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

2005－ＣＳＥＣ－30（48）
2005／7／22

光子数分割攻撃に対する安全性の改善

西田　佳史†　桑門　秀典††　森井　昌克††　田中　初一†††

† 神戸大学大学院自然科学研究科
〒 657-8501 神戸市灘区六甲台町 1-1
†† 神戸大学工学部
〒 657-8501 神戸市灘区六甲台町 1-1
††† 神戸情報大学院大学
〒 650-0001 神戸市中央区加納町 2-2-7
E-mail: †059t240n@y05.kobe-u.ac.jp, ††{kuwakado,mmorii}@kobe-u.ac.jp, †††tanaka@kic.ac.jp

あらまし　単一光子による量子鍵配送方式の実装では，単一光子を発生させることが容易でないため，弱コヒーレント光で代用されることが多い．ところが，弱コヒーレント光を用いると，光子数分割攻撃により，第三者は，通信を行っている二者に盗聴を検出されることなく，盗聴が可能になる．この論文では，光子数分割攻撃に対する安全性を向上させるために，送信者が基底を等確率で選択しない量子鍵配送方式を提案する．送信者が基底を等確率で選択しないと，盗聴者が基底を正しく推定する確率が大きくなる（単純な盗聴攻撃）ため，送信者は基底を等確率で選択する必要があった．しかし，基底を等確率で選択しないことが，光子数分割攻撃と単純な盗聴攻撃の二つの攻撃に対する安全性を同時に向上させるために，鍵生成に必要な送受信するビット数の点で有効な方法であることを示す．
キーワード　量子鍵配送方式，弱コヒーレント光，光子数分割攻撃

Improvement of the Security against Photon Number Splitting Attacks

Yoshifumi NISHIDA†, Hidenori KUWAKADO††,
Masakatu MORII††, and Hatsukazu TANAKA†††

† Graduate School of Sience and Technology, Kobe University
1-1 Rokkodai-cho, Nada-ku, Kobe, 657-8501 Japan
†† Faculty of Engineering, Kobe University
1-1 Rokkodai-cho, Nada-ku, Kobe, 657-8501 Japan
††† Kobe Institute of Computing
2-2-7 Kano-cho, Chuo-ku, Kobe, 650-0001 Japan
E-mail: †059t240n@y05.kobe-u.ac.jp, ††{kuwakado,mmorii}@kobe-u.ac.jp, †††tanaka@kic.ac.jp

Abstract　Since it is difficult for practical optical devices to output a single-photon pulse, a weak laser pulse is often substituted for it in implementations of a single-photon quantum key distribution protocol. It should be noted that the use of the weak laser pulse allows an adversary to eavesdrop communications by photon number splitting attacks. To improve the security against photon number splitting attacks, we propose a quantum key distribution protocol such that the probability that a sender chooses a base from two bases is not 1/2. It follows that the adversary can guess the chosen base with probability greater than 1/2. Hence, the choice with the unequal probability has not been used in single-photon quantum key distribution protocols. However, we show that the choice with the unequal probability is effective in improving the security against photon number splitting attacks and the guess attack in terms of the amount of transmitted bits for generating the key.
Key words　photon number splitting attacks, quantum key distribution, weak laser pulse

1. はじめに

量子鍵配送方式では，第三者の盗聴により，量子状態に変化が起こるので，通信を行っている二者は盗聴を検知できる．このように，量子鍵配送方式の安全性は不確定性原理に基づくため，原理的には技術の進歩に依らず保証される．

光ファイバを用いた量子鍵配送方式では，一つの光子に 1 ビットの情報を符号化して通信を行う．このとき，二つの非直交基底から一方の基底を確率 1/2 で選択し，その基底に属する二つの異なる状態で 1 ビットの情報を表現する．この方式が安全であるためには 1 ビットの情報を一つの光子の状態で表すこと，つまり単一光子の生成が必要となる．

しかし，現在の技術では単一光子の生成が非常に困難であるため，弱コヒーレント光で代用している．弱コヒーレント光を用いると，発生する光子の数が一個とは限らず，多光子が発生することがある．そのため，光子数分割攻撃と呼ばれる攻撃が可能になり，長距離での量子鍵配送を安全に行うことができなくなる [1].

本論文では，BB84 [2] と SARG [3] を組み合わせた方式である MIX [4] の光子数分割攻撃に対する安全性の改善方法を提案する．平均光子数 (弱コヒーレント光に含まれる光子の平均数) を少なくすれば，多光子が発生する確率が低くなるので，光子分割攻撃に対する安全性は向上する．しかし，平均光子数を少なくすると，鍵を生成するために必要となる光子数が多くなる．つまり，一つの光子が鍵の一部となる割合 (鍵生成率) が減少する．そこで，本論文では，基底を選択する確率を等確率にしないことにより，鍵生成率の減少を補うことを検討する．基底の選択確率を等確率にしないと，第三者が選択された基底を正しく推定できる確率が大きくなるため，単純な盗聴攻撃に対する安全性が低下することが懸念される．しかし，光子数分割攻撃と単純な盗聴攻撃の二つの攻撃に対する安全性を同時に向上させるために，基底の選択確率を等確率にしないことが鍵生成に必要な送受信するビット数の点で有効であることを示す．

本論文の構成は以下の通りである．第 2 章で既存の量子鍵配送方式である BB84，SARG，MIX の三方式，光子数分割攻撃について述べる．第 3 章で基底選択の確率の重み付けについて述べた後，光子数分割攻撃，単純な盗聴攻撃に対する安全性の評価を示す．最後に第 4 章で結論を述べる．

2. 量子鍵配送方式と光子数分割攻撃

本章では，量子鍵配送方式 BB84，SARG，MIX の光子数分割攻撃への安全性に関する従来研究を述べる [4].

2.1 量子鍵配送方式

本節では，量子鍵配送方式である BB84，SARG，MIX について説明する．これらの方式は，量子通信フェーズと篩い分けフェーズから構成され，篩い分けフェーズのみが異なる．以下に，量子通信フェーズと各方式の篩い分けフェーズについて述べる．また，一個の量子を送ったときに，鍵が生成される確率を鍵生成率と呼ぶ．送信者を Alice，受信者を Bob，盗聴者を Eve とする．量子状態として，基底 X に属する二状態 $|\pm x\rangle$ と基底 Z に属する二状態 $|\pm z\rangle$ の四状態を用いる．ただし，X 基底，Z 基底は非直交基底とする．

量子通信フェーズ：Alice は四状態からランダムに選択し，選択した量子状態である量子を量子通信路を経由して Bob へ送る．Bob は二つの基底 X，Z から確率 1/2 で選択した基底を用いて，Alice から送られた量子を観測する．

BB84 の篩い分けフェーズ：Alice は送信した量子の状態が属する基底を Bob に，Bob は観測に用いた基底を Alice に知らせる．Alice と Bob は，互いの基底が一致した場合のみ結果を残す．その後，$|+x\rangle, |+z\rangle$ を 0 に，$|-x\rangle, |-z\rangle$ を 1 に変換することにより，秘密鍵を共有する．つまり，鍵となるのは Alice と Bob の基底が一致した場合である．よって，BB84 の鍵生成率は 1/2 となる．

SARG の篩い分けフェーズ：Alice は，送信した量子の状態が属する基底とは異なる基底からランダムに状態を選択する．そして，その選択した状態と送信した量子の状態を古典情報 S として Bob へ知らせる．Bob の観測結果が S に含まれていない場合のみ，Bob は観測した状態と異なる基底に属する状態へ変換する．ただし，変換後の状態は S に含まれている状態とする．その後，$|\pm x\rangle$ を 0 に，$|\pm z\rangle$ を 1 に変換することにより，秘密鍵を共有する．つまり，鍵となるのは Alice と Bob の基底が不一致，かつ，Bob の観測結果が S に含まれない場合である．よって，鍵生成率は $(1/2)^2 = 1/4$ となる．

MIX の篩い分けフェーズ：Alice はランダムコイン投げを行う．このコイン投げは，確率 a で表が出力され，確率 $1-a$ で裏が出力されるものとする．コイン投げの結果が表であるならば BB84 と同じ篩い分けを行い，裏であるならば SARG と同じ篩い分けを行い，秘密鍵を共有する．よって，鍵生成率は $(1+a)/4$ となる．

2.2 光子数分割攻撃

量子鍵配送方式を弱コヒーレント光を用いて実装し，光ファイバで伝送する場合の各パルスに含まれる光子数の分布は平均光子数 μ のポアソン分布に従う．量子状態は，光子数 n の状態の重ね合わせとなり，

$$\sum_n \sqrt{p_\mu(n)}|n\rangle \tag{1}$$

となる．ただし，

$$p_\mu(n) = \frac{e^{-\mu}\mu^n}{n!} \tag{2}$$

である．このとき Bob の光子検出確率の期待値 $R(\delta)$ は，

$$\begin{aligned} R(\delta) &= \sum_{n\geq 1} p_\mu(n)\left[1-(1-\eta_{det}\eta_\delta)^n\right] \\ &\approx \eta_{det}\eta_\delta\mu \end{aligned} \tag{3}$$

となる．ここで，η_{det} は検出器の量子効果，η_δ は Alice–Bob 間の光ファイバの光子損失率である．このとき，多光子が発生することから可能になる攻撃として貯蔵攻撃 (Storage Attack) と完全判別遮断再送攻撃 (Intercept Resend Unambiguous Discrimination Attack) がある．これらを光子数分割攻撃 (Photon Number Splitting Attacks) と呼ぶ [4].

2.2.1 貯蔵攻撃

貯蔵攻撃とは，以下の手順に従って行われる攻撃である．まず，Eve は量子非破壊測定を行い，各パルスの光子数を測定する．次に，一光子しか含まれていないパルスは光子が含まれていないパルスとして Bob へ送り，二光子以上含まれているパルスは一光子だけ Eve が持つ量子メモリに貯蔵し，残りは無損失な量子通信路（$\eta_\delta = 1$）を経由して Bob へ送る．その後，篩い分けフェーズで交換される情報を用いて，量子メモリに貯蔵した光子を観測することにより量子状態を判別する．

Eve が貯蔵攻撃を行ったときの Bob の光子検出確率の期待値 $R(\delta_{ST})$ は，

$$R(\delta_{ST}) = \sum_{n\geqq 2} p_\mu(n)\left[1-(1-\eta_{det})^{n-1}\right] \approx \eta_{det}\frac{e^{-\mu}\mu^2}{2} \tag{4}$$

となる．このとき，

$$\eta_\delta = \frac{e^{-\mu}\mu}{2} \tag{5}$$

を満たす通信距離 ℓ で量子鍵配送を行ったとき，Bob は Eve の攻撃を検知できず，貯蔵攻撃が成功する．ただし，貯蔵攻撃で Eve が得ることができる秘密鍵に関する情報量は，プロトコル毎に以下のように制限される．

BB84 では，篩い分けフェーズで交換される基底の情報により，光子状態は同基底の二状態に制限される．このとき，Eve は光子の基底が分かるため，光子状態は確率 1 で正確に判別できる．よって，BB84 で Eve が貯蔵攻撃により得ることができる秘密鍵に関する情報量の最大値 I_{BB84} は，

$$I_{BB84} = 1 \tag{6}$$

となる．

SARG では，篩い分けフェーズで交換される基底の情報により，光子状態は非直交基底に属する二状態に制限される．このとき，SARG で Eve が貯蔵攻撃により得ることができる秘密鍵に関する情報量の最大値 I_{SARG} は，

$$I_{SARG} = 1 - \mathcal{H}(P) \tag{7}$$

となる．ただし，

$$P = \frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right) \tag{8}$$

であり，$\mathcal{H}(x)$ はエントロピー関数

$$\mathcal{H}(x) = -x\log_2 x - (1-x)\log_2(1-x),\ 0 \leqq x \leqq 1 \tag{9}$$

である．

MIX プロトコルでは，確率 a で BB84 を，確率 $1-a$ で SARG を行うことと等しいため，MIX で Eve が貯蔵攻撃により得ることができる秘密鍵に関する情報量の最大値 I_{MIX} は，

$$I_{MIX} = aI_{BB84} + (1-a)I_{SARG} \tag{10}$$

となる．

2.2.2 完全判断遮断再送攻撃

完全判別遮断再送攻撃とは，以下の手順に従って行われる攻撃である．まず，Eve は量子非破壊測定を行い，各パルスの光子数を観測する．そして二光子以下しか含まれていないパルスは光子が含まれていないパルスとして Bob へ送る．また，三光子以上含まれているパルスには三光子を用いて次のような多光子一括測定 M を行う．

三光子の量子状態は $|\Psi_1\rangle = |+x\rangle^{\otimes 3}$，$|\Psi_2\rangle = |-x\rangle^{\otimes 3}$，$|\Psi_3\rangle = |+z\rangle^{\otimes 3}$，$|\Psi_4\rangle = |-z\rangle^{\otimes 3}$ のいずれかの状態である．ただし，$|+x\rangle^{\otimes 3}$ は三光子全てが $|+x\rangle$ の状態であることを示す．このとき，M は基底 $\{|\Phi_1\rangle, |\Phi_2\rangle, \cdots, |\Phi_8\rangle\}$ を用いて観測する測定であり，

$$\langle\Psi_i|\Phi_j\rangle = \begin{cases} \frac{1}{\sqrt{2}}, & i=j; \\ 0\ , & i \neq j \end{cases} \tag{11}$$

を満たす．ただし，$|\langle\Psi_i|\Phi_j\rangle|^2$ は量子状態が $|\Phi_j\rangle$ である量子を観測したときに $|\Psi_i\rangle$ が得られる確率を意味する．この観測 M を行うことにより，確率 $p_{ok} = 1/2$ で量子状態を完全に判別できる．その後，量子状態が完全に判別できた場合のみ，その状態の量子を複製し，無損失な量子通信路を経由して Bob に送る．Eve が完全判別遮断再送を行ったときの Bob の光子検出確率の期待値は，

$$R(\delta_{IR}) = \sum_{n\geqq 3} p_{ok}p_\mu(n)\left[1-(1-\eta_{det})^{n-1}\right] \approx \eta_{det}\frac{e^{-\mu}\mu^3}{12} \tag{12}$$

となる．このとき，

$$\eta_\delta = \frac{e^{-\mu}\mu^2}{12} \tag{13}$$

を満たす通信距離 ℓ で量子鍵配送を行ったとき，Bob は Eve の攻撃を検知できず，完全判別遮断再送攻撃が成功する．

2.2.3 安全性

以下の仮定の下での光子数分割攻撃に対する安全性の評価を示す [4]．

- 平均光子数以外の物理的なパラメータは一切変更しない．また光ファイバの光子損失以外の誤りは起きない．
- 全てのプロトコルにおいて，プロトコル終了時の鍵生成率を等しくするために，篩い分けフェーズで残る鍵の割合が異なる場合には，平均光子数を変化させる．ただし，BB84 の鍵生成率 1/2 を基準とし全てのプロトコルでの鍵生成率が 1/2 になるように平均光子数を変化させる．
- 光ファイバの光子損失 $\alpha = 0.25$[dB/km]，平均光子数 $\mu = 0.1$[photon/pulse]，光子損失率 $\eta_\delta = 10^{-\alpha\ell/10}$（$\ell$：通信距離 [km]）とする．

通信距離 ℓ で量子鍵配送を行った場合，貯蔵攻撃により Eve に漏洩する秘密鍵に関する情報量 $I_{ST}(\ell)$ は，

$$I_{ST}(\ell) = (10^{\alpha\ell/10}-1)\frac{a+(1-a)L}{\frac{2}{e^{-\mu_a}\mu_a}-1} \tag{14}$$

となる．ただし，L は Eve が貯蔵攻撃により得ることのでき

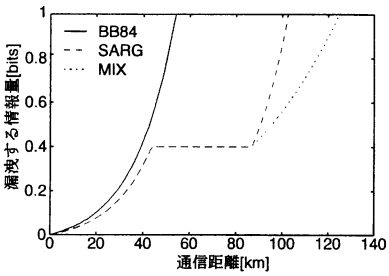

図 1　光子数分割攻撃に対する安全性

る秘密鍵に関する情報量の最大値，μ_a は鍵生成率が 1/2 になるように変化させた平均光子数，a は篩い分けフェーズで Alice が行うコイン投げの表が出る確率とする．$a=1$ は BB84，$a=0$ は SARG を表す．また，完全判別遮断再送攻撃により Eve に漏洩する秘密鍵に関する情報量 $I_{IR}(\ell)$ は，

$$I_{IR}(\ell) = (10^{\alpha\ell/10}-1)\frac{1}{\frac{12}{e^{-\mu_a}\mu_a^2}-1} \tag{15}$$

となる．通信距離 ℓ で量子鍵配送を行った場合，Eve に光子数分割攻撃により漏洩する秘密鍵に関する情報量 $I_{PNS}(\ell)$ を

$$I_{PNS}(\ell) = \max\{I_{ST}(\ell), I_{IR}(\ell)\} \tag{16}$$

と定義する．

式 (14) – (16) から BB84，SARG，MIX の光子数分割攻撃に対する安全性を図 1 に示す [4]．ただし，MIX においてコイン投げで表の出る確率 a の値は，距離に応じて $I_{PNS}(\ell)$ が最小となる値を選ぶ．図 1 より，MIX は約 125 km，BB84 は約 55 km，SARG は約 100 km が安全限界であり，長距離では量子鍵配送が安全に行えない．ただし，安全限界とは Eve が秘密鍵に関する全ての情報を得る Alice–Bob 間の通信距離の最小値を指す．

3. 基底選択の確率に重みを付けた量子鍵配送方式

光子数分割攻撃に対する安全性の向上を目的として，本章では，基底を選択する確率を等確率にしないことを提案し，光子数分割攻撃に対する安全性を評価する．その後，基底選択の確率と単純な盗聴攻撃に対する安全性との関係を示す．

3.1　基底選択の確率の重み付け

光子数分割攻撃に対する安全性の評価は，平均光子数を変化させて鍵生成率を等しくして行われる．よって，平均光子数を少なくすることで光子数分割攻撃に対する安全性が向上する．そこで，光子数分割攻撃に対する安全性の向上のために，鍵生成率の改善を目指す．鍵となるのは篩い分けで残った結果である．そこで鍵生成率を改善するために，篩い分けで残る確率を大きくする方法を示す．

従来，量子通信フェーズにおける Alice と Bob の基底選択時には，二つの非直交基底から確率 1/2 で一方の基底を選択していた．提案方式では篩い分けで残る確率を大きくするように，Alice と Bob が二つの基底から一方を選択する確率を 1/2 より大きくする．このように，基底選択の確率に重みを付けることにより鍵生成率を改善する．Alice と Bob が X 基底を選択する確率をそれぞれ p, q とする．このとき，各方式の鍵生成率は以下のようになる．

BB84 では，鍵となるのは Alice と Bob の基底が一致した場合である．よって，鍵生成率 K_{BB84} は，

$$K_{BB84} = pq + (1-p)(1-q) \tag{17}$$

となる．

SARG では，鍵となるのは Alice と Bob の基底が不一致であり，かつ Bob の観測結果が S に含まれない場合である．よって，鍵生成率 K_{SARG} は，

$$\begin{aligned} K_{SARG} &= \frac{1}{2}\Big(p(1-q)+(1-p)q\Big) \\ &= \frac{1}{2}(1-K_{BB84}) \end{aligned} \tag{18}$$

となる．また，篩い分け後，残った結果を 0, 1 に変換し鍵を生成する．このとき，SARG では，光子状態が X 基底であれば 0 に，Z 基底であれば 1 に変換する．そのため，重みを付けることにより，鍵に 0, 1 が等確率で現れず，鍵自体の情報量が減少する．X 基底の鍵である確率が，$p(1-q)/2$ であるため，重み付けによる鍵の減少量は，

$$1-\mathcal{H}\left(\frac{\frac{1}{2}p(1-q)}{K_{SARG}}\right) \tag{19}$$

となる．また，貯蔵攻撃に対する安全性も変化してしまい，Eve が貯蔵攻撃により得ることができる秘密鍵に関する情報量の最大値は次のようになる．

$$1-\mathcal{H}(\mathcal{P}) \tag{20}$$

ただし，

$$\mathcal{P} = \begin{cases} \dfrac{\frac{1}{2}p+\frac{\sqrt{2}}{4}p-\left(\frac{1}{2}+\frac{\sqrt{2}}{4}\right)pq}{K_{SARG}}, & p \geq q; \\ \dfrac{\frac{1}{2}q+\frac{\sqrt{2}}{4}q-\left(\frac{1}{2}+\frac{\sqrt{2}}{4}\right)pq}{K_{SARG}}, & p < q \end{cases} \tag{21}$$

とする．

MIX は，$a=1$ のときは BB84 を，$a=0$ のときは SARG を行うことと等しい．よって，鍵生成率 K_{MIX} は，

$$K_{MIX} = aK_{BB84} + (1-a)K_{SARG} \tag{22}$$

となる．また，重み付けによる鍵の減少量は，

$$(1-a)\left(1-\mathcal{H}\left(\frac{\frac{1}{2}p(1-q)}{K_{SARG}}\right)\right) \tag{23}$$

となる．また，Eve が貯蔵攻撃により得ることができる秘密鍵に関する情報量の最大値は，

$$a+(1-a)\Big(1-\mathcal{H}(\mathcal{P})\Big) \tag{24}$$

となる．

3.2 確率の重み付けを独立に行う MIX

式 (18) より，基底選択の重み付けにより BB84 の鍵生成率 K_{BB84} を改善すると，SARG の鍵生成率 K_{SARG} が低下することが分かる．つまり，SARG の鍵生成率は BB84 の鍵生成率に依存する．この二者の鍵生成率 K_{BB84} と K_{SARG} を独立に変化させることができるように，MIX を以下のように改良する．

量子通信フェーズ：Alice は四状態 $|\pm x\rangle, |\pm z\rangle$ の量子を準備し，ランダムコイン投げを行う．このコイン投げは，MIX と同様に確率 a で表が出力され，確率 $1-a$ で裏が出力されるものとする．Alice は，コイン投げの結果が表であるならば，確率 p で X 基底の二状態 $|\pm x\rangle$ から，確率 $1-p$ で Z 基底の二状態 $|\pm z\rangle$ からランダムに状態を選択して Bob へ送る．コイン投げの結果が裏であるならば，確率 p' で X 基底の二状態 $|\pm x\rangle$ から，確率 $1-p'$ で Z 基底の二状態 $|\pm z\rangle$ からランダムに状態を選択して Bob へ送る．Bob は確率 q で X 基底を，確率 $1-q$ で Z 基底を選択する．そして，選択した基底の観測器を用いて Alice から受信した量子を観測する．

篩い分けフェーズ：量子通信フェーズのランダムコイン投げの結果に従い篩い分けを行う．量子通信フェーズでのコイン投げの結果が表であったならば，Alice は送った量子の状態が属する基底を，Bob は観測に用いた基底を Alice へそれぞれ相手に知らせる．Alice と Bob は，互いの基底が一致した場合のみ結果を残し，不一致であった結果は全て削除する．その後，$|+x\rangle, |+z\rangle$ を 0 に，$|-x\rangle, |-z\rangle$ を 1 に変換することにより，秘密鍵を共有する．また，量子通信フェーズでのコイン投げの結果が裏であったならば，Alice は送信した量子の状態が属する基底と異なる基底から，ランダムに状態を選択する．そして，その選択した状態と送信した量子の状態を古典情報 S として Bob へ知らせる．Bob の観測結果が S に含まれている場合，Alice と Bob は結果を全て削除する．また，観測結果が S に含まれていない場合，Bob は観測した状態が属する基底と異なる基底に属する状態へ変換する．ただし，変換後の状態は S に含まれているものとする．その後，$|\pm x\rangle$ を 0 に，$|\pm z\rangle$ を 1 に変換することにより，秘密鍵を共有する．つまり，重み付けを独立に行う MIX は，確率 a で p の重みを付けた BB84 を，確率 $1-a$ で p' の重みを付けた SARG を行うことに等しい．よって，鍵生成率 K'_{MIX} は，

$$K'_{MIX} = aK'_{BB84} + (1-a)K'_{SARG} \tag{25}$$

となる．ただし，K'_{BB84} は，

$$K'_{BB84} = pq + (1-p)(1-q) \tag{26}$$

であり，K'_{SARG} は，

$$K'_{SARG} = \frac{1}{2}\Big(p'(1-q) + (1-p')q\Big) \tag{27}$$

である．このとき，p と p' は独立であるため，K_{BB84} と K_{SARG} を独立に変化させることが可能となる．

3.3 光子数分割攻撃に対する安全性

2.2 節と同じ仮定をおいて，MIX の重み付けによる光子数分割攻撃に対する安全性の変化について評価する．式 (14) - (16) と式 (23)，(24) と式 (25) - (27) を用いて Eve に漏洩する秘密鍵に関する情報量を求め，重み付けを行った MIX の光子数分割攻撃に対する安全性を図 2 に示す．ただし，MIX においてコイン投げで表の出る確率 a の値は，距離に応じて $I_{PNS}(\ell)$ が最小となる値とした．

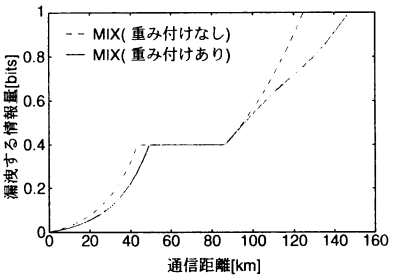

図 2　重み付けの光子数分割攻撃に対する有効性

図 2 より安全限界が 125km から 150km に延びていることが分かる．特に，100km 以上では，重みを付けることにより，安全性が大きく改善された．また，短距離での安全性も向上したことが分かる．つまり，光子数分割攻撃に対して，基底選択の確率に重みを付けることは有効であることが分かる．

3.4 単純な盗聴攻撃に対する安全性

3.3 節では，基底選択の確率の重み付けによる光子数分割攻撃に対する安全性のみを評価した．そこで本節では，基底選択の確率の重み付けによる他の攻撃に対する安全性として単純な盗聴攻撃に対する安全性を評価する．ここでいう単純な盗聴攻撃とは，Eve が Alice から送信される量子を Bob が受信する前に観測し，その後，観測結果と同じ状態の量子を複製し，Bob へその量子を送信する攻撃を指す．

量子鍵配送方式の安全性は不確定原理に根拠をおいている．つまり，Eve の誤った観測により量子の状態に変化が起こり，その変化により盗聴を発見する．この誤った観測とは誤った基底を用いた観測を意味する．従来方法では，Alice，Bob は二つの基底から確率 1/2 で選択するため，Eve は確率 1/2 で誤った観測を行う．しかし，基底選択の確率に重みを付けると，Eve が誤った観測をする確率が小さくなり得る．よって，盗聴を見逃す確率も大きくなり得る．つまり，基底選択の確率に重みを付けることにより鍵生成率は変化するが，単純な盗聴攻撃に対する安全性も変化する．そこで，以下では，重み付けと BB84 の単純な盗聴攻撃に対する安全性の関係を示す．

BB84 において，盗聴の検出は鍵の生成後，生成された鍵の一部を犠牲にして行われる．盗聴がなければ，プロトコル終了後，Alice と Bob が得たランダム列は一致しているはずである．そこで，Alice と Bob は生成された鍵の一部を互いに公開して，比較テストを行う．比較テストで公開したランダム列をテストビットと呼び，テストビットの不一致が，盗聴が行われたことを示す．そこで，テストビットの一致，不一致により盗聴の検出を行う．

鍵の一ビットを比較テストに用いたとする．このとき，盗聴を見逃す確率である盗聴見逃し確率を示す．Alice，Bob，Eve が X 基底を選択する確率をそれぞれ p, q, r とする．盗聴が発見されるのは Eve が Alice，Bob と異なる基底で観測を行ったときであり，かつ，Alice と Bob のビットが異なるときである．

Alice が $|+x\rangle$ を Bob へ送った場合，盗聴が発見される確率を考える．Eve が Alice と Bob とは異なる Z 基底で後にテストビットに使われる量子に対して観測を行うとする．このとき，Eve は X 基底の量子を Z 基底で観測するため，Eve が得る観測結果は確率 1/2 で $|+z\rangle$，確率 1/2 で $|-z\rangle$ となる．その後，観測結果の状態と同じ量子を Bob へ送る．Bob は Alice と同じ X 基底を行うため，Eve から送られた量子が $|+z\rangle$ と $|-z\rangle$ のどちらであろうと基底が異なるため，Bob が得る観測結果は確率 1/2 で $|+x\rangle$，確率 1/2 で $|-x\rangle$ となる．その後，Alice と Bob は，$|+x\rangle, |+z\rangle$ を 0 に，$|-x\rangle, |-z\rangle$ を 1 に変換することにより，秘密鍵を共有する．このとき，Alice と Bob のビットが異なっていると，比較テストにより盗聴が発見される．今，Alice は $|+x\rangle$ を Bob へ送ったため，Bob の観測結果が $|-x\rangle$ であれば Alice と Bob のビットが不一致となり盗聴が露呈する．

以上より，Eve の基底が Alice，Bob の基底と異なり，かつ，その 1/2 のとき盗聴が発見される．よって，テストビットが 1 ビットのとき，盗聴発見確率 P_1 は，

$$P_1 = \frac{\frac{1}{2}pq(1-r) + \frac{1}{2}(1-p)(1-q)r}{K_{BB84}} \tag{28}$$

となる．よって，テストビットが 1 ビットのとき，盗聴見逃し確率 $\overline{P_1}$ は，

$$\overline{P_1} = 1 - P_1 \tag{29}$$

となる．また，テストビットが n ビットのとき，盗聴見逃し確率 $\overline{P_n}$ は，

$$\overline{P_n} = \overline{P_1}^n \tag{30}$$

となる．

以下の仮定の下で基底選択の確率に重みを付けた場合の単純な盗聴攻撃に対する安全性の評価を行い，盗聴見逃し確率と送受信する総ビット数の関係を示す．

- Alice，Bob，Eve が X 基底を選択する確率をそれぞれ p, q, r とする．
- 安全性評価は BB84 において行い，Eve は Alice，Bob の基底選択の確率 p, q を知っている．
- Eve は Alice が Bob に送信する全ての量子を盗聴する．
- 光ファイバの光子損失を含め，あらゆる誤りは起きない．

式 (28) – (30) より，図 3 – 5 に盗聴見逃し 2^{-10} の鍵をそれぞれ図に示したビット数だけ生成するために必要な送受信する総ビット数と基底選択の確率との関係を示す．各図では生成する鍵のビット数を同じにしたときの送受信する総ビット数を比較している．そのため，総ビット数が最少の場合が最も安全であるといえる．また，各図の p, q はそれぞれ Alice，Bob が X 基底を選択する確率を意味する．

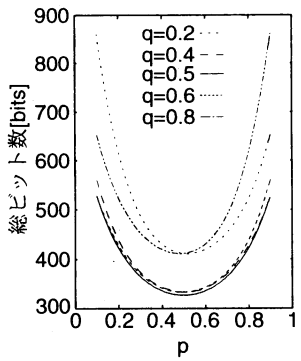

図 3　盗聴見逃し確率 2^{-10} で鍵 128[bits] 生成

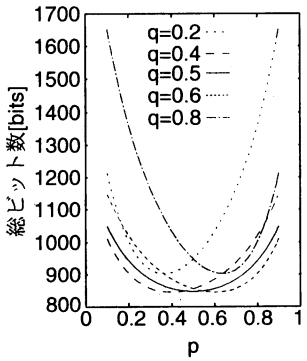

図 4　盗聴見逃し確率 2^{-10} で鍵 388[bits] 生成

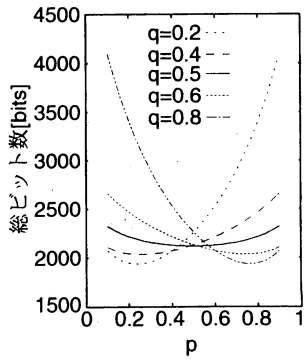

図 5　盗聴見逃し確率 2^{-10} で鍵 1[kbit] 生成

図 3 においては，$p = q = 0.5$ の場合に送受信する総ビットが最少になっているが，図 4 においては，$p = q = 0.5$ の場合と，$p = 0.4, q = 0.6$ または $p = 0.6, q = 0.4$ の場合の総ビット数が同数で最少となっている．そして，図 5 では，重みのない $p = q = 0.5$ の場合より基底選択の確率に重みを付けた場合の総ビット数が少ないことが分かる．つまり，確率に重みを付けることで常に安全性が下がるというのではなく，必要とする鍵のビット数によっては，基底選択の確率に重みを付けることで単純な盗聴攻撃に対する安全性が向上することが分かる．また，必要な鍵のビット数が少ない場合は重みを付けない場合が

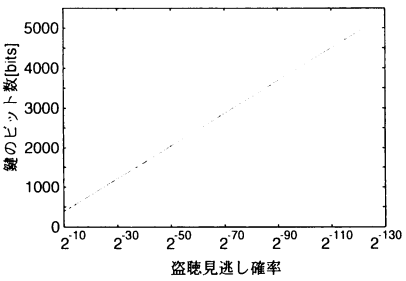

図 6　盗聴見逃し確率と重み付けなしで最も安全となる鍵のビット数の上限の関係

安全であり，必要な鍵のビット数が増えると確率に重みを付けることにより，安全性が増すことが分かる．

そこで，生成する鍵のビット数と単純な盗聴攻撃に対する安全性の関係を図 6 に示す．図 6 において縦軸の鍵のビット数は，確率の重み付けなし（$p = q = 0.5$）が最も安全である場合における生成する鍵のビット数の最大値を示す．例えば，盗聴見逃し確率が 2^{-30} のとき，鍵のビット数は 1215 ビットである．このとき，生成する鍵が 1215 ビット以下であるならば，確率の重み付けなしで BB84 を行うことで最も送受信する総ビット数を少なくでき，生成する鍵が 1215 ビットより多いならば，確率に重みを付けないで BB84 を行うよりも基底選択の確率に適切な重みを付けて BB84 を行うことで最も送受信する総ビット数を少なくできることを意味する．図 6 より，生成する鍵のビット数が多いほど，安全性が低い（盗聴見逃し確率が大きい）ほど，確率の重み付けを行うことにより送受信する総ビット数を少なくできることが分かる．

4. ま と め

本論文は，光子数分割攻撃に対する安全性の向上を目的とし，基底選択の確率の検討を行った．弱コヒーレント光を用いた量子鍵配送方式には，光子数分割攻撃により長距離では安全に鍵配送を行えないという問題がある．この問題に対し，既存のプロトコルである MIX を改良した上で基底選択の確率を変えることを提案した．提案方法による光子数分割攻撃に対する安全性を評価し，特に長距離において安全性が大きく向上することを示した．また結果として，基底選択の確率の重み付けが光子数分割攻撃に対して有効であることが分かった．確率の重み付けを行った場合の他の攻撃に対する安全性として，単純な盗聴攻撃に対する安全性を検討し，単純な盗聴攻撃に対する鍵の安全性と確率の重み付けの関係を示した．それにより，必要とする鍵のビット数と鍵の安全性によって基底選択の確率の重み付けは通常攻撃に対する安全性も向上させることが判明した．

論文中では，重み付けを行った場合の安全性の評価を光子数分割攻撃，単純な盗聴攻撃に対する安全性という点から行った．そこで，他の盗聴攻撃に対する安全性を評価する必要がある．

文　献

[1] N. Lütkenhaus, "Security against individual attacks for realilstic quantum key distribution," *Physical Review A*, vol. 61, no. 5, 052304, 2000.

[2] C. H. Bennet and G. Brassard, "Quantum cryptography: public-key distribution and coin tossing," *Proceedings of the ieee International Confernce on Conputers, Systems and Signal Processing*, pp. 175–179, 1984.

[3] V. Scarni, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Physical Review Letters*, vol. 92, no. 5, pp. 579–582, 2004.

[4] 江口誠，萩原学，今井秀樹，"量子鍵配送プロトコルの光子数分割攻撃に対する頑強性に関する研究," CSS2004 予稿集, pp. 541–546, 2004.