様式 C-19

科学研究費補助金研究成果報告書

平成２１年　４月２３日現在

研究種目：若手研究（B）
研究期間：2007～2008
課題番号：19700009
研究課題名（和文）ストリーム暗号用乱数生成器の安全性評価に関する研究

研究課題名（英文）ON AN EVALUATION OF PSEUDO-RANDOM NUMBER GENERATOR FOR STREAM CIPHER

研究代表者
福田洋治（FUKUTA YOUJI）
愛知教育大学・教育学部・講師
研究者番号：80402642

研究成果の概要：高速相関攻撃(FCA)は，擬似乱数生成器の構造を既知と仮定して，平文系列と暗号文系列の対から得られる擬似乱数系列から，擬似乱数生成器の内部状態を再構成するという既知平文攻撃である．FCA の議論では，一般に，攻撃対象として，非線形コンバイナ型乱数生成器(NCG)と呼ばれる複数の 2 元の線形フィードバックシフトレジスタ(LFSR)と非線形ブール関数から構成された擬似乱数生成器が想定されている．本研究では，LFSR の出力系列を推定する際に,過去に推定したビットの情報を用いてパリティ検査式の集合を動的に構成し，それを用いてビットを推定するという FCA の手法を提案し，攻撃の成功確率，攻撃に要する計算量，メモリサイズの式を導出して，提案手法が既存手法に比べて LFSR の出力系列を高い精度で推定できることを示した.

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	1,300,000	0	1,300,000
２００８年度	900,000	0	900,000
年度			
年度			
年度			
総　計	2,200,000	0	2,200,000

研究分野：　総合領域
科研費の分科・細目：　情報学・情報学基礎
キーワード：　暗号系

１．研究開始当初の背景

ストリーム暗号は，秘密鍵および公開 IV で決まるシードから擬似乱数系列を生成し，平文系列とシンボル毎に排他的論理和することで平文系列の情報を秘匿する対称鍵暗号の１つである.ストリーム暗号の安全性は，擬似乱数生成器の安全性に根拠が置かれており，擬似乱数生成器の出力系列の統計的特性や，各種攻撃に対する擬似乱数生成器の耐性が議論されている.

擬似乱数生成器に対する攻撃は，擬似乱数生成器の構造(内部状態，遷移関数，フィルタ関数)と出力系列を既知と仮定した攻撃として，識別攻撃や出力予測，鍵復元攻撃に大きく分類できる．高速相関攻撃(Fast Correlation Attack; FCA)は，鍵復元攻撃の 1 つであり，擬似乱数生成器の構造を既知と仮定し，擬似乱数生成器の出力系列と内部状態の相関関係および遷移関数の線形性から，線形符号の復号法を利用して内部状態を再

構成する攻撃である.

FCA では，一般に，攻撃対象として，非線形コンバイナ型乱数生成器(Nonlinear Combiner Generator; NCG)と呼ばれる，GF(2)上の複数の線形フィードバックシフトレジスタ(Linear Feedback Shift Register; LFSR)と非線形ブール関数から構成される擬似乱数生成器が想定されている(図 1).

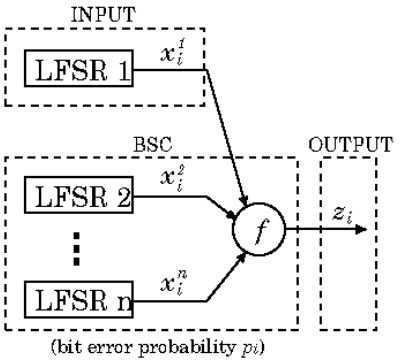

図 1 高速相関攻撃のモデル

FCA は，NCG のような，内部状態と遷移関数の部分に LFSR を採用している擬似乱数生成器に適用される攻撃であり，LFSR を駆動するクロックを制御する，GF(2^m)上の LFSR を用いる，フィルタ関数の出力を間引くなどの仕組みを導入することで攻撃が困難になるが，攻撃性能が向上した場合はこの限りではない.

近年では，線形符号の復号法を利用して LFSR の初期値を構成する改良手法が提案されており，攻撃が成立するときの NCG の出力系列の長さが可能な限り短く，計算量やメモリサイズが少なくなるように，性能向上が追求されており，その中で安全性を確保するための設計基準について議論されている.

２．研究の目的

本研究の目的は，NCG およびそれに関連する擬似乱数生成器の解析法の性能を追求することで，既存の擬似乱数生成器の強度を維持するための条件，脆弱性とその対策を明らかにし，既存の擬似乱数生成器の運用や新たな擬似乱数生成器の開発に役立つ情報を得ることである.

擬似乱数生成器の予測不可能性の解析アプローチの１つである FCA に関して，次の 2 点に取り組んだ.

(1)NCG の FCA におけるパリティ検査式構成アルゴリズム，LFSR の初期値再構成アルゴリズムの効率化

(2)NCG と同様の構造を持つ乱数生成器の予測不可能性の解析

上記(1)では，NCG の FCA において，NCG の出力系列の情報(NCG の出力系列に含まれる LFSR の出力系列の情報)を有効に利用すること，LFSR の初期値の推定確度を利用することに注目して，LFSR の初期値を再構成するときに用いられるパリティ検査式を構成するアルゴリズムと，LFSR の初期値を再構成するアルゴリズムの効率化を行う.

上記(2)では，上記(1)で得られたアルゴリズムに注目して，NCG と同様の構造を含む擬似乱数生成器の中で，LFSR を駆動するクロックを制御する，フィルタ関数の出力を間引く乱数生成器に対する FCA の適用可能性について検討する.

３．研究の方法

本研究の 2 つの課題に対し，次のような方法で取り組む.

(1)NCG の FCA におけるパリティ検査式構成アルゴリズムと LFSR の初期値再構成アルゴリズムの効率化

①パリティ検査式の項数，個数と LFSR の初期値推定誤り確率との関係を明らかにして，LFSR の出力系列の情報を限界まで利用できるパリティ検査式の構成方法を導出する.

②LFSR の出力系列の１ビットが高い確度で得られたとき，そのビットを利用して新たに構成できるパリティ検査式について明らかにして，LFSR の初期値再構成の方法を導出する.

③既存の FCA との性能の比較を行うために主要な FCA を実装して，現実的なストリーム暗号の擬似乱数生成器の運用を想定して，評価の基準となるパラメータの条件を設定して，シミュレーション実験と理論値の計算により提案手法の性能を評価する.

(2)NCG と同様の構造を持つ乱数生成器の予測不可能性の解析

①NCG と同様の構造を持つ既存の擬似乱数生成器の中から，LFSR を駆動するクロックを制御する，フィルタ関数の出力を間引く乱数生成器を選択して，検討対象の擬似乱数生成器のリストを作る.

②検討対象の擬似乱数生成器に対し，提案手法の適用可能性を検討し，攻撃および前提条件等を明らかにして，シミュレーション実験，理論的解析を行う.

４．研究成果

(1)パリティ検査式を動的に構成する高速相関攻撃

①パリティ検査式の動的構成

推定済みのビットの情報を用いて，任意の 1 ビットで直交する，3 項のパリティ検査式の集合の動的な構成について示し，これが攻撃の性能にどのように関係するかを述べる.

まず，前処理において，LFSR の特性多項式を用いて構成される状態遷移行列 A から，パリティ検査式の基本集合 S_1, S_2 を構成する(図 2).

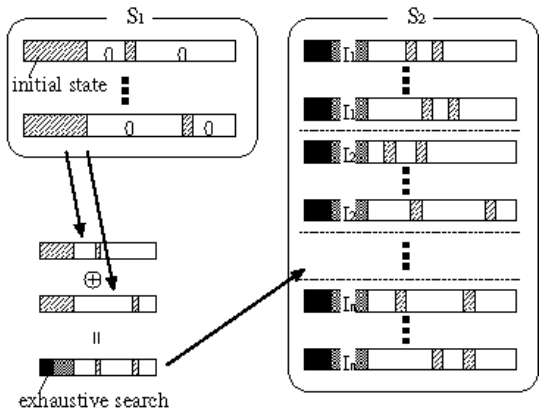

図 2 パリティ検査式の基本集合 S_1, S_2 の構成

集合 S_1 のパリティ検査式は，A^k の第 1 行ベクトル A_1^k として，次のように構成する．

$$x_k \oplus A_1^{k-L} x_0 = 0, L < k \le N.$$

集合 S_2 のパリティ検査式は，集合 S_1 から 2 つの式を抽出して，次のように構成する．

$$(x_m \oplus A_1^{m-L} x_0) \oplus (x_n \oplus A_1^{n-L} x_0) = 0,$$
$$m \ne n, L < \{m, n\} \le N.$$

次に，LFSR の初期値を再構成することを試みる主処理において，推定済みのビットの情報を用いて推定対象の 1 ビットで直交する 3 項のパリティ検査式の集合を構成する(図 3)．

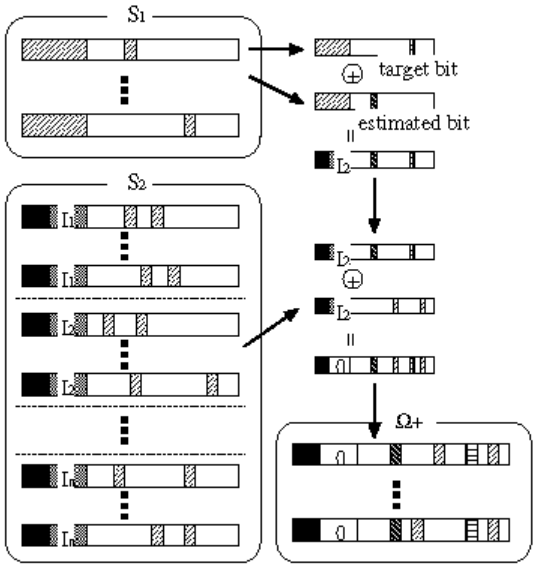

図 3 パリティ検査式の集合 Ω^+ の構成

例えば，推定対象の 1 ビットを $x_i, L < i$，推定済みの 1 ビットを $x_j, L < j$ とすると，集合 S_1 から 2 つの式を抽出して，次の式が構成できる．

$$(x_i \oplus A_1^{i-L} x_0) \oplus (x_j \oplus A_1^{j-L} x_0) = 0.$$

$A_1^{i-L} \oplus A_1^{j-L}$ で得られるベクトルの，$x_l, B < l \le L$ の位置のビットパターンに一致する式を集合 S_2 から抽出して，上記の式を排他的論理和することで，次のパリティ検査式の集合 Ω_i^+ を構成できる．

$$(x_i \oplus A_1^{i-L} x_0) \oplus (x_j \oplus A_1^{j-L} x_0)$$
$$\oplus (x_m \oplus A_1^{m-L} x_0) \oplus (x_n \oplus A_1^{n-L} x_0) = 0.$$

$A_1^{i-L} \oplus A_1^{j-L} \oplus A_1^{m-L} \oplus A_1^{n-L}$ で得られるベクトルの，$x_l, B < l \le L$ の位置のビットは全て 0 であり，$x_l, 1 \le l \le B$ の位置のビットおよび x_j は推定済みのビットとして扱えることから，集合 Ω_i^+ の式はビット x_j で直交する 3 項のパリティ検査式となる．

集合 S_1 から，推定対象のビット x_j から決まる式 $L_1 = x_i \oplus A_1^{i-L} x_0$，推定済みのビット x_j から決まる式 $L_2 = x_j \oplus A_1^{j-L} x_0$ を取り出し，2 つの式を排他的論理和し，$A_1^{i-L} \oplus A_1^{j-L}$ で得られるベクトルの $x_l, B < l \le L$ の位置のビットパターン P を容易に計算できる．集合 S_2 の式は，$A_1^{m-L} \oplus A_1^{n-L}$ で得られるベクトルの $x_i, B < i \le L$ の位置のビットパターンをインデックス $I_l, 1 \le l \le n = 2^{L-B}$ として，前処理で事前に整理しておくことができ，集合 S_1 の式から得られたビットパターン P をインデックスに持つ式の集合 $S_2^{I_P}$ が無視できる計算量で得られる．ビット x_j で直交する 3 項のパリティ検査式の集合 Ω_i^+ は，式 $L_1 \oplus L_2$ と集合 $S_2^{I_P}$ の式を排他的論理和して得られるが，集合 Ω_i^+ の式のパリティ検査和は，式 $L_1 \oplus L_2$ のパリティ検査和，集合 $S_2^{I_P}$ の式のパリティ検査和を個別に計算して，適宜足し合わすことで得られる．

②攻撃のアルゴリズム

LFSR の初期値を推定する際に，推定済みのビットの情報を用いて 3 項のパリティ検査式の集合を動的に構成し，それを用いて他のビットを推定する，APP one-step decoding に基づく FCA のアルゴリズムを示す．

Input

・NCG の出力ビット列 $[z_i]_{i=1}^N$ (長さ N，BSC の誤り確率 p)，
・LFSR の特性多項式 $f(x)$ (段数 L)，
・LFSR の初期値の全数探索するビット数 B，
・LFSR の出力ビット列の推定ビット数 D，
・LFSR の出力ビットの推定で用いる値 t，閾値 T．

Pre-processing

(PP-1)LFSR の状態遷移行列 A から，次の式を構成して集合 S_1 に含める．A は LFSR の特性多項式から構成され，A_1^k は A^k の第 1 行ベ

クトルとする．集合S_1の式はkをインデックスとして取り出せるようにしておく．

$$x_k \oplus A_1^{k-L} x_0 = 0, L < k \le N.$$

(PP-2)集合S_1から 2 つの式を取り出して，次の式を構成して集合S_2に含める．集合S_2の式は，$A_1^{m-L} \oplus A_1^{n-L}$で得られるベクトルの，$x_l, B < l \le L$の位置のビットパターンをインデックスとして取り出せるようにしておく．

$$(x_m \oplus A_1^{m-L} x_0) \oplus (x_n \oplus A_1^{n-L} x_0) = 0,$$
$$m \ne n, L < \{m,n\} \le N.$$

Processing

(P-1)LFSR の初期値のうちBビット$(\hat{x}_1, \hat{x}_2, \ldots, \hat{x}_B)$の値を重複なく設定する．全てのパターンを設定した場合 Output の a)へ．

(P-2)推定対象のDビットのうち，全数探索で求めるBビットと推定済みのビット$\hat{x}_j \in \alpha$（推定済みのビットの集合をαとする）を除いた，$D - B - |\alpha|$ビットのそれぞれについて，値を推定するためのパリティ検査式の集合を次のように構成する．

1)ビット$\hat{x}_i, B < i \le L$を推定する場合，そのビットの位置を 1，その他を 0 とした，L次のベクトルuを構成する．

$$u = [0, \ldots, 0, u_{B+1}, \ldots, u_L],$$
$$if\ k = i\ then\ u_k = 1\ else\ u_k = 0$$

また，ビット$\hat{x}_i, L < i \le D$を推定する場合，そのビット位置をインデックスとして，集合S_1から式を取り出して次の式C_uを構成する．

$$C_u = x_i \oplus A_1^{i-L} x_0.$$

2)推定済みのビット$\hat{x}_j \in \alpha, B < j \le L$の場合，推定済みのビット位置を 1，その他を 0 とした，L次のベクトルvを重複なく設定する．

$$v = [0, \ldots, 0, v_{B+1}, \ldots, v_L],$$
$$if\ k = j\ then\ v_k = 1\ else\ v_k = 0$$

推定済みのビット$\hat{x}_j \in \alpha, L < j \le D$の場合，ビット位置をインデックスとして，集合$S_1$$S_1$から式を取り出して次の式$C_v$を構成する．

$$C_v = \sum_{j \in \alpha, L < j \le D} (x_j \oplus A_1^{j-L} x_0).$$

3)ビット$\hat{x}_i, B < i \le L$を推定する場合，$u \oplus v \oplus \sum_{j \in \alpha, L < j \le D} A_1^{j-L}$.で得られるベクトルの，$x_l, B < l \le L$の位置のビットパターンをインデックスとして，集合$S_2$から式を取り出し，次の式を構成して集合$\Omega_i^+$に含める．

$$(x_m \oplus A_1^{m-L} x_0) \oplus (x_n \oplus A_1^{n-L} x_0) \oplus C_v = 0.$$

また，ビット$\hat{x}_i, L < i \le D$を推定する場合，$A_1^{i-L} \oplus v \oplus \sum_{j \in \alpha, L < j \le D} A_1^{j-L}$.で得られるベクトルの，$x_l, B < l \le L$の位置のビットパターンをインデックスとして，集合$S_2$から式を取り出し，次の式を構成して集合$\Omega_i^+$に含める．

$$(x_m \oplus A_1^{m-L} x_0) \oplus (x_n \oplus A_1^{n-L} x_0) \oplus C_u \oplus C_v = 0.$$

推定済みのビット$\hat{x}_j \in \alpha$のパターンを重複なく選択して，全てのパターンを選択していない場合は 2)へ．

(P-3)推定するビット$\hat{x}_i, B < i \le D$について，集合Ω_i^+の式に，推定済みのビット$\hat{x}_j \in \alpha$および NCG の出力ビット列$[z_i]_{i=1}^N$を代入，パリティ検査和を計算して，パリティ検査和が 0 になる個数s_iをカウントする．そして，$|s_i / |\Omega_i^+| - 1/2|$が最大となる$\hat{x}_i$の値を，次のように推定する．

$$\hat{x}_i = \begin{cases} z_i \oplus 1, & s_i / |\Omega_i^+| < 1/2 \\ z_i, & s_i / |\Omega_i^+| > 1/2 \end{cases}$$

値が得られたビットは，推定済みのビットとしてαに追加する．推定済みのビットが増加して，その個数がt未満の場合は，(P-2)へ，それ以外の場合は，残りのビットについて，$|s_i / |\Omega_i^+| - 1/2|$の大きなビットを$L - B - t$個抽出し，上記の方法で値を推定して，LFSR の初期値$\hat{x}_0$を再構成する．

(P-4)初期値$\hat{x}_0$とする LFSR の出力ビット列$[\hat{x}_i]_{i=1}^N$を生成して，NCG の出力ビット列$[z_i]_{i=1}^N$との相関値を計算し，閾値Tによりその正当性を確認する．正しい初期値が得られた場合は，Output の b)へ，それ以外の場合は(P-1)へ．

Output

a)LFSR の初期値が得られなかったものとし処理を終了する．

b)LFSR の初期値が得られたものとし$\hat{x}_0$を出力して終了する．

提案した FCA では，LFSR の出力系列を推定する過程で，推定済みのビットがt個のとき，構成されるパリティ検査式の個数が2^t倍に増加し，NCG の出力系列が有効利用され，ビット推定の性能が大きく向上する．ビット推定の性能は，全数探索するビットの個数Bに注目すると，それをtビット増やすのと同等

の効果が，NCG の出力系列の長さ N に注目すると，それを $2^{t/2}$ 倍に増やすのと同等の効果がある．

(2)攻撃の成功確率，計算量，メモリサイズの解析

①攻撃の成功確率

提案手法により，正しく LFSR の初期値が再構成される確率 P_{corr} は，次の式で書ける．

$$P_{corr} = \prod_{k=0}^{t-1}(1-p_{err(k)})(1-p_{err(t)})^{L-B-t}$$

$$\approx \prod_{k=0}^{t-1}(1-p_{err(k)}), L-B \geq t >> 1.$$

$p_{err(k)}$ は，k ビットを推定した後で，他の 1 ビットを推定したとき，それが誤りである確率を表しており，次の式で書ける．

$$p_{err(k)} =$$

$$\frac{\Pr^2(e_i=0)}{\sum_{s=0}^{\alpha(k)}\Pr_{(k)}(s_i=s)}\sum_{s=0}^{\alpha(k)}\Pr_{(k)}(s_i=s\,|\,e_i=0)$$

$$+\frac{\Pr^2(e_i=1)}{\sum_{s=\beta(k)}^{|\Omega^{+k}|}\Pr_{(k)}(s_i=s)}\sum_{s=\beta(k)}^{|\Omega^{+k}|}\Pr_{(k)}(s_i=s\,|\,e_i=1),$$

$$\sum_{s=0}^{\alpha(k)}\Pr_{(k)}(s_i=s) \geq (1-p)\eta/(D-B-k),$$

$$\sum_{s=\beta(k)}^{|\Omega^{+k}|}\Pr_{(k)}(s_i=s) \geq p\eta/(D-B-k),$$

$$if\ k \leq t\ \ then\ \ \eta=1\ else\ \ \eta=L-B-t.$$

$\Pr_{(k)}(s_i=s\,|\,e_i=0)$，$\Pr_{(k)}(s_i=s\,|\,e_i=1)$，$\Pr_{(k)}(s_i=s)$ はそれぞれ次の式で書ける．k は推定済みビットの個数とする．

$$\Pr_{(k)}(s_i=s\,|\,e_i=0)=\binom{|\Omega^{+k}|}{s}(1-p_w)^s p_w^{|\Omega^{+k}|-s},$$

$$\Pr_{(k)}(s_i=s\,|\,e_i=1)=\binom{|\Omega^{+k}|}{s}p_w^{\,s}(1-p_w)^{|\Omega^{+k}|-s},$$

$$\Pr_{(k)}(s_i=s)=\Pr(e_i=0)\Pr_{(k)}(s_i=s\,|\,e_i=0)$$

$$+\Pr(e_i=1)\Pr_{(k)}(s_i=s\,|\,e_i=1).$$

推定済みのビットを用いてパリティ検査式の集合を構成し，それを用いて他のビットを推定することを繰り返す．攻撃の成功確率 P_{corr} の式において，ビット推定を続ける度に $p_{err(k)}$ が大きく減少することから，$t>>1$ のとき $\prod_{k=0}^{t-1}(1-p_{err(k)})$ の値が支配的になる．従来の攻撃は推定するビットの個数 $L-B$ に依存して成功確率が低下していたが，提案手法はそれに依存しない．

②攻撃に要する計算量

提案した手法において，パリティ検査式の基本集合 S_1, S_2 を構成する際の計算量 Com_{PP} は，排他的論理和の式の演算回数として評価すると，次の式のように書ける．

$$Com_{PP} \approx N^2$$

集合 S_1 のパリティ検査式は $N-L \approx N$ 個あり，集合 S_2 のパリティ検査式は集合 S_1 から異なる 2 つの式を抽出して構成され，それを構成するときの計算量は ${}_{N-L}C_2 \approx {}_N C_2 \approx N^2, |S_1| << |S_2|$ となる．

次に，LFSR の初期値を再構成する際の計算量 Com_P は，排他的論理和の式の演算回数として評価すると次の式のように書ける．

$$Com_P \approx$$

$$2^B((D-B)\log_2(2^{B-L+t}{}_N C_2)+N)$$

提案した FCA では，LFSR の出力系列の $D-B$ ビットの推定を行い，1 ビットを推定する際には $|\Omega^{+t}| = 2^{B-L+t}{}_N C_2$ 個のパリティ検査和の計算を行う．パリティ検査和の計算は，Chose らが提案した Walsh 変換による手法を用いることで，計算 $|\Omega^{+t}|$ 回を $\log_2|\Omega^{+t}|$ 回に低減できる．LFSR の出力系列の $D-B$ ビットのうち，推定の確度の高いビットを $L-B$ ビット抽出，それから LFSR の初期値を再構成して，LFSR を N 回動作させて出力系列を生成，NCG の出力系列との相関値を計算して，初期値の正当性を確認する．LFSR の初期値のうち B ビットに重複無くビットを設定しながら，以上の処理を 2^B 回繰り返すことで，攻撃が実施されることから，上記のような式が得られる．

③攻撃に要するメモリサイズ

我々の提案した FCA において，攻撃を実行する際に必要となるメモリサイズ(Byte)は，次の式のように書ける．

$$Mem \approx \binom{N}{2}(L+2)\lceil \log_{256} N \rceil.$$

攻撃を実行する際に，パリティ検査式を動的に構成するための集合 S_1, S_2 を保持する必要があり，そのために主にメモリを消費する．$|S_1| << |S_2|$ であり，集合 S_2 のパリティ検査式は ${}_N C_2$ 個，1 つのパリティ検査式の情報は多くとも $L+2$ 個の項の位置を保持できればよいので，上記のような式が得られる．

④性能の評価

現在最も性能が優れているとされる Chose らの手法と提案手法に関して，成功確率，計算量，メモリサイズを比較する．

まず，シミュレーション実験により，既存手法と提案手法において，攻撃の成功率を求

め，図 4 のような結果が得られた．グラフの横軸は BSC の誤り確率，グラフの縦軸は LFSR の初期値を正しく推定できた成功率である．攻撃の試行回数は 1,000 回，対象の LFSR は次のような特性多項式とする．

$$f(x) = 1 + x + x^3 + x^5 + x^9 + x^{11} + x^{12} + x^{17} + x^{19} + x^{21} + x^{25} + x^{27} + x^{29} + x^{32} + x^{33} + x^{38} + x^{40}$$

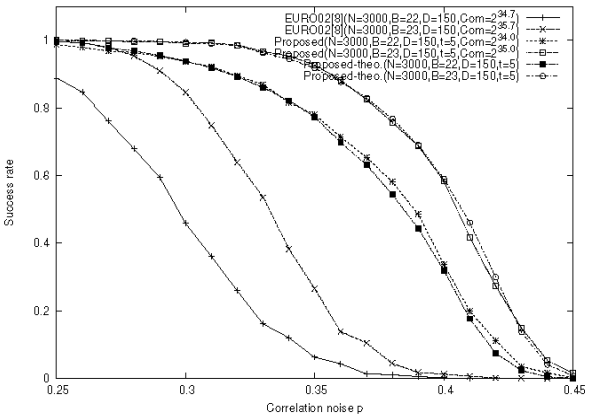

図 4 実験から得た攻撃の成功率と理論式から得た攻撃の成功確率

NCG の出力系列の長さを N，推定対象のビットの個数を D，推定対象のビットのうち全数探索するビットの個数を B，前処理を除いた攻撃の計算量を Com，提案手法で用いる推定済みビットの個数の上限を t とする．パラメータ N=3,000,B=22,D=150 では提案手法がリミットノイズで約 0.05，成功率で最大 0.72 上回り，N=3000,B=23,D=150 では提案手法がリミットノイズで約 0.06，成功率で最大 0.74 上回っている．また，提案手法の攻撃の成功確率の式の計算結果と，実験から得られた提案手法の攻撃の成功率が一致することを確認した．

ストリーム暗号用の擬似乱数生成器に対する攻撃は，擬似乱数生成器の構造に依存しており，本研究で注目した FCA においても，LFSR を駆動するクロックを制御する，フィルタ関数の出力を間引く，GF(2^m) 上の LFSR を使用するなどの仕組みを有する擬似乱数生成器に対しては，適用が困難である．現在，このような擬似乱数生成器への FCA の適用はオープン問題となっているが，Shrinking generator や Cascade generator，LILI128 のような構造が単純なものについては，FCA の適用が可能と考えられる．この検討は今後の課題とする．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔学会発表〕（計　２件）
①福田 洋治，白石 善明，森井 昌克，``動的に構成するパリティ検査式を用いた高速相関攻撃について，''2008 年暗号と情報セキュリティシンポジウム(SCIS2008)予稿集，2A3-3，2008 年 1 月，宮崎市．
②福田 洋治，白石 善明，毛利 公美，森井 昌克，``パリティ検査式を動的に構成する高速相関攻撃の解析，''電子情報通信学会 技術研究報告(ISEC 研究会)，ISEC2008-111，vol.108，no.473，pp.57-64，2009 年 3 月，函館市．

６．研究組織
(1)研究代表者
福田洋治（FUKUTA YOUJI）
愛知教育大学・教育学部・講師
研究者番号：80402642