様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年６月１８日現在

機関番号：２０１０３
研究種目：若手研究（B）
研究期間：2009～2011
課題番号：２１７０００８３
研究課題名（和文）　センサ・ネットワークへの次世代公開鍵暗号の効率的アセンブリ実装の研究
研究課題名（英文）　Efficient Assembly Implementation of Next-Generation Public Key Cryptosystem to Sensor Network
研究代表者
白勢　政明　（MASAAKI SHIRASE）
公立はこだて未来大学・システム情報科学部・准教授
研究者番号：70530757

研究成果の概要（和文）：本研究では、Block comb 法による η T ペアリングのセンサノードへのアセンブリ高速実装手法を確立し、センサノードへの実装を目的として Ate ペアリングを定義する有限体と楕円曲線の構成の効率化、Ate ペアリングの対称化、及びペアリング暗号によるタイムスタンプ署名方式を提案した。

研究成果の概要（英文）：This research provided a method for fast implementing the ηT pairing with assembly to sensor nodes using the Block comb method, proposed algorithms for efficiently constructing a finite field and an elliptic curve defining the Ate pairing, provided a method for modifying the Ate pairing from asymmetric one to symmetric one, and proposed a timestamp signature system using pairing.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	1,300,000	390,000	1,690,000
２０１０年度	800,000	240,000	1,040,000
２０１１年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,100,000	930,000	4,030,000

研究分野：総合領域
科研費の分科・細目：情報学、計算機システム・ネットワーク
キーワード：ネットワークセキュリティ技術

１．研究開始当初の背景

ワイヤレス・センサ・ネットワーク(WSN)は、数百または数千のセンサノードと、基地局から構成される。低消費電力、低価格及び小型という特徴により、センサノードはユビキタス・ネットワークに最適なデバイスであると言われている。しかしながら、WSN ではセンサノードが管理者不在の場所に設置されるため、セキュリティに関する攻撃が容易であると指摘されてきた。更に、ネットワーク共通の攻撃以外にも、ノード選択攻撃や複製ノードの設置等の WSN 特有の攻撃法が存在する。従って、WSN の安全性の確保は重要な課題であり、公開鍵暗号技術の応用はその解決策となる。そのため、センサノードへの公開鍵暗号の実装も近年盛んになっており、現在最も普及している RSA 暗号、鍵長の短い楕円曲線暗号(ECC)、楕円曲線の双線形性写像を利用する次世代(ペアリング)暗号の実装例があり、これらの公開鍵暗号の処理は数秒程度で可能となっていた。しかしながら，センサノードの計算資源の制約を考慮すると，ペアリング計算の低コスト化と高速化が必要であった。

２．研究の目的

(1) ηT ペアリングのセンサノードへの実装

本研究の当初の目的は、MICAz を含む代表的なセンサノードを実装対象とし、高速性、計算資源節約の双方の観点から、冗長なコードを削減するためアセンブリ・レベルでの、ηT ペアリングによるペアリング暗号の最適実装を行うことであった。

(2) Ate ペアリングの改良

しかしながら、当初ηT ペアリングが計算コストの面で最適なペアリングと一般的に考えられていたが、本研究の実施中に暗号分野において Ate ペアリングの研究が進行し、Ate ペアリングまたはその改良版が最も計算コストの低いペアリングとなった。そのため、本研究ではηT ペアリングの MICAz への最高速実装を達成した後、Ate ペアリングを実装対象に変更することとなった。Ate ペアリングのセンサノードへの実装を行う際、

① Ate ペアリングを定義する有限体と楕円曲線の率的構成法、
② 非対称である Ate ペアリングの対称ペアリング化、
③ 実用的なアプリケーションの検討、

が必要となり、これらを実施した。

３．研究の方法

(1) ηT ペアリングのセンサノード実装では、初めにアルゴリズムレベルでの高速化(Block comb 法の提案と Vandermonde 行列乗算法の改良)を行い、これらの成果を基にセンサノードへηT ペアリングによるペアリング暗号をアセンブリ・レベルで実装を行った。

(2)Ate ペアリングの改良及びアプリケーションの開発では、主に理論レベルとしての研究となった。センサノードへの Ate ペアリングの実装は今後の課題となる。

４．研究成果

(1) ηT ペアリングのセンサノードへの実装

①Block comb 法によるアセンブリ実装

センサノード MICAz 上に有限体$F_{3^{97}}$上のηT ペアリングを Block Comb 法を用いてアセンブリ実装を行った。なお、F_{3^n}上ηT ペアリングとは、双線形写像$E(F_{3^n}) \times E(F_{3^n}) \to F_{3^{6n}}$（$E$は$y^2 = x^3 + x \pm 1$で与えられる楕円曲線）のことである。Block comb 法とは、有限体乗算において、アセンブリ言語を使用することにより、 レジスタに可能な限りデータを取り込み、RAM とレジスタ間のメモリアクセスの削減を行う手法である。 Block comb 法の適用により，$F_{3^{97}}$上ηT ペアリングの計算時間が従来の 5.79 秒から 2.15 秒に改善され、2.69 倍の高速化が達成された。

②$F_{3^{6n}}$の元に対する Vandermonde 行列乗算法の改良

$F_{3^{6n}}$の元の高速乗算法に Vandermonde 行列乗算法があり、①の実装でも使用した。更なるηT ペアリングの高速実装のために Vandermonde 行列乗算法の改良を行った。従来の Vandermonde 行列乗算法では、$F_{3^{6n}}$を$F_{3^{6n}} = F_{3^{2n}}[\rho] \,/\, (\rho^3 - \rho - 1)$ 、 と $F_{3^{2n}} = F_{3^n}[\sigma] \,/\, (\sigma^2 + 1)$ と構成し、$F_{3^{6n}}$の元の乗算に 15 回のF_{3^n}乗算を要する。これに対して提案手法では$F_{3^{6n}}$を$F_{3^{6n}} = F_{3^n}[z]/\,(z^6 + z - 1)$と構成し、$F_{3^{6n}}$の元の乗算は$12 + 132/n$回の$F_{3^n}$乗算(及びシフト処理)、つまり漸近的に 12 回のF_{3^n}乗算で計算可能となった。

③改良 Vandermonde 行列乗算法の適用

改良 Vandermonde 行列乗算法は、実際にパソコン上でのペアリング計算には効果があることが確認できたが、センサノード IRIS(MICAz の後継機、RAM 容量以外 MICAz と同じ)へのηT ペアリング実装には、期待された効果が得られなかった。その原因として、IRIS が搭載している CPU は 8 ビットの ATMega128 シリーズであり、8 ビット CPU を用いるとき、パソコンが用いる 32 ビットや 64 ビット CPU と比較して，有限体の元のシフトに必要なシフト命令の回数が増大する、ATmega128 シリーズでは，シフト命令は加減算と同じ時間を要し速い処理とは言えない、ためであることが判明した。

```
movw    r30     R26
ldd     r5      Z+i
movw    r30     R2
ldd     r16     Y+i
eor     r16     R5
ld      r17     X+
mov     r15     R16
eor     r15     R17
ld      r4      Z
eor     r4      R17
or      r15     R4
std     Z+i     R15
eor     r5      R4
or      r16     R5
st      Z+      R16
movw    r2      R30
```

図 1 Block comb 適用前のアセンブリコードの一例

```
eor     r4      r16
mov     r15     r4
eor     r4      r17
eor     r5      r17
or      r4      r5
eor     r5      r16
or      r5      r15
```

図 2 Block comb 適用後のアセンブリコードの一例

図 1 のアセンブリコードが、Block comb 法により図 2 のように改良される。

(2)Ate ペアリングの改良

Ate ペアリングとは、双線形写像

$$G_2 \times G_1 \to F_{p^k}、$$

（但し、$G_1 = E[l] \cap (\pi_p - [1])$, $G_2 = E[l] \cap (\pi_p - [p])$ 、π_pはp乗 Frobenius 写像）であり、一旦拡大体、楕円曲線が構成されるとηT ペアリングより計算が低コストで高速となる。しかしながら、拡大体の構成には一般的には確率的要素が含まれ、試行錯誤が必要である。また、Ate ペアリングに使用できる楕円曲線の構成には一般には Complex Multiplication(CM) 法が必要である。Barreto と Naehrig が提案した手法(BN 法)では、$p = p(z) = 36z^4 + 36z^3 + 18z^2 + 6z + 1$ で与えられる素数p(BN 素数)に対して、F_p上の楕円曲線を構成する場合には CM 法は不要だが、その構成にも確率的要素は含まれる。これらは、センサノードにとっては、重い処理である。本研究では、3072 ビット RSA 暗号や 256 ビット楕円曲線暗号と同等の安全性レベルを持つ$k = 12$の Ate ペアリングに焦点を当て、Ate ペアリングのセンサノードへの実装をするため、拡大体と楕円曲線の効率的な構成法を研究し達成した。本研究のこれらの成果を使った Ate ペアリングのセンサノードへの高速実装は今後の課題となる。

更に Ate ペアリング問題点として非対称性、つまり Ate ペアリング$G_2 \times G_1 \to F_{p^k}$に対して第 1 引数の集合$G_2$と第 2 引数の集合$G_1$が異なっている点が挙げられる。センサノードに有効なアプリケーションに ID ベース暗号や放送型暗号、キーワード検索暗号があるが、これらの実装には対称ペアリングを用いる必要がある。本研究では Ate ペアリングの対称化を行った。

①拡大体$F_{p^{12}}$の普遍的構成

定理 1

BN 素数$p(z) = 36z^4 + 36z^3 + 24z^2 + 6z + 1$ に対して、$z \equiv 7,11 \pmod{12}$とする。すると

$$F_{p^2} = F_p[u] / (u^2 + 1)$$
$$F_{p^{12}} = F_{p^2}[v] / (v^6 - v - 1)$$

と構成できる。

この定理により、$z \equiv 7,11 \pmod{12}$と選ぶ時は、どんな BN 素数pに対しても、$F_{p^{12}}$を普遍的に構成できる。拡大体$F_{p^{12}}$を定義する既約多項式の係数がすべて± 1であるため、効率的な$F_{p^{12}}$上の四則演算も可能である。

②Ate ペアリングを定義する楕円曲線の構成

ここでは、Ate ペアリングを定義する楕円曲線の効率的構成に関する本研究での最終成果を説明する。

補題 2

$p(z) = 36z^4 + 36z^3 + 24z^2 + 6z + 1$を BN 素数とし、多項式$n_0(z)$、$n_1(z)$、$n_2(z)$、$n_3(z)$、$n_4(z)$、$n_5(z)$を以下のように定義する。

$n_0 = n_0(z) = 12z^2(3z^2 + 3z + 1)$
$n_1 = n_1(z) = 36z^4 + 36z^3 + 18z^2 + 1$
$n_2 = n_2(z) = 3(12z^4 + 12z^3 + 10z^2 + 2z + 1)$
$n_3 = n_3(z) = 4(9z^4 + 9z^3 + 9z^2 + 3)$
$n_4 = n_4(z) = 3(12z^4 + 12z^3 + 10z^2 + 4z + 1)$
$n_5 = n_5(z) = 36z^4 + 36z^3 + 18z^2 + 6z + 1$

また、δを$2^i 3^j$と表わされる有理数、$b = 16/\delta$とする。更に、楕円曲線$y^2 = x^3 + b$をE_bで表すことにする。すると、$\#E(F_p)$は以下で与えられる。

(a) δがpで立方剰余かつ平方剰余のとき

$\#E(F_P)$=
- n_0 $\#E_{16}(F_p) = n_0$のとき
- n_2 $\#E_{16}(F_p) = n_2$のとき
- n_4 $\#E_{16}(F_p) = n_4$のとき

(b) δがpで立方剰余かつ平方非剰余のとき

$\#E(F_P)$=
- n_1 $\#E_{16}(F_p) = n_4$のとき
- n_3 $\#E_{16}(F_p) = n_0$のとき
- n_5 $\#E_{16}(F_p) = n_2$のとき

(c) δがpで立方非剰余かつ平方剰余のとき

$\#E(F_P)$=
- n_0 bがpで立方剰余、かつ $\#E_{16}(F_p) = n_2$またはn_4のとき
- n_2 bがpで立方非剰余、かつ $\#E_{16}(F_p) = n_4$のとき
- n_4 bがpで立方非剰余、かつ $\#E_{16}(F_p) = n_2$のとき
- n_2またはn_4 $\#E_{16}(F_p) = n_0$のとき

(d) δがpで立方非剰余かつ平方非剰余のとき

$\#E(F_P)$=
- n_1 bがpで立方非剰余、かつ $\#E_{16}(F_p) = n_2$のとき
- n_3 bがpで立方剰余、かつ $\#E_{16}(F_p) = n_2$またはn_4のとき
- n_5 bがpで立方非剰余、かつ $\#E_{16}(F_p) = n_4$のとき
- n_1またはn_5 $\#E_{16}(F_p) = n_0$のとき

補題 2 から 2、3 の平方剰余性と立方剰余性が分かれば、$\#E_{2^i 3^j}(F_p)$を求めることができるが、これは比較的容易に可能である。以上より、命題 2 に「または」が含まれることによる一部の不確定さを除き、BN 体F_p上の$\#E_{2^i 3^j}(F_p)$が与えられた。ここで、位数がn_5の楕円曲線が Ate ペアリングに適している。なお、この不確定さは、″中島俊哉, BN 体上の楕円曲線$y^2 = x^3 + 2^i 3^j$ のトレースの全決定, ISEC 2011-30″によって解決された。

更に、本研究では、*k=4*、*6*、*8* の Ate ペアリングのための楕円曲線の係数の決定についても考察を行った。

④Ate ペアリングの対称化

命題 3

Ate ペアリング$e:G_2 \times G_1 \to F_{p^k}$対して、$g_1 \in G_1$、$g_2 \in G_2$をそれぞれ生成元とし、群$G$を$g_1 + g_2$で生成される群とする。

$$G =< g_1 + g_2 >$$

すると、Gは$E[l]\left(\subset E\left(F_{p^k}\right)\right)$の位数$l$の部分群となる。

命題 4

命題 3 と同じ記号を用いるとする。整数l'を

$$l' = (p-1)^{-1} \bmod l$$

とし、写像ext_1とext_2を

$$ext_1 = \left([p] - \pi_p\right) \circ [l']$$
$$ext_2 = \left(\pi_p - [1]\right) \circ [l']$$

と定義する。写像e_1を$P, Q \in G$に対して

$$e_1(Q,P) = e(ext_2(Q), ext_1(P))$$

と定義すると、以下が成り立つ。

(a) e_1は$G \times G$からF_{p^k}への写像。

(b) 任意の整数n, mに対して

$$e_1(ng, mg) = e(ng_2, mg_1)$$

が成り立つ。

(c) e_1は可換な対称ペアリング。

命題 5

命題 3、4 と同じ記号を用いるとする。群G'を

$$G' = \{\boldsymbol{g} = (ng_1, mg_2) : n, m\text{は整数}\}$$

と定義する。$\boldsymbol{g} \in G'$に対して、$\boldsymbol{g_1}$は$\boldsymbol{g}$の第 1 成分、$\boldsymbol{g_2}$は$\boldsymbol{g}$の第 2 成分を表すとする。$\boldsymbol{g}, \boldsymbol{g'} \in G'$に対して

$$e_2(\boldsymbol{g'}, \boldsymbol{g}) = e(\boldsymbol{g_2'}, \boldsymbol{g_1})$$

と定義すると以下が成り立つ。

(a)e_2は$G' \times G'$からF_{p^k}への写像。

(b) 任意の整数n, mに対して

$$e_2(n\boldsymbol{g}, m\boldsymbol{g}) = e(n\boldsymbol{g_2}, m\boldsymbol{g_1})$$

が成り立つ。

(c)e_2は可換な対称ペアリング。

これらの結果により、高速であるが非対称な Ate ペアリングを、対称ペアリングを必要とする暗号プロトコルへの使用が可能となった。

(3)センサノードに適したタイムスタンプ署名方式の提案

タイムリリース暗号では、受信者の公開鍵と送信者が指定する復号時刻の情報を暗号化鍵として平文を暗号化し、受信者の秘密鍵と時刻鍵を復号鍵として暗号文を復号する。なお、時刻鍵は時刻に時刻サーバから発行される。本研究では、ペアリング暗号によるタイムリリース暗号に基づき、時刻情報による署名検証で「受理」となることが、署名生成時刻を保証するタイムスタンプ署名を提案した。本方式はタイムリリース暗号の署名版である。提案方式におけるタイムスタンプ・サーバは、タイムリリース暗号と同じく時刻鍵を生成する機能を有し、時刻鍵を使ってタイムスタンプ生成を行う。なお、センサネットワークでは基地局が存在し、基地局に時刻サーバの機能を持たせることができるため、提案タイムスタンプ署名号式はセンサネットワークに適している。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計１件）

① Masaaki Shirase, Universal Construction of a 12th Degree Exstension Field for Asymmetric Pairing, IEICE Transactions, 査読有, E94-A, 2011, 156-164, http://search.ieice.org/bin/summary.php?id=e94-a_1_156

〔学会発表〕（計１１件）

① 白勢政明、MICAz への Vandermonde 行列乗算法の適用について、CSEC、2012 年 3 月 1 日、横浜市開港記念会館

② 白勢政明、埋め込み次数 4, 6, 8 の Pairing-friendly 曲線の定義体について、ISEC、2011 年 11 月 15 日、大阪電気通信大学

③ 白勢政明、吉田 洸輝、タイムリリース暗号によるタイムスタンプ署名、CSS2011、2011 年 10 月 19 日、新潟コンベンションセンター

④ 白勢政明、Barreto-Naehrig 体上の楕円曲線$y^2 = x^3 + 2^i 3^j$の位数、ISEC、2011 年 5 月 13 日、機械振興会館

⑤ 白勢政明、通常楕円曲線上の対称ペアリング、CSS2010、2010 年 10 月 20 日、岡山コンベンションセンター

⑥ 白勢政明、係数が固定されている Pairing-friendly 楕円曲線の構成法の改良、ISEC、2010 年 3 月 4 日、信州大学

⑦ 白勢政明、Ate ペアリングのための 12 次拡大体の普遍的構成、SCIS2010、2010 年 1 月 22 日、サンポートホール高松

⑧ 北村晃輔、白勢政明、MICAz 上における標数 3 のηT ペアリングの高速実装、SCIS2010、2010 年 1 月 21 日、サンポートホール高松

⑨ 北村 晃輔、白勢政明、MICAz 上でのηT ペアリング高速実装、CSS2009、2009 年 10 月 27 日、富山国際会議場

⑩ 白勢政明、係数が固定されている Pairing-friendly 楕円曲線、CSS2009、2009 年 10 月 26 日、富山国際会議場

⑪ Yuta Sasaki, Masaaki Shirase, Tsuyoshi Takagi, An Efficient Residue Group Multiplication for the ηT Pairing over F_{3^m}, SAC 2009, 査読有, LNCS5867,

364-375, 2009 年 8 月 14 日, カナダ・カルガリー大学
http://www.springerlink.com/content/g98323126037r768/

〔その他〕
ホームページ等
http://www.fun.ac.jp/staff/staff_arch/shirasemasaaki.html

６．研究組織
(1)研究代表者
白勢　政明（MASAAKI SHIRASE）
公立はこだて未来大学・システム情報科学部・准教授
研究者番号：7053075