数理ソルバーを用いた暗号の解析

情報科学研究科　データ計算科学専攻

◎D1　内海（うつみ）　潮音（しおん）、教授　五十部（いそべ）　孝典（たかのり）

キーワード　**共通鍵暗号，安全性評価，数理最適化**

研究概要

近年の急速な情報技術の発展に伴う超スマート社会(Society 5.0)や DX に向けた動向から、より強固なセキュリティ技術が求められる。共通鍵暗号は多くのセキュリティ技術の基礎技術の一つであり、システムの安全性が共通鍵暗号の安全性と密接に関わっているため安全な共通鍵暗号は必要不可欠である。しかし、暗号技術は安全性が計算量から見積もられているため、計算技術向上の著しい近年では危殆化の恐れがあり、継続的に安全性評価をすることが強固なセキュリティを確保する上で重要である。

本研究では共通鍵暗号の安全性評価を目的に、2011 年に提案された混合整数線形計画法や、2022 年に提案された充足可能性問題を利用し、差分や線形などの統計的性質の暗号演算上での遷移を数理ソルバーで評価を行う手法を利用する。従来の手計算による評価では困難であった、軽量ブロック暗号に関する以下の課題へ取り組んだ。

1.軽量ブロック暗号 Piccolo のラウンド置換の最適性が検証されていない
2.軽量ブロック暗号 Piccolo に対する bit 単位の安全性評価が実施されていない
3.軽量ブロック暗号 Piccolo などに対する関連鍵差分攻撃に対する安全性評価が実施されていない

結果として 1.では Piccolo の安全性を上回るラウンド置換が存在しないこと、2、3.ではこれまでの安全性の境界を更新し、いずれも仕様のラウンド数では安全であることを示した。

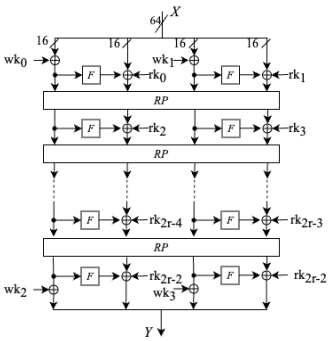

図 1 Piccolo の演算

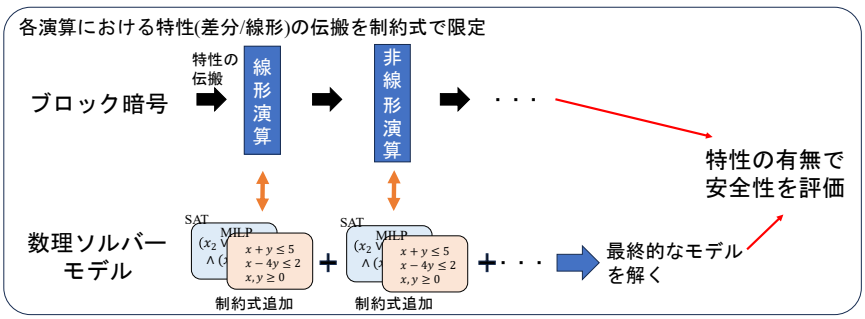

図 2 数理ソルバーを用いた評価の概要

アピールポイント

上記の数理ソルバーを活用した手法は、従来の手計算や経験則に基づく解析手法に比べ、より広範な探索空間に対しての評価が可能である点で優れている。暗号に対する解析精度は向上し、その結果、脆弱性の事前防止や新たな暗号設計の際に 1 の指標となるため、よりセキュアな情報通信のために役立つことが期待される。発表者はこれまでの解析結果を 査読付き国際学術誌へ掲載済みである。(1. *IET Information Security*, 2. *Information Processing Letters*, 3. *IEICE Transaction on Information and systems*)