暗号解析評価技術

新たな暗号解読法の発見により最難関国際会議で最優秀論文賞を獲得

NTTセキュアプラットフォーム研究所では長年にわたって暗号理論の研究開発を進めている。2015年に挙げた大きな成果の1つが、20年近く破られていなかった「MISTY1」という国産共通鍵暗号の解読方法を発表したことである。この解読方法を示した論文は、国際暗号学会が主催する暗号分野における最難関国際会議「CRYPTO」で最優秀論文賞を受賞した。同解読手法の概要や、そのインパクトなどについて紹介する。

20年間安全性を維持してきた国産共通鍵暗号「MISTY1」

データの暗号化と復号に同じ鍵を使う「共通鍵暗号」は非常に用途が広い暗号で、これまでに多数の種類が開発されてきた。

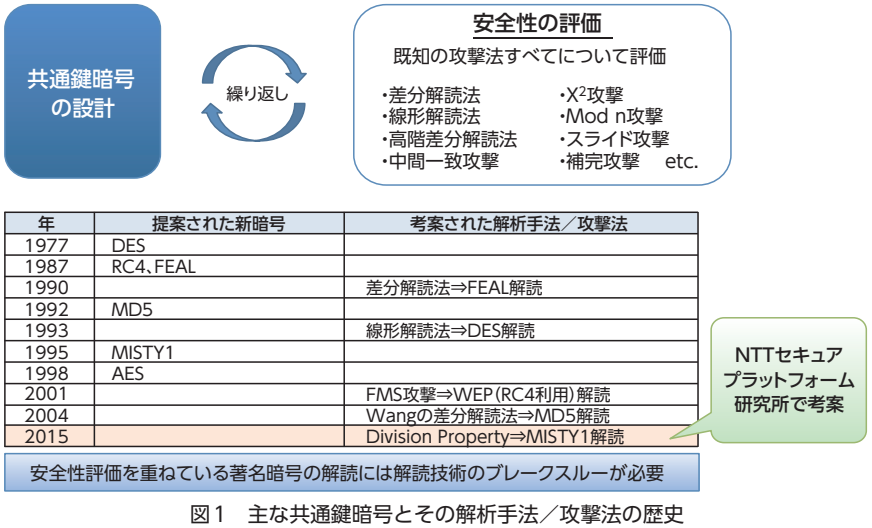
共通鍵暗号の歴史は、解析手法／攻撃法の発達に伴う淘汰の歴史である（図1）。共通鍵暗号の安全性は、既知の解析手法／攻撃法を使った第三者評価と、その評価結果を設計に取り入れるサイクルを回すことで担保されている。新しい解析手法／攻撃法の考案によって、それまで使われていた暗号が設計者の想定した安全性を備えていないと判明することは珍しくない。差分解読法や線形解読法といった強力な解析手法が考案された1990年代には、多くの共通鍵暗号が淘汰されていった。

そうした淘汰の歴史を生き残ってきた共通鍵暗号の1つが「MISTY1」である。1995年に三菱電機の松井充氏らによって開発された同暗号は、さまざまな国際標準で推奨暗号と規定されて20年間以上使われ続けている。

MISTY1がこれほど長い期間安全性を維持できた理由は主に2つある。1つは、開発時点で既知であった差分解読法や線形解読法に対して安全だと数学的に証明された設計を採用したこと。もう1つは「ラウンド数」の設定が巧みだったことである。MISTY1のような共通鍵ブロック暗号は、データを乱雑化する「段関数（ラウンド関数）」という関数を繰り返し実行することで暗号として必要な複雑さを獲得する仕組みになっていることが多い。段関数の実行回数がラウンド数である。

MISTY1とほぼ同時期に考案された攻撃法に「高階差分攻撃」（図2）というものがある。これは、ラウンド数と複雑さの関係を評価して、暗号が十分な複雑さを確保できているかどうかを調べることによる攻撃手法である。暗号として必要な複雑さを獲得できるラウンド数を設定していれ

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 藤堂 洋介氏



年	提案された新暗号	考案された解析手法／攻撃法
1977	DES	
1987	RC4、FEAL	
1990		差分解読法⇒FEAL解読
1992	MD5	
1993		線形解読法⇒DES解読
1995	MISTY1	
1998	AES	
2001		FMS攻撃⇒WEP(RC4利用)解読
2004		Wangの差分解読法⇒MD5解読
2015		Division Property⇒MISTY1解読

NTTセキュアプラットフォーム研究所で考案

安全性評価を重ねている著名暗号の解読には解読技術のブレークスルーが必要

図1　主な共通鍵暗号とその解析手法／攻撃法の歴史

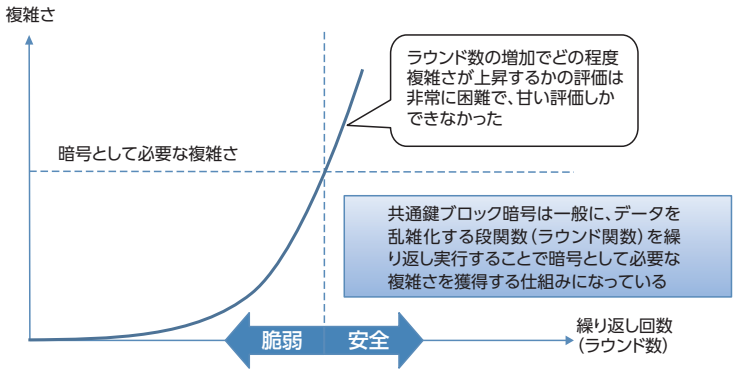


図2　共通鍵ブロック暗号の安全性を評価する高階差分攻撃の概要

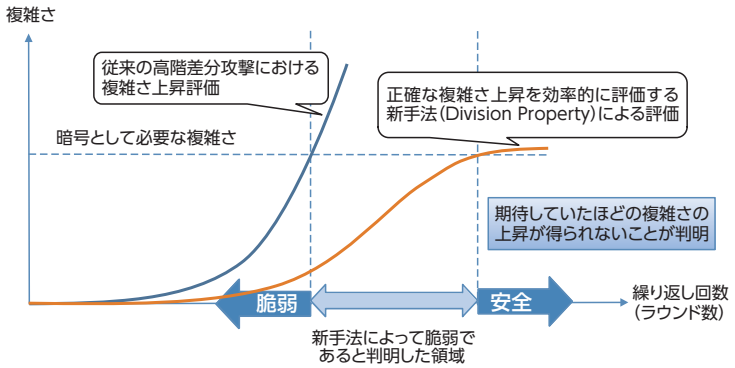


図3　新手法によって従来の安全性評価に問題があったことが判明

ばその暗号は安全、それより少ないラウンド数であれば脆弱だと判断できる。MISTY1のラウンド数は8。「これは従来の評価方法においては処理効率と安全性をうまくバランスさせる絶妙な設定でした。」（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 藤堂 洋介氏）

暗号の複雑さを正確に評価する新方式「Division Property」

しかし高階差分攻撃で使われていた従来の複雑さ評価方法には問題があることを藤堂氏は発見した。「2012年12月頃、鍵の全探索が可能な小規模な自作暗号に対して高階差分攻撃を試す実験をしていたところ、理論的に想定されるものよりも大きなラウンド数の暗号を解読できるケースがあるのに気付きました。当初はなぜそうした現象が生じるのか分かりませんでしたが、2014年1月頃までに全容を解明して新しい評価方法の考案に至りました。」（藤堂氏）

藤堂氏が考案した「Division Property」という新方式によって、ラウンド数を増加させても従来の安全性評価が期待していたほどの複雑さの上昇が得られないことが判明した（図3）。条件によっては、従来評価で安全とされていた暗号が安全ではないと評価されることになる大発見である。藤堂氏は早速、この発見を論文にまとめて暗号国際会議「ASIACRYPT」に投稿した。

しかし結果は不採択。「新理論が出来たという喜びで、それを愚直に論文にしてしまいました。読む側のことを考慮して、過去の手法との関係性や技術の汎用性を説明するなどのブラッシュアップが必要でした。」（藤堂氏）

MISTY1の鍵を全数探索する場合の計算量	Division Propertyによる解読に必要な計算量	Division Propertyによる解読に必要なデータ量
2^{128}	$2^{107.9}$	$2^{63.994}$
	2^{121}	$2^{63.58}$

表1　CRYPTO2015で発表したMISTY1解読の計算量

手直しした論文は別の暗号国際会議「EUROCRYPT」に採択された。

さらに藤堂氏は、この新手法をMISTY1の解読に適用する論文をまとめ上げた。そしてこれが最難関の暗号国際会議「CRYPTO」に採択され、さらに2015年の最優秀論文賞を受賞した。この論文で同氏は、新手法を使用することでMISTY1の解読に必要な計算量を全数探索する場合に比べて大幅に削減できることを示している（表1）。

なお、この論文はMISTY1が暗号学的な意味での安全性を備えていないことを示すものである。表1に挙げた通り、発表された手法による解読には多数のデータ（ここでは平文と暗号文の組を指す）が必要で、これによる解読は現実的なものとは言えない。現時点で直ちにMISTY1の実用上の安全性が失われたわけではないことに注意する必要がある。「MISTY1の現実的な解読方法が考案されるのはまだ先のことでしょう。それまでに次の暗号をじっくり検討して移行の準備を進めることが肝要です。」（藤堂氏）