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

2006－CSEC－33 (4)
2006／5／12

利用履歴を秘匿できるコンテンツ配信・課金方式の改良

飛田 孝幸[†,††] 山本 博紀[‡] 土井 洋[†] 真島 恵吾[*]

† 情報セキュリティ大学院大学 221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1
‡ 中央大学 112-8551 東京都文京区春日 1-13-27
* NHK 放送技術研究所 157-8510 東京都世田谷区砧 1-10-11
†† NEC ソフト株式会社 136-8627 東京都江東区新木場 1-18-7
E-mail: †{mgs054509,doi}@iisec.ac.jp, ‡hiyamamo@chao.ise.chuo-u.ac.jp, *majima.k-fu@nhk.or.jp

あらまし 近年，高速・広帯域の通信ネットワークの急速な普及により，映像・音楽等のコンテンツ配信サービスの利用者が増加している．また，サーバ型放送などデジタル放送の高度化により，放送・通信連携による高度な情報サービスが期待されている．これらのサービスではコンテンツの利用履歴や利用傾向はプライバシ保護の観点から秘匿することが望ましい．一方，有料サービスにおいては，視聴内容に応じて利用料金が正確に計算され利用者に正しく課金される必要がある．本稿では，これらの要件を満たす利用履歴を秘匿できるコンテンツ配信・課金方式の一つとして，Ateniese らにより提案されたグループ署名を利用し，利用者の計算・通信コストが利用可能なコンテンツの総数に依存せず利用したコンテンツ数のみに依存する方式を提案する．

Efficient Content Distribution and Charging Scheme with Privacy

Takayuki TOBITA[†,††], Hironori YAMAMOTO[‡], Hiroshi DOI[†], and Keigo MAJIMA[*]

† Institute of Information Security
2-14-1, Tsuruya-cho, Kanagawa-ku, Yokohama Kanagawa, 221-0835 Japan
‡ The University of Chuo 1-13-27, Kasuga, Bunkyou-ku Tokyo, 112-8551 Japan
* NHK Science and Technical Research Laboratories
1-10-11, Kinuta, Setagaya-ku Tokyo, 157-8510 Japan
†† NEC Soft, Ltd. 1-18-7, Shinkiba, Koto-ku, Tokyo, 136-8627 Japan
E-mail: †{mgs054509,doi}@iisec.ac.jp, ‡hiyamamo@chao.ise.chuo-u.ac.jp, *majima.k-fu@nhk.or.jp

Abstract As broadband IP networks have spread rapidly, the number of users of content distribution services has grown. Also, the new possibilities brought by digital broadcasting, such as broadcasting based on home servers, are expected to lead to sophisticated information services utilizing broadcasting and communication networks. Although for privacy reasons it is desirable to protect the usage history and preferences provided that usage charges is calculated correctly based on the contents that the user got. This paper proposes content distribution and charging scheme with privacy, based on the group signature proposed by Ateniese et al. In this construction, the computation/communication cost only depends on the number of contents that the user got. They do not depend on the number of all contents that the user can get.

1. まえがき

近年，高速・広帯域の通信ネットワークの急速な普及により，映像・音楽等のコンテンツ配信サービスの利用者が増加している．また，ディジタル放送の開始により放送と通信ネットワークを利用した新しい情報サービスが期待されている．TV Anytime Forum [17] はその代表例であり，蓄積機能を持ったディジタル放送受信機向けのマルチメディアサービスの国際標準仕様を策定している [19], [20]．これはテレビ放送の即時性とインターネットの柔軟性を結合し，利用者が任意のタイミングで外部やディジタル放送受信機に蓄積した情報を検索して視聴できるものである．これらのサービスでは，コンテンツの視聴等に伴う利用履歴や視聴傾向はプライ

バシの観点から秘匿することが望ましい．一方，利用者及びコンテンツ配信事業者の双方にとって，視聴内容に応じて利用料金が正確に計算され正しく課金される必要がある（コンテンツ配信方式に関しては文献[11]〜[13]等で研究されている）．この様なコンテンツ配信・課金方式（以下CDCS）を提案することが，本稿の目的である．

各コンテンツの料金が均一であれば，利用者が視聴したコンテンツ数と単価から，CDCSはAaptive Oblivious Transfer[14]により実現できる．しかし一般に，各コンテンツの視聴料金は一定では無く，各コンテンツの単価から利用者の視聴傾向が推測されないように秘匿し，合計金額のみが正しく計算される必要がある．準同型暗号を利用する電子投票方式[9]は合計値のみを計算することを実現している．従って問題は実際に利用者が得たコンテンツと利用者が支払う料金の対応の正当性をいかに証明するかである．

文献[16]では，1-out-of-n署名を利用してCDCSを実現したが，利用者の計算・通信コストが利用可能なコンテンツ総数に比例していた．そこで本稿では，Ateniese らにより提案されたグループ署名[2]を利用し，利用者の計算・通信コストが利用可能なコンテンツの総数に依存せず，利用者が利用したコンテンツ数のみに依存する方式を提案する．

1.1 関連技術

1.1.1 Aaptive Oblivious Transfer

Oblivious transfer（OT）[15]は1981年にRabinにより提案され，その後AdaptiveOT_t^n[14]等の応用が提案されている．AdaptiveOT_t^nは，コミットフェーズと転送フェーズにより構成されている．コミットフェーズで，コンテンツ配信サーバ（D）はn個の秘密情報（$C_1,\cdots,C_n$）を利用者にコミットし，転送フェーズで，利用者（U）がコミットされたn個のインデックスから任意の$\{k(i)\}_{1\leqq i\leqq t}$を選択し，$D$と交信後，秘密情報$\{C_{k(1)},\cdots,C_{k(t)}\}$を得る．但しこの際，$U$は$\{C_{k(1)},\cdots,C_{k(t)}\}$以外の秘密情報は得られず，$D$は$\{k(1),\cdots,k(t)\}$についての情報を一切得られない．

1.1.2 準同型電子投票方式

電子投票方式は，既に多くの研究が行われ，提案されている．準同型電子投票方式は，ある候補者に投票された総数のみが得られる方式で，Cramer らにより安全かつ効率的な方式[9]が提案されている．この方式は，公開掲示板，複数の選挙管理人及び多くの登録された有権者により構成されている．そして，投票と復号にしきい値準同型暗号方式と知識の証明を利用しており，効率性，頑強性，検証性及びプライバシを実現している．

1.1.3 知識の署名（SPK）

知識の署名（SPK）とは，知識の零知識証明を非対話形に変換した署名で，証明者が秘密情報自体を明かすことなく，その秘密情報を知っていることのみを，検証者に証明するものである．本稿では，証明者が述語$Predicates$を満たす秘密情報$\alpha,\beta,\cdots$を知っていることのSPKを$SPK\{(\alpha,\beta,\cdots):Predicates\}(m)$と記述する．ここでは$m\in\{0,1\}^*$は署名するメッセージを表している．

i） 離散対数のSPK[10]

後述する強RSA仮定の下で，RSAの法nに対して，$g\in\mathbb{Z}_n$，$G=\langle g\rangle$，$y\in G$とした時，$SPK\{(\alpha):y=g^\alpha \bmod n\}(m)$を証明・検証できる．またこれを拡張した様々なSPKも構成できる[6]．

ii） 1-out-of-n署名

$SPK\{\alpha_k\in\{1,\cdots,n\}:\bigvee g^{\alpha_i}=h\}(m)$は，文献[6]に示されている one of the two discrete logarithm を一般化したものであり，1-out-of-n署名[1],[8]において実現されている．

なおグループ署名も登録されたメンバ証明書とメンバ秘密情報の両方を持つ利用者のうちの一人であることのSPKであると言える．安全なグループ署名は，正当性，偽造不可能生，匿名性，リンク不能性，なりすまし不能性，追跡可能性等を満たしている．Ateniese らにより提案されたグループ署名[2]は，さらにCoalition-Resistanceを実現しており，グループメンバが結託してもグループ管理者によって受理され，結託したメンバの一人にリンクできないような署名を作る事は出来ない．提案方式では，文献[2]のtheorem1を利用してCDCSを構成する（3.8節参照）．

iii） 離散対数の範囲のSPK[5],[7]

提案方式では離散対数の範囲のSPKを利用する．t及びlをセキュリティパラメータとし，$[0,b]$の範囲で設定した離散対数xが，より広い範囲$[-2^{t+l}b,2^{t+l}b]$に含まれている事の証明$SPK\{(x):E=g^xh^r \bmod n\wedge x\in[-2^{t+l}b,2^{t+l}b]\}$を効率よく構成できる．具体的な構成方法は，3.5節にて示す．

2. モデル

コンテンツ配信システムの構成を図1に示す．本システムは，コンテンツ配信サーバ（D），利用者（U）そしてt個の合算サーバ（T_i）の3つのエンティティにより構成される（提案方式ではセットアップ時のみ，信頼できる第三者機関を利用する）．なお簡単の為に，本稿では利用者は一人として扱っている．CDCSは，セットアップ，コミットフェーズ，転送フェーズ，課金フェーズの4つのフェーズからなる．以下各フェーズについて説明する．

セットアップでは，システムパラメータと各エンティティの秘密鍵・公開鍵を生成する．

コミットフェーズでは（例えば毎月の月初），Dが各コンテンツ（$Content_i$）をコンテンツ鍵（κ_i）により暗号化し，暗号化したコンテンツ（$\mathcal{E}_{\kappa_i}(Content_i)$）と，暗号化したコンテンツ鍵を利用者に送付する．同時に，Dはコンテンツリスト（CL）を利用者に送付もしくは公開する．CLは(i,I_i,s_i,p_i)により構成される（$1\leqq i\leqq n$）．iはインデックス，p_iは$Content_i$の価格，s_iは署名鍵や価格情報を含むコンテンツ情報，I_iは付加情報（コンテンツ名等）である．

転送フェーズでは，利用者（U）が視聴したいコンテンツ（$k(j)$）のコンテンツ復号鍵$\kappa_{k(j)}$を，UとD間でadaptiveOT_1^nを実行することにより得る．この時，Dは

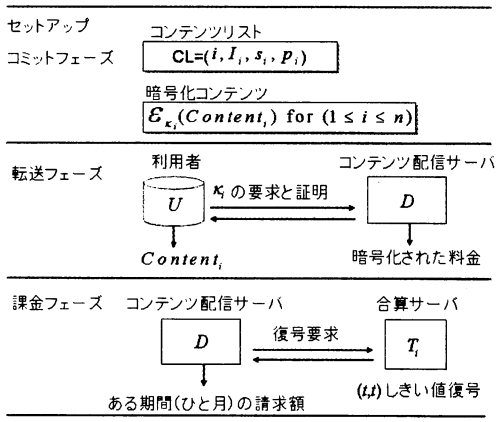

図 1　CDCS モデル図

暗号化されたコンテンツの価格 p_i を得るが，利用者が視聴したインデックス等のコンテンツに関する情報は一切得られない．

課金フェーズでは（例えば毎月一度），D は暗号化されたままのコンテンツの料金情報を合算して $T_i(i=1,\ldots,t)$ に送り，D は T_i より利用者への請求金額（利用料金の合算値）を得る．この時，T_i は，(t,t) しきい値復号を行う．ここで，利用者の毎月の合計金額（$T^{(U)}(=\sum p_i)$）は，高々10^5 程度と仮定する．

なお，我々はコンテンツの復号作業を，利用者のセキュリティモジュールで行われることを想定している．この手法は実際に多くのディジタル放送システムで想定されている [18]．

2.1　セキュリティ要件

この節では CDCS のセキュリティ要件を定義する．モデルを図 2 のように一つのシステムと置き換える．これにより，D の秘密の入力を $\{\kappa_i\}_{1\leq i\leq n}$，$U$ の秘密の入力を $\{k(i)\}_{1\leq i\leq m}$，U の秘密の出力を $\{\kappa_{k(i)}\}_{1\leq i\leq m}$，$T^{(U)}$ は公開された出力とみなす事ができる．

また説明の為に，S_U を，$\{\kappa_{k(1)},\ldots,\kappa_{k(m)}\}$ の集合とする．

[**定義 1**]　（健全性）各エンティティU，D 及び T_i がプロトコルに従わない時は，エンティティU もしくは D は不正を検出できる．

（以下，全エンティティがプロトコルに従ったと仮定する．）

[**定義 2**]　（利用者の正当性）U は $k(i)(1\leq i\leq m)$ の入力に対して，$\kappa_{k(i)}(1\leq i\leq m)$ を出力する．

[**定義 3**]　（課金の正当性）全ての $T_i(i=1,\ldots,t)$ が協力した時のみ，合計金額 $T^{(U)}=\sum_{i=1}^{m} p_{k(i)}$ は，正しく計算される．

[**定義 4**]　（コンテンツの安全性）$\{k(i)\}_{1\leq i\leq m}$，S_U，全ての通信及び全ての公開鍵を入力とし，$\kappa_j(j\notin\{k(1),\ldots,k(m)\})$ を多項式時間で出力するようなアルゴリズム $\bar{U}$ は存在しない．

[**定義 5**]　（利用者のプライバシ）$\{\kappa_i\}_{1\leq i\leq n}$，$T^{(U)}$，全ての通信，$j\in\{1,\cdots,n\}$ 及び全ての公開鍵を入力とし，$1(\kappa_j\in S_U)$ もしくは $0(\kappa_j\notin S_U)$ を多項式時間で出力するアルゴリズム $\bar{D}$ が存在したと仮定する．また，$\{\kappa_i\}_{1\leq i\leq n}$，$T^{(U)}$，$j\in\{1,\cdots,n\}$ 及び全ての公開鍵を入力とし，$1(\kappa_j\in S_U)$ もしくは $0(\kappa_j\notin S_U)$ を多項式時間で出力するアルゴリズム $\tilde{D}$ が存在したと仮定する．

この時，$^\forall j$ において，$|Pr[\bar{D}(j,\cdots)=1]-Pr[\tilde{D}(j,\cdots)=1]|<\epsilon$ となる（$^\forall\epsilon>0$）．

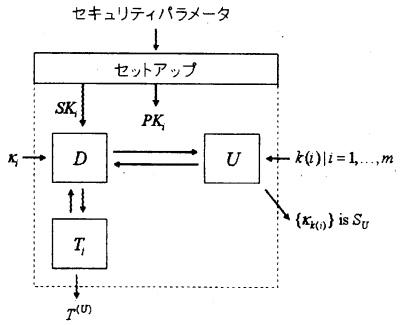

図 2　CDCS システム図

3.　提案方式

この章では，ACJT2000 [2] を利用した具体的な提案方式の構成を示す．

提案方式の特徴は，ACJT2000 [2] の Coalition-Resistance 特性を利用してグループ署名鍵（SK_i）を，CL の一部として公開することである．

3.1　事前準備

提案方式の安全性は，強 RSA 仮定及び Decisional Diffie-Hellman（DDH）仮定及びランダムオラクルモデルに基づいている．$n(=pq)$ を $p=2p'+1, q=2q'+1$ で p,q,p',q' が全て素数となる RSA の法とする．このとき，位数 $p'q'$ になる $\mathbb{Z}_n^*$ の巡回部分群 $QR(n)$ は，以下の 2 つを仮定を満たすと仮定する．

3.1.1　強 RSA 仮定

G を $QR(n)$ とする．このとき，n 及び $z\in G$ を入力とし，無視できない確率で $z\equiv u^e(\mathrm{mod}n)$ となる $u\in G$ 及び $e\in Z_{>1}$ を出力する確率的多項式時間アルゴリズムは，存在しない [2], [10]．

3.1.2　Decisional Diffie-Hellman 仮定

G を g を原始元とする $QR(n)$ とし，位数 $u=\#G$ とする．このとき，$x,y,z\in_R\mathbb{Z}_u$ である (g,g^x,g^y,g^z) と $x,y\in_R\mathbb{Z}_u$ である (g,g^x,g^y,g^{xy}) を，無視できない確率で区別する確率的多項式時間アルゴリズムは存在しない [3]．

3.2　プロトコル

ここでは簡単の為に，合算サーバを 1 つとし，T と表す．また新たなエンティティとしてシステムマネージャ M を定義

表 1　素数 e_i の構成例

$\{0\}^{120}$	$\{$ 価格 $e_{i1}\}^{20}$	$\{0\}^{120}$	$\{$ 乱数 $e_{i2}\}^{760}$
		← 2^{γ_3}	→

する．M は信頼できる第三者機関等であり，グループ署名の秘密情報，公開情報及び署名鍵を作る為に，セットアップ時のみ利用する．

3.2.1　セットアップ

セキュリティパラメータはグループ署名（ACJT2000 方式[2]）の $\epsilon > 1, k, l_p$ に，離散対数の範囲の証明で利用する t, s, l 及び γ_3 を加えたものとする（ここで文献[2]と同様に，$\lambda_1 > \epsilon(\lambda_2 + k) + 2$，$\lambda_2 > 4l_p$，$\gamma_1 > \epsilon(\gamma_2 + k) + 2$，$\gamma_2 > \lambda_1 + 2$ を満足する設定とし，範囲の定義として $\Lambda = [2^{\lambda_1} - 2^{\lambda_2}, 2^{\lambda_1} + 2^{\lambda_2}]$ 及び $\Gamma = [2^{\gamma_1} - 2^{\gamma_2}, 2^{\gamma_1} + 2^{\gamma_2}]$ を定義する）．さらに，$\mathcal{H} : \{0,1\}^* \rightarrow \{0,1\}^k$ を衝突困難性をもったハッシュ関数とし，G を疑似ランダム生成関数とする．

最初に，M は秘密鍵として素数 p, q, p', q' を，$|p'| = |q'| = l_p$，$p = 2p' + 1$，$q = 2q' + 1$ を満たすように生成し，M は，以下の公開パラメータを生成する．

$$n(= pq),$$
$$a, a_0, g, h \in_R QR(n)(\text{order } p'q').$$

次に，コンテンツ配信サーバ（D）は（$i = 1, \ldots, n$）について価格 $e_{i1}(= p_i)$ を定め M に送る．M は乱数 $x_i \in_R \Lambda$，価格 e_{i1} の情報を埋め込んだ素数 $e_i(= 2^{\gamma_3} e_{i1} + e_{i2}) \in_R \Gamma$（表1参照），$A_i = (a^{x_i} a_0)^{\frac{1}{e_i}} \bmod n$ を生成して，(e_i, A_i, x_i) を D に送る．これはグループ署名の JOIN フェーズを利用している．同時に，各エンティティは秘密鍵と公開鍵をそれぞれ以下のように設定し，PK_D, PK_U, PK_T を公開する．

$$(SK_D, PK_D) = (\omega, h_D = g^{\omega} \bmod n),$$
$$(SK_U, PK_U) = (\chi, h_U = g^{\chi} \bmod n),$$
$$(SK_T, PK_T) = (\tau, h_T = g^{\tau} \bmod n).$$

3.2.2　コミットフェーズ

step1　D は，$\mathrm{CL}\{i, e_i, x_i, A_i, e_{i1}\}_{(i=1,\ldots,n)}$ を U に送る（もしくは公開する）．

step2　D は，$Content_i$ を暗号化アルゴリズム $\mathcal{E}$ とコンテンツ鍵 κ_i で暗号化し，$\mathcal{E}_{\kappa_i}(Content_i)_{(i=1,\ldots,n)}$ を U に送る．

最後に $i = 1, \ldots, n$ について D は以下を計算し，暗号化されたコンテンツ復号鍵（$E_1, \cdots, E_n$）を U に送る．

$$K_i = (A_i)^{\omega} \bmod n,$$
$$E_i = G(K_i || A_i) \oplus \kappa_i.$$

3.2.3　転送フェーズ

step1　U は視聴したいコンテンツ j を CL から選択し，(e_j, A_j, x_j, e_{j1}) を得る．

step2　U は乱数 $r_0, r_{01} \in_R \{0,1\}^{2l_p}$ 及び，$r_{02} \in_R [-2^s n + 1, 2^s n - 1]$ を生成し，以下の計算を行う．

$$T_1 = A_i h_U^{r_0} \bmod n,$$
$$T_2 = g^{r_0} \bmod n,$$
$$T_3 = g^{e_i} h_T^{r_0} \bmod n,$$
$$T_4 = g^{r_{01}} \bmod n,$$
$$T_5 = g^{e_{i1}} h_T^{r_{01}} \bmod n,$$
$$T_6 = g^{e_{i2}} h_T^{r_{02}} \bmod n.$$

U は $r_1 \in_R \pm\{0,1\}^{\epsilon(\gamma_2+k)}$，$r_2 \in_R \pm\{0,1\}^{\epsilon(\lambda_2+k)}$，$r_3 \in_R \pm\{0,1\}^{\epsilon(\gamma_1+2l_p+k+1)}$，$r_4 \in_R \pm\{0,1\}^{\epsilon(2l_p+k)}$ を選び，以下の計算を行う．

$$d_1 = \frac{T_1^{r_1}}{a^{r_2} h_U^{r_3}} \bmod n,$$
$$d_2 = \frac{T_2^{r_1}}{g^{r_3}} \bmod n,$$
$$d_3 = g^{r_4} \bmod n,$$
$$d_4 = g^{r_1} h_T^{r_4} \bmod n.$$

U は $c = \mathcal{H}(g||h_T||h_U||a_0||a||T_1||T_2||T_3||d_1||d_2||d_3||d_4||ID)$ を計算し，$s_1 = r_1 - c(e_i - 2^{\gamma_1})$，$s_2 = r_2 - c(x_i - 2^{\lambda_1})$，$s_3 = r_3 - ce_i r_0$ 及び $s_4 = r_4 - cr_0$ を計算する．そして $\sigma_1 = (c, s_1, s_2, s_3, s_4, T_1, T_2, T_3, T_4, T_5, T_6)$ とする．σ_1 から (T_4, T_5, T_6) を除いたものは文献[2]のグループ署名であり，U が (T_1, T_2, T_3) を正しく計算した事と，選択したコンテンツの (e_j, A_j, x_j) が CL の中のどれか一つの組であることを証明する．なお (T_1, T_2)，(T_5, T_4) はそれぞれ利用者の秘密鍵を用いたコンテンツ情報，合算サーバの秘密鍵を用いた価格情報の ElGamal 暗号文となっている．次に U は以下の SPK を計算する（各 SPK の詳細は 3.3，3.4 及び 3.5 節に記載する）．以下の SPK はコンテンツの料金 (e_{j1}) が CL の中から選ばれている事と，改ざんされていないことを証明する（ここで $r_0' = 2^{\gamma_3} r_{01} + r_{02}$，SPK 内は全て法 n である）．

$$\sigma_{e_j} = SPK\{(e_j, r_0, r_0') : T_5^{2^{\gamma_3}} T_6 = g^{e_j} h_T^{r_0'} \wedge T_3 = g^{e_j} h_T^{r_0}\},$$
$$\sigma_{r_{01}} = SPK\{(e_{j1}, r_{01}) : T_4 = g^{r_{01}} \wedge T_5 = g^{e_{j1}} h_T^{r_{01}}\},$$
$$\sigma_{e_{j2}} = SPK\{(e_{j2}, r_{02}) : T_6 = g^{e_{j2}} h_T^{r_{02}}$$
$$\wedge e_{j2} \in [-2^{t+l} b, 2^{t+l} b]\}.$$

最後に，U は自身用の署名 σ_U（DSA 署名等）を付加し，D に $(\sigma_1, \sigma_{e_j}, \sigma_{r_{01}}, \sigma_{e_{j2}}, \sigma_U)$ を送る．

step3　D は $(\sigma_1, \sigma_{e_j}, \sigma_{r_{01}}, \sigma_{e_{j2}}, \sigma_U)$ を検証し，正しければ $r_D \in_R \{0,1\}^{2l_p}$ を生成して，以下の再暗号化と，自分の秘密鍵を使って正しく再暗号化した SPK の計算を行う．σ_D の詳細は，3.6 節に記載する．

$$K' = (T_1', T_2') = (h_U^{r_D} T_1^{\omega}, g^{r_D} T_2^{\omega}) \bmod n,$$
$$\sigma_D = SPK\{(\omega, r_D) : h_D = g^{\omega}$$
$$\wedge T_2' = g^{r_D} T_2^{\omega} \wedge T_1' = h_U^{r_D} T_1^{\omega} = (c_D, s_D, \bar{s}_D)\}.$$

そして，D は (K', σ_D) を U に送る．

step4　U は σ_D を検証し，正しければ以下の計算を行い．コンテンツ復号鍵（κ_j）を得る．

$$K = \frac{T_1'}{(T_2')^{\chi}} = (A_j)^{\omega} \bmod n,$$
$$\kappa_j = E_j \oplus G(K||A_j).$$

3.2.4 課金フェーズ

step1: D は $(\bar{T_4} = \prod_{i=1}^{m} T_{4_i}, \bar{T_5} = \prod_{i=1}^{m} T_{5_i})$ を計算し，T に送る（一定期間毎に送る）．

step2: T は電子投票 [9] の技法を使い以下の計算を行う．

$$A = \frac{\bar{T_5}}{(\bar{T_4})^{\tau}} \bmod n (= g^{\sum_{i=1}^{m} e_{j1_i}}).$$

そして，$\sum_{i=1}^{m} e_{j1_i} = log_g A$ を計算し，合計金額 $T^{(U)}$ を得る．一般的にこれは計算することが困難であるが，合計値が小さければ（このモデルでは，高々10^5 なので）計算可能である．

step3: T は自分の秘密鍵（τ）を使って正しく復号した証拠として，

$$\sigma_T = SPK\{\tau : h_T = g^{\tau} \wedge \frac{\bar{T_5}}{A} = (\bar{T_4})^{\tau}\}.$$

を計算して，$(\sigma_T, T^{(U)})$ を D に送る．

step4: D は σ_T を検証して，正しければ $T^{(U)}$ を受理する．σ_T の詳細は 3.7 節に記載する．

3.3 σ_{e_j} の構成

$M_U = (g||h_T||T_5^{2^{\lambda_2}} T_6||T_3)$ とし，$\sigma_{e_j} = SPK\{(e_j, r_0, r_0') : T_5^{2^{\lambda_2}} T_6 = g^{e_j} h_T^{r_0'} \wedge T_3 = g^{e_j} h_T^{r_0}\}$ を構成する．

署名生成　証明者 U は乱数 $\alpha_1 \in_R \{0,1\}^{\epsilon(k+\gamma_1)}$，$\alpha_2 \in_R \{0,1\}^{\epsilon(k+2l_p)}$ 及び $\alpha_3 \in_R \{0,1\}^{\epsilon(k+\gamma_3+2l_p)}$ を生成し，

$$t_1 = g^{\alpha_1} h_T^{\alpha_2} \bmod n,$$
$$t_2 = g^{\alpha_1} h_T^{\alpha_3} \bmod n,$$
$$c_U = \mathcal{H}(M_U||t_1||t_2),$$
$$s_U = \alpha_1 - c_U e_j,$$
$$\bar{s}_U = \alpha_2 - c_U r_0,$$
$$\hat{s}_U = \alpha_3 - c_U r_0'$$

を計算し，$\sigma_{e_j} = (c_U, s_U, \bar{s}_U, \hat{s}_U)$ を検証者 D へ送る．

署名検証　検証者 D は，

$$c_U \stackrel{?}{=} \mathcal{H}(M_U||(T_5^{2^{\lambda_2}} T_6)^{c_U} g^{s_U} h_T^{\hat{s}_U}||T_3{}^{c_U} g^{s_U} h_T^{\bar{s}_U})$$

を検証し成立すれば σ_{e_j} を受理し，さもなくば棄却する．

3.4 $\sigma_{r_{01}}$ の構成

$M_U = (g||h_T||T_4||T_5)$ とし，$\sigma_{r_{01}} = SPK\{(e_{j1}, r_{01}) : T_4 = g^{r_{01}} \wedge T_5 = g^{e_{j1}} h_T^{r_{01}}\}$ を構成する．

署名生成　証明者 U は $\alpha_1 \in_R \{0,1\}^{\epsilon(k+\gamma_1-\gamma_3)}$，$\alpha_2 \in_R \{0,1\}^{\epsilon(k+2l_p)}$ を生成し，

$$t_1 = g^{\alpha_2} \bmod n,$$
$$t_2 = g^{\alpha_1} h_T^{\alpha_2} \bmod n,$$
$$c_U = \mathcal{H}(M_U||t_1||t_2),$$
$$s_U = \alpha_1 - c_U e_{j1},$$
$$\bar{s}_U = \alpha_2 - c_U r_{01}$$

を計算し，$\sigma_{e_j} = (c_U, s_U, \bar{s}_U)$ を検証者 D へ送る．

署名検証　検証者 D は，

$$c_U \stackrel{?}{=} \mathcal{H}(M_U||T_4^{c_U} g^{\bar{s}_U}||T_5^{c_U} g^{s_U} h_T^{\bar{s}_U})$$

を検証し成立すれば $\sigma_{r_{01}}$ を受理し，さもなくば棄却する．

3.5 $\sigma_{e_{j2}}$ の構成

$\sigma_{e_{j2}} = SPK\{e_{i1}, r_{01} : T_5 = g^{e_{i1}} h_T^{r_{01}} \wedge e_{i1} \in [-2^{t+l}b, 2^{t+l}b]\}$ を構成する．但し，$\mathcal{H}_2$ は，出力が $2t$-bit となるハッシュ関数とする．

署名生成　証明者 U は $\omega \in_R [0, 2^{t+l}b - 1]$，$\eta \in_R [-2^{t+l+s}n + 1, 2^{t+l+s}n - 1]$ を生成し，

$$W = g^{\omega} h_T^{\eta} \bmod n,$$
$$C = \mathcal{H}_2(W),$$
$$c = C \bmod 2^t,$$
$$D_1 = \omega + e_{i1} c,$$
$$D_2 = \eta + r_{01} c (\in \mathbb{Z})$$

を計算し，$D_1 \in [cb, 2^{t+l}b - 1]$ ならば，$\sigma_{e_{j2}} = (C, D1, D2)$ を検証者 D へ送る．さもなくば，署名生成をやり直す．

署名検証　検証者 D は，

$$D_1 \in [cb, 2^{t+l}b - 1],$$
$$C \stackrel{?}{=} \mathcal{H}_2(g^{D_1} h_T^{D_2} T_5^{-c})$$

を検証し成立すれば $e_{i1} \in [-2^{t+l}b, 2^{t+l}b]$ であることを受理し，さもなくば棄却する．

3.6 σ_D の構成

$M_D = (g||h_U||h_D||T_1'||T_2')$ とし，

$$\sigma_D = SPK\{(\omega, r_D) : h_D = g^{\omega} \wedge T_2' = g^{r_D} T_2^{\omega} \wedge T_1' = h_U^{r_D} T_1^{\omega}\}$$

を構成する．

署名生成　証明者 D は $\alpha_1 \in_R \{0,1\}^{\epsilon(k+2l_p)}$，$\alpha_2 \in_R \{0,1\}^{\epsilon(k+2l_p)}$ を生成し，

$$t_1 = g^{\alpha_1} \bmod n,$$
$$t_2 = g^{\alpha_2} T_2^{\alpha_1} \bmod n,$$
$$t_3 = h_U^{\alpha_2} T_2^{\alpha_1} \bmod n,$$
$$c_D = \mathcal{H}(M_D||t_1||t_2||t_3),$$
$$s_D = \alpha_1 - c_D \omega,$$
$$\bar{s}_D = \alpha_2 - c_D r_D$$

を計算し，$\sigma_D = (c_D, s_D, \bar{s}_D)$ を検証者 U へ送る．

署名検証　検証者 U は，

$$c_D \stackrel{?}{=} \mathcal{H}(M_D||h_D^{c_D} g^{s_D}||T_2'^{c_D} g^{\bar{s}_D} T_2^{s_D}||T_1'^{c_D} h_U^{\bar{s}_D} T_1^{s_D})$$

を検証し成立すれば σ_D を受理し，さもなくば棄却する．

3.7 σ_T の構成

$M_T = (g||h_T||\frac{\bar{T_5}}{A})$ とし，

$$\sigma_T = SPK\{\tau : h_T = g^{\tau} \wedge \frac{\bar{T_5}}{A} = (\bar{T_4})^{\tau}\}$$

を構成する．

署名生成　証明者 T は $\alpha \in_R \{0,1\}^{\epsilon(k+2l_p)}$ を生成し，

$$t_1 = g^{\alpha} \bmod n,$$
$$t_2 = (\bar{T_4})^{\alpha} \bmod n,$$
$$c_T = \mathcal{H}(M_T||t_1||t_2),$$
$$s_T = \alpha - c_T \tau$$

を計算し，$\sigma_T = (c_T, s_T)$ を検証者 D へ送る．

署名検証　検証者 D は，

$$c_T \stackrel{?}{=} \mathcal{H}(M_T||h_T^{c_T} g^{s_T}||(\frac{\bar{T}_5}{A})^{c_T}(\bar{T}_4)^{s_T})$$

を検証し成立すれば σ_T を受理し，さもなくば棄却する．

3.8 セキュリティ

[補題 1]　3.2.1 節の (e_i, A_i, x_i) は，Ateniese らのグループ署名 [2] の署名鍵 (S_K) である．このとき強 RSA 仮定のもとで，グループマネージャ (M) の作り出す S_K の数が多項式有限であれば，CL として公開されている以外の組 (e_i, A_i, x_i) は，M 以外が生成することはできない．

(証明) 文献 [2] の Theorem1 より明らかである．

[定理 1]　提案方式は，強 RSA 仮定，DDH 仮定及びランダムオラクルモデルのもとで，2.1 節のセキュリティ要件（健全性，利用者の正当性，課金の正当性，コンテンツの安全性及び利用者のプライバシ）を満たす．

(健全性) D は U 及び T が出力する署名 $(\sigma_1, \sigma_{e_j}, \sigma_{r_{01}}, \sigma_{e_{j2}}, \sigma_U, \sigma_T)$ により，U 及び T がプロトコルに従っていることを検証できる．同様に，U は D が出力する署名 (σ_D) により，D がプロトコルに従っていることを検証できる．

(利用者の正当性) 署名 (σ_1, σ_D) の完全性と健全性の性質により，U の要求が正しい時，U はコンテンツ復号鍵 (κ_j) を得る．

(課金の正当性) 合算サーバの (t,t) しきい値復号，課金情報 $(\bar{T}_4, \bar{T}_5)$ の準同型性及び [補題 1] より本定義は満たされる．

(コンテンツの安全性) 提案方式のコミットフェーズにおけるコンテンツ復号鍵 (κ_i) の受け渡しは，AdaptiveOT_t^n [14] を利用している．文献 [14] の 4 章の Sender's Security より，$\bar{U}$ は $\kappa_j (j \notin \{k(1), \ldots, k(m)\})$ を計算することが出来ない．

(利用者のプライバシ) 提案方式の σ_1 は，Ateniese らのグループ署名 [2] の署名であり，DDH 仮定とランダムオラクルのもとで，匿名性及びリンク不能性を満たしたいる．さらに，$\sigma_{e_j}, \sigma_{r_{01}}, \sigma_{e_{j2}}$ のゼロ知識性により，本定義は満たされる．

[定理 2]　3.2 節で示した提案方式において，利用者の計算量及び通信量は，利用可能なコンテンツ総数に依存せず，利用者が利用したコンテンツ数のみに依存する．

(証明) 提案方式では，署名長が一定なグループ署名 [2] を利用している．また，利用する SPK の通信量は，利用可能なコンテンツの総数に依存せずセキュリティパラメータのみに依存する．

4. 結論と課題

本稿において，我々は利用履歴を秘匿できるコンテンツ配送・課金方式（CDCS）のモデルを整理し，Ateniese らのグループ署名 [2] を利用した構成を提案した．提案方式は，CDCS のセキュリティ要件を満たした上で，計算量及び通信量が利用者が利用したコンテンツ数のみに依存している．今後，CDCS の一般的な構成を示し，さらに short group signature [4] 等への応用を検討する．

文　献

[1] M Abe, M Ohkubo and K Suzuki : 1-out-of-n Signatures from a Variety of Keys. Proc. ASIACRYPT'02, LNCS 2501, pp.415–432, Springer, 2002.

[2] G. Ateniese, J. Camenisch, M. Joye and G. Tsudik : A practical and provably secure coalition-resistant group signature scheme. Proc. CRYPTO 2000, LNCS 1880, pp.255–270, Springer, 2000.

[3] D. Boneh : The decision Diffie-Hellman problem. In Algorithmic Number Theory (ANTS-III), LNCS 1423, pp.48–63, Springer, 1998.

[4] D. Boneh, X. Boyen and H. Shacham : Short Group Signatures. Proc. CRYPTO 2004, LNCS 3152, pp. 41–55, Springer, 2004.

[5] F.Boudot : Efficient Proofs that a Committed Number Lies in an Interval. Proc. EUROCRYPT'00, LNCS 1807, pp.431–444, Springer, 2000.

[6] J. Camenisch and M. Michels : A group signature scheme with improved efficiency. Proc. ASIACRYPT'98, LNCS 1514, pp.160–174, Springer, 1998.

[7] A.Chan, Y.Frankel and Y.Tsiounis : Easy Come-Easy Go Divisible Cash. Proc. EUROCRYPT'98, LNCS 1403, pp.561–575, Springer, 1998.

[8] R. Cramer, I. Damgard and B. Schoenmakers : Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. Proc. CRYPTO 1994, LNCS 839, pp.174–187, Springer, 1994.

[9] R. Cramer, R. Gennaro, B. Schoenmakers : A Secure and Optimally Efficient Multi-Authority Election Scheme. Proc. EUROCRYPT'97, LNCS 1233, pp.103–118, Springer, 1997.

[10] E. Fujisaki and T. Okamoto : Statistical zero knowledge protocols to prove modular polynomial relations. Proc. CRYPTO 1997, LNCS 1297, pp.16–30, Springer, 1997.

[11] 藤原晶, 岡村真吾, 吉田真紀, 藤原融 ：コンテンツ配信サービス提供者だけが試聴動向を把握できる委託配信システム. SCIS 予稿集, pp.487–492, 2004.

[12] 藤原晶, 岡村真吾, 吉田真紀, 藤原融 ：マーケティング情報が保護されたオフライン委託配信システム. CSS2004 論文集, pp.469–474, 2004.

[13] 小西祥之, 吉田真紀, 藤原融 ：分岐構造をもつコンテンツに対する分岐選択履歴を配信者から秘匿可能な配信システム. CSS2003 論文集, pp.367–372, 2003.

[14] W. Ogata, K, Kurosawa : Oblivious keyword search. Journal of Complexity, Vol.20 No.2–3, pp.356–371, 2004.

[15] M. Rabin : How to exchange secrets by oblivious transfer. Technical Report TR 81, Aiken Computation Lab, Harvard University 1981.

[16] 山本 博紀, 土井 洋, 真島 恵吾, 藤井 亜里砂 ：利用履歴を秘匿できるコンテンツ配信・課金方式に関する考察. CSS2005 論文集, pp.451–456, 2005.

[17] http://www.tv-anytime.org/

[18] Broadcast Technology No.12, NHK Science and Technical Research Laboratories, Autumn 2002. http://www.nhk.or.jp/strl/publica/bt/en/frm-set-le12.html

[19] ETSI TS 102 822-2 V1.3.1 : Broadcast and On-line Services : Search, select, and rightful use of content on personal storage systems ("TV-Anytime") ; Part 2 : System description, etc.

[20] ETSI TS 102 822-6-3 V1.1.1 : Broadcast and On-line Services : Search, select, and rightful use of content on personal storage systems ("TV-Anytime") ; Part 6 : Delivery of metadata over a bi-directional network ; Sub-part 3 : Phase 2 - Exchange of Personal Profile, etc.