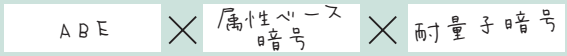


暗号とアクセス制御を組み合わせる革新的な属性ベース暗号（ABE）技術の最新動向

NTT Research, Inc. において取り組んでいる，暗号技術と属性によるアクセス制御を組み込んだ属性ベース暗号「ABE」に関する研究の論文を解説します．ABEはオフライン環境でも設定された属性に基づいて復号可能なデータを制御できる画期的な技術です．高効率なスキームや耐量子暗号への対応など，最新の技術動向を紹介するとともに，技術の普及に向けた活動についても紹介します．

Yannis Rouselakis

後藤（ごとう）　隆（たかし）

NTT Research, Inc.

はじめに

誰もがセキュアなデータにアクセスした経験があるでしょう．その場合，パスワードと，おそらく，別に生成されたパスワードとは異なるセキュリティコードを入力する必要があります．これらが認証されればセキュアなサーバによって，データが送信されます．

この流れの裏では，もっとさまざまなことが起きています．例えばパスワードは，通常，鍵導出関数によって鍵に変換されます．公開鍵とそれに対応する秘密鍵のペアは，今日の一般的なセキュリティモデルである公開鍵暗号（PKE：Public Key Encryption）の中核を成すものです．しかし，それだけではありません．2004年，2人の暗号技術者が，従来のPKEを一般化した形式で，ユーザのポリシーや属性に基づいてデータを共有する方法を発表しました．属性ベース暗号（ABE：Attribute-Based Encryption）と呼ばれるこのアプローチは，専門家がその可能性の探求を続けている段階であるにもかかわらず，商用利用が始まっています．業界のリーダーたちは新たな用途を見出し，暗号技術者は最適化された，より安全な暗号化構造を構築しています．

従来のデータセキュリティに加えて，ABEは継続的な研究成果の下，新たなデータセキュリティの手法として浮上しています．研究成果には，ABEの効率の良い実装に関する論文と，量子計算機に対して安全と思われるABEに関する論文という，NTTが関係する2つの論文が含まれます．暗号理論に裏打ちされ，ABEの魅力的なアプリケーションの数も増えてきています．

歴史と定義

Amit Sahai博士とBrent Waters博士は，暗号研究に関する国際会議「Crypto 2005」において，論文の一部として，ABEを初めて発表しました．SahaiとWatersは，IDベース暗号（IBE：Identity-Based Encryption）と呼ばれる以前の方式に基づき，アイデンティティを記述的な属性の集合ととらえることを提案しました．この新鮮な発想が，新たな可能性を生み出したのです．

従来の暗号は，特定の者をターゲットにして，「全」か「無」かのアクセスを提供するものでした．それに対して，ABEはより詳細なアクセス制御を組み込み，ユーザのポリシーや属性に基づいて暗号化されたデータ（暗号文）を共有することができます．ユーザが属性「X」の秘密鍵を要求した場合，暗号機関では，このユーザが本当に属性「X」を持つか，持つ資格があることを検証します．この検証を行うのは，従来の認証システムです．データを復号化する際には，ユーザの属性が暗号文に数学的に組み込まれたポリシー（条件式）に合致しているか，「暗号処理の内側」で行われ，暗号文の復号は，ユーザ鍵の属性が条件式と一致する場合にのみ行われます．

SahaiとWatersは，共著の論文の中で，大学の学科長が採用委員会メン

バ向けの文書を暗号化したいという仮想のケースを用いて，ABEの説明を行いました．この場合，ABEは，「採用委員会」「教員」「学問の専門性」といった属性から構成されるアイデンティティを暗号化することになり，すべての属性を含むアイデンティティを持つユーザであれば，文書を復号化することができます．

この論文によって，より柔軟で，きめ細かな暗号化モデルという考え方が根付いたのです．この論文は，2020年までに何千回も引用されるようになり，同年，国際暗号学会（IACR）のTest of Time Awardも受賞しています．2019年にNTT Research, Inc.に入社したWatersは，2022年，岡本龍明フェローの後任として，NTT Research, Inc. Cryptography and Information Security Laboratories（CIS研）のDirectorに就任しました．

最近の論文

ときが経つとともに，さまざまな特性を持つABEの方式が研究されてきています．これらの多くの方式を1つの方式としてまとめることができるでしょうか．

これを成し遂げたのが，ルール大学ボーフムのDoreen Riepel博士とNTT ResearchのHoeteck Wee博士の共著の論文『FABEO：Fast Attribute-Based Encryption with Optimal Security』です（Riepelは，CIS研で研究インターンシップに参加しながら，本研究の一部を完成させました）．両博士は，汎用版のABEの可能性を示すと同時に，他の大多数のABEアルゴリズムよりも優れた性能を実現しました．FABEOの4つの特性を紹介します．

■表現力（Expressiveness）

選択したポリシーと属性で，条件を多様に表現できます．想像し得るあらゆるポリシーを実現するのが，ABEの黄金律であるモノトーンスパンプログラムと呼ばれる技術で，秘密を複数に分割し，再分配し，共有することができます．モノトーンスパンプログラムとは任意のブール式，例えば“（A OR B）AND（C AND（X OR Y））”のようなものです．以前の方式ではORのみ，ANDのみ，ORのANDのみ，などの使用の制限がありました．本特性は，4つの特性の中でもっとも重要な特性といえ，ABEがより実用的に利用できるようになっています．

■無制限なサイズ（No limits on size）

鍵や暗号文に付加するポリシーと属性のサイズの制限がありません．最初のABE方式では，Sahai，Watersの共著の論文の例を挙げると，「採用委員会」「教員」「専門性」という属性を含めることができますが，属性の数が3つなど一定の上限を超えると，安全性に欠けていました．この特性は，表現力に関係するもので，10，20，あるいは，それ以上の数の属性を持つことができます．

■大領域の属性（Large attribute universe）

好みの属性を使用することができます．最初の方式では特定の属性のみが使用可能でしたが，この特性によって，ランダムな文字列，名前，日付と時刻，その場でつくった単語など，何でも属性として使用することができます．より細かなアクセス制限が可能となります．

■適応的安全性（Adaptive security）

この特性は実質的に，私たちが証明できるもっとも強いセキュリティの概念を満たしています．適応的安全性では，仮想の攻撃者の能力を高めることで，結果として自分たちの方式がより強いということを証明できます．例えば，攻撃者は複数の秘密鍵を要求し，暗号文の内部に深く入り込み，秘密鍵について学んだことに応じて適応することができる能力を持つと想定します．これは現実世界の脅威のシナリオによく似ています．

これらの特性を実現することに加えて，RiepelとWeeは，FABEOシステムを非常に効率的に設計し，双線形ペアリング楕円曲線に正確に当てはめました．これまでの楕円曲線の構築においては，いくつかの操作の相対的な速さを考慮していないことが問題でした．楕円曲線は数学者の創造物です．暗号技術者は，楕円曲線という道具箱に何が入っているかはあまりコントロールできませんが，道具を選び，その使い方を決めることはできます．

最近の別の論文『Decentralized Multi-Authority ABE for DNFs from LWE』では，NTT Researchの Pratish Datta 博　士，Ilan

Komargodski博士，Brent Waters博士が量子計算機の脅威に言及しています．著者らの成果は，耐量子の計算難度が高いともっとも広く信じられている誤差を伴う学習（LWE：Learning With Errors）仮定から，分散型のマルチオーソリティMA-ABEを初めて構築したことです．また，本方式は，自動定理証明に有用なDNF（Disjunctive Normal Form）式で表されるアクセスポリシーをサポートしています．

暗号システムの安全性を証明するには，特定の数学的予想が必要です．今後の目標は，量子の世界で通用するシステムを構築することで，ノイズの下で線形方程式を解く問題であるLWEは，そのような予想の1つです．著者らはLWEから最初のMA-ABEを構築する過程で別のものを達成しました．それが，以前の方式で使用していた非常に非効率な変換を必要としない，最初の暗号文ポリシー（CP：Ciphertext Policy）シングルオーソリティABEです（注：ABEは，条件がデータに埋め込まれたCPと，条件が鍵に埋め込まれたキーポリシーのいずれかの形態をとります）．

著者らが，マルチオーソリティではなくシングルオーソリティのABEを最初に構築したのは，それがマルチオーソリティ化のために必要だったからです．LWEから構築したこれまでのCP ABE方式では，普遍的な回路ベースの変換を使用していましたが，これは，MA-ABEの設定で使用するには非効率的で非実用的なものでした．シングルオーソリティCP ABEの構築では，複数の秘密鍵を集める共謀を防ぎ，ポリシーを少数のパラメータで符号化しなければならない，という2つの課題をクリアする必要があり，しかも，現状の変換技術を使用せずにそれを実現する必要がありました．

これらの課題を克服するため，2つの技術を改良しました．1つは再構成係数が小さく線形独立性が保証された新しい線形非単調秘密分散方式（LSSS）の設計です．LSSSは秘密パラメータをエンコードするためにさまざまな暗号構造で採用されている線形代数手法です．もう1つは，LSSSの性質を利用し既存の構成と証明方法をLWEに適応させることです．LWE仮定を用いることで実用的な暗号化方式を構築し，2つの課題の克服に成功しました．

シングルオーソリティを経てマルチオーソリティのCP ABEに移行するには，さらに2つの課題を克服する必要がありました．秘密鍵の共謀を回避し続けるために，鍵どうしを結びつける公開ランダム性を用いて実現しました．そして，1つのオーソリティで鍵を生成するための条件として，セットアップと鍵生成アルゴリズムにおいてモジュール性を実現する必要がありました．そうでなければ，マルチオーソリティとはいえません．シングルオーソリティの設計時にこの2つの課題を特に意識して設計したため，自然にマルチオーソリティに拡張することができました．

なおマルチオーソリティは，以下に述べる方式を考えるうえで自然な方法と考えられています．例えば，職業と国籍（例，「医学博士」と「アメリカ人」）に基づいて暗号化を行いたい場合，性質の異なる2つの属性を持つことになります．病院や大学の誰かが，あなたが医師であるかどうかを確認することはできますが，国籍を確認するには，政府当局の助けが必要です．これらの機関を組み合わせ，すべてをチェックする（さらに，機密データを共有する）ことができる集権センタを配置することは非現実的です．そのためマルチオーソリティの仕組みが必要になります．

勢いを増すABE

前述の両論文は，ABEの進化を支えています．FABEO論文は，最適な機能を網羅したABEの構築が可能であり，より実用可能性が高まりました．LWEからMA-ABEを構築した論文は，耐量子ABEの大規模な実用化に一歩近づいた技術です．実際，NTT Researchの技術推進チームは，この論文の耐量子ABEの初期実装をすでに終え問題のない動作を確認していますが，今後はより高速で効率的な実装に取り組んでいきます．

NTT Researchは，基礎研究を重視する一方で，開発した研究コンセプトの製品化を支援する「技術推進チーム」を設置しています．本チームは，ABEがヘルスケア，医療，金融，教育，政府などの分野におけるセキュリティやプライバシのニーズに対応できると考え，NTTの事業会社と協議を重ね

てきました．2021年，NTTは，シドニー工科大学（UTS）と，UTSの内部システムをよりセキュアにすることを目的としたABEの概念実証プラットフォームの構築を含む契約を締結したと発表しました．また，ABE暗号方式は，ETSI（European Telecommunications Standards Institute）による標準化の支援を得ています．

2022年，NTT Researchは，2週間にわたるABEハッカソンを開催し，世界中から5つのNTT関連チームが集まりました．優勝したベルギーのNTTチームは，ロゴ，顔，ナンバープレートなど人物を特定できる情報を含む画像のパーツやGPS情報を含むメタデータにABEを適用するという新たな手法のデモンストレーションを行いました．同チームは，スキャンした医療文書やテストの回答など，写真画像のみならず個人情報保護の対象となる他の画像にも同様にABEを適用できる可能性があることを示しました．

他のデモは，残りの4カ国のNTTチームが作成したもので，以下のユースケースが紹介されました．

- 金融（インド）：銀行システムを，単一の要素に基づいてアクセスを許可または拒否する役割ベースのアクセス制御（RBAC）システムから，ABEを使用した，より繊細な制御へと移行
- 公共交通機関（イタリア）：ローマの新交通サービスにABEを導入し，チケット購入と物理的アクセス制御を支援
- 通信（日本）：ABEを使用した，プライバシが保護された通話ソリューションの導入により，適切な場所にいる，適切な役職のスタッフや，緊急通話の必要があるスタッフが，従業員の個人携帯番号に電話をかけることができる
- 個人データ（ルーマニア）：ABEを使用して，自動車の電子センサ上でセキュアなIoT（Internet of Things）プロトコルを実現し，自動車のオーナーがデータの収益化オプションを制御できる

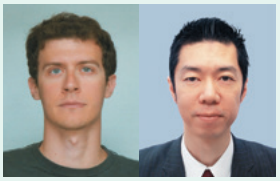
同ハッカソンでは，アクセスが容易で，HTTPエンドポイントの役割を果たし，鍵を使用して暗号化，復号化を行い，ソリューションをすばやく試作することができるWebツール「ABE Resolver」が利用できることも確認されました．

今後の展開

Watersによると，ABEは，長年にわたりさまざまな結果をもたらしてきました．まず，アプリケーション単体としてのABEがあります．さらに，他の暗号システムを構築するためのコンポーネントとしてのABEがあり，研究コミュニティにも大きな影響を与えてきています．第三に，ABEの「精神と概念」があり，関数暗号など他の暗号技術に影響を与えています．

ABEそのものについては，ユースケースは急増しています．開発ツールへのアクセスが容易なことも，このトレンドを後押ししています．今後，さまざまな状況で商品化が行われるでしょう．ほとんどの用途に最適で，非常に高速な，ABEのベースバージョンが登場すると思われます．また属性を秘匿可能なABE，耐量子セキュリティ，そして付加機能を持つものなど複数のABEが登場すると思われます．

ポスト量子環境の到来には何年もかかるかもしれませんが，この分野における私たちの活動は，私たちがABEの長期的な展望をどう見ているかを示す良い指標となると考えています．この革新的な暗号化手法の背景には20年近い歴史があり，私たちは，さらに長く耐えられるソリューションを準備していきます．



（左から）Yannis Rouselakis/
後藤　隆

NTT Research, Inc.は，暗号技術のほか，Quantum Computing，Bio Digital Twinなどの基礎研究にフォーカスしたアメリカ・カリフォルニアにある海外研究所です．NTT Research, Inc.の現実をアップグレードする，Upgrade Realityを実現する研究活動にぜひご期待ください．

◆問い合わせ先
NTT Research, Inc.
Technology Promotion Team
E-mail　tech_promotion @ ntt-research.com