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　　盛合志帆　ほか 8 名

次世代ネットワークサービスを支える暗号技術の安全性評価において 2 つの世界記録を達成

【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、第 3 期中期計画において下記の 4 つの研究テーマを掲げ、現代暗号理論から量子セキュリティまで、実用性を重視した次世代暗号技術の確立をめざし、研究開発を推進している。

1　**量子セキュリティ技術**：量子 ICT 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など、長期にわたり高い安全性を維持できる長期利用可能暗号技術に関する研究
3　**実用セキュリティ技術**：プライバシ情報を含むビッグデータのセキュリティ処理に関する研究や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**：わ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 24 年度は、次世代ネットワークサービスを変える暗号技術の安全性評価において 2 つの世界記録を達成するなど大きな成果を挙げることができた。

【平成 24 年度の成果】

1　量子セキュリティ技術・情報論理的安全性に基づくセキュリティ技術

量子セキュリティネットワーク構築に向けて、平成 23 年度に基本設計を行った認証機能付き秘密分散方式の機能拡張及び安全性検証を行った。具体的には、クラウド上の複数サーバにデータを分散して保存する際に、各サーバが攻撃を受けデータが流出したとしても、サーバが結託しない限り情報漏洩が起こらない安全性の高い新方式を東京工業大学と共同で設計した（図 1）。本方式は平成 25 年度に量子 ICT 研究室と連携してシステムを構築し、実証を行う予定である。

また、複数のユーザを一度に認証する量子同時複数認証方式の実現や、秘密分散方式において、従来よりも多くの秘密情報を分散可能な複数閾値複数秘密分散法の提案を行った。

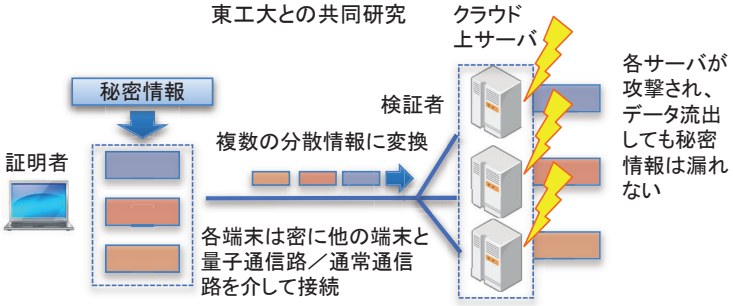

図 1　認証機能付秘密分散方式

2　長期利用可能暗号技術

平成 24 年度は、格子理論に基づく方式に集中して研究を行った。特に、格子暗号の安全性評価に関して、格子暗号の安全性の根拠となっている最短ベクトル問題の難しさの評価を行った（株式会社日立製作所との共同研究）。この問題に対する最も有効なアプローチである BKZ 2.0 アルゴリズムの実装を行い、高速化のための改良を行った。このアルゴリズムをドイツのダルムシュタット工科大学が主催する暗号解読コンテスト TU Darmstadt Lattice Challenge に適用したところ、これまでの世界記録であった Chen-Nguyen の記録を上回る 825 次元の問題を解くことに成功した（図 2）。

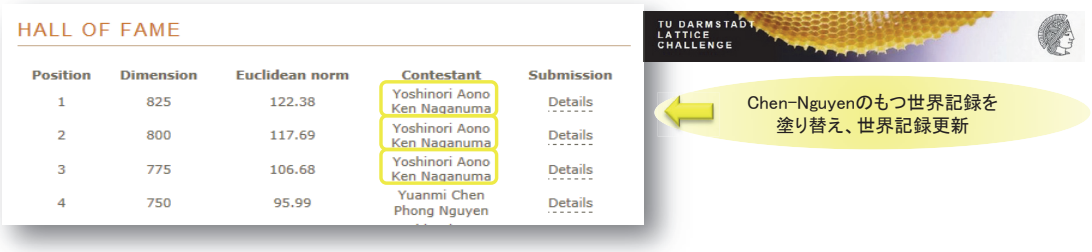

図 2　格子暗号の安全性評価で世界記録達成
（ダルムシュタット工科大学主催 TU Darmstadt Lattice Challenge）

3　実用セキュリティ技術

センサのようなリソースの限られたデバイスに実装可能な「軽量暗号」を、クラウド上で高速に並列復号処理する実装法を世界で初めて開発した。これにより軽量暗号がローエンドデバイスにおける小型ハードウェア実装での優位性のみならず、ハイエンドプラットフォームの高速ソフトウェア実装でも優位性をもつことを示し、暗号技術の実装に関する最高峰の国際会議 CHES2012 で発表を行った（ソニー株式会社との共同研究）。さらに、軽量暗号に求められる安全性・実装性能等の要件を規定した国際標準 ISO/IEC 29192-1 の規格化を完了、平成 24 年 5 月に出版された （国際規格開発賞受賞）。

また、平成 23 年度に基本設計を行った暗号技術「サイドチャネル攻撃に対して安全な ID-based 暗号」に関して機能拡張を行い、国際会議で発表を行った。

4　暗号安全性評価技術の高度化

（1） ペアリング暗号の安全性評価

データを暗号化したまま検索できる機能など、クラウド上でのプライバシ保護機能が期待されている次世代公開鍵暗号「ペアリング暗号」の安全性を評価するための解読実験を九州大学、株式会社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 3）。今回の成果によりペアリング暗号の安全なパラメータを算出することができ、今後の実用化に向けた大きな一歩となった。本成果は、国際会議 ASIACRYPT2012 で採録されたほか、情報処理学会より喜安記念業績賞を受賞した。

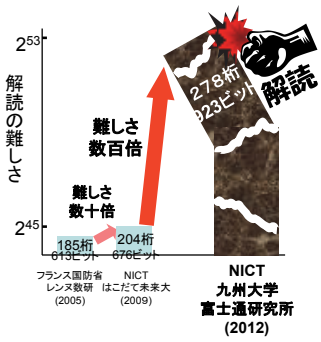

図 3　ペアリング暗号の安全性評価で世界記録達成

（2） 公開鍵検証・可視化システム

ネットワーク上での安全な通信を支えている公開鍵認証基盤における公開鍵証明書のデータを収集し、そこで用いられている公開鍵の安全性を高速に検証し、脆弱性の分布を可視化するシステムの構築を開始した。このシステムでは、公開鍵証明書で使われている公開鍵の種別や鍵長などの統計情報のほか、特に RSA 暗号の公開鍵において、他の公開鍵証明書と秘密鍵が共有され危険な状態にあるものの分布を表示する機能を有している。このシステムは、現在利用されている RSA 公開鍵の上述の脆弱性の有無を確認できるほか、より安全な鍵長への移行状況の把握、公開鍵証明書新規発行時の脆弱性確認などに活用できる。

（3） CRYPTREC 電子政府推奨暗号リスト改定

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 CRYPTREC プロジェクトにおいて、平成 24 年度は 10 年ぶりの電子政府推奨暗号リスト改定という節目の年であった。NICT は（独）情報処理推進機構 （IPA）とともに暗号方式委員会、暗号実装委員会、暗号運用委員会の事務局を務めており、リスト改定にあたり必須となる評価対象暗号アルゴリズムの安全性評価を実施するなど、学術面・事務局運営面双方から多大な貢献を行った。