_1, ..., Y_m = y_m)$ for m realizations y_i of Y_i.

From the definition of the conditional probability we have

$$\begin{aligned} Q &= \frac{\Pr(X = 1, Y_1 = y_1, ..., Y_m = y_m)}{\Pr(Y_1 = y_1, ..., Y_m = y_m)} \\ &= \frac{\Pr(X = 1, Y_1 = y_1, ..., Y_m = y_m)}{\Pr(X = 0, Y_1 = y_1, ..., Y_m = y_m) + \Pr(X = 1, Y_1 = y_1, ..., Y_m = y_m)} \\ &= \frac{1}{1 + \frac{\Pr(X=0, Y_1=y_1, ..., Y_m=y_m)}{\Pr(X=1, Y_1=y_1, ..., Y_m=y_m)}}. \end{aligned}$$

The independance hypothesis implies
$\Pr(X = 0, Y_1 = y_1, ..., Y_m = y_m) = \Pr(X = 0, E_1 = y_1, ..., E_m = y_m) =$
$p_0 \prod_{i=1}^{m} \Pr(E_i = y_i)$ and $\Pr(X = 1, Y_1 = y_1, ..., Y_m = y_m) =$

$\Pr(X = 1, E_1 = y_1 \oplus 1, ..., E_m = y_m \oplus 1) = q_0 \prod_{i=1}^{m} \Pr(E_i = y_i \oplus 1)$.

But $\Pr(E_i = y_i) = q_i y_i + p_i(y_i \oplus 1)$, so we obtain $Q = \frac{1}{1+\frac{p_0}{q_0}\prod_{i=1}^{m}\frac{q_i y_i + p_i(y_i \oplus 1)}{q_i(y_i \oplus 1)+p_i y_i}}$.

Moreover, we see that $\frac{q_i y_i + p_i(y_i \oplus 1)}{q_i(y_i \oplus 1)+p_i y_i} = (\frac{p_i}{q_i})^{1-2y_i}$, and finally $Q = \frac{1}{1+\frac{p_0}{q_0}\prod_{i=1}^{m}(\frac{p_i}{q_i})^{1-2y_i}}$.

We can write $Q = \frac{1}{1+R}$ with $R = \frac{p_0}{q_0}\prod_{i=1}^{m}(\frac{p_i}{q_i})^{1-2y_i}$, so $Log(R) = Log(\frac{p_0}{q_0}) + \sum_{i=1}^{m}(1-2y_i)Log(\frac{p_i}{q_i})$.

If we denote $\theta_i = \frac{1}{2}Log(\frac{q_i}{p_i})$, we obtain $Log(R) = -2(\theta_0 + \sum_{i=1}^{m}(1-2y_i)\theta_i)$, and then, if we denote $\hat{\theta} = -\frac{Log(R)}{2}$, i.e. $R = e^{-2\hat{\theta}}$,we have the final formula:

$$\Pr(X = 1 | Y_1 = y_1, ..., Y_m = y_m) = \frac{1}{1 + e^{-2\hat{\theta}}}, \quad (1)$$

$$\text{with } \hat{\theta} = \theta_0 + \sum_{i=1}^{m}(1-2y_i)\theta_i \text{ and } \theta_i = \frac{1}{2}Log(\frac{q_i}{p_i}). \quad (2)$$

This result constitutes one of the fondations of iterative or one-pass correlation attacks. Knowing noisy values $y_1, ..., y_m$, it enables to estimate X by maximum likehood.

4.2 Sketch of the algorithm

Another foundation of one-pass or iterative fast correlation attacks on stream ciphers, builded with autonomous LFSRs, lies on algebraic relations (or parity-checks) satisfied by bits of the sequence generated by the LFSR. We don't develop this point and refer to [1, 3, 8] for details.

We use the notations of §3 and define k-omials multiples of $P(X)$ as polynomials $Q(X) = 1 \oplus X^{i_1} \oplus X^{i_2} \oplus ... \oplus X^{i_{k-1}}$, with $1 \leq i_1 < ... < i_{k-1}$ and $k \geq 2$, verifying $P(X)|Q(X)$ in $\mathbf{F}_2[X]$.

Associated to $Q(X)$, the sequence $(x_n)_{n\geq 1}$ verifies the algebraic relation $x_n = x_{n+i_1} \oplus ... \oplus x_{n+i_{k-1}}$ for each n and each initialization R. We deduce from this that

$$x'_{n+i_1} \oplus ... \oplus x'_{n+i_{k-1}} = x_n \oplus e_{n+i_1} \oplus ... \oplus e_{n+i_{k-1}} \quad (3)$$

$$\Pr(e_{n+i_1} \oplus ... \oplus e_{n+i_{k-1}} = 1) = \frac{1}{2}(1 - (-1)^{k-1}\varepsilon^{k-1}). \quad (4)$$

The relations $x_n = x_{n+i_1} \oplus ... \oplus x_{n+i_{k-1}}$ constructed from k-omials $Q(X)$ will be called k-omials relations, or parity-checks, associated to x_n.

If we have a sequence of keystream bits x'_n, $1 \leq n \leq L$, correlated with a binary sequence x_n of same length generated by a LFSR, and if we know a certain number of k-omials relations $x_n = x_{n+i_1} \oplus ... \oplus x_{n+i_{k-1}}$, $1 \leq n + i_j \leq L$,

the value of $x'_{n+i_1} \oplus ... \oplus x'_{n+i_{k-1}}$ gives us an information on x_n. In the sequel, we denote $N_k(n)$ the number of k-omials relations associated to x_n and usable for the length $L << 2^r - 1$, and

$$N_{0,k}(x_n) = \#\left\{ \begin{array}{c} (i_1, ..., i_{k-1}) \text{ such that} \\ 1 \leq i_1 < ... < i_{k-1} \leq L \\ \text{and } 1 \leq n + i_j \leq L \end{array} \mid \begin{array}{c} P(X)|1 \oplus X^{i_1} \oplus ... \oplus X^{i_{k-1}} \\ \text{and } x'_{n+i_1} \oplus ... \oplus x'_{n+i_{k-1}} = 0 \end{array} \right\}.$$

Remark 1 *The primitivity's hypothesis of $P(X)$ implies $k \geq 3$ to have $N_k(n) \geq 1$, but if $P(X)$ is only irreductible not primitive (so if $2^r - 1$ is not a prime number), it's possible to have $N_2(n) \geq 1$.*

Inspecting the different values $N_{0,k}(x_n) \in [0, N_k(n)]$, with $3 \leq k \leq d$ for $d << L$, we want to estimate the x_n value. If we consider x_n and $N_{0,k}(x_n)$ as random variables, our aim is to calculate $\Pr(x_n = 1|N_{0,k}(x_n),\ 3 \leq k \leq d)$, therefore we are bringing back to the estimation's problem of 4.1. Using (1), (2) we obtain $\Pr(x_n = 1|N_{0,k}(x_n),\ 3 \leq k \leq d) = \frac{1}{1+e^{-2\hat{\theta}(n)}}$ with

$$\hat{\theta}(n) = \theta_0(n) + \sum_{k=3}^{d} \left(\sum_{\substack{1 \leq i_1 < ... < i_k \leq L, \\ P(X)|1 \oplus X^{i_1} \oplus ... \oplus X^{i_{k-1}}}} 1 - 2(x'_{n+i_1} \oplus ... \oplus x'_{n+i_{k-1}}) \right) \theta_k(n)$$

$= \theta_0(n) + \sum_{k=3}^{d} (2N_{0,k}(x_n) - N_k(n))\theta_k(n)$ and $\theta_k(n) = \frac{1}{2} Log(\frac{q_k(n)}{p_k(n)})$ with $q_k(n) = \Pr(E_k(n) = 1) = \Pr(e_{n+i_1} \oplus ... \oplus e_{n+i_{k-1}} = 1)$ so, from (4) we obtain $\theta_k(n) = \frac{1}{2} Log(\frac{1-(-1)^{k-1}\varepsilon^{k-1}}{1+(-1)^{k-1}\varepsilon^{k-1}}) = \arg\tanh((-1)^k \varepsilon^{k-1})$.

Moreover $\theta_0(n) = \frac{1}{2} Log(\frac{q_0(n)}{p_0(n)}) = \frac{1}{2} Log(\frac{1+\varepsilon_0}{1-\varepsilon_0})$. But $(x_n)_{n \geq 1}$, generated by a LFSR, is such that $\frac{1}{2}(1 + \varepsilon_0) = \Pr(x_n = 1) \approx \frac{1}{2}$. So $\varepsilon_0 \approx 0$, and we may assume $\theta_0(n) = 0$.

Therefore, as $\frac{1}{1+e^{-2\hat{\theta}(n)}} \geq \frac{1}{2}$ if and only if $\hat{\theta}(n) \geq 0$ (see Fig. 3), we have an estimation process of x_n summarized by $\hat{x_n} = 1$ if and only if $\hat{\theta}(n) \geq 0$.

From definition of $\hat{\theta}(n)$ and $\theta_k(n)$, we obtain the following equivalence:
$\hat{x_n} = 1$ if and only if

$$\sum_{k=3}^{d} N_{0,k}(x_n) \arg\tanh((-1)^k \varepsilon^{k-1}) \geq \frac{1}{2} \sum_{k=3}^{d} N_k(n) \arg\tanh((-1)^k \varepsilon^{k-1}). \qquad (5)$$

Considered as random variables, $N_{0,k}(x_n)$ for each $k \in [3, d]$, are binomial variables: for each $i \in [0, N_k(n)], \Pr(N_{0,k}(x_n) = i) =$
$\binom{N_k(n)}{i} (\frac{1}{2}(1 + (-1)^{x_n}(-1)^{k-1}\varepsilon^{k-1}))^i (\frac{1}{2}(1 - (-1)^{x_n}(-1)^{k-1}\varepsilon^{k-1}))^{N_k(n)-i}$.

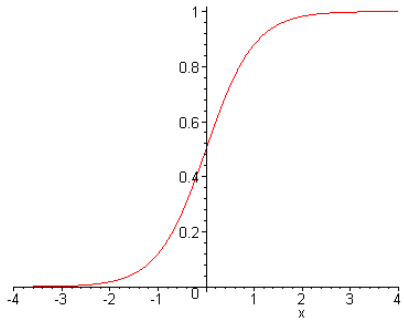

Figure 3: The graph of $\theta \longmapsto \frac{1}{1+e^{-2\theta}}$

Let q be the integer $\min\{k \geq 3 | N_k(n) \geq 1\}$, i.e. $N_2(n) = ... = N_{q-1}(n) = 0$, $N_q(n) \geq 1$.

From (5), if we denote $S = \frac{1}{2}\sum_{k=q}^{d} N_k(n) \arg\tanh((-1)^k \varepsilon^{k-1})$, we get

$$\hat{x_n} = 1 \text{ if and only if } \sum_{k=q}^{d} N_{0,k}(x_n) \arg\tanh((-1)^k \varepsilon^{k-1}) \geq S. \tag{6}$$

From (3, 4) the expectation and variance of $N_{0,k}(x_n)$ are
$m_k(x_n) = N_k(n) \Pr(x'_{n+i_1} \oplus ... \oplus x'_{n+i_{k-1}} = 0) = \frac{N_k(n)}{2}(1+(-1)^{x_n}(-1)^{k-1}\varepsilon^{k-1})$,
$\sigma_k^2 = \frac{N_k(n)}{4}(1+\varepsilon^{2(k-1)})$.

Let us consider now $N_0(x_n) = \sum_{k=q}^{d} N_{0,k}(x_n) \arg\tanh((-1)^k \varepsilon^{k-1})$ as a random variable. The linearity of the expectation implies

$E(N_0(x_n)) = \sum_{k=q}^{d} \arg\tanh((-1)^k \varepsilon^{k-1}) E(N_{0,k}(x_n)) = \sum_{k=q}^{d} m_k(x_n) \arg\tanh((-1)^k \varepsilon^{k-1})$.

If we suppose that $N_{0,q}(x_n), ..., N_{0,d}(x_n)$ are independent random variables, we get

$\sigma^2(N_0(x_n)) = \sigma^2[\sum_{k=q}^{d} N_{0,k}(x_n) \arg\tanh((-1)^k \varepsilon^{k-1})]$

$= \sum_{k=q}^{d} [\arg\tanh^2((-1)^k \varepsilon^{k-1})] \sigma^2(N_{0,k}(x_n)) = \sum_{k=q}^{d} \sigma_k^2 \arg\tanh^2((-1)^k \varepsilon^{k-1})$ (because $\sigma^2(X+Y) = \sigma^2(X) + \sigma^2(Y)$ when X and Y are independent, and $\sigma^2(\lambda X) = \lambda^2 \sigma^2(X)$).

We denote $N_0 = N_0(x_n)$, $N_{0,k} = N_{0,k}(x_n)$ and $m_k = m_k(x_n)$.

From central limit theorem, when $N_k(n)$ is enough large, $N_{0,k} \backsim \mathcal{N}(m_k, \sigma_k)$, so $\lambda_k N_{0,k} \backsim \mathcal{N}(\lambda_k m_k, |\lambda_k| \sigma_k)$.

Therefore $N_0 = \sum_{k=q}^{d} \lambda_k N_{0,k}$, which is asymptotically a sum of $d - q + 1$

independent normal laws $\mathcal{N}(\lambda_k m_k, |\lambda_k|\sigma_k)$, is also asymptotically a normal law $\mathcal{N}(m,\sigma) : \Pr(N_0 \leq x) \underset{N_q(n),\ldots,N_d(n) \text{ larges}}{\sim} \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\frac{x-m}{\sigma}} \exp(-\frac{t^2}{2})dt$, with

$$m(x_n) = \sum_{k=q}^{d} m_k \arg\tanh((-1)^k \varepsilon^{k-1}), m_k = \frac{N_k(n)}{2}(1 + (-1)^{x_n}(-1)^{k-1}\varepsilon^{k-1}), \tag{7}$$

$$\text{and } \sigma^2 = \sum_{k=q}^{d} \sigma_k^2 \arg\tanh^2((-1)^k \varepsilon^{k-1}), \sigma_k^2 = \frac{N_k(n)}{4}(1 - \varepsilon^{2(k-1)}). \tag{8}$$

It is now possible to evaluate the error between the estimation $\hat{x_n}$ obtained using (6) and x_n.

$$\begin{aligned}
\Pr(\hat{x_n} \neq x_n) &= \Pr(\hat{x_n} \neq x_n | x_n = 0) \Pr(x_n = 0) + \\
&\quad \Pr(\hat{x_n} \neq x_n | x_n = 1) \Pr(x_n = 1) \\
&= \tfrac{1}{2}(\Pr(\hat{x_n} = 1 | x_n = 0) + \Pr(\hat{x_n} = 0 | x_n = 1)) \\
&\sim \frac{1}{2}\left(\frac{1}{\sqrt{2\pi}} \int_{\frac{S-m_0}{\sigma}}^{+\infty} \exp(-\tfrac{t^2}{2})dt + \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\frac{S-m_1}{\sigma}} \exp(-\tfrac{t^2}{2})dt \right) \text{ and finally}
\end{aligned}$$

$$\Pr(\hat{x_n} \neq x_n) \sim \frac{1}{2}\left(1 - \frac{1}{\sqrt{2\pi}} \int_{\frac{S-m1}{\sigma}}^{\frac{S-m_0}{\sigma}} \exp(-\frac{t^2}{2})dt\right). \tag{9}$$

We have

$$\begin{aligned}
S - m_0 &= \tfrac{1}{2}\sum_{k=q}^{d} N_k(n) \arg\tanh((-1)^k\varepsilon^{k-1}) - \sum_{k=q}^{d} m_k(0) \arg\tanh((-1)^k\varepsilon^{k-1}) \\
&= \tfrac{1}{2}\sum_{k=q}^{d} (N_k(n) - 2m_k(0)) \arg\tanh((-1)^k\varepsilon^{k-1}),
\end{aligned}$$

$S - m_1 = \frac{1}{2}\sum_{k=q}^{d} (N_k(n) - 2m_k(1)) \arg\tanh((-1)^k\varepsilon^{k-1})$, and from (7) we obtain

$$S - m_0 = -\tfrac{1}{2}\sum_{k=q}^{d} (-1)^{k-1}\varepsilon^{k-1} \arg\tanh((-1)^k\varepsilon^{k-1}),$$

$$S - m_1 = \tfrac{1}{2}\sum_{k=q}^{d} (-1)^{k-1}\varepsilon^{k-1} \arg\tanh((-1)^k\varepsilon^{k-1}) = -(S - m_0).$$

We deduce from this and from (8) that

$$\frac{S-m_0}{\sigma} = -\frac{\sum_{k=q}^{d} (-1)^{k-1}\varepsilon^{k-1} N_k(n) \arg\tanh((-1)^k\varepsilon^{k-1})}{\left(\sum_{k=q}^{d} N_k(n)(1-\varepsilon^{2(k-1)}) \arg\tanh^2((-1)^k\varepsilon^{k-1})\right)^{\frac{1}{2}}} = -\frac{S-m_1}{\sigma}.$$

On the other hand, it's easy to prove that

$$\int_0^r \exp(-\frac{t^2}{2})dt = r\left(1 + r^2 R(r)\right) \text{ with } R(r) \underset{r\to 0}{\to} R(0) = -\frac{1}{6}. \tag{10}$$

When $\varepsilon \to 0_-$, we have $\frac{S-m_0}{\sigma} \longrightarrow 0$, so from (9) and (10) we asymptotically obtain

$\frac{1}{2}\left(1 - \frac{1}{\sqrt{2\pi}} \int_{\frac{S-m1}{\sigma}}^{\frac{S-m_0}{\sigma}} \exp(-\frac{t^2}{2})dt\right) \underset{\varepsilon \to 0_-}{\sim} \frac{1}{2}\left(1 - \frac{1}{\sqrt{2\pi}} \frac{m_0 - m_1}{\sigma}\right)$, and finally from (8),

$$\Pr(\hat{x_n} \neq x_n) \underset{N_q(n),...,N_d(n) \text{ larges and } \varepsilon \longrightarrow 0_-}{\sim}$$

$$\frac{1}{2}\left\{1 + \sqrt{\frac{2}{\pi}} \frac{\sum_{k=q}^{d} (-1)^{k-1}\varepsilon^{k-1} N_k(n) \arg\tanh((-1)^k \varepsilon^{k-1})}{\left[\sum_{k=q}^{d} \left(1 - \varepsilon^{2(k-1)}\right) N_k(n) \arg\tanh^2\left((-1)^k \varepsilon^{k-1}\right)\right]^{\frac{1}{2}}}\right\}$$

The computation of the estimation $\hat{x_n}$, for each $n \in [1, L]$, is the first iteration of the algorithm. Therefore, from $(x_n)_{1 \leq n \leq L}$, we obtain the new binary sequence $(x_n(1))_{1 \leq n \leq L}$ defined by $x_n(1) = \hat{x_n}$, and we may write, for $|\varepsilon|$ small and $N_q(n), ..., N_d(n)$ larges, $\Pr(x_n(1) \neq x_n) = \frac{1}{2}(1 + \varepsilon_n(1))$ with

$$\varepsilon_n(1) \sim \sqrt{\frac{2}{\pi}} \frac{\sum_{k=q}^{d} (-1)^{k-1}\varepsilon^{k-1} N_k(n) \arg\tanh((-1)^k \varepsilon^{k-1})}{\left[\sum_{k=q}^{d} \left(1 - \varepsilon^{2(k-1)}\right) N_k(n) \arg\tanh^2\left((-1)^k \varepsilon^{k-1}\right)\right]^{\frac{1}{2}}}. \tag{11}$$

.

Remark 2 *As $\varepsilon < 0$, we also have $\varepsilon_n(1) < 0$.*

A sufficient condition for convergence of the algorithm is the decreasing of the noise after the first iteration: $\Pr(x_n(1) \neq x_n) < \Pr(x_n^{'} \neq x_n)$, i.e. $\varepsilon_n(1) < \varepsilon$.

Translating this condition for $|\varepsilon|$ small, $N_k(n)$ large $(q \leq k \leq d)$, and using the equivalent $\arg\tanh(\varepsilon) \sim \varepsilon$, the value (9) gives us the following inequality

$$\sqrt{\frac{2}{\pi}} \frac{\sum_{k=q}^{d} (-1)^{k-1}\varepsilon^{k-1} N_k(n)(-1)^k \varepsilon^{k-1}}{\left[\sum_{k=q}^{d} \left(1-\varepsilon^{2(k-1)}\right) N_k(n)((-1)^k \varepsilon^{k-1})^2\right]^{\frac{1}{2}}} < \varepsilon.$$

After simplification we obtain

$\sum_{k=q}^{d} \varepsilon^{2(k-1)} N_k(n) > -\sqrt{\frac{\pi}{2}}\varepsilon \left[\sum_{k=q}^{d} \left(1 - \varepsilon^{2(k-1)}\right) N_k(n) \varepsilon^{2(k-1)}\right]^{\frac{1}{2}}$ or equivalently,

if we denote $U = \sum_{k=q}^{d} \varepsilon^{2(k-1)} N_k(n)$ and $V = \sum_{k=q}^{d} \varepsilon^{4(k-1)} N_k(n)$,

$$U > -\sqrt{\frac{\pi}{2}}(\varepsilon U - V)^{\frac{1}{2}}$$

with $U > 0, V > 0$, and $U - V > 0$.

A sufficient condition to realize this last inequality is $U > -\sqrt{\frac{\pi}{2}}\varepsilon U^{\frac{1}{2}}$, i.e. $U > \frac{\pi}{2}\varepsilon^2$.

Consequently, we obtain the asymptotical sufficient convergence condition

$$\sum_{k=q}^{d} \varepsilon^{2(k-2)} N_k(n) > \frac{\pi}{2}. \tag{12}$$

We have seen that $S - m_1 = -(S - m_0)$, so, from (9), it's easy to see that $\Pr(\overset{\wedge}{x_n} \neq x_n) \sim \frac{1}{2}\left(1 - \sqrt{\frac{2}{\pi}} \int_0^{\frac{S-m_0}{\sigma}} \exp(-\frac{t^2}{2})dt\right)$ because $\int_{\frac{S-m1}{\sigma}}^{\frac{S-m_0}{\sigma}} \exp(-\frac{t^2}{2})dt = 2\int_0^{\frac{S-m_0}{\sigma}} \exp(-\frac{t^2}{2})dt$.

In the following, the function $\varphi :]-1, 0[\to]-1, 0[$ is defined by $\varepsilon \longmapsto \varphi(\varepsilon) = -\sqrt{\frac{2}{\pi}} \int_0^{\frac{S-m_0}{\sigma}} \exp(-\frac{t^2}{2})dt$, and we study, for each $n \in [1, L]$, the recurrent sequence of real numbers $\varepsilon_n(k) = \varphi(\varepsilon_n(k-1))$ for $k \geq 1$, with $\varepsilon_n(0) = \varepsilon$.

The iterative algorithm at iteration $k \geq 1$ generates the sequence $(x_n(k))_{1 \leq n \leq L}$ defined by $x_n(k) = \overset{\wedge}{x_n}$ with the estimation process (6) applied on sequence $(x_n(k-1))_{1 \leq n \leq L}$ and $x_n(k-1) = x_n \oplus e_n(k-1)$, with the initial values $x_n(0) = x_n^{'}, e_n(0) = e_n$, and the condition for convergence $\varepsilon_n(1) < \varepsilon$ realized. In this case, using the central limit theorem for $N_q(n), ..., N_d(n)$ enough large, we have $\Pr(x_n(k) \neq x_n) \sim \frac{1}{2}(1 + \varepsilon_n(k))$.

Now, the problem is to prove that $\lim_{k \longrightarrow +\infty} \varepsilon_n(k) = -1$, i.e. that $x_n(k)$ converges to x_n.

From $\frac{S-m_0}{\sigma} = -\frac{\sum_{k=q}^{d} (-1)^{k-1}\varepsilon^{k-1} N_k(n) \arg\tanh((-1)^k\varepsilon^{k-1})}{\left(\sum_{k=q}^{d} N_k(n)(1-\varepsilon^{2(k-1)}) \arg\tanh^2((-1)^k\varepsilon^{k-1})\right)^{\frac{1}{2}}}$ seen p. 8, we deduce $\lim_{\varepsilon \to 0_-} \frac{S-m_0}{\sigma} = 0_+$ and $\lim_{\varepsilon \to -1_+} \frac{S-m_0}{\sigma} = +\infty$, so $\lim_{\varepsilon \to 0_-} \varphi(\varepsilon) = 0_-$, $\lim_{\varepsilon \to -1_+} \varphi(\varepsilon) = -1_+$. Moreover, the sufficient condition for convergence is $\varphi(\varepsilon) < \varepsilon$.

φ is derivable on $]-1, 0[$, we have $\varphi^{'}(\varepsilon) = -\sqrt{\frac{2}{\pi}}(\frac{S-m_0}{\sigma})^{'} \exp(-\frac{1}{2}(\frac{S-m_0}{\sigma})^2)$ and we denote $\frac{S-m_0}{\sigma} = \frac{N}{D}$. Using $\arg\tanh(\varepsilon) \sim \varepsilon$, the above formula implies $N = \sum_{k=q}^{d} \varepsilon^{2(k-1)} N_k(n)$ and

$$D = \left(\sum_{k=q}^{d} N_k(n)(1 - \varepsilon^{2(k-1)})\varepsilon^{2(k-1)}\right)^{\frac{1}{2}}.$$

It's clear that $sign(\varphi^{'}) = -sign(N^{'}D - ND^{'})$, and after simplification, we get $N^{'}D - ND^{'} = \sum_{q \leq k,l \leq d} (k-1)N_k(n)N_l(n)\varepsilon^{2(k+l-2)-1} < 0$, so φ is increasing on $]-1, 0[$. From the definition of φ we have $\varepsilon_n(k) = \varphi^k(\varepsilon)$, and we have seen,

from (12), that $\varphi(\varepsilon) < \varepsilon$. The increasing of φ implies $\varphi^{k+1}(\varepsilon) < \varphi^k(\varepsilon)$, therefore $(\varepsilon_n(k))_k$ is a decreasing sequence of negative real numbers, lower bounded by -1, so $l_n = \lim_{k\to+\infty} \varepsilon_n(k)$ exists and $l_n \geq -1$. On the other hand, φ is clearly a continuous function on $]-1, 0[$, so, if $l_n > -1$, the continuity at point l_n implies $\varphi(l_n) = \varphi(\lim_{k\to+\infty} \varepsilon_n(k)) = \lim_{k\to+\infty} \varphi(\varepsilon_n(k)) = \lim_{k\to+\infty} \varepsilon_n(k+1) = l_n$.

But, for each $\varepsilon' \in]-1, \varepsilon]$ and from (12) we deduce $\sum_{k=q}^{d} \varepsilon'^{2(k-2)} N_k(n) > \frac{\pi}{2}$, and then $\varphi(\varepsilon') < \varepsilon'$. Consequently, the hypothesis $l_n > -1$ implies a contradiction with the fact that l_n is a fixed point of φ. So, the only other possibility is $l_n = -1$, which proves that $\lim_{k\longrightarrow+\infty} \varepsilon_n(k) = -1$.

5 An improvement of the basic algorithm

5.1 Description

We have seen at Remark 1 that, in the case $P(X)$ primitive, we have $N_2(n) = 0$. However, if we consider the n-th bit of keystream $x'_n = x_n \oplus e_n$ as an estimation of x_n, we may integrate this value in the estimation process described § 4.2.

This is equivalent to compute $\Pr(x_n = 1 | N_{0,k}(x_n),\ 2 \leq k \leq d)$ with $N_2(n) = 1$ and we must rewrite (6) with $N_q(n) \geq 1$ for $q \geq 3$.

More exactly, together with $N_2(n) = 1$, when $q \geq 4$ we have $N_k(n) = 0$ for $k \in [3, q-1]$, and when $q = 3$ we have $N_3(n) \geq 1$.

Remark that if $x'_n = 0$ (resp. 1) we have $N_{0,2}(n) = 1$ (resp. 0), therefore $2N_{0,2}(x_n) - N_2(n) = 2N_{0,2}(x_n) - 1 = (-1)^{x'_n}$.

Using this remark to rewrite (6) we obtain

$$\begin{aligned} \hat{x_n} \quad = \quad & 1 \text{ if and only if } \sum_{k=q}^{d} N_{0,k}(x_n) \arg\tanh((-1)^k \varepsilon^{k-1}) \geq \\ & \frac{1}{2}\left[\sum_{k=q}^{d} N_k(n) \arg\tanh((-1)^k \varepsilon^{k-1}) - (-1)^{x'_n} \arg\tanh(\varepsilon)\right]. \quad (13) \end{aligned}$$

In the following, as precedently, we use the approximation $\arg\tanh(\varepsilon) \sim \varepsilon$. With this approximation, and because $\varepsilon < 0$, we obtain

$$\hat{x_n} = 1 \text{ if and only if } \sum_{k=q}^{d} N_{0,k}(x_n)(-1)^k \varepsilon^{k-2} \leq S' \quad (14)$$

with

$$S' = \frac{1}{2}\left[\sum_{k=q}^{d} N_k(n)(-1)^k \varepsilon^{k-2} - (-1)^{x'_n}\right]. \quad (15)$$

Therefore, we have now a new estimation scheme leading on a new fast iterative algorithm. Our aim is now to compare him with the basic algorithm.

5.2 Performance and comparison

We consider $N_{0,q}(n), ..., N_{0,d}(n)$ as $d-q+1$ binomial variables, and we suppose these variables independent. Using central limit theorem for $N_k(n)$ enough large for $q \leq k \leq d$, we have $N_{0,k}(x_n) \sim \mathcal{N}(m_k(x_n), \sigma_k)$ and, as already seen at §4.2, $N_0(x_n) = \sum_{k=q}^{d} N_{0,k}(x_n)(-1)^k \varepsilon^{k-2} \sim \mathcal{N}(m(x_n), \sigma)$ with

$$\begin{aligned} m(x_n) &= \sum_{k=q}^{d} (-1)^k \varepsilon^{k-2} m_k(x_n),\ m_k(x_n) = \frac{N_k(n)}{2}\left(1 + (-1)^{x'_n}(-1)^{k-1}\varepsilon^{k-1}\right), \\ \sigma^2 &= \sum_{k=q}^{d} \varepsilon^{2(k-2)}\sigma_k^2, \text{ and } \sigma_k^2 = \frac{N_k(n)}{4}(1-\varepsilon^{2(k-1)}) \end{aligned} \tag{16}$$

because $N_0(x_n)$, considered as random variable, is a linear combination of $d-q+1$ binomial independent variables $N_{0,k}(x_n)$.

As S' depends of $x'_n = x_n \oplus e_n$, we have

$$\begin{aligned} \Pr(\overset{\wedge}{x_n} \neq x_n) = {} & \Pr(\overset{\wedge}{x_n} \neq x_n | x_n = 0 \text{ and } e_n = 0)\Pr(x_n = 0 \text{ and } e_n = 0) + \\ & \Pr(\overset{\wedge}{x_n} \neq x_n | x_n = 0 \text{ and } e_n = 1)\Pr(x_n = 0 \text{ and } e_n = 1) + \\ & \Pr(\overset{\wedge}{x_n} \neq x_n | x_n = 1 \text{ and } e_n = 0)\Pr(x_n = 1 \text{ and } e_n = 0) + \\ & \Pr(\overset{\wedge}{x_n} \neq x_n | x_n = 1 \text{ and } e_n = 1)\Pr(x_n = 1 \text{ and } e_n = 1) \end{aligned}$$

In the following, for each $n \geq 1$, we suppose x_n and e_n independent random variables.

For $i, j \in \mathbf{F}_2$, if we denote $p_{ij} = \Pr(\overset{\wedge}{x_n} \neq x_n | x_n = i \text{ and } e_n = j)$ and $S' = S'(x'_n)$, we have successively

$p_{00} = \Pr(\overset{\wedge}{x_n} = 1 | x_n = 0 \text{ and } e_n = 0) = \Pr(N_0(0) \leq S'(0))$,
$p_{01} = \Pr(\overset{\wedge}{x_n} = 1 | x_n = 0 \text{ and } e_n = 1) = \Pr(N_0(0) \leq S'(1))$,
$p_{10} = \Pr(\overset{\wedge}{x_n} = 0 | x_n = 1 \text{ and } e_n = 0) = \Pr(N_0(1) > S'(1))$,
$p_{11} = \Pr(\overset{\wedge}{x_n} = 0 | x_n = 1 \text{ and } e_n = 1) = \Pr(N_0(1) > S'(0))$,
with

$$S'(0) = \tfrac{1}{2}\left[\sum_{k=q}^{d} N_k(n)(-1)^k\varepsilon^{k-2} - (-1)^0\right] = \tfrac{1}{2}\left[\sum_{k=q}^{d} N_k(n)(-1)^k\varepsilon^{k-2} - 1\right],$$

$$S'(1) = \tfrac{1}{2}\left[\sum_{k=q}^{d} N_k(n)(-1)^k\varepsilon^{k-2} - (-1)^1\right] = \tfrac{1}{2}\left[\sum_{k=q}^{d} N_k(n)(-1)^k\varepsilon^{k-2} + 1\right],$$

and
$\Pr(\overset{\wedge}{x_n} \neq x_n) = \frac{1}{4}(1-\varepsilon)(p_{00}+p_{10}) + \frac{1}{4}(1+\varepsilon)(p_{01}+p_{11})$.
Furthermore, $N_0(x_n) \sim \mathcal{N}(m(x_n), \sigma)$ implies
$\Pr(N_0(x_n) \leq x) \sim \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{x} \exp(-\frac{1}{2}(\frac{t-m(x_n)}{\sigma})^2)dt$ with $m(x_n)$ and σ given by (16). From this we obtain $\Pr(\overset{\wedge}{x_n} \neq x_n) \sim$

$$\frac{1}{4\sqrt{2\pi}}(1-\varepsilon)\left(\int_{-\infty}^{\frac{S'(0)-m(0)}{\sigma}} \exp(-\tfrac{t^2}{2})dt + \int_{\frac{S'(1)-m(1)}{\sigma}}^{+\infty} \exp(-\tfrac{t^2}{2})dt\right) +$$

$\frac{1}{4\sqrt{2\pi}}(1+\varepsilon)\left(\int_{-\infty}^{\frac{S'(1)-m(0)}{\sigma}}\exp(-\frac{t^2}{2})dt+\int_{\frac{S'(0)-m(1)}{\sigma}}^{+\infty}\exp(-\frac{t^2}{2})dt\right)$.

After simplification, we have

$\frac{S'(0)-m(0)}{\sigma}=\frac{\sum_{k=q}^{d}N_k(n)\varepsilon^{2k-3}-1}{\left(\sum_{k=q}^{d}\varepsilon^{2(k-2)}(1-\varepsilon^{2(k-1)})N_k(n)\right)^{\frac{1}{2}}}=-\frac{S'(1)-m(1)}{\sigma}$, and

$\frac{S'(1)-m(0)}{\sigma}=\frac{\sum_{k=q}^{d}N_k(n)\varepsilon^{2k-3}+1}{\left(\sum_{k=q}^{d}\varepsilon^{2(k-2)}(1-\varepsilon^{2(k-1)})N_k(n)\right)^{\frac{1}{2}}}=-\frac{S'(0)-m(1)}{\sigma}$, so finally

$$\Pr(\hat{x_n}\neq x_n)\sim\frac{1}{4}(1-\varepsilon)\left(1-\frac{2}{\sqrt{2\pi}}\int_0^{-\frac{S'(0)-m(0)}{\sigma}}\exp(-\frac{t^2}{2})dt\right)+\frac{1}{4}(1+\varepsilon)\left(1+\frac{2}{\sqrt{2\pi}}\int_0^{\frac{S'(1)-m(0)}{\sigma}}\exp(-\frac{t^2}{2})dt\right). \quad (17)$$

On the other hand, for $|\varepsilon|$ small,

$\frac{S'(1)-m(0)}{\sigma}=\frac{1+\varepsilon\sum_{k=q}^{d}N_k(n)\varepsilon^{2k-4}}{\left(\sum_{k=q}^{d}\varepsilon^{2(k-2)}(1-\varepsilon^{2(k-1)})N_k(n)\right)^{\frac{1}{2}}}\sim\frac{1+4\varepsilon\sigma^2}{2\sigma}=\frac{1}{2\sigma}+2\varepsilon\sigma$ and

$-\frac{S'(0)-m(0)}{\sigma}=\frac{1-\varepsilon\sum_{k=q}^{d}N_k(n)\varepsilon^{2k-4}}{\left(\sum_{k=q}^{d}\varepsilon^{2(k-2)}(1-\varepsilon^{2(k-1)})N_k(n)\right)^{\frac{1}{2}}}\sim\frac{1-4\varepsilon\sigma^2}{2\sigma}=\frac{1}{2\sigma}-2\varepsilon\sigma$, therefore,

we obtain the following asymptotic development:

$\frac{1}{4}(1-\varepsilon)\left(1-\frac{2}{\sqrt{2\pi}}\int_0^{-\frac{S'(0)-m(0)}{\sigma}}\exp(-\frac{t^2}{2})dt\right)+$

$\frac{1}{4}(1+\varepsilon)\left(1+\frac{2}{\sqrt{2\pi}}\int_0^{\frac{S'(1)-m(0)}{\sigma}}\exp(-t^2)dt\right)\sim$

$\frac{1}{2}+\left(\sqrt{\frac{2}{\pi}}\sigma\exp(-\frac{1}{8\sigma^2})+\frac{1}{2}\frac{2}{\sqrt{\pi}}\int_0^{\frac{1}{2\sqrt{2}\sigma}}\exp(-t^2)dt\right)\varepsilon+O(\varepsilon^3)$.

Finally, using (17) we obtain

$$\Pr(\hat{x_n}\neq x_n)\sim\frac{1}{2}+\left(\sqrt{\frac{2}{\pi}}\sigma\exp(-\frac{1}{8\sigma^2})+\frac{1}{\sqrt{\pi}}\int_0^{\frac{1}{2\sqrt{2}\sigma}}\exp(-t^2)dt\right)\varepsilon. \quad (18)$$

The sufficient convergence condition studied was $\Pr(x_n(1)\neq x_n)<\frac{1}{2}(1+\varepsilon)$. With our modification, we shall see that this condition is automatically verified. Let α be a real negative number such that $-1<\alpha\leq\varepsilon$, and consider the

new condition $\Pr(x_n(1) \neq x_n) < \frac{1}{2}(1+\alpha)$. From (18) we can translate this condition by

$(2\sqrt{\frac{2}{\pi}}\sigma \exp(-\frac{1}{8\sigma^2}) + \frac{2}{\sqrt{\pi}} \int_0^{\frac{1}{2\sqrt{2}\sigma}} \exp(-t^2)dt)\varepsilon < \alpha$ which gives us

$$2\sqrt{\frac{2}{\pi}}\sigma \exp(-\frac{1}{8\sigma^2}) + \frac{2}{\sqrt{\pi}} \int_0^{\frac{1}{2\sqrt{2}\sigma}} \exp(-t^2)dt > \frac{\alpha}{\varepsilon}. \tag{19}$$

This condition can be interpreted as an inequation's family parameterized by $\lambda = \frac{\alpha}{\varepsilon} \geq 1$ and with unkwown factor σ.

For each $\lambda \geq 1$, this inequation can be graphically solved with a computer algebra system. The inequation (19) can be write as $2\sqrt{\frac{2}{\pi}}\sigma \exp(-\frac{1}{8\sigma^2}) + \operatorname{erf}(\frac{1}{2\sqrt{2}\sigma}) - \lambda > 0$ and, for $\lambda = \frac{7}{6}$, we obtain (see Figure 4) $\sigma > \frac{1}{2}$.

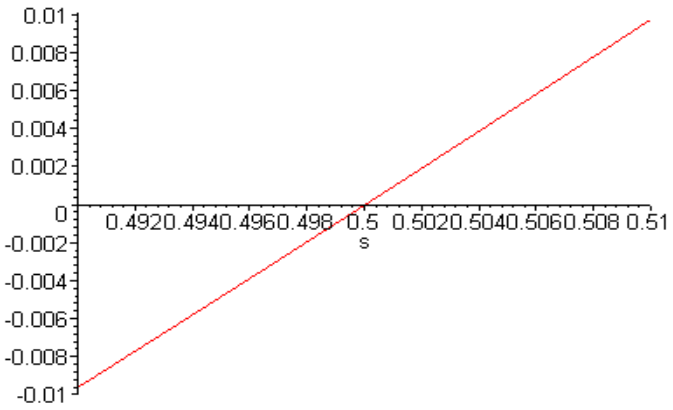

Figure 4: The graph of $\sigma \mapsto 2\sqrt{\frac{2}{\pi}}\sigma \exp(-\frac{1}{8\sigma^2}) + \operatorname{erf}(\frac{1}{2\sqrt{2}\sigma}) - 7/6$

From (16) we have $\sigma = \frac{1}{2}(\sum_{k=q}^{d} \varepsilon^{2(k-2)}(1-\varepsilon^{2(k-1)})N_k(n))^{\frac{1}{2}}$, therefore an equivalent condition to realize $\sigma > \frac{1}{2}$ is $\sum_{k=q}^{d} \varepsilon^{2(k-2)}(1-\varepsilon^{2(k-1)})N_k(n) > 1$.

So, if $\sum_{k=q}^{d} \varepsilon^{2(k-2)}(1-\varepsilon^{2(k-1)})N_k(n) > 1$, i.e. approximatively $\sum_{k=q}^{d} \varepsilon^{2(k-2)}N_k(n) > 1$ for $|\varepsilon|$ small, we have $\Pr(x_n(1) \neq x_n) < \frac{1}{2}\left(1+\frac{7}{6}\varepsilon\right) < \frac{1}{2}(1+\varepsilon)$ while, without our modification we have seen at §4.2 that $\Pr(x_n(1) \neq x_n) < \frac{1}{2}(1+\varepsilon)$ only if $\sum_{k=q} \varepsilon^{2(k-2)}N_k(n) > \frac{\pi}{2}$.

This property proves that our modification improves the efficacity of the algorithm.

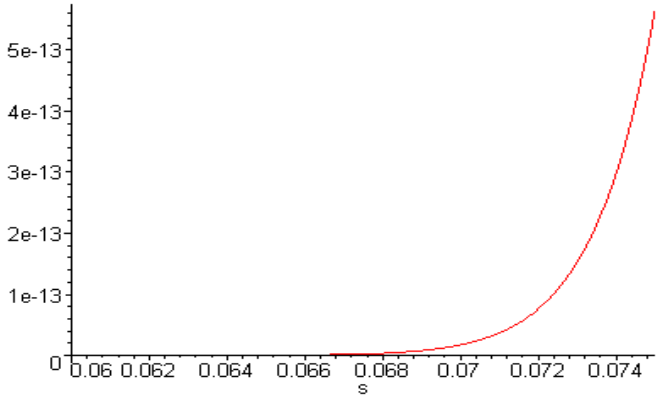

Figure 5: The graph of $\sigma \mapsto 2\sqrt{\frac{2}{\pi}}\sigma \exp(-\frac{1}{8\sigma^2}) + \mathrm{erf}(\frac{1}{2\sqrt{2}\sigma}) - 1$

Another property, which confirms the precedent conclusion, is that the inequation $2\sqrt{\frac{2}{\pi}}\sigma \exp(-\frac{1}{8\sigma^2}) + \frac{2}{\sqrt{\pi}} \int_0^{\frac{1}{2\sqrt{2}\sigma}} \exp(-t^2)dt - 1 \geq 0$ is verified for each $\sigma > 0$ (see Fig. 5).

Indeed, if $\Psi(\sigma) = 2\sqrt{\frac{2}{\pi}}\sigma \exp(-\frac{1}{8\sigma^2}) + \frac{2}{\sqrt{\pi}} \int_0^{\frac{1}{2\sqrt{2}\sigma}} \exp(-t^2)dt - 1$, it's easy to see that $\Psi'(\sigma) = 2\sqrt{\frac{2}{\pi}} \exp(-\frac{1}{8\sigma^2}) > 0$. As Ψ is an increasing function and because $\int_0^{+\infty} \exp(-t^2)dt = \frac{\sqrt{\pi}}{2}$ (i.e. $\mathrm{erf}(+\infty) = 1$) we obtain finally $\Psi(\sigma) \geq \lim_{u \to 0_+} \Psi(u) = 0$.

Then, from (19) with $\lambda = 1$, we see that our modification implies always $\Pr(x_n(1) \neq x_n) \leq \frac{1}{2}(1 + \varepsilon)$.

In brief, for $|\varepsilon|$ small, the integration of values x'_n in the estimation process implies always the condition $\Pr(x_n(1) \neq x_n) \leq \frac{1}{2}(1 + \varepsilon)$ without condition on the $N_k(n)$. Moreover, if $\sum_{k=q}^{d} \varepsilon^{2(k-2)} N_k(n) > 1$, we have $\Pr(x_n(1) \neq x_n) < \frac{1}{2}\left(1 + \frac{7}{6}\varepsilon\right) < \frac{1}{2}(1 + \varepsilon)$.

5.3 Convergence

The proof is the same than at § 4.2.

From (17), we can write $\Pr(x_n(1) \neq x_n) \sim \frac{1}{2}(1 + \phi(\varepsilon))$ with

$\phi(\varepsilon) = \frac{1}{\sqrt{2\pi}} \left[(1 + \varepsilon) \int_0^{\frac{S'(1) - m(0)}{\sigma}} \exp(-\frac{t^2}{2})dt - (1 - \varepsilon) \int_0^{-\frac{S'(0) - m(0)}{\sigma}} \exp(-\frac{t^2}{2})dt \right]$,

$\frac{S'(0)-m(0)}{\sigma} = r - \frac{1}{\sigma}$, $\frac{S'(1)-m(0)}{\sigma} = r + \frac{1}{\sigma}$ and $r = \frac{\sum_{k=q}^{d} N_k(n)\varepsilon^{2k-3}}{\sigma}$.
It's easy to see that ϕ is derivable on $]-1,0[$, and

$$\begin{aligned}\sqrt{2\pi}\phi^{'}(\varepsilon) &= \int_0^{\frac{S'(1)-m(0)}{\sigma}} \exp(-\frac{t^2}{2})dt + \int_0^{-\frac{S'(0)-m(0)}{\sigma}} \exp(-\frac{t^2}{2})dt + \\ &(1+\varepsilon)(\frac{S'(1)-m(0)}{\sigma})' \exp(-\frac{1}{2}(\frac{S'(1)-m(0)}{\sigma})^2) + \\ &(1-\varepsilon)(\frac{S'(0)-m(0)}{\sigma})' \exp(-\frac{1}{2}(\frac{S'(0)-m(0)}{\sigma})^2) \qquad (20)\end{aligned}$$

and after simplification we obtain

$$\begin{aligned}\sqrt{\frac{\pi}{2}}\phi^{'}(\varepsilon) &= \exp(-\frac{r^2}{2})\int_0^{\frac{1}{\sigma}} \cosh(rt)\exp(-\frac{t^2}{2})dt + \\ &\exp(-\frac{1}{2}(r^2+\frac{1}{\sigma^2}))(\frac{\sigma'}{\sigma^2}\left[\sinh(\frac{r}{\sigma}) - \varepsilon\cosh(\frac{r}{\sigma})\right] + \\ &r'\left[\cosh(\frac{r}{\sigma}) - \varepsilon\sinh(\frac{r}{\sigma})\right]). \qquad (21)\end{aligned}$$

Consider the term $\Delta = \frac{\sigma'}{\sigma^2}\left[\sinh(\frac{r}{\sigma}) - \varepsilon\cosh(\frac{r}{\sigma})\right] + r'\left[\cosh(\frac{r}{\sigma}) - \varepsilon\sinh(\frac{r}{\sigma})\right]$. Our aim is to prove that $\Delta > 0$ because in this case the property $\phi^{'}(\varepsilon) > 0$ is proved. We have

$r = \frac{u}{\sigma}$ with $u = \sum_{k=q}^{d} N_k(n)\varepsilon^{2k-3}$, and $r' = \frac{1}{\sigma^2}(u'\sigma - u\sigma') = \frac{u'}{\sigma} - \frac{u\sigma'}{\sigma^2}$, so
$\Delta > 0$ if and only if
$\frac{\sigma'}{\sigma}\left[\sinh(\frac{r}{\sigma}) - \varepsilon\cosh(\frac{r}{\sigma})\right] + (u' - \frac{u\sigma'}{\sigma})\left[\cosh(\frac{r}{\sigma}) - \varepsilon\sinh(\frac{r}{\sigma})\right] =$
$\frac{\sigma'}{\sigma}\left[\sinh(\frac{r}{\sigma}) - \varepsilon\cosh(\frac{r}{\sigma}) - u(\cosh(\frac{r}{\sigma}) - \varepsilon\sinh(\frac{r}{\sigma}))\right] + u'\left[\cosh(\frac{r}{\sigma}) - \varepsilon\sinh(\frac{r}{\sigma})\right]$
> 0.
When $\varepsilon \to 0_-$ we have from (16) $\frac{r}{\sigma} = \frac{u}{\sigma^2} \sim \frac{N_q(n)\varepsilon^{2q-3}}{\frac{1}{4}N_q(n)\varepsilon^{2(q-2)}} = 4\varepsilon$ and
$u' = \sum_{k=q}^{d}(2k-3)N_k(n)\varepsilon^{2k-4}$, so we obtain successively
$\cosh(\frac{r}{\sigma}) = 1 + O(\varepsilon^2)$, $\sinh(\frac{r}{\sigma}) = 4\varepsilon + O(\varepsilon^3)$,
$\cosh(\frac{r}{\sigma}) - \varepsilon\sinh(\frac{r}{\sigma}) = 1 + O(\varepsilon^2), \sinh(\frac{r}{\sigma}) - \varepsilon\cosh(\frac{r}{\sigma}) = 3\varepsilon + O(\varepsilon^3)$,
$u(\cosh(\frac{r}{\sigma}) - \varepsilon\sinh(\frac{r}{\sigma})) = N_q(n)\varepsilon^{2q-3} + O(\varepsilon^{2q-1})$,
$u'(\cosh(\frac{r}{\sigma}) - \varepsilon\sinh(\frac{r}{\sigma})) = (2q-3)N_q(n)\varepsilon^{2q-4} + O(\varepsilon^{2q-2})$.
On the other hand, from $\sigma = \frac{1}{2}(\sum_{k=q}^{d}\varepsilon^{2(k-2)}(1-\varepsilon^{2(k-1)})N_k(n))^{\frac{1}{2}}$, we have
$\sigma' = \frac{1}{2\sigma}\sum_{k=q}^{d}\left[(k-2) - (2k-3)\varepsilon^{2k-2}\right]N_k(n)\varepsilon^{2k-5}$, and finally
$\frac{\sigma'}{\sigma} = \frac{1}{4\sigma^2}[(q-2)N_q(n)\varepsilon^{2q-5} + O(\varepsilon^{2q-3})] = (q-2)\varepsilon^{-1} + O(\varepsilon)$.

It results from this that
$\Delta = [(q-2)\varepsilon^{-1} + O(\varepsilon)][3\varepsilon + O(\varepsilon^3) - N_q(n)\varepsilon^{2q-3} + O(\varepsilon^{2q-1})] +$
$(2q-3)N_q(n)\varepsilon^{2q-4} + O(\varepsilon^{2q-2})$
$= 3(q-2) + O(\varepsilon^2)$.

As $q \geq 3$, we see that $\Delta > 0$ for $|\varepsilon|$ small, and, under this hypothesis, the property $\phi^{'}(\varepsilon) > 0$ is proved .

At iteration k we can write $\Pr(x_n(k) \neq x_n) = \frac{1}{2}(1 + \varepsilon_n(k))$ with $\varepsilon_n(k)$ such that, if $N_q(n), ..., N_d(n)$ are large enough to use the central limit theorem, $\varepsilon_n(k) \sim \phi^k(\varepsilon)$. For $|\varepsilon|$ small we have seen that $\phi :]-1, 0[\rightarrow]-1, 0[$, verifying $\phi' > 0$, is increasing. We also have seen at §5.2 that, under this condition and for each $N_q(n), ..., N_d(n)$, $\Pr(x_n(1) \neq x_n) < \frac{1}{2}(1 + \varepsilon)$ therefore $\phi(\varepsilon) < \varepsilon$. Using the increasing of ϕ we obtain $\phi^{k+1}(\varepsilon) < \phi^k(\varepsilon)$ for each $k \geq 0$,

From (16), we have $\lim_{\varepsilon \to 0_-} \sigma = \lim_{\varepsilon \to -1+} \sigma = 0+$, so $\lim_{\varepsilon \to 0_-} \phi(\varepsilon) = 0$ and $\lim_{\varepsilon \to -1_+} \phi(\varepsilon) = -1$ (because $\int_0^{+\infty} \exp(-\frac{t^2}{2})dt = \sqrt{\frac{\pi}{2}}$). This last property, jointly with the increasing of ϕ, also implies $\phi(\varepsilon) > -1$. Therefore $(\varepsilon_n(k))_k$ is a decreasing sequence of negative real numbers lower bounded by -1, so consequently $l_n = \lim_{k \to +\infty} \varepsilon_n(k)$ exists and $l_n \geq -1$.

In the case where $l_n > -1$, firstly we have $\phi(l_n) < l_n$. But ϕ is a continuous function on $]-1, 0[$, so at point l_n we must have $\phi(l_n) = \phi(\lim_{k \to +\infty} \varepsilon_n(k)) = \lim_{k \to +\infty} \phi(\varepsilon_n(k)) = \lim_{k \to +\infty} \varepsilon_n(k+1) = l_n$ which contradicts the property $\phi(l_n) < l_n$. Therefore the only possibilty is $l_n = -1$ and the convergence is proved.

5.4 Estimation of L

We search now to estimate the length L necessary to realize the condition $\sum_{k=q}^{d} \varepsilon^{2(k-2)} N_k(n) > 1$ under the hypothesis $3 \leq q \leq d << L$.

To translate the precedent condition, we must evaluate the integers $N_k(n)$. An estimation of $N_k(n)$ is given by kO_k where O_k is the number of $k-$omials $Q(X) = 1 + \sum_{1 \leq j \leq k-1} a_{i_j} X^{i_j}$ multiples of $P(X) = \det(T \oplus XI_r)$ and such that $d^\circ(Q) \leq L$. If $P(X)$ is irreductible, each such $Q(X)$ is characterized by the relation $1 + \sum_{1 \leq j \leq k-1} a_{i_j} \alpha^{i_j} = 0$ in the finite field $\mathbf{F}_2[X]/(P(X)) = \mathbf{F}_2(\alpha) \cong \mathbf{F}_{2^r}$ where α is a root of $P(X)$. On the other hand, for each $Q(X) = 1 + \sum_{1 \leq j \leq k-1} a_{i_j} X^{i_j} \in \mathbf{F}_2[X]$, in $\mathbf{F}_2[X]/(P(X))$ we have $\Pr(Q(\alpha) = 0) \approx 2^{-r}$, therefore an estimation of O_k is given by the formula $\binom{L}{k-1} 2^{-r}$.

Consequently, our problem is now to estimate L such that $\sum_{k=q}^{d} k\varepsilon^{2(k-2)} \binom{L}{k-1} 2^{-r} >$

1, and finally

$$\sum_{k=q}^{d} k\varepsilon^{2(k-1)} \binom{L}{k-1} > 2^r \varepsilon^2 \tag{22}$$

A sufficient condition to verify (22) is $q\varepsilon^{2(q-1)}\binom{L}{q-1} > 2^r\varepsilon^2$, and then

$$q\binom{L}{q-1} > 2^r \varepsilon^{-2(q-2)}. \tag{23}$$

When L is large and $q << L$, we can use Stirling's formula $m! \sim m^m e^{-m}(2\pi m)^{\frac{1}{2}}$ to evaluate $\binom{L}{q-1}$. If we denote $n = q-1$,we have $\binom{L}{n} \sim \frac{1}{n!}\frac{L^L e^{-L}(2\pi L)^{\frac{1}{2}}}{(L-n)^{L-n}e^{-(L-n)}(2\pi(L-n))^{\frac{1}{2}}}$
$= \frac{1}{n!}\left(\frac{L}{L-n}\right)^{L+\frac{1}{2}}\left(\frac{L-n}{e}\right)^n$, and using $\left(\frac{L}{L-n}\right)^{L+\frac{1}{2}} = \left(1+\frac{n}{L-n}\right)^{L+\frac{1}{2}} =$
$\exp((L+\frac{1}{2})\ln(1+\frac{n}{L-n})) \sim \exp((L+\frac{1}{2})\frac{n}{L-n}) = \exp(n\frac{1+\frac{1}{2L}}{1-\frac{n}{L}}) \sim e^n$, we obtain finally $\binom{L}{q-1} \sim \frac{1}{(q-1)!}(L-(q-1))^{q-1}$ so $q\binom{L}{q-1} \sim \frac{q}{(q-1)!}(L-(q-1))^{q-1}$.

Translating the condition (23), we obtain $L-(q-1) > (\frac{1}{q}(q-1)!)^{\frac{1}{q-1}} 2^{\frac{r}{q-1}} \varepsilon^{-2\frac{q-2}{q-1}}$, and for sufficient final condition we may assume $L > ((q-2)!)^{\frac{1}{q-1}} 2^{\frac{r}{q-1}} \varepsilon^{-2}$.

Remark that this length is an estimation of the number of bits of keystream to obtain, from the iterative algorithm, the value x_n. But, as each k-omial $Q(X)$ generating one of $N_k(n)$ relations is also usuable for all the others x_m, i.e. generates one of $N_k(m)$ relations verifying $m \neq n$, an estimation of length of keystream, sufficient to obtain the initialisation of the LFSR of length r, is also

$$L > ((q-2)!)^{\frac{1}{q-1}} 2^{\frac{r}{q-1}} \varepsilon^{-2}. \tag{24}$$

Information theory also gives us the possibility to compute a lower bound for L. The information quantity on x_n, given by one keystream bit $x'_n = x_n \oplus e_n$, is $1 - H(p)$ with $H(p) = -\frac{1}{2}\left[(1+\varepsilon)\log_2(\frac{1}{2}(1+\varepsilon)) + (1-\varepsilon)\log_2(\frac{1}{2}(1-\varepsilon))\right]$
$= -\frac{1}{2}\left[(1+\varepsilon)(\varepsilon - \frac{1}{2}\varepsilon^2 + O(\varepsilon^3) - 1) + (1-\varepsilon)\left(-\varepsilon - \frac{1}{2}\varepsilon^2 + O(\varepsilon^3) - 1\right)\right]$
$= 1 - \frac{1}{2}\varepsilon^2 + O(\varepsilon^3)$. So, for $|\varepsilon|$ small, $1 - H(p) \sim \frac{1}{2}\varepsilon^2$. So, the information quantity given by L bits of keystream is $L(1-H(p)) \sim \frac{L}{2}\varepsilon^2$ and we obtain a lower bound for L when $L(1-H(p)) > r$, i.e. $L > \frac{r}{1-H(p)} \sim \frac{2r}{\varepsilon^2}$.

We see that, if we use the lower bound (24) with $q = r+1$, we obtain $L > ((r-1)!)^{\frac{1}{r}} 2\varepsilon^{-2} \approx \frac{1}{e}\frac{2r}{\varepsilon^2}$ (because $(r!)^{\frac{1}{r}} \sim \frac{r}{e}$ for $r \to +\infty$) which is of the same order $O(\frac{r}{\varepsilon^2})$ than the bound from information theory.

5.5 Some experimental results

The results of simulation presented here are just given to illustrate theorical topics developped precedently. They absolutely don't constitute an experimental study of the algorithms which stays to make subsequently. In these simulations we compare the behavior of the improved algorithm with trinomials relations $N_3(n)$ (column IT), and the improved algorithm with trinomials-quadrinomials

relations $N_3(n), N_4(n)$ (column ITQ). For the LFSR of characteristic polynomial $P(X) = 1 \oplus X \oplus X^{63}$ we compute, for 100 random initializations of this register, the minimal length expectation L necessary to converge from x'_n to x_n for each $n \in [1, L]$, for $|\varepsilon| = 0.5, 0.4, 0.3, 0.2, 0.1$.

	IT	**ITQ**
0.5	712	640
0.4	1144	1008
0.3	2096	1728
0.2	8816	5640
0.1	41048	28128

6 Conclusion

In this paper, we have presented an asymptotic analysis and an improvement of fast iterative correlation attack algorithms. This improvement is theorically analyzed and the new convergence condition clearly shows the gain obtained. Experimental illustration is given, but complementary experimental further work is necessary to validate the probabilistic model developped here.

References

[1] A. Canteaut and M. Trabbia, Improved fast correlations attacks using parity-check equations of weights 4 and 5, In *Advances in Cryptology - EUROCRYPT'00,* Vol. 1807 of *Lecture Notes in Computer Science,* pp. 573-588, Springer Verlag , 2000.

[2] V. V. Chepyzhof, T. Johansson and B. Smeets, A simple algorithm for fast correlation attacks on stream ciphers, in *Fast Software Encryption - FSE'00,* Vol. 1978 of *Lecture Notes in Computer Science,* Springer Verlag, 2000.

[3] P. Chose, A. Joux and M. Mitton, Fast correlation attacks: an algorithmic point of vue, in *Advances in Cryptology - EUROCRYPT 2002,* Vol. 2332 of *Lecture Notes in Computer Science,* pp. 209-221, Springer Verlag, 2002.

[4] T. Johansson and F. Jönsson, Fast correlation attacks through reconstruction of linear polynomials, in *Advances in Cryptology - CRYPTO'00,* Vol. 1880 of *Lectures Notes in Computer Science,* pp. 300-315, Springer Verlag, 2000.

[5] W. Meier and O. Staffelbach, Fast correlation attacks on certain stream ciphers, *Journal of Cryptology,* Vol. 1(?), pp.159-176, 1989.

[6] M. Mihaljevic, M. P. C. Fossorier and H. Imai, A low-complexity and high-performance algorithm for fast correlation attacks, in *Fast Software Encryption - FSE'00,* pp.196-212, Springer Verlag, 2000.

[7] M. Mihaljevic, M. P. C. Fossorier and H. Imai, Fast correlation attack algorithm with list decoding and an application, in *Fast Software Encryption - FSE'01,* pp.208-222, Springer Verlag, 2001.

[8] W. T. Penzorhn and G. J. Kuhn, Computation of low-weight parity-check for correlation attacks on stream ciphers, in *Cryptology and coding - 5th IMA Conference,* Vol. 1025 of *Lecture Notes in Computer Science,* pp. 74-83, Springer Verlag, 1995.

[9] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, in *IEEE Trans. on Information Theory,* Vol. IT-30, pp. 776-780, 1984.

[10] T. Siegenthaler, Decrypting a class of stream ciphers using cipertext only, in *IEEE Trans. on Comput.,* Vol. C-34, pp.81-85, 1985.