コンピュータセキュリティ　14−11
(2001. 7. 25)

楕円曲線上のペアリングに基づく二, 三の暗号方式

境 隆一†,　　光成滋生††,　　笠原 正雄†††

†大阪電気通信大学
光システム工学科

〒 572-8530
大阪府寝屋川市初町 18-8
Tel:072–820–9024
FAX:072–820–9024
email:sakai@isc.osakac.ac.jp

††株式会社ピクセラ

〒 590-0985
大阪府堺市戎島 4-45-1

email:VEZ04653@nifty.com

†††大阪学院大学情報学部

〒 564-8511
大阪府吹田市岸辺南 2-36-1
Tel:06-6381-8434
FAX:06-6382-4363
email:kasahara@utc.osaka-gu.ac.jp

あらまし　従来, 楕円曲線上定義されたペアリングは楕円暗号の解読に応用されていたが, 近年, このようなペアリングが双線形写像であることを利用した暗号方式がいくつか提案されている. 本稿では, これらの暗号方式を紹介すると共に, 不正利用者の追跡が可能な放送用鍵配送の基本方式を提案する. この方式は, 黒澤-Desmet の方式では実現されなかった, 利用者の結託攻撃に対する安全性を有していると考えられ, 実用上も極めて重要な方式である. また, 新たなペアリングを利用した暗号方式についても考察する.

キーワード　Weil ペアリング, 鍵配送, 不正端末追跡, 公開鍵暗号, 電子署名

Cryptographic Schemes based on Pairing over Elliptic Curve

Ryuichi SAKAI†,　　Shigeo MITSUNARI††,　　Masao KASAHARA†††

†Osaka Electro-Communication University

Hatu-chou, Neyagawa-shi,
Osaka 572-8530 JAPAN
Tel:072–820–9024
FAX:072–820–9024
email:sakai@isc.osakac.ac.jp

††Pixela Corporation,

4-45-1, Ebisuzima, Sakai,
Osaka, 590-0985 JAPAN

email:VEZ04653@nifty.com

†††Osaka Gakuin University

Kishibe-Minami, Suita-shi,
Osaka 572-8530 JAPAN
Tel:06-6381-8434
FAX:06-6382-4363
email:kasahara@utc.osaka-gu.ac.jp

Abstract　Weil pairing and Tate pairing are the bilinear mappings from n torsion points of elliptic curves to a finite field. In this report, we review some cryptographic schemes based on Weil pairing or Tate pairing over elliptic curves. These schemes can be realized by the bilinear mapping of the pairings. We then propose a new key distribution scheme for broadcast encryption which is traceable traitors. The new broadcast key distribution scheme for the traitor tracing whose broadcasting data contain the constant header is firstly realized the security against the collusion attacks.

key words　Weil pairing, elliptic curve, key distribution, traitor tracing, public key cryptosystem, digital signature

1 まえがき

近年, 楕円曲線上定義されたペアリングは楕円暗号の解読に応用されていたが, 近年, ペアリングが双線形写像であるという性質を利用した暗号方式が多数提案されている.

以下に近年提案された Weil-Tate ペアリングを用いた暗号方式を列挙する.

Weil-Tate ペアリングを用いた暗号方式

1. ISEC(1999 年 11 月) (大岸, 境, 笠原)[5]
   結託フリーな IDNIKS
2. SCIS2000(境, 大岸, 笠原)[6]
   検証者指定グループディジタル署名の提案
   従来の結託攻撃 (DLP, ECDLP の安全性と等価)
3. ANTS(Antoine Joux) [7]
   3 者間 Diffie-Hellman 鍵共有法のための 1 ラウンドプロトコル
4. 暗号理論とそれを支える代数曲線理論 (2000,8 月 30 日-9 月 1 日)[8], SCIS2001 (境, 大岸, 笠原)[10]
   公開鍵暗号方式の提案
5. SCIS2001(光成, 境, 笠原)[11]
   不正利用者追跡法の提案 (結託閾値を改善)
6. SCIS2001(井上, 桜井)[12]
   鍵供託機能を備えた会議鍵共有方式の提案
7. 第 4 回 FACT(光成, 境, 笠原)[13], 今回の提案
   不正利用者追跡法の提案 (結託困難)

これらの方式は, いずれの方式もペアリングの双線形写像を利用しており, ペアリングを用いることによって実現可能な方式となっている. 本稿では, 不正利用者 (端末) の追跡が可能な放送用鍵配送方式の基本方式を提案する. この方式は, 黒澤-Desmet[4] が提案した従来方式では実現されなかった, 利用者の結託攻撃に対する安全性を有していると考えられ, 実用上も極めて重要な方式である. また, これまでに提案されたペアリングを利用した暗号方式の幾つかを紹介し, ペアリングを利用した新たな方式について考察する.

2 ベイユペアリング

楕円曲線上のペアリングはベイユペアリング, テイトペアリングが良く知られている [1][2].

ベイユペアリングは, 楕円曲線上の点のなす群 $E(\boldsymbol{F}_q)$ の部分群である n ねじれ群 $E[n] \subset E(\boldsymbol{F}_q)$ から有限体上 $\boldsymbol{F}_{q^k}$ の乗法群への写像である. ここでは, 楕円曲線上の n ねじれ点 $P, Q, R \in E[n]$ のペアリングを $e_n(\ ,\ ) \in \boldsymbol{F}_{q^k}$ で記述するものとする. ベイユペアリングの性質は以下の通りである.

$$
\begin{aligned}
e_n(P,Q) &= 1 \text{ for all } P \in E[n] && \text{非退化}\\
&\quad \text{if and only if } Q = 0 &&\\
e_n(P,Q) &= e_n(Q,P)^{-1} && \text{反対称}\\
e_n(P+Q,R) &= e_n(P,R)e_n(Q,R) && \left.\begin{array}{l}\\ \text{双線形}\end{array}\right\}\\
e_n(P,Q+R) &= e_n(P,Q)e_n(P,R) &&
\end{aligned}
$$

双線形であることから, 以下の等式が成り立つ.

$$
\begin{aligned}
e_n(kP,Q) &= e_n(P,Q)^k\\
e_n(P,kQ) &= e_n(P,Q)^k
\end{aligned}
$$

双線形写像であることを巧みに利用することによって, 従来困難とされていた様々な暗号方式が実現可能となる.

3 複数利用者への鍵配送方式 (不正利用者追跡法)

有料放送等を行う際に, 不正な受信機を排除するために視聴料を払っている正当な受信者のみが視聴できるような仕組みが必要である. 放送番組は同一のセッション鍵で暗号化されるので, 多数の利用者へ同一のセッション鍵を配送する方式が必要となる. このセッション鍵を配送する際に, ある共通の鍵を用いている場合, その鍵を複製すれば, 不正端末が容易に製造されてしまい, また, この鍵がどの端末から複製されたかは不明である. これを防止する簡単な方法としては, 予め各端末毎に異なる鍵を与えておき, 放送時に端末数だけの鍵を同時に配送する方式が考えられる. しかし, 端末数に比例して, 鍵配送用のヘッダは長くなる上, 鍵と利用者とを対応させる, あるいは, 利用者の新規登録と同時に配送用ヘッダを更新する必要がある.

本章では先ず, 鍵配送用のヘッダの大きさが固定であり, かつ端末に内蔵された鍵に, 端末利用者の ID 情報を埋め込むことが可能な従来方式として黒澤-Desmet の方式を紹介する. この方式は, 鍵配送用のヘッダが固定の長さであり, 端末に内蔵された鍵に端末利用者の ID 情報を埋め込むことが可能である. しかし, この基本方式では, 利用者の結託により追跡不可能な不正端末を作成することが可能となってしまう. 筆者等は SCIS2001 において, ペアリングを用いることによって, この不正端末を作成するのに必要な結託人数がより大きくなる手法を提案した [11].

本章では, さらに楕円曲線上のペアリングを用いた新たな方式を提案する [13]. この提案方式は, 利用者の結託があった場合でも複製元の追跡が不可能な端末を複製することが困難であり, この複製問題は, ある種の拡張 Diffie-Helman 問題に等価である [13].

3.1 従来方式

以下では放送主体をプロバイダという.

放送に先だってプロバイダは, 利用者 のID情報が埋め込まれたセッション鍵復号用の秘密鍵を以下のように生成し, これを利用者 へ配布する.

1. 大きな素数 p を生成する.
2. $k-1$ 次多項式 $f(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots a_1x + a_0$ を選び, これをプロバイダの秘密鍵とする.
3. 利用者 $\boldsymbol{i}$ のID情報 ID_i より, $f(ID_i)$ を計算し, これをセッション鍵復号用の秘密鍵として利用者 $\boldsymbol{i}$ へ配布する.

実際の放送では, プロバイダは次のようにヘッダを生成し, これを放送時に添付することにより, セッション鍵 K_S を配送する.

1. $\boldsymbol{F}_p$ の元 y を定める.
2. セッション鍵 K_S を定めた後, $yK_S, y^{a_{k-1}}, y^{a_{k-1}}, \cdots, y^{a_1}, y^{a_0} \pmod p$ をヘッダとしてセッション鍵 K_S によって暗号化された放送内容と共に放送する.

利用者 $\boldsymbol{i}$ は秘密鍵 $f(ID_i)$ を用いて, 以下のようにセッション鍵 K_S を復号し, これを用いて放送内容を復号する.

1. $\prod_{j=0}^{k-1} (y^{a_j})^{ID_i{}^j} \equiv y^{f(ID_i)} \pmod p$ を計算する.
2. $\left(y^{f(ID_i)}\right)^{\frac{1}{f(ID_i)}} \equiv y \pmod p$ を計算し $\frac{yK_S}{y} \equiv K_S \pmod p$ を復号する.

ただし, $ffrac1f(ID_i) \pmod{p-1}$ の計算が可能とするために, 法 p や, 多項式にある条件をつける必要がある. また, y をランダムに選ぶとすれば, y そのものをセッション鍵にして, ヘッダ情報を1つ小さくすることができる.

この方式では, $f(ID_i)$ を利用者 に配布しているため, k 人の利用者 がこの $f(ID_i)$ を見せ会うことにより, プロバイダの秘密鍵 $f(x)$ が露呈する. 一度 $f(x)$ が露呈すると, 任意の利用者 $\boldsymbol{v}$ のID情報 ID_v を用いて, 復号用の利用者 の秘密鍵 $f(ID_v)$ を計算できるので, 複製元が特定できない不正端末を複製されてしまう.

3.2 楕円曲線上のペアリングを用いた方式

本節では, 基本方式においての課題であった結託問題が解消された方式を提案する. 提案する方式のあるクラスは, 結託攻撃がある観点で見た場合の弱いDiffie-Hellman問題と等価であることが示される [13].

秘密鍵の配布

プロバイダは, 利用者 のID情報が埋め込まれたセッション鍵復号用の秘密鍵を以下のように生成し, これを利用者 へ配布する.

1. 有限体 $\boldsymbol{F}_q$ 上の楕円曲線 $E/\boldsymbol{F}_q$ を生成する. ただし, この楕円曲線は楕円離散対数問題が十分困難であり, この曲線上のペアリング $e_n(\ ,\ )$ が計算可能であるものとする.
2. 楕円曲線 $E/\boldsymbol{F}_q$ 上の n ねじれ点 $P \in E[n] \subset E(\boldsymbol{F}_q)$ および, $k-1$ 次多項式 $f(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_1x + a_0$ を選び, これをプロバイダの秘密鍵とする.
3. 利用者 i のID情報 ID_i より, $\frac{1}{f(ID_i)}P$ を計算し, これをセッション鍵復号用の秘密鍵として利用者 $\boldsymbol{i}$ へ配布する.

セッション鍵の配送

放送では, プロバイダは次のようにヘッダを生成し, これを放送時に添付することにより, セッション鍵 K_S を配送する.

1. 楕円曲線 $E/\boldsymbol{F}_q$ 上の n ねじれ点 $Q \in E[n] \subset E(\boldsymbol{F}_q)$ を定める.
2. セッション鍵 K_S を定めた後, $e_n(P,Q)K_S$, $a_{k-1}Q$, $a_{k-2}Q, \cdots, a_1Q, a_0Q$ をヘッダとしてセッション鍵 K_S によって暗号化された放送内容と共に放送する.

利用者 $\boldsymbol{i}$ は秘密鍵 $\frac{1}{f(ID_i)}P$ を用いて, 以下のようにセッション鍵 K_S を復号し, これを用いて放送内容を復号する.

1. $\sum_{j=0}^{k-1} ID_i{}^j a_j Q = f(ID_i)Q$ を計算する.
2. $e_n\left(\frac{1}{f(ID_i)}P, f(ID_i)Q\right) = e_n(P,Q)$ を計算し, $\frac{e_n(P,Q)K_S}{e_n(P,Q)} = K_S$ を復号する.

提案方式の特徴

この方式では, プロバイダは直接 $f(ID_i)$ を利用者に配布していないので, 通常の結託により, $f(x)$ が露呈することはない. $f(x)$ が一次式の場合, 結託攻撃がある種の弱いDiffie-Hellman問題と等価であることが証明されている [13]. この場合, $f(x) = x + a_0$ すなわち $a_1 = 1$ としても, 方式上の差は全くないことに注意されたい. さらに, 従来方式と同様に, n ねじれ点 Q をランダムに選べば, $e_n(P,Q)$ そのものをセッション鍵として用いることができる. $e_n(P,Q)$ をセッション鍵とし, $f(x)$ が一次式の場合, ヘッダ情報は, Q, a_0Q と2つの n ねじれ点でよいことになり, ヘッダの大きさや計算量の点で提案方式は格段に効率のよい方式となる.

4 ペアリングを用いた暗号方式

本章では, これまでに提案されてきたペアリングを用いた暗号方式の概要を記述すると共に, ペアリングを用いた新暗号方式を提案する.

4.1 ベイユペアリングに基づく IDNIKS

信頼のおけるセンタと利用者は以下のようにして鍵共有に必要なデータを準備する.

準備

利用者 $\boldsymbol{i}$ の ID 情報 を ID_i とする. センタはベイユペアリングのアルゴリズム $e_n(\ ,\ )$ と ID 情報 ID_i を楕円曲線上の n ねじれ点 $P_i \in E[n]$ に変換する一方向関数 $f(\ )$ を公開する. さらに, センタは秘密の乱数 l を生成し, 利用者 $\boldsymbol{i}$ に対して, $Q_i = lP_i$ を計算し, これを利用者 $\boldsymbol{i}$ に秘密裏に配送する. これらセンタの生成する情報とアルゴリズムをまとめると以下のようになる.

センタの秘密情報	: l (疑似乱数)
センタの公開アルゴリズム	: $f(\ )$, $e_n(\ ,\ )$
利用者 $\boldsymbol{i}$ の秘密情報	: Q_i
利用者 $\boldsymbol{i}$ の公開情報	: ID_i, P_i

次に利用者 $\boldsymbol{a}$ と $\boldsymbol{b}$ の鍵共有手順を示す. ここで, ID 情報 ID_a と ID_b の順序が与えられているものとする. ID_a と ID_b の順序としては, 例えば 辞書順や, 2 進数で表したときの大小関係が考えられる.

鍵共有法

利用者 $\boldsymbol{a}$ と 利用者 $\boldsymbol{b}$ の共通鍵 $K_{ab} = K_{ba} \in \boldsymbol{F}_{q^k}$ は各自の秘密鍵と相手の ID 情報 ID_a, ID_b から得られる P_a, P_b を用いて以下のようにして生成することができる.

$$\begin{aligned} &\text{利用者 } \boldsymbol{a}: && K_{ab} = e_n(Q_a, P_b) = e_n(P_a, P_b)^l, \\ &\text{利用者 } \boldsymbol{b}: && K_{ba} = e_n(P_a, Q_b) = e_n(P_a, P_b)^l. \end{aligned}$$

ベイユペアリングの性質により $K_{ab} = K_{ba}$ が成り立つことは明らかである.

なお, 安全性を確保するためには, センタ秘密 l が利用者に知られてはならない. すなわち, n ねじれ部分群 $E[n]$ 上の離散対数問題 $Q_i = lP_i$ を求めるのが困難であること, および有限体 $\boldsymbol{F}_{q^k}$ の n ねじれ部分群の離散対数問題 $(P_i, P_j)^l = (Q_i, P_j)$ を求めるのが困難であることが必要である. 本稿で紹介する全ての暗号方式は, このような楕円曲線上のおよび有限体の n ねじれ部分群の離散対数問題が困難とする必要があり, そのためには, 次の条件が必要である.

1. q, n は 2^{160} 以上に設定すること.
2. $n | q^k - 1$ かつ $q^k \simeq 2^{1024}$ を満たすような整数 k が存在すること.

q^k の大きさは, 安全性が保たれる範囲で, ペアリングの計算を効率良く行うことができるように設定すればよい. q^k を 1024 ビット程度に設定した場合, 1024 ビットの RSA 暗号の処理のおよそ 10 倍以内で鍵共有を行うことができる [9].

ベイユペアリング以外のペアリングとして, テイトペアリングや, 超楕円曲線上定義されるペアリングも利用可能である.

4.2 ペアリングを用いた ID 情報に基づくデジタル署名方式

本節では, ペアリングを用いた ID 情報に基づく署名方式を紹介する. 以下では署名者を $\boldsymbol{a}$ とする.

センタと利用者は次のようなデータを準備する.

センタ の 秘密情報	: l
センタ の 公開情報	: $R \in E[n]$(ランダムな元), $R' = lR$ ペアリング $e_n(\ ,\ )$, 一方向関数 $f(\ )$
利用者 $\boldsymbol{a}$ の秘密鍵	: $Q_a = lP_a \in E[n]$
利用者 $\boldsymbol{a}$ の公開鍵	: ID_a

関数 $f(\ )$ は, ID 情報 ID_a から楕円曲線上の n ねじれ点 $P_a \in E[n]$ への一方向関数である.

準備されるデータは, 4.1 の IDNIKS のシステム情報に $R, R' = lR$ を付加したものとなっている.

署名生成

平文 m に対して, $f(m) = M \in E[n]$ および, 乱数 r を生成し, 署名文 $\left(S_a^{(0)}, S_a^{(1)}\right)$ を以下のように生成する.

$$\begin{aligned} S_a^{(0)} &= Q_a + rM, \\ S_a^{(1)} &= rR, \qquad \text{署名文 } (S_a^{(0)}, S_a^{(1)}). \end{aligned}$$

署名の検証

検証者は先ず以下のペアリングの計算をする.

$$\begin{aligned} v_1 &= e_n(S_a^{(0)}, R) = e_n(P_a, R)^l e_n(M, R)^r \\ v_2 &= e_n(P_a, R') = e_n(P_a, R)^l \\ v_3 &= e_n(M, S_a^{(1)}) = e_n(M, R)^r \end{aligned}$$

署名の正当性は, 次式が成立することによって確認する.

$$v_2 v_3 = v_1,$$

この署名方式の特徴をまとめると以下のようになる.

1. ID 情報とセンタの公開情報のみから利用者の公開鍵を生成可能.
2. センタ公開データは署名者 (利用者) 毎に変える必要なし. すなわち, 共通にすることが可能.
3. 署名者毎に公開データを認証する必要なし. センタ公開データと署名者の ID 情報のみで検証可能.

また, センタの生成する秘密情報を全て利用者が個別に生成するようにすれば, センタ不要の方式が実現できるが, この場合, 秘密情報 l が利用者毎に異るため, 公開鍵 R, R' の認証が必要となり, 従来方式との違いはなくなる. ペアリングを用いて複数の署名者が同一文書に署名する多重ディジタル署名方式も文献 [6] で提案されている.

4.3 ペアリングを用いた ID 情報に基づく公開鍵暗号

本節では, ペアリングを用いた ID 情報に基づく公開鍵暗号を紹介する [8][10].

センタと受信者 $\boldsymbol{a}$ は公開鍵として, 次の情報を公開する.

センタと利用者が準備するデータは前節の署名法と全く同じものである.

暗号化

送信者 $\boldsymbol{b}$ は, 乱数 r を生成した後, 平文 m を 受信者 $\boldsymbol{a}$ の公開鍵 $E/\boldsymbol{F}_q, E[n], P_a, R, R' = lR \in E(\boldsymbol{F}_{q^k})$ を用いて, 以下のように暗号化し, 暗号文 C_1, C_2 を得る.

$$\begin{aligned} C_1 &= rR \\ C_2 &= m \cdot e_n(P_a, rR') = m \cdot e_n(P_a, R)^{lr} \end{aligned}$$

復号

受信者 $\boldsymbol{a}$ は, 暗号文 C_1, C_2 を, 秘密鍵 Q_a を用いて, 以下のように復号し, 平文 m を得る.

$$\frac{C_2}{e_n(Q_a, C_1)} = \frac{m \cdot e_n(P_a, R)^{rl}}{e_n(P_a, R)^{rl}} = m$$

本方式の特徴は, 公開鍵をセンタの公開情報と受信者の ID 情報のみから生成可能であることであり, 従来公開鍵暗号のように公開鍵を認証する必要がない. また, 4.1 の IDNIKS を用いた場合の応用上の違いは, 送信者の ID 情報が不要であり, 匿名で受信者に送信することが可能となることである. さらに, 前節の署名法同様にセンタの生成する秘密情報を全て利用者が個別に生成するようにすれば, センタ不要の方式が実現できるが, この場合, R と R' の認証が必要となる.

4.4 1 ラウンド 3 者間 DH 鍵共有法

本節では, ANTS-IV で Joux が提案した 1 ラウンドで, 3 者の間で共通の鍵を共有する方式を紹介する [7].

共通のパラメータは, ペアリングの計算が可能な楕円曲線のパラメータとその曲線上の 2 つの n ねじれ点 P, Q であり, 利用者 $\boldsymbol{i}$ は, 自分の秘密鍵 i を生成した後, 公開鍵として iP, iQ を公開する.

例えば, 利用者 $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ の秘密鍵および公開鍵は, 表 4.4 のようになり, これら 3 者間の鍵共有は, 次式によって算出される.

$$\begin{aligned} &\text{利用者 A}: && e_n(bP, cQ)^a = e_n(P, Q)^{abc} \\ &\text{利用者 B}: && e_n(cP, aQ)^b = e_n(P, Q)^{abc} \\ &\text{利用者 C}: && e_n(aP, bQ)^c = e_n(P, Q)^{abc} \end{aligned}$$

表 1. 利用者の秘密鍵と公開鍵

	秘密鍵	公開鍵
利用者 $\boldsymbol{a}$	a	aP, aQ
利用者 $\boldsymbol{b}$	b	bP, bQ
利用者 $\boldsymbol{c}$	c	cP, cQ

4.5 多重暗号

ペアリングを鍵供託方式に応用する手法が提案されている [12]. これは, 前節の鍵共有法で用いた秘密鍵と公開鍵を用い, 暗号文を生成するときに, 2 者 $\boldsymbol{a}, \boldsymbol{b}$ の公開鍵を用いて暗号化を行い,

$$\begin{aligned} C_1 &= m\, e_n(aP,\, bQ)^r \\ C_2 &= rP \end{aligned}$$

と暗号化し, 2 者のどちらか一方だけで,

$$m = \frac{C_1}{e_n(C_2, bQ)^a} = \frac{C_1}{e_n(C_2, aQ)^b}$$

と復号することが可能とするものである. この方式を

$$\begin{aligned} C_1 &= m\, e_n(aP,\, bQ)^r \\ C_2 &= (P, Q)^r \end{aligned}$$

という暗号文に変形すると, 2 者 $\boldsymbol{a}, \boldsymbol{b}$ の双方が協力しなければ

$$m = \frac{C_1}{C_2^{ab}}$$

と復号することができない公開鍵暗号とすることができる. ただし, このような機能は従来の ElGamal 暗号でも実現可能であり, ペアリングを用いる利点は特にない.

4.6 多重署名

本節では, 多重署名を行う手法を提案する. なお以下では, 前節と同様に 4.4 と同じ公開鍵を用いる.

はじめに, ElGamal 署名の手法を用いる方法について考える.

署名

利用者 a は 利用者 b の公開鍵 P_b と自分の秘密鍵 a を用いて, 次のように署名する.

$$\begin{aligned} R &= kQ \\ S &= \frac{h(m)}{k}P - \frac{ar_x}{k}P_b = \frac{h(m) - abr_x}{k}P \end{aligned}$$

ただし, r_x は点 R の x 座標 $(R = (r_x, r_y))$ である.

検証

署名データ S と R のペアリングを計算すると,

$$e_n(S, R) = e_n(P, Q)^{h(m)-abr_x}$$

となるので,

$$e_n(S, R)e_n(P_a, Q_b)^{r_x} = e_n(P, Q)^{h(m)}$$

が成立することにより, 署名の正当性を確認する.

次に Schnorr 署名の手法を用いる場合を考えよう.

署名

$$\begin{aligned} r &= e_n(P, Q)^k \\ S &= h(m||r)aP_b + kP = (h(m||r)ab + k)P \end{aligned}$$

検証

次式が成立することにより, 署名の正当性を確認する.

$$e_n(S, Q) = e_n(P_a, Q_b)^{h(m||r)}r$$

本節で提案した多重署名は, 作成された署名は二人の利用者の秘密鍵に対して対称であるのため, この署名から, どちらが署名したかを判別することが不可能とすることができる. ただし, この二人の利用者のうち, どちらかが署名したことを確認することはできる. このような署名法の応用については, 今後検討していきたい.

5 まとめ

本稿では, ペアリングを用いた暗号方式のいくつかを紹介し, 新たな方式を提案した. 特に, 不正利用者追跡可能な方式は, 利用者の結託攻撃に対する安全性を有していると考えられ, 実用上も極めて重要な方式である.

参考文献

[1] J. H. Silverman, "The Arithmetic of Elliptic Curves", Springer-Verlag, 1986.'

[2] A. Menezes, T. Okamoto, S. Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field", IEEE Trans. Inf. Theory 39, pp.1639–1646, 1993.

[3] I. Blake, G. Seroussi, N. Smart, Elliptic Curves in Cryptography, London Mathematical Society Lecture Note Series 265, Cambridge University Press, 1999.

[4] K. Kurosawa and Y. Desmedt, "Optimum Traitor Tracing and Asymmetric Schemes", Proc. of EUROCRYPT'98, LNCS vol. 1403, Springer-Verlag, pp. 145-157, 1998.

[5] 大岸聖史, 境隆一, 笠原正雄, "楕円曲線上の ID 情報に基づく鍵共有法に関する考察", 信学技報 ISEC99-, Nov.1999.

[6] R. Sakai, K. Ohgishi, M. Kasahara, "Cryptosystems Based on Pairing", Proc. of SCIS2000,C20,Jan.2000.

[7] A. Joux, K. Nguyen, "A one round protocol for tripartite Diffie-Hellman", Proc. of ANTS IV, pp.385-394,Aug. 2000.

[8] 境隆一, 大岸聖史, 笠原正雄, "ペアリングに基づく暗号方式", Aug.31-Sep.2 2000.

[9] 山中忠和, 大岸聖史, 境隆一, 笠原正雄, "ペアリングを用いた ID-NIKS の構成に関する考察", Proc. of SCIS2001,7B-1,Jan.2001.

[10] 境隆一, 大岸聖史, 笠原正雄, "楕円曲線上のペアリングを用いた暗号方式", Proc. of SCIS2001,7B-2,Jan.2001.

[11] 光成滋夫, 境隆一, 笠原正雄, "楕円曲線を使った不正ユーザ追跡法", Proc. of SCIS2001,7B-3,Jan.2001.

[12] SCIS2001(井上 徹, 櫻井幸一)[?] "鍵供託機能を備えた会議鍵共有方式の提案", Proc. of SCIS2001,14B-4,Jan.2001.

[13] 光成滋生, 境隆一, 笠原正雄, "新しい不正ユーザ追跡法", FACT4(先端暗号理論フォーラム),Mar.2001.