01−01039

WEP 方式と互換性を有する高速・低消費電力・暗号強度強化型暗号の開発

代表研究者　佐　藤　友　暁　弘前大学総合情報処理センター助教授
共同研究者　深　瀬　政　秋　弘前大学理工学部教授

概要

公衆無線 LAN において一般的に使用されている暗号である WEP 方式は脆弱性が指摘されている。本研究では WEP（Wired Equivalent Privacy）方式と互換性を有しながら高速・低消費電力・暗号強度が高い暗号を開発することを目的として，この暗号開発に不可欠なウェーブパイプライン方式 PRNG（Pseudo-Random Number Generator）の開発をおこなう。この擬似乱数発生器は 1.2μm C-MOS テクノロジィを用いたチップの開発とプログラマブルデバイスである CPLD（Complex Programmable Logic Devices）の両方で実現する。ゲートレベルシミュレーションの結果，ウェーブパイプライン方式 PRNG は，従来のレジスタを使用した PRNG と比較して高速かつ低消費電力で動作することを示す。加えて，ウェーブパイプライン方式 PRNG は，動作クロックをコントロールすることで容易に擬似乱数製整列を変更することが可能であること検討する。

1　はじめに

今日，公衆無線 LAN のアクセスポイントの設置広がっている。我々はこの公衆無線 LAN を通じて，世界中の空港やホテル，コーヒーショップ等の様々な場所でインターネットへのアクセスが可能である。無線 LAN は電波を用いてデータを送受信するため，データの盗聴を防ぐ上で暗号化が必要である。

公衆無線 LAN 上の暗号方式は，一般的に WEP（Wired Equivalent Privacy）方式が用いられている。しかし以下の問題等により暗号強度が低いと指摘されている[1][2]。

・暗号に使う鍵長が短い
・初期化ベクタが 24bit と短い
・非公開の RC4 のアルゴリズムが解読されている

この暗号方式の脆弱性を改善することを目的として，IEEE802.1x，WPA（Wi-Fi Protected Access)，IEEE802.11I が規格化されている。しかし無線 LAN のクライアント側の設定が複雑であり，クライアント側でそれらの方式に対応していない機器が存在する。このため公衆無線 LAN においては EEE802.1x，WPA，IEEE802.11I の普及が進んでいない。さらに暗号を設定されていない公衆無線 LAN も存在する。

無線 LAN 上で暗号方式を用いることは，暗号のエンコードとデコード処理の実行によってスループットの低下と消費電力の増大をもたらす。この傾向は暗号強度が高くなるにつれて顕著になる。公衆無線 LAN では，バッテリで駆動するノート PC を用いた接続が多いため，消費電力は考慮される必要がある。さらに新たな暗号方式の導入は，従来の無線 LAN クライアントとの互換性の問題から普及が進まない。

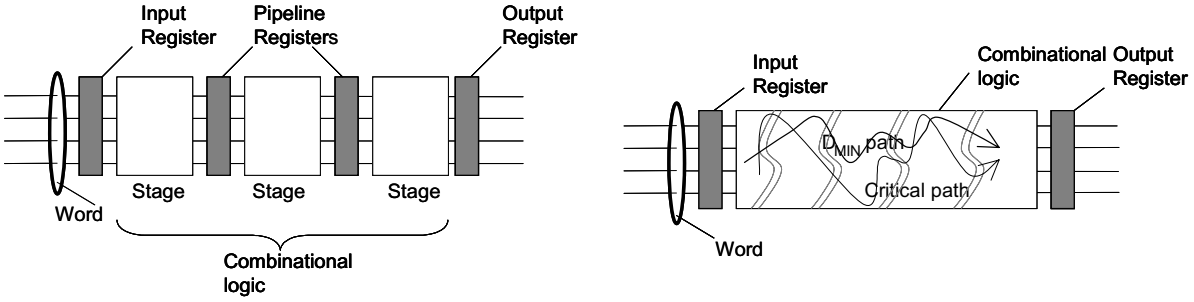
本研究開発では無線 LAN で使用する暗号の脆弱性の解決と普及に不可欠な，WEP 方式と互換性を有し，高速・低消費電力で動作する暗号アルゴリズムの実現を目的として，ウェーブパイプライン方式を用いた PRNG（Pseudo-Random Number Generator）を 1.2μm C-MOS テクノロジィとプログラマブルデバイスである CPLD（Complex Programmable Logic Devices）を用いて設計と製作をおこなう。プログラマブルデバイスを用いて設計する理由は，不正侵入を防御するためのシステム[3],[4]において必要なためである。ゲートレベルシミュレーションによって従来方式の PRNG と比較し，ウェーブパイプライン方式の優位性をしめす。さらに動作クロックをコントロールすることで容易に擬似乱数生成列を変更することが可能であること検討する。

2　ウェーブパイプライン技術

高速化と低消費電力化を両立するための設計手法の一つとして，レジスタを用いずにパイプライン動作が可能であるウェーブパイプライン手法があげられる。ウェーブパイプライン手法は，Maximum Rate Pipeline[5]とも呼ばれるとおり，最大レートでパイプライン動作を行い[6]-[8]，パイプラインレジスタを使用しないため，消費電力が従来のパイプライン手法と比較して減少する特徴を有する[9]。

ウェーブパイプライン手法を用いるプロセッサは，商用ベースではサン・マイクロシステムズの Ultra SPARC III の SRAM の制御といった単純な構造の回路[10]，研究レベルでは加算回路[11]，乗算回路[12]といった単機能な回路で，最近になってようやく多機能回路であるスーパースカラプロセッシングユニット[13]が実現されたのみである。これらはすべて組み合わせ論理回路であり，PRNG で必要となる順序回路は実現されていなかった。このため我々は，PRNG を構成する最小単位の LFSR（Linear Feedback Shift Register）回路のウェーブパイプライン化を行った[14],[15]。

クロック周波数の設定に応じたウェーブパイプライン化回路の設計法を説明するため，従来方式と比較したウェーブパイプラインの同期方式を**図 1** に示す。組合せ回路の信号経路には遅延時間のばらつきがあるので，あるクロックで取り込まれる 1 組の信号の中で高速な信号は，直前のクロックで取り込まれた遅い信号に追突する可能性がある。**図 1** (b)に示すウェーブパイプラインの組合せ回路では，全ての信号経路の遅延時間をクリテカルパスの遅延時間に近づけることによりこの問題を解決している。**図 2** に遅延時間と論理震度の関係，**表 1** にウェーブパイプラインと従来のパイプラインの定性的な比較を示す。設計に要する労力の評価は，ウェーブパイプライン特有の CAD ツールが充実していない現状から判断したものである。



(a)　従来のパイプライン　　(b)　ウェーブパイプライン

図 1　パイプラインの同期方式

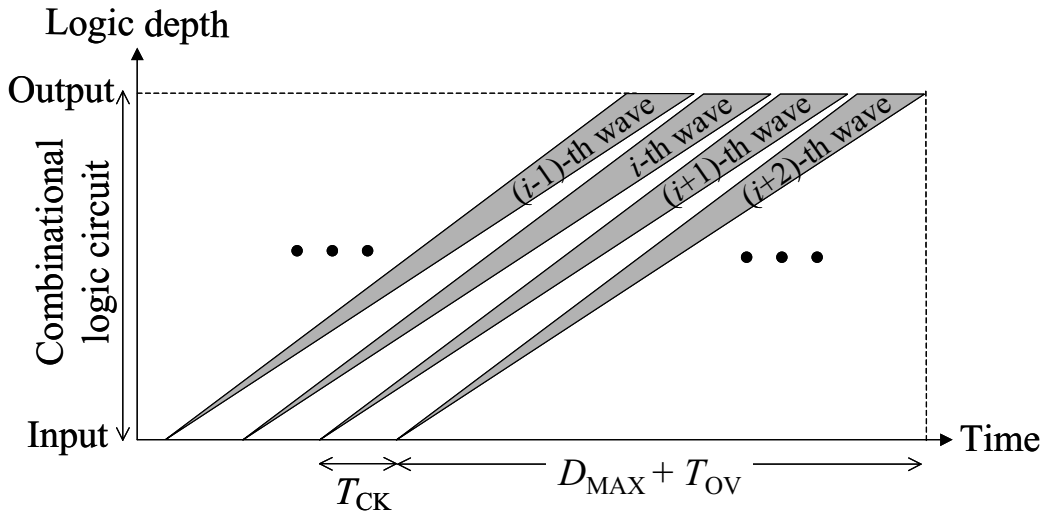


図 2　図 1 (b)に対するウェーブモデル

表 1　ウェーブパイプラインと従来のパイプラインの現状比較

Pipeline	Clock	Area	Designing efforts
Wave-pipeline	Fast	Small	Cumbersome
Conventional pipeline	Moderate	Moderate	Moderate

図 1 (b)から分かるとおり，組合せ回路内に前後して放出される信号間の衝突の回避がウェーブパイプライン化の条件である。この条件下で信号の放出頻度，すなわち，クロック速度が上限の値をとる時に，ウェーブパイプラインの処理効率は最大となる。よって，クロック周期に関して，

$$T_{CK} > (D_{MAX} - D_{MIN}) + T_{OV} \quad (1)$$

$$T_{OV} = T_S + T_H + 2\Delta_{CK} \quad (2)$$

$$D_{MAX} = D_{max} - (T_H + T_S) \quad (3)$$

$$D_{MIN} = D_{min} - (T_H + T_S) \quad (4)$$

なる関係を得る[7]。ここでは，

T_{CK}：クロック周期

T_{OV}：オーバーヘッド時間

T_H, T_S：**図 1 (b)**の入出力レジスタのセットアップ時間，ホールド時間

Δ_{CK}：**図 1 (b)**の入出力レジスタ間のクロックスキュー

D_{MAX}, D_{MIN}：**図 1 (b)**の組合せ回路の最大，最小遅延時間

D_{max}, D_{min}：**図 1 (b)**の入出力レジスタ間の最大，最小遅延時間

である。

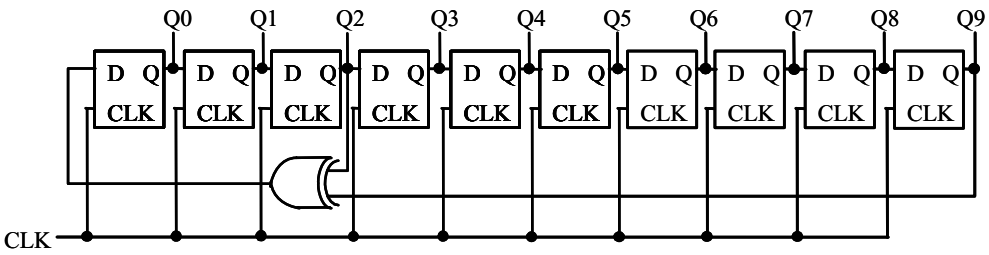
3　ウェーブパイプライン方式PRNG

3.1　LFSR

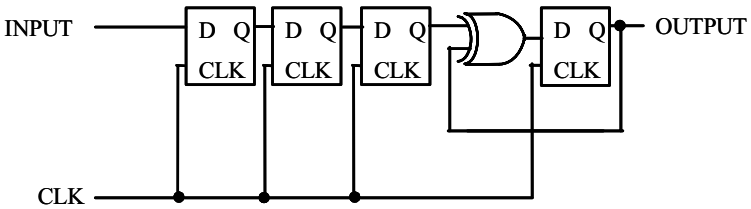
LFSR 回路は**図 3** に示すとおり，EX-OR で帰還をかけたシフトレジスタにより構成される。**図 3 (a)**の PRNG 回路と**図 3 (b)**の CRC 回路 は両方とも LFSR 回路に分類される。CRC（Cyclic Redundancy Check）は WEP のエンコードとデコード組み込まれ，イーサネットフレームのパリティチェックに用いられる処理である。PRNG は WEP の初期値生成に必要とし，24個のレジスタで構成されている。イーサネットフレームを処理する CRC-32 は32個のレジスタで構成されている。レジスタは常に動作するクロック信号を用いて動作するため，電力を消費する原因となる。

3.2　CPLD による PRNG 回路の設計

表 2 に設計環境，**図 4** に従来方式の PRNG とウェーブパイプライン方式 PRNG の論理回路を示す。ウェーブパイプライン手法は，レジスタの使用以外の方法で遅延時間を調整する必要がある。このため，我々は**図 4 (b)**に示すようにバッファを挿入することで遅延時間の調整を行っている。



(a)



(b)

図 3　LFSR 回路　(a)　PRNG　(b)　CRC

表 2　CPLD を用いた設計環境

Function	Name	Vendor
Microprocessor	Celeron 2.4GHz	Intel
Main Memoru	512 Mbytes	
Operationg System	Windows 2000 Professional	Microsoft
Development Software	Quartus II Version 5.1	Altera
CPLD Device	MAX7000S EPM7128LC84-15	Altera
Power Estimator	MAX Power Calculator Spreadsheet Version 1.2	Altera

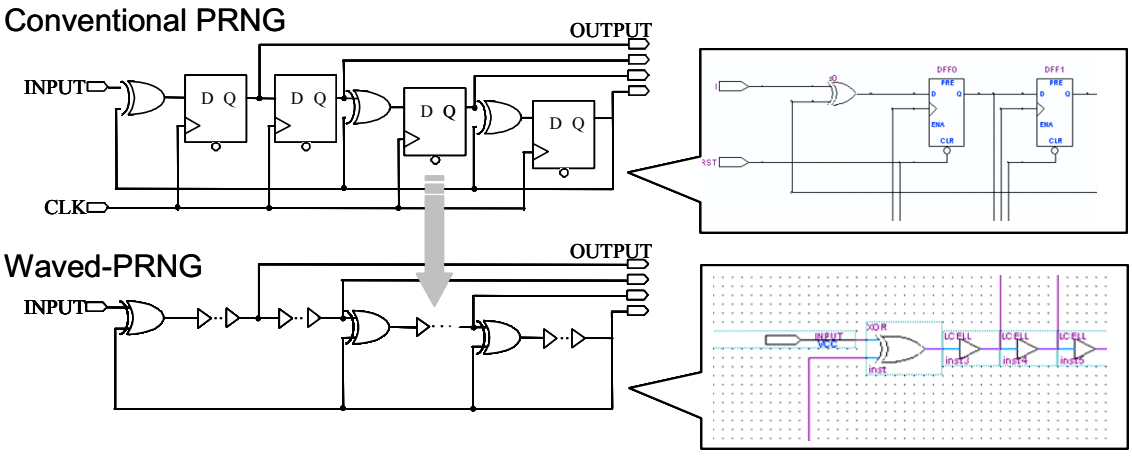


図 4　従来方式の PRNG とウェーブパイプライン方式の PRNG の論理回路

3.3　CMOS テクノロジィを用いた PRNG 回路の設計

1.2 μCMOS テクノロジィとスタンダードセルライブラリを用いて，ウェーブパイプライン方式 PGNG チップ

の設計を行う。設計するチップは，4-bit のウェーブパイプライン方式 PRNG 回路と，比較を行うことを目的とされている従来方式の 4-bit PRNG 回路である。これらの回路は**図 5** に示すように一つのチップに搭載する。

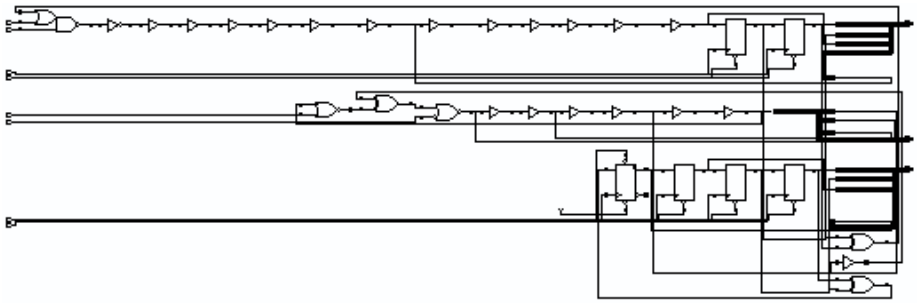


図 5　1.2 μ CMOS チップの論理回路図

設計は，**表 3** の計算機と表 4 のソフトウェアを用いて行っている。設計手法は3.2章同様のバッファ挿入による遅延時間の調整を行っている。しかしながら，LFSR はフィードバックを含む状態遷移回路であることから，マクロセル単位でタイミングを持つ CPLD とは異なり，タイミングの調節が非常に困難であった。よって今回は，小規模回路である 4-bitPRNG での設計評価をおこなう。破線に囲まれた部分が，ウェーブパイプラインが施されている部分である。**図 6** にレイアウトツールを用いて設計した同チップのレイアウト図を示す。

表 3　CMOS チップの設計環境

Platform	Sun Blade 1000 / ATX-PC
MPU	Sun UltraSPARC-II 750MHz / Intel Pentium4 3.0 GHz
Main Memory	1024 MB / 2058MB
Virtual Memory	1787 MB / 4183 MB
OS	Solaris 8 / Red Hat Enterprise Linux WS

表 4　開発ツール

Tool name	Function	CAD vender
Compiler	Design Compiler	Synopsys
Simulator	Synopsys VCS	Synopsys
	Verilog-Simulator	
Layout	Avant! Apollo II	Synopsys
	Avant! Milkyway	

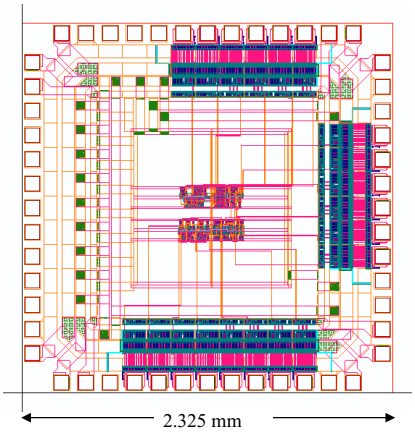


図 6　1.2 μ C-MOS チップのレイアウト図

4　評価

4.1　動作速度と電力消費

我々は，**図 4** の従来方式 PRNG 回路とウェーブパイプライン方式 PRNG 回路をゲートレベルシミュレーションによって評価を行う。**図 7** は WEP 処理で用いる 24-bit のウェーブパイプライン方式 PRNG 回路のシミュレーション結果である。**図 7** は，111.1MHz においてレジスタを使用せずに，正常動作することを示している。

図 8 は従来方式の PRNG 回路とウェーブパイプライン方式 PRNG 回路の動作速度の比較結果を示す。**図 9** は電力消費について比較した結果を示す。**図 8** と**図 9** は，4, 8, 16, 24, 32, 48 bit の回路における動作速度と電力消費をプロットしたものである。**図 8** と**図 9** の結果より，ウェーブパイプライン方式 PRNG 回路は高速・低消費電力の両立を実現することを示す。

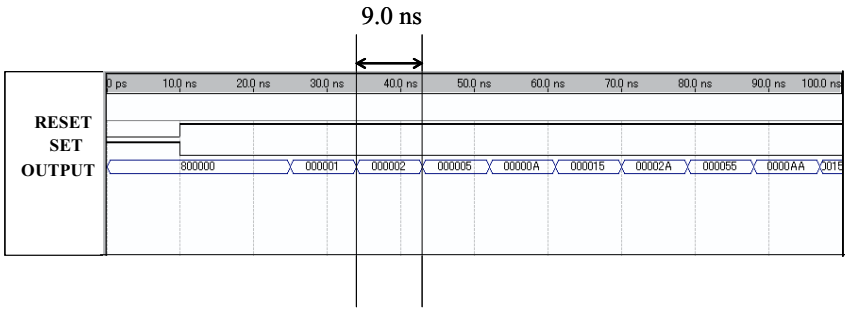


図 7　CPLD による 24-bit ウェーブパイプライン方式 PRNG のゲートレベルシュミュレーション

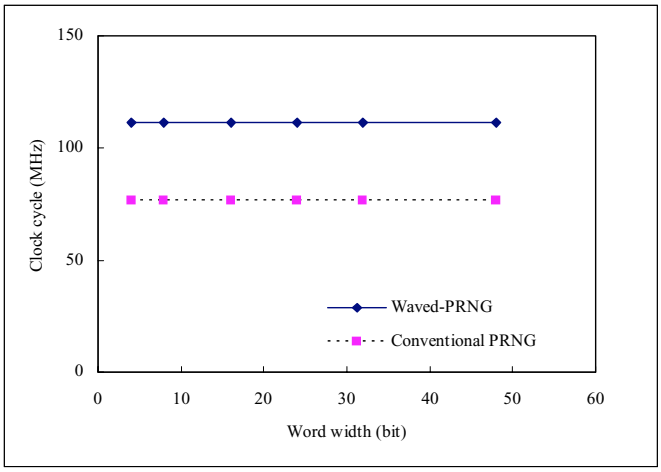


図 8　CPLD によるPRNG 動作速度比較

4.2　擬似乱数生成列

我々は，ウェーブパイプライン方式 PRNG はクロック周波数をコントロールすることで容易に新たな擬似乱数生成列が生成できることを述べる。**図10**(a)が示すように，ウェーブパイプライン方式 PRNG 回路は擬似乱数を生成する。このため，**図11**のようにトリガするタイミングをクロック 1/2 のクロック周波数で動作させた場合，擬似乱数生成回路が出力する値の並びが変更される。**図11**(b)の従来方式の PRNG 回路は，動作クロック周波数を 1/2 に出力した場合でも出力する値の並びは変更されない。

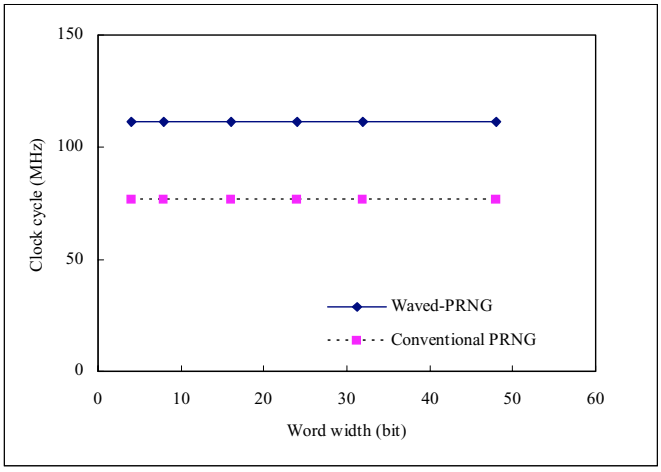
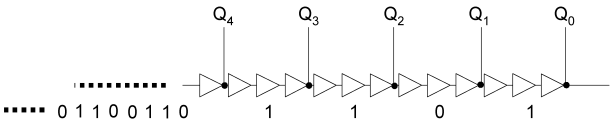
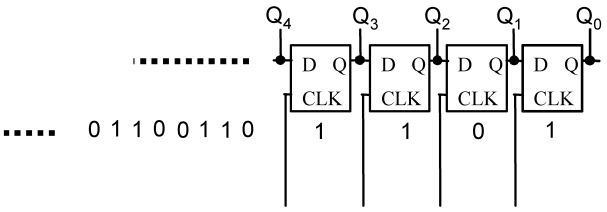


図 9　CPLD によるPRNG 消費電力比較



(a)



(b)

図10　PRNG の動作　(a)　ウェーブパイプライン方式　(b)　従来方式

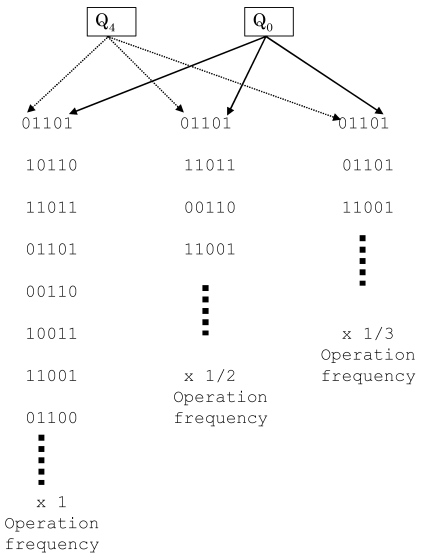


図11　クロック周波数をコントロールした場合の擬似乱数列の出力

５　まとめ

本研究開発では，ウェーブパイプライン方式の PRNG 回路は 1.2μm C-MOS テクノロジィとスタンダードセルライブラリを用いたチップの開発が行われ，また CPLD を用いることで実現した。ゲートレベルシミュレーションの結果，ウェーブパイプライン方式 PRNG 回路は従来方式の PRNG よりも高速かつ低消費電力で動作することが示された。今後の研究開発では，このウェーブパイプライン方式 PRNG 回路を WEP のエンコーダとデコーダ回路に組み込むことで，WEP 方式と互換性を有する高速・低消費電力・暗号強度強化型暗号の開発を行う。

謝辞

本研究開発を実施するにあたり，多大なご援助を頂いた財団法人電気通信普及財団に厚く御礼申し上げます。また，日本アルテラ㈱によるユニバーシティプログラムによる支援のもとで実施したものである。本チップ試作は東京大学大規模集積システム設計教育研究センターを通し オンセミコンダクター㈱，日本モトローラ㈱，HOYA㈱，京セラ㈱，およびシノプシス㈱の協力で行われたものである。

参考文献

[1] 村井純，“インターネット構成法第 4 回：レイヤ 2 技術,”
http://www.soi.wide.ad.jp/class/20040021/slides/04/index_48.html, 2004.

[2] 結城浩，“暗号技術入門,”ソフトバンクパブリッシング, 2003.

[3] T. Sato, R. Sakuma, D. Miyamori, M. Fukase,“Waved-LFSR Circuit for Hardware-based Intrusion Detection System,”Proc. of ECTI-CON2006, Vol.I, pp.30-33, 2006.

[4] 佐藤友暁, 深瀬政秋，“学内無線 LAN における不正アクセス・コンピュータウイルス問題のハード的解決手段の開発,”学術情報処理研究, No. 9, pp. 15-26, 2005.

[5] L. Cotton,“Maximum rate pipelining systems,”Procs. AFIPS Spring Joint Computer Conference, pp. 581-586, 1969.

[6] F. Klass and M. J. Flynn,“COMPARATIVE STUDIES OF PIPELINED CIRCUITS,”Stanford University Technical Report, No. CSL-TR-93-579, July 1993.

[7] W. P. Burleson, M. Ciesielski, F. Klass, and W. Liu,“Wave-Pipelining: A Tutorial and Research Survey,”IEEE Trans. on Very Large Scale Integration (VLSI) Systems, Vol. 6, No. 3, pp. 464-474, Sept. 1998.

[8] Masa-aki Fukase, Tomoaki Sato, Ryusuke Egawa, and Tadao Nakamura,“Scaling up of Wave-Pipelines,”Proc. of The Fourteenth International Conference on VLSI Design, pp. 439-445, Jan. 2001.

[9] Masa-aki Fukase, Tomoaki Sato, Ryusuke Egawa, and Tadao Nakamura,“A Wave-Pipelined Biprocessor Achieving Remarkable Compatibility between Low Power and High Speed,”Proc. of 10th NASA Symposium on VLSI Design, pp. 8.3.1-8.3.8, 2002.

[10] Tim Horel and Gary Lauterbach,“UltraSPARC-III: Designing Third-Generation 64-Bit Performance,”IEEE Micro, Vol. 19, No. 3, pp. 73-85, 1999.

[11] W. Liu et al.,“A 250-MHz wave pipelined adder in 2-um CMOS,”IEEE J. Solid-State Circuits, vol. 29, no. 9, pp. 1117-1128, 1994.

[12] F. Klass et al.,“Fast multiplication in VLSI using wave-pipelining,”J. VLSI Signal Processing, 1994.

[13] M. Fukase, T. Sato, R. Egawa, and T. Nakamura,“Breakthrough of Superscalar Processors by Multifunctional Wave-Pipelines,”Proc. of 9th NASA Symposium on VLSI Design, pp. 6.3.1-6.3.17, Nov. 2000.

[14] Tomoaki Sato, Rena Sakuma, Daisuke Miyamori, and Masa-aki Fukase,“High-Speed and Low-Power LFSR by Wave-Pipelining,”Proc. of CCCT, Vol. III, pp. 396-401, 2004.

[15] Tomoaki Sato, Rena Sakuma, Daisuke Miyamori, and Masa-aki Fukase,“Performance Analysis of Wave-Pipelined LFSR,”Proc. of ISCIT 2004, pp. 694-699, 2004.

〈発 表 資 料〉

題　　名	掲 載 誌 ・ 学 会 名 等	発 表 年 月
Waved-LFSR Circuit for Hardware-Based Intrusion Detection System	Proc. of ECTI-CON 2006	2006年 5 月
Waved-PRNG for a Wave-Pipelining Test Circuit	Proc. of 12th NASA Symposium on VLSI Design	2005年10月
Hardware Cryptography-Embedded Multimedia Mobile Processor for Ubiquitous Computing	Proc. of 12th NASA Symposium on VLSI Design	2005年10月
Hardware Cryptography for Ubiquitous Computing	Proc. of ISCIT 2005	2005年10月
学内無線 LAN における不正アクセス・コンピュータウイルス問題のハード的解決手段の開発	学術情報処理研究	2005年 9 月
Development of a Security-Enforced Network Interface Card for Wireless LAN	電気関係学会東北支部連合大会	2005年 8 月