主役登場

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

西巻　陵
NTT社会情報研究所
特別研究員

暗号技術が達成する安全性は大きく分けて２種類あります．１つが情報理論的安全性であり，無限大の計算能力があっても破られることがない安全性です．もう１つは計算量的安全性であり，現在の計算機では破ることが難しいとされている安全性です．可能ならば情報理論的安全性を達成できるほうがもちろん望ましいです．しかし，公開鍵暗号に代表されるように多くの暗号技術において情報理論的安全性を達成することは不可能です．また，情報理論的安全性を達成できる暗号技術であっても，効率が非常に悪いことがほとんどです．ここでは，情報秘匿のための暗号の話だけに焦点を当てます．

１つの妥協点として考えられたものが，暗号文を消去することで消去した後は，無限大の計算能力をもってしても暗号を解読することができない消去証明可能暗号と呼ばれる暗号技術です．つまり，暗号文が消去される以前は計算量的安全性を達成し，消去後は情報理論的安全性を達成しています．仮に計算機の能力が将来飛躍的に向上するか，あるいは全く新しい革命的なアルゴリズムが生まれたとしても，暗号文を消去さえすればどうやっても解読できないので現実的な折衷案といえます．

問題はそのような暗号文の消去が実現できるかということです．これは古典計算機では不可能な暗号技術であり，量子計算機を利用することで初めて実現可能になります．量子力学の不確定性原理は，ある物理量Ａと別の物理量Ｂ（代表的なものは位置と運動量）について２つを同じくらいの正確さで測定することはできない，という原理です．これを応用することで，暗号文の消去（つまり含まれていた平文の情報消去）を実現することができます．消去証明可能暗号では，平文から量子状態の暗号文を生成します．平文の情報（仮にＸとする）に関する正確さが一定以上下がるような情報量（仮にＹとする）を，量子状態の暗号文から観測させることによって暗号文を消去することが可能になります．暗号文を生成したときに付加的に生成される検証用の情報を使って，情報量Ｙをチェックすることで暗号文を確かに消去したことを確認できます．量子状態の観測は不可逆的な操作なので，観測を行うと元の量子状態の暗号文は復元できません．このように量子力学の原理を応用することで古典計算機では実現できない高い安全性を持つ暗号技術を実現できます．

最近の私の研究で，このような消去証明可能な公開鍵暗号方式やさらに公開鍵暗号の発展形である関数型暗号について消去証明可能な方式を設計しました．古典計算機では実現不可能な暗号技術として，ほかには暗号文がコピー不可能な暗号などもあります．私はこの量子力学の強大な力に魅せられ，消去証明可能暗号をはじめとする古典計算機では実現不可能な暗号技術の実現のために研究に取り組んでいます．