通信・情報処理

非可換代数をもとにした安全、高速、軽量な暗号

Secure, fast, light encryption based on non-commutative algebra

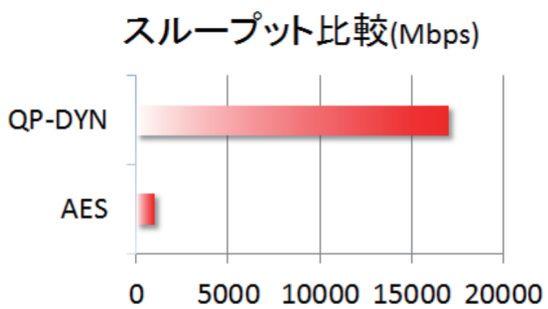
入山　聖史　Satoshi IRIYAMA　（東京理科大学　理工学部　情報科学科　准教授）

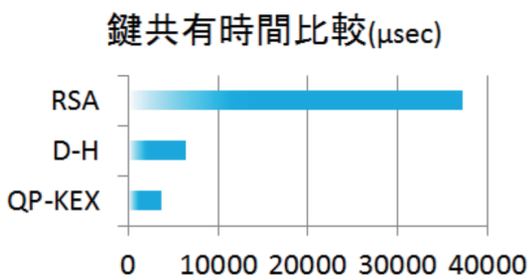
研究の目的

東京理科大学名誉教授大矢雅則とローマII大学教授アカルディらは、20年以上に渡る数学（非可換代数学、非可換確率論）などの研究をベースとして、新しい暗号方式を開発しました。我々は、非可換代数をもとにした暗号、新しい原理にもとづいた暗号理論の研究を行っています。

研究の概要

共通鍵ストリーム暗号(QP-DYN)では独自の数学理論がもとになっており、高品質な乱数を発生できます。鍵交換(QP-KEX)は行列型離散対数問題を内包する数学で構成されており、安全です。また、ベクトル型計算であり、並列処理が可能なので高速です。





クリプトボックス
（8cm x 8cm, 500g）

従来・競合との比較

AESと比較して10倍以上のスループットを達成しました。また、RSAと比較して鍵生成、鍵交換の速度が10倍程度の高速です。FPGAでの実装ではAESと比較して75%程度の回路サイズの縮小を達成しました。

想定される用途

・クラウドサーバーなどでの高速処理
・モバイル環境での安全性向上
・4K、8K環境の映像配信でのリアルタイム処理

実用化に向けた課題

・魅力的なサービスの開発
・暗号規格への申請
・仕様の標準化

企業へ期待すること

共同での製品・サービス開発、小型チップ化、新たな暗号利用への挑戦に取り組んでくれる共同研究企業を募集しています。

POINT

・安全なOne-Time-Pad暗号
・鍵生成、鍵交換、暗号化が高速
・回路サイズが小さく軽量

今後の展開

製品のパイロット版を多数開発中です。国内のみならず海外展開も視野に入れて周知して行く予定です。

■ 試作品
持ち運びできる暗号化装置「クリプトボックス」
電子メール暗号化（Outlook、Google対応）
モバイルアプリ

東京理科大学 研究戦略・産学連携センター

〒162-8601　東京都新宿区神楽坂一丁目３番地　TEL:03-5228-7440　E-MAIL:ura@admin.tus.ac.jp

2015.08
(2019.04)