IoT時代に必要とされる軽量共通鍵暗号の安全性評価に貢献
――国際暗号学会主催国際会議に採録された論文がTop3に選出される

NTTはドイツのルール大学ボッホム校および神戸大学との共同研究により，IoT時代に必要とされる軽量共通鍵暗号の安全性評価に大きく貢献する，共通鍵暗号に対する新たな解析手法を開発しました．

■研究の成果

これまでの大多数の解析手法による安全性評価では，攻撃者が選んだ平文を暗号化してもらい出力された暗号文をテラバイト単位で用意するという，攻撃者にとって非現実的な環境が必要とされていました．今回の解析手法による安全性評価では，いくつかの（軽量）共通鍵暗号に対し，平文が繰り返しを含む場合や，同じ平文が複数回暗号化される場合において，1キロバイト未満の暗号文だけから平文の一部が導出されてしまう危険性を指摘しました．今回開発した解析手法（非線形不変量攻撃）は，今後新規に軽量共通鍵暗号を設計する際の安全性評価に大きく貢献します．この研究結果は，国際暗号学会主催の暗号関連のトップ会議Asiacrypt 2016に採録され，優秀論文Top3に位置付けられる「Journal of Cryptology 招待」に選ばれました．

■技術のポイント

① 1993年に発表された線形解読法は，当時，暗号の事実上の国際標準方式であったDESに対する有効な解読手法でした（**図1**）．線形解読法は暗号を線形近似することで秘密鍵を解読する攻撃手法でした．今回，線形近似を非線形近似へと拡張することで，新たな解読法の発見につながりました．従来，非線形近似を利用することは不可能とされてきました．今回，暗号を構成する一要素であるS-boxと呼ばれる非線形関数に対して確率1の非線形近似を発見でき，さらに線形変換部に二値直交行列が用いられている場合は，ここでも確率1の非線形近似が存在することを示し，不可能とされていた非線形近似の利用に成功し，解読へとつながりました（**図2**）．

② 共通鍵暗号は実装効率化のため処理の多くに繰り返し構造を用います．軽量共通鍵暗号の場合，通常よりも厳しい実装効率の要求を満たすため，繰り返し構造以外の処理を極限まで省略します．今回の解読手法では，この極端に省略された構造をセキュリティホールとして利用しています．

③ 今回解析対象としている共通鍵暗号はブロック暗号と呼ばれ，それ単一では任意長のメッセージを処理す

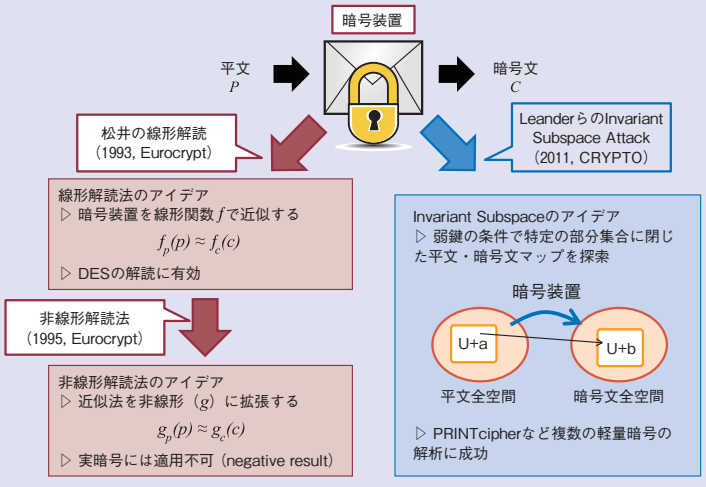
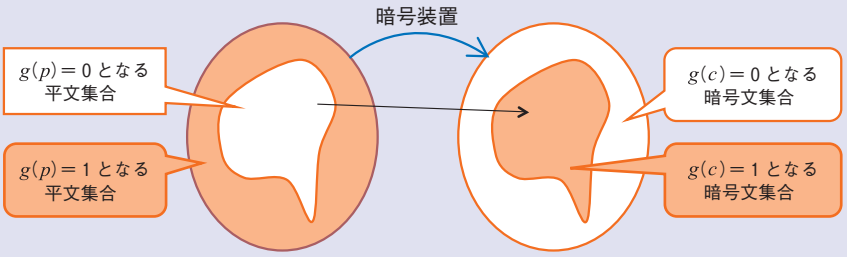


図1　研究背景

非線形不変量攻撃のアイデア

▷ 非線形解読法とInvariant Subspaceの両方からインスピレーションを得た新しい解析手法



3つの技術ポイント

①世界で初めて，平文と暗号文の関係を非線形関数gで近似し，その有効性を示す（20年来の未解決問題）
②軽量暗号で省略される個所に注目
③頻用される暗号の“使われ方”に注目し，一瞬で解読する，暗号学的に強力な攻撃に成功

図2　新評価法

ることができません．そのため，任意長のメッセージを処理できるようブロック暗号利用モードが用いられます．非線形不変量攻撃は，この暗号利用モードにおける“ブロック暗号の使われ方”に注目することで，一瞬で暗号文のみから平文を解読する，暗号学的に強力な攻撃の危険性の指摘につながりました．

◆問い合わせ先

NTTサービスイノベーション総合研究所
広報担当
TEL　046-859-2032
URL　http://www.ntt.co.jp/news2016/1612/161201a.html

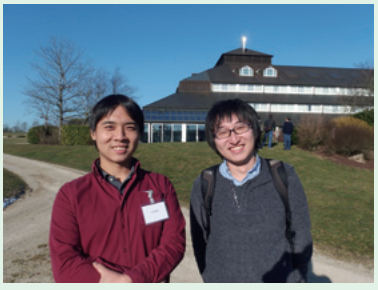
より軽量かつ安全な軽量共通鍵暗号をめざして

研究者紹介

佐々木　悠
NTTセキュアプラットフォーム研究所
データセキュリティプロジェクト　セキュリティ基盤研究グループ
研究主任

軽量共通鍵暗号の設計はわずか1ゲートでも軽量化をめざすという極限のテーマであり安全性向上への貢献度が不明な処理を残しておく余裕はありません．一方で防御機構を省略しすぎてしまうと解読を許してしまうため，どこまで軽量化しても安全性が保たれるか，というシビアな判断を求められます．合理的な判断を下す能力は，職人芸のように，良い設計をめざして試行錯誤することでしか得られません．

安全か脆弱か，明確な判断ができない場合も多いのですが，今回の研究では誰もが認める脆弱性を指摘することができ，嬉しく思っています．この経験を活かし，NTT発の軽量暗号がIoTを席巻する世界をめざして研究を続けていきたいと思います．


（左から）佐々木悠，藤堂洋介

藤堂　洋介
NTTセキュアプラットフォーム研究所
データセキュリティプロジェクト　セキュリティ基盤研究グループ
研究員

非線形不変量攻撃の研究はLeander教授との議論から始まります．そこで，私たちは非線形不変量攻撃とは似ても似つかない攻撃手法を用いてSCREAMと呼ばれる改ざん検知暗号の安全性評価に取り組んでいました．そんな中，SCREAMの構成要素の1つであるS-boxに不可思議な性質があることを発見しました．私たちは，この何に使えるかも分からない性質を“magical property”と呼び，有効利用の模索に努めました．試行錯誤の中，S-boxだけでなくSCREAMを構成するすべての要素が“magical property”を持っていることに気付き，この発見が“非線形不変量攻撃”という新しい解析手法の発見につながったのです．

一見何に使えるか分からない性質も，さまざまな角度から見れば大きな発見につながる．そんな“研究あるある”を肌で感じることができた，貴重な体験でした．