東北大学サイエンスカフェ実施報告 ―偏光板による量子暗号の模擬実験―

林正人[1], 木村元[2]

[1] 東北大学 大学院情報科学研究科 数学教室

[2] 産業技術総合研究所 情報セキュリティ研究センター

1 はじめに

近年，様々な研究分野，様々な機関でサイエンスカフェという形で，科学の専門家が一般の人々に向けて自身の研究活動を語りかける機会が増えています．数学の分野も例外ではなく，他の分野と同様に，このような機会を設けるよう求められることが増えつつあります．

しかしながら，数学の分野の場合，成果を視覚的に伝えることが難しく，数学以外の研究者に対してさえ，成果を伝えることが難しいという現状があります．まして，一般の方にその研究の実態を伝えるとなると色々と難しいところがあります．数学の場合，他の分野に比べ，小学校の段階から触れる機会があるという点で，分野そのものの存在は知ってもらい易いという特徴があります．しかし，逆にその点がかえって，目新しさを失わせているのも事実です．サイエンスカフェでは，普通学校で学ばない，ある種の目新しさが無いと，なかなか，関心を持ってもらいにくいという点があります．特に，数学ではなかなか写真や映像にできる内容が少ないため，苦労することが多いようです．この点は，数学に限らず，電気通信の分野でも，同様のようです．

このような中，東北大学は地元の新聞社である河北新報や仙台市と協力して全国の大学に先駆けて，2005 年 8 月にサイエンスカフェをスタートさせました．以後，月 1 回の割合で東北大学の広報戦略会議主催で講師となった教員の企画という形で実施してきました．これまでの活動は以下のページに記録されています:

- 東北大学サイエンスカフェのトップページ：http://cafe.tohoku.ac.jp/
- 東北大学サイエンスカフェの活動記録：http://cafe.tohoku.ac.jp/event/
- 河北新報サイエンスカフェ特集ページ:http://www.kahoku.co.jp/spe/sciencecafe/index.html

会場は仙台市にあるせんだいメディアテーク（詳細は下記）という複合的な文化施設のエントランスホールを用いることが多いです:

- せんだいメディアテーク：http://www.smt.city.sendai.jp/

まれに，宮城県内の他の市のホールを用いることもあります．2008 年 5 月 23 日にせんだいメディアテークで行われた第 34 回東北大学サイエンスカフェでは「量子暗号・量子情報処理～新しい通信と情報処理～」というタイトルの下，林が講師を担当し，木村が司会を担当して開かれました．今回のカフェでは，量子暗号の模擬実験を参加者に体験してもらう企画でした．

2　東北大学でのサイエンスカフェの枠組み

はじめに，今回著者らが担当したサイエンスカフェについて説明する前に，東北大学の情報科学研究科 数学教室について簡単に説明します．東北大学には，本教室とは別に，昔から存在する理学部・理学研究科の数学教室があります．一方，大学院情報科学研究科は教養部改革において，教養部数学教室の一部の教員，工学部電気系の情報関係の教員，工学部機械系の情報関係の教員，教養部の文系の一部の教員などが集まって独立研究科として，1993 年に発足しました．本教室は情報科学研究科の数学関係の教員をメンバーとするグループとして運営されています．また，本教室のメンバー全員に関わる共通事項に関する運営・調整は教室世話人が行うことになっています．

東北大学のサイエンスカフェは，研究科などの各部局の推薦に基づいて担当講師が決まります．また，サイエンスカフェの翌日には，地元紙である河北新報にその内容が取り上げられ，ほぼ2ヵ月後に地元のケーブルテレビであるケーブルテレビ キャベツでその内容は放映されることになっています．通常は会場内に数ヶ所テーブルを設け，各テーブルに，一般参加者との交流を図るため，ファシリテータ（学生の補助員）を配属します．多くの場合，一方的な講演ではなく，講演時間の合間に設けるディスカッションタイムに参加者が講師が準備した企画を体験する双方向型の内容となっています．標準的な場合で，100 人の参加者を見込むと，5 人用のテーブルを 20 個準備するので，20 人のファシリテータの手配が必要となります．

数学関係では，これまで理学研究科の数学教室の小谷元子先生が担当しました．一方，情報科学研究科では，メディアリテラシーを専門にされている坂田邦子先生やロボット工学を専門にされている篠原歩先生が担当されました．そして，2008 年度は情報科学研究科では，数学教室のメンバーが１名サイエンスカフェを担当することになり，林が担当することになりました．2008 年度は本研究科の他のグループからロボット工学が専門の田所諭先生が担当されました．

3　サイエンスカフェの準備

2008 年の 1 月に大学の広報部のサイエンスカフェ担当者から林へ連絡があり，3 月に林の研究室にて，広報部担当者と林との間で東北大学のサイエンスカフェ実施のための打ち合わせが行われました．

そのときに，上述のようなサイエンスカフェの概要とサイエンスカフェ実施の手引きを渡され，20 名のファシリテータの手配が必要となることを告げられました．（学生がファシリテータを担当する場合，サイエンスカフェの予算から一定の額の謝金を支払うことができます．）同時に，ファシリテータの他に，司会となる人を確保の必要性も告げられました．普通は，講師と同じ所属研究室の准教授または助教の方で比較的講師の研究をよく理解している人が担当されることが多いそうです．しかしながら，林は 2007 年 9 月に着任したばかりであり，辛うじて 1 名の学生がいるものの，自分の学生だけでは必要なファシリテータの人数には到底足りません．また，林自身が准教授であり，2008 年 4 月の時点では本数学教室内に司会を依頼できる人が居ないという困難に直面しました．

最初に必要なことは，司会の確保でした．林は，2007 年度まで日本学術振興会の特別研究員として本数学教室に所属し，同じ量子情報を専門にしている木村に司会を依頼し，木村が司会を担当することになりました．次に，ファシリテータの確保ですが，教室世話人の浦川肇先生に相談し，情報科学研究科の数学教室の院生の方に呼びかけてもらったところ，林の学生の

他に，なんとか 9 名の大学院生がファシリテータとして協力してくれることになりました．その他，理学研究科の物理学専攻で量子情報を研究している堀田昌寛先生に依頼したところ，2 名の理学部物理学科の 4 年生をファシリテータとして紹介していただきました．また，本学の通信研究所で量子情報の実験を研究している枝松圭一先生にお願いしたところ，7 名の大学院生をファシリテータとして紹介していただきました．そして，林の共同研究者である国立情報学研究所の博士研究員の今井寛さんにも，ファシリテータとして協力していただけることになり，総勢 20 名のファシリテータの確保が可能となりました．

当日の企画内容は，林と木村が何度も電話で打ち合わせの上で，練り上げました．しかし，ほとんどのファシリテータが数学か物理のどちらかの専門的な知識を有するものの，量子暗号に関しては非専門家であるため，企画内容をファシリテータに理解してもらう機会が必要でした．そのために，ファシリテータへの説明会を 2 回開催することになりました．また，今回の企画では，後に述べるように，模擬実験のための小道具が必要で，これを 10 セット準備する必要がありました．偏光板や厚紙などの小道具を作成するために必要な資材は，あらかじめサイエンスカフェのために準備された予算で購入しました．ファシリテータへの説明会の時には，ファシリテータの方にこれらの小道具の作成をしてもらい，同時に，模擬実験実施時に陥りやすいミスをチェックしてもらいました．当日，参加者が無理なく模擬実験をこなせるよう模擬実験の手引書も著者たちの方で準備しました．このような準備を経て，2008 年 5 月 23 日のサイエンスカフェに望みました．

結果は，100 名を超える参加者が参加し，盛況のうちに終了しました．林の講演の後，多くの参加者がファシリテータの協力の下，あらかじめ準備した量子暗号の模擬実験を体験し，量子暗号の仕組みを多くの参加者が体験することができました．また，模擬実験の後の質疑応答においても，多くの参加者から質問がありました．質問に立った方には，高校生と思われる方から，東北大の学部学生と思われる方，そして，初老の方までおり，量子暗号，量子情報への一般市民の関心の高さを伺うことができました．

4　量子情報について

ここで，簡単に量子情報という研究分野について説明します．光子などの量子力学的な素子を用いて，通信や計算などの情報処理を行う分野が量子情報です．従来の情報処理技術では不可能であった情報処理をこれらの量子力学的な素子を用いることで可能にする分野です．詳しくは参考文献 [1, 2, 3, 4, 5, 6] を参照して頂くことにして，ここでは概略を述べます．

もちろん，これらの情報処理の実現にはデバイス技術の進展が欠かせませんが，現在のコンピュータや通信が単なる物理的なデバイス技術の集積だけでは，何の効力も発揮しません．いくら優れた CPU を作ったところで，アルゴリズムが無ければ，ただの半導体の塊に過ぎません．情報伝送技術も単に光子を用いて伝送するだけで，誤り訂正符号が無ければ，雑音だらけで使い物になりません．もちろん，秘匿性を確保した通信には，その安全性を保証するために，数学的な裏づけが必要となります．このように現在の情報処理技術でさえ，半導体や光に関するデバイス技術だけでは，使い物にならず，数学的な情報処理の理論が必要となります．ましてや，量子系では，量子論的非可換性のため，完全に制御できない部分が多くなりますから，誤り訂正技術などの情報理論的な数学技術が不可欠になります．

例えば，量子暗号では，光源の不完全性や通信路のノイズのため，盗聴者が部分的に情報を盗み取ることが原理的には可能になります．しかし，完璧なデバイスを作ることは現状では難

しいようです．また，近似的に単一光子源や無ノイズ通信路に見なせるデバイスを作ることはできても，やはり少しの誤差は残ることになります．

このような事情を考慮すると，確実に安全性を確保するには，量子通信終了後に秘匿性を確保するための秘匿性増強処理が必要になります．もちろん，そのようなプロトコルを実行するだけでは，数学的な議論は必要ないですが，最終的な安全性を評価するには数学的に緻密な議論が必要となります．このように，現在使われている暗号技術と同様に，量子暗号でも数学的な議論による安全性の保証が不可欠となります．

量子情報では，情報科学的な概念を用いることで量子力学系の問題を解析することも行います．従来の物理学の手法と異なり，近似を用いることが少なく，情報科学的な手法と相性の良い数学的に厳密なアプローチを取ることが多くなっています．そのため，群論的対称性のように，数学的に強力なテクニックが活躍することが多い分野です [9]．

5　量子暗号について

今回行った量子暗号の模擬実験の内容に入る前に，量子暗号の概略を説明します．特に，量子暗号の典型的なプロトコルである BB84 プロトコル [10] について説明します．

5.1　量子暗号とは

量子暗号は，量子力学の原理を利用して無条件に安全な暗号方式を提供するものです．すなわち，盗聴者の攻撃能力に何の制限も置くことなく，情報理論的に安全なメッセージ通信を行うことを保証します．ただし — その名前から誤解されがちですが — 量子暗号は，暗号方式その物を提供するものではないことに注意してください．暗号方式は，古くからその安全性が知られているワンタイムパッド方式[1]を利用します．量子暗号は，ワンタイムパッドで使用される秘密鍵を安全に配送する手段として考案されたものです．（したがって，より正確には「量子鍵配送」と言うことがありますが，本稿では「量子暗号」の用語を用いることにします．）ワンタイムパッド方式の安全性は，あくまでも秘密鍵を安全に共有できたことを前提としています．ところが，容易に想像つくように，秘密鍵の安全な配送を実現すること自体が，既に極めて困難な問題となります（鍵配送問題）．そのために，比較的容易に遠距離間の安全な鍵配送を実現する量子暗号が注目を浴びています．

それでは，なぜ量子論を利用すると秘密鍵の安全な配送が可能となるのでしょうか？量子論によると，一般に物理系は測定によって不可避的に乱されることが知られています（不確定性原理）．盗聴者がどのような手段で盗聴を試みたとしても，それは，秘密鍵の情報を得るための測定行為に他ありません．したがって，秘密鍵を（光子などの）量子系に符号化して（光ファイバ網などで）配送することにより，途中で盗聴者が鍵を盗聴（測定）すると，量子論の原理から必然的に系が乱されることになり，盗聴の痕跡が検知できます．盗聴されていない鍵（ま

[1] ワンタイムパッド方式は，メッセージの送信者（アリス）と受信者（ボブ）が，あらかじめ秘密鍵 K（ランダムな二進数列）を共有しておいて，送りたいメッセージ（二進数列に符号化された）M を K とビットごとの排他的論理和（XOR）を取ることで暗号化します．例えば $M = 0001101$，$K = 1101001$ であれば，$E := M \oplus K = 1100100$ が暗号文になります．アリスは E を公開通信路（手紙や電話など）でボブに送ります．ボブは E と K のビットごとの XOR を取ることで M を復号することができます（$E \oplus K = (M \oplus K) \oplus K = M$）．もし秘密鍵 K を知っているのがアリスとボブのみであり，暗号化に用いる鍵 K は一度だけ使う（ワンタイム）のであれば，この暗号方式は完全に安全であることが知られています [11]．つまり，仮に盗聴者が E を盗聴したとしても，それから M を解読することができません．

たは秘匿性増強を通じて盗聴者の情報をなくした鍵）をワンタイムパッドの秘密鍵として利用することができます.

現在主流となっている暗号方式は，計算量的な安全性に基づく（公開鍵）方式です．したがって，将来数学の発展によって解読される可能性があります．しかも，量子情報理論のもう一つの応用である量子コンピュータが実現されると，因数分解が高速に解けることがわかっています．例えば，有名な RSA 暗号は，簡単に言うと因数分解の困難さを利用した暗号方式なので，量子コンピュータによって簡単に解読されることになってしまいます．これに対して（ワンタイムパッド方式に基づく）量子暗号は，自然法則にのみ依拠するものであり，情報理論的な安全性が保証された究極の暗号なのです．この先どんなに数学が発展しようと，また，量子コンピュータが実現されたとしても，絶対破られることはありません[2].

幸いにも（？），現在量子コンピュータの技術に比べて，量子暗号の技術のほうがはるかに進んでいます．量子暗号は，ある条件を満たす任意の量子系で実現することができますが，通常は光子（光の粒）を利用します．光子は偏光と呼ばれる内部自由度を持っており，そこに鍵の情報を乗せることができます．さらに，光ファイバなどを利用して,（偏光状態を保ちながら）比較的容易に遠隔地間の送受信が可能です．光ファイバ網などのインフラが整えば，近い将来量子暗号は，政府間の — さらには一般のユーザーにとっても — 標準的な暗号技術になる可能性があります[3].

5.2 BB84 プロトコル

量子暗号には様々なプロトコルが提案されていますが，今回の模擬実験のベースとしたものは BB84 プロトコル [10] です．これは，1984 年に Benett と Brasard により世界で初めて考案されたもので，量子暗号のプロトタイプとみなされています．ここで，ごく簡単に BB84 プロトコルを説明しておきましょう.

（1 ビットの）秘密鍵（「0」または「1」）を光子状態に符号化して配送するためには，少なくとも（識別可能な）2 状態が必要となります．BB84 プロトコルでは，光子の偏光状態として四つの直線偏光 — 垂直偏光 $|0\rangle_+$ と水平偏光 $|1\rangle_+$，および，45° 偏光 $|0\rangle_\times$ と 135° 偏光 $|1\rangle_\times$ — を利用します．後で説明しますが，二つではなく四つの状態を利用することで，盗聴行為の検知が可能となります．この四つの状態を二つのタイプに分類して,「+ 基底」（$|0\rangle_+$ と $|1\rangle_+$）と「× 基底」（$|0\rangle_\times$ と $|1\rangle_\times$）と呼ぶことにします[4].

送信者（アリス）は 1 ビットの秘密鍵（「0」または「1」）をランダムに選ぶと同時に，基底（「+」または「×」）もランダムに選びます．例えば，秘密鍵「0」と「× 基底」を選んだ場合には，45° 偏光 $|0\rangle_\times$ の光子を受信者（ボブ）に送ります.（また，秘密鍵「1」と「× 基底」の場合は $|1\rangle_\times$，秘密鍵「0」と「+ 基底」の場合は $|0\rangle_+$，秘密鍵「1」と「+基底」の場合は $|1\rangle_+$ の光子を送ります.）これらの状態は偏光板を利用すると簡単に準備することができます．例えば，

[2]ただし量子論が正しいという前提は必要です．もっとも，量子論の予言に抵触するような現象は現在知られておらず，量子論は物理学の基本法則としての確固たる地位を確立しています.

[3]量子暗号はすでに実験の粋を出ており，製品化もされている技術です．また，スイスでは量子暗号を利用して選挙を行う計画もあるようです.

[4]量子力学では，これらの状態を 2 次元 Hilbert 空間 $\mathcal{H} \simeq \mathbb{C}^2$ の単位ベクトルで表します．$\{|0\rangle_+, |1\rangle_+\}$ と $\{|0\rangle_\times, |1\rangle_\times\}$ は，それぞれ $\mathcal{H}$ の正規直交基底であり，$|0\rangle_\times = \frac{1}{\sqrt{2}}(|0\rangle_+ + |1\rangle_+)$，$|1\rangle_\times = \frac{1}{\sqrt{2}}(|0\rangle_+ - |1\rangle_+)$ の関係を満たします．量子力学によると，直交する状態同士は確率 1 で識別することができますが，非直交する状態同士を確実に識別することはできません.

状態 $|0\rangle_+$，$|1\rangle_+$，$|0\rangle_\times$，及び $|1\rangle_\times$ は，それぞれ（ある基準角から）0 度，90 度，45 度，135 度に傾けた偏光板に光子を通すことにより作ることができます．

鍵の値を知りたいボブは，ランダムに「+ 基底」か「× 基底」を選び，アリスから送られてくる光子をその基底で測定します．この測定には，やはり偏光板を利用するのが一番簡単な方法です．実際，偏光板をある基準となる角度から（「+」を選んだ場合は）0 度に，（「×」を選んだ場合は）45 度に傾け，光子がこの偏光板を通過するかどうかを確認することが，それぞれの基底で測定することに相当します．

量子力学の法則によると，アリスとボブの基底が（たまたま）同じ場合には，ボブは状態に符号された鍵の値（光子が偏光板を通る場合が「0」，通らない場合が「1」）を確率 1 で知ることができます．例えば，アリスとボブの両者が「×」基底を選んでおり，アリスが送った状態が $|0\rangle_\times$（または $|1\rangle_\times$）であるならば，ボブは確実に「0」（または「1」）を測定することになります．ふたりの基底が「+」の場合にも同様です．このようにして，アリスとボブの基底が同じ場合には，秘密鍵を共有できます．一方で，基底が異なる場合は，ボブの測定値は（アリスの選んだ鍵の値と関係なく）確率 1/2 で「0」または「1」となります．例えばアリスの選んだ秘密鍵及び基底が「0」と「+」で，ボブの選んだ基底が「×」の場合，ボブの測定値は確率 1/2 で「1」となります．したがって，両者の基底が異なる場合は，秘密鍵を確実に共有することはできません．

これらのことに注意して，アリスは毎回ランダムに鍵の値と基底を選択して多数の光子をボブに送信します．ボブも毎回基底をランダムに選んで測定を行います．十分回数を重ねた後に，アリスとボブは公開通信路（たとえば電話）で，各回に選んだ基底を伝えます（ただし鍵の値や測定値は伝えません）．上に説明したように，たまたま基底がそろっている回では，鍵を確実に共有することができます．一方基底が異なる場合は共有できないので，そのような回のデータは捨てることにします（回数が多ければ，ほぼ半分のデータが残るでしょう）．量子暗号における秘密鍵の配送（及び共有）はこのようにして行われます．

上述した少し複雑なプロトコルを経由する目的は通信途中での盗聴者による盗聴の有無を検知することにあります．一方，盗聴者（イブ）の目的は，伝送中の光子を測定し，鍵のデータを読み取ることにあります．ただし，盗聴者イブの盗聴手段は，ボブと同じようにどちらかの基底を選んで測定する方法に限られているとします．

アリスとボブはたまたま基底が一致した回のデータのみを残しますが，そのような回にイブも同じ基底を選べるとは限りません（確率 1/2 で異なるでしょう）．量子論によると，イブが誤った基底を測定した場合は，状態は不可避的に乱されます．その場合，本来アリスとボブが共有するはずの鍵の値が異なる可能性があります．実際，鍵の値が異なる確率は 1/2 になります．よって，アリスとボブの基底が一致している場合に，イブが異なる基底を選ぶことで，アリスとボブの鍵の値が異なる確率は $1/2 \times 1/2 = 1/4$ になります．このようにイブの盗聴行為は，（アリスとボブの基底が一致している場合）本来一致するはずのデータに擾乱を与えるので，盗聴検知が可能となります．

アリスとボブは，盗聴行為の有無を調べるために，（基底が一致した回の）鍵の何割かを公開して，その中に鍵の不一致が無いかどうか調べます．（ノイズなどがない理想的な状況では）盗聴者がいなければ，それらは全て一致しているはずです．もし一致していれば，（極めて高い確率で）盗聴行為がなかったことを確信することができ，（残りの鍵も一致しているはずなので）アリスとボブは残りの鍵を安全な秘密鍵として，暗号に用います．一致しないデータが存在する場合（上述の盗聴の場合は約 1/4 のデータが一致しない）は，盗聴行為があったことになり，

残されているデータも安全でないので使用しません.

以上が BB84 プロトコルの概略です．プロトコルをまとめると次のようになります:

1. アリスは秘密鍵の値（$x = 0, 1$）と基底（$\alpha = +, \times$）をランダムに選び，状態 $|x\rangle_\alpha$ の光子をボブに送る.
2. ボブはランダムに基底（$\beta = +, \times$）を選び，アリスから送られてきた光子を基底 β で測定する（測定値を $y = 0, 1$ とする）.
3. 1,2 を $N(\gg 1)$ 回繰り返す.
4. アリスとボブは公開通信路を通じて，各回にどの基底を選んだかを伝え，たまたま一致した回（$\alpha = \beta$）のみ残す（約 $N/2$ 個のデータが残る）.
5. アリスとボブは，残ったデータの何割かを犠牲にして，その各回の秘密鍵の値（x, y）を公開する.
6. それらが一致していれば，公開しなかったのデータの（約 $N/4$ ビットの）鍵共有ができたことを確信できる．一方で，それらに不一致が見出されれば（典型的には約 $1/4$ の確率でデータに不一致がある），盗聴された可能性があるために，プロトコル全体をやり直す.

ただし，現実的な設定では,（たとえ盗聴者がいなくても，通信中の物理的ノイズを避けることはできないので），誤り訂正を通じて鍵の共有を行い，秘匿性増強を通じて盗聴された可能性のある情報を消す操作が必要となります.

6　模擬実験の内容

今回行った模擬実験の狙いは，暗号理論も量子論も知らない一般の聴衆を対象として，量子暗号の原理や仕組みを体感しながら身に付けてもらうことです.（模擬実験の前に，林が約 1 時間にわたり，暗号理論，量子論，及び量子暗号に関する講義を行いました.）実際の量子暗号を実現するレーザー装置や光ファイバなどの最先端技術を使用するのでなく，懐中電灯や偏光板など，安価ですぐ手に入れることができる道具だけを利用しました．ただし，光の偏光の性質に秘密鍵の情報を乗せる点や，量子暗号のプロトコルも同じものを利用している点は，実際の量子暗号技術と本質的にはほとんど同じものになるように工夫しました．したがって，量子暗号を気軽に体験し，その原理や仕組みを自然と理解することができるものになったと思います.

模擬実験のベースは，前節で説明した BB84 プロトコルです．実際の実験と異なる点は，光子一つではなく懐中電灯の光（多数の光子）の偏光に秘密鍵を乗せる点のみです．偏光の準備や測定は,（単一光子のときと同様に）懐中電灯の光を適切に傾けた偏光板を通すことによって達成できます.

まずは，アリス，ボブ役に分かれてもらい，アリスは秘密鍵と基底をそれぞれランダムに選び，偏光板を適切に傾けてから懐中電灯の光をボブに送ります．ボブは基底をランダムに選び，適切に傾けた偏光板を通じて懐中電灯の光が見えるかどうかを記録します.（見えた場合に「0」を，光が見えなかった場合に「1」と約束します.）この実験を多数回繰り返して，アリスとボブの基底がたまたま一致した回には，秘密鍵の共有ができたことを確認してもらいました.

続いて，イブが偏光板を利用して盗聴する場合の実験も行いました．イブ役の人は，アリスとボブの間で偏光板を用いて盗聴を行います．この場合，アリスとボブの基底が同じデータのうち，約 1/4 の鍵が一致しないことを確認してもらいました．この不一致によって，盗聴者の検知ができます．

以上，ごく簡単ではありますが，今回行った模擬実験の内容を説明しました（図 1 参照）．ただし，この模擬実験はあくまでも模擬であって，本当は安全ではないことに注意してください．繰り返し強調しますが，実際の量子暗号の実験とは異なり，懐中電灯の光はマクロな数の光子からなります．そのために，光子の偏光状態を変化させずに光子の一部を盗み見ることによって，痕跡を残さずに盗聴を行うことができます．

実際今回の模擬実験でも，最後にガラスを介して光線を二つに分け，一つはイブに，一つはそのままボブに行くようなデモンストレーションを行いました[5]．いわゆるビームスプリット攻撃と呼ばれる盗聴攻撃です．量子暗号が無条件に安全となるのは，やはり光子一つ一つを利用するなどして，量子効果（測定による不可避的な系の擾乱）が顕著に現れるスケールを実現する必要があります．この事実も含めて，今回行った模擬実験は，容易に入手できる道具のみを用いて，量子暗号の原理や仕組みを体感して自然と理解することができるものとなったと思います．

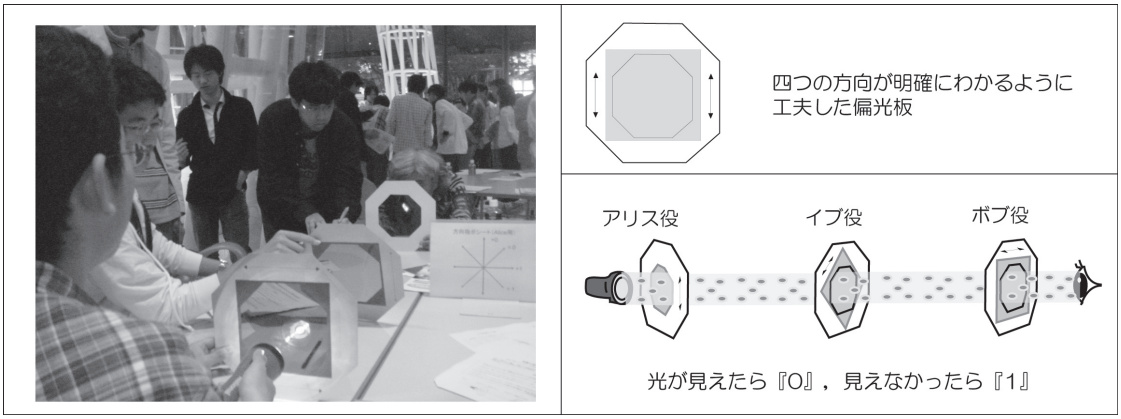

図 1: 模擬実験の写真（左）と模擬実験の図（右）

7　今後の展望

第 34 回東北大学サイエンスカフェとして実施した量子暗号に関するサイエンスカフェについてまとめました．今後数学の分野においても，一般市民や高校生を対象にした広報活動が必要とされることが増えることでしょう．日本では理系離れが問題になっているため，このような活動の必要性が今後向上すると思われます．

一方で，数学の分野で研究されている対象があまりにも一般生活からかけ離れた概念になってしまっていることも事実です．そのために，一般市民に対するアピール力が失われている面は否定できません．普段研究していると，自分の専門分野の中の概念に閉じこもって，研究活動を行いがちです．そのため，サイエンスカフェのような機会は，数学者にとっては負担になりがちですが，一方で，自分が取り組んでいる数学的概念を一般的視点から見直すよい機会です．

[5]ただし，反射によって偏光が変化してしまうために，盗聴者の偏光板の向きの調節が必要になります．

量子情報の分野は比較的新しい分野であるため，その研究活動の実態をより広くアピールすることが求められてきました．そのため，著者の１人である林はこれまで，海外の研究者を招聘し，国際会議を開催したり，所属していた研究プロジェクトの紹介ビデオの作成に携わりました [7]．また，所属プロジェクトの紹介冊子も作成し [8]，全国のスーパーサイエンススクールに配布するなどの活動も行いました．

その他，2009 年の 2 月には「量子情報科学　春の勉強会」を開催し，より広い層に研究活動を知ってもう機会を設けました．また，今回の述べた模擬実験は，2008 年 10 月 8 日に鬼怒川温泉にて開かれた第 31 回情報理論とその応用シンポジウムの夜のワークショップでも実施しました．この場合も多くの情報理論の研究者が参加し，昼間の研究発表では十分に伝わらない量子暗号について，理解を深めて頂きました．その後，21 年度の東北大学の学部 1 年生向けの企画である基礎ゼミでも，このような模擬実験を行っています．このように，従来の枠に囚われない形で，研究活動を広くアピールすることが今後求められるでしょう．

参考文献

[1] 小芦雅斗，小柴健史，量子暗号理論の展開 SGC ライブラリ 67, サイエンス社, 東京, 2008.

[2] 根本香絵, 「量子力学の考え方」〜 物理で読み解く量子情報の基礎 〜, SGC ライブラリ 68, サイエンス社, 東京, 2009.

[3] 林正人，量子情報理論入門 SGC ライブラリ 32, サイエンス社, 東京, 2004.

[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, Cambridge, 2000).

[5] M. Hayashi, Quantum Information: An Introduction, Springer-Verlag, 2006.

[6] 林正人，量子情報理論とその難しさ—より多くの人に知ってもらうために, 電子情報通信学会 基礎・境界ソサイエティ誌（Fundamentals Review: F R） 第９号掲載（2009 年 7 月）予定: http://w2.gakkai-web.net/gakkai/ieice/index.html

[7] サイエンスチャンネル （１４）量子情報技術の潮流〜量子計算・量子暗号の実現に向けて〜(第 16 回 TEPIA ハイテクビデオ・コンクールに入選)

`http://sc-smn.jst.go.jp/8/bangumi.asp?i_series_code=D047001&i_renban_code=014`

[8] 量子情報技術の潮流 pdf 版: http://www.qci.jst.go.jp/erato/kaisetu.pdf

[9] 林正人，量子情報と対称性，岩波数学叢書，岩波書店（準備中）.

[10] C. H. Bennett and G. Brassard,“Quantum cryptography: Public key distribution and coin tossing,” Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing (Bangalore, India, IEEE, New York, 1984) 175.

[11] C. E. Shannon,“Communication Theory of Secrecy Systems”, Bell System Technical Journal, vol. 28(4), pp. 656-715 (1949).