クラウドの普及を支える新たな暗号技術への期待

データを暗号化したまま演算処理を行う完全準同型暗号の研究が進んでいる。金融業界でも新たな暗号技術の活用により、暗号化データのまま解析処理等をクラウド上で行い、データの機密性を確保した業務委託ができるようになると期待される。

金融機関におけるクラウドサービスの利用は、年々増加している[1]ものの、機密性が高いデータを含む処理は依然自社で行う傾向にある。クラウド上でデータを扱う場合は、情報漏洩のリスクを考慮しなければならず、委託先のセキュリティ管理の状況を把握する責務も生じる。複数の事業者へ委託する際は、管理負担も大きい。このため、現状クラウドの利用はデータの保管や機密性の高いデータを扱わない業務が中心になり、金融機関はクラウド本来の価値をビジネスに活かしきれていない。

この問題を解決する1つの鍵が、暗号である。従来の暗号技術では、機密性の高いデータを暗号化してクラウド上へ保管することはできるが、演算処理を行う際にはデータを復号化しなければならなかった。仮に、すべてのデータの計算を暗号化したまま行うことができれば、クラウド利用時の懸念は大きく低下する。それを可能にする暗号技術として、完全準同型暗号がある。

暗号化したまま演算ができる完全準同型暗号

完全準同型暗号[2]は、暗号化されたデータ同士の加算と乗算ができる暗号である。暗号化データを復号化せず演算処理できるため、金融機関は暗号化したデータをそのまま委託先へ渡し、統計解析などの処理を依頼できるようになる。

データを暗号化したまま演算を行う概念は1970年代後半に提唱されていたが、加算、乗算の一方のみを計算する準同型暗号しか実現できず、完全準同型暗号は30年近く研究が続いていた。2009年、Craig Gentryがブートストラップ[3]という手法を用いて、加算、乗算の両方を回数制限なく演算する方法を提案すると、改良や高速化が進んだ。2013年には、完全準同型暗号を実装したライブラリ[4]がオープンソース化されている。

最も完全準同型暗号の研究が進んでいるのが医療分野である。今年3月に発表されたCREST[5]のプロジェクト[6]では、ゲノム解析を想定した数万件の暗号化データに対して、標準的な統計計算や評価を数秒～10分程度で実現しており、実用化研究のフェーズへと進んでいる。

完全準同型暗号は、暗号処理の計算量が多く処理速度が実用的でないことが一番の課題であったが、この部分を改良したものに、Somewhat準同型暗号[7]がある。乗算回数に制約を設けることで、処理速度の改善に成功している。既にITベンダーやクラウド事業者がサービスを提供しており、セキュリティ要件の高いブロックチェーンへの適用も、MicrosoftやMITのEnigma[8]等で研究されている。ただし、演算回数の制限から汎用的には使えず、適用できる機能は限られたものとなる。

高機能暗号の金融業界への適用

完全準同型暗号は、クラウドサービスの利用が進む金融業界でも活用が可能と考えられる。金融業務へ適用する場合、アルゴリズムの強度や機密性の保持に関する要件が医療分野とは異なるため、相応しい暗号のパラメータ設定や安全性の評価が必要になる。

例えば、セキュリティの強度に関する検証がある。医療分野の研究では、ゲノムの個人情報は3世代、100年にわたって解読されない要件が必須であるが、金融で同等のレベルは必要ない。データの処理結果を翌日取得し数ヶ月データ保管ができれば、制度要件は満たすことも多く、セキュリティの強度を変えることで処理時間を短縮できる

NOTE

1) FISCのH27年度調査では、約半数の金融機関がクラウドを利用、あるいは利用を検討中。プライベートクラウドは13.0%、パブリッククラウドは17.4%の金融機関が利用している。
2) FHE（Fully Homomorphic Encryption）。任意の演算は、乗算の（AND）と加法の排他的論理和（XOR）の組み合わせで構成され、両方ができる準同型暗号は完全準同型暗号と言われる。
3) 暗号化状態を維持したまま、暗号化データに含まれるノイズを削減する処理。膨大な計算量を要する。ノイズは準同型演算を行う度に増加するため、復号化が不正確になる課題があった。
4) HElib（Homomorphic Encryption library）。完全準同型暗号をC++で実装したライブラリ。
5) CREST（Core Research for Evolutional Science and Technology）。JST（科学技術振興機構）の戦略的創造研究推進事業。
6) 「自己情報コントロール機構を持つプライバシー保護データ収集・解析基盤の構築と個別化医療・ゲノム疫学への展開」プロジェクト。
7) SHE（Somewhat Homomorphic Encryption）。制限付き準同型暗号。
8) Enigmaを使った初の投資プラットフォームCatalystは、今年7月にα版がリリースされている。https://www.enigma.co/
9) データが破壊や改竄されていない状態。
10) 例えば、PFM（Personal Financial Management）個人向け資産管理サービスでは、複数の金融機関から口座残高や取引履歴データなどを収集し、ネット上で一元的に把握できる資産管理機能を顧客へ提供している。

可能性もある。また、クラウドのように外部へ暗号化データを保管して処理を委託するケースでは、データが漏洩せず、改竄されないという安全性要件が必須である。完全準同型暗号は、公開鍵型の暗号方式を用いることで機密性は確保できるが、不正なデータにより行われた演算処理と正しい処理結果とを識別できず、データの完全性[9]を確保することが難しいという課題がある。

完全準同型暗号は、あくまでも演算処理を行う暗号技術であるため、実際の業務へ適用する場合は他の機能も必要になる。金融取引のデータは、監査の観点からも一定期間DBに蓄積して管理する業務が多く、クラウド上で処理を行うには、ユーザー認証や暗号化データの検索機能も実装しなければならない。基本的な暗号機能に加えて、高度な機能を有する高機能暗号には、アクセス制御が可能な属性ベース暗号、暗号化データのキーワード検索ができる検索可能暗号などもある。金融系業務へ適用する際には、これらを組み合わせて活用することになる。

属性ベース暗号は、復号化のポリシー（条件）に関する情報を、暗号化データか秘密鍵に組み込むことで、復号化できるユーザーやデータを制御する暗号である。例えば、「企画部の課長のみ参照可」というポリシーを暗号化データに設定すると、該当するメンバーのみがデータを復号化できる。「株式または債券、ただし外国株式は除く」のように、データの属性を指定したポリシーを、秘密鍵に組み込むこともできる。属性ベース暗号は、暗号化鍵と復号鍵が1：1に限られず、復号化のポリシーをANDとORの組み合わせで指定できるため自由度が高い。

完全準同型暗号は、従来の暗号と比較すると暗号化データのサイズが大きく、リアルタイム性が強く求められる業務には適していない。導入する場合は、システムやデータの重要性を整理し、特性に応じて対象の業務を選定することも重要である。安全対策基準に則って、ビジネスモデルやサービスに相応しいセキュリティレベルを熟慮し、対象を絞り込んで適用することになる。

事業環境の変化と暗号技術への期待

このように、完全準同型暗号を金融業界へ適用するには、更なる研究が必要である。しかし、金融業界のクラウドを取り巻く環境は変化しており、より安全で利便性の高いサービスのために、高機能暗号を応用し得る範囲は拡がっている。FinTechの進展により、ここ1、2年で金融機関がノンバンク企業と組んで金融サービスを展開するビジネスモデルも増えてきた。これまで金融取引や資産に関するデータは、金融機関と顧客間のみで取り扱われていたが、両者の間にFinTech企業が介在し、金融機関から入手した口座・取引関連のデータを集約して顧客へ提供するサービスも出てきた[10]。FinTechのサービスはクラウドを利用したものが多く、今後もオープンイノベーションの促進により、これまで以上に多様な事業者が金融事業へ参入し、金融機関がデータを外部へ連携する機会は増えていくと予想されている。

我々は、高機能暗号は金融業界のシステムインフラを改革していく重要な技術の1つであると認識している。この進展に注力していきたい。

Writer's Profile

北原 真由美 Mayumi Kitahara
証券ホールセール事業推進部
システムコンサルタント
専門は新サービス企画、海外動向調査
focus@nri.co.jp