

平成17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

# Weil 対を用いた認証システムの実現

数理情報科学専攻 情報科学講座 太田 浩 祐

## 1. はじめに

従来のデジタル署名は RSA 暗号や ElGamal 暗号を応用して実現されていたが、近年、双一次形式を利用したデジタル署名が注目されてきている。中でも、双一次形式のひとつである楕円曲線上の Weil 対の応用に関して研究が進み、supersingular な楕円曲線を利用する方式が既に実用レベルに達している。

本研究では CM 曲線と呼ばれる楕円曲線の中で特に Weil 対計算に適した曲線の生成方法について報告する。この方法の利点は、確実かつ短時間に目的の楕円曲線を生成できることである。

## 2. Weil 対

$E$  を有限体  $K$  上の楕円曲線とすると、 $\bar{K}$ -有理点のなす群  $E(\bar{K})$  はねじれ群である。自然数  $n$  に対して  $n$ -分点のなす部分群を

$$E[n] = \{P \in E(\bar{K}) \mid nP = \mathcal{O}\}$$

で定義する。Weil 対とは、 $\bar{K}$  における 1 の  $n$  乗根の群  $\mu_n$  への関数

$$e_n : E[n] \times E[n] \rightarrow \mu_n$$

である。Weil 対は Miller のアルゴリズムによって計算が可能であり、また双線形性を持つことからデジタル署名への応用が期待されている。ただしその時  $E[n]$  の点の座標を全て含む体を扱う必要があり、ランダムな楕円曲線ではその体が極めて大きくなるため実用化は望めない。

有限素体  $F_p$  上の楕円曲線  $E$  がもし条件

$$E(F_p) \supseteq (Z/nZ) \times (Z/nZ) \dots (*)$$

を満たすなら、全ての計算が  $F_p$  内で行え理想的であると言える。(上記 supersingular の場合は拡大体を必要とする。)

## 3. CM 曲線

$E$  の自己同型環  $\text{End}(E)$  が虚二次体のある整環に等しいときこの曲線は虚数乗法 (complex multiplication) を持つと言い、暗号への応用を考えて意図的に生成した場合特にこれを CM 曲線と呼ぶ。

有限素体  $F_p$  上の CM 曲線では、Frobenius 写像  $\varphi_p$  は  $\text{End}(E)$  に属しており、 $\varphi_p$  を整数底の一次結合として表した係数を用いて

$$E(F_p) \cong (Z/dZ) \times (Z/d'Z)$$

となる  $d, d'$  を書き下すことができる。本研究ではこの事実を利用して数百ビットの自然数  $n$  に対して (\*) を満たす CM 曲線  $E/F_p$  を生成することに成功した。

## 4. アルゴリズム

従来の CM 曲線生成アルゴリズムには、基本判別式  $-D$  と素数  $p$  を指定して

$$4p = u^2 + Dv^2$$

を満たす  $u, v$  を求めるステップがあるが、条件 (\*) を満たすためにはさらに条件

$$u \equiv 2, v \equiv 0 \pmod{n} \dots (**)$$

が必要になる。そこで我々は (\*\*) の条件下で先に  $u, v$  を走らせ  $p = (u^2 + Dv^2)/4$  を素数判定することにした。このアイデアにより曲線の生成時間が飛躍的に短縮された。

## 5. まとめ

本研究では双一次形式を用いたデジタル署名に有効な楕円曲線を生成する効率的なアルゴリズムを見つけることができた。現在、楕円曲線暗号では鍵長 200 bits あれば安全であると言われている。このアルゴリズムを用いれば鍵長 200 bits の楕円曲線が数十秒程度で生成できるようになった。

## データベース応用ソフトウェアの構築手法に関する研究

### — Plone/ArcheTypes を用いたシラバス作成システム —

数理情報科学専攻 情報科学講座 木谷由実

現在、インターネットの普及により、この情報空間を支える基本的な技術のひとつとしてデータベースの重要性が認識されている。たとえば、インターネットにおいて提供されている情報ページにおいてはその外観デザインとコンテンツを切り離し、コンテンツをデータベースによって管理する、コンテンツ管理システム(CMS: Content Management System)が導入されるようになってきている。ここで取り上げる、Zope は Web・FTP サーバの機能を備えたオブジェクトデータベースであって、その上に Plone を組み合わせることによりポータルサイトを構築することができ、さらに ArcheTypes を用いてコンテンツのタイプを定義し、各種のウェブ情報サービスに応用を広げることができる。

一方、本研究で取り上げる高知学園短期大学においては、平成 15 年度に学内ネットワークが再整備されて学内の至る所から Web アクセスが可能となったことから、シラバス公開システムの導入が課題となっていた。本研究では、オープンソースの CMS ソフトウェアが利用可能となってきている状況を考慮し、単なる公開システムではなくシラバスの作成から公開までを一貫して行えるようなシステム構築を目指した。

シラバス作成システムでは、担当教員によるシラバス原稿の作成から教務係への提出、教務係での点検と公開といった作業が必要であるが CMF が提供するワークフローにより、全てをウェブ上で管理することが可能となる。また、シラバスには、教員が作成する教科の授業計画だけでなく対象学科・学年・開講時間・教科書参考書の指定など、各種の付加情報が必要であるが、ArcheTypes を利用することでデータ型の定義を統一かつ容易な形で実現することができた。

また、ウェブインタフェースからのシラバス投稿は一般の教員にとって扱いやすいものであるが、教務係において雛形を作成するなどの、繰り返し同じ作業が発生する場合には GUI の利用は大変な作業となる。このため、過去に Word 文書で作成されたシラバスを一括投稿することができれば、このシステムがより便利になると考え、Python スクリプトを用いて自動投稿プログラムを作成した。

以上の研究を通じて、オープンソース CMS の利用によって、従来よりも安価に十分な機能を備えたデータベース応用ソフトウェアを構築することができた。

## ネットワーク応用ソフトウェアの構築手法に関する研究

### — Plone/ArcheTypes を用いたシラバス公開システム —

数理情報科学専攻 情報科学講座

須藤藍子

現在、インターネットは情報提供者・利用者数の拡大という量的な面だけでなく、各種サービスの充実という意味で質的な発展を遂げつつある。とりわけ、検索とその結果を利用した動的な情報提供の仕組みが発展してきており、この面でのソフトウェア構築手法の進化も目覚ましい。インターネットにおける情報検索では、ロボットによるページ収集とその結果を利用した検索サイトがよく利用されている。

しかし、一方で外部の検索サイトに依存した方法では、自組織内でのみ利用するような情報を検索することはできず、自前で検索インタフェースを構築する必要がある。たとえば、自組織内の情報がサーバ上のファイルという形で存在すれば、検索コマンドを利用することも考えられるが、一般には検索効率を考慮して特別なインデックス作成・検索ソフトを利用しなければならない。この場合にも、ページ作成からインデックス作成までの間は検索ができないことになる。

また、検索だけでなく、サイトのページを複数の製作者が分担する際にそのデザインを統一したり、掲示板・カレンダー・ブログといった類型的なパターンを持ったページを効率的に作成したいという要求から、最近、CMS (Content Management System) が注目されている。CMS ではサイトのページにおいて外観的デザインとコンテンツ(本文)を切り離し、作成・編集・管理・公開など一連の作業をウェブ上から行えるようになっており、コンテンツ作成と同時にインデックスの更新が行えて、従って、直ちに検索可能となるものもある。

本研究においては、そのような多機能 CMS のひとつである Zope/Plone 上に新しいページの「型」を定義できる ArcheTypes を利用して、高知学園短期大学向けのシラバス公開システムを作成した。本システムにおいては、シラバス本文内に記述された言葉をキーワードに全文検索を行うだけでなく、シラバス「型」に学科・学年・開講時間などの変数をキーワードとして登録することによって、(1)時間割表示、(2)教員名検索、(3)免許・資格取得のための検索、(4)トピック検索など多彩な応用が可能となっている。さらに、教員は Plone の持つ CMS としての機能を全て利用できるため、シラバスだけでなく講義資料の作成、掲示板を利用した質疑応答、ブログの作成などを行うことも可能で、今後 e-Learning システムへの発展も可能と思われる。

# グローバル配線の評価関数の考察

数理情報科学専攻 情報科学講座 小嶋 真平

高度情報化社会とともに電子機器の高度化が進んでいる。その心臓部となる大規模集積回路には高速・高性能な機能が要求されこれらの設計方法が求められている。その中でもレイアウト設計は信号配線経路を決定付けるため重要である。その配線が一部に集中した場合、配線が未完となることさえ生じる。そこで、通常的设计では、配線密度を評価して大まかな経路を決定するグローバル配線処理がおこなわれる。

一般的なグローバル配線においては、配線密度を均質化するため配線領域内の配線通過密度の分布の評価について自乗和などが用いられてきた。それは自乗和により均質化が図れるからである。しかし、自乗和の最小化を目指した場合、混雑度の高い場所の改善は進むが、逆に混雑の問題のないところへの配線分散を進めるという難点をもつ。その結果、最も配線混雑度が高い場所が改善されず、その領域において未配線が起こることもある。

そこで本研究では、配線の密度分布において最大となる領域への配線経路の通過を改善し、配線密度の小さい領域については考慮しない新たな評価関数を考案した。同評価関数は、配線密度の低い領域は感知しないため「より自由度が高い」と思われ、そのためより改善された結果が得られると考えたためである。

提案する評価関数と従来の評価関数を比較するためにランダムに発生した2ピンネットのデータに対して適用することにした。最適化する手法は、ペアワイズ交換法(グリーディ手法)、およびシミュレーテド・アニーリング(SA)法の2種類で評価した。その結果、提案手法は3~4%最も配線が混雑している領域が改善された配線経路を得られることがわかった。

## 製造コスト最小を目指す自動再配線法

数理情報科学専攻 情報科学講座 武永 秀

大規模な素子を1チップLSIに搭載するため、半導体製造の微細化プロセスが進展している。微細化は同時に配線遅延、歩留まりの低減、マスクコストの増加などの様々なDSM(Deep-Submicron問題)を深刻化させる。

特に、多品種少量生産を基本とするSoCでは、設計エラーや仕様変更の回数も多くなるためマスク修正期間やマスク製造コストが問題となる。

一方、従来の設計技術は、設計機関を短時間に済ませるため、「既存の設計を修正するインクリメンタルレイアウト」が提案されている。しかし、修正に要するマスク層数の最適化に関しては知られていない。

そこで、マスクコストも同時に削減する再配線法、すなわち配線マスク層数のより少ない変更により再配線を行う多層再配線手法の研究を行った。

提案手法は、従来の配線法が各配線層を効率的に使うための経験則として層毎に縦方向・横方向を使った配線制限(HVルール)が用いられてきたのに対して、再配線に限って制限を取り除く方法である。さらに、Via(層間をつなぐ接続)に特別な重みを付加する方法などを加えた。

本手法による再配線システムを構築し、数万の配線端子を持つベンチマーク回路(IBM01)を分割したいくつかの部分回路について評価を行ったところ、再配線に限りHVルールを取り除くことによって、各配線層の隙間を使った縦横自由(非HVルール)配線が実現し、使用層数が11層から10層まで削減することがわかった。

また、別の実験では、配線抵抗の大きいVia(例えばTSMCのプロセスルールによるとVia1個あたり配線長500単位分に相当することもある)数を削減することが出来るなど、DSMの配線遅延の改善や歩留まり向上にも役立つ配線手法であることがわかった。

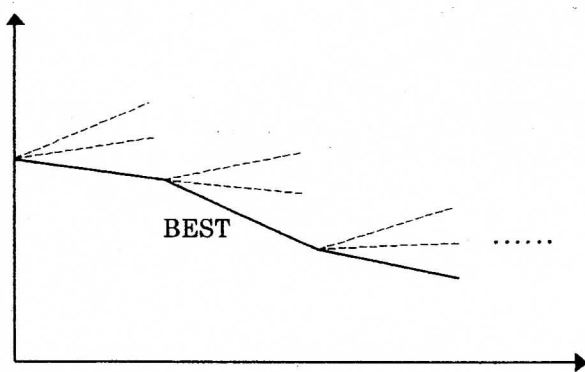
# ばらつきを考慮したシミュレーテドアニーリング法

数理情報科学専攻 情報科学講座 田辺和之

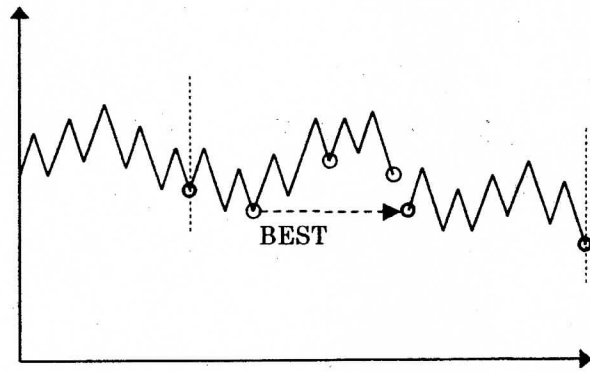
近年の VLSI (Very Large Scale Integrated Circuit ; 超大規模集積回路) の設計では、半導体プロセスの微細化に伴う配線抵抗の増加や、電圧降下、熱集中などの様々な DSM (Deep-Submicron) 問題への対処が不可欠となっている。このような多数の因子からなる複雑な問題の最適近似解を求める方法として、シミュレーテドアニーリング (SA) 法が用いられる。

シミュレーテドアニーリング (SA) 法は、多数の要素から構成される組み合わせ問題について、評価関数を擬似エネルギーとみなし、擬似温度  $T$  において、擬似乱数を用いた組み合わせ変更と評価を繰り返して熱平衡解を求め、徐冷によりごく低温における組み合わせを導出して近似最適解とする手法であり、経験的なアルゴリズムに比べて高品質な解が得られることが知られている。SA 法では、擬似乱数を利用し、熱平衡解に至るまでの繰り返し回数や、次の温度へ移る冷却割合により、得られる近似解の品質に影響を与えるが、そのばらつきについての定量的な実験は、われわれの知る限り報告されていない。

本論文で、われわれは簡単な配置問題に限って SA 法が近似解に至る過程におけるばらつき範囲の上限、下限を定量的に求める方法として、CASE-1 と CASE-2 の 2 手法を提案し、実験をおこなう。



CASE-1 のイメージ



CASE-2 のイメージ

実験の結果、CASE-1 において、最終解における上限、下限の評価値の差は 30 ~ 50% 程度になることが判明した。CASE-2 においても同様に、最終解の評価値に差が見られた。本手法は、様々な SA 改善手法において、従来の SA 法を用いた手法との改善の効果をより確実に評価することができる。また、本手法の下限プロセスを利用することによって、より安定して良質な近似解が得られるアルゴリズムとして用いることができると考える。

# タイル群によるフロアプラン法の研究

数理情報科学専攻 情報科学講座 趙 岩松

近年、電子機器は目覚ましい進展を遂げている。その中心的な部品は半導体によって設計製造されるLSI(Large Scale Integration)チップである。より性能のいいLSIを作るために、CPU、メモリ、制御論理、データ処理回路、インターフェース回路といったシステムの主要素を1チップに集積したLSI (SoC: System on a Chip) が開発されている。それに伴って、VLSIレイアウト設計の大規模化が進み、信号遅延の改善をはじめ、チップ面積、消費電力などさまざまな新たな問題が生じている。

これらの問題に対して、大局的な改善方法として、配線長、チップ面積と信号伝播遅延などを考慮するより良質なフロアプランが必要不可欠である。

フロアプランモデルとしてシーケンスペア表現やBツリー表現などが提案されているが、これらはスライス構造を前提としており、非スライス構造や配線長の考慮が困難であるため、根本的なモデルの見直しが必要であると考える。

本研究はこのような複雑な組み合わせ問題に有効に適用される最適化手法シミュレーテドアニーリング法 (Simulated Annealing法: SA) を用いて、フロアプラン問題に取り組んだ。SAを利用して、大規模なブロックを扱う場合は最適解を得られない場合はあるため、ブロックを小領域(タイル)に分割して、ブロック内部仮想接続を設けることにより、形状に依存しない柔軟なフロアプラン配置モデルを提案した。MCNCフロアプランベンチマークに対して、小領域(タイル)に分割するフロアプランモデルの有効性を確かめた。そして、大小さまざまなブロックを扱う場合でも、配線長の最小化などの最適解を得ることができた。