T-49

非線形コンバイナ型乱数生成器に対する Sum-Product Algorithmを用いる攻撃に関する一考察

久保航汰，齋藤翔太，鎌塚明，松嶋敏泰（早稲田大学）

未知変数の推定

ストリーム暗号に対する攻撃：未知変数の推定問題

変数間に制約ある
⇒グラフィカルモデルで表現可能

誤り率最小の推定
⇒事後確率最大の変数の値に決定

グラフィカルモデル上でSum-Product Algorithmを用い事後確率計算

問題

グラフにループがある
↓
どうアルゴリズムを適用するか

⇒
どんなグラフか
どんなスケジューリングか
硬判定（各変数の値を確定させる）か

アルゴリズムの適用法

適用法1：**ループを除去**する
適用法2：部分グラフ内でメッセージ伝播→ほかの**部分グラフに伝播**させる
適用法3：**硬判定にする条件**を決める