ID ベース暗号に関する調査報告書

平成 21 年 3 月

CRYPTREC
ID ベース暗号調査 WG

IDベース暗号調査WG委員構成

主査：高木　剛　　公立はこだて未来大学

委員：伊豆　哲也　　株式会社富士通研究所

委員：岡本　健　　国立大学法人筑波技術大学

委員：小林　鉄太郎　　日本電信電話株式会社

委員：境　隆一　　大阪電気通信大学

委員：高島　克幸　　三菱電機株式会社

委員：田中　秀磨　　独立行政法人情報通信研究機構

委員：花岡　悟一郎　　独立行政法人産業技術総合研究所

目次

第 1 章

ID ベース暗号/ペアリング技術の概要

1.1 ID ベース暗号の概説

1.1.1 ID ベース暗号とは

本報告書では ID に基づく暗号を ID ベース暗号と称する．ここで ID とは Identity または Identification の略語であり，一般に個人を特定することが可能な情報を意味する．例えば住所氏名，email アドレス，携帯電話の番号，基礎年金番号等，は ID として扱うことが可能である．email アドレスは個人との対応関係が明かではない場合があるが，各団体等で公式に与えられたアドレスであれば，それを管理する団体等で本人と email アドレスとの対応が取れるので，このような場合，ID として扱うことができる．

広い意味の ID ベース暗号とは，認証，署名，暗号化等の方式を ID に基いて実現する方式である．認証や署名方式は，認証（署名）データ，共通パラメータおよび認証（署名）者の ID を用いて認証（署名）データの検証を行うことができる方式であり，暗号化方式は，平文，共通パラメータおよび受信者の ID を用いて暗号文を作成できる方式である．ここで共通パラメータとは全てのユーザに共通の共有情報を指す．

狭い意味での ID ベース暗号とは，オフライン処理が可能な，すなわち対話的な通信（予備通信[*1]）を不要とする暗号化，認証，署名方式のことである．ただし，非対話的な ID ベース認証（署名）は，公開鍵認証センタ（PKI）に基く電子署名を用いて容易に実現できる．例えば公開鍵認証センタが認証（署名）者の公開鍵と ID を連接したデータに対して署名データを作成し，これを認証（署名）データに含めれば ID ベース認証（署名）と同じ機能が容易に実現される．[*2]．したがって，より狭い意味で ID ベース暗号といえば，非対話的な ID ベース鍵共有方式，ID ベース鍵配送方式および ID ベース暗号化方式のことを指すと考えてよい[*3]．

ID ベース鍵共有方式は送信者と受信者間で共通の鍵を ID に基づいて共有する方式であり，共有した鍵を任意の共通鍵暗号の鍵として使用する．また，ID ベース暗号化方式は平文，受信者の ID および共通パラメータだけを用いて受信者への暗号文を作成する暗号である．ゆえに，公開鍵暗号のように公開鍵認証センタは必要なく，公開鍵認証センタが公開鍵に与える信頼性のかわりに，ID の信頼性を利用する方式と考えることができる．一方，ID ベース鍵配送方式は，受信者の ID および共通パラメータだけを用いて共通鍵暗号で用いる鍵を配送する方式であり，ID ベース暗号化方式の平文を配送する鍵に置き換えることによって実現することも可能である．

以上で述べたように対話的な通信が必要である ID ベース暗号方式は，公開鍵暗号システムを用いて容易に実現する

[*1] 対話的な通信において，最後の通信以外を予備通信ということもある．

[*2] 対話的な通信が必要な ID ベース暗号と同等の機能は，PKI と公開鍵暗号を用いて容易に実現できる．

[*3] ID ベース暗号を利用するという環境において，ユーザの作成した公開暗号の公開鍵の認証手続きを省きたい場合や，ユーザの署名鍵を ID ベース暗号のユーザ秘密鍵としたい場合においては，ID ベース認証 (署名) を採用する利点がある．

ことができるので，以下では対話的な通信が不要な ID ベース暗号化方式を IBE と称し，この方式を主に述べる．

1.1.2 IBE の一般的な利点

一般に，ICT 技術に関わるシステムにおいて，安全性と利便性はトレードオフの関係にあるとされる．すなわち，安全性を高く設定すると利便性が損なわれ，利便性を高くすると安全性が低下する．

これまでに公開鍵暗号は，我々に多くの利便性を与えてくれた．しかし，一般のシステム管理者やユーザにとって，この公開鍵暗号を安全に運用するためのインターフェースは，様々な面で改善の余地がある．IBE は，従来の公開鍵暗号に比べて，利便性が高いと考えられており，暗号利用の普及に貢献すると期待されている．IBE の主な利点は次の通りである．

公開鍵認証センタが不要: IBE においては暗号送信者は，受信者の ID と共通パラメータのみから暗号文を作成することが可能であり，この共通パラメータと ID の信頼性が確保できれば安全な通信が実現できる．したがって，ID ベース暗号は受信者の公開鍵とその認証が必要な公開鍵暗号方式に比べてより高い利便性を有している．この差は，一見，僅かのように見えるが，一般の管理者やユーザに，利便性と安全性を兼ね備えた暗号システムを提供するという場合には，大きな差となる場合がある．例えば，受信者の公開鍵を暗号作成時に入手できないような場合においても，受信者の ID が信頼できれば，暗号文を作成することが可能である．**ただし，共通のパラメータとユーザの復号鍵を生成する信頼のおける機関，PKG，を必要とする**

新規ユーザへの対応が容易: 新規ユーザを追加する際の利点としては，例えばメール暗号システムにおいて新規ユーザが増えた場合，公開鍵暗号では，そのユーザの公開鍵の入手と認証を行った上で，公開鍵リストを更新する必要があるが，IBE では，メールアドレス以外に新たに必要な情報を追加する必要はない．そして，送信者側に関しては暗号システム導入前の作業環境と同等にすることができる．送信メールを送信先アドレスを用いてメールサーバが自動的に暗号化するシステム[*4]は，この特性の活用例であり，公開鍵暗号を用いたシステムに比べて，ユーザの利便性を損なわないのと同時に管理者の負担増を小さくできる．このように，ID として email アドレスや携帯電話の番号等の個人固有の情報を採用すれば，ID の入手の容易さという利便性と，これらの ID を普段から利用しているという意味での信頼性を同時に得ることができる．

未登録者への送信が可能: 暗号利用を促進したい送信者が，受信者が復号したいと思うような情報を暗号化して送信すれば，自身の秘密鍵を有していない受信者に，秘密鍵の入手手続きを行わせる動機を与えて暗号の利用を始めさせることができるので，送信者側で受信者の IBE の利用を促進させることができる．

上記の諸利点を鑑みるに，IBE は PKI に代わる新たな暗号インフラの強力な要素技術となるものと期待を抱かせている．そのような利用における具体的な利点や問題点は，1.2 節において詳しく述べる．

1.1.3 ID ベース暗号の一般的な課題

ID ベース暗号を利用する上での留意点は一般的に以下の項目がある．

ID の信頼性/更新可能性: すでに広く周知がなされているような利用者ごとの固有情報を ID として採用すべきと考えられるが，そのような固有情報が実際に利用可能であるかについては慎重な検討が必要である．しかし，その一方で，そのような固有情報が存在したとして，それが柔軟に変更可能であるかも重要な検討事項である．

[*4] Voltage 社によって実用化されている．

鍵生成センタ (PKG) の信頼性: IBE においては，PKG は任意のユーザ宛の暗号文を (不正に) 復号可能である．したがって，PKG にはそのような不正復号を行わないことが期待できるような高い信頼性が要求されることになる．

マスター鍵の更新: ユーザ鍵の生成のために PKG が利用する秘密情報はマスター鍵と呼ばれるが，このマスター鍵が漏洩するなどした場合，これを更新する必要がある．しかしながら，マスター鍵を更新する場合，それに付随してすべてのユーザ鍵の更新および公開の共通パラメータの更新が必要となる．予備通信が不要であるという IBE の利点は，これらの更新を考慮すると大きく損なわれる可能性がある．

ユーザ鍵の更新: ユーザ鍵が漏洩してしまった場合，これを速やかに更新することが必要になる．しかし，ユーザの ID として周知の固有情報が通常用いられることになるが，そのような広く周知された固有情報を併せて更新する必要まで生じてしまう．その場合，やはり IBE の利点を大きく損なう可能性がある．

ユーザ鍵の無効化: さらに，ユーザ鍵が漏洩した場合，この鍵を入手した攻撃者は，当該ユーザ宛の暗号文を自由に復号可能となる．やはり，ID の性質を考えるとそれを無効化することは容易ではなく，仮にユーザ鍵の更新を行ったとしても元々の ID に宛てられた暗号文の不正な解読を防ぐことは難しい．

IBE を PKI に代わる暗号インフラとして用いた場合の具体的な利点や問題点は，1.2 節において詳しく述べる．

1.1.4 ID ベース暗号の発展

ID ベース暗号の発展には，過去から現在まで我が国の研究者達が多大な貢献をしており，我が国の暗号研究のレベルの高さを示す一例となっている．ここでは ID ベース暗号を狭義の “予備通信を必要としない ID ベース暗号” とする．

■IBE の概念の提唱と 2000 年以前の試み． ID ベース暗号の研究は公開鍵暗号の場合と同様に，先ずその概念が岡本，Shamir によって発表された [OT84][S84]．そして，その後具体的な方式が提案されたのであるが，それらは必ずしも十分な安全性を有していなかった．実用的，かつ安全な方式の基本的なアイデアが初めて提案されたのは 1999 年のことであり，ID ベース暗号の概念が提案されてから 15 年という歳月が経っていた．この間の ID ベース暗号の研究は，我が国を中心に活発に研究されており，鍵事前配送方式 KPS（Key Predistribution System）もしくは ID に基づく予備通信不要の鍵共有方式 ID-NIKS（ID based Non-Interactive Key Sharing）と呼ばれていた [MI87][B82]．当時の ID ベース暗号の最大の問題点は，ユーザの結託による攻撃を許してしまうということであり，ユーザが公開鍵の要素数と同じ数だけ結託すると，マスター鍵（PKG の秘密鍵）が露呈してしまうという致命的なものであった．

一方，合成数を法とした離散対数問題を解いて，ユーザの秘密鍵を作成するという方式が 1990 年に提案された [MK90][MY91]．この方式は，ユーザ間の結託に対しても十分安全であると見なせるが，この方式を実現するには比較的大きな離散対数問題を解いてユーザの秘密鍵を算出することが必要であり，現在の計算機環境では効率の良い方式としての実現は難しいとされている．

■2000 年頃の大きな進展: ペアリングの利用． ID ベース暗号の概念が提案されてから実に 15 年後，初めて実用的でかつユーザ間の結託に対して十分安全な ID ベース鍵共有方式が大岸，境，笠原 [SOK00] によって提案された．この方式は楕円曲線上のペアリングを用いたところが最大の特徴であり，ペアリングの双線形性という性質を ID ベース暗号の構成に用いている．その後，Boneh, Franklin によって，distortion 写像を組み入れた ID ベース暗号（以下 BF 方式）が提案された．BF 方式は distortion 写像を組み入れた意外は，基本的に境等の方式と同じ方式であったが，彼らの提案を機に世界の暗号研究者が ID ベース暗号をはじめとするペアリングを用いた暗号に注目するようになり，ペアリングを用いた暗号研究は急速に進展したのである．ここで注意すべきことは，暗号理論においてペアリングは，楕円

曲線上の離散対数問題を解く手法である MOV 攻撃として知られていたことである [MOV93].

一方，ほぼ同時期に Cocks[C04] により，平方剰余判定問題の困難性に基づき，1bit のみを暗号化する ID ベース暗号が提案されている．この方式ではペアリングは必要とされていない．

1.1.5 ID ベース暗号の具体的構成例

以下では，ペアリングを用いたいくつかの代表的な ID ベース暗号を簡単に紹介する．このようなペアリングを用いた暗号方式の暗号化および復号の仕組みは，双線形性というペアリングの性質を形式的に認めれば理解することが可能であるので，はじめに楕円曲線上のペアリング[*5]について概説する．ただし，これらの仕組みが暗号として機能し得るということを納得するためには，2 章で記される双線形写像の一方向性や双線形 Diffie-Hellman 問題のような新たな数論的問題を学ぶ必要がある．

■楕円曲線上のペアリング． 楕円曲線上の離散対数問題に安全性の根拠をおく暗号 [K94][C-R02] でも用いられる有限体 $\mathbb{F}_q$ 上定義された楕円曲線 $E/\mathbb{F}_q$ において，拡大体 $\mathbb{F}_{q^\kappa}$ 上の点 $E(\mathbb{F}_{q^\kappa})$ のなす加法群について，位数 n の部分群 $E[n] \subset E(\mathbb{F}_{q^\kappa})$ があるとする．ただし，n は $q-1$ を割り切る自然数である．楕円曲線上の点 $P, Q \in E(\mathbb{F}_{q^\kappa})$ は加算 $P+Q \in E(\mathbb{F}_{q^\kappa})$ が可能であり，整数倍 $lP \in E(\mathbb{F}_{q^\kappa})$ も効率良く計算できる．ペアリング $e(P,Q)$ は，この部分群 $E[n]$ の任意の 2 点 P, Q から，$\mathbb{F}_{q^\kappa}$ の乗法群 $\mathbb{F}_{q^\kappa}^\times$ の位数 n の部分群のある元への写像である．

ペアリング $e(P,Q)$ には，幾つかの性質があるが，ここでは ID ベース暗号についての暗号化および復号の仕組みを理解するための最小限の性質である双線形性についてのみ記す．

双線形性とは，任意の点 $P, Q, R \in E[n]$ に対して成立する関係，

$$e(P, Q+R) = e(P,Q)e(P,R), e(P+Q,R) = e(P,R)e(Q,R)$$

をいう．この性質から直ちに，ある整数 l に対して

$$e(lP, Q) = e(P, lQ) = e(P,Q)^l$$

という関係が導ける．このような楕円曲線上のペアリングの値 $e(P,Q)$ は P, Q が与えられているとき，効率の良いアルゴリズム（3 章参照）によって計算される．

■ID ベース鍵共有法． 楕円曲線上のペアリングを用いて，下記の要領にて予備通信の不要な鍵共有を行うことができる [SOK00]．鍵共有法は，送信者の秘密鍵を用いる方法と共通のパラメータを用いて共有鍵作成に必要な情報を暗号文と共に送る方法がある．そして，どちら方式も送信者は共有鍵で暗号化した暗号文を受信者に送る．

鍵設定：鍵生成機関,PKG, は，ペアリング演算が可能な楕円曲線 $E/\mathbb{F}_q$ を設定し，PKG のマスター秘密鍵 $s \in \mathbb{Z}_n^\times$ を 1 つ選ぶ．また，ID のハッシュ値より，$E[n]$ の点への変換関数 $H_1(x)$ を定めておく [K94]．この際の楕円曲線上の点への変換については，幾つかの方法があるが，3.4 節で詳しく述べられる．

ユーザ鍵生成：PKG はユーザ A の ID, ID_A, より，ハッシュ関数 $H_1(x)$ を用いて，楕円曲線上の点 $P_A = H_1(ID_A) \in E(F_q)$ に変換する．

[*5] ID ベース暗号のより一般的な記述として，双線形写像の存在を仮定して暗号を構成するという表現が多くの論文で採用されており，この場合双線形写像はある乗法群から乗法群への写像として記述される．

そしてユーザ A の秘密鍵として $S_A = sP_A$ を計算しユーザ A に秘密裏に渡す．ユーザ B も同様に秘密鍵 $S_B = sP_B$ を PKG から秘密裏に受け取る．

鍵共有 (ID-NIKS)：ユーザ A はユーザ B との秘密鍵を $K_{AB} = e(sP_A, P_B)$ として計算し，ユーザ B はユーザ A との秘密鍵を $K_{BA} = e(P_A, sP_B)$ で計算する．
鍵共有 (鍵配送)：送信者 B は乱数 $x \in \mathbb{Z}_n^\times$ を選び，受信者 A との共有鍵（セッション鍵）を受信者の ID を用いて $K_S = e(P_A, xsP) = e(P_A, P)^x s$ と計算する．そしてこのセッション鍵で暗号化した暗号文と共に xP を受信者 A に送る．受信者 A は共有鍵 $K_S = e(S_A, xP)$ を計算した後，暗号文を復号する．

前者の ID-NIKS は，認証機能を有しているが，ユーザ間で固定の秘密鍵が共有されることとなる．後者の鍵配送は認証機能は有していないが，共有鍵 K_S は通信毎に異なるものであり，共通鍵暗号のセッション鍵として扱われる．

■IBE の代表例． 次に IBE の具体的な実現例のひとつについて説明する．この方式の基本的なアイデアは境，大岸，笠原 [SOK01] によって示され，Boneh，Franklin[BF01] によって，distortion 写像を用いた方式として定式化された．

鍵設定：共通のパラメータおよびユーザの秘密鍵は上述の鍵共有法におけるものと同じものを利用する．ただし，ユーザの秘密鍵は復号鍵として機能する．また，PKG は点 $P \in E[n]$ を一つ選び，追加の共通パラメータ，P, sP，を公開する．

暗号化：送信者 B は乱数 $x \in \mathbb{Z}_n$ を選び，受信者 A の ID を用いて平文 $m \in \mathbb{Z}_n$ の暗号文を $C = (C_1, C_2) = (xP, m \cdot h_2(e(P_A, xsP)))$ として計算する．ただし，$h_2(y) \in \mathbb{Z}_n (y \in \mathbb{F}_{q^\kappa})$ は公開のハッシュ関数である．
復号：受信者 A は暗号文を自身の秘密鍵 S_A を用いて，$m = C_2/h_2(e(S_A, C_1))$ を復号する．

■その他の代表的な IBE． ここでは，上記のもの以外の代表的な IBE をいくつか紹介する．境-笠原方式 [OSK99] は，Boneh-Franklin 方式とは大きく異なる代数的構造を利用して IBE を構成している (ペアリングは利用する)．Boneh-Franklin 方式と同程度に効率的であり，ランダムオラクルモデルにおける安全性証明も与えられている．Boneh-Boyen1 方式 [BB04a] は，ランダムオラクルを用いずに安全性を証明可能な方式であるが，selective-ID 安全性 (2.1 節を参照) しか持たない．Boneh-Boyen2 方式 [BB04a] も同様の性質をもつが，境-笠原方式に類似の代数的構造が用いられている点が異なる．Boneh-Boyen3 方式 [BB04b] は，ランダムオラクルモデルに依存せずに，adaptive-ID 安全性 (もっとも妥当とされる安全性．2.1 節を参照) を証明可能な方式であるが，鍵サイズ，暗号文サイズ，計算量のいずれの観点からも，効率性が非常に悪い．Waters 方式 [W05] は，Boneh-Boyen1 方式の変形であり，Boneh-Boyen3 方式と同様に，adaptive-ID 安全性を証明可能である．この方式では共通パラメータのサイズを除いては，どの面に関しても極めて効率的であり，実用性が高い．Gentry 方式 [G06] は，公開鍵サイズを含めたいずれの観点からも実用的な効率性をもっている (ただし，暗号文の構成要素に $\mathbb{F}_{q^\kappa}$ の元を含むことに注意)．また，帰着効率 (2.1 節参照) についても，Waters 方式を凌駕していることも特筆すべきであるが，依拠する数学的困難性の仮定が両者で異なるため，単純に比較することは困難と思われる．ここで述べた一連の IBE については，付録にて具体的な構成について紹介する．

1.2 暗号アプリケーション

1.1 節において述べられたように，IBE にでは，システムの立ち上げ時に，一旦システム全体の共通パラメータを周知させると，その後それに一切手を加えられることなく，任意の文字列 (ID) に対して，それを公開鍵とする復号鍵の作成が可能となる．このような性質を利用して，従来の公開鍵暗号技術では実現できなかったようなさまざまな機能が

提供可能となる．(なお，共通パラメータを動的に変更可能とする場合，従来の公開鍵暗号でも同様の性質が容易に得られることにも注意されたい．したがって，システム立ち上げ時の共通パラメータが固定されていることこそに IBE の特徴があるといえる．)

その一般的な利点については，1.1 節で述べたとおり，各公開鍵とその所有者の関連付けが不要であるため，公開鍵認証センタのような存在を取り除くことが可能であり，また，システム立ち上げ後も任意に新規ユーザを追加可能で，なおかつ，未登録のユーザに対してすら暗号文の作成が可能である．これらの性質を利用した多彩なアプリケーションが考えられる．本節では，IBE の特性を利用したそのようなアプリケーションを紹介し，また，その実用性について触れる．すでに述べたとおり，最も興味深いアプリケーションは PKI に代わる新たな暗号インフラとしての利用であるため，それについて特に詳しく述べることにする．

1.2.1 新たな公開鍵インフラの基盤技術としての利用

■概要と利点． もっともよく知られた IBE の利用のされ方は，たとえば e-mail アドレス等を各利用者固有の ID として用いることで，従来の PKI で最も負荷が大きいとされる鍵証明書の存在を取り除く用途である [S84]．つまり，通常の PKI では (多くの場合) 利用者自身で鍵生成を行い，それにより作成された公開鍵が当該利用者のものであることを記した電子データに CA と呼ばれる信頼できる機関が電子署名を添付することで，鍵証明書の作成がなされる．各利用者は自分の公開鍵とこの鍵証明書をパブリックディレクトリなどを用いて誰でも入手可能な状態にする．暗号化を行う際は，受信者の公開鍵と鍵証明書を入手し，鍵証明書に添付された CA の署名を検証することで，それが受信者の正しい公開鍵であることを確認した上で，その公開鍵を用いて暗号文の作成を行う．一方，IBE においては，同様に PKG と呼ばれる信頼できる機関が存在し，PKG がマスター鍵と共通パラメータの作成を行い，このうち共通パラメータを周知させ，PKG 自身がマスター鍵と利用者固有の ID を用いて各利用者の復号鍵の鍵生成を行う．暗号化を行う際は，受信者の ID と共通パラメータのみを用いて暗号文を作成可能であるため，鍵証明書が不要となっていることが確認できる．公開鍵インフラを構築する上で鍵証明書の管理にかかる負荷は大きく，この問題点の解消の有力な要素技術として IBE は大きな注目を集めている．

■問題点． 上記の通り，IBE を利用することで，公開鍵インフラにおける鍵証明書を排除できるものと大きく期待されているが，その直接的な適用では必ずしも問題は解決されない．つまり，実利用においては，鍵の更新や無効化の問題を考える必要があり，これらを考慮すると，結局はなんらかの方法で無効化された利用者情報などを利用者たちに掲示板などを用いて通知せねばならず，また，そのような通信路の存在を認める場合，それを用いて従来の公開鍵暗号の公開鍵や鍵証明書もすべての利用者に配信可能であるため，従来の公開鍵暗号に対する IBE の優位性はほとんど失われてしまう．これは，IBE を実利用する上での最大の検討事項と考えることができ，IBE の利点を損なうことなく鍵更新と無効化を行う手法が明らかとならない限り，現行の PKI から直ちに IBE に移行することには慎重になるべきである．そのような手法として，すでにいくつかの提案はなされているものの [HHS+05, BGK08]，さらに検討を進める必要がある．

また，IBE では PKG がすべての利用者の復号鍵を作成するため，PKG 自身も任意の受信者宛ての暗号文を復号することができてしまう．そのため，問題となりうる．また，ひとつの PKG ですべての利用者の鍵生成を行う場合，PKG の負担が非常に大きいので，PKI 同様，複数の PKG を階層的に用いて鍵生成を行う必要が生じる．その際は，通常の IBE ではなく，階層的 IBE(HIBE)[HL02, GS02] を利用しなくてはならないことにも注意したい．

1.2.2 その他のアプリケーション

IBE の直接的で，なおかつ，もっとも強力なアプリケーションは前節で述べたとおりであるが，そのほかにも多彩な応用が知られている．以下において，それらを列挙する．

■Key-Insulated **暗号** [DKX+02]． 従来の公開鍵暗号における鍵更新や鍵無効化の問題を，IBE の上記とは異なる利用法により効率的に解決する手法も検討されている．この手法は Key-Insulated 暗号と呼ばれる．Key-Insulated 暗号においては，IBE におけるマスター鍵と共通パラメータを各利用者自身が個別に作成し，また，各利用者に個別の共通パラメータをその利用者の公開鍵とする．この場合，利用者の ID を公開鍵として用いることはできないため，鍵証明書自体は必要となる．しかし，利用者はマスター鍵はネットワークから隔離された安全な装置に保存しておき，たとえば，一日一回のみ，このマスター鍵から “その日の日付 (をなんらかの文字列に変換したもの)” を ID とみなして IBE の復号鍵を作成し，これのみを自分の利用する端末に格納する．一方，送信者は，受信者の公開鍵 (すなわち，受信者に固有の “共通パラメータ”) および “その日の日付” を ID とみなした IBE の暗号化を行い，受信者に送信する．このようにすることで，受信者は，ある日，端末上の復号鍵を漏洩させてしまったとしても，翌日には翌日分の復号鍵が新たに作成されるため，公開鍵を無効化することなく鍵更新を行うことが可能となっている．また，鍵漏洩が起こった時点から，過去に遡った安全性も保証されていること (所謂，forward security) も大きな特徴といえる．

■Forward-Secure **暗号** [CHK03]． Key-Insulated 暗号では，ある時点で鍵漏洩が起こったとしても，その時点以外の安全性には影響しないことが保証される反面，マスター鍵が必要であり，その安全な管理のための負荷が少なくない．これに対し，forward security のみを考慮することで，マスター鍵の必要性を取り除く方向性も検討されている．そのような手法は Forward-Secure 暗号と呼ばれる．たとえば，上記の Key-Insulated 暗号と同じ要領で，各利用者は IBE におけるマスター鍵と共通パラメータを個別に作成し，また，すべての日付について，各日付を ID とみなした IBE の復号鍵をそれぞれ作成する．これらすべての復号鍵の作成後，利用者はマスター鍵を消去する．送信者は，上記の Key-Insulated 暗号の場合と同様に暗号化を行い，受信者は自身が保持する多数の復号鍵のうち，当日の日付に対応したものを用いて復号する．また，過去の日付に対応した復号鍵は順次消去していく．このようにすることで，公開鍵を固定したまま過去に遡った安全性を保証可能とすることができる．しかしながら，このままでは利用者が保持する秘密情報 (すなわち，当日および未来の日付に対応したすべての復号鍵) のサイズが膨大となる．そこで，さらに IBE ではなく，HIBE を用いて木構造により階層的にこれら多数の復号鍵を管理することで，復号鍵サイズに関して著しく効率化を図る手法の提案がなされている [CHK03]．

■Proxy **暗号** [BF01]． 上記の Key-Insulated 暗号や Forward-Secure 暗号では，日付情報を ID とみなして IBE の暗号化が行われているが，これは本来マスター鍵がもっている完全な復号機能のうち，該当日のみ有効な復号機能の部分的委譲を行っているものと解釈することができる．したがって，日付情報以外にもさまざまな情報を用いることで，より多様な形態での復号機能の部分的委譲も可能である．たとえば，送信者が受信者に電子メールを暗号化して送信する際，“件名” を ID とみなして IBE の暗号化を行うものとしたとき，受信者は，ある “件名” を ID とみなした IBE の復号鍵を作成し，それを他者に与えることで，その件名の電子メールに関する復号機能のみを委譲することができる．このような手法は Proxy 暗号と呼ばれる．

■Keyword searchable **暗号** [BCO+04]． 上記の Proxy 暗号の非常に興味深い拡張として，Keyword searchable 暗号が知られている．Keyword searchable 暗号では，たとえば，次のような状況が想定されている．受信者は自分宛の電子メールのうち，ある件名のものだけをメールサーバから自分の端末に転送したいが，メールサーバにはその件名が

何であるかを知られたくないと考える．このとき，送信者が受信者に電子メールを送信する際，そのヘッダ情報の一部として，“件名” を ID とみなしてある定められた文字列 (たとえば，“00...0”) に IBE の暗号化を施したものを添付する．また，受信者はあらかじめメールサーバに，その “件名”を ID とみなした IBE の復号鍵を与えておく．メールサーバは，受信者宛の電子メールを受信した際，ヘッダ情報の該当する部分を，受信者から与えられた復号鍵で復号して，所定の文字列が復元されるかを確認する．所定の文字列が復元されたときのみ，この電子メールを受信者に転送する．このとき，ヘッダ情報，受信者から与えられた復号鍵 (およびメール本文) などから，それらに該当する “件名”が何であったのかが一切わからなければ，受信者は当初の目的を果たしたことになる．そのような性質をもつ IBE は特に Anonymous IBE[ABC+05] と呼ばれる．

■電子署名への変換 [BF01, CFH+09]． 興味深いことに，任意の IBE が与えられたとき，これを直ちに電子署名に変換することも可能である．これは，次のような議論により明らかである．IBE では，マスター鍵を用いることで，任意の文字列に対してそれを公開鍵とする復号鍵を作成可能である．したがって，あるメッセージに対して，そのメッセージを ID とみなした IBE の復号鍵が示されたとき，そのような復号鍵を作成することが可能なのはマスター鍵を所有している者のみであることから，その復号鍵は上記のメッセージに対するマスター鍵所有者の電子署名とみなすことができる．このような観測に基づいて，実際に IBE の構成に用いられる数学的構造を応用して，さまざまな効率的な電子署名の提案がなされている．Boneh-Lynn-Shacham 署名 [BLS04]，Boneh-Boyen 署名 [BB04]，Waters 署名 [W05] はそのような署名方式の代表例といえる．

■選択暗号文攻撃に対して安全な公開鍵暗号への変換 [CHK04]． IBE は電子署名だけでなく，高度に安全な公開鍵暗号にも変換が可能である．より具体的には，選択平文攻撃に対して安全な任意の IBE は，選択暗号文攻撃に対して安全な公開鍵暗号に変換することができる．この方法論は単に両者の存在性の関係を示唆するだけのものではなく，これに基づいて設計された公開鍵暗号方式が実際に非常に効率的となりうる点も驚くべき事実といえる．この方法論に基づいて構成された公開鍵暗号方式の代表的な例として，Boyen-Mei-Waters 暗号 [BMW05] が挙げられるが，この方式はランダムオラクルに依存せずに選択暗号文攻撃への安全性が証明できるものとしては最も効率的な方式の一つであることが知られている．特に，暗号文長に関しては，これよりも優れた方式は知られていない．

■その他． IBE の直接的な応用ではないが，その性質や構成手法の研究により得られた知見が生かされたアプリケーションとしては，たとえば次のようなものが挙げられる．放送暗号とは，受信者全体の集合のうち，送信者が自由に選んだ部分集合に属する受信者のみが復号可能となる暗号文を作成可能な暗号方式である [BGW05]．放送暗号と HIBE の構成方法に用いられる代数的構造には類似性が観測できることが知られており，実際，これらの両方を包含するようなフレームワークの提案もなされている [BH08]．グループ署名とは，署名者が，自分自身を他者に特定させることなく，正規利用者集合に属することを証明可能な署名方式である．(IBE を構成する上で有用な技術として知られる) ペアリングは，離散対数を知ることなく Diffie-Hellman 判定問題を解くことを可能とするものであり，グループ署名に必要とされるような “言語の証明 (proof of language)” の機能を簡便に提供するものである．そのため，ペアリングを利用することで，さまざまな効率的なグループ署名の提案もなされている [BBS04]．属性ベース暗号とは，IBE を拡張した概念であり，IBE の一般化のひとつともみなすことができる．属性ベース暗号においては，IBE とは異なり，送信者は復号に関するさまざまな条件を指定して暗号化を行うことができる．受信者のうち，送信者が指定した条件を満足する復号鍵をもつもののみが復号を行うことが出来る [SW05]．

1.2.3 IBS について

ID ベース署名 (IBS) は，IBE と同様，任意の文字列を公開鍵として指定することが可能な電子署名である．IBE の概念の提唱から，最低限の機能を完備した具体的な IBE の実際の提案まで 20 年近くもかかったのに対して，IBS は驚くほど容易に構成できることも知られている [S84]．より具体的には，鍵証明書の利用による従来の電子署名は，形式的にはすでに IBS としての用件を満足しており，したがって，IBS を利用することでただちに従来の電子署名インフラにおける煩雑な処理を取り除くことが可能になるとは考えづらい．IBS と従来の電子署名インフラの形式的な機能が等価であることを鑑みるに，計算コストや署名長といった基本的な評価基準において顕著な優位性が確認できない限り IBS を積極的に利用する特段の必要はないように思われる．

付録

本付録では，1.1.2 節で紹介した代表的な IBE の具体的な構成を記す．より詳しい IBE の解説は，IBE の入門書 [M08] に記されている．和書では，[KS02][TK08] に基本的な IBE が記されており，[OOK07] はペアリング演算を主に扱った解説論文である．

本付録で記す各方式は，次の記号で略記する．

BF：Boneh-Franklin 方式 (full scheme)[BF01]
SK：境-笠原方式 [SK02]
BB1：Boneh-Boyen1 方式 [BB04a]
BB2：Boneh-Boyen2 方式 [BB04a]
BB3：Boneh-Boyen3 方式 [BB04b]
W05：Waters 方式 [W05]
G06：Gentry 方式 [G06]

以下では，可能な限り各方式に共通の記号を用いる．このために，原著の記号とは異なるものを用いている．PKG のマスター秘密鍵は $s \in \mathbb{Z}_n^\times$ である．BB1 では $\beta \in \mathbb{Z}_n^\times$ もマスター鍵として加わる．このマスター鍵以外に，各ユーザ固有の秘密として，$\gamma_A, \gamma_{A_i} \in \mathbb{Z}_n^\times$ を利用する．各方式で用いられる共通のパラメータ $P, Q, P_2, U, U_{i,j}$ は $E[n]$ から，$s, \beta, \gamma_A, \gamma_{A_i}$ は $\mathbb{Z}_n^\times$ からそれぞれ適切に選ばれたものである．

各方式における共通のパラメータ，ID の変換およびユーザの復号鍵を表 1.1 に記す．また，暗号化および復号を表 1.2 に記す．ただし，BB1 については，階層が 1 の場合について記す．

表 1.1　共通パラメータおよび鍵生成

方式	共通パラメータ	ID の変換	復号鍵
BF	$P,\ sP$	$P_A = H_1(ID_A) \in E[n]$	$S_A = sP_A$
SK	$Q,\ sQ,\quad y$	$I_A = H_1(ID_A) \in \mathbb{Z}_n$	$S_A = (s + I_A)^{-1}P$
BB1	$P,\ sP,\ P_2,\ U$	$I_A = H_1(ID_A) \in \mathbb{Z}_n$	$S_{A_1} = sP_2 + \gamma_A(I_A sP + U)$ $S_{A_2} = \gamma_A P$
BB2	$P,\ sP,\ \beta P$	$I_A = H_1(ID_A) \in \mathbb{Z}_n$	$S_{A_1} = (I_A + s + \beta\gamma_A)^{-1}P$ $S_{A_2} = \gamma_A$
BB3	$P,\ sP,\ P_2,\ U_{i,j}$	$\boldsymbol{v}_A = H_1(ID_A) \in \{0,1\}^N$	$S_{A_0} = sP_2 + \sum_{i=1}^{N} \gamma_{A_i} U_{i,a_i}$ $S_{A_i} = \gamma_{A_i} P$
W05	$P,\ sP,\ P_i,\ U$	$\boldsymbol{v}_A = H_1(ID_A) \in \{0,1\}^N$	$S_{A_1} = sP + \gamma_A(U + \sum_{i=1}^{N} v_{A_i} P_i)$ $S_{A_2} = \gamma_A P$
G06	$P,\ sP,\ U$	$I_A = H_1(ID_A) \in \mathbb{Z}_n$	$S_{A_1} = (s - I_A)^{-1}(U - \gamma_A P)$, $S_{A_2} = \gamma_A$

ただし，$i = 1, 2, \ldots, N, j = 0, 1$, $\boldsymbol{v}_A = (v_{A_1}, \ldots, v_{A_N}) \in \{0,1\}^N$, $y = e(P, Q)$ である．

$e(P, sP)$, $e(P_2, sP)$, $e(P, P)$ 等のペアリング値は，固定の値であるので，SK と同様に，事前に計算された共通パラメータと見なせば，BF 以外の方式では，暗号化時にペアリング演算を必要としない．また，上述の方式の中で SK のみ非対称ペアリングの利用を想定しているが，対称ペアリングを用いても実現可能である．逆に SK 以外の方式でも，非対称ペアリングを用いることができるものもある．例えば BF は非対称ペアリングで構成することが可能である[*6]．

[*6] 非対称ペアリングを用いると安全性の根拠となる数論モデルが異なる．

表 1.2　暗号化および復号

方式	暗号化	復号
BF	$C_1 = xP, \quad x = h_3(\sigma, m),$ $C_2 = \sigma \oplus h_2(e(xP_A, sP))$ $C_3 = m \oplus h_4(\sigma)$	$\sigma' = C_2 \oplus h_2(e(sP_A, C_1))$ $C_3 \oplus h_4(\sigma') = m$ Check : $C_1 = h_3(\sigma', m)P$
SK	$C_1 = x(I_A Q + sQ)$ $C_2 = m \cdot h_2(y^x)$	$C_2 \cdot h_2(e(S_A, C_1))^{-1}$ $= C_2 \cdot h_2(y^x) \cdot h_2(e(P, Q)^x)^{-1} = m$
BB1	$C_1 = xP$ $C_2 = x(I_A sP + U)$ $C_3 = m \cdot e(P_2, sP)^x$	$C_3 \cdot e(C_2, S_{A_2}) \cdot e(S_{A_1}, C_1)^{-1}$ $= C_3 \cdot \frac{e(x(I_A sP+U), \gamma_A P)}{e(sP_2+\gamma_A(I_A sP+U), xP)}$ $= m$
BB2	$C_1 = x(I_A P + sP)$ $C_2 = x\beta P$ $C_3 = m \cdot e(P, P)^x$	$C_3 \cdot e(C_1 C_2^{S_{A_2}}, S_{A_1})^{-1}$ $= C_3 \cdot e(x(I_A + s + \beta\gamma_A)P, S_{A_1})^{-1}$ $= m$
BB3	$A = m \cdot e(sP, P_2)^x$ $B = xP$ $C_i = xU_{i,v_{A_i}}$	$\frac{A \cdot \prod_{i=1}^N e(C_i, S_{A_i})}{e(B, S_{A_0})}$ $= \frac{A \cdot e(\sum_{i=1}^N C_i, \gamma_{A_i} P)}{e(xP, sP_2 + \sum_{i=1}^N \gamma_{A_i} U_{i,v_{A_i}})}$ $= \frac{A \cdot e(\sum_{i=1}^N \gamma_{A_i} C_i, P)}{e(P, xsP_2 + \sum_{i=1}^N \gamma_{A_i} C_i)} = m.$
W05	$C_1 = xP$ $C_2 = x(U + \sum_{i=1}^N v_{A_i} P_i)$ $C_3 = m \cdot e(P, sP)^x$	$C_3 \cdot e(C_2, S_{A_2}) \cdot e(S_{A_1}, C_1)^{-1}$ $= C_3 \cdot \frac{e(x(U + \sum_{i=1}^N v_{A_i} P_i),\ \gamma_A P)}{e(sP + \gamma_A(U + \sum_{i=1}^N v_{A_i} P_i),\ xP)}$ $= m$
G06	$C_1 = x(sP - I_A P)$ $C_2 = e(P, P)^x$ $C_3 = m \cdot e(P, U)^{-x}$	$C_3 \cdot e(C_1,\ S_{A_1}) \cdot C_2^{S_{A_2}}$ $= C_3 \cdot e(xP,\ U - \gamma_A P) \cdot C_2^{\gamma_A}$ $= C_3 \cdot e(xsP, U) e(xP, \gamma_A P)^{-1} e(P, P)^{x\gamma_A} = m$

ただし，BF において，σ はランダムな系列，h_3, h_4 はハッシュ関数である．

第 1 章の参照文献

[ABC+05] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, H. Shi, "Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions," J. Cryptology Vol.21, no.3, pp.350–391, 2008.

[BGK08] A. Boldyreva, V. Goyal, V. Kumar, "Identity-based encryption with efficient revocation," ACM Conference on Computer and Communications Security 2008, pp.417-426, 2008.

[B82] R. Blom, "Non-public key distribution," CRYPTO 1982, pp.231–236, 1983.

[BB04a] D. Boneh and X. Boyen, "Efficient selective-ID secure identity based encryption without random oracles," EUROCRYPT 2004, LNCS 3027, Springer-Verlag, pp. 223–238, 2004.

[BB04] D. Boneh and X. Boyen, "Short signatures without random oracles," EUROCRYPT 2004, LNCS 3027, Springer-Verlag, pp. 56–73, 2004.

[BB04b] D. Boneh, X. Boyen, "Secure identity based encryption without random oracles," CRYPTO 2004, LNCS 3152, Springer-Verlag, pp.443–459, 2004.

[BBS04] D. Boneh, X. Boyen, H. Shacham, "Short group signatures," CRYPTO 2004, LNCS 3152, Springer-Verlag, pp.41–55, 2004.

[BCO+04] D. Boneh, G. D. Crescenzo, R. Ostrovsky, G. Persiano, "Public key encryption with keyword search," EUROCRYPT 2004, LNCS 3027, Springer-Verlag, pp.506-522, 2004.

[BF01] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," CRYPTO 2001, LNCS 2139, Springer Verlag, pp. 213–229, 2001.

[BGW05] D. Boneh, C. Gentry, B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," CRYPTO 2005, LNCS 3621, Springer-Verlag, pp.258–275, 2005.

[BH08] D. Boneh, M. Hamburg, "GeneralizediIdentity based and broadcast encryption schemes," ASIACRYPT 2008, LNCS 5350, Springer-Verlag, pp.455–470, 2008.

[BLS04] D. Boneh, H. Shacham, and B. Lynn, "Short signatures from the Weil pairing," Journal of Cryptology, vol.17, no.4, pp.297–319, 2004.

[BMW05] X. Boyen, Q. Mei, B. Waters, "Direct chosen ciphertext security from identity-based techniques," ACM Conference on Computer and Communications Security 2005, pp.320–329, 2005.

[CHK03] R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-key encryption scheme," EUROCRYPT 2003, LNCS 2656, Springer-Verlag, pp. 255–271, 2003.

[CHK04] R. Canetti, S. Halevi and J. Katz, "Chosen-ciphertext security from identity-based encryption," EUROCRYPT 2004, LNCS 3027, Springer-Verlag, pp. 207–222, 2004.

[C04] C. Cocks, "An identity based encryption scheme based on quadratic residues," IMA International Confer-

ence on Cryptography and Coding–IMA Int. Conf.2001, LNCS 2260, Springer-Verlag, pp.360–363, 2001.

[CFH+09] Y. Cui, E. Fujisaki, G. Hanaoka, H. Imai, R. Zhang, “Formal security treatments for IBE-to-signature transformation: Relations among security notions,” IEICE Transactions Vol.92-A, No.1, pp.53–66, 2009.

[DKX+02] Y. Dodis, J. Katz, S. Xu, M. Yung, “Key-insulated public key cryptosystems,” EUROCRYPT 2002, LNCS 2332, Springer-Verlag, pp.65–82, 2002.

[G06] C. Gentry, “Practical identity-based encryption without random oracles,” EUROCRYPT 2006, LNCS 4004, Springer-Verlag, pp. 445–464, 2006.

[GS02] C. Gentry, A. Silverberg, “Hierarchical ID-based cryptography,” ASIACRYPT 2002, LNCS 2501, Springer-Verlag, pp.548–566, 2002.

[HHS+05] Y. Hanaoka, G. Hanaoka, J. Shikata, H. Imai, “Identity-based hierarchical strongly key-insulated encryption and its application,” ASIACRYPT 2005, LNCS 3788, Springer-Verlag, pp.495–514, 2005.

[HL02] J. Horwitz, B. Lynn, “Toward hierarchical identity-based encryption,” EUROCRYPT 2002, LNCS 2332 Springer-Verlag, pp.466–481, 2002.

[K94] N. Koblitz, “A Course in Number Theory and Cryptography”, GTM114, Springer, 1994.

[M08] L. Martin, “Introduction to Identity-Based Encryption”, ARTECH HOUSE, 2008.

[MI87] T. Matsumoto, H. Imai, “On the key predistribution system: A practical solution to the key distribution problem,” CRYPTO 1987, LNCS 293, Springer-Verlag, pp.185–193, 1987.

[MY91] U. M. Maurer, Y. Yacobi, “Non-interactive public-key cryptography,” EUROCRYPT 1991, LNCS 547, Springer-Verlag, pp.498–507, 1991.

[MOV93] A. Menezes, T. Okamoto, S. A. Vanstone, “Reducing elliptic curve logarithms to logarithms in a finite field,” IEEE Transactions on Information Theory, Vol. 39, No. 5, pp.1639–1646, 1993.

[SW05] A. Sahai, B. Waters, “Fuzzy identity-based encryption,” EUROCRYPT 2005, LNCS 3494, Springer Verlag, pp.457–473, 2005.

[S84] A. Shamir, “Identity-based cryptosystems and signature schemes,” CRYPTO 1984, LNCS 196, Springer Verlag, pp. 47–53, 1984.

[W05] B. Waters, “Efficient identity based encryption without random oracles,” EUROCRYPT 2005, LNCS 3494, Springer Verlag, pp. 114–127, 2005.

[OT84] 岡本龍明, 白石旭, 河岡司, “単一管理情報による安全なユーザ認証方式,” 電子情報通信学会 IN83-92, Jan.1984

[MK90] 村上恭通, 笠原正雄, “合成数を法とする離散対数問題,” 信学技報 ISEC90-42, pp.29-36, 1990.

[OSK99] 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 ISEC99-57, pp.37-42, Nov.1999.

[SOK00] 境隆一, 大岸聖史, 笠原正雄, “Cryptosystems Based on Pairing”, 暗号と情報セキュリティシンポジウム予稿集, SCIS2000, C20,Jan.2000.

[SOK01] 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”, 暗号と情報セキュリティシンポジウム予稿集, SCIS2001, SCIS2001,7B-2,2001 年 1 月.

[SK02] 境隆一, 笠原正雄, “楕円曲線上のペアリングに基づく二，三の暗号方式 (その 2),” 信学技報, ISEC2002-52, pp.131-138, Jul.2002.

[KS02] 笠原正雄, 境隆一, 「暗号〜ネットワーク社会の安全を守る鍵」，インターネット時代の数学シリーズ， 共立出版, 2002.

[TK08] 辻井重男，笠原正雄編書, 「暗号理論と楕円曲線」5 章，森北出版, 2008.

[OOK07] 岡本栄司, 岡本 健, 金山直樹, “ペアリングに関する最近の研究動向,” 電子情報通信学会 Fundamentals Review, Vol. 1, No.1, pp.51-60, 2007.
[C-R02]「CRYPTREC Report 2002 暗号技術評価報告書 (2002 年度)」, pp.95-113, 2002.

第 2 章

安全性評価について

2.1 節では，安全性評価手法についてまとめ，2.2 節では，数学的仮定についてまとめる．

2.1 安全性評価手法

2.1.1 概要

ここでは，具体的な個々の IBE の安全性を評価するための手法について述べる．IBE の安全性評価は，他の暗号プリミティブと同様に，まず，安全性レベルの定義を行い，その上で，評価の対象となる個々の IBE がどのような安全性レベルを有しているかを調べることで行われる．また，ある IBE がある安全性レベルを有していることを主張する際には，その IBE のその安全性レベルを破る困難さと，ある種の数学的問題の困難さが密接に関係していることを示す必要がある．

2.1.2 帰着による安全性証明

ある安全性レベル $\mathcal{L}$ の意味である IBE 方式 $\mathcal{I}$ を破る手法が存在すると仮定し，その手法を用いて，解くことが不可能とされるような，ある数学的問題 $\mathcal{P}$ を解くことが可能であることを示せたものとする．これは，つまり，IBE 方式 $\mathcal{I}$ の安全性レベル $\mathcal{L}$ を破るような手法が何か存在すれば，直ちに，数学的問題 $\mathcal{P}$ が解けたものと見なされることになる．すなわち，数学的問題 $\mathcal{P}$ を解くことが不可能であると仮定する限りは，IBE 方式 $\mathcal{I}$ の安全性レベル $\mathcal{L}$ は絶対に保証されるものと考えることができる．

言い換えれば，安全性レベル $\mathcal{L}$ の意味で IBE 方式 $\mathcal{I}$ を破るアルゴリズムをブラックボックスとして，数学的問題 $\mathcal{P}$ を解いてみせることが，安全性の証明そのものといえる．数学的問題 $\mathcal{P}$ を解くことが不可能であると仮定したうえで，IBE 方式 $\mathcal{I}$ の安全性レベル $\mathcal{L}$ を破ることも不可能であるといえる場合，通常，「$\mathcal{P}$ の困難性の仮定の下，$\mathcal{I}$ は $\mathcal{L}$ の意味で安全」などと表現する．

具体的な IBE 方式同士で安全性の優劣を判断する際は，安全性レベルと数学的仮定の強さが主な判断基準となる．以下では，それらについて簡単に述べる．

2.1.3 安全性レベルの定義と評価

安全性レベルの定義をするにあたり，まずは IBE 自体の定義を行う必要がある．公開鍵暗号方式 $\mathcal{I}$ は，セットアップアルゴリズム SET，鍵生成アルゴリズム GEN，暗号化アルゴリズム ENC，復号アルゴリズム DEC の 4 つのアルゴ

リズムの組として定義される．

SET: 1^k を入力とし，マスター鍵と共通パラメータのペア (msk, prm) を出力するアルゴリズム．ここで，k はセキュリティパラメータとする．

GEN: マスター鍵 msk，文字列 ID と共通パラメータ prm を入力とし，ID に対応した復号鍵 sk_{ID} を出力するアルゴリズム．

ENC: 平文 $m \in M$，文字列 ID と共通パラメータ prm を入力とし，暗号文 c を出力するアルゴリズム．ただし，M は平文空間とする．

DEC: 暗号文 c と復号鍵 sk_{ID} を入力とし，平文 m（もしくは，失敗を表すシンボル “$\perp$”）を出力する確定的アルゴリズム．

PKG は SET により，マスター鍵と共通パラメータのペアを生成し，このうち共通パラメータを周知させる．（PKG については 1.2 節を参照されたい．）PKG は GEN により各利用者の復号鍵を生成する．送信者は ENC により平文を受信者の公開鍵で暗号化し，受信者に送信する．受信者は DEC により，復号鍵を用いて受信した暗号文の復号を行う．IBE 方式の安全性のレベルは次のように定義される．

定義 2.1 任意の多項式時間アルゴリズム $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対して，IBE 方式 $\mathcal{I} = (\mathsf{SET}, \mathsf{GEN}, \mathsf{ENC}, \mathsf{DEC})$ が次式を満足するものとする:

$$|\Pr[\mathbf{Exp}^{ind-1}_{\mathcal{I},\mathcal{A}}(k) = 1] - \Pr[\mathbf{Exp}^{ind-0}_{\mathcal{I},\mathcal{A}} = 1]| < \epsilon(k)$$

($\epsilon(k)$ は無視できる値)．ただし，$\mathbf{Exp}^{ind-b}_{\mathcal{I},\mathcal{A}}(k)$ は，$b \in \{0, 1\}$ に対する次の試行とする:

$\mathbf{Exp}^{ind-b}_{\mathcal{I},\mathcal{A}}(k)$
$(msk, prm) \leftarrow \mathsf{SET}(1^k)$; $(\mathsf{ID}^\star, m_0, m_1, s_1) \leftarrow \mathcal{A}_1^{\mathcal{E},\mathcal{D}}(prm)$; $c^\star \leftarrow \mathsf{ENC}(m_b, \mathsf{ID}^\star, prm)$;
$b' \leftarrow \mathcal{A}_2^{\mathcal{E},\mathcal{D}}(\mathsf{ID}^\star, m_0, m_1, c^\star, prm, s_1)$;
return b'.

このとき，$\mathcal{E}$ は ($\mathsf{ID}^\star$ 以外の) 任意の文字列 ID に対して sk_{ID} を返答するオラクルとし，$\mathcal{D}$ は (($\mathsf{ID}^\star, c^\star$) 以外の) 任意の文字列と暗号文のペア (ID, c) に対して c を sk_{ID} で復号した結果を返答するオラクルとすると，$\mathcal{I}$ は安全性レベルとして IND-ID-CCA 安全性を有しているという．また，$\mathcal{D}$ は任意の入力に対してランダムな値を返答するものとすると，$\mathcal{I}$ は安全性レベルとして IND-ID-CPA 安全性を有しているという [BF01].

定義 2.2 任意の多項式時間アルゴリズム $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ に対して，IBE 方式 $\mathcal{I} = (\mathsf{SET}, \mathsf{GEN}, \mathsf{ENC}, \mathsf{DEC})$ が次式を満足するものとする:

$$|\Pr[\mathbf{Exp}^{ind-1}_{\mathcal{I},\mathcal{A}}(k) = 1] - \Pr[\mathbf{Exp}^{ind-0}_{\mathcal{I},\mathcal{A}} = 1]| < \epsilon(k)$$

($\epsilon(k)$ は無視できる値)．ただし，$\mathbf{Exp}^{ind-b}_{\mathcal{I},\mathcal{A}}(k)$ は，$b \in \{0, 1\}$ に対する次の試行とする:

$\mathbf{Exp}^{ind-b}_{\mathcal{I},\mathcal{A}}(k)$
$(\mathsf{ID}^\star, s_1) \leftarrow \mathcal{A}_1(1^k)$;
$(msk, prm) \leftarrow \mathsf{SET}(1^k)$; $(m_0, m_1, s_2) \leftarrow \mathcal{A}_2^{\mathcal{E},\mathcal{D}}(prm, s_1)$; $c^\star \leftarrow \mathsf{ENC}(m_b, \mathsf{ID}^\star, prm)$;
$b' \leftarrow \mathcal{A}_3^{\mathcal{E},\mathcal{D}}(\mathsf{ID}^\star, m_0, m_1, c^\star, prm, s_2)$;
return b'.

このとき，$\mathcal{E}$ は ($\mathsf{ID}^\star$ 以外の) 任意の文字列 ID に対して sk_{ID} を返答するオラクルとし，$\mathcal{D}$ は (($\mathsf{ID}^\star, c^\star$) 以外の) 任意の文字列と暗号文のペア ($\mathsf{ID}, c$) に対して c を sk_{ID} で復号した結果を返答するオラクルとすると，$\mathcal{I}$ は安全性レベルとして IND-sID-CCA 安全性を有しているという．また，$\mathcal{D}$ は任意の入力に対してランダムな値を返答するものとすると，$\mathcal{I}$ は安全性レベルとして IND-sID-CPA 安全性を有しているという [CHK03].

明白な事実として，IBE 方式 $\mathcal{I}$ が IND-ID-CCA 安全性を満足するとき，IND-ID-CPA 安全性，IND-sID-CCA 安全性，IND-sID-CPA 安全性はすべて自動的に満足される．すなわち，IND-ID-CCA 安全性はこれらの安全性レベルの定義のなかでは，もっとも強い安全性の概念であるといえる．また，IBE 方式 $\mathcal{I}$ が IND-sID-CCA 安全性を満足するとき，IND-sID-CPA 安全性は自動的に満足され，IBE 方式 $\mathcal{I}$ が IND-ID-CPA 安全性を満足するとき，IND-sID-CPA 安全性は自動的に満足される．

2.1.4 数学的仮定の強さの評価

安全性の根拠となる数学的問題が実際により困難であるほど，その数学的問題を解くことを不可能とする仮定はより弱いものとみなすことができる．したがって，同じ安全性レベルを達成しているのであれば，より弱い仮定のみを必要とする方式のほうが高い安全性を有しているといえる．これまでに提案されているさまざまな IBE 方式は，たとえば，2.2 節に示されるような仮定を用いて安全性が根拠づけられている．ここでは，実際に利用される数学的仮定についての紹介は，2.2 節に譲り，数学的仮定の強さの評価手法について説明を行う．

■数学的仮定同士の直接的な比較． 数学的問題同士の困難性の比較は，一方を解く手法が存在したとして，その手法を用いてもう一方も解ければ，前者は後者と同等かより難しいと考えることができる．たとえば，CBDH 問題 [BF01] を解くことができれば，ほぼ自動的に DBDH 問題 [CHK03] を解くこともできるため，CBDH 問題は DBDH 問題よりも難しいことがわかる．（CBDH 問題及び DBDH 問題については 2.2.4 節を参照されたい．）したがって，すでに十分に困難だと考えられている数学的問題があれば，それよりも難しいことを示すことで，別の数学的問題の困難性の妥当性も主張することができる．

■Generic group モデルを用いた比較． 上記の要領で妥当性を示すことができなかった場合は，generic group モデルにおいて，計算量の下界を導出することで数学的問題の困難性を評価する手法もよく利用される [Sh97, BBG05]．ただし，この手法はあくまで一つの目安を与えるものであって仮定の妥当性について全幅の信頼を保証するものではない．generic group モデルとは，評価の対象となる数学的問題が利用する群について，群構造以外の一切の代数的性質が無いものとする数学モデルであり，したがって，(乗法群であれば) 群の元同士の乗算以外の操作はできないものとしている．離散対数問題から派生する数学的問題の多くは，この generic group モデルにおいて，必要な計算量の下界を導出することができ，それを用いて困難性をある程度評価することができる．

■ハッシュ関数の理想化の度合いに関する比較． 安全性の仮定において，数学的問題の困難性のほかに，方式内で副次的に利用されているハッシュ関数の理想化の度合もしばしば評価の対象となる．特に，最も理想化されたハッシュ関数の概念であるランダムオラクルを利用しなければ安全性が証明可能でない場合には，注意が必要となる．なぜなら，ランダムオラクルは理想化の度合いが極端に強く，現実世界には絶対に存在しえないことが証明されている [CGH98]．したがって，ランダムオラクルを利用して安全性の証明が可能な方式が存在したとして，そのようなハッシュ関数を実際に用いることは不可能であるため，実際に実装された方式の安全性は不明となる．そのため，ランダムオラクルを用いることでしか安全性の証明ができない方式は，random oracle モデルに依存していることを明示することで，それを用いない方式と区別される．ランダムオラクルを利用しない場合，standard モデルと呼ばれることが多い．これらふ

たつのモデルを比較した場合，当然，standard モデルで証明可能な方式のほうがより優れているとされる．

■帰着効率に関する比較．別の安全性の評価尺度として，帰着効率と呼ばれるものがある．上述のとおり，ある IBE がある安全性レベルを有していることを主張するために，その安全性を破ることの困難性と，安全性の根拠となる数学的問題の困難性が密接に関係しあっていることを示すことになるが，その際，これらの関係の強さを示す度合が帰着効率である．今，「$\mathcal{P}$ の困難性の仮定の下，$\mathcal{I}$ は $\mathcal{L}$ の意味で安全」であることを証明しようとするものとしよう．このとき，$\mathcal{I}$ を $\mathcal{L}$ の意味で破る手法 $\mathcal{A}$ が存在したとして，$\mathcal{A}$ をブラックボックスとして用いて $\mathcal{P}$ を解くことが可能であることを示すことになる．その際，$\mathcal{I}$ を $\mathcal{L}$ の意味で破るための計算時間 t と成功確率 ω と，$\mathcal{P}$ を解くための計算時間 t' と成功確率 ω' に関して，t と t' の差と ω と ω' の差がいずれも小さければ小さいほど，$\mathcal{I}$ の安全性と $\mathcal{P}$ の困難性とが強く結び付いていることが確認できる．また，これらの差の一方，もしくは，両方ともが大きい場合，$\mathcal{P}$ が困難であるからと言って $\mathcal{I}$ が ($\mathcal{L}$ の意味で) 安全であるとの主張は弱まる．したがって，二つの方式が同じ安全性レベルを同じ数学的仮定で証明可能であったとしても，このような評価尺度を用いることで安全性に優劣をつけることが可能である．とくに ω' と ω の比率に注目して，そのような評価がなされることが多いため，ω'/ω がしばしば帰着効率と呼ばれている．

2.2 数学的仮定について

従来，標準的に使用されてきた公開鍵暗号の多くは，素因数分解問題の困難性，又は（楕円）離散対数問題の困難性にその安全性の根拠を置いていた．そして，それらの派生問題として，RSA 問題，CDH 問題，DDH 問題等が考えられ，その困難性と共に，問題間の帰着関係などが考えられてきた．前節までに述べてきたように，IBE は楕円曲線上のペアリングを用いて効率的に実現される．更に，ペアリングは多くの暗号応用を有することが知られている．以降，ペアリングを用いて実現された暗号系をペアリング暗号と総称し，それらペアリング暗号の安全性を保証する（計算困難な）数学的問題とそれが導く数学的仮定について述べる．

ペアリング暗号は，有限体乗法群と楕円曲線有理点群上の離散対数問題困難性がその安全性基盤である（一部，素因数分解問題困難性を組み合わせた方式も存在する）．つまり，従来の離散対数問題困難性に基づいた暗号と異なり，ペアリング暗号では，用いられる 3 種（又は 2 種）の巡回群全てで離散対数問題が困難であることが必要になり，考慮すべき事項も複雑化する．よって，安全なペアリング暗号の実現のために，使用する各巡回群上での離散対数問題困難性に関して考慮すべき点について，2.2.2 節で述べる．

また，ペアリング演算固有の基本的な計算問題として，ペアリング逆関数問題が考えられている．その困難性研究の現状を報告すると共に，CDH 問題や CBDH 問題等の基本問題との関連を 2.2.3 節で扱う．

前節までに述べたように，暗号系に対して，計算困難な問題への帰着を用いて，安全性証明が行われる．ペアリング暗号では，その実現する機能の豊富さゆえに，従来とは比較にならない個数の数学的問題が安全性証明のために考案されている（既に述べたように，それら問題の基盤は離散対数問題である）．例えば，双線型 Diffie-Hellman 問題 (BDH)，双線型 Diffie-Hellman 指数問題 (ℓ-BDHE)，Diffie-Hellman 逆元問題 (ℓ-BDHI)，強 Diffie-Hellman 計算問題 (ℓ-SDH) 等がある．それら基本的な計算問題の派生問題を 2.2.4 節で扱い，各問題が規定する仮定に基づいて安全性証明される方式に言及する．また，いくつかの問題については generic group モデルでの困難性証明についても述べる．

2.2.1 ペアリングのタイプ分け

3 つの素数位数 n の巡回群 $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ に関するペアリング

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$$

は，通常，効率的に計算できる同型写像 $\psi_1 : \mathbb{G}_1 \to \mathbb{G}_2$ 及び $\psi_2 : \mathbb{G}_2 \to \mathbb{G}_1$ の存在有無に応じて，以下の 3 タイプに分けて論じられる [GPS08, B08].

1. $\mathbb{G}_1 = \mathbb{G}_2$．つまり，$\psi_1, \psi_2$ 共に存在する．
2. $\mathbb{G}_1 \neq \mathbb{G}_2$ かつ ψ_2 が存在する（及び ψ_1 の存在は知られていない）．
3. $\mathbb{G}_1 \neq \mathbb{G}_2$ かつ ψ_1 及び ψ_2 の存在が知られていない．

タイプ 1 は対称ペアリングと呼ばれ，タイプ 2 及び 3 は非対称ペアリングと呼ばれている．各タイプの有利及び不利な点の詳細に関しては，[GPS08] を参照することとする．ここでは，以降の記述に関連する範囲でその一部を記述する．

対称（タイプ 1）ペアリングでは，標数 3 有限体上の楕円曲線を用いること等により，高速なペアリング演算が実現できるという有利な点が存在する．また，対称ペアリングでは，効率的な ψ_1 や ψ_2 を用いることで，暗号系構成や安全性証明が行われることがある．しかし，限定された楕円曲線しか使用できないことにより，柔軟なセキュリティレベルの設定ができないなどの不利な点も存在する．例えば，2.2.2 節で述べるように，埋め込み次数 κ というパラメータが高々 6 に制限されることで，用いる巡回群位数 n が他のタイプと比較して大きな値に制限されたりすることがある．

タイプ 2 ペアリングでは，タイプ 1 同様，効率的な ψ_2 を用いて暗号系構成や安全性証明が行われることがある．そして，非対称ペアリングでは，タイプ 1 と異なり，埋め込み次数や群位数に関して比較的制限がなくパラメータ生成ができるのが利点である．しかし，タイプ 2 では，群 $\mathbb{G}_2$ へ直接写像するハッシュ関数が構成できない場合があり，そのようなハッシュ関数が必要な暗号系構成においては不利となる場合がある．

タイプ 3 ペアリングでは，パラメータ生成に関しタイプ 2 と同様の利点を有すると共に，タイプ 2 と異なり，群 $\mathbb{G}_2$ へのハッシュ関数が構成できる．また，効率的な ψ_2 の非存在を積極的に数学的仮定として用いて従来にない暗号系構成を行うという研究報告もある．しかし，タイプ 3 では，ψ_2 が存在しないために，暗号プロトコルが構成できなかったり，安全性証明が成立しない場合があるなど不利な場合もある．

また，ペアリング暗号が導入された当初は，対称ペアリングに限定される場合が多かったが，宮地-中林-高野の研究 [MNT01] を契機として，上に述べたような固有の利点を有する方法として，非対称ペアリングも研究されてきている．非対称ペアリング用の楕円曲線パラメータ構成法に関しては多くの研究成果が報告されている．

2.2.2 $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ 上の離散対数問題困難性

次に，$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ を実現するペアリングに適した楕円曲線に関連する記法を定める．ペアリング暗号に適した楕円曲線 E は有限体 $\mathbb{F}_q$ を係数とする 2 変数多項式方程式

$$y^2 + h(x)y = f(x) \quad \text{但し，} \deg(f) = 3,\ \deg(h) \leq 1$$

で定義される．ペアリング暗号に適した曲線では埋め込み次数 κ と呼ばれる整数パラメータが比較的小さく設定できる必要がある．その κ に対して，上記方程式を満たす有限体 $\mathbb{F}_{q^\kappa}$ の要素の対 (x, y) と無限遠点からなる集合を $E(\mathbb{F}_{q^\kappa})$ と表す．集合 $E(\mathbb{F}_{q^\kappa})$ は，効率的に計算可能な群演算を有し，巡回群 $\mathbb{G}_1$ 及び $\mathbb{G}_2$ は，$E(\mathbb{F}_{q^\kappa})$ の部分群として実現される．多くの場合，$\mathbb{G}_1$ は，部分群 $E(\mathbb{F}_q)$ $(\subset E(\mathbb{F}_{q^\kappa}))$ 内の部分群として実現される．そして，巡回群 $\mathbb{G}_T$ は，乗法群 $\mathbb{F}_{q^\kappa}^\times$ の部分群として実現される．

従来，離散対数問題困難性は，一般数体ふるい法が適用可能な場合と，そうでない場合，即ち，BSGS 法等の任意の巡回群に対して適用可能な方法が最善法である場合の 2 種類に分けて考えられてきた．ここでは，それら 2 種の計算法に関し安全な群のサイズを規定するパラメータを，それぞれ B_1 及び B_2 と書き，その凡その指標を，[GPS08] に従い，

出典	k	B_1	B_2
NIST [NIST05]	80	160	1024
	128	256	3072
	256	512	15360
Lenstra [L05]	80	160	1329
	128	256	4440
	256	512	26268
ECRYPT [EC05]	80	160	1248
	128	256	3248
	256	512	15424

表 2.1　B_1 と B_2 の推奨値

表 2.1 にまとめる．表 2.1 で，k はセキュリティパラメータで 2^k 回の基本演算で解読可能なセキュリティレベルを表す．その算出に必要な有限体上の離散対数問題の一般理論に関しては，[U03] 及び，その参考文献を参照し，楕円曲線上の離散対数問題の一般理論に関しては，[CF06, Part V] を参照する．

ペアリングを有する群を用いる場合の顕著な特徴は，それら 2 種類の安全性条件を同時に考慮する必要があることである．また，以下で見るように，$\mathbb{G}_T$ の離散対数問題に関しては，楕円曲線パラメータの選び方によっては，一般数体ふるい法より効率的な解法が知られている場合があるので，その場合には，表 2.1 内の B_2 より大きな値を用いて群サイズを決定する必要がある．

下記の 3 つの（2 種類の）離散対数問題の困難性が，全てのペアリング暗号の計算量仮定の基盤であり，実際のパラメータ選択は，それが定めるセキュリティパラメータに基づいて行われる．

■$\mathbb{G}_1$ 及び $\mathbb{G}_2$ 上の楕円離散対数問題　$\mathbb{G}_1$ 及び $\mathbb{G}_2$ は，楕円曲線上の有理点からなる群で実現される．現状では，楕円離散対数問題に対する最適な方法は BSGS 法等の一般的な巡回群に対する方法である．よって，$\mathbb{G}_1$ 及び $\mathbb{G}_2$ 上の離散対数問題困難性を保証するには，$\log_2 n \geq B_1$ が必要となる．

■$\mathbb{G}_T$ 上の有限体乗法群離散対数問題　$\mathbb{G}_T$ は有限体乗法群で実現されるので，$\mathbb{G}_T$ 上の離散対数問題の困難性を保証するには，$\kappa \log_2 q \geq B_2$ が必要となる．但し，パラメータに応じて最適化された以下の離散対数計算法に対する対策が必要である．

また，対称ペアリングの場合は $\kappa \leq 6$ であるので，$\kappa \log_2 q \geq B_2$ より，$\log_2 q$ を大きくする必要が生じる場合がある．一方，非対称ペアリングでは，例えば $\kappa = 12$ のパラメータ生成法が知られているので，そのような制約を回避できる場合がある．

有限体の標数が 2 又は 3 の場合は，関数体ふるい法 [JL05, GHP+04, HST09] が有効な離散対数計算法を与える．よって，$\kappa \log_2 q$ を，上記の評価より更に大きい値に設定する必要がある．この正確な値を評価するには，離散対数計算実験を実際に行い，検証する必要がある．しかし，既存の実験検証報告には，まだ改良の余地が認められる．特に，標数 3 での実験検証は遅れている（[HST09] 参照）．標数 3 の離散対数計算実験では，$\mathbb{F}_{3^{277}}$, 即ち，有限体乗法群のサイズが $277 \cdot \log_2(3) \approx 440$ ビット相当の場合の報告しかされていない．また，標数 2 では，613 ビット相当の報告がある [JL05].

また，標数が $2, 3$ でない場合にも，ペアリング暗号用の楕円曲線生成法と関連して，一般数体ふるい法より効率化できる可能性があることが報告されている [Sc06]．本報告は，関数体ふるい法の場合と同様，$\kappa \log_2 q$ の設定と関連する

が，その実験検証報告はまだ行われていない状況である．

2.2.3 ペアリング逆関数問題の困難性

ペアリング逆関数問題は，FAPI-1 問題，FAPI-2 問題，GPI 問題に類別され，ここでは，特に，FAPI-1 問題, FAPI-2 問題が効率的に計算できれば，ペアリング暗号にとって基本的な数学問題が効率的に計算できることを述べる．また，ペアリング逆関数問題の困難性評価研究は，2.2.2 節で扱った離散対数問題困難性研究に比べ歴史も浅く，今後の動向を監視する必要性が高い．

また，以下では，計算問題の帰着関係を表すのに，問題 $\mathrm{Problem}_1$ が問題 $\mathrm{Problem}_2$ に (確率的) 多項式時間帰着可能である時，$\mathrm{Problem}_1 \leq_p \mathrm{Problem}_2$ と書く．

■一般的な帰着関係 ペアリング関数 $e(P,Q)$ は，P と Q に関する二変数関数であり，どの変数に関して問題の定式化を行うかによって，以下のように，FAPI-1 問題，FAPI-2 問題，GPI 問題が定義される．

定義 2.3 一変数に関する（通常の）ペアリング逆関数問題 *(Fixed Argument Pairing Inversion : FAPI-1, FAPI-2)* と二変数に関する（一般化された）ペアリング逆関数問題 *(Generalized Pairing Inversion : GPI).*

$$e(P,Q) = z \tag{2.1}$$

1. *FAPI-1* 問題*:* P, z が与えられて *(2.1)* を満たす Q を答える問題.
2. *FAPI-2* 問題*:* Q, z が与えられて *(2.1)* を満たす P を答える問題.
3. *GPI* 問題*:* z が与えられて *(2.1)* を満たす P と Q を答える問題.

定理 2.4 *FAPI-1* 及び *FAPI-2* が共に効率的に解けるなら，全ての $i = 1, 2, T$ に対し，$\mathbb{G}_i$ 内の *CDH* 問題が効率的に解ける．

という Verheul の帰着により，ペアリング逆関数問題は，ペアリング暗号安全性にとって基本的な問題と位置づけられる．定理 2.4 は，ペアリング逆関数問題の困難性を評価することが重要であることを示す一方で，CDH 問題の困難性を仮定すれば，FAPI-1 問題又は FAPI-2 問題の困難性が保証されることを示している．

ペアリング逆関数問題困難性の研究はまだ多くはないが，[GHV07, GhES07, Sa07, Ver08] 等の報告がある．現状，実際にペアリング逆関数計算可能な特別なパラメータは報告されていない．が，各研究成果があり，例えば，超特異曲線かそうでないかとか，Ate ペアリングかそうでないかといった観点で，問題の困難性や特性の違いが論じられている．明らかに，GPI $\leq_p$ FAPI-1 及び GPI $\leq_p$ FAPI-2，つまり，FAPI-1 問題又は FAPI-2 問題が解けると GPI 問題が解ける，という帰着関係が成立する．しかし，既に述べたように，FAPI 問題より潜在的に容易である GPI 問題に対しても，現状では，GPI 問題計算可能な特別なパラメータは報告されていない．

FAPI 問題と群の同型写像 ψ_1, ψ_2 の関係として，次の 3 条件は同値であることが知られている．

1. FAPI-1 問題 と FAPI-2 問題 が効率的に解ける．
2. FAPI-1 問題が効率的に解け，効率的な ψ_2 がある．
3. FAPI-2 問題が効率的に解け，効率的な ψ_1 がある．

これにより，タイプ 1 ペアリングに関しては，FAPI-1 又は FAPI-2 問題が効率的に解ければ，全ての $i = 1, 2, T$ に関し，$\mathbb{G}_i$ 内の CDH 問題が効率的に解けることが定理 2.4 より導かれ，タイプ 2 ペアリングに関しては，FAPI-1 問題が効率的に解ければ，全ての $i = 1, 2, T$ に関し，$\mathbb{G}_i$ 内の CDH 問題が効率的に解けることが同様に導かれる．

また，ψ_1, ψ_2 共に存在しないタイプ 3 ペアリングに対しても，FAPI-1 又は FAPI-2 問題が解ければ，（適当な）BDH 問題が解けることが知られている．つまり，一つの FAPI-i $(i = 1, 2)$ が解けるだけでも基本的なペアリング暗号の安全性が損なわれる．

また，FAPI-2 問題のみ解ける時に，Cheon アルゴリズム [C06] を利用して $\mathbb{G}_2$ 内の離散対数計算を若干効率化する方法も報告されている [M08]．

■個別のペアリングに関する安全性評価　既に述べたように，現状，ペアリング逆関数計算に成功する曲線及びペアリングの例は知られていないが，その困難性の解析及び評価は進んでおり，その現状を把握することは大変重要である．

Tate ペアリングや Ate ペアリングといったペアリング計算は，Miller アルゴリズム実行後，最終べき乗算を実行することで行われる．よって，ペアリング逆関数の計算法として，まず，最終べき乗算逆関数計算を行い，次に Miller アルゴリズム逆関数計算を行うという 2 段階での計算法が自然に考えられる．

以下では，FAPI-2 問題を，Miller アルゴリズム逆関数問題 (Miller Inversion : MI) と最終べき乗算逆関数問題に分割する定式化と関連する既存報告結果について述べる [GHV07, GhES07, Ver08]．多くのペアリング関数は Miller 関数 $f_{s,P}$ と整数 L によるべき乗算を用いて，

$$z = e(P, Q) = f_{s,P}(Q)^L \quad \text{即ち，} \quad z_0 = f_{s,P}(Q),\ z = z_0^L$$

と表される．この時，MI 問題は，$P \in \mathbb{G}_1, z_0$, 及び部分集合 $S \subset \mathbb{G}_2$ が与えられて $z_0 = f_{s,P}(Q)$ となる $Q \in S$ を答えるか，「S に解なし」を答える問題と定式化されている [GHV07]．最終べき乗算逆関数問題は，z と L が与えられて，z_0 を計算する問題である．

[GHV07, GhES07] 等において MI 問題が容易である実例や最終べき乗算が必要ないような実例が提示されている．しかし，どの場合も最終的な FAPI 問題又は GPI 問題の効率的な計算には成功していない．また，最終べき乗算逆関数問題と関連して，オラクルアクセス付きの HRP (Hidden Roots Problem) 問題という形の問題が研究されている [Ver08]．

2.2.4　安全性証明に用いられる各数学的仮定の定義と特性

ペアリング暗号の安全性証明に用いられる各数学的仮定の定義と特性をまとめる．それらは，数学的問題の困難性に対する仮定であるので，以下では，その各数学的問題を記述する．ここでは，ペアリングにより実現される代表的な IBE・署名方式の安全性証明で用いられる数学的仮定を記述する．そして，各仮定に基づき安全性が証明される IBE・署名方式についてコメントした．

ペアリングを用いない従来の安全性証明付き各種暗号・署名方式と比較して，ペアリングを用いる各種暗号・署名方式に関しては，各方式ごとに特化した多様な数学的仮定が，その安全性証明に用いられるのが特徴的である．それゆえに，今後も，ペアリングを用いた新しい応用の開発によって新たな数学的仮定が追加されていくと予想される．それら各仮定の困難性評価がペアリング暗号にとって重要であることは言うまでもない．その評価には，多様な数学的仮定に対応するための有識者の広い協力が必要であると共に，新規の数学的仮定に対応するための継続的な監視が必要である．

一般に，対称ペアリングと非対称ペアリングの場合で，同名の仮定が若干異なって参照される場合があるが，ここでは Boyen のサーベイ論文 [B08] を参考にして，全てのタイプのペアリングで有効になる数学的問題及び仮定を代表として記述した．また，generic group モデル での安全性帰着及びその評価状況の一部についてもまとめた．多くの文献では，数学的仮定の記述で巡回群 $\mathbb{G}_1, \mathbb{G}_2$ の群演算を乗法表記しているが，前節までの表記法との統一を図るため，以下でも，巡回群 $\mathbb{G}_1, \mathbb{G}_2$ の群演算を加法で表記する記法を採用する．

また，パラメータ ℓ 付きの仮定を始めて導入したのは 光成-境-笠原 [MSK02] であり，以後，その先駆的な枠組みが拡張／整備されてきている．

■計算問題と判定問題　本節で述べる計算量問題には，CDH 問題のような解を求める計算問題と，DDH 問題のような実際の解とランダムな値を判別させる判定問題との 2 種類の問題がある．その多くは，CDH 問題と DDH 問題のように，計算問題に対応して判定問題も困難な問題として，安全性証明に有用な数学的仮定を与える．しかし，例えば，計算問題である ℓ-SDH 問題のように，ペアリングを有する群上では，その判定問題は自明な解法を有する場合もある．

■数学的問題と数学的仮定

co-Diffie-Hellman 計算問題

入力：$R \in \mathbb{G}_1$，　$Q, \alpha Q \in \mathbb{G}_2$
出力（計算問題：co-CDH）：$\alpha R \in \mathbb{G}_1$

co-CDH 問題が困難であるという仮定を co-CDH 仮定という．ランダムオラクルモデル 及び co-CDH 仮定の下で，Boneh-Lynn-Shacham 署名 [BLS04] は，選択的メッセージ攻撃に対する存在的偽造不可能性が証明される．

双線型 Diffie-Hellman 計算問題

入力：$P, \alpha P, \gamma P \in \mathbb{G}_1$，$Q, \alpha Q, \beta Q \in \mathbb{G}_2$
出力（計算問題：CBDH）：$e(P,Q)^{\alpha\beta\gamma}$

CBDH 問題が困難であるという仮定を，CBDH 仮定という．ランダムオラクルモデル 及び CBDH 仮定の下で，Boneh-Franklin IBE 方式 [BF01] は，IND-ID-CCA 安全性（2.1 節参照）が証明される．CBDH 問題に対応する判定問題である DBDH 問題は，以下のように与えられる．

双線型 Diffie-Hellman 判定問題

入力：$P, \alpha P, \gamma P \in \mathbb{G}_1$，$Q, \alpha Q, \beta Q \in \mathbb{G}_2$
出力（判定問題：DBDH）：テスト入力 $v \in \mathbb{G}_T$ に対して，$v \stackrel{?}{=} e(P,Q)^{\alpha\beta\gamma}$ を判定

DBDH 問題が困難であるという仮定を，DBDH 仮定という．standard モデル及び DBDH 仮定の下で，Boneh-Boyen IBE 第 1 方式 [BB04a]（BB_1 IBE 方式）は，IND-sID-CCA 安全性（2.1 節参照）が証明される．また，同じく standard モデル及び DBDH 仮定の下で，Waters IBE 方式 [W05] は，IND-ID-CCA 安全性（2.1 節参照）が証明される．共に，選択平文攻撃（CPA）に対して安全な 2 階層の階層的 IBE 方式を CHK 変換 [CHK04] 又は BK 変換 [BK05] を用いて選択暗号文攻撃（CCA）に対して安全な IBE 方式へ変換している．

以下の ℓ-wBDHI (Inversion) 仮定は，形の上では，ℓ-BDHE (Exponent) 系の仮定であるが，[BBG05] で指摘されている ℓ-BDHI 仮定との関連性から，Boyen [B08] によりこの名称が与えられている．また，ℓ-wBDHI 仮定は，系列

$$P, \alpha P, \ldots, \alpha^{\ell} P$$

が与えられて，系列の次の要素 $\alpha^{\ell+1}P$ と βQ のペアリング $e(P,Q)^{\alpha^{\ell+1}\beta}$ を計算，又は判定する問題であるが，ℓ-BDHE 仮定では，系列

$$P, \alpha P, \ldots, \alpha^{\ell-1} P,\ \alpha^{\ell+1} P, \ldots, \alpha^{2\ell} P$$

が与えられて，中央に抜けた要素 $\alpha^{\ell}P$ と βQ のペアリング $e(P,Q)^{\alpha^{\ell}\beta}$ を計算，又は判定する問題である．truncated Augmented 双線型 Diffie-Hellman 指数仮定は，形の上では ℓ-wBDHI 仮定と相似しているが，ℓ-BDHE 仮定の入力の一部を切り詰めた（truncate）した形になっているので，その仮定を導入した Gentry [G06] により，このように呼

ばれた．また，本稿では truncated Augmented 双線型 Diffie-Hellman 指数仮定に関しても [B08] の記述法に準じて記載した．[G06] での元来の仮定は，本稿の仮定で $\beta = 1$ としたものである．以下では，計算問題と判定問題が対応して存在する場合は，両問題をまとめて記述した．

双線型 Diffie-Hellman 逆元計算問題 及び 判定問題

入力：$P, \alpha P, \alpha^2 P, \ldots, \alpha^\ell P \in \mathbb{G}_1$，$Q \in \mathbb{G}_2$

出力（計算問題：ℓ-CBDHI）：$e(P,Q)^{1/\alpha}$

出力（判定問題：ℓ-DBDHI）：テスト入力 $v \in \mathbb{G}_T$ に対して，$v \stackrel{?}{=} e(P,Q)^{1/\alpha}$ を判定

弱 双線型 Diffie-Hellman 逆元計算問題 及び 判定問題

入力：$P, \alpha P, \alpha^2 P, \ldots, \alpha^\ell P \in \mathbb{G}_1$，$Q, \beta Q \in \mathbb{G}_2$

出力（計算問題：ℓ-wCBDHI）：$e(P,Q)^{\alpha^{\ell+1}\beta}$

出力（判定問題：ℓ-wDBDHI）：テスト入力 $v \in \mathbb{G}_T$ に対して，$v \stackrel{?}{=} e(P,Q)^{\alpha^{\ell+1}\beta}$ を判定

truncated Augmented 双線型 Diffie-Hellman 指数計算問題 及び 判定問題

入力：$P, \alpha P, \alpha^2 P, \ldots, \alpha^\ell P \in \mathbb{G}_1$，$Q, \beta Q, \alpha^{\ell+2} Q \in \mathbb{G}_2$

出力（計算問題：ℓ-CtABDHE）：$e(P,Q)^{\alpha^{\ell+1}\beta}$

出力（判定問題：ℓ-DtABDHE）：テスト入力 $v \in \mathbb{G}_T$ に対して，$v \stackrel{?}{=} e(P,Q)^{\alpha^{\ell+1}\beta}$ を判定

双線型 Diffie-Hellman 指数計算問題 及び 判定問題

入力：$P, \alpha P, \alpha^2 P, \ldots, \alpha^{\ell-1} P,\ \alpha^{\ell+1} P, \ldots, \alpha^{2\ell} P \in \mathbb{G}_1$，$Q, \beta Q \in \mathbb{G}_2$

出力（計算問題：ℓ-CBDHE）：$e(P,Q)^{\alpha^\ell \beta}$

出力（判定問題：ℓ-DBDHE）：テスト入力 $v \in \mathbb{G}_T$ に対して，$v \stackrel{?}{=} e(P,Q)^{\alpha^\ell \beta}$ を判定

上記の各問題が困難であるという仮定が，それぞれ対応する各仮定を規定する．ランダムオラクルモデル及び ℓ-CBDHI 仮定の下で，境-笠原 IBE 方式 [SK03] は，IND-ID-CCA 安全性（2.1 節参照）が証明される．standard モデル及び ℓ-DBDHI 仮定の下で，Boneh-Boyen IBE 第 2 方式 [BB04a]（BB_2 IBE 方式）は，IND-sID-CPA 安全性（2.1 節参照）が証明される．[B07] では，BB_2 IBE 方式を階層的 IBE 方式へ拡張する方法が示された．これにより，BB_2 IBE 方式の IND-sID-CCA 安全な IBE 方式への拡張も CHK 変換 [CHK04] 又は BK 変換 [BK05] を用いることで得られる．

standard モデル及び ℓ-DtABDHE 仮定の下で，Gentry IBE 方式 [G06] は，IND-ID-CCA 安全性（2.1 節参照）が証明される．

強 Diffie-Hellman 計算問題

入力：$P, \alpha P, \alpha^2 P, \ldots, \alpha^\ell P \in \mathbb{G}_1$，$Q, \alpha Q \in \mathbb{G}_2$

出力（計算問題：ℓ-SDH）：$(w, \frac{1}{\alpha+w} P)$

ℓ-SDH 問題が困難であるという仮定を ℓ-SDH 仮定という．standard モデル及び ℓ-SDH 仮定の下で，Boneh-Boyen 署名 [BB04b] は，選択的メッセージ攻撃に対して強存在的偽造不可能性が証明される．その詳細については，[BB04b] を参照されたい．

パラメータ ℓ 付きの上記の各問題に対しては，Cheon による特別な計算法 [C06, KKM07] が知られている．今後も，CDH 仮定や BDH 仮定といった（長さパラメータ ℓ なしの）仮定には適用されないような，ℓ 付き仮定に対する固有な計算法に十分注意する必要がある．また，本計算法を考慮してセキュリティマージンをとる必要がある．

■数学的仮定に対する generic group モデルでの安全性証明　その基本的説明は 2.1 節で行われた．[B08] に基づいて記述する．

各判定問題に対する解答者に与えられる $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ の要素を，その係数を表す多項式で表現し，それぞれ $\mathcal{U} = (u_1, \ldots, u_v) \in \mathbb{F}_n[X_1, \ldots, X_c]^v$, $\mathcal{S} = (s_1, \ldots, s_\sigma) \in \mathbb{F}_n[X_1, \ldots, X_c]^\sigma$, $\mathcal{T} = (t_1, \ldots, t_\tau) \in \mathbb{F}_n[X_1, \ldots, X_c]^\tau$ として，判定する $\mathbb{G}_T$ の元の $e(P, Q)$ を底とする離散対数を表す多項式を ρ とする．ここで，n は巡回群 $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ の位数である．また，$d_\mathcal{U} := \max_{u_i \in \mathcal{U}}\{\deg(u_i)\}$, $d_\mathcal{S} := \max_{s_i \in \mathcal{S}}\{\deg(s_i)\}$, $d_\mathcal{T} := \max_{t_i \in \mathcal{T}}\{\deg(t_i)\}$, $d_\rho := \deg(\rho)$ とし，

$$d := \begin{cases} \max\{2d_\mathcal{U}, 2d_\mathcal{S}, d_\mathcal{U} + d_\mathcal{S}, d_\mathcal{T}, d_\rho\} & \text{タイプ 1 ペアリングの時} \\ \max\{2d_\mathcal{S}, d_\mathcal{U} + d_\mathcal{S}, d_\mathcal{T}, d_\rho\} & \text{タイプ 2 ペアリングの時} \\ \max\{d_\mathcal{U} + d_\mathcal{S}, d_\mathcal{T}, d_\rho\} & \text{タイプ 3 ペアリングの時} \end{cases}$$

とする．ρ が $(\mathcal{U}, \mathcal{S}, \mathcal{T})$ と独立であれば，generic group モデルでの解答者 $\mathcal{A}$ の advantage は，次式で上からバウンドされる．

$$\mathtt{Adv}_\mathcal{A} \leq \frac{(\tau + 2c + 2)^2 \cdot d}{2n} \tag{2.2}$$

但し，τ は，$\mathcal{A}$ の計算中における，全ての群演算オラクル，ペアリングオラクルへのアクセス総数を表す．本節で述べたいくつかの判定問題に対し，不等式 (2.2) は $\mathcal{A}$ の advantage がセキュリティパラメータに対して無視できる関数で上から押さえられることを示しているので，それら判定問題が導く仮定の妥当性を示している．また，複数の判定問題に対する generic group モデルでの $\mathcal{A}$ の advantage の上界の比較で，各仮定間の優劣が検討される．詳しくは [B08] 等を参照されたい．

■その他の数学的仮定　上記の他にも，線型性判定仮定や SDH 仮定の変形版などのペアリングを有する群に関する数学的仮定が，種々の暗号及び署名系の安全性証明の中で用いられている．詳しくは [B08] 等を参照されたい．

第 2 章の参照文献

[BB04a] D. Boneh and X. Boyen, "Efficient selective-ID secure identity based encryption without random oracles," EUROCRYPT 2004, LNCS 3027, Springer-Verlag, pp. 223–238, 2004.

[BB04b] D. Boneh and X. Boyen, "Short signatures without random oracles," EUROCRYPT 2004, LNCS 3027, Springer-Verlag, pp. 56–73, 2004.

[BBG05] D. Boneh, X. Boyen and E. Goh, "Hierarchical identity based encryption with constant size ciphertext," EUROCRYPT 2005, LNCS 3494, Springer-Verlag, pp. 440–456, 2005.

[BF01] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," CRYPTO 2001, LNCS 2139, Springer Verlag, pp. 213–229, 2001.

[BK05] D. Boneh and J. Katz, "Improved efficiency for CCA-secure cryptosystems built using identity based encryption," CT-RSA 2005, LNCS 3376, Springer Verlag, pp. 87–103, 2005.

[BLS04] D. Boneh, H. Shacham, and B. Lynn, "Short signatures from the Weil pairing," Journal of Cryptology, vol. 17, no. 4, pp. 297–319, 2004.

[B07] X. Boyen, "General ad hoc encryption from exponent inversion IBE," EUROCRYPT 2007, LNCS 4515, Springer-Verlag, pp. 394–411, 2007.

[B08] X. Boyen, "The uber-assumption family: A unified complexity framework for bilinear groups," Pairing 2008, LNCS 5209, Springer-Verlag, pp. 39–56, 2008.

[CGH98] R. Canetti, O. Goldreich, and S. Halevi, "The Random Oracle Methodology, Revisited (Preliminary Version)," STOC 1998, ACM, pp. 209–218, 1998.

[CHK03] R. Canetti, S. Halevi, and J. Katz, "A Forward-Secure Public-Key Encryption Scheme," EUROCRYPT 2003, LNCS 2656, Springer-Verlag, pp. 255–271, 2003.

[CHK04] R. Canetti, S. Halevi and J. Katz, "Chosen-ciphertext security from identity-based encryption," EUROCRYPT 2004, LNCS 3027, Springer-Verlag, pp. 207–222, 2004.

[C06] J.H. Cheon, "Security analysis of the strong Diffie-Hellman problem," EUROCRYPT 2006, LNCS 4004, Springer Verlag, pp. 1–11, 2006.

[CF06] H. Cohen and G. Frey ed., Handbook of Elliptic and Hyperelliptic Curve Cryptography, Chapman & Hall, 2006.

[EC05] ECRYPT Yearly Report on Algorithms and Keysizes (2004), March 2005. Available from http://www.ecrypt.eu.org/documents/D.SPA.10-1.1.pdf.

[GHV07] S.D. Galbraith, F. Hess, and F. Vercauteren "Aspects of pairing inversion," IEEE Transactions on Information Theory, vol. 54, no. 12, pp. 5719–5728, December 2008.

[GhES07] S. D. Galbraith, C. O hEigeartaigh, C. Sheedy, "Simplified pairing computation and security implica-

tions", J. Mathematical Crypt, vol. 1, no. 3, pp. 267–281, 2007.

[GPS08] S.D. Galbraith, K.G. Paterson, N.P. Smart, "Pairings for cryptographers", Discrete Applied Mathematics, vol. 156, pp. 3113–3121, 2008.

[G06] C. Gentry, "Practical identity-based encryption without random oracles," EUROCRYPT 2006, LNCS 4004, Springer-Verlag, pp. 445–464, 2006.

[GHP+04] R. Granger, A. Holt, D. Page, N. Smart, F. Vercauteren, " Function Field Sieve in Characteristic Three." ANTS-VI, LNCS 3076, Springer-Verlag, pp. 223–234. 2004.

[HST09] 林卓也，白勢政明，高木剛 "GF(3^n) 上の関数体篩法における篩処理の実装実験," SCIS 2009, 3F1–1，2009.

[JL05] A. Joux, R. Lercier, "Discrete logarithms in GF(2^{607}) and GF(2^{613})," Number Theory List, available at http://perso.univ-rennes1.fr/reynald.lercier/file/nmbrJL05a.html.

[KKM07] S. Kozaki, T. Kutsuma, K. Matsuo, "Remarks on Cheon's algorithms for pairing-related problems," Pairing 2007, LNCS 4575, Springer-Verlag, pp. 302–316, 2007.

[L05] A.K. Lenstra, Key lengths, in: Handbook of Information Security, vol. 2, Wiley, pp. 617–635, 2005.

[M08] D.J. Mireles Morales, "Cheon's algorithm, pairing inversion and the discrete logarithm problem," IACR ePrint 2008/300.

[MSK02] S. Mitsunari, R. Sakai, and M. Kasahara, "A new traitor tracing," IEICE Transactions on Fundamentals, vol. E85-A, no. 2, pp. 481–484, Feb. 2002.

[MNT01] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," IEICE Transactions on Fundamentals, vol. E84-A, no. 5, pp. 1234–1243, May 2001.

[NIST05] NIST Recommendation for Key Management Part 1: General, NIST Special Publication 800-57. August, 2005. Available from http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf.

[Sa07] T. Satoh, "On pairing inversion problems," Pairing 2007, LNCS 4575, Springer-Verlag, pp. 317–328, 2007.

[SK03] R. Sakai and M. Kasahara, "ID based cryptosystems with pairing on elliptic curve," IACR ePrint 2003/54.

[Sc06] O. Schirokauer, "The number field sieve for integers of low weight," preprint, IACR ePrint 2006/107, to appear in Mathematics of Computation.

[Sh97] V. Shoup "Lower Bounds for Discrete Logarithms and Related Problems," EUROCRYPT 1997, LNCS 1233, Springer-Verlag, pp. 256–266, 1997.

[U03] 内山成憲, "有限体上の離散対数問題 – 数体ふるい法，関数体ふるい法 –," 日本応用数理学会論文誌 vol.13, no.2, pp. 245–256, 2003.

[V08] F. Vercauteren, "The hidden root problem," Pairing 2008, LNCS 5209, Springer-Verlag, pp. 89–99, 2008.

[W05] B. Waters, "Efficient identity based encryption without random oracles," EUROCRYPT 2005, LNCS 3494, Springer Verlag, pp. 114–127, 2005.

第 3 章

実装動向

前章までで述べた通り, 本報告書が主題としている ID ベース暗号 (IBE) は, 楕円曲線上のペアリング (pairing) と呼ばれる双線形写像を用いて構成されており, 実際に IBE を使用するにはペアリングの実装が必要となる. そこで本章では, IBE の実装において広く用いられているペアリングとして, Tate ペアリング (3.1 節), η_T ペアリング (3.2 節), Ate ペアリング (3.3 節) の具体的な計算手順と, さまざまな実行環境における実装結果をまとめる[*1]. 本報告書では, 国内では電子情報通信学会の情報セキュリティ (ISEC) 研究会, 暗号と情報セキュリティシンポジウム (SCIS), 情報処理学会のコンピュータセキュリティ (CSEC) 研究会, コンピュータセキュリティシンポジウム (CSS), 海外では国際暗号研究学会 (IACR) が主催する国際会議である CRYPTO, EUROCRYPT, ASIACRYPT, PKC, CHES, およびペアリング関連技術の国際会議である Pairing において, 2000 年から 2008 年までの間に発表された論文を主たる調査対象とした[*2]. また 3.4 節では, IBE を構成するために必要となる, ID 情報から楕円曲線上の点への変換関数 (MapToPoint 関数) の計算手順についても述べる.

本章で使用する記号・用語を以下にまとめる. 3 つの素数位数 n の巡回群 $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$ に対するペアリングを $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ と記す. ここでペアリング e は

- [双線形性] 任意の整数 a, b と任意の要素 $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$ に対し $e(aP, bQ) = e(P, Q)^{ab}$

を満たすものとする. 巡回群 $\mathbb{G}_T$ における出力値の一意性を確保するために, 本報告書では最終ベキと呼ばれる計算もペアリング計算の一部として扱う. また, $\mathbb{F}_q$ を要素数 q の有限体 (q は素数 p のべきで, p は有限体の標数と呼ばれる), E を有限体 $\mathbb{F}_q$ 上の楕円曲線 (elliptic curve), $\#E(\mathbb{F}_q)$ を ($\mathbb{F}_q$-有理点の) 位数とする. κ を楕円曲線 E の埋め込み次数とするとき, 以下では, 巡回群 $\mathbb{G}_1$, $\mathbb{G}_2$ として $E(\mathbb{F}_{q^\kappa})$ の部分群が, 巡回群 $\mathbb{G}_T$ として $\mathbb{F}_{q^\kappa}^\times$ の部分群が用いられる (このため, 巡回群 $\mathbb{G}_1$, $\mathbb{G}_2$ の演算は加法的, 巡回群 $\mathbb{G}_T$ の演算は乗法的であることに注意せよ). また, 楕円曲線 E のトレース $t = q + 1 - \#E(\mathbb{F}_q)$ が標数 p で割り切れるとき, この楕円曲線は超特異 (supersingular) であるといい, そうでないときは通常 (ordinary) であるという. 超特異な楕円曲線の埋め込み次数は 6 以下になることが知られている [MOV93]. なお, 本章ではペアリングの数学的な背景には触れないため, 必要に応じて, 適当な文献 (例えば [BSS05] など) を参照されたい.

[*1] 暗号研究で最初に用いられたペアリングは Weil ペアリングだったが, 他のペアリングに比べて計算効率が劣ることから, 実装ではあまり使用されていない.

[*2] ただし SCIS 2009 については調査対象とした. また, (Weierstrass 型と呼ばれる標準的な) 楕円曲線上で定義されたペアリングのみを調査対象とした.

アルゴリズム 3.1　Tate ペアリングの計算手順

Input: $P \in E(\mathbb{F}_q)[n]$, $Q = (x_Q, y_Q) \in E(\mathbb{F}_{q^\kappa})$	
Output: $e_T(P, Q) \in \mu_n$	
(初期設定)	$T \leftarrow P$, $f \leftarrow 1$
(ループ計算)	for i from $\lceil \log_2 n \rceil - 2$ downto 0
	$T \leftarrow 2T$
	$f \leftarrow f^2 \cdot \ell_{T,T}(x_Q, y_Q)$
	if n_i=1 then
	$T \leftarrow T + P$
	$f \leftarrow f \cdot \ell_{T,P}(x_Q, y_Q)$
	end if
	end for
(最終べき計算)	$f \leftarrow f^{(q^\kappa - 1)/n}$
(結果出力)	return f

3.1　Tate ペアリング

本節では Tate ペアリングの計算手順と実装例をまとめる.

3.1.1　Tate ペアリングの計算手順

$E(\mathbb{F}_q)[n] = \{P \in E(\mathbb{F}_q) | nP = \mathcal{O}\}$, $\mu_n = \{x \in \mathbb{F}_{q^\kappa}^\times | x^n = 1\}$ とおくとき, ペアリング

$$e_T : E(\mathbb{F}_q)[n] \times E(\mathbb{F}_{q^\kappa})/nE(\mathbb{F}_{q^\kappa}) \to \mu_n \tag{3.1}$$

を Tate ペアリング (Tate pairing) [*3] と呼ぶ. Tate ペアリングの計算手順をアルゴリズム 3.1 に示す. ここで $\sum_{i=0}^{\lceil \log_2 n \rceil - 1} n_i 2^i$ は n の 2 進展開を表す. また, $\ell_{T,T}$ は楕円曲線 E 上の点 T における接線, $\ell_{T,P}$ は楕円曲線 E 上の点 T, P を通る直線を表す.

アルゴリズム 3.1 からわかる通り, Tate ペアリングの計算はループと最終べきの 2 つの計算から構成される. ループ部分は Miller が提案した多項式時間アルゴリズム [M86] であり, Miller アルゴリズムとも呼ばれる.

3.1.2　Tate ペアリングの実装例

Tate ペアリングの実装例として, PC での実装報告を表 3.1 に, FPGA での実装報告を表 3.2 (標数 2), 表 3.3 に, スマートカードでの実装報告を表 3.4 に, 組み込み用 CPU での実装報告を表 3.5 にまとめる. 各表には参照文献・楕円曲線パラメータ・実行環境・周波数・実行時間などが, 楕円曲線の定義体の標数別 (2, 3, $p > 3$) にまとめられている. なお $E(\mathbb{F}_{3^{97}})$ は有限体 $\mathbb{F}_{3^{97}}$ 上の楕円曲線を表すが, 楕円曲線の具体的なパラメータ (係数) は省略されているため, 異なる箇所で同じ記号が用いられていても, それらの楕円曲線自体が等しいとは限らない. 同様に p_{512} は 512 ビッ

[*3] Tate-Lichtenbaum ペアリング (Tate-Lichtenbaum pairing) ともいう.

表 3.1　Tate ペアリングの実装例 (PC)

参照文献	楕円曲線	実行環境	実行時間 (μs)
○標数 2			
[BKL+02]	$E(\mathbb{F}_{2^{271}})$	Intel Pentium 3 (1.0 GHz)	23000
○標数 3			
[BKL+02]	$E(\mathbb{F}_{3^{97}})$	Intel Pentium 3 (1.0 GHz)	26200
○標数 p			
[S07]	$E(\mathbb{F}_{p_{160}})$ (MNT 曲線, $\kappa = 6$)	Intel Pentium 4 (3.0 GHz), 前計算なし	6200
		Intel Pentium 4 (3.0 GHz), 前計算あり	4500
[AON+06]	$E(\mathbb{F}_{p_{216}})$ (MNT 曲線, $\kappa = 6$)	Intel Pentium 4 (3.8 GHz)	44400
[AON+06]	$E(\mathbb{F}_{p_{223}})$ (MNT 曲線, $\kappa = 4$)	Intel Pentium 4 (3.8 GHz)	30900
[SKN+08] [NAS+08]	$E(\mathbb{F}_{p_{254}})$ (BN 曲線, $\kappa = 12$)	Intel Pentium 4 (3.0 GHz)	27200
[DSD07]	$E(\mathbb{F}_{p_{256}})$ (BN 曲線, $\kappa = 12$)	Intel Pentium 4 (3.4 GHz)	46100
[BKL+02]	$E(\mathbb{F}_{p_{512}})$ (超特異曲線, $\kappa = 2$)	Intel Pentium 3 (1.0 GHz), 前計算なし	20000
		Intel Pentium 3 (1.0 GHz), 前計算あり	8600
[S05]	$E(\mathbb{F}_{p_{512}})$ (超特異曲線, $\kappa = 2$)	Intel Pentium 4 (3.0 GHz)	8900
[S05]	$E(\mathbb{F}_{p_{512}})$ (通常曲線, $\kappa = 2$)	Intel Pentium 4 (3.0 GHz)	7200
[SCA06]	$E(\mathbb{F}_{p_{512}})$ (通常曲線, $\kappa = 2$)	Intel Pentium 4 (3.0 GHz)	2970
[S07]	$E(\mathbb{F}_{p_{512}})$ (CP 曲線, $\kappa = 2$)	Intel Pentium 4 (3.0 GHz), 前計算なし	6700
		Intel Pentium 4 (3.0 GHz), 前計算あり	3000
[S07]	$E(\mathbb{F}_{p_{512}})$ (通常曲線, $\kappa = 2$)	Intel Pentium 4 (3.0 GHz), 前計算なし	5100
		Intel Pentium 4 (3.0 GHz), 前計算あり	3000

トの素数を表すが, 素数値そのものは省略されているため, 異なる箇所で同じ記号が用いられていても, 素数自体が等しいとは限らない. いずれにしても各表は実装報告を簡易的にまとめたものであるため, 詳細な計算パラメータ・計算方法・使用言語・計算環境・コンパイルオプション等については, 参照文献をあたられたい.

Tate ペアリングは基本的なペアリングであり, 有限体の標数や楕円曲線の選択に対する制限が少ないため, IBE が提案された直後からさまざまなパラメータ・実行環境での実装がすすめられ, その実装結果が報告されてきている. Tate ペアリングは, 超特異な楕円曲線上で計算された場合, 楕円曲線の位数計算や, 点 Q の生成が簡単になるというメリットがあるため, 初期の実装報告では超特異な楕円曲線が好んで用いられていた. しかし楕円曲線選択の制約の緩和や, 実装におけるさらなる高速化を図るため, 近年は通常の楕円曲線, 特に MNT 曲線 (Miyaji-Nakabayashi-Takano 曲線, [MNT01]), BN 曲線 (Barreto-Naehrig 曲線, [BN06]), CP 曲線 (Cocks-Pinch 曲線, [BSS05]) のような, ペアリングの高速計算目的で生成された曲線 (Pairing-friendly 曲線) が用いられるようになっている.

表 3.2　Tate ペアリングの実装例 (FPGA, 標数 2)

参照文献	楕円曲線	実行環境	周波数 (MHz)	回路規模 (slice)	実行時間 (μs)
○標数 2					
[SKG06]	$E(\mathbb{F}_{2^{239}})$	Xilinx xc2vp100	84	25287	41
[BBD+08a]	$E(\mathbb{F}_{2^{239}})$	Xilinx xc2vp20	123	4557	107
			165	2736	127
			199	2366	196
[KKC+06]	$E(\mathbb{F}_{2^{251}})$	Xilinx xc2v6000	40	27725	2370
			43	21955	2580
			50	16621	6440
[KRM+07]	$E(\mathbb{F}_{2^{251}})$	Xilinx xc2v6000	40	13387	2600
				6181	3200
				3788	4900
[BBD+08a]	$E(\mathbb{F}_{2^{251}})$	Xilinx xc2vp20	126	4861	117
			145	3140	157
			185	2270	227
[KKC+06]	$E(\mathbb{F}_{2^{283}})$	Xilinx xc2v6000	47	24655	2810
			49	22636	3230
			50	18599	7980
[SKG06]	$E(\mathbb{F}_{2^{283}})$	Xilinx xc2vp100	72	37803	61
[KRM+07]	$E(\mathbb{F}_{2^{283}})$	Xilinx xc2v6000	40	15065	3000
				6981	3800
				4273	6000
[BBD+08a]	$E(\mathbb{F}_{2^{283}})$	Xilinx xc2vp20	127	5350	140
			140	3481	200
			169	2517	313
[ROM+06]	$E(\mathbb{F}_{2^{313}})$	Xilinx xc2vp100	33	44060	146
			50	41078	124
			55	34675	203
[BBD+08a]	$E(\mathbb{F}_{2^{313}})$	Xilinx xc2vp20	111	6310	186
			156	3731	213
			182	2661	347
[BBD+08a]	$E(\mathbb{F}_{2^{459}})$	Xilinx xc2vp20	115	8153	327
			135	5297	492
			168	3809	771

表 3.3　Tate ペアリングの実装例 (FPGA, 標数 3)

参照文献	楕円曲線	実行環境	周波数 (MHz)	回路規模 (Gate)	実行時間 (μs)
○標数 3					
[GP05]	$E(\mathbb{F}_{3^{89}})$	Xilinx xc2vp4	16	4233	6059
			150	4233	1141
[GP05]	$E(\mathbb{F}_{3^{97}})$	Xilinx xc2vp4	16	4481	4055
			150	4481	432
[KMP+05]	$E(\mathbb{F}_{3^{97}})$	Xilinx xc2vp125	15	55616	850
[BBD+08a]	$E(\mathbb{F}_{3^{97}})$	Xilinx xc2vp20	105	4455	92
			128	2711	117
			156	1896	178
[BBD+08a]	$E(\mathbb{F}_{3^{103}})$	Xilinx xc2vp20	103	4695	99
			126	2841	132
			151	2003	217
[BBD+08a]	$E(\mathbb{F}_{3^{119}})$	Xilinx xc2vp20	99	5293	127
			125	3225	166
			140	2223	299
[BBD+08a]	$E(\mathbb{F}_{3^{127}})$	Xilinx xc2vp20	99	5596	145
			129	3379	186
			149	2320	317
[BBD+08a]	$E(\mathbb{F}_{3^{193}})$	Xilinx xc2vp20	90	8266	298
			111	4905	433
			147	3266	682

表 3.4　Tate ペアリングの実装例 (スマートカード)

参照文献	楕円曲線	実行環境	周波数 (MHz)	実行時間 (ms)
○標数 p				
[SCA06]	$E(\mathbb{F}_{p_{512}})$ (通常曲線, $\kappa = 2$)	Philips HiPerSmart	9	1010
			20.57	470
			36	290
[DSD07]	$E(\mathbb{F}_{p_{256}})$ (BN 曲線, $\kappa = 12$)	Philips HiPerSmart	9	19770
			20.57	9960

表 3.5　Tate ペアリングの実装例 (組み込み用 CPU)

参照文献	楕円曲線	実行環境	周波数 (MHz)	実行時間 (ms)
○標数 2				
[SOS+08]	$E(\mathbb{F}_{2^{271}})$	Atmel ATmega128L	7.3828	10960
[SOS+08]	$E(\mathbb{F}_{2^{271}})$	TI MSP430	8.192	5250
○標数 3				
[YTK+08]	$E(\mathbb{F}_{3^{97}})$	ARM 9	150	98.96
			225	66.00
[YTK+08]	$E(\mathbb{F}_{3^{167}})$	ARM 9	150	549.39
			225	356.11
[YTK+08]	$E(\mathbb{F}_{3^{193}})$	ARM 9	150	701.18
			225	457.93
[YTK+08]	$E(\mathbb{F}_{3^{239}})$	ARM 9	150	1303.07
			225	847.56
[YTK+08]	$E(\mathbb{F}_{3^{313}})$	ARM 9	150	2616.63
			225	1702.64
○標数 p				
[OAM+07]	$E(\mathbb{F}_{p_{256}})$ (超特異曲線, $\kappa = 2$)	Atmel ATmega128L	7.3828	30210
[SOS+08]	$E(\mathbb{F}_{p_{256}})$ (通常曲線, $\kappa = 4$)	Atmel ATmega128L	7.3828	17930
[YKF+09]	$E(\mathbb{F}_{p_{512}})$ (通常曲線, $\kappa = 2$)	ARM 9	150	1463.13
			225	969.25

3.2　η_T ペアリング

本節では η_T ペアリングの計算手順と実装例をまとめる.

3.2.1　η_T ペアリングの計算手順

標数が小さな有限体上の超特異な楕円曲線上で Tate ペアリングを計算する際に, Frobenius 写像を利用することで高速計算が可能となることを Duursma-Lee は示した (Duursma-Lee アルゴリズム, [DL03]). Barreto-Galbraith-O'hEigeartaigh-Scott はこの改良をさらに推し進め, η_T ペアリングと呼ばれるペアリングを導入した [BGO+05].

$E(\mathbb{F}_{3^m})[n] = \{P \in E(\mathbb{F}_{3^m}) | nP = \mathcal{O}\}$, $\mu_n = \mathbb{F}_{3^{6m}}^{\times}/(\mathbb{F}_{3^{6m}}^{\times})^n$ とおくとき, ペアリング

$$e_\eta : E(\mathbb{F}_{3^m})[n] \times E(\mathbb{F}_{3^m})[n] \to \mu_n \tag{3.2}$$

によって定義されるペアリングを (標数 3) における η_T ペアリング (η_T pairing) と呼ぶ [BGO+05]. 定義からわかる通り, η_T ペアリングは対称ペアリング (タイプ 1 ペアリング) となっている (2.2.1 節参照). 有限体 $\mathbb{F}_{3^m}$ に対して定義される超特異な楕円曲線 $E : y^2 = x^3 - x + b$ $(b = \pm 1)$ 上での η_T ペアリングの計算手順をアルゴリズム 3.2 に示す.

アルゴリズム 3.2　η_T ペアリングの計算手順 (標数 3)

Input: $P=(x_P, y_P)$, $Q=(x_Q, y_Q) \in E(\mathbb{F}_{3^m})[n]$	
Output: $e_\eta(P,Q) \in \mu_n$	
(初期設定)	if $b=1$ then $y_P \leftarrow -y_P$
	$f \leftarrow \sigma y_Q + y_P(\rho - x_P - x_Q - 1)$
(ループ計算)	for i from 0 upto $(m-1)/2$
	$u \leftarrow x_P + x_Q + b$
	$g \leftarrow \sigma y_P y_Q - u^2 - \rho u - \rho^2$
	$f \leftarrow fg$
	$x_P \leftarrow x_P^{1/3}$, $y_P \leftarrow y_P^{1/3}$
	$x_Q \leftarrow x_Q^3$, $y_Q \leftarrow y_Q^3$
	end for
(最終べき計算)	$f \leftarrow f^{(3^{3m}-1)(3^m+1)(3^m-3^{(m+1)/2}+1)}$
(結果出力)	return f

ここで σ は $\sigma^2+1=0$ を満たす ($\mathbb{F}_{3^{2m}}$ の) 要素, ここで ρ は $\rho^3-\rho-1=0$ を満たす ($\mathbb{F}_{3^{3m}}$ の) 要素を表す.

アルゴリズム 3.2 からわかる通り, η_T ペアリングの計算はループと最終べきの 2 つの計算から構成されるが, ループ部分の繰り返し回数は (Tate ペアリングに対する) Duursma-Lee アルゴリズムの半分となっている.

さらなる高速化を目的として, η_T ペアリングを変型した Universal η_T ペアリング [STO07, SKT+07] が提案されているが, 本報告書では調査の対象外とした.

3.2.2　η_T ペアリングの実装例

η_T ペアリングの実装例として, PC での実装報告を表 3.6 に, FPGA での実装報告を表 3.7 (標数 2) に, スマートカードでの実装報告を表 3.8 に, 組み込み用 CPU での実装報告を表 3.9 に, ASIC での実装報告を表 3.10 にまとめる (3.1.2 節で述べた表に対する注意事項を参照のこと).

Barreto-Galbraith-O'hEigeartaigh-Scott が η_T ペアリングを導入した背景は標数 3 の有限体では 3 乗計算が高速に計算できる点であるため [BGO+05], これまでに標数 3 の有限体を用いた η_T ペアリング実装が多く報告されている. 実際, η_T ペアリングは他のペアリングに比べて高速に計算可能であり, 標数の小ささから, FPGA (表 3.7), スマートカード (表 3.8), ASIC (表 3.10) などの非 PC 環境での実装が盛んに進められている. さらには, 表に含まれていない報告結果として, 携帯電話での実装例も報告されている [KTO06, YTK+06, KTO08].

3.3　Ate ペアリング

本節では Ate ペアリングの計算手順と実装例をまとめる.

3.3.1　Ate ペアリングの計算手順

Tate ペアリングは超特異楕円曲線以外では (高速) 実装しにくいという問題があった. そこで Hess-Smart-Vercauteren は Tate ペアリングを変型することで, より広い範囲の楕円曲線に適用可能な Ate ペアリングを提案した

表 3.6　η_T ペアリングの実装例 (PC)

参照文献	楕円曲線	実行環境	実行時間 (μs)
○標数 2			
[ZKO08]	$E(\mathbb{F}_{2^{241}})$	Intel Core 2 Duo (2.0 GHz) [Java]	9960
[SCA06]	$E(\mathbb{F}_{2^{379}})$	Intel Pentium 4 (3.0 GHz)	3880
○標数 3			
[KST+07]	$E(\mathbb{F}_{3^{97}})$	AMD Opteron 275 (2.2 GHz)	1164
		AMD Opteron 275 (2.2 GHz, SSE2)	479
[IST07]	$E(\mathbb{F}_{3^{97}})$	Intel Core 2 Duo (1.86 GHz)	5410
[KTO08]	$E(\mathbb{F}_{3^{97}})$	Intel Pentium D (3.2 GHz) [Java]	3772
[IST08]	$E(\mathbb{F}_{3^{97}})$	Intel Core 2 Duo (1.86 GHz)	6990
[KAT08]	$E(\mathbb{F}_{3^{97}})$	AMD Opteron 275 (2.2 GHz)	614
[M09]	$E(\mathbb{F}_{3^{97}})$	Intel Core 2 Duo (2.6 GHz, single)	149
		Intel Core 2 Duo (2.6 GHz, multi)	92
[SST09]	$E(\mathbb{F}_{3^{97}})$	Intel Core 2 Duo (1.86 GHz)	1730
[KTO08]	$E(\mathbb{F}_{3^{167}})$	Intel Pentium D (3.2 GHz) [Java]	17371
[KST+07]	$E(\mathbb{F}_{3^{167}})$	AMD Opteron 275 (2.2 GHz)	4406
[IST08]	$E(\mathbb{F}_{3^{167}})$	Intel Core 2 Duo (1.86 GHz)	25740
[KAT08]	$E(\mathbb{F}_{3^{167}})$	AMD Opteron 275 (2.2 GHz)	1687
[KTO08]	$E(\mathbb{F}_{3^{193}})$	Intel Pentium D (3.2 GHz) [Java]	26707
[KST+07]	$E(\mathbb{F}_{3^{193}})$	AMD Opteron 275 (2.2 GHz)	6267
[IST08]	$E(\mathbb{F}_{3^{193}})$	Intel Core 2 Duo (1.86 GHz)	41960
[KAT08]	$E(\mathbb{F}_{3^{193}})$	AMD Opteron 275 (2.2 GHz)	2611
[M09]	$E(\mathbb{F}_{3^{193}})$	Intel Core 2 Duo (2.6 GHz, single)	975
		Intel Core 2 Duo (2.6 GHz, multi)	553
[KTO08]	$E(\mathbb{F}_{3^{239}})$	Intel Pentium D (3.2 GHz) [Java]	43270
[KST+07]	$E(\mathbb{F}_{3^{239}})$	AMD Opteron 275 (2.2 GHz)	10753
[IST08]	$E(\mathbb{F}_{3^{239}})$	Intel Core 2 Duo (1.86 GHz)	65610
[KAT08]	$E(\mathbb{F}_{3^{239}})$	AMD Opteron 275 (2.2 GHz)	3157
[KTO08]	$E(\mathbb{F}_{3^{313}})$	Intel Pentium D (3.2 GHz) [Java]	71897
[KST+07]	$E(\mathbb{F}_{3^{313}})$	AMD Opteron 275 (2.2 GHz)	21796
[KAT08]	$E(\mathbb{F}_{3^{353}})$	AMD Opteron 275 (2.2 GHz)	8299
[KAT08]	$E(\mathbb{F}_{3^{509}})$	AMD Opteron 275 (2.2 GHz)	16295

表 3.7　η_T ペアリングの実装例 (FPGA)

参照文献	楕円曲線	実行環境	周波数 (MHz)	回路規模 (slice/LE)	実行時間 (μs)
○標数 3					
[RMK+07]	$E(\mathbb{F}_{3^{97}})$	Xilinx xc2vp100	61.6	7036	309
				11635	250
				16290	232
				20943	233
				25626	228
				39553	227
			70.4	4995	294
				7491	203
				10000	178
				12520	178
				15056	173
				22632	172
			84.8	4125	432
				5657	275
				7265	213
				8887	199
				10540	187
				15401	183
			91.2	3610	1170
				4420	659
				5190	454
				6069	391
				7093	325
				9652	268
[J07]	$E(\mathbb{F}_{3^{97}})$	Xilinx xc4vlx200	199	89088	8
[BST+07]	$E(\mathbb{F}_{3^{97}})$	Altera Cyclone II ep2c35	147	18553 LEs	27
			149	14895 LEs	33
[BBD+07]	$E(\mathbb{F}_{3^{97}})$	Xilinx xc2vp4	147	1888	222
[BBD+08b]	$E(\mathbb{F}_{3^{97}})$	Xilinx xc2vp4	145	1833	192

表 3.8　η_T ペアリングの実装例 (スマートカード)

参照文献	楕円曲線	実行環境	周波数 (MHz)	実行時間 (ms)
○標数 2				
[SCA06]	$E(\mathbb{F}_{2^{379}})$	Philips HiPerSmart	9	480
			20.57	220
			36	140

表 3.9　η_T ペアリングの実装例 (組み込み用 CPU)

参照文献	楕円曲線	実行環境	周波数 (MHz)	実行時間 (ms)
○標数 2				
[MST+08]	$E(\mathbb{F}_{2^{239}})$	Atmel ATmega128L	7.3282	1930
[OSL+07]	$E(\mathbb{F}_{2^{271}})$	Atmel ATmega128L	7.3282	5450
○標数 3				
[IST07]	$E(\mathbb{F}_{3^{97}})$	Atmel ATmega128L	7.3828	5789
[IST08]	$E(\mathbb{F}_{3^{97}})$	Atmel ATmega128L	7.37	5800
[YTK+08]	$E(\mathbb{F}_{3^{97}})$	ARM 9	150	56.50
			225	37.52
[SST09]	$E(\mathbb{F}_{3^{97}})$	ルネサステクノロジ SH7730	266	58.13
[IST08]	$E(\mathbb{F}_{3^{167}})$	Atmel ATmega128L	7.37	15300
[YTK+08]	$E(\mathbb{F}_{3^{167}})$	ARM 9	150	337.25
			225	218.27
[IST08]	$E(\mathbb{F}_{3^{193}})$	Atmel ATmega128L	7.37	34600
[YTK+08]	$E(\mathbb{F}_{3^{193}})$	ARM 9	150	401.27
			225	261.88
[IST08]	$E(\mathbb{F}_{3^{239}})$	Atmel ATmega128L	7.37	60200
[YTK+08]	$E(\mathbb{F}_{3^{239}})$	ARM 9	150	738.23
			225	478.54
[YTK+08]	$E(\mathbb{F}_{3^{313}})$	ARM 9	150	1459.65
			225	947.30

表 3.10　η_T ペアリングの実装例 (ASIC)

参照文献	楕円曲線	実行環境	周波数 (MHz)	回路規模 (Gate)	実行時間 (μs)
○標数 3					
[AIO+08]	$E(\mathbb{F}_{3^{97}})$	TSMC CL018G (0.18μm)	200	193765	46.7

アルゴリズム 3.3　Ate ペアリングの計算手順

Input: $P=(x_P,y_P)\in E(\mathbb{F}_q)[n]\cap\mathrm{Ker}(\pi-[1])$, $Q\in E(\mathbb{F}_q)[n]\cap\mathrm{Ker}(\pi-[p])$	
Output: $e_A(P,Q)\in\mu_n$	
(初期設定)	$T\leftarrow Q$, $f\leftarrow 1$
(ループ計算)	for i from $\lceil\log_2(t-1)\rceil-2$ downto 0
	$T\leftarrow 2T$
	$f\leftarrow f^2\cdot\ell_{T,T}(x_P,y_P)$
	if n_i=1 then
	$T\leftarrow T+Q$
	$f\leftarrow f\cdot\ell_{T,Q}(x_P,y_P)$
	end if
	end for
(最終べき計算)	$f\leftarrow f^{(q^\kappa-1)/n}$
(結果出力)	return f

[HSV06].

$E(\mathbb{F}_q)[n]=\{P\in E(\mathbb{F}_q)|nP=\mathcal{O}\}$, $\mu_n=\{x\in\mathbb{F}_{q^\kappa}^\times|x^n=1\}$, π を Frobenius 写像とするとき, ペアリング

$$e_A:E(\mathbb{F}_q)[n]\cap\mathrm{Ker}(\pi-[1])\times E(\mathbb{F}_q)[n]\cap\mathrm{Ker}(\pi-[p])\to\mu_n \tag{3.3}$$

を Ate ペアリング (Ate pairing) と呼ぶ [HSV06]. Ate ペアリングの計算手順をアルゴリズム 3.3 に示す. ここで $t=q+1-\#E(\mathbb{F}_q)$ は楕円曲線のトレースである. また, $\ell_{T,T}$ は楕円曲線 E 上の点 T における接線, $\ell_{T,Q}$ は楕円曲線 E 上の点 T, Q を通る直線を表す.

アルゴリズム 3.1 からわかる通り, Ate ペアリングの計算と Tate ペアリングの計算の類似性は高く, 実際, Tate ペアリング $e_T(P,Q)$ を, n と P に対して定義される関数 $f_{n,P}(X)$ に点 Q を代入したもの (つまり $f_{n,P}(Q)$) と見なすとき, Ate ペアリング $e_A(P,Q)$ は $f_{t-1,Q}(P)$ と表すことができる. 従って $t-1$ が小さくなるような楕円曲線を選択すると, Ate ペアリングは高速な計算が可能となる. 実際, BN 曲線 [BN06] 上で高速計算できることが知られている.

さらなる高速化を目的として, Ate ペアリングを変型した twisted Ate ペアリング [HSV06], Rate ペアリング [LLP08], Cross-twisted Ate (Xate) ペアリング [AKO+08], optimal Ate ペアリング [Ver08] などが提案されている.

3.3.2　Ate ペアリングの実装例

Tate ペアリングの実装例として, PC での実装報告を表 3.11 に, スマートカードでの実装報告を表 3.12 に, 組み込み CPU での実装報告を表 3.13 にまとめる (3.1.2 節で述べた表に対する注意事項を参照のこと).

3.4　MapToPoint 関数

Boneh-Franklin による IBE 方式 (BF 方式, 具体的なアルゴリズムは第 1 章の付録を参照のこと) などでは, 与えられた ID から巡回群 $\mathbb{G}_1$ へのハッシュ関数 (MapToPoint 関数) が必要となる. 本節では具体的な MapToPoint 関数の計算アルゴリズムを示す.

以下, Tate ペアリングを用いた BF 方式における MapToPoint 関数の 2 種類の構成法を述べる [BF01].

表 3.11　Ate ペアリングの実装例 (PC)

参照文献	楕円曲線	実行環境	実行時間 (μs)
○標数 p			
[SKN+08] [NAS+08]	$E(\mathbb{F}_{p_{254}})$ (BN 曲線, $\kappa = 12$)	Intel Pentium 4 (3.0 GHz)	31600
[SCA06]	$E(\mathbb{F}_{p_{256}})$ (通常曲線, $\kappa = 4$)	Intel Pentium 4 (3.0 GHz)	3160
[S07]	$E(\mathbb{F}_{p_{256}})$ (FST 曲線, $\kappa = 4$)	Intel Pentium 4 (3.0 GHz), 前計算なし	9100
		Intel Pentium 4 (3.0 GHz), 前計算あり	3100
[DSD07]	$E(\mathbb{F}_{p_{256}})$ (BN 曲線, $\kappa = 12$)	Intel Pentium 4 (3.4 GHz)	39300

表 3.12　Ate ペアリングの実装例 (スマートカード)

引用文献	楕円曲線	実行環境	周波数 (MHz)	実行時間 (ms)
○標数 p				
[SCA06]	$E(\mathbb{F}_{p_{256}})$ (通常曲線, $\kappa = 4$)	Philips HiPerSmart	9	1210
			20.57	590
			36	380
[DSD07]	$E(\mathbb{F}_{p_{256}})$ (BN 曲線, $\kappa = 12$)	Philips HiPerSmart	9	16880
			20.57	8470

表 3.13　Ate ペアリングの実装例 (組み込み用 CPU)

引用文献	楕円曲線	実行環境	周波数 (MHz)	実行時間 (ms)
○標数 p				
[SOS+08]	$E(\mathbb{F}_{p_{256}})$ (通常曲線, $\kappa = 4$)	TI MSP430	8.192	11820
[YKF+09]	$E(\mathbb{F}_{p_{256}})$ (通常曲線, $\kappa = 4$)	ARM 9	150	1068.88
			225	696.69

3.4.1　**例 1**

$p \equiv 11 \pmod{12}$ を満たす素数 p に対し, 有限体 $\mathbb{F}_p$ 上の楕円曲線として超楕円曲線 $E : y^2 = x^3 + 1$ を選ぶ. また, n を位数 $\#E(\mathbb{F}_p) = p + 1$ の適当な素因数とする. このとき, 任意のビット列 ID $\in \{0,1\}^*$ から巡回群 $\mathbb{G}_1 = E(\mathbb{F}_p)[n]$ へのハッシュ関数 $H_1 : \{0,1\}^* \to \mathbb{G}_1$ は以下の手順によって求められる.

まず, 適当なハッシュ関数 $H : \{0,1\}^* \to \{0,1\}^\ell$ を用いて, ID を ℓ ビットのビット列 $H(\mathrm{ID})$ に変換し, さらにビッ

ト列 $H(\mathrm{ID})$ を整数と同一視してから p で割った余り y を求める．ここで

$$x = (y^2 - 1)^{1/3} \pmod{p} \tag{3.4}$$

とすると，点 $P = (x, y)$ は楕円曲線 $E(\mathbb{F}_p)$ 上の点となるので，$P_{\mathrm{ID}} = \frac{p+1}{n} P \in E(\mathbb{F}_p)[n]$ となる．この点 P_{ID} を ID のハッシュ値，すなわち $H_1(\mathrm{ID}) = P_{\mathrm{ID}} \in \mathbb{G}_1$ と定める．

ここで式 (3.5) の計算に 3 乗根が必要となるが，$p \equiv 11 \pmod{12}$ であることから，$\alpha^{1/3} \equiv \alpha^{(2p-1)/3} \pmod{p}$ となり，3 乗根計算をべき乗計算に置き換えることができる．

3.4.2 例 2

$p \equiv 11 \pmod{12}$ を満たす素数 p に対し，有限体 $\mathbb{F}_p$ 上の楕円曲線として超楕円曲線 $E : y^2 = x^3 + x$ を選ぶ．また，n を位数 $\#E(\mathbb{F}_p) = p + 1$ の適当な素因数とする．このとき，任意のビット列 $\mathrm{ID} \in \{0,1\}^*$ から巡回群 $\mathbb{G}_1 = E(\mathbb{F}_p)[n]$ へのハッシュ関数 $H_1 : \{0,1\}^* \to \mathbb{G}_1$ は以下の手順によって求められる．

まず，適当なハッシュ関数 $H : \{0,1\}^* \to \{0,1\}^\ell$ を用いて，ID を ℓ ビットのビット列 $H(\mathrm{ID})$ に変換し，さらにビット列 $H(\mathrm{ID})$ を整数と同一視してから p で割った余り x を求める．ここで

$$y = (x^3 + x)^{1/2} \pmod{p} \tag{3.5}$$

とすると，点 $P = (x, y)$ は楕円曲線 $E(\mathbb{F}_p)$ 上の点となるので，$P_{\mathrm{ID}} = \frac{p+1}{n} P \in E(\mathbb{F}_p)[n]$ となる．この点 P_{ID} を ID のハッシュ値，すなわち $H_1(\mathrm{ID}) = P_{\mathrm{ID}} \in \mathbb{G}_1$ と定める．

ここで式 (3.5) の計算に平方根が必要となるが，$p \equiv 11 \pmod{12}$ であることから，$\alpha^{1/2} \equiv \alpha^{(p+1)/4} \pmod{p}$ となり，平方根計算をべき乗計算に置き換えることができる．

第 3 章の参照文献

[AIO+08] Vithanage Ananda, 猪俣 敦夫, 岡本 栄司, 岡本 健, 金岡 晃, 上遠野 昌良, 志賀 隆明, 白勢 政明, 曽我 竜司, 高木 剛, 土井 洋, 藤田 香, Beuchat, J., 満保 雅浩, 山本 博康, “ペアリング演算 ASIC の開発”, 情報処理学会コンピュータセキュリティ (CSEC) 研究会, 2008-CSEC-41-(6), 2008.

[AON+06] 赤根 正剛, 沖本 卓求弥, 野上 保之, 森川 良孝, “All One Polynomial Field を用いた MNT 曲線に対する Pairing 計算の実装”, 電子情報通信学会情報セキュリティ (ISEC) 研究会, ISEC2006-11, 2006.

[AKO+08] 赤根 正剛, 加藤 英洋, 沖本 卓求弥, 酒見 由美, 野上 保之, 森川 良孝, “部分体計算を活用する高速な Ate ペアリングの提案”, 2008 年暗号と情報セキュリティシンポジウム (SCIS 2008), 3D1-5, 2008.

[BBD+07] J. Beuchat, N. Brisebarre, J. Detrey, and E. Okamoto, “Arithmetic Operators for Pairing-based Cryptography”, CHES 2007, LNCS 4727, Springer-Verlag, pp.239-255, 2007.

[BBD+08a] J. Beuchat, N. Brisebarre, J. Detrey, E. Okamoto, and F. Rodríguez-Henríquez, “A Comparison between Hardware ccelerators for the Modified Tate Pairing over $\mathbb{F}_{2^m}$ and $\mathbb{F}_{3^m}$”, Pairing 2008, LNCS 5209, Springer-Verlag, pp.178-191, 2008.

[BBD+08b] J. 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, no.11, 2008.

[BF01] D. Boneh and F. Franklin, “Identity-based encryption from the Weil pairing”, CRYPTO 2001, LNCS 2139, Springer-Verlag, pp.213-229, 2001.

[BGO+05] P. Barreto, S. Galbraith, C. O’hEigeartaigh, and M. Scott, ”Efficient Pairing Computation on Supersingular Abelian Varieties”, Designs, Codes, and Cryptography, vol.42, pp.239-271, 2005.

[BKL+02] P. Barreto, H. Kim, B. Lynn, and M. Scott, “Efficient Algorithms for Pairing-based Cryptosystems”, CRYPTO 2002, LNCS 2442, Springer-Verlag, pp.354-368, 2002.

[BN06] P. Barreto and M. Naehrig, “Pairing-friendly Elliptic Curves of Prime Order”, SAC 2005, LNCS 3897, Springer-Verlag, pp.319-331, 2006.

[BSS05] I. Blake, G. Seoussi, and N. Smart (Eds), Advances in Elliptic Curve Cryptography, Cambridge Univercity Press, 2005.

[BST+07] J. 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 Symposium on Computer Arithmetic, pp.97-104, 2007.

[DL03] I. Duusma and H. Lee, “Tate Pairing Implementation for Hyperelliptic Curves $y^2 = x^p - x + d$”, ASIACRYPT 2003, LNCS 2894, Springer-Verlag, pp.111-123, 2003.

[DSD07] A. Devegili, M. Scott, and R. Dahab, “Implementing Cryptographic Pairings over Barreto-Naehrig

Curves", Pairing 2007, LNCS 4575, Springer-Verlag, pp.197-207, 2007.

[GP05] P. Grabher and D. Page, "Hardware Acceleration of the Tate Pairing in Characteristic Three", CHES 2005, LNCS 3659, Springer-Verlag, pp.398-411, 2005.

[HMS08] D. Hankerson, A. Menezes, and M. Scott, "Software Implementation of Pairings", CACR Technical Report, CACR 2008-8, University of Waterloo, 2008. (Available at http://www.cacr.math.uwaterloo.ca/techreports/2008/cacr2008-08.pdf)

[HSV06] F. Hess, N. Smart, and F. Vercauteren, "The Eta Pairing Revisited", IEEE Transactions on Information Theory, vol.52, pp.4595-4602, 2006

[IST07] 石黒 司, 白勢 政明, 高木 剛, "ATmega128L 上でのペアリング暗号の高速実装", コンピュータセキュリティシンポジウム 2007 (CSS 2007), 2D-4, pp.187-192, 2007.

[IST08] 石黒 司, 白勢 政明, 高木 剛, "ATmega128L 上でのペアリング暗号の高速実装", 情報処理学会論文誌, vol.49, no.11, pp.3743-3753, 2008.

[J07] J. Jiang, "Bilinear Pairing (Eta_T Pairing) IP Core (Version 2.0)", Technical report, City-University of Hong Kong, 2007. (Available at http://www.cs.cityu.edu.hk/~ecc/doc/etat_datasheet_v2.pdf)

[KAT08] Y. Kawahara, K. Aoki, and T. Takagi, "Faster Implementation of η_T Pairing over GF(3^m) Using Minimum Number of Logical Instructions for GF(3)-Addition", Pairing 2008, LNCS 5209, Springer-Verlag, pp.178-191, 2008.

[KKC+06] M. Keller, T. Kerins, F. Crowe, and W. Marnane, "FPGA Implementation of a GF(2^m) Tate Pairing Archtechture", ARC 2006, LNCS 3985, Springer-Verlag, pp.358-369, 2006.

[KMP+05] T. Kerins, W. Marnane, E. Popovici, and P. Barreto, "Efficient Hardware for the Tate Pairing Calculation in Characteristic Three", CHES 2005, LNCS 3659, Springer-Verlag, pp.412-426, 2005.

[KRM+07] M. Keller, R. Ronan, W. Marnane, and C. Murphy, "Hardware Archtecture for the Tate Pairing over GF(2^m)", Computers and Electrical Engineering, vol.33 (5-6), pp.392-406, 2007.

[KST+07] 川原 祐人, 白勢 政明, 高木 剛, 岡本 栄司, "η_T ペアリングの高速ソフトウェア実装", 2008 年暗号と情報セキュリティシンポジウム (SCIS 2008), 2E3-2, 2008.

[KTO06] 川原 祐人, 岡本 栄司, 高木 剛, "Java を利用した携帯電話上での Tate ペアリングの高速実装", コンピュータセキュリティシンポジウム 2006 (CSS 2006), 9A-1, pp.591-596, 2006.

[KTO08] 川原 祐人, 岡本 栄司, 高木 剛, "Java を利用した携帯電話上での Tate ペアリングの高速実装", 情報処理学会論文誌, vol.49, no.1, pp.427-435, 2008.

[LLP08] E. Lee, H. Lee, and C. Park, "Efficient and Generalized Pairing Computation on Abelian Variety", IACR ePrint Archive, Report 2008/040, 2008. (Available at http://eprint.iacr.org/2008/040)

[M86] V. Miller, "Short Programs for Functions on Curves", unpublished manuscript, 1986. (Available at http://crypto.stanford.edu/miller/miller.pdf)

[M09] S. Mitsunari, "A Fast Implementation of η_T Pairing in Characteristic Three on Intel Core 2 Duo Processor", IACR ePrint Archive, Report 2009/032, 2009. (Available at http://eprint.iacr.org/2009/032)

[MNT01] A. Miyaji, M. Nakabayashi, and S. Takano, "New Explicit Conditions of Elliptic Curve Traces for FR-reduction", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, vol.E84-A, no.5, pp.1234-1243, 2001.

[MOV93] A. Menezes, T. Okamoto, and S. Vanstone, "Reducing Elliptic Curve Logarithms to Logarithmes in a Finite Field", IEEE Transactions on Information Theory, vol.39, no.5, pp.1639–1646, 1993.

[MST+08] 宮崎 行規, 白勢 政明, 高木 剛, Dong-Guk Han, Dooho Choi, “MICAz 上での高速ペアリング暗号実装”, コンピュータセキュリティシンポジウム 2008 (CSS 2008), D2-4, pp.199-204, 2008.

[NAS+08] Y. Nogami, M. Akane, Y. Sakemi, H. Kato, and Y. Morikawa, “Integer Variable χ-based Ate Pairing”, Pairing 2008, LNCS 5209, Springer-Verlag, pp.178-191, 2008

[OAM+07] L. Oliveira, D. Aranha, E. Morais, F. Daguano, J. López, and R. Dahab, “TinyTate: Computing the Tate Pairing in Resorce-constrained Sensor Nodes”, NCA 2007, pp.318-323, IEEE, 2007.

[OSL+07] L. Oliveira, M. Scott, J. López, and R. Dahab, “TinyPBC: Pairings for Authenticated Identity-based Non-interactive Key Distribution in Sensor Networks”, IACR ePrint Archive, Report 2007/482, 2007. (Available at http://eprint.iacr.org/2007/482)

[RMK+07] R. Ronan, C. Murphy, T., Kerins, C. ÓhÉigeartaigh, and P. Barreto, “A Flexible Processor for the Characteristic 3 η_T Pairing”, International Journal of High Performance Systems Architecture, vol.1, issue 2, pp.79-88, 2007.

[ROM+06] R. Ronan, C. ÓhÉigeartaigh, C. Murphy, M. Scott, and T. Kerins, “FPGA Acceleration of the Tate Pairing in Characteristic 2”, FPT 2006, pp.213-220, IEEE, 2006.

[S05] M. Scott, “Faster Pairings Using an Elliptic Curve with an Efficient Endomorphism”, INDOCRYPT 2005, LNCS 3797, Springer-Verlag, pp.258-269, 2005.

[S07] M. Scott, “Implementing Cryptographic Pairings”, Pairing 2007, LNCS 4575, Springer-Verlag, pp.177-196, 2007.

[SCA06] M. Scott, N. Costigan, and W. Abdulwahab, “Implementing Cryptographic Pairings on Smartcards”, CHES 2006, LNCS 4249, Soringer-Verlag, pp.134-147, 2006.

[SKG06] C. Shu, S. Kwon, and K. Gaj, “FPGA Accelerated Tate Pairing Based Cryptosystems over Binary Fields”, FPT 2006, pp.173-180, IEEE, 2006.

[SKN+08] 酒見 由美, 加藤 英洋, 野上 保之, 森川 良孝, “整数変数 χ を用いて改良したクロスツイスト Ate ペアリング”, コンピュータセキュリティシンポジウム 2008 (CSS 2008), D1-4, pp.97-102, 2008.

[SKT+07] M. Shirase, Y. Kawahara, T. Takagi, and E. Okamoto, “Universal η_T Pairing Algorithm over Arbitrary Extension Degree”, WISA 2007, LNCS 4867, Springer-Verlag, pp.1-15, 2007.

[SOS+08] C. Szczechowaiak, L. Oliveria, M. Scott, M. Collier, and R. Dahab, “NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor Networks”, EWSN 2008, LNCS 4913, Springer-Verlag, pp.305-320, 2008.

[SST09] 佐々木 勇太, 白勢 政明, 高木 剛, “η_T ペアリングに対するファンデルモンド行列を用いた高速乗算法”, 2009 年暗号と情報セキュリティシンポジウム (SCIS 2009), 3C3-2, 2009.

[STO07] 白勢 政明, 高木 剛, 岡本 栄司, “任意の拡大次数において計算可能な η_T ペアリング”, 電子情報通信学会情報セキュリティ (ISEC) 研究会, ISEC2006-131, 2007.

[Ver08] F. Vercauteren, “Optimal Pairings”, IACR ePrint Archive, Report 2008/096, 2008. (Available at http://eprint.iacr.org/2008/096)

[YKF+09] 吉富 基, 清本 晋作, 福島 和英, 田中 俊明, 高木 剛, “BREW 携帯電話における通常楕円曲線上のペアリングの実装”, 2009 年暗号と情報セキュリティシンポジウム (SCIS 2009), 3C2-2, 2009.

[YTK+06] 吉富 基, 高木 剛, 清本 晋作, 田中 俊明, “BREW 携帯電話でのペアリング暗号の高速実装”, 情報処理学会コンピュータセキュリティ (CSEC) 研究会, 2006-CSEC-35, 2006.

[YTK+08] M. Yoshitomi, T. Takagi, S. Kiyomoto, and T. Tanaka, “Efficient Implementation of the Pairing on

Mobilephones using BREW", IEICE Transactions on Information and Systems, vol.E91-D, no.5, pp.1330-1337, 2008.

[ZKO08] 張 一凡, 金山 直樹, 岡本 栄司, "$\mathbb{F}_{2^m}$ 上の楕円曲線ペアリングの Java 実装", コンピュータセキュリティシンポジウム 2008 (CSS 2008), D2-1, pp.181-186, 2008.

第 4 章

国際会議動向と標準化動向

4.1 国際会議動向

4.1.1 ペアリング関連の論文投稿数

暗号技術に関する重要な学会の一つに IACR(International Association for Cryptologic Research, 米国) がある．IACR は現在，CRYPTO, Eurocrypt, Asiacrypt という 3 つの国際会議を運営している．表 4.1 は，これら国際会議の中で，ペアリング関連の投稿論文を調べたものである．それぞれの会議をグラフにしたものを図 4.1〜図 4.3 に，3 つの国際会議をまとめてグラフにしたものを図 4.4 に示す．また IACR はインターネットを活用した電子出版を運営しており，このアーカイブは Cryptology ePrint Archive [IACR] と呼ばれる．この中からペアリング関連の論文について調べたものが表 4.2 である．これをグラフにしたものを図 4.5 に示す．

表 4.1 について，国際会議の種類によりペアリング関連の論文掲載数にばらつきがあるが，これは各々の国際会議におけるプログラム委員の意向が反映されていると考えられる．一方，3 つの会議を合わせた各年の掲載論文 (表 4.1 の

表 4.1　IACR の国際会議におけるペアリング関連論文数の推移

		2002 年	2003 年	2004 年	2005 年	2006 年	2007 年	2008 年
EUROCRYPT	論文数	35	39	36	33	35	33	31
	ペアリング関連論文数	1	4	9	9	6	5	4
	比率 (%)	2.8	10.2	25.0	27.2	17.1	15.2	12.9
ASIACRYPT	論文数	36	33	37	37	31	33	33
	ペアリング関連論文数	2	7	3	8	4	4	6
	比率 (%)	5.5	21.2	8.1	21.6	12.9	12.1	18.2
CRYPTO	論文数	39	36	34	33	36	33	32
	ペアリング関連論文数	3	3	5	6	8	3	1
	比率 (%)	7.6	8.3	14.7	18.1	22.2	9.1	3.1
合計	論文数	110	108	107	103	102	99	96
	ペアリング関連論文数	6	14	17	23	18	12	11
	比率 (%)	5.5	13.0	15.9	22.3	17.6	12.1	11.5

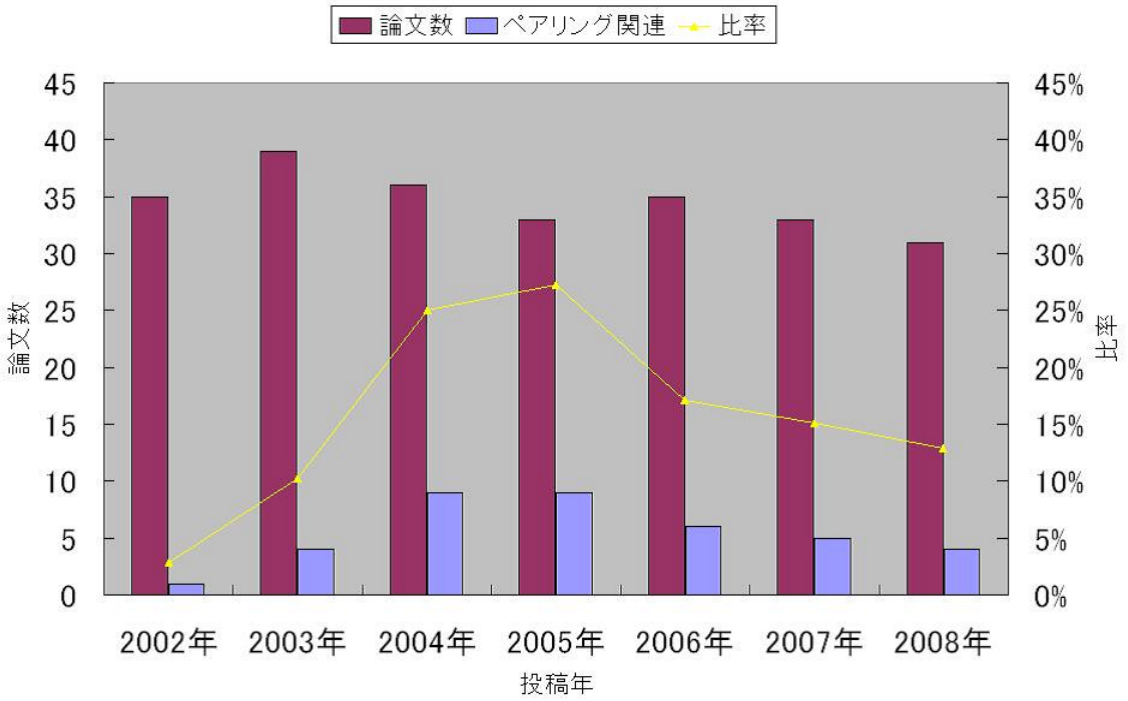

図 4.1　EUROCRYPT におけるペアリング関連論文数の推移グラフ

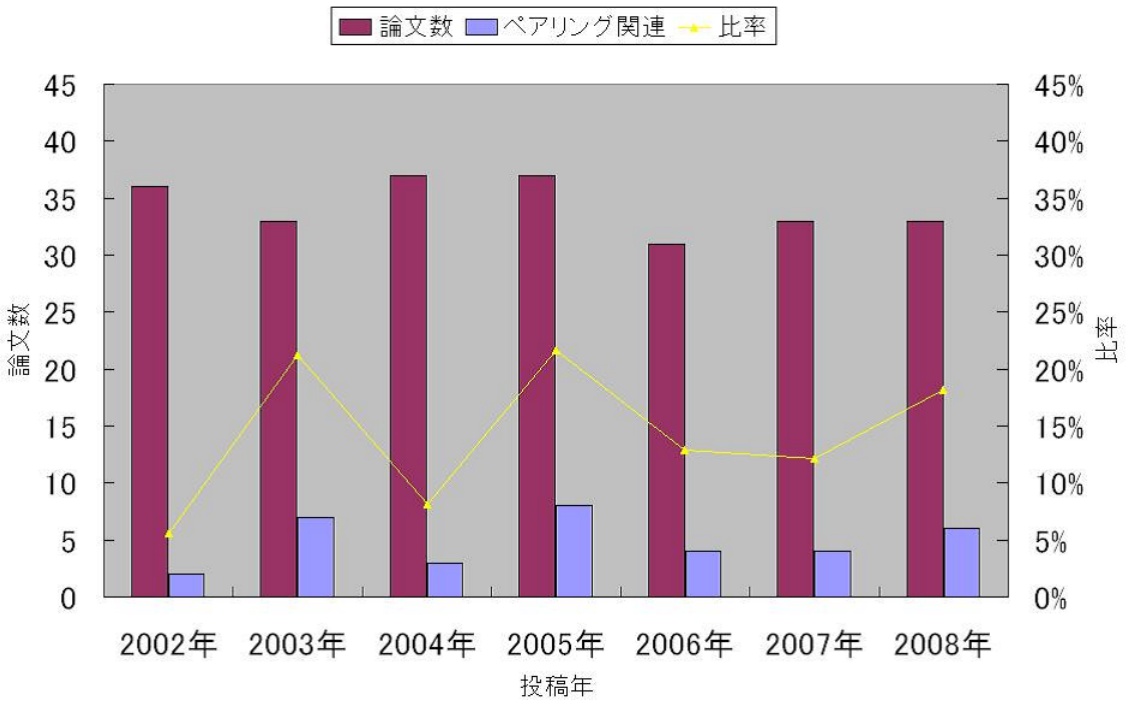

図 4.2　ASIACRYPT におけるペアリング関連論文数の推移グラフ

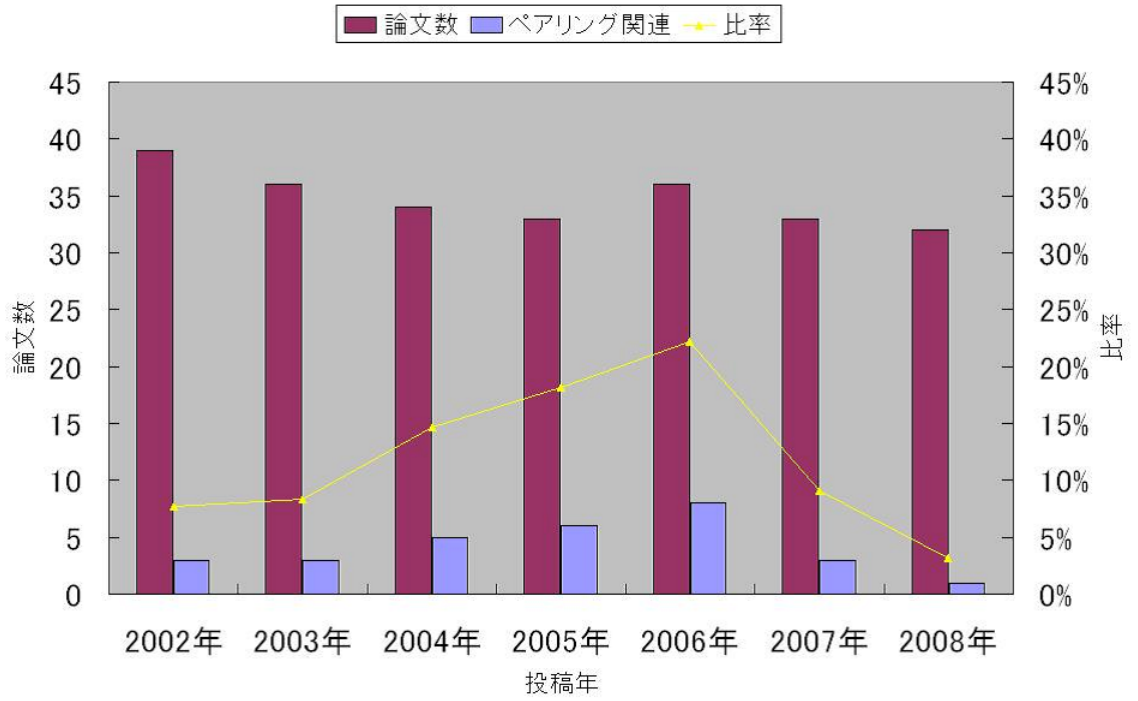

図 4.3　CRYPTO におけるペアリング関連論文数の推移グラフ

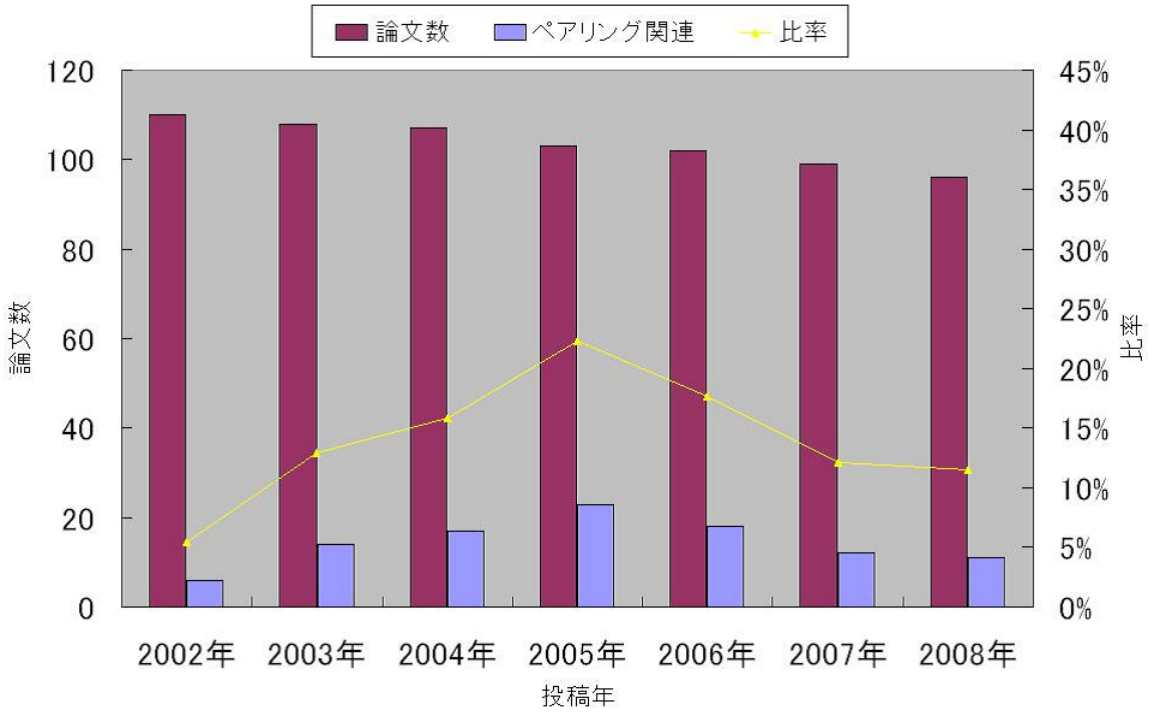

図 4.4　IACR の国際会議におけるペアリング関連論文数の推移グラフ

表 4.2　IACR ePrint Archive におけるペアリング関連論文数の推移

	2002 年	2003 年	2004 年	2005 年	2006 年	2007 年	2008 年
論文数	195	265	377	469	486	482	545
ペアリング関連論文数	13	38	65	97	113	127	124
比率 (%)	6.7	14.3	17.2	20.7	23.3	26.3	22.8

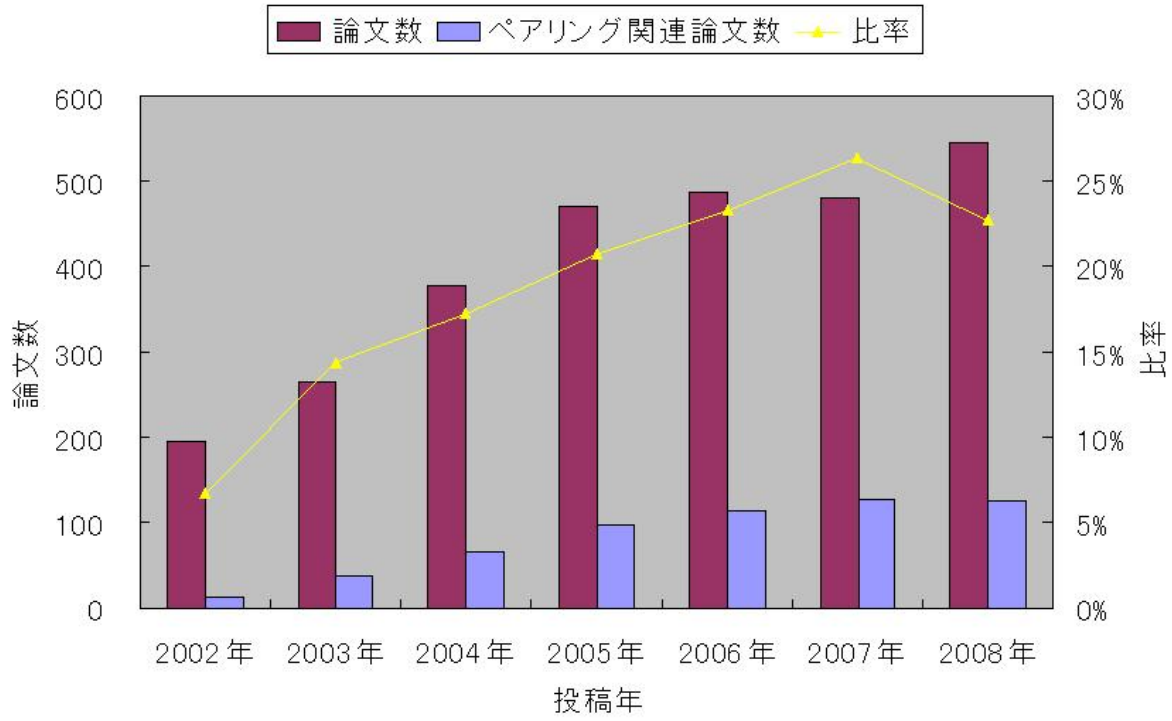

図 4.5　IACR ePrint Archive におけるペアリング関連論文数の推移グラフ

最下行) を見ると，2005 年に最も高い掲載比率を示しており，その後安定の方向に向かっている．また，Cryptology ePrint Archive については，表 4.2 より， 2007 年の比率が最も高いことがわかる．

これらの論文で取り上げているテーマは，以下のような 2 つのグループに分類できる．

- 基本技術 (暗号プリミティブ)：主にペアリング計算の高速化等，アルゴリズムの改良を目的とする．例として，ペアリング演算手法 (Tate, Weil, Ate)，ペアリング関数の効率的な実装方法，等があげられる．
- 応用技術 (暗号アプリケーション)：主に暗号プロトコルの提案．例として，IBE 方式，IBS 方式，暗号方式，署名方式 (Short Signature を含む)，パスワード管理，ディレクトリ管理，ネットワーク，Web サービス，PKI システムへの適用，等がある．

4.1.2 国際会議とワークショップ

現在，暗号や情報セキュリティに関する多くの国際会議やワークショップが開催されており，これらの中にペアリングに関する論文が数多く掲載されている．また，最近はペアリング技術に特化した会議も増加している．ここでは，これらの特徴的な会議について述べる．

■ECC ワークショップ (Workshop on Elliptic Curve Cryptography)　楕円曲線暗号とそれに関連したワークショップ [ECC]．主に楕円曲線暗号に関するテーマを扱っているが，これまでに電子投票，量子力学，AES, ハッシュ関数など，開催時期に話題となっているテーマについて取り上げることもある．毎回複数の研究者を招いて講演会を開き，参加者と議論を行うことで会議が進められる．第 1 回目のワークショップは，1997 年にカナダのトロントで開催された．また，第 13 回目となる 2009 年は，カナダのカルガリーで開催される予定．

■NIST ワークショップ (Identity Based Encryption Workshop)　米国の国立標準技術研究所 (NIST) が開催した IBE に関するワークショップ [NIST-IBE]．このワークショップは，IBE の発展を促すために，基礎と応用の研究を推し進めることを目的としている．第 1 回目は，2008 年 6 月に NIST の本部 (米国メリーランド州) で開催され，公募による暗号技術の発表とパネルディスカッションという形式で行った．2 回目以降の開催については，2009 年 3 月現在アナウンスされていない．

■ペアリング国際会議 (International Conference on Pairing-based Cryptography)　ペアリングを用いた暗号に関する国際会議 [Pairing]．ペアリングの基礎から応用まで幅広いテーマを取り上げている．2007 年から毎年開催されており，Pairing 2007(プログラム委員: 岡本龍明, 高木剛) は東京の一橋記念講堂，Pairing 2008(プログラム委員: Steven Galbraith, Kenny Paterson) はイギリスのロンドン大学ロイヤル・ホロウェイ校にて開催された．Pairing 2009(プログラム委員: Hovav Shacham, Brent Waters) は，アメリカのスタンフォード大学にて開催を予定している．予稿集は，いずれも Springer LNCS から出版されている (Pairing 2009 については出版予定)．

4.2 標準化動向

本節では，今後 CRYPTREC で ID ベース技術に基づく方式を扱う場合の参考として，先だって標準化されている事例をまとめる．

現在，ID ベース技術に関する標準は，IETF，ISO/IEC，IEEE の 3 つがある．

- IETF
  - draft-ietf-smime-ibearch-09.txt
  - draft-ietf-smime-bfibecms-10.txt
  - RFC5091 （Dec. 2007）
- ISO/IEC
  - ISO/IEC 14888-3 離散対数問題に基づく署名方式
  - ISO/IEC 14888-2 素因数分解問題に基づく署名方式
  - ISO/IEC 11770-3 鍵管理 非対称技術に基づく方式
- IEEE P1363.3

4.2.1 IETF

以下の 3 つのインターネットドラフトおよび RFC が存在する.

- draft-ietf-smime-ibearch-09.txt
  - タイトル: Identity-based Encryption Architecture and Supporting Data Structures
  - 著者: G. Appenzeller, L. Martin, M. Schertler
  - 内容: IBE 全体アーキテクチャ（IBE を利用した暗号の全体構成）を示したドキュメント.
- draft-ietf-smime-bfibecms-10.txt
  - タイトル: Using Boneh-Franklin and Boneh-Boyen identity-based encryption algorithms with the Cryptographic Message Syntax (CMS)
  - 著者: L. Martin, M. Schertler
  - 内容: Cryptographic Message Syntax (CMS:暗号メッセージ構文) での暗号化のために Boneh-Franklin IBE[BF01] および Boneh-Boyen IBE[BB04a] を使う規定を定義する.
- RFC5091 （Dec. 2007）(ドラフトの時点では draft-martin-ibcs-05.txt)
  - タイトル: Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems
  - Boneh-Franklin IBE[BF01] および Boneh-Boyen IBE[BB04a] の実装法.

4.2.2 ISO/IEC 14888-3

タイトル: Information technology . Security techniques. Digital signatures with appendix . Part 3: Discrete logarithm based mechanisms

2007 年 08 月 16 日に出版されている.（規格化済）
ISO/IEC 14888-3 は，DLP 問題に基づくメッセージ添付型デジタル署名方式についてのドキュメントであり，7 章「Identity-based mechanisms」で 2 つの IBS 方式が標準化されている.

- 7.1 IBS-1
  This mechanism is based on the algorithm designed by Hess in [H02].
- 7.2 IBS-2
  This mechanism is based on the algorithm designed by Cha and Cheon in [CC02].

4.2.3 ISO/IEC 14888-2

タイトル: Information technology — Security techniques — Digital signatures with appendix — Part 2: Integer factorization based mechanisms

2008 年 04 月 01 日 出版されている.（規格化済）ISO/IEC 14888-2 は，素因数分解問題に基づくメッセージ添付型デジタル署名方式についてのドキュメントであり，7 章「GQ1 scheme3 (identity-based scheme)」で 1 つの IBS 方式

が標準化されている．ただし，ペアリングに基づく方式ではない．

- GQ1 scheme3 (identity-based scheme)
  The GQ1 scheme is due to Guillou and Quisquater [GQ88-1, GQ88-2]. It makes use of zero-knowledge techniques for proving, without revealing, the knowledge of the RSA signature of a sequence of identification data (see also ISO/IEC 9798-5).

4.2.4 ISO/IEC 11770-3

タイトル: Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques

2008 年 7 月 2 日 出版されている．（規格化済）ISO/IEC 11770-3 は，非対称暗号技術に基づく鍵交換方式についてのドキュメントであり，C.2 章で，1 つの ID ベース鍵交換方式が標準化されている．ただし，ペアリングに基づく方式ではない．

- C.2 Identity-based mechanism
  [GP90] is an example of Key agreement Mechanism 1, which is identity-based in the following sense: - the public key of an entity can be retrieved from some combination of its identity and its certificate; - the authenticity of the certificate is not directly verified, but the correct public key can only be recovered from an authentic certificate.

4.2.5 IEEE P1363.3

IEEE P1363.3 は 2006 年から活動を開始し，現在以下のサイトでドラフトおよびサブミットされたドキュメントを公開している．
http://grouper.ieee.org/groups/1363/IBC/index.html
以下の方式がサブミットされているが，現在ドラフトを作成中なので，方式については増減の可能性がある．

- The BF Identity-based encryption system, X. Boyen, Submitted 2006-08-14.
- The BB1 Identity-based cryptosystem: A standard for Encryption and Key Encapsulation, X. Boyen, Submitted 2006-08-14.
- IEEE P1363.3 submission: Pairing-Friendly Elliptic Curves of Prime Order with Embedding Degree 12, P. Barreto, M. Naehrig, Submitted 2006-08-14.
- Efficient and secure identity-based signatures and signcryption from bilinear maps, P. Barreto, B. Libert, N. McCullagh, J-J. Quisquater, Submitted 2006-08-14.
- Proposal for P1363.3: HIBE, HIBS, IBKIE, NTT DoCoMo, Submitted 2006-08-14.
  - C.Gentry, A.Silverberg, Hierarchical ID-Based Cryptography, Presented at AsiaCrypt 2002.
  - Y.Hanaoka, G.Hanaoka, J.Shikata, H.Imai, Identity-Based Hierarchical Strongly Key-Insulated Encryption and Its Application, Presented at Asiacrypt 2005.
  - P. Yang, T. Kitagawa, G. Hanaoka, R. Zhang, K. Matsuura, H. Imai, Applying Fujisaki-Okamoto

to Identity-Based Encryption, Presented at 16th Applied Algebra, Algebraic Algorithms, and Error Correcting Codes, 2006.
  - August 2006 meeting presentation, Submitted 2006-08-14.
- Proposal for P1363.3: Proxy Re-encryption, NTT Data. August 2006 meeting presentation, Submitted 2006-08-14.
- Identity-based Key Agreement Protocols from Pairings, L. Chen, Z. Cheng, N. P. Smart, Submitted 2006-07-03.
- SK-KEM: An Identity-Based KEM, M. Barbosa, L. Chen, Z. Cheng, M. Chimley, A. Dent, P. Farshim, K. Harrison, J. Malone-Lee, N. P. Smart, F. Vercauteren, Submitted 2006-06-07.
- Implicitly Authenticated ID-Based Key Agreement Protocol, Yongge Wang, Submitted 2006-03-22.

4.2.6 まとめ

IETF では Voltage 社が BF 方式 [BF01]，BB1 方式 [BB04a] のドキュメントを S/MIME WG に提案している．5.1 節に示すように，既にこの標準に基づく製品が販売されている．

現時点では，ISO における ID ベース技術の標準は署名，鍵交換技術の一種として記載されているのみであり，ID ベース技術に焦点を当てたドキュメントは存在しない．また，3 つのうち 14888-2, 11770-3 の 2 つはペアリング技術に基づかない 2000 年以前の方式によるものである．ID ベース技術による方式の標準化は，これから本格化すると考えられる．

IEEE P1363.3 では BF 方式，BB1 方式を含む多数の方式が提案されている．まだドラフトの段階であるが，今後の他の ID ベース技術の標準化でも IEEE P1363.3 を参考にする可能性がある．

第 4 章の参照文献

[BF01] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” CRYPTO 2001, LNCS 2139, Springer Verlag, pp. 213–229, 2001.

[BB04a] D. Boneh and X. Boyen, “Efficient selective-ID secure identity based encryption without random oracles,” EUROCRYPT 2004, LNCS 3027, Springer-Verlag, pp. 223–238, 2004.

[ECC] Workshop on Elliptic Curve Cryptography (ECC). Available from `http://www.eccworkshop.org/`

[H02] F. Hess, “Efficient identity based signature schemes based on pairings,” SAC 2002, LNCS 2595, Springer-Verlag, pp.310–324, 2003.

[CC02] J. C. Cha and J. H. Cheon, “An identity-based signature from gap Diffie-Hellman groups,” PKC 2002, LNCS 2567, Springer-Verlag, pp. 18–30, 2002.

[GQ88-1] L. C. Guillou and J.-J. Quisquater, “A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory,” EUROCRYPT ’88, LNCS 330, Springer-Verlag, pp. 123–128, 1988.

[GQ88-2] L. C. Guillou and J.-J. Quisquater, “A paradoxical identity-based signature scheme resulting from zeroknowledge,” CRYPTO ’88, LNCS 403, Berlin, Springer-Verlag, pp. 216–231, 1988.

[GP90] M. Girault, J. C. Pailles, “An identity-based Scheme providing zero-knowledge authentication and authenticated key exchange”, ESORICS 90, pp. 173–184, 1990.

[IACR] International Association for Cryptologic Research, Cryptology ePrint Archive. Available from `http://eprint.iacr.org/`

[NIST-IBE] Applications of Pairing-Based Cryptography: Identity-Based Encryption and Beyond. Available from `http://csrc.nist.gov/groups/ST/IBE/index.html`

[Pairing] International Conference on Pairing-based Cryptography. Available from `http://www.pairing-conference.org/`

第 5 章

製品動向と知的財産権動向

5.1 製品動向

本節では，ID ベース技術の実際の応用例や普及度に関する情報の一環として，製品のリスト，および製品の概略，入手方法などを示す．

以下に示す 16 製品が発売または発表されている．

項番 1〜14 は BF 方式 [BF01] および BB1 方式 [BB04a] に基づく製品である．項番 15 は SK-KEM 方式 [SK-KEM] に基づく製品である．項番 16 はペアリング装置であるため，どの IBE 方式にも使うことができる．

1. Voltage Secure Mail
   - 企業名: Voltage
   - 概略: IBE 暗号メール .
   - 参照先: http://www.voltage.com/products/securemail.htm
2. Voltage SecureMail Gateway
   - 企業名: Voltage
   - 概略: Voltage Secure Mail の IBE 関連製品（機能）．ネットワークのエッジに配置する機能．IBE によるデータの保護，アーカイブ，アンチスパム，アンチウイルスの機能を提供．
   - 参照先: http://www.voltage.com/products/securemail_gateway.htm
3. Voltage Zero Download Messenger (ZDM)
   - 企業名: Voltage
   - 概略: Voltage Secure Mail の IBE 関連製品（機能）．Web 経由の暗号メッセージダウンロード．
   - 参照先: http://www.voltage.com/products/zdm.htm
4. Voltage SecureMail Client
   - 企業名: Voltage
   - 概略: Voltage Secure Mail の IBE 関連製品（機能）．Voltate Secure Mail および ZDM 対応のクライアント機能．
   - 参照先: http://www.voltage.com/products/client.htm
5. Voltage Anti-Phishing
   - 企業名: Voltage
   - 概略: Voltage Secure Mail の IBE 関連製品（機能）．フィッシング対策機能．

- 参照先: http://www.voltage.com/products/anti_phishing.htm

6. Voltage SecureMail Archive Connector for Symantec Enterprise Vault
   - 企業名: Voltage
   - 概略: Voltage Voltage Secure　Mail の IBE 関連製品（機能）．暗号メールのアーカイブ．
   - 参照先: http://www.voltage.com/products/connector.htm
7. Voltage Secure Mail, Voltage IBE Gateway Server
   - 企業名: 三井物産セキュアディレクション
   - 概略: Voltage Secure　Mail の日本総合代理店
   - 参照先: http://www.mbsd.jp/
   - 備考: 2007 年頃までは製品情報を公開していたが，現在は製品情報が公開されていない．
8. Voltage Secure Mail
   - 企業名: さくら情報システム
   - 概略: 三菱物産セキュアディレクションと連携し Voltage Secure Mail を販売
   - 参照先: http://www.sakura-is.co.jp/solutions/category/product/pdf/secu002.pdf
9. Voltage Secure Mail Gateway
   - 企業名: キャノン IT ソリューションズ
   - 概要: 電子メールフィルタリング製品「GURDIANWALL」を Voltage Secure Mail と連動
   - 参照先: http://canon-its.jp/product/vt/index.html
   - 備考: 2008/12/19 に新バージョンを発売開始し，6 億円の売り上げを見込んでいる．http://www.canon-its.co.jp/company/news/20081219vt.html
10. Proofpoint Secure Messaging
    - 企業名: 日本プルーフポイント
    - 概要: Proofpoint Messaging Security Gateway アプライアンス，バーチャルアプライアンス，Proofpoint Protection Server?ソフトウェアの暗号モジュール．Voltage IBE を利用
    - 参照先: http://www.proofpoint.com/jp/products/module.html
11. Exchange Hosted Encryption
    - 企業名: マイクロソフト
    - 概要: Microsoft Exchange に Voltage Secure Mail を連動
    - 参照先: http://canon-its.jp/product/vt/vt_camp.html
12. OCN 暗号メール
    - 企業名: NTT コミュニケーションズ
    - 概要: OCN の暗号メールサービスに Voltage IBE を利用
    - 参照先: http://www.ocn.ne.jp/business/security/encryption/
13. Sentrion MP シリーズ
    - 企業名: sendmail
    - 概要: ポリシーベース暗号機能．Voltage IBE 技術を利用．
    - 参照先: http://sendmail.com/pdfs/resources/DS_encryption_9_07.pdf
14. CI-750, CI-1500
    - 企業名: CODE GREEN NETORKS
    - 概要: ポリシーベースの電子メール自動暗号化機能, Voltage IBE 技術を利用．

- 参照先: http://www.codegreennetworks.jp/technology/email_encryption.html

15. ID ベース暗号関連ニュースリリース
    - 企業名: トレンドマイクロ
    - 概要: ID ベースのメール暗号化技術を擁する英 Identum 社を買収
    - 参照先: http://jp.trendmicro.com/jp/about/news/pr/article/20080305022616.html
16. ペアリング演算用 IC
    - 企業名: FDK 株式会社, 筑波大学, 公立はこだて未来大学情報セキュリティ大学院大学
    - 概要: 世界初となるペアリング演算用のＩＣを開発
    - 参照先: http://www.fdk.co.jp/whatsnew-j/release080415-j.html

5.1.1 まとめ

ID ベース技術の市場規模は詳細は不明であるが，記事 [M08] によれば，「世界で少なくとも 600 万人が使用している」という報告もある．

国内では，資料 [SoucePod08] によれば，暗号化以外の機能を含むメール市場は全体で 590 億円の規模があるとされている．キャノン IT ソリューションズの製品では 6 億円の売り上げを見込んでいることから，そのうち数億円が ID ベースメール暗号製品ということになる．

ID ベース技術が新しい技術であることを考えると，今後の普及について注目するべきである．

また，現時点では ID ベース技術による製品は電子メールに関連するものが多く，そのほとんどが Voltage 社の技術を用いているが，今後は電子メール以外の応用も増えていくと考えられる．

5.2 知的財産権の動向

5.2.1 ペアリング技術の特許出願状況

本節では，まず最初に特許出願状況の全般的動向について説明する．日本特許庁へのペアリング技術に関する特許の出願件数とその累計を表 5.1 に，これをグラフ化したものを図 5.1 に示す．また，特許の上位出願人とその推移を表 5.2 に示す．同様に，米国特許商標庁への出願の場合をそれぞれ，表 5.3，図 5.2，表 5.4 に示す．米国は特許登録するまで出願人を公表しなくてもよいという制度をもつ．このため，一部の特許については，発明者から出願人を推定した．

日本では特許出願して 1 年 6 ヶ月を経過すると，その内容が公開される．米国でも非公開の請求がない場合，出願日より 1 年 6 ヶ月で公開される．よって最近，特許出願されたものについては，これらの表に組み込まれていない．また，日本では特許出願後 3 年以内に審査請求することにより，特許の審査が行われる (2001 年 9 月 30 日以前の出願は 7 年以内)．一方，米国では全ての特許出願が審査される．このため，米国において特許出願されたものの多くは審査中の段階である．

これらの表からわかるように特許の申請時期は日米共に 2001 年以降，急速に増えており，ペアリングは近年注目されている新しい技術であることがわかる．出願件数の累計は，日本では 98 件，米国では 107 件となっており，今後更なる増加が見込まれる．傾向としては，日本，米国のいずれも ID ベースの暗号システムについて出願している場合が多い．

日本特許庁への出願は，NTT および家電メーカ，情報通信メーカが上位を占めている．そして上位 3 出願人は 2004 年以降に出願件数を伸ばしていることがわかる．Voltage 社は出願総数の累計では 4 位であるが，1 特許あたりの特許

表 5.1　日本におけるペアリング技術の特許出願推移

出願年	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008
出願件数	0	0	1	2	4	10	12	15	16	18	20
累計件数	0	0	1	3	7	17	29	44	60	78	98

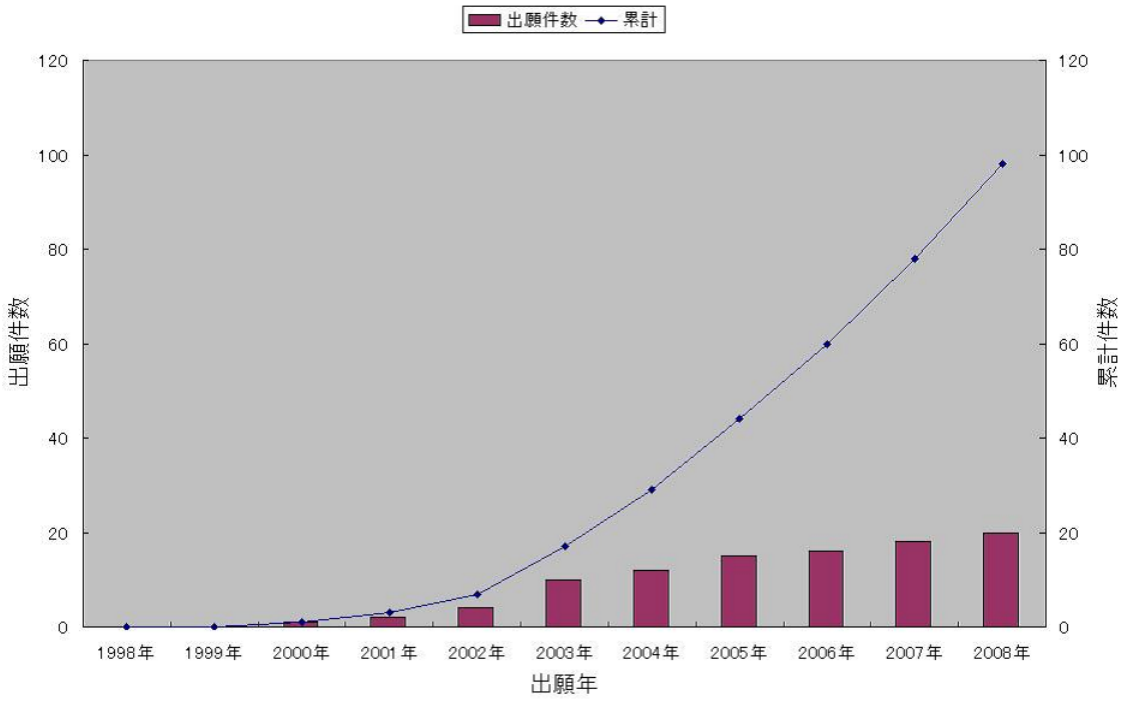

図 5.1　日本におけるペアリング技術の特許出願推移

請求項の数は多い．

一方，米国特許商標庁への出願は，米国企業と日本の NTT DoDoMo が上位を占めている．上位出願人は 2002 年から特許出願を行い，急速に出願件数を増やしている．特に Hewlett-Packard 社は，多くの特許件数をもつが，これは同社の研究者が狭い技術範囲で多くの特許を出願し，発明人になっている．このような傾向は日米に限らず，この分野の共通の傾向であると考えられる．

5.2.2　公開特許に関する調査

日本への特許出願

ペアリング技術を用いない IBE 方式として，岡本 (栄) らは以下のような特許を取得している．これは，RSA 暗号と Diffie-Hellman 鍵共有を組み合わせた方式であり，予備通信を必要とするタイプである．

特許番号：特許 2104721
出願日　：1989 年 5 月 9 日

表 5.2　日本国特許庁における上位出願人 (1997 年～2007 年の出願累計)

出願件数	出願人
14	日本電信電話株式会社
10	株式会社日立製作所
7	ドコモコミュニケーションズ
4	ソニー株式会社
4	ボルテージセキュリティ
4	株式会社エヌ・ティ・ティ・データ
3	エヌ・ティ・ティ・ソフトウェア
3	マイクロソフト
3	高度移動通信セキュリティ技術
3	株式会社東芝
3	村田機械株式会社
2	富士通株式会社
2	学校法人韓国情報通信学園
2	株式会社メビウス
2	日本電気株式会社

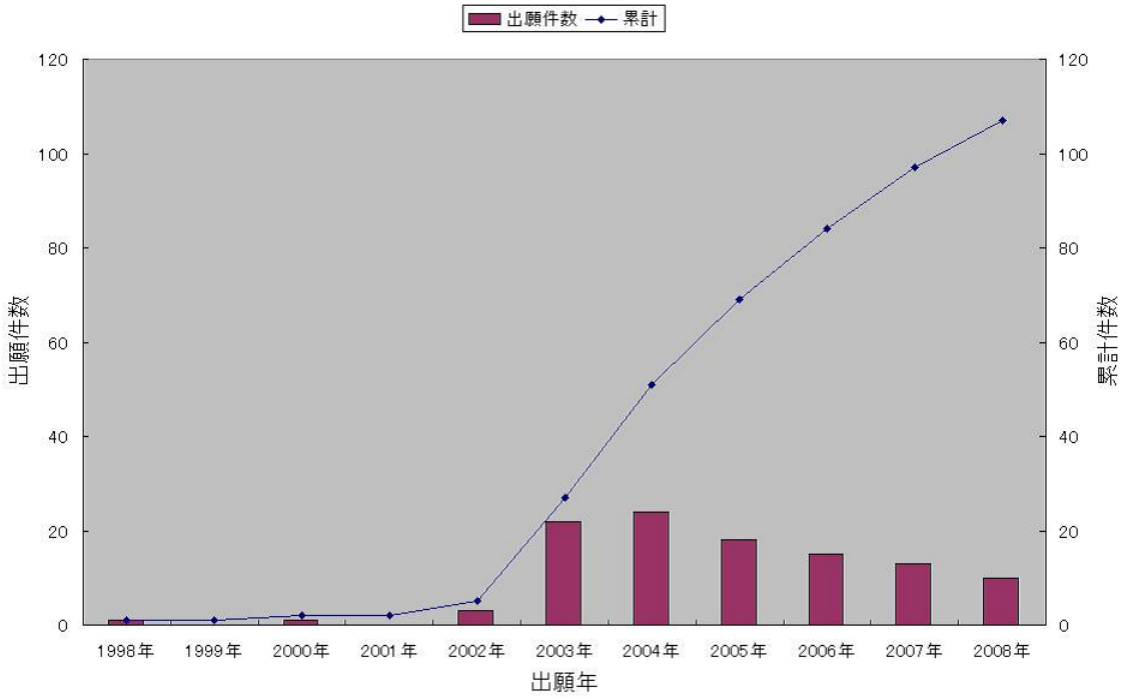

図 5.2　米国におけるペアリング技術の特許出願推移

表 5.3　米国におけるペアリング技術の特許出願推移

出願年	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008
出願件数	1	0	1	0	3	22	24	18	15	13	10
累計件数	1	1	2	2	5	27	51	69	84	97	107

表 5.4　米国特許商標庁における上位出願人 (1999 年〜2007 年の出願累計)

出願件数	出願人
25	Hewlett-Packard Development Company, L.P.
12	NTT Docomo Inc.
11	Microsoft Corporation
9	Voltage Security Inc.
3	Palo Alto Research Center Incorporated
2	The Board of Trustees of the Leland Stanford University
2	Identicrypt, Inc.
1	Citibank, N.A.
1	Matsushita Electric Industrial Co., Ltd.
1	Murata Machinery Ltd.

登録日　：1996 年 11 月 6 日
出願人　：日本電気株式会社
発明者　：岡本栄司, 田中和恵
請求項数：2
発明名称：暗号化及び復号化装置

境らによって以下の特許が出願されている．ペアリング技術を用いた IBE 方式という意味では，日米欧の中で最も早い時期に出願されたものの一つである．

公開番号：特開 2002-026892
出願日　：2000 年 11 月 1 日
出願人　：村田機械株式会社, 境隆一, 笠原正雄
発明者　：大岸聖史, 境隆一, 笠原正雄
請求項数：16
発明名称：鍵共有方法，秘密鍵生成方法，共通鍵生成方法，暗号通信方法，秘密鍵生成器，共通鍵生成器，暗号通信システム及び記録媒体

その他，ペアリング技術を用いた IBE 方式として，境らは以下の特許を出願している．

公開番号：特開 2004-201124
出願日　：2002 年 12 月 19 日

出願人　：村田機械株式会社, 境隆一, 笠原正雄
発明者　：境隆一, 笠原正雄
請求項数：29
発明名称：公開鍵暗号方法，署名方法，暗号通信システム及びコンピュータプログラム

上記を分割して出願したものが以下になる．

公開番号：特開 2007-325318
出願日　：2007 年 9 月 3 日
出願人　：村田機械株式会社, 境隆一, 笠原正雄
発明者　：境隆一, 笠原正雄
請求項数：78
発明名称：署名システム

また，Voltage 社の Boneh らによって，以下の特許が出願されている．現在，Voltage 社から販売されている IBE 関連のソフトウェアのいくつかは，こちらのものが要素技術になっていると考えられる．

公表番号：特表 2005-500740
出願日　：2002 年 8 月 13 日
出願人　：ザ ボード オブ トラスティーズ
発明者　：ダン ボネ，マシュー フランクリン
請求項数：134
発明名称：ID ベース暗号化および関連する暗号手法システムおよび方法

こちらについて，2008 年 9 月 4 日に特許請求が出されているが，特許電子図書館 [IPDL] の審査記録によれば，2009 年 3 月 1 日現在，特許として権利化されていない．一方で，これと同じ内容で米国に申請したもの (US Patent No 7,113,594, 後述の「米国への特許出願」の 4 番) については，既に権利化されている．この特許案件 (特表 2005-500740) について，請求項の中から抜粋したものを以下に示す．

【請求項 01】暗号システムにおいて，送信者と受信者との間で ID ベース秘密メッセージを共有する方法
【請求項 07】公開識別し ID に基づいて解読鍵を作成する方法
【請求項 12】ID ベース暗号システムでメッセージを暗号化し，対応する暗号文を出力する方法
【請求項 24】ID ベース暗号システムでメッセージを解読し，オリジナルのメッセージを出力する方法
【請求項 35】メッセージを暗号化し，暗号文を出力する方法
【請求項 36】暗号文を解読し，メッセージを出力する方法
【請求項 38】暗号文を宛先とする電子メール・メッセージを暗号化する方法
【請求項 76】送信者と受信者との間で通信を行う方法
【請求項 81】ID ベース暗号システムでメッセージを暗号化し，対応する暗号文を出力するシステム

この特許案件の請求項の中で，ID について以下のように記載されている (請求項 11 から抜粋).

■ID の定義　識別子 ID は，個人名，エンティティの名前，ドメイン名，IP アドレス，電子メール・アドレス，社会保障番号，パスポート番号，ライセンス番号，連続番号，郵便番号，住所，電話番号，URL，日付，時刻，件名，事例，所轄区，州，国，信任状，機密取扱資格レベル，および肩書きからなる有限の組み合わせからなるグループから選択さ

れた識別子

ペアリング技術のプリミティブに関連した特許については以下のものがある．

- 楕円曲線上で定義される Tate ペアリングの計算を行う際の演算負荷を軽減する方式 (株式会社日立製作所, 特許出願 2004-135867, 出願日 2004 年 4 月 30 日)
- 楕円曲線上のペアリング演算の高速化を図る方式 (日本電信電話株式会社, 特許出願 2004-124047, 出願日 2004 年 4 月 20 日)
- 楕円曲線ペアリング高速演算方法及び装置 (株式会社日立製作所, 特許出願 2004-50737, 出願日 2004 年 2 月 26 日)
- 楕円曲線暗号のペアリング計算を高速で行う方式 (富士通株式会社, 特許出願 2002-343942, 出願日 2002 年 11 月 27 日)

米国への特許出願

IBE に関連した論文は，72 件存在する．これは，要約 (Abstract), 請求 (Claim) のいずれかに IBE というキーワードを入れて検索し，ヒットした数である．この中で出願人が Boneh となっているのは 9 件，Voltage Inc. となっているのは，10 件存在する．また，この 72 件の中で，既に権利化されているものは，8 件あり，出願人が Boneh となっているのは 4 件，Voltage Inc. となっているのは，4 件存在する．

その他，IBE に関する特許出願のいくつかを以下に示す．ここで出願番号は US Patent No, 公開番号は Patent Application Publication を意味する．

1. 出願番号： 6,886,096
   出願日　：2005 年 4 月 26 日
   出願人　：Voltage Inc.
   発明名称：Identity-based encryption system
   状態　　：権利化されている
   概要　　：IBE を用いたディレクトリの操作

2. 出願番号： 7,017,181
   出願日：2006 年 3 月 21 日
   出願人：Voltage Inc. Identity-based-encryption messaging system with public parameter host servers
   状態　：権利化されている
   概要　：IBE を用いた種々のサービス

3. 出願番号： 7,103,911
   出願日　：2006 年 9 月 5 日
   出願人　：Voltage Inc.
   発明名称：Identity-based-encryption system with district policy information
   状態　：権利化されている
   概要　：サブグループのある IBE システム

4. 出願番号： 7,113,594

出願日：2006 年 9 月 26 日
出願人：The Board of Trustees of the Leland Stanford University および
University of California Davis
発明名称：Systems and methods for identity-based encryption and related cryptographic techniques
状態　：権利化されている
概要　：IBE の主要方式に関する内容

5. 公開番号： 20050071632
出願日：2005 年 3 月 31 日
出願人：Voltage Inc.
発明名称：Secure message system with remote decryption service
状態　：公報
概要　：IBE を用いた web サービス

6. 出願番号： 7,003,117
出願日　：2006 年 2 月 21 日
出願人　：Voltage Inc.
発明名称：Identity-based encryption system for secure data distribution
状態　　：権利化されている
概要　　：IBE を用いたデータ配布サービス

Boneh らのグループは，IBE 方式以外の ID ベース暗号系についても複数の特許出願をしている．これらの多くは特許協力条約 (PCT) を用いて，日米欧を含む複数の国に国際特許として出願 (PCT 出願) されている．

第 5 章の参照文献

[BF01] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” CRYPTO 2001, LNCS 2139, Springer Verlag, pp. 213–229, 2001.

[BB04a] D. Boneh and X. Boyen, “Efficient selective-ID secure identity based encryption without random oracles,” EUROCRYPT 2004, LNCS 3027, Springer-Verlag, pp. 223–238, 2004.

[SK-KEM] M. Barbosa, L. Chen, Z. Cheng, M. Chimley, A. Dent, P. Farshim, K. Harrison, J. Malone-Lee, N. P. Smart, F Vercauteren, “SK-KEM: An Identity-Based KEM”, Standardization Proposal, IEEE P1363.3: Identity-Based Public Key Cryptography, 2006.

[M08] L. Martin, “Identity-Based Encryption Comes of Age”, IEEE Computer, August 2008, pp. 93–95

[SoucePod08] “国内メール市場分析レポート 2008”, http://www.source-pod.com/intelligence/ic2008/

[IPDL] 特許電子図書館. Available from
http://www1.ipdl.inpit.go.jp/IPDL/keika.htm

第 6 章

電子政府用途に対する課題

6.1 CRYPTREC における検討対象の領域

表 6.1 から表 6.4 に ID ベース暗号全般における特徴をまとめる．表中の “ROM” と “StM” はそれぞれランダムオラクルモデルとスタンダード (Standard) モデル[*1]を示す．ここで掲載する各表中における安全性評価欄の記載は，あくまで簡略化した目安の提示であり，その比較検討には，第 2 章各項目及び各方式が発表された原論文の詳細な検討を要する．そして，「標準化で取り上げられた方式」は必ずしも，論文で高い安全性証明が付いた方式そのものではないことを注意する必要がある．

狭義の ID ベース暗号は，発行される ID の信頼性や PKG 運用の信頼性を前提としており，そうしたシステム全体の運用に関する技術的蓄積が少なく，正しい運用方法の周知は一般の公開鍵暗号に比べて十分とは言えない状況にある．従って電子政府推奨暗号リストに記載されているような暗号プリミティブと同等の評価手法を現時点で適用することは，いたずらな誤用を避けるという観点で，適切とは言い難い．また PKI からの移行を考えた場合，1.2.1 節に示されるように問題点も多く，現時点では PKI を完全に置き換えるような移行先技術とは言えない状況にある．

一方で外部との連携を必要としない運用，例えば部署内や組織内においては，ID ベース暗号は ID と共通パラメータのみで運用が可能な為，鍵証明書の管理が必要な PKI 等より導入が相当に容易であると考えられている．さらに広義の ID ベース暗号は表 6.4 に示したように要素技術であるペアリングやその使用方法の発展に伴い多くのアプリケーションが開発されており製品の導入例もあることから，電子政府での利用も検討しておく必要性があると考える．

ID ベース暗号は以下のように大きく 4 つの領域に分けて考えることができる．

1. 数学的理論 (安全性の帰着)
2. 基礎アルゴリズム (利用するペアリングなど)
3. アプリケーション (プロトコル)
4. 運用 (PKG, ID 発行など)

CRYPTREC の評価活動との整合から，何を電子政府推奨暗号リストに記載すべきか，リストガイドで何が補完されるべきかの議論が必要である．ここでは公開鍵暗号と同様に ID ベース暗号が提供できる機能やアプリケーションで技術を分類し，それらが利用する基礎アルゴリズムが選択すべきパラメータや運用などはリストガイドで補完することを想定する．従って電子政府推奨暗号リストに記載される技術は，例えば

[*1] ここの Standard は標準化の意味ではなく，ハッシュ関数の理想化の度合いの観点において，ランダムオラクルを利用しないことを示す (2.1.4 節参照)．

表 6.1　ID ベース暗号 (守秘) の特徴に関する一覧

	技術成熟度	安全性評価	備考
IBE Maurer-Yacobi	岡本 1986 太田 1987		離散対数方式
Cocks [C04]			二次剰余方式
境・笠原方式 (SK 方式) [SK02]		IND-ID-CCA 安全 ROM・ℓ-CBDHI 仮定	
Boneh-Franklin 方式 (BF 方式) [BF01]	IETF:draft-ietf-smime-bfibecms-10.txt IETF:RFC5091(Dec.2007) IEEE P1363.3 Voltage 製品シリーズ 1-14（第 4 章 2 節）	IND-ID-CCA 安全 ROM・CBDH 仮定	
Boneh-Boyen 1 方式 (BB1 方式) [BB04a]	IETF:draft-ietf-smime-bfibecms-10.txt IETF:RFC5091(Dec.2007) IEEE P1363.3 Voltage 製品シリーズ 1-14（第 4 章 2 節）	IND-sID-CCA 安全 StM・DBDH 仮定	
Boneh-Boyen 2 方式 (BB2 方式) [BB04a]		IND-sID-CPA 安全 StM・ℓ-DBDHI 仮定	
Boneh-Boyen 3 方式 (BB3 方式) [BB04b]		IND-ID-CCA StM・DBDH 仮定	
Gentry 方式 [G06]		IND-ID-CCA 安全 StM・ℓ-DtABDHE 仮定	
Waters 方式 [W05]		IND-ID-CCA 安全 StM・DBDH 仮定	

- 守秘 (IBE)
- 署名 (IBS)，グループ署名
- 鍵交換
- 階層的 ID ベース暗号，鍵隔離暗号，代理再暗号，放送暗号など各アプリケーション

のようなカテゴリに分類されるのが適当と考える．各カテゴリで利用すべき基礎アルゴリズムと運用についてはリストガイドで示す．

電子政府推奨暗号リストへの導入の検討においては，各カテゴリにおいて普及や利用が活発になっている利用形態や国際標準の動向を見極める必要がある．

6.2　評価に向けた課題

ID ベース暗号を評価する場合は，以下のように 4 つの観点から行う必要があると考えられる．

表 6.2　ID ベース暗号 (署名) の特徴に関する一覧

	技術成熟度	安全性評価	備考
Hess の IBS [H02]	ISO/IEC 14888-3 7.1 IBS-1		
Cha-Cheon の IBS [CC02]	ISO/IEC 14888-3 7.2 IBS-2		
Guillou-Quisquater の IBS [GQ88-1, GQ88-2]	ISO/IEC 14888-2 GQ1 Scheme 3		RSA ベース方式
Boneh-Boyen の Short Signature [BB04]		選択的メッセージ攻撃に対して 強存在的偽造不可能 StM・SDH 仮定	
Boneh-Boyen-Shacham の Group Signature [BBS04]		 ROM・SDH 仮定	

表 6.3　ID ベース暗号 (鍵管理) の特徴に関する一覧

	技術成熟度	安全性評価	備考
SK-KEM 方式 [SK-KEM]	IEEE P1363.3 トレンドマイクロ・Identum 社		
ID ベース鍵交換 1 Girault-Pailles [GP90]	ISO/IEC 11770-3 C.2		離散対数方式
ID ベース鍵交換 2 Chen-Cheng-Smart	IEEE P1363.3		
ID ベース鍵交換 3 Wang	IEEE P1363.3		

1. プロトコル (アプリケーション) の安全性評価
2. ペアリングなど数学的基礎技術の評価 (適切なパラメータ選択)
3. 実装性能
4. 運用性

安全性評価においては，新しい数学的仮定の妥当性，帰着効率，ハッシュ関数を理想化しての安全性評価の妥当性などが挙げられる．また数学的な安全性証明の手法としてランダムオラクルモデルであるかスタンダードモデルであるかの違いをどのように扱うか，という問題もある．安全性を重視しスタンダードモデルで評価したパラメータ選択を行うか，実装性能を重視しランダムオラクルモデルで評価したパラメータ選択を行うかなど，安全性と実装性がトレードオフになっているという特徴もあり，一元的な評価の適用が適切ではない．また利用できるペアリング技術も複数から選択可能であり，利用したペアリングで安全性や実装性が異なる場合があり，適切な選択を示す必要もある．運用においては，ID 発行と PKG 運用の信頼性，鍵更新やユーザ鍵の無効化処理などがある．以上より，評価を実施し推奨技術を選定するためには以下のような課題について解決しなければならない．

表 6.4　ID ベース暗号 (その他のアプリケーション) の特徴に関する一覧

	技術成熟度	安全性評価	備考
Boneh-Gentry-Waters の放送暗号 [BGW05]		IND-CCA 安全 ℓ-BDHE 仮定	
Matsuo の Proxy 再暗号 (M1 PRE, M2 PRE) [M07]	IEEE P1363.3		M1: 階層 Proxy 再暗号 M2: ID ベース Proxy 再暗号
Sahai-Waters の属性暗号 ABE [SW05]		selective-attribute set 安全 StM・DBDH 仮定	IND-sID-CCA の拡張
Boneh-Crescenzo-Ostrovsky-Persiano の Keyword searchable 暗号 (匿名 IBE) [BCO+04]			
Dodis-Katz-Xu-Yang の Key-Insulated 暗号 [DKX+02]	IEEE P1363.3		離散対数方式
Gentry-Silvergberg の HIBE 方式 [GS02]	IEEE P1363.3	IND-HID-CCA ROM・CBDH 仮定	
Canetti-Halevi-Katz の Forward-Secure 暗号 [CHK03]		DBDH 仮定	

- アプリケーション (プロトコル) の安全性評価手法の確立
- 異なる数学的仮定を用いた安全性評価の比較や相対評価の確立
- 安全性レベルの定義づけ
- 安全性と実装性の関連づけ
- 運用に関する問題の分析手法の確立

第 6 章の参照文献

[BB04a] D. Boneh and X. Boyen, “Efficient selective-ID secure identity based encryption without random oracles,” EUROCRYPT 2004, LNCS 3027, Springer-Verlag, pp. 223–238, 2004.

[BB04b] D. Boneh, X. Boyen, “Secure identity based encryption without random oracles,” CRYPTO 2004, LNCS 3152, Springer-Verlag, pp.443–459, 2004.

[BB04] D. Boneh and X. Boyen, “Short signatures without random oracles,” EUROCRYPT 2004, LNCS 3027, Springer-Verlag, pp. 56–73, 2004.

[BBG05] D. Boneh, X. Boyen and E. Goh, “Hierarchical identity based encryption with constant size ciphertext,” EUROCRYPT 2005, LNCS 3494, Springer-Verlag, pp. 440–456, 2005.

[BBS04] D. Boneh, X. Boyen, H. Shacham, “Short group signatures,” CRYPTO 2004, LNCS 3152, Springer-Verlag, pp. 41–55, 2004.

[BCO+04] D. Boneh, G. D. Crescenzo, R. Ostrovsky, G. Persiano, “Public Key Encryption with Keyword Search,” EUROCRYPT 2004, LNCS 3027, Springer-Verlag, pp. 506–522, 2004.

[BF01] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” CRYPTO 2001, LNCS 2139, Springer Verlag, pp. 213–229, 2001.

[BGW05] D. Boneh, C. Gentry and B. Waters, “Collusion resistant broadcast encryption with short ciphertexts and private keys,” CRYPTO 2005, LNCS 3621, Springer-Verlag, pp. 258–275, 2005.

[CHK03] R. Canetti, S. Halevi, and J. Katz, “A forward-secure public-key encryption scheme,” EUROCRYPT 2003, LNCS 2656, Springer-Verlag, pp. 255–271, 2003.

[CC02] J. C. Cha and J. H. Cheon, “An identity-based signature from gap Diffie-Hellman groups,” Proceedings of PKC 2002, LNCS 2567, Springer-Verlag, pp. 18–30, 2002.

[C04] C. Cocks, “An identity based encryption scheme based on quadratic residues,” IMA International Conference on Cryptography and Coding–IMA Int. Conf.2001, LNCS 2260, Springer-Verlag, pp.360–363, 2001.

[DKX+02] Y. Dodis, J. Katz, S. Xu, M. Yung, “Key-insulated public key cryptosystems,” EUROCRYPT 2002, LNCS 2332, Springer-Verlag, pp. 65–82, 2002.

[G06] C. Gentry, “Practical identity-based encryption without random oracles,” EUROCRYPT 2006, LNCS 4004, Springer-Verlag, pp. 445–464, 2006.

[GS02] C. Gentry, A. Silverberg, “Hierarchical ID-based cryptography,” ASIACRYPT 2002, LNCS 2501, Springer-Verlag, pp.548–566, 2002.

[GP90] M. GIRAULT, J.C. PAILLES, “An identity-based scheme providing zero-knowledge authentication and authenticated key exchange,” Proc. ESORICS 1990, pp. 173–184,1990.

[GQ88-1] L.C. Guillou and J.-J. Quisquater, “A practical zero-knowledge protocol fitted to security micropro-

cessor minimizing both transmission and memory," Advances in Cryptology–Eurocrypt '88, LNCS 330, Springer-Verlag, pp. 123–128, 1988.

[GQ88-2] L.C. Guillou and J.-J. Quisquater, "A paradoxical identity-based signature scheme resulting from zeroknowledge," Advances in Cryptology–Crypto '88, LNCS 403, Berlin, Springer-Verlag, pp. 216–231, 1988.

[H02] F. Hess, "Efficient identity based signature schemes based on pairings," Proceedings of SAC 2002, LNCS 2595, Springer-Verlag, pp.310–324, 2003.

[M07] T. Matsuo, "Proxy re-encryption systems for identity-based encryption," Pairing 2007, LNCS 4575, Springer Verlag, pp.247–267, 2007.

[SW05] A. Sahai, B. Waters, "Fuzzy identity-based encryption," EUROCRYPT 2005, LNCS 3494, Springer Verlag, pp.457–473, 2005.

[SK02] 境隆一, 笠原正雄, 楕円曲線上のペアリングに基づく二，三の暗号方式 (その 2), 信学技報, ISEC2002-52, pp.131–138, Jul.2002.

[SK-KEM] M. Barbosa, L. Chen, Z. Cheng, M. Chimley, A. Dent, P. Farshim, K. Harrison, J. Malone-Lee, N. P. Smart, F Vercauteren, "SK-KEM: An Identity-Based KEM", Standardization Proposal, IEEE P1363.3: Identity-Based Public Key Cryptography, 2006.

[W05] B. Waters, "Efficient identity based encryption without random oracles," EUROCRYPT 2005, LNCS 3494, Springer Verlag, pp. 114–127, 2005.

付録 A

用語・記号一覧

表 A.1　ID ベース暗号用語・記号一覧

用語・記号	説明	ページ検索
【常用用語】		
ID	Identity or Identification，ID 情報	1-67
CA	PKI において信頼できる機関	6
PKG	Private key generator:IBE において信頼できる機関	2-6,9,16,64,66
Problem 1 $\leq_p$ Problem 2	問題 Problem 1 を問題 Problem 2 に 確率的多項式時間で帰着可能	20-21
【ペアリングベース暗号】		
ID ベース暗号，IBE	ID based encryption	2-66
ID ベース署名，IBS	ID based signature	9,48,50,65-66
ID-NIKS	ID based Non-Interactive Key Sharing	3,5
HIBE	階層的 IBE	6-8,51,67
属性ベース暗号，ABE	Attribute-based encryption	8,67
放送暗号，Broadcast 暗号	Broadcast encrypiton	8,65,67
グループ署名	Group signature	8,65
Keyword searchable 暗号	Keyword searchable PKE	7,67
Key insulated 暗号	Key insulated PKE	7,51,67
Forward secure 暗号	Keyword searchable PKE	7,67
Proxy 暗号	Proxy PKE	7,52,67
KPS	Key Predistribution System	3
BF 方式	Boneh-Franklin IBE 方式 [BF01]	3,9-11,38,50-52,54,65
SK 方式	境-笠原 IBE 方式 [SK02]	9-11,52,54,65-66
BB1 方式	Boneh-Boyen1 IBE 方式 [BB04a]	5,9-11,23,50-54,65
BB2 方式	Boneh-Boyen2 IBE 方式 [BB04a]	5,9-11,24,65
BB3 方式	Boneh-Boyen3 IBE 方式 [BB04b]	5,9-11,65
W05 方式	Waters IBE 方式 [W05]	5,9-11,23,65
G06 方式	Gentry IBE 方式 [G06]	5,9-11,23-24,65
【安全性定義】		
IND-ID-CPA	IBE に選択平文攻撃に対する識別不可能性	16-17
IND-sID-CPA	選択的 ID, IBE に選択平文攻撃に対する識別不可能性	17,24,65
IND-ID-CCA	IBE に選択暗号文攻撃に対する識別不可能性	16-17,23-24,65
IND-sID-CCA	選択的 ID, IBE に選択暗号文攻撃に対する識別不可能性	17,23-24,65,67

用語	説明	ページ検索
【仮定難問】		
CBDH	双線形 Diffie-Hellman 計算問題	17-18,23-24,65,67
CDH	Diffie-Hellman 問題	18,21,23-24
DBDH	双線形 Diffie-Hellman 判定問題	17,23,65,67
FAPI-1	Fixed Argument Pairing Inversion： given 1st input point	21-22
FAPI-2	Fixed Argument Pairing Inversion： given 2nd input point	21-22
GPI	Generalized Pairing Inversion: 二変数に関する一般化されたペアリング逆関数問題	21-22
MI	Miller Inversion：Miller アルゴリズム逆関数問題	22
HRP	Hidden Root Problem：最終べき乗算逆関数問題	22
ℓ-ABDHE	Augmented 双線形 Diffie-Hellman 指数判定問題	24,65
ℓ-CBDHI	Computational ℓ-BDHI	24,65
ℓ-DBDHI	Decisional ℓ-BDHI	24,65
ℓ-SDH	強 Diffie-Hellman 計算問題	18,23-25,66
DDH	Diffie-Hellman 判定問題	18,23
【楕円曲線】		
$\#G$	群 G の位数 (要素数)	28,38-40
n	位数	4-5,9,10,18-20,25,28-29, 33-34,38-40
κ	埋め込み次数	19,28
$\mathbb{F}_q$, $\mathbb{F}_{q^\kappa}$	有限体	4,19,28-29,33,38
$E(\mathbb{F}_q)$	$\mathbb{F}_q$ 上の楕円曲線上の点	4,19,28-40
$E(\mathbb{F}_{q^\kappa})$	$\mathbb{F}_{q^\kappa}$ 上の楕円曲線上の点	4,19,28-29
$E(\mathbb{F}_q)[n]$	$E(\mathbb{F}_q)$ の位数 n の部分群	4-5,9-10,29,33-35,38-40
$\mathbb{G}_1$	$E(\mathbb{F}_q)$ の部分群	18-25,28,38-40
$\mathbb{G}_2$	$E(\mathbb{F}_{q^\kappa})$ の部分群	18-25,28,38-40
P, Q	楕円曲線上の点	4-5,9-11,21-25,28-29, 33-34,38-40
p	素数	28-30,38-40
q	素数または素数のべき乗	4,19-20,28-29,38
【システムのパラメータ】		
H_1	map to point in G_1	4,10,39-40
H_2	map to point in G_2	39-40
k	システムのセキュリティパラメータ	16,20
s	msk: master secret key	4,9-11,25
prm	システムの共通パラメータ	16

用語	説明	ページ検索
【Pairing】		
e	一般的なペアリング	4-5,10-11,18,21-25,28
e_T	Tate ペアリング	29-33
e_η	η_T ペアリング	33-37
e_A	Ate ペアリング	34-38
【アルゴリズム】		
SET	システム Setup アルゴリズム	15-16
GEN	ユーザの秘密鍵生成アルゴリズム	15-16
ENC (E)	暗号化アルゴリズム	15-16
DEC (D)	復号化アルゴリズム	15-16
$\mathcal{A}$	攻撃アルゴリズム	16,18,25

発行日　2009年5月14日　第1版　第1刷
発行者
・〒184-8795
東京都小金井市貫井北四丁目2番1号
独立行政法人 情報通信研究機構
（情報通信セキュリティ研究センター セキュリティ基盤グループ）
NATIONAL INSTITUTE OF
INFORMATION AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI,KOGANEI
TOKYO,184-8795 JAPAN

・〒113-6591
東京都文京区本駒込二丁目28番8号
独立行政法人 情報処理推進機構
（セキュリティセンター 暗号グループ）
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
2-28-8 HONKOMAGOME,BUNKYO-KU
TOKYO,113-6591 JAPAN