楕円曲線暗号ハードウェアの構成法と設計評価

白勢 政明 (110062)

北陸先端科学技術大学院大学 情報科学研究科

2003 年 2 月 14 日

キーワード: 楕円曲線暗号, 剰余計算アルゴリズム, 暗号演算, Wallace tree 乗算器.

1 研究の背景と目的

情報化社会の進展にともない情報セキュリティの重要性が増大している。暗号技術は情報セキュリティにおける主要な技術の 1 つである。大きなネットワークによる不特定多数の人との通信には暗号化鍵を公開できる公開鍵暗号が適している。

楕円曲線暗号は一般的な公開鍵暗号である RSA と較べて、同じ安全性に対する鍵長が短く、ソフトウェアによる処理が速いという長所を持つ公開鍵暗号である。しかしながら楕円曲線暗号の処理は十分には速くはない。本研究は楕円曲線暗号の処理を効率的かつ高速に行うためのハードウェアを設計する。

2 楕円曲線暗号

楕円曲線は $E : y^2 = x^3 + ax + b$, や $E : By^3 = x^3 + Ax^2 + x$, などで表される 3 次曲線で、前者は Weierstrass 型、後者は Montgomery 型と呼ばれる。F_p を元の個数が素数 p の有限体とする。集合

$$E(F_p) = \{(x,\ y) \in F)p \times F_p : x \text{ と } y \text{ は楕円曲線の式を満たす } \} \cup \{\mathcal{O}\},$$

を E の F_p 有理点の集合という。$\mathcal{O}$ は無限遠点と呼ばれる特別な点である。$E(F_p)$ は $\mathcal{O}$ を零とする群になっている。つまり $E(F_p)$ の元 $P,\ Q$ に対して $P + Q$ が定義できる。$P + P + \cdots + P(t$ 個の和) を tP と書く。楕円曲線暗号は tP と P から t を求めるのは困難であるという性質を利用している。

楕円曲線暗号システムでは $E(F_p)$ と $E(F_p)$ の元であるベースポイント B が公開されている。暗号システム参加者は任意の整数 s を選び、$P_k = sB$ を計算する。s が秘密鍵となり、P_k が公開鍵となる。

P_k の公開者へのメッセージ m の暗号文は $(C_1,\ c_2) = (rB,\ x(rP_k) \oplus m)$ となる。ここで r は乱数値、$x(rP_k)$ は rP_k の x 座標、$\oplus$ はビット毎の排他的論理和を表している。復号化は $x(sC_1) \oplus c_2$ を計算する。

楕円曲線暗号では $E(F_p)$ の元 P と整数 t から tP を計算することが主な処理となる。tP の計算には $P+Q$ を計算するための加算公式と $2P$ を計算するための 2 倍公式を使う。これらの公式には F_p での四則演算が必要である。元の個数が素数 p である有限体 F_p では、加減乗算は普通に計算した結果の p による剰余をとればよい。F_p では $x/y = x \cdot y^{p-2}$ となり、除算は乗算に還元される。

本研究では $p = 2^n - k,\ k^2 < 2^n,\ k > 0$ の場合のハードウェア処理に適した剰余アルゴリズムを紹介する。このアルゴリズムを使うことで楕円曲線暗号の暗号処理を高速に行うことができるようになる。

3 暗号処理の効率化

F_p での除算は $x/y = x \cdot y^{p-2}$ で得られるが、べき乗計算には多くの乗算が必要なので、除算はコストが大きい。2 つの除算 $a/b,\ c/d$ を $a/b = ad(bd)^{-1},\ c/d = bc(bd)^{-1}$ と計算すれば $(bd)^{-1}$ を求めるための 1 回の除算で 2 つの除算結果が得られる。この方法を取り入れると暗号処理に必要な乗算を約 8%減らせる。

$X_0, X_1, X_2, X_3 \in (F_p),\ i, j \in \{0, 1\}$ に対して暗号演算 $ecc(X_0, X_1, X_2, X_3, i, j)$ を

1. $Y_0 = X_0 + X_1,\ Y_1 = X_2 - X_3$,
2. $Y_i \cdot Y_j$ を返す,

と定義する。楕円曲線暗号の演算は ecc だけで計算でき、演算のための制御が簡単になる。

4 命令

暗号ハードウェアを制御するための命令形式は

オペコード	オペランド 0	オペランド 1	オペランド 2	next アドレス

となる。オペコード 0 とオペコード 1 は ecc で使用するデータのアドレスと出力先のアドレスが書かれている。例えば tP を求めるとき、t のあるビット t_i が 0 ならばオペランド 0 を使用し、t_i が 1 ならばオペランド 1 を使用する。

next アドレスには次の命令のアドレスが書かれている。暗号処理にはループがあり、ループの回数をカウンタで数え、カウンタが桁上りを起こすときループは終わるとする。カウンタの初期値やジャンプするときのアドレスがオペランド 2 に書かれている。

命令長は 80 ビットで、暗号ハードウェアが 14 段にパイプライン化がなされているときは 882 ワードの命令が必要となる。

5 暗号ハードウェアの概要

暗号処理には ecc 演算結果にあるデータとの排他的論理和をとる場合がある。この操作を行うコンポーネントを出力制御器と呼ぶことにする。暗号ハードウェアは ecc 演算器、出力制御器のほかに、入力データを一時蓄積するためのキューと乱数発生器と途中結果を記録するためのメモリと命令 ROM、制御器から構成される。

6 暗号ハードウェアの設計

ecc 演算器は F_p 加算器と F_p 減算器と F_p 乗算器をから構成される。本研究は p を 162 ビットの素数とするので、F_p 加算器は 162 ビット加算器と剰余計算器から構成される。162 ビット加算器は高速性を得るために桁上げ先見加算器とする。F_p 減算器は F_p 加算器と同様の構造となる。

F_p 乗算器も 162 ビット乗算器と剰余計算器に分けられる。高速性のために 162 ビット乗算器は小さなビットの乗算器の組合わせにするのではなく、162 ビットの Wallace tree 乗算器とする。162 ビット Wallace tree 乗算器は CSA 部の論理段数はわずか 36 段となる。Wallace tree 乗算器は一般に配線が複雑になるが、本研究では配線が簡単になるような配置を考える。特に部分的な斜め配線が可能ならば Wallace tree は単純な構造となる。

暗号ハードウェアの ecc 演算器以外の部分は簡単な構造となる。

7 性能評価

暗号ハードウェアを SFL で記述し、PARTHENON のシミュレータにより性能や回路規模を計測する。他の公開鍵暗号ハードウェアやソフトウェア処理との比較も行う。