2008－CSEC－41 (6)
2008／5／22

ペアリング演算ASICの開発

Vithanage Ananda [1] 猪俣 敦夫 [2] 岡本 栄司 [3] 岡本 健 [4] 金岡 晃 [3]
上遠野 昌良 [5] 志賀 隆明 [1] 白勢 政明 [6] 曽我 竜司 [5] 高木 剛 [6]
土井 洋 [7] 藤田 香 [5] Jean-Luc Beuchat [3] 満保 雅浩 [3] 山本 博康 [5]

[1] FDK 株式会社
[2] 奈良先端科学技術大学院大学
[3] 筑波大学
[4] 筑波技術大学
[5] FDK モジュールシステムテクノロジー株式会社
[6] 公立はこだて未来大学
[7] 情報セキュリティ大学院大学

双線形写像を利用するペアリング暗号は、ユビキタスネットワークに適した新しい暗号プロトコルを実現できるため、近年注目されている。しかしながら RSA 暗号のような普及している公開鍵暗号より、演算時間が数倍必要であることが欠点であった。我々はペアリング暗号を高速に計算するため、ペアリングアルゴリズムの軽量化、FPGA 実装を経て、世界初となるペアリング演算 ASIC、"Pairing Lite"を開発し動作確認を行った。Pairing Lite のゲート数は約 200,000、動作周波数は 200MHz で、1 回のペアリング演算を 46.7μ 秒で行うことを確認した。

ASIC Implementation of the η_T Pairing

Vithanage ANANDA [1] Atsuo INOMATA [2] Eiji OKAMOTO [3] Takeshi OKAMOTO [4]
Akira KANAOKA [3] Masayoshi KATOUNO [5] Takaaki SHIGA [1] Masaaki SHIRASE [6] Ryuji SOGA [5]
Tsuyoshi TAKAGI [6] Hiroshi DOI [7] Kaoru FUJITA [5] Jean-Luc BEUCHAT [3] Masahiro MAMBO [3]
Hiroyasu YAMAMOTO [5]

[1] FDK Corporation
[2] Nara Institute of Science and Technology
[3] University of Tsukuba
[4] Tsukuba University of Technology
[5] FDK Module System Technology Corporation
[6] Future University Hakodate
[7] Institute of Information Security

Pairing cryptosystems that utilize a bilinear map have attracted much attention because they can create new cryptographic protocols suitable for ubiquitous networks. However, their calculation time is several times longer than that for RSAs. We have developed an ASIC for calculating a pairing, "Pairing Lite," that is the world's first ASIC implementation of the pairing through improving algorithms for calculating the pairing and implementing FPGA. The scale of the circuit for Pairing Lite is about 200,000 gates, its operating frequency is 200 MHz, and it takes only 46.7μ seconds to calculate one pairing.

1 Introduction

近年の情報ネットワークの拡大によりインフラ化しつつあるネットワークでは、高い価値を持った情報のセキュリティが非常に重要なものとなっている。さらに、ユビキタスネットワーク時代にあたってはさらに多くの情報がネットワークで結

ばれることとなり、そのセキュリティは欠かすことができない。

現在では情報セキュリティを保持するためにさまざまな暗号技術が利用されている。一方で、拡張性の問題など現状の暗号技術では来るべきユビキタスネットワーク時代の要求に応じられないという面も存在し、新たな暗号技術の開発が急務である。

双線形写像を利用するペアリング暗号は、これらの要件を満たす新たな暗号技術である。ペアリング暗号は、非常に単純な公開鍵の扱いと鍵の共有プロトコルを不必要とすることが可能であり、公開鍵の取得などで複雑な機能を持つ公開鍵基盤（PKI）を容易にできる可能性がある。単純で安全というこれらの特性は、ユビキタスネットワークにおいては大きな効果を持つ。

ペアリング暗号に関する研究は実装を含め近年盛んに研究されており、大きな注目を浴びている。しかし、有効な特性を持つペアリング暗号は、現在主流の公開鍵暗号の方式であるRSAなどと比較して、計算量の面で問題を抱えており、計算量の軽量化に関する研究は大きな課題である。さらに数多くの実装も実施されているが、そのほとんどがソフトウェアやFPGAでの実装となっている。

本研究では、世界で初となるペアリング演算を行うASIC “Pairing Lite” の開発を行った。Pairing Liteは20万ゲートの規模と200MHzの周波数で動作し、ペアリングの演算を46.7μsecで実行する。第2章では実装に用いられたペアリングのアルゴリズムに関して述べ、3章ではPairing Liteのハードウェアアーキテクチャについて述べる。4章では開発したASICのハードウェア仕様と評価結果、また試作アプリケーションについて述べ、5章で本稿をまとめる。

2 ペアリング

ペアリングは、有限体上で定義される楕円曲線上の2つの点の入力と拡大体の元を出力し、双線形性（Bilinearity）を持つ関数である。双線形性は関数$e(P,Q)$が$e(P_1+P_2,Q)=e(P_1,Q)e(P_2,Q)$, $e(P,Q_1+Q_2)=e(P,Q_1)e(P,Q_2)$となる性質を言う。

ペアリングを計算する手法にはWeilペアリング、Tateペアリング、η_Tペアリング[1]、Ateペアリングがある。ペアリングを用いる暗号プロトコルではTateペアリングが最も多く利用されているが、計算コストの面や、Tateペアリングとの互換が可能なことなどからη_Tペアリングを実装した。

2.1 η_T ペアリング

Barretoらによって提案されたη_Tペアリング[1]は、標数3の場合に以下のようにあらわされる。

$$\eta_T : E^b(\mathbb{F}_{3^m})[l] \times E^b(\mathbb{F}_{3^m})[l] \rightarrow \mathbb{F}^*_{3^{6m}},$$

ここでE^bは$E^b : y^2 = x^3 - x + b$、$b=1$または$b=-1$で定義される超特異楕円曲線である。また$E^b(\mathbb{F}_{3^m})$は、x,y座標の双方が有限体$\mathbb{F}_{3^m}$の元である楕円曲線上の点の集合を表し、lは楕円曲線の位数である。

η_TペアリングはTateペアリングと下記の関係を持っており、Tateペアリングを計算するにあたり効率的にη_Tペアリングを利用することも可能である。

$$\left(\eta_T(P,Q)^W\right)^{3T^2} = \left(\hat{e}(P,Q)^W\right)^L$$

ここで$T=-\mu b 3^{\frac{m+1}{2}}$, $L=-\mu b 3^{\frac{m+3}{2}}$、また$\mu$は以下の値となる。

$$\mu = \begin{cases} +1 & \text{if} m \equiv 1,11 \pmod{12}, \text{or} \\ -1 & \text{if} m \equiv 5,7 \pmod{12}. \end{cases}$$

η_Tペアリングを計算するにあたり、Reversed-Loopアプローチ[4]を用いた。Reversed-Loopアプローチでは$\eta_T(P,Q)^{3^{\frac{m-1}{2}}}$を効率的に行うアルゴリズムを用いて、次のように入力を変えることとしてη_Tペアリングを計算する。

$$\eta_T(P,Q)^W = \left(\eta_T\left(P, \left[3^{-\frac{m-1}{2}}\right]Q\right)^{3^{\frac{m-1}{2}}}\right)^W$$

2.2 パラメータ設定

η_Tペアリングが十分な安全性を持つための条件として、楕円曲線の位数lが160ビット程度の素数であることが求められる。また同時に拡大体$\mathbb{F}_{3^{6m}}$のサイズも1024ビット程度の大きな値が求められる。

$m=97, b=1$の場合では、lは151ビットの素数であり、$\mathbb{F}_{3^{6m}}$のサイズは923ビットとなる。これはそれぞれ多少小さな値となっているものの、多くのη_Tペアリングの研究や実装ではこのパラメータが用いられている[2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13]。

本研究でもこれらのパラメータを利用した実装を行った。なお、より強い安全性を持つ

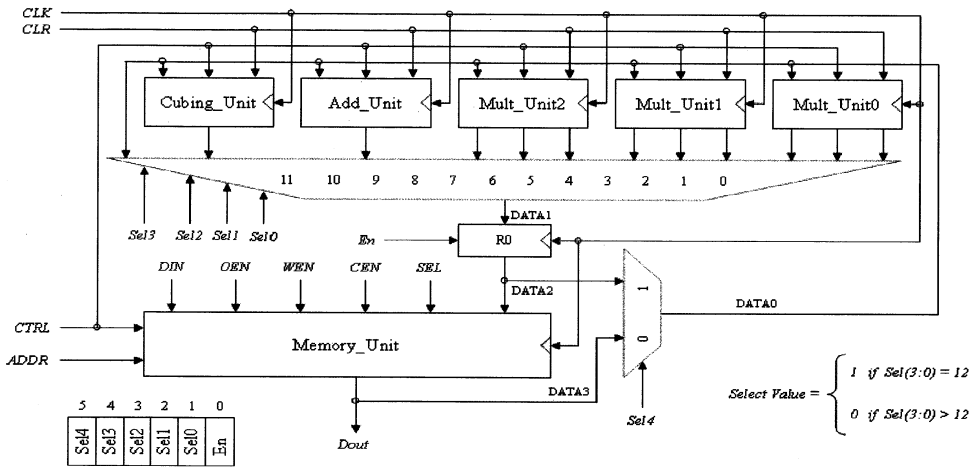

Fig. 1 Pairing Lite : η_T ペアリング ALU アーキテクチャ

パラメータの組み合わせとしては、$(m, b) = (167, 1), (193, 1), (239, 1)$ がある。

2.3 有限体上の演算

η_T を計算するにあたって、$\mathbb{F}_{3^{6m}}$ 上の乗算が必要になるが、$\sigma^2 = -1$, $\rho^3 = \rho + b$ となる σ, ρ を用いた基底 $\{1, \sigma, \rho, \sigma\rho, \rho^2, \sigma\rho^2\}$ を利用することで $\mathbb{F}_{3^{6m}}$ 上の元 A を以下のようにあらわせる。

$$A = A_0 + A_1\sigma + A_2\rho + A_3\sigma\rho + A_4\rho^2 + A_5\sigma\rho^2$$

ここで $A_i \in \mathbb{F}_{3^m}$ である。

これを利用して、$\mathbb{F}_{3^{6m}}$ 上の乗算を $\mathbb{F}_{3^m}$ 上の演算で行うことが可能である。

3 ハードウェアアーキテクチャ

3.1 拡大体上の演算

$\eta_T(P, Q)$ を計算するにあたり、標数 3 の場合では $\mathbb{F}_{3^m}$ 上の演算だけでなく、$\mathbb{F}_{3^{6m}}$ 上の乗算が必要となる。

前章で述べたとおり、これら $\mathbb{F}_{3^{6m}}$ 上のすべての演算は、すべて $\mathbb{F}_{3^m}$ の演算で置き換えることができる。$\mathbb{F}_{3^m}$ 上の演算を用いて効率的に $\mathbb{F}_{3^{6m}}$ 上の乗算を求める方法はいくつか存在し、Gorla らは、12 回の乗算と 59 回の加算により $\mathbb{F}_{3^{6m}}$ を求める方法を提案している [5]。また Beuchat らは 15 回の乗算と 29 回の加算により $\mathbb{F}_{3^{6m}}$ の乗算を行う方法を提案している [3]。Beuchat らの方式は、Gorla らの方式と比較して乗算回数が多いものの加算回数が少ないものとなっている。

また最終べきの計算に関しても $\mathbb{F}_{3^m}$ 上の演算以外にいくつかの演算が必要となる。その中で $\mathbb{F}_{3^{6m}}$ 上の乗算に関しては、Kerins らによる 18 回の $\mathbb{F}_{3^m}$ 上の乗算で計算する方法 [11] を採用し、同じく必要な $\mathbb{F}_{3^{3m}}$ 上の乗算に関しては、Beuchat らによる [4] 方法を採用した。

3.2 η_T ペアリング ALU アーキテクチャ

本研究で開発したハードウェアでは、η_T ペアリングを計算する ALU を以下の演算ユニットを用いて構成した (Fig. 1)。

- $\mathbb{F}_{3^{97}}$ 上の乗算ユニット:9 個
- $\mathbb{F}_{3^{97}}$ 上の加算ユニット:1 個
- $\mathbb{F}_{3^{97}}$ 上の 3 乗 (Cubing) ユニット:1 個

9 個の乗算ユニットと 1 個の加算ユニットという構成により、前項で示した双方の $\mathbb{F}_{3^{6\cdot 97}}$ 上の乗算を効率的に行うことが可能である。

3.3 FPGA によるペアリング実装事例

本研究で開発したペアリング演算 ASIC“Pairng Lite ” は世界初であるが、ペアリングの演算を FPGA で実装を行う研究は盛んに実施されている [6, 11, 14, 15]。筆者らも ASIC 実装に先立ち、

FPGA での η_T ペアリング演算の実装を実施済みである [2, 3, 4]。

[3] において、われわれの実装では実行速度に重きを置き、当時の FPGA でのペアリング演算の最高速を記録した。また [2] では、FPGA で利用するエリアの削減に焦点を当てた実装を行った。

4 ASIC の開発

2 章で示した η_T ペアリング、およびそれに必要なパラメータ、さらに 3 章で示したハードウェアアーキテクチャを用いて、ASIC を開発した。本章では ASIC の仕様や、ASIC 評価に用いる試作アプリケーションについて解説する。

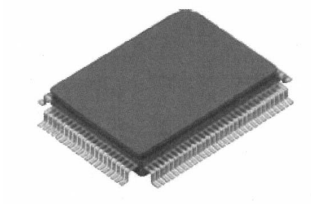

Fig. 2 開発した ASIC "Pairing Lite"

4.1 データ表現

$\mathbb{F}_{3^{97}}$ 上の元を表すため、われわれは多項式基底を用いて各係数を表す方法を選択した。$\mathbb{F}_{3^{97}}$ の元は、97 個の $\mathbb{F}_3$ 上の元の集まりとして表現でき、データ表現ではそれぞれの $\mathbb{F}_3$ の元 $0, 1, 2$ を '00', '01', '10' と表し、$\mathbb{F}_{3^{97}}$ 上の元はそれら係数データを接続した 194 ビットのデータで表現した。

4.2 入力と出力

ASIC は、$P = (x_p, y_p), Q = (x_q, y_q) \in E^1(\mathbb{F}_{3^{97}})[l]$ として、$\mathbb{F}_{3^{97}}$ 上の 4 つの元を入力とする。そして出力として $\eta_T(P,Q)^{49} = (A_0, A_1, A_2, A_3, A_4, A_5)$ を出力する。A_i は $\mathbb{F}_{3^{97}}$ 上の元であり、6 つの元により $\mathbb{F}_{3^{6\cdot 97}}$ 上の元を表している。

4.3 仕様

作成した ASIC の仕様を Table 1 に示す。

4.4 評価用アプリケーションの試作

ペアリングを利用した暗号プロトコルには ID ベース暗号 [16, 17] や、Short Signature[18] など多くの応用が存在する。これらのすべてがペアリングの持つ双線形性を利用して構成されたものとなっている。

Process	TSMC CL018G (0.18μm CMOS Logic General Purpose 1 p6M)
Scale	193,765 gates in 2NAND except ROM, RAM, IO
Speed	200 MHz
Calculation time	46.7μsec
Core size	$3,849.6\mu m \times 3,849.6\mu m$
Package	TSMC CQFP 100 pin
Memory configuration	2 RAMs and 1 ROM
Operating voltage	VDD CORE: 1.8V, VDD IO: 3.3V
Power consumption	Total power = 671.739 (mW)
Consumption current	Total current = 373,188(mA)
Temperature conditions	25°C
Output terminal	Drive capability 4 mA

Table 1 ASIC "Pairing Lite" 仕様

本研究では、Pairing Lite の開発を行うとともに、ペアリングを用いた暗号プロトコルを実装するアプリケーションを試作した。ID ベースで実現される暗号プロトコルや、Short Signature のように署名長が短いアプリケーションは、小さな計算力やメモリサイズ、低帯域に適していることから、試作アプリケーションでは RFID を用いたアプリケーションを開発した。

開発したアプリケーションは 2 つであり、ひとつは ID ベース暗号を実装したアプリケーションである。ID ベース暗号アプリケーションは Microsoft 社 Visual Studio .NET Visual C++で開発されたものであり、Pairing Lite を搭載した評価ボードを接続し、Windows XP/Windows 2000 の PC で動作する。また別のアプリケーションとして、Short Signature を実装したアプリケーションを開発した。こちらは C#で実装したアプリケーションであり、同じく評価ボードを接続し、Windows XP で動作する。

5 まとめ

ペアリングを用いた暗号技術は新たな可能性を多く提供する一方で、その計算コストに問題を抱えている。われわれは世界初のペアリング演算用 ASIC "Pairing Lite" を開発し、計算コスト問題の解消を図った。実行時間は 46.7μsec であり、ペアリングを利用した暗号システムの開発と拡大に寄与するものと考えられる。

Acknowledgement

本研究は独立行政法人 新エネルギー・産業技術総合開発機構（NEDO）の委託・助成により行われた。

参考文献

[1] P. Barreto, S. Galbraith, C. Ó hÉigeartaigh, and M. Scott, "Efficient pairing computation on supersingu-

lar abelian varieties", *Designs, Codes and Cryptography*, Springer–Verlag, Vol. 42, No. 3, pp 239-271, 2007.

[2] J.-L. Beuchat, N. Brisebarre, J. Detrey, and E. Okamoto, "Arithmetic Operators for Pairing-Based Cryptography", *CHES 2007*, LNCS 4727, pp.239-255, 2007.

[3] J.-L. Beuchat, M. Shirase, T. Takagi, and E. Okamoto, "An algorithm for the η_T pairing calculation in characteristic three and its hardware implementation", *18th IEEE International Symposium on Computer Arithmetic, ARITH-18*, pp.97-104, 2007.

[4] J.-L. Beuchat, N. Brisebarre, J. Detrey, E. Okamoto, M. Shirase, and T. Takagi, "Algorithms and Arithmetic Operators for Computing the η_T Pairing in Characteristic Three", *IEEE Transactions on Computers*, Vol. 57, 2008, to appear.

[5] E. Gorla, C. Puttmann, and J. Shokrollahi, "Explicit formulas for efficient multiplication in $\mathbb{F}_{36m}$", *SAC 2007*, LNCS 4876, pp.173-183, 2007.

[6] P. Grabher and D. Page, "Hardware acceleration of the Tate pairing in characteristic three", *CHES 2005*, LNCS 3659, pp.398-411, 2005.

[7] R. Granger, D. Page, and M. Stam, "Hardware and software normal basis arithmetic for pairing-based cryptography in characteristic three", *IEEE Transactions on Computers*, Vol. 54, No. 7, July 2005, pp.852-860, 2005.

[8] R. Granger, D. Page, and M. Stam, "On Small characteristic algebraic tori in pairing-cased cryptography", *LMS Journal of Computation and Mathematics*, vol. 9, pp.64-85, 2006.

[9] K. Harrison, D. Page, and N. P. Smart, "Software implementation of finite fields of characteristic three", *LMS JCM*, Vol. 5, November, pp.181-193, 2002.

[10] Y. Kawahara, T. Takagi, and E. Okamoto, "Efficient implementation of Tate pairing on a mobile phone using Java", *CIS 2006*, LNAI 4456, pp.396-405, 2007.

[11] T. Kerins, W. Marnane, E. Popovici, and P. Barreto, "Efficient hardware for the Tate pairing calculation in characteristic three", *CHES 2005*, LNCS 3659, pp.412-426, 2005.

[12] R. Ronan, C. Ó hÉigeartaigh, C. Murphy, T. Kerins and P. Barreto, "Hardware implementation of the η_T pairing in characteristic 3", Cryptology ePrint Archive, Report 2006/371, 2006.

[13] M. Yoshitomi, T. Takagi, S. Kiyomoto, and T. Tanaka, "Efficient implementation of the pairing on mobilephones using BREW", *WISA 2007*, to appear.

[14] R. Ronan, C. Ó hÉigeartaigh, C. Murphy, M. Scott, T. Kerins, and W. Marnane, "An embedded processor for a pairing-based cryptosystem", *Information Technology : New Generations, ITNG 2006*, pp.192-197, IEEE Computer Society, 2006.

[15] C. Shu, S. Kwon, and K. Gaj, "FPGA accelerated Tate pairing based cryptosystems over binary fields", Cryptology ePrint Archive, Report 2006/179, 2006.

[16] D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing", *SIAM Journal of Computing*, Vol. 32, No. 3, pp. 586-615, 2003.

[17] R. Sakai and M. Kasahara, "ID based cryptosystems with pairing on elliptic curve", Cryptology ePrint Archive, Report 2003/054, 2003.

[18] D. Boneh, B. Lynn, and H. Shacham, "Short signature from the Weil pairing", *Journal of Cryptology*, Vol. 17, No. 4, pp. 297-319, 2004.