経済産業大臣賞

超高速ストリーム暗号KCipher-2の研究開発

株式会社KDDI 研究所　情報セキュリティグループ

清本 晋作　田中 俊昭

九州大学

櫻井 幸一

1. 緒　言

インターネットやモバイルネットワークのブロードバンド化に伴い、大容量、高速なデータの伝送サービスが発展するとともに、高精細な動画像や個人情報など左記のサービスで扱われるデータの付加価値がますます高まっている。このような中、個人情報の漏えいや、ディジタルコンテンツに不正コピーなどの問題も顕在化しており、本課題を解決する技術として、暗号技術は不可欠である。また、ネットワークに接続される端末は、PC に加え、携帯電話、スマートフォン、タブレットなどの通信機器、ゲーム機、ディジタルテレビ等の情報家電、さらには、スマートグリッドでの各種センサーデバイスと多様化の一途を辿っており、センサーのようなローエンドな環境においても、高速に動作する暗号技術が必要となってきた。

現在、AES と呼ばれる米国発の暗号方式が一般的に用いられているが、今後のさらなるネットワークの高速化やデバイスの多様化にともない、あらゆる環境において高速に動作する暗号技術が喫緊の課題となっている。そこで、筆者らは、従来の AES と比較して最大 10 倍高速動作する世界最高レベルを達成し、かつ、高い安全性を確保した暗号方式KCipher-2の研究開発を行った。本方式は、2011年に国際標準機関ISO/IEC において規格化され国際標準となっている。

2. 研究の目的と進め方

インターネットの普及により、人類にとって暗号技術は、身近なものとなった。暗号技術といえば主に軍事目的であったものが、インターネット上でのオンラインショッピングなどにより、利用者の情報を守り、生活を支える大切なインフラ技術となったのである。しかし、暗号技術は、元来、安全性と処理コストは、いわばトレードオフの関係にあり、そのトレードオフを打破し、速くて安全な暗号技術を研究開発することは、暗号研究者にとって宿願とされてきた。特に、暗号が様々な環境での利用が想定されるに到り、暗号アルゴリズムの性能面に対する要求はより厳しくなっている。例えば、携帯端末は既に従来のコンピュータの置き換えとして普及しており、さらには近い将来、センサーやロボット、自動車などの各種装置、利用者がもつ端末が通信を行なう M2M(Machine to Machine) サービスが実現すると予想されており、あらゆる環境で高い性能を発揮する暗号方式が求められている。

暗号方式は、まず使用する鍵により、公開鍵暗号と共通鍵暗号に大別される。共通鍵暗号方式は、同じ鍵で暗号化・復号を行う方式であり、“合言葉(鍵)”を知らないものは、暗号化も復号もできない。共通鍵暗号は、公開鍵暗号と比較すると数十倍高速であるため、データの暗号化に主に利用される。例えば、インターネットで使用されている TLS 通信[6] では、まず公開鍵暗号で共通鍵暗号に使用する鍵を安全に交換し、実際に送受信するデータは共通鍵暗号で暗号化・復号する。共通鍵暗号方式は、さらに、ブロック暗号とストリーム暗号の２つの方式に分類される。ブロック暗号は、データが入力される都度同様の処理を行うのに対し、ストリーム暗号は、前回の処理結果を引継いで次の処理を行うことによって１つ１つの処理を軽量化しようという手法である(図１)。

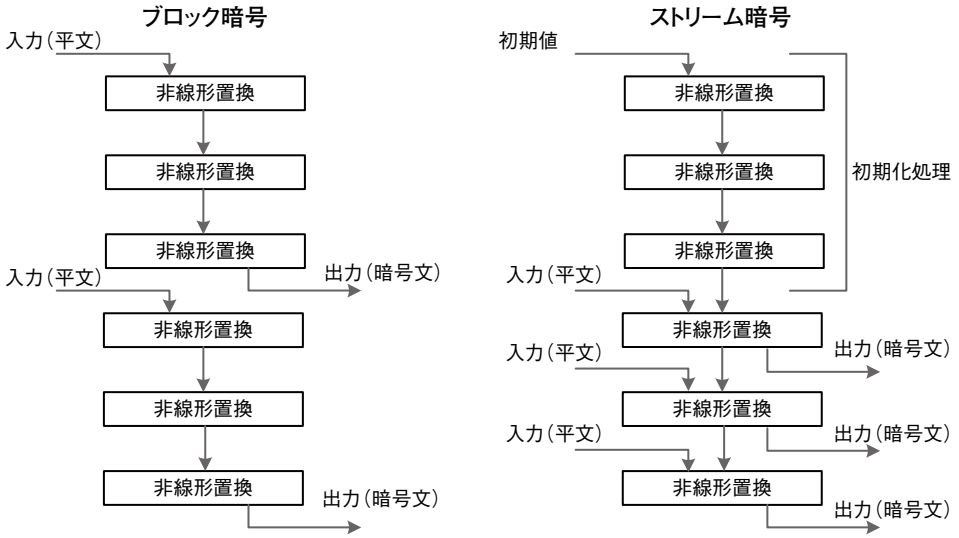

図1

2004年の研究開始当初、共通鍵暗号の研究の主流は、ブロック暗号であり、ストリーム暗号は設計方針や安全性評価が十分に定まっていない状況であった。特に、米国標準暗号であるAESがデファクトスタンダードとして君臨していた。しかしながら、ブロック暗号の設計を見直しても、これ以上の高速化は期待できないほどに技術が洗練されつつあった。一方で、我々は、従来方式よりも一桁速い暗号方式を実現する、という野心的な目標を掲げていた。この目標は、数年先の技術を想定したとしても十分競争力のある方式とするという考えと、当時の携帯端末では、暗号化処理は非常にコストがかかり、マルチメディアコンテンツなど大容量データの暗号化は従来の暗号方式では困難であったというニーズから導き出されたものである。実際、有料放送サービスを携帯電話に提供する場合には、リアルタイムに暗号化された放送データを復号しつつ再生しなければならないが、当時の技術では実現が困難であり、専用のハードウェアを実装するなどの手段に頼らざるを得なかった。上記の目標を達成するために、大幅な性能向上が難しいと考えられるブロック暗号ではなく、ストリーム暗号をターゲットとして研究開発を開始することとなった。

まずは、従来方式の調査と問題点の検証から開始した。従来方式の主流となっていたのは、周期的な乱数を生成する部分と、非線形関数によってその乱数を変換して出力する部分の2つから構成されるストリーム暗号であった。これらの方式の問題点は、周期的な乱数を生成する部分の規則性(線形性)にあり、この規則性を利用して解読されている事例が散見された。一方で、ソフトウェア実装において、高速にストリーム暗号を実現する手法については、徐々に研究成果が出始めている時期であった。我々は、ビット単位での演算をワード(32bits)単位での演算に拡張するというソフトウェア高速実装手法を早期に確立するとともに、上記の規則性の問題について、処理速度を落とす事無く改善する手法を考案できれば、高速かつ安全なストリーム暗号が実現できると考えた。ソフトウェア高速実装手法については、アルゴリズムの設計を支援する様々な設計ツールを開発し、試行錯誤しつつ設計手法を確立し

た。また、規則性の問題を解決するため、毎回計算する関数が制御信号に従って選択されるDynamic Feedback Shift Register (DFSR) という新たな手法を考案し、速度の低下を最小限に抑えつつ、安全性を向上させた。

KCipher-2 アルゴリズムは、2006年には一旦完成し、安全性評価、性能評価を十分に行った後に、2007年に国際会議で発表した。その後、ISO/IEC JTC1 SC27 WG2 に国際標準暗号として提案を行い、2011年 12月には国際標準[5] となった。KCipher-2 は、以下の特徴を有する共通鍵暗号方式である。

・高速性：従来の方式と比べて高速かつ軽量である。例えば、米国標準暗号AES[2] と比較すると 5-10倍高速である。
・安全性：独自構造の採用により安全性を向上させている。CRYPTREC[3] 等の第三者評価[4] により、鍵長の 2倍以上の安全性を有することが確認されている。
・汎用性：排他的論理和、算術加算、テーブル参照等の基本的な演算のみから構成され、あらゆる環境に適用可能で、かつ十分な性能を発揮する。

3. ストリーム暗号 KCipher-2

本節では、ストリーム暗号KCipher-2 について説明する。まず、KCipher-2 の設計について論じ、次いで性能評価、安全性評価の結果について述べる。

3. 1　KCipher-2 アルゴリズム

KCipher-2 アルゴリズムの概要を図 2 に示す。

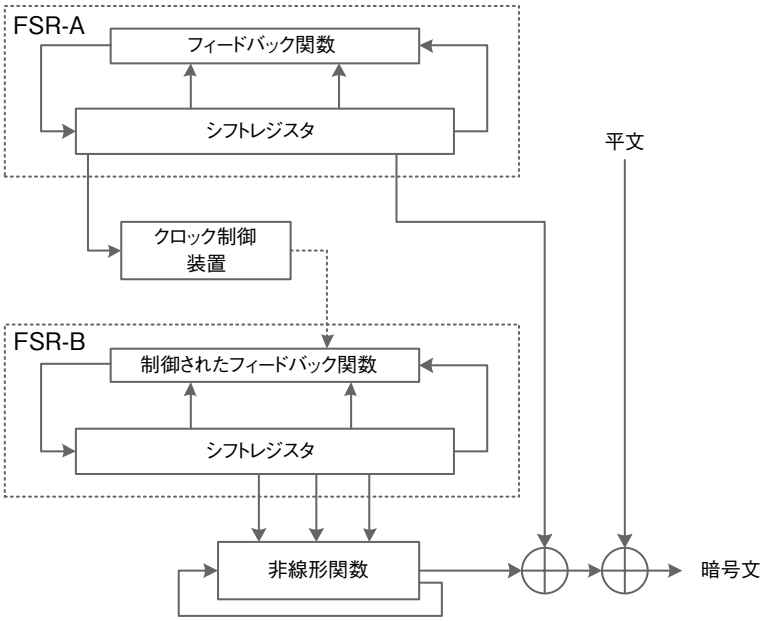

図2　ストリーム暗号KCipher-2

アルゴリズムは、乱数系列を生成する 2 つのシフトレジスタ、FSR-A, FSR-B と、出力される乱数列に非線形要素を導入する非線形変換部から構成される。以下にそれぞれの設計方針、方式、特性を順に説明する。

3. 1. 1　FSR-A

FSR-A を導入した理由は、理論的に周期が保証された乱数系列を生成するためである。従って、FSR-A は 32bit レジスタとする線形フィードバックシフトレジスタとして構成される。線形フィードバックシフトレジスタは、以下の式のように記述されるものであり、生成する乱数列は長周期であることが保証される。具体的には、32bits のレジスタ 5個で、160bits のデータを保持するため、最大周期である 2^{160} の周期を持つ。

$$f_A(x) = \alpha_0 x^5 + x^2 + 1 \in GF(2^{32})[x]$$

ここで α_0 は 32bit から 32bit への変換を与える。KCipher-2 では、この変換において事前計算されたテーブルを用いることにより、高速な処理を実現している。従来、各レジスタが 1 ビットである線形フィードバックシフトレジスタが用いられてきたが、ソフトウェア実装では低速になることが知られていた。そこで、新たに考案されたソフトウェア向けの構成法を改良することにより、上記のフィードバックシフトレジスタを設計した。

3. 1. 2　FSR-B

FSR-B は、線形フィードバックシフトレジスタの Feedback 関数を FSR-A からの出力に従って動的に変更する Dynamic Feedback Shift Register（DFSR, 動的フィードバックシフトレジスタ）という形式を取る。DFSR とすることにより、従来は一意に決定されていた Feedback 関数が複数の関数から選択されるため、攻撃者が予測不可能となり安全性を向上させることが出来る。また、KCipher-2 が使用する DFSR は、後述するようにテーブル変換によって構成可能であるため、速度低下を最小限に抑えることが出来る。フィードバック関数を決定する 2 つの制御信号、*cl*1、*cl*2 は LFSR-A のレジスタ値から 2 ビットを選択して用い、表 1 のように Clock Controller により決定される。

表1　FSR-Bの動的フィードバックシフトレジスタの動作

*cl*1	*cl*2	フィードバック関数
0	0	$f_B(x) = \alpha_2 x^{11} + x^{10} + x^5 + x^3 + 1$
0	1	$f_B(x) = \alpha_2 x^{11} + x^{10} + x^5 + \alpha_3 x^3 + 1$
1	0	$f_B(x) = \alpha_1 x^{11} + x^{10} + x^5 + x^3 + 1$
1	1	$f_B(x) = \alpha_1 x^{11} + x^{10} + x^5 + \alpha_3 x^3 + 1$

攻撃者は、攻撃を行う際には、まずどのフィードバック関数が使用されているのかを予測しなければならず、攻撃に要するコストはその分増大する。従って、この動的フィードバックシフトレジスタによって安全性は飛躍的に向上する。

3. 1. 3　非線形変換部

図 3 に非線形変換部の構成を示す。非線形変換部は、FSR-A の 2 つのレジスタと、FSR-B の 4 つのレジスタ、さらに、4 つの 32bit 内部メモリから Keystream を導出する。FSR-A、FSR-B から取得するレジスタは、Full Positive Difference Set [7] と呼ばれる規則に従って選択されている。非線形変換部は、内部処理として Sub 変換を持つ。Sub 変換については、十分に評価されており、多くの暗号で使用されているものと同様の変換処理を使用することで、信頼性を確保する。また、非線形変換部が、独自の結線構造によって Sub 関数を介して接続された 4 つの内部メモリ、R1、R2、L1、L2 を有することにより、代数攻撃等に対する安全性を向上させている。この独自に考案した八の字構造により通常の 2 倍の長さの乱数列を出力することが可能となり、KCipher-2 の安全性を向上させつつ、処理速度も同時に向上させることができた。

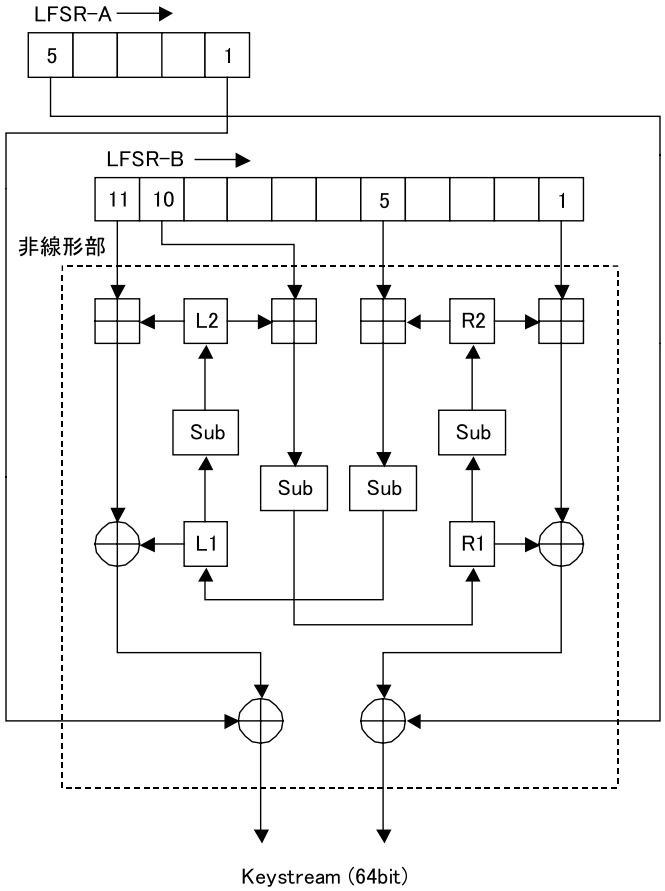

図3　非線形変換部の構成

3. 2　性能評価結果

ストリーム暗号KCipher-2 の性能評価結果について表 2、表 3 に示す。表 2 は、ソフトウェア実装評価結果であり、表 3 は、FPGA 実装による評価結果である。鍵系列生成処理とは、暗号化・復号のためのビット列を生成する処理であり、cycle/byte は、1 バイトのデータを暗号化するのに必要とするサイクル数を表している。一般的に、CPU のクロック数に依存せずに暗号アルゴリズムの処理性能を表すために、この cycle/byte という指標を用いる。(1byte=8bit であるため)8 をこの値で割って、CPU のクロック数を掛ければ、その環境での最大スループットが計算できる。例えば、Core i7 のケースでは、KCipher-2 は 3.50cycle/byte の処理性能を達成しており、CPU のクロック数が 3.4GHz だとすると、約 7.8GBps のスループットを達成することが出来る。AES-NI とは、最新の CPU に用意された特殊な演算命令である。本来、AES 向けに実装されたものであるが、KCipher-2 にも一部適用可能である。AES の性能が 18－ 24cycle/byte であるため、ソフトウェア実装評価の結果から、KCipher-2 は、AES と比較して 5倍以上の処理速度を実現していることがわかる。また、携帯電話を用いた評価では、暗号化処理のスループットが、AES が 14Mbit/s に対して、KCipher-2 が 130Mbit/s であった。プログラマブルなハードウェアである FPGA における評価では、標準実装と､2つの高速実装を評価した。高速実装では、最も高い高速実装 1 が最も効率性が高く、22.06Slice/Mbps を実現した。また、高速実装 2 では、約 17GBps の処理性能を実現した。

表2　ソフトウェア実装評価結果

CPU	初期化処理（cycle）	鍵系列生成処理（cycle/byte）
Core i7 with AES-NI	561	2.88
Core i7	694	3.50
Core 2	860	4.01
Pentium 4	1162	4.87
Pentium III	1194	5.40

表3　ハードウェア実装評価結果

	最大動作 周波数	スループット (Mbps)	回路規模 (Slice)	効率性 (スループット/回路規模)
標準実装	95.630	6120	1214	5.04
高速実装 1	252.398	16153	732	22.06
高速実装 2	271.150	17354	813	21.34

3.3 安全性評価結果

本節では、安全性評価結果について述べる。ストリーム暗号に対する攻撃手法は、EU における ECRYPT プロジェクトなどを通して、近年急速に体系化され、いくつかの典型的な攻撃手法に集約された。従って、KCipher-2 に対する安全性評価についても、典型的な攻撃手法について評価を行うと共に、DFSR の効果についても考察する。評価結果を表 4 にまとめる。推測決定攻撃 [8] は、いくつかのレジスタの値を推測し、その値を利用することで他のレジスタの値を推測する攻撃手法である。計産量は、2^{320} となっており、現在のところ、KCipher-2 に対するもっとも効率の良い攻撃手法となっている。識別攻撃 [9] は、出力鍵系列のビット間に成立する線形式を利用して、真の乱数と出力された鍵系列を識別する攻撃手法である。FSR-A をすべて推測し、識別攻撃を実施した場合、FSR-A を推測するのに要した計算量を無視したとしても 2^{515}程度の計算量を要する。また、FSR-A を推測せずに識別攻撃を実施した場合には、攻撃可能な計算量で成立する線形式を見出せなかった。また、代数攻撃 [10] は、KCipher-2 には直ちに適用できない。Coutois らの方式 [11] により、代数的攻撃の計算量の見積りを行うと 2^{646} である。DFSR の導入により、推測決定攻撃、識別攻撃においては FSR-A を推測せずに、攻撃することは事実上困難となっており、代数的攻撃においては、攻撃に要する計算量が、DFSR がない場合と比較して 2^{160}倍以上となる。従って、DFSR が効率的に安全性を向上させていると判断できる。また、表 4以外の攻撃についても、検証しているが有効な攻撃は発見されなかった。これは、CRYPTREC による第三者評価においても同様の指摘がされている。初期化処理についても、13回目の空回しによって、すべてのレジスタに鍵並びに初期値(IV)が拡散することが確認されており、それから更に 2 つの FSR の長さ以上の 11回の空回しを行う初期化処理は十分安全であると考えられる。

最良の攻撃である推測決定攻撃の計算量が 2^{320} であり、鍵の全数探索による攻撃の計算量 2^{128} と比較して、鍵長に換算して 2倍以上の差がある。従って、セキュリティマージンが十分であると考えられ、標準暗号として長期間の使用にも耐えうると判断できる。なお、AES については、既に鍵の全数探索を下回る計算量で攻撃可能な手法[12](計算量は、2^{126})が提案されている。

表4　安全性評価結果

	計算量
推測決定攻撃	2^{320}
識別攻撃	$> 2^{515}$
代数的攻撃	2^{646}

4. 利用実績

筆者らが考案した KCipher-2 の有効性を実証するため、2007年に本方式を携帯電話のワンセグサービスに実装し検証した。実験システム構成を図 5 に示す。ワンセグの試験放送用設備で KCipher-2 を用いて暗号化したコンテンツを受信側の携帯電話で、受信してリアルタイムに復号可能であることを確認した。ワンセグサービスは現在、放送波は暗号化されていない。ワンセグサービス開始時から、地上波とのサイマル放送のみであり画質が地上波と比較して高精細でない点に加え、携帯電話の性能上リアルタイムでの復号処理が困難であると考えられていたためである。本実験において KCIpher-2 を用いることにより、400Kpbs 程度のワンセグのスループットの復号処理を携帯電話の CPU 負荷 0.5% 程度で、達成できることを確認した。KCipher-2 は、携帯端末向け放送規格である MediaFLO の日本サービスにおいても、暗号方式としても規格に盛り込まれた。

図5　ワンセグ動画リアルタイム復号アプリ

また、実サービスの採用実績としては、官公庁系の携帯電話を用いた情報通信システムにおける携帯電話のデータをセンター側の設備に送信する際の暗号化機能、スマートフォンのファイル暗号化ソフトでの利用、医療用画像を緊急時に携帯電話に送信するシステム、衛星を用いた可搬型のセキュアな映像伝送システム、大容量動画像伝送システム、商用マルチメディアコンテンツサービスなど多岐にわたっている。また、図 6 のようなソリューションビジネスにも積極的に活用されている。KCipher-2 は、日本発の国際標準技術として、国際的な競争力を有する暗号技術であり、今後もさらなる普及展開が見込まれる。

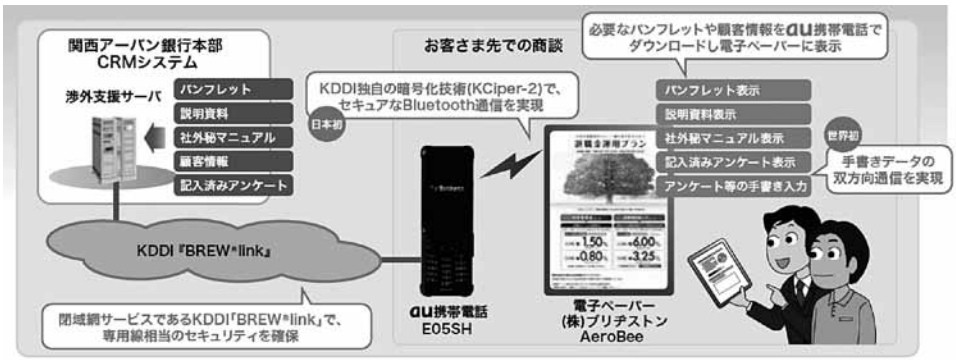

図6　ソリューションビジネスの例[13]

5. まとめと今後の展開

本稿では、ストリーム暗号KCipher-2 の設計、安全性評価、及び実装評価結果について述べた。KCipher-2 は、米国標準暗号AES と比べて数倍高速な処理を実現しながら、鍵長に対して、2倍以上のマージンを有する安全性の高い方式を実現している。KCipher-2 は、ストリーム暗号の国際標準である ISO/IEC 18033-4 に採択されており、IETF 等の標準化団体においても、標準化に向けた審議を行っている。また、KCipher-2 は、アルゴリズムそのものについては、ライセンスフリーで使用することが出来る。その高い性能と安全性から、KDDI 株式会社が提供する商用マルチメディアコンテンツサービスや官公庁向けソリューションサービスの暗号方式としても採用され、KDDI 株式会社以外の会社においても自社製品の暗号方式として採用されている。現在、大量データの国際間伝送やデータセンター事業など、世界市場を狙っての普及展開も検討中である。ISO 国際標準であり、性能、安全性の双方で国際競争力のある KCipher-2 は、日本製品が海外に出ていくときの強力な武器として今後貢献していくものと考えられる。

参考文献

[1] S. Kiyomoto, T. Tanaka, and K. Sakurai, "K2: A stream cipher algorithm using dynamic feedback control," In Proc. of SECRYPT 2007, pp.204-213, 2007.

[2] NIST, "ADVANCED ENCRYPTION STANDARD (AES)," FIPS-PUB 197, 2001.

[3] Cryptography Research and Evaluation Committees (CRYPTREC), http://www.cryptrec.go.jp/

[4] A. Bogdanov, B. Preneel, and V. Rijmen, "Security Evaluation of the K2 Stream Cipher," 2011, available at http://www.cryptrec.go.jp/estimation/techrep_id2010_2.pdf.

[5] ISO/IEC 18033-4 Ed.2, "Information technology, Security techniques, Encryption algorithms, Part 4: Stream ciphers", 2011.

[6] IETF, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246, 2008.

[7] J. D. Golic, "On security of nonlinear filter generators," In Proc. of FSE'96, LNCS, volume1039, pp. 173-188, 1996.

[8] P. Hawkes and G. G. Rose, "Guess-and-Determine Attacks on SNOW," In Proc. of SAC 2002, LNCS, volume 2595, pp. 37-46, 2002.

[9] K. Nyberg, and J. Wallen, "Improved linear distinguishers for SNOW 2.0," In Proc. of FSE 2006, LNCS, volume 4047, pp. 144-162, 2006.

[10] O. Billet, and H. Gilbert, "Resistance of SNOW 2.0 against algebraic attacks," In Proc. of CT-RSA 2005, LNCS, volume 3376, pp. 19-28, 2005.

[11] N. Courtois, "Algebraic attacks on combiners with memory and several outputs," In Proc. of ICISC 2004, LNCS, volume 3506, pp. 3-20, 2004.

[12] A. Bogdanov., D. Khovratovich, and C. Rechberger, "Biclique Cryptanalysis of the Full AES," Proc. of ASIACRYPT 2011, LNCS, volume 7073, pp.344-371, 2011.

[13] KDDI 株式会社HP, http://www.kddi.com/business/case_study/kansaiurban/index.html