〈一般研究課題〉　安心・安全・快適なネット環境を提供する
量子通信に関する基礎研究

助 成 研 究 者　愛知県立大学　　臼田　毅

安心・安全・快適なネット環境を提供する量子通信に関する基礎研究

臼田　毅
(愛知県立大学)

Fundamental study on quantum communications: Toward realization of a safe, secure, and comfortable information network

Tsuyoshi Sasaki Usuda
(Aichi Prefectural University)

Abstract：

Recently, the KCQ (Keyed Communication in Quantum noise) principle has been received much attention as a new quantum cryptographic principle. The KCQ principle is expected to bring about a secure and fast communication. In this study, we consider KCQ key generation protocols based on non-symmetric signals such as ASK or finite CPPM signals. As a result, dependence of attackers' error performance on initial keys is shown to be negligible and advantage creation of legitimate users is possible under individual attacks with semi-classical quantum receivers.

１．はじめに

「一家に１台パソコン」「１人１台携帯電話」と叫ばれた時代も終わり，iPhoneやiPadなどの携帯情報端末の普及によって，１人で複数の情報機器を取り扱うのが当たり前になってきた。情報機器は住民生活の奥深くに入り込み，インターネットなどの情報ネットワークは道路などと同じレベルのインフラとなりつつある。しかし，便利なネット生活とは裏腹に，プライバシー侵害，ウイルス感染，情報流出といった問題も深刻になっており，より安心・安全なネット環境が望まれる。他方，ネット上を流れる情報量はますます増大し，快適なネット生活を享受し続けるため，通信のさ

らなる高速化も必要であり，安心・安全と快適さの両立が望まれる。

安心・安全を追求するものとしては，暗号や認証技術が盛んに研究され，導入されているが，WEPなどに代表されるように，少なくとも10年以上は安全と言われた暗号技術も破られている。これは，現在の暗号技術が数学的な複雑さを安全性の根拠とし，時間さえかければ原理的には解読可能であることによる。これに対し，物理学の原理を安全性の根拠とする量子暗号技術が注目されている。これまでの量子暗号の研究のほとんどを占めているのは，1984年に提案されたプロトタイプであるBB84方式 [1] あるいはその派生方式 (例えば，[2], [3]) の研究である。このBB84方式に関しては，理論研究はもちろん，実験研究も数多く行われ，特に2000年以降は，国内外で多額の予算をかけた継続的な実験研究が進められているが，実験研究が本格化してから10数年以上経った現在でも，極低温への冷却を要するなど高コストで通信速度も低く，現状の延長線上で開発が順調に進んだとしても軍用など用途が限られるとも言われている。このため，一般住民の安全なネット生活に結びつけることは，このままでは期待できない。また，ヨーロッパ製の量子暗号装置を使った実験で，盗聴不可能とされる量子暗号の盗聴に成功したとの報告があったり [4]，安全性解析の研究に疑問が投げかけられている (例えば，[5], [6], [7])。前者は実装上の問題で，本来のBB84方式自体の問題ではないとも言われ，後者の主張は，最悪の場合にセキュリティが破られることを否定できないというものではあるが，BB84ファミリーを唯一の解とすることには危険性があるとは言える。

本研究は，次々世代の超高速光通信と目されるコヒーレント状態を用いた量子通信技術を基盤とし，攻撃者と正規受信者の量子検出限界の違いを利用したシステム設計により，真に安心・安全かつ高速(快適)なネット環境を提供する量子通信システムを明らかにすることを目指している。攻撃者と正規受信者の量子検出限界の違いを利用する，いわゆるKCQ (Keyed Communication in Quantum noise) 方式 [8] は，BB84ファミリーとは全く異なる原理を安全性の根拠とするものといえる。本稿では，KCQ方式を用いた鍵生成の安全性に関わる基本解析として，非対称量子信号を用いたKCQ実現法における攻撃者と正規受信者の量子検出限界について明らかにする。

2．非対称量子信号を用いたKCQにおける攻撃者と正規受信者の量子検出限界

2.1. KCQ方式の概要

従来の量子暗号鍵配布(QKD: Quantum Key Distribution)とは異なる原理による鍵生成であるKCQ (Keyed Communication in Quantum noise) 鍵生成が，Yuenによって提案されている。旧来のBB84プロトコルなどの量子暗号は，鍵生成の機能を追求するもので，量子鍵配布とも呼ばれ，その安全性は，盗聴者の侵入レベル検出あるいは侵入レベル推定に基づいている。これに対し，KCQプロトコルは，2つの点で旧来の量子暗号と異なっている。まず第一番目に，安全性の根拠が，侵入レベル推定ではなく，正規受信者と盗聴者の量子最適受信能力の違いによっている点が，BB84とは異なる。この量子最適受信能力の違いは，送受信者であらかじめ共有した秘密鍵により引き起こされる。すなわち，鍵を持つ受信者が可能な量子最適受信機と，鍵を持たない盗聴者の量子最適受信機が異なることが重要な意味を持つ。第二番目に，プロトコルの機能として，鍵生成だけでなく直接暗号化ができる点が，BB84等とは異なっている。これまでに，KCQプロトコルの装置化が米国と日本で行われているが，いずれも直接暗号化の機能を追求するものであり (例えば，

[9], [10]), 物理暗号として超高速な直接暗号化を追求することが，現在のKCQプロトコル実装のメインテーマである。安全性の議論も直接暗号化に関するものがほとんどである (例えば，[11], [12], [13], [14])。KCQの直接暗号化プロトコルは，AlphaEta (α η) あるいはY-00プロトコルと呼ばれている。しかし，近年，KCQ鍵生成に関するYuenの論文がIEEEのジャーナルに掲載された [5]。その内容は，2003年に公表されていたKCQの一般理論の中で，特に鍵生成に関する部分を強調し加筆されたものである。量子暗号による鍵生成は，BB84以来，25年以上の歴史があり，一見新しくないようにも見えるが，先述の通り，KCQによる鍵生成 (以降KCQ鍵生成) はBB84とは全く異なる原理に基づく鍵生成であり，今後発展していく余地がある。BB84一辺倒で研究が進められることが危険であるという側面も考慮すべきであろう。KCQの研究は直接暗号化に関するものがほとんどであると述べたが，鍵生成についても皆無というわけではない。実際，発明者のYuen自身が考察を進めているが，Yuenのグループの実験部隊は，いわゆるPSK (Phase Shift Keying) 方式を進めており [9]，YuenによるKCQ鍵生成の考察もPSK方式が主で，あとは原理を説明するためにCPPM (Coherent Pulse Position Modulation) を用いた漸近的特性の考察があるのみである [5]。しかしながら，これだけでは十分とは言えない。KCQ直接暗号化の研究は，Yuenグループ以外に，日本の玉川大学のグループが進めており，そこで採用されている方式は，ASK (Amplitude Shift Keying)，あるいは正確にはISK (Intensity Shift Keying) 方式である [10]。PSKあるいは(漸近的な)CPPMとASKやISKとの大きな違いは，前者がいわゆる対称信号であるのに対し，後者が非対称信号である点にある。前者は理論的には扱いやすいが，実装あるいはコスト面では圧倒的に後者が優れており，また，大容量通信のために不可欠なQAM (Quadrature Amplitude Modulation) なども非対称信号であることを考えると，設計の自由度や可能性という意味でも，非対称信号に関する研究を進めることは有意義である。なお，QAMを用いた直接暗号化については，加藤による理論研究がある [15]。このように，非対称信号を用いたKCQ鍵生成の安全性解析を行うことが必要であり，本研究ではASK方式と有限のCPPM方式に関する研究を進めた [16], [17]。以下，ASK方式について説明していく。

2.2. ASKを用いたKCQ鍵生成

本研究では，以下のM元ASK コヒーレント状態を扱う。

$$|\psi_i\rangle = \left|\frac{i-1}{M-1}\alpha\right\rangle \quad (i = 1, 2, \cdots, M) \tag{1}$$

ここで，αは最大コヒーレント振幅である。図1にM = 14の場合のASKコヒーレント状態の位相平面表示を示す。

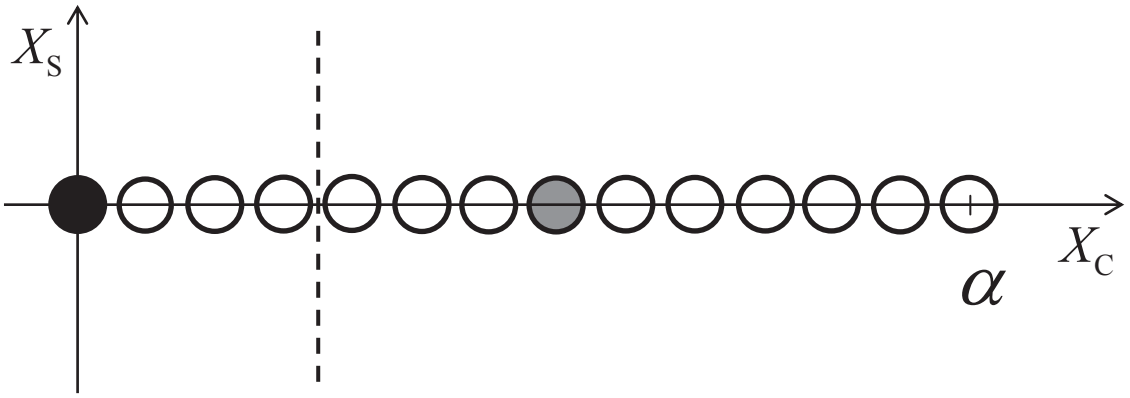

図1　ASKコヒーレント状態（*M*=14の場合）

送信者は，***M*** 個の状態のうち，初期共有鍵に基づいて定められた2 つの状態のいずれかを2 値信号として送り，正規受信者は，信号間距離が約 $\alpha/2$ の2ASK信号の識別を行う。一方，盗聴者は，鍵の知識がないため，いったん多値信号 (***M***-ASK) の測定を行わなければならない。盗聴戦略としては，通信路を流れる信号を分岐してエネルギーの一部を奪うビームスプリッティング攻撃やプローブ攻撃などが考えられるが，ここでは，Yuenの安全性解析を踏襲し，盗聴者には送信量子状態のフルコピーが一つ与えられるものとする。これにより，盗聴者の能力の上界を評価できる。さらに，盗聴者は，測定後，仮想的に鍵の開示を受けるものとする。これも「上界」評価のための解析テクニックである。盗聴者が，この「鍵」を用いて古典的な最適決定を行った場合を考える。例えば，*M*=14の場合の例として，鍵がkey-1 のときに送信者は図1の黒色または灰色の状態を送信するものとすると，結果として盗聴者は図の黒破線を閾値とする最適決定を行う。このような測定・決定を行う受信機は，半古典的量子受信機と呼ばれる。同様に，鍵がkey-k のとき送信者は状態$|\psi_k\rangle$または$|\psi_{k+6}\rangle$を送信するものとする。なお，$|\psi_k\rangle$と$|\psi_{k+6}\rangle$に対する送信ビット情報0, 1の割り当て方は，別途適切に定める。$|\psi_k\rangle$には0，$|\psi_{k+6}\rangle$には1というような固定的な割り当て方は適切ではない。

さて，正規受信者が2 値信号に対する量子最適受信機を利用可能であるのに対し，盗聴者の利用可能な受信機は，上界評価のための仮想的な状況下でも最高で半古典的量子受信機となるため，両者の誤り率特性に差ができる。これがKCQ鍵生成における優位性の確立である。実際のシステムでは，盗聴者は量子状態のフルコピーを与えられるわけでもなく，測定後に鍵の開示も受けないので，半古典的量子受信機による誤り率特性は，実際の盗聴者の受信機性能の緩い上界となる。この状況は，侵入レベル推定を正確に行うことが安全性の起源であり，少しでも緩い上界を扱おうものなら安全に生成できる鍵レートがすぐにゼロになってしまうBB84とは，まったく異なっている。優位性の確立ができたならば，必要に応じ，誤り訂正や秘匿性増強を行い，安全な鍵を得る。現在，BB84には秘匿性増強がうまく働かないのではないかという指摘がなされている。BB84などは，盗聴者によって量子状態が乱されることを利用するため，優位性の確立の時点での送信者－正規受信者および送信者－盗聴者の通信路が，盗聴者の意図したようないびつな通信路になっている恐れがあり，相互情報量からわかる安全性レベルに大きな幅ができてしまい，安全性レベルが極めて低いことを否定できないとの指摘である。一方，KCQは，侵入レベル推定をせず，盗聴者に翻弄される仕組みになっていないこと，盗聴者に量子状態のフルコピーを与えるというように，余裕

を持った安全性解析を行うこと，解析自体が相互情報量規準ではなく，誤り率規準で行われていることなどから，BB84への指摘をそのまま受けるものではない。

2.3. ASK型KCQ鍵生成における盗聴者と正規受信者の誤り率特性

非対称信号であるASKを用いた場合，対称信号であるPSKなどとの大きな違いとして，初期鍵に依存して盗聴者の誤り率が変わることが挙げられる。これは，いわば通信路がいびつになることを意味するため，真っ先に調べておく必要がある。以下，これを調べる。

まず，盗聴者は，半古典的量子受信機における量子測定として，M-ASK信号に対するSRM (Square-root measurement) を行うものとする。SRM は，2ASK 信号に対しては誤り率を最小とする量子最適測定であり，M-ASK 信号に対しても準最適測定であることが知られている。結論を先に言えば，盗聴者の誤り率の初期鍵依存性は，多少はあったものの，その変動幅は非常に小さいものであった。例えば，M=14の場合，key-k (k = 2, ... , 7) を使用した場合の誤り率P_{e}(key-k)とkey-1 の誤り率P_{e}(key-1)の差を規格化した以下の量について，その特性を調べた結果，平均光子数40以下では，key-1 との差が最大で約6%であることから，用いる鍵の種類によらず，誤り率にほとんど変化が無いと言える。

$$\triangle P_{\mathrm{e}}(k) = \frac{P_{\mathrm{e}}(\text{key-1}) - P_{\mathrm{e}}(\text{key-}k)}{P_{\mathrm{e}}(\text{key-1})} \times 100 \quad [\%] \tag{2}$$

盗聴者の誤り率の鍵による依存性がほとんど無いことがわかったので，次に，各平均誤り率を調べる。図2は，パラメータN_0に対する平均誤り率のグラフである。N_0は送信される2値信号をOOK (On-Off Keying) に対応させた場合のOnの平均光子数である。

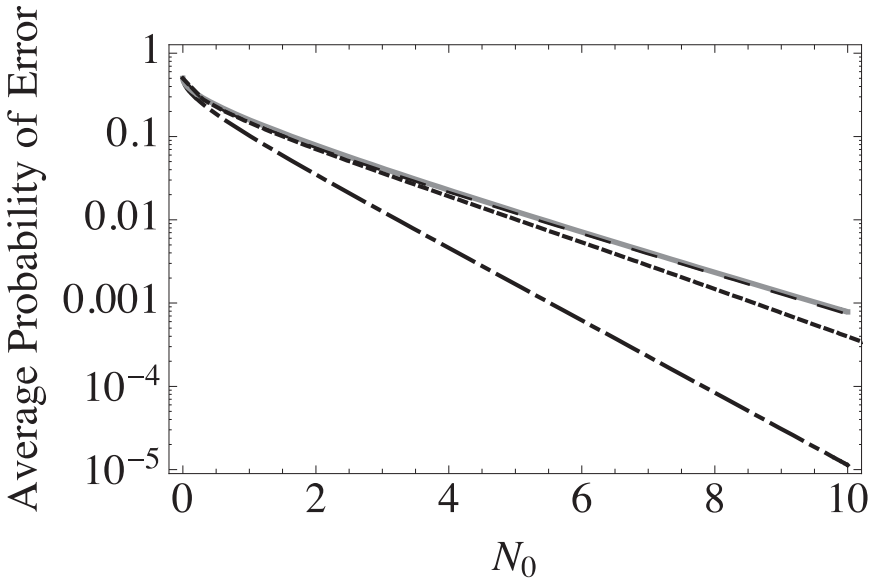

図2　ASK型KCQ鍵生成における正規受信者の誤り率と盗聴者の誤り率（下界）
一点破線：量子最適受信機（正規受信者），グレー実線：ホモダイン受信機，
点線と破線：半古典的量子受信機（点線はM=10，破線はM=30）

図2において，一番下の線が正規受信者の誤り率を表しており，残りの3本の線が盗聴者の誤り率下界を表している。図から，明らかに正規受信者の誤り率の方が良い(低い)。また，盗聴者に

とっての最適測定に対応する半古典的量子受信機は，信号数Mが大きいほど誤り率が高くなっているが，M=30でもすでに古典的最適受信機であるホモダイン受信機とほぼ同じ特性となることがわかる。実際の信号数は，現在のY-00の実験でもすでに数百から数千であるため，ホモダイン受信機の誤り率特性を調べることによって，盗聴者の能力をおよそ見積もることができることがわかる。

4．まとめ

本稿では，安心・安全・快適なネット環境を提供する量子通信に関する基礎研究の中で，主に「安心・安全」に着目した新量子暗号KCQについてASK型の基本特性を明らかにした [16]。KCQの中でCPPM型の基本特性に関しては [17] に示している。また，「快適」なネット環境のため，波長分割多重による量子通信路容量 [18]，量子準最適受信機の実現化 [19], [20]，擬似ベル状態援助による古典情報伝送 [21], [22]，エンタングルメント純粋化 [23] などの研究も進めている。詳細な結果については，各公表論文 ([16]-[23]) を参照していただきたい。「安心・安全」を目指す新量子暗号の安全性解析の基礎をなすのは量子最適検出の研究であり，「快適」を目指す量子通信の実現のためには量子受信機の研究が不可欠である。また，量子信号の数学的な取り扱いと言った基礎研究も重要である。関連研究成果に [24]-[31] などがある。

謝辞

本研究を遂行するにあたり，研究協力していただいた愛知県内大学量子情報研究グループの学生の皆さんに謝意を表します。

参考文献

[1] C.H. Bennett, G. Brassard, Quantum Cryptography: Public Key Distribution and Coin Tossing, Proc. of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, pp.175-179, (1984).

[2] A.K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett., vol.67, no.6, pp.661-663, (1991).

[3] C.H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett., vol.68, no.21, pp.3121-3124, (1992).

[4] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nature Photonics, vol.4, pp.686–689, (2010).

[5] H.P. Yuen, Key generation: Foundations and a new quantum approach, IEEE J. of Selected Topics in Quantum Electronics, vol.15, pp.1630-1645, (2009).

[6] H.P. Yuen, Fundamental quantitative security in quantum key distribution, Phys. Rev., vol. A82, 062304, (2010).

[7] O. Hirota, Incompleteness and limit of quantum key distribution theory, arxiv.org:quant-ph/1208.2106v2, (2012).

[8] H.P. Yuen, KCQ: A new approach to quantum cryptography I. General principles and key generation, arxiv.org:quant-ph/0311061v6, (2004).

[9] E. Corndorf, C. Liang, G.S. Kanter, P. Kumar, and H.P. Yuen, Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks, Phys. Rev., vol.A71, 062326, (2005).

[10] O. Hirota, M. Sohma, M. Fuse, and K. Kato, Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme, Phys. Rev., vol.A72, 022335, (2005).

[11] S. Donnet, A. Thangaraj, M. Bloch, J. Cussey, J. M. Merolla, and L. Larger, Security of Y-00 under heterodyne measurement and fast correlation attack, Phys. Lett., vol.A356, pp.406-410, (2006).

[12] H.P. Yuen and R. Nair, On the security of Y-00 under fast correlation and other attacks on the key, Phys. Lett., vol.A364, pp.112-116, (2007).

[13] O. Hirota and K. Kurosawa, Immunity against correlation attack on quantum stream cipher by Yuen 2000 protocol, Quantum Information Processing, vol.6, no.2, pp.81-91, (2007).

[14] M.J. Mihaljevic, Generic framework for the secure Yuen 2000 quantum-encryption protocol employing the wire-tap channel approach, Phys. Rev., vol.A75, 052334, (2007).

[15] K. Kato and O. Hirota, Quantum quadrature amplitude modulation system and its applicability to coherent-state quantum cryptography, Quantum Communications and Quantum Imaging III, Proc. of SPIE, vol.5893, pp.19-26, (2005).

[16] 清水麻衣子, 山下比呂, 臼田毅, ASK型KCQ鍵生成における盗聴者の誤り率の初期共有鍵依存性, 平成24年度電気関係学会東海支部連合大会, 講演論文集, P1-5, (2012).

[17] H. Yamashita, T.S. Usuda, and S. Usami, Error performance of semi-classical quantum receivers for CPPM signals in KCQ key generation, Proc. of ISITA2012, pp.311-314, (2012).

[18] K. Ohashi and T.S. Usuda, Property of capacity by WDM for attenuated quantum channel, Proc. of ISITA2012, pp.215-218, (2012).

[19] 近藤隆司, 山下比呂, 宇佐見庄五, 臼田毅, 3相PSK信号に対する量子準最適受信機における信号決定方針の考察, 平成24年度電気関係学会東海支部連合大会, 講演論文集, O2-8, (2012).

[20] 近藤隆司, 山下比呂, 宇佐見庄五, 臼田毅, 多元信号に対する量子準最適受信機におけるフィードバック機構の最適化, 第35回情報理論とその応用シンポジウム, pp.139-144, (2012).

[21] H. Takeuchi, S. Yamaguchi, and T.S. Usuda, Entanglement-assisted classical communication using quasi-Bell states, The 1st International Workshop on Entangled Coherent State and Its Application to Quantum Information Science -Towards Macroscopic Quantum Communications-, (2012).

[22] 山口翔太, 竹内博貴, 臼田毅, 減衰を受けた擬似ベル状態を用いたエンタングルメント援助通信のエンコード最適化, 第35回情報理論とその応用シンポジウム, pp.550-555, (2012).

[23] S. Nagahashi, T.S. Usuda, and I. Takumi, Improvement of 2-EPP using quantum error correcting codes and binary search, Proc. of ISITA2012, pp.202-205, (2012).

[24] T.S. Usuda, Y. Ishikawa, and K. Shiromoto, A class of group covariant signal sets and its necessary and sufficient condition, Abstract of Papers of QCMC2012, p.361, (2012).

[25] K. Nakahira and T.S. Usuda, A generalized Dolinar receiver with inconclusive results, Abstract of Papers of QCMC2012, p.229, (2012).

[26] K. Nakahira, T.S. Usuda, and K. Kato, Discrimination between geometrically uniform quantum states with inconclusive results, Phys. Rev., vol.A86, no.3, 032316, (2012).

[27] K. Nakahira and T.S. Usuda, Optimal receiver for discrimination of two coherent states with inconclusive results, Phys. Rev., vol.A86, no.5, 052323, (2012).

[28] K. Nakahira and T.S. Usuda, Minimum Bayes-cost discrimination for symmetric quantum states, Phys. Rev., vol.A86, no.6, 062305, (2012).

[29] 中平健治, 臼田毅, 加藤研太郎, Inconclusive 量子最適測定およびその導出過程に対する幾何学的解釈, 電子情報通信学会論文誌 (A), vol.J96-A, no.1, pp.56-66, (2013).

[30] K. Nakahira and T.S. Usuda, Quantum measurement for group covariant state set, Phys. Rev., vol.A87, no.1, 012308, (2013).

[31] Y. Yazaki, S. Usami, and T.S. Usuda, Superiority of 2-EPPs to 1-EPPs with finite entangled resources, Proc. of ISITA2012, pp.206-210, (2012).