現代暗号の発展と量子計算機時代の暗号研究に向けて

1976年から始まる現代暗号理論では，攻撃者を多項式時間チューリング機械とみなして安全性を考えていました．しかし，近年の汎用量子計算機の実現可能性はこのモデルを覆すインパクトを現代暗号にもたらしました．NTTの暗号研究は現代における情報システムの安全性を確立する技術を提供するとともに，量子計算機が普及した未来における応用の創出もテーマとしています．本稿では40年に及ぶNTTの暗号研究を概観し，現在の取り組みについて概説します．

阿部（あべ）　正幸（まさゆき）
NTT社会情報研究所

NTTの暗号研究を取り巻く状況

1982年の電電公社職員による銀行カード偽造事件に端を発したNTTの暗号研究は40周年を迎えました．発足当時わずか3名による暗号研究チームは，1992年に情報通信網研究所内で8名からなる正式な研究グループとなりました．これ以降，Webブラウザ Mosaicの登場（1993年）とともにインターネットが爆発的に普及してゆく時期と重なり，情報セキュリティの重要性が認識されて情報セキュリティプロジェクト（1999年）となり，さらにNTTセキュアプラットフォーム研究所（2012年）となりました．今日，情報セキュリティ技術はコモディティ化して日常生活を支えるものとなり，NTT社会情報研究所として広く暗号・情報セキュリティの研究に取り組んでいます．

ネットワークの高度化はさまざまな情報流通システムを可能とし，暗号も秘匿・認証という基本的な「守り」から，暗号通貨やクラウドコンピューティングなど新たな応用を創出する「攻め」へと適用範囲を拡大してきました．また，汎用量子計算機の実現可能性が高まり，現在実用化されている公開鍵暗号が急激に危殆化することが明らかになったことで，「守り」の利用でも新たな対応が迫られるようになりました．さらに将来を考えれば，汎用量子計算機を積極的に利用した暗号応用の創出と，それを支える基礎理論の確立が期待されるようになりました．

本稿では，暗号利用者と攻撃者の双方が現在利用できる計算機である，古典的な計算機を用いる「現代暗号」，攻撃者のみが量子計算機を用いる「耐量子暗号」，利用者も攻撃者も量子計算機を用いる「量子暗号」について（**図**），公開鍵暗号に関するトピックを中心に概観し，NTTの暗号理論研究とのかかわりについて述べます．もう1つの重要な研究トピックである共通鍵暗号については耐量子暗号の観点で述べることにします．

現代暗号理論の発展

安全で効率的な暗号は，あるクラスの問題を確率的チューリング機械で解

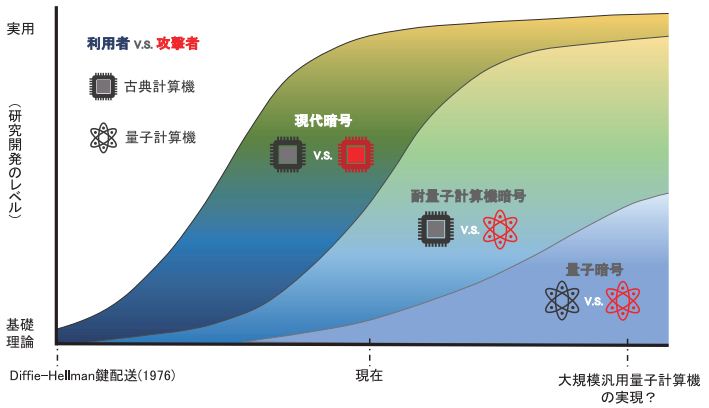

図　現代暗号・耐量子・量子 暗号の研究開発レベル

くことが平均的に難しいという計算量的な仮定に基づいて構成されます．攻撃者が利用できるアルゴリズムやハードウェアが進歩すると，個々の問題は以前より短い時間で解けるようになります．すると，その問題のクラスに基づく暗号では，安全性確保のためにより大きな公開鍵が必要となり，パフォーマンスが低下します．公開鍵暗号の先駆であるRSA暗号（1977年），Rabin暗号（1978年）やNTTが開発したデジタル署名方式ESIGN（1990年）は素因数分解問題の困難性を利用しています．開発当時，RSAの公開鍵は512ビットで安全と考えられていましたが，現在では3072ビット以上が推奨されています[(1)]．同じく先駆的な暗号技術であるDiffie-Hellman鍵配送（1976年），El Gamal暗号（1985年），DSA署名（1993年）は当初，乗法群上の離散対数問題を利用して構成されましたが，同じセキュリティレベルで公開鍵をより小さくできる楕円曲線上の離散対数問題に基づく構成（ECDSA署名など，2005年）に移行しました．

ネットワークの高度化によってクラウドコンピューティングのような高度な応用が出現し，暗号は基本的な秘匿・認証という守りの技術から，高度な情報流通サービスを構築するための攻めの技術へと発展してきました．楕円曲線上の群における双線形形写像（ペアリング）は，当初B. S. Kalisky Jr.によって安全な鍵生成に利用され（1987年），NTTの岡本龍明らによる楕円曲線暗号の安全性解析（MOV帰着，1991年）で広く知られました．その後，個人のIDを公開鍵にできるIDベース鍵交換（大岸聖史，境隆一，笠原正雄，2000年）やIDベース暗号（Dan Bonehら，2001年）で本格的に暗号に利用され，現在まで数多くの実用的な応用を創出しました．特に，それまで限定的だった非対話ゼロ知識証明の利用領域がペアリングの導入によって一気に拡大し（Jens Grothら，2008年），NTTでもペアリング群上でゼロ知識証明と署名などを自由に組み合わせて高度な機能を実現する群構造維持暗号系（阿部正幸ら，2009年）の研究が進展しました．ペアリングは，複雑なステートメントを短い証明書で効率的に検証できるComputationally Sound Proofという先進的な概念（Silvio Micali, 2000年）を，Zero-Knowledge Succinct Non-interactive Argument（zkSNARG）（Rosario Gennaroら，2012年）として実現することに大きく貢献しました．短い証明書はブロックチェーン上の応用に大変有効であるため，zkSNARGはWeb 3時代の基盤技術となることが期待され，C++のような高級言語で表現したステートメントをzkSNARGが扱いやすいNP完全な中間言語にコンパイルするフロントエンドの開発が進み，実用性が急速に向上しています．

暗号がさまざまな応用で利用されることや，暗号自体の高機能化に伴って，求められる安全性も高度化してきました．識別不可能性といった比較的単純な安全性に関しては，離散対数問題に基づくBlum-Micaliの疑似ランダム生成器（1982年）や素因数分解問題に基づくRabin暗号（1986年）のように，単一の困難性仮定への比較的単純な帰着による証明が示されてきました．しかし，攻撃者がより積極的に暗号システムの入出力に関与することを許した適応的選択暗号文攻撃に対する安全性（IND-CCA安全性，1991年）のような高度な安全性は，それを達成する暗号方式の構成も安全性証明も複雑になりました．Mihir Bellareらによる，ハッシュ関数を理想化して扱うランダムオラクルモデル（1993年）は，暗号の構成と安全性証明を単純化することに大きく貢献し，ランダムオラクルモデルが安全性の証明されたさまざまな暗号方式や応用が1990年代後半から2000年代に提案され，証明可能安全性のパラダイムが広まりました．NTTでは，IND-CCA安全な公開鍵暗号の一般的構成手法Fujisaki-Okamoto変換（FO変換，1998年），鍵カプセル化メカニズムPSEC-KEM（1999年），メッセージ回復型署名方式ECAOS（2008年）などがランダムオラクルモデルで安全性を証明できる方式として開発されました．一方，ランダムオラクルに基づかない効率的で証明可能安全な構成を追求する研究もさかんに行われました．

現在の計算機を対象として発展してきた暗号技術は，後述する量子計算機の登場以降の世界においても安全な暗号の構成に示唆を与えるものであり，暗号基礎理論として引き継がれていきます．

現代暗号から耐量子暗号へ

攻撃者が汎用量子計算機を実際に利用できるようになるまでにはまだ相当の時間がかかると考えられています．とはいえ，現時点で流通している情報の多くは収集され蓄積されているため，その将来的な安全性を確保するには，現在の暗号技術が汎用量子計算機を利用した未来の攻撃に耐える必要があります．耐量子計算機の安全な暗号の構成に用いる基本的な困難性仮定として，格子（Lattices）に基づく問題が有望視されています．格子問題の暗号への利用はAjtaiによる一方向性関数の構成（1996年）に始まり，その後，格子ベースで実用的な効率を持つNTRU暗号（1998年）が提案されています．デジタル署名については多変数多項式やハッシュ関数に基づく構成も耐量子安全性への有望な選択肢です．

2017年から開始されたNIST(米国国立標準技術研究所)によるPost-Quantum

Cryptography（PQC）Competitionで耐量子計算機安全な公開鍵暗号，デジタル署名の公募が行われ，2022年に最終候補が発表されたことから耐量子暗号は実用へと急速に近づきました．2024年には新たな標準となり，2030年までに現在の暗号に置き換えることが想定されています．NTTはNTRU暗号の提案元として，また，多数の候補の評価を行うかたちでNIST PQCコンペに貢献しています．量子計算機では重ね合わせ状態での演算が可能で攻撃者の計算原理が異なるため，安全性証明技法も量子計算機に合わせて再構築されてきました．前述のFO変換も量子状態で計算するハッシュ関数をモデル化した量子ランダムオラクルモデルで安全性が成り立つよう再検討され，NIST PQCコンペで採用された暗号方式CRYSTALS-KyberをIND-CCA安全とするために使われています．

格子は耐量子安全性の観点に加えて，高機能暗号を実現する基盤技術でもあります．特に，暗号化したまま平文の加算・乗算が可能である完全準同型暗号は，クラウドコンピューティングをはじめ，広範な応用を持つ強力な暗号技術です．NTTでは格子暗号の安全性解析や完全準同型暗号の研究（2013年～）に取り組んでいます．

ブロック暗号やハッシュ関数のような共通鍵暗号系の暗号技術については，内部構造を考慮しない汎用的な量子アルゴリズムを用いた鍵探索攻撃に対しては鍵長やブロック長を2～3倍にすることで安全性を維持できるため，整数論的仮定に基づく公開鍵暗号のような致命的な影響は受けないと考えられています．その一方で，よく知られた特定の構造に対して効果的な攻撃が示されているため，量子計算機による攻撃は共通鍵暗号にとっても新たなリスクです．本特集記事『量子計算機を用いた攻撃に対するハッシュ関数の安全性のより良い理解へ向けて』[2]では，量子計算機を用いた攻撃に対するハッシュ関数の安全性，特に，現在もっとも広く使われているハッシュ関数SHA-256やSHA-512を含むSHA-2の耐量子安全性について解説します．

耐量子安全なゼロ知識証明や暗号プロトコルの研究も進展していますが，直ちに現在の技術を代替する性能となるにはさらなる研究が必要です．例えば匿名電子投票では，従来の古典暗号技術で数kBの投票が，耐量子安全性の下では数100kBに増大してしまいます．これらは現在の暗号技術による情報流通システムの耐量子安全性への移行に不可欠な要素技術であり，早期の発展が期待されます．

そして量子暗号へ

近年のエッジデバイスの著しい計算能力向上はさまざまなアプリケーションを可能にしてきました．量子計算機が攻撃者だけでなく一般利用者にまで普及した未来では，どのような技術や応用があり得るでしょうか．量子物理学者のStephen Wiesnerは観測による量子状態の喪失を偽造不可能な量子マネーに応用するアイデアを1969年に述べています〔現在の暗号通貨や電子マネーの偽造防止は，取引台帳によるオンライン検証，暗号技術による事後検出，またはTEE（Trusted Execution Environment）の耐タンパー性などに拠っています〕．現在のデジタル技術では，情報が保管されていることを証明することはできても，消去されたことを証明することはできません．そのことが情報の廃棄を不確実にし，情報漏洩のリスクを生じています．本特集記事『秘密鍵を安全に貸与できる関数型暗号』[3]では，暗号の秘密鍵を消去したことを証明する研究を紹介します．量子計算機の話題が一般的になった現在，従来にない応用が模索されるだけでなく，基礎理論の確立をめざして量子物理，量子情報処理と暗号理論を融合する研究が行われています．本特集記事『新たな応用分野を切り拓く量子計算機向けアルゴリズム』[4]では，量子優位性，すなわち量子計算機の計算能力が現在の計算機を特定のタスクにおいて超えること，を示す研究を紹介します．

おわりに

NTT暗号研究を量子計算機の実現に関連して3つの分野に大別して概観しました．NTT社会情報研究所では基礎分野として今後も重要であり続ける暗号基礎理論から胸躍る遥か未来の応用まで多彩なテーマで暗号研究を進め，現在と将来の情報流通に貢献する技術を発信し続けます．

■参考文献

(1) https://www.cryptrec.go.jp/list.html
(2) 細山田：“量子計算機を用いた攻撃に対するハッシュ関数の安全性のより良い理解へ向けて，”NTT技術ジャーナル，Vol. 35，No. 5，pp.26-29，2023.
(3) 西巻：“秘密鍵を安全に貸与できる関数型暗号，”NTT技術ジャーナル，Vol. 35，No. 5，pp.19-21，2023.
(4) 山川：“新たな応用分野を切り拓く量子計算機向けアルゴリズム，”NTT技術ジャーナル，Vol. 35，No. 5，pp.22-25，2023.

阿部　正幸

暗号理論研究もその動機は目前のセキュリティリスクやこんな応用があったらいいという夢から始まっています．強固な理論を積み上げて，夢に届く技術を提供したいと思います．

◆問い合わせ先
NTT社会情報研究所
企画担当
E-mail　solab＠ml.ntt.com