社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2005－ＣＳＥＣ－30（46）
2005／7／22

Y-00プロトコルが古典的なストリーム暗号と等価であることについて

今福健太郎† 今井　秀樹††,† 西岡　毅††† 長谷川俊夫††† 石塚　裕一†††

† 産業技術総合研究所情報セキュリティ研究センター
〒101-0121 東京都千代田区外神田 1-18-13
†† 東京大学生産技術研究所
〒153-8505 東京都目黒区駒場 4-6-1
† 三菱電機株式会社情報技術総合研究所
〒247-8501 神奈川県鎌倉市大船 5-1-1
E-mail: †imafuku-kentaro@aist.go.jp

あらまし 無条件安全性を達成する“量子ストリーム暗号”として提案されたY-00プロトコルが，実際には古典的なストリーム暗号と同じ安全性であるとする我々の主張[1]について，より精緻にその主張を再構成することにより，その主張の意味をより明確にする．

キーワード 量子暗号，Y-00プロトコル，安全性解析，

Critical cryptoanalysis for Y-00

Kentaro IMAFUKU†, Hideki IMAI††,†, Tsuyoshi NISHIOKA†††,

Toshio HASEGAWA†††, and Hirokazu ISHIZUKA†††

† Research Center for Information Security, Advanced Industrial Science and Technology (AIST)
Sotokanda 1-18-13, Chiyoda-ku, Tokyo 101-0121, JAPAN
†† Institute of Industrial Science, University of Tokyo
Komaba 4-6-1, Meguro-ku, Tokyo 153-8505, JAPAN
† aInformation Technology R & D Center, Mitsubishi Electric Corporation
Ofuna 5-1-1, Kamakura, Kanagawa 247-8501, JAPAN
E-mail: †imafuku-kentaro@aist.go.jp

Abstract We clarify our claim that Y-00 protocol, which was proposed as a protocol achieving “secure communication based on quantum noise”, does not actually provide higher security than a classical stream cipher. We have already discussed the claim in our previous paper [1] but we found that there are still misunderstanding on our argument. In the present article, we describe the essence of our idea in a bit more formal way than our previous paper.

Key words Quantum cryptography, Y-00 protocol, cryptoanalysis

1. イントロダクション

物理系の量子論的な振る舞いや性質が，情報論的なリソースとして注目されるようになって久しい．その元始的なWiesnerの考察[2]以来30年以上の時間が経過した．その間，提案された幾つかのアイディアが実際の物理系として実現されたでなく，「なぜ，量子系は役に立つのか」あるいは「量子系を使って何が達成され，何が達成できないのか」といった，本質的な問いに対しても，多くの知見が蓄積されてきた．特に，量子系を用いて，いわゆる無条件安全な通信を実現しようとする「量子暗号」については，鍵配布のための量子プロトコルが，実際に製品として実装されるまでになっている．また同時に，安全性証明などの理論的な考察を通じ，「そこで達成されるべき安全性」あるいは「量子暗号の暗号としての位置づけ」自体への理解が深められてきた．量子暗号研究開発にとってこの30年間は，これら応用，基礎の異なる側面を持つ二つの大きな成果によって特徴付けられると考えることができるだろう．

一方で，これらの華々しい発展が，非常に多くの試行錯誤あ

るいは提案と検証の繰り返しを土台として進められてきたことも，注目すべき事実である．量子暗号の基礎は，暗号理論，情報理論，量子論といった，広範な領域におよんでいる．量子暗号の発展は，それぞれの分野からその特徴的な考え方や斬新な発想を吸収し，さらに各分野へのフィードバックを行いながら加速してきた．このような発展は，非常に多くの試行錯誤を通じて，量子暗号へのさらに深い理解のための知見を蓄積してきた歴史でもある．この（比較的短いと言えるかもしれない）30年の歴史には，量子暗号が多くの分野の融合的な位置にあることの帰結としての意味合いだけでなく，他のいかなる暗号と同じく，「提案と検証」という暗号の研究開発にとって極めて本質的で健全なプロセスが存在していることを見て取ることができる．今後の発展のどの段階においても，これまでと同様に自由な発想による提案ときちんとした検証を，広い分野の深い知見に基づいて活発に行っていくことが，量子暗号研究の面白さと信頼性を普遍的に支えていくだろう．

本報告の目的も，上記の認識に基づき，最近我々の行ったY-00プロトコル[3]の検証的解析を紹介しその知見を広く共有することにある．無条件安全性を持つプロトコルとして提案されたこのY-00方式が，実際には古典的なストリーム暗号と同じ計算量的安全性しか持たないことについては，実は既に我々の論文[1]で議論されている．しかし残念ながら，未だ一部において，我々の議論が十分に理解されておらず，さらに，この論文に対する反論として[4],[5]などが公開されたことなどもあり，やや混乱した状況が続いている．実際には，本報告でもみるように，これらの反論は，[1]で議論された攻撃方法とは無関係の攻撃に対する議論となっており，残念ながら反論としての意味をそこに見出すことはできない．しかしながら，いずれにしても状況を整理し，論文[1]の議論を明確にするためにも，きちんとした学術的解説が有意義であると考えられる．そこで，我々は[1]での議論を精緻に再構成し，Y-00プロトコルが古典ストリーム暗号と同等であることについて，より詳細な報告を行うことにした．

以下，本報告は次のように構成される．第二節において，Y-00プロトコルの紹介をしながら本報告における表記や記号の導入を行う．また，しばしばY-00プロトコルの安全性の根拠とされる議論についても反省しておく．第三節で，論文[1]の議論を再構成し，実際にY-00プロトコルが古典ストリーム暗号と同等であることを示す．特に本報告では，(1)盗聴者（以下，イブ）が行う量子測定過程を導入し，(2)イブはその測定によって得られる情報を使って決定論的な復号アルゴリズムを構成できること，の二点を具体的に示す．これにより，Y-00プロトコルが古典的なストリーム暗号と同等の安全性しか持たないことが明確となる．さらに，本報告での議論と論文[1]における議論の関係を整理する．第四節では，本報告や[1]における議論と，[4],[5]の中で我々の攻撃として紹介されている議論が異なっていることを指摘するとともに，周辺の議論を整理する．最後に本報告のまとめを行う．

2. Y-00プロトコル

ここで，本報告の記号を導入しながら，Y-00プロトコルの紹介を行う．Y-00プロトコルは以下のように記述できる．

[Y-00 プロトコル]

(1) アリスとボブは，あらかじめ秘密鍵 $\mathbf{K}_s$ を共有しておく．

(2) 擬似乱数アルゴリズム $PRNG(\cdot)$ を使い，アリスとボブは擬似乱数列 $\mathbf{K} = PRNG(\mathbf{K}_s) = (K_1, K_2, \cdots, K_{N-1}, K_N)$ をランニング鍵として生成する．ただし $K_i = PRNG_i(\mathbf{K}_s) \in \{0, 1, \cdots, M-1\}$ とする．

(3) アリスは，メッセージ（あるいは乱数）$\mathbf{R}_N = (r_1, r_2, \cdots, r_{N-1}, r_N)$（ただし $r_i \in \{0,1\}$ とする）を準備し，各 r_i を量子状態（コヒーレント状態）

$$|\Psi(K_i, r_i)\rangle = |\alpha e^{i\theta_{K_i, r_i}}\rangle, \tag{1}$$

に“暗号化”する．ここで α は複素数，$\theta_{K_i,r_i} = (K_i/M + (r_i \oplus \Pi(K_i)))\pi$，さらに $\Pi(K_i) \in \{0,1\}$ の写像，である．

(4) アリスは上記で準備した量子状態を量子チャンネルを通じてボブへ送る．

(5) 量子状態を受け取ったボブは，受け取った状態が $|\Psi(K_i, r_i)\rangle$ であるか $|\Psi(K_i, r_i \oplus 1)\rangle$ であるかの判別をするための量子測定を行う．この際，ボブは K_i を知っていることに注意．彼が，$|\Psi(K_i, r_i)\rangle$ を受け取ったと判断すれば，彼は受け取った量子状態を r_i へ“復号”し，$|\Psi(K_i, r_i \oplus 1)\rangle$ であったと判断すれば，$r_i \oplus 1$ へ“復号”する．

ここで，ランニング鍵 K_i を知っているボブにとって，上の判別は $|\Psi(0,0)\rangle$ と $|\Psi(0,1)\rangle$ の二つの状態の区別と同等であることに注意しよう．このどちらの状態も同じ確率で受信する場合には，ボブが最適な量子測定を行った場合，その誤り確率は

$$p_B = \frac{1}{2}(1 - \sqrt{1 - |\langle\Psi(0,0)|\Psi(0,1)\rangle|^2}) \tag{2}$$

$$= \frac{1}{2}\left(1 - \sqrt{1 - e^{-4|\alpha|^2}}\right) \sim \frac{1}{4}\exp(-4|\alpha|^2) \tag{3}$$

となることが知られている．即ち，$|\alpha|^2$（コヒーレント状態の平均光子数）が大きければこの確率は無視できる状況になる．一方，ランニング鍵 K_i を知らないイブはボブと同様の方法では r_i を得ることができない．例えば

$$\theta_{K_i,r_i} - \theta_{K_i',r_i\oplus 1} = \frac{\pi}{M}. \tag{4}$$

のとき，$|\Psi(K_i, r_i)\rangle$ と $|\Psi(K_i', r_i \oplus 1)\rangle$ を区別するだけの問題を考えても，その誤り確率はイブの量子最適測定を仮定したとしても

$$p_E = \frac{1}{2}(1 - \sqrt{1 - |\langle\Psi(K_i, r_i)|\Psi(K_i', r_i \oplus 1)\rangle|^2}) \tag{5}$$

$$\sim \frac{1}{2} - \frac{|\alpha|\pi}{2M}. \tag{6}$$

となり，$|\alpha|^2$ が大きくても，$|\alpha|\pi/2M \ll 1$ となるような M の取り方を採用すれば，p_E は $1/2$ に漸近する．これにより，一見，量子論的なゆらぎにより，r_i に関する情報のイブへの漏洩

が防がれているように考えられ，無条件安全性が主張されてきた．実際，このような議論を根拠として[3]の中では

$$|\alpha|^2 > 100, \quad M = 200, \tag{7}$$

が物理パラメータとして想定されている．このようなコヒーレント状態は比較的扱いやすく現在の光通信ネットワークとの相性も（単一光子と比較すれば）よいと考えられることから，単一光子を用いることを想定しているBB84プロトコルなどと比較して，その技術的優位性が主張されることもある．

しかしながら，上記の議論は単に，イブは状態の区別により直接（ボブと同じ方法では）r_iに関する情報を得ることができないことを意味しているに過ぎず，例えば，イブが量子測定により得た何らかの情報を利用して，秘密鍵$\mathbf{K_S}$の探索を行うような計算量的操作が存在する可能性については，実は何も考察されていない．実際，論文[1]では，そのような攻撃の一つの例が示されているのだが，次節では，イブの行う測定過程の記述も含め，より詳細に考察をおこなうことにより，このような攻撃を具体的に構成してゆくことにする．

3. 攻撃の記述とその評価

この節では，はじめにイブが行う量子測定を記述し，次にそこから得られる情報を使うと，イブが秘密鍵$\mathbf{K}_s$の全数探索を行うために必要な「復号アルゴリズム」を構成することができることを示す．さらに，ここでの議論と我々の論文[1]の関係を解説する．

3.1 量子測定の記述

簡単のため（多くの量子プロトコルの安全性証明において仮定されるのと同様に）イブは，アリスが準備した量子状態をそのまま手に入れるものと仮定する．ここで，イブは次の正の演算子達で記述されるPOVM測定を行うものとする．

$$\hat{E}_j = \frac{1}{\pi}\int_0^\infty rdr \int_{\theta_j-\pi/2M}^{\theta_j+\pi/2M} d\theta \; |re^{i(\theta+\arg\alpha)}\rangle\langle re^{i(\theta+\arg\alpha)}| \tag{8}$$

ただし$j \in \{0,1,\cdots,2M-1\}$, $\theta_j = \pi j/M$とする．

$$\sum_{j=0}^{2M-1} \hat{E}_j = I \tag{9}$$

に注意しよう．K_i, r_iが与えられた場合の、測定値jが得られる条件付確率は

$$P(j|K_i,r_i) = \frac{1}{\pi}\int_0^\infty rdr \int_{\theta_j-\pi/2M}^{\theta_j+\pi/2M} d\theta \; |\langle re^{i(\theta+\arg\alpha)}|\alpha e^{i\theta_{K_i,r_i}}\rangle|^2$$

$$= \frac{e^{-|\alpha|^2}}{\pi}\int_0^\infty rdr \int_{\theta_j-\pi/2M}^{\theta_j+\pi/2M} d\theta \; e^{-(r^2-2r|\alpha|\cos\delta_{K_i,r_i}(\theta))}, \tag{10}$$

$$\delta_{K_i,r_i}(\theta) = \theta_{K_i,r_i} - \theta. \tag{11}$$

で与えられる．以下ではi番目の量子状態に対するイブの測定値を$j^{(i)}$と書く．即ち、$j^{(i)}$は確率分布$P(j^{(i)}|K_i,r_i)$を持つことになる。

3.2 復号アルゴリズムの構成

イブは上記の測定で得られる$j^{(i)}$を使って、$q \in \{0,1,\cdots,M-1\}$の関数として次のような関数を定義する．

$$F_{j^{(i)}}(q) = \begin{cases} \tilde{r}_{j^{(i)}} & \text{for } q \in C^+_{j^{(i)}} \\ \tilde{r}_{j^{(i)}} \oplus 1 & \text{for } q \in C^-_{j^{(i)}} \end{cases} \tag{12}$$

ただし、ここで$\tilde{r}_{j^{(i)}}$や$C^{\pm}_{j^{(i)}}$は，

$$\tilde{r}_{j^{(i)}} = \frac{j^{(i)} - \tilde{j}^{(i)}}{M} \oplus \Pi(\tilde{j}^{(i)}), \quad \tilde{j}^{(i)} = j^{(i)} \bmod M, \tag{13}$$

$$C^+_{j^{(i)}} = \{q \mid \; c_{q,j^{(i)}} \geqq 0\} \tag{14}$$

$$C^-_{j^{(i)}} = \{q \mid \; c_{q,j^{(i)}} < 0\}, \tag{15}$$

$$c_{q,j^{(i)}} = \cos\left(\left(\frac{q-\tilde{j}^{(i)}}{M} + (\tilde{r}_{j^{(i)}} \oplus \Pi(q)) - \left(\tilde{r}_{j^{(i)}} \oplus \Pi(\tilde{j}^{(i)})\right)\right)\pi\right)$$

として定義しておく。

イブは，K_iやr_iの値と無関係に（それらを知る必要もなく），測定値$j^{(i)}$のみを用いて，関数$F_{j^{(i)}}(q)$を構成することができることに注意しよう．

このように構成した関数は次の関係式を満たすことが証明できる．

$$F_{j^{(i)}}(K_i) = \begin{cases} r_i, & \text{when } \cos\left(\delta_{K_i,r_i}(\theta_{j^{(i)}})\right) > 0 \\ & \cdots \text{case I} \\ r_i \oplus 1, & \text{when } \cos\left(\delta_{K_i,r_i}(\theta_{j^{(i)}})\right) < 0, \\ & \cdots \text{case II} \\ \text{不定} & \text{when } \cos\left(\delta_{K_i,r_i}(\theta_{j^{(i)}})\right) = 0 \\ & \cdots \text{case III} \end{cases} \tag{16}$$

ただし$\theta_{j^{(i)}} = \pi j^{(i)}/M$であり，$\delta_{K_i,r_i}(\cdot)$は式(11)で与えられている．(図1とキャプションを参照のこと．) ここで，若干の注意が必要である．イブはK_iとr_i（即ち，図1のガウスのピークの位置）を知らないので，自ら構成した関数$F_{j^{(i)}}(q)$が，caseIからcase IIIまでのどのケースに当てはまるか**一見**，判断がつかない．さらに，導入した量子測定に対する不可避の揺らぎのために三つの場合は確率的にすべてが起こり得る．しかしながら，実際には，caseIIやcase IIIが起こる確率を議論することが，**杞憂に過ぎない**ことを，以下のように直接その確率を評価することによって示すことができる．

[case II と case III が起きる確率]

（1） $M \geqq 2$の場合

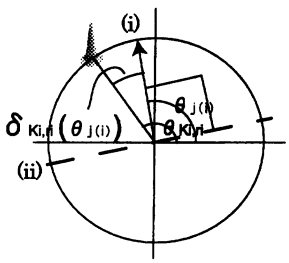
$$\Omega_{K_i,r_i} = \{j \,|\cos\left(\delta_{K_i,r_i}(\theta_j)\right) \leqq 0\}, \tag{17}$$

として，

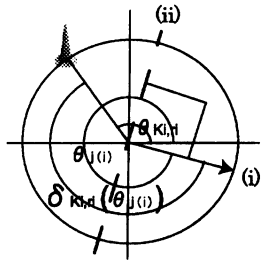
$$Pr[caseII] + Pr[caseIII] = \sum_{j\in\Omega_{K_i,r_i}} P(j|K_i,r_i) \tag{18}$$

$$= \frac{1}{\pi}\int_{\pi/2-\pi/(2M)}^{3\pi/2+\pi/(2M)} d\theta \int_0^\infty rdr \; \exp\left(-\left(\left|r-|\alpha|e^{i\theta}\right|^2\right)\right)$$

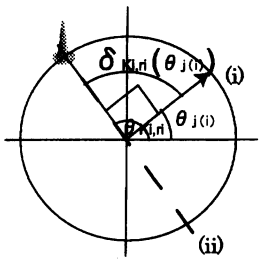
$$< \frac{1}{2}e^{-|\alpha|^2} + \frac{1}{2|\alpha|\sqrt{\pi}\cos\frac{\pi}{2M}}(f_{|\alpha|,\beta_1} - f_{|\alpha|,\beta_2}), \tag{19}$$



case I



case II



case III

図 1 $re^{i(\theta+\arg\alpha)}$ 平面上でみた三つのケース．ガウス型の影は $\frac{1}{\pi}|\langle re^{i(\theta+\arg\alpha)}|\alpha\rangle|^2$ をあらわしている．この三つの場合わけは次のように定義される．(i) イブは測定値として，$\theta_{j(i)}$ (図中の矢印に相当) を得た後，(ii) 原点を通り，矢印に直行する直線によって平面を二つの領域に分ける．(iii) このとき，ガウスのピークと矢印が同じ半平面に含まれているなら case I と呼ぶ．お互いに別の半平面に含まれるなら case II，さらに，ガウスのピークが，(ii) で定義した直線上に乗る場合を case III と呼ぶ．言うまでも無く，イブにはガウス型の影が見えるわけではないので，自分の測定値が case I から case III のどの場合に含まれているかを直接確認できるわけではない．

ただし，

$$\beta_1 = \sin\frac{\pi}{2M}, \quad \beta_2 = \sin\frac{\pi}{2M} - \frac{\pi}{2M}\cos\frac{\pi}{2M}, \tag{20}$$

$$f_{|\alpha|,x} = e^{-|\alpha|^2(1-x^2)}(1 + Erf(|\alpha|x)), \tag{21}$$

とする．

(2) $M = 1$ の場合定義により，

$$Pr[caseIII] = 0 \tag{22}$$

は明らか．さらに

$$Pr[caseII] = \frac{1}{\pi}\int_{\pi/2}^{3\pi/2} d\theta \int_0^\infty rdr\ \exp\left(-\left(\left|r - |\alpha|e^{i\theta}\right|^2\right)\right) < \frac{1}{2}e^{-|\alpha|^2} \tag{23}$$

を得る．

数値にあたってみよう．前述の [3] で想定されている $|\alpha|^2 = 100$, $M = 200$ を用いた場合，case II や case III の起きる確率は

$$Pr[caseII] + Pr[caseIII] \lesssim 10^{-44}. \tag{24}$$

と評価できることがわかる．この確率が意味することは，例えば毎秒アリスが $10^9 (= 1\ G)$ の量子状態を送り続ける状況の場合，case II か case III が起きるのは，期待値として 10^{34} 秒後のことである．この時間スケールは，宇宙の年齢 ($\sim 10^{18}$ 秒) と比べても格段に長い．(即ち，「杞憂」以下の話だということ．) 実際の量子チャンネルによる通信を考える場合，このような稀有な事象を想定しなければならない理由は存在しないだろう．即ち，この場合**イブの構成した関数 $F_{j(i)}(q)$ は“確実に”case I に属しているとしても，なんの問題もない**．後に見るように，この「関数 $F_{j(i)}(q)$ が常に case I に含まれる」という事実は，Y-00 プロトコルの安全性にとって，致命的な問題となる．

また，式 (6) の議論では，M は大きければ大きいほど安全であるように見えたが，上記の観点から考えると，実際には $M = 2$ の選択がベストであることがわかる．ただし，この場合にも case II や case III は，上記と同じ評価をすると，約 10 万年に一度起こる程度であり，「関数 $F_{j(i)}(q)$ が“常に” case I に含まれる」としてもなんの問題にもならない．ここではむしろ，しばしば Y-00 プロトコルの根拠とされる式 (6) の議論が安全性の議論として不完全であったことに注目されたい．

さらに，ここで評価した case II や case III が起きる確率をより小さくするような最適量子測定が存在する可能性があることも指摘しておこう．(このプロトコルの安全性を議論する上では，我々がここで導入した量子測定で十分である．)

ここで，イブが，case I に含まれる関数 $F_{j(i)}(q)$ を確実に構成できるという事実が，Y-00 プロトコルの安全性にとって，いかに致命的な問題となるかを見ていくことにしよう．繰り返しになるが，この関数は，次の性質を持っている．

$$F_{j(i)}(K_i) = F_{j(i)}(PRNG_i(\mathbf{K}_s)) = r_i. \tag{25}$$

即ち，イブは“暗号文” $j^{(i)}$ を手に入れたことにより，秘密鍵 $\mathbf{K}_s$ を入力すれば，メッセージ r_i を出力する復号アルゴリズム $F_{j(i)}(PRNG_i(\cdot))$ を構成することができることを意味している．これは，古典ストリーム暗号において，盗聴者が暗号文を入手して復号アルゴリズムを構成できるのと全く同じ状況であることに注意してほしい．(通常の古典ストリーム暗号の場合，メッセージと秘密鍵が与えられれば暗号文が一意に決定されるのに対し，ここで言う“暗号文” $j^{(i)}$ はコヒーレント状態の持つ不可避な量子揺らぎにより，(case I の範囲にあったとしても) 一意には決定できない．しかし，ここでは復号アルゴリズムを

決定論的に得られることが重要なのであって，もしこの違いを理由に測定値 $j^{(i)}$ を“暗号文”と呼ぶことに抵抗があるのであれば，特にそう呼ばなければいけない理由はないので，安心してほしい．即ち，何を“暗号文”と呼ぶかは単なる解釈の問題ある．この点については，次節も参照のこと．）あとは，古典ストリーム暗号における秘密鍵の探索と全く同じストーリーとなる．既知平分攻撃（あるいはアリスが $|\mathbf{K}_s|$ よりも冗長の大きなメッセージを送る状況）を考えれば，イブは計算量 $2^{|\mathbf{K}_s|}$ の全数探索攻撃を行うことにより，高い確率で秘密鍵 $\mathbf{K}_s$ を探し出すことができる．より正確には，**Y-00 プロトコルは，そこで用いられた $PRNG$ を使った古典同期ストリーム暗号と全く同じ安全性であることが証明されたことになる**．

3.3 式 (25) の操作論的な意味について

ここでは，式 (25) の操作論的な意味についてコメントし，我々の論文 [1] とここでの議論の関係を明確にしておこう．

まず，簡単だが面白い事実として，関数 $F_{j^{(i)}}(q)$ が次のように分解できることに着目しよう．

$$F_{j^{(i)}}(q) = G_{j^{(i)}}(q) \oplus l_{j^{(i)}}, \tag{26}$$

ただし，

$$G_{j^{(i)}}(q) \in \{0,1\}, \quad l_{j^{(i)}} \in \{0,1\}, \tag{27}$$

とする．ここで $l_{j^{(i)}}$ は，測定値 $j^{(i)}$ だけに依存した関数であるとする．このとき，式 (26) を (25) に代入すると，

$$l_{j^{(i)}} = r_i \oplus G_{j^{(i)}}(PRNG_i(\mathbf{K}_s)), \tag{28}$$

が得られるが，ここで $\tilde{k}_i = G_{j^{(i)}}(PRNG_i(\mathbf{K}_s))$ と書き換えれば，この式は我々の論文 [1] の式 (10) に他ならないことがわかる．この $\tilde{k}_i$ は，決定論的アルゴリズム

$$PRNG_i^{(j^{(i)})}(\cdot) := G_{j^{(i)}}(PRNG_i(\cdot)), \tag{29}$$

に，秘密鍵 $\mathbf{K}_s$ を代入して得られる擬似乱数列であると解釈することができる．さて，式 (28) の左辺がイブの測定値のみを含んでいることに注目しよう．これは，イブが右辺の値を秘密鍵 $\mathbf{K}_s$ の助けなしに得られることを意味している．やはりここでも，暗号文として $r_i \oplus \tilde{k}_i$ を出力する古典ストリーム暗号において，盗聴者がその暗号文を手に入れるのと全く同じ状況になっていることが理解できる．

注意してほしいのは，$l_{j^{(i)}}$ の値が i に依存している点である．これは，$i \neq i'$ であれば，たとえ $j^{(i)} = j^{(i')}$ であったとしても必ずしも $l_{j^{(i)}} = l_{j^{(i')}}$ が成立する必要がないことを意味いている．**大事なのは，測定値 $j^{(i)}$ を得て，各 i ごとに $l_{j^{(i)}}$ を決定するイブにとって，アルゴリズム (29) を完全に決定論的に構成できる点**なのである．さらに言えば，イブは $j^{(i)}$ の値に拠らず，常に $l_{j^{(i)}} = 0$ としても全く構わない．この場合には，イブにとってアルゴリズム (29) が $F_{j^{(i)}}(PRNG_i(\cdot))$ そのものになるだけである．前述のように彼女は，測定値 $j^{(i)}$ だけを使って関数 $F_{j^{(i)}}(PRNG_i(\cdot))$ を得られるのだから，彼女にとって何も不都合はないのである．

このように，今回の議論に沿って我々の論文 [1] を見直すと，そこでの我々の議論は，関係式 (28) を満たす $l_{j^{(i)}}$ の別の選び方を，具体的に一つ与えたことに他ならないことがわかる．

4. [1] への反論に対するコメント

既に述べたように，我々の論文 [1] に対して，幾つかの反論が公開されている．それらは，我々の議論への誤解に基づいているように見え，反論としての意味があるかよくわからないが，状況を明確にするために，幾つかのコメントをつけておくことにする．

4.1 我々の議論で無視している量について

反論 [4] の中で，著者達は，本報告中の (28)（我々の論文 [1] の式 (10)）が成立しない確率がおよそ $1\% \sim 10^{-2}$ 程度であり，この誤り確率は無視できず，この関係式に基づいた我々の提案した攻撃手法は無意味だと主張している．(実際，もしこの誤り確率が 1% 程度の大きさであれば，実用的なシステムに対する安全性解析の中でこの確率を無視することはできない．) しかしながら，これは単に，彼らが本報告中の (28) の意味を誤解して，我々が議論している量と違うものについて誤り確率を評価しているだけのように見受けられる．実際彼らは，反論 [4] の中で，式 (28) の左辺の l_i について次のように説明している．*Each l_i is 0 or 1 according to whether the qumode lies on the upper or lower half-circle with respect to the "horizontal" basis given by the all zero running key.* (反論 [5] でも，全く同じ議論が見られる．) しかしながら，本報告や論文 [1] を見ればわかるように，我々の l_i の値は，測定値が平面の上にあるか下にあるかで決定されるものではなく，彼らが何か別のものを議論しているのは明らかである．我々の式 (28) が成立しない確率は，前節で評価した case II と case III が起こる確率そのものであり，その大きさは $Pr[caseII] + Pr[caseIII] \sim 10^{-44}$ あるいは 10^{-23} (式 (24) をみよ．) 程度となる．このような確率で起こる現象を無視することが，リーズナブルである理由は既に説明した通りである．我々が「Y-00 プロトコルが古典ストリーム暗号と等価である」という時には，この確率を無視しているのであり，彼らの言う 1% のなにか別の誤り確率を無視しているわけではない．

4.2 Y-00 はランダム暗号か否かについて

彼らはこの誤解に基づいて同じく [4] の中で，$\mathbf{L}_N = (l_{j^{(1)}}, \cdots l_{j^{(N-1)}})$ に対し，

$$H(\mathbf{L}_N|\mathbf{R}_N, \mathbf{K}_s) \neq 0, \tag{30}$$

が成立するため，Y-00 プロトコルはランダム暗号 [6] の一種であると主張している．これについては，まず，上記の議論と同様に我々の $\mathbf{L}_N$ の意味を正確に把握し，さらに 10^{-44} や 10^{-23} という確率を無視すれば，式 (28) が成立しているのだから，上記 (30) は（この範囲において）誤りであるであることがわかる．さらに，Y-00 プロトコルの安全性を議論する場合には，「メッセージ $\mathbf{R}_N$ と秘密鍵 $\mathbf{K}_S$ を与えたときに暗号文がユニー

クに決定できるか否か」という問題自体が実はあまり重要な意味を持たないことに注意してほしい．前節でも論じたように，この場合，イブが得た情報の何を暗号文と呼ぶかは全く解釈の問題だからである．繰り返しになるが，Y-00 プロトコルの安全性解析で本質的に重要な点は，イブが得た情報により復号アルゴリズムを決定論的に構成できる点であり，何を“暗号文”と呼ぶかではない．

4.3 弱コヒーレント状態を用いた“改良”Y-00 について

以上見てきたように，ここまでの我々の議論は我々が確率 $O(10^{-44})$ あるいは $O(10^{-23})$ で起こる事象を確実に無視できることに基づいている．したがって，我々の提案した攻撃手法を無効とするような Y-00 プロトコルの“改良”を考えるのであれば，まずはこの確率が大きくなるような状況を考えなければならない．上記の確率がこれほどまでに小さな理由は，比較的平均光子数の大きなコヒーレント状態を用いたことにあるので，実装に用いるコヒーレント状態の平均光子数をオリジナルの Y-00 よりも，ずっと小さくすることが考えられる．(実は，この改良の可能性についても我々は論文 [1] の中で言及している．)

実際，反論 [4] の中で著者達も弱コヒーレント状態 ($S := |\alpha|^2 \sim 7 \ll 200$) を用いた Y-00 による鍵配布のシナリオを吟味し，それが可能であると主張している．(ここでは，このシナリオを便宜的に改良 Y-00 と呼ぶことにしよう．) この議論は，(2) で与えられるボブの誤り確率

$$p_B(S) = \frac{1}{2}\left(1 - \sqrt{1 - e^{-4S}}\right) \sim \frac{1}{4}\exp(-4S), \qquad (31)$$

と (19) で与えられるイブの誤り確率（の上限）

$$\bar{p}_E(S) = \frac{1}{2}e^{-S} + \frac{1}{2\sqrt{S}\sqrt{\pi}\cos\frac{\pi}{2M}}\left(f_{\sqrt{S},\beta_1} - f_{\sqrt{S},\beta_2}\right) \qquad (32)$$

が，$S = 7$ の場合に

$$p_B(7) \sim 10^{-13}, \quad \bar{p}_E(7) \sim 10^{-2} \ (\text{for } M = 2). \qquad (33)$$

(アリスとボブが，オリジナルの Y-00 で想定されていたように $M = 200$ と選べば，$\bar{p}_E(7) \sim 10^{-3}$) となり，“有限な”確率の差が生じることを利用したものである．例えば，10^9 回の事象を考えた場合，ボブはほぼ確実に 10^9 個のエラーのないデータを得るのに対し，イブのデータには 10^7 個のエラーが含まれていることになるので，この差を用いてアリスとボブの間で秘密鍵を情報論的に安全な形で生成することになる．$S \sim 7$ という，かなり小さなコヒーレント状態を用いることにより，当初オリジナルの Y-00 が持つと期待されていた「実装のしやすさ」や「扱いやすさ」という利点は大きく損なわれているにしても，安全性を回復する意味においては確かにこのアイディアは（我々自身も [1] で議論していたように）有望な方法であるように見えるかもしれない．しかしながら，次のような実際の実装状況を考えると，このような上記の評価がナイーブであり，やはり安全な鍵配布は行えないことがわかる．というのは，実際の量子チャンネルに必ず存在してしまう減衰の問題である．特に，光ファイバによって実装された量子チャンネルについてはその減衰が大きく，容易にイブよりもボブの方が悪い状況となってしまうからである．このあたりの事情をもう少し丁寧に見ておこう．今，50km のファイバ（透過効率を 0.2 dB/km としよう）によって実装された量子チャンネルを考えよう．この場合，50km の伝送後に受け取るボブの量子状態の光強度（コヒーレント状態の平均光子数）を S^B，アリスが容易したのとほぼ同じ状態を受け取ることのできるイブの光強度を S^E と書けば，この二つの間には $S^B \sim 0.1S^E$ という関係が成立することになる．この場合，$S \sim 7$ が $S^B \sim 7$ を意味するのであれば (33) は，

$$p_B(7) \sim 10^{-13}, \quad \bar{p}_E(70) \sim 10^{-16} \ (\text{for } M = 2), \qquad (34)$$

あるいは $S \sim 7$ が $S^E \sim 7$ を意味していたのであれば，(33) は

$$p_B(0.7) \sim 1.5 \times 10^{-2}, \quad \text{and} \quad \bar{p}_E(7) \sim 1.0 \times 10^{-2}. \qquad (35)$$

と評価しなおされなければならない．イブの誤り確率（の上限）が，既にボブの誤り確率よりも小さくなってしまったことに注目してほしい．このような場合，既に彼ら自身が反論 [4] や [7] で説明しているように（[4] の式 (8) が成立していないため），安全に秘密鍵を生成することができない．ここで，

また，アリスから 100km 離れたボブの場合には

$$S^B \sim 0.01S^E \qquad (36)$$

となるので，安全に鍵配布を行うための必要条件である $p_B(S^B) < \bar{p}_E(S^E)$ が成立するためには，アリスは $S^A \lesssim 1$ のコヒーレント状態を準備しなければならないことがわかる (図 2. を参照のこと)．また，仮に $p_B(S^B) < \bar{p}_E(S^E)$ が満たされたとしても（さらに，そこで安全性証明がつけられたとしても），安全な鍵を生成するためには，秘匿性増強などが必要なことを考えると，鍵の生成率は極めて小さなものとなるだろう．

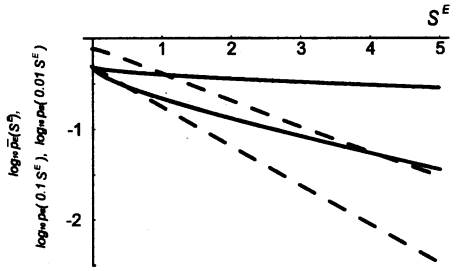


図 2　$p_B(0.01S^E)$（上の実線），$p_B(0.1S^E)$（下の実線），$M = 2$ の $\bar{p}_E(S^E)$（上の破線），および $M = 200$ の $\bar{p}_E(S^E)$（下の破線）の S^E 依存性．$p_B < \bar{p}_E$ は，安全な鍵配布のための必要条件にしか過ぎないことに注意．

さらに，効率については，実装の観点からもう一つ指摘しておきたい．量子プロトコルの鍵生成効率を実験的に見積もると，q をプロトコル固有の因子（例えば BB84 については 1/2），S をアリスが生成する量子状態の平均光子数，ν を繰り返し周波数，η_t を量子チャンネルの透過効率，η_d を検出器の検出効率として

$$R = qS^A\nu\eta_t\eta_d, \qquad (37)$$

となることが知られている [8]. 当初のオリジナルの Y-00 で主張されていたように $S^A\eta_t\eta_d > 1$ であれば，その効率は $R = q\nu$ とすることができた．しかしながら，ここで見てきたように，Y-00 が安全であるためには $S^A\eta_t\eta_d < 1$ とならなければならない．このような場合，その効率は $S^A\eta_t\eta_d$ となり，既に [1] で指摘したように実装的な意味においても，当初主張されていたような効率は達成できないことが理解できる．

5. ま と め

以上見てきたように，本報告において我々は論文 [1] の議論を精緻に再構成し，「Y-00 プロトコルが古典的なストリーム暗号と等価である」という結論を再確認した．この結論は，結局「Y-00 プロトコルは，イブが (25) を満たすような復号アルゴリズム $F_{j^{(i)}}(\cdot)$ を得ることを妨げない」という事実に集約することができる．言い換えれば，Y-00 プロトコルにおける量子性の利用の仕方は，本来量子暗号が持つべき安全性を達成するようなものではなかった，ということになるだろう．量子性の利用により，イブの攻撃に求められる計算量の増加すらなかった点に注意してほしい．このように，少なくとも安全性の観点からは，Y-00 プロトコルをあえて実装しなければならない理由は見当たらない．

新暗号方式の提案とその理論解析（攻撃手法の提案）は，暗号研究の宿命であり，極めて健全なプロセスである．我々の今回の報告もこのプロセスの中の一つに過ぎず，それ以上，あるいはそれ以下の意味を持つものではないだろう．しかしながら，特に今回の解析に関して言えば，我々の成果は（従来あまり見られなかった）情報セキュリティ分野と量子物理のきちんとした融合の結果と考えられるのではないかと自負している．その意味において，特にこの Y-00 プロトコルは，この分野の活性化に貢献したということもできるだろう．さらに，本報告は安全性と効率を兼ね備えたプロトコルの存在を否定するものではなく，むしろここで得られた知見を活かして BB84 を凌駕するような新プロトコルの理論的な探索を積極的に推し進めるべきものであると考えている．また言うまでもないことだが，量子暗号としての意味を別にすれば，光通信技術としての Y-00 周辺技術の開発に水を差すものではない．

我々は，本報告の知見により，量子暗号研究に対する「面白さの共有」と「信頼性の構築」が促進されることを切に希望している．

本研究は，総務省「量子情報通信技術の研究開発」の一環として，情報通信研究機構の委託研究「量子暗号技術の研究開発」として実施された．

文　献

[1] T. Nishioka, T. Hasegawa, H. Ishizuka, K. Imafuku, and H. Imai, "How much security does Y-00 protocol provide us ?," Phys. Lett. **A 237**, pp.28-32, (2004).

[2] S.Wiesner,Sigact News,bf 15, 78, 1983;original manuscript written circa 1970.

[3] G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, "Secure Communication Using Mesoscopic Coherent States," Phys. Rev. Lett. **90** (2003), 227901.

[4] H. P. Yuen, P. Kumar, and E. Corndorf, "Security of Y-00 and similar quantum cryptographic protocols," quant-ph/0407067

[5] 広田　修，"光通信量子暗号 (Y-00) への攻撃は真に攻撃か?PART1" 信学技報, vol. 104, no. 732, ISEC2004-126, pp. 1-6, 2005 年 3 月.

[6] J. L. Massey, "An introduction to contemporary cryptology," Proc. IEEE, **76** (1988), 533-549.

[7] H. P. Yuen, "KCQ: A new approach to quantum cryptography I. General principles and qumode key generation," quant-ph/0311061.

[8] H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, and G. Ribordy, "Quantum cryptography," Appl. Phys. **B67**, pp.743-748, (1998).