Cryptography & Information Security Laboratoriesの目標と研究

2019年7月に米国シリコンバレーで発足したNTT Research, Inc. の3つの研究所の中の1つがCryptography & Information Security Laboratories（NTT CIS Labs）です．NTT CIS Labsでは，暗号分野の理論研究を行い，暗号基礎理論を研究するグループとブロックチェーン理論を研究するグループを持っています．本稿では，このような体制で出発したNTT CIS Labsが何をめざしてどのような研究を行うかについて紹介します．

おかもと　たつあき†1　†2
岡本　龍明　/Brent Waters
まつお　しんいちろう†2
松尾　真一郎

NTT Research, Inc. NTT CIS Labs　所長†1
NTT Research, Inc.†2

はじめに

Cryptography & Information Security Laboratories（NTT CIS Labs）は，暗号基礎理論を研究するグループとブロックチェーン理論を研究するグループを持ち，暗号基礎理論グループの中には，Brent Waters を室長として暗号理論を深く研究するWaters研究室を設けています．本稿では，Waters研究室とブロックチェーングループについて焦点を当て，NTT CIS Labsの取り組みや目標，研究内容について紹介します．

暗号基礎理論研究グループ Waters研究室の取り組み

私たちは従来の暗号機能を超えた新たな暗号機能を実現することから，暗号基礎理論をより良くより深く理解することまでさまざまな分野の暗号理論の研究を行います．最初に注力するテーマの1つが暗号システムです．

暗号は，対処とするデータを特定の受信者だけが復号して読むことができるような暗号文に変換するプロセスです．暗号は私たちのセキュリティエコシステムの基盤です．それらは物理的に盗まれる可能性のあるデバイス（ラップトップPC, 携帯電話など）や，第三者のクラウドサーバなどに格納されているような機密情報を守るために使われています．また，暗号はしばしば大きくマスコミで取り上げられることも多く，例えば2015年のサンバーナーディーノでの乱射事件での議論や，ある事件の容疑者のiPhoneの暗号解読にApple社が強要されるべきかなどの議論がありました．

従来は利用者が公開鍵pkを公開し，それに対応する秘密鍵skを秘密に保持するという暗号の姿が広く知られていました．ある人がデータmsgを公開鍵pkを使って暗号文ctに暗号化するとします．このとき，データmsgはskを持つ者だけが復号でき，その鍵を知らない攻撃者はmsgについて一切の情報を知り得ません．

ところが最近になって，暗号に関するこのような姿は多くの応用にとってあまりに制約が大き過ぎることを認識するようになりました．例えば，アリスのメールサーバが彼女の公開鍵で暗号化されたメールを受信し，保存しているとします．このとき，彼女は保存された暗号文のうちスパムメールは自動的にサーバが削除するようにしたい（現時点では，サーバによってはそれを復号して削除している）とか，メールの内容に彼女の子どもの名前や「非常」「病院」などといった言葉が含まれていればサーバに警告メッセージを出してほしいといった要望を持っているとします．このような機能を実現するため，彼女は自分の秘密鍵をサーバに渡すこともできます．しかし，このことは第三者に彼女のすべてのメールを読むことを許すことになります．一方, 彼女が秘密鍵を管理している以上，スパム削除や非常警告といった機能を享受することはできません．これは，私たちが望む機能を手に入れるために従来の暗号の概念を超えた新たな概念や方式を生み出す必要を示した典型的な例となっています．現在，暗号分野では，このことが大変重要な目的であることが広く認識されており，そのような方向に沿ってさまざまな概念の暗号がつくられるようになってきました．そのような概念として，関数型暗号，完全準同型暗号，IDベース暗号，属性ベース暗号，トレータ追跡，代理再暗号化やそれ以外にも多くの概念が提案されるようになってきました．

私たちの研究所においても，このような研究を強力に推し進めていきます．目標の1つは，標準仮定の下で安

全性が証明された高度な機能を持った暗号方式を実現することです. まずは, 以下の3つの分野に焦点を当てて研究を進めていきます.

■選択暗号文安全性

選択暗号文安全性（IND-CCA）は従来の暗号においても新たな暗号機能においてもいずれも正しい安全性概念となっています. しかし, 多くの新たな暗号の結果は, 選択平文（IND-CPA）モデルでその暗号機能の安全性を論じています. 最近, 私たちはどのようなIND-CPA安全な属性ベース暗号（ABE）も, hinting PRGと呼ぶ新たな手法を用いることでIND-CCA安全なABEに変換できることを示しました. そこで, 数論の手法を用いてより高速でコンパクトなhinting PRGを実現することをめざします. さらに, ABEを超えてより一般的な関数型暗号や再ランダム化暗号に対しても適用できるIND-CCA変換方法の実現をめざしていきます. 最後に, これはIND-CPAを証明すればIND-CCAを意味するかという古典的な問題を新たな発想で解決しようとするアプローチとなっています.

■暗号システムの追跡

トレータ追跡は, 放送システムにおいて不正コピーした元デコーダ装置を追跡する問題です. 私たちは最近, 共謀不可な追跡システムとしてN利用者に対して$\lg(N)$サイズの暗号文となる方式を実現し, その安全性を標準仮定の1つであるLWE（Learning with Errors）仮定の下で証明しました. 従来の標準仮定に基づく最良の結果では, 暗号文サイズが$N^{1/2}$でした. ここで, 私たちが新たに目標とする問題は次のようなものを含みます.

- どのような定数cに対しても暗号文サイズが$N^{1/c}$の追跡・放送システムの実現
- 上記と同じ暗号文サイズで公開追跡機能の実現
- 追跡手法を利用した適応的安全性の証明手法の開拓

■LWEに基づく暗号における新たな開拓

LWE仮定はその耐量子計算機安全性や格子のワースト問題との関連において暗号における優れた方法として広く認識されています. また, よく検証された仮定から新たな暗号機能をつくる手法としてもLWE仮定を用いた方法は多くの結果を生み出してきました. 例えば最近の結果として, 完全準同型暗号, 任意の回路に関する属性ベース暗号, ロック可能難読化などがあります. これらは, 今のところ, 他の標準的な数論仮定を用いては実現されていません. ここで私たちは, LWEベース暗号を実現する新たな野心的な目標を提案します. まず最初に疑似ランダム関数を難読化する新たな概念とその応用を検討します. 次にLWE仮定から証拠暗号をつくるための方法を述べます. そこへの中間段階として, ビットを定めた機能に対する制限付きPRFを実現します.

私たちの理論研究所はこの分野で幸先の良いスタートをしました. WatersとDaniel Wichsは, 共著のCrypto2019論文にて, 暗号文サイズが$N^{1/c}$の追跡・放送機能をLWEに基づくトレータ追跡と双線形写像による放送暗号の手法を組み合わせることで実現しました. 現在, Waters, WichsとMark Zhandryは, LWEベースの属性ベース暗号の適応的安全性を実現する新たな手法と限界について共同研究を行っています.

ブロックチェーン理論研究グループの取り組み

■ブロックチェーンの歴史

2008年にSatoshi Nakamotoがビットコインの論文を公表して以来, 暗号技術, ピー・ツー・ピー（P2P）ネットワーク, ゲーム理論, 経済学などの要素を組み合わせたインターネット上における新たなデータの信頼モデルの基盤として, ブロックチェーンと呼ばれる技術が, 幅広い注目を集めています. ビットコイン自体は, 支払いの履歴の帳簿を, 中央管理を行う主体なし

に，P2Pネットワークに接続されたユーザの協力の下で，一定時間ごとに更新していく仕組みです．そして，その帳簿に記録されたデータそのものをお金のように考えることで，ユーザ間の支払い（Payment）に応用したものです．ビットコイン自体は，支払いというアプリケーションに特化したシステムになっています．しかし，「P2Pで接続されたユーザの協力で，共通の帳簿をアップデートしていく」という仕組みは，支払い以外のアプリケーションが広く考えられるために，その中核的なプロトコルの部分を「ブロックチェーン」と名付けて，より汎用的な技術として世界中で研究開発が行われています．

ブロックチェーンの研究のインパクトを理解するための一番のキーワードは，Permissionless Innovation（許可のいらないイノベーション）です．インターネットが中央的な組織を介さないグローバルな通信を実現し，誰もが新しいイノベーションのつくり手になるチャンスをつくり出しました．ブロックチェーンは，帳簿の維持と多様なステークホルダがプログラム可能な帳簿を共有し，帳簿に基づいた新しいアプリケーションを誰もが自由につくり出せるようにするというインパクトがあります．ブロックチェーンの有望なアプリケーションは何かという質問は，インターネットの有望なアプリケーションは何かという質問と同じで，個別の明確な答えがあるわけではなく，むしろ誰もが新しいアプリケーションを思いついて実験できる場がある，ということそのものに価値があります．

上記の意味において，ブロックチェーンにおける研究開発の大きなゴールは，「プログラム可能な共有された帳簿を利用したアプリケーションを，誰もが自由につくることができるような状態を実現する」ことです．ビットコインやブロックチェーンが近年大きく話題になり，あたかも広く普及する時期が間近であるようにも思えますが，実際に上記のゴールを達成するのは，非常に大きなチャレンジであり，長期にわたる基礎的，理論的な研究開発が必要であるのが現状です．

ブロックチェーンを構成する部品となる技術は，実は枯れた技術が多くあります．ブロックチェーンに使われる電子署名アルゴリズムECDSAや，暗号学的ハッシュ関数SHA-256は，長い歴史を持つ標準的な暗号アルゴリズムです．また，情報のハッシュ値を計算し，それをリンクさせていくことで，情報の存在の前後性を証明できるようにする暗号学的タイムスタンプも1990年の暗号技術のトップカンファレンスCRYPTOで発表されたものです．P2Pの通信を使って，帳簿のデータをすべての参加者で共有する技術も新しいものではありません．また，分散コンピューティングの世界では，複数の計算機の間でのデータの内容を合意する合意プロトコルの研究も長い歴史があります．ビットコインにおいては，セキュアな合意プロトコルとしてProof of Workと呼ばれるプロトコルが採用されていますが，これも元々はスパムメールを減らす方法の一環として暗号学的パズルと呼ばれる技術の1つの例として発明され，ハッシュベースの電子マネー方式であるHashCashの中で確立されていたものです．しかし，ビットコインとブロックチェーンが画期的であったのは，それらの枯れた技術を絶妙に組み合わせて，それまでには存在していなかった，中央サーバがなくても，一定のビジネスルール（例えば支払い）に従ったプログラムで帳簿をアップデートできる方法を初めて提示したことにあります．また，こういったネットワークが持続的に存在するために，ネットワークの維持に協力した人に新しいビットコインなどの暗号資産を付与するという，インセンティブ構造をシステムに組み込んだことが挙げられます．

■ブロックチェーンの課題

ブロックチェーンのセキュリティは，単に暗号学やネットワーク理論だ

けに支えられているわけではなく，前述のようなインセンティブ設計の妙が大きく寄与しています．また，性能とセキュリティの間には複雑なトレードオフの関係が存在しており，単純に性能を向上させようとすると，セキュリティが犠牲になるという微妙なバランスの上に成り立っています．現時点では，どのようなトレードオフの関係にあるのか，という点も理論的に十分解明されているわけではありません．むしろ，これからその理論的関係を明らかにして，より多くのユーザが，十分な性能を持ってブロックチェーンを使えるようにするための理論構築と実証を改めて1から行う必要があります．これは，極めて基礎的で長期的な研究課題であるといえます．ブロックチェーンにおける，理論的な大きな問題として知られているのは，スケーラビリティ問題で，オリジナルのビットコインでは1秒当り7トランザクションしか全世界で処理することができませんが，ビットコインのセキュリティの良さを損なうことなく，処理性能を上げるということは理論的に困難な問題で，世界中でこの問題を解決するための基礎的な研究が行われています．

■異なる専門性を持った研究者で構成

NTT CIS Labsのブロックチェーングループでは，前述のブロックチェーンの根本的な大きなゴールを実現するための基盤的な研究にフォーカスを当てています．特にフォーカスを当てるべき研究領域として，セキュアかつよりスケーラブルな分散合意アルゴリズムの研究，プログラム可能な帳簿のための安全なプログラミング環境を実現するための研究，そして，ブロックチェーン上での情報処理を行う際のプライバシ保護の実現のための研究に取り組んでいます．

前述のとおり，ブロックチェーンの理論研究はさまざまな異なる性質が絶妙に組み合わさっているため，異なる専門性を持った研究者のチームを組む必要があります．そのため，ブロックチェーングループのメンバーも，必要な専門性を考慮して構成しています．暗号プロトコルの安全性の専門家，ソフトウェアエンジニアリングの専門家，形式検証の専門家，そしてゲーム理論と経済学の専門家など，それぞれの分野で，第一線の研究者がグループに加わっています．ブロックチェーンはまだ若い研究分野であることもあり，今後トップレベルの研究成果を出すことが期待されるポストドクターや助教年代の研究者を早いうちに集めることも重要であり，そのような研究者も加えていく方針です．さらに，FacebookのLibraに対する各国規制当局の反応にも表れているように，規制当局の方針との整合性も，研究を進めていく時点ではバイデザインで考慮する必要があり，ブロックチェーンにまつわる規制の研究で先進的な米国の大学との共同研究も予定しています．

（左から）岡本　龍明/ Brent Waters/
松尾　真一郎

新たに米国シリコンバレーに誕生したNTT CIS Labsが何をめざしてどのような研究を行うかについて紹介しました．新天地で世界トップの研究者を集めてスタートした研究所から，暗号基礎・ブロックチェーン理論分野で世界をリードする結果が数多く生まれることを期待してください．

◆問い合わせ先
NTT Research, Inc.
NTT CIS Labs
E-mail　info@ntt-research.com