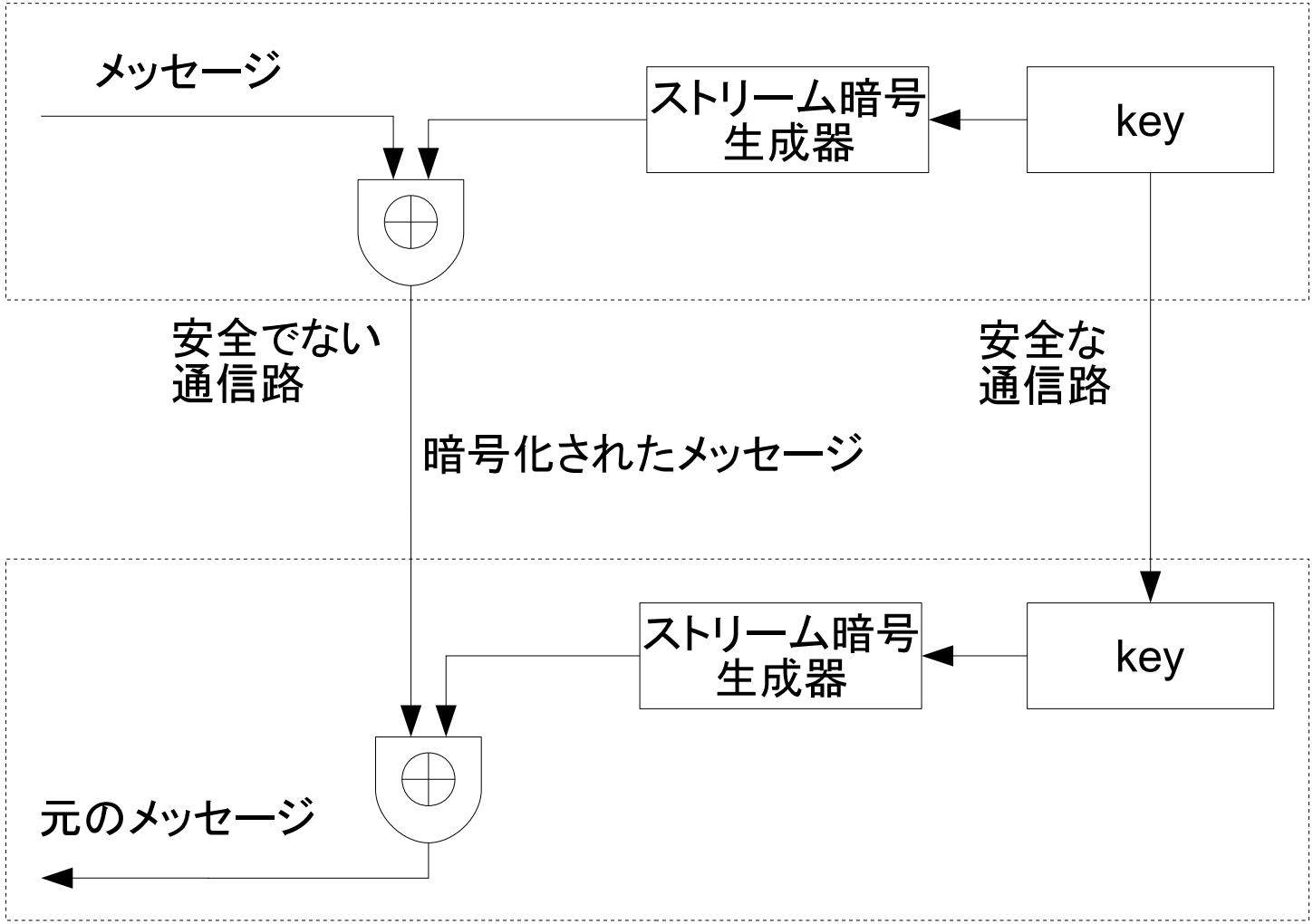
準群フィルターの利用により周期と分布に保証のある高速ストリーム暗号

松本眞 (広島大学)
斎藤睦夫 (広島大学)
西村拓士 (山形大学)
萩田真理子 (お茶の水大学)

2007年9月17日　JSIAM 2007

This study is supported in part by
JSPS Core-to-Core Program 18005

0. （同期式）ストリーム暗号



1. イントロダクション

ここでは、新しいタイプのストリーム暗号を提案する。

(1) 長い周期と高次元均等分布性をもつ LFSR (Mother Generator)

(2) 準群に基づいた、メモリ付きフィルター(準群フィルター)

の結合によるストリーム暗号。

1. イントロダクション

ここでは、新しいタイプのストリーム暗号を提案する。

(1) 長い周期と高次元均等分布性をもつ LFSR (Mother Generator)

(2) 準群に基づいた、メモリ付きフィルター(準群フィルター)

の結合によるストリーム暗号。
そのようなストリーム暗号は全体としての長周期と高次元均等分布を保証することを示す。

1. イントロダクション

ここでは、新しいタイプのストリーム暗号を提案する。

(1) 長い周期と高次元均等分布性をもつ LFSR (Mother Generator)

(2) 準群に基づいた、メモリ付きフィルター(準群フィルター)

の結合によるストリーム暗号。
そのようなストリーム暗号は全体としての長周期と高次元均等分布を保証することを示す。

最後に具体的な実例として CryptMT ver. 3 を提案する。これは eSTREAM phase 3 候補の中で最も速いストリーム暗号のひとつである。

2. Combined Generator

ここでは、いわゆるCombined Generatorを扱う。つまり、

- 疑似乱数生成器としての無入力オートマトン
  (Mother Generator, MG)
- その疑似乱数をより安全な数列に変換する
  入力付きオートマトン (フィルター, F)

この二つを結合したオートマトンである。

2-1. 無入力オートマトン

無入力有限状態オートマトン M(M はマザー)は、以下の構成要素から成る。

- 状態の集合 S_M
- 状態遷移関数 $f_M : S_M \to S_M$
- 出力記号の集合 O_M
- 出力関数 $o_M : S_M \to O_M$

2-1. 無入力オートマトン

無入力有限状態オートマトン M(M はマザー)は、以下の構成要素から成る。

- 状態の集合 S_M
- 状態遷移関数 $f_M : S_M \to S_M$
- 出力記号の集合 O_M
- 出力関数 $o_M : S_M \to O_M$

与えられた初期状態 s_0 に対して、M は次の漸化式によって状態を変える。

$$s_n := f_M(s_{n-1}) \quad (n = 1, 2, 3, \ldots)$$

そして次の出力列を生成する。

$$o_M(s_0), o_M(s_1), o_M(s_2), \ldots \in O_M$$

2-2. 入力付きオートマトン

入力付き有限状態オートマトンF(Fはフィルター)は、以下の構成要素から成る。

- 状態の集合 S_F
- 入力記号の集合 I_F
- 状態遷移関数 $f_F : I_F \times S_F \to S_F$
- 出力記号の集合 O_F
- 出力関数 $o_F : S_F \to O_F$

2-2. 入力付きオートマトン

入力付き有限状態オートマトンF(Fはフィルター)は、以下の構成要素から成る。

- 状態の集合 S_F
- 入力記号の集合 I_F
- 状態遷移関数 $f_F : I_F \times S_F \to S_F$
- 出力記号の集合 O_F
- 出力関数 $o_F : S_F \to O_F$

与えられた初期状態s_0と入力列$i_0, i_1, \ldots \in I_F$に対して、Fは次の漸化式によって状態を変える。

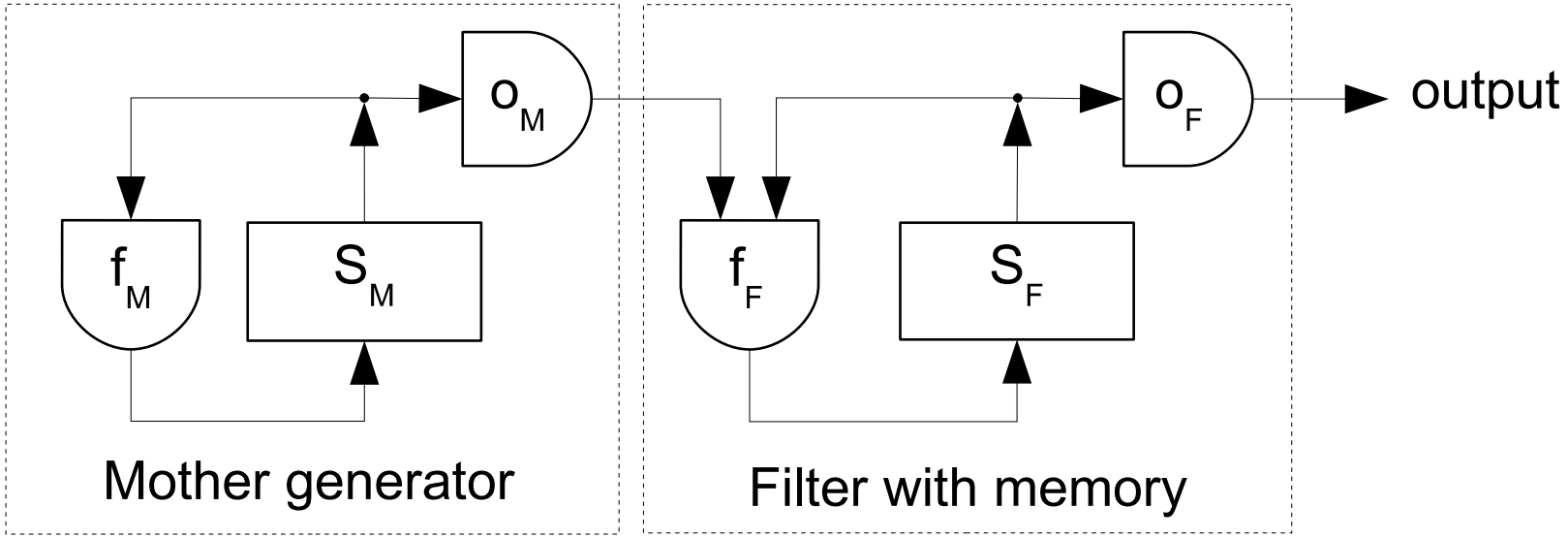
$$s_n = f_F(i_{n-1}, s_{n-1}) \quad (n = 1, 2, 3, \ldots)$$

そして次の出力列を生成する。

$$o_F(s_0), o_F(s_1), o_F(s_2), \ldots \in O_F$$

2-3. 二つのオートマトンの結合

Combined Generatorはこの二つのオートマトンの結合である。



Combined Generatorは、状態空間$S_M \times S_F$をもったひとつの無入力オートマトンとみなせる。
この出力をストリーム暗号として使う。

3. Mother Generator

Combined Generatorの周期と分布を保証するために、Mother Generatorは次の性質をもつと仮定する。

- 周期は大きな素数 (または大きな素因数をもつ)
- 高次元均等分布 (後述 4節)

3. Mother Generator

Combined Generatorの周期と分布を保証するために、Mother Generatorは次の性質をもつと仮定する。

- 周期は大きな素数 (または大きな素因数をもつ)
- 高次元均等分布 (後述 4節)

Mersenne Twister (MT, Matsumoto-Nishimura '97) と
SIMD-oriented Fast Mersenne Twister (SFMT, Saito-Matsumoto '06)
はこの仮定を満たす。

4. 無入力オートマトンの均等分布

k を整数、M を無入力オートマトンとする。
k-組出力関数 $o_M^{(k)}$ を考える。

$$o_M^{(k)} : S_M \to O^k \quad s \mapsto (o_M(s), o_M(f(s)), o_M(f^2(s)), \ldots, o_M(f^{k-1}(s)))$$

(つまり、$o_M^{(k)}$ はある状態から生成される連続したk個の出力への写像である。)

4. 無入力オートマトンの均等分布

k を整数、M を無入力オートマトンとする。
k-組出力関数 $o_M^{(k)}$ を考える。

$$o_M^{(k)} : S_M \to O^k \quad s \mapsto (o_M(s), o_M(f(s)), o_M(f^2(s)), \ldots, o_M(f^{k-1}(s)))$$

(つまり、$o_M^{(k)}$ はある状態から生成される連続したk個の出力への写像である。)
初期状態をすべて動かしたとき、得られるk組の出力の多重集合

$$O_M^{(k)} := \{o_M^{(k)}(s) \mid s \in S_M\}.$$

を考える。これは重複度を考慮した S_M の $o_M^{(k)}$ による像である。

4. 無入力オートマトンの均等分布

k を整数、M を無入力オートマトンとする。
k-組出力関数 $o_M^{(k)}$ を考える。

$$o_M^{(k)} : S_M \to O^k \quad s \mapsto (o_M(s), o_M(f(s)), o_M(f^2(s)), \ldots, o_M(f^{k-1}(s)))$$

(つまり、$o_M^{(k)}$ はある状態から生成される連続したk個の出力への写像である。)
初期状態をすべて動かしたとき、得られるk組の出力の多重集合

$$O_M^{(k)} := \{o_M^{(k)}(s) \,|s \in S_M\}.$$

を考える。これは重複度を考慮した S_M の $o_M^{(k)}$ による像である。
O^kの要素が$O_M^{(k)}$に同じ重複度で現れるとき、オートマトンMは
k-次元均等分布するという。

4. 無入力オートマトンの均等分布

k を整数、M を無入力オートマトンとする。
k-組出力関数 $o_M^{(k)}$ を考える。

$$o_M^{(k)} : S_M \to O^k \quad s \mapsto (o_M(s), o_M(f(s)), o_M(f^2(s)), \ldots, o_M(f^{k-1}(s)))$$

(つまり、$o_M^{(k)}$ はある状態から生成される連続したk個の出力への写像である。)
初期状態をすべて動かしたとき、得られるk組の出力の多重集合

$$O_M^{(k)} := \{o_M^{(k)}(s) \,|s \in S_M\}.$$

を考える。これは重複度を考慮した S_M の $o_M^{(k)}$ による像である。
O^kの要素が$O_M^{(k)}$に同じ重複度で現れるとき、オートマトンMは
k-次元均等分布するという。

注: Mが$\mathbb{F}_2$線形生成器の時（MTやSFMTの場合）は、これは$o_M^{(k)}$の全射性と一致し、したがって計算が可能である。

5. 準群フィルター

準群フィルター とは入力付きオートマトンで、その状態遷移関数

$$f_F : I_F \times S_F \to S_F$$

が bi-bijective なものである。

5. 準群フィルター

準群フィルター とは入力付きオートマトンで、その状態遷移関数

$$f_F : I_F \times S_F \to S_F$$

が bi-bijective なものである。

関数

$$f : X \times Y \to Z$$

が、**bi-bijective** であるとは、任意の y を固定したときに、

$$f(-, y) : X \to Z,\ x \mapsto f(x, y)$$

が全単射でかつ、任意の x を固定したときに、

$$f(x, -) : Y \to Z,\ y \mapsto f(x, y)$$

も全単射であることをいう。
$X = Y = Z$ ならば、これは準群の概念と一致する。

6. 二つの定理

6-1. 分布に関する定理

写像

$$g : X \to Y$$

は、$g^{-1}(y)$の濃度が$y \in Y$に依存しないならば **一様**である。

全単射と全射群準同型は一様である。

一様写像の合成は一様である。

6. 二つの定理

6-1. 分布に関する定理

写像

$$g : X \to Y$$

は、$g^{-1}(y)$ の濃度が $y \in Y$ に依存しないならば **一様** である。
全単射と全射群準同型は一様である。
一様写像の合成は一様である。

定理 1. Combined Generator が、

- k-次元均等分布する Mother Generator
- 準群フィルター F
- F の一様出力関数 o_F

をもてば、Combined Generator は $(k+1)$-次元均等分布する。(証明は容易)

6-2. 周期に関する定理

以下を仮定する。

- Mother Generatorはk-次元均等分布する
- Mother Generatorの周期はQqで、Q は(大きな) 素数
  (q はあまり大きくない整数)
- F は準群フィルター
- o_F は一様

6-2. 周期に関する定理

以下を仮定する。

- Mother Generatorはk-次元均等分布する
- Mother Generatorの周期はQqで、Q は(大きな) 素数
  (q はあまり大きくない整数)
- F は準群フィルター
- o_F は一様

このとき、

$$(\#(O_F))^{k+1} > q \cdot (\#(S_F))^2$$

が成り立つならば、Combined Generatorの出力列の周期はQの倍数になる。

MGの周期 Qq、MGの均等分布次元 k

$$\#(O_F)^{k+1} > q \cdot \#(S_F)^2 \Rightarrow \text{周期} \geq Q$$

大まかに言うと、

- k : 大きい。 (MG は十分高い均等分布性をもつ)
- Qq : (MGの周期は支配的に大きな素因数をもつ)
- $\#(S_F)$: (準群フィルターは相対的に小さな状態空間 S_F をもつ)

ならば、Combined Generatorの周期は素数 Q の倍数になる。

MGの周期 Qq、MGの均等分布次元 k

$$\#(O_F)^{k+1} > q \cdot \#(S_F)^2 \Rightarrow \text{周期} \geq Q$$

大まかに言うと、

- k : 大きい。 (MG は十分高い均等分布性をもつ)
- Qq : (MGの周期は支配的に大きな素因数をもつ)
- $\#(S_F)$: (準群フィルターは相対的に小さな状態空間 S_F をもつ)

ならば、Combined Generatorの周期は素数 Q の倍数になる。

定理は巨大なMGとより小さなFを要求する。
CryptMT ver. 3 はこれらの条件を満足する。

- $Q = 2^{19937} - 1, \quad 1 \leq q \leq 2^{31} - 1,$
- $k = 155, \quad \#(S_F) = 2^{128}, \quad \#(O_F) \geq 4.$

7. 乗算フィルター

ここで、準群フィルターの例を二つ示す。

例 1. 乗算フィルター

$I_F = S_F = (\mathbb{Z}/2^{32})^\times$ を $Z/2^{32}$ の中の奇数の集合とする。

$$f_F : I_F \times S_F \to S_F$$

を $\bmod 2^{32}$ での整数乗算とする。

これは環の乗法群であり、したがって準群である。

7. 乗算フィルター

ここで、準群フィルターの例を二つ示す。

例 1. 乗算フィルター

$I_F = S_F = (\mathbb{Z}/2^{32})^\times$ を $Z/2^{32}$ の中の奇数の集合とする。

$$f_F : I_F \times S_F \to S_F$$

を $\bmod 2^{32}$ での整数乗算とする。

これは環の乗法群であり、したがって準群である。

出力関数

$$o_F : S_F \to O_F = \{0,1\}^8$$

は、32ビット整数の上位8ビットを取り出す一様関数とした。

このフィルターはCryptMT ver. 1で使用した。

例 2. 修正乗算フィルター

以下の全単射によって

$$\mathbb{Z}/2^{32} \longrightarrow (\mathbb{Z}/2^{33})^{\times}$$
$$x \longmapsto 2x+1$$

$\mathbb{Z}/2^{32}$ は、$(\mathbb{Z}/2^{33})^{\times}$ の群構造から導かれる群構造 $\tilde{\times}$ をもつ。

$$\tilde{\times} : (x,y) \mapsto x \tilde{\times} y := 2xy + x + y \bmod 2^{32}.$$

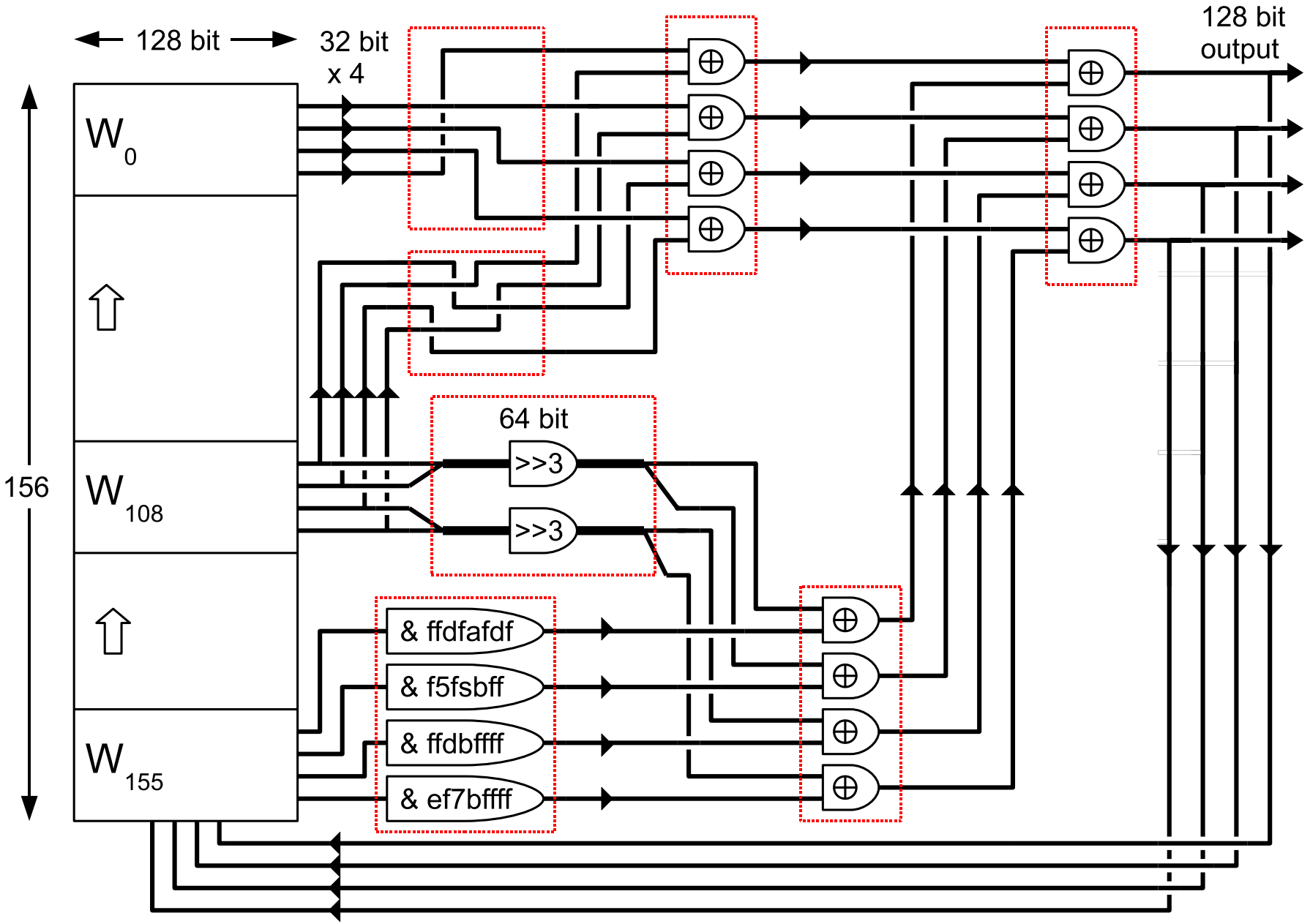
この対応を $I_F = S_F = \mathbb{Z}/2^{32} = 32$ ビット整数の準群フィルターの f_F に採用する。

8. CryptMT version 3

CryptMT version 3 は、これまで述べたようなCombined Generatorである。

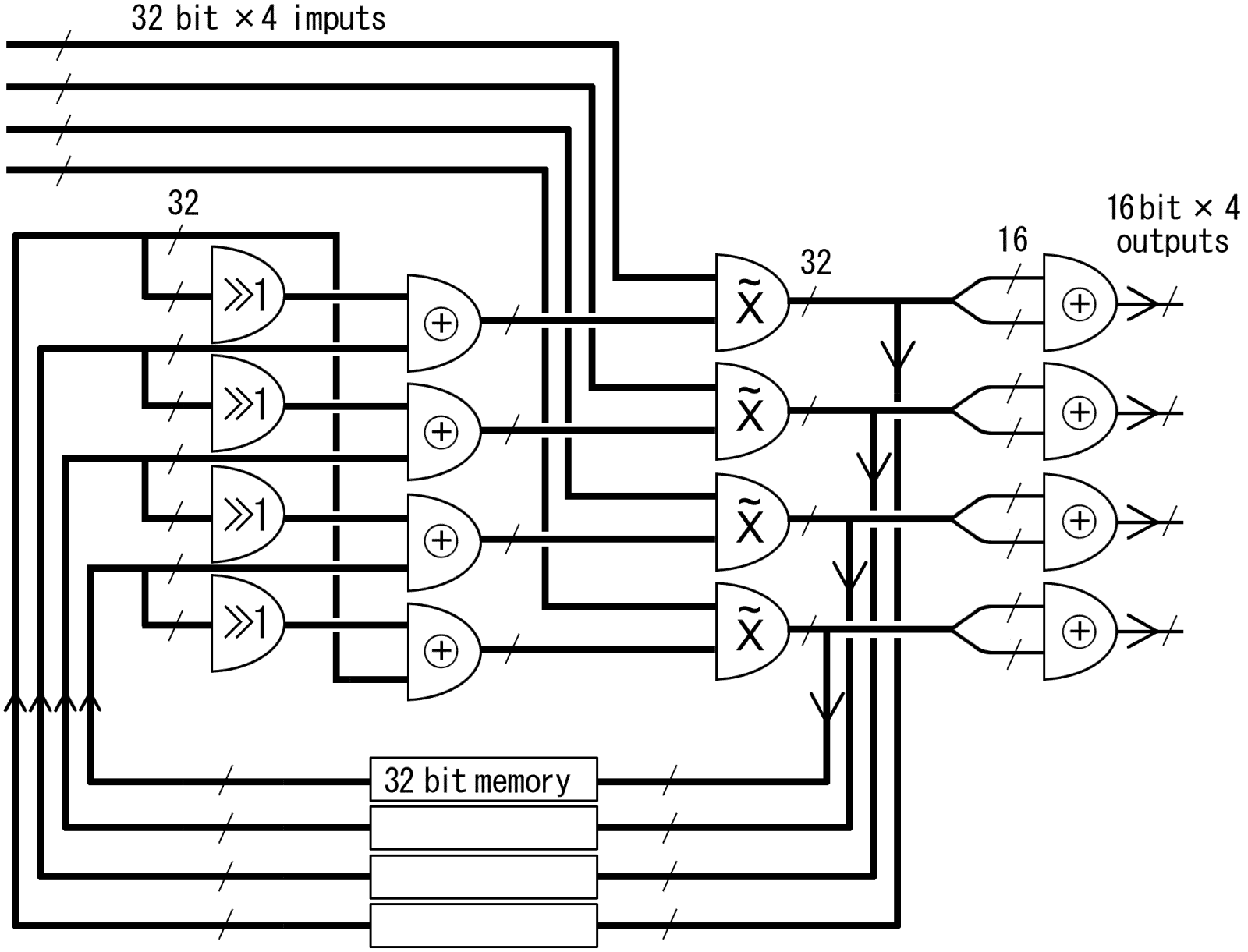
8-1. Mother Generator: SIMD-oriented Fast Mersenne Twister (SFMT)

- 128 ビット列の LFSR 疑似乱数生成器
- 128 ビット演算を使用:
  Single Instruction Multiple Data (SIMD) 命令
- 周期は $2^{19937} - 1$ の倍数
- 均等分布次元は少なくとも 155


128 bit
32 bit
x 4
128 bit
output
156
W0
W108
W155
64 bit
>>3
>>3
& ffdfafdf
& f5fsbff
& ffdbffff
& ef7bffff

8-2. Filter: SIMDを使用した修正乗算フィルター

- S_Fは128ビットメモリー
- ４つの32ビット整数それぞれに群演算$\tilde{\times}$を行う
- 追加の128ビットのビットミキシング
- 出力関数は128ビットから64ビットを抽出


32 bit ×4 imputs
32
≫1
≫1
≫1
≫1
32
16
16 bit × 4
outputs
32 bit memory

8-3. 性質

CryptMT ver. 3 は以下の理論的に保証された性質を持っている。

- 周期は $2^{19937} - 1$ の倍数
- ８ビットの出力列として、少なくとも1241次元に均等分布する

そして、

- 高いalgebraic degreeを持つと期待できる。

8-4. 速度比較

比較したストリーム暗号:

- CryptMT3,
- SOSEMANUK,
- Dragon,
- SNOW 2.0,
- HC-256,
- Salsa20,
- AES (counter-mode)

eSTREAM software cipher phase 3 [2007, ECRYPT] の中で、256 ビットキーを使える 5 候補と、 2 つの参照暗号 SNOW 2.0 and AES.

CPUs:

- Intel Core 2 Duo 2137MHz,
- AMD Athlon X2 2000MHz,
- Motorola PowerPC G4 533MHz.

１バイトの暗号化に消費するＣＰＵサイクル数

	Core 2 Duo	Athlon 64 X2	PowerPC G4
CryptMT3	2.95	4.73	9.23
HC-256	3.42	4.26	6.17
SOSEMANUK	3.67	4.41	6.17
SNOW-2.0	4.03	4.86	7.06
Salsa20	7.12	7.64	4.24
Dragon	7.61	8.11	8.39
AES-CTR	19.08	20.42	34.81

この表はBernstein氏のホームページのデータを元にした:

http://cr.yp.to/streamciphers/timings.html.

CryptMT3 はIntel Core 2 Duo CPUで最も速い、これはこのCPUのSIMD演算の高速性を反映している。

(PowerPC のSIMDには32-bit 乗算命令がない)

10. 結論

ソフトウェアストリーム暗号として、LFSRと一様準群フィルターの組み合わせを提案した。

- 周期と均等分布次元は理論的に保証することができる
- CryptMT ver. 3 という高速な具体的実例

10. 結論

ソフトウェアストリーム暗号として、LFSRと一様準群フィルターの組み合わせを提案した。

- 周期と均等分布次元は理論的に保証することができる
- CryptMT ver. 3 という高速な具体的実例

この発表では触れなかったが、以下の性質も期待できる。

- 乗算フィルターの高いalgebraic degree
  (乗算に対する分析の結果と、トイモデルでの実験から)
- 大きな状態空間、高い非線形性と高い均等分布性から通常の暗号攻撃法でこの暗号を破ることは難しいと思われる。

ご清聴ありがとうございました。