情報学部　情報学科　教授
吉岡　大三郎　YOSHIOKA　Daisaburo

IoT時代に向けた暗号の軽量化を図る

～IoTデバイス向き軽量カオス暗号の設計に関する研究～

キーワード

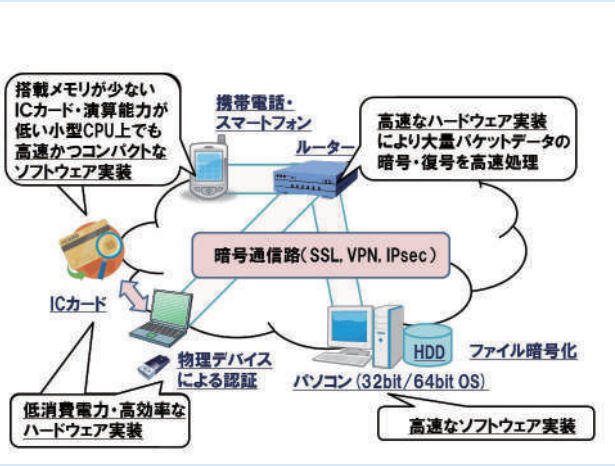
軽量暗号、カオス、IoT

研究シーズ概要

暗号は高度情報社会のセキュリティを支える主要素技術であり、一般的には2000年に策定された標準暗号AES(Advanced Encryption Standard)が広く知られ、利用されています。

今後、様々な小型機器や多様なデバイスとの接続が進み、生活やビジネスにおいての利便性が大きく向上するIoT(Internet of Things)時代に向けて、省リソースなハードウェア・ソフトウェア実装に可能な暗号の"軽量性"が求められています。(右図)

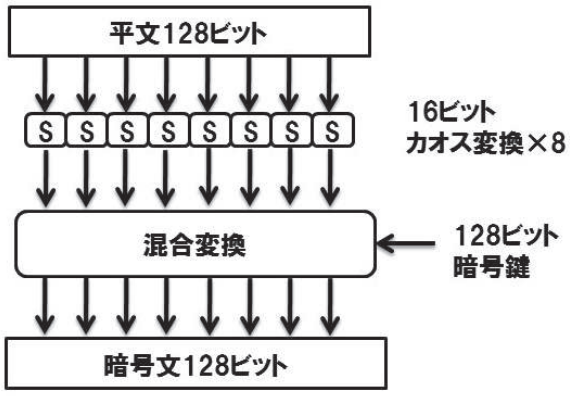
本研究は、簡単な規則から得られる不規則現象"カオス"を応用し、デジタル実装に適した新しい軽量カオス暗号を提案します。



利点・特長・成果

■センサーや小型デバイスなど様々なモノが情報のやり取りを行うIoT時代に向けて、それら小型デバイスに実装できる小面積・低消費電力に適した軽量暗号が必要とされています。そこで本研究では、簡単な整数演算に基づくディジタルカ オス写像に基づく軽量カオス暗号(図１)を提案しています。

■現在、標準暗号AESが使用されていますが、ガロア拡大体の計算を必要とするので、小型デバイス実装には不向きとされています。提案する軽量カオス暗号は、簡単な組み合わせ論理回路のみで実装でき、AESと比べて十分な解読耐性を有しつつ半分以下の回路面積で実装可能です。



E-mail
yoshioka@cis.sojo-u.ac.jp