

TYPE OF  
INDUSTRY

## 科学技術・大学

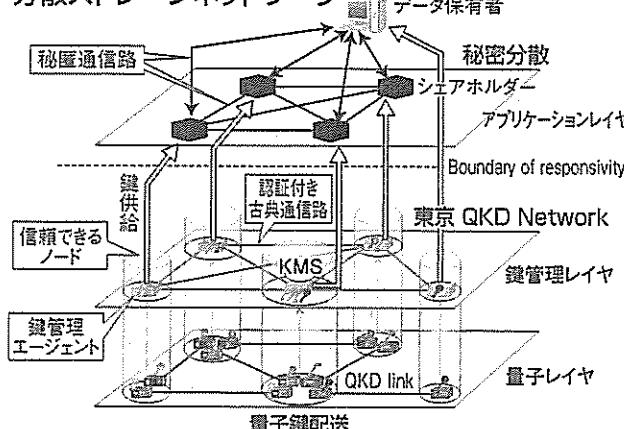
元NSA・CIA職員のスノーデン氏によるリーク情報でも喧伝されているが、インターネットで使用される暗号の一部は既に解読されている可能性がある。また現在解読されていなくても将来

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)。

## 情 報 漏えいなし 分散ストレージ開発



## 分散ストレージネットワーク



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。我々は今後重要なデータのバッファ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)

情報通信研究機構

# NICT 先端研究

(44)

計算機の能力が向上し金性を保証できる情報性を否定できない。一方で我々自身のゲノムデータなど、世纪単位での秘匿を要する

NICTでは長年解説不可能な通信を可能と行き来し、保管としている。この情報漏洩(KD)の開発を進めて向上去に安全性を重視するべきである。この技術はデータ伝送時の情報漏えいに対する対策であるが、データ保

エ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

み合わせはお互いの欠點が復元できると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。

しかししながら、これらは複数のデータが一つで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

つの技術の組み合わせで未解決な重要な課題があつた。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、パスワード認証、生体認証などを防ぐ上で不可欠な認証、デバイス認証などがある。

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。我々は今後重要なデータのバッファアップへの実利用に向けて働きかけを進めしていく。