2005.2

平成16年度

高知大学大学院 理学研究科 数理情報科学専攻

情報科学講座 修士論文要旨集

高知学園短期大学におけるLAN監視システム構築

数理情報科学専攻 情報科学講座　濱田美晴

高知学園短期大学においては、平成11年度から12年度にかけて構内ネットワークの導入・整備が行われた。しかし、その後端末の増加に伴い、順次必要箇所へHUBとケーブルを増設していったため、多段接続となり、その構造が複雑化していた。このため、問題点の多かった旧ネットワークを改善し、平成15年度末には、スター型の光ケーブル配線による新ネットワークへと移行した。本研究では、新旧それぞれのネットワークについて、パケット流量計測による監視システムを構築した。システム構築監視の基本目的は、(1)ネットワークの一部あるいは全体に障害が発生した場合や接続不良の要因を特定すること、(2)ネットワーク構成機器の障害や故障に迅速に対応すること、(3)ネットワーク構成機器のトラフィックを測定すること、(4)管理者の負担を軽減することである。

ネットワークシステムを管理するためのツールとして、一般的にSNMP（Simple Network Management Protocol）が用いられている。SNMPは、ネットワークを構成する機器（エージェント）に内部情報を保持し、管理サーバ（マネージャ）からネットワークを通じてその情報を管理する仕組みであり、本研究ではこのSNMPを利用した監視システムを構築した。

旧ネットワークでは、数値の統計を取得してWeb上でサーバに記録したログや、グラフ化されたパケット流量のデータを確認することができるMRTG(Multi Router Traffic Grapher)のツールを導入し、性能計測を行った。しかし、MRTGでは、過去ログの検索が困難であることや、Webインタフェースの構成上、管理側に負担のかかるものであった。そこで、可視化の手法に工夫をこらし、高知学園短期大学に即したネットワーク監視システムを構築した。

システム構築には、データベース部にPostgreSQLを、データベースとの連携を図るためPythonプログラム言語とApacheウェブサーバを用いた。本システムの最大の利点は、データベースの検索機能を付加したことで、グラフ表示に自由度を持たせたことである。管理画面は、パケット流量の大きさや異常を、数値のみでなく、画像で表現できる仕組みを備えた。また、メール通知システムの導入により、障害発生時にメールで異常を知らせる機能を持つため、迅速な対応が可能となっている。

メールシステムに関する研究

-- Apache/Mod_Python を利用した簡易 POP リーダの作成 --

数理情報科学専攻　情報科学講座　　氏名　朱　濱源

インターネットにおいて種々のアプリケーションが開発されているが、最も広く利用されているのはメールとウェブである。ウェブについては、ネットカフェなどにより、どこでも利用可能な環境が整っているが、メールについては、セキュリティ上の制限からどこでも利用というわけにはいかない。そこで、ウェブ経由でメールを読み書きできる環境を作るため、様々のウェブメールが開発されている。

しかし，ウェブメールにおいては、POP サーバとブラウザの間に CGI などの動的ページ生成のためのゲートウェイサーバが必要となるため、セキュリティ上の問題が生じる。特に、POP サーバとの接続においてはユーザ認証が必要であるため、ユーザが入力したパスワードのような重要な情報をゲートウェイサーバで一時保管しなければならない。また、ウェブメールを誰でも利用できるようにすると問題になることも考えられ、パスワードでの認証が必要であるが、一般に用いられているウェブ認証では、そのためのパスワードファイルの作成が必要であり、あらかじめパスワードを登録するのは煩雑である。

一方、ウェブサーバとして広く利用されている Apache HTTP サーバでは、外部モジュールとして mod_python を付加することにより、Python プログラミング言語を用いて認証やページ生成といったことが簡単にできるようになっている。

そこで、ウェブにおける認証、つまりウェブメール利用資格の判定によって POP サーバへの接続資格判定を行うことを考え、POP 認証そのものを利用するようにプログラムを作成した。ユーザが入力した ID/パスワードは素通りして POP サーバへ伝えられるため、ファイルに一時保存して覗き見される心配は無い。また、一般にブラウザは立ち上げから終了までの間、入力された ID/パスワードを再利用するので、ウェブメール利用の途中でパスワードを入れなおす必要も無い。

以上のような考察に基き、携帯からも利用できるウェブメールとして簡易 POP リーダを作成した。また、同様の認証を用いてメール送信インターフェスを作成することもできた。

メーリングリスト管理システム Mailman と保存書庫 Zest の連携

数理情報科学専攻 情報科学講座 氏名 劉　承嘯

現在、インターネットではホームページだけでなく、コミュニケーションの手段としてメールシステムが重要な役割を果たしている。なかでもメーリングリストは、小さな仲間うちでの連絡や討論から、メールマガジン、フリーソフトのボランティアサポートなど広く利用されている。メーリングリストに流れる情報をウェブで公開し検索できるようにすれば、それ自体が知識ベースとなって有効に活用できる可能性がある。

Mailman はウェブ連携メーリングリスト管理システムであり、討論用の一般的なメーリングリストから、メールマガジン用リストまで、多様な利用形態を想定した設定がブラウザを使ってできるようになる。また、Mailman に付属する保存書庫 pipermail においては、日付順、発信者のアルファベット順などに並べる他に、「スレッド」と呼ばれるメールとそのメールに対する返信の筋をたどることができるように、木構造に並べるといったことが行われている。いずれの並べ方においても、メール本文はそのまま表示するだけに終わっているため、本文を読んでいるときにその中の引用部分がどこから引き継がれているのかなど、議論の経過を把握することが難しい状態であった。

一方、Ka-Ping Yee (2002) によって開発されたメール保存書庫 Zest においては、メール本文に入っている「前のメールの引用」という構造に注目し、もし内容が別のメールによって引用されている場合には、リンクによって次のメールを表示し、その引用部分とそれに対するコメントを読むことができるようになっている。

Mailman においては、保存書庫として内蔵の pipermail でなく別の保存書庫システムを利用したい場合には、External Archiver (外部保存書庫)を指定することができる。ここでは、外部保存書庫として、zest を指定することを試みた。

本研究においては、zest 本体と入力インターフェス部の改良によって、UTF-8 文字集合によるウェブページ生成を行うことができた。Unicode を用いているため、英語日本語に限らずあらゆる言語に対応した保存書庫を構築することができるようになった。

ファジィ制御におけるＬＵＴの圧縮について

数理情報科学専攻　情報科学講座　　　市原 奈穂子

ファジィ制御の原理は，観測された入力とメンバーシップ関数で定義されるルールからファジィ推論手法により得られた結果を，フィードバック出力し制御するものである。実際の家電製品などに利用する場合は，制御処理の高速化・回路の小型化などの為，予め全ての推論演算結果を LSI 内部のメモリ等に LUT（ルックアップテーブル）として記憶させておき，それを参照する方法がとられている。さらにこの LUT は，LSI の小型化・省電力化・生産コストの削減などを目指して様々な研究がされてきた．これに関する研究として，冗長表現の畳み込みや近似関数分解などメモリ量の圧縮を中心としたものと，ファジィ推論方法や演算手法などアルゴリズムについての研究，さらには FDL (Fuzzy system Description Language) という特別なプログラミング言語を用いる研究などがされてきた．しかし，メモリ量とアルゴリズムを総合的に扱うことによる高速化・小型化に関する研究の報告は少ない．本研究では LUT の圧縮とファジィ推論段階での前処理との関連について着目し，特に LUT を作成する際，FDL によるルール記述段階での間引きがどのように LUT に影響するかを知ることを目的とする．

まず，LUT の圧縮について具体的に考察する為，ロケットの軟着陸における燃料消費と速度を扱う制御モデルを対象とするサンプルプログラムを作成し，家電などで使われている等間隔間引きによる圧縮方法のサイズと精度の関係を測定した．その結果，単純な間引きでもある程度の圧縮は可能であるが，圧縮により制御精度が落ちるため，実際の使用で許容できる範囲で圧縮を行う必要があることがわかった．そこで同制御モデルを FDL 記述で作成し，ファジィ推論段階でのルール間引きの影響を LUT のサイズと精度の関係から考察した．その結果，LUT の参照範囲を考慮した上でファジィ推論のルール間引きをした場合の LUT は，等間隔間引きを行った LUT の 1/3 のサイズで同程度の制御精度となり，FDL 記述段階での前処理が LUT の精度を保つ圧縮に効果があることがわかった。

VLSIポストレイアウト設計のウォーターマーキング法の研究

数理情報科学専攻　情報科学講座　ニエテイエン

半導体製造処理技術の進歩は，膨大なトランジスタ素子数を1チップ上に実装することを可能にし，一方，SoCの設計は大変複雑になり，既存の設計，いわゆるIntellectual Property，を利用して集積する新設計手法が重要になってきている．SOCデザインのコストと開発時間を減らすことに最も効果的であることがわかってきた．しかし，IP設計は，セキュリティ上の危険を引き起こす。

私は、本論文において，IPの著作情報を，IP自体の機能への影響を最小にするポストレイアウト設計段階における新ウォーターマーク法を提案する。

我々は,Watermarkingにより設計著作者情報を埋め込んだ物理設計IPを不正使用から保護するための方法。処理の流れの概要は，以下の工程となる：

i）著作情報をビット列に変換しDES暗号化する。

ii）　暗号化された著作情報を物理設計IPに，ウォーターマーク手法により埋め込む。

iii）　IP利用者は，DES暗号キーと，レイアウト設計を利用する。

iv）　物理設計IPを利用したSoC設計からWatermark情報を抽出し，DESによる復号化により正当性をチェックする。

我々の提案したポストレイアウト設計段階における実験をおこなった。物理設計ベンチマーク回路としては、64ビット情報を数回刻印することができる3端子ネット（192ネット，576端子）を生成し，端子位置をランダムに配置して多層迷路配線により結線したレイアウトデータを作成した。ベンチマーク回路の配線領域は150x150グリッドだ。実際我々は5つのタイプの回路お30種類ずつ,合計で150種類の回路を用意した。

個々のベンチマーク回路に対して、全情報の書き込み成功率は，3回の試行でいずれも90%より多なった。実際の回路では，より広い配線領域とより多くのネット数が期待できることから,5～6回繰り返すことが可能であり,書き込み成功率を100%に近づけることが可能であることがわかった。同時、同じ機能をもつレイアウト設計で，Watermarkingに起こった変化も気づくことが現実的に不可能であることがわかる。

私達は、本論文において，IPの著作情報をより確実に，DES暗号方式と特別な配線法を使って，数度にわたり繰り返して書き込まれた。そのため，ポストレイアウト設計で予想される配線変更の難しい問題を解決し，捏造に対して，耐性を強くすることができる。ウォーターマークテクニックが効果的で、安全で，高い確率で実現可能であることがわかった。物理設計IPについて，著作権者と利用者が安心して利用するための強い保護ツールであると考えている。

特定用途プロセッサの設計研究

数理情報科学専攻　情報科学講座　　　　　　前田一樹

現在携帯電話、デジタル家電製品や車載機器などをはじめとするさまざまな製品の中核部分としてLSIが搭載されている。

半導体集積回路製造技術の進歩により、わずか10数ミリ四方のLSIチップ上に集積できるトランジスタ数は例えばメモリの場合、数億トランジスタにも達している。半導体集積回路の微細化が進んでいるために、半導体の集積度は18ヶ月で2倍という高い値を維持しつづけている。

このような集積回路製造技術を用いると、大規模な電子システムを単一のLSI上に実装可能になる。そのような大規模集積回路は、システムLSIと呼ばれている。

しかしそこで大きな問題が生じてくる。LSIの集積度が飛躍的に伸びるということは、設計規模と設計の複雑さが爆発的に拡大し、設計生産性が製造技術の進歩に追いつかない、つまり半導体の集積度の向上率に対して、その設計生産性の伸びは低いということである。そこでLSIの大規模化・複雑化に対応する設計手法にも革新が起こった。RTL回路をHDL（Hardware Description Language：ハードウェア記述言語）で記述し、LSIをトップダウン的に設計する手法が開発され、広く用いられるようになってきた。

HDLを使ってLSIの設計を行うことにより次のようなメリットが生まれる。まず、RTLはゲートレベルより上位の階層なので回路表現の抽象度が高く構成要素の数が少ないため、大きい規模の回路を短期間で設計できることである。次にRTL設計の段階でシミュレーションを行うことが出来るので、バグの発見、HDLの修正、シミュレーションの繰り返しをすばやく行うことが出来ることである。次にRTL回路をHDLで記述し、論理合成ツールに入力すれば、論理回路が出力されるので、人的要因によるケアレスミスや時間短縮できるということである。

このHDLを用いて特定用途プロセッサの設計について説明する。

楕円曲線上のトレース写像を用いた暗号方式

数理情報科学専攻　情報科学講座　佐伯忠典

1. 序

近年、公開鍵暗号の分野では、楕円曲線暗号に注目が集まっている。それは、他の暗号方式（例えばRSA暗号）に比べて鍵サイズが小さくてすむことにある。実際、RSA暗号において、1024bit、4096bitと同等のセキュリティレベルを楕円曲線暗号においては、173bit、313bitで実現できる。このことは、小さな計算処理能力、少ないメモリ領域で実装可能であることを意味する。本研究では、楕円曲線上に新しい暗号システムを提案し、実装したので、これを報告する。

2. 暗号システムの概要

有限体 F_p 上定義された楕円曲線 E に対し、トレース写像

$$Tr : E(F_{p^f}) \to E(F_p)$$

を定義することができる。このとき、核

$$Ker(Tr) = \{P|Tr(P) = 0\}$$

が群構造をなすことを利用して、ElGamal方式を適用した暗号システムが設計できる。このシステムにより、従来の楕円曲線暗号に比べ、セキュリティレベルを同等に保ったまま鍵サイズの縮小、計算処理にかかる負荷の軽減につながることが期待できる。

3. 実装上の課題

次数 f が増すごとに、$Ker(Tr)$ の定義方程式が複雑になるので（$f = 6$ のときは8個の連立方程式）、情報を群の点に対応させるアルゴリズムに工夫が必要になる。このため現時点で実用レベルの実装に成功しているのは $f = 2$ の場合で、$f = 6$ の場合はプロトタイプまでが完成している。次なる目標は $f = 30$ である。

4. $f = 2$ の場合

$Ker(Tr)$ 自体は E のtwistと同型であることが判明した。計算処理速度、鍵サイズともに従来のものより大きくなるにも関わらず、セキュリティレベルが変わらない。このことから、このままではメリットがない。しかし、$Ker(Tr)$ と元の曲線 E を同時に利用することでこのデメリットを解消できる。さらには従来の楕円曲線暗号の欠点である冗長ビットを除去することも可能となった。また、2つの曲線を同時利用する際にどちらの曲線も位数が十分に大きな素因子をもつ問題（Pohlig-Hellman攻撃に対する安全性）についても実験により無作為に選ばれた曲線が約50％で条件を満たすことも証明された。

量子エンタングルメントによる量子情報処理

数理情報科学専攻　情報科学講座　鄭　琳琳

量子レジスタの状態は各々の量子ビットが分けられるかどうかで、分離可能な状態か分離不可能な状態に分類できる。この分離不可能な絡み合い状態はエンタングルメント状態と呼ばれ、量子情報処理独自の資源として非常に重要であると考えられている。現在までに、2 量子ビットのエンタングルメント状態は深く研究され、明確に理解されている。しかし、量子ビットの数が増えると量子状態は複雑になって、エンタングルメントの種類と程度の判定が困難になる。本研究においては、「k–subsystem total semi-separability (TSS)」と「k–subsystem partial semi-separability (PSS)」と呼ばれる二つの判定基準 [1] を使って、多粒子系エンタングルメント状態の判定を行った。

n 個粒子を含む多粒子系を k 組 ($n > k$) のサブシステムに分割して、k 組のサブシステムの分離可能性をチェックしたとき、互いに分離可能なら、完全に準分離できる k 組のサブシステム (TSS) と定義する。互いに分離できない場合、必ず何らかのエンタングルメントを含むことになり、その場合は $\overline{TSS}$ と表記する。一方、その n 粒子系を $k+1$ 組のサブシステムに分割して、まず、任意の一組のサブシステムをのけて、残った k 組のサブシステムの分離可能性をチェックしたとき、互いに分離可能なら、部分的に準分離できる k 組のサブシステム (PSS) と定義する。互いに分離不可能な場合、必ず何らかのエンタングルメントが含まれ、それを $\overline{PSS}$ と表記する。この 2 つの判定方法を使えば n 粒子系は 2 粒子系に分解される。個々の粒子と粒子の関係を明らかにした後、元の n 粒子系の状態を判定することができる。

この 2 つの判定方法から四つの結果を得た。**(1)** あらゆる TSS あるいは PSS が成立する純粋状態は分離可能な状態であるための必要十分条件になる。**(2)** $\overline{TSS}$ あるいは $\overline{PSS}$ が存在する純粋状態はエンタングルメント状態であるための必要十分条件になる。**(3)** あらゆる TSS あるいは PSS が成立する混合状態は分離可能な状態であるための必要条件になる。**(4)** $\overline{TSS}$ あるいは $\overline{PSS}$ が存在する混合状態はエンタングルメント状態であるための十分条件になる。この四つの結果を使えば量子レジスタの状態を判定しやすくなると考えられる。

エンタングルメント状態を判定するのはそれを応用するためである。エンタングルメントは、近年急速に発達している量子情報処理における重要な資源であり、量子コンピューティングや量子テレポーテーションなどに利用されている。

参考文献

[1] “Multi-particle Entanglement via Two-Particle Entanglement” , Gilles Brassard and Tal Mor , C.P. Williams (Ed.): QCQC’98, LNCS (Lecture Notes in Computer Science) **1509**, pp.1-9 (1999).