FinTechのセキュリティ強化に貢献するマルチパーティ計算技術

岡村 利彦　寺西 勇

要 旨

FinTechの発展に向けてサイバー攻撃に対するセキュリティ技術の強化が不可欠です。情報漏えいはそのなかでも大きな脅威であり、データを暗号化したままで処理することを可能にする秘密計算は強固な情報漏えい対策技術として期待されています。本稿では、秘密計算のなかでもデータを複数のマシンに秘密分散したまま処理するマルチパーティ計算技術について、NECの高速方式及び認証情報の保護を中心としたFinTechへの想定適用例を紹介します。

KeyWords

セキュリティ／情報漏えい防止／認証／秘密計算／マルチパーティ計算

1. はじめに

FinTechによるさまざまな金融サービスの実現に向けてサイバー攻撃に対するセキュリティの強化が不可欠になっています。FinTechで特徴的なスマートフォンの利用は、利便性の高いサービスを実現する一方でサイバー攻撃の機会拡大にもつながります。サイバー攻撃の脅威のなかでも情報漏えいへの不安は大きく、ユーザーへのFinTechのイメージ調査でも、情報漏えいに対する不安が最上位に挙げられているとの結果が報告されています(2016年Macromill[1])。

認証情報の漏えいはなりすましを通じて不正な決済や大量の情報漏えいにつながるため、特に強固な対策が必要になります。パスワードレスの認証方式の標準であるFIDO（Fast IDentity Online）では、ユーザーの生体情報と公開鍵暗号を使った認証を安全に行うための枠組みを規定していますが、ユーザーの生体特徴量と秘密鍵をユーザー端末に「安全に」保管することが前提とされています。しかし、端末の紛失やマルウェアによって端末が攻撃者によりクラックされた場合は、これらの情報の秘密を担保できなくなります。生体特徴量は個人情報でもあり、その漏えい対策は一層重要となります。

本稿ではこうした強力な攻撃に対しても強固な情報漏えい防止を実現する暗号技術である「秘密計算」、そのなかでも現在セキュリティ研究所で注力している「マルチパーティ計算」について説明し、NECの高速方式及びFinTechにおける想定適用例を中心に紹介します。

2. 秘密計算

暗号化は、データが流出した際にも情報漏えいを防げる有効な手段です。しかし、データを処理する際に元データに一旦戻す必要があり、例えば管理者権限を悪用すると攻撃者は元データを復元して入手できる可能性がありました。「秘密計算」は暗号化したデータを元のデータに戻さずそのまま処理することで、管理権限が悪用されても情報漏えいを防ぐことが可能な技術です（**図1**）。

秘密計算は、「検索可能暗号」や「準同型暗号」など特定の処理に対応した特殊な暗号化と、複数のサーバで秘密分散したまま処理する「マルチパーティ計算」のアプローチに、大きく分類することができます（**図2**）。前者は現在のところ、処理に応じて異なる暗号化方式を設計する必要があります。これに対して、マルチパーティ計算は排他的論理和と論理積など、基本演算に対応するアルゴリズムを組

み合わせて原理的には任意の処理に対応できる特徴があります。本項ではマルチパーティ計算について紹介します。

2.1 マルチパーティ計算

マルチパーティ計算の処理イメージを図3に示します。最初にデータaの持ち主がaを分散値x,y,…に秘密分散し、x,y,…をそれぞれ管理者が異なるマシンに送信します。そしてaが秘密分散されたままの状態で互いに通信を行いつつ計算を進め、最後に各マシンの計算結果である出力の分散値u,v,…を集めて「復元処理」を行うことで、計算結果のF(a)が得られます。

秘密分散は、分散値x,y,…を集めた個数が一定数以下であればaの情報はいっさい漏れないことを保証します。マルチパーティ計算では更に計算中もこの性質が保たたれるため、マシンのハードディスク上はもちろん、メモリ上にも秘密データaはいっさい現れません。このため、マルチパーティ計算は一定数以下のマシンが攻撃者の支配下に置かれたとしても安全性を担保できます。特に攻撃者が組織内である内部犯行の場合は、暗号などの既存技術では対策が難しく、単独の管理者による漏えいを原理的に防止できるマルチパーティ計算は有効です。

マルチパーティ計算は、前述のように任意の計算に原理的には対応可能ですが、一般にマシン間の通信量と計算量ともに非常に大きくなり、永らく理論上の技術でしかありませんでした。しかしここ数年、アルゴリズム改良とプロセッサやネットワークの高速化によって、マルチパーティ計算はここ数年で急速に進展してきています。

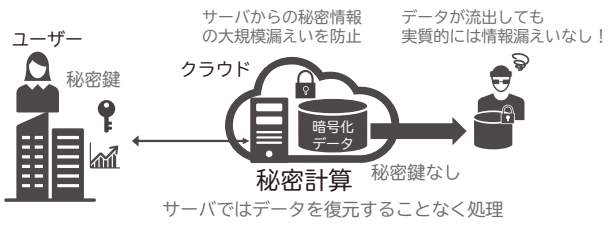


図1　秘密計算による情報漏えい防止

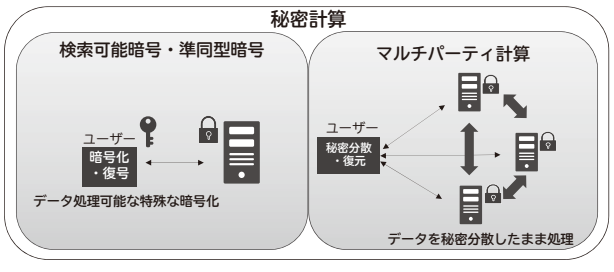


図2　秘密計算の分類

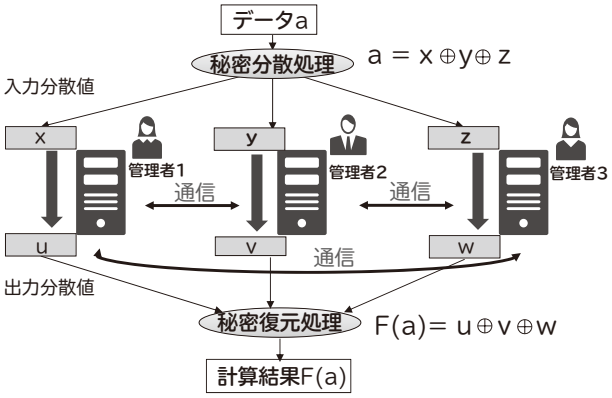


図3　マルチパーティ計算のイメージ図

2.2 NECの高速マルチパーティ計算

NECは、マシン3台の設定による高速なマルチパーティ計算方式の開発に成功しました。マシン3台のうち1台が攻撃者の支配下に置かれても、情報漏えいを防止することができます。

マルチパーティ計算は前述のように、データ処理を排他的論理和と論理積の論理式で表現して各論理ゲートを順に計算していきますが、NECはボトルネックとなる論理積ゲートの計算処理を改良することで、大幅な高速化を達成しました[2)]。この高速化は、秘密分散の方法を工夫することにより通信なしにマシン内で計算可能な処理を最大化し、かつその計算処理の最適化を図ることによって実現することができました。

マルチパーティ計算の性能ベンチマークとなる、標準暗号AESに適用した場合のスループットを表に示します。AESのマルチパーティ計算は、秘密鍵を秘密分散して3台のサーバに設定し、秘密鍵とデータを秘密分散したまま暗号化処理を実行します。表で示したC社方式は、従来の最高性能の方式でした(2016年12月時点)。NEC方式は、2013年のC社方式に対して400倍、2016年の比較でも14倍のスループットを達成しました。

前述のNEC方式AESマルチパーティ計算の実用性検証のために、ディレクトリサービスなどで広く利用されているKerberos認証サーバ(AES利用)に適用して評価

表　マルチパーティ計算処理性能

(AESブロック数/秒)

年	方式	スループット
2013	C社方式（1）	3,450
2016	C社方式（2）	25,000
2016	C社方式（3）	90,000
2016	NEC方式	1,324,117

しました。その結果、秒間35,000件の認証処理を実現し[3]、Kerberos認証の大企業での利用の目安となる、秒間1万件の処理を越える性能を達成しました。

一方、マルチパーティ計算自体の安全性の課題として、マシンが攻撃者の支配下に置かれると計算が不正に操作されるという問題があります。例えば攻撃者支配下のマシンでは、データ自体が分からなくても計算の途中で故意にビットを反転したり、ある値を加算したりすることで計算結果を操作することが可能になります。このようなマシンの不正を他のマシンが迅速に検知できるようにすることは、実用化に向けて重要となります。NECは、マルチパーティ計算における不正サーバ検知に関しても安全かつ高速な方式を開発しています[2]。

またNECの高速化のアプローチは、排他的論理和と論理積だけではなく、整数や小数の算術演算による秘密分散に基づいた、算術演算の和と積に対するマルチパーティ計算にも適用することが可能です。生体認証やデータ分析などに対しては、算術演算に基づくマルチパーティ計算を適用することで高速化が可能です。現在アルゴリズムの詳細設計と評価を進めています。

3. マルチパーティ計算のFinTechへの想定適用例

3.1 認証情報の保護

ユーザー認証や機器認証は、モバイル決済をはじめとしてFinTechの多くのサービスの安全性の起点となります。マルチパーティ計算は認証情報の強固な保護を実現します。

本項では認証情報をマルチパーティ計算で守る適用例を2つ紹介します。第1の適用例はFIDOの認証情報の保護です。FIDOでは生体情報を使ってユーザーを認証し、この認証をパスすれば、ユーザー端末は端末に設定された秘密鍵を使ってデジタル署名を生成して、認証サーバが機器認証します。**図4**はこの際に用いる生体情報の特徴量と秘密鍵をマルチパーティ計算で守る構成例を示しています。この構成例では、端末以外に外部に秘密計算サーバを設置し、生体情報の特徴量と秘密鍵のそれぞれを、端末と秘密計算サーバで秘密分散します。認証の際には、端末は秘密計算サーバと通信してマルチパーティ計算を行うことで、特徴量と秘密鍵を復元することなくユーザー認証のための生体認証の照合処理と、機器認証の署名生成を行います。

図4の機器認証でRSA署名の場合、アルゴリズムの性質を利用して次のように簡易なマルチパーティ計算が可能です(**図5**)。RSAの秘密鍵dに対して、秘密分散した2つの分散値$d[1], d[2]$は$d = d[1] - d[2]$を満たすデータです。端末は認証サーバからのRSA認証のチャレンジmに対して、mに時刻情報などを付加したデータMへの署名文σを

$$\sigma = H(M)^d \bmod N = H(M)^{d[1]} / H(M)^{d[2]} \bmod N$$

として、端末とサーバで協力して生成します。ここでN

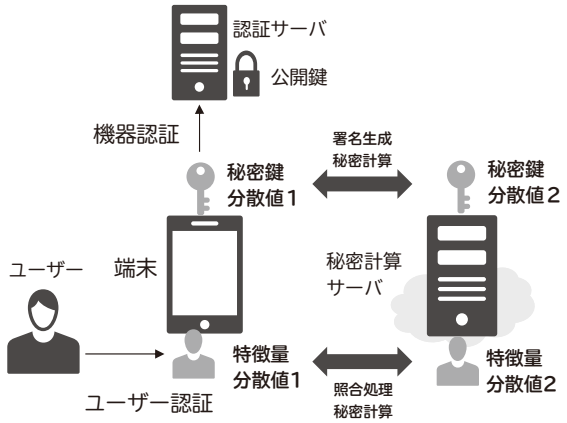


図4　FIDO認証情報のマルチパーティ計算による保護

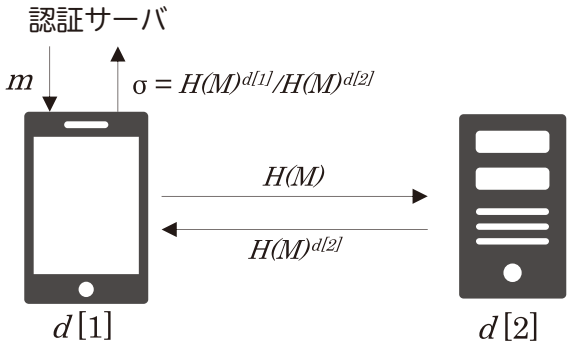


図5　FIDOにおけるRSA署名のマルチパーティ計算

はRSAの公開鍵、Hは署名生成で用いるハッシュ関数です。マルチパーティ計算によって、このように秘密鍵dを復元することなく署名文σを生成することが可能になります。

第2の適用例はクラウド上のユーザー認証基盤における認証情報の保護です。ここで想定する認証基盤は、POSなどさまざまな端末やサービスに対してユーザー認証機能を提供するものであり、大量に認証情報が登録されるためにそれを強固に保護する必要があります。こうした大量の認証情報を複数のサーバに秘密分散し、それらのサーバ間で認証処理をマルチパーティ計算することで、サーバ1台が攻撃者に支配されても実質的な情報漏えいを防ぐことが可能になります。**図6**は生体認証の場合の例を示しています。認証時には端末は照合する特徴量を秘密分散し、端末と各サーバ間を別途暗号化してこの分散値を送信し、各サーバは登録している特徴量の分散値を用いてマルチパーティ計算による照合処理を実行します。この利用形態では大量の認証をクラウド側で処理することを想定しているので、利用するマルチパーティ計算には高いスループットが求められます。第2章2節でNECの高速マルチパーティ計算のKerberos認証においての実用性を示しましたが、生体認証の照合処理でも実用的な性能が出せるよう開発を進めています。

3.2 顧客情報の保護

購買履歴、SNSなどインターネット上の情報の収集、APIによる銀行の口座情報の提供など、FinTechにおいては従来よりも膨大な顧客情報を活用して高度な融資や資産管理アドバイスのサービスが始まっています。その一方で、収集した顧客情報の漏えい対策の強化も必須となります。データ処理を可能にしながら管理者からの情報漏えいも防ぐマルチパーティ計算は、FinTechにおける顧客情報の強固な保護を実現します。

FinTech事業者が保有する顧客情報はその競争力の源泉となりますが、その一方で、事業者間で保有情報を合わせて分析することによって、例えば顧客の信用度の精度向上を通じてサービスの一層の高度化を図ることができます。この際、データをお互いに開示せずに必要な分析結果だけが提供できることが望まれます。ここでマルチパーティ計算を適用することによって、お互いだけでなく第三者にもデータを開示せずにデータを結合して分析を行うことが可能になります。このようにマルチパーティ計算は、FinTechにおいて事業者間のデータ活用を促進するセキュリティ技術としても活用することができます。

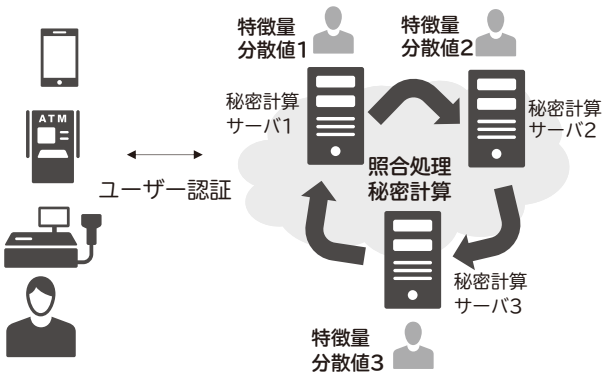


図6　ユーザー認証基盤におけるマルチパーティ計算適用例

4. おわりに

本稿では秘密計算、特に複数のサーバにデータを秘密分散して秘匿したまま処理するマルチパーティ計算について紹介し、NECの高速方式と認証情報の漏えい防止を中心に、FinTechへの想定適用例を紹介しました。FinTechにおける情報漏えいのリスクを解消するセキュリティ基盤の実現を目指して、今後もマルチパーティ計算の一層の性能改善の研究と、先行適用事例の開拓を推進していく所存です。

*FIDOは、FIDO Allianceの商標です。
*その他記述された社名、製品名などは、該当する各社の商標または登録商標です。

参考文献

1) 今話題のFinTech（フィンテック）とは何か？（Macromill）
http://www.macromill.com/honote/20160405/report.html
2) T.Araki, J.Furukawa, Y.Lindell, A.Nof, and K.Ohara. High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority. ACM CCS, 2016.
3) J.Furukawa, Y.Lindell, A.Nof, and O.Weinstein, High-Throughput Secure Three-Party Computation for Malicious Adversaries and an Honest Majority, to appear in Eurocrypt2017

執筆者プロフィール

岡村 利彦
セキュリティ研究所主任研究員

寺西 勇
サイバーセキュリティ戦略本部

関連URL

NEC、機密情報の漏えいを強固に防止する秘密計算の高速化手法を開発
～大規模な認証システムで利用できる性能を実現～
http://jpn.nec.com/press/201612/20161215_02.html

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報(日本語)　　NEC Technical Journal(英語)

Vol.69 No.2　デジタルトランスフォーメーションを加速するFinTech特集

デジタルトランスフォーメーションを加速するFinTech特集によせて
NECが目指すFinTechの全体像

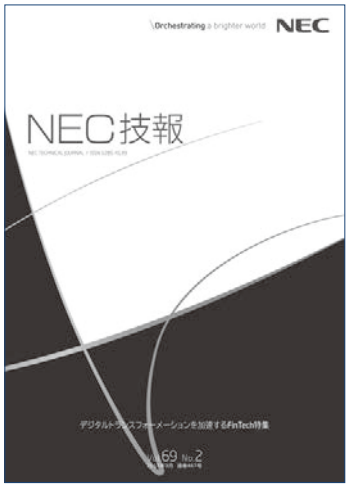
◇ 特集論文

FinTech時代の新しい金融と技術の関係
AIがもたらす金融サービスの変革
ブロックチェーンによる企業間連携の実用化に向けた取り組み
ロボットとAIの組み合わせによる顧客コミュニケーションの高度化
ウェアラブルデバイスを用いた安全・安心・便利な見守りサービス
生体認証によるモバイルサービスのセキュリティと利便性の両立
新たなサービスのスピーディな提供を可能にするモバイルアプリ高速開発
サイバーセキュリティ対策推進による金融サービスの安全性向上
FinTechのセキュリティ強化に貢献するマルチパーティ計算技術

◇ NEC Information

C&Cユーザーフォーラム&iEXPO2016　Orchestrating a brighter world
基調講演
展示会報告

NEWS
2016年度C&C賞表彰式開催



Vol.69 No.2
（2017年3月）

特集TOP