

TYPE OF INDUSTRY



科学技術・大学

情報通信研究機構

NICT 先端研究

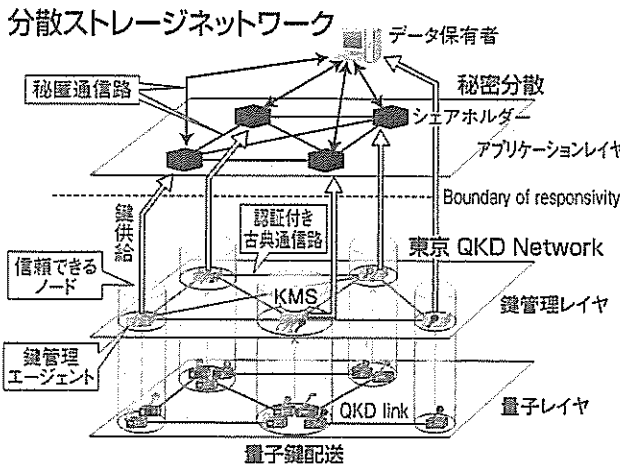
④

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る暗号も将来

計算機能力が向上し、全性を保証できる情報管に別は別の技術、情報漏えいを完全に防ぐことができる。一方でシエアの伝送は安全に行うことを仮定している。従って量子鍵配送と秘密分散の組み合わせは、鍵配送と秘密分散の組み合わせは、お互いの欠点を補完しあっている。NICTでは長年解読不可能な通信を可能にする量子鍵配送(QKD)の開発を進めてきた。この技術は、データを復元するにはある一定以上のシエアを集める必要がある。合理的な融合である。しかしながら、これら技術の組み合わせが、将来にわたり安定以上集まらない場合でも未解決な重要な課題があった。それは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、生体認証、生体認証など、特に生体認証などはコピーされる恐れがある。

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)。



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用に向けて働きかけを進めていく。
(火曜日に掲載)