情報通信
電気電子

小型デバイス向き暗号の開発

～軽量カオス暗号の研究～

情報学部　情報学科　准教授

吉岡 大三郎　YOSHIOKA daisaburo

■キーワード

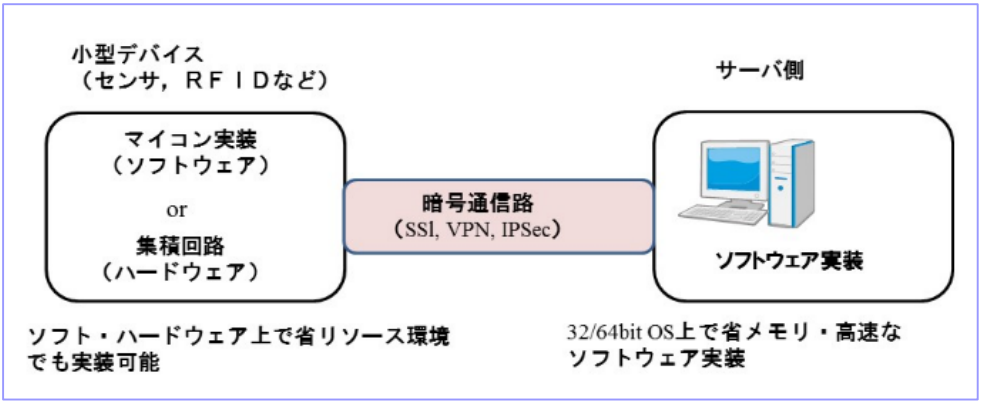
軽量暗号、カオス、セキュリティ

■シーズ概要

暗号は通信の秘匿性確保や認証を実現するセキュリティの基盤技術です。暗号設計では、いかに実装効率を上げつつ、解読できない難しさを持たせるかが課題となっています。

当研究室では、簡単な方程式に基づく不規則で複雑な現象“カオス”を応用した暗号の研究を行っています。

ユビキタスセンサや RFID、正規品認証など、通信端末の小型化のニーズは今後ますます高まるものと推測します。当研究室では、それら小型デバイス（マイコン、ディジタル集積回路）上で効率よく実装できる軽量暗号の実現を目指します。

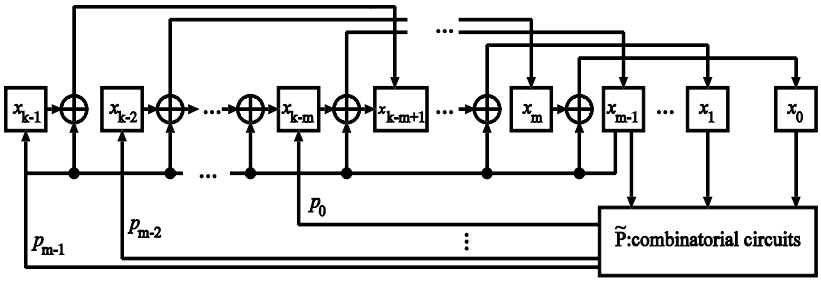


■アピールポイント

■暗号の主要部となる S-box を設計し、2000 年に策定された標準暗号 AES と比べ、同等以上の解読耐性を達成しました。

■簡単な整数演算上の計算を使用するだけなので、AES と比べてソフトウェア実装におけるコードサイズ、メモリ使用量、計算時間の改善を実現します。

■ハードウェア実装は論理演算のみを使用するため（下図参照）、AES と比べ、回路規模、消費電力を抑えることができます。



■その他の研究シーズ

■カオスに基づく疑似乱数設計

■OFDM 通信の電力効率改善

■メッセージ

■70 年代以前までは暗号の詳細は秘密でした。一方で現代の暗号は、そのような“隠すことによるセキュリティ”でなく、アルゴリズムはオープンにして、専門家からの検証を受けることが大事とされています。当研究室で提案した暗号化関数は、電子・情報分野の国内最大手学会である電子情報通信学会が発行する国際誌 IEICE に採録され、公表しています。（IEICE Trans. Fundamentals, vol.E97-A, no.6, pp.1396—1404, 2014.）

■暗号・セキュリティ分野に興味があり、製品化をお考えの方は、ぜひお気軽にご相談ください。