SCIS 2007 The 2007 Symposium on Cryptography and Information Security
Sasebo, Japan, Jan. 23-26, 2007
The Institute of Electronics, Information and Communication Engineers

ID-base 暗号によるデータ共有のための proxy cryptography
Proxy cryptographic scheme in IBE with Applications to Data Storage

扇 裕和*
Hirokazu Ougi

あらまし データを暗号化してファイルサーバに格納し、複数のユーザで共有して利用する場合、格納するデータ、もしくはデータ暗号化用に使用する共通鍵は、ファイルサーバ内では露呈せずに管理することが求められる。公開鍵暗号を利用する場合、たとえば Alice がデータ作成と同時に自身の公開鍵で格納した暗号化データを、Bob が後から利用する場合、Bob に復号可能となるように当該暗号化データを変換して提供する必要がある。本稿は、Proxy cryptography と呼ばれるこのような暗号化データの変換方法を、ユーザにとって利便性の高い ID-base 暗号技術により構成する方式について検討したものである。

キーワード ID-base 暗号,Proxy cryptography,公開鍵,

1 はじめに

ID-base 暗号は、PKI では必要でとなる公開鍵に対する認証確認が不要となるため、とてもユーザにとって利用しやすい方式となっている。本稿は、この ID-base 暗号に、proxy cryptography と呼ばれる暗号化データの変換機能を組み込み、この変換機能を利用して使いやすくかつ安全なファイルシステムの構成法、即ち暗号化データの共有方式について検討したものである。

様々の組織、部署において複数のユーザがデータを共有するファイルサーバは広く利用されており、このデータを共通鍵暗号、たとえば AES などにより暗号化して格納することも可能となった。

暗号を利用するファイルサーバでは、管理者によるオペレーションミスなどに配慮して、共通鍵やデータは当該ファールサーバ内では露呈させないなどの対応が必要である。

G. Ateniese *et al*(2005)[3]は、このようなファイルサーバを untrusted server としてとらえ、公開鍵の Proxy cryptography を利用したデータ格納方式を提案した。

Proxy cryptography とは、一つの鍵で暗号化したデータを他の鍵で復号可能となるよう、暗号化データに変換を与える暗号処理技術である。

Ateniese の方式では、暗号化データの変換情報は、re-encryption key により与えられる。Alice が暗号化したデータを、Bob が復号しようとする場合、Bob は Alice が復号権限を委譲するために作成した、re-encryption key を取得し、当該暗号化データを平文にもどすことなく、Bob 自身の秘密鍵で復号することが可能である。

2 背景となる関連研究をよび本稿の検討内容

本稿の暗号化データ変換のベースとなる方式は、1998 年、M.Blaze, G.Bleumer, M. Strauss[1]により提案された、「atomic proxy cryptography」という概念である。

2003 年、Y. Dodis, A. Ivan[3]は、ElGamal, RSA, IBE において、この Proxy cryptography を検討し、「unidirectional proxy encryption」の機能を提案した。2005 年 G. Ateniese *et al*(2005)[3]は、この ElGamal 暗号と、PKI をベースとする、proxy cryptography を適用したファイルシステムの構成法を提案した。本稿では、このような proxy cryptography と呼ばれる暗号化データ変換方式を、さらに IBE で構成する方式について検討した。IBE(Identity-based encryption scheme)については、2001 年、D. Boneh, M. Franklin の提案以来様々の検討が進み、CCA 等の安全性に関しても十分な検討がなされている[4]。本稿ではこれらの研究のうち、暗号方式については[5]を、電子署名方式については[6]を利用して、proxy cryptography の機能構成を検討した。本方式は、ID により、複数のユーザ間で暗号化データを共有させる方式である。2006 年に提出された D. Boneh *et al* の IBE の方式[5]は、共通鍵(AES)と組み合わせる方式であり、CCA の安全性も確保され、完成度の高い方式となっている。

グループによる暗号化データの共有方式として、IBE には Hierarchy を構成することが可能である[7][8][9]。本稿では、proxy と Hierarchy とを組み合わせる柔軟な方式の構成についても検討を行った。

3 proxy cryptography ファイルシステムの機能構成

D. Boneh *et al* [5]の ID-base 暗号をベースに、proxy cryptopgaphic scheme を組み込んだ本提案のファイルシステムの構成について示す。

3.1 暗号処理に関するシステムの構成

(1) PKG(Public key Generator)
- master secret key をもとに各ユーザが利用する master public key を生成し公開する。
- 各ユーザの ID に対応する秘密鍵を生成し、secure chanel により各ユーザに配布する。
- proxy secret key を有し、ユーザ間の復号権限の委譲に関する proxy-key 生成に関与する。

(2) ファイルサーバ(untrusted)
- ユーザが暗号化したデータを格納して利用する。
- 暗号処理に関する鍵管理機能は有しない。

(注) ファイル管理用のソフトウェアとしては、unix 系では NFS,windows 系では CFIS などが知られている。パスワード程度のサポートのものは、セキュリティ上の信頼性は低いと考えられる。

(3) ファイル管理用の鍵の構成

(i) FEK(file encryption key)
AES などのデータ暗号化に使用する共通鍵

(ii) ID(owners ID, public key used in encryption)
名前、部署、mail-adres、phone number 等の ID
ID-base 暗号では暗号化の公開鍵として使用する

(iii) PKID(owners secret key used in decryption)
ID に対応する復号用の秘密鍵
PKG が ID をもとに作成し、各ユーザに配布する。

(iv) Q_{ID}(owners public key used in signature)
ID に対応する署名検証用の公開鍵

(v) dQ_{ID}(owners secret key used in signature)
Q_{ID} に対応する署名作成用の秘密鍵
PKG が Q_{ID} をもとに作成し、各ユーザに配布する。

(vi) pRK(proxy-key)
復号権限委譲機能を与える鍵

（注）pRK は、Q_{ID} を変換して作成される。
pRK をもとに、PKID から別のユーザ ID による暗号化データの復号鍵が作成される。

3.2 暗号処理に関する機能構成

Alice がデータ M(plaintext)を暗号化してファイルサーバに格納するとともに、Bob に当該暗号の復号権限を委譲する proxy-key を作成し、Bob がこの proxy-key を取得して当該暗号データを復号する手順を参照し、暗号処理の機能について説明する。

ここで

IDa, PKIDa ; Alice の ID、および（復号）秘密鍵
IDb, PKIDb ; Bob の ID、および（復号）秘密鍵
$pRK_{A\text{-}B}$; Alice が Bob に復号権限を委譲する proxy-key とする。

以下の説明ではこのように、Alice または Bob に関する演算処理によって作成されるデータには、適宜 a,b,A,B の識別子(sufix)を付加するが、特に混乱はないと考える。

3.2.1 (通常の) 暗号処理

(1) データの暗号化(Encf, Encp)

(i) Encf(FEK, M) = Cf (共通鍵による M の暗号化)
FEK; 共通鍵, M; plaintext, Cf; ciphertext

(ii) Encp(IDa, FEK)= Ck (ID による共通鍵の暗号化)
IDa; Alice の ID, FEK; 共通鍵, Ck; ciphertext

(2) データの復号(Decf,Decp)

(i) Decp(PKIDa, Ck) = FEK

(ii) Decf(FEK, Cf) = M

(3) 電子署名

dQ_{ID} による署名作成、Q_{ID} による署名検証

3.2.2 ID による proxy 暗号処理

(1) Proxy 処理に関する鍵の構成

PKID は、Q_{ID} を要素として含む。
即ち、.PKID=(K, Q_{ID})となり、
PKIDa= (Ka, Q_{IDa})
PKIDb=(Kb, Q_{IDb})

(i) proxy-key $pRK_{A\text{-}B}$
Alice が Bob に Alice の暗号化データの復号権限を委譲する鍵(以降 proxy-key と呼ぶこととする。)

(ii) Bob の proxy-accept key Q_{IDb}
Bob は、Q_{IDb} を proxy-accept key とし、PKG と Alice の Q_{IDb} に関する変換処理により proxy-key $pRK_{A\text{-}B}$ を受け取る。変換処理を R とすると $pRK_{A\text{-}B}=R(Q_{IDb})$

(iii) $PKID_{A\text{-}B}$ (proxy-decryption-key)
Bob が Alice の暗号化データの復号に使用する鍵
$PKID_{A\text{-}B}$ = (Kb, $pRK_{A\text{-}B}$)
(以降、proxy-decryption-key と呼ぶことこする。)

(2) Proxy-key の作成と登録

(i) Alice が復号権限を委譲するユーザの IDbi ($1 \leqq i \leqq n$) を指定し、このユーザ ID に対応する公開データ (proxy-accept-key)Q_{IDbi} ($1 \leqq i \leqq n$) を PKG に proxy-key 作成要求として送付する。

(ii) PKG は、Alice の IDa と所有する master secret key をもとに proxy-key $pRK_{A\text{-}Bi}$($1 \leqq i \leqq n$)を作成し、Alice に送付する。

(iii) Alice は、(1)項で作成した、暗号化データとともに、proxy-key をファイルサーバ（untrusted）に登録する。

（注）PKG に送付する proxy-key 作成要求は、要求元が Alice であることを保証する必要があり、電子署名で作成する。

(3) proxy-key の取得

Bob はファイルサーバに Alice の暗号を復号する権限を委譲する proxy-key $pRK_{A\text{-}B}$ が登録されているか確認する。登録されていれば、この proky-key $pRK_{A\text{-}B}$ と PKIDb により、$PKID_{A\text{-}B}$= (Kb, $pRK_{A\text{-}B}$)を作成する。

(4) Bob の Alice の暗号化データの復号(Decp,Decf)

(i) $PKID_{A\text{-}B}$,により Cf を復号し FEK を取得する。
i.e. Decp($PKID_{A\text{-}B}$,, Cf) = FEK

(ii) FEK により Ck を復号しデータ M(plaintext)を取得する。 i.e. Decf(FEK, Ck) = M

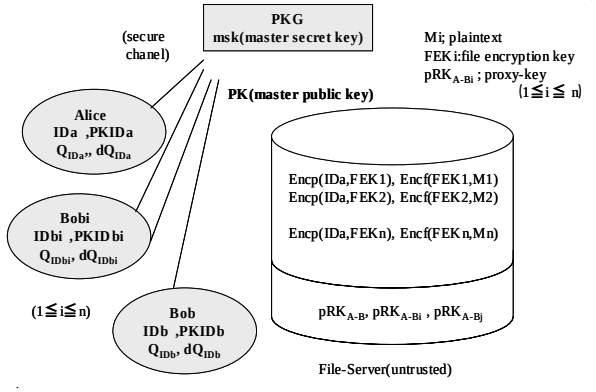

図1 ID-base 暗号前提のファイルシステムの構成
Figure1. File-system using on IBE

4 Proxy 暗号処理に要求される機能.

2 項では、proxy-key を利用した、暗号化、復号の処理手順を示した。次にこの proxy-key を使用した処理に要求される機能について示す。

4.1 PKG の信頼性

この ID-base 暗号方式は、PKG が、master-key により各ユーザの秘密鍵を生成する。

したがって PKG は、各ユーザに暗号文を復号することが可能である。また、各ユーザの ID と master-key をもとに、proxy-key を生成することが可能である。従って、PKG は、Trusted とする必要がある。

この key-escrow に関する解決策として、C. Gentry, P. Morillo, C. Rafols は 、 CBE(Certificate-Based Encryption)方式を提案しているが、このような検討は、今後の課題としたい。

4.2 Proxy cryptographic scheme の処理の特性

(1) 透明性(proxy-invisibility)

ユーザの ID とシステムパラメターpram で平文 M の暗号化データ C_M が作成される。この暗号化データは、ユーザの所有する秘密鍵で復号されるが、proxy-key を与えられた場合も、同じ復号 Alogoritm で復号されるものとし、ユーザ側は、proxy-key の存在をほとんど意識しないで利用可能である。

(2) 自己管理性(original-access)

Alice は、自身の ID でデータを暗号化して格納するが、自身の所有する秘密鍵で復号可能であり、格納したデータの保守管理が実施可能である。

(3) proxy-key サイズの不変性（key-optimal）

システムに加入するユーザの加入数に関係することなく、proxy-key のサイズは system parameter のみで定まり不変となる。

4.3 Proxy-key の安全性

Alice は、復号権限を proxy-key により委譲するため、proxy-key は、Alice が関与しないと生成できない性質をもつ必要がある。このため、下記の性質を有する。

(1) 非可逆性(unidirectional)

Bob が Alice から取得した proxy-key $pRK_{A\text{-}B}$ をもとに、$pRK_{B\text{-}A}$ を算出することはできない。

(2) 非遷移性(Non-transitive)

$pRK_{A\text{-}B}$, $pRK_{B\text{-}C}$ から $pRK_{A\text{-}C}$ を算出することはできない。

(3) 結託回避性(collusion –safe)

任意の n ユーザの proxy-key $pK_{A\text{-}Bi}$(1 ≦i≦n)から Alice の秘密鍵 PKIDa を算出することはできない。

(4) 非導出性(Non-transfeable)

任意の n ユーザの proxy-key $pRK_{A\text{-}Bi}$(1 ≦i≦n)から第3者 craroll の proxy-key $pRK_{A\text{-}C}$ を算出することはできない。

5 IBE での proxy cryptography の実装

5.1 ID-based Encryption Scheme

まず、Boneh *et al.*(2006) [7]に従って、proxy cryptographic scheme を組み込むために使用する ID-based Encryption Scheme について述べる。

5.1.1 The Bilinear Diffie-Hellman Assumption(BDH)

群 G, W を素数位数 q の巡回群とし、群 G の生成元を g とする。

(1) non-trivial Bilinear map e: G x G → W

直積群 GxG から W への計算可能な写像 e は以下の性質を有する。

(i) μ, $\nu \in G$, a,b ∈ Zq に対して
$e(\mu^a, \nu^b) = e(\mu, \nu)^{ab}$

(ii) e(g,g) = Z は、巡回群Wを生成する。

(2) The Bilinear Diffie-Hellman Asuumption(BDH)

IG(input generater) を security parameter (1^k) より {G, W, g, e} を生成する algorithm とする。

(i) The Computational BDH problem

$\{g, {}^{\alpha}g^{\beta}, g^{\gamma}\}$（任意の$\alpha, \beta, \gamma \in Zq$）に対して

$e(g,g)^{\alpha\beta\gamma}$を多項式時間内に求めることは、計算量的に困難であるとする。

(ii) The Decisional BDH problem

$\{g, {}^{\alpha}g^{\beta}, g^{\gamma}\ e(g,g)^{\alpha\beta\gamma}\}$ $\{g, {}^{\alpha}g^{\beta}, g^{\gamma}\ e(g,g)^{\mu}\}$

（任意の$\alpha, \beta, \gamma, \mu \in Zq$）を(1/2)以上の確率で多項式時間内に区別することは、計算量的に困難であるとする。

5.1.2 IBE Scheme の algorithm の構成

IBE Scheme は、４組の algorithm **Setup, Derive Encrypt(Enc), Decrirt(Dec)** で構成される。

IG(1^k) により、system parameter {G,, W, g, e}は既に構成されているものとし、L, H を次の関数とする。

L； W → $\{0,1\}^k$ ；一様分布関数

H ; $\{0,1\}^*$ → G ； cryptographic hash 関数とする。

(1) **Setup**

PKG(Public key generator)は、次の msk, PK を生成する。

(i) msk (master secret key)

任意 random に、x, y ∈ Zq を定め、master secret key を msk = { x, y } とする。

(ii) PK(master public key)

Z = e(g,g) , $g_1 = g$, $g_2 = g^y$, $g_3 = g^x$ とし, これより master public key を PK = { g_1, g_2, g_3, Z^x} として、加入ユーザに公開する。

(2) Drive

PKG は、msk と、各ユーザの ID を用いて、対応する秘密鍵 SKID を生成し、secure chanel により配布する。

$Q_{ID} = H(ID) \in G$, $K = g^x Q_{ID}^y Q_{ID}^{x*ID}$ を算出し、

SKID = { K, Q_{ID} } とする。

(3) Encrypt(Enc ; 暗号化)

message M ∈ { 1,0 }^{k} (Message Space)を、ID ∈ Zq 及び random s ∈Fq を設定し、PK をもとに暗号化する。

Enc(ID, M) = C_M = (A, B, C) (C_M ; ciphertext)とすると、

$A = g_1^s$,

$B = g_2^s g_3^{s*ID}$

$C = L((Z^x)^s) \oplus M$

(4) Decrypt(Dec ; 復号)

ciphertext C_M は、ユーザの秘密鍵 SKID により復号可能である。

Dec(PKID, C_M)

$= C \oplus L(e(A,K)/e(B,Q_{ID})) = M$

5.1.3 Boneh *et al.*(2006) [7]の IBE からの変更点

本 IBE Scheme の４組の algorithm は、Boneh *et al.*(2006) [7]のとまったく同じである。

ただし、秘密鍵 SKID = { K, Q_{ID} }の構成要素である、Q_{ID} を、各ユーザの ID から、hash 関数 H で定まる方式とした。このことにより、

(i) Q_{ID} は、proxy key pKR を作成するための accept key であるが、認証することなく、ユーザの Q_{ID} を取得することが可能である。

(ii) Q_{ID} を IBE の署名検証鍵として使用することが可能となる。

5.2 proxy cryptographic scheme 機能

5.2.1 proxy cryptographic scheme 機能の組み込み

本 IBE Sc Alice が作成した暗号文(ciphertext)を Bob の秘密鍵で復号するための機能を提供する proxy key pRK_{A-B} を定める方式について検討する。

(1) KG（鍵の構成）

Alice の ID を IDa , 秘密鍵を PKIDa

Bob の ID を IDb, 秘密鍵を PKIDb とする。

PKIDa = (K_a, Q_{IDa}) ($K_a = g^x Q_{IDA}^y Q_{IDA}^{x*ID\,a}$)

Q_{IDa}= H(IDa) (accept key)

PKIDb = (K_b, Q_{IDb}) ($K_b = g^x Q_{IDB}^y Q_{IDB}^{x*ID\,b}$)

Q_{IDB} = H(IDb) (accept key)

(2) Proxy-key pRK_{A-B} の構成

Alice は IDa で平文 M(plaintext) から暗号文 C_M(ciphertext)を作成し、Bob は、proxy key pRK_{A-B} をもとに、この暗号文を復号する。Proxy-invisibility を与えるため、復号 Algorithm は同一とする。

このとき Bob の復号鍵 $PKID_{A-B}$ を

$PKID_{A-B}$= (K_b, pRK_{A-B}) として与える。

$pRK_{A-B} = Q_{IDb} \cdot Q_{IDb}^{\alpha}$ とする。

α を求めるため、ta, tb∈Zq により、

$Q_{IDa} = g^{ta}$, $Q_{IDB} = g^{tb}$ とすると、

$pRK_{A-B} = g^{tb(1+\alpha)}$

Alice の作成した、暗号文を C_M = (A, B, C) とすると、

$A = g^s$

$B = g^{(s*y + s*x*IDa)}$

$C = L((Z^x)^s) \oplus M$

これより、復号演算により定まる関係は、

$e(A, K_b) = e(B, pRK_{A-B}) \cdot Z^{s*x}$

$e(A, K_b) = e(g^s, g^{(x+ y*tb + x*tb*IDb)})$

$e(B, pK_{A-B}) = e(g^{(s*y + s*x*IDa)}, g^{tb(1+\alpha)})$

これより、

$s(x+ y*tb+ x*tb*IDb) = (s*y+ s*x*IDa)tb(1+\alpha) + s*x$

$\alpha(y + x*IDa) = x*(IDb - IDa)$

$\sigma = y/x$ とすると

$\alpha = (IDb - IDa)/(\sigma + IDa)$

Alice が Bob に与える proxy-key pK_{A-B} が ID と Trusted PKG が所有する秘匿データ σ で定まる。

以降、この σ を master proxy key と呼ぶこととする。

5.2.2 本 proxy cryptographic scheme の特徴

master proxy key σ を Bob が取得すると、Bob は、システムに加入している任意のユーザに対して、公開されている ID から、当該ユーザの暗号化データを復号可能な proxy-key を生成することが可能となる。従って

master proxy key σ は、PKG により厳重に管理する必要がある。また、hash 関数 H が random oracle であれば、proxy-key はユーザの結託攻撃から安全であり、4.2, 4.3 項で定めた proxy 暗号処理に要求される機能を満足していることを確認することができる。

5.3 電子署名(signiture)機能の組み込み

(1) PKG の sig master secret key
(i) PKG は、電子署名用の parameter として、sig master secret key = s_k ($s_k \in Zq$)を設定し所有する。
(ii) PKG は、電子署名用の master public key $P_{pub}=g^{s_k}$ を公開する。
(2) ユーザ(Alice)の電子署名用秘密鍵
Alice の IDa をもとに、$Q_{IDa}=H(IDa)$を生成し、Alice の電子署名作成用の秘密鍵として $dQ_{IDa}=Q_{IDa}^{s_k}$ を生成し、PKG は Alice に配布する。
(注) Short Signature 機能
D. Boneh *et al*[6]に従って、Short Signature の機能を構成することも可能である。この場合、MNT-curve 上の異なる生成元 Go,Ge を使用する。これにあわせて、Enc, Dec の演算の修正も必要となるが、ほとんど同じ alogorithm で構成することが可能である。

6 グループ編成によるデータ共有方式

ID-base 暗号では、PKG が、master secret key をもとに、各ユーザの秘密鍵を生成し、また、各ユーザ間の暗号化データ共有のための proxy-key の生成に関与している。従って、システムに加入するユーザ数が、多くなると、PKG に対する処理の負荷が増大する。そこで、組織、部署、仕事のプロジェクト単位等、データを共有する可能性の高いメンバーでグループを編成し、PKG への負荷を分散させて暗号システムを構成する方式について示す。

(1) グループ編成の PKG の構成
グループを GMi(1≦i≦n)とする。
GMi に対して PKGi(1≦i≦n)を設置し、各 PKGi の所有する master secret key を
mski = { x , yi , σi }
x, yi ∈ Zq σi = yi/x (1≦i≦n)
とする。ただし、x はシステム全体で共通とする。

(2) 異なるグループ間の proxy-key
Alice が GMa, に Bob が GMb に属すものとする。
Alice Bob の ID には所属するグループの識別子（番号）が付与されているものとする。秘密鍵は、
PKIDa = (K_a, Q_{IDa}) ($K_a= g^x Q_{IDa}^{ya} Q_{IDa}^{ya*IDa}$)
PKIDb = (K_b, Q_{IDb}) ($K_b= g^x Q_{IDb}^{yb} Q_{IDa}^{yb*IDb}$)
Bob が Alice の暗号文を復号するための復号鍵を
$PKID_{A-B}$= (K_b, pRK_{A-B})
Proxy-key を $pRK_{A-B} = Q_{IDb}^{\alpha}$ とする。
5 項と同様の手順で α をもとめると
α = (σ_b + IDb)/(σ_a + IDa)

(3) proxy-key の取得と登録
$\mu_b = \sigma_b$ + IDb
β_a= 1/(σ_a + IDa)
Alice は Bob から認証して $Q_{IDb}^{\mu b}$ を取得し、5.4 項と同様の手順で、$pRK_{A-B} = (Q_{IDb}^{\mu b})^{\beta a}$ を GMa から取得する。
Bob は、$Q_{IDb}^{\sigma b}$ を公開することが可能であるが、Bob の ID から生成されるデータではないため、Alice は、Bob を認証して $Q_{IDb}^{\sigma b}$ を取得する必要がある。

(4) グループ編成方式の特徴
各グループの PKGi(1≦i≦n)の master secret key mski = { x, yi }のうち、x を共通とすることで、master public key PKi を異にするグループ間でも、proxy-key を生成することができ、暗号化データが共有可能であるという特徴を有している。

7 HIBE での proxy cryptography

Hierarchical IBE(HIBE)system では、グループで暗号化データを共有することが可能である。HIBE では、あらかじめ、暗号化データを共有可能なように、各ユーザの秘密鍵を設定する。この HIBE system でも、復号権限を与え、データ共有させるための proxy-key を設定することが可能である。ここでは、D. Boneh *et al* [10] の HIBE に対し proxy key の設定法について示す。異なる階層に位置するユーザ間において proxy key を設定すれば、1 回の proxy key の設定で、複数のユーザによるデータの共有が可能となり、データを共有するグループ設定の効率化を図ることが可能である。
HIBE では、Public key 即ち、ID は vector で与えられる。Alice と Bob の IDa、IDb が、図 2 に示す通り、sysytem prameter は同一で、異なる階層に位置する場合の proxy-key pRK_{A-B} の設定方式について示す。

7.1 HIBE system

(1) Setup(l):
maximum depth l の system parameter 生成
params : public parameter
master-key : master secret key
とすると、
params = { g, g_1, g_2, g_3, h_1, h_2,,h_i,,,h_l }
(g, g_1, g_2, g_3, h_1, h_2,,h_i,,,h_l ∈ G)
master-key z = g_2^{α}
master proxy key = { μ, ξ_1, ξ_2,,, ξ_i,,,, ξ_l,}
(注：PKG が、proxy-key 生成に関与し使用する。)
ここで、g ∈ G (random generator)
$g_1= g^{\alpha}$ ($\alpha \in Z_p$; random)
$g_3 = g^{\mu}$ ($\mu \in Z_p$; random)
$h_i = g^{\xi_i} (1 \le i \le l)$
($\xi_i \in Z_p$; 1≦i≦l ; random)

(2) KeyGen(d_{IDa}, IDa)

IDa = (I_1, I_2,,,,,I_j,,,,I_k) ∈ $(Zp^*)^k$ (1≦k≦l)

$$d_{IDa} = (g_2^{\alpha} \cdot (h_1^{I_1} \cdots h_k^{I_k} \cdot g_3)^r, g^r, h_{k+1}^r, , , h_l^r) \in G^{2+l-k}$$

r ∈ Zp (random)

(3) Encrypt(暗号化)

Encrypt(params, IDa, M)

$$= CT_a = (e(g_1, g_2)^s \cdot M, g^s, (h_1^{I_1} \cdots h_k^{I_k} \cdot g_3)^s) \in W \times G^2$$

s ∈ Zp (random)

(4) Decrypt(復号)

d_{IDa} = (a_0, a_1, b_{k+1}, ・ ・,b_l)

CTa = (A, B, C)

とすると、

Decrypt(d_{IDa}, CTa)

$$= \frac{A \cdot e(a_1, C)}{e(B, a_0)} = M$$

7.2 proxy key の設定

IDb = (J_1, J_2,,,J_i,,,J_m) ∈ $(Zp^*)^m$ (1≦m≦l)

$$d_{IDb} = (g_2^{\alpha} \cdot (h_1^{J_1} \cdots h_m^{J_m} \cdot g_3)^t, g^t, h_{m+1}^t, , , h_l^t) \in G^{2+l-m}$$

t ∈ Zp (random)

Alice の IDa と Bob の IDb と異なる階層の位置に存在し、proxy-key は、Bob の秘密鍵 d_{IDb} の要素の g^t を accept key として、PKG の所有する master proxy key をもとに生成する。(注；g^t の取得には、認証を必要とする。)

$pRK_{A\text{-}B} = (g^t)^{\tau}$

$$\tau = \frac{\mu + \sum_{i=1}^{m} \xi_i J_i}{\mu + \sum_{j=1}^{k} \xi_j I_j}$$

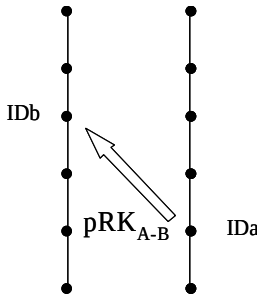

図 2 ID の階層構成

Figure2 ID Hierarchy

$$d_{ID_{A-B}} = (g_2^{\alpha} \cdot (h_1^{J_1} \cdots h_m^{J_m} \cdot g_3)^t, pRK_{A-B}, h_{m+1}^t, , , h_l^t) \in G^{2+l-m}$$

この $d_{IDA\text{-}B}$ より、

$$Decrypt(d_{ID_{A-B}}, CT_a) = M$$

8 まとめ

本稿は、proxy cryptographic 機能を有する ID-base 暗号の構成と、データを格納するファイル暗号としての有効性について検討したものである。暗号化データの復号権限を委譲する proxy-key を利用して複数のユーザ間でデータの共有が可能となる。この proxy-key は、ユーザの ID 情報をもとに生成されるが、ユーザ間の認証に関する over-head が存在せず、利便性の高い方式と考えられる。また、グループ編成や、Hierarchy 構成との組合せの可能性についても検討を行った。

参考文献

[1] M. Blaze, G. Bleumer, and M. Strauss. “Divertible protocols and atomic proxy cryptography”, In Proceeding of eurocrypto ’98, volume 1403, pages 127-144, 1998

[2] Y. dodis, and A. Ivan, “Proxy cryptography revisited.” In Proceedings of the Tenth Network and Distributed System Security Symposium, February 2003

[3] G, Ateniese, K. Fu, M. Green, and S. Hohenberger “Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage” full version accepted to appear in ACM Transaction on Information and System Security(TISSEC) Also in Cryptology eprint Archive, Report 2005/028

[4] Nuttapong Attrapadung, Yang Cui, David Galindo, Goichiro Hanaoka, Ichiro Hasuno, Hideki Imai, Kanta Matuura, peng Yang, Rui Zhang, “Relations Among Notions of Security for Identity Based Encryption Schemes. LATIN 2006 , 130-141

[5] D. Boneh, R. Canetti, S. Halevi, and J. Katz, “Chosen-Ciphertext Security from Identity-Based Encryption” June 13, 2006 To appears in SIAM Journal on Computing(SICOMP)

[6] D. Boneh, B. Lynn, and H.Shacham. “Short Signiture from the Weil Paring”. J. Cryptology 17(4) 297-319(2004)

[7] C. Gentry and A. Silverg. “Hierarchical Identity Based Cryptography.”.Proc.. of Asiacrypto’02, pages 548-566, 2002.

[8] Danfeng Yao, Nelly Fazio, Yevgeniy Dodis, and Anna Lysyanskaya. “ID-based encryption for complex hierarchies with applications to forward security and broadcast encryption.” In Bright Pfitzmann, editor, Proceedings of the ACM Conference on Computer and Comunications Security 2004, pages 354-63, 2004

[9] Yumiko Hanaoka, Goichiro Hanaoka, Junji Shikata, Hideki Imai, “Identity-Based Hierarchical Strongly Key-Insulated Encryption and Its Application”, ASIACRYPT 2005, 495-514

[10] D. Boneh, X. Bonyen, and E-J Goh, “Hierarchical Identity-Based Encryption With Constant-Size Ciphertexts” Adv. In Cryptology – Eurocrypto 2005, LNCS vol.3494, Springer-Verlag, pp440-456,2005 Full version available at http://eprint.iacr.org/2005/015