秘密鍵を安全に貸与できる関数型暗号

「ないことを証明する」，この困難な命題を“悪魔の証明”などといいます．しかし量子のふるまいを利用すれば，関数型暗号における秘密鍵の消去，つまり「消去したこと」を証明できます．また量子のふるまいを利用することで秘密鍵の複製防止も可能となります．本稿では，2022年の国際暗号学会において発表した技術の概要と，実装された場合に期待されるイノベーションについて解説します．

西巻（にしまき）　陵（りょう）
NTT社会情報研究所

クラウド時代に対応する高機能暗号と秘密鍵

「1対多」の通信に活用される暗号のうち「公開鍵暗号」と呼ばれるものがあります．事前に鍵を共有しなくとも誰でもメッセージを暗号化でき，復号には秘密鍵を用います．現在，公開鍵暗号に高度なロジックを埋め込むさまざまな「インテリジェント暗号」が提案されています．よく知られているのが，ユーザの属性ごとに鍵のアクセス権限を設定できる「属性ベース暗号」です．例えば「人事部」「課長」という条件を組み込んで暗号化した場合，完全に同じ属性の鍵を持つ人だけが復号できます．条件に適合しない，あるいは部分適合の「人事部/係長」「営業部/課長」といった属性の鍵では復号できず，メッセージの秘匿性が守られます．

2023年1月に発表した論文『Functional Encryption with Secure Key Leasing』[(1)]に登場する「関数型暗号」は，インテリジェント暗号の中でもより強力なものとなります．属性ベース暗号では平文を得ることしかできないのに対し，関数型暗号では平文から特定の情報だけを復号して任意の計算結果を得ることができます．実用化されれば，難病患者の医療情報がストックされているデータベースから，患者のプライバシに触れることなく統計情報だけを計算するといったユースケースが可能になります．高機能な暗号はクラウド時代の情報セキュリティに大きな力を発揮すると期待されています．

これらの秘密鍵は既存のコンピュータでも生成できます．反面，いったん配布された鍵データのコピーを防ぐことはできません．ユーザが鍵の返却や削除を主張しても，複製した鍵を隠し持っていれば依然として暗号文を復号できます．そこで，関数型暗号の秘密鍵を量子力学の原理を使って「消去」および「コピー不可能」にできることを数学的に証明し，よりセキュアな鍵の貸与を提案しました（**図1**）．

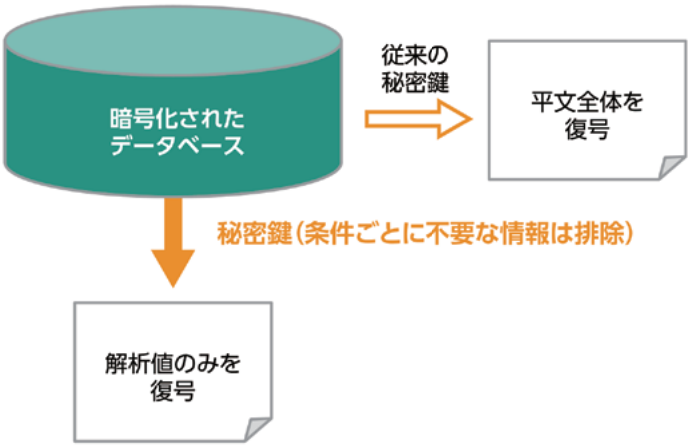

図1　高機能な関数型暗号

不確定性原理を利用し，「測定」で鍵を消去

前提として，鍵を貸与するホスト側も借り手のユーザも，共に量子計算機を使用していると仮定します．量子状態を保存できるメモリと，任意のアルゴリズムが実行できる量子計算機が実用化されており，ユーザに貸与する秘密鍵も量子の状態に変換して表現されています．この秘密鍵は重ね合わせ状態になっており，観測により状態が変化します．

このような秘密鍵を削除する方法は，まず量子ビットをなんらかのユニタリ変換*1で加工し，量子鍵を生成します．このとき計算基底（|0〉，|1〉）*2で測定すると鍵としての情報が残り，アダマール基底（|＋〉，|－〉）*3で測定すると鍵の情報が壊れるように設定します．

返却の時期が来たらユーザにアダマール基底で量子鍵を測定してもらいます．正しく観測されていれば不確定性原理によって鍵の情報は消去され，0か1で記述される古典情報だけが残ります．残った古典情報は消去の証拠として提出されます．

もし指定と異なる測定方法をとった場合，鍵の情報が残存しますから，返却したとは認められません．このように，状態を観測する方法を変えることで情報を部分的に消去し，鍵の機能を削除します（**図2**）．

秘密鍵が消えたことをどのように証明するのか，ないものを証明する「悪魔の証明」は可能なのか，これはとてもシンプルな方法です．秘密鍵を削除したときに，証拠として古典情報が提出されます．ホスト側はそれを確認した後，再度暗号文をユーザに送り，復号してもらいます．復号ができなければ鍵は存在しないと判断できます．つまり「復号失敗＝消去」と定義します．これを定式化するのです（**図3**）．

ノークローニングによるコピープロテクト

■秘密鍵のコピー防止

秘密鍵のコピー防止には量子の性質を利用します．自分自身が作成した量子状態は複製できますが，他人から与えられた未知の量子状態は「量子複製不可能定理（ノークローニング定理）」によって複製ができません．もし攻撃的なユーザが複製を試みたとしても2つの量子鍵のうちどちらかは正しい復号ができないのです．

しかもこの量子鍵は，鍵の機能を規定する情報を取り出すことができません．なぜなら前述したように，コピーしようと観測した瞬間に不確定性原理によって状態が変化し，鍵が消失するからです．測定せずに量子状態のまま置いておくしかありません．このような秘密鍵のコピープロテクトを定式化して証明しました．

暗号理論の安全性を，膨大な計算量から証明する「計算量的安全性」と，無限の計算能力を持った攻撃者にも解読されない「情報理論的安全性」に大別するならば，今回提案した手法は量子の性質と暗号理論の両方を利用するため前者の計算量的安全が保証されます（**図4**）．

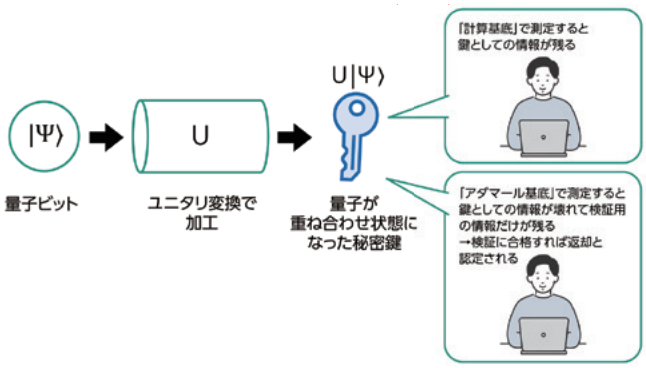

図2　量子秘密鍵の仕組み

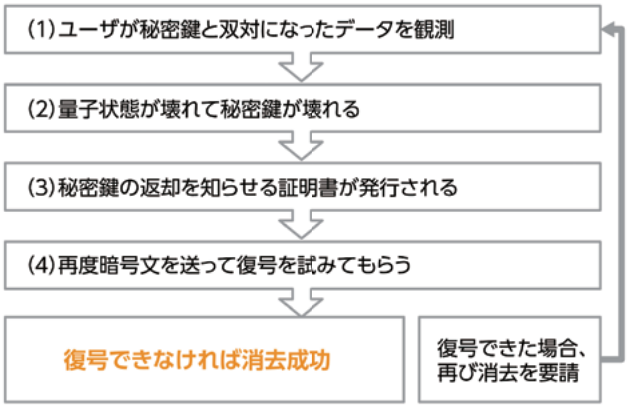

図3　量子秘密鍵の消去証明

＊1　ユニタリ変換：入力した量子ビットに演算を加えて変化させること．

＊2　計算基底：量子状態から情報を得るために行う基本的な測定．重ね合わせ状態になっている量子ビットは$|\Psi\rangle=\alpha|0\rangle+\beta|1\rangle$で表されますが，計算基底による測定を行うと，確率$|\alpha|^2$で測定値0を得て状態が|0〉になるか，あるいは確率$|\beta|^2$で1を得て状態が|1〉になります．

＊3　アダマール基底：量子状態が|＋〉か|－〉かを測定する．|0〉は|＋〉に，|1〉は|－〉に変換されます．

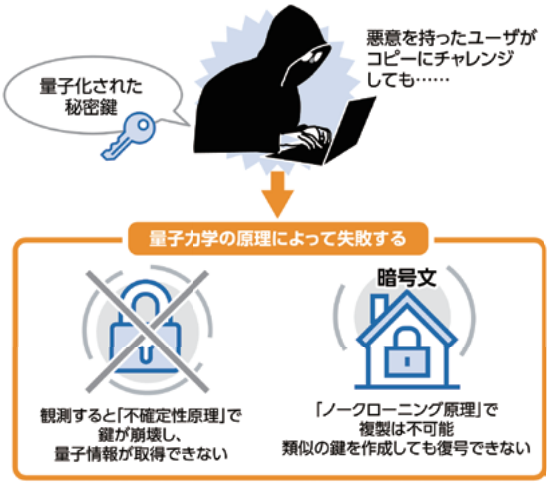

図 4　量子秘密鍵のコピープロテクト

■未来の量子社会に対応する暗号技術

現在，オンプレミス*4よりもクラウドが重視され，米国やカナダで公開されている量子計算機もクラウドサービスによって運用されています．このような 1 対多の通信環境においてより強力な暗号技術が求められています．

古典計算機でも鍵のデータを失効化する技術はいくつか提案されていますが，暗号文を生成するごとに秘密鍵をつくり直すタイプだと非効率で利便性に欠けます．また暗号文を一度全部更新するものだと元データの容量に比例してさまざまなコストが発生します．古いデータが残存するリスクも心配です．高機能暗号に量子力学を援用することで暗号化に伴うコストやリスクをスマートに解決できると考えました．

また，暗号化する手続きや具体的な技術へと発展させる理論など研究の範囲はまだまだ広がりそうです．

コンテンツサービスや忘れられる権利への展開

将来，今回の論文を軸としたものが国際標準となり，社会実装される可能性もゼロではないと思います．米国の国立標準技術研究所（NIST）などが次世代の暗号方式として選定すれば世界で標準化されるからです．

今回は秘密鍵に限定していますが，最終的にはプログラムの削除証明やコピー防止をめざしています．これらが実現した場合，企業の研究開発や情報管理，あるいはコンテンツサービスの提供方法なども変わるでしょう．顧客に量子鍵を渡してサービス利用期間中のみ有効とし，契約期間の満了と同時に鍵が無効化されるといったかたちで実装される可能性があります．第三者のサーバやクラウドサービスへの信頼性も高まりますし，著作権などのプロテクションもより強固になるでしょう．

また検索エンジンに残る古い暗号文を完全に抹消できれば，欧州連合（EU）が一般データ保護規則（GDPR）第17条に定めた「忘れられる権利（right to be forgotten）」にも応用できるかもしれません．今は「消しました」という相手の主張を信用するしかない状態ですが，量子力学を利用すれば新しい権利概念にも技術的に対応できる可能性があります（**図 5**）．

ただし，ある程度量子計算機が汎用化されて，一般的なユーザが使うようになれば，の話であり，現在のエラー訂正能力から考えると，もう少しエンジニアリングが発展しなければ実装はまだまだ先の話ではないかと思います．

さらに暗号技術は，いったんシステムが動き始めると世界規模となるため，更新は簡単ではありません．理論の構築から技術開発を経て社会実装に至るまではさまざまな要素が絡み合い，相応の時間を要すると考えています．

図 5　実装できるカテゴリ例

*4　オンプレミス：情報システムを使用者（企業など）自身が管理する設備内に導入，設置して運用すること．

■参考文献

(1)　https://link.springer.com/chapter/10.1007/978-3-031-22972-5_20

西巻　陵

古典計算機では実現が不可能な暗号機能を量子計算機の力によって実現できるようになります．今後量子計算機の力を利用した暗号技術は研究が進み応用が広がっていくことが期待されます．

◆問い合わせ先

NTT 社会情報学研究所
企画担当
E-mail　solab @ ml.ntt.com