社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2008－CSEC－42（33）
2008 / 7 / 25

あるIDベース放送暗号の端末追跡能力について

境　　隆一†

† 大阪電気通信大学情報通信工学部　〒572-8530 大阪府寝屋川市初町 18-8
E-mail: †sakai@isc.osakac.ac.jp

あらまし　IDベース放送暗号[7]は，従来にない幾つかの利点を有している．例えば各端末をID情報等の任意の情報で管理できる他，登録端末の総数が増えなければ，登録と無効化を繰り返し行うことが可能となっている．ただし，登録端末数に比例した公開鍵と演算量が必要である．この登録端末に比例した公開鍵と演算は，登録端末の集合が変る度に必要であり，その集合に合せた演算を行う．本稿では，この特性を生かして，MSK不正端末追跡法[1]への線形結託攻撃が困難となるような方式を提案する．ただし，提案方式はリボーク機能は有していないので，リボーク機能は鍵更新作業等で行う等，他の対策が必要である．

キーワード　IDベース，放送暗号，不正端末追跡，結託耐性

Traitor Tracing from ID based Broadcast Encryption

Ryuichi SAKAI†

† Faculty of Information and Communication Engineering, Osaka Electro-Communication University, Hatsucho 18-8, Neyagawa-shi, Osaka, 572-8530 Japan
E-mail: †sakai@isc.osakac.ac.jp

Abstract　ID based broadcast encryption scheme based on MSK-TT [1] key setting(ID-BE-MSK) [7] has several new advantages. For example, every receiver can be managed by their identity information and the system can continuously subscribe and revoke receivers, when the total number of receivers is bounded. On the other hand, the system requires many public keys and many operations which is proportional to a number of receivers. These many public keys and operations are required when the set of the receivers is changed. This property is one of the disadvantage of ID-BE-MSK. Based on this property, this paper presents new traitor tracing scheme with resistance against the collusion attack which uses the keys linear combination of the private keys.

Key words　identity based, broadcast encryption, traitor tracing, collusion resistance

1. まえがき

IDベース放送暗号[7]は，従来にない幾つかの利点を有している．例えば各端末をID情報等の任意の情報で管理できる他，登録端末の総数が増えなければ，登録と無効化を繰り返し行うことが可能となっている．ただし，登録端末数に比例した公開鍵と演算量が必要である．この登録端末に比例した公開鍵と演算は，登録端末の集合が変る度に必要であり，その集合に合せた演算を行う．

本稿では，この特性を生かして，光成-境-笠原によって提案されたMSK不正端末追跡法[1]への線形結託攻撃が困難となるような方式を提案する．提案する方式は，この特性により，結託端末においても変化するヘッダ情報の集合に合わせて中間復号データを作成する必要があり，その際に結託端末のID情報を回避することができないようにしている．また本提案方式は，例えばランダムに与えた1000ビット程度の2進系列が2つあった場合に，その内の300ビット以上は非常に高い確率（$> 1 - 2^{-123}$）で一致することを利用している．本提案方式の特徴を以下に列挙する．

（1） ID情報は1000ビット程度の2進系列（ベクトル）I_iに変換される．

（2） 暗号化においては1000ビット程度のランダムな2進系列Rを利用する．

（3） I_iとRの異なるビットが700ビット以上となるとセッション鍵の復号に失敗するが，その確率は2^{-123}以下である．

（4） ランダム系列を利用しているので，結託者はそれを予測できず，追跡不可能な不正端末を偽造することができない．

本稿では，2章でMSK不正端末追跡法を，3章でIDベース放送暗号を記述し，それぞれの方式に対しての結託攻撃について考察する．そして4章でIDベース放送暗号に基づいて構成

した新しい不正端末追跡法を提案する．また，5 章では 4 章の方式よりも若干効率の良い構成法を示し，6 章では，結託攻撃に対して，より耐性の高いと期待される修正方式を提案する．

2. MSK 不正端末追跡法

本章では，MSK 不正端末追跡法 [1] を再掲する．本方式は，結託端末の秘密鍵の線形結合を端末鍵とすることによって，追跡を逃れる不正端末を構成するという結託攻撃が可能である．しかし，後に提案された境-笠原 ID ベース公開鍵暗号方式と秘密鍵が同一であり，双線形を用いた暗号方式における基本的アイデアを含んでいる．この境-笠原 ID ベース公開鍵暗号方式は，効率の良い 2 つの ID ベース公開鍵暗号の中で，2 つ目に提案された方式である．本 MSK 不正端末追跡法は，端末内の復号鍵を抽出し，そこに含まれている端末の ID 情報を検出することによって不正に複製された端末の複製元を特定する方式である．

2.1 パラメータ設定

位数 n の 2 つの乗法群 G_1 と群 G_2 に対して，G_1 から G_2 への双線形写像 $e_n(*,*)$ $(G_1 \times G_1 \to G_2)$ を用いる．具体的には，$e_n(*,*)$ はいわゆる distortion 写像を導入した修正ペアリング（対称ペアリング）であり，この場合，G_1 は楕円曲線上の n ねじれ点のなす加法群であるが，最近の記述に合わせて G_1 も乗法群で表現することにする．鍵生成センタは効率の良く双線形写像を計算できる群 G_1, G_2 を選び，双線形写像の計算に必要な全ての情報を公開する．ここでは簡単のため，n は素数とする(注1)．

2.2 鍵 設 定

鍵生成センタは秘密の乱数 $s \in \mathbb{Z}_n$ を選び，秘密の多項式として

$$f(x) = s + x,$$

を設定する．この多項式は 1 次以上の任意の次数の多項式に設定することが可能であるが，ここでは最も効率の良い 1 次式とする．また，群 G_1 からランダムに元 g, g_1 を選ぶ．

2.3 公開鍵の作成

センタはシステムの秘密鍵として，$s(\in \mathbb{Z}_n)$ をランダムに選び，以下のような公開鍵を生成する．

$$e = (e_0, e_1) = (g_1, g_1^s),$$

$$y = e_n(g, g_1).$$

ここで，e および y は暗号化鍵 P_{ENC} である．

2.4 端末 i の復号鍵 (秘密鍵) k_i の生成

鍵生成センタは秘密の多項式

$$f(X) = X + s,$$

を定める(注2)．そして端末 ID_i の復号鍵 k_i として鍵生成センタは端末 ID_i の復号鍵 k_i として

$$k_i = g^{f(I_i)^{-1}} = g^{(I_i+s)^{-1}},$$

を計算する．ただし，$I_i = h(ID_i) \in \mathbb{Z}_n$ であり，$h()$ は衝突耐性ハッシュ関数である．以降では簡単の為 (特に混乱の無い限り)，ID_i を I_i と記述する．

2.5 暗 号 化

放送事業者は乱数 $k \in Zn$ を生成し，これと公開鍵および登録端末の ID，$I_j \in S$ を用いてヘッダ情報

$$H = (H_0, H_1) = (e_0^k, e_1^k) = (g_1^k, g_1^{sk}),$$

を作成する．このヘッダ情報に対するセッション鍵

$$K_S = y^k = e_n(g, g_1)^k,$$

を計算し，これと共通鍵暗号の暗号化関数 Enc() を用いてメッセージ m を以下のように暗号化する．

$$C = \mathrm{Enc}(K_S, m).$$

放送事業者は，暗号文 C にヘッダを付けて (H, C) を放送する．

2.6 復 号

正規端末は，ヘッダ H および自身の秘密鍵を用いて以下のようにセッション鍵 K_S を復号する．

$$K_S = e_n(k_i, H_0^{I_i} H_1) = e_n(g^{(I_i+s)^{-1}}, g_1^{(I_i+s)k}) = e_n(g, g_1)^k.$$

復号されたセッション鍵と共通鍵暗号の復号関数 Dec() を用いて暗号文 C を復号し，メッセージ m を復号する．

2.7 結 託 攻 撃

本不正端末追跡法に対して，以下のような結託攻撃が可能である．ここでは簡単のため結託者を $ID_1, ID_2, \cdots, ID_M$ とする．結託鍵 $\tilde{k}$ は $\sum_{i=1}^{M} \lambda_i = 1$ を満たす任意の $\lambda_i \in \mathbb{Z}_n$ $(i < M$ をランダムに選択可能$)$ を用いて以下のように生成する．

$$\tilde{k} = (\tilde{k}_0, \tilde{k}_1) = \left(\prod_{i=1}^{M} k_i^{I_i \lambda_i}, \prod_{i=1}^{M} k_i^{\lambda_i} \right),$$

を計算し，この鍵を不正端末の復号鍵とする．この鍵を用いてヘッダ情報からセッション鍵を復元するには，以下の 2 つのペアリング演算を実行する．

$$e_n(\tilde{k}_0, H_0) e_n(\tilde{k}_1, H_1) = e_n(\prod_{i=1}^{M} k_i^{I_i \lambda_i}, g_1) e_n(\prod_{i=1}^{M} k_i^{\lambda_i}, g_1^s)$$

$$= \prod_{i=1}^{M} \left\{ e_n(k_i, g_1^{I_i}) e_n(k_i, g_1^s) \right\}^{\lambda_i} = K_S^{\sum_{i=1}^{M} \lambda_i} = K_S.$$

この不正端末内から復号鍵 $\tilde{k}$ を抽出できたとしても，ランダムなデータ λ_i が指数部にあるため，複製元の ID 情報を特定することができない．しかし，センタの秘密の多項式 $f(X)$ の次数を d 次とすると，不正端末に必要な復号鍵は $d+1$ 個になり，復号に必要な演算はペアリング演算が $d+1$ 回となる．d を大きな値に設定し，鍵更新を上手く運用することによって，この結託攻撃を困難にするようにすることも検討されている [5]．また，境-笠原 ID ベース公開鍵暗号方式を用いて，各端末の鍵更新を行うようにすれば，不正端末といえども，鍵更新の際に複製元の復号鍵を必要とするために結託攻撃が成立する期間を鍵更新を行うまでに限定することも可能である．

(注1)：ここで提案する各暗号方式は各パラメータを適切に設定することにより Weil, Tate ペアリングのように非対称ペアリングでも構成可能である．

(注2)：$f(X)$ は X を多変数 $X = (X_0, X_1, \cdots, X_d)$ として $f(X) = X_0 + sX_1 + \cdots s^i X_i$ のように定義することもできる

3. ID 情報に基づく放送用暗号方式

本章では，ID 情報に基づく放送暗号方式を再掲する．この方式では各端末は通し番号ではなく端末固有の ID 情報を用いることが可能であり，暗号に必要な公開鍵をより柔軟に扱うことができる．

3.1 特　　徴

以下に本稿で提案する ID 情報に基づく暗号方式の特徴を列挙する．

（1） 秘密鍵は [1] および [2] の方式と同じである．

（2） 公開鍵は暗号化用と復号用で約 N 個づつである（N は登録端末の数以上の数，BGW 方式は $2N+1$ 個）

（3） ID ベース方式である．

（4） 登録の抹消，追加を行っても登録端末数が N を越えなければ鍵を更新する必要がない (BGW 方式は鍵の更新が必要である)．

（5） 登録端末の数の増加に応じて公開鍵を増加させることができる．

（6） BGW 方式に比べて計算量が若干増加する．

本方式の優れている点は上述の 3.,4.,5. であり，特に 4. は興味深い．

3.2 鍵設定および端末 i の秘密鍵 k_i の生成

前章の不正端末追跡法と同じものを利用する．

3.3 公開鍵の準備

センタはシステムの秘密鍵として，s を既に選んでいるが，これに加えて $r(\in \mathbb{Z}_n)$ をランダムに選び，$g_r = g_1^r$ とする．そして，これらの値を用いて以下のような公開鍵を生成する．

$$e = (e_0, e_1, \cdots, e_n) = (g_r, g_r^s, \cdots, g_r^{s^N}),$$
$$d = (d_1, d_2, \cdots, d_{N-1}) = (g_1^s, g_1^{s^2}, \cdots, g_1^{s^{(N-1)}}),$$
$$v = g^r, \quad y = e_n(g, g_r) = e_n(g, g_1)^r.$$

ここで，e，v および y は公開暗号化鍵 P_{ENC}，d は公開復号鍵 P_{DEC} である．

3.4 暗　号　化

放送事業者は乱数 $k \in \mathbb{Z}_n$ を生成し，これと公開鍵および登録端末の ID，$I_j \in S$ を用いてヘッダ情報

$$H = (H_1, H_2, S) = (g_r^{k\prod_{I_j \in S}(s+I_j)}, v^k, S),$$

を作成する(注3)．このヘッダ情報に対するセッション鍵

$$K_S = e_n(g, g_1)^{rk},$$

を計算し，これと共通鍵暗号の暗号化関数 Enc() を用いてメッセージ m を以下のように暗号化する．

$$C = \mathrm{Enc}(K_S, m).$$

放送事業者は，暗号文 C にヘッダを付けて (H, C) を放送する．

3.5 復　　号

正規端末は，公開鍵 d と登録端末集合 S を用いて

$$b_i = g_1^{\prod_{I_j \in S, j\neq i} I_j - \prod_{I_j \in S, j\neq i}(s+I_j)},$$

を計算する(注4)．この b_i，ヘッダ情報および自身の秘密鍵を用いて以下のようにセッション鍵 K_S を復号する．

$$W = e_n(k_i, H_1)e_n(H_2, b_i)$$
$$= K_S^{\prod_{I_j \in S, j\neq i} I_j},$$
$$K_S = W^{\prod_{I_j \in S, j\neq i} I_j^{-1}}.$$

復号されたセッション鍵と共通鍵暗号の復号関数 Dec() を用いて暗号文 C を復号し，メッセージ m を復号する．

3.6 修 正 方 式

セッション鍵を以下のような K_S' に修正することにより，僅かではあるが，提案方式の計算量を削減することができる．

$$K_S' = e_n(g, g_1)^{rk\prod_{I_j \in S} I_j}.$$

このときセッション鍵の復号は

$$K_S' = W^{I_i},$$

となる．

3.7 暗号化および復号における計算量

集合 S が固定の場合は，一度 $g_r^{\prod f(I_j)}$ および $g_1^{\prod_{j\neq i} f(I_j)}$ を生成しておけば，これを毎回計算する必要はないので，ヘッダ作成時は 2 つの点のべき倍演算のみとなり，ヘッダ情報からセッション鍵の復元ではペアリングの計算が主な計算処理となり，それほど大きな計算量とはならない．しかし，S が変化した場合，その度に $g_r^{\prod f(I_j)}$ および $g_1^{\prod_{j\neq i} f(I_j)}$ の計算をする必要がある．この計算はおおよそ N に比例した計算量が必要となる．しかし，いずれも $\mathbb{F}_q$ 上の楕円曲線上の演算であるので，N が数千程度以下であれば，パソコンでは実用的な計算時間で計算することが可能である．

3.8 不正端末追跡について

本稿で提案した方式は，[1] と同じ鍵を使用しているので，[1] に対する攻撃と同様に，次の 2 種類の事前データを不正端末内に記憶させておくことによって結託攻撃が成立する．

（1） 結託端末の秘密鍵の線形結合 $\tilde{k}_0$ を用いる．

（2） 中間復号データ b_i に相当するものを作成するために，復号公開鍵 d に変わる復号鍵 $\tilde{d} = (\tilde{d}_1, \tilde{d}_2, \cdots, \tilde{d}_{N-M})$ を事前に計算しておく．

$$\tilde{d}_1 = g_1^{\sum_{i=1}^M \lambda_i I_i \prod_{j=1, j\neq i}^M (s+I_j) - \prod_{j=1}^M I_j},$$
$$\tilde{d}_2 = g_1^{\sum_{i=1}^M \lambda_i I_i \prod_{j=1, j\neq i}^M s(s+I_j)},$$
$$\vdots$$
$$\tilde{d}_k = g_1^{\sum_{i=1}^M \lambda_i I_i \prod_{j=1, j\neq i}^M s^{k-1}(s+I_j)},$$
$$\vdots$$

(注3)：$\prod_{I_j \in S}(s+I_j)$ は，s の N 次以下の多項式であるので，H_1 は公開暗号化鍵 e を用いて作成することができる．

(注4)：$\prod_{I_j \in S, j\neq i} I_j - \prod_{I_j \in S, j\neq i}(s+I_j)$ は，s の $N-1$ 次以下で定数項が 0 の多項式であるので，b_i は公開復号鍵 d を用いて計算することができる．

$$\tilde{d}_{N-M} = g_1^{\sum_{i=1}^{M} \lambda_i I_i \prod_{j=1, j\neq i}^{M} s^{N-M-1}(s+I_j)}.$$

ただし，この場合，中間復号データ b_i に相当するデータを作成する際に，集合 S に属する I_j の中で結託に利用されているものを除いて b_i を作成する必要があるので，そこで結託端末の情報を特定することができる．これを特定されないようにするためには，$\tilde{d}$ を計算する際に使用している I_j の中に，結託端末以外の I_j を $\prod$ の箇所にのみ（すなわち $\sum$ は結託端末に関するもののみである）混ぜておくと，復号に使用するデータから不正端末を結託端末を特定することができなくなる．ただし，この際に混合する I_j は，この時点で固定されてしまうので，ここで混合した I_j がリボークされると，この結託攻撃は成立しない．このようなことから，SCIS2007 においては，ダミーの ID データを事前に混ぜておき，その ID 情報を放送毎に変えるという手法を提案したが，この場合，攻撃者にダミーの ID を特定されてしまうと，ダミー以外の ID データを用いて $\tilde{d}$ を作成することができてしまうのである．

以上の考察より，攻撃者にリボークされる ID 情報を予測されないように，かつ事前に固定した ID データが必ずリボークされるような工夫をすれば，上述のような結託攻撃を防ぐことができる．次章で提案する方式は，この考え方に基づいた方式である．ただし，提案する方式は個別の端末のリボーク機能は有していない．

4. 新しい不正端末追跡法 (1)

ID 情報のハッシュ値を t_1 ビットの 2 進系列で表示する．すなわち

$$h(ID_i) = I_i = (I_{i1}, I_{i2}, \cdots, I_{it_1}),$$

とする．

4.1 鍵 設 定

2 進系列 $X = (X_1, X_2, \cdots, X_{t_1})(X_j \in \{0,1\})$ に対して，鍵生成センタは秘密の乱数 $s, U_j, L_j \in \mathbb{Z}_n$ を選び，秘密の多項式として

$$f(X) = f(X_1, X_2, \cdots, X_{t_1}) = \prod_{j=1}^{t_1} (s+U_j)^{X_j}(s+L_j)^{1-X_j},$$

を設定する．

4.2 端末 i の秘密鍵 k_i の生成

鍵生成センタは端末 ID_i の秘密鍵 k_i として

$$k_i = g^{f(I_i)^{-1}} = g^{\prod_{j=1}^{t_1}(s+U_j)^{-I_{ij}}(s+L_j)^{I_{ij}-1}},$$

を計算する．

4.3 公開鍵の準備

前節の方式と同様に以下のような公開鍵を準備する $(N > t_1)$.

$$e = (e_0, e_1, \cdots, e_N) = (g_1^r, g_1^{rs}, \cdots, g_1^{rs^N}),$$
$$d = (d_1, d_2, \cdots, d_{N-t_1}) = (g_1^s, g_1^{s^2}, \cdots, g_1^{s^{N-t_1}}),$$
$$v = g^r, \quad y = e_n(g, g_1)^r.$$

4.4 暗 号 化

ランダムに t_1 ビットの 2 進系列 $\boldsymbol{R} = (R_1, R_2, \cdots, R_{t_1})$ を選ぶ $(t_1 < N)$.

暗号作成者は乱数 $k \in Zn$ を生成し，これと公開鍵および受信者の所属する部署の ID を用いて以下のヘッダ情報を作成する．

$$H = (H_0, H_1, H_2, \ldots, H_{N-t_1}, v^k, R),$$
$$H_i = g^{ks^i f(R)} \ (\text{for } 0 \leq i \leq N-t_1).$$

そして，このヘッダ情報に対するセッション鍵

$$K_S = e_n(g, g_1)^{rk},$$

を計算し，これと共通鍵暗号を用いてメッセージ m を

$$C = \mathrm{Enc}(K_S, m),$$

と暗号化する．暗号作成者は，暗号文 C にヘッダを付けて (H, C) を受信者に送信する．

4.5 セッション鍵の復元

以下では 2 つの t_1 ビットの 2 進系列 $\boldsymbol{R}$ と $\boldsymbol{I}_i$ が，t_2 個の箇所で異なっているとする．ただし，$t_2 \leq N - t_1$ である．正規受信者は，ヘッダ $H_0, \ldots, H_{N-t_1}$ と自身の ID 情報 $I_{i1}, \ldots, I_{it}$ を用いて

$$B_i = g^{kf(R)\prod_{j=1, I_{ij}\neq R_j}^{t_2}(s+U_j)^{I_{ij}}(s+L_j)^{1-I_{ij}}}$$
$$= g^{kf(I_i)\prod_{j=1, R_j\neq I_{ij}}^{t_2}(s+U_j)^{R_j}(s+L_j)^{1-R_j}},$$

を計算し，公開鍵 $\boldsymbol{d}$ を用いて

$$b_i = g_1^{\prod_{j=1, R_j\neq I_{ij}}^{t_2} U_j^{R_j} L_j^{1-R_j} - \prod_{j=1, R_j\neq I_{ij}}^{t_2}(s+U_j)^{R_j}(s+L_j)^{1-R_j}},$$

を計算する．以上のデータおよび自身の秘密鍵を用いて以下のようにセッション鍵 K_S を復号する．正規端末はヘッダ情報と自分の秘密鍵を用いてセッション鍵 K_S を以下のように復号する．

$$W = e_n(k_i, B_i)e_n(v^k, b_i) = K_S^{\prod_{j=1, R_j\neq I_{ij}}^{t_2} U_j^{R_j} L_j^{1-R_j}},$$
$$K_S = W^{\prod_{j=1, R_j\neq I_{ij}}^{t_2} U_j^{-R_j} L_j^{R_j-1}}.$$

復号されたセッション鍵を用いて暗号文 C を復号し，メッセージ m を復号する．上述の方式では t_1 ビットのランダムな 2 進系列 $\boldsymbol{R}$ のうち，$N - t_1$ ビット以下のビットが $\boldsymbol{I}_i$ と異なっていると仮定している．この条件が満たされない確率すなわち $N - t_1 + 1$ ビット以上が相異なる確率 $Pr(Err)$ は，$t_1 = 1000$, $N = 1700$ の場合，$Pr(Err) = \sum_{k=0}^{1000} \binom{1000}{k}/2^{1000} < 2^{-123}$ であり，正規端末がセッション鍵の復元に成功する確率 $Pr(Succ)$ は $Pr(Succ) > 1 - 2^{-123}$ となり，実用的に十分高い確率である．表 1 に $t_1, N - t_1, Pr(Err)$ の関係を示す．詳細は割愛するが，結託攻撃に対する耐性を考えると t_1 を大きくとり，比 $(N - t_1)/t_1$ が大きくなる方が良いと考えられる．

$t_1 = 1000$ とした場合，2 つの端末 ID_1 および ID_2 の復号鍵の線形結合を作成しておくとすると、それらの I_1 および I_2 の共通のビットを多く見積もって 600 ビットとすると，分母

表 1　パラメータと失敗確率
Table 1　Relation of Parameters and Error Probability.

t_1	$N-t_1$	$Pr(Err)$
1000	650	8.1×10^{-22}
1000	700	8.8×10^{-38}
1000	750	6.7×10^{-59}
2000	1215	3.0×10^{-22}
2000	1285	7.1×10^{-38}
2000	1360	9.7×10^{-60}

5. 新しい不正端末追跡法 (2)

前章では，実用的に十分高い確率でセッション鍵を復元させるためには，多項式 $f(X)$ の s における次数，すなわち t_1 の値を 1000 程度に設定する必要があることを見た．本章では，この次数を半分程度にすることが可能な方式を示す．

ID 情報のハッシュ値から適切な処理によって生成されるハミング重み $t_1/2$ の t_1 ビットの 2 進系列を

$$h(ID_i)=I_i=(I_{i1},I_{i2},\cdots,I_{it_1}),$$

とする．

5.1 鍵 設 定

ハミング重み $t_1/2$ の 2 進系列 $X=(X_1,X_2,\cdots,X_{t_1})(X_j\in\{0,1\})$ に対して，鍵生成センタは秘密の乱数 $s,U_j\in\mathbb{Z}_n$ を選び，秘密の多項式として

$$f(X)=f(X_1,X_2,\cdots,X_{t_1})=\prod_{j=1}^{t_1}(s+U_j)^{X_j},$$

を設定する．このとき，$f(X)$ の次数は $t_1/2$ である．

5.2 端末 i の秘密鍵 k_i の生成

鍵生成センタは端末 ID_i の秘密鍵 k_i として

$$k_i=g^{f(I_i)^{-1}}=g^{\prod_{j=1}^{t_1}(s+U_j)^{-I_{ij}}},$$

を計算する．

5.3 公開鍵の準備

前節の方式と同様に以下のような公開鍵を準備する $(N>t_1/2)$.

$$e=(e_0,e_1,\cdots,e_N)=(g_1^r,g_1^{rs},\cdots,g_1^{rs^N}),$$
$$d=(d_1,d_2,\cdots,d_{N-t_1})=(g_1^s,g_1^{s^2},\cdots,g_1^{s^{N-t_1/2}}),$$
$$v=g^r,\quad y=e_n(g,g_1)^r.$$

5.4 暗 号 化

ハミング重みが $t_1/2$ の t_1 ビットの 2 進系列 $R=(R_1,R_2,\cdots,R_{t_1})$ をランダムに選ぶ $(t_1<N)$.

暗号作成者は乱数 $k\in\mathbb{Z}_n$ を生成し，これと公開鍵および受信者の所属する部署の ID を用いて以下のヘッダ情報を作成する．

$$H=(H_0,H_1,H_2,\ldots,H_{N-t_1/2},v^k,R),$$
$$H_i=g^{ks^if(R)}\ (\text{for } 0\leqq i\leqq N-t_1/2).$$

そして，このヘッダ情報に対するセッション鍵

$$K_S=e_n(g,g_1)^{rk},$$

を計算し，これと共通鍵暗号を用いてメッセージ m を $C=\mathrm{Enc}(K_S,m)$ と暗号化する．暗号作成者は，暗号文 C にヘッダを付けて (H,C) を受信者に送信する．

5.5 セッション鍵の復元

以下では 2 つの t_1 ビットの 2 進系列 R と I_i が，t_2 個の箇所で異なっているとする．ただし，$t_2\leqq N-t_1/2$ である．正規受信者は，ヘッダ $H_0,\ldots,H_{N-t_1}$ と自身の ID 情報 $I_{i1},\ldots,I_{it}$ を用いて

$$B_i=g^{kf(R)\prod_{j=1,I_{ij}\neq R_j}^{t_2}(s+U_j)^{I_{ij}}}$$
$$=g^{kf(I_i)\prod_{j=1,R_j\neq I_{ij}}^{t_2}(s+U_j)^{R_j}},$$

を計算し，公開鍵 d を用いて

$$b_i=g_1^{\prod_{j=1,R_j\neq I_{ij}}^{t_2}U_j^{R_j}-\prod_{j=1,R_j\neq I_{ij}}^{t_2}(s+U_j)^{R_j}},$$

を計算する．以上のデータおよび自身の秘密鍵を用いて以下のようにセッション鍵 K_S を復号する．正規端末はヘッダ情報と自分の秘密鍵を用いてセッション鍵 K_S を以下のように復号する．

$$W=e_n(k_i,B_i)e_n(v^k,b_i)=K_S^{\prod_{j=1,R_j\neq I_{ij}}^{t_2}U_j^{R_j}},$$
$$K_S=W^{\prod_{j=1,R_j\neq I_{ij}}^{t_2}U_j^{-R_j}}.$$

復号されたセッション鍵を用いて暗号文 C を復号し，メッセージ m を復号する．上述の方式では t_1 ビットのランダムな 2 進系列 R のうち，$N-t_1/2$ ビット以下のビットが I_i と異なっていると仮定している．$t_1=1000$, $N=1200$ の場合，$N-t_1/2=700$ であるので，前章の方式と同様に，正規端末がセッション鍵の復元に成功する確率 $Pr(Succ)$ を実用的に十分高い確率とすることができる．

6. 新しい不正端末追跡法 (3)

第 4,5 章で示した不正端末追跡法において，秘密鍵 k_i を以下のように 2 つの鍵として配布する方式にすると，各端末固有の乱数 r_{I_i} により [9]，結託攻撃をより困難にすると期待される．

6.1 端末 i の秘密鍵の生成

鍵生成センタは端末 ID_i の秘密鍵 $k_i=(k_{i1},k_{i2})$ として

$$k_{i1}=k_i^{1+r_{I_i}},$$
$$k_{i2}=g_1^{r_{I_i}},$$

を生成する．ただし，k_i は第 4,5 章で定義した秘密鍵である．

6.2 セッション鍵の復元

この秘密鍵 k_{i1} を k_i の代わりに用いれば，最終的に得られるセッション鍵の形は

$$K_S^{1+r_{I_i}}=e_n(g,g_1)^{rk(1+r_{I_i})},$$

であるので，もう一つの秘密鍵 k_{i2} とヘッダ $H_2=v^k=g^{rk}$ を用いて

$$K_S=K_S^{1+r_{I_i}}/e_n(H_2,k_{i2})=e_n(g,g_1)^{rk(1+r_{I_i})}/e_n(g,g_1)^{rkr_{I_i}},$$

を計算してセッション鍵を復号することができる．

7. まとめと今後の課題

本稿で提案した幾つかの不正端末追跡方式は幾つかの新しい手法を用いている．また，復号は確率的に失敗する可能性があるものの，パラメータを適切に設定することにより，その失敗確率を無視できるほど小さくすることができる．本提案手法を用いることにより，従来の鍵の線形結合による結託攻撃を困難とすることができると考えられるが，詳しい検討は今後の課題としたい．

文　献

[1] Shigeo Mitsunari, Ryuichi Sakai and Masao Kasahara, "A New Traitor Tracing", IEICE Trans. Vol. E85-A, No.2, pp. 481–484, Feb.2002.

[2] Ryuichi Sakai and Masao Kasahara, "ID based Cryptosystems with Pairing on Elliptic Curve", IACR eprint, 054, Mar. 2003.

[3] D. Boneh, C. Gentry and B. Waters, " Collusion Resistant Broadcast Encryption With Short Cihpertexts and Private Keys" Euro-crypt2005.

[4] 境隆一, "ID 情報に基づく公開鍵暗号の鍵生成について", Technical Report of IEICE, ISEC 2006-105 pp.25-28, (2006-12).

[5] 境隆一, 笠原正雄, "放送用暗号の実現法", Symposium on Cryptography and Information Security 2005(SCIS2005), 3D4-1(2005-1).

[6] 境隆一, 笠原正雄, "効率の良い放送暗号", Symposium on Cryptography and Information Security 2007(SCIS2007), p249, 3C3-1(2007-1).

[7] Ryuichi Sakai and Jun Furukawa, "Identity-based Broadcast Encryption", IACR eprint, 217, Jun. 2007.

[8] 境隆一, "ID ベース公開鍵暗号の応用", Symposium on Cryptography and Information Security 2008(SCIS2008), 4D2-3(2008-1).

[9] Jun Furukawa et al., "A Fuzzy ID-based Encryption Efficient when Error Rate is Low", Symposium on Cryptography and Information Security 2008(SCIS2008), 4D2-4(2008-1).