URL https://journal.ntt.co.jp/article/28852
DOI https://doi.org/10.60249/24081101

NTT社会情報研究所
フェロー

阿部正幸 Masayuki Abe

量子計算機が普及した環境を想像して，それに耐えることができる暗号の基礎理論と応用技術の実現をめざす

情報漏洩やサイバー攻撃等に起因するインシデントに関する報道をしばしば見かけるようになりました．こうしたインシデントに際して，大切な情報そのものを守ってくれるのが暗号です．持ち出しや漏洩により外部に出た情報に強固な暗号がかかっていて解読されなければ，そのデータは単に「1」「0」の数字の羅列でしかなく，改ざんも行うことができません．こうした暗号技術は，インターネットの普及に伴い，ネット通販等の電子商取引や仮想通貨といったかたちで日常生活の中に広くいきわたっています．暗号化や解読は，コンピュータによる演算処理で行われていますが，コンピュータの性能向上とともに強靭性を確保するためにより複雑化してきています．こうした暗号に関する研究に取り組んでいるNTT社会情報科学研究所 阿部正幸フェローに，暗号を活用した新たな情報売買のモデル，知識を漏洩することなく何かを証明するためのツールであるゼロ知識証明の新たな展開，そしてお互いにリスペクトし合える居心地の良いコミュニティに対する思いを伺いました．

量子計算機の時代においても不変の基礎理論に立脚した暗号応用技術

現在，手掛けていらっしゃる研究について教えていただけますでしょうか．

2022年にフェローとなり，阿部特別研究室という新しい体制で，暗号に関して3つの領域における研究に取り組んでいます（**図1**）．時系列順に，「現在」「少し先の未来」「さらにずっとはるか先の未来」というかたちで大まかな分類をしていますが，ポイントとして量子計算機が登場する以前か以降か，そして，それが一般に広く普及した後という観点で分類してあり，現在は量子計算機が出てくる前の時代になります．

暗号は，悪意を持った人によるハッキングや攻撃，あるいはシステムトラブル等による漏洩から情報を安全に守ることが目的なので，悪意を持った人がどれくらいの計算能力を持っているのかを知ることがキーとなります．古典計算機（一般に普及している従来型の計算機）では，計算能力の向上もこれまでの延長線上で予想が可能です．一方，量子計算機は古典計算機の延長では考えられないパワフルな計算能力を有しているため，それを利用した今までにないタイプの攻撃者が登場します．したがって，量子計算機の実用化の前後で，暗号としても対応の仕方が全く異なります．さらにその先の量子計算機の普及により新たなアプリケーションも登場することで，それに対応する暗号も必要になってきます．そのため，量子計算機は暗号にとって非常に重要なファクターとなります．現在は，大規模汎用な量子計算機の登場の可能性やその時期がよく分からない状況なので，今からその出現に備えて研究を進めているところです．

こうした流れの中で，古典計算機の世界で研究されてきた暗号の理論については，今後も不変的な基礎理論となるものであり，その研究を継続して新たな理論を構築していくのが1番目の領域のテーマです．2番目の領域のテーマは，量子計算機が登場した段階でも安全な暗号構築をめざした研究です．そして，量子計算機が現在のスマートフォンのように完全に普及したときに，どのようなアプリケーションが登場し，世界がどのようになるのかということを想像して，それに対応する暗号を研究するのが3番目の領域のテーマで，若手の研究者を中心としてこのテーマに取り組んでいます．

私自身が取り組むテーマとしては，1番目と2番目の領域で，前回，本コーナーに掲載された時点（2021年5月号）では，ブロックチェーン上でスマートコントラクトを使って，売り手の持っている（正しい）情報を買い手が（正しい対価で）買うといった，

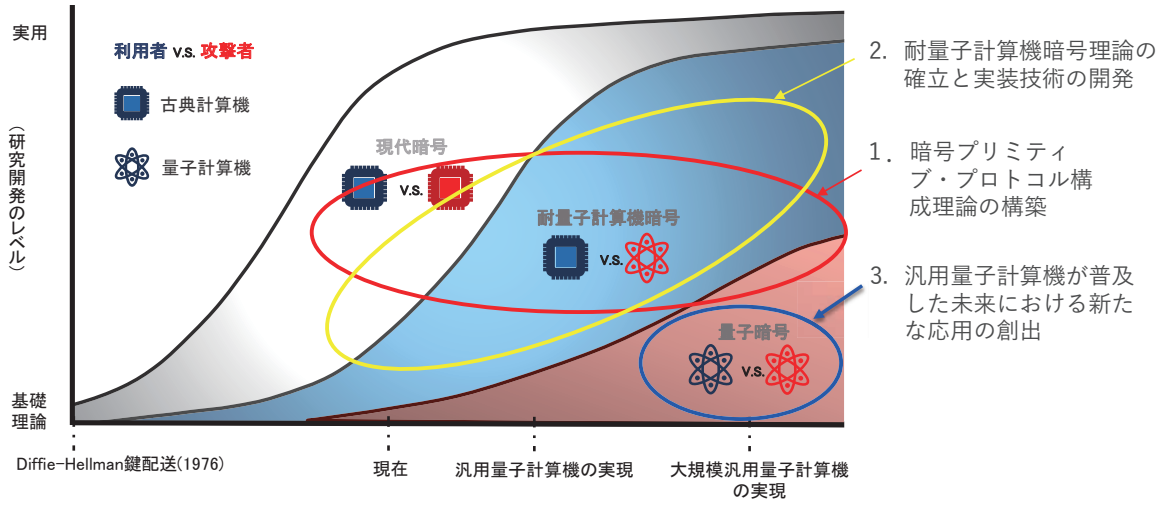


図1　NTT暗号研究の現在：3つの研究テーマ領域

安全・確実に情報売買する仕組みの1つとして，ゼロ知識証明とスマートコントラクトを組み合わせた方式を紹介しました（**図2** ⓐ）．現在はこれを一歩先に進め，売り手と買い手がお互いに何らかの情報を提供し合って，その結果を買い手が買うということを考えます．例えば，売り手が高精度な予測モデル（回路）を持っていて，買い手は，自分の保有する情報を売り手のモデルで予測した結果が欲しい場合に相当します．売り手は回路，買い手は入力情報を提供して演算することになりますが，モデル，入力情報ともに秘密性が高く相手方にそれを知られたくない場合の演算結果を安全・確実に売買する仕組みを研究しています（図2 ⓑ）．

前述のスマートコントラクトを活用して仲介者をたてることで実現する方法もあるのですが，コストが非常に高くなります．買い手の入力情報を暗号化して，暗号化された状態のまま売り手の側で演算し，暗号化された状態で買い手に戻す完全準同型暗号を使う方法もありますが，売り手の回路がオープンな状態であること，それにもかかわらず売り手の演算結果が正しいかどうかについて，買い手には分からないという課題があります．

そこで，2者間秘密計算として，暗号化された回路に暗号化（符号化）された情報を入力し，最終結果もある意味暗号化されたまま出てくるアプローチを考えました．演算過程の正しさは，売り手と買い手との間で回路をつくるための，お互いの情報に基づかない事前の予備的なやり取りを行うことで保証されます．そのやり取りが正しいとそこから先は実際の計算は絶対に正しい方法にしかできないことが保証される仕組みです．もし，予備的なやり取りの中でエラー等が発生したら，その段階ではお互いの情報はただの乱数として計算しているだけであり，元の情報の改ざんも秘密漏洩もないので，処理を中断すればいいだけなのです．現在，これを活用して計算結果の安全な媒介システムを開発しています．最近はAI（人工知能）を利用した予測等がかなり普及してきているので，計算結果を売ることが実際ビジネスとして登場してくるのではないかと期待しています．

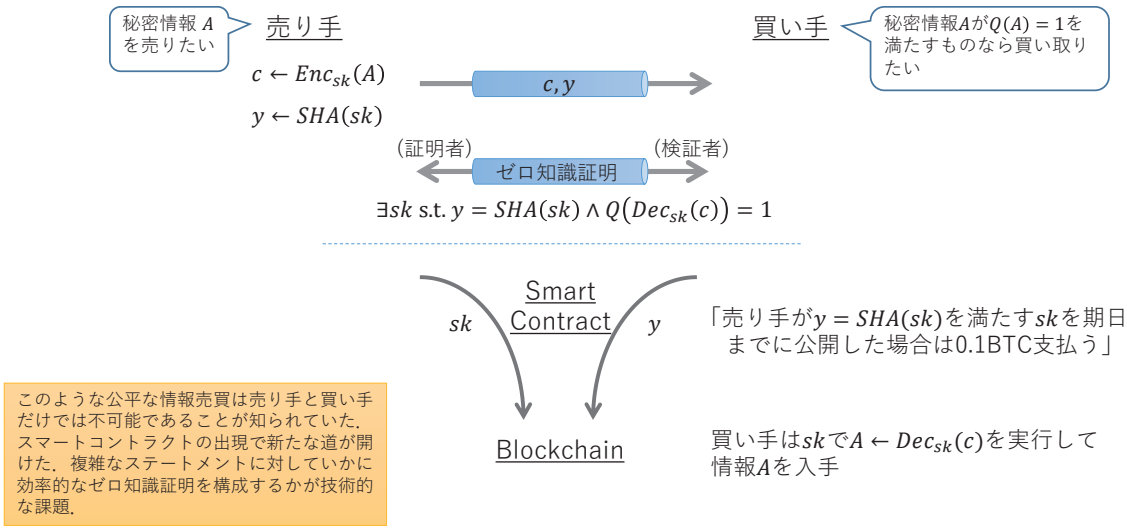
「安全な情報の売買を可能にする技術」以外に取り組んでいるテーマを教えてください．

暗号プロトコルを大きな柱としてのテーマにしています．暗号プロトコルは，いくつかのコンポーネントを，ある目的のために安全に組み合わせる方法を中心とした研究です．その中で，「ゼロ知識証明のcomposition技術」の研究に注力しています．

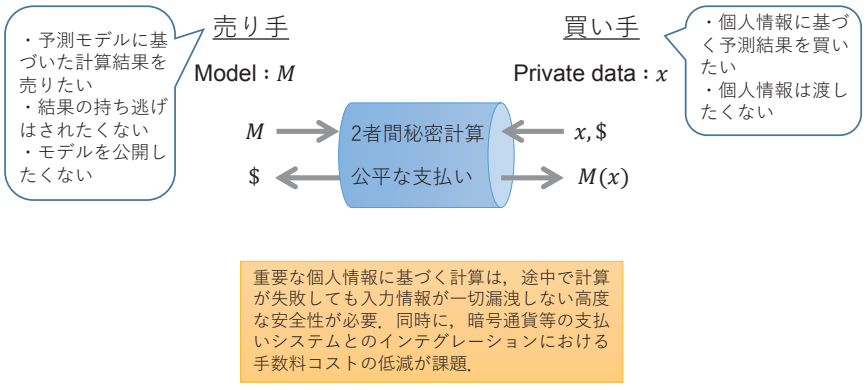
ゼロ知識証明は，知識を漏洩することなく何かを証明するためのツールです．例えば，羊の群れの中に特定のドリーという名前の羊がいるという事実を，ドリーが群れの中のどこにいるかという具体的な情報を漏らさずに，単にいるという事実だけを説明する技術です．例えば公開鍵を持っている人が，それに対応する秘密鍵を持っているという事実だけを相手に知らせるだけで，ゼロ知識証明によりそれは直ちに認証に使えることになります．この事例は1985年に開発されていますが，最近はブロックチェーンの領域では非常に有効な技術だと認識されて，応用技術の開発がここ数年で一気に進み，スタートアップ等の参入により，Web3，特にブロックチェーンとWeb3の領域において実際に使われて始めています．とはいえ，関連する理論がすべて出つくしたわけではなく，さらに開発が進んだ結果，新しい領域が登場してきたので，それに対応する技術を理論的に構築しているのが現在のテーマです．

さて，ゼロ知識証明で，前述の「公開鍵に対する秘密鍵を知っている」こと，かつ，例えば「私は1000ビットコイン以上の金額を保有している」ことを証明する方法がこのテーマのポイントとなります．「かつ（and）」の場合は，個々に証明されている2つの事実を両方同時に成立していることを証明すればいいのですが，「または（or）」の場合，特にどちらの事実が成立しているのかということを情報として相手に与えたくないようなケースでは，片方だけ証明すればいいわけではなくて，この2つのゼロ知識証明系をうまく組み合わせないと，どちらの事実が成立しているという情報が漏れてしまいます．したがって，orの場合は何らかの内部的な結合（composition）を行わないとうまく証明できません（ゼロ知識証明のcomposition）．

ゼロ知識証明のcompositionの研究は，1994年に大きな進展があったのですが，2つのゼロ知識証明系がそれぞれ持っている性質によりその組み合わせ方も次々と変化してきています．そして，3更新ゼロ知識証明といわれる従来からよく知られたスタイルのゼロ知識証明に対して，特にここ数年方式の進歩が目覚ましく，3更新ゼロ知識証明には合わないような，効率の良いゼロ知識証明が新たに出現してきました．これにより，5更新以上の更新回数のゼロ知識証明が効率良く実行できるようになりました．ただし，面白いことに，3更新のときにはうまくいっていたcompositionの方法が，5回の更新回数になるとアタックと呼



(a) ブロックチェーン上のスマートコントラクトを用いた安全な情報売買



(b) 計算結果の安全な売買

図2　情報売買

ばれる，例えば，（A and B）or（C and D）というステートメントの証明でAとC しか成立しないにもかかわらず検証にパスする証明をつくることが可能になるといった，証明の不完全性ができて情報が漏れる，もしくは安全性がうまく証明できないといった事例が出てきました．このため，新しく出てきた最新のゼロ知識証明に対応したcompositionの方法を開発する必要が出てきました．そこで，５更新・７更新等，定数ラウンドのゼロ知識証明を安全に組み合わせる方法を提案しました．この結果は，2024年８月18～22日に米国Santa Barbaraで開催される，暗号系の最高峰，最難関の国際会議である「Crypto 2024」において発表する予定です．

さて，従来のゼロ知識証明が使われている部分に，この技術を適用することで，より一層使いやすいものになるはずです．さらに，こういった技術は，今後，Web3やブロックチェーンの領域のみならず，さらに広い領域，効率的なゼロ知識証明を必要とするような領域全体に寄与していくような技術だと思っています．

研究者がお互いにリスペクトし合える居心地の良いコミュニティをめざして

研究者として心掛けていることを教えてください．

これまでも，暗号研究でNTTの研究開発に寄与していきたいという気持ちはありましたが，フェローになったことで，さらに広い視野で，コミュニティ全体において後継者，若い世代を育てていきたいという気持ちがより強くなりました．研究開発は，理論的な萌芽があるからこそ花開いている状況があるはずで，もし，その花を愛でて実を食べたらそこで終わってしまいます．だからこそ，後継者や若い世代の育成が必要になるのです．それと同時に，花（応用）を支える土壌（基礎・理論）は，常に栄養を供給しなければならないので，そこを強固なものにしていくことが必要であることを意識して，楽しみを見出しながら一生懸命取り組んでいきたいと思っています．さらにそのうえで，応用分野はスピードが速く，成果がいつまでもそこにあり続けることはないので，基礎の部分を活用して結果を次々と出していけるよう日々努力しています．

さて，現在は，特別研究室長と研究者の２つの立場があるのですが，室長としては，私のグループのメンバーは独立した優秀な研究者なので，独立性を尊重してメンバーがやりたいようにできる環境を整えることが自分のやるべきことと強く意識しています．一方研究者としては，私は先輩の背中を見て育ってきたのですが，今の研究者の研究スタイル・ライフスタイル等は昔の研究者とは違っていて，自分がメンバーにとっていいモデルになれるのか，ということを自問自答しています．私のスタイルがすべてではありませんし，年齢等に関係なく研究者として対等な関係なので，あくまでも１人の研究者として，若い人たちにとってのモデルの１例として背中を見せるように努力しています．

加えて，国際会議では，さまざまな人たちとつながりを持って議論することがコラボレーションの直接のきっかけになりますので，このスタイルは今後も保っていきたいと思っています．会議の場の議論や背中を見せることで，一緒に研究をしたいと思ってくれる人が出てくることほど嬉しいことはありません．

後進の研究者へのメッセージをお願いします．

世の中で，ミレニアル世代やZ世代等，生年・世代によって行動やライフスタイルの特徴を一括りにした言葉があります．研究者の世界も，研究環境の変化もあり，研究スタイル，ライフスタイル，そして考え方等が，若手，中堅，さらにその上職と異なり，中堅や上職が若手であったころと比較しても異なっていると思います．さらに，それが個人によっても異なります．

このようなメンバーによりコミュニティやチームが形成されると，自分の流儀を押し付ける傾向が出てきたり，お互いを理解することに時間がかかるため，どうしても不協和音が生じがちになり，決して居心地の良いコミュニティ，チームではなくなります．一方でコミュニティやチームとして前進して成果を出していくためには，この居心地が大切だと思います．居心地を良くするためには，時間をかけて理解し合えばいいのですが，それには年代，役職等に関係なく「自分に余裕をもって」，「お互いをリスペクトし合う」ことが第一歩ではないでしょうか．各世代それぞれ違う悩みがあり，その中で生き方や進む方向を模索しているのが現状だと思います．経験豊富な先輩が相談に乗り，または自身の経験を１つの事例として示すことができるので，そんなときには声をかけていただければと思います．

さて，コロナ禍においては人と直接会えなくなったので，研究をやりにくいと思っていたのですが，現在では種々の制約もなくなり環境も大幅に改善されてきたため，一気にフェース・ツー・フェースの直接コミュニケーションが活発になってきました．私は，これを嬉しく思い，この機を逃さずに，リモートワークの良い面を残しつつ，人対人の対面のコミュニケーションを活発にしていきたいと思っています．この対面コミュニケーションもコミュニティの居心地を良くするためには必要なことです．

居心地の良いコミュニティで一緒に研究をしていきましょう．