電気学会論文誌 D（産業応用部門誌）
IEEJ Transactions on Industry Applications
Vol.136 No.10 pp.698–702　DOI: 10.1541/ieejias.136.698

論　文

量子暗号 Y-00 方式の安全性評価に関する検討

非会員　大嶺　沢仁*　正　員　山田　親稔*
非会員　宮城　　桂*　非会員　市川　周一**

Security Analysis of Quantum Key Distribution Protocol

Takuto Omine*, Non-member, Chikatoshi Yamada*, Member, Kei Miyagi*, Non-member, Shuichi Ichikawa**, Non-member

（2016年2月15日受付，2016年7月18日再受付）

Recently, the Y-00 protocol has been developed as a defense against cryptanalysis. The Y-00 protocol has a high affinity with existing public communication networks and has also been shown to achive a large-capacity transmission. In this article, we aim to improve Key DSR, which is part of the functionality of Y-00. We propose a new model of Key DSR, and a discussion of the efficiency of the new model is presented. Finally, we show that the proposed method can contribute to the composition of a safety design approach for Y-00 encryption.

キーワード：Y-00, シミュレータ，強度変調，量子暗号
Keywords: Y-00, simulator, intensity modulation, quantum cryptography

1. まえがき

近年，現代社会の情報交換において，インターネットなどの種々の通信手段が広範囲に利用されている。その際，重要な要素として挙げられるのが通信の秘匿性である。そして，暗号化はその秘匿性を確保するために用いられる方法の一つである。現代暗号の主流の一つに AES（Advanced Encryption Standard）がある。この代表的な暗号は，秘匿性を確保するために素因数分解の計算量の膨大さに安全基準をおいている。しかしながら，量子計算機が実現すると，従来の計算機とは比較にならないほどの高速な並列処理により，従来の安全基準が揺らいでしまう可能性が指摘されている[1]。そこで考案されたのが，計算量に関係なく安全性を補強することができる光通信量子暗号（Yuen-00，以下，Y-00）である。Y-00 はショット雑音に分類される量子雑音（量子的ゆらぎ）を用いて，識別不可能領域を作り出すことで盗聴者の受信能力を劣化させ，送信信号自体を隠蔽するという新しい安全基準を用いている。そして，Key DSR は Y-00 の機能の一つであり，量子雑音をシフトを用いて各基底に拡散させ，受信能力劣化処理を補助する役割を有している。しかし，問題点として Key DSR による量子雑音の拡散は盗聴者だけでなく受信者にも影響するために，現在では数 bit のシフトのみしか扱えない。そのため，暗号の強化を行うには限定された範囲のシフトを一様にすることがもっとも最適である。

本稿では，量子雑音をより拡散させることができる暗号鍵の生成を目標とし，機能の一部である Key DSR の構造に対する提案を行い，その有用性を考察する。まず，Y-00 の概要について述べ，本研究で使用した擬似乱数生成器であるフィボナッチ LFSR（Fibonacci Linear Feedback Shift Register）について説明し，既存の手法と提案手法の概要を示す。そして，提案手法に使用した攪拌という概念や前提条件である使用乱数列の相関関係の証明，一様さを比較するための評価方法について述べたあと，提案手法も含めた 3 つの擬似乱数生成器を評価する。最後に，結果について考察を行ない，今後の展望を述べたあと，まとめとした。

2. 原　　理

〈2･1〉 Y-00 プロトコル　光通信量子暗号（Y-00）は，Northwestern 大学の Yuen らによって提案された方式である。その主な特徴は，量子雑音（量子的ゆらぎ）を用いることである。この量子雑音の中に伝送情報（暗号文）を混ぜてしまうことで盗聴者に伝送情報自体を読ませないようにしている[2]。以下にその性質を示す。

（1）　共通鍵暗号方式

Y-00 は送信者と受信者が同じ秘密鍵を共有して通

* 沖縄工業高等専門学校
〒905-2192　沖縄県名護市辺野古 905
Okinawa National College of Technology
095, Henoko, Nago, Okinawa 905-2192, Japan
** 豊橋技術科学大学
〒441-8580　愛知県豊橋市天伯町雲雀ヶ丘 1-1
Toyohashi University of Technology
1-1, Hibarigaoka, Tempaku-cho, Toyohashi, Aichi 441-8580, Japan

信を行う共通鍵暗号方式である。これは，Y-00 が従来の秘密鍵暗号と同様に，秘密鍵をどのように管理・共有するかという問題を内包しているということである。この問題に関しては，量子暗号の一つである BB84 を用いるなどの提案がされている[3]。

（2） 大容量通信が可能

Y-00 は大容量の通信が可能である。その理由として挙げられるのが，現在の光通信に対する親和性である。Y-00 は商用の光ファイバーを用いることが可能で，それらを使い，既に実際の機器による 360 km，10 Gbps の通信実験も行われている[4]。

〈2･2〉 強度変調方式 Y-00 の原理 Y-00 の変調方式には位相変調や強度変調などが挙げられるが，本稿では強度変調方式を採用している。以下に，強度変調を採用したプロトコルによる Y-00 信号への暗号化と，その逆の動作である復号の原理を Fig. 1 と Fig. 2 に示し，詳細を説明する。

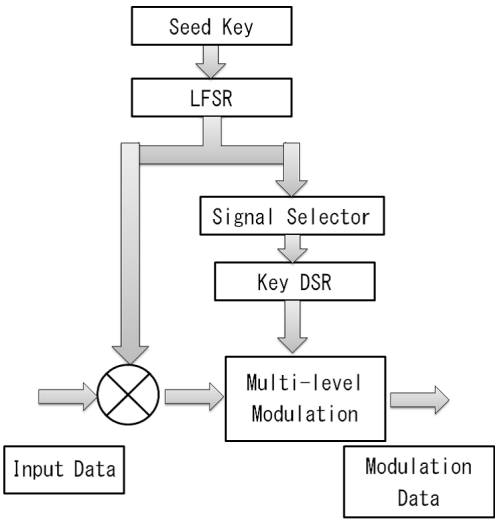

Fig. 1. Modulation (Y-00).

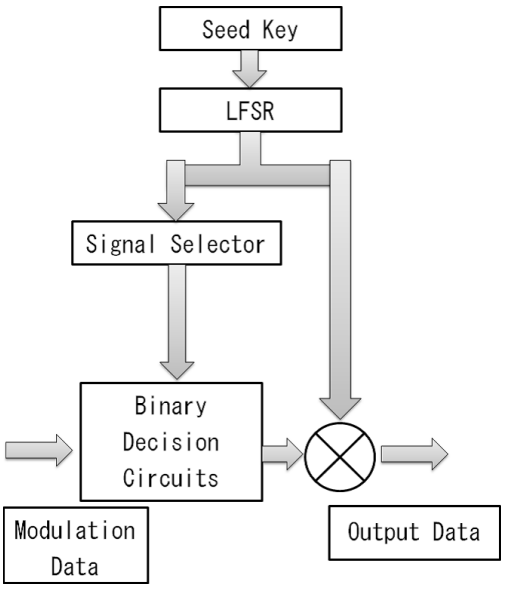

Fig. 2. Demodulation (Y-00).

（1） シード鍵（初期鍵）K_s を擬似乱数発生器によって拡張し，その結果，ランニング鍵 K を生成する。

〈2･1〉(1)節で述べたように，Y-00 では送信者と受信者の間で共通の秘密鍵 K_s が共有されている。そして，その秘密鍵を擬似乱数発生器によって，拡張し，その結果，生成されるのがランニング鍵 $K = k_1 k_2 \cdots k_t$ である。なお，現状として擬似乱数発生器は線形帰還シフトレジスタ（LFSR）で代用されているものとする。ランニング鍵の各要素はディジットと呼ばれる。ある時刻 t においてディジットは集合 $K_g = 1, 2, \ldots M$ の中のある一つの値を取る。M は基底数であり，$2^{\mu}-1$ で表される。すなわち，M は常に奇数の値を取る。μ は適当な正の整数である。

共通鍵暗号方式は大きく分けて，ブロック暗号とストリーム暗号の 2 種類に分けられる。そして，上記（Fig. 1 および Fig. 2）の方式はストリーム暗号に属する。この方式には原理的に再現が容易で処理速度に優れているという利点がある。

（2） ランニング鍵を $logM$ ビットごとに区切ってブロック化し，10 進数の基底選択信号を生成する。

〈2･1〉節で述べたように，Y-00 暗号は量子雑音の中に送信信号を混入し，盗聴者に正確な信号を読み取らせないのが特徴である。しかし，受信者も同様に雑音の影響を受けてしまうために，量子雑音の中から “0”, “1” を取り出す仕組みが必要となる。それが，基底 M と基底選択信号である。共通鍵暗号方式により受信者も基底選択信号を生成できるため，雑音の中のどこに本来の信号が存在するのかが判定できる。

（3） 基底選択信号と基底の組合わせを対応付ける。

基底選択信号を用いて，光の強度レベル α が決定したとき，同時に “0”, “1” を表現する組 (α_i, α_{i+M}) も決定する。

（4） Key DSR（Deliberate Signal Randomization）で，受信時の雑音が拡散して見えるように，基底選択信号値の確率分布を補正

理論的な安全性評価を可能にするためには，盗聴者の信号識別に関与する条件付確率を一様にする必要がある。そのため，基底選択信号情報を一度拡散回路（Random shifter）でランダムに拡散させる。これに用いられるのが小林らの提案する Key DSR[5] である。この拡散が理想的に実現された場合，その安全性は次の式で表すことができる。

$$Q = \Gamma^{|k|/log_2 M} \quad \cdots\cdots (1)$$

Q は安全指数，Γ は隣接レベルの量子雑音が重なり合う範囲，$|k|$ は鍵長，M は基底数である。そして，最終的な基底選択信号を生成する信号セレクト回路（Select signal）を介してから，基底選択信号は多値変調回路に入力される。ただ，補足すると KeyDSR

は直接的に安全を強化するものではなく，更に OSK（Overlap Selection Keying）などを加える必要がある[6]。

（5） スクランブルした信号を，基底選択信号でビット毎に変調し，2M 値の送信信号を生成

上記の〈2･2〉(4)節でも述べたが，Y-00 では基底選択信号を用いて，変調の際のビットの光強度値を基底数 M の集合の中からランダムに設定する。

上記の処理を行うことで，強度変調を用いた Y-00 の信号光を生成することができる。また，復号を行うにはこれとは逆の処理を行う。

3. 擬似乱数生成器（Pseudo Random Number Generator）の構造検討

（1） フィボナッチ LFSR

本稿ではフィボナッチ LFSR を用いることを想定している。Fig. 3 にその概念図を示す。

LFSR では，最長の周期を実現する LFSR のことを最長 LFSR と呼び，その性質は以下のようになる。なお，以下で述べられているタップとは次の入力ビットに影響を与えるビットであり，Fig. 3 における Prime bit のそれぞれを指す。

（a） LFSR が最長となるのは，タップ数が偶数の場合のみである。

（b） タップ集合は互いに素でなければならない。

（c） LFSR の長さによっては，最長となる複数の多項式が存在する。

（d） 最長の場合，その周期は全ビットがゼロという状態以外の全ての取りうる状態 $(2^n - 1)$ である。

次に述べる構造検討では，この性質に留意して LFSR が用いられているものとする。

（2） 構造の検討

本研究では，提案手法を含めて 3 つの構造をプログラムで再現し，比較している。以下の Fig. 4，Fig. 5，Fig. 6 にそれらを示し，それぞれの概要について簡単に説明する。

PRNG1（Fig. 4）は LFSR のみを用いた通常の擬似乱数生成器である。先に示した最長 LFSR に従って挿入ビットを作ることで，相関性の無いほぼ一様な乱数を新しく生成できるようになっている。

PRNG2（Fig. 5）は先行研究[5]にあるように，PRNG1 に Key DSR を追加した擬似乱数生成器である。LFSR1 で作成した乱数の下位数ビットに，Key DSR で作成したビットを加算することでシフトを実現している。

PRNG3（Fig. 6）は改良を加えた Key DSR = Key DSR’ を PRNG1 に追加した擬似乱数生成器である。Key DSR’ では，従来の Key DSR の bit に対して新たな入力との排他的論理和（XOR）をとることで，

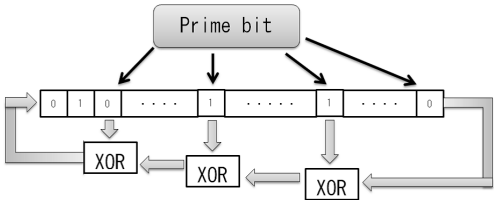

Fig. 3. Fibonacci LFSR.

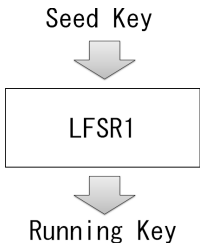

Fig. 4. PRNG1.

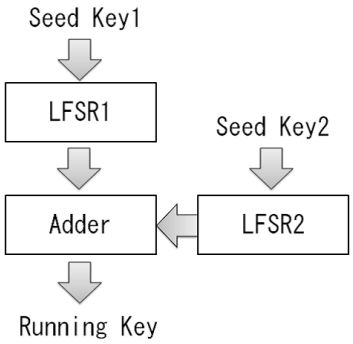

Fig. 5. PRNG2 (Previous Research, Key DSR).

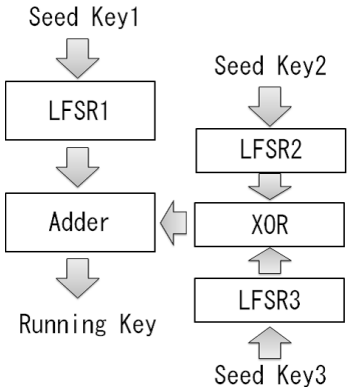

Fig. 6. PRNG3 (The Proposed Method, Key DSR’).

攪拌という概念を適用している。

（3） Key DSR’（提案手法）

Key DSR’ について詳しく述べる。Key DSR’ は攪拌という概念を従来の Key DSR に適応することで，良質な一様乱数の生成を目指した機構である。本稿で取り上げる攪拌とは相関性の少ない（無い）2 つの変数において，単 bit ごとの排他的論理和（XOR）が取られたときに，その出力はより良質（偏りの少ない）な乱雑 bit を形成するというもので，攪拌の中では最も単純な手法である[7]。

（4） 使用データの相関性

攪拌を用いるにあたって，使用データは相関性の少ない（無い）という前提条件を持つ必要がある。そのため，ここではピアソンの積率相関係数を用いて用意した二つの乱数列の相関性を評価し，十分に前提を満足したと判断した場合に Key DSR' に使用した。ピアソンの積率相関係数を (2) 式に示す。

$$r = \frac{\frac{1}{N}\sum_{i=1}^{N}(X_i - \overline{X})(Y_i - \overline{Y})}{\sqrt{\frac{1}{N}\sum_{i=1}^{N}(X_i - \overline{X})^2}\sqrt{\frac{1}{N}\sum_{i=1}^{N}(Y_i - \overline{Y})^2}} \quad \cdots\cdots\cdots\cdots (2)$$

式の X，Y は Key DSR' における Seed Key2，Seed Key3 が該当し，N は bit の取り出し回数である。このとき，相関係数の範囲は $-1 < 0 < 1$ をとり，0 に近ければ近いほど 2 つの変数は相関性を失うことになる。以下に，実際に計算した初期乱数列（Seed Key2，Seed Key3）と，それらを LFSR によって冗長した場合の相関係数を示す。

（a） 初期乱数列（Seed Key2，Seed Key3）の相関係数

0.101723 ⇒ 0.2 以下でほとんど相関無し

（b） 冗長後の乱数列の相関係数

0.007623 ⇒ 良質なほぼ無想間データであると判断

ここからわかるように，乱数列の相関係数は 0 に近いものとなり，前提を満足していることが分かる。

4. 評価方法

評価を行うには，一様さを定量化する必要がある。そこで，本研究では平均情報量（エントロピー）を用いた。以下にその式を示す。

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (3)$$

H が平均情報量，i が試行回数，n が最大出現回数，p_i が各基底の発生確率である。以上の (3) 式を元に検討を行う。

5. シュミレーション

シミュレーション環境を以下の Table 1 に示す。

3 つの乱数生成器に対する平均情報量 H のシミュレーション結果を Table 2 に示す。ここで，下位数 bit の攪拌をとることで平均情報量は，僅かではあるが向上が確認された。

6. 考　　察

以上の結果より次の二つが結論として得られた。

（1）「見せ掛けの相互関係（擬似相関）」により攪拌が機能しなかった。

（2） Key DSR の一様性向上は暗号鍵の平均情報量には大きく影響しなかった。

以下にこれら二つの結論を詳しく解説していく。

Table 1. Simulation environment.

OS	windows 7 Enterprise 32 bit
PC	Dyna book R730/E730/E26BR
Memory	4 GB
Processor	Intel(R) Core(TM) i3 CPU M380 2.53 GHz
Programming language	C++
Compiler	Bcc32

Table 2. Entropy of each random number generator.

Key length(bit)	Trial frequency	PRNG	Entropy(bit)	Processing time(s)
480	100,000	PRNG1	10.173238	179.59
		PRNG2	10.178172	127.97
		PRNG3	10.178336	157.67
240	100,000	PRNG1	10.362873	130.28
		PRNG2	10.367232	86.61
		PRNG3	10.367232	83.15
120	100,000	PRNG1	9.992770	91.31
		PRNG2	9.996543	55.88
		PRNG3	9.9965865	79.31

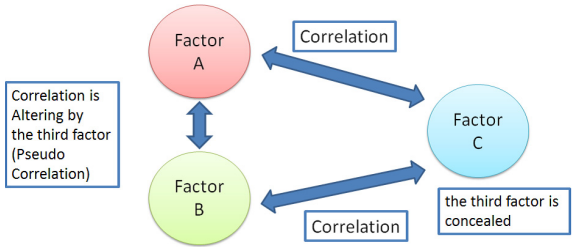

Fig. 7. Pseudo correlation.

〈6･1〉 考察 1（擬似相関）　擬似相関とは，二つの事象の相関関係が，見えない（潜伏している）第三要素によって変動することである。Fig. 7 にその概念図を示す。

しかし，相関係数に影響を及ぼす第三要素はピアソンの積率相関係数のみでは推定することはできず，その他の検討が必要となってくる。そのため，現時点では Seed Key2 と Seed Key3 の間に本当に擬似相関があるのかは不明だが，今回，乱数として使用している C 言語の rand 関数や，同条件で使用したフィボナッチ LFSR が原因かどうかも含めて今後検討する必要があると思われる。

〈6･2〉 考察 2（暗号鍵の平均情報量への影響）　暗号鍵の平均情報量への影響を考察するために，例として 480 bit の平均情報量を取り上げ，以下に，PRNG1 と PRNG2，PRNG2 と PRNG3，それぞれの平均情報量の差を示す。

（1） PRNG1 と PRNG2 のエントロピーの差

$10.178172 - 10.173238 = 4.934 \times 10^{-3}$ [bit]

（2） PRNG2 と PRNG3 のエントロピーの差

$10.178336 - 10.178172 = 1.64 \times 10^{-4}$ [bit]

これらより変化量の上昇率を求めてみると，3%となった。このことより，Key DSR' によって数ビットを良質な一様にすることは達成できているが，暗号鍵としての大きなビット列には充分大きな変化を与えることは出来なかったと考える。

〈6･3〉 考察のまとめ　一様さの向上は見られたが，そ

の効果は僅かなものであった。前述の考察として挙げた 2 つの結論より，その原因は

（1） 擬似相関により，攪拌の効果が減少した。

（2） 全体への影響が小さかった。

であると考察できる。

7. ま と め

本稿では，Y-00 の隣接間レベルで発生する量子雑音の識別不可能領域の拡散に用いられる Key DSR の乱数生成手法を提案した。受信者の受信感度の問題から使用ビット数に制限がある状態での一様さの向上のために，ビット数を変えずにビット生成に使われる LFSR の台数を増やし，攪拌の概念を適用することで，一様さの改善を試みた。今後の展開としては，擬似乱数の潜伏変数を明確にし，定量化，改善案を検討したいと考えている。

提案手法による利点をまとめる。

（1） 一様になる確率が向上する

上記で述べたことだが，値の出現数を増やすことにより，試行回数はより無限に近づき，確率は一様に近づく。

（2） シミュレーション実現への貢献

量子暗号 Y-00 のシミュレーションは多くなく，実装前に実験・検討するとコストダウンなどの面からシミュレーションは有効であると考えられる。また，乱数生成器のプログラムは量子暗号の実現に大きく貢献すると考えられる。

謝　辞

本研究は，豊橋技術科学大学高専連携教育研究プロジェクト及び日本学術振興会の科学研究費補助金（No.40412902）の支援を受けた。

文　献

（1） 情報処理推進機構：「次世代暗号・認証方式の研究・開発に関する調査報告」, 情報処理振興事業協会 (2001)

（2） 長迫勇輝：「強度変調方式を用いた光通信量子暗号（Y-00）に対する盗聴者の能力評価の一考察」, 信学技報, OCS2009-57, OPE2009-123, LQE2009-82 (2009)

（3） 中本　衛：「量子暗号 BB84 シミュレータ」, 高知工科大学情報システム工学科, 平成 21 年度, 学士学位論文 http://hdl.handle.net/10232/4884 (2008)

（4） 二見史生・広田　修：「光通信量子暗号（Y-00）の高いセキュアフォトニックネットワークへの展開に関する検討」, 信学会, 新世代ネットワーク・ワークショップ (2010)

（5） 小林洋平・水上勇輝・渡部　圭・広田　修：「光通信量子暗号（Y-00）における量子ゆらぎエラーの均一化」, 2006 年信学会総合大会, B-10-38 (2006)

（6） 原澤克嘉・広田　修・山下喜市・本田　真・圷　重人・細井健司・土井吉文・大畠賢一・片山武彦・清水哲也：「Yuen 2000 プロトコルによる物理暗号のための Randomization の実装回路の考察」, 信学論, Vol.J91-C, No.8, pp.399–408 (2008)

（7） S. Eastlake, 3rd and J.I. Schiller:「セキュリティのための乱雑性についての用件」(2005) https://www.ipa.go.jp/security/rfc/RFC4086JA.html#051

大　嶺　沢　仁　（非会員） 2016 年沖縄工業高等専門学校情報通信システム工学科卒業。2016 年同高等専門学校専攻科創造システム工学専攻電子通信システム工学コース入学。現在，在学中。

山　田　親　稔　（正員） 2000 年琉球大学大学院理工学研究科博士前期課程修了。2004 年同大学大学院博士後期課程単位取得満期修了。同年拓殖大学北海道短期大学専任講師。2007 年沖縄工業高等専門学校情報通信システム工学科助教。2009 年同高等専門学校情報通信システム工学科准教授。2014 年ビクトリア大学（カナダ）客員研究員。2015 年より，沖縄工業高等専門学校情報通信システム工学科准教授。現在に至る。博士（工学）。形式的設計検証，リコンフィキャラフルシステムの研究・教育に従事。IEEE，電子情報通信学会，各会員。

宮　城　　桂　（非会員） 2008 年高知工科大学情報システム工学科卒業。2010 年同大学大学院修士課程修了。2014 年同大学大学院博士課程修了。同年沖縄工業高等専門学校情報通信システム工学科助教。現在に至る。博士（工学）。自己同期型パイプラインを用いた低消費電力 VLSI の研究に従事。電子情報通信学会会員。

市　川　周　一　（非会員） 1985 年東京大学理学部卒業。1987 年同大学大学院理学系研究科修士課程修了。1987 年新技術事業団創造科学推進事業（ERATO）後藤磁束量子情報プロジェクト研究員。1991 年三菱電機（株）LSI 研究所，システム LSI 開発研究所勤務。1994 年名古屋大学工学部助手。1997 年豊橋技術科学大学工学部知識情報工学系講師。2001 年豊橋技術科学大学工学部知識情報工学系助教授。2007 年豊橋技術科学大学工学部知識情報工学系准教授。2010 年豊橋技術科学大学大学院工学系研究科准教授。2011 年沼津工業高等専門学校制御情報工学科教授。2012 年より，豊橋技術科学大学大学院工学系研究科教授。現在に至る。理学博士。並列計算機，並列処理，および専用計算システムアーキテクチャの研究に従事。IEEE（senior member），電子情報通信学会（シニア会員），ACM，情報処理学会，各会員。