2007－ＣＳＥＣ－38（５）
2007／7／19

安全性が変化する乱数生成方式とその解析

田中 恭之　　石津 晴崇　　森 直彦

NTT コミュニケーションズ株式会社

あらまし　本稿では，擬似乱数生成器の出力する擬似乱数系列と真性乱数系列を組み合わせた乱数（混合乱数と呼ぶ）を構成し，その安全性について解析を行った．その結果，混合乱数系列は，もとの擬似乱数系列よりも高い安全性を持ち，混合する真性乱数の割合を増やしていくことで安全性が高まっていくことが確認できたので，その理論的考察結果を示す．安全性の考察にあたり，従来から知られる安全性定義である NBT(Next Bit Test)をベースに新たな安全性定義 NBT-MAX を定義し，新定義のもとで解析を行った．

A random number generation method with a variable degree of safety and its analysis

Yasuyuki TANAKA　　Harutaka ISHIZU　　Naohiko MORI

NTT Communications Corporation

Abstract In this report, a method for generating a random number sequence, which we call a mixture random number sequence, by mixing a pseudo-random number sequence with true random numbers is shown, and its degree of safety is analyzed. The analysis shows that the mixture random number sequence has a higher degree of safety than that of the pseudo-random number sequence used, and that the degree of safety gets higher as more bits of true random numbers are mixed. We analyze the presented scheme under a new security definition called ``NBT-MAX,"which is based on the conventional notion of NBT (Next-Bit Test).

1.　はじめに

乱数は，鍵の生成，初期ベクトルの生成，暗号技術の中で重要な役割を担っている．また，ストリーム暗号は，一般に平文と乱数系列をビット単位で排他的論理和演算するが，安全性は用いる乱数の暗号学的な性質に依存することが知られている．ここで乱数とは，真性乱数や擬似乱数等を示す．

本稿では，真性乱数と擬似乱数を組み合わせた混合乱数を構成し，その安全性についての理論的解析結果を示す．

2.　混合乱数生成方式

擬似乱数の要件や生成方法[1][2]を参考に，本稿での解析対象である混合乱数の生成方式を以下の様に定義した．

$\pi \geq 1$および$r \in \{0,1\}$に対し，ビット置換関数$S[\pi](r):\{0,1\}^* \to \{0,1\}^*$を以下に定義する．

$$S[\pi](r)(y) \stackrel{\text{def}}{=} y_1 \cdots y_{\pi-1} r y_{\pi+1} \cdots y_m$$

ただし$y = y_1 \cdots y_m \in \{0,1\}^*$，$y_i \in \{0,1\}$である．
また，

$$S[\pi_1,\ldots,\pi_\alpha](r_1,\ldots,r_\alpha) \stackrel{\text{def}}{=} S[\pi_1](r_1) \circ \cdots \circ S[\pi_\alpha](r_\alpha)$$

と書くことにする．
擬似乱数生成器$f:\{0,1\}^n \to \{0,1\}^{kt}$とする．セキュリティパラメータ$\alpha$を持つ擬似乱数生成器の族$\{f_\alpha\}$

$$f_\alpha : \{0,1\}^n \times \{1,\ldots,k\}^\alpha \times \{0,1\}^{\alpha t} \to \{0,1\}^{kt}$$
$$(x,\pi_1,\ldots,\pi_\alpha,r_1^1,\ldots,r_t^1,\ldots,r_1^\alpha,\ldots,r_t^\alpha) \mapsto y$$

を，

$$f_0(x) \stackrel{\text{def}}{=} f(x),$$

$$f_\alpha(x,\pi_1,\ldots,\pi_\alpha,r_1^1,\ldots,r_\ell^1,\ldots,r_1^\alpha,\ldots,r_\ell^\alpha)$$
$$\stackrel{\text{def}}{=} S[\pi_\alpha,\pi_\alpha+k,\ldots,\pi_\alpha+k(\ell-1)](r_1^\alpha,\ldots,r_\ell^\alpha)$$
$$\circ f_{\alpha-1}(x,\pi_1,\ldots,\pi_{\alpha-1},r_1^1,\ldots,r_\ell^1,\ldots,r_1^{\alpha-1},\ldots,r_\ell^{\alpha-1})$$

によって構成し，以後，混合乱数生成方式と呼ぶ．

3. 各種定義

定義した混合乱数生成方式の安全性の変化を見るために，各種定義を行った．

3.1. 安全性定義 NBT-c

まず，本稿における NBT(Next Bit Text)[3]を以下の様に定義する．

定義 1. $f:\{0,1\}^n \to \{0,1\}^m$ を関数とする．攻撃者 $A:\{0,1\}^c \to \{0,1\}$ を確率的アルゴリズムとし，$c \in \{0,\ldots,m-1\}$ を固定する．このとき，

$$\mathrm{Adv}_f^{\text{NBT-}c}(A)$$
$$\stackrel{\text{def}}{=} 2\cdot \Pr[A(y_1\cdots y_c)=y_{c+1} \,|\, x \stackrel{\$}{\leftarrow} \{0,1\}^n, y \leftarrow f(x)] - 1$$

と定義する．ただし，$y_i \in \{0,1\}$ は $y_1 \| \cdots \| y_m = y$ とする．また，$c=0$ の場合は，$y_1\cdots y_c$ は空ストリングを表すこととする．

3.2. 攻撃者のリソース制限

攻撃者のリソースに関して，Bellare[4]の枠組みをベースに，以下の様に定義を行った．

定義 2. GOAL を安全性定義，max を時間リソース t 以内の攻撃者全体をわたるものとして，

$$\mathrm{Adv}_f^{\text{GOAL}}(t) \stackrel{\text{def}}{=} \max_A \mathrm{Adv}_f^{\text{GOAL}}(A)$$

と定義する．

3.3. 安全性定義 NBT-MAX

次に，本稿で安全性評価に用いる NBT-c において c を可変にした NBT-MAX を定義した．

定義 3. $f:\{0,1\}^n \to \{0,1\}^m$ を関数とする．また，攻撃者 $A=(A_1,A_2)$ を 2 つの確率的アルゴリズム

$$A_1:\{\cdot\} \to \{0,\ldots,m-1\}$$
$$A_2:\{0,1\}^C \to \{0,1\}$$

の組とする．ただし，「 · 」は空ストリングを表し，また，

$\mathrm{Im}\,A_1 = \{c \in \{0,\ldots,m-1\} \,|\, \Pr[c=A_1(\cdot)]>0\}$ を A_1 の像としたとき，C は $\mathrm{Im}\,A_1 \subseteq C \subseteq \{0,\ldots,m-1\}$ を満たす集合となり，A_2 の定義域は

$$\{0,1\}^C \stackrel{\text{def}}{=} \bigcup_{c\in C} \{0,1\}^c$$

と定義する．このとき，

$$\mathrm{Adv}_f^{\text{NBT-MAX}}(A)$$
$$\stackrel{\text{def}}{=} 2\cdot \Pr\left[A_2(y_1\cdots y_c)=y_{c+1} \,\middle|\, x \stackrel{\$}{\leftarrow} \{0,1\}^n, y \leftarrow f(x), c \leftarrow A_1(\cdot)\right] - 1$$

と定義する．A の時間リソースは，A_1 および A_2 の時間リソースを足したものにほぼ一致する．

命題 1. 関数 $f:\{0,1\}^n \to \{0,1\}^m$ および時間リソース t に対し，

$$\mathrm{Adv}_f^{\text{NBT-MAX}}(t) \le \max_{c\in\{0,\ldots,m-1\}} \mathrm{Adv}_f^{\text{NBT-}c}(t)$$

が成立する．

証明. ある $\tilde{c} \in \{0,\ldots,m-1\}$ が存在して，

$$\mathrm{Adv}_f^{\text{NBT-MAX}}(t) \le \mathrm{Adv}_f^{\text{NBT-}\tilde{c}}(t)$$

となることを示せば良い．$A=(A_1,A_2)$ を f に対する時間リソース t 以内の NBT-MAX 攻撃者とすると，

$$\begin{aligned}
&\Pr[A_2(y_1\cdots y_c)=y_{c+1} \,|\, c \leftarrow A_1(\cdot)] \\
&= \sum_{c\in C} \Pr[c=A_1(\cdot) \text{かつ } A_2(y_1\cdots y_c)=y_{c+1}] \\
&= \sum_{c\in C} \Pr[c=A_1(\cdot)]\cdot \Pr[A_2(y_1\cdots y_c)=y_{c+1}]
\end{aligned}$$

と計算でき，ある $\tilde{c} \in \{0,\ldots,m-1\}$ が存在して

$\Pr[A_2(y_1\cdots y_c)=y_{c+1} \,|\, c \leftarrow A_1(\cdot)] \le \Pr[A_2(y_1\cdots y_{\tilde{c}})=y_{\tilde{c}+1}]$

が成立する．したがって，任意の c に対して，

$$\begin{aligned}
\mathrm{Adv}_f^{\text{NBT-MAX}}(A) &= 2\cdot \Pr[A_2(y_1\cdots y_c)=y_{c+1} \,|\, c \leftarrow A_1(\cdot)] - 1 \\
&\le 2\cdot \Pr[A_2(y_1\cdots y_{\tilde{c}})=y_{\tilde{c}+1}] - 1 \\
&= \mathrm{Adv}_f^{\text{NBT-}\tilde{c}}(A_2) \\
&\le \mathrm{Adv}_f^{\text{NBT-}\tilde{c}}(t)
\end{aligned}$$

となる．ここで A は任意だったので，求める不等式

$$\mathrm{Adv}_f^{\text{NBT-MAX}}(t) \le \mathrm{Adv}_f^{\text{NBT-}\tilde{c}}(t)$$

を得る．

命題 2. 関数 $f:\{0,1\}^n \to \{0,1\}^m$ および時間リソース t に対し，

$$\max_{c\in\{0,\ldots,m-1\}} \mathrm{Adv}_f^{\text{NBT-}c}(t) \le \mathrm{Adv}_f^{\text{NBT-MAX}}(t')$$

が成立するような時間リソース t' （$\approx t$）が存在

する．

証明. 各 $c\in\{0,\ldots,m-1\}$ に対し，

$$\mathrm{Adv}_f^{\text{NBT-}c}(t)\le \mathrm{Adv}_f^{\text{NBT-MAX}}(t')$$

が成立するようなt'の存在を示せば良い．そこでcを固定し，Aをfに対する時間リソースt以内のNBT-c攻撃者とする．Aを利用して，fに対するNBT-MAX攻撃者 $B=(B_1,B_2)$を次のように構成する．B_1は，ただ単にcを出力する．B_2は，Aをそのまま実行する．

Aの時間リソースがtに等しい場合のBの時間リソースをt'（$\approx t$）とすると，

$$\begin{aligned}\mathrm{Adv}_f^{\text{NBT-MAX}}(t') &\ge \mathrm{Adv}_f^{\text{NBT-MAX}}(B)\\ &= 2\cdot\Pr[B_2(y_1\cdots y_c)=y_{c+1}]-1\\ &= 2\cdot\Pr[A(y_1\cdots y_c)=y_{c+1}]-1\\ &= \mathrm{Adv}_f^{\text{NBT-}c}(A)\end{aligned}$$

となる．Aは任意だったので，求める不等式

$$\mathrm{Adv}_f^{\text{NBT-MAX}}(t')\ge \mathrm{Adv}_f^{\text{NBT-}c}(t)$$

を得る．

4. 攻撃者の時間リソースに関する工夫

定義2.による攻撃者の時間リソースに関する制限では，冒頭で定義した混合乱数生成方式の安全性の変化を見る際，時間リソースが増加してしまい，正確な比較が困難であることが判明した．

そこで時間リソースt以内の攻撃者A全体の集合を$\mathcal{A}(t)$で表すことにして，定義2.を以下の様に再定義した．

$$\mathrm{Adv}_f^{\text{GOAL}}(t)=\max_{A\in\mathcal{A}(t)}\mathrm{Adv}_f^{\text{GOAL}}(A)$$

4.1. NBT-cにおける排他的論理和演算

NBT-c攻撃者$A:\{0,1\}^c\to\{0,1\}$を考える．

$r\in\{0,1\}^c$に対し，確率的アルゴリズム

$A\circ\oplus r:\{0,1\}^c\to\{0,1\}$を

$$(A\circ\oplus r)(y)\stackrel{\text{def}}{=}A(y\oplus r)$$

で定義する．さらに

$$\mathcal{A}(t,\oplus)\stackrel{\text{def}}{=}\{A\circ\oplus r \mid A\in\mathcal{A}(t), r\in\{0,1\}^c\}\cup\mathcal{A}(t)$$

と定義する．$\mathcal{A}(t,\oplus)\supseteq\mathcal{A}(t)$に注意し，$A\circ\oplus 0^c$と$A$を同一視する．また，$A\in\mathcal{A}(t,\oplus)$の時間リソースは，高々$t$に1回の$c$bit排他的論理和に掛かる時間リソースを加えたものであることにも注意する．そして

$$\mathrm{Adv}_f^{\text{NBT-}c}(t,\oplus)\stackrel{\text{def}}{=}\max_{A\in\mathcal{A}(t,\oplus)}\mathrm{Adv}_f^{\text{NBT-}c}(A)\quad(3.1.)$$

と定義する．

命題3. $A:\{0,1\}^c\to\{0,1\}$を確率的アルゴリズムとする．$A\in\mathcal{A}(t,\oplus)$ならば，任意の$r\in\{0,1\}^c$に対し，$A\circ\oplus r$と等価な確率的アルゴリズム$B$が存在し，$B\in\mathcal{A}(t,\oplus)$が成立する．

証明. $A\in\mathcal{A}(t,\oplus)$，$r\in\{0,1\}^c$とする．定義より，ある$A'\in\mathcal{A}(t)$および$r'\in\{0,1\}^c$が存在して$A=A'\circ\oplus r'$と書ける．よって$r''\stackrel{\text{def}}{=}r'\oplus r$と置けば，以下の2式は等価となる。

$$B\stackrel{\text{def}}{=}A'\circ\oplus r''=A'\circ\oplus(r'\oplus r)$$
$$A\circ\oplus r=(A'\circ\oplus r')\circ\oplus r$$

定義より$B\in\mathcal{A}(t,\oplus)$である．□

4.2. NBT-MAXにおける考察

NBT-MAX攻撃者$A=(A_1,A_2)$を考える．$\mathcal{A}(t_1,t_2)$で，A_1，A_2の時間リソースがそれぞれt_1，t_2以内であるような攻撃者A全体を表すことにする．また，単純にある定数$c\in\{0,\ldots,m-1\}$を出力するアルゴリズムA_1，時間リソースt以内の$A_2:\{0,1\}^c\to\{0,1\}$という形をした確率的アルゴリズムA_2の組からなる攻撃者A全体を$\mathcal{A}(\cdot,t)$と表すことにする．命題1.と同様の議論により，

$$\max_{A\in\mathcal{A}(t_1,t_2)}\mathrm{Adv}_f^{\text{NBT-MAX}}(A)\le\max_{A\in\mathcal{A}(\cdot,t_2)}\mathrm{Adv}_f^{\text{NBT-MAX}}(A)$$

であり，また$\mathcal{A}(t_1,t_2)\supset\mathcal{A}(\cdot,t_2)$であるから，

$$\max_{A\in\mathcal{A}(t_1,t_2)}\mathrm{Adv}_f^{\text{NBT-MAX}}(A)\ge\max_{A\in\mathcal{A}(\cdot,t_2)}\mathrm{Adv}_f^{\text{NBT-MAX}}(A)$$

が成立する．すなわち

$$\max_{A\in\mathcal{A}(t_1,t_2)}\mathrm{Adv}_f^{\text{NBT-MAX}}(A)=\max_{A\in\mathcal{A}(\cdot,t_2)}\mathrm{Adv}_f^{\text{NBT-MAX}}(A)$$

となっている．したがって今後は$A\in\mathcal{A}(\cdot,t)$であるような攻撃者のみを考え，

$$\mathrm{Adv}_f^{\text{NBT-MAX}}(\cdot,t)\stackrel{\text{def}}{=}\max_{A\in\mathcal{A}(\cdot,t)}\mathrm{Adv}_f^{\text{NBT-MAX}}(A)\quad(3.2.)$$

と定義しこれを用いる．

4.3. まとめ

定義1.，定義3.，式(3.2.)より，

$$\mathrm{Adv}_f^{\text{NBT-MAX}}(\cdot,t)=\max_c\mathrm{Adv}_f^{\text{NBT-}c}(t)$$

であることに注意し，$\mathcal{A}(\cdot,t,\oplus)$で，$A_1$は単純に

ある定数 $c \in \{0,\ldots,m-1\}$ を出力するアルゴリズムで，$A_2 : \{0,1\}^c \to \{0,1\}$ は $A_2 \in \mathcal{A}(t,\oplus)$ であるような攻撃者 $A=(A_1,A_2)$ 全体を表すことにする．

ここで

$$\mathrm{Adv}_f^{\text{NBT-MAX}}(\cdot,t,\oplus) \stackrel{\text{def}}{=} \max_{A \in \mathcal{A}(\cdot,t,\oplus)} \mathrm{Adv}_f^{\text{NBT-MAX}}(A)$$

と定義すれば，

$$\mathrm{Adv}_f^{\text{NBT-MAX}}(\cdot,t,\oplus) = \max_c \mathrm{Adv}_f^{\text{NBT-}c}(t,\oplus) \quad (3.3.)$$

が成立する．

5. 安全性の可変性の定義

これまでに行った定義を用い，混合乱数の安全性可変化を定義する．

定義 4. セキュリティパラメータ $0 \le \alpha \le \beta$ に対し

$$\left(\frac{k-1}{k}\right)^{\beta-\alpha} \cdot \mathrm{Adv}_{f_\alpha}^{\text{NBT-MAX}}(\cdot,t,\oplus) \ge \mathrm{Adv}_{f_\beta}^{\text{NBT-MAX}}(\cdot,t,\oplus)$$

が成立する．特に，十分大きな時間リソース t に対しては

$$\mathrm{Adv}_{f_0}^{\text{NBT-MAX}}(\cdot,t,\oplus) > \mathrm{Adv}_{f_1}^{\text{NBT-MAX}}(\cdot,t,\oplus) > \cdots$$

が成り立つ．すなわち，真性乱数で置換する回数を増やしていくと，安全性が増していくことが NBT-MAX に関して成立する．

6. 混合乱数生成方式の安全性解析

6.1. NBT-c での評価

以下この節では $c \in \{0,\ldots,m-1\}$ を固定する．この節の目的は次の命題を示すことである．

命題 4. 任意の $\alpha \ge 1$ に対して不等式

$$\mathrm{Adv}_{f_\alpha}^{\text{NBT-}c}(t,\oplus) \le \frac{k-1}{k} \cdot \mathrm{Adv}_{f_{\alpha-1}}^{\text{NBT-}c}(t,\oplus)$$

が成立する．

証明に先立ち，まず記号を準備する．擬似乱数生成器 $g : \{0,1\}^v \to \{0,1\}^m$ と $\pi \in \{1,\ldots,m\}$ に対し，$g[\pi] : \{0,1\}^v \times \{0,1\} \to \{0,1\}^m$ を

$$g[\pi](x,r) \stackrel{\text{def}}{=} S[\pi](r) \circ g(x)$$

で定義する．

同様に，$\pi_1,\ldots,\pi_\alpha \in \{1,\ldots,m\}$ に対し，$g[\pi_1,\ldots,\pi_\alpha] : \{0,1\}^v \times \{0,1\}^\alpha \to \{0,1\}^m$ を

$$g[\pi_1,\ldots,\pi_\alpha](x,r_1,\ldots,r_\alpha) \stackrel{\text{def}}{=} S[\pi_1,\ldots,\pi_\alpha](r_1,\ldots,r_\alpha) \circ g(x)$$

で定義する．

補題 4. 1. 不等式

$$\mathrm{Adv}_{g[\pi]}^{\text{NBT-}c}(t,\oplus) \le \mathrm{Adv}_g^{\text{NBT-}c}(t,\oplus)$$

が成立する．

証明. $\pi = c+1$ の場合は $\mathrm{Adv}_{g[\pi]}^{\text{NBT-}c}(t,\oplus) = 0$ なので除外する．また $\pi \ge c+2$ の場合は

$$\mathrm{Adv}_{g[\pi]}^{\text{NBT-}c}(t,\oplus) = \mathrm{Adv}_g^{\text{NBT-}c}(t,\oplus)$$

なので自明である．よって $\pi \le c$ とする．

$A : \{0,1\}^c \to \{0,1\}$ を $A \in \mathcal{A}(t,\oplus)$ であるような確率的アルゴリズムとすると（以下，確率のランダムテープは $x \xleftarrow{\$} \{0,1\}^n$，$r \xleftarrow{\$} \{0,1\}$ とし，$y \leftarrow g(x)$，$y = y_1 \cdots y_m$ とする．また，$\overline{y}_\pi$ は y_π の反転，すなわち $y_\pi \oplus 1$ を表す），

$$\begin{aligned}
&\mathrm{Adv}_{g[\pi]}^{\text{NBT-}c}(A) \\
&= 2 \cdot \Pr[A(\cdots r \cdots) = y_{c+1}] - 1 \\
&= 2 \cdot \Pr[A(\cdots r \cdots) = y_{c+1} \text{ かつ } r = y_\pi] \\
&\quad + 2 \cdot \Pr[A(\cdots r \cdots) = y_{c+1} \text{ かつ } r = \overline{y}_\pi] - 1 \\
&= 2 \cdot \Pr[r = y_\pi] \cdot \Pr[A(\cdots r \cdots) = y_{c+1} \mid r = y_\pi] \\
&\quad + 2 \cdot \Pr[r = \overline{y}_\pi] \cdot \Pr[A(\cdots r \cdots) = y_{c+1} \mid r = \overline{y}_\pi] - 1 \\
&= 2 \cdot \frac{1}{2} \cdot \Pr[A(\cdots y_\pi \cdots) = y_{c+1}] \\
&\quad + 2 \cdot \frac{1}{2} \cdot \Pr[A(\cdots \overline{y}_\pi \cdots) = y_{c+1}] - 1 \\
&= \Pr[A(\cdots y_\pi \cdots) = y_{c+1}] - \frac{1}{2} + \Pr[A(\cdots \overline{y}_\pi \cdots) = y_{c+1}] - \frac{1}{2} \\
&= \frac{1}{2} \cdot \mathrm{Adv}_g^{\text{NBT-}c}(A) + \frac{1}{2} \cdot \mathrm{Adv}_g^{\text{NBT-}c}(A \circ \oplus 0 \cdots 010 \cdots 0)
\end{aligned}$$

ここで命題 3. を用いて，

$$\begin{aligned}
\mathrm{Adv}_{g[\pi]}^{\text{NBT-}c}(A) &\le \frac{1}{2} \cdot \mathrm{Adv}_g^{\text{NBT-}c}(t,\oplus) + \frac{1}{2} \cdot \mathrm{Adv}_g^{\text{NBT-}c}(t,\oplus) \\
&= \mathrm{Adv}_g^{\text{NBT-}c}(t,\oplus)
\end{aligned}$$

となる．

A は任意だったので，求める不等式

$$\mathrm{Adv}_{g[\pi]}^{\text{NBT-}c}(t,\oplus) \le \mathrm{Adv}_g^{\text{NBT-}c}(t,\oplus)$$

を得る．□

補題 4. 2. 不等式

$$\mathrm{Adv}_{g[\pi_1,\ldots,\pi_\alpha]}^{\text{NBT-}c}(t,\oplus) \le \mathrm{Adv}_g^{\text{NBT-}c}(t,\oplus)$$

が成立する．

証明. 定義より

$$\begin{aligned}
&g[\pi_1,\ldots,\pi_\alpha](x,r_1,\ldots,r_\alpha) \\
&\stackrel{\text{def}}{=} S[\pi_1,\ldots,\pi_\alpha](r_1,\ldots,r_\alpha) \circ g(x) \\
&= S[\pi_1](r_1) \circ \cdots \circ S[\pi_\alpha](r_\alpha) \circ g(x)
\end{aligned}$$

なので，前補題の結果を帰納的に適用していけば，

求める不等式を得る．□

次に，さらなる準備として

$$\Pi \stackrel{\text{def}}{=} \{1,\ldots,k\} \setminus \{(c+1) \bmod k\}$$

と置く．ここで $(c+1) \bmod k$ は $c+1$ を k で割った時の剰余を表し，$c+1$ が k の倍数である時は $(c+1) \bmod k \stackrel{\text{def}}{=} k$ とする．また，f_α の定義域を $\{0,1\}^n \times \{1,\ldots,k\}^{a-1} \times \Pi \times \{0,1\}^{a\ell}$ に制限した擬似乱数生成器を

$$\tilde{f}_\alpha : \{0,1\}^n \times \{1,\ldots,k\}^{a-1} \times \Pi \times \{0,1\}^{a\ell} \to \{0,1\}^{t\ell}$$

と書く．すなわち，$\tilde{f}_\alpha$ は f_α と殆ど同じだが，π_α の取り得る範囲が $\{1,\ldots,k\}$ ではなく Π になっている点だけが異なる．

補題 4.3. 不等式

$$\mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{\tilde{f}_\alpha}(t,\oplus) \le \mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{f_{\alpha-1}}(t,\oplus)$$

が成立する．

証明. $A:\{0,1\}^c \to \{0,1\}$ を $A \in \mathcal{A}(t,\oplus)$ であるような 確率的アルゴリズムとする．以下，確率のランダムテープは $x \xleftarrow{\$} \{0,1\}^n$，$\pi_1,\ldots,\pi_{\alpha-1} \xleftarrow{\$} \{1,\ldots,k\}$，$\pi_\alpha \xleftarrow{\$} \Pi$，$r_1^1,\ldots,r_\ell^1,\ldots,r_1^\alpha,\ldots,r_\ell^\alpha \xleftarrow{\$} \{0,1\}$ とし，$y \leftarrow f_{\alpha-1}(\cdots)$，$y = y_1 \cdots y_m$ と書く．また，$\ell' \stackrel{\text{def}}{=} \lceil c/k \rceil$ とおく．定義より

$$\begin{aligned}
&\mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{\tilde{f}_\alpha}(A) \\
&= 2 \cdot \Pr[A(\cdots r_1^\alpha \cdots r_2^\alpha \cdots r_\ell^\alpha \cdots) = y_{c+1}] - 1 \\
&= 2 \cdot \sum_{\pi \in \Pi} \{ \Pr[\pi_\alpha = \pi] \\
&\qquad \cdot \Pr[A(\cdots r_1^\alpha \cdots r_2^\alpha \cdots r_\ell^\alpha \cdots) = y_{c+1} \,|\, \pi_\alpha = \pi] \ \} - 1 \\
&= \sum_{\pi \in \Pi} \{ \Pr[\pi_\alpha = \pi] \\
&\qquad \cdot (2 \cdot \Pr[A(\cdots r_1^\alpha \cdots r_2^\alpha \cdots r_\ell^\alpha \cdots) = y_{c+1} \,|\, \pi_\alpha = \pi] - 1) \ \} \\
&= \sum_{\pi \in \Pi} \{ \Pr[\pi_\alpha = \pi] \cdot \mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{f_{\alpha-1}[\pi,\pi+k,\ldots,\pi+k(\ell'-1)]}(A) \} \\
&\le \sum_{\pi \in \Pi} \{ \Pr[\pi_\alpha = \pi] \cdot \mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{f_{\alpha-1}[\pi,\pi+k,\ldots,\pi+k(\ell'-1)]}(t,\oplus) \} \\
&\le \sum_{\pi \in \Pi} \{ \Pr[\pi_\alpha = \pi] \cdot \mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{f_{\alpha-1}}(t,\oplus) \} \\
&= \mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{f_{\alpha-1}}(t,\oplus) \cdot \sum_{\pi \in \Pi} \Pr[\pi_\alpha = \pi] \\
&= \mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{f_{\alpha-1}}(t,\oplus)
\end{aligned}$$

となる．A は任意だったので，求める不等式

$$\mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{\tilde{f}_\alpha}(t,\oplus) \le \mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{f_{\alpha-1}}(t,\oplus)$$

を得る．□

補題 4.4. 等式

$$\mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{f_\alpha}(t,\oplus) = \frac{k-1}{k} \cdot \mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{\tilde{f}_\alpha}(t,\oplus)$$

が成立する．

証明. $A:\{0,1\}^c \to \{0,1\}$ を確率的アルゴリズムとし，

$$\mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{f_\alpha}(A) = \frac{k-1}{k} \cdot \mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{\tilde{f}_\alpha}(A)$$

を示す．以下，確率のランダムテープは $x \xleftarrow{\$} \{0,1\}^n$，$\pi_1,\ldots,\pi_\alpha \xleftarrow{\$} \{1,\ldots,k\}$，$r_1^1,\ldots,r_\ell^1,\ldots,r_1^\alpha,\ldots,r_\ell^\alpha \xleftarrow{\$} \{0,1\}$ とし，$y \leftarrow f_\alpha(\cdots)$，$y = y_1 \cdots y_m$ と書く．また，$\ell' \stackrel{\text{def}}{=} \lceil (c+1)/k \rceil$ とおく．

$\mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{f_\alpha}(A)$ は

$$\begin{aligned}
&\mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{f_\alpha}(A) \\
&= 2 \cdot \Pr[A(y_1 \cdots y_c) = y_{c+1}] - 1 \\
&= 2 \cdot \Pr[A(y_1 \cdots y_c) = y_{c+1} \text{ かつ } \pi_\alpha = (c+1) \bmod k] \\
&\quad + 2 \cdot \Pr[A(y_1 \cdots y_c) = y_{c+1} \text{ かつ } \pi_\alpha \in \Pi] - 1
\end{aligned}$$

と分割できる．さらに

$$\begin{aligned}
&\Pr[A(y_1 \cdots y_c) = y_{c+1} \text{ かつ } \pi_\alpha = (c+1) \bmod k] \\
&= \Pr[A(y_1 \cdots y_c) = r_t^\alpha \,|\, \pi_\alpha = (c+1) \bmod k] \\
&\quad \cdot \Pr[\pi_\alpha = (c+1) \bmod k] \\
&= \frac{1}{2} \cdot \frac{1}{k} = \frac{1}{2k}
\end{aligned}$$

と計算でき，また

$$\begin{aligned}
&\Pr[A(y_1 \cdots y_c) = y_{c+1} \text{ かつ } \pi_\alpha \in \Pi] \\
&= \Pr[A(y_1 \cdots y_c) = y_{c+1} \,|\, \pi_\alpha \in \Pi] \cdot \Pr[\pi_\alpha \in \Pi] \\
&= \frac{\mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{\tilde{f}_\alpha}(A) + 1}{2} \cdot \frac{k-1}{k} \\
&= \frac{k-1}{2k} \cdot \mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{\tilde{f}_\alpha}(A) + \frac{1}{2} - \frac{1}{2k}
\end{aligned}$$

と計算できる．よって

$$\begin{aligned}
&\mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{f_\alpha}(A) \\
&= 2 \cdot \frac{1}{2k} + 2 \cdot \left(\frac{k-1}{2k} \cdot \mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{\tilde{f}_\alpha}(A) + \frac{1}{2} - \frac{1}{2k} \right) - 1 \\
&= \frac{k-1}{k} \cdot \mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{\tilde{f}_\alpha}(A)
\end{aligned}$$

を得る．ここで $A \in \mathcal{A}(t,\oplus)$ とすると，

$$\begin{aligned}
\mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{f_\alpha}(A) &= \frac{k-1}{k} \cdot \mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{\tilde{f}_\alpha}(A) \\
&\le \frac{k-1}{k} \cdot \mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{\tilde{f}_\alpha}(t,\oplus)
\end{aligned}$$

を得る．A は任意だったので

$$\mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{f_\alpha}(t,\oplus) \le \frac{k-1}{k} \cdot \mathrm{Adv}^{\mathrm{NBT}\text{-}c}_{\tilde{f}_\alpha}(t,\oplus)$$

が言える.

同様に, $A \in \mathcal{A}(t,\oplus)$ に対し

$$\mathrm{Adv}_{f_\alpha}^{\mathrm{NBT\text{-}c}}(t,\oplus) \geq \mathrm{Adv}_{f_\alpha}^{\mathrm{NBT\text{-}c}}(A) = \frac{k-1}{k}\cdot \mathrm{Adv}_{j_\alpha}^{\mathrm{NBT\text{-}c}}(A)$$

となる. A は任意だったので

$$\mathrm{Adv}_{f_\alpha}^{\mathrm{NBT\text{-}c}}(t,\oplus) \geq \frac{k-1}{k}\cdot \mathrm{Adv}_{j_\alpha}^{\mathrm{NBT\text{-}c}}(t,\oplus)$$

も示すことができ, 求める等式を得る. □

命題 4 の証明. 補題 4.3. 及び 4.4. より

$$\mathrm{Adv}_{f_\alpha}^{\mathrm{NBT\text{-}c}}(t,\oplus) = \frac{k-1}{k}\cdot \mathrm{Adv}_{j_\alpha}^{\mathrm{NBT\text{-}c}}(t,\oplus) \leq \frac{k-1}{k}\mathrm{Adv}_{f_{\alpha-1}}^{\mathrm{NBT\text{-}c}}(t,\oplus)$$

となる. □

6.2. NBT-MAX での評価

命題 5. 不等式

$$\mathrm{Adv}_{f_\alpha}^{\mathrm{NBT\text{-}MAX}}(\cdot,t,\oplus) \leq \frac{k-1}{k}\cdot \mathrm{Adv}_{f_{\alpha-1}}^{\mathrm{NBT\text{-}MAX}}(\cdot,t,\oplus)$$

が成立する.

証明. 今までの結果を組み合わせると

$$\begin{aligned}\mathrm{Adv}_{f_\alpha}^{\mathrm{NBT\text{-}MAX}}(\cdot,t,\oplus) &= \max_c \mathrm{Adv}_{f_\alpha}^{\mathrm{NBT\text{-}c}}(t,\oplus)\\ &\leq \max_c \frac{k-1}{k}\cdot \mathrm{Adv}_{f_{\alpha-1}}^{\mathrm{NBT\text{-}c}}(t,\oplus)\\ &= \frac{k-1}{k}\cdot \max_c \mathrm{Adv}_{f_{\alpha-1}}^{\mathrm{NBT\text{-}c}}(t,\oplus)\\ &= \frac{k-1}{k}\cdot \mathrm{Adv}_{f_{\alpha-1}}^{\mathrm{NBT\text{-}MAX}}(\cdot,t,\oplus)\end{aligned}$$

となり, 示したい不等式を得る. □

6.3. 解析結果

各 $\alpha \geq 1$ に対し

$$\mathrm{Adv}_{f_\alpha}^{\mathrm{NBT\text{-}MAX}}(\cdot,t,\oplus) \leq \frac{k-1}{k}\cdot \mathrm{Adv}_{f_{\alpha-1}}^{\mathrm{NBT\text{-}MAX}}(\cdot,t,\oplus)$$

が言えているので, セキュリティパラメータ $0 \leq \alpha \leq \beta$ に対し,

$$\left(\frac{k-1}{k}\right)^{\beta-\alpha}\cdot \mathrm{Adv}_{f_\alpha}^{\mathrm{NBT\text{-}MAX}}(\cdot,t,\oplus) \geq \mathrm{Adv}_{f_\beta}^{\mathrm{NBT\text{-}MAX}}(\cdot,t,\oplus)$$

が成立する. また f_α の入力長は出力長よりも短くなるような α のみを考察しているので, NBT-MAX の非零性より, 十分大きな時間リソース t に対し

$$\mathrm{Adv}_{f_\alpha}^{\mathrm{NBT\text{-}MAX}}(\cdot,t,\oplus) > 0$$

となっている. このような t に対しては, セキュリティパラメータ $\beta > \alpha$ に対し

$$\mathrm{Adv}_{f_\alpha}^{\mathrm{NBT\text{-}MAX}}(\cdot,t,\oplus) > \mathrm{Adv}_{f_\beta}^{\mathrm{NBT\text{-}MAX}}(\cdot,t,\oplus)$$

が成立する. □

7. まとめ

安全性定義 NBT-MAX で, 混合乱数生成方式により構成した混合乱数の安全性の解析を行った. 混合乱数の特徴として,

- もとの擬似乱数よりも高い安全性をもつ
- 混合する真性乱数の割合を増やしていくことで安全性が高まっていく

を示すことが出来た.

今後は, この混合乱数を NTT コミュニケーションズの秘密分散技術[5]へ適用した場合についての安全性考察を進める予定である。

謝辞

本研究は独立行政法人情報通信研究機構から委託を受け実施している「大容量データの安全な流通・保存技術に関する研究開発」の成果の一部である.

参考文献

[1] 岡本龍明・山本博資著, 『現代暗号』, 産業図書株式会社 ISBN4-7828-5353-X C3355 pp.45～62.

[2] M. Blum, S. Micali, "How to generate cryptographically strong sequences of pseudo-random bits," SIAM Journal of Computing, pp.850-864, 1984.

[3] M. Luby, "Pseudorandomness and Cryptographic Applications," Princeton University Press, pp.49-55, 1996.

[4] M. Bellare, A. Desai, E. Jokipii and P. Rogaway, "A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation," Proceedings of 38th Annual Symposium on Foundations of Computer Science (FOCS 97), pp. 394-403, IEEE Press, 1997.

[5]石津晴崇, 荻原利彦, 電子データの長期保存に関する一考察, 電子情報通信学会, 2004 年総合大会, Mar. 2004.