U753

一筆書き多項式を用いた、ストリーム暗号アルゴリズム

ライセンス契約を受けていただき 本発明の実用化を目指していただける企業様を求めます。

高い安全性、かつ実行速度が速いことを特徴とするストリーム暗号アルゴリズムです。

◆背景

オンラインで電子データのやり取りをする機械が格段に増えた現代、電子データの暗号化技術は、非常に重要なセキュリティ技術です。暗号化技術はその用途特性上、安全性の高い手法であることが重要ですが、純粋に安全性を高めようとすると計算量が膨大になるため、処理に時間がかかり、ユーザビリティが低下します。そのため、高い安全性に加え、高速な計算実行速度、さらに軽量アルゴリズム、という3つの特徴をあわせもつ手法が求められています。

◆発明概要と利点

京都大学では、独自のアイデアに基づき、一筆書き多項式を用いた新しいストリーム暗号アルゴリズムを発明しました。

- **高速な計算実行速度、かつ軽量なアルゴリズム**
  3Gbps以上の速度で実行することが可能です（表1）。
- **高い安全性**
  NIST SP 800-22検定により、本発明手法で得られた乱数は良好な乱数性であることが証明されています（表2）。
- **大容量データの暗号化に最適**
  高速かつ軽量なため、4K／8K画像や映像の暗号化、また電力制限のあるデバイスを用いた暗号化に適します。

	実行環境	暗号化速度 (cycle/byte)
従来手法	―	2.88
本発明手法 (実装例①)	➢ 1.3GHz Core i5 ➢ 4GB 1600MHz DDR3 ➢ 最適化オプション Ofast (家庭用パソコンでの実行)	**2.16**
本発明手法 (実装例②)		**2.46**

表1：実装評価結果

合格したテスト項目数	セット数
188	71
187	22
186	6
185	1

検定セット数：100セット

表2：NIST SP 800-22検定結果

◆研究段階
乱数特性は確認済み（表1）

◆発表状況
日本応用数理学会 第12回研究部会連合会発表会
(2016年3月4日～5日)

◆用途
- 大容量データの暗号化
  - 4K／8K画像、医療画像
  - 映像
- データセンターの暗号化
- プリンター／複合機内の電子データの暗号化
- 電力制限のあるデバイス内での暗号化
  - スマートフォン
  - ウェアラブル端末
  - センサーデバイス

◆希望の連携形態
- 実施許諾 (非独占/独占)
- オプション (非独占/独占)

※本発明は京都大学から特許出願中です。

◆お問い合わせ先
京都大学産学連携担当
関西TLO株式会社
ライセンシング・アソシエイト
担当：藤ヶ崎　諒平

〒606-8501
京都市左京区吉田本町
京都大学国際科学イノベーション棟５階
(075)753-9150
fujigasaki@kansai-tlo.co.jp

Office of Society-Academia Collaboration for Innovation
KYOTO UNIVERSITY

関西TLO株式会社
TECHNOLOGY LICENSING ORGANIZATION