デュプレックス構造に基づく軽量認証付き暗号に関する研究

Research on The Duplex-based Lightweight Authenticated Encryption Schemes

張 東
有田研究室
情報セキュリティ大学院大学

Duplex structure authenticated encryption is lightweight because it has the functions desired for weight reduction (one-pass, state memory size estimation, no back processing, no cache required, few processing steps, ideal for short messages, etc.). Especially applicable to authenticated encryption. Select the applicable lightweight cryptographic member from the lightweight cryptographic algorithm family or algorithm group according to the device restriction requirements.

背景

IoTの普及に伴い、リソースに制限のあるデバイス（フットプリント制限、電力消費制限、メモリ使用制限など）はサイバー攻撃とサイドチャネル攻撃を受け易くなっている。

IoT においては、保護すべき情報に対する不正アクセス、盗聴、改ざん・偽造、成りすましといった脅威への対策として、暗号技術を用いた認証、暗号化、電子署名を導入することが必要である。

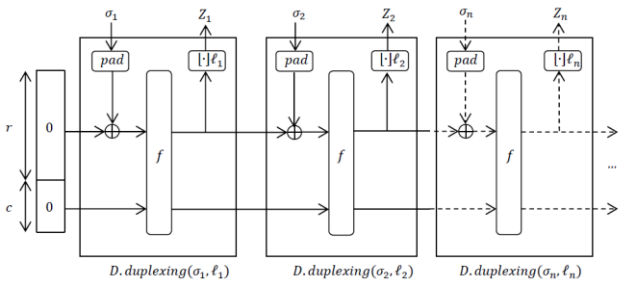
ただし、多くの従来の暗号化標準（AES-GCMなど）では、セキュリティ、パフォーマンス、およびリソース要件間のトレードオフがデスクトップ環境とサーバー環境向けに最適化されているため、リソースが制約されたデバイスに実装することが困難または不可能である。

2017年、日本の「CRYPTREC 暗号技術ガイドライン（軽量暗号）」、2018年、CAESAR：認定暗号化コンペティション、2020年、NIST軽量暗号化コンペティションは、リソース制限デバイス向けの認証暗号ソリューションを提供することを目的とする。

デュプレックス構造認証付き暗号

限られた環境に適用される軽量認証暗号は、軽量利点がある機能（ワンパス、逆処理不要、キャッシュ不要、処理ステップの少なさ、短いメッセージに適応可能など）が望まれる。

デュプレックス構造が有望



デュプレックス構造

認証付き暗号

➢ 暗号化アルゴリズムW (Wraping)

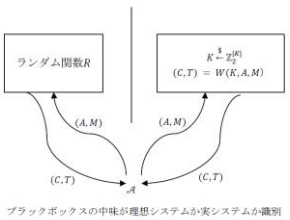
$W: \mathbb{Z}_2^{|K|} \times (\mathbb{Z}_2^*)^2 \to \mathbb{Z}_2^* \times \mathbb{Z}_2^{|T|}$:

$(K, A, M) \to (C, T) = W(K, A, M)$.

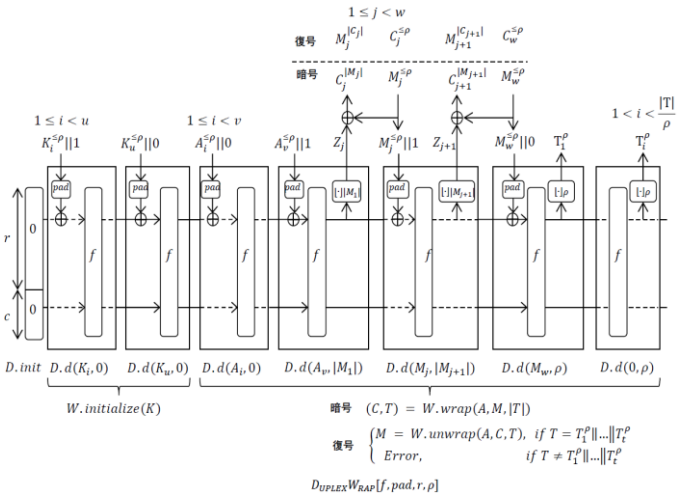
➢ 復号アルゴリズムU (Unwraping)

$U: \mathbb{Z}_2^{|K|} \times (\mathbb{Z}_2^*)^2 \times \mathbb{Z}_2^{|T|} \to \mathbb{Z}_2^* \cup \{error\}$:

$(K, A, C, T) \to M \text{ or } error$.



ブラックボックスの中味が理想システムか実システムか識別



➢ 安全性

$$\mathrm{Adv}^{\mathrm{priv}}(\mathcal{A}) = \left| \Pr\left[K \xleftarrow{\$} \mathbb{Z}_2^{|K|} : \mathcal{A}[W(K,\cdot,\cdot)] = 1\right] - \Pr[\mathcal{A}[R(\cdot,\cdot)] = 1] \right|$$

$$\mathrm{Adv}^{auth}(\mathcal{A}) = \Pr\left[K \xleftarrow{\$} \mathbb{Z}_2^{|K|} : \mathcal{A}[W(K,\cdot,\cdot)] \text{が偽造暗号文を出力}\right]$$