L-002

耐量子暗号実現のための疑似乱数の乱数検定による評価
Evaluation of Pseudorandom Numbers for Quantum Cryptography

森下 航‡　松本 大輝‡　馬場 優作‡　三重野 凌‡　荒木 智行‡
Koh Morishita　Hiroki Matsumoto　Yusaku Baba　Ryo Mieno　Tomoyuki Araki

1. はじめに

量子コンピュータの研究が進められている。それに伴い耐量子暗号が必要とされている。耐量子暗号には、ランダム性の高い疑似乱数が必要不可欠である[1][2]。

本研究の目的は、Y-00 への適用を目的とした疑似乱数生成の新しい手法を提案することである。その手法としてベント関数を用いて作成した S-Box を、LFSR を用いて生成した疑似乱数に適用することで　LFSR の線形性による脆弱性を解消した非線形な疑似乱数の生成を目指した。そして生成された疑似乱数を評価し、実際にランダム性の高い疑似乱数が生成されたのかを検討した。

2. 諸準備

以下、研究にあたっての数学的な諸準備を示す。

2.1 Y-00 プロトコル

2000 年に Yuen によって、KCQ 原理(“keyed communication in quantum noise”)とよばれる概念を基礎とした暗号構成理論が提案された。これが現在 Y-00 プロトコルとよばれているランダムストリーム暗号の原型となっている[3]。Y-00 のプロトコルは以下の通りである。

(1)送信者 Alice と受信者 Bob は共通の短い鍵 K_S を交換する。
(2)Alice は 2M 個の位相信号を用意し、180° 離れた２つをセットとして M 個の基底とする。
(3)共通鍵 K_S を疑似乱数生成期で伸長し、長い鍵 K とする。この鍵から使用する基底が決められる。
(4)Bob は Alice と同じ疑似乱数を持つためどの基底が用いられているかがわかる。そのため常に 1 と 0 の 2 値位相偏移変調での受信が可能となる。しかし、盗聴者は用いられる基底が分からないため 2M 個の量子状態を識別できない限り情報を得ることはできない。ここで、2M 個の信号は密に並んでいるため誤り確率が非常に高い状況となっている。

2.2 線形フィードバックシフトレジスタ

線形フィードバックシフトレジスタ(LFSR)[4]とは疑似乱数生成器の一種であり、一連のビット列をシフトしながら特定のタップに基づいて XOR 演算を行い、新しいビットを生成する仕組みを持つ。この構造により、長周期かつ高速なビット列の生成を可能にしている。

しかし、LFSR が持つ線形性は暗号通信で用いるには問題がある。線形攻撃によって比較的容易にビット列のパターンが解読される可能性があり、暗号システムにおける安全性が損なわれる恐れがある。

2.3 ベント関数

ベント関数[5]とは、変数 n が偶数の時その非線形性が最大なブール関数のことであり、その非線形性は以下の(1)式で表せる。

$$N_f = 2^{n-1} - 2^{\frac{n}{2}-1} \tag{1}$$

非線形性とはブール関数fと最も近いアフィン関数とのハミング距離で定義され(2)式で表せる。

$$N_f = \min_{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2} dist(f, l_{a,b}) \tag{2}$$

と表せる。ここで$dist(x,y)$は x と y のハミング距離で、(3)式で表せる。

$$dist(x,y) = \sum_{i=1}^{n} \delta(x_i, y_i) \tag{3}$$

$$\delta(x_i, y_i) = \begin{cases} 0 (x_i = y_i) \\ 1 (x_i \neq y_i) \end{cases} \tag{4}$$

$l_{a,b}$はアフィン関数で、(5)式で表せる。

$$l_{a,b}(x) = \langle a, x\rangle \oplus b \tag{5}$$

$$\langle a, x\rangle = a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n \tag{6}$$

2.4 S-Box

S-Box とは、入力された nbit の入力を別の mbit に変換して出力する置換関数のことである[6]。これを線形な疑似乱数に適用することによって非線形な疑似乱数へ変換し、線形攻撃への耐性を高めるために用いられる。しかし、S-Box を線形関数に近似して解読を試みる手法も存在する。

2.5 バランス化

作成した S-Box の出力に偏りがある場合、S-Box を適用して出力した疑似乱数の出力にも偏りが出てしまい、ランダム性が不十分となってしまう。そのためバランス化を行う必要がある。

バランス化の手順は、以下のとおりである。
(1)S-Box を作成し、表にする。
(2)作成された S-Box に存在しない値を抜き出す。
この S-Box では{1, 3, 4, 7, C, D, E}である。

‡広島工業大学 Hiroshima Institute of Technology

＼	00	01	10	11
00	F	9	2	8
01	0	B	F	8
10	6	6	A	6
11	5	8	B	A

図 1．S-Box(16 進数表記)

(3)S-Box の値を左上から見ていき、二度以上出てきた値を出てきていない値で置き換える。

＼	00	01	10	11
00	F	9	2	8
01	0	B	1	3
10	6	4	A	7
11	5	C	D	E

図 2.バランス化された S-Box(16 進数表記)

3. 新しい手法の提案

本研究では、ベント関数を用いて線形関数に近似しにくい S-Box を作成し LFSR に適用することで、非線形な疑似乱数を生成することを目標とし、新しい手法を検討した。具体的な手順は以下の通りである。

(1)4 変数ベント関数を 4 つ選択し、S-Box を作成する。
(2)作成した S-Box にバランス化を行う。
(3)LFSR を用いて 55×10^6bit の疑似乱数を出力する。
(4)生成した疑似乱数に S-Box を適用し変換を行う。この際 1 つの S-Box のみを用いて変換したものと、4 つの S-Box を用いて 2.5×10^5bit 毎に用いる S-Box を変更して変換したものを生成する。
(5)NIST SP800-22[7]を用いて、生成された疑似乱数を 10^6bit ずつ、計 55 回の評価を行う。

4. 結果と考察

LFSR のみで出力した疑似乱数の場合 Binary Matrix Rank Test と Linear Complexity Test において 55 回全てにおいて欠陥があるという結果となった。

それに対し S-Box を適用した疑似乱数では Binary Matrix Rank Test は 52/55、Linear Complexity Test は 55 回全てにおいて欠陥がないという結果となった。また、複数の S-Box を適用した疑似乱数は Binary Matrix Rank Test、Linear Complexity Test どちらも 54/55 回欠陥がないという結果になった。よって、今回提案した手法による疑似乱数の生成は十分ランダムな疑似乱数を生成する手段として適切といえる。また、S-Box を変更しない手法とする手法では、今回のテスト結果からは大きな違いは見られなかった。

5. むすび

本研究では、Y-00 への適用を目的とした疑似乱数の生成と評価を行った。今後としては、用いる S-Box の数や適用する間隔を変更しても行いたい。また、Y-00 への適用を目的として研究を行ったが、実際に Y-00 へ適用して動作させることが出来ていないため、実際に Y-00 への適用も目指したい。

謝辞

本研究をまとめるにあたり江田英雄教授にご指導をいただきました。心より感謝を申し上げます。

参考文献

[1] 杉本 幹太, 方 穆湧, 荒木 智行, “ベント関数の量子鍵交換プロトコルへの適用について”, 多値論理研究会, 第 46 回多値論理フォーラム研究ノート, Vol. 46, No. 4, (2023).
[2] 方 穆湧, 杉本 幹太, 荒木 智行, “ベント関数を使った量子鍵交換プロトコルの評価について”, 多値論理研究会, 第 46 回多値論理フォーラム研究ノート, Vol. 46, No. 5, (2023).
[3] 広田修, 相馬正宜, 川西悟基, “量子雑音によるランダムストリーム暗号 Y-00”, 日本光学会誌, 光学 39. 1 pp. 17-22, (2010).
[4] Peter Alfke, “Efficient Shift Resisters, LFSR Counters, and Long Pseudo-Random Sequence Generators”, XAPP 052 July 7,1996(Version1.1), (1996).
[5] Natalia Tokareva, “Bent Functions: Results and Applications to Cryptography”, Academic Press, (2015).
[6] Zijing Jiang and Qun Ding, “Construction of an S-Box Based on Chaotic and Bent Functions”, Symmetry 2021,13,671,March 11, (2021).
[7] Andrew Rukhin et al, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications”, NIST Special Publication 800-22 Revision la, (2010).