NEWS RELEASE
NTT
日本電信電話株式会社

2005年10月25日

暗号化したままで自由な演算が可能な秘密計算アルゴリズムで世界最高速を達成

～世界初の実装により、安全なアンケート集計や解析困難なプログラムの実用化に大きく前進～

日本電信電話株式会社(以下NTT、本社：東京都千代田区、代表取締役社長：和田紀夫）は、世界最高速の秘密計算アルゴリズムを開発、これをNTTの持つ高度な暗号実装技術によって実装・評価し、安全性が保証された秘密計算技術において実用水準の性能が見込めることを明らかにしました。これは、暗号化したまま自由な演算が可能な秘密計算アルゴリズムに対する、商用化に向けた世界初の実装となります。

入力データや演算ロジックを暗号化したままで任意の計算を可能にする秘密計算技術は、アルゴリズムとしては10年以上前から研究されていましたが、計算量の大きさから机上の理論にとどまっていました。このたびNTTでは、計算コスト・通信コストの両方で世界最小となる秘密計算アルゴリズムを開発、これをNTTが培ってきた高度な暗号実装技術によって世界で初めて実装し、基本処理に要する時間を測定しました。この結果、VPNなど相互認証を必要とする暗号通信を、耐タンパハードウェア(※1)なしにソフトウェアだけで行うことや、アンケートや医療情報処理などにおいて暗号化された機微情報を扱う際、復号すること無く集計するシステムの構築が実現可能なことを明らかにし、実用化に大きく前進しました。

今後、企業や公共機関、教育現場などにおける、プログラムの不正解析防止、知的財産の侵害防止、情報漏えい防止、プライバシー保護などの多様な分野への応用が期待できます。

なお、本技術の実装評価結果は、１０月２６日から愛媛県松山市で開催される情報処理学会（コンピュータ・セキュリティ・シンポジウム）で発表する予定です。

＜秘密計算技術の背景と到達点＞

情報をやりとりする場合、ある特定の情報だけを開示し、そのほかの情報は伏せておきたい場合があります。例えば、業務上機密性が要求される計算をアウトソーシングする場合など、データはもちろんのこと、どのような計算を行うかということまで機密性が要求されることもあります。また、個人情報保護

の観点から、各種のアンケートなどにおいて、個人を特定できない集計データは明らかにする一方、個々のアンケート結果は漏えいさせないような取り扱いが必要になる場合もあります。

秘密計算技術を用いると、情報を暗号化したまま自由な演算が可能になるため、こうした計算処理や集計処理の安全性を飛躍的に高めることができます。この技術についての理論的研究は10年以上前から世界的に行われていましたが、要求される計算量の大きさから、現在に至るまで実用化が可能とは考えられていませんでした。しかし、さきにIETF標準として採用されたCamelliaをはじめ、世界トップレベルの暗号研究を行ってきたNTT情報流通プラットフォーム研究所ではこのたび、世界最小の計算コスト・通信コストで動作する秘密計算の基本アルゴリズムを開発し、これを高度な暗号実装技術によって実装、世界で初めて処理性能を実測しました。これにより、従来に比べて飛躍的に安全性の高い、新たなセキュリティシステムの実用化に道が開かれました。

＜本技術の適用分野＞

本技術の適用分野としては、現在、以下のようなものを想定しています。

(1) ソフトウェア認証トークン

VPNなどの暗号通信において相互認証を行う際、安全性を高める方法として、従来はICカードやUSBキー、ワンタイムパスワード生成器のようなハードウェアの認証トークン(※2)が用いられてきました。これらのハードウェアトークンは、認証に必要な演算やデータを、耐タンパ性を備えたハードウェア内部で処理することで、トークンの解析を事実上不可能にして、高い安全性を確保しています。しかしこの方法では安全性は高いものの、ハードウェアの購入や配布にコストや時間がかかるという問題があります。

秘密計算技術を用いると、ソフトウェアのみで、事実上解析不可能な認証トークンを実現することができます。このソフトウェア認証トークンでは、認証プログラムが暗号化された状態で実行されるため、認証に用いるデータや演算が不正に知られることはありません。一方、ソフトウェアのみで構成されているため、ネットワークを介した配布が可能になり、利便性の向上やコストの削減が期待できます。

(2) プライバシー保護アンケート(図1)

従来、アンケート情報を外部に依頼して集計を行う必要がある場合、個人を特定できないようにデータを加工してから外部依頼を行うということが一般に行われていました。しかし、この方法では、データの加工に手間がかかるうえ、そうした加工が行われたために集計者の希望する統計処理が行えないケースが生じてしまうこともありました。また最近では個人情報保護法の施行により、アンケートなどの取り扱いにも、さらなる慎重さが求められるようになっています。

秘密計算技術を用いると、アンケート結果を暗号化したままで任意の演算が

行えるため、個々のアンケート情報を漏らすことなく、集計者に統計処理を行わせて、その結果だけを提示する、プライバシー保護アンケートが実現可能になります。

＜秘密計算の特徴＞

（1）暗号化されたデータを復号せずに、各種計算が可能（図2）
　入力データを暗号化したまま復号せずに任意の演算ができます。また、同様の手法により演算ロジックを暗号化したまま演算結果を求めることもできます。

（2）マルチパーティモデル
　マルチパーティプロトコル（※3）により、安全性が保証された秘密計算を実現できます。演算時は、複数の参加者の協力を必要とし、各参加者には分散された秘密鍵が与えられます。一定数以上の参加者が不正に結託しない限りは、入力データやロジックを解析できないことが、暗号学的に保証されています。この場合の「一定数」は、アプリケーションごとに任意に設定できます。

＜今後の展開＞
　NTTでは今後、秘密計算技術を適用したアプリケーションについて3年後の商用開発を目指します。また更に、本技術の改良を重ね、暗号化されたデータベースに対する検索・データマイニングなどの高度な処理や、電子透かしなどの知的財産保護アプリケーションへの適用を目指し、これを通じて安心・安全な情報化社会の実現に貢献していきたいと考えています。

＜用語解説＞

※1　耐タンパハードウェア
　不正な手段による機密データの読み取りを防ぐ能力を備えたハードウェア。

※2　認証トークン
　認証を行うために必要なデータやプログラム。成りすましなどの攻撃を防ぐために、一般にそれらデータやプログラムは保護されていることが望ましい。

※3　マルチパーティプロトコル（multiparty protocol）
　N人のうち任意のK人が協力した場合に限り、「入力データを暗号化したまま計算」や「暗号化された演算ロジックの実行」が可能になるプロトコル。一般にKが大きくなるにつれセキュリティも高まる。

・図1　アプリケーション例：プライバシー保護アンケート
・図2　秘密計算技術の概要

【本件に関するお問い合わせ】
ＮＴＴ情報流通基盤総合研究所
企画部　広報担当　遅塚（ちづか）、佐野、井田
TEL：0422-59-3663
E-mail：koho@mail.rdc.ntt.co.jp