情報処理学会論文誌 Vol. 50 No. 9 2228–2242 (Sep. 2009)

利用履歴を秘匿できるコンテンツ配信・課金方式に関する研究

飛田 孝幸[†1,*1] 山本 博紀[†2]
土井 洋[†1] 真島 恵吾[†3]

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，サーバ型放送等デジタル放送の高度化により，通信と放送を融合した高度な情報サービスの普及が期待されている．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（視聴したコンテンツの ID や単価）はプライバシの観点から秘匿されることが望ましい．一方，有料サービスにおいては，視聴内容に応じた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．本稿ではこれらの要件を満たす効率の良いコンテンツ配信・課金方式の構成方法を提案する．さらに提案方式の理論的性能評価について報告する．

Research of Privacy-enhanced Content Distribution and Charging Scheme

Takayuki Tobita,[†1,*1] Hironori Yamamoto,[†2]
Hiroshi Doi[†1] and Keigo Majima[†3]

The number of users of content distribution services utilizing broadcasting and networks, such as broadcasting based on home servers, has grown. In these services, it is desirable that the user's usage history are kept confidential in order to protect privacy. On the other hand, the usage charges need to be calculated correctly based on the contents received by the user. In this paper, we propose efficient constructions of the content distribution and charging scheme satisfying above requirements. Furthermore, we discuss the efficiency of two concrete schemes.

1. はじめに

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，デジタル放送の開始により放送と通信ネットワークの融合による新しい情報サービスが期待されている．TV Anytime Forum[21] はその代表例であり，蓄積機能を持ったデ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[24]．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デ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．この標準化は，権利マネジメントおよび保護，利用者のプライバシとセキュリティおよび金銭取引も視野としている[25]．こういったサービスでは，利用者のコンテンツの視聴にともなう利用履歴はプライバシの観点から秘匿することが望ましい．一方，利用者およびコンテンツ配信事業者の双方にとって，視聴内容に応じた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．文献 9)，10)，12) 等でも利用者のプライバシを意識したコンテンツ配信方式が研究されているが，コンテンツ視聴時の各コンテンツの単価が秘匿されていないために利用履歴が推測される可能性がある．たとえば**表 1** のようなコンテンツリストが公開されている環境で，1 カ月間に利用者が 4 つのコンテンツを視聴し，その合計金額が 600 円であった場合を考えたとき，通信ごとの単価が秘匿されていれば，利用者の利用履歴の組合せは複数あり特定されない．しかし単価が秘匿されておらず，通信ごとの単価が 100 円 3 回と 300 円 1 回であった場合，利用者の利用履歴は $\{A, B, C, H\}$ であると容易に特定されてしまう．

一方，単価が等しいコンテンツグループが複数設けられている場合も考えられる．**表 2** は，カテゴリごとに同一単価であるコンテンツ群 $\{A_i\}$，$\{B_i\}$，$\{C_i\}$ が提供され，単価が各々50 円，100 円，150 円の場合である．ある利用者が，1 カ月間に 8 コンテンツを利用し，総額が 800 円であった場合を考える．視聴した 8 コンテンツがすべてカテゴリ B であ

†1 情報セキュリティ大学院大学
Institute of Information Security
†2 中央大学
Chuo University
†3 NHK 放送技術研究所
Science and Technical Research Laboratories, JAPAN BROADCASTING CORPORATION (NHK)
*1 現在，みずほ情報総研株式会社
Presently with Mizuho Information & Research Institute

© 2009 Information Processing Society of Japan

表 1　コンテンツリスト（例 1）
Table 1　Example of the contents list 1.

コンテンツ ID	A	B	C	D	E	F	G	H
単価	100 円	100 円	100 円	150 円	150 円	200 円	200 円	300 円

表 2　コンテンツリスト（例 2）
Table 2　Example of the contents list 2.

コンテンツ ID	A_i	B_i	C_i
単価	50 円	100 円	150 円

るか，それともカテゴリ A，C が 4 つずつであるかを識別ができない方が，利用者の嗜好が漏えいしないという観点からは望ましい．

そこで本稿では，コンテンツ視聴時のコンテンツ単価も含めた利用履歴を秘匿できるコンテンツ配信・課金方式（以下 CDCS）を提案する．

CDCS は視聴傾向も含めて利用履歴を完全に秘匿するため，現在の TV 放送の視聴と同様のプライバシを通信・放送融合によるサービスにおいて実現するといえる．完全な秘匿は，コンテンツ配信事業者の視聴傾向を収集したいという要件に反する場合があるが，この要件は TV 放送における視聴率調査と同様に，別プロトコルを併用することにより可能であるため，本稿では要件として扱わない．

CDCS は，各コンテンツの単価が均一であれば，利用者が視聴したコンテンツ数と単価から Adaptive Oblivious Transfer [14] を用いて実現することができる．しかし一般に各コンテンツの単価は一定ではないため，コンテンツ視聴時のコンテンツ単価を秘匿したまま，一定期間ごとの合計金額のみを正しく計算する方式の構築は容易ではない．実際，6 章および付録 A.2 に示すように，各コンテンツの単価が一定でない場合にも，単価の種類ごとに Adaptive Oblivious Transfer を用いる等の工夫により，高速な方式を実現することは可能である．しかし，コンテンツ単価の秘匿は実現できない．

Priced Oblivious Transfer [1] や，1-out-of-n 署名を用いて構成した CDCS [20] はこれらの要件を満たすが，6 章および付録 A.2 に示すように，利用者やコンテンツ配信事業者の計算・通信コストの一部がコンテンツ総数に比例する．実社会におけるデジタル放送受信機向けのサービスを考えた場合，コンテンツ総数が巨大になる可能性が高く，限られた応用分野を除いて，コンテンツ総数に比例する部分がないプロトコルを利用するのが望ましいと考えられる．

そこで我々は，グループ署名[3),7)] を用いることにより計算・通信コストを一定とした効率的な方式を 2 種類提案する．また，それらの方式の理論的性能評価について報告する．

1.1 関 連 研 究

1.1.1 Adaptive Oblivious Transfer

Oblivious transfer [15]（以下 OT）は 1981 年に Rabin により提案され，その後 Adaptive OT_t^n [14] 等の応用が提案されている．Adaptive OT_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おり，コミットフェーズでサーバ（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）はコミットされた n 個のインデックスから任意に t 個のインデックス（$\{k(i)\}_{1 \le i \le t}$）を選択し，秘密情報 $\{C_{k(1)}, \cdots, C_{k(t)}\}$ を得る．ただしこの際，U は $\{C_{k(1)}, \cdots, C_{k(t)}\}$ 以外の秘密情報は得られず，D は $\{k(1), \cdots, k(t)\}$ についての情報をいっさい得られない．

1.1.2 知識の署名（SPK）

知識の署名（SPK）とは，知識のゼロ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，文献 6) 等と同様，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 $m \in \{0,1\}^*$ は署名するメッセージを表している．たとえば $y = g^\alpha$ を満たす離散対数 α を知っていることの SPK は，$SPK\{(\alpha) : y = g^\alpha\}(m)$ と記述する．また，文献 2) 等で 1-out-of-n 署名として知られている SPK は，n 個の秘密のうちの，1 個を知っていることの SPK であり，$SPK\{(\alpha_k) : \bigvee_{i \in \{1,\cdots,n\}} g^{\alpha_i} = h\}(m)$ と記述する．これに対して文献 3), 7) 等のグループ署名は，管理者により配布されたメンバ証明書とメンバ秘密情報の正しい組合せのうちの，1 個を知っていることの SPK であるといえる．

SPK により離散対数の範囲を証明することもできる．たとえば文献 5) で紹介されている方式は，$[0, b]$ の範囲で設定した離散対数 x に対して，より広い範囲（t および l をセキュリティパラメータとし，$[-2^{t+l}b, 2^{t+l}b]$ の範囲）に含まれる離散対数 x を知っていることの SPK であり，$SPK\{(x) : E = g^x h^r \wedge x \in [-2^{t+l}b, 2^{t+l}b]\}$ と記述する．

2. モデルと要件

提案するコンテンツ配信システムの構成を**図 1** に示す．本モデルは，配信サーバ（D），

© 2009 Information Processing Society of Japan

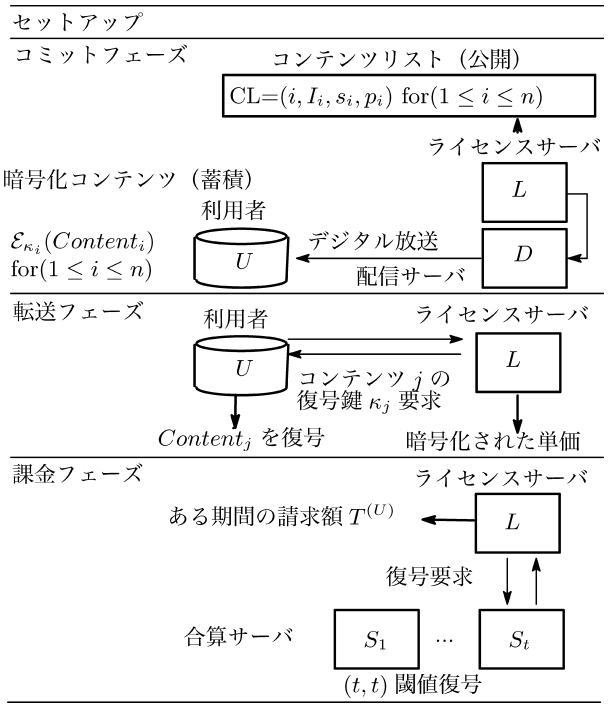

図 1　モデル図
Fig. 1　Outlines of the model.

複数の利用者（U）[⋆1]，ライセンスサーバ（L），そして複数の合算サーバ（S_i）の 4 つのエンティティにより構成される．具体的な例としては U は各家庭に設置された専用のデジタル放送受信機，L はコンテンツを配信するプロバイダ，D は L が利用する放送衛星等のデジタル放送設備を想定することができる．また S_i は L と独立した機関と考えることができる．ここで D は秘密鍵の保持や暗号化および復号の処理は行わないため，理論上 D と L を 1 つのエンティティと見なすこともできる．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，D 以外のエンティティの秘密鍵・公開鍵（$SK_i, PK_i (i = L, U, S_1, \ldots, S_t)$）を生成する[⋆2]また，このフェーズは 1 度だけしか実行されないことから，本稿ではセットアップフェーズの間のみ存在する信頼できる第三者機関の存在を仮定し，個々のエンティティが生成すべき（$SK_i, PK_i (i = L, U, S_1, \ldots, S_t)$）以外のパラメータを信頼できる第三者機関[⋆3]が生成することとする．

コミットフェーズでは，L が各コンテンツ（$Content_i$）をコンテンツ鍵（κ_i）により暗号化した暗号化コンテンツ（$\mathcal{E}_{\kappa_i}(Content_i)$）を D を用いて U に送付し，$\mathcal{E}_{\kappa_i}(Content_i)$ は U のストレージに蓄積される[⋆4]．ここでの送付とは放送衛星等からのブロードキャストが考えられる．同時に，L はコンテンツリスト（CL）を配布，もしくは公開する．なお，CL が事前に配布もしくは公開され，後日 $\mathcal{E}_{\kappa_i}(Content_i)$ の放送時に購入しておいたコンテンツのみ視聴できるといったシステムも可能だが，本稿では簡単のために事前に $\mathcal{E}_{\kappa_i}(Content_i)$ も送付されていることとして説明する．なお本フェーズの間は，L は信頼でき，U は正しいデータを受け取るとする．CL は (i, I_i, A_i, p_i) により構成される．i はインデックス（$1 \le i \le n$），p_i はコンテンツの価格，A_i は転送フェーズ以降のプロトコルで用いるコンテンツ ID，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，U は CL から視聴したいインデックス j のコンテンツを選び，L と通信することによりコンテンツ復号鍵 κ_j を得る．このとき，L は U が視聴するコンテンツの単価 p_j の情報を代わりに得るが，U の利用履歴を秘匿するため，暗号化した形（$\mathcal{E}_S(p_j)$）で得ることとする．本フェーズの間は U が不正を行ったとしても κ_j 以外のコンテンツ復号鍵は得られず，また L が不正を行ったとしても U の得たコンテンツに関する情報は得られないことが要件となる．これは，具体的にはオペレータや外部侵入者による情報漏えい対策が考えられるが，たとえ L が不正を働いても U のプライバシ（利用履歴）が保護されるという，CDCS を利用するうえでの信頼性を保つために必要な保証である．

課金フェーズでは（たとえば毎月 1 度），L は合算サーバ S_i（$i = 1, \ldots, t$）の協力を得て，(t,t) 閾値復号により利用者への請求金額（利用料金の合算値）$T^{(U)}$ のみを計算する．ただし本フェーズを実行するためには U の同意を必要とする．これは，L が S_i を任意に用いることにより不正にコンテンツ単価を復号し，U の利用履歴を推測することを防止するために

⋆1 記述を簡単にするために，利用者 U にはインデックスをつけないが，モデルとしては複数利用者を対象としている．

⋆2 SK_U，PK_U は記述を簡略化するため，セットアップフェーズで生成するものとする．

⋆3 利用者利益の確保・向上の観点から，情報セキュリティや視聴者のプライバシの取扱いに関して責任を持つ機関等が考えられる．

⋆4 すべてのコンテンツが蓄積される必要はなく，期間，チャネル，ジャンル等で選択されて蓄積される．

© 2009 Information Processing Society of Japan

必要となる．なお，転送フェーズおよび課金フェーズにおいて，すべての S_i（$i = 1, \ldots, t$）が結託して不正を行うことはないと仮定する．これはすべての S_i が結託することにより，転送フェーズの通信盗聴による p_j の復号と，課金ファーズで $T^{(U)}$ の計算ができることを防ぐために必要となる．また S_i を分散してもすべての通信を盗聴されると $T^{(U)}$ が漏洩してしまう．$T^{(U)}$ は利用履歴ではないものの，一般に請求金額が漏洩するのは好ましくないため，L と各 S_i の間は秘匿された通信路（SSL 等）を使用することとする．

課金フェーズの後，L は請求処理[⋆1]を行う．請求金額に対して L による不正請求，もしくは U が正当な金額を認めない場合，課金フェーズで付加した U の署名（同意）を用いて裁判等で不正であることを証明できる．またその際も利用者の視聴したコンテンツの単価は漏洩しないことを目標とする．

ここで，利用者の毎月の合計金額（$T^{(U)}(= \sum p_{k(i)})$）は，たかだか 10^6 程度[⋆2]と仮定する．この仮定は，実社会において 1 人の利用者が 1 カ月間に 100 万円以上の金額を視聴することは考えにくいため，適切であるといえる．

なお，本稿では，コンテンツの復号作業は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数の利用者を想定した多くのデジタル放送システムで想定されており[23]，コンテンツ復号鍵 κ_j の購入者以外への漏洩を防止するために SK_U と SK_U から計算される κ_j を保護するために用いるが，我々の方式ではたとえセキュリティモジュールが機能しなくても，利用者は購入した κ_j 以外を計算によって得ることはできないこととする．

2.1　システム要件

まず，システムとしての要件を整理する．

R1　U が視聴したコンテンツおよび単価の情報が漏洩しない．

R2　U は L に要求したコンテンツ復号鍵を正しく得ることができる．

R3　転送フェーズにおいて U が正規の L と交信していることが保証される．

R4　L は U が一定期間に視聴したコンテンツの合計金額を S_i と協力することによってのみ，正しく計算することができる．

R5　U は L が U に配信したコンテンツ復号鍵以外の復号鍵に関する情報を得ることができない．

⋆1 たとえば紙による請求等．

⋆2 文献 8) から，この上限は離散対数への総当たりによる計算が可能な範囲である．解の候補をメモリ上に展開し，マッチングすることを考えると，現在のサーバ用マシン数台を用いて，10^{10} 程度までは可能である．

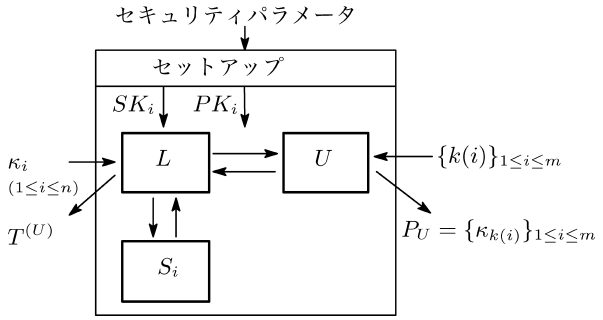

図 2　機能要件図
Fig. 2　Function requirements.

R6　転送フェーズにおいて L が正規の U と交信していることが保証される．

R7　課金フェーズにおいて L が正規の S_i と交信していることが保証される．

R8　転送フェーズにおける L や U の計算・通信コストが小さくなる．

R9　S_i は単独ではコンテンツの合計金額を計算することができない．

R1〜R3 は利用者（U）からのセキュリティやプライバシに関する要件であり，R5〜R7 はライセンスサーバ（L）からのセキュリティに関する要件である．そして R4，R9 は課金に関する要件である．

本稿では，デジタル放送により，暗号化コンテンツがデジタル放送受信機（U）にあらかじめ蓄積されていることを想定している．そのため，性能に関しては実際にコンテンツを利用する際に要する転送フェーズの計算・通信コストを小さくすることを要件（R8）とした．実際，各家庭に設置される U の計算・通信コストを小さくすることは必要な要件であるといえる．

2.2　セキュリティとプライバシの定義

セキュリティとプライバシの定義を行うために，モデル図（図 1）を**図 2** のように 1 つのシステムとして記述する．ここで，SK_i はセットアップにより生成する L，U，S_i への秘密の入力，PK_i は公開情報と見なすことができる．さらに，U は n 個のコンテンツから任意に m 個を選択したとすると，L の秘密の入力は $\{\kappa_i\}_{1 \le i \le n}$，$L$ の秘密の出力は $T^{(U)}$ であり，U の秘密の入力は $\{k(i)\}_{1 \le i \le m}$，U の秘密の出力は $\{\kappa_{k(i)}\}_{1 \le i \le m}$，と見なすことができる．なおここで秘密の入出力とは，機密性および正当性が保たれた通信である．

なお，説明を簡潔にするために，$P_U = \{\kappa_{k(i)}\}_{1 \le i \le m}$，すなわち U が CL から選択した

© 2009 Information Processing Society of Japan

コンテンツ $k(i)$（$1 \leq i \leq m$）に対して L から得た情報の集合とする．

さて，2.1 節で示した要件のうち，R3，R6 および R7 は相手認証を意味している．これは，電子署名等で達成することができるので，以後 R3，R6 および R7 は満たされているとして議論する．また，プロトコルを定めれば，L，U，S_i が正しく動作していることは，知識の署名（SPK）を付加することにより保証できる．この結果，R2 や R4 に対する不正（値の改変）を防ぐことができる．なお，R4 が満たされており，L と S_i の通信路が秘匿されている場合，(t,t) 閾値復号を用いることができれば R9 を満たすことは可能である．

逆に，各エンティティがきちんと認証されており，各エンティティがプロトコルに従ったときには，

(1)　各エンティティが適切な情報を得ることができること，

(2)　得られるべきではない秘密情報を得ることができないこと，

を実現するように設計する必要がある．

これらの考察から，プロトコルに強く依存する要件（R1，R2，R4，R5）については，以下に述べる 4 つの定義を満たすことを示す必要がある．

定義 1　（R2）U は $k(i)$（$1 \leq i \leq m$）を入力すると，$\kappa_{k(i)}$ を得る．　□

定義 2　（R4）L とすべての S_i（$i = 1, \ldots, t$）がプロトコルに従って協力したときのみ，合計金額 $T^{(U)} = \sum_{i=1}^{m} p_{k(i)}$ を，得ることができる．　□

定義 3　（R5）$\{k(i)\}_{1 \leq i \leq m}$，$P_U$，$SK_U$[⋆1]および公開情報（$PK_i$，$T^{(U)}$，すべての通信）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 3 は，たとえ悪意のある U でも購入したコンテンツ以外の情報を知ることはできないことを意味する．

定義 4　（R1）$\{\kappa_i\}_{1 \leq i \leq n}$，$SK_L$ および公開情報（PK_i，$T^{(U)}$，すべての通信）のみで識別できる場合を除き，それらを入力とし，$j \in \{1, \cdots, n\}$ において $\kappa_j \in P_U$ もしくは $\kappa_j \notin P_U$ を多項式時間で識別するようなアルゴリズム $\bar{L}$ は存在しない．　□

定義 4 は，たとえ悪意のある L でも公開情報のみで識別できる場合[⋆2]を除き，U がどのコンテンツを利用したかの情報を知ることはできないことを意味する．

⋆1 セキュリティモジュールを想定した場合，P_U および SK_U は入力として与えられないが，我々の提案方式はそれらを入力に加えたより強い要件を満たす．

⋆2 たとえば U が 1 カ月に 1 つの特徴的な価格のコンテンツしか利用しなかったため，公開情報である $T^{(U)}$ と通信回数から U の利用したコンテンツが特定されてしまう場合が考えられる．

3. 構成方法の検討

提案方式の説明のために，本章で，まず構成方法についてのインフォーマルな議論を行う．続いて，4 章および 5 章において具体的な方式の提案を行う．

すでに 1 章で述べたように，各コンテンツの単価が均一ならば，Adaptive OT_t^n を利用することにより，CDCS を実現できる．本稿でも基本的には Adaptive OT に近い構成を利用するが，各コンテンツの単価が異なることに注意する必要がある．我々のプロトコルは，セットアップ，コミットフェーズ，転送フェーズ，課金フェーズから構成され，詳細を以下に述べる．なお，以下に述べるプロトコルにおいて，各エンティティ間のやりとりでは，送信者（データ生成者）はデータにその電子署名を付加して送信し，受信者は電子署名を検証することとする．これにより相手認証を達成するとともに，改ざんも防ぐことが可能となる．

3.1 プロトコル

3.1.1 セットアップ

システム全体が共有するパラメータ，ライセンスサーバ（L），利用者（U）および合算サーバ（S_i）の秘密鍵と公開鍵（$SK_i, PK_i (i = L, U, S_1, \ldots, S_t)$）を生成する．

3.1.2 コミットフェーズ

L は，n 個のコンテンツ（$Content_i$）をコンテンツ鍵 κ_i で暗号化した暗号化コンテンツ（$\mathcal{E}_{\kappa_i}(Content_i)$）を，$U$ に送る．

次に L は U が，次に述べる転送フェーズで得る出力および E_i から κ_i を得ることができるように暗号化した，n 個の暗号化コンテンツ復号鍵（$E_1, \cdots, E_n$）を U に送る．

最後に，L はコンテンツリスト（$CL = (i, I_i, A_i, p_i)$（$1 \leq i \leq n$））を生成して公開する．

3.1.3 転送フェーズ

U は得たいコンテンツ j に対して κ_j を得るために，コンテンツ ID（A_j）を用いて，$\mathcal{E}_U(A_j)$ を L に送る．これに加えて，暗号化した（均一ではない）コンテンツ単価 $\mathcal{E}_S(p_j)$ も同時に送るが，さらに A_j と p_j のインデックスが同一で，CL の中のうちの 1 つであることの知識の署名（SPK）を付加する．

L は受け取ったデータおよび SPK を検証し，正しければ U に E_j から κ_j を得るための情報を送る．U は結果として κ_j を得る．なおこの際 L は正しく処理を行っていることを証明する SPK を付加し，U は SPK の検証を行う．

3.1.4 課金フェーズ

最初に L は U との通信で得た m 個の暗号化コンテンツ単価 $\mathcal{E}_S(p_{k(i)})$（$1 \leq i \leq m$）を合

© 2009 Information Processing Society of Japan

算した $\mathcal{E}_S(\sum_{i=1}^{m} p_{k(i)})$ を生成し，これを U に送る．U は受け取ったデータと，自身に保存されている暗号化した利用履歴を比較し，正しければ $\mathcal{E}_S$（$\sum_{i=1}^{m} p_{k(i)}$）に U の署名（σ_{U2}）を付加して L に返す．

次に L は U から受け取った署名と $\mathcal{E}_S(\sum_{i=1}^{m} p_{k(i)})$ を S_i に送る．

最後に S_i は σ_{U2} を検証し，正しければ (t,t) 閾値復号により L は $\sum_{i=1}^{m} p_{k(i)}$ を得る[⋆1]．この際，T_i はプロトコルに従って処理をしていることを証明する SPK を付加する．

3.2　安全な構成方法

本節では，安全な構成方法についてのインフォーマルな議論を行う．3.1 節で示した構成とする場合，まず，送信データに電子署名を付加していることから，R3，R6，R7 を満たすことは可能である．具体的な構成は 4 章および 5 章で示すが，各エンティティの不正がないことを SPK で証明しているので，R2（定義 1）と R4（定義 2）を満たすことは可能である．同時に，コンテンツ ID およびコンテンツ単価については，識別不可能性を有する適切な暗号化を行い，3.3 節で示す Adaptive OT に似た技術を用い，暗号化されたコンテンツ ID からコンテンツ鍵を U が得ることができるようにすれば R1（定義 4），R5（定義 3）を満たすことも可能となる．なお，R4 を満たした状態において，L と S_i の通信路が秘匿され，(t,t) 閾値復号を用いていることから R9 も満たすことは可能である．これらの要件のうち，R1，R2，R4，R5 を満たすか否かは具体的な実現方式に強く依存する．

利用者 U にとって負担となるコンテンツ ID の暗号文 $\mathcal{E}_U(A_j)$，およびコンテンツ単価の暗号文 $\mathcal{E}_S(p_j)$ のインデックスが等しいことの SPK は，たとえば 1-out-of-n 署名を用いて構成することができる[20]．しかしこの構成は，ライセンスサーバ（L）や利用者（U）の計算・通信コストがコンテンツ総数に比例して大きくなってしまうので，R8 を満たしているとはいい難い．R8 を満たすためには，独自の SPK を付加するというアプローチも可能であるが，本研究では性能等の向上が著しく，実用化の可能性もあるグループ署名を利用して SPK を構成した．SPK の一部にグループ署名を用いることにより，1-out-of-n 署名を用いて構成した場合に比べて，転送フェーズにおける計算・通信コストが，コンテンツ総数に依存せず一定となる．これはコンテンツ総数が膨大となるコンテンツ配信サービスにおいて有効であり，一般的に計算・通信コストが大きいグループ署名を用いても 6 章で評価するとおり十分効率が良い．ただしグループ署名本来の利用方法とは異なり，本来は秘密にすべきグループ署名鍵をコンテンツリスト（CL）の一部として公開するという点が，我々の方式の特徴である．グループ署名の結託耐性から，複数のグループ署名鍵を公開しても安全性に影響はない．

3.3　コンテンツ鍵を得る仕組み

本節では，コンテンツ ID（A_j）の暗号文から，コンテンツ鍵 κ_j を得るための情報を得る仕組みについて説明する．本稿で使う仕組みでは，A_j に対して，コンテンツ鍵を得るための情報 $(A_j)^{w}$[⋆2]を得る．なお，このように $(A_j)^{w}$ を得るという構成は，たとえば文献 14) 等でも用いられている．具体的には，識別不可能な確率的暗号関数である ElGamal 暗号関数 $\mathcal{E}$（ただし，U の公開鍵を使う）を用いて，

(1)　U は $\mathcal{E}(A_j)$ を L に送り，

(2)　L は $\mathcal{E}(A_j)^{w}$ を ElGamal 暗号の準同型性を用いて計算し，さらに乱数 r を用いて再暗号化した結果 $(\mathcal{E}(A_j)^{w}\mathcal{E}(1)^{r})$ を U に返す，

という方法を利用する．この構成の場合，L は $\mathcal{E}(A_j)$ から A_j の情報を得ることができない．その一方，U は $(A_j)^{w}$ を得ることができるが，これ以外の情報を得ることはできない．この Adaptive OT に似た技術を用い，4 章および 5 章で示すように，R1（定義 4），R5（定義 3）を満たすことを可能とする．

4.　グループ署名 ACJT2000 を利用した方式

本章ではグループ署名 ACJT2000[3] を利用した具体的な方式[18),19)] を示す．

4.1　仮　　定

本方式の安全性は，強 RSA 仮定，（位数が未知である群上での）DDH 仮定およ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' がすべて素数となる 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，以下の仮定を満たすと仮定する．

4.1.1　強 RSA 仮定

G を $QR(N)$ とする．このとき，N および $z \in G$ を入力とし，無視できない確率で $z \equiv u^{e} (\mathrm{mod} N)$ となる $u \in G$ および $e \in \mathbb{Z}_{>1}$ を出力する確率的多項式時間アルゴリズム

⋆1 離散対数の位数が既知であれば，文献 26) で t 人中 n 人以上の協力があればメッセージ（M）を復号可能な (n,t) 閾値復号が説明されている．位数が未知の場合でも，(t,t) 閾値復号であれば準同型性を持つ ElGamal 暗号を用いて簡単に構成できる．$S_1,\ldots,S_t$ 個の秘密鍵と公開鍵 $(SK_i, PK_i) = (\tau_i, h_{S_i} = g^{\tau_i})$ を生成し，U は $h_S(=\prod h_{S_i})$ を用いて，$(T_4,T_5) = (g^r, Mh_S{}^r)$ を計算し L に送る．L は (T_4,T_5) をすべての S_i に送り，S_i は $\hat{T}_{4i} = T_4{}^{\tau_i}$ を計算し L に送る．L は t 個の $\hat{T}_{4i}$ から $M = T_5/\prod \hat{T}_{4i}$ を計算できる．

⋆2 w は L の秘密鍵であり，$(A_j)^{w}$ は L にしか計算できない．

© 2009 Information Processing Society of Japan

は，存在しない[3]．

4.1.2 DDH 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識別する確率的多項式時間アルゴリズムは存在しない[4]．

4.1.3 RSA-KTI 仮定

G を $QR(N)$ とし，(N, e) を RSA 公開鍵，d を秘密鍵とし，$u_k \equiv z_k^d (\mathrm{mod} N)$ とする．このとき，$\{z_1, \ldots, z_{m+1}\} \in_R G$, $\{u_1, \ldots, u_m\}$ および公開鍵を入力とし，$u_{m+1} \in G$ 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[14]．

4.2 プロトコル

ここでは簡単のために，合算サーバを 1 つとし S と表す[⋆1]．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，公開情報および署名鍵を作るために，セットアップ時のみ利用する．また，各エンティティ間のやりとりでは，送信者（データ生成者）はデータにその電子署名を付加して送信し，受信者は電子署名を検証することとする．また，L と S_i の通信路は，SSL 等を用いて秘匿されているものとする．

4.2.1 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[3]）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 および γ_3 を加えたものとする（ここで文献 3) 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 $\Lambda = [2^{\lambda_1} - 2^{\lambda_2}, 2^{\lambda_1} + 2^{\lambda_2}]$ および $\Gamma = [2^{\gamma_1} - 2^{\gamma_2}, 2^{\gamma_1} + 2^{\gamma_2}]$ を定義する）．さらに，$\mathcal{H} : \{0,1\}^* \to \{0,1\}^k$ を衝突困難性を持ったハッシュ関数とし，G を疑似乱数生成関数とする．

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 N（$= pq$）および a，a_0，g，$h \in_R QR(N)$ を公開する．

次に，ライセンスサーバ（L）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 $e_i (= 2^{\gamma_3} e_{i1} + e_{i2}) \in_R \Gamma$（**図 3**，および付録 A.2 参照），$A_i = (a^{x_i} a_0)^{1/e_i} \bmod N$ を生成して，(e_i, A_i, x_i) を L 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

⋆1 3.1.4 項で示した閾値復号により t 個のサーバに分散することは可能である．

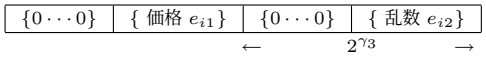

図 3　素数 e_i の構成方法
Fig. 3　Construction of the prime number e_i.

開鍵をそれぞれ

$(SK_L, PK_L) = (\omega, h_L = g^\omega \bmod N)$，$(SK_U, PK_U) = (\chi, h_U = g^\chi \bmod N)$，
$(SK_S, PK_S) = (\tau, h_S = g^\tau \bmod N)$

と設定し，h_L，h_U，h_S を公開する．

4.2.2 コミットフェーズ

step1　L 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）．次に，$Content_i$ を暗号化アルゴリズム $\mathcal{E}$ とコンテンツ鍵 κ_i で暗号化した $\mathcal{E}_{\kappa_i}(Content_i)_{(i=1,\ldots,n)}$ を U に送る．

step2　ライセンスサーバ（L）は，$i = 1, \ldots, n$ について，

$$K_i = (A_i)^\omega \bmod N,\ E_i = G(K_i \parallel A_i) \oplus \kappa_i$$

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．

4.2.3 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，$r_{01} \in_R \{0,1\}^{2l_p}$ および，$r_{02} \in_R [-2^s n + 1, 2^s n - 1]$ を生成し

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

を計算する．次に 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，

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

を計算する．最後に U は $c = \mathcal{H}(g \parallel h_S \parallel h_U \parallel a_0 \parallel a \parallel T_1 \parallel T_2 \parallel T_3 \parallel d_1 \parallel d_2 \parallel d_3 \parallel d_4 \parallel ID)$ を計算し，$s_1 = r_1 - c(e_i - 2^{\gamma_1})$，$s_2 = r_2 - c(x_i - 2^{\lambda_1})$，$s_3 = r_3 - c e_i r_0$ および $s_4 = r_4 - c r_0$ 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 3) のグループ署名であり，U が（T_1, T_2, T_3）を正しく計算したことと，選択したコンテンツの（e_j, A_j, x_j）が CL の中のどれか 1 つの組であることを証明している．また（T_1, T_2），（T_5, T_4）はそれぞれ 3 章の $\mathcal{E}_U(A_j)$，

© 2009 Information Processing Society of Japan

$\mathcal{E}_S(p_j)$ に対応した 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 の詳細は付録 A.1.1，A.1.2 および A.1.3 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ことと，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 内はすべて法 N である）．

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

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

step3　L は $(\sigma_1, \sigma_{e_j}, \sigma_{r_{01}}, \sigma_{e_{j2}}, \sigma_U)$ を検証し，正しければ $r_L \in_R \{0,1\}^{2l_p}$ を生成して

$$K' = (T_1', T_2') = (h_U^{r_L} T_1^{\omega}, g^{r_L} T_2^{\omega}),$$
$$\sigma_L = SPK\{(\omega, r_L) : h_L = g^{\omega} \wedge T_2' = g^{r_L} T_2^{\omega} \wedge T_1' = h_U^{r_L} T_1^{\omega}\}$$

を計算し（K', σ_L）を U に送る．σ_L の詳細は，付録 A.1.4 に記載する．

step4　U は σ_L を検証し，正しければ

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

を計算し，コンテンツ復号鍵（κ_j）を得る．

4.2.4　課金フェーズ

step1　L 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，$U$ に送る．

step2　U は自身の通信履歴から（$\tilde{T_4} = \prod_{i=1}^{m} T_{4_i}$，$\tilde{T_5} = \prod_{i=1}^{m} T_{5_i}$）を計算し，$\bar{T_4} = \tilde{T_4}$ および $\bar{T_5} = \tilde{T_5}$ を検証して正しければ $\bar{T_4}$，$\bar{T_5}$ に対する署名（σ_{U2}）を生成し，L に送る．

step3　L は $\bar{T_4}$，$\bar{T_5}$ および σ_{U2} を S に送る．

step4　S は σ_{U2} を検証し，正しければ $\bar{A} = (\bar{T_4})^{\tau} \bmod N$ を計算する．

step5　S は自分の秘密鍵（τ）を使って正しく復号した証拠として，

$$\sigma_S = SPK\{\tau : h_S = g^{\tau} \wedge \bar{A} = (\bar{T_4})^{\tau}\}$$

を計算して，$(\sigma_S, \bar{A})$ を L に送る．

step6　L は σ_S を検証して，正しければ $A = \frac{\bar{T_5}}{\bar{A}} \bmod N (= g^{\sum_{i=1}^{m} e_{j1_i}})$ を計算し，合計金額 $T^{(U)} = \log_g A$ を計算する$^{\star 1}$．σ_S の詳細は付録 A.1.5 に記載する．

$^{\star 1}$ 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，たかだか 10^6 なので）計算可能である[8]．

4.3　安　全　性

本方式のセキュリティは，グループ署名の安全性に依存する部分が多い．まず 2 つの補題を示す．

補題 1　4.2.1 項の（e_i, A_i, x_i）は，Ateniese らのグループ署名[3] の署名鍵（Sig_K）である．このとき強 RSA 仮定のもとで，システムマネージャ（M）の作り出す Sig_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 3) の Theorem1 より明らかである．∎

補題 2　4.2.1 項の（e_i, A_i, x_i）は，Ateniese らのグループ署名[3] の署名鍵（Sig_K）であり，$\{A_i^{\omega} | i \neq j\}$ を ω の情報なしに与えられたとする．このとき RSA-KTI 仮定のもとで，A_i^{ω}（$i \neq j$）の数が多項式有限であれば，A_j^{ω} を計算することはできない．

（証明）RSA 暗号の公開鍵を (e, n)，秘密鍵を ω とする．RSA-KTI 仮定により，RSA 暗号の公開鍵 (e, n) が与えられている状態で，A_i^{ω}（$i \neq j$）の数が多項式有限であれば，A_j^{ω} を計算することはできない．補題 2 では，e も与えられないので，A_j^{ω} を計算することはできない．∎

定理 1　強 RSA 仮定，DDH 仮定，RSA-KTI 仮定が成り立つと仮定する．また，すべての S_i はプロトコルを順守するとともに，少なくとも 1 つの S_i から秘密鍵が漏れないと仮定する．すると，4.2 節で示した方式は方式はランダムオラクルモデルのもとで，2.1 節のシステム要件 R1〜R7 および R9 を満たす．また，転送フェーズのデータ量がコンテンツ総数に依存しないという意味で R8 を満たす．

（証明）R3，R6，R7 は，各エンティティがデータに電子署名を付加して送信していること，および受信者が検証していることから，満たされている．R2，R4 はプロトコルの構成と SPK を付加していること，および補題 1 が成り立つことから，満たされていることが分かる．また，R9 は，S_i がすべて結託しない限り満たされることが分かる．

L から U へ送られる情報は，U が復号できる $(A_j)^w$ の ElGamal 暗号文と SPK であるから，U は A_j に対して $(A_j)^w$ のみを得ることができることになる．したがって，補題 2 とあわせて，R5 を満たしていることが分かる．一方，DDH 仮定より，U が L に送る ElGamal 暗号は識別不可能性を有している．グループ署名の性質から，U が CL のどのインデックス j（たとえば，どの A_j）を用いたかを L が識別できないこと，他の SPK もゼロ知識性を有することにより，R1 が満たされていることが分かる．また，転送フェーズのデータ量がコンテンツ総数に依存しないという意味で R8 も満たす．∎

© 2009 Information Processing Society of Japan

5. グループ署名 CG2004 を用いた方式

次に，4 章で用いたグループ署名（ACJT2000）を，2004 年に Camenisch らにより提案されたより効率的なグループ署名（CG2004）[7] に置き換えたプロトコルを示す．CG2004 は ACJT2000 と同じく強 RSA 仮定および DDH 仮定のもと安全性を証明しており，グループメンバが生成する署名サイズは ACJT2000 の約 1/2 となっている．以下に仮定と具体的なプロトコルを示す．

5.1 仮　　定

本方式の安全性は，4 章と同じく強 RSA 仮定，（位数が未知である群上での）DDH 仮定，RSA-KTI 仮定およ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' がすべて素数となる RSA の法とし，位数 $p'q'$ になる $\mathbb{Z}_N^*$ の巡回部分群 $QR(N)$ は，強 RSA 仮定および DDH 仮定を満たすと仮定する．

5.2 プロトコル

4 章と同様に，新たなエンティティとしてシステム管理者 M（CG2004 のグループ管理者）を定義する．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，公開情報および署名鍵を作るために，セットアップ時のみ利用する．また，各エンティティ間のやりとりでは，送信者（データ生成者）はデータにその電子署名を付加して送信し，受信者は電子署名を検証することとする．

5.2.1 セットアップ

セキュリティパラメータは CG2004 と同様に l_N，l_P，l_E，l_Q，l_c，l_e，l_s とする．さらに，$\mathcal{H}:\{0,1\}^* \to \{0,1\}^{l_c}$ をハッシュ関数とし，G を疑似乱数生成関数とする．

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 N（$=pq$）および a，g，$h \in_R QR(N)$ を選ぶ．続けて M は素数 $Q \in \{0,1\}^{l_Q}$ および $P \in \{0,1\}^{l_P}$ を $Q|P-1$ となるように選び，F を位数が Q となる $\mathbb{Z}_P^*$ の元とする．さらに M は $X_H \in_R \mathbb{Z}_Q$ を選び，$H=F^{X_H} \bmod P$ を計算し，(N,a,g,h,Q,P,F,H) を公開する．

次に，ライセンスサーバ（L）は $i=(1,\ldots,n)$ について価格 $x_i(=p_i)$ を定めて M に送る[⋆1]．M は乱数 $r_i \in_R \mathbb{Z}_N$ を選び，$E_i=2^{l_E}+e_i$ が素数となるような異なる n 個の乱数 $e_i \in_R \{0,1\}^{l_e}$ を選び，$A_1,\ldots,A_n$ を $A_i^{E_i}=ag^{x_i}h^{r_i} \bmod N$ となるように計算して，(x_i,A_i,e_i,r_i) を L に送る．同時に，各エンティティは秘密鍵と公開鍵をそれぞれ

$(SK_L,PK_L)=(\omega,h_L=g^{\omega} \bmod N),(SK_U,PK_U)=(\chi,h_U=g^{\chi} \bmod N),$

$(SK_S,PK_S)=(\tau \in_R \mathbb{Z}_Q,h_S=F^{\tau} \bmod P)$

と設定し，h_L，h_U，h_S を公開する．

5.2.2 コミットフェーズ

step1　L は，$\mathrm{CL}\{i,x_i,A_i,e_i,r_i\}_{(i=1,\ldots,n)}$ を U に送る（もしくは公開する）．次に，$Content_i$ を暗号化アルゴリズム $\mathcal{E}$ とコンテンツ鍵 κ_i で暗号化した $\mathcal{E}_{\kappa_i}(Content_i)_{(i=1,\ldots,n)}$ を U に送る．

step2　ライセンスサーバ（L）は，$i=1,\ldots,n$ について，

$K_i=(A_i)^{\omega} \bmod N,\ E_i=h_S(K_i \parallel A_i) \oplus \kappa_i$

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．

5.2.3 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，(x_j,A_j,e_j,r_j) を得る．

step2　U は乱数 r，$r' \in_R \{0,1\}^{l_N/2}$ および，$R \in_R \mathbb{Z}_Q$ を生成し

$$u_1=h^r A_i \bmod N,\ u_2=h_U^{r'}A_i \bmod N,\ u_3=g^{r'} \bmod N,$$
$$U_1=F^R \bmod P,\ U_2=h_S^{R+x_i} \bmod P,\ U_3=H^{R+e_i} \bmod P$$

を計算する．次に U は $r_x \in_R \{0,1\}^{l_Q+l_c+l_s}$，$r_r \in_R \{0,1\}^{l_n/2+l_c+l_s}$，$r_e \in_R \{0,1\}^{l_e+l_c+l_s}$，$R_R \in_R \mathbb{Z}_Q$ を選び，

$v=u_1^{r_e}g^{-r_x}h^{r_r} \bmod N,$

$V_1=F^{R_R} \bmod P,\ V_2=h_S^{R_R+r_x} \bmod P,\ V_3=H^{R_R+r_e} \bmod P$

を計算する．最後に U は $c=\mathcal{H}(gpk \parallel u_1 \parallel u_2 \parallel u_3 \parallel U_1 \parallel U_2 \parallel U_3 \parallel v \parallel V_1 \parallel V_2 \parallel V_3 \parallel ID)$ を計算し，$z_x=r_x+cx_i$，$z_r=r_r+c(-r_i-rE_i)$，$z_e=r_e+ce_i$，$Z_R=R_R+cR \bmod Q$ を計算する．そして $\sigma_1=(c,u_1,u_2,u_3,U_1,U_2,U_3,z_x,z_r,z_e,Z_R)$ とする．

ここで，σ_1 から（u_2,u_3）を除いたものはグループ署名（CG2004）であり，U が (u_1,U_1,U_2,U_3) を正しく計算したことと，選択したコンテンツの（x_j,A_j,e_j,r_j）が CL の中のどれか 1 つの組であることを証明できる．また（u_2,u_3），（U_2,U_1）はそれぞれ U の公開鍵を用いて暗号化したコンテンツ情報，S の公開鍵を用いて暗号化した価格情報の 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 の詳細は省略するが 4.2.3 項と同様に構成

⋆1 簡単のため省略するが，M は 4.2.1 項と同様，価格 x_i を埋め込んだ乱数を生成する．

© 2009 Information Processing Society of Japan

できる）．以下の SPK はコンテンツ情報の暗号文（u_2, u_3）が正しく価格情報と対応していることと，u_2，u_3 が正しく構成されていることを証明する（SPK 内はすべて法 N である）．

$$\sigma_{A_j} = SPK\{(A_j, r, r') : u_1 = h^r A_i \wedge u_2 = h_U^{r'} A_i \wedge u_3 = g^{r'}\}.$$

最後に，U は自身用の署名 σ_U を付加し，L に $(\sigma_1, \sigma_{A_j}, \sigma_U)$ を送る[⋆1]．

step3　L は $(\sigma_1, \sigma_{A_j}, \sigma_U)$ を検証し，正しければ $r_L \in_R \{0,1\}^{l_N/2}$ を生成して

$K' = (u_2', u_3') = (h_U^{r_L} u_2^{\omega}, g^{r_L} u_3^{\omega})$,

$\sigma_L = SPK\{(\omega, r_L) : h_L = g^{\omega} \wedge u_3' = g^{r_L} u_3^{\omega} \wedge u_2' = h_U^{r_L} u_2^{\omega}\}$

を計算し（K', σ_L）を U に送る．σ_L は自分の秘密鍵を使って正しく暗号化した SPK であり，4.2.4 項と同様に構成できる．

step4　U は σ_L を検証し，正しければ

$$K = \frac{T_1'}{(T_2')^{\chi}} = (A_j)^{\omega} \bmod N,\ \kappa_j = E_j \oplus h_S(K \parallel A_j)$$

を計算し，コンテンツ復号鍵（κ_j）を得る．

5.2.4　課金フェーズ

step1　L は（$\bar{U_1} = \prod_{i=1}^{m} U_{1_i}$，$\bar{U_2} = \prod_{i=1}^{m} U_{2_i}$）を計算し，$U$ に送る．

step2　U は自身の通信履歴から（$\tilde{U_1} = \prod_{i=1}^{m} U_{1_i}$，$\tilde{U_2} = \prod_{i=1}^{m} U_{2_i}$）を計算し，$\bar{U_1} = \tilde{U_1}$ および $\bar{U_2} = \tilde{U_2}$ を検証して正しければ $\bar{U_1}$，$\bar{U_2}$ に対する署名（σ_{U2}）を生成し，L に送る．

step3　L は $\bar{U_1}$，$\bar{U_2}$ および σ_{U2} を S に送る．

step4　S は σ_{U2} を検証し，正しければ $\bar{A} = (\bar{U_1})^{\tau} \bmod N$ を計算する．

step5　S は自分の秘密鍵（τ）を使って正しく復号した証拠として，

$\sigma_S = SPK\{\tau : h_S = F^{\tau} \bmod P \wedge \bar{A} = (\bar{U_1})^{\tau}\}$

を計算して，（$\sigma_S, T^{(U)}$）を L に送る．σ_S は 4.2.4 項と同様に構成できる．

step6　L は σ_S を検証して，正しければ $A = \frac{\bar{U_2}}{\bar{A}} \bmod N (= h_S^{\sum_{i=1}^{m} x_{j_i}})$ を計算し，$T^{(U)} = \log_G A$ を計算する．

5.3　安　全　性

定理 2　強 RSA 仮定，DDH 仮定，RSA-KTI 仮定が成り立つと仮定する．また，すべての S_i はプロトコルを順守するとともに，少なくとも 1 つの S_i から秘密鍵が漏れないと仮定する．すると，5.2 節で示した方式はランダムオラクルモデルのもとで，2.1 節のシステム要件 R1〜R7 および R9 を満たす．また，転送フェーズのデータ量がコンテンツ総数に依存しないという意味で R8 を満たす．

（証明）R3，R6，R7 は，各エンティティがデータに電子署名を付加して送信していること，および受信者が検証していることから，満たされている．R2，R4 はプロトコルの構成と SPK を付加していること，およびグループ署名 CG2004 の性質から，満たされていることが分かる．また，R9 は，S_i がすべて結託しない限り満たされることが分かる．

L から U へ送られる情報は，U が復号できる $(A_j)^w$ の ElGamal 暗号文と SPK であるから，U は A_j に対して $(A_j)^w$ のみを得ることができることになる．したがって，補題 2（定理 1，定理 2 のいずれにも使える）とあわせて，R5 を満たしていることが分かる．一方，DDH 仮定より，U が L に送る ElGamal 暗号は識別不可能性を有している．グループ署名の性質から，U が CL のどのインデックス j（たとえば，どの A_j）を用いたかを L が識別できないこと，他の SPK もゼロ知識性を有することにより，R1 が満たされていることが分かる．

また，転送フェーズのデータ量がコンテンツ総数に依存しないという意味で R8 も満たす．

∎

6. 評　　価

CDCS では，大量のコンテンツの取り扱いが想定される場合もある．Adaptive Oblivious Transfer[14] を使う方式，1-out-of-n 署名を用いて構成した方式[20]，Priced Oblivious Transfer [1]，および提案方式について，転送フェーズにおける計算・通信コストおよびプライバシに関する比較結果を付録 A.2 に示す．

単価の種類ごとに Adaptive Oblivious Transfer を用いる等の工夫により計算・通信コストが小さい方式を実現することは可能であるが，この方式ではプライバシ保護の実現（視聴したコンテンツの単価を秘匿すること）ができない[⋆2]．

1-out-of-n 署名を用いて構成した方式および Priced Oblivious Transfer は，転送フェーズにおける計算・通信コストの一部が $O(n)$，すなわちコンテンツ総数に比例する．したがって，扱うコンテンツ総数が巨大となる場合には，転送フェーズの一部が実用に耐えられない

⋆1 簡単のため省略するが，4.2.3 項と同様，乱数に埋め込まれた価格 x_i を正しく用いるための SPK も付加する．

⋆2 コンテンツ単価の秘匿までは求められない応用分野の場合は，この方法を選択することも考えられる．

© 2009 Information Processing Society of Japan

ため，グループ署名を利用した方式が適していると考えられる．

次に，コンテンツ総数が小さい場合について評価を行う．まず，CDCS を 1-out-of-n 署名を用いて構成した方式[20] と，本稿で提案したグループ署名を用いた 2 方式の，転送フェーズにおける利用者の計算・通信コストに関する評価（要件 R8）を付録 A.2.2 および A.2.3 の計算に基づいて行う．なお，NIST SP800-57[22] に示されている 112 ビット安全性を満たす基準で評価を行った．各方式の通信コストを比較すると，1-out-of-n 署名を利用した方式では，U から L への通信コストはコンテンツ総数 n に比例し，$84 + 28n$ バイトとなる．それに対して，4 章のグループ署名を利用した方式では，U から L への通信コストは一定で約 9519 バイトとなり，コンテンツ総数が 337 以上であれば効率的であるといえる．さらに 5 章の方式では 4343 バイト程度となり，コンテンツ総数が 153 以上であれば 1-out-of-n 署名を利用した方式より効率的であるといえる．

Priced Oblivious Transfer[1] を用いた方式は，転送フェーズにおける L の計算量が $\mathrm{O}(n)$ である．U の計算量や通信量に $\mathrm{O}(n)$ を要する部分がないが，利用者の課金時の合計金額の上限を $T^{(U)}$ とすると，計算量や通信量は $\mathrm{O}(\log T^{(U)})$ となる．したがって，L に要する計算量が実用に耐えるかどうかで，他方式との優位性を比較できる．付録 A.2.4 で示したように，システムとして利用できる L の性能に依存するが，コンテンツ総数が数千から数万程度と限定してよい場合は，Priced Oblivious Transfer を用いた方式の方が優位性があると考えられる．しかし大量のコンテンツを想定した場合は，L の計算量が一定であるグループ署名を用いた方式に優位性があるといえる．

いずれにせよ，コンテンツ総数が小さい場合は，デジタル放送受信機等の性能に依存する部分が大きいため，システム構築時に想定されるデバイス等を定めた後に各種パラメータを再度吟味して方式を決定する必要がある．

なお，課金フェーズにおいて，利用者が署名 σ_{U2} の発行を拒否した場合，結果として請求に対する否認ができる可能性がある．課金フェーズにおける利用者の計算は署名および暗号文の積のみであり，セキュリティモジュール等を準備し，処理することも可能である．したがって，本研究で提案したプロトコル以外での解決を図ることが，現実的な対策であると考えられる．

⋆1 たとえば文献 13) では，電子投票向けの効率的な正当性証明が提案されていて，利用者の計算・通信コストは一定である．

7. 結　　論

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）のシステム要件を定義した．次に，計算・通信コストを一定とするためにグループ署名を用いた 2 つの具体的な構成を提案し，最後に安全性および効率の理論的評価を行った．

利用履歴を秘匿するためにコンテンツ視聴時のコンテンツ単価の秘匿も必要とする場合，効率の評価の結果，コンテンツ総数 n の数を事前に評価することにより，方式を使い分けることが考えられる．ただし 1 章で述べたように，実社会におけるデジタル放送受信機向けのサービスを考えた場合，計算・通信コストが一定で，サービスの発展等にともなうコンテンツ総数の増加に影響さないグループ署名を用いた提案方式は，より実装を想定しやすいと考えられる．

また他の計算コストおよびデータ長が一定で短い署名方式⋆1 を用いることにより，CDCS はさらに効率化することができると考えられるが，それは今後の検討課題である．

参 考 文 献

1) Aiello, B., Ishai, Y. and Reingold, O.: Priced Oblivious Transfer: How to Sell Digital Goods, *Proc. EUROCRYPT'01*, LNCS 2045, pp.119–135, Springer (2001).
2) Abe, M., Ohkubo, M. and Suzuki, K.: 1-out-of-n Signatures from a Variety of Keys, *Proc. ASIACRYPT'02*, LNCS 2501, pp.415–432, Springer (2002).
3) Ateniese, G., Camenisch, J., Joye, M. and Tsudik, G.: A practical and provably secure coalition-resistant group signature scheme, *Proc. CRYPTO 2000*, LNCS 1880, pp.255–270, Springer (2000).
4) Boneh, D.: The decision Diffie-Hellman problem, *Algorithmic Number Theory* (*ANTS-III*), LNCS 1423, pp.48–63, Springer (1998).
5) Boudot, F.: Efficient Proofs that a Committed Number Lies in an Interval, *Proc. EUROCRYPT'00*, LNCS 1807, pp.431–444, Springer (2000).
6) Camenisch, J. and Michels, M.: A group signature scheme with improved efficiency, *Proc. ASIACRYPT'98*, LNCS 1514, pp.160–174, Springer (1998).
7) Camenisch, J. and Groth, J.: Group Signatures: Better Efficiency and New Theoretical Aspects, *Proc. SCN 2004*, LNCS 3352, pp.120–133, Springer (2005).
8) Cramer, R., Gennaro, R. and Schoenmakers, B.: A Secure and Optimally Efficient Multi-Authority Election Scheme, *Proc. EUROCRYPT'97*, LNCS 1233, pp.103–118, Springer (1997).
9) 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，SCIS2004 予稿集，pp.487–492 (2004).

© 2009 Information Processing Society of Japan

10) 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).
11) 保坂範和，岡田光司，加藤岳久：携帯電話向け匿名認証方式の実装，CSS2005 論文集，pp.31–36 (2005).
12) 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).
13) 中武真治，中西　透，舩曳信生：投票内容の正当性証明に要するコストを軽減した電子投票プロトコル，CSS2005 論文集，pp.517–522 (2005).
14) Ogata, W. and Kurosawa, K.: Oblivious keyword search, *Journal of Complexity*, Vol.20, No.2-3, pp.356–371 (2004).
15) Rabin, M.: How to exchange secrets by oblivious transfer, Technical Report TR 81, Aiken Computation Lab, Harvard University (1981).
16) 佐古和恵，米沢祥子，古川　潤：セキュリティとプライバシを両立させる匿名認証技術について，情報処理，Vol.47, No.4, pp.410–416 (2006).
17) Stern, J.P.: A new and effcient all-or-nothing disclosure of secrets protocol, *ASIACRYPT'98*, pp.357–371 (1998).
18) Tobita, T., Yamamoto, H., Doi, H. and Majima, K.: Privacy-enhanced Content Distribution and Charging Scheme Using Group Signature, *Proc. WISA2006*, LNCS 4298, pp.324–338, Springer (2007).
19) 飛田孝幸，山本博紀，土井　洋，真島恵吾：利用履歴を秘匿できるコンテンツ配信・課金方式の改良，IPSJ SIG Technical Reports, 2006-CSEC-33, pp.19–24 (2006).
20) 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).
21) http://www.tv-anytime.org/
22) http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf
23) 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
24) 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.
25) 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.
26) 黒沢　馨，尾形わかは：現代暗号の基礎数理，コロナ社 (2004).

付　　録

A.1　SPK の詳細

ここでは 4 章の提案方式で使用している SPK（σ_{e_j}，$\sigma_{r_{01}}$，$\sigma_{e_{j2}}$，σ_L，σ_O）についてプロトコルの詳細を説明する．

A.1.1　σ_{e_j}の構成

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

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

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

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

署名検証　検証者 L は，$c_U = \mathcal{H}(M_U \parallel (T_5^{2^{\lambda_2}} T_6)^{c_U}\ g^{s_U} h_S^{\hat{s}_U} \parallel T_3^{c_U} g^{s_U} h_S^{\bar{s}_U})$ 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．

A.1.2　$\sigma_{r_{01}}$の構成

$M_U = (g \parallel h_S \parallel T_4 \parallel T_5)$ とし，$\sigma_{r_{01}} = SPK\{(e_{j1}, r_{01}) : T_4 = g^{r_{01}} \wedge T_5 = g^{e_{j1}} h_S^{r_{01}}\}$ 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，

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

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

署名検証　検証者 L は，$c_U = \mathcal{H}(M_U \parallel T_4^{c_U} g^{\bar{s}_U} \parallel T_5^{c_U}\ g^{s_U} h_S^{\bar{s}_U})$ 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．

A.1.3　$\sigma_{e_{j2}}$の構成

$\sigma_{e_{j2}} = SPK\{(e_{j2}, r_{02}) : T_6 = g^{e_{j2}} h_S^{r_{02}} \wedge e_{j2} \in [-2^{t+l}b, 2^{t+l}b]\}$ を構成する．ただし，$\mathcal{H}_2$ 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，

$$W = g^{\omega} h_S^{\eta} \bmod N,$$
$$C = \mathcal{H}_2(W),\ c = C \bmod 2^t,\ D_1 = \omega + e_{j2}c,\ D_2 = \eta + r_{02}c (\in \mathbb{Z})$$

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 L へ送る．さもな

© 2009 Information Processing Society of Japan

くば署名生成をやり直す．

署名検証　検証者 L は，$D_1 \in [cb, 2^{t+l}b-1]$ および $C = \mathcal{H}_2(g^{D_1}h_S^{D_2}T_6^{-c})$ を検証し成立すれば $e_{j2} \in [-2^{t+l}b, 2^{t+l}b]$ であることを受理し，さもなくば棄却する．

A.1.4　σ_L の構成

$M_L = (g \parallel h_U \parallel h_L \parallel T_1' \parallel T_2')$ とし，$\sigma_L = SPK\{(\omega, r_L) : h_L = g^{\omega} \wedge T_2' = g^{r_L}T_2^{\omega} \wedge T_1' = h_U^{r_L}T_1^{\omega}\}$ を構成する．

署名生成　証明者 L 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，

$$t_1 = g^{\alpha_1} \bmod N,\ t_2 = g^{\alpha_2}T_2^{\alpha_1} \bmod N,\ t_3 = h_U^{\alpha_2}T_2^{\alpha_1} \bmod N,$$
$$c_L = \mathcal{H}(M_L \parallel t_1 \parallel t_2 \parallel t_3),\ s_L = \alpha_1 - c_L\omega,\ \bar{s}_L = \alpha_2 - c_L r_L$$

を計算し，$\sigma_L = (c_L, s_L, \bar{s}_L)$ を検証者 U へ送る．

署名検証　検証者 U は，$c_L = \mathcal{H}(M_L \parallel h_L^{c_L}g^{s_L} \parallel T_2'^{c_L}\ g^{\bar{s}_L}T_2^{s_L} \parallel T_1'^{c_L}h_U^{\bar{s}_L}T_1^{s_L})$ を検証し成立すれば σ_L を受理し，さもなくば棄却する．

A.1.5　σ_S の構成

$M_S = (g \parallel h_S \parallel \bar{A})$ とし $\sigma_S = SPK\{\tau : h_S = g^{\tau} \wedge \bar{A} = (\bar{T}_4)^{\tau}\}$ を構成する．

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

$$t_1 = g^{\alpha} \bmod N,\ t_2 = (\bar{T}_4)^{\alpha} \bmod N,\ c_S = \mathcal{H}(M_S \parallel t_1 \parallel t_2),\ s_S = \alpha - c_S\tau$$

を計算し，$\sigma_S = (c_S, s_S)$ を検証者 L へ送る．

署名検証　検証者 L は，$c_S = \mathcal{H}(M_S \parallel h_S^{c_S}g^{s_S} \parallel \bar{A}^{c_S}(\bar{T}_4)^{s_S})$ を検証し成立すれば σ_S を受理し，さもなくば棄却する．

A.2　理論的性能評価

Adaptive Oblivious Transfer を利用した方式，1-out-of-n 署名を利用した方式，グループ署名を利用した 2 つの方式，Priced Oblivious Transfer を利用した方式についての理論的性能評価を示す．なお，各方式のデータサイズと計算量は，NIST SP800-57 [22] に示されている 112 ビット安全性を満たす基準で統一した．計算量は，べき乗剰余演算 1 回分（法および指数が 2048 ビット）を C_N で，楕円スカラー倍算 1 回分（楕円曲線の法およびスカラー値が 224 ビット）を C_E として，各々の回数で評価する．データサイズはバイト数で評価する．なお，いずれの方式でも共通して必要となるエンティティ認証のための通常の署名の生成コストと署名サイズを除いた評価を与える．以下，n をコンテンツ総数とする．

A.2.1　Adaptive Oblivious Transfer を利用した方式の評価

単価の種類ごとに Adaptive Oblivious Transfer（以下 AOT）を用いることを考える．たとえば，表 2 の例の場合，コンテンツ単価が 50 円のコンテンツのための AOT のコミットフェーズ，コンテンツ単価が 100 円のコンテンツのための AOT のコミットフェーズ等をコンテンツ単価の種類だけ行う．利用者は，50 円のコンテンツ A_j を必要とする場合は，単価が 50 円のコンテンツ $\{A_i\}$ から 1 つを AOT の転送フェーズを用いて得ることとなる．文献 14) の AOT を用いた場合を考える．コンテンツ視聴時，転送フェーズで利用者（U）がライセンスサーバ（L）に送信するデータ長はべき乗剰余演算の結果のみであり 256 バイトとなる．その際の計算コストは C_N となる．利用者 U からのデータを受信後，L の計算コストは C_N であり，L から U に送信するデータ長も 256 バイトである．U がこのデータからコンテンツ復号鍵を得るコストは無視できる．ただし，コンテンツの単価を秘匿することはできない．

なお，AOT を 1 回行うための金額をあらかじめ定め，コンテンツ単価に応じて，複数回の AOT を行うことにより，コンテンツ単価を秘匿するというアプローチも考えられる．たとえば，表 2 の例の場合，AOT を 1 回行うための金額を 50 円とし，コンテンツ復号鍵は，コンテンツ $\{B_i\}$ については 2 つに，コンテンツ $\{C_i\}$ については 3 つに分割しておく．コンテンツ B_j 利用する場合は，2 回の AOT を繰り返すことにより，コンテンツ復号鍵を得るという方法である．この場合，計算コストやデータ長は上記の方法より小さくなることはない．また，ライセンスサーバ（L）は，比較的短い期間に連続する AOT の要求回数から，利用するコンテンツの単価をある程度推測することができる．

A.2.2　1-out-of-n 署名を利用した方式の評価

1-out-of-n 署名を利用して構成した方式[20] における利用者（U）の通信コストを考える．ここでは楕円曲線上での構成を考え，p，q の bit 長をそれぞれ $|p| = 224$，$|q| = 224$ とする．コンテンツ視聴時，転送フェーズで利用者（U）がライセンスサーバ（L）に送信するデータ長は (X, Y, Z, σ_0) の合計であり，$84 + 28n$ バイトとなる．その際の計算コストは $(6+7n)C_E$ となる．利用者 U からのデータを受信後，L の計算コストは $(9+7n)C_E$ であり，L から U に送信するデータ長は 140 バイトである．U がこのデータからコンテンツ復号鍵を得るコストは C_E である．

A.2.3　グループ署名を利用した方式の評価

グループ署名に ACJT2000 [3] を用いた場合，4.2.1 項のセキュリティパラメータ ϵ，k，l_p を文献 11) の 3.3 節をもとに $\epsilon = 1.25$，$k = 224$，$l_p = 1024$ とし，t，s，l を文献 5) の 1.2.3 項をもとに $t = 112$，$s = 56$，$l = 56$ とする．また，文献 3) をもとに $\gamma_3 = 7037$ とした．p'，q' は l_p(bit) の素数であるから，$|p'| = |q'| = 1024$ となり，文献 11) より $|N| = 2048$ とする．ここで，a，a_0，g，h および各エンティティの公開鍵は位数が $p'q'$ の群 $QR(N)$ から選ぶので，

© 2009 Information Processing Society of Japan

$|a| = |a_0| = |g| = |h| = |h_L| = |h_U| = |h_S| = 1024 \times *2 + 1 = 2049$ とする．最後に各エンティティの秘密鍵のサイズは群 $\mathbb{Z}^*_{p'q'}$ から選ぶので，$|\omega| = |\chi| = |\tau| = 1024 \times 2 + 1 = 2049$ とする．

コンテンツ視聴時，転送フェーズで利用者（U）がライセンスサーバ（L）に送信するデータ長は $(\sigma_1, \sigma_{e_j}, \sigma_{r_{01}}, \sigma_{e_{j2}})$ のデータ長の合計であり，ここで各署名のバイト長を計算すると $|\sigma_1| = 4928$，$|\sigma_{e_j}| = 2973$，$|\sigma_{r_{01}}| = 418$，$|\sigma_{e_{j2}}| = 1200$ となり合計で 9519 バイトとなり，その際の計算コストは $64C_N$ となる．利用者 U からのデータを受信後，L の計算コストは $65C_E$ であり，L から U に送信するデータ長は 1242 バイトである．U がこのデータからコンテンツ復号鍵を得るコストは C_N である．

一方グループ署名に CG2004[7] を用いた場合の通信コストは，CG2004 の SIGN フェーズでグループメンバが生成する署名サイズは ACJT2000 より小さくなるが，それに付加するいくつかの SPK のコストを評価する必要がある．CG2004 を用いて CDCS を構成した場合，データは 4343 バイトとなり，その際の計算コストは $15C_N$ となる．利用者 U からのデータを受信後，L の計算コストは $14C_N$ であり，L から U に送信するデータ長は 1242 バイトである．U がこのデータからコンテンツ復号鍵を得るコストは C_N である．

A.2.4　Priced Oblivious Transfer を利用した方式の評価

文献 1) の構成方式では，コンテンツ（x^i（$1 \leq i \leq n$））購入ごとに，ライセンスサーバ（L）は，

(1)　新たに生成した乱数 u^t，v^t を生成し，

(2)　利用者（U）がプロトコルを順守している場合に限り，U に u^t，v^t を送り，

(3)　PIR（Private Information Retrieval）プロトコルで，U に $m_i = \mathcal{E}_k(x^i + v^t)$ を送る，

必要がある．なお，t はトランザクションに対応するインデックスである．U はこれらの情報から x^i を得ることができる．暗号化と復号には楕円 ElGamal 暗号を用いることができる．

U から L へのデータ長は，コンテンツ単価を $\log T^{(U)}$ ビットで表現できるとすれば，$168 \log T^{(U)} + 28$ バイトとなり，その際の計算コストは $(12 \log T^{(U)} + 1)C_E$ となる．しかしながら，利用者 U からのデータの受信後に行う L の計算コストは小さくない．文献 1) の 3.4 節で記述されているとおり，n 回の暗号化処理が必要であり，データ長は $56n$，計算量は $2nC_E$ 以上となる．一方，データ長は 56 バイトとなる．U がこのデータからコンテンツ復号鍵を得るコストは C_E である．

A.2.5　各方式の比較

AOT を利用した方式，1-out-of-n 署名を利用した方式，グループ署名を利用した 2 つの方式，Priced Oblivious Transfer を利用した方式についての理論的性能評価を**表 3** に示す．ここで，n はコンテンツ総数，$\log T^{(U)}$ はコンテンツ単価を表現するために必要なビット数である．プライバシとは，コンテンツ単価の秘匿が可能かどうかを意味する．

表 3　5 方式の比較
Table 3　Comparision of 5 schemes.

	AOT	1-out-of-n	4 章の方式	5 章の方式	POT
U が送るデータ長	256	$84 + 28n$	9519	4343	$168 \log T^{(U)} + 28$
U の計算量	C_N	$(7 + 7n)C_E$	$65C_N$	$16C_N$	$(12 \log T^{(U)} + 2)C_E$
L が送るデータ長	256	140	1242	1242	$56n$
L の計算量	C_N	$(9 + 7n)C_E$	$65C_N$	$14C_N$	$2nC_E$
プライバシ	×	○	○	○	○

コンテンツ単価に関連する $\log T^{(U)}$ はたかだか 20 程度と考えられる．コンテンツ総数はシステムに依存するパラメータであるが，数万を超える場合も十分考えられる．また，べき乗剰余 C_N と楕円スカラー倍算 C_E の性能比は，数 10 倍から数百倍となることが予想される（文献 16) 等）．これらのことを勘案すると，コンテンツ総数 n により，以下のような結果となる．

(1)　Adaptive Oblivious Transfer を利用した方式は，コンテンツ単価の守秘を必要としない応用分野の場合は，優れている．

(2)　1-out-of-n 署名を利用した方式は，n が数十程度までなら優れている．

(3)　Priced Oblivious Transfer を利用した方式は，U の計算量で n に比例する部分はない．n が大きくない場合は優れているが，n が数万を超えると L の計算量が大きくなり，L がボトルネックになる可能性が高い．

(4)　グループ署名を利用した提案方式は，計算量とデータ量が n に比例しないのでコンテンツ総数 n が巨大な場合は，他の方式より性能が優れている．4 章の方式と 5 章の方式では，後者の方が性能面では優れている．なお，前者のべき乗剰余演算等の法は 1 種類であることから，設計のしやすさ等の条件も考慮しながら方式を選択することになると考えられる．

(平成 20 年 12 月 1 日受付)
(平成 21 年 6 月 4 日採録)

© 2009 Information Processing Society of Japan

飛田　孝幸（正会員）

1997 年東京電気大学工学部情報通信工学科卒業．同年 NEC ソフト株式会社入社．2007 年情報セキュリティ大学院大学情報セキュリティ研究科修士課程修了．2008 年みずほ情報総研株式会社入社．現在，同社の情報セキュリティ評価室所属．情報セキュリティ大学院大学客員研究員，電子情報通信学会会員．

山本　博紀

2004 年中央大学理工学部情報工学科卒業．2006 年中央大学大学院理工学研究科情報工学専攻博士課程前期課程修了．同年東日本電信電話株式会社入社．

土井　　洋（正会員）

1988 年 3 月岡山大学理学部数学科卒業．同年日立ソフトウェアエンジニアリング株式会社入社．1994 年北陸先端科学技術大学院大学情報科学研究科博士前期課程修了．2000 岡山大学大学院自然科学研究科博士課程修了．同年より中央大学研究開発機構助教授．2004 年より情報セキュリティ大学院大学教授．暗号理論，情報セキュリティの研究に従事．博士（理学），電子情報通信学会会員．

真島　恵吾

1984 年早稲田大学理工学部電子通信学科卒業．同年 NHK 入局．1992 年より放送技術研究所において，高密度ディジタル記録，サーバ型放送システム，コンテンツの権利保護，および情報セキュリティの研究に従事．現在，同研究所（次世代プラットフォーム）主任研究員．電子情報通信学会，映像情報メディア学会，画像電子学会各会員．

© 2009 Information Processing Society of Japan