様式 C-19

科学研究費補助金研究成果報告書

平成 22 年　6 月 17 日現在

研究種目：若手研究(B)
研究期間：2008～2009
課題番号：20700018
研究課題名（和文）　量子理論を用いたセキュリティ基盤プロトコルとその応用

研究課題名（英文）　Basic protocol for security using quantum theory and its application

研究代表者
早稲田　篤志（WASEDA ATSUSHI）
独立行政法人情報通信研究機構･情報通信セキュリティ研究センターセキュリティ基盤グループ・専攻研究員
研究者番号：10455454

研究成果の概要（和文）：量子通信路の評価と新たな量子秘密分散法の提案を行った．量子通信路の評価として量子測定ができると通信路容量が劇的に向上することが示された．量子秘密分散法は多くのセキュリティプロトコルに応用される基盤技術の一つである．この量子秘密分散法について新たなプロトコルを提案し，評価を行い，既存研究において耐性がなかった攻撃に対し強い耐性を有することを示した．

研究成果の概要(英文)：I evaluate the quantum channel and propose the quantum secret sharing scheme(QSSS). In evaluation of the quantum channel, I obtain the result the quantum measurements provide a drastic increase of the transmission rates. Quantum secret sharing is one of the basic protocols of information security. I propose the QSSS and show that proposal scheme is secure against several well-known attacks on QSSS.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	800,000	240,000	1,040,000
2009 年度	700,000	210,000	910,000
年度			
年度			
年度			
総　計	1,500,000	450,000	1,950,000

研究分野：量子セキュリティ
科研費の分科・細目：情報学・情報学基礎
キーワード：量子計算理論，量子セキュリティ

１．研究開始当初の背景

現在利用されている代表的なセキュリティシステムである RSA 暗号や DSA 署名などは安全性を計算量的困難性においている．しかしながら，昨今の計算機性能の発達，特に量子計算機の研究と 1994 年に Shor により提案された Shor のアルゴリズムにより，これらのセキュリティシステムの安全性が危ぶまれている．その一方で量子理論を取り入れたセキュリティ方式については量子鍵配送の無条件安全性で知られているように，量子状態を導入することで既存のセキュリティプ

ロトコルよりも高いレベルでセキュリティが確保できるであろうことが期待できる．しかしながら，量子鍵配送こそ実現に向けた実験が行われているが，それ以外のセキュリティプロトコルについてみると実験はもちろんのこと理論的な提案すら十分になされていないのが現状である．さらに，現状では実用段階の量子計算機の登場は2035年以降になるといわれているが，実現すると古典情報と併用して量子状態も秘密情報として扱えるほうが便利であり，そのような場合に対応するセキュリティプロトコルが求められるようになるのも想像に難くない．しかしながら，このようなプロトコルは先に述べた量子鍵配送以外のプロトコルよりもさらに少ないのが現状である．よって，量子状態を取り入れたセキュリティプロトコルや，量子状態を秘密情報として取り扱うセキュリティプロトコルや量子通信の研究は非常に重要であるため研究を行った．

２．研究の目的

本研究では，量子状態を情報として取り扱うセキュリティプロトコルの提案を目的として研究を行う．

３．研究の方法

量子状態を使用したセキュリティプロトコルとして量子秘密分散法を，また，プロトコル上量子状態を使用した通信を行う関係から量子通信路の評価を行った．

（１） 量子秘密分散法

秘密分散法は秘密情報を分散符号化して保存し，特定の分散情報が集めることで秘密情報を復元することができるというセキュリティ基盤プロトコルに一つであり，多くのセキュリティプロトコルに使われる．量子秘密分散法は秘密分散法に量子状態を使用したものである．本研究ではこの量子秘密分散法のうち2グループが協力して秘密情報の分散を行い，それぞれのグループ全員の情報を持ち寄ることで秘密の復元ができるという方式である．同様の方式の既存研究としてYanらにより提案された方式などが存在するが，これに対する攻撃法としてthe attack with single photons / EPR pairやthe fake-signal attackといった攻撃法が提案され，十分な安全性を持たないことが示されている．そこで，既存方式を改良した新たなプロトコルを提案し，上記の攻撃をはじめとした既存研究に対して有効な攻撃法に対し耐性評価を行い，十分な安全性を持つことを示す．

（２） 量子通信路の評価

代表的な量子通信路である光ファイバ，および自由空間について具体的な変調方式や測定法を与え通信路容量に評価を行う．またその結果をGiovannettiらが導出した理論限界との比較を行う．調査する変調方式としてコヒーレント光をquadrature amplitude modulation (QAM)とphase-shift keying (PSK)に変調する方式を対象とし，測定法として典型的なヘテロダイン検波，および量子測定であるSingle-shot square root detection (Single-shot SRD)およびCollective SRDの3つを対象として調査を行う．

４．研究成果

（１） 量子秘密分散法

提案する量子秘密分散法を記述する．グループ１のメンバ数をm，グループ２のメンバ数をnとする．

提案法では以下の６つの量子状態を使用する．

$|\varphi_0^0\rangle = |0\rangle, |\varphi_0^1\rangle = |1\rangle,$

$|\varphi_1^0\rangle = -\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle,$

$|\varphi_1^1\rangle = -\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle,$

$$|\varphi_2^0\rangle = -\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle,$$

$$|\varphi_2^1\rangle = \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle$$

量子操作として以下の5つの操作を使用する．

$$U_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$U_1 = \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix},\ U_2 = \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix},$$

$$V_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ V_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

以上の状態を使用した提案方式は以下のようになる．

(STEP1) グループ2の各メンバjは$C_i \in \{0,1\}$と$D_j \in \{0,1,2\}$をランダムに選び量子状態$\left|\varphi_{D_j}^{C_i}\right\rangle$を生成する．盗聴検出用の量子状態を生成し，まとめてグループ1の一人目に送信する．

(STEP2) グループ1の各メンバiは送られてきた量子状態の一部を使用して盗聴者検出を行う．盗聴者が存在しないことを確認したら，ランダムに長さnの$A_{i,j} \in \{0,1\}$と$B_{i,j} \in \{0,1,2\}$を選び対応する量子操作$U_{B_{i,j}}V_{A_{i,j}}$をグループ2のjから送られた量子状態の一つに適用する．同様に乱数生成，及び対応する量子操作の適用をすべての量子状態に行い，次のメンバに送信する．このときグループ1の最後のメンバであるなら，グループ2の各メンバに生成した量子状態を送り返す．そうでないなら，すべての量子状態をグループ1の次のメンバに送信し(STEP2)を繰り返す．

(STEP3) グループ2の各メンバjは送られてきた量子状態の一部を使用して盗聴者検出を行う．盗聴者が存在しないことを確認したら，グループ1の全メンバに$B_{i,j}$の公開を求める．$x_j = D_j + \sum_j B_{i,j}$を計算し，基底$\left\{\left|\varphi_{x_j}^0\right\rangle\left\langle\varphi_{x_j}^0\right|, \left|\varphi_{x_j}^1\right\rangle\left\langle\varphi_{x_j}^1\right|\right\}$で測定を行う．測定結果を$E_j$とする．

(STEP4) グループ1の分散情報は$S1_i = \sum_j A_{i,j}$であり，グループ2の分散情報は$S2_j = C_j + E_j$である．このとき，$\sum_i S1_i = \sum_j S2_j$が成り立ち秘密分散法となっている．

なお(STEP2)，(STEP3)において行われている盗聴者検出は既存研究によって導入されている典型的な方法を想定おり，この盗聴者検出によってすでにPNS攻撃，IPE攻撃，Trojan horse攻撃といった攻撃法に対する対策はなされている．

提案プロトコルは既存研究では十分に耐性を有しないthe attack with single photons / EPR pairとthe fake-signal attackの2つの攻撃に対し耐性を有するのが特色である．the attack with single photons / EPR pairはグループ1の最後のメンバが攻撃者としてグループ2の各メンバに送り返すはずの量子状態をこれまで各グループメンバにより操作された量子状態ではなく自らが生成した量子状態に置き換えることでグループ2の測定結果を予想しようというものである．既存研究ではこの攻撃に対する検出確率が両グループのメンバ数に比例して小さくなるのに対し，提案プロトコルではメンバ数によらず1/2という結果を実現している．the fake-signal attackでは攻撃者は量子もつれ合い状態を用意し，その一方を送信して量子操作が施された後の量子状態を回収することで量子状態に施された量子操作を予想し，これによってグループ1の分散情報を予測しようという攻撃である．既存研究ではこの攻撃に対する検出確率は約30%であるのに対し，提案方式では50%であるという結果が得られた．以上より両攻撃に対し，提案プロトコルは耐性を有するということができる．今後の展望としては，この形式の量子

秘密分散法は他の量子プロトコルの多くと同様に完全な安全性証明がなされているわけではなく，個別の攻撃に対して耐性を有していることを示している．そのため，攻撃法によらない安全性証明を行うことなどがあげられる．

（2） 量子通信路の評価

評価は 2PSK, 4PSK, 9QAM, 16QAM のそれぞれに対し，典型的なヘテロダイン検波，および 2PSK と 4PSK に対し single-shot SRD, Collective SRD について行った．光ファイバについて silica ファイバの物理的な性質から中心周波数 220Thz とした幅 50TH z に設定し，これを 400 チャネルに分割して波長分割多重にすると想定する．信号の生成レートは 125×10^{9} signals/sec とし，またアンプ込の信号の transmissivity を $\eta=10^{-2}$ と想定しており，これは距離で約 100km に相当する．

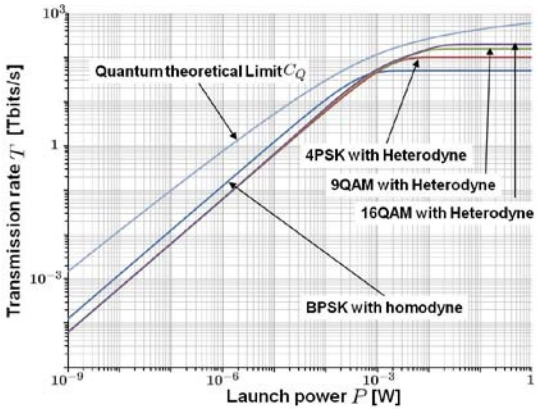


図 1 ファイバ通信路における通信路容量

典型的なヘテロダイン検波のみに測定法を限定した場合について図 1 に示す．ファイバ通信路では理論限界として約 1Pbit/sec が限界であることが見て取れる．次に各変調法を比較すると，結果として量子ノイズが支配的いなるほどの弱電力の領域においては複雑な変調を行うよりももっとも単純な変調方式である 2PSK を行うほうが良いという結果が得られた．このとき理論限界値との間には 7.5dB 程度の劣化があることが分かる． 逆に強電力の領域ではより多値に変調した方が良いという結果が得られる．

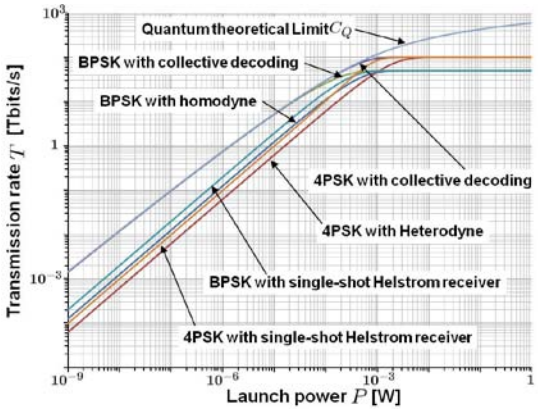


図 2 量子測定との比較

次に各量子測定と比較する．結果として single-shot SRD を実現するだけでも典型的ヘテロダイン検波に比べて 3dB 程度に改善が認められることが分かった．また波長分割多重を使用していても collective SRD が実現できればそれぞれのチャネルで collective SRD を行えば理論限界の 95%程度まで実現することができることが分かった．

自由空間の量子通信としては惑星間通信を考える．変調方式は 2PSK, 4PSK, 9QAM, 16QAM の 4 つであり，ファイバ通信路と同じく 2PSK と 4PSK については single-shot SRD, Collective SRD についても評価を行った．このときのチャネル Transmissivity はアンテナの直径と波長の 2 乗に比例し距離の 2 乗に反比例する．評価時には送信アンテナの直径を 305mm，受信アンテナの直径を 10000mm，中心周波数を 192THz と想定し評価を行った．

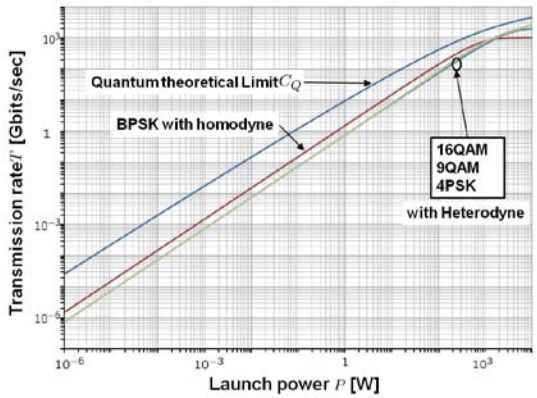


図 3 地球-火星間の通信路容量

図 3 に通信距離を地球-火星間と想定した場合のグラフ示す．まず理論限界を注目すると，最大で約 20Tbit/sec まで実現する可能性があることが分かるファイバ通信路とほぼ同じ特性が見て取れ，弱電力の領域では 2PSK が最も良いという結果が得られる．

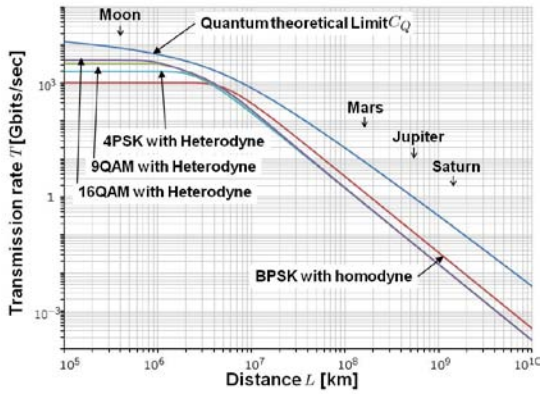
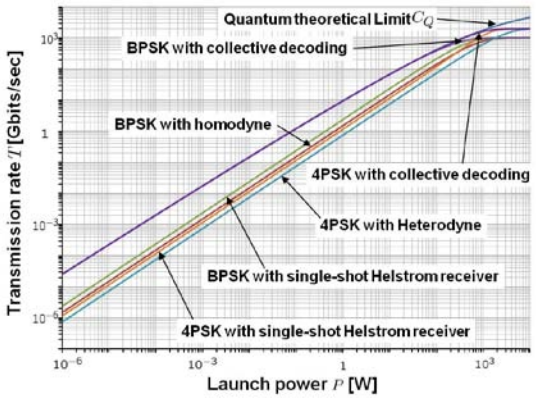


図 4 電力 1W のときの通信路容量

一方信号生成に使用する電力を 1W に固定した場合のグラフを図 4 に示す．理論限界を見ると本報告書における設定では火星までであれば 10Gbit/sec まで実現する可能性があることが分かる．また，典型的ヘテロダイン検波を行ったときの通信路容量に関しては長距離が弱電力に，近距離が強電力に対応して電力の場合とほぼ同じ傾向が見て取れる．



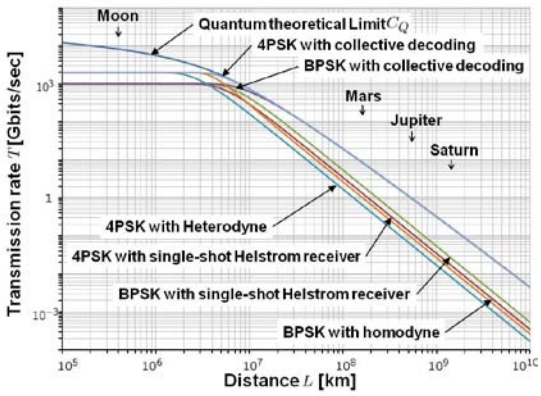


図 5 測定法による比較

測定法による比較でもファイバ通信路とほぼ同じことが言え，Collective SRD が実現できたなら，理論限界値をほぼ実現することができることが分かる．

まとめると量子通信路について，量子的性質を十分に使用すると古典的な Shannon の限界を超えることができることが良く知られている．本研究では量子測定が実現できれば Shannon の限界を超えることができるということ，また波長分割多重された通信路に対し，複数通信路間にまたがる collective SRD を行う必要はなく，それぞれの分割された通信路毎の collective SRD が実現できれば通信路容量の量子的な限界まで実現できることが分かった．

今後の展望としては自由空間の通信路についてはほかに興味深い変調方式として pulse position modulation (PPM)が存在する．これについても同様に通信路容量を評価する

ことなどがあげられる.

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計１件）

① Atsushi Waseda, Masahiro Takeoka, Masahide Sasaki, Mikio Fujiwara, and Hidema Tanaka, “Quantum detection of wavelength division multiplexing optical coherent signals” Journal of the Optical Society of America B-OPTICAL PHYSICS, Vol.27 , No.2 , 259-265, 2010, 査読あり

〔学会発表〕（計３件）

① Atsushi Waseda, Masahide Sasaki, Masahiro Takeoka, Mikio Fujiwara, Morio Tyoshima, and Hidema Tanaka. “Quantum detection of wavelength division multiplexing optical coherent signals in lossy channels”, 2010 International Conference on Availability and Security, Krakow, Poland, February 17, 2010.

② 早稲田篤志, 武岡正裕, 佐々木雅英, 藤原幹生, 田中秀磨. “光ファイバー帯域におけるコヒーレント光通信の通信路容量に関する一考察”, 暗号と情報セキュリティシンポジウム 2009, 大津プリンスホテル, 大津市, 2009 年 1 月 22 日.

③ A. Waseda, T. Takagi, M. Soshi, and A. Miyaji. “Quantum Secret Sharing between Multiparty and Multiparty against the Attack with Single Photons or EPR-pair”, The 2008 International Symposium on Information Theory and its Applications, Auckland, New Zealand, December 7, 2008.

６．研究組織

(1)研究代表者

早稲田　篤志（WASEDA ATSUSHI）

独立行政法人情報通信研究機構・情報通信セキュリティ研究センターセキュリティ基盤グループ・専攻研究員

研究者番号：10455454

(2)研究分担者

（　　）

研究者番号：

(3)連携研究者

（　　）

研究者番号：