3.4.3　ネットワークセキュリティ研究所　セキュリティ基盤研究室

室長　　高橋幸雄　ほか 8 名

情報通信ネットワークを誰もが安心・安全に利用できるためのセキュリティ基盤技術の研究開発

【概　要】

本研究室では、情報通信ネットワークを誰もが安心・安全に利用できるためのセキュリティ基盤技術の研究開発を行っており、今まさに必要とされている現在志向の研究から、10 年後、20 年後を見据えた未来志向の研究までを推進している。

1　**量子セキュリティ技術**: 量子技術と現代暗号技術を融合した、情報理論的安全性をもつセキュリティネットワーク構築のための研究

2　**長期利用可能暗号技術**: 量子計算機が出現しても安全性を維持できる次世代公開鍵暗号アルゴリズムの研究

3　**実用セキュリティ技術**: サイドチャネル攻撃による秘密漏洩に対する耐性を備えた暗号技術の研究

4　**暗号安全性評価技術の高度化**: 我が国の電子政府推奨暗号の継続的な安全性評価と、CRYPTREC（Cryptography Research and Evaluation Committees）を通じた将来の暗号技術移行指針への反映

【平成 23 年度の成果】

1　量子セキュリティ技術

未来 ICT 研究所　量子 ICT 研究室等との連携プロジェクトとして進めている量子セキュリティネットワークは、第 3 期中期計画（平成 23 ～ 27 年度）中に試験利用を開始し、平成 28 年以降、国家用途へ適用し社会還元できるよう取り組みを進めている。本研究室では、量子セキュリティ技術のネットワーク化を進める上で統一的なセキュリティ評価手法を開発するために、量子秘匿雑音通信方式の安全性評価を行った。これまで、この方式は安全性についての議論が極めて少なく、安全性の定義すらなかったが、本方式を暗号方式の利用モードと見なすことにより安全性の定義を行い、安全性評価を可能にした。また、量子秘匿雑音通信方式の実現方法として深宇宙通信への応用を検討しており、帯域幅やコヒーレント光の変調法を与え、通信路容量（通信性能）の評価も行った（図 1）。また、ネットワークの L2、L3 スイッチに量子鍵配送装置からの情報理論的に安全な鍵を供給し、改ざん・なりすましに対して耐性をもつスイッチの開発に着手、安全性評価を行った。さらに、量子鍵配送技術と秘密分散技術を組み合わせ、情報理論的に安全な認証機能付き秘密分散方式の基本設計を行った（図 2）。

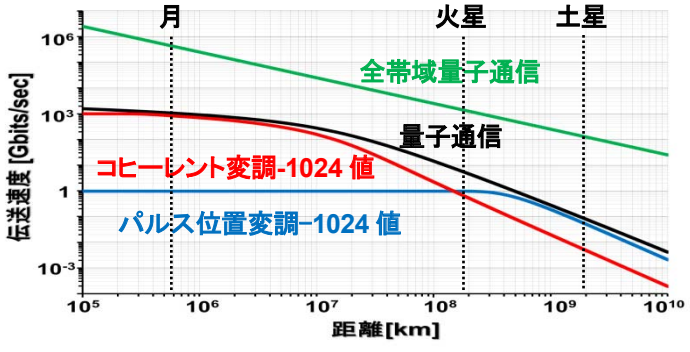

図 1　深宇宙通信における通信路容量

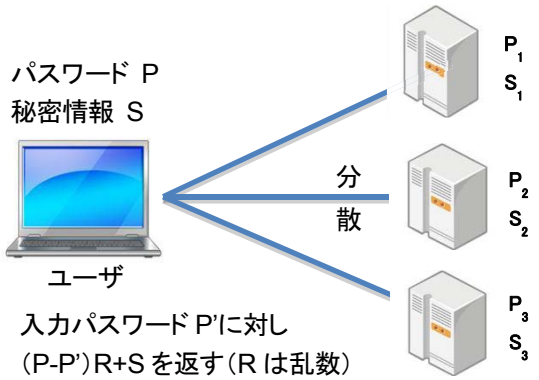

図 2　情報理論的に安全な認証機能付き秘密分散方式

2　長期利用可能暗号技術

現在、我が国の電子政府をはじめ、世界で広く利用されている RSA 暗号や DSA 署名などの公開鍵暗号は、その安全性が素因数分解や離散対数問題の困難性に依存しており、将来、量子計算機が実現されると安全性が保たれなくなるという課題がある。そこで、量子計算機が実現しても安全性が維持できる、別の数学上の困難な問題に基づく公開鍵暗号方式（耐量子暗号、ポスト量子暗号）についての研究が盛んに行われている。例えば、格子理論や符号理論における困難な問題に基づく新たな公開鍵暗号や、多変数多項式の求解の困難性に基

づく方式、Braid 群を用いた方式などさまざまなアプローチが模索されている。本研究室では、平成 23 年度は、格子理論、符号理論の一種である LPN（Learning Parity with Noise）問題を使った方式の基本設計を行った。また、Braid 群を使った方式についても基本設計を終了した。さらに設計と同時に安全性評価に関する研究も並行して行った。公開鍵暗号の安全性評価に用いられる LLL（Lenstra-Lenstra-Lovász）格子基底縮小アルゴリズムにおいて、より小さくより近い直交格子基底を求めるが、この処理を高速に行うアルゴリズムの 1 つである Random Sampling Reduction を改良し、GPU を用いて実装したところ、従来の 30 倍の高速化を達成することができた。これは RSA 暗号の解析や格子暗号の安全性の根拠となる問題の安全性評価速度向上に寄与する成果である。

3　実用セキュリティ技術

実用暗号技術においては、コールド・ブート攻撃等による秘密鍵漏洩に対して耐性をもつ内積述語暗号の設計を行った。コールド・ブート攻撃とは実行中またはシャットダウンしてから数分以内のコンピュータに物理的にアクセスし、メモリを一気に冷却してパスワードや秘密鍵の一部情報をメモリに保持し、そこからパスワードや秘密鍵全体を推測する攻撃である（図 3）。本方式は、現在広く利用されている RSA 暗号などよりも安全性が高く、暗号化時に任意の論理式を埋め込むことで復号条件等を設定することができるなど、柔軟なアクセス制御を可能とする機能を有している。さらに被害時被災者向け個人認証システム試験構築に向けた取り組みとして、バイオメトリクスや位置認証方式等の研究を行った。

図 3　コールド・ブート攻撃

4　暗号安全性評価技術の高度化

安全性評価の高度化においては、電子政府推奨暗号リストに記載されている暗号、並びに新規応募暗号の安全性評価を行った。共通鍵暗号系については、リスト記載のブロック暗号の関連鍵攻撃に対する安全性評価、およびストリーム暗号 Multi-S01 とメッセージ認証 PC-MAC-AES の鍵回復攻撃に対する安全性評価を行った。公開鍵暗号系については、次世代公開鍵暗号として注目されているペアリング暗号の安全性評価を行うために、この暗号の安全性の根拠となっている離散対数問題を解く大規模計算機実験を九州大学、富士通研究所と連携して行い、923 ビットの離散対数問題を解くことに世界で初めて成功した（図 4）。この計算機実験には NICT で導入した図 5 に示す計算機群を活用した。この成果はペアリング暗号の安全性を確立し、次世代暗号の標準化に寄与するものである。また、RSA の秘密鍵の部分情報が得られた場合に、これを再構成するアルゴリズムを一般化し、多項式時間で再構成できるための条件や理論限界を導出した。また、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト CRYPTREC の事務局として、平成 25 年に予定されている電子政府推奨暗号リスト改訂に向けたプロジェクト運営および外部機関との連携を行った。

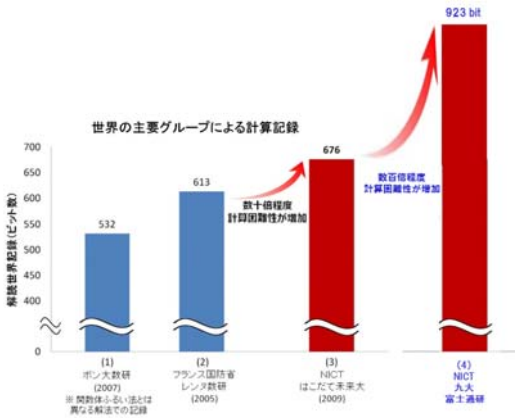

図 4　ペアリング暗号（離散対数問題）の解読で世界記録を達成

図 5　解読実験に使用した計算機群