疑似ランダムビット列生成器暗号化システムの研究開発（102311001）

Research and Development for Encryption System by Pseudo-Random Bit-Stream Generator

研究代表者
又吉光邦　沖縄国際大学
Mitsukuni Matayoshi　Okinawa International University

研究分担者
名嘉村盛和†　喜屋武盛基††　島真一†††
Morikazu Nakamura†　Seiki Kyan††　Shinichi Shima†††
琉球大学†　アクシオヘリックス株式会社††　アクシオヘリックス株式会社†††
University of the Ryukyus†　AXIOHELIX Co. Ltd.††　AXIOHELIX Co. Ltd.††

研究期間　平成 22 年度～平成 23 年度

概要

数ふるい回路を用いた擬似ランダムビット列生成器に基づく暗号化／復号回路を USB 接続の FPGA ボード上にハードウェア回路として実装した。それを応用して、リアルタイムに取得した画像データを暗号化し、TCP/IP プロトコルネットワークを介して、そのデータの送信と受信、ならびにリアルタイムの復号を実現した。

また、Bluetooth デバイスを用いてマルチホップ通信のための共通鍵の管理方式を開発するとともに、ルーティングプロトコルの開発及びシミュレーション実験を行い、アドホックネットワークへの適用の検討を行った。

Abstract

An encryption / decoder circuit based on the Pseudo-random Bit Stream Generator that used Number Sieve Circuit was implemented as a hardware circuitry on FPGA board of USB Connection. The implementing encryption / decoder circuit succeeds in encrypting and transmitting image (video) data / reception of cryptogram on TCP/IP protocol network system and the decoding. The management method of the common key for the multihop communication is developed by using Bluetooth device. Application to the Ad-Hoc Network is examined by development of the routing protocol and the simulation experiment.

１．まえがき

現在、ネットワークを介したストリーミングデータなどの電子データの送受信が爆発的に増えている。電子メールやその他の電子データと共にネットワークを介して送受信される電子データの秘匿性は、個人のプライバシーから企業情報の保全など、非常に重要な事項である。

本研究では、筆者等が整数論などで使う連立合同式の解のみを求める“数ふるい（Number Sieve)”の構造をほとんど変えずに発明した“数ふるい疑似ランダムビット列生成器”をベースに、ネットワークによる電子データ送受信に対応した暗号装置の研究開発を行った。開発した暗号化／復号システムは、今後の汎用性・多目的性の観点から USB 接続による外部接続装置の FPGA (Field-Programmable Gate Array) ボード上で実装した。そして検証のため、製作した暗号化／復号装置を使用した暗号画像送受信のアプリケーションの開発を行った。

また、その一方で、疑似ランダムビット列生成回路の特徴である１ビット遅延の応用例の一つとしてBluetooth を用いたアドホックネットワークへの適用の検討をシミュレーション実験で行った。

２．研究内容及び成果

２．１　数ふるい疑似ランダムビット列生成器による暗号化／復号装置の開発[1]

ストリーミングデータなどのデジタルデータを暗号化／復号する外部接続型の装置開発へ向けて、数ふるい疑似ランダムビット列生成器を USB 接続の FPGA ボード上にハードウェア回路として製作した。回路の概念図を図１に示す。製作に際し、FPGA に暗号回路を組み込むための回路記述言語(HDL)以外に２つの言語を用いて２つのドライバを開発した。一つは、FPGA 側へのデータ送受信用のドライバで、C++言語を用いて開発した。もう一つは、利用方法の多様性を持たせるためのドライバで、Java 言語の Java Native Interface (JNI)を用いてアプリケーション用のデータ送受信用ドライバを開発した。

本研究開発において、暗号化／復号をハードウェアで実現するために用いた FPGA ボードは、プライムシステムズ社製の CX-CARD Ⅱ (USB2.0 準拠、バルク転送対応、実効転送レート 16Mbyte/s)である。開発および実験環境は、WindowsXP Intel(R) Core(TM)2, Duo 2.53GHz, 1.86GBRAM である。

実証実験では、ファイル単位、およびバイト単位のデータの暗号化と復号を問題なく行うことが示された。

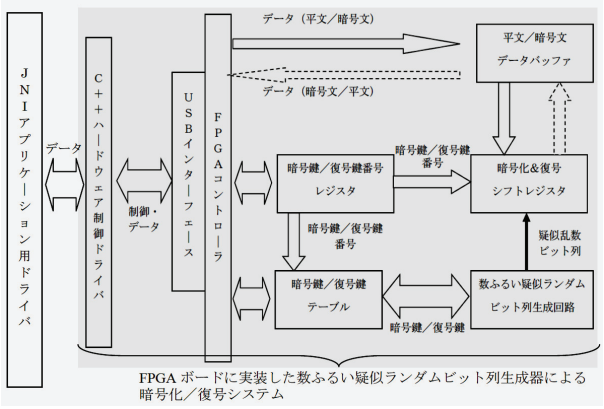

図１　回路の概念図

２．２　暗号化／復号装置を用いた暗号画像送受信システムの開発[2]

２．１で製作した数ふるい疑似ランダムビット列生成器による暗号化／復号装置を用いて画像を暗号化して送信するシステム、および受信し復号するシステムの開発を行った。今後の汎用的な展開を考えて、開発したシステムはUSB 接続にされた機器での暗号化／復号のシステム構成となっている。

開発したシステムでは、送信側となる PC 接続の Web カメラ等からリアルタイムに得られた画像データを PC と USB接続されたFPGAボード上に作成した暗号回路で暗号化し、そのデータ（暗号文）を TCP／IP プロトコルを用いてネットワーク上のサーバへ送信する。受信側は、クライアントとしてサーバに TCP／IP 接続して、サーバから暗号化されたデータ（暗号文）を TCP／IP プロトコルで取得する。取得された暗号文は、受信側（クライアント側）に接続された FPGA ボードの暗号／復号装置で復号し、受信側 PC で元画像（平文）として見ることができる（図２上部）。ここで、アプリケーション開発には、情報端末への普及を鑑みて Java とした。図２に製作したシステム全体の概念図を示す。一方、Android 端末用の数ふるい疑似ランダムビット列生成器による暗号化／復号の外部装置製作をめざして、アプリケーションとしてソフトウェア的に実装した（図２下部）。

FPGA ボードによるハードウェア版暗号化／復号装置、ならびに Android 端末でのソフトウェア版暗号化／復号装置とも正常に動作した。

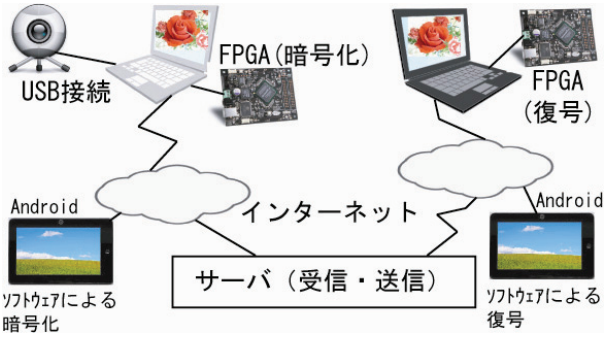

図２　暗号文の送信・受信、および復号の概念図
FPGA を用いた場合(上)とソフトウェアによる場合(下)

ここで、本システムの実証実験のため、Java 言語を用いて専用のクライアント／サーバシステムを新たに構築した。これは、暗号文がネットワークを介して送受信できるかどうかの検証、および暗号文（暗号化された画像データ）が、サーバ側で確実に暗号文として存在しているかどうかを確認するためである。既設のクライアント／サーバシステムでのデータのチェックは、サーバ管理者権限や他者の電子データの保全の観点から容易に実施できない。しかしながら、本研究において暗号文が TCP／IP プロトコルで電送されることを確認することは非常の重要である。そのため確認用のクライアント／サーバシステムを新たに構築し、実証実験に用いた。

２．３　マルチホップ暗号化通信方式[3]

数ふるい疑似ランダムビット列生成器暗号システムも応用例の一つとしてアドホックネットワークへの適用を検討した。アドホックネットワークは、現状のセキュリティレベルがインフラネットワークと比較して脆弱であるため、セキュリティレベルを向上させることが求められている。我々が開発した暗号システムは基本的に P2P 型の共通鍵暗号化通信を行うものであり、マルチホップネットワークに適用可能である。また、本暗号システムの暗号・復号化に要する遅延は１ビットであるため、オーバーヘッドも無視できる。

本プロジェクトでは端末に搭載されている Bluetooth 機能によるアドホックネットワーク構築を想定した場合の共通鍵管理方式の開発を行った。また、位置情報取得機能を活用したルーティングプロトコルを開発し性能評価を行った。

図３は Bluetooth における共通鍵管理方式の信号伝達回路を示している。Seed テーブルには、あらかじめ幾つかの Seed が登録されており、通信相手の Bluetooth アドレスより共通鍵が特定され、数ふるい疑似ランダムビット列生成器暗号システムに設定される。マルチホップの各ステップで通信相手が変更になる度に、Seed が共通鍵として設定されるので、P2P の共通鍵暗号化通信が可能となる。

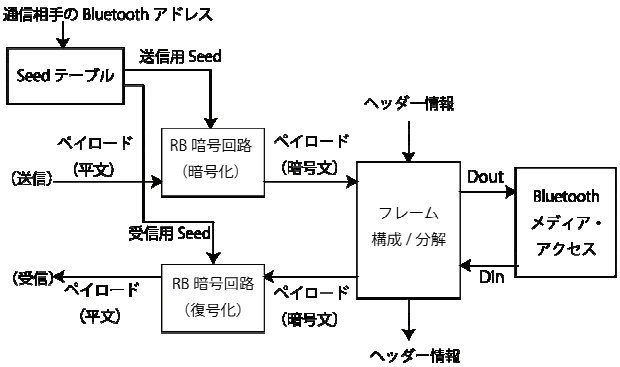

図３ Bluetooth における共通鍵管理方式の信号伝達回路

３．むすび

本研究では、疑似ランダムビット列生成器による暗号化／復号装置のハードウェアによる実装、アプリケーションソフトウェアによる実装、そして疑似ランダムビット列生成器による暗号法の１ビット遅延という特徴を利用したアドホックネットワークへの適用の検討を行った。

今後は、電子データのセキュリティが叫ばれている昨今の高度情報化社会において、必須となりつつある電子データの暗号化という手法・技法の製品化を通して地場産業に還元できればと考えている。具体的には、本研究成果を ASIC 回路で実現し、暗号化／復号の速度向上を図り、PC や Android などの高度情報端末に接続することで、外部暗号化／復号装置として製品化し、携帯端末の爆発的普及によって現れたセキュリティ機能に関わるソフトウェア、ハードウェア市場への貢献が期待できる。

【誌上発表リスト】

[1]野村慧、又吉光邦、宮城調佑、島真一、喜屋武盛基、“数ふるい疑似ランダムビット列生成器による暗号システムの FPGA 実装”、2012 年電子情報通信学会総合大会講演論文集 A-7-7（2012 年 3 月 21 日）
[2]又吉光邦、宮城調佑、野村慧、島真一、喜屋武盛基、“数ふるい疑似ランダムビット列生成器による暗号システムの FPGA 実装”、2012 年電子情報通信学会総合大会講演論文集 A-7-8（2012 年 3 月 21 日）
[3]金城大樹、名嘉村盛和、島真一、喜屋武盛基、“位置ベースアドホックルーティングプロトコルにおける経路修復手法”、2012 年電子情報通信学会総合大会講演論文集 A-12-3（2012 年 3 月 21 日）