コンピュータセキュリティ　18−38
(2002. 7. 19)

楕円曲線上のペアリングを用いた不正者追跡法の拡張

光成　滋生†　渡辺　秀行††　吉田　真紀†††　境　隆一††††　笠原　正雄†††††

† (株) ピクセラ
〒 590-0985 大阪府堺市戎町 4 丁目 45 番 1 号
†† (株) アイビス
〒 450-0002　愛知県名古屋市中村区名駅 3 丁目 18 番 11 号新明ビル 4F
††† 大阪大学大学院情報科学研究科
〒 560-8531 大阪府豊中市待兼山町 1-3
†††† 大阪電気通信大学工学部
〒 572-8530 大阪府寝屋川市初町 18 丁目 8 番
††††† 大阪学院大学情報学部
〒 564-8511 大阪府吹田市岸部南 2 丁目 36 番 1 号

E-mail: †VEZ04653@nifty.com, ††watanabe@ibis.ne.jp, †††maki-yos@ist.osaka-u.ac.jp,
††††sakai@isc.osakac.ac.jp, †††††kasahara@utc.osaka-gu.ac.jp

あらまし　本稿では放送型コンテンツ配信における不正者追跡問題を考える．従来の配信法は，想定された人数以上の不正者の結託により追跡不可能な海賊版復号器を作製することが可能になるという問題点をもつ．筆者等は，既に楕円曲線上のヴェイユペアリングを用いることにより，この結託問題を解決する方式を提案した．本稿ではこの方式を拡張し，鍵漏洩の自己抑止力と非対称不正者追跡機能，および加入者排除機能をもつ方式を提案する．提案方式では放送量は従来方式より小さく，また加入者が何人結託したとしても結託者以外の個人鍵を生成することができないという拡張前の方式の特長を受けもつ．
キーワード　放送型コンテンツ配信，非対称鍵配付方式，限定排除，ヴェイユペアリング

An extension of traitor tracing scheme using Weil-pairing on elliptic curves

Shigeo MITSUNARI†, Hideyuki WATANABE††, Maki YOSHIDA†††, Ryuichi SAKAI††††, and Masao KASAHARA†††††

† Pixela Co., Ltd.
Ebisu-cho 4–45–1, Sakai-shi, Osaka-fu, 590-0985 Japan
†† Ibis Inc.,
4F Shinmei-bill 3–18–11, Mei-eki Nakamura-ku, Nagoya-shi, Aichi-ken, 450-0002 Japan
††† Dept. of Multimedia Engineering, Graduate School of Information Science and Technology, Osaka University, 1–3 Machikaneyamacho, Toyonaka, Osaka 560-8531 Japan
†††† Faculty of Engineering, Osaka Electro-Communication University
Hatsucho 18–8, Neyagawa-shi, 572-8530 Japan
††††† Faculty of Informatics, Osaka Gakuin University
Kishibeminami 2–36–1, Suita-shi, 564-8511 Japan

E-mail: †VEZ04653@nifty.com, ††watanabe@ibis.ne.jp, †††maki-yos@ist.osaka-u.ac.jp,
††††sakai@isc.osakac.ac.jp, †††††kasahara@utc.osaka-gu.ac.jp

Abstract　In the previous traitor tracing schemes, there exists an upper bound on the number of traitors who attack the schemes for certifying the security. We proposed one resolution of the problem using Weil-pairing on the elliptic curves. In this paper, we extend the scheme, yielding an asymmetric self-enforcement and revocation scheme.
Key words　traitor tracing, asymmetric, self-enforcement, revocation, collusion attack free, Weil-pairing

1. まえがき

本稿では, 配信者が加入者に予め個人鍵を有する復号器を配付しておき, コンテンツを暗号化して配信する放送型コンテンツ配信システムを考える. このシステムでは加入者による個人鍵の漏洩が特に問題となる. この問題を解決するために様々な機能や, その機能を実現するための方式が提案されてきた.

例えば加入者の個人鍵に各自の個人情報を含めることで漏洩に対する自己抑止力 (self-enforcement) をもたせる方式が提案されている [6]. また漏洩した個人鍵や, 個人鍵から作成された海賊版復号器が押収された場合に, その個人鍵を漏洩した加入者 (不正者) を特定することが可能な, つまり不正者追跡機能を持つ方式も提案されている [1, 3-6, 8-10, 12-17]. 不正者追跡機能をもつ方式として海賊版復号器を押収した場合, その復号器を解析して個人鍵を取り出すことによりその個人鍵を持つ加入者を特定する方式のほかに, 復号器の入力と出力の情報のみから加入者を特定することが可能なブラックボックス型方式も提案されている [1, 6, 8, 9, 12, 14-17].

さらに悪意ある配信者によって罪のなすりつけが行われないことを保証する非対称不正者追跡機能をもつ方式も提案されている [5-8, 12, 13, 15].

放送型コンテンツ配信システムに対して, 個人鍵の漏洩を抑止する機能のほかに加入者の排除機能を実現することも考えられている. 加入者排除とは, どの加入者の鍵も変更せずに暗号化コンテンツ配信の際のヘッダ情報のみを変更することにより, 特定の加入者だけが復号不可能にすることである. この機能により不正者や配信システムから退会した加入者を排除することができる.

有限体上の離散対数問題や ElGamal 暗号の困難さを安全性の根拠におくことにより [5] を初めとして上述の機能の一部あるいは全ての機能を実現させる方式が提案されている. しかし, いずれの方式においても不正者の結託人数の上限が予め想定された閾値以下では離散対数問題の困難さにより安全性が保証されているが, その閾値を超えると結託者が新たな個人鍵を作ることが可能になる. そのため個人鍵の漏洩に対する抑止力が失われる.

文献 [10] において筆者らは楕円曲線上における通常の Diffie-Hellman 問題の困難さよりやや強い仮定を置くことで, たとえ全加入者が結託したとしても新たな個人鍵を構成できない, つまり結託攻撃者の上限を想定しない方式を提案した. この方式はコンテンツ配信時のヘッダサイズと個人鍵のサイズの両方とも加入者の総数と不正者追跡の安全性を保証する結託人数の閾値に依存せず一定である.

本稿では [10] の方式に非対称不正者追跡機能と鍵漏洩自己抑止力を付加した方式を提案する. 更に加入者排除機能を加えた方式も提案する. 後者の方式は想定した閾値を超える結託攻撃を受けた場合, 排除は不可能になるが結託者が新たな個人鍵を作ることはできない. 従って押収した海賊版復号器から個人鍵が取り出せるという仮定の下で依然として不正者の追跡が可能である.

2. 準　　備

2.1 モデル

本稿で考えるシステムの参加者を以下に示す.

配信者: コンテンツを暗号化し配信する. 加入者に復号器を配付する際と, 押収した海賊版復号器をもとに不正者を特定し第三者 (調停者など) に証明する際に, 第三機関による署名付きの公開情報を利用する.

加入者: 暗号化されたコンテンツを受信し復号器を用いて復号する. 各加入者は配信者から各加入者ごとに異なる個人鍵を含む復号器が配付されている. 加入者のうち復号器に含まれる個人鍵を漏洩した者を**不正者**とよび, またコンテンツ配信対象者から除外される加入者を**排除対象者**とよぶ.

第三機関: PKI においてユーザとユーザの公開鍵との対応を保証し, 公開する. 暗号方式として楕円 ElGamal 暗号を利用する.

2.2 システムの機能

本稿で述べるコンテンツ配信システムは次の機能をもつ.

加入者限定配信機能: 加入者以外は海賊版復号器なしにコンテンツを復号できない.

***k*-加入者排除機能**: コンテンツ配信ごとに配信者は k 人以下の排除対象者が復号できないようにコンテンツを暗号化できる.

鍵漏洩の自己抑止力: 配信者は加入者の個人鍵の一部を, その加入者が秘密にしたい数値に設定することができる.

***t*-不正者追跡機能**: 海賊版復号器が t 人以下の不正者の個人鍵から作成されていた場合, その海賊版復号器を押収することで, その復号器の作成に関与した不正者の少なくとも 1 人を特定できる.

不正者捏造防止機能: 配信者がある加入者を不正者として第三者に立証できるのは, その加入者が本当に不正者であるとき, そのときのみであり, 立証は不正者の協力無しにできる. なお不正者追跡可能な不正者捏造防止機能を**非対称不正者追跡機能**とよぶ.

2.3 表　　記

配信者を $\mathcal{S}$, 加入者の総数を n, 加入者の集合を $\Phi = \{1, ..., n\}$, 第三機関を $\mathcal{A}$ とする. また加入者 i の $\mathcal{A}$ により認証された秘密情報を u_i とする. 提案方式は有限体上の楕円曲線上で構築される群を利用するため以下のパラメータを設定する. これらの表記は本稿全体で使われる.

E : 標数 p の有限体 $\mathbf{F}_q$ 上の楕円曲線,

m : $m \neq p, m > n$ となる素数,

$E[m]$: E の m 等分点のなす群,

s : $E[m] \subset E(\mathbf{F}_{q^s})$ となる最小の自然数,

$e_m(\cdot,\cdot)$: $E[m]$ 上の Weil-pairing.

3. 非対称不正者追跡機能と鍵漏洩の自己抑止力をもつコンテンツ配信法

本節では, 文献[10] で提案した不正者追跡機能をもつコンテンツ配信法を拡張し, 非対称不正者追跡機能と不正の自己抑止力を付加した配信法を提案する. なお提案法では Oblivious Polynomial Evaluation プロトコルを利用している.

Oblivious Polynomial Evaluation(OPE)

OPE プロトコルとは多項式 $g(x)$ を持つ A と, ある整数 u を持つ B との間の 2 者間プロトコルであり次の条件を満たす:

- A は u の情報を得ることができない.
- B は $g(u)$ の値を取得することができるが, それ以外の $g(x)$ に関する情報を得ることはできない.

文献[2][11] で, 効率の良い OPE プロトコルが提案されている. ただしプロトコルのパラメータの取り方によって, 効率よく破ることができることが知られており [2], 利用の際には 上述の条件を満たす (安全となる) ようにパラメータを選択する必要がある.

本稿では, 安全で効率のよい OPE プロトコルが存在すると仮定する.

3.1 提　案　法

システムの初期化

配信者 $\mathcal{S}$ は 2 次元 $\mathbf{Z}/m\mathbf{Z}$ ベクトル空間 $E[m]$ の基底 $\langle P, R\rangle$ を 1 つとる. ただし $R \in E(F_q)$ とする. 次に $\mathbf{Z}/m\mathbf{Z}^*$ の元 a をランダムにとる. そして (a, P) を秘密に保持し $(R, e_m(P,R))$ を公開する. 暗号化鍵は $(R, aR, e_m(P,R))$ である.

第三機関 $\mathcal{A}$ は PKI における各加入者 i の秘密鍵 $u_i \in \mathbf{Z}/m\mathbf{Z}^*$ に対応する公開鍵 u_iR と i の識別子のリスト (i, u_iR) に署名をつけて一般に公開する.

鍵の生成と配付

加入者 i は安全な通信路を用いて以下の方法で $\mathcal{S}$ から個人鍵 $(u_i, \frac{1}{u_i+a}P)$ を受け取る.

1. $\mathcal{S}$ は加入者 i 用に $\mathbf{Z}/m\mathbf{Z}^*$ の元 b_i, c_i をランダムに選び $g_i(x) := b_ix + ab_i$ とする.
2. 加入者 i は $g_i(x)$ を持つ $\mathcal{S}$ との間で OPE プロトコルを実行することにより $g_i(u_i) = b_i(u_i + a)$ を取得する.
3. $\mathcal{S}$ は c_iP を加入者 i に送信する.
4. 加入者 i は

$$\frac{1}{g_i(u_i)} \cdot c_iP = \frac{c_i}{b_i(u_i+a)}P$$

を計算し $\mathcal{S}$ に送信する.

5. $\mathcal{S}$ は

$$K_i := \frac{b_i}{c_i} \cdot \frac{c_i}{b_i(u_i+a)}P = \frac{1}{u_i+a}P$$

を計算する. 第三機関 $\mathcal{A}$ のリストから i に対する u_iR を取得し

$$e_m(K_i, u_iR + aR) = e_m(P, R)$$

の等号が成立するかを調べて $K_i = \frac{1}{u_i+a}P$ となることを確認する. 成立すれば K_i を加入者に送信する.

6. 加入者は

$$e_m(K_i, u_iR + aR) = e_m(P, R)$$

の等号が成立するかを調べる. 確認できれば (u_i, K_i)=$(u_i, \frac{1}{u_i+a}P)$ を個人鍵とする.

コンテンツの暗号化

$\mathcal{S}$ は $\mathbf{Z}/m\mathbf{Z}^*$ の元 r をランダムに選び $Q = rR$ とする. $r(aR) = aQ$ を計算し, (Q, aQ) をヘッダ, $e_m(P,R)^r = e_m(P,Q)$ をセッション鍵としてコンテンツを暗号化し配信する.

コンテンツの復号

加入者 i は個人鍵 (u_i, K_i) とヘッダ (Q, aQ) から以下の計算,

$$e_m(K_i, u_iQ + aQ) = e_m(P, Q)$$

によりセッション鍵を取得しコンテンツを復号する.

不正者の特定

押収した海賊版復号器から個人鍵 (u_i, K_i) を取り出すことができ, かつ $\mathcal{A}$ によって公開されているリストにおいて $u_iR = uR$ となる (i, u_iR) が存在すれば加入者 i を不正者として特定する.

第三者への立証

押収した海賊版復号器から取り出された個人鍵 (u_i, K_i) の u_i と $\mathcal{A}$ により保証された (i, u_iR) を提示することで第三者に i が不正者であることを示す.

3.2 安全性

提案法の安全性の根拠となる問題

提案方式は $E[m]$ における楕円 ElGamal 問題の困難さを仮定する. これは Weil-pairing による $\mathbf{F}_{q^s}$ 内の像における有限体の ElGamal 問題の困難さの仮定も含んでいる. さらにそれらの混在型問題の困難さも仮定する.

まず問題の定義を行う. S, T を $e_m(S,T) \neq 1$ を満たす $E[m]$ の一般の元とし x, y を $\mathbf{Z}/m\mathbf{Z}$ の一般の元とする.

問題 1. $\{T, x\}$ を未知とし $\{e_m(S,T), S, xS\}$ が与えられたときに $e_m(S,T)^x$ を求める.

問題 2. $\{x, y\}$ を未知とし $\{S, xS, yS\}$ が与えられたときに xyS を求める.

問題 3. x を未知とし $\{S, xS, T, xT\}$ が与えられたときに x を求める.

問題 4(k-$wDHA$). x を未知とし $\{S, xS, \ldots, x^kS\}$ が与えられたときに $x^{-1}S$ を求める.

問題 5(k-$wDHA'$). x を未知とし $\{S, xS, \ldots, x^kS\}$ および $\{T, xT\}$ が与えられたときに $x^{-1}S$ を求める.

$k = 1$ のときの問題 4 と 問題 2 の 同値性は [10] の Lemma 3.4 で示される. また 1-$wDHA'$ の困難さを仮定すると 問題 3 は困難である.

加入者限定配信機能

[**補題** 3.21] 問題 1 の困難さを仮定すると海賊版復号器なしに非加入者は復号できない.

証明 定義から明らか. □

t-不正者追跡機能

以降では t 人の不正者の集合を $\mathcal{C} = \{i_j : 1 \leqq j \leqq t\} \subseteqq \Phi$ とする.

[**補題** 3.22] a, P を未知として $\{(u_i, K_i) : i \in \mathcal{C}\}$ が与えられたときに, ある u $(u \notin \{u_i : i \in \mathcal{C}\})$ に対する $\frac{1}{u+a}P$ を求める問題は $(t-1)$-$wDHA$ を解くことと同値である.

証明 文献 [10] の Theorem 3.5 で示されている. □

[**定理** 3.23] a, P, $\{(b_i, c_i) : i \in \mathcal{C}\}$ を未知として R, aR および $\{(u_i, K_i, c_iP, b_i(u_i+a)) : i \in \mathcal{C}\}$ が与えられたときに, ある u $(u \notin \{u_i : i \in \mathcal{C}\})$ に対する $\frac{1}{u+a}P$ を求める問題 ($\mathbf{Forge}_t$ とする) は $(t-1)$-$wDHA'$ を解くことと同値である.

[定理 3.23] を証明するために, 次の補題を示す.

[**補題** 3.24] 補題中の $\mathbf{Forge}_t$ を解くことは次の問題 $\mathbf{Forge}_t'$ を解くことと同値である.

$\mathbf{Forge}_t'$: a, P を未知として R, aR および $\{(u_i, K_i) : i \in \mathcal{C}\}$ が与えられたときに, ある u $(u \notin \{u_i : i \in \mathcal{C}\})$ に対する $\frac{1}{u+a}P$ を求める.

証明 問題 $\mathbf{Forge}_t$ の仮定が与えられたときに b_i を $b_i = (u_i + a)^{-1}$ となる未知変数, c_i を $c_iP = K_1$ となる未知変数とみなすことで $\mathbf{Forge}_t'$ の仮定条件が得られ $\mathbf{Forge}_t$ を解くことができる. 逆は自明である. □

定理の証明 証明のアウトラインを述べる. 文献 [10] の Theorem 3.5 の証明において問題 4 の x と $\mathbf{Forge}_t$ の a との間に $x = a + u$ という関係があることに注意することで [定理 3.23] を示すことができる. □

3.1 節の鍵生成と配付における 5 で, 配信者 $\mathcal{S}$ は加入者 i に K_i を送信する前に $K_i = \frac{1}{u_i+a}P$ であるか否かを判定し $K_i \neq \frac{1}{u_i+a}P$ であれば送信しない. これより, 加入者 i に配付される個人鍵は必ず $(u_i, \frac{1}{u_i+a}P)$ となる. すなわち次の定理が成り立つ.

[**定理** 3.25] OPE プロトコルの安全性と $(t-1)$-$wDHA'$ の困難さと, 押収された海賊版復号器の中から個人鍵をそのままの形で取り出せるという仮定の下で提案方式は t-不正者追跡機能をもつ.

特に $(n-1)$-$wDHA'$ の困難さを仮定すると, 押収された海賊版復号器の中から個人鍵をそのままの形で取り出せるという仮定の下で結託者の人数にかかわらず不正者追跡が可能である.

結託者が与えられた個人鍵をそのまま用いずにコンテンツを復号する方法については検討中である. 例えばもし結託することで P を入手することができれば個人鍵を使わずにヘッダ情報の Q を直接用いて $e_m(P,Q)$ を計算することができる. したがって P を含む海賊版復号器を作成した場合, その復号器を押収しても不正者を追跡することはできない. しかし次の補題により $(t-1)$-$wDHA$ の困難さを仮定すると t 人の結託者 $\mathcal{C}$ では P の計算は困難である.

[**補題** 3.26] $\{(u_i, K_i) : i \in \mathcal{C}\}$ が与えられたときに P を求める問題は $(t-1)$-$wDHA$ を解くことと同値である.

証明 補題 3.22 と同様に示すことができる. □

非対称不正者追跡機能

問題 3 の困難さと OPE の安全性を仮定すると $\mathcal{S}$ は u_i を求めることができない. よって $\mathcal{S}$ は, 不正者ではない加入者 i の個人鍵 (u_i, K_i) を入手できないため, 第三者に立証できない.

鍵漏洩の自己抑止力

[定理 3.23] より OPE プロトコルの安全性と $(t-1)$-

$wDHA'$ の困難さを仮定すると各加入者は $\mathcal{S}$ から与えられた (u_i, K_i) 以外の (u_i', K_i') を入手できない．つまり加入者 i は u_i として $\mathcal{A}$ によって保証された PKI における公開鍵に対応する秘密鍵しか使えない．

3.3 配信効率

セッション鍵のサイズを I ($\sim$ 1024bit) とする．従来の t-不正者追跡機能をもついずれの方法においてもコンテンツ配信の際のヘッダサイズは $O(tI)$ であった．3.2 節で定義した問題と OPE プロトコルの安全性の仮定の下で任意の t $(t \leq n)$ について t-不正者追跡機能をもつ本提案方式ではヘッダサイズと個人鍵のサイズはいずれも $2I$ である．

4. k-加入者排除機能をもつ配信法

前節の方式を拡張し k-加入者排除機能も備えた方式を提案する．

4.1 提案法

システムの初期化

3.1 節のシステムの初期化処理を行い，更に配信者 $\mathcal{S}$ は k 次の $\mathbf{Z}/m\mathbf{Z}$ 係数多項式 $f(x) = \sum_{i=0}^{k} a_i x^i$ をランダムに選ぶ．暗号化鍵を $(R, aR, e_m(P,R), f(0)aR, a_0R, \ldots, a_kR)$ とする．

鍵の生成と配付

3.1 節の鍵の生成と配付を行う．そのとき関数 H を

$$H : \mathbf{Z}/m\mathbf{Z} \ni u \mapsto (\text{点 } uR \text{ の } x \text{ 座標}) \in \mathbf{Z}/m\mathbf{Z}$$

と定義し，配信者 $\mathcal{S}$ は各加入者 i に K_i を配付する際に $f(H(u_i))$ も送信する．各加入者 i は $(u_i, K_i, f(H(u_i)))$ を個人鍵とする．

関数 H は楕円曲線上の離散対数問題の困難さを仮定すると一方向性関数となる．ただし

$$\begin{aligned} & H(u) = H(u') \\ \Longleftrightarrow\ & uR = u'R \text{ または } uR = -u'R \\ \Longleftrightarrow\ & u = u' \text{または} u = -u' \end{aligned}$$

という性質をもつため，システムの初期化において $\mathcal{A}$ はユーザの秘密鍵の集合 $\{u_i\}$ の中で $u_i = -u_j$ となる i, j $(i \neq j)$ が存在しないようにする必要がある．そのためには i, j $(i \neq j)$ に対して $\mathcal{A}$ は $u_iR \neq -u_jR$ であることを検証すればよい．

排除を伴わないコンテンツ配信

前章と同様に行う．すなわち $\mathbf{Z}/m\mathbf{Z}^*$ の元 r をランダムに選び $Q = rR$ とする．(Q, aQ) をヘッダとし $e_m(P,Q)$ をセッション鍵としてコンテンツを暗号化し配信する．復号も同様である．

排除を伴うコンテンツ配信

排除対象者の集合を $\mathcal{R}$ とする．なお $0 < |\mathcal{R}| \leq k$ である．

- **コンテンツの暗号化**

配信者 $\mathcal{S}$ は $\mathcal{R}$ を排除するために，以下のようにコンテンツを暗号化する．

1. $\mathcal{A}$ の公開情報にある u_iR $(i \in \Phi)$ から $H(u_i)$ を計算し $\Psi = \{H(u_i) : i \in \Phi\}$, $\Lambda = \{H(u_i) : i \in \mathcal{R}\}$ とする．
2. $\mathbf{Z}/m\mathbf{Z}^* \setminus \Psi$ から $k - |\mathcal{R}|$ 個の元をランダムに選び，これらの元の集合を Θ とする．$\Lambda \cap \Theta = \emptyset$ より $|\Lambda \cup \Theta| = k$ となる．$\Lambda \cup \Theta = \{v_1, \ldots, v_k\}$ とする．
3. $\mathbf{Z}/m\mathbf{Z}^*$ の元 r をランダムに選び $Q = rR$ とする．$Q, r, \Lambda \cup \Theta$ および暗号化鍵の一部 $(aR, f(0)aR, a_0R, \ldots, a_kR)$ から

$$(Q, f(0)aQ, v_1, \ldots, v_k, f(v_1)Q, \ldots, f(v_k)Q)$$

を生成しヘッダとする．なお $v \in \mathbf{Z}/m\mathbf{Z}^*$ に対して $f(v)Q$ は r と $a_0R, \ldots, a_kR$ から $r(a_0R + va_1R + \cdots + v^k a_kR) = f(v)Q$ により計算できる．$f(0)aQ$ は $r(f(0)aR)$ により計算できる．
4. $e_m(P, r(a_0R)) = e_m(P, f(0)Q) = e_m(P,Q)^{f(0)}$ をセッション鍵としてコンテンツを暗号化する．

- **コンテンツの復号**

排除対象者以外の加入者 i $(i \notin \mathcal{R})$ は，個人鍵 $(u_i, K_i, f(H(u_i)))$ とヘッダ $(Q, f(0)aQ, v_1, \ldots, v_k, f(v_1)Q, \ldots, f(v_k)Q)$ および公開されている R から次のようにセッション鍵を求める．

1. R と u_i から $v = H(u_i)$ を求める．$i \notin \mathcal{R}$ より $v \notin \Lambda \cup \Theta = \{v_1, \ldots, v_k\}$.
2. $f(v)$ とヘッダにある Q から $f(v)Q$ を求める．
3. $\{(v_i, f(v_i)) : 1 \leq i \leq k\}$ と $(v, f(v)Q)$ から Lagrange 補間を用いて $f(0)Q$ を求める．
4. 個人鍵にある u_i, K_i と，ヘッダにある $f(0)aQ$ より

$$e_m(K_i, u_i f(0)Q + f(0)aQ) = e_m(P,Q)^{f(0)}$$

を計算してセッション鍵を取得する．

排除対象者 j は，ヘッダ内の $\{v_1, \ldots, v_k\}$ に $v = H(u_j)$ が含まれるため $f(0)Q$ を計算できない．

不正者の特定と立証

前章と同様に行うことができる．

4.2 安全性

$k+1$ 人の不正者が結託しない限り $f(x)$ を求めることができないことは従来の方法と同様に示すことができる．$k+1$ 人以上で結託すると $f(x)$ が求められ排除は不可能となる．しかしこの場合でも結託した不正者以外の加入者 i の個人鍵 (u_i, K_i) は計算で

きない．そのため依然として各自の個人鍵を使わない限り復号はできない．

3.2 節で示した問題 1-5 の困難さと利用する OPE プロトコルの安全性を仮定することで 4.1 節の提案方式が加入者限定配信機能，非対称不正者追跡機能，鍵漏洩の自己抑止力をもつことは 4.2 節と同様に証明できる．

4.3 配信効率

セッション鍵のサイズを I とすると，本提案方式における個人鍵のサイズは $3I$ であり，ヘッダサイズは $2(I+1)k$ である．このヘッダサイズは [15] で提案された鍵漏洩の自己抑止力および k-排除機能をもつ非対称不正者追跡法における $3Ik$ より小さい．

5. その他の拡張

本章では 4 章で提案した方式に，従来方式を利用してさらに機能を付加するためのアイデアを述べる．

5.1 ブラックボックス型不正者追跡機能

ブラックボックス型 t-不正者追跡機能とは，押収された海賊版復号器が最大 t 人の不正者の結託により構成されていた場合，その復号器の入出力のみからその復号器の作成に関与した不正者の少なくとも 1 人を特定できる機能である．

$\mathcal{S}$ が最大 t 人までを自由に排除できることを利用すると [8], [9], [16], [17] と同様ブラックボックス型 t-不正者追跡が可能となる．また [15], [17] と同様に係数を変更した $f(x)$ を用いて作成したヘッダを利用するブラックボックス型不正者追跡も可能である．

5.2 排除対象者人数を配信時に決定できる機能

4 章で提案した方式は，システムの初期化時に安全に排除できる最大人数 k をあらかじめ決定しておく．配信時のヘッダサイズは排除しない場合は例外的に小さくできるが，排除を行う場合は排除人数に係わらず $O(k)$ で一定であり，また排除人数が k を超えることができない．文献 [8] では，システム初期化時に安全に排除できる加入者の最大人数を決めておき，配信時には排除可能な人数を任意に設定できる方式が提案されている．ヘッダサイズは排除人数に応じて動的に変わる．

文献 [8] の方式において利用する群を $E[m]$ の部分群とすることで [8] の機能を本稿で提案した方式に取り入れることができる．すなわち，我々の提案方式に排除対象者の人数を配信時に任意に決定できる機能を付加することができる．

6. まとめ

本稿では文献 [10] で提案した方式を拡張することで結託人数に対する閾値をもたず，加入者排除機能と鍵漏洩自己抑止力かつ非対称不正者追跡機能をもつコンテンツ配信システムを構成した．このため従来提案されてきた手法はこの方式でも同様に議論することができる．さらに，ブラックボックス型の不正者追跡機能と，排除対象人数を配信時に決定できる加入者排除機能を付加するためのアイデアを示した．これらの拡張後でも結託人数に係わらず個人鍵を計算できないという特長は受け継がれている．

文献

[1] D. Boneh and M. Franklin, "An Efficient Public Key Traitor Tracing Scheme," Crypto'99, LNCS 1666, pp. 338–353, 1999.

[2] D. Bleichenbacher and P. Q. Nquyen, "Noisy Polynomial Interpolation and Noisy Chinese Remaindering," EUROCRYPT 2000, LNCS 1807, pp. 53–69, 2000.

[3] B. Chor, A. Fiat and M. Naor, "Tracing traitors," Crypto'94, LNCS 839, pp. 257–270, 1994.

[4] B. Chor, A. Fiat, M. Naor and B. Pinkas, "Tracing Traitors," IEEE Trans. on Information theory, vol. 46, No. 3, pp. 893–910, May 2000.

[5] K. Kurosawa and Y. Desmedt, "Optimum Traitor Tracing and Asymmetric Schemes," EUROCRYPT'98, LNCS 1403, pp. 145–157, 1998.

[6] H. Komaki, Y. Watanabe, G. Hanaoka and H. Imai, "Efficient Asymmetric Self-Enforcement Scheme with Public Traceability," PKC 2001, LNCS 1992, pp. 225–239, 2001.

[7] 駒木寛隆, 渡邊裕治, 花岡悟一郎, 今井秀樹, "検証可能な紛失多項式評価," SCIS2001, pp. 471–476, 2001.

[8] T. Matsushita, "Efficient Black-box Tracing with Revocation," SICS 2002, pp. 739–744, 2002.

[9] T. Matsushita, H. Imai, "Black-box Tracing with Revocation of Subscribers," SCIS 2001, pp. 207–212, 2001.

[10] S. Mitsunari, R. Sakai and M. Kasahara, "A New Traitor Tracing," IEICE TRANS. Fundamentals, vol. E85-A, No. 2, pp. 481–484, 2002.

[11] M. Naor and B. Pinkas, "Oblivious Transfer and Polynomial Evaluation," STOC'99, pp. 245–254, 1999.

[12] S. Okamura, M. Yoshida and T. Fujiwara, "Validatable Revocation and Black-Box Traitor Tracing Scheme," SCIS 2002, pp. 733–738, 2002.

[13] B. Phitzmann, "Trials of Traced Traitors," Information Hiding, LNCS 1174, pp.49–64, 1996.

[14] D. R. Stinson and R. Wei, "Key Preassigned Traceability Schemes for Broadcast Encryption," SAC'98, LNCS 1556, pp. 144–156, 1998.

[15] Y. Watanabe, G. Hanaoka and H. Imai, "Efficient Asymmetric Public-Key Traitor Tracing without Trusted Agents," CT-RSA 2001, LNCS 2020, pp. 392–407, 2001.

[16] M. Yoshida and T. Fujiwara, "An Efficient Traceability Scheme for Broadcast Encryption," ISIT 2001, pp. 463, 2001.

[17] M. Yoshida and T. Fujiwara, "A Subscriber-Excluding and Traitor-Tracing Broadcast Distribution System," IEICE Trans. Fundamentals, vol. E84-A, No. 1, pp. 247–255, 2001.