

特集

量子計算機時代を見据えた 暗号研究の最前線

近年、暗号技術は単に情報を秘匿するというだけでなく、属性ベース暗号のような高機能暗号により、データの安全な利活用を支える技術としての役割も担うようになってきている。

また、昨今の量子技術の発展により、耐量子暗号や量子の特性を活かした新たな暗号技術の研究も進んでいる。

本特集では、NTTの暗号技術の研究者らによる論文をベースに、これらの最新暗号技術について紹介する。

暗号理論

耐量子暗号

量子アルゴリズム

ハッシュ関数

属性ベース暗号

Cryptography

現代暗号の発展と量子計算機時代の暗号研究に向けて 16

40年に及ぶNTTの暗号研究の歴史を、現在インターネット等でも広く用いられている「現代暗号」、汎用量子計算機の登場に備える「耐量子暗号」、量子の特性を活かした全く新たな「量子暗号」のフェーズごとに紹介する。

秘密鍵を安全に貸与できる関数型暗号 19

量子の特性を活用することで「秘密鍵を消去したことの証明」や「秘密鍵の複製防止」を可能にする暗号技術の概要と、実装された場合に期待されるイノベーションについて紹介する。

新たな応用分野を切り拓く量子計算機向けアルゴリズム 22

量子計算機で高速に解くことができる問題の領域を広げ得る、新たな量子計算機向けアルゴリズムの論文（Verifiable Quantum Advantage without Structure）の概要について紹介する。

量子計算機を用いた攻撃に対する ハッシュ関数の安全性のより良い理解へ向けて 26

世界中で幅広く利用されている暗号学的ハッシュ関数「SHA-2」の安全性が、量子計算機の登場によってどのような影響を受けるのかについて紹介する。

暗号とアクセス制御を組み合わせる革新的な 属性ベース暗号（ABE）技術の最新動向 30

NTT Research, Inc. において取り組んでいる、暗号技術と属性によるアクセス制御を組み込んだ属性ベース暗号「ABE」に関する研究について紹介する。

主役登場 西巻 陵（NTT社会情報研究所） 34

古典計算機では不可能な暗号技術を実現する量子力学の力