特集
Special Feature

［面白いぞ量子技術］

8 量子暗号の原理と実用化に向けた動向 ―絶対安全な通信の実現に向けて―

応用

水谷明博 | 三菱電機（株）情報技術総合研究所

現代暗号と量子暗号

現代において暗号は必須の技術である．たとえば，ブラウザで Web サイトにアクセスする場合，Web サイトの URL が https で始まっていればブラウザと Web サーバ間で暗号通信が行われている．これにより，機微なデータの盗聴，改ざんや通信相手のなりすましを防ぐことができる．この暗号通信では，RSA 暗号や楕円曲線暗号などの公開鍵暗号と AES や Camellia などの共通鍵暗号が使われている．このような普段我々が使っている暗号を現代暗号と呼ぶ．一方，量子暗号は現在実用化に向けて世界中で研究開発が進んでいる未来の技術である☆1．

2 つの暗号の相違点

はじめに，現代暗号と量子暗号の相違をまとめる（表 -1 も参照されたい）．まず，現代暗号は現代のコンピュータによる実装が可能である．暗号化の速度も高速であり，インターネットにさえ接続していれば通信距離の限界もない．一方,量子暗号は実装に専用の送受信機（たとえば，送信機にレーザ，受信機にアバランシェ・フォトダイオード）が必要になる．微弱な光を使って通信を行うが，その光は通信距離が延びるとより頻繁に損失が起こる．そのため，通信距離 100km で通信速度は 1Mbps 程度である．機能に関して，現代暗号は鍵共有，秘匿，デジタル署名や関数型暗号など高機能な暗号を実現できる．量子暗号は鍵共有という機能を持つ．

安全性に関しては，現代暗号と量子暗号で質的に大きく異なる．たとえば RSA 暗号の安全性は，大きい桁の合成数の素因数分解が効率的に解けないという仮定のもとに成立している．共通鍵暗号も効率的な解読アルゴリズムが存在しないという仮定のもとに成立している．このように「解読には膨大な時間がかかるはず」という予想のもとでの安全性を計算量的安全性という．この安全性の暗号では，今後の計算機や解読方法の改良により安全性が損なわれる可能性がある．たとえば，素因数分解は，量子計算機があればショアのアルゴリズムを実行することで効率的に解くことができる．また共通鍵暗号も DES や MISTY は 20 年程度で脆弱性（鍵の全数探索より効率的な解読方法）が見つかっている．現在，公開鍵暗号は量子計算機でも解けない問題に基づく暗号方式の選定が米国標準技術研究所によって行われており，2024 年頃に米国標準方式が決まる予定である．しか

■表 -1　現代暗号と量子暗号の比較のまとめ

	現代暗号	量子暗号
方式	RSA，AES など	BB84，差動位相シフト方式など
実装	通常のコンピュータで実装可能	専用の送受信機が必要
速度	高速（AES のハードウェア実装で数 Gbps）	低速（1Mbps 程度）
距離	限界なし	数 100km が限界☆2
機能	鍵共有，署名，秘匿など高機能	鍵共有
安全性	計算量的安全性	量子力学に基づく安全性

☆1　量子暗号というと，量子力学の性質を用いた暗号タスク全般を指し，量子鍵配送（Quantum Key Distribution, QKD）はその一例である．ただ，最もよく知られ，実現に近い技術が量子鍵配送であるため，本記事では量子暗号と量子鍵配送を同一視する．量子鍵配送以外の量子暗号に興味があれば，文献 1）を参照されたい．

☆2　数 100km という限界は，直接 2 者間で光を送受信した場合である．鍵共有の中継を行うノードがあれば，この限界を超えることは可能．

し，これも予想に基づく安全性にすぎず，いつでも今がショアのアルゴリズム発表前夜と同じ状況かもしれないという不安は残ることになる．一方の量子暗号は，量子力学という物理法則を安全性の根拠にしている．そのため，量子力学が正しい限りは量子暗号の安全性は決して脅かされることはない．

量子暗号の概要

量子暗号の目的

量子暗号は，以下の性質を満たす鍵（K_A, K_B）をアリス（A）とボブ（B）間に共有することを目的とする．

性質 1：2 者の鍵は同一のビット列である．

性質 2：第三者（盗聴者）が持つシステムと鍵に一切の相関がない．

性質 3：鍵の値の確率分布は一様ランダムである．

1 つ目の性質は 2 者間でビット誤りのないビット列を共有していることを示し，2 つ目の性質は鍵の値が第三者に漏洩していないことを示し，3 つ目の性質は 2 者が得る鍵は完全にランダムな確率分布から得られることを示している．2 者がこのような鍵 K を n ビット共有している場合，鍵は一度使ったら使い捨てる運用（ワンタイムパッド）のもとで，平文 M（n ビット）と排他的論理和を取ったデータ M⊕K を暗号文として伝送することで，無限の計算能力を持つ盗聴者に対しても安全な通信が可能になる．このような安全性を情報理論的安全性と言う．

量子暗号の前提

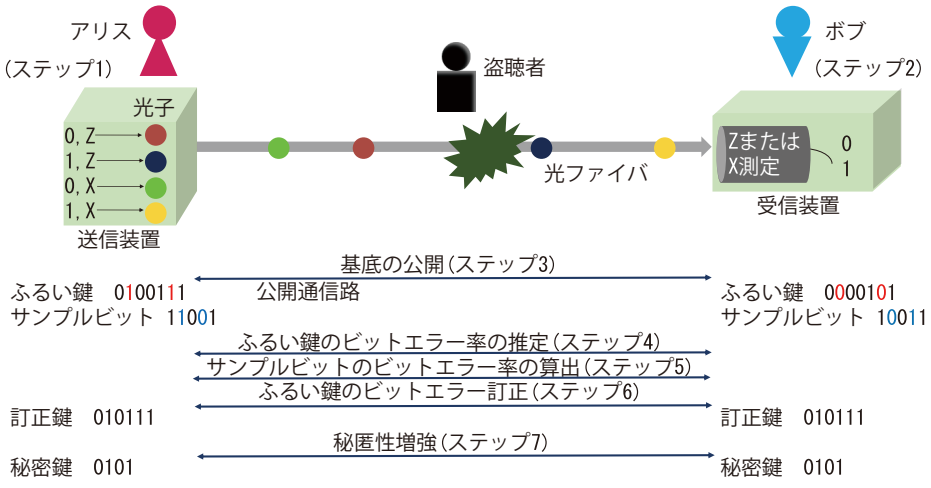
アリスとボブが持つ送受信装置の構成，通信路と盗聴者の前提をまとめる．図 -1 も参照されたい．

送受信装置

アリスはランダムな乱数データを生成し，乱数データが載った光を送信する送信装置を持つ．ボブはアリスから送信された光の状態を読み取る受信装置を持つ．たとえば，送信機はレーザと偏光回転素子が，受信機はアバランシェ・フォトダイオードが使われる．

通信路

量子暗号では 2 種類の通信路が使われる．1 つが，乱数データが載った光を伝送するための量子通信路（光ファイバ等）で，もう 1 つが認証された公開通信路（電



■図 -1　BB84 プロトコルの処理の流れ：（ステップ 1）アリスはビット値と基底をランダムに選択し，対応する光子をボブに送る．（ステップ 2）ボブは，Z または X 基底を選択し，その基底で光子を測定する．光子の送受信が終わった後，公開通信路を用いたデータ処理を行う．まず，（ステップ 3）アリスとボブは選択した基底を公開し，ふるい鍵とサンプルビットを得る．その後，（ステップ 4）ふるい鍵のビット誤り率を推定，（ステップ 5）サンプルビットのビット誤り率を算出し，（ステップ 6）ふるい鍵のビット誤りを訂正する．訂正鍵の一部の情報は盗聴者に漏れている可能性があるので，（ステップ 7）秘匿性増強でそれをキャンセルすることで秘密鍵を得る．

話やインターネット等）である．盗聴者は，量子通信路を流れる光を好きに操作できるが，公開通信路を流れる情報は盗聴できるが改ざんできないと仮定する．

盗聴者

盗聴者は量子通信路を流れる光に対して量子力学で許されるあらゆる操作ができると仮定する．これは，物理の世界で許されるどんな操作でも行える最強の盗聴者を考えるという意味である．この「あらゆる操作」は，数学的にはトレース保存完全正写像として定式化される．詳しくは文献 2）を参照されたい．量子暗号では通常，盗聴者がアクセスできるのは量子通信路と公開通信路のみで，アリスとボブが持つ送受信装置が置かれた部屋は完全にシールドされているとする．

代表的な量子暗号プロトコル

次に，上記で述べた性質 1 ～ 3 を満たす鍵の配送方法を，1984 年に Bennett と Brassard によって提案された BB84 を例に説明する．

送受信装置

送信装置は 4 つの光子[☆3]の偏光状態 $\{|0_Z\rangle, |1_Z\rangle, |0_X\rangle, |1_X\rangle\}$ のいずれかを放出するものとする．ここで $|0_Z\rangle$, $|1_Z\rangle$, $|0_X\rangle$, $|1_X\rangle$ は，それぞれ 0，90，45，135 度の方向に振動する光子の偏光状態を表す．$|0_Z\rangle = (1, 0)^T$ と $|1_Z\rangle = (0, 1)^T$ を 2 次元ベクトル空間の正規直交基底に取り，Z 基底の状態と呼ぶことにする．すると $|0_X\rangle$, $|1_X\rangle$ は各々 2 次元ベクトル $|0_X\rangle = (|0_Z\rangle + |1_Z\rangle)/\sqrt{2}$, $|1_X\rangle = (|0_Z\rangle - |1_Z\rangle)/\sqrt{2}$ と表現でき，これらを X 基底の状態と呼ぶ．アリスはランダムにビット値 $a \in \{0, 1\}$ と基底 $b \in \{Z, X\}$ を選択し，$|a_b\rangle$ をボブに送る．ボブは測定基底を {Z, X} からランダムに選択し，受信装置を用いてその基底で測定することで測定結果を得る．測定結果は {ビット 0 を観測，ビット 1 を観測，光子を観測しない} のいずれかになる．光子を観測しない事象は，通信路での光子の損失や受信機の効率が 1 でないなどの理由により起こる．

BB84 プロトコル

BB84 プロトコルの流れは以下である．図 -1 も参照されたい．

1. アリスはビット値と Z または X 基底のいずれかをランダムに選択し，選択したビット値と基底に対応する光子の偏光状態を，量子通信路を通じてボブに送る．この操作を N 回繰り返す．
2. ボブは，Z または X 基底を選択し，選択した基底で光子を測定して測定結果を得る．この操作を N 回繰り返す．
3. アリスとボブは，選択した基底を公開通信路で公開する．アリスとボブが共に同じ基底を選択したビットのうち，Z 基底を選択したビット値をふるい鍵，X 基底を選択したビット値をサンプルビットと呼び，基底が一致しないビット値はすべて破棄する．
4. アリスとボブはふるい鍵の一部を，公開通信路を通じて公開し，公開していないふるい鍵のビット誤り率を推定する．この推定結果を e とする．
5. アリスとボブはサンプルビットを公開通信路で公開し，サンプルビットのビット誤り率 e_X を算出する．
6. ふるい鍵のビット誤り率 e が誤り訂正可能な閾値よりも低い場合，アリスとボブは誤り訂正符号を用いてビット誤りを訂正する．訂正後にアリスとボブが共有する鍵を訂正鍵（R_A, R_B）と呼ぶ．
7. アリスとボブは訂正鍵に対して秘匿性増強を行うことで，秘密鍵（K_A, K_B）を共有する．

ここでステップ 7 の秘匿性増強は，大体秘密な乱数を完全に秘密な乱数にする統計処理である．実際の操作は，訂正鍵（R_A, R_B）に行列要素がランダムな値を持つ行列を作用させることに対応し，作用の結果が秘密鍵（K_A, K_B）になる．ステップ 6 のビット誤り訂正が鍵の性質 1 を満たすため，ステップ 7 の秘匿性増強が性質 2 と 3 を満たすために行うデータ処理である．なぜ，秘匿性増強を行った後の秘密鍵が第三者に一切漏洩しないかを次で説明する．

☆3 光子は電磁波におけるそれ以上分割できないエネルギーの最小単位である．

量子暗号の安全性

不確定性原理

量子暗号の安全性は量子の持つ不思議な性質である不確定性原理を根拠にしている．不確定性原理は，量子状態の測定と密接に関連している．例として，$|0_X\rangle$ を Z または X 測定することを考える．Z 測定の測定結果の候補は $\{|0_Z\rangle, |1_Z\rangle\}$ であり，X 測定の測定結果の候補は $\{|0_X\rangle, |1_X\rangle\}$ である．測定者が Z または X 測定を選ぶことは，測定結果の候補を決めることに対応する．X 測定を選択したとすると，測定される状態 $|0_X\rangle$ は，測定結果の候補 $\{|0_X\rangle, |1_X\rangle\}$ に入っていることが分かる．そのため，$|0_X\rangle$ を X 測定すると必ず $|0_X\rangle$ が測定結果になる．これは日常世界の言葉で言うと，コインが表の状態（$|0_X\rangle$ に対応）で渡され，それが表（$|0_X\rangle$ に対応）か裏（$|1_X\rangle$ に対応）かを見ることに対応する．

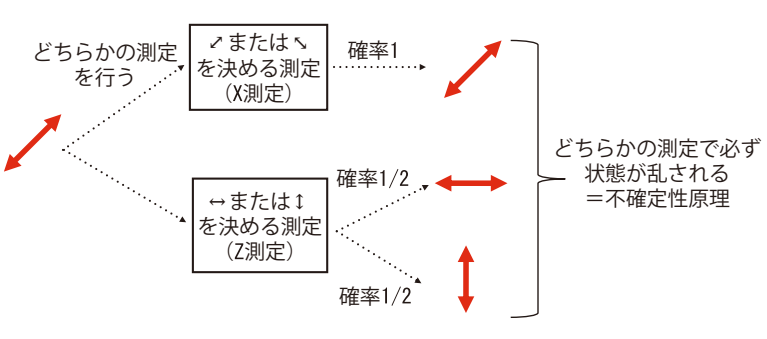
ここで重要なのは，コインの状態は測定の前後で変化しないということである．日常世界ではこれは当たり前のことだが，量子の世界ではこの常識が成り立たなくなる．つまり，測定の前後で測定される状態が変わる場合がある．それが，$|0_X\rangle$ を Z 測定した場合である．$|0_X\rangle$ を Z 測定する場合，測定結果の候補 $\{|0_Z\rangle, |1_Z\rangle\}$ に $|0_X\rangle$ は入っていない．このような場合，測定後の状態はもはや $|0_X\rangle$ ではなく別の状態に変化してしまう．さらにこの変化は確率的に起こり，確率 1/2 で測定結果 $|0_Z\rangle$，確率 1/2 で測定結果 $|1_Z\rangle$ を得ることになる．確率 1/2 は測定結果が完全にランダムになることを意味するが，これは測定の仕方を上手く工夫すると確定的な結果が得られるようになるわけではない．どれだけ技術が進歩しても，この測定結果を予測することは不可能である．量子力学というゲームのルールから確率 1/2 になることが決まるのである．

まとめると，どんな量子状態も Z または X 測定すると，少なくとも一方の測定で必ず測定対象の状態が乱される．これを不確定性原理と呼ぶ（図 -2 参照）．ここで説明した不確定原理は，情報エントロピーの言葉を使うと，H(W|Z) と H(W|X) をそれぞれ Z 測定と X 測定をした場合の測定結果 $W \in \{0, 1\}$ の条件付きエントロピーとすると，$H(W|Z)+H(W|X) \geqq 1$ と表せる．エントロピーの和が 0 より大きいところに，測定結果の「予測のできなさ」という気持ちが現れている．

BB84 プロトコルの安全性

盗聴検知の仕組み

不確定性原理のおかげで，アリスとボブは量子通信路上の盗聴行為を検知することができる．例として，量子通信路を流れる各光子を Z または X 測定する盗聴者を考え，盗聴がどのようにして検知されるかを説明する．もし BB84 プロトコルのステップ 1 と 2 でアリスとボブが選択する基底が X で一致しているにもかかわらず，盗聴者が Z 測定すると，不確定性原理より光子の状態が乱される．その変化した状態をボブが X 測定すると，ボブが得る測定結果はアリスが選んだ乱数と異なるという事象が起きる．この事象が起きると，サンプルビットにビット誤りが生じる．つまり，盗聴者が間違ってアリスとボブが選択した基底と違う基底で測定すると，その痕跡が「ビット誤り」という形でアリスとボブに検知されるのである．ここでは，Z,



■図 -2　不確定性原理の説明：↔，↕，↗，↖はそれぞれ文中で定義した $|0_Z\rangle$，$|1_Z\rangle$，$|0_X\rangle$，$|1_X\rangle$ を表す．X 測定は測定結果が ↗ または ↖ のどちらか，Z 測定は測定結果が ↔ または ↕ のどちらかを決めることに対応する．↗ を X 測定すると状態は乱れずに ↗ がそのまま測定結果になるが，Z 測定をするとランダムな測定結果が得られ，状態は乱される．

X 測定に限定したが，盗聴者がどれだけ複雑な攻撃をしても光子から情報を抜き取る操作を行うと光子の状態を乱してしまう．つまり，アリスとボブに気付かれずに情報を抜き取ることは原理的にできないのである．このため，ステップ 5 でアリスとボブが算出するビット誤り率 e_X が，どれだけ盗聴されていたかの度合いを表すことになる．ビット誤り率 e_X が大きければより多くの情報が盗聴されていることになる．ステップ 6 は，盗聴によって乱されたビット列を直し，アリスとボブで同一のビット列を共有するための手続きになる．

秘匿性増強で短くする鍵の量

ステップ 6 で得られる訂正鍵（R_A, R_B）は,同一のビット列ではあるが，盗聴者に一部情報が漏れている可能性がある．そのため，ステップ 7 で盗聴者に情報が一切漏れていないことが保障される長さまで訂正鍵を短くする秘匿性増強を行う．上記の BB84 プロトコルに関して結果だけを述べると，2 値エントロピー関数を $h(p)=-p\log_2(p)-(1-p)\log_2(1-p)$，ふるい鍵の長さを M とすると，M が無限の極限では $M\cdot h(e_X)$ だけ鍵を縮めるとステップ 7 で得られる秘密鍵は性質 1 ～ 3 を満たすことが示されている[☆4]．どれだけ鍵を縮めると安全な鍵になるかを示すことを安全性証明という．この安全性証明では盗聴者の攻撃は一切制限しないため，例に挙げた Z,X 測定をする盗聴行為は一例にすぎない．たとえば光子を個別に操作せずに，量子通信路を流れる N 個すべての光子を同時に操作し，情報が最も抜き取れる最適な測定をすることも可能である．このような盗聴者に対しても，秘匿性増強で $M\cdot h(e_X)$ だけ鍵を縮めると，安全な鍵が得られるというわけである．しばしば量子暗号の説明で，「盗聴されたビット数分だけ鍵を短くすることで安全な鍵を得る」と言うが，量子力学で許される最強の盗聴者が原理的に盗聴できる情報量の限界を「ビット誤り率」という古典的な情報を用いて推測できる点が，安全性証明の非自明さであり面白いところである．誌面の都合上この面白さを存分に説明できないが，安全性証明の詳細に興味がある方は文献 3) も参照されたい．

☆4 量子暗号の安全性証明では，秘匿性増強で訂正鍵を短くするビット長を推定する際，確率論における集中不等式（Hoeffding 不等式や Azuma の不等式など）を用いる．ふるい鍵の長さ（M）が有限の場合，推定量の期待値からのずれ（統計誤差）を考慮する必要があり，安全性証明が煩雑になる．そのため，多くの安全性証明では証明の簡単のため，ふるい鍵の長さは無限とすることで統計誤差を無視している．もちろん，ふるい鍵の長さが無限というのは現実的でないため，代表的な量子暗号プロトコル（BB84 や総当たり差動位相シフト方式など）では，ふるい鍵の長さが有限の場合の安全性証明（有限長解析）も行われている．

量子暗号の開発動向

ここでは，量子暗号の実用化に向けた世界の開発動向について述べる．表 -2 も参照されたい．

中国

量子暗号の開発で世界をリードしているのが中国である．中国は 2017 年に衛星を用いた量子暗号の実証実験に世界で初めて成功している．具体的には，7,600km 離れた中国とウィーンの 2 点（A，B）で鍵を共有するために，地点 A は鍵 K_A を，地点 B は K_B を量子暗号により衛星と共有する．その後，衛星が $K_A\oplus K_B$ を公開することで，$K_A\oplus K_B$ を地点 A が自分の鍵に足して K_B を地点 A と B が共有するという仕組みである．衛星を信頼できる古典ノード[☆5]として使うことで，大陸間での量子暗号に成功しているのである．また，2018 年には上海～北京におよぶ全長 2,000km の世界最大の量子暗号ネットワークを構築し，現在ではすでに ICBC などの銀行や保険会社がこのネットワークを利用している．今年の量子暗号

☆5 信頼できる古典ノードは，量子暗号では通信を行う 2 者以外は盗聴者と考えるが，中間の第三者も信頼できると仮定し，秘密鍵共有の中継を行うノード．

■表 -2　量子暗号の実用化に向けた世界の開発状況のまとめ

地域	開発動向
中国	衛星を用いた大陸間での量子暗号通信に成功．世界最長の量子暗号ネットワークを構築し，実運用が開始している．
米国	Quantum Xchange 社が金融機関向けに，量子暗号通信サービスの運用開始を発表．
欧州	ユースケースが設定された 16 個の量子暗号拠点を欧州全域に作り，各拠点でのユースケースの実施と，拠点を相互接続するテストベッドプロジェクトが始動している．
日本	東京 QKD ネットワークの試験運用の継続と，医療データの秘密分散に QKD ネットワークを活用する独自の試みを実施．

の国際会議 QCrypt 2020 で発表があったが，今後は小型衛星や小型地上局の開発を行い，地上のネットワークを中国全土に拡大する構想があるようである．

米国

米国では，2018 年に量子通信の企業 Quantum Xchange 社が，ウォールストリートにある金融機関を顧客ターゲットにした米国初の量子暗号通信サービスの運用開始を発表した．現在は，ボストン～ワシントン DC 間の 800km のネットワークだが，今後はアメリカ中部，西海岸まで拡大する計画があるようである．

欧州

欧州では，2019 年から大規模な量子暗号プロジェクト (Open QKD) が始動している．これは，約 1,500 万ユーロを投じ，2022 年までに欧州全域に 16 個の量子暗号拠点を作り，それらを相互接続するテストベッドプロジェクトである．16 個の拠点は，ウィーン，ブラチスラヴァ，オストラバ，グラーツ，パドバ，マテラ，アテネ，バルセロナ，オーバープファッフェンホーフェン，ジュネーブ，パリ，ケンブリッジ，デルフト，マドリード，ベルリン，ポーゼンである．各拠点で量子暗号のユースケースが設定され，量子暗号リンクを設置する計画である．すでにジュネーブでは 6 個の量子暗号リンクの設置（各リンク間の距離は 5 ～ 10km）が完了し，すでにユースケースが始まっている．今後は，オーストリア，スペイン，ドイツでの量子暗号リンクの設置が始まる予定である．

日本

日本は，2010 年に東京 QKD ネットワークテストベッドを構築し，現在も試験運用を行っている．このネットワークは，都内に敷設された光ファイバを使い，4 拠点（大手町，白山，本郷，小金井）を結ぶ総延長 200km ほどのネットワークである．また 2019 年には，NICT と NEC が量子暗号と秘密分散[☆6]を組み合わせ，医療データや生体認証データを管理するシステムを開発している．量子暗号ネットワークを 2 地点間の秘匿通信だけに利用するのではなく，データの分散バックアップに利用するという独自の活用も行っている．

今後の展望

量子暗号は現代暗号と比較して導入コストが高いと考えられる．ただ，世界の開発動向で述べたように，徐々に量子暗号の利用が広まっている状況を踏まえると，今後需要がさらに高まれば，量子暗号装置の価格も下がっていくことが予想される．量子暗号は鍵共有という用途に限定されるが，もし価格が数十万円となれば，量子暗号で（たとえば共通鍵暗号で使用する）鍵を配送しよう，という風潮が広まっても不思議ではない．このような将来が来るために，今後も量子暗号の理論家と実験家が協力して研究開発を進めることが不可欠である．現在，量子情報技術は世界中で活発に研究開発が行われているが，量子だからできる情報処理の実用化に最も近い技術が量子暗号である．究極のセキュリティという太古の昔から人類が求めてきた技術の実用化に向けて，我々も理論的な側面から研究開発を促進していきたい．

参考文献

1) Broadbent, A. and Schaffner, C. : Quantum Cryptography beyond Quantum Key Distribution, Designs, Codes and Cryptography 78, pp.351-382 (2016).
2) Nielsen, M. A. and Chuang, I. L. : Quantum Computation and Quantum Information, Cambridge Univ. Press., Cambridge (2000).
3) 小芦雅斗，小柴健史：量子暗号理論の展開，SGC ライブラリ 67 (2008).

(2020 年 9 月 30 日受付)

■水谷明博　Mizutani.Akihiro@dy.MitsubishiElectric.co.jp

2018 年大阪大学基礎工学研究科物質創成専攻博士後期課程修了．博士（理学）．同年三菱電機（株）に入社．情報技術総合研究所 情報セキュリティ技術部に所属し，量子情報の理論研究と情報セキュリティの開発を行っている．

☆6 秘密分散は，データを無意味化されたデータに分割し，各々を異なる遠隔のサーバに保管することで，一部のサーバが棄損しても元データを復元できる技術．