■1 群（信号・システム）- 3 編（暗号理論）

2 章 ストリーム暗号

（執筆者：田中秀磨）［2008 年 11 月 受領］

■概要■

秘密鍵暗号方式の一つであるストリーム暗号は，ブロック暗号よりも古くから利用されている歴史のある暗号方式である．疑似乱数生成器を利用する方式であることから，ストリーム暗号の開発は，すなわち疑似乱数生成器の開発ということができる．疑似乱数生成器の構成には様々な手法があり，秘密鍵暗号方式のもう一つの方式であるブロック暗号と比較して構成手法についての体系的なまとまりがない．そのような構成手法の背景から，安全性の評価手法も統一的ではない．本稿では，このようなストリーム暗号を運用的な構造を示し，ストリーム暗号用途の疑似乱数生成器に求められる乱数特性，安全性の概要をまとめた．ストリーム暗号は小型軽量実装が可能であることから，様々な電子機器で利用されている．ストリーム暗号の標準化動向をまとめ，最新の安全性評価に関するトピックスを紹介した．

【本章の構成】

■1 群 - 3 編 - 2 章

2-1 ストリーム暗号技術の概要

（執筆者：田中秀磨）[2008 年 11 月 受領]

ストリーム暗号は秘密鍵暗号方式の一つであり，乱数生成器からの出力系列を鍵として扱い，平文と排他的論理和して暗号文を生成する．復号はその逆の処理であり，暗号文に鍵を排他的論理和して平文を得る．厳密には Blum と Goldwasser が提案しているストリーム暗号的な公開鍵暗号方式も存在する[1)]ので，秘密鍵暗号方式のみに分類されるわけではない．

平文長と鍵長が等しく，かつ鍵が真の 2 進乱数生成器からの出力であれば，鍵の全数探索によって暗号文から平文を復元することは不可能である．これは平文と暗号文が確率的に独立になるためであり，このような暗号は Vernam 暗号や One-time Pad と呼ばれる．ストリーム暗号は簡易な Vernam 暗号として，早くから実用化された．更に，共通鍵暗号のもう一方の方式であるブロック暗号と比較すると，誤り伝搬が小さく同期が取りやすいことから，通信における回線暗号装置では好んでストリーム暗号が使われる傾向がある．ISO における物理レイヤ暗号装置に対する相互運用要求事項（IS-9160）では，1 ビットか 8 ビットごとのストリーム暗号を用いるように規定している．またハードウェア実装においては回路規模が小さく，処理速度が速いという特徴をもつ．

ストリーム暗号は，外部同期型と自己同期型に分類される．外部同期型は，平文と暗号文の生成とは独立に外部からの信号により鍵生成器の同期が取られる方式である．ブロック暗号の利用モードの一つである OFB（Output FeedBack）は，ブロック暗号を鍵生成器と見なせば外部同期型ストリーム暗号と見なせる．外部同期型は，送受信者間で完全に同期可能な場合に採用され，再同期が必要な場合のための付加的な仕組みが不可欠である（図 2･1）．

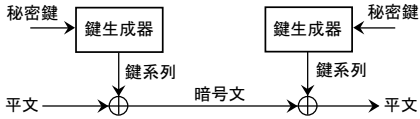

図 2･1　外部同期型ストリーム暗号

これの最大の特徴は誤り伝搬がないことにある．常に送受信者間で同期しているため，削除，挿入，再送といった能動的な攻撃が行われた場合，即座に同期がとれなくなるので，送受信者がすぐに検知することができる．しかしながら，暗号文に対する改ざんが平文に与える影響を攻撃者が知ることができるので，このような攻撃の対策としてメッセージ認証やデータの完全性を確認できる仕組みも必要となる．自己同期型は，同期のずれを自動的に回復する仕組みをもった方式である（図 2･2）．

図中の「鍵生成器+」とは鍵生成器と外部レジスタからの入力を処理する構造とを合わせたものを意味する．暗号文をためておくための外部レジスタをもち，レジスタ長だけの暗号文が誤りなく送信できれば，もし同期がとれなくてもレジスタ内容が一致し同期が回復する．誤りが生じたとしても，最大でもレジスタ長分の伝搬で済む．したがって，削除，挿入といった攻撃が行われた場合，外部同期型と比較して攻撃が行われたのか誤りが生じたのか区別が付きにくい．外部同期型と同様にメッセージ認証やデータの完全性を確認できる仕組みが必

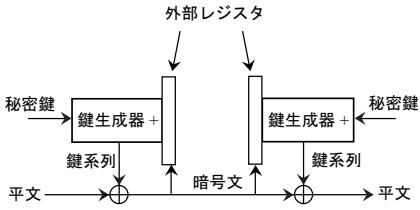

図 2·2　自己同期型ストリーム暗号

要である．なお，ブロック暗号の利用モードである CFB（Cipher FeedBack）は，自己同期型ストリーム暗号の良い例である．

平文系列を $X = (x_1, x_2, \cdots)$，鍵系列を $K = (k_1, k_2, \cdots)$，暗号文列を $Y = (y_1, y_2, \cdots)$ とし，暗号化関数を $e(\cdot)$ とすれば，ストリーム暗号の処理は以下のように書ける．

$$Y = y_1 y_2 y_3 \cdots = e(x_1; k_1) e(x_2; k_2) e(x_3; k_3) \cdots \tag{2·1}$$

これに対してブロック暗号は，暗号利用モードを無視すれば（ECB（Electronic CodeBook）モードであれば）以下のように書ける．ブロック暗号では CBC（Cipher Block Chaining）モードなどでこの問題を解決しているが，誤り伝搬がブロック長単位で影響を受ける一方，ストリーム暗号のように 1 ビット単位でしか生じない．ブロック暗号の利用モードに関する詳細は第 3 章に譲る．

$$Y = y_1 y_2 y_3 \cdots = e(x_1; K) e(x_2; K) e(x_3; K) \cdots \tag{2·2}$$

このように，ブロック暗号では同じ鍵に対して同じ平文を入力すれば，同じ暗号文が得られるが，ストリーム暗号では時刻に応じて鍵の値が異なるため，同じ平文に対して同じ暗号文が得られることは確率的に小さい．

現代暗号方式に対する攻撃手法は，暗号文単独攻撃，既知平文攻撃，選択平文攻撃，選択暗号文攻撃に分類される．ストリーム暗号は時刻の概念があり，平文と暗号文はその前に処理された平文と暗号文に対して独立な関係にはない．したがって，ストリーム暗号を対象とした攻撃手法には，選択平文攻撃と選択暗号文攻撃が含まれないのが普通である．

一般にストリーム暗号では，暗号化関数 $e(\cdot)$ には，排他的論理和が採用されることが多い．

$$\begin{aligned} y_i &= x_i \oplus k_i \qquad \text{・・・暗号化} \\ x_i &= y_i \oplus k_i \qquad \text{・・・復号} \end{aligned} \tag{2·3}$$

ストリーム暗号を式 (2·1) に示せるように，鍵が時刻依存で生成されると定義すれば暗号化，復号は式 (2·3) にこだわらない．例えば算術和を利用するものもある．

■1 群 - 3 編 - 2 章

2-2 疑似乱数生成器とストリーム暗号

（執筆者：田中秀磨）[2008 年 11 月 受領]

Vernam 暗号は暗号文単独攻撃に対して完全な安全性をもつ．しかしながら通信者間で平文と同じ長さの乱数列を安全に共有しなければならない問題が発生する．そこで，適当な長さの乱数の種を秘密鍵として共有し，確定的アルゴリズムで乱数列を生成する疑似乱数生成器を利用するのが一般的である．疑似乱数生成器の構成法は様々であるが，生成される乱数列に対する要求は一貫しており以下があげられる．これらは，特に暗号用にこだわったものではなく，一般に 2 進乱数に求められる性質と同等である．

1. 出力値 0 と 1 の等頻度性
2. 長周期性
3. 予測不能性
4. 連長の出現度数に偏りがないこと
5. 顕著なパターンが発見されないこと

出力値に偏りが生じないことを要求することは，理解に難しくないであろう．疑似乱数生成器は確定的アルゴリズムを採用しているため，必ず周期かある固定の値のみを出力するように収束する．予測不能性とは，次の出力値を予測できないことや，種の値を逆算できないことを意味する．特にストリーム暗号用の疑似乱数生成器には重要な要求事項である．連長の出現頻度やパターン性があることなどは，乱数性を損なう特徴である．これらがどの程度満たされているかの検定法として代表的なものに以下がある．

1. NIST FIPS PUB 140-2 [2)]
2. NIST Special Publication 800-22 [3)]
3. DIEHARD [4)]

これらはいくつかの検定法のセットで構成されている．我が国の電子政府（e-Government）で利用可能な暗号技術のリストアップを目的とした暗号技術評価委員会（CRYPTography Research and Evaluation Committees : CRYPTREC）[5)]では，必要最低限の評価法をリストアップしている．乱数検定に関する詳細は第 11 章に譲る．

以上のような検定に合格する系列を出力できるだけでなく，更に安全性が求められる．ストリーム暗号に対する攻撃方法としては様々なものがあるが，最も汎用性が高く派生型も多い攻撃方法として相関攻撃[6)]があげられる．これ以外にも代数的解読手法や関連鍵攻撃などの攻撃方法にも留意する必要はあるが，以下の観点から安全性が評価される．

1. 非線形性が高い
2. 線形複雑度が大きい
3. 種と出力系列の相関が小さい

非線形性とは，出力間に線形性が成立しないことを意味する．線形複雑度は，ある生成器が出力する系列と同じ系列を出力する LFSR を構成するとすれば，その LFSR は最小何段で構成されるかを示す値である．種と出力系列の相関性は，そのまま相関攻撃への耐性へつな

がる．このように，乱数性と安全性の両方を満たすことがストリーム暗号用途に求められる．このような疑似乱数生成器の構成法として，様々なものが提案されているが大きく二つに分けることができる．

1. LFSR など有限状態機械を利用するもの
2. ブロック暗号技術などを応用したもの

LFSR を用いた疑似乱数生成器は比較的伝統的な構成法であり，90 年代半ばまでは主流であった．これは LFSR に関する研究成果が充実していて，乱数性と安全性の両面で理論的に解析が可能なことによる．ハードウェア実装においても小型実装が可能で安価な傾向があった．FCSR など非線形フィードバックシフトレジスタを利用したものも最近は見られる．ブロック暗号の設計技術を応用したストリーム暗号は近年多く提案されるようになり，状態遷移型と呼ばれることもある．これには SHA-1 などハッシュ関数を内部関数に利用したものも含まれる．最近のブロック暗号は小型実装を重要視しているので，ストリーム暗号としての実装性能の向上にも寄与しているといえる．これら以外にも種々雑多な構成方法があり正確な分類は難しい．

■1 群 - 3 編 - 2 章

2-3 標準化動向など

（執筆者：田中秀磨）[2008 年 11 月 受領]

暗号技術全体の標準化に関する詳細は第 15 章に譲るが，ストリーム暗号の標準技術を定めている主な機関として以下があげられる．

- ISO
- CRYPTREC
- ETF
- eSTREAM [7)]

各機関で標準技術として採用されているものを表 2･1 に示す．

表 2･1　ストリーム暗号の標準（推奨）アルゴリズム

ISO	SNOW2.0, MUGI, MULTI-S01	
CRYPTREC	MUGI, MULTI-S01	
IETF	RC4	
eSTREAM	SW	HC-128, Rabbit, Salsa 20/12, SOSEMANUK
	HW	Grain v1, MICKEY v2, Trivium

eSTREAM は，ヨーロッパで行われているストリーム暗号評価活動である．学術成果主体の研究プロジェクトであることから正確には標準化機関ではないが，この中では最も新しい選定作業を行った結果である（2008 年）．ソフトウェア実装向き（SW）とハードウェア実装向き（HW）と，実装を意識した選定を行ったという特徴がある．

ISO，CRYPTREC，IETF はストリーム暗号を実装する暗号モジュール製品に大きい影響をもつ．特に IETF はインターネットの SSL 機能や無線 LAN の暗号化機能の標準を決定しているため，結果的に RC4 はストリーム暗号として最も普及しているといえる．無線 LAN の暗号化方式の一つである WEP で利用されている RC4 は古くから安全性評価が活発に行われ，問題点を多く指摘されてきた．最近では一般的な PC を利用して約 10 秒で解読できる攻撃結果が得られている．暗号アルゴリズムのぜい弱性だけでなく，実装運用の面でのぜい弱性により安全に利用できなくなる場合もあるので注意が必要である[8)]．

ISO 及び CRYPTREC（電子政府推奨暗号リスト，2003 年公開）で採用されている MUGI[5)]及び MULTI-S01[5)]は日立製作所が開発したストリーム暗号であり，ブロック暗号の技術を応用した状態遷移型の構造をもつ．MULTI-S01 はメッセージ認証コード機能を有する特徴がある．このように，暗号化機能だけでなく，付加機能をもつものも提案されてきている．また，ストリーム暗号は小型軽量実装に向いたものであることから BROUILLARD（三菱，ただし仕様は公開されていない），Enocoro（日立）[9)]，K2（KDDI）[10)]など，新たな小型高速実装を目指したものも多く提案されてきている．これらは携帯電話アプリへの実装や，RFID など小型デバイスへの利用を想定にしている．このような状況から，ISO では軽量暗号（ストリーム暗号に限定していない点に注意が必要であるが）という技術カテゴリの新設が提案され，標準化活動が開始されている．

ディジタルデータのやりとりが複雑化するにつれて，守るべき情報の性質や実装性能の関

係から適切な暗号アルゴリズムを選ぶことが重要になりつつある．このような状況からストリーム暗号を利用するのに適当と考えられる場面も多くなっている．各暗号技術の特徴をよくとらえ，適切なアルゴリズム選択と安全な実装を行うことが求められている．

■参考文献

1) M. Blum and S. Goldwasser, " An efficient probabilistic public-key encryption scheme wich hides all partial information, "Springer Verlag, Advances in Cryptology Proceedings of CRYPTO 84, LNCS 196, pp.289-299, 1985. .
2) NIST, " FIPS PUB 140-2 Security requirement for cryptographic modules "
3) NIST, " Special Publication 800-22 A Statistical Test Suite For Random and Pseudorandom Number Generators for Cryptographic Applications, " 2001.
4) G. Marsaglia, " DIEHARD, " http://stat.fsu.edu/pub/diehard/
5) CRYPTREC, http://www.cryptrec.go.jp/
6) N. Courtois and W. Meier, " Algebraic Attacks on Stream Ciphers with Linear Feedback, "Springer Verlag, Proceedings of EUROCRYPT 2003, LNCS 2656, pp.345-359, 2003.
7) eSTREAM, http://www.ecrypt.eu.org/stream/
8) 寺村亮一, 曽谷紀史, 仲神秀彦, 朝倉康生, 大東俊博, 桑門秀典, 森井昌克, " WEP の現実的な鍵導出法（その 2）, " 情報処理学会，CSS2008 予稿集 pp.421-426, 2008.
9) D. Watanabe, K. Ideguchi, J. Kitahara, K. Muto, and H. Furuichi, " Enocoro-80: A Hardware Oriented Stream Cipher, "IEEE, Third International Conference on Availability, Reliability and Security 2008 (ARES 08), pp.1294-1300, 2008.
10) S. Kiyomoto, T. Tanaka and K. Sakurai," K2 Stream Cipher, "Springer, E-business and Telecommunications, Communications in Computer and Information Science vol.23, pp.214-226, 2007.