

# 擬似ランダムビット列生成器及びそれを使用する ストリーム暗号通信方式ならびに応用としての パソコン鍵、PC 間暗号化通信、高質度暗号生成器

喜屋武 盛基<sup>†1</sup>

名嘉村 盛和<sup>†2</sup>

島 真一<sup>†3</sup>

<sup>†1</sup>沖縄大学マルチメディア教育研究センター

<sup>†2</sup>琉球大学工学部情報工学科

<sup>†3</sup>専修学校 国際電子ビジネス専門学校

【あらまし】 沖縄大学マルチメディア教育研究センター紀要第2号pp41-47に本論文の著者の一人喜屋武盛基は“擬似ランダムビット列生成器及びそれを使用するストリーム暗号通信方式”を提案した。

我々は“擬似ランダムビット列生成器及びそれを使用する暗号通信方式”を具現化する研究を更にすすめ詳細な論理・回路設計を行いFPGAによる実証実験に成功した。

更にまた、実証実験の結果の応用としてのパソコン鍵、PC間暗号化通信、高質度暗号生成器などの提案について述べる。

## Stream Cipher Cryptography by Pseudo-random bit stream Generator and It's Application on PC-key, Encryption-communications between PCs, and Very high quality Cipher Generator

Kyan, Seiki, Nakamura, Morikazu, Shima, Sinnichi  
Multimedia Education & Research Center, Okinawa University  
Dept. of Information Engineering, University of the Ryukyus  
KBC International Business College, Naha, Okinawa

**Abstract** One of the authors of this paper, Kyan, Seiki has proposed “Pseudorandom bit-stream Generator and its associated Stream Cipher Cryptograph” on the Bulletin of Multimedia Education and Research Center, 2002 issue. We have continued our research to realize the proposal.

This paper describes in detail how the objective accomplished and proposed the new applications such as PC-key, Encryption-communications between PCs, and very high quality cipher generation system.

## 1. はじめに

近年、インターネットの発達により多種のメディア（音声、文字、静止画、動画など）がインターネットによって運ばれるようになった。インターネットがグローバルに開かれており、誰でも簡単な手続きによりインターネットの送受信者となる。ネット利用の利便性の裏にセキュリティ問題が大きくクローズアップされるようになった。

データ通信を行なう際には、情報を安全に運用する技術すなわち情報セキュリティ技術の重要性が増してきている。特に、データ秘匿のための暗号法は、種々の研究が行なわれている。秘匿性を伴うデータ通信やインターネットにおける回線暗号装置では、一般にストリーム暗号が用いられており、ISO の国際規格 IS-9160（物理レイヤ暗号装置に対する相互運用要求事項）においても、回線暗号装置で用いる暗号としては、1ビットまたは8ビット（1文字）ごとのストリーム暗号を使うように規定している。

本研究はデジタル化されたデータを高速に暗号化、復号化するためのハードウェア・デバイス、“擬似ランダムビット列生成器及びそれを使用する暗号通信方式”について述べ、その特性を生かしたインターネット上のセキュリティシステムについて論ずる。

## 2. 数ふるい

連立合同式を解くためだけの単能計算機数ふるい回路は（図5、p.10）のように、互いに素の長さを持つ複数のフィードバックシフトレジスタ（2ビット....., 127ビット.....）とそれらの出力の論理積（AND）をとった比較的簡素な回路である。

この単能計算機システムを汎用計算機システムのサブシステム（sub-system or co-processor）とする研究が平成元年度文部省科学研究費一般研究C“特殊目的計算機システム「数ふるい」とマルチプロセッサシステムの研究”（2年継続）である<sup>[4]</sup>。

## 3. データの暗号化

インターネットは誰でも加入できるオープンなネットワークであるので、第3者によって盗聴され悪用される可能性は高い。それを防ぐための手段の一つがデータの暗号化である。暗号はジュリアス・シーザーの時代から使われていて、その後、暗号法の基礎となったシーザー暗号<sup>[8]</sup>がある。それらは一般に換字法と呼ばれている平文中の文字を何らかの方法で他の文字や記号に変換する技術である。

近年のインターネット時代の暗号法には大きく分けて共通鍵暗号法と公開鍵暗号法がある。本論文の暗号法は前者に属し、送り手と受け手が同一の鍵を使って暗号化・復号化を行うものである。

したがって鍵が第3者に渡れば簡単に解読されてしまう欠点を持つ。（太平洋戦争中、日本軍が使用した、乱数表を鍵とした暗号文は、乱数表が漏れたのではなくアメリカ軍の統計的な手法の結果破られたものと近代史は伝えている。）

公開鍵法は送り手と受け手で違う鍵を用いて暗号化・復号化を行う。どちらかの鍵で暗号化したデータはもう一つの鍵を使わないと復号化できない。一方の鍵を公開し（パブリッ

ク・キー)、それを使って暗号化したデータをもう一つの鍵（プライベート・キー）で復号化する方式である。勿論プライベート・キーは秘密にする。共通鍵暗号法は公開鍵法に比較して暗号化や復号化に要する計算時間が短くてすむ（本論文の装置では、ストリーム信号との同期をとれば、計算時間は理論的にゼロ）反面、受け手に安全な手段で秘密鍵を渡す必要がある。

公開鍵法は暗号化や復号化に膨大な時間がかかるが（一般に数百倍かかると言われている）受け手一人一人に秘密鍵を渡す必要はない。この欠点と特徴をうまく使えば共通鍵法と組み合わせることにより、高速で非常に安全な通信方法ができる。すなわち、公開鍵法により共通鍵となる seed を受け手側に送り、以後、それを使ってお互いに暗号化・復号化を行えばよい。

図1は共通鍵の原理図である。

#### 4. “数ふるい”を用いたランダム・ビットストリーム生成器

“数ふるいを用いた擬似乱数生成器”<sup>[5]</sup>について述べる。図5は“数ふるい”で異なる素数のビット長を持つ循環レジスタを8個ならべ（2, 3, 5, …19）それらの出力を NAND ゲートで取ったものである。

この装置は次の連立合同式を解くことができる。

$$\begin{aligned}
 X &= 0, 1 && (\text{mod } 2) && \dots && (1) \\
 X &= 1, 2 && (\text{mod } 3) && \dots && (2) \\
 X &= 2, 3 && (\text{mod } 5) && \dots && (3) \\
 X &= 0, 1, 2, 3, 5, 6 && (\text{mod } 7) && \dots && (4) \\
 X &= \dots && (\text{mod } 11) && \dots && (5) \\
 X &= \dots && (\text{mod } 13) && \dots && (6) \\
 X &= \dots && (\text{mod } 17) && \dots && (7) \\
 X &= \dots && (\text{mod } 19) && \dots && (8)
 \end{aligned}$$

すなわち、(1) から (8) までの剰余式のすべてを同時に満足する値 X を求めることができる。

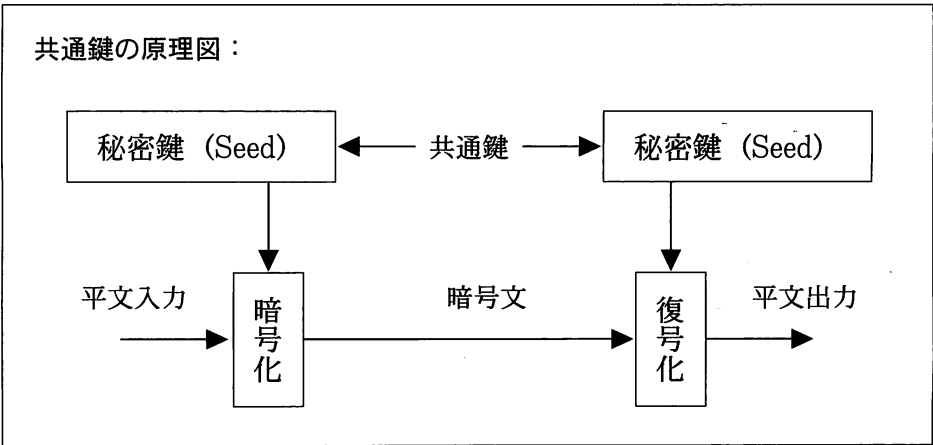


図1 共通鍵の原理図

## 5. “数ふるいを用いた擬似乱数生成器”の乱数性の検証

本論文の乱数ビット列生成器によって発生するビット列は、真の物理乱数ではなく有限の周期を持つ出力系列である。暗号に使用する際はどの程度真の乱数に近いかを検証する必要がある。

乱数性を検定する方法として次の3つの方法を用いた。

- 1) 等頻度性検定
- 2) 一様分布検定
- 3) 間隔検定

測定方法はランダムに選んだ10000種の Seed (初期ビット列) により、それぞれ1周期のビット列を発生させ、(0) と (1) の出現頻度を調べた結果、すべての場合で(+0.1% ~ -0.1%) であった。その他  $\chi^2$ 、一様分布検定、間隔検定の結果、非常に良好な高品質な乱数列であることが分かった<sup>[8]</sup>。

## 6. バーナム暗号法 (Vernam Cipher)

バーナム暗号法は1917年に電信用暗号として開発されたストリーム暗号の一種で、通信ネットワークにおける秘匿通信によく用いられる。換字暗号の鍵を十分に長い乱数とすることで安全な暗号を構成できる(乱数が平文以上の長さである場合、完全暗号という)。

送り手側で平文をキーストリームで1ビットずつ論理演算を施して暗号化すれば受信側では同じキーストリームで復号化できる。本論文のランダムビット列生成器は自然乱数にきわめて近く(5章の乱数性の検定で証明済み)周期の長い良質のビット・ストリームを生成するので、バーナム暗号法に最適なものである。

この方式は原理が簡単で且つキーストリームが使い捨てであるため、安全性の高い暗号法として良く用いられている。この暗号法はキーストリームを如何にして生成するかが最も重要な問題である。

たとえば、真の物理的ランダムビット列を用いた場合には理論的に解析が不可能な唯一の暗号となるがしかし、通信文と同じ量のキーストリームを(解読のため)送信先に送ることは非現実的でほとんど不可能であることから、乱数として真の物理的ランダムビット列は用いずに比較的簡単な方法で生成した擬似ランダムビット列を用いる。従って、この擬似ランダムビット列の性質が、暗号の強度を大きく左右することになる。擬似ランダムビット列生成には、比較的短い秘密鍵(70ビット程度、本論文では種 Seed と呼ぶ)から長い擬似ランダムビット列を生成する必要があるが、その手段として、

1. 線形フィードバックシフトレジスタ (Linear Feedback Shift Register : LFSR) を組み合わせた方法
2. DES (Data Encryption Standard : DES) 暗号装置等を用いる方法
3. LFSRと論理素子を組み合わせた非線形結合による方法
4. クロック制御型の擬似ランダムビット系列生成器 (Clock-Controlled Generator : CCG) を用いる方法等がある。

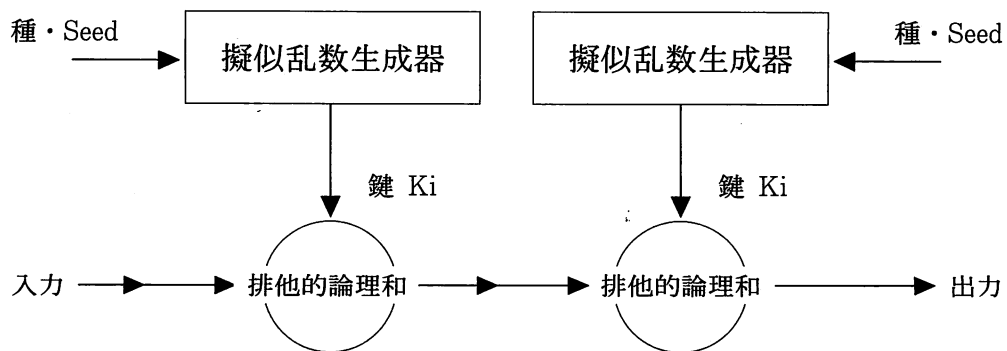


図2 バーナム暗号法の構成図

上図はバーナム暗号法の構成図である。送信側で平文入力をキーストリーム $K_i$ で1ビットずつ論理演算、排他的論理和 (XOR) を施して暗号化する。暗号文 $C_i$ は受信側で同一構造の乱数生成器から同一の種 (Seed) によって生成されたキーストリーム $K_i$ で排他的論理和を施して復号化して入力と同じ平文出力を得る。上図の左側が送信パソコンで右側が受信パソコンと考えると2台を結ぶ回線の中は暗号化されている。回線は直接ケーブルであってもインターネットであってもLANであっても良い。2台のパソコンはVPNを構成することができる。

また、乱数ビット列による論理演算を通信速度と同期させることにより暗号・復号化に要する時間をゼロにすることができるので高速なデータ通信ができる。

暗号化と復号化の原理を述べる。

上図の平文のビット列を  $M=m_1 m_2 \cdots$  とし、鍵のビット系列を  $k=k_1 k_2 \cdots$  とすると、暗号文のビット系列  $C=c_1 c_2 \cdots$  は

$$c_i = m_i \oplus k_i$$

と表される。復号は同じ鍵を使って論理演算、排他的論理和をとるので

$$m_i = c_i \oplus k_i$$

すなわち

$$\begin{aligned} m_i &= m_i \oplus k_i \oplus k_i && \text{したがって} \\ &= m_i && \text{で復号される。} \end{aligned}$$

## 7. 実証実験の結果

### 1) 暗号・復号器同士の通信

市販のFPGAボード上に暗号通信モジュールを実装した。(写真1) 図3にそのブロックダイアグラムを示す。また、PCとFPGAボードで実験用システム構成し、2台のPC間でデータ転送実験を行った(写真2)。予想通りの結果が得られた。

(1) 第1段階

FPGA ボード側に USB インターフェースを作成し、PC より USB ポートを介して接続する。FPGA ボード間はシリアルポート (RS-232C) で連結する。(図 4)

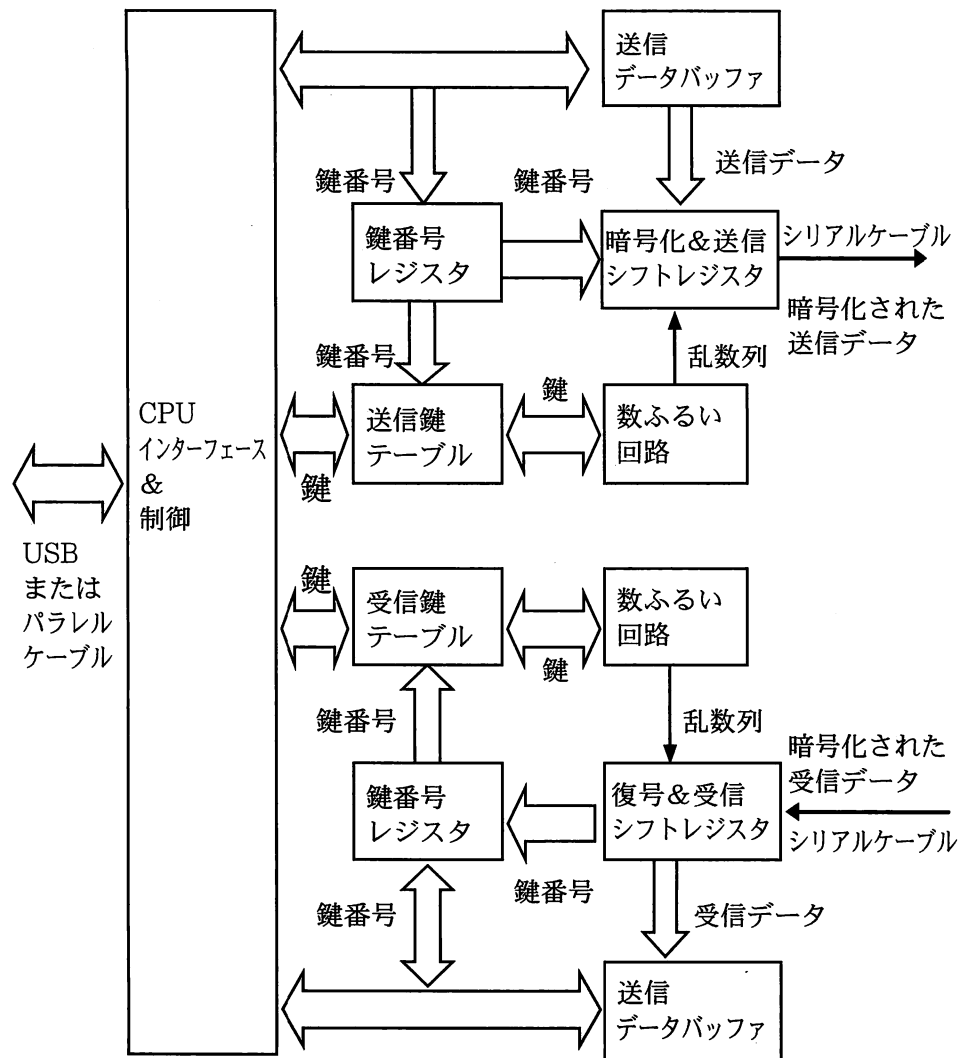


図3 暗号通信モジュールブロックダイアグラム



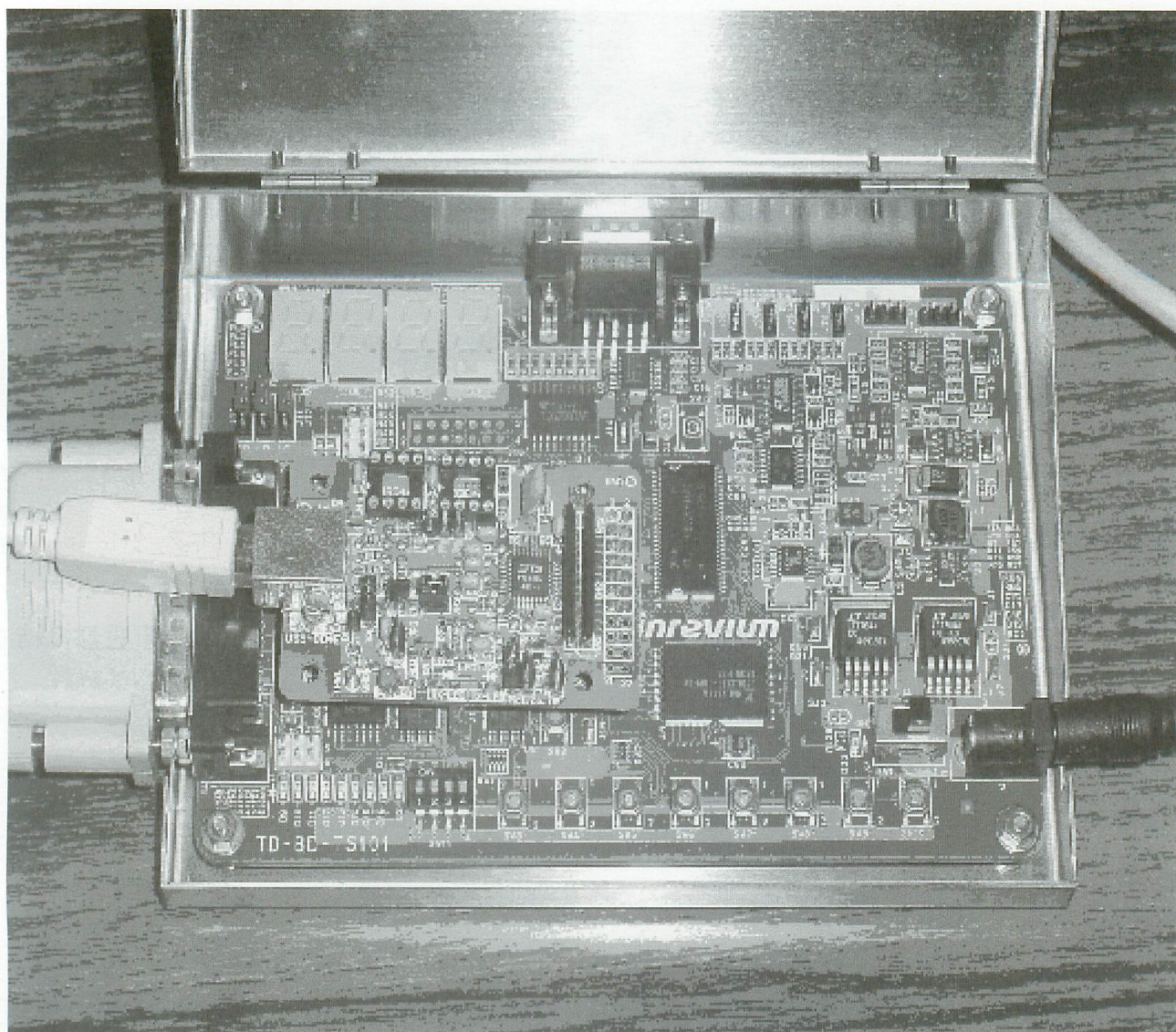


写真1 暗号通信モジュールの構成（暗号・復号器 FPGA モジュール細部写真）

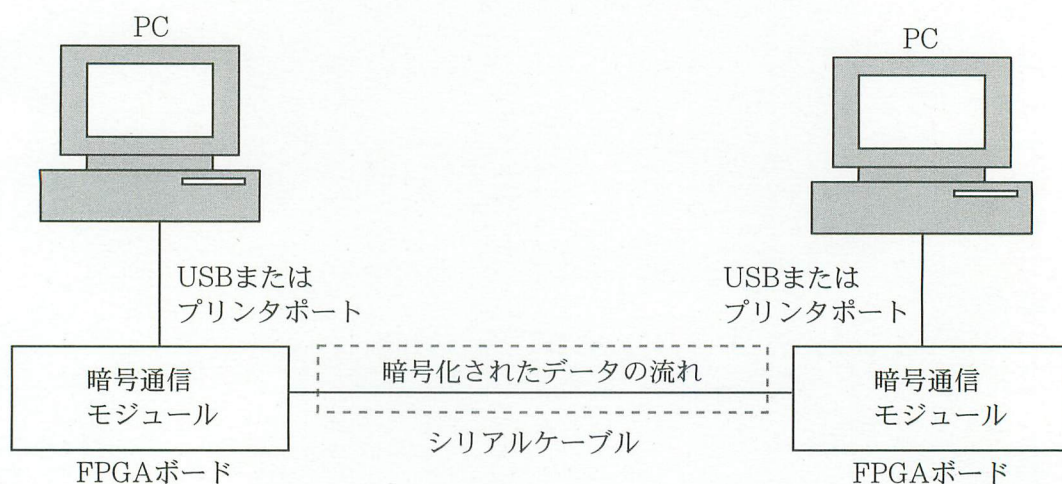


図4 実験用試作システム



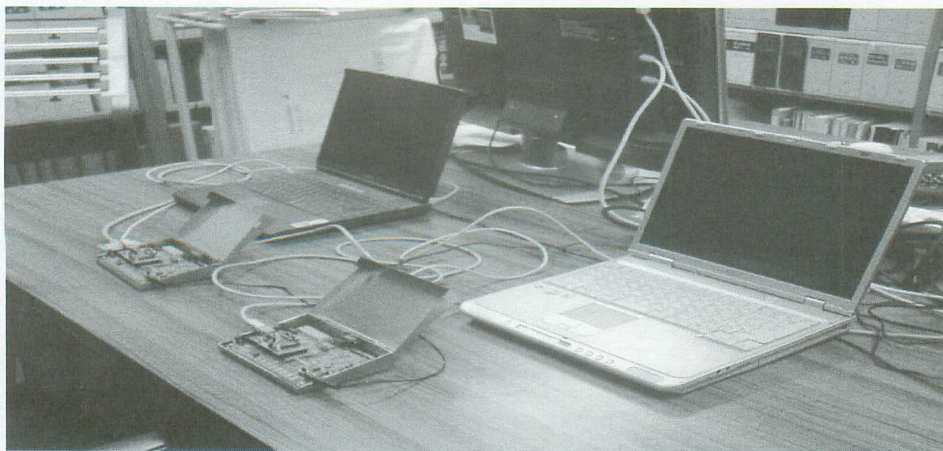


写真 2 研究室内の実験用機器配置図

写真 2 は実験用試作システム（図 4）と同一の配置にしてある。

- (2) 第 2 段階 第 1 段階 USB インターフェースの作成の部分が完了し、予想通りの結果を得た。



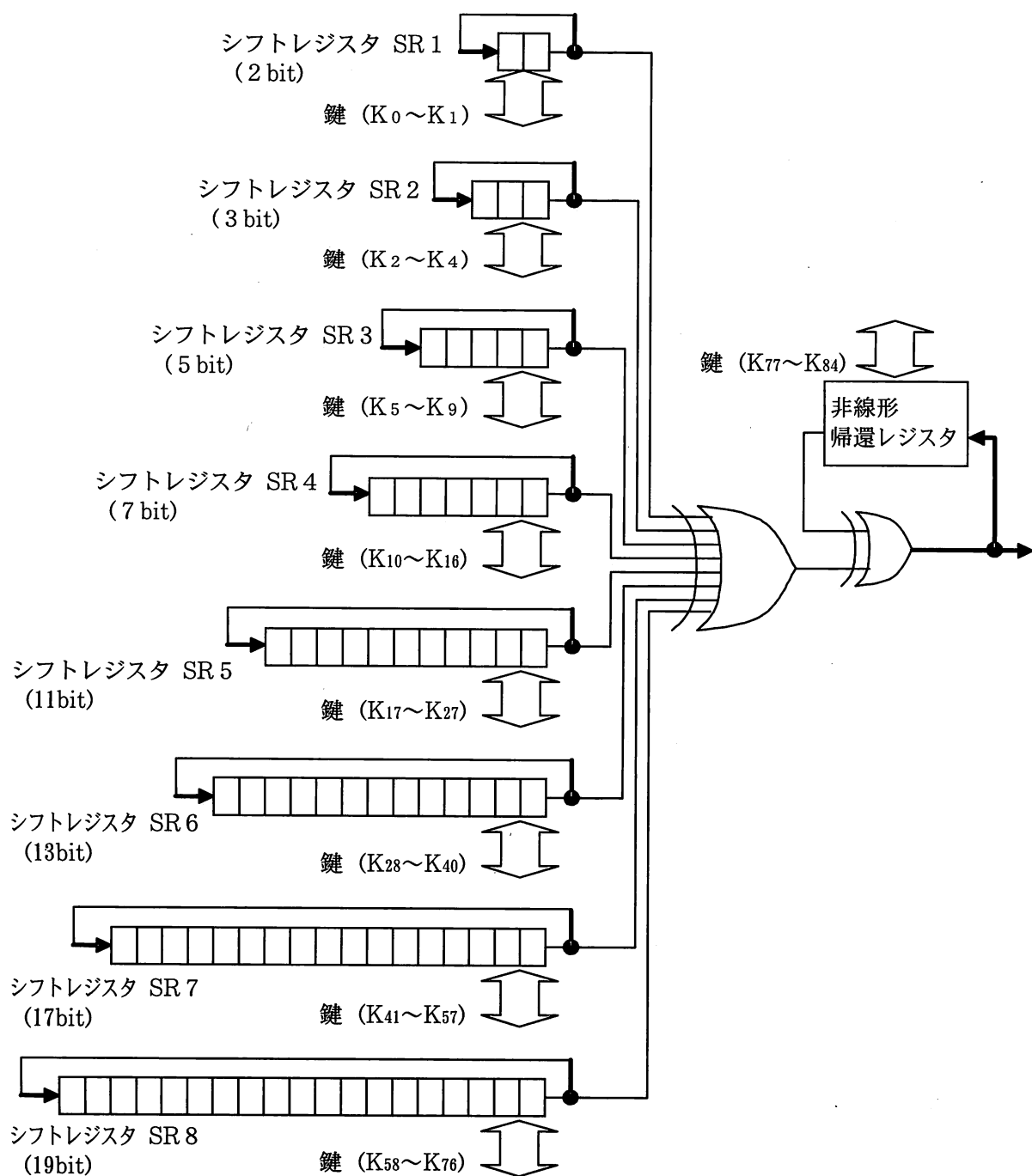


図 5 擬似乱数生成用数ふり回路

## 8. モジュールを活用した応用システム

### (1) 乱数生成モジュール

乱数モジュールを USB を介してパソコンシステムに取り入れ、高速で高品質の乱数を利用する。複数個のモジュールを使えば複数個のそれぞれ独立した乱数を同時に使うことができるのでコンピュータシミュレーションなどに有効である。

## (2) パソコン鍵

USB スロットに挿入したままパソコンを使い、終了するときは必ず抜くようにすれば、パソコンに入力されたデータは暗号化されているので、盗難にあってもデータが外部に漏れることはない。パソコン鍵はパワーオンの機能も付加する。

入出力は必ずパソコン鍵（暗号・復号器）を通るように USB 周辺のロジックが組み立てられているので内部データは常に暗号化されている。（図6）

パソコン内部のデータが暗号化されるので鍵を抜いておけば盗難に遭っても内部データが漏洩しない。仮に鍵ごと盗難に遭っても一定時間後に鍵が不能化する仕組みをつければ安全である。また Winny などによる情報漏洩もない。

## (3) インターネット接続

図4. に示す「実験用試作システム」のシリアルケーブルの中は暗号化されたデータが流れているので、シリアルケーブルを他の例えば光ケーブルに置き換えてもよいが、インターネット接続にすればインターネット上での暗号化された通信を可能にする。ただしプロトコルの問題を解決する必要がある。（注）プロトコル：コンピュータ同士で通信や情報のやりとりをするときに必要な約束ごとや取り決めなどで、RS-232C 同士のような機械レベルの取り決めや、通信相手の確認などのソフトウェア・レベルでのプロトコルなど、同じレベル間で規定されている。（「マルチメディア・インターネット事典」）

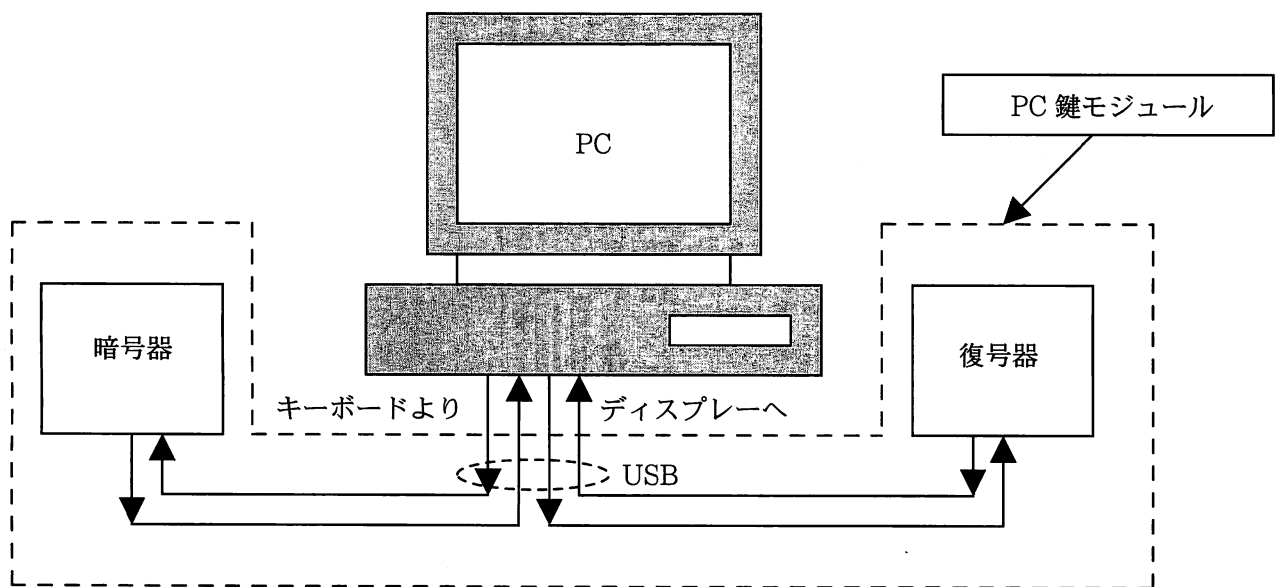


図6 PC 鍵の概念図

## (4) インターネット接続 2

上述のインターネット接続で可能な通信方式につぎの3種類がある。

1. 1 対 1
2. 1 対 n
3. n 対 n

1. は1対1のvpnであり2. は1対多である。組織内のサーバーと組織内の職員が使用している各パソコンを想定してもよい。3. は組織同士の bipartite 状の接続関係で

ある。

参考：最近2007年9月総務省は相次ぐ機密漏えい対策として自動的に入力データを暗号化するシステムを構築中で近日中に稼動する予定とのことだが我々のシステムでも可能である。

## 9. まとめ

ハードウェアによる擬似ランダムビット列生成の特徴はその高速性にある。種を変えることによってまったく異なるランダムビット列が生成されるので、種を安全に受信側に送ることができれば、きわめて信頼性の高い暗号法になる。

種を送る手段としては公開鍵暗号法、すなわち共通鍵暗号法との組み合わせが最適であるが、より簡易な方法としてはインターネット以外の通信手段、たとえばファックスや電話を通してあらかじめ番号付きの複数個の種を送り、通信を実行する時点でランダムに発生した番号で種の順番を選ぶ方法もある。またストリーム暗号であることから匿秘性を増すために2重、3重に重ねて使うことも困難ではない。種々なレベルの安全性とシステムのコストや目的に合わせた多用なシステムを構築することができる。暗号生成器の構造もきわめて多くのバリエーションをとることが可能である。たとえば2個の素数からなる2本のシフトレジスタのみで構成されているものから、2から $n$ 番目の素数のすべてを使い $n$ 本のシフトレジスタを使うものまで含まれる。超高速ネットワーク対応のIC化と、生産ラインのFA (Flexible Automation) まだがこれからの課題である。

1対1、1対 $n$ 、 $n$ 対 $n$ の通信にも容易に対応することが可能であり、仮想的にインターネットを専用線のように使うことができるVPN (Virtual Private Network) への応用も考えられる。前章で述べたパソコン間の通信が適用できる例である。

またパソコン鍵としての適用は図5に示すように暗号・復号器と新たに追加した論理回路とをチップ化して外付けUSB装置し、これを鍵とする。この鍵が挿入している間は内部データ（すでに暗号化されているので）は見えない。パソコン内のデータを暗号化・復号化するだけである。鍵が抜かれておればパソコンが盗難にあっても内部データを解読することは不可能である。

市場のニーズが高く商品化の期待がもてる。

我々の研究はハードウェアによって一挙にランダムビット列が生成できる装置、「擬似ランダムビット列生成器」である。特徴として挙げられるのは1. 高速性 2. 高品質 3. ロジック回路が単純なため高い信頼性。4. 高速性を活用したユニークな“シード交換方式”により解読をほとんど不可能にすることである。

## 謝 辞

当該研究は沖縄電力株式会社 IT 推進本部の研究費によるものである。絶えまないご支援をいただいた沖縄電力に厚くお礼を申し上げます。

## 参考文献

- [1] Lehmer D.H. "The mechanical Combination of Linear Forms", American Mathematical Monthly, Vol.35,1928
- [2] Kyan, S. "Logic and Circuits of a Delay-line Number Sieve" Science Bulletin of the Division of Agriculture, Home Economics and Engineering, University of the Ryukyus, Vol.11, Dec.1964.
- [3] 喜屋武盛基、島真一、渡嘉敷直盛 “連立合同式と関連問題を解くためのプロセッサ「数ふるい」の IC チップの論理設計・製作およびプリ・ポストプロセッシング” 琉球大学工学部紀要、第38号、1989年
- [4] 喜屋武盛基 “特殊目的計算機システム「数ふるい」とマルチプロセッサシステムの研究” 成果報告書、平成元年度文部省科学研究費一般研究 C（2年継続）
- [5] 喜屋武盛基、照屋寛嗣 “数ふるいを用いた擬似乱数生成器” 琉球大学工学部紀要、第44号、1992年
- [6] 新垣良太、照屋寛嗣、喜屋武盛基 “数ふるいを用いた擬似乱数生成器の検証”、平成4年、電気関係学会九州支部連合大会講演論文集、p.58
- [7] 新垣良太、名嘉村盛和、喜屋武盛基 “動的数ふるいを用いた擬似乱数生成器” 1993年電子情報通信学会秋季全国大会講演論文集、A-205
- [8] 喜屋武盛基 “擬似ランダムビット列生成器及びそれを使用するストリーム暗号通信方式”、沖縄大学マルチメディア教育研究センター紀要第2号、2002年3月 pp41-47
- [9] ウィリアム・スターリング著、石橋啓一郎ほか “暗号とネットワークセキュリティ” pp.32-34 (2001)
- [10] 日経バイト編、“パソコン技術大系2000” pp.588-594, (1999)