



情報理論とその応用学会ニュースレター

寄稿

- 量子暗号の“量子”でない部分..... 鶴丸豊広 (三菱電機)
- 私が出会った本..... 山本博資 (東京大学)
- ワークショップ等開催報告
- 2006 Hawaii, IEICE, and SITA Joint Conference on Information Theory (HISC2006) 開催報告
..... 藤原融 (大阪大学)
- ワークショップ等開催案内
- 第 5 回アジア・ヨーロッパ情報理論ワークショップ (AEW5) 開催案内
- 2006 年度第 2 回理事会報告
- 国際会議のお知らせ
- ニュースレター原稿募集

量子暗号の“量子”でない部分

鶴丸豊広 (三菱電機)



鶴丸豊広 (三菱電機)

1 はじめに

量子暗号 (cryptography) は「絶対に破れない暗号」として知られる暗号である。量子力学を安全性の根拠としており、量子暗号が破れるとしたら量子力学が正しくなかったという証拠を見つけたことになる。

なおかつ量子暗号はすでに装置が完成しており、距離 100km 超での暗号通信が可能であるなど、現在

の技術である。しかし実装や性能競争が激化しつつあるがゆえに、誤り訂正符号や秘匿性増強など、量子でないいわゆる古典情報理論^{*1}の重要性が改めて際立ってくる。

三菱電機の筆者の所属するチームでも、2000 年前後から量子暗号装置の実装を行ってきているが、最近の世間の流れとして、通信距離数十 km~100km ではあまり驚かない時代になっている。鍵共有速度も重要視され、数十~数百 kbps、場合によっては 1Mbps を目指す時代であり、性能競争の様相を呈し始めている。このような状況では、用いられる誤り訂正符号や秘匿性増強方式の処理速度や性能が、量子暗号の性能に直接的な影響を及ぼすことになる。そこで符号理論や暗号理論の研究者の助言や協力が欲しい、と思うことがしばしばあるし、少なくとも議論のできる同僚が増えてほしいと願う。

^{*1} “量子” (quantum) のつかない通常の情報理論のこと。歴史的な経緯で“非量子的”なものを指して“古典” (classical) と呼ぶ。

だが一方でそういう研究者 (主に同僚だが) が「量子暗号=自分と関係のないもの」という認識を始めてから持っていて、まともな協力が得られないという場面もしばしばある。これは自分も含めて量子暗号を宣伝する人間が、“不確定性原理”や“量子もつれあい”など大げさな単語を始めてから並べすぎるせいもあると思う。原理を短く明確に説明できるなら始めからそうしたいが、実際にはそういうときはむしろ、うまく説明しきれないのでキーワードでごまかして逃げていることが多いと思う。そもそもこの文章の出だしも大げさである。しかし量子暗号でもやはり古典情報理論が重要なので、そのような宣伝の仕方は自らの首を絞めているともいえる。

そこで本稿のテーマは「誤り訂正符号や秘匿性増強が量子暗号でどのように使われているかを、量子力学に深入りせず説明する」である。量子力学の知識がゼロでも分かるとまでは言わない。しかし量子力学の教科書 [8, 17] が一冊あったとしたら、量子暗号の議論に必要な内容はその中のほんの一部分だけなのではないか、としばしば思うので、その線にそって説明を試みる。

具体的にはまず第2節で、代表的な量子鍵共有プロトコルである BB84 方式について説明し、その安全性について第3節で議論し、第4節ではそれを量子暗号の実装例と比較する。また第5節では量子暗号における認証方式について説明する。このうち第3節と第5節で扱っている誤り訂正や秘匿性増強や認証の話は、本来は第2節や第4節の内容に深入りせずとも説明できる箇所なのではないか、と常々思っていた。加えて量子暗号を実装するにあたっては、いかにしてこの部分を効率的かつ高速に設計できるかが重要な意味を持つので、少しでも多くの方に興味を持っていただければと願う。

2 量子鍵配送方式 —BB84 方式—

まずこの節では量子鍵配送の代表的なプロトコルとして、BB84 方式について説明する [1]。現在でも量子暗号の実装報告多くで、このプロトコルが用いられている。

2.1 機能

BB84 方式の目的は、送信者 Alice と受信者 Bob の間で、秘密のビット列 $k = (k_1, \dots, k_n)$, $k_i \in \{0, 1\}$ を共有することである。なおかつこの k が、いかなる盗聴者 Eve にも盗み見られていないことを、証明つきで保証できる。ただし“盗み見られない”の意味が通常の暗号とはやや異なる。

まず、秘密のビット列 $k = (k_1, \dots, k_n)$ を送信者または受信者が自由に選ぶことはできない。もし k を自由に選べるとすれば、初めからメッセージ m を k として選べば、直接に暗号通信ができる。しかし実際のところ k の具体的な値は、このプロトコルが終わるまで判明しない。

次に、送ったビット列を途中で誰かに盗み見られた場合、事後の検証でそのことをほぼ 1 の確率で検出できるが、 k が盗み見られた事実は覆えせない。なのでこの場合は、その乱数列 k は捨て去って、このプロトコルを再び実行する。そして、乱数列 k が盗聴されていないことが検証できるまで繰り返す (この場合もちろん、 k の値は毎回異なる)。ここでもし攻撃者 Eve がいつまでも盗聴を続けるとした場合には、Alice と Bob は永遠に秘密通信ができないことになる。しかし古典暗号通信の場合でも、攻撃者が通信線を遮断すると同じ状況になるので、このことは決して量子暗号の方が弱いことを意味するものではない。

まとめると量子暗号の機能は、Alice-Bob 間で (毎回異なる) ビット列 k を共有することであり、事後の検証に成功した場合には、それが途中で盗聴されていないことを確信できる、というものである。特定のメッセージ m を秘密に送るには、まず乱数列 k を m と同じ長さだけ共有し、それを秘密鍵として、ワンタイムパッド (one-time pad) で通信する。つまり $k \oplus m$ を暗号文として送ればよい。

2.2 通信媒体

上記の機能を実現するためには、「手が加えられた場合には、高い確率で変化が起こる」媒体があればいいが、それが一般に量子 (quantum) である。量子

の正確な定義は教科書 [8, 17] を参照願いたい。概略を述べると、まず、世の中を構成する物質および全ての力 (相互作用) は、電子、核子、光などの微小な粒子を構成要素としているが、これらは全て量子としての性質を示す。つまり物質を微小に分割して精密測定を行うと、上記の“手を加えられた場合”の性質が現れてくる。

従って原理的には、どんな物質や場 (field) でも充分微小に分割すれば量子暗号に用いることができるのだが、現状では、雑音への耐性や制御の容易さから、もっぱら光のみを用いて実験が行われている。光の場合には、微小に分割すること＝光の強度を弱めることであり、レーザ光を減衰器で弱めた微弱コヒーレント光 (weak coherent light) を用いることが多い。

2.3 符号化

充分強度を弱めると、光を 1 個、2 個、…と数えられるようになり、この粒子を光子 (photon) と呼ぶ。量子暗号通信では、この光子ひとつあたりに 1 ビットずつ乱数列 k の情報を乗せていく*2。光には電磁場としての空間ベクトル成分、つまり偏光 (polarization) があって、波長やモードを決め打ちして考えると、これは 2 次元のベクトル (状態ベクトル) で表現できる。

そこで例えば $b = 0, 1$ を

$$|\uparrow\rangle = |0\rangle_+ = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |\leftrightarrow\rangle = |1\rangle_+ = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (1)$$

という状態に符号化して送ることにする。この 2 状態は直行基底をなしているので「+基底」と呼ぶことにする。量子力学においては、状態 $|\psi\rangle$ を、基底 $\{|\varphi_0\rangle, |\varphi_1\rangle\}$ を指定して測定すると、値 a が確率 $P_a = |\langle\varphi_a|\psi\rangle|^2$ で得られる*3。したがって (1) の場合、Bob は測定によって b の値を常に正確に求められる。しかしながら盗聴者 Eve も同様のことができるので、この方式は暗号には使えない。

*2 以下では、厳密な単一光子を制御できる技術があるとして話を進める。

*3 $\langle\varphi_a|\psi\rangle$ は $|\varphi_a\rangle, |\psi\rangle$ の内積の意味。

*4 $|\langle\uparrow|\uparrow\rangle|^2 = |\langle\leftrightarrow|\uparrow\rangle|^2 = \dots = \frac{1}{2}$ から。

*5 量子力学の公理による。

そこで符号化法をランダム化する。上記の+基底に加えて、もうひと組「×基底」を導入し、

$$\begin{aligned} |\nearrow\rangle &= |0\rangle_\times = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \\ |\searrow\rangle &= |1\rangle_\times = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \end{aligned} \quad (2)$$

+基底と $1/2$ ずつの確率で併用する。つまり $b = 0$ に対しては $\{\uparrow, \nearrow\}$ のどちらか、 $b = 1$ には $\{\leftrightarrow, \searrow\}$ のどちらかの偏光をランダムに選んで送る。なおかつ Alice は、Bob が全ての光子の観測を終えるまで、用いた基底を秘密にしておく。

Alice が送信に用いた基底と、Bob が受信に用いた基底とが一致した場合には、Bob は b を正しく知ることができるが、一致しなかった場合には Bob の観測する値は全くの乱数となる*4。なおかつ、そのときの状態はすでにそのランダムな状態に変化して*5、正しい基底をもちいて観測を再挑戦したとしても、やはりランダムな値しかえられない。

ただし元々送信しているのは乱数なので、Bob が測定できなかった分は捨ててしまえばよくて、Alice-Bob 間の鍵共有としては害が無い。

2.4 盗聴の検出

一方で「測定に再挑戦しても情報量が増えない」ということは、盗聴者 Eve にとっても同様である。

まず Eve の目的は：Alice の送信した光を途中で傍受して b の情報を得て、なおかつ Bob の受信機にはうまく偽装した状態の光を送りこんで、盗聴の痕跡を消す、ということである。

例えば盗聴戦略のうちもっとも簡単なものは：Eve が+、×のいずれかの基底を予測し、それを用いて Alice が送信した状態を観測する、というものである。しかしこのとき必ず $1/2$ の確率で誤った基底を選ぶので、偏光を 45 度か 135 度変えてしまう。もちろんここでも、観測によって一度変化した状態は元に戻すことができない。この結果 Bob の側として

は、正しい基底を用いた場合でも、測定する b の値には確率 $1/4$ で誤りがおこることになる。もし仮に何らかの理由で、Eve はこの方法しか用いていない、ということを Alice と Bob が知っているとする。そのとき Alice, Bob は、誤り率が $1/4$ 未満であることさえ検証すれば、秘密通信ができていると結論付けられる。

もちろん本当は、このような粗い攻撃方法よりもっと賢い戦略があるが、とにかくここで強調したいことは、Bob の測定する誤り率と、Eve が秘密鍵 b に関して得る情報量との間にトレードオフがあるということである。実際に多くの場合、量子暗号の安全性証明はこの考え方に沿ってなされている。

2.5 方式

ここで、BB84 方式の手続きを具体的に書いてみる。まず最初に光を用いた量子通信がある。その後は上記のトレードオフを活用すべく、誤り率を検証するフェーズと、ひきつづいて秘密鍵を抽出するフェーズとに分かれている。

■量子通信フェーズ

1. Alice は、乱数列 $a = (a_1, \dots, a_n)$, $a_i \in \{0, 1\}$ と、ランダムな基底の列 $x = \{x_1, \dots, x_n\}$, $x_i \in \{+, \times\}$ を選ぶ。
2. Bob はランダムな基底の列 $y = (y_1, \dots, y_n)$, $y_i \in \{+, \times\}$ を選ぶ。
3. Alice は Bob に、 n 個の光子をそれぞれ $|a_i\rangle_{x_i}$ の状態にして送る。
4. Bob は Alice から受け取った光子を、それぞれ基底 y_i で観測し、結果を $b = \{b_1, \dots, b_n\}$, $b_i \in \{0, 1\}$ として記録する。

■誤り率検証フェーズ

1. Alice は Bob に、基底 x を公開通信路で伝える。
2. Bob は基底 x と基底 y とを比較し、基底の一

致した光子の番号を $I = \{i \mid 1 \leq i \leq n, x_i = y_i\}$ とし、公開通信路で Alice に伝える。

3. I のうち一部を誤り率検証用としてランダムに選び $J \subset I$ とする。 J に対応するビット列 $a_J = \{a_i \mid i \in J\}$, $b_J = \{b_i \mid i \in J\}$ を公開通信路で教えあい、それらの間のビット誤り率を求める。

■秘密鍵抽出フェーズ

1. 検証用に使わなかった分のビット列を、Alice, Bob が鍵としてそれぞれ保存する。つまり $I' = I - J$ として、ビット列 $a_{I'} = \{a_i \mid i \in I'\}$, $b_{I'} = \{b_i \mid i \in I'\}$ を Alice, Bob がそれぞれ保存する。これを篩にかけられた鍵ということで“ふるい鍵” (sifted key) と呼ぶ。

要するに、基底をランダムに振って乱数を送り、Alice と Bob の基底が確率的にあった分だけを秘密鍵の候補として残す。通信路が完全で盗聴者もないとすると a_I と b_I は全て一致するはずだが、実際には b_I には誤りがのっているので、一部を a_J, b_J としてランダム抽出して誤り率を評価する。ビット長を充分長く取った場合は、このようにして検出した誤り率によって、残りの $b_{I'}$ に乗っている ($a_{I'}$ を基準としたときの) ビット誤り率 ε を確率的に上から抑えることができる。

3 個別攻撃

やや天下りのだがここで、Alice は厳密な単一光子パルスを発する技術を持つとし、また攻撃者 Eve は「個別攻撃」 (individual attack^{*6}) と呼ばれる種類の攻撃のみを行っている、と仮定する [9]。無条件安全性を達成するためにはいわゆるコヒーレント攻撃 (coherent attack) まで考える必要があるが、現状の実装報告ではもっぱら個別攻撃を想定しているのでそれに倣うことにする。量子論的な議論の詳細はすべて省略するが、そうすると上記の量子暗号プロトコルの入出力を、古典通信路と捉えることができる。

^{*6} 個別攻撃では Eve が、それぞれの光パルスに個別に量子操作をしているとし、また Alice と Bob が基底情報の交換をした直後に Eve が量子論的な測定を行うとする。

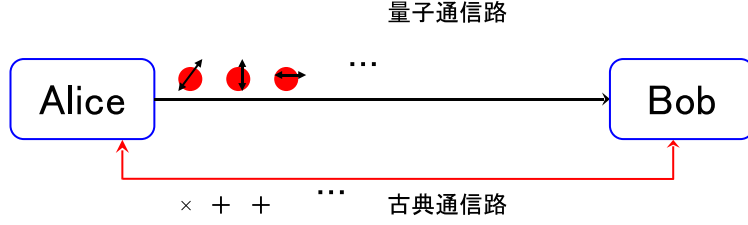


図1 量子鍵配送では、量子通信路と古典通信路がある。

3.1 誤り率と、盗聴される情報量のトレードオフ

前節で述べたように、ふるい鍵 $a_{I'}$, $b_{I'}$ には誤りが乗っているが、その誤り率 ε の上界は分かっている。なおかつその一部の情報は Eve に漏れているが、その情報量と誤り率 ε の間にはトレードオフがある。個別攻撃を考えた場合には、各ビットについてそのトレードオフを独立に考えることができ、なおかつその様子を具体的に計算することができる。

以下では簡単のため $a_{I'}$, $b_{I'}$ を改めて a , b と定義し直す。そして a , b の従う確率分布を A , B とする。また Eve の情報の確率分布を E とする。

■**相互情報量での評価** Eve の情報量を相互情報量で評価した場合、各ビットにつき、

$$I(A; E) \leq 1 - H_2\left(\frac{1}{2} + \sqrt{\varepsilon(1-\varepsilon)}\right) \quad (3)$$

のように上から抑えることができる [9]。

■**Rényi エントロピーでの評価** 一方で、3.3.2 節で議論する秘匿性増強を考慮すると、Eve の情報量の尺度として Rényi エントロピーを用いた方が便利である。まず衝突確率および Rényi エントロピー (オーダー $\alpha = 2$ の) は以下で定義されていた：

$$P_c(A) = \sum_{a \in A} P_A(a)^2,$$

$$R(A) = -\log_2 P_c(X).$$

$R_\alpha(A)$ は Shannon エントロピー $H(A)$ の一般化で、 $H(A)$ と同様に情報の曖昧さをあらわす。そこでふるい鍵 $A_{I'}$ の各ビットを Eve から見たときの曖昧さを、以下の条件つきエントロピーであらわすことが

できる

$$R(A|E) = \sum_{e \in E} P_E(e) R(A|E = e).$$

この場合にも、誤り率と $R(A|E)$ にはトレードオフがあり、各ビットに対して

$$R(A|E) \geq -\log_2\left(\frac{1}{2} + 2\varepsilon - 2\varepsilon^2\right) \quad (4)$$

が成立する [13]。ただしここで誤り率 $\varepsilon \leq 1/2$ であるとした。

3.2 秘密鍵抽出

ここで強調したいのは、ふるい鍵ができた段階では、問題は完全に古典情報理論的になっている、ということである。まず Alice は偏りの無いビット列 a を、誤り率 ε の通信路を通じて Bob に送り、Bob は b を得る。同時に Eve は情報 e を得ているが、その秘密鍵 a との相関は、たとえば (3) 式や (4) 式で与えられる。

この状態から、Alice と Bob は (誤りの無い) 公開通信路を活用して、秘密鍵 K の抽出を行う。つまり Alice と Bob は古典通信 $c_1, \dots, c_r$ を行って $k_A = F_A(a, c_1, \dots, c_r)$, $k_B = F_B(b, c_1, \dots, c_r)$ を求め、高い確率で $k_A = k_B (= k)$ が満たされているようにする。それと同時に、Eve には k に関する情報が殆ど分からないようにする: $I(K; E, C_1, \dots, C_r) \ll |K|$ 。

この問題は Advantage Distillation などと呼ばれているが、ある程度一般的な結果が知られていて [7], 秘密鍵 K の生成速度を $S(A, B|E)$ とかくと、

$$\geq \max\{I(A; B) - I(A; E), I(A; B) - I(B; E)\}$$

となる。また Alice-Bob の古典通信が一方向である場合には等号がなりたつ。今の場合ビットあたりでは $I(A; B) \geq H_2(\varepsilon)$ なので、(3) 式と対比すると、誤り率 ε が 15% 程度かそれ以下であれば、理論的には鍵生成が可能である。

一方で実際問題として、ソフトウェアや FPGA で実装するためには計算量的に効率的なプロトコルを用いなければならない。しかし現状では、そのようなプロトコルの具体形としては (筆者の知る限り)、以下の様に誤り訂正と秘匿性増強を組合わせたものしか知られていない。

3.3 効率的な秘密鍵抽出方式

以下の方式では、まず Bob のふるい鍵 b に誤り訂正を施して Alice のふるい鍵 a と一致させる。次に秘匿性増強と呼ばれる方式によって Eve に漏洩した情報を消去する。

3.3.1 誤り訂正

■誤り訂正符号を用いる方式 あらかじめ符号の具体形を Alice-Bob 間で共有しておき、ふるい鍵ビット列のシンδροームを Alice から Bob に公開通信路で送って誤りを訂正する。

ただしこのシンδροームは公開通信路上を流れるので、ふるい鍵に関する情報が ((3), (4) 式で与えられているのとは別個に) Eve に漏洩することになる。これを防ぐために、予め Alice と Bob で秘密鍵を共有しておき、それを用いてシンδροームをワンタイムパッドで暗号化して送ることにする^{*7}[13]。ここで消費される秘密鍵長の方が、最後に生成される秘密鍵長よりも短ければ、鍵共有プロトコルとして成立するという考えである。

■Cascade 方式 量子暗号の実装では、BBBSS 方式 [2] および Cascade 方式 [5] と呼ばれるものもよく使われている。これらの方式では、公開通信路での双方向通信を積極的に利用して、誤り訂正の符号化率

を高めている。

BBBSS 方式では大まかには：

1. ふるい鍵 a をブロックに分割して、各ブロックのパリティを公開する。
2. b のブロックとのパリティの違いが検出された箇所については、公開通信路上でデータをやり取りして二分探索を行い (この間さらにパリティを公開する)、誤りの位置を特定して訂正する。

ということを繰り返す。Cascade 方式ではさらにこれを改良して、符号化率を Shannon 限界まで近づけている。ただし誤り訂正符号によっても LDPC 符号等を利用すれば同様に限界に近づけられるうに、他方で Cascade 方式等では通信回数 (ラウンド数) が莫大に増えるという問題もある。したがって今後の量子暗号実装では誤り訂正符号の方が重要になると思われるので、以下ではこれらの方式には深入りしない。

3.3.2 秘匿性増強

以上で Alice と Bob のふるい鍵が一致して、両者とも a を共有できた。しかし依然として Eve も a の情報を一部もっているのので、次に秘匿性増強 (Privacy Amplification, プライバシ増幅と呼ぶこともある) と呼ばれる方式をもちいてこれを消去する [2, 4]。 “消去する” というのは具体的に言うと； Alice と Bob が公開通信 $c_1, \dots, c_r$ をして、ある値 $k = f(a, c_1, \dots, c_r)$ を計算し、そのとき k に関する情報量を Eve が殆ど持っていないようにする、ということである。

このための効率的なプロトコルとしては Bennett, Maurer ほかによって提案された Generalized Privacy Amplification と呼ばれる方式がある [3]。この方式では Alice と Bob は $universal_2$ と呼ばれる関数の集合 G から [6]、関数 $g \in G$ をランダムに選び、ハッシュ値 $k = g(a)$ を求める。そのとき G の入出

^{*7} 実際には、漏れた分を後から秘匿性増強で消去してもいいのだが、そうすると、除去すべき情報量の計算 (衝突確率の計算) が複雑になるという問題がある。また漏れる情報を差し引くのが、先か後かの違いだけで、鍵生成率としてもメリットは無いので、議論を簡単にすべく予め暗号化しておく (つまり先に差し引いておく) ことにする。

力のビット長を適切に選ぶと、 $I(K; G, E)$ を任意に小さくすることができる。

具体的には：各 $g \in G$ は $g : \{0, 1\}^n \rightarrow \{0, 1\}^r$ であるとする。また A が $\{0, 1\}^n$ 上の一様分布で、なおかつ $R(A|E) = n - t$ であれば、“Eve の A に関する Rényi 情報量は t である”ということにする。このとき以下が成り立つ

$$I(K; G, E) \leq 2^{n-t-r} / \ln 2.$$

つまり n が充分大きいところで考えると、ほぼ $R(A|E)$ ビット分の秘密鍵が共有できるということになる。

3.3.3 秘密鍵生成レート

まず、 n ビットの b を修正して a と一致させるために、 a のシンドロームをワンタイムパッドで暗号化して送る必要がある。ここで Shannon 限界に達した誤り訂正符号を用いる場合には、シンドローム長は誤り率 ε に対して $nH_2(\varepsilon)$ ビットであり、それと同じ長さの秘密鍵が消費される。次にそうやって一致した n ビットのうち、Eve に漏洩している分 ((4) 式で与えられる) を秘匿性増強で取り除く。結果として、生成される鍵長から消費する鍵長を差し引いた、正味の鍵生成速度 G (= 生成される秘密鍵長 / ふるい鍵長) は以下で与えられる [14]。

$$G = -\log_2 \left(\frac{1}{2} + 2\varepsilon - 2\varepsilon^2 \right) - H_2(\varepsilon). \quad (5)$$

したがって鍵共有が可能となるためには、誤り率が $\varepsilon < 11\%$ 程度でなければならない。つまり効率的なプロトコルに限定したことによって、理論的な限界である 15% (本節の始め参照) との間に差が生じている。

3.4 安全性証明の前提についての補足

なお上記の議論は飽くまで、単一光子を用いた BB84 方式の安全性を、個別攻撃を仮定して解析したものである。BB84 以外の方式を用いる場合 [21] や、光子源の不完全性を考慮に入れた場合 [14] についても、個別攻撃の枠内であれば同様の議論ができ

る。ただし出発点となる (3) 式や (4) の表式がやや異なる。

4 実装例との比較

4.1 実装例

量子暗号は現在では、国外 (ジュネーブ大学, IBM, Los Alamos 研究所ほか)、国内 (三菱電機, NEC, NTT, 日本大学, 産総研ほか) とも多くのグループによる実装報告があり、通信距離 100km 超の実験も複数報告されている (詳しくは文献 [10] 等を参照願いたい)。最近の主だった実装例としては三菱電機が '04 年に、既設光ファイバーを用いた 96km の量子暗号通信に成功している (図 2 および文献 [11])。

一方で第 3 節末では、誤り率 ε が分かれば、(5) 式から鍵生成速度が分かると述べた。その ε の具体的な値は光子検出器の性能やファイバーの距離に依存して決まるが、大まかな傾向としては通信距離に対して指数関数的に増える。現状の典型的な実装例では、通信距離 50km で誤り率が 1% 程度、100km で 10% 程度である (図 3(1))。誤り率 10% というのは量子暗号以外の応用ではお目にかかる数字だが、これは量子暗号においては、光の強度が通常の光通信と比べて 7 桁程度異なることによる。量子鍵配送が可能となるためには $\varepsilon < 11\%$ が必要であったから、ほぼ 100km で距離的な限界に達することになる。量子暗号の長距離実装例がどれも 100km 前後であるのはこのような事情による。

4.2 誤り率 ε の解釈について

ちなみに、装置で測定される誤り率 ε をそのまま (5) 式に代入してよい理由は下記の通りである：

第 3 節ではあたかも、“盗聴者がいない段階では誤り率は $\varepsilon = 0$ で、盗聴者がいると $\varepsilon > 0$ になる”かのように話をしてきた。しかし上記の通り現実には、盗聴者がいない場合でも $\varepsilon > 0$ である。そこで以下のように考えたい：“盗聴者がいるときは、いないときに比べて誤り率が增大する。もし観測した誤り率が 15% であれば、そのうち 10% は装置の性能によるもので、残り 5% は盗聴者によるものである。これは閾値 11% と比較しても低いので鍵共有は可

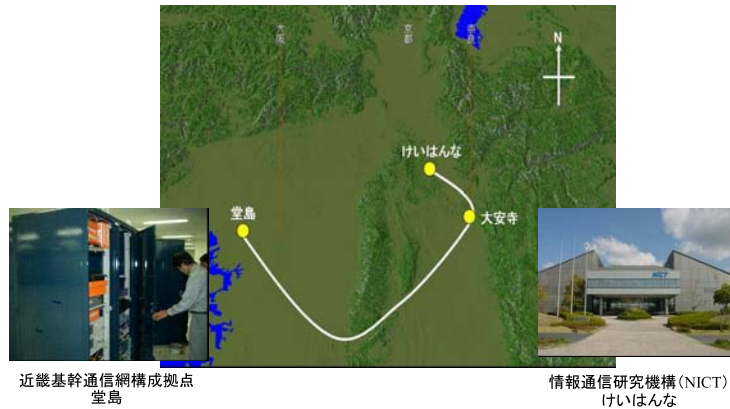


図2 既設光ファイバを用いた量子鍵配送 (三菱電機).

能である。”しかし量子暗号の安全性解析では通常そのような考え方はせずに、観測された誤りは全て盗聴者によるものだと仮定して話を進める^{*8}(図3(2)).そして閾値をこえた誤り率が検出された場合には、何者かに盗聴されていると結論して鍵共有を止める.このような考え方は議論を“安全サイド”に倒しているのみであり、与えられた量子暗号装置の安全性を証明する分には問題が無い.つまり Eve が最大限の攻撃力を持っていると仮定した状況で安全だと証明できれば、現実の使用環境での安全も示したことになる.

5 古典通信路の認証

これまでの説明において Alice と Bob は、光による量子通信路とは別に、古典的な公開通信路を使えると仮定していた.公開なのでここを流れる情報は攻撃者に漏れてもかまわないのだが、通信途中で改変されると安全性を維持できなくなる.極端な場合には、攻撃者 Eve が Alice または Bob の役割を丸ごと行う、いわゆる“なりすまし攻撃”の危険性がある.このような事情から、公開通信路は認証つきである必要がある.

しかしここで従来型のデジタル署名など、計算量的仮定に基づく方式で認証を行うと、量子暗号の無

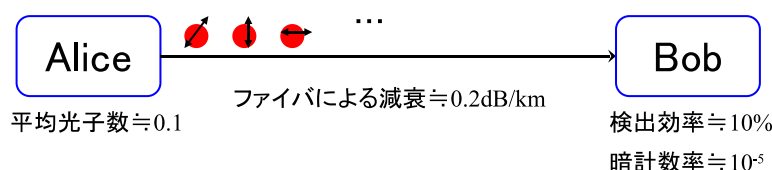
条件安全性が損なわれる.これを説明するために例えば、秘密通信を量子暗号、認証を RSA 方式とした場合を考えてみる.このとき、攻撃者 Eve が量子計算機を持っているとすれば、Eve は RSA 方式を破って Bob になりすまして Alice と量子暗号で通信し、秘密情報を全て手に入れることができる.つまり認証方式が弱ければ、量子鍵配送部分は破られてしまう.

この問題を解決するための手段としては、情報理論的に安全な認証方式が知られている [22].この方式では Alice と Bob が予め秘密鍵 k を共有しておき、そしてメッセージ m とともに鍵付きのハッシュ値 $h = f(m, k)$ を認証タグとして送る.なおかつ一度使った鍵 k は使い捨てにして、二度と使わないことにする.ここで、秘匿性増強でも出てきた $universal_2$ 関数 [6] の性質をうまく利用すると、鍵 k の長さを $O(\log \log |m|)$ に抑えつつ、Eve による成りすましの確率を任意に小さくすることができる.

このように量子暗号を認証を含めて考えた場合、現状では秘密鍵を事前に共有しておく必要があり、この意味で量子暗号は共通鍵暗号方式に類するものである.量子暗号を用いて公開鍵的な認証を行う具体的な方式はまだ知られていないが、その方向性の研究としては例えば文献 [19, 20] がある.

^{*8} 例えば Bob 側の光子検出効率を 1 に高めることは、実際には Eve にとって不可能だが、安全性証明ではそう仮定する.これは盗聴者に起因する誤り率と、装置の不完全性からくる誤り率とを切り分けようとする、装置の物理的な特性について詳細に立ち入る必要があって、議論が非常に複雑になるためであると思われる.

(1) 実際の量子暗号通信



(2) 安全性解析むけのモデル

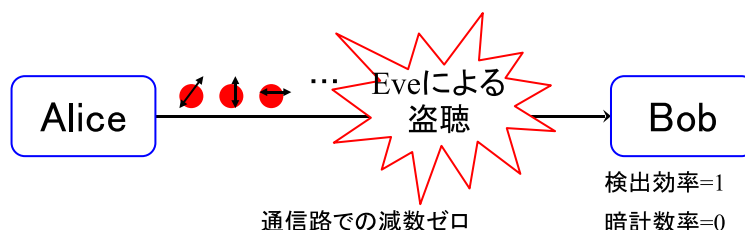


図3 量子暗号の雑音源. (1) 量子暗号の実装ではしばしば、平均光子数 0.1 のコヒーレント光パルスを用いて、それを近似的な単一光子とみなす。光ファイバによる減衰率は 0.2dB/km であり、典型的な光子検出器の検出効率は 0.1 程度である (波長 1550nm)。結果として通信距離 100km では、Alice の発した光パルスを Bob が検出される確率は 10^{-4} となる。一方で暗計数率 (光の有無に関わらずランダムに検出器が反応する確率) は典型的には 10^{-5} 程度であり、これが主な雑音源だとすると誤り率は $\varepsilon \approx 10\%$ となる。(2) 量子暗号としての安全性を証明するときには、誤りは全て Eve の盗聴によるものと仮定する。

6 まとめ

本稿では量子暗号において、古典情報理論的な方式がどのように利用されているかについて説明した。ここで強調したかったのは、量子暗号装置の性能を上げようとする、誤り訂正符号、秘匿性増強、情報理論的認証などを効率的に実装する必要があり、なおかつその性能が量子暗号の鍵生成速度に直接影響するということである。

長距離の量子暗号では、誤り率 10% 弱という、通常の応用ではお目にかからないレベルの誤り訂正符号が必要となるし、秘匿性増強の効率化も重要となる。またその際に古典通信路でやり取りされるデータは、全て情報理論的に安全な方式で認証する必要がある。量子暗号の実装報告の論文では通常、誤り率 ε を実験的に測定し、3 節の議論にしたがって鍵生成速度を算出するところまでで終わりである。実際に回路やソフトウェアで誤り訂正などを行って、リ

アルタイムに秘密鍵を計算するということは殆どない。しかし今後、量子暗号を暗号製品として実運用していく段階においてはこれらの方式の高速化や小型化が重要な課題になってくると思われる。そこで少しでも多くの方に、この分野に興味をもっていただければと切に願う。

また本稿では、単一光子源を仮定した場合の個別攻撃というかなり限られた話題についてのみ説明した。しかしこれはあくまで筆者の興味がそこにあるということであり、量子暗号の理論全体を見渡せば、他にも例えば Calderbank-Shor-Steane 符号を用いた無条件安全性の証明 [18] や、コヒーレント光の性質を考慮に入れた安全性証明 [14, 12] など、重要な話題はたくさんある。それらも含めて興味のある方は、優れた文献 [16, 10, 15] があるので参照願いたい。

参考文献

- [1] C. H. Bennett and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” in Proceedings of International Conference on Computers, Systems & Signal Processing Bangalore, India, (1984). なおこの文献は Bennett のホームページ <http://www.research.ibm.com/people/b/bennetc/> で入手可能.
- [2] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, “Experimental Quantum Cryptography,” J. Cryptology, 5, 3–28 (1992).
- [3] C. H. Bennett, G. Brassard, C. Crépeau and U. M. Maurer, “Generalized Privacy Amplification,” IEEE Trans., IT-41, 1915–1923 (1995).
- [4] C. H. Bennett, G. Brassard and J.-M. Robert, “Privacy Amplification by Public Discussions,” SIAM. J. Comput., 17, 210 (1988).
- [5] G. Brassard and L. Salvail, “Secret-Key Reconciliation by Public Discussion,” in Proceedings of Eurocrypt93 (1993).
- [6] J. L. Carter and M. N. Wegman, “Universal Classes of Hash Functions,” J. Comput. System Sci., 18, 143–154 (1979).
- [7] I. Csiszár and J. Körner, “Broadcast Channels with Confidential Messages,” IEEE. Trans. IT-24, 339 (1973).
- [8] P. A. M. Dirac, Principles of Quantum Mechanics, (Clarendon Press, 1981); 日本語訳は, 朝永振一郎ほか訳「量子力学」岩波書店, 1968 年.
- [9] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu and A. Peres, “Optimal Eavesdropping in Quantum Cryptography.I. Information Bound and Optimal Strategy,” Phys.Rev.A, 56, 1163–1172 (1997)
- [10] N. Gisin et al., “Quantum Cryptography,” Rev. Mod. Phys., 74, 145–195 (2002).
- [11] T. Hasegawa et al., in Proceedings of CLEO/Europe-EQEC2005, Munich (2005).
- [12] H. Inamori, N. Lütkenhaus and D. Mayers, “Unconditional Security of Practical Quantum Key Distribution,” quant-ph/0107017, (2001).
- [13] N. Nütkenhaus, “Estimates for practical quantum cryptography,” Phys.Rev.A, 59, 3301 (1999).
- [14] N. Lütkenhaus, “Security against Individual Attacks for Realistic Quantum Key Distribution,” Phys.Rev.A, 61, 052304 (2000).
- [15] N. Lütkenhaus, “Quantum Cryptography,” arXiv.org, quant-ph/0601207 (2006).
- [16] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, (Cambridge Univ. Press, 2000); 日本語訳は「量子コンピュータと量子通信 I, II, III」木村達也訳, オーム社, 2004 年.
- [17] J. J. Sakurai, Modern Quantum Mechanics, (Addison-Wesley, 1994); 日本語訳は, 桜井明夫訳「現代の量子力学 上, 下」吉岡書店, 1989 年.
- [18] P. W. Shor and J. Preskill, “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol,” Phys.Rev.Lett., 85, 441–444 (2000).
- [19] T. Tsurumaru, “Implementable quantum bit-string commitment protocol,” Phys.Rev.A, 71, 012313 (2005).
- [20] T. Tsurumaru, “Group Covariant Protocols of Quantum String Commitment,” arXiv.org, quant-ph/0606030 (2006).
- [21] E. Waks, H. Takesue and Y. Yamamoto, “Security of differential-phase-shift quantum key distribution against individual attacks,” Phys.Rev.A, 73, 012344 (2006).
- [22] M. N. Wegman and J. L. Carter, “New Hash Functions and Their Use in Authentication and Set Inequality,” J. Comput. System Sci., 22, 265–279, (1981).

私が出会った本

山本博資 (東京大学)



山本博資 (東京大学)

編集理事から、本に関して何か思い出話を書いて欲しいとの依頼があった。どの本を取り上げようと部屋の書架を眺めてみると、情報理論の研究を進める上でお世話になった本が、多数あることに改めて気付かされた。思い出深い本の一つにしぼるのは難しい。修士で情報理論の研究を始めて以降、若い時代に Shannon 理論を勉強するのに役立った幾つかの本について思い出話を書くことにしたいと思う。

私は 1975 年に修士に入学したが、当時は洋書の値段が非常に高かった。1971 年まで続いた 1 ドル 360 円の固定為替が、1971 年のニクソンショックで 1 ドル 308 円に下がり、さらに 1973 年のオイルショックで変動相場制に移行して 1 ドル 270 円ほどに下がってはいたが、現在の為替レートから考えると 2 倍以上の高額なレートであった。また、洋書の取扱店が利益確保のため、洋書の値段に対する換算率は 1 ドル 360 円に近い高額なレートがかなり長く続いていた。そのため、洋書の購入は、私のような貧乏学生に取っては高嶺の花であった。

そのような状況のため、洋書は研究室の本をコピーして読むのが普通であったが、自分で初めて買った洋書は、Wozencraft と Jacobs の “Principles of Communication Engineering” [1] であった。この本は 720 ページの分厚い本であるが、東京大学出版会が 2800 円という安価な値段で Reprint を出版していた。この本を購入することになった理由は、東

大電気系の大学院の講義で、原島博先生^{*9}が教科書として使ったためでした。その授業では、本の内容に関しては全く何も講義をせずに、本の章末問題を順番に学生に解かせるという形式のものでした。自分に割り当てられた問題を解いたり、他の学生が解いた問題の説明を理解するためには、自分で本を読んで理解しておく必要があった。2,3 週間で一章ずつ進み、月に 1 度程度は割当が回ってきたので、なかなかしんどい授業であった。しかし、半年間でほぼ全部を読み終えたときには、科学英語を読む力がかなり付いたように感じた。章末の問題数がかなり多いため、我々が講義を受けた年は奇数番目の章末問題を解き、その 2 年後に開講された同じ講義では偶数番目の章末問題を解いていた。後輩から偶数番目の解答を手に入れ、全て揃った解答集が今も手元に残っている。この授業形式は、教師にとっては講義の準備がほとんど必要なく、自分の興味のある本に対して章末問題の解答集を作ることができるので、とても旨味のある講義方法と思う。自分が大学教員になって以来、一度まねをしたいと考えているが、私の大学院の講義は受講者数がそれほど多くないため、その機会がないまま現在に至っている。

修士と博士のときに一番お世話になった本は、それぞれ、Gallager の “Information Theory and Reliable Communication” [2] と、Berger の “Rate Distortion Theory” [3] であった。[2] の本は、いわゆる Gallager 流のランダム符号化と誤り指数の導出テクニックが詳しく書かれている。この本でそれらのテクニックを習得できたおかげで、修士の研究で提案した「再送要求を伴う Viterbi 復号法」に対して、その誤り指数の下界 (誤り率の上界) の導出を行うことができ、IEEE IT Transactions に初めて論文を掲載することができた。

博士課程では、多端子通信システムにおけるレー

^{*9} 1999 年本学会会長

トひずみ理論の研究を行っていたが、レートひずみ理論に特化して詳しく書かれた Berger の本 [3] が非常に役立った。特に, Berger が “Remote Source” と呼んだ通信モデル (情報源出力を雑音通信路を通して観測したものを符号器で符号化して送信するモデル) が紹介されていたが, この Remote Source を Slepian-Wolf 型に拡張した通信システムが, 博士論文で取り扱った大きなテーマのうちの 1 つとなった。

Shannon 理論の強力な解析手法としてタイプ理論があるが, Csiszár と Körner によりその詳しい本 [4] が出版されたのが 1981 年である。出版前に, その Preprint を韓太舜さん^{*10}や小林欣吾さん^{*11}らが入手し, その本の勉強会に加えてもらった。専修大の佐藤創さんの世話で, 箱根や白浜などの寮で数日間泊まり込みで何度か勉強会が行なわれた。当時, 徳島大に就職した直後だったため, 科研費もなく, また情報理論と無関係な講座に所属していたため上司からの旅費のサポートもない状況であったが, 自費で関東まで出かけて勉強会に参加していた。この投資のおかげで, タイプ理論をマスターすることができ, その後のシャノン理論の研究で, 投資以上の実りを得ることができた。

もうひとつ思い出深い本に, Cover と Thomas の “Elements of Information Theory” [5] がある。1989～1990 年に Stanford 大学に 1 年ほど滞在していたときに, 丁度この本の執筆中であった。Thomas が

TeX で原稿を書き, その印刷出力を Cover が修正するというプロセスを繰り返して執筆を進めていた。当時, Thomas は博士課程の学生で, 本の作成と平行して博士論文の執筆も行っていたが, Thomas も Cover も博士論文より, この本の執筆に力を入れていたように思う。本と博士論文の両方の Preprint をもらって読んだが, ある日, 博士論文の内容に関して Thomas に質問していたときに, たまたま Cover が来て「本に関して何か問題点でも見つけたのか?」と質問され, 「本ではなく, 博士論文の疑問点について質問している」というと, 興味がないように出て行ったのが今でも印象に残っている。なお, この本は今年の 6 月に第 2 版が出版されている。

参考文献

- [1] John M. Wozencraft and Irwin Mark Jacobs, “Principles of communication engineering,” John Wiley and Sons, Inc, 1965 (東京大学出版会, Reprint 1971)
- [2] Robert G. Gallager, “Information Theory and Reliable Communication,” John Wiley and Sons, Inc, 1968
- [3] Toby Berger, “Rate Distortion Theory A Mathematical Basis for Data Compression,” Prentice-Hall, Inc. 1971
- [4] Imre Csiszár and János Körner, “Information Theory : Coding Theorems for Discrete Memoryless Systems,” Academic Press, Inc. 1981
- [5] Thomas M. Cover and Joy A. Thomas, “Elements of Information Theory,” John Wiley and Sons, Inc. 1991 (2nd. Edition 2006)

^{*10} 2000,2001 年本学会会長

^{*11} 2004,2005 年本学会会長

2006 Hawaii, IEICE, and SITA Joint Conference on Information Theory (HISC2006) 開催報告

藤原融 (大阪大学)



藤原融 (大阪大学)

2006 Hawaii, IEICE, and SITA Joint Conference on Information Theory (2006 HISC) は、2006 年 5 月 23 日 (火) から 25 日 (木) までの 3 日間、奈良市にある奈良県新公会堂で開催されました。

昨年 5 月にハワイ大学マノア校で第 1 回が開催され、今回が 2 回目に当たります。第 1 回のハワイでの会議が参加者に好評で次回は日本でということで、古都での開催となりました。前回同様、主催が本学会と電子情報通信学会情報理論研究専門委員会で、IEEE IT Society、ハワイ大学電気工学科の協賛でした。



会場の奈良県新公会堂

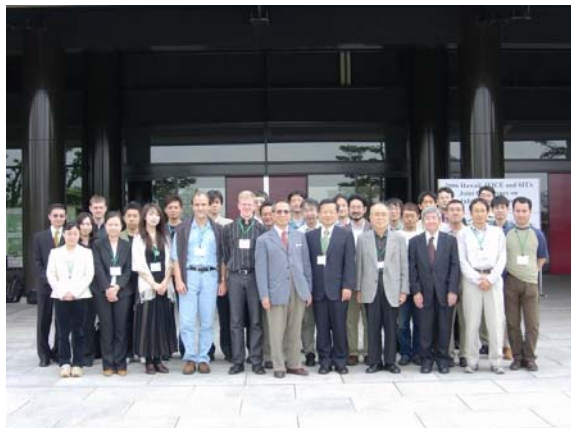
会議は、招待講演 2 件、一般講演 8 セッション 24 件で、45 名の参加をいただきました。招待講演は、米国プリンストン大の小林久志先生と中央大/産総研の今井秀樹先生にお願いしました。小林先生には、”35

years' progress in digital recording”というタイトルで、今井先生には、”Error-correcting codes and Cryptography”というタイトルで、興味深く、また、若手研究者を勇気づけるお話をいただきました。



小林久志先生の招待講演

参加者 45 名の内訳は、招待講演者 2 名、日本人の一般参加者 38 名 (うち、学生 9 名)、外国人の一般参加者 5 名 (うち、学生 2 名) となっています。今回、海外からの参加が少なかったですが、アメリカの大学における留学生は、米国外へ出ることが難しいという事情があるようで、これが大きく影響したようです。この会議の目指すところの一つは学生同士が積極的に交流することなのですが、その意味では、事前調査が十分でなかったことを反省しております。とは言え、懇親会も含め、参加者同士の交流は活発に行われておりました。



HISC2006 参加者の集合写真

ある先生からは、実効のある国際交流をするためには、こういう小規模な学会が(特に学生には)良いと伺いました。私も以前からそう思っておりましたが、特に、若手研究者や学生の方にとって、小さな会議は海外の研究者や学生と交流する良い機会だと思います。最近では業績評価等で、著名な国際会議で発

表することが重要視されております。もちろん、それも極めて大事なことです。小さい会議の効用も考えていただければと思います。

今回の会議は、松嶋敏泰先生(早稲田大)、Marc Fossorier 先生(ハワイ大)、私の3名が世話役となり、幹事の榎勇一先生(奈良先端大)、渋谷智治先生(メディア教育開発センター)を中心に多くの方のご協力で開催いたしました。幹事のお二人をはじめ、実行委員としてご活躍いただいた皆様、特に日本側実行委員の岡育生先生(大阪市大)、鴻巣敏之先生(大阪電通大)、村松純氏(NTT)、和田山正先生(名古屋工大)に深く御礼申し上げます。

来年(2007年)は主催団体等に変更がありますが、5月頃に初回と同じハワイ大学マノア校で開催する予定で準備を始めております。CFP等準備が整いましたら、ご案内させていただきますので、特に若手研究者や学生の方、是非ご参加下さい。

第5回アジア・ヨーロッパ情報理論ワークショップ(AEW5)開催案内

主催 Shannon Foundation

共催 デュイスブルグ・エッセン大学実験数学研究所, IEEE German Chapter on Information Theory, IEEE IT Society Japan Chapter (申請中)

協賛 情報理論とその応用学会

開催期間 2006年10月25日(水)-10月27日(金)

開催場所 西帰浦 KAL ホテル, 済洲島, 韓国

URL <http://www.exp-math.uni-essen.de/mdd1/Registration.pdf>

2006 年度第2回理事会報告

情報理論とその応用学会

2006 年度第2回理事会

2006 年 7 月 29 日(土) 13:30~17:30

於 東京工業大学 大岡山南3号館2階
201号室(電気情報系第一会議室)

議事

1. 2006 年度第1回理事会議事録確認

2. 2005 年度予算執行状況・会費徴収状況

3. 2006 年度予算案

4. 2006 年度事業中間報告及び計画

5. 2006 年度ニューズレター発行状況及び計画

6. SITA2005 開催報告・監査報告

7. SITA2006 開催計画

8. SITA2007 開催計画

9. ISITA2006 開催計画

- | | |
|----------------------|----------------------------|
| 10. ISITA2008 開催計画 | 17. 予稿集 DVD について |
| 11. 名誉会員の推薦について | 18. その他 |
| 12. SITA2005 奨励賞について | (a) 会費無料会員に関して |
| 13. 新規入退会者の承認について | (b) 役員に関して |
| 14. 会則の修正について | (c) 英文表記に関して |
| 15. 英語 web page について | (d) レクチャーノート著者見本について |
| 16. 協賛依頼の取扱について | (e) ISITA2010 開催候補の可能性について |

国際会議のお知らせ

以下のご案内する内容につきましては, 変更になっている場合もありますので, ご自身でのご確認をお願い致します。最新情報は以下のサイトなどをご覧ください。

IEEE ConferenceSearch

URL <http://www.ieee.org/conferencesearch/>

ICC 2008

日時 2008 年 5 月 19 日-5 月 23 日

場所 Beijing, China

URL 未定

締切 未定

Globecom 2007

日時 2007 年 11 月 26 日-11 月 30 日

場所 Washington, DC, USA

URL 未定

締切 未定

VTC 2007-fall

日時 2007 年 10 月 1 日-10 月 3 日

場所 Baltimore, MD, USA

URL <http://www.ieeevtc.org/vtc2007fall/index.html>

締切 未定

PIMRC 2007

日時 2007 年 9 月 2 日-9 月 6 日

場所 Athens, Greece

URL 未定

締切 未定

ITW 2007

日時 2007 年 7 月 1 日-7 月 6 日

場所 Bergen, Norway

URL <http://www.selman.uib.no/ITW2007.html>

締切 2007 年 3 月 16 日

ISIT 2007

日時 2007 年 6 月 24 日-6 月 29 日

場所 Nice, France

URL <http://www.isit2007.org/>

締切 2007 年 1 月 8 日

ICC 2007

日時 2007 年 6 月 24 日-6 月 28 日

場所 Glasgow, Scotland

URL <http://www.icc2007.org/>

締切 締切済み

INFOCOM 2007

日時 2007 年 5 月 6 日-5 月 12 日

場所 Anchorage, AK, USA

URL <http://www.ieee-infocom.org/2007/>

締切 締切済み

VTC 2007-Spring

日時 2007 年 4 月 23 日-4 月 25 日

場所 Dublin, Ireland

URL <http://www.ieeevtc.org/vtc2007spring/>

締切 締切済み

ICASSP2007

日時 2007年4月16日-4月20日
場所 Honolulu, HA, USA
URL <http://www.icassp2007.org/>
締切 締切済み

WCNC 2007

日時 2007年3月11日-3月15日
場所 Hong Kong, China
URL <http://www.comsoc.org/confs/wcnc/2007/>
締切 締切済み

Globecom 2006

日時 2006年11月27日-12月1日
場所 San Francisco, CA, USA
URL <http://www.ieee-globecom.org/2006/>
締切 締切済み

TENCON 2006

日時 2006年11月14日-11月17日
場所 Hong Kong, China
URL <http://www.ieee.org.hk/tencon2006/>
締切 締切済み

ISITA 2006

日時 2006年10月29日-11月1日
場所 COEX, Seoul, Korea
URL <http://www.isita2006.org/>
締切 締切済み

ITW 2006

日時 2006年10月22日-10月26日
場所 Chengdu, China
URL <http://sist.swjtu.edu.cn/imc/itw06/>
締切 締切済み

ISCIT 2006

日時 2006年10月18日-10月20日
場所 Bangkok, Thailand
URL <http://www.telecom.kmitl.ac.th/iscit2006/>
締切 締切済み

ニューズレター原稿募集

ニューズレター編集担当では、会員の皆様からの原稿をお待ちしております。研究会やワークショップなどの call for papers や国際会議などの参加報告、会員の声など、気軽に投稿して下さい。

今年最後のニューズレターの原稿の締切は11月末ですが、随時投稿を受け付けており、原稿を頂いた

時点での最近号に掲載する予定です。原稿は、できるだけ L^AT_EX のソースファイルが望ましいですが、その他の形式でも受け付けます。写真などの掲載も歓迎します。詳細は、巻末の編集理事・幹事にお尋ね下さい。

編集後記

本年度のニューズレターにおいて、何か新しい企画ができないものかと編集担当者で知恵を絞っていたところ、SITA 会長である坂庭先生より「通信学会誌に以前連載されていた『私のブックシェルフ』に類した企画をニューズレターでも行えば、若い学生の方々にとっても良い動機付けになるのではないか」というご意見を頂きました。SITA のニューズレターとしては、過去に『私の Key Paper』という企画がありましたが、書籍を題材としたものはありませんでしたので、坂庭先生のアイディアを頂戴しまし

て『私が出会った本』という新企画として本号よりスタートすることとなりました。大変お忙しいところ、新企画第 1 回目の執筆を快くお引き受け下さいました東京大学の山本先生、ならびにアイディアを提供して下さいった坂庭先生に心よりお礼を申し上げます。

今後も新しい企画などがあれば積極的に取り入れていきたいと考えておりますので、会員の皆様にはアイデア等ございましたら、是非編集担当までお知らせくださいますようお願い申し上げます。(中澤)

編集担当者

田島正登 (編集理事)

〒 930-8555 富山県富山市五福 3190
富山大学工学部知能情報工学科
Tel. 076-445-6766
Fax. 076-445-6703
E-mail: tajima@eng.u-toyama.ac.jp

中澤真 (編集幹事)

〒 965-8570 福島県会津若松市一箕町八幡門田 1-1
会津大学短期学部産業情報学科
Tel. 0242-37-2300
Fax. 0242-37-2412
E-mail: nakazawa@jc.u-aizu.ac.jp

植松友彦 (編集理事)

〒152-8552 東京都目黒区大岡山 2-12-1
東京工業大学大学院理工学研究科集積システム専攻
Tel. 03-5734-3243
Fax. 03-5734-2905
E-mail: uematsu@it.ss.titech.ac.jp

松本隆太郎 (編集幹事)

〒152-8552 東京都目黒区大岡山 2-12-1
東京工業大学大学院理工学研究科集積システム専攻
Tel. 03-5734-3864
Fax. 03-5734-2905
E-mail: ryutaroh@it.ss.titech.ac.jp

情報理論とその応用学会事務局

〒606-8585 京都市左京区松ヶ崎御所海道町
京都工芸繊維大学 工芸学部電子情報工学科内 若杉耕一郎 気付
Tel. 075-724-7481
Fax. 075-724-7400
E-mail: sita-office@sita.gr.jp
URL: <http://www.sita.gr.jp/>