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

2006－CSEC－34 (45)
2006／7／21

電子マネーの取引を利用した電子指紋プロトコル

山根 進也† 栗林 稔†† 森井 昌克††

† 神戸大学大学院自然科学研究科
〒657-8501 神戸市灘区六甲台町 1-1
†† 神戸大学工学部
〒657-8501 神戸市灘区六甲台町 1-1
E-mail: †060t256n@stu.kobe-u.ac.jp, ††{kminoru,mmorii}@kobe-u.ac.jp

あらまし 電子指紋プロトコルは，ディジタルコンテンツ配信システムにおいて不正配布者の検挙を可能とする暗号プロトコルであるが，コンテンツの売買における料金の支払いに関してはあまり考えられていない．本論文では，料金の支払いを可能とするために，信頼できるセンタによる電子マネーの運用を想定した電子指紋プロトコルを提案する．ユーザはセンタが発行する電子マネーを用いて，電子指紋の埋め込まれたコンテンツの取引と決済を同時に行うことができる．

キーワード 電子透かし，電子指紋プロトコル，電子マネー

Fingerprinting Protocol Equipping Electronic Payment System

Shinya YAMANE†, Minoru KURIBAYASHI††, and Masakatu MORII††

† Graduate School of Science and Technology, Kobe University
1-1 Rokkodai-cho, Nada-ku, Kobe, 657-8501 Japan
†† Faculty of Engineering, Kobe University
1-1 Rokkodai-cho, Nada-ku, Kobe, 657-8501 Japan
E-mail: †060t256n@stu.kobe-u.ac.jp, ††{kminoru,mmorii}@kobe-u.ac.jp

Abstract On digital contents distribution system fingerprinting protocols enable sellers to trace the buyer who redistributed a copy illegally. However, conventional fingerprinting protocols do not give much consideration to the payment for the charge of the contents. In this paper, we propose fingerprinting protocols which equip the function of digital cash managed by a trusted center for electronic payment. Using the digital cash, buyers can obtain fingerprinted contents and simultaneously pay the charge of the contents.

Key words watermarking, fingerprinting protocol, digital cash

1. はじめに

近年，動画や音楽，画像などのマルチメディアコンテンツがディジタル情報として取り扱われるようになり，インターネットなどのネットワーク上での公開・販売が盛んに行われている．このようなコンテンツ配信により，簡単にディジタルコンテンツを入手し，鑑賞することができる．しかし，ディジタル情報はコンピュータを用いて加工やコピーなどの処理を容易に行うことができるため，ディジタルコンテンツの不正コピーやネットワーク上での不正配布などの著作権侵害行為が問題となっている．

この問題を解決するための方法の一つとして，電子透かし技術が注目されている．電子透かし技術は，ディジタルコンテンツに副情報（透かし情報）を埋め込み，後でその情報を抽出または検出することを可能とする技術である．埋め込む情報の種類によって様々な応用が考えられており，著作者情報や秘密情報を埋め込むことにより，著作権主張や改ざん検知などが可能である．電子指紋技術は，電子透かし技術の応用の一つであり，透かし情報としてユーザ毎に異なる識別情報をコンテンツに埋め込む方式である．不正コピーが発見された場合，抽出した透かし情報より不正配布者を特定することが可能となり，不正コピーの抑止効果を期待できる．

電子指紋プロトコルは，電子指紋技術を利用し，不正配布者の不正を第三者に証明することを目的とする暗号プロトコルである．最初に提案された電子指紋プロトコルは，対称方式[1]である．対称方式では，コンテンツの販売者が直接，購入者を

示す情報をコンテンツに埋め込むため，販売者も透かし入りコンテンツを入手できる．この状況では不正コピーが発見されたとき，流出元が販売者であるか購入者であるかを第三者は判断することができない．この問題を解決するために，非対称方式[2], [3]が提案された．非対称方式では暗号技術を利用し，プロトコル終了後に購入者のみが透かし入りコンテンツを入手できるようにプロトコルを構成している．したがって，販売者は第三者に不正配布の事実を証明することが可能である．さらに，購入者の購買履歴などのプライバシーを保護する機能を備えた匿名方式[4]が提案された．匿名方式では，購入者は匿名で取引することができるが，不正配布を行ったことが証明された場合には匿名性が剥奪される．Leiらの電子指紋プロトコル[5]は匿名方式であり，信頼できるセンタを利用することにより安全性と匿名性を実現している．

電子指紋プロトコルはコンテンツ配信システムに用いられることが想定されているが，Leiらの方式を含め，既存の電子指紋プロトコルではコンテンツの料金の支払いについてあまり考えられていない．特に匿名方式では，匿名で料金を支払う必要があり，そのためには別途複雑なプロトコルが必要となる．

本論文では，料金の支払いを可能とするために，信頼できるセンタによる電子マネーの運用を想定した電子指紋プロトコルを提案する．提案電子指紋プロトコルにおけるセンタは，Leiらの方式と同様に，透かし情報の発行や秘密情報の管理を行い，安全性と匿名性を実現する．それに加え，提案方式では，センタが電子マネーの発行・管理を行うことにより，ユーザは電子マネーを用いて電子的に決済を行うことが可能である．一つのセンタに機能を集約することにより，ユーザは一連のプロトコルで電子指紋の埋め込まれたコンテンツの取引と料金の授受を同時に行うことができる．提案方式はプリペイド型の支払い形態を採用しているが，同様の構成でポストペイ型の支払いを実現できることを示す．また，匿名性を高めた改良方式についても考察を行う．

本論文の構成は次の通りである．まず，第2章で既存技術について述べた後，第3章で提案電子指紋プロトコルについて述べる．次に，第4章で提案方式の評価を行い，第5章で提案方式を改良した方式の提案と考察を行う．最後に第6章でまとめを述べる．

2. 準　　備

本章では，提案方式で利用する基本技術について説明する．まず，電子指紋プロトコルの要件について述べ，それから電子指紋プロトコルで利用される公開鍵暗号の性質について述べる．次に，提案電子指紋プロトコルの基となる方式であるLeiらの電子指紋プロトコルについて説明し，最後に電子マネーについて説明する．

2.1 電子指紋プロトコルの要件

電子指紋プロトコルを構成する際，不正配布者の不正を第三者に証明可能とするためには，非対称方式である必要がある．また，購入者のプライバシの保護も電子商取引において重要な要求事項とみなされており，匿名方式である方が好ましい．

本稿では匿名電子指紋プロトコルの要件として以下のもの考える．まず，安全性に関する要件として次の三つを考える．

追跡可能性：販売者は発見した不正コピーをもとに，不正配布者を特定することができる．

購入者の安全性：不正配布を行っていない正規の購入者が，販売者や別の購入者によって陥れられることはない．

販売者の安全性：不正配布者が不正コピーの流出を否認できない．

購入者のプライバシ保護に関わる要件としては次の二つを考える．

匿名性：購入者は匿名で取引を行うことができる．

関連付け不能性：二つのディジタルコンテンツが与えられたとき，それらのコンテンツが同一の購入者のものであるかを判断できない．

2.2 公開鍵暗号の準同形写像

非対称方式を実現するための一つの方法として，公開鍵暗号の準同形写像の性質が利用されている．公開鍵暗号が演算$\oplus$に関して準同型写像であるとは，$E_K(\cdot)$を公開鍵暗号の暗号化関数，Kを公開鍵としたとき，任意のメッセージaとbに対して

$$E_K(a \oplus b) = E_K(a) \oplus E_K(b) \qquad (1)$$

が成立するときである．暗号領域での演算$\oplus$がメッセージ領域での演算$\oplus$となるため，メッセージの内容を秘匿したまま，メッセージに対する演算を行うことが可能である．今，aをコンテンツ，bを透かし情報とすれば，暗号領域でコンテンツに透かし情報を埋め込み，秘密鍵を持つユーザのみが，透かし情報の埋め込まれたコンテンツを復号することが可能なシステムが構成できる．RSA暗号[6]の乗法性の準同型写像の性質を用いて埋め込みを行う方式[3]や，岡本-内山暗号[7]の加法性の準同型写像写像の性質を用いて埋め込みを行う方式[8]などが提案されている．

2.3 Leiらの方式の概要

Leiらの電子指紋プロトコルは匿名電子指紋プロトコルであり，その実現のために信頼できるセンタを利用している．Leiらのプロトコルは，販売者S，購入者B，そして2つのセンタである認証局CA，電子透かし認証局WCAから構成される．BがSからコンテンツXを購入する場合，プロトコルは以下の操作を順次行うことにより完了する．

1) BはCAにユーザ登録を行い，仮名に対する証明書の発行を受ける．

2) Bは仮名を用いてSと通信し，交渉をして取引固有の情報ARGを生成する．Bはワンタイムキーのペア(pk^*, sk^*)を生成し，秘密鍵sk^*を用いて署名$Sign_{sk^*}(ARG)$を作成する．ここで，$Sign(\cdot)$は署名アルゴリズムである．Bは証明書，公開鍵pk^*，ARGと署名$Sign_{sk^*}(ARG)$をSに送信する．

3) Sは，証明書，署名の有効性を確認する．有効であれば，透かし情報Vを生成し，

$$X^{(V)} = X \oplus V \quad (2)$$

を計算して X に V を埋め込む．ただし，$\oplus$ は電子透かしの埋め込み演算である．S は，証明書，pk^*，ARG，$Sign_{sk^*}(ARG)$，$X^{(V)}$ を WCA に送信する．

4) WCA は証明書と署名の有効性を検証し，有効であれば，透かし情報 W を生成し，$E_{pk^*}(W)$，$E_{pk_{WCA}}(W)$ 計算する．ただし，E_K は埋め込み演算 $\oplus$ に関して準同型写像の性質を持ち，K を公開鍵として入力する公開鍵暗号の暗号化関数である．続いて，WCA は署名

$$Sign_{WCA} = Sign_{WCA}(E_{pk^*}(W), pk^*, Sign_{sk^*}(ARG)) \quad (3)$$

を生成し，$E_{pk^*}(W)$，$E_{pk_{WCA}}(W)$ と共に S に送信する．

5) S は受け取った透かし情報を暗号領域で埋め込む．

$$E_{pk^*}(X^{(V,W)}) = E_{pk^*}(X^{(V)}) \oplus E_{pk^*}(W) \quad (4)$$

S は $E_{pk^*}(X^{(V,W)})$ を B に送信し，コンテンツ X に関する取引の記録として，V，証明書，pk^*，ARG，$Sign_{sk^*}(ARG)$，$E_{pk^*}(W)$，$E_{pk_{WCA}}(W)$，$Sign_{WCA}$ をデータベースに保存する．

B は $E_{pk^*}(X^{(V,W)})$ に復号処理を行い、透かし入りのコンテンツ $X^{(V,W)}$ を入手する．

不正コピーが発見されたとき，S は第三者に不正を証明するために，審判者とともに以下のプロトコルを実行する．ただし，透かし入りのコンテンツ $X^{(V,W)}$ は圧縮や透かし情報を取り除くための攻撃を受けている可能性がある．そこで，発見された不正コピーを $\hat{X}^{(V,W)}$ として以下の操作を行う．

1) S は不正コピーからステップ3) で埋め込んだ透かし情報 V を抽出する．抽出された透かし情報を $\hat{V}$ とすると，S はそれに対応する取引記録をデータベースから探す．用いられる電子指紋技術にも依るが，一般的に $\hat{V}$ と最も相関の高い V_i が選ばれる．ただし，V_i はデータベースに保存された透かし情報の i 番目の項目を表す．S は $X^{(V_i)}(= X \oplus V_i)$，$\hat{X}^{(V,W)}$，証明書，$pk^*$，$ARG$，$Sign_{sk^*}(ARG)$，$E_{pk^*}(W)$，$E_{pk_{WCA}}(W)$，$Sign_{WCA}$ を審判者に送信する．

2) 審判者は証明書と署名の有効性を確認し，もし無効なものがあれば訴えを棄却する．有効であれば，審判者は WCA に $E_{pk_{WCA}}(W)$ を送信し復号を請求する．

3) 審判者は復号された W，$X^{(V_i)}$，$\hat{X}^{(V,W)}$ を入力とした抽出または検出アルゴリズムを実行する．W が不正コピーから発見されれば証明書に記された仮名に対応する B を有罪とし，CA に ID 情報の公開を請求する．

Lei らの方式において，B は CA に発行してもらった仮名を用いて匿名で取引することが可能である．また，ステップ5) において，透かし情報 W は公開鍵暗号の準同形写像を利用して暗号領域で埋め込まれ，S は透かし入りのコンテンツを知ることができないため，B が陥れられることはない．さらに，WCA の署名 $Sign_{WCA}$ が，W と ARG に記述された特定のコンテンツとの関連を証明している．したがって，不正コピーから抽出した透かし情報を別のコンテンツに対応させることは不可能であり，B は行っていない再配布に対する罪を被ることはない．

2.4 電子マネー

電子マネーは，現金を電子化してネットワークや電子的な手段で決済を可能とする技術である．本稿では，電子マネーシステムとして支払者，受取者，発行機関からなるシンプルな基本モデルを考える．電子マネーの要件としては以下のものが挙げられる．

偽造不可能性：電子マネーを発行機関を介さずに作成することはできない．

なりすまし不可能性：電子マネーの所有者以外は誰もその電子マネーを使用できない．

二重使用不可能性：同じ電子マネーを2回以上使用することはできない．

これらに加え，支払者のプライバシ保護も重要な要件であると考えられており，受取者だけでなく発行機関に対する匿名性も重要視されている．

電子マネーは取引に関する決済が行われる時期の観点より，大きくプリペイド (前払い) 型とポストペイ (後払い) 型に分類される．プリペイド型電子マネーは，取引が行われる前の段階で予め口座より引き落としを行い，現金の価値を持つディジタル情報 (電子マネー) として保有しておく方式である．

プリペイド型電子マネーを構成する一つの方法は，発行機関が電子マネー固有の識別情報に対してディジタル署名を付与し，その偽造不可能性を根拠にお金としての価値を保証する方法である．その際，電子マネーの額面は署名に使用する秘密鍵を変えることにより設定できる．なりすまし不可能性，二重使用不可能性を満たし，そして識別番号から発行機関にプライバシ情報が洩れることを防ぐためには，以下のような手法を利用することが考えられている．

- 支払い時に支払者が受取者からのチャレンジに正しい反応を行い，他人の電子マネーのコピーではないことを証明する．
- 支払いの度に電子マネーを発行機関に還流させ，発行機関が検証することによって二重使用を検出可能とする．
- ブラインド署名を利用し，識別番号を発行機関に知らせることなく署名の付与を受ける．

ブラインド署名とは，メッセージの内容を秘匿しつつ，メッセージに署名を付加してもらう署名技術であり，RSA 署名 [6] に基づく方式 [9] などが提案されている．ブラインド署名の手順を簡単に示すと，まず署名依頼者 A はメッセージ M にブライ

ンド処理を施し，署名者Bに送信する．次に，Bはブラインド処理されたM対して署名を作成し，Aに返信する．Aはアンブラインド処理を施し，Mに対するBの署名$Sign_B(M)$を得，手順を終了する．しかし，この方法では，AがBの意図しない情報に署名を付加させる恐れが生じる．そこで，電子マネー方式[10]ではブラインド署名とカット-選択法(cut-and-choose methodology)とを組み合わせている．カット-選択法とは，いわば抜き取り検査であり，検査回数を増やせば高い確率で不正を検出することができる．

ポストペイ型電子マネーは，取引が行われた時点もしくは後で支払者の口座より引き落としが行われる方式である．電子マネーは発行機関が支払者の預金を引き落としたり，受取者の口座へ振り替えたりするための情報から構成される．

3. 電子マネーの取引を利用した電子指紋プロトコル

この章では，提案手法である電子マネーの取引を利用した電子指紋プロトコルについて述べる．提案電子指紋プロトコルではLeiらの方式における認証局と電子透かし認証局の役割を1つのセンタが担い，さらに，電子マネーの運用を行う．すなわち，センタには以下の3つの機能が集約される．

- ユーザ登録
- 透かし情報発行
- 電子マネー発行

提案プロトコルは以下の三者により構成され，その概要は図1に示す通りである．

販売者$\mathcal{S}$： コンテンツを販売し利益を得ることを目的とする．コンテンツの著作者であるか，もしくは著作者に代理で販売することを許可されている者である．

購入者$\mathcal{B}$： $\mathcal{S}$から電子マネーを用いてディジタルコンテンツを購入することを目的とする．

センタ$\mathcal{C}$： $\mathcal{S}$と$\mathcal{B}$に信頼されているセンタである．$\mathcal{S}$と$\mathcal{B}$の口座を管理し，電子マネーの発行や預け入れに伴う引き落とし，振り込みを自由に行うことができる，銀行のような機関を想定する．

$\mathcal{B}$はコンテンツの取引を行う前に，まず$\mathcal{C}$に対価を支払い，電子マネーを発行してもらう．取引時に$\mathcal{B}$は，その電子マネーを用いて$\mathcal{S}$に支払いを行い，$\mathcal{C}$は還流してきた電子マネーが有効であると判断すれば$\mathcal{S}$の口座に金額を振り込み，さらに透かし情報を発行する．$\mathcal{S}$は透かし情報をコンテンツに埋め込み$\mathcal{B}$に配信する．

提案プロトコルに関して，まずプロトコルの前準備について述べ，次に提案プロトコルを構成する3つのサブプロトコルである電子マネー発行プロトコル，電子指紋プロトコル，不正配布者追跡プロトコルについて詳細を述べる．

3.1 前準備

$\mathcal{C}$は，$\mathcal{S}$と$\mathcal{B}$が$\mathcal{C}$の署名と，電子マネーの有効性，そして電子マネーの金額を検証することを可能とするために，各種署名を検証するための公開鍵，電子マネーの額面と公開鍵の対応表を公開しておく．

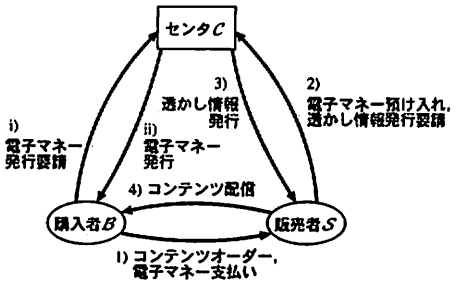

図1 提案電子指紋プロトコルの概要

3.2 電子マネー発行プロトコル

コンテンツの購入に先立ち，$\mathcal{B}$は$\mathcal{C}$から電子マネーを受け取る．$\mathcal{B}$は複数の電子マネーを所持しておくことも可能である．このプロトコルは図1に示すi)，ii)のステップによって構成される．各ステップの詳細を以下に示す．

i) $\mathcal{B}$はワンタイムキーのペア(pk^*, sk^*)を生成し，続いてID情報ID，公開鍵pk^*，引き出す金額情報$WITHDRAWAL$を$\mathcal{C}$に送信し，電子マネーの発行を要請する．

ii) $\mathcal{C}$は$\mathcal{B}$の口座から$WITHDRAWAL$の預金を引き落とし，金額に対応した秘密鍵で署名$Sign_{\mathcal{C}}(pk^*)$を生成し，$\mathcal{B}$に送信する．$(pk^*, Sign_{\mathcal{C}}(pk^*))$のペアが電子マネーとなる．ここで，署名$Sign_{\mathcal{C}}(pk^*)$は$pk^*$の有効性を$\mathcal{C}$が保証するものであるため，このペアは電子マネーとしてだけではなく$\mathcal{B}$の仮名として使うことができる．すなわち，この操作により$\mathcal{C}$はユーザ登録と電子マネー発行を同時に行うことができる．

$\mathcal{C}$はIDとpk^*の対応関係をデータベースに記録し，秘密に保持する．

3.3 電子指紋プロトコル

$\mathcal{B}$が$\mathcal{S}$からコンテンツXを購入する場合，$\mathcal{B}$は電子マネーで支払いを行うだけで，透かし入りのコンテンツを手に入れることができる．このプロトコルは図1に示すステップ1)〜4)であり，各ステップの詳細を以下に示す．

1) $\mathcal{B}$はpk^*を仮名として$\mathcal{S}$と取引するために，電子マネー$(pk^*, Sign_{\mathcal{C}}(pk^*))$を$\mathcal{S}$に送信する．$\mathcal{S}$は正当性を確認した後に，注文書$ORDER = \{PARTY, DESC_X, VALUE_X, TIME\}$を生成し，$\mathcal{B}$に送信する．ただし，$ORDER$を構成する要素はそれぞれ，

$PARTY$：$\mathcal{B}$の仮名pk^*および$\mathcal{S}$のID情報
$DESC_X$：コンテンツXの描写
$VALUE_X$：コンテンツXの価格
$TIME$：取引時刻

である．

$\mathcal{B}$は$ORDER$の内容を確認し，秘密鍵sk^*を用いて署名$Sign_{sk^*}(ORDER)$を作成して$\mathcal{S}$に送信する．

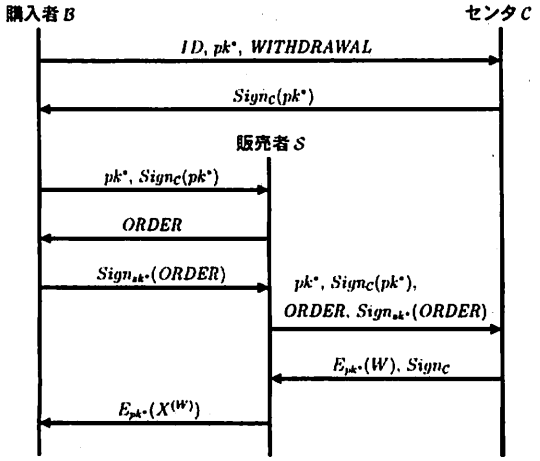

図 2　電子指紋プロトコルにおける通信の流れ

2) S は，$Sign_{sk^*}(ORDER)$ の有効性を検証し，さらに電子マネーの額面がコンテンツの金額に相当するかを検証する．その電子マネーでの支払いを認めるならば，pk^*, $Sign_C(pk^*)$, $ORDER$, $Sign_{sk^*}(ORDER)$ を C に送信し，電子マネーの預け入れと透かし情報の発行を要請する．

3) C は $Sign_C(pk^*)$, $Sign_{sk^*}(ORDER)$ を検証し，電子マネー及び注文書の有効性を確認し，さらに，データベースを検索して，電子マネー $(pk^*, Sign_C(pk^*))$ が二重使用されていないかを検査する．どれか 1 つでも無効なものがあればプロトコルを中止する．検査に合格すれば，C は販売者の口座に金額を払い込み，さらに透かし情報 W をランダムに生成する．C は透かし情報と現在の取引との関連性を証明する署名

$$Sign_C = Sign_C(E_{pk^*}(W), pk^*, Sign_{sk^*}(ORDER)) \quad (5)$$

を作成し，W を暗号化した $E_{pk^*}(W)$ と共に S に送信する．C はデータベースに pk^*, W の対応関係を保存しておく．このデータベースは，電子マネーの二重使用検査にも利用する．すなわち，W を既に発行した電子マネーは，使用済み電子マネーであると判断する．

4) S は公開鍵暗号の準同型写像の性質を用いて，暗号領域での透かし情報の埋め込みを行う．

$$E_{pk^*}(X^{(W)}) = E_{pk^*}(X) \oplus E_{pk^*}(W) \quad (6)$$

そして，$E_{pk^*}(X^{(W)})$ を B に送信し，コンテンツ X に関する取引の記録として $E_{pk^*}(W)$, $ORDER$, $Sign_{sk^*}(ORDER)$, $Sign_C$ をデータベースに保存する．B は $E_{pk^*}(X^{(W)})$ を復号して，透かし情報の埋め込まれたコンテンツ $X^{(W)}$ を入手する．

以上の電子マネー発行プロトコルと電子指紋プロトコルにおける通信の流れを図 2 に示す．

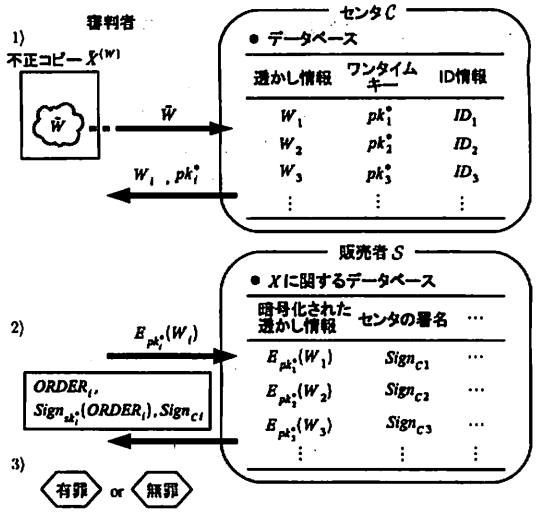

図 3　不正配布者追跡プロトコル

提案方式のステップ 1) において，電子マネーの額面よりもコンテンツの価格 $VALUE_X$ が高い場合が考えられる．その場合，B は複数の電子マネーに関して同様に $ORDER$ 対する署名を作成し，それらをまとめて販売者に送信することにより，価格に見合う支払いが可能である．

3.4　不正配布者追跡プロトコル

不正コピー $\tilde{X}^{(W)}$ が発見されたとき，S は不正配布者追跡プロトコルを実行することにより不正配布者を特定し，第三者にその不正を証明することができる．不正配布者追跡プロトコルの概要を図 3 に示す．

1) S はオリジナルのコンテンツ X と不正コピー $\tilde{X}^{(W)}$ を審判者に送信する．審判者は，それらを入力とする透かし情報抽出アルゴリズムを実行して透かし情報 $\tilde{W}$ を抽出し，C に送信する．C はデータベースを検索し，$\tilde{W}$ に最も相関の高い W を探す．そして，検索結果 W_i, pk_i^* を審判者に送信する．

2) 審判者は $\tilde{W}$ と W_i の相関が十分に高ければ，S に $E_{pk^*}(W_i)$ を送信し，証拠となる取引の記録の提出を求める．S はコンテンツ X に関する取引のデータベースから $E_{pk_i^*}(W_i)$ に対応する $ORDER_i$, $Sign_{sk_i^*}(ORDER_i)$, $Sign_{Ci}$ を検索し，その結果を審判者に送信する．

3) 審判者は $ORDER_i$ の内容，すなわち $PARTY$ や $DESC_X$ を参照して，案件と一致しているかを確認し，さらに $Sign_{sk_i^*}(ORDER_i)$, $Sign_{Ci}$ の有効性を確認する．どれか一つでも無効なものがある場合や，S が取引の記録を提出をできない場合，審判者は訴えを棄却する．提出された記録がすべて有効である場合は，仮名 pk_i^* に対応する B を有罪として，C に ID 情報 ID_i の開示を求める．

4. 提案電子指紋プロトコルの評価

この章では，前章で提案した電子指紋プロトコルの評価を行う．まず，安全性について検証し，次に匿名性について検証する．そして最後に，提案方式の特徴について説明する．ただし，次に示す三つの条件の仮定のもと，評価を行う．

A1 用いる暗号法，署名法は安全である．

A2 センタは信頼できる機関であり，販売者及び購入者と結託しない．すなわち，秘密情報を漏洩しない．

A3 用いる電子透かし技術は攻撃に対して耐性がある．

4.1 安 全 性

まず，電子指紋プロトコルの安全性に関する要件を評価する．

追跡可能性：販売者は自らの利益に反するため，オリジナルのコンテンツ X と暗号化された透かし情報 $E_{pk^*}(W)$ を購入者に明かすことはしない．また，仮定 A2 が成立するならばセンタは透かし情報 W を購入者に漏洩しない．そのため，購入者は透かし情報の埋め込まれていないコンテンツをつくり出すことは不可能である．さらに，仮定 A3 が成立するならば，購入者が透かし入りのコンテンツに攻撃を行ったとしても，透かし情報は正しく抽出される．そして，提案方式では W はセンタにより一意に各購入者に対応付けられている．したがって，販売者は発見した不正コピーから不正配布者を特定することができる．

購入者の安全性：販売者が購入者の透かし入りのコンテンツを偽造するためには，購入者固有の透かし情報 W を知る必要がある．しかし，仮定 A1 が成立するならば，購入者の秘密鍵を持たない販売者は，$E_{pk^*}(W)$ を復号することができず，また仮定 A2 が成立するならば，販売者はセンタから W を知ることができない．したがって，購入者は販売者の偽造により陥れられることはない．また，センタの署名 $Sign_C(= Sign_C(E_{pk^*}(W), pk^*, Sign_{sk^*}(ORDER)))$ が W と特定の取引 $(ORDER)$ とを結びつけているため，不正配布を行った購入者が別の不正配布について二重に訴えられることはない．以上より，購入者の安全性は保たれる．

販売者の安全性：仮定 A1，A2 が成立するならば，秘密鍵を持つ購入者のみが自分の ID 情報に対応する透かし入りのコンテンツを入手することができる．そのため，不正コピーの流出元は，透かし情報の示す購入者ただ一人であることが保証され，販売者は不正の事実を第三者に証明することができる．したがって，販売者の安全性は保証される．

次に，2.4 節で挙げた電子マネーの要件について評価する．

偽造不可能性：仮定 A1 が成立するならば，購入者はセンタを介さずに電子マネーを作成することは不可能である．

なりすまし不可能性：ステップ 1) において B は取引時刻 $TIME$ の含まれた $ORDER$ に署名を行い，正当な電子マネーの所有者であることを証明しなければならいため，電子マネーの盗用は不可能である．

二重使用不可能性：ステップ 3) において，センタが環流してきた電子マネーを検証し，二重使用は検出されるため，電子マネーを二重使用することは不可能である．また，電子マネーはセンタにより一意に購入者に対応付けられているため，二重使用者は特定される．

4.2 匿 名 性

この節では，購入者のプライバシ保護に関する要件について評価を行う．

匿名性：

[定理 1] 仮定 A2 が成り立つならば，購入者は販売者に対して匿名で取引することができる．

(証明) ステップ 1) において，販売者は購入者より pk^*, $Sign_C(pk^*)$, $Sign_{sk^*}(ORDER)$ を受信する．pk^* は購入者によってランダムに生成されるため，購入者の ID 情報 ID とは統計的に独立である．また，$Sign_C(pk^*)$ は ID に依存しないセンタの秘密鍵を用いた署名であり，$Sign_{sk^*}(ORDER)$ にも ID を特定する情報は含まれない．

ステップ 3) において，販売者はセンタより $E_{pk^*}(W)$, $Sign_C$ を受信する．透かし情報 W は，センタによりランダムに生成されているため，これらの情報は購入者の ID 情報 ID とは統計的に独立である．

以上より，仮定 A2 が成立するとき，販売者は得られる情報から購入者を特定することができない．すなわち，購入者は販売者に対して匿名で取引を行うことができる． □

関連付け不能性：

定理 1 より，購入者は販売者に対して匿名で取引でき，さらに，pk^*，W は取引ごとに異なるものが生成される．したがって，販売者は異なる取引を関連付けることはできない．

4.3 特 徴

この節では，提案電子指紋プロトコルの特徴について述べる．提案方式の基とした Lei らの方式との比較を表 1 に示す．

表 1 提案方式と Lei らの方式との比較

		Lei らの方式	提案方式
料金支払い		不可能	可能
センタの数		2 (CA, WCA)	1 (C)
匿名性	対販売者	有	有
	対透かし情報	(対 WCA)	(対 C)
	発行機関	有	無
センタの記憶装置		無	有
透かし情報の種類		2 (V, W)	1 (W)

まず，提案方式では Lei らの方式の技術を基に，さらに電子マネーの取引を利用することにより，料金の支払いを可能とした．次に，利用する信頼できるセンタの数を 2 つから 1 つに削減した．しかし，これにより透かし情報の発行機関に対する匿名性は損なわれている．一般に信頼できるセンタを多く利用すれば，センタに実名性を吸収させ匿名性を高めることができる．提案方式は，購入者，販売者，そしてセンタの三者という最小の構成要員によるシンプルなモデルでありながら，販売者に対する匿名性は確保している．これは，通常のクレジットカード決済などに比べれば匿名性は高いと言える．最後に，センタの

記憶装置と透かし情報の種類については，トレードオフの関係がある．Lei らの方式では，センタは W に署名を付加して偽造できないようにし，販売者に記録させている．しかし，その W は暗号化されており，直接，抽出した透かし情報との関連性を検索することができないため，V を対応させる必要が生じている．一方，提案方式ではセンタの記憶装置は必要であるが，埋め込むべき透かし情報は 1 種類となっている．そのため，埋め込むべき情報量の削減が見込め，同品質のコンテンツに対してより攻撃に対する耐性の高い埋め込みを行うことができる．

5. 改良電子指紋プロトコル

この章では，3 章で提案した電子指紋プロトコルを改良した方式を提案し，考察を行なう．

5.1 ポストペイ方式

提案した電子指紋プロトコルでは，プリペイド型の支払い形態を採用したが，一部に変更を加えるだけでポストペイ型の支払いが可能な方式を構築できる．ここでは，プリペイド方式と異なる操作についてのみ説明を行なう．

まず，電子マネー発行プロトコルのステップ i) において $\mathcal{B}$ は $WITHDRAWAL$ を $\mathcal{C}$ に送信しないようにし，金額の対応付けを行わずにユーザ登録のみを行う．そして，電子指紋プロトコルにおいて $\mathcal{C}$ は $ORDER$ に含まれている金額情報 $VALUE_X$ をもとに，$\mathcal{B}$ の口座から $\mathcal{S}$ の口座へとコンテンツの料金の振替を行う．

ポストペイ方式では，任意の額の支払いが可能である．プリペイド方式と同様の構成で構築可能であるため，ユーザの要求に応じて，プリペイド方式とポストペイ方式を使い分けることができる．

5.2 完全匿名方式

先に提案した 2 つの方式では，$\mathcal{C}$ に対する $\mathcal{B}$ の匿名性が確保されていない．電子マネーにおいて，発行機関に対する匿名性はプライバシ保護の観点から重要であるとされている．この節では，$\mathcal{C}$ に対する匿名性を確保した改良方式の構築について議論する．

まず，前節で提案したポストペイ方式では，コンテンツの取引後に $\mathcal{B}$ の口座から振替が行われるため，$\mathcal{B}$ は取引の際に $\mathcal{C}$ へ ID 情報を伝える必要があり，$\mathcal{C}$ に対する匿名性の確保は難しい．したがって，3 章で述べたプリペイド方式である提案方式を改良することを考える．

ここでは一つの方式として，ブラインド署名とカット-選択法を利用することにより，ただ 1 つのセンタを利用して，完全に匿名である方式が構築可能であることを示す．以下が完全匿名方式における電子マネー発行プロトコルと電子指紋プロトコルの概要であり，前者の概要を図 4 に示す．

[電子マネー発行プロトコル]

i) $\mathcal{B}$ は $\mathcal{C}$ から ID 情報に対応する透かし情報 W の発行を受ける．続いて，n 組のワンタイムキーのペア (pk_i^*, sk_i^*) $(i = 1, \cdots, n)$ を生成し，W を n 個の公開鍵でそれぞれ暗号化して $E_{pk_i^*}(W)$ を作成する．$\mathcal{B}$ は n 組のペア $(pk_i^*, E_{pk_i^*}(W))$ をブラインド処理して $\mathcal{C}$ に送信する．

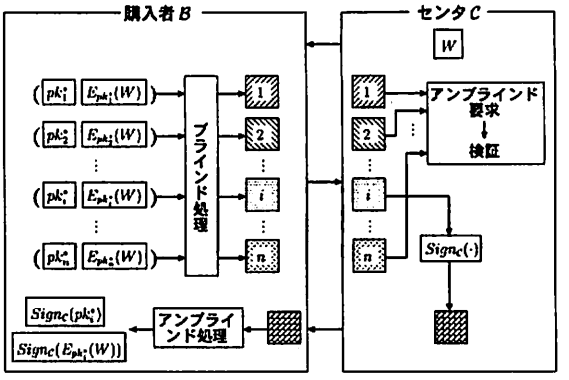

図 4 完全匿名方式における電子マネー発行プロトコルの概要

ii) $\mathcal{C}$ はその内 $n-1$ ペアを選択し，$\mathcal{B}$ にアンブラインドを要求する．$\mathcal{C}$ はアンブラインド処理された $n-1$ ペアが公開鍵とその公開鍵によって暗号化された W であるかを確かめる．検査に合格すれば残った 1 つのペア (ここでは i 番目のペアとする) に対して金額に応じた署名をして，$\mathcal{B}$ に送信する．$\mathcal{B}$ はそれをアンブラインド処理することにより，電子マネー $(pk_i^*, Sign_{\mathcal{C}}(pk_i^*))$ と暗号化された透かし情報 $E_{pk_i^*}(W)$ とその署名 $Sign_{\mathcal{C}}(E_{pk_i^*}(W))$ が利用可能になる．

[電子指紋プロトコル]

$\mathcal{B}$ は $\mathcal{S}$ に対して電子マネーで支払いを行い，同時に $E_{pk_i^*}(W)$ と $Sign_{\mathcal{C}}(E_{pk_i^*}(W))$ を送信する．$\mathcal{S}$ は暗号領域で透かし情報の埋め込みを実行する．その際，$Sign_{\mathcal{C}}(E_{pk_i^*}(W))$ を検証することにより，透かし情報が $\mathcal{C}$ が保証する正当な情報であることを確認できる．

この方式において，$\mathcal{B}$ がブラインド署名を利用することにより，$\mathcal{C}$ は署名した内容と作成した署名を知ることができない．したがって，$\mathcal{B}$ は pk_i^*, $Sign_{\mathcal{C}}(pk_i^*)$, $E_{pk_i^*}(W)$, $Sign_{\mathcal{C}}(E_{pk_i^*}(W))$ より特定されず，$\mathcal{C}$ に対する匿名性を確保できる．さらにカット-選択法を利用することにより，$\mathcal{B}$ が pk_i^*, $E_{pk_i^*}(W)$ とは異なる情報に対して署名を付加させる不正を検出可能としている．すなわち，$\mathcal{C}$ が n ペアの内 $n-1$ ペアのアンブラインドを要求し，それらを確認することにより，$\mathcal{B}$ の不正を $(n-1)/n$ の確率で発見することができる．高い確率で不正を発見するためには n の値を大きく設定すれば良い．ただし，n を大きくすれば，n 組の鍵のペア生成やその鍵を用いた W の暗号化などに要する計算量が増加し，それらを送信するための通信量も増加するため，これらのトレードオフの関係を考慮しなければならない．不正が行われていなければ，コンテンツに埋め込まれる W が，$\mathcal{C}$ により一意に $\mathcal{B}$ に対応付けられているため，不正配布者を追跡することができる．

この方式では $\mathcal{C}$ は透かし情報 W を $\mathcal{B}$ に送信するため，元のプリペイド方式と異なり W が $\mathcal{B}$ に洩れている．したがって，より攻撃に耐性のある電子透かし技術を利用する必要がある．また，使用済みの電子マネーをデータベースに登録することにより，二重使用の検出は可能であるが，匿名性より二重使用者

の追跡は不可能となっている．この点に関してはさらに改良が必要である．

6. ま と め

本論文では，電子マネーの取引を利用し，コンテンツの料金の支払いが可能である電子指紋プロトコルを提案した．提案方式はシンプルな構成でありながら，安全性と匿名性を確保している．また，支払い形態の異なるプリペイド方式とポストペイ方式を提案した．この２つの方式は，同様の構成で実行可能であり，状況によって使い分けることができる．そして，プリペイド方式ではより匿名性を高めた方式の構築が可能であることを示した．今後の課題としては，より多機能な電子マネーを利用する方式や，より実用性の高い方式について検討することなどが挙げられる．

文 献

[1] N. R. Wagner, "Fingerprinting," *IEEE Symp. Security and Privacy*, pp. 18–22, 1983.

[2] B. Pfitzmann and M. Schunter, "Asymmetric fingerprinting," *Proc. EUROCRYPT'96*, LNCS 1070, pp. 84–95, Springer-Verlag, 1996.

[3] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," *IEEE Trans. Image Processing*, vol. 10, no. 4, pp. 643–649, 2001.

[4] B. Pfitzmann and M. Waidner, "Anonymous fingerprinting," *Proc. EUROCRYPT'97*, LNCS 1233, pp. 88–102, Springer-Verlag, 1997.

[5] C. Lei, P. Yu, P. Tsai, and M. Chan, "An efficient and anonymous buyer-seller watermarking protocol," *IEEE Trans. Image Processing*, vol. 13, no. 12, pp. 1618–1626, 2004.

[6] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[7] T. Okamoto and S. Uchiyama, "A new public-key cryptosystem as secure as factoring," *Proc. EUROCRYPT'98*, LNCS 1403, pp. 308–318, Springer-Verlag, 1998.

[8] M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property," *IEEE Trans. Image Processing*, vol. 14, no. 12, pp. 2129–2139, 2005.

[9] D. Chaum, "Blind signatures for untraceable payments," *Proc. CRYPTO'82*, pp. 199-203, Plenum Press, 1983.

[10] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," *Proc. CRYPTO'88*, LNCS 403, pp. 319–327, Springer-Verlag, 1998.