情報通信研究機構

NICT 先端研究 ㊹

情報漏えいなし 分散ストレージ開発

未来ICT研究所・量子ICT先端開発センター研究マネージャー 藤原 幹生
01年より量子情報技術の研究に従事。12年前島賞、17年文部科学大臣表彰科学技術賞受賞。博士（理学）。

元NSA・CIA職員のスノーデン氏によるリーク情報でも喧伝されているが、インターネットで使用されている暗号の一部は既に解読されている可能性がある。また現在解読されていなくても将来計算機の能力が向上した時に解読される可能性を否定できない。

一方で我々自身のゲノムデータなど、世紀単位での秘匿を要するデータがインターネットを行き来し、保管されている。この情報漏えいの実は深刻な状況に対し、計算機の性能向上に安全性を脅かされず、将来にわたり安全性を保証できる情報伝送・保存システムが必要であった。

（分散ストレージ）の開発が急務となっている。

NICTでは長年解読不可能な通信を可能とする量子鍵配送（QKD）の開発を進めてきた。この技術はデータ伝送時の情報漏えいの脅威を排除できる技術であるが、データ保管に関しては別の技術

一方現代暗号ではデータを、データサイズが同じのいくつかのシェアと呼ばれる状態に分割・保存し、データを復元するにはある一定以上のシェアを集めて初めて復元できるという秘密分散法が知られていた。シェアが一定以上集まらない場合、情報漏えいを完全に防ぐことができる。

一方でシェアの伝送は安全に行うことを仮定していた。従って量子鍵配送と秘密分散の組み合わせはお互いの欠如した機能を補完しあうことができ、極めて合理的な融合である。

しかしながら、これらの技術の組み合わせでも未解決な重要な課題があった。それはデータを復元する際、その人が相応しい人であるかという、情報漏えいを防ぐ上で不可欠な本人認証の技術である。現在広く使用されている本人認証技術はパスワード認証、生体認証、デバイス認証などが挙げられる。これらの技術は残念ながら計算量的安全性しかなく、特に生体認証などはコピーされる恐れがある。

NICTではパスワードに、シェア同士の計算が可能である機能を応用し、パスワードとデータとの秘密計算の結果データが復元できるシステムを実現した。

この結果、本人認証も計算機能力に依存しない安全性を持つことが可能となる。我々は今後重要データのバックアップへの実利用に向けて働きかけを進めていく。

（火曜日に掲載）