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

2003－ＣＳＥＣ－22　(29)
2003／7／18

認証局と販売者の共謀攻撃に対して安全な匿名消費者-販売者透かし方式

崔 在貴† 櫻井 幸一‡ 朴 志煥†

† 釜慶大学校 情報保護学科 〒608-737 釜山市南区大淵　599-1
‡ 九州大学 大学院システム情報科学研究院 〒812-8581 福岡市東区箱崎 6-10-1
E-mail: †jae@mail1.pknu.ac.kr, jpark@pknu.ac.kr, ‡sakurai@csce.kyushu-u.ac.jp

あらまし 消費者-販売者透かしプロトコルはコンテンツに消費者の情報を挿入することによって不正コピーを抑制する，著作権保護の技術の一つである．本論文では，最近，提案された 2 つの匿名消費者-販売者透かしプロトコルの弱点を指摘する．この 2 つのプロトコルは認証局と販売者が共謀する場合，プロトコルの安全性が損なわれる壊れる問題点を持っている．また，本論文で我々は 可換暗号を利用することよって，この問題を解決した消費者-販売者透かしプロトコルを提案する．

キーワード 電子透かし，共謀攻撃，可換暗号．

Secure Anonymous Buyer-Seller Watermarking Protocol Against Conspiracy Attack

Jae-Gwi Choi† Kouichi Sakurai‡ and Ji-Hwan Park†

† Department of Information Security, Pukyong national university, Busan, Korea.
‡ Faculty of Computer Science and Communication Engineering, Kyushu university, Fukuoka, Japan.
E-mail: †jae@mail1.pknu.ac.kr, jpark@pknu.ac.kr, ‡sakurai@csce.kyushu-u.ac.jp

Abstract Copyright marking schemes are techniques applied to protect the copyright on digital contents. They are the embedding of marks into digital contents that can later be detected to identify owners (watermarking) or recipients (fingerprinting) of the content. Anonymous buyer-seller watermarking protocol allows the buyers to purchase watermarked contents anonymously. However, on illegal redistribution the anonymity can be revoked. In this paper we show serious shortcomings of recent proposals on anonymous buyer-seller watermarking protocol. The problem is that it allows the seller to cheat honest buyers. Thus, if another copy with specific watermark turns up, one cannot assign responsibility to one of the buyer and the seller. In this paper, we present secure buyer-seller watermarking protocol using commutative cryptosystems, which prevents the buyer from cheating honest buyers.

Keyword Digital watermarking, digital fingerprinting, copyright violators, conspiracy attack, commutative cryptosystems.

1. はじめに

著作権保護に対する研究は大きく三つに分けられる．

・ **対称型手法**：従来の手法[11,14]は販売者もコンテンツに挿入される消費者の情報(watermark)を知っていると点において対称型である．したがって，この透かしを挿入されたコンテンツが発見された時，消費者は販売者がこれを配布したと主張できる．これは大きな問題である．

・ **非対称型手法**：対称型手法の問題は非対称型手法[2,15]によって解決される．なぜなら，ここには消費者のみが透かしの挿入されたコンテンツを持てるので，消費者はこれを販売者が配布したと言えない．それでも，この手法は消費者のプライバシーを守ることができない．

・ **匿名型手法**：消費者のプライバシーを守るために，2 つの手法[3,7]が提案された.基本アイディアは，販売者は透かしが挿入されたコンテンツと消費者の身元

を知ることができないということである．しかし後で著作権違反者を追跡できる． 身元の確認に関する過程は著作権違反者にのみ適用される．したがって，正当な消費者の匿名性は守られる．それでも[3]手法は高い計算量を必要とする secure two-party computation[5]を使ったので非効率が非現実的である．最近に Ju らが，Memon-Wong の手法（MW 手法）[15]に匿名性と非連結性を追加した“匿名販売者-消費者電子透かし”というプロトコルを提案している[7]．Ju らによる手法とMWによる手法はでBS方式[4]を使わなくて，結託攻撃に抵抗力が強い Cox の非可視的電子透かし[8]を使う．しかし JK の手法は消費者の秘密鍵が露呈してしまう問題がある．さらに，販売者と透かし認証局が共謀すれば，消費者の透かしが挿入されたコンテンツと同じものが偽造できる．また，ひとたび不正配布されたコンテンツが見つかると，著作権侵害者の特定を行なうために，販売者，透かし認証局，裁判官が集まらなければならないという問題もある．

JK 方式の問題点を解決するために我々は Oblivious transfer protocol[12]を使った CKP 方式[10]を提案した．しかし CPK 方式でも電子透かし認証局の不正が可能なので，JK 手法を解決したとはいえない．なぜなら，oblivious transfer protocol を実行する時，電子透かし認証局が同じ電子透かしを入力したら，電子透かし認証局は消費者の電子透かしを容易に特定できるからである．

本論文で我々は既に提案された 2 つの匿名消費者-販売者電子透かしプロトコルの問題点，すなわち，電子透かし認証局（判定者）と販売者の共謀攻撃の可能性を示して，これの解決策を提案しようとする．

2 章では既存の提案方式の概要と共謀攻撃の可能性の問題点を指摘し，3,4 章では提案方式に対する説明及び安全性を分析し，5 章で結論を下す．

2. 従来方式

2.1. JK 手法

2.1.1. プロトコル[7]

この手法ははじめに電子透かし方式に匿名性を提供した点に意味がある．簡略化の為に，JK 手法と同じ表示を使う．

A. 事前処理：全ての参加者は認証局から認証された公開鍵と秘密鍵の組 (sk, pk) を持っている．

B. 透かし生成：消費者は匿名の鍵の組 (sk_B^*, pk_B^*) を生成する．消費者は次のように verifiable 暗号手法を用いて透かし認証局に登録する．まず，消費者は判定者の公開鍵 pk_J で自分の秘密鍵 (sk_B^*) を暗号化する．次に，消費者は暗号文 $(C = E_{pk_J}(sk_B^*))$ と認証書 $(cert)$ を透かし認証局に送る．また，$cert$ は sk_B^* が pk_B^* の離散対数（または e-乗根）であることを証明するものである．ここには安全な verifiable 暗号方法[9]の存在を仮定する．検証されると，認証局は暗号文 (C) が正確に sk_B^* を暗号したものであると納得することができる．上の課程が検証されると，消費者は透かし $(E_{pk_B^*}(W), W = \{w_1, w_2, \cdots, w_n\})$ と透かしを pk_B^* で暗号されたものを証明する認証局の署名 $(sign_{sk_w}(W \| pk_B^*))$ を貰う．認証局は $Table_{wa}$ に $C, cert$ と B（消費者の身元），$w = E_{pk_B^*}(W), s = sign_{sk_w}(w \| pk_B^*), sign_{sk_B}(pk_B^*)$ を貯蔵する．ここに暗号アルゴリズムは同型 $(E_k(a \oplus b) = E_k(a) \oplus E_k(b))$ である．

C. 透かし挿入：消費者は透かしを挿入されたコンテンツを受けるの為に販売者に $pk_B^*, w, sign_{sk_w}(w \| pk_B^*)$ を送る．販売者は透かしの妥当性を確認する．販売者は認証局の公開鍵を用いて，検証が正しげれば，販売者はユニークな透かし (V) を生成し，これをコンテンツに挿入する． $X'(= X \oplus V)$ を挿入されたコンテンツとする．コンテンツの不正コピーが見っかった際には，このユニークな透かし V は元の消費者の身元を追跡するのに使われる． $E_{pk_B^*}(W)$ を復号せず， 2 番目の透かしを挿入するために販売者は pk_B^* で透かし挿入されたコンテンツを暗号化して，$\sigma(E_{pk_B^*}(W)) = E_{pk_B^*}(\sigma(W))$ を満足する置換を捜す．透かし認証局によって使われた暗号アルゴリズム E の同型特徴のため，販売者は式 1 の過程によって透かしされたコンテンツを計算することができる．ここで $\oplus$ は挿入演算を意味する．販売者は計算された $E_{pk_B^*}(X'')$ を消費者に伝達する．

D. 不正配布者身元確認：不法配布されたコピー Y が発見されば，販売者は抽出アリゴリズムを用いて，

$$
\begin{aligned}
E_{pk_B^*}(X'') &= E_{pk_B^*}(X') \oplus \sigma E_{pk_B^*}(W) \\
&= E_{pk_B^*}(X') \oplus E_{pk_B^*}\sigma(W) \\
&= \{E_{pk_B^*}(x_1'), \cdots, E_{pk_B^*}(x_m')\} \oplus \\
&\quad \{E_{pk_B^*}(w_{\sigma(1)}), \cdots, E_{pk_B^*}(w_{\sigma(n)})\} \qquad (1) \\
&= \{E_{pk_B^*}(x_1' \oplus w_{\sigma(1)}), \cdots, \\
&\quad E_{pk_B^*}(x_n' \oplus w_{\sigma(n)})\} \\
&= E_{pk_B^*}(X' \oplus \sigma(W)), m \geq n
\end{aligned}
$$

コピーYからユニークな透かしUを抽出する．そして，販売者は自分の$Table_{wa}$に保存されたすべてのVと抽出された透かしUの相関関係を調査してVと一緒に貯蔵された消費者の情報$pk_B^*, w, sign_{sk_w}(w \| pk_B^*), \sigma$を捜し出す．販売者は$X, Y$と一緒にこれら情報を判定者(Judge)に送る．判定者は透かし認証局の助けを得てs，$sign_{sk_B}(pk_B^*)$と$cert$を検証して，該当の消費者の匿名秘密鍵をCから修復する．検証が成功すれば，判定者は$\sigma(W)$を計算して，Yから抽出された$\sigma(W)$の存在可能性を確認して，これと$\sigma(W)$の相関関係を測定する．この$\sigma(W)$が存在すれば，該当消費者は著作権違反者になることで，その消費者の身元は販売者に知らせる．

2.1.2. 分析

JKの手法の一番望ましくない点は販者が透かし認証局または判定者と共謀をすれば消費者の情報が入さされたコンテンツのコピーを作ること可能である点である．なぜならば，透かし認証局は消費者のユニークな透かしを知っており，判定者は$E_{pk_J}(sk_B^*)$を彼の秘密鍵で復号することによって消費者の秘密鍵(sk_B^*)を知ることができる．

A. 販売者と透かし認証局の共謀

特別な透かし(W)を持ったコピー(Y)を偽造するため，販売者はある消費者から受けとったpk_B^*, sを透かし認証局に送る．透かし認証局は彼の保存テーブルから該当の消費者の透かしを捜して販売者に送れば販売者はその消費者と同じコピーを作ることができる．

B. 販売者と判定者の共謀

JK手法では，透かしを挿入されたコンテンツが消費者の公開鍵によって暗号化されるので，消費者であるけが透かしを挿入されたコンテンツを復号することができると主張している．しかし,このプロトコルで販売者は安全ではない通信路を介して送信される$C, Epk_B^*(X'')$を得ることができる．後に販売者は$Table_{wa}$から得られた$C, Epk_B^*(X'')$を正確に一致する情報を捜すことができ，彼はここで得られた$C, Epk_B^*(X'')$を判定者に送る．これは判定者の立場では簡単に復号できるので，販売者はケースIのように消費者のコピー同じコピーを作ることができる．

2.2. CKP 方式

2.2.1. プロトコル[10]

CPK 手法は簡単に電子透かし生成であるけ説明する．

[仮定]

Alice は販売者で,Bob は消費者で，Carol は透かし認証局を表す．また本方式に使われるアルゴリズムは安全であると仮定する．

[定義]

透かし挿入過程は$X' = X \oplus W$で 表示する，

- X:原本コンテンツ
- W:透かし
- X':透かし挿入されたコンテンツ
- $\oplus$: 挿入演算
- $X \oplus W = \{x_1 \oplus w_1, \cdots, x_n \oplus w_n, x_m\}$
- $p(\leq n\,bits)$: $q = (p-1)/2$を満足する大きい次数
- G : 次数$p-1$の群
- g : 群Gの生成元
- $sk_{A(BorC)}$: Alice(Bob or Carol)の秘密鍵 $(pk_A = g^{sk_A})$

透かし生成： Bob は$sk_{B1}^* \cdot sk_{B2}^* = sk_B$のような乱数$sk_{B1}^*, sk_{B2}^*$を選択する．Bob は$pk_B^*$ $(pk_B^* = g^{sk_{B1}^*})$を送り，認証局の公開鍵pk_Cを使ってsk_{B2}^* $(E_{pk_C}(sk_{B2}^*))$を暗号化する．Bob はゼロ知識証明を用いて，sk_{B1}^*を持っていることを認証局に証明する．Bob は oblivious transfer プロトコル[6,12,13]を実行するための公開鍵と秘密鍵の組$< x, (\beta_0, \beta_1) >$を生成する．認証局は先に自分の秘密鍵を利用して秘密鍵復号して,Bob の公開鍵pk_Bを用いて$pk_B^{*\,sk_{B2}^*} = pk_B \bmod p$を確認する．これが検証されれば，認証局は次のように oblivious transfer プロトコル実行のために2つの透かしを生成

する． 認証局は次の多項式 $f(x)=\sum_{i=0}^{n} a_i x^i (\mathrm{mod}\, p)$ を生成して

$f(i), i=\{0,1\}$, $F(i)=pk_B\cdot(pk_B^*)^{a_0}(pk_B^*)^{a_1 i_0}\cdots(pk_B^*)^{a_k i^k}$ を計算する．認証局は Bob の匿名公開鍵を用いて $(f(i),F(i))$ を暗号化して(式(２))，これに対する署名を実行する（式(３)）．これは透かしの妥当性とともに該当の透かしが Bob の匿名公開鍵で暗号化されたものを認証してくれる役目をする．

$$\begin{aligned} Enc-W_0 &= E_{pk_B^*}(f(0)\|F(0)) \\ Enc-W_1 &= E_{pk_B^*}(f(1)\|F(1)) \end{aligned} \quad (2)$$

$$\begin{aligned} Sig_0 &= sign_{sk_{wa}}(Enc-W_0\|pk_B^*) \\ Sig_1 &= sign_{sk_{wa}}(Enc-W_1\|pk_B^*) \end{aligned} \quad (3)$$

認証局は oblivious transfer プロトコルのため s_0, s_1 を準備して，ここで s_0, s_1 は２つの透かしと認証局の署名を表わす．

$$\begin{aligned} s_0 &= \{Epk_B^*(f(0)\|F(0))\|sig_0\} \\ s_1 &= \{Epk_B^*(f(1)\|F(1))\|sig_1\} \end{aligned} \quad (4)$$

Bob は２つの透かしの中で１つを選択して，ここで認証局は Bob がどんな透かしを選択したのか知ることができない．そしてから Bob は式(５)のように認証局から受けたすべての情報を確認する．

$$\begin{aligned} & D_{sk_{B1}^*}\{E_{pk_B^*}(f(i)\|F(i))\} = f(i)\|F(i) \\ & y_B = \frac{F(i)}{(pk_B^*)^{f(i)}},\quad i\in\{0,1\} \end{aligned} \quad (5)$$

提案方式に 1-out-of-2 oblivious transfer プロトコルを使うが，偽造に対する確率を減らすために 1-out-of-n oblivious transfer プロトコルを使うこともできる．もちろんこれらの関係は偽造確率と効率性に対するトレードオフである．

2.2.2. 分析

CPK 方式は JK 方式の２種の共謀可能性，(1) 販売者と判定者の共謀 (2)販売者と電子透かし認証局の共謀の中で販売者と判定者の共謀可能性は取り除いた．CPK 方式は販売者と電子透かし認証局の共謀可能性をとり除くために，すなわち電子透かし認証局が消費者がどんな電子透かしを選択したのか知ることができないようにするために， oblivious transfer protocol を用いた．しかし，もし電子透かし認証局が複数個の電子透かしを生成しなくて，同じ電子透かしのみを生成して oblivious transfer protocol の入力値で入れたら，電子透かし認証局は消費者がどんな電子透かしを選択したのか分かる．したがってCPK方式 でも電子透かし認証局と販売者の共謀可能性は存在する．

3. 提案方式

提案方式では可換暗号[16]を使って電子透かし認証局と販売者との共謀攻撃を防止しようとする．ここで共謀攻撃というのは電子透かし認証局と販売者，または判定者と販売者が自分の利益のために消費者のコンテンツ(消費者の情報が挿入されたコンテンツ)とまったく同じなコンテンツを作るための攻撃を意味する．提案方式で使う可換暗号はたとえ電子透かし認証局が消費者に妥当な電子透かしを生成してくれても，電子透かし認証局は消費者がどんな電子透かしを選択したのかに関しては分からないようにする役目をする．

3.1. 可換暗号

可換暗号はインターネット上の poker ゲーム[6]によく使われる暗号化手法である．Mental poker ゲームはその媒介体が電話やインターネットというのと具体的なカードがないということを除けば，実際の poker ゲームのようである．Mental poker ゲームの実行の時，一番難しい部分はカード分配である．カード分配は必ずランダムするように成り立たなければならず，カード分配者は参加者がどんなカードを選択したのか分からなくなければならなくて，参加者も自分がわがままカードを選択することができなければならない．我々は Elgamal cryptosystem に基盤した可換暗号を取り入れようとする．この手法はどんな情報の漏出もなくて，暗号をする手順が変わっても得られる最終の暗号文は同じであるから，多重参加暗号で拡張させることができる長所を持っている．手短に可換暗号に対して説明する．

Alice(カード分配者)と Bob(ゲーム修行者)，２人の参加者いて，彼らは同じパラメタを持っている．

$$K_A = \{(p, \alpha_A, k_A, \beta_A) = \beta_A \equiv {\alpha_A}^{k_A} (\mathrm{mod}\, p)\}$$
$$K_B = \{(p, \alpha_B, k_B, \beta_B) = \beta_B \equiv {\alpha_B}^{k_B} (\mathrm{mod}\, p)\}$$

A. 暗号

1. Alice はランダムな値 r_A を選択して，暗号化結果の K_A は式(5)の y_{1A} と y_{2A} で成り立つ．

$$K_A = \{(p, \alpha_A, k_A, \beta_A) = \beta_A \equiv {\alpha_A}^{k_A} (\mathrm{mod}\, p)\}$$
$$K_B = \{(p, \alpha_B, k_B, \beta_B) = \beta_B \equiv {\alpha_B}^{k_B} (\mathrm{mod}\, p)\} \quad (5)$$

2. Bob はランダム値 r_B を選択した後，式(6)を計算する．

$$y_{1B} = {\alpha_B}^{r_B} \bmod p, y_{2AB} = x{\beta_A}^{r_A}{\beta_B}^{r_B} \bmod p \quad (6)$$

ここで Alice が先に暗号をしていても，Bob が先に暗号をしていても彼らは同じ暗号文を得る．

B. 復号

1. Alice が先に復号するために自分の秘密鍵を使って式(9)を計算した後，

$$d_{K_A}(y_{1A}, y_{2AB}) = y_{2AB}({y_{1A}}^{k_A})^{-1} = y_{2B} \bmod p \quad (9)$$

2. Bob が自分の秘密鍵を使って式(10)を計算する．

$$d_{K_B}(y_{2B}) = y_{2B}({y_{1B}}^{k_B})^{-1} = x \bmod p \quad (10)$$

3.2. プロトコル

[仮定]

消費者が購買しようとするコンテンツを停止映像で限定する．もちろん他の手法と同様に，購買されるコンテンツは音楽，ビデオデータで拡張することができる．本論文で Alice は販売者で，Bob は消費者を表す．そして Carol は消費者の電子透かしを生成して，彼らの要請によってこれを生成してくれる電子透かし認証局を表す．

[定義]

- X: 原本イメージ，$X = \{x_1, \cdots, x_m\}$
- W: 電子透かし，$W = \{w_1, \cdots, w_n\}\ m \geq n$
- X': 電子透かしされたイメージ
- $X' = X \oplus W = \{x_1 \oplus w_1, \cdots, x_n \oplus w_n, x_m\}$
- $\oplus$: 電子透かし挿入アルゴリズム
- E: 暗号アルゴリズム
- D: 復号アルゴリズム
- E_H :同型特徴を持った暗号アルゴリズム
  $E_A(x) \cdot E_A(y) = E_A(x \cdot y)$
- E_T :置き換え特徴を持った暗号アルゴリズム
- $p(\leq nbits)$: $q = (p-1)/2$ を満足する大きい次数
- G:次数 $p-1$ の群
- g:群 G の生成元

Alice, Bob, Carol は次のように秘密鍵と公開鍵を持っている．$(sk_A, pk_A), (sk_B, pk_B), (sk_C, pk_C)$
$pk = g^{sk} \bmod p$．公開鍵はもう認証局に登録されたことで仮定する．

A. 電子透かし生成:

1. Bob は $sk^*_{B1} \cdot sk^*_{B2} = sk_B$ の条件を満足するランダムな値 sk^*_{B1}, sk^*_{B2} を選択する．Bob は pk_B, pk^*_B $(pk^*_B = g^{sk^*_{B1}})$ と Carol の公開鍵 pk_C で暗号化した sk^*_{B2} $(E_{Hpk_C}(sk^*_{B2}))$ を Carol に送る．この時 Bob は自分が sk^*_{B1} を所有していることをゼロ知識証明を利用して Carol に証明する．
2. Carol は先に自分の秘密鍵 sk_C を利用して $E_{Hpk_C}(sk^*_{B2})$ を復号して，${pk^*_B}^{sk^*_{B2}} = pk_B \bmod p$ と Bob の公開鍵 pk_B が等しいか確認する．2 つの値が等しければ，Carol は妥当な k 個の電子透かし $(W_1, W_2, \cdots, W_k)$ をランダムに生成し，Bob におくる．$W_i = \{w_{i1}, w_{i2}, \cdots, w_{in}\}$ である．

   Remark 1: 電子透かし認証局，Carol は k 個の電子透かしを生成して，これを受けた Bob はこれらの中で一つを選択する．この時，Carol が消費者 Bob が選択する電子透かしを正確に推測する確率は $1/k$ である．まである，k をどのくらいですることに対する問題は効率性と正確性のトレードオフである．

   Remark 2: 提案方式で我々は Cox ら[8]のアルゴリズムを電子透かしアルゴリズムで使う．[8]で Cox は平均値 0，分散 1 を持った電子透かしを用いて，これは実験的に結託攻撃に強い．
3. Carol は式(11)のように暗号アルゴリズムを利用して暗号された k 個の電子透かし $(P_1, \cdots, P_k)$ を暗号し，これらの署名をする．電子透かし (W_i) を Bob の匿名公開鍵 pk^*_B で暗号化して，これに対して署名 $sign_{sk_C}(E_{Hpk^*_B}(W_i)), i = \{1,2,\cdots,k\}$ をする．この時，Carol がした署名は電子透かしの妥当性を証明し妥当な電子透かしが Bob の匿名公開鍵で暗号化されたことを証明する．その後，Carol は鍵ペア (r_C, r'_C) を生成して，暗号アルゴリズム E_T を利用

して $P_1,\cdots,P_k$ を暗号する．ここで r_C は暗号用鍵で，r'_C は r_C に相等する復号化鍵である．そしてから，Carol は Bob に $(EP_1,\cdots,EP_k)$ を送る．

$$\begin{aligned} w_1 &= E_{Hpk_B^*}(W_1),\cdots,w_k = E_{Hpk_B^*}(W_k) \\ s_1 &= sign_{sk_C}(w_1),\cdots,s_k = sign_{sk_C}(w_k) \\ P_1 &= (w_1 \| s_1),\cdots,P_k = (w_k \| s_k) \\ EP_1 &= E_{T_{r_C}}(P_1),\cdots,EP_k = E_{T_{r_C}}(P_k) \end{aligned} \quad (11)$$

4. $(EP_1,\cdots,EP_k)$ が Carol の秘密鍵に暗号化されられたから，Bob は電子透かしとこれの署名 $(P_1,\cdots,P_k)$ を知ることができない．Bob はランダム値 (r_B,r'_B) を生成して，この時 r_B は暗号用鍵で，r'_B は復号用鍵で使われる．Bob は $(EP_1,\cdots,EP_k)$ 中から 1 つを選択する．ここでは Bob が $EP_3 = E_{T_{r_C}}(P_3) = E_{T_{r_C}}(w_3 \| s_3)$ を選択したと仮定する．Bob は暗号アルゴリズム E_T を利用して r_B で自分が選択した EP_3 を暗号化して，これを再び Carol に送る．

$$E_{T_{r_B}}(EP_3) = E_{T_{r_B}}(E_{T_{r_C}}(w_3 \| s_3)) \quad (12)$$

5. Carol は式(13)を計算して，自分のデータベースに pk_B, pk_B^* を保存しておいて，Bob は式(13)なように計算した $E_{T_{r_B}}(w_3 \| s_3)$ を Bob に送る．ここで Carol は Bob がどんな電子透かしを選択したのか知ることができない．何故ならば $(P_1,\cdots,P_k)$ は Bob の秘密鍵で再暗号化されられたからである．

$$D_{T_{r'_C}}(EP_3)\ D_{T_{r'_C}}\{E_{T_{r_B}}(EP_3)\} = E_{T_{r_B}}(w_3 \| s_3) \quad (13)$$

6. Bob は Carol の公開鍵 pk_C と自分の秘密鍵 sk_{B1}^*，そして r'_B を持って $E_{T_{r_B}}(w_3 \| s_3)$ を復号する．

B．電子透かし挿入：

今後，我々は表現の簡略化のために Bob が選択した w_i, s_i を w,s で表す．

1. Bob は Alice に w,s,pk_B^* を送る．
2. Alice は w が電子透かし認証局から生成された妥当な電子透かしなのか確認するため，s を検証する．検証が確認されれば，
3. Alice は X' を得るために原本コンテンツ X に挿入する電子透かし V をランダムに生成する．この時生成した V は Bob の唯一の情報であり，これは後に不正配布されたコンテンツが発見されられた時，不正配布者を確認するための使われる．ここで，X は Bob が購買するコンテンツである．Alice は Bob から受けた電子透かしを切り替えるため，$\sigma(E_{Hpk_B^*}(W)) = E_{Hpk_B^*}(\sigma(W))$ の条件を満足するランダムな置換 σ を生成する．
4. Alice は X' に二番目電子透かしを挿入する．Bob から受けた電子透かしがたとえ Bob の公開鍵に暗号化されていると言っても，同型特徴を持った暗号アルゴリズムの特徴の上，Alice は $E_{Hpk_B^*}(W)$ を復号せずに，2 番目の電子透かしを式(14)と一緒に挿入することができる．

$$\begin{aligned} E_{Hpk_B^*}(X'') &= E_{Hpk_B^*}(X') \oplus \sigma(E_{Hpk_B^*}(w)) \\ &= E_{Hpk_B^*}(X') \oplus E_{Hpk_B^*}(\sigma(w)) \\ &= E_{Hpk_B^*}(X' \oplus \sigma(w)) \end{aligned} \quad (14)$$

5. Alice は Bob に $E_{Hpk_B^*}(X'')$ を送って，自分のデータベース $Table_A$ に pk_B^*, V, σ, s, w を保存しておく．Alice が販売した各コンテンツによって分類された，すなわち各コンテンツを購買した消費者に対する情報を保存しておいた Alice のデータベースである．
6. Bob は式(15)なように X'' を得るために Alice から受けたコンテンツを復号化する．

$$\begin{aligned} D_{Hsk_{B1}^*}(E_{Hpk_B^*}(X'')) &= X'' = X' \oplus \sigma(w) \\ &= X' \oplus \sigma(f(i) \| F(i)) \\ &= X \oplus V \oplus \sigma(f(i) \| F(i)) \end{aligned} \quad (15)$$

今，Bob は Alice が再生成できない電子透かしが挿入されたコンテンツ X'' を持っている．なぜなら，Alice は Bob の秘密鍵 sk_{B1}^* が知ることができないし，電子透かし認証局 Carol と共謀しても，Bob が選択した電子透かしを知ることができないからである．一方，Bob も σ と V が分かっていないので X'' から $\sigma(w)$ と V をとり除くことができない．

C．不正配布者身元確認：

X の不正配布されたコンテンツを Y であると表す．Alice は Y で唯一の電子透かしを抽出して，これを利用してコピー Y の持ち主を追跡することができる．

1. 不正配布されたコンテンツ Y が発見されれば，Alice は Y で唯一の電子透かし U を抽出する．
2. Alice は自分のデータベース $Table_A$ に保存されたすべての電子透かしの中で抽出された電子透かし U と一番高い係わり合いが電子透かし V と彼にあ

たる使用者のレコードを捜す．もし Alice が自分のデータベースで係わり合いが高い V を捜せなければ，Alice は不正配布者を特定できない．一応，Alice のデータベース $Table_A$ から V が発見させなら，Alice は 該当の消費者の匿名公開鍵 pk_B^* と σ,s を判定者(任意の第3者)に送る．

3. 判定者は先に $s=sign_{sk_C}(E_{Hpk_B^*}(W))$ を検証して，これが確認できれば，該当の消費者の Real Id を Carol に要請する．
4. 判定者は該当の消費者に(Carol と Alice から不正配布者に指定された消費者)秘密鍵 sk_{B1}^* を要求した後，Y の中に $\sigma(W)$ があるのか確認して，W の存在を確認する．もちろんここで該当の消費者は自分の秘密鍵を露出しない．この場合は消費者が自分の秘密鍵を露出する代わり，$E_{Hpk_B^*}(W)$ を復号した結果の W を判定者に送る．判定者は Bob の匿名公開鍵でこれをまた暗号して，W を検証して，これが $E_{Hpk_B^*}(W)$ と等しいかを確認する．W が検証されれば，判定者は電子透かし抽出アルゴリズムを利用して，Y の中に $\sigma(W)$ の存在を確認する．もし $\sigma(W)$ の存在が確認されれば，Bob は不正配布者で特定される．

4. 比較と分析

以前の章で我々は電子透かし認証局と判定者に対する信頼を仮定しない匿名消費者-販売者電子透かし方式を提案した．提案方式で使われた基本アルゴリズムと電子透かしアルゴリズムは安全であると仮定を置いて，本章では提案方式の安全性を分析する．

4.1. 安全性の分析

[前提 1]

電子透かし認証局と販売者が共謀しても，消費者は安全に提案方式を実行できる．

[証明 1]

販売者が，どんな電子透かし W を持った電子透かしコンテンツ Y を偽造するためには， 販売者は消費者の秘密鍵 sk_{B1}^* または消費者の唯一の電子透かし W が分からなければならない． 提案方式では，sk_{B1}^* と W は消費者であるけが分かっている情報なので，販売者が共謀しても(離散対数問題が困難で，使われられた暗号アルゴリズムが安全であるという条件の下)，消費者は安全に提案方式を実行できる．提案方式で我々は電子透かし認証局が電子透かしを生成しても，消費者がどんな電子透かしを選択したのか分からないようにするために，commutative プロトコルを利用した．したがって販売者はどんな場合にも消費者のようなコンテンツの生成ができない．

また提案方式は消費者の匿名性も保障する．もちろん提案方式では正直な消費者の場合には，電子透かし認証局が消費者の Real ID を露出させないという仮定は置いている．

[前提 2]

提案方式は販売者の安全を保障する．

[証明 2]

提案方式に使われた暗号方式と電子署名の特徴のため，消費者は電子透かし認証局から受けた電子透かしを変えるとかとり除くことが不可能のである．また提案方式では消費者であるけが sk_{B1}^* が分かっているから，消費者は自分が不正配布者に指定された後に，不正配布されたコンテンツが販売者が再生成したコンテンツという主張ができない．したがって不正配布されたコンテンツが発見されて，不正者識別アルゴリズムを通じて不正配布者が決まれば，これは販売者ではなく該当の消費者が不正配布されたものを確認させられる．

4.2. 従来方式と比較

JK 方式では，販売者が判定者または電子透かし認証局と共謀すれば，販売者は容易に電子透かし W を持った消費者のコンテンツ Y を偽造することができる．したがって JK 方式では判定者と電子透かし認証局を信頼機関(TTP)で前提した．

CKP 方式でも，電子透かし認証局が Oblivious transfer protocol を実行する時，すべて同一の電子透かしを入力値で入れたら，電子透かし認証局が消費者の電子透かしが知ることができ，販売者と電子透かし認証局が共謀すれば，消費者のコンテンツ Y を偽造することができる．一方に，提案方式は販売者が電子

透かし認証局と共謀しても，消費者のコンテンツは偽造することができない．なぜなら，プロトコルに参加する個体の中で消費者を除いた誰も消費者の秘密鍵 sk_{B1}^{*}，消費者が選択した電子透かし W を知ることができないからである．

5. まとめと今後の課題

本提案方式で我々は販売者が電子透かし認証局と共謀した場合でも消費者のコンテンツを偽造できない方式を提案した．提案方式では電子透かし認証局が電子透かしを生成すると言っても消費者がどんな電子透かしを選択したのか分からない方法で上の従来方式の問題点を解決した．提案方式の問題点は不正者識別過程にすべて個体が参加しなければならないというのである．これからの研究課題は効率的な不正配布者識別プロトコル設計である．

謝辞

第一著者は「日本国際教育協会」と「韓国科学財団の基礎科学研究事業(No.01-2002-000-00589-0)」の支援を受けている．

参考 文献

[1] B.Pfitzman and Ahmad-Reza Sadeghi, "Coin-Based Anonymous Fingerprinting", *Eurocrypt'99, LNCS 1592*. pp.150-164. 2000.

[2] B.Pfitzman and M.Schunter, "Asymmetric Fingerprinting", *Eurocrypt'96, LNCS 1070*, 1996.

[3] B.Pfitzman and W.Waidner, "Anonymous Fingerprinting", *Eurocrypto'97, LNCS 1233*, 1997.

[4] D.Boneh and J.Shaw, "Collusion-secure Fingerprinting for Digital Data", *Crypto'95, LNCS 963*. 1995.

[5] D.Chaum, Ivan Bjerre Damgard and Jeroen van de Graaf., "Multiparty Computation Ensuring Privacy of Each Party's Input and Correctness of the Result", *Crypto'87, LNCS 293*, 1987.

[6] Goldwasser, S. and Micali, S. "Probabilistic Encryption and How to play Mental Poker Keeping Secret All Partial Information", *Proceedings of the 14th STOC*, pp.365-377, 1982.

[7] Hak-Soo Ju, Hyung-Jeong Kim, Dong-Hoon Lee and Jong-In Lim., "An Anonymous Buyer-Seller Watermarking Protocol with Anonymity Control", *ICISC2002, LNCS 2587*, 2002

[8] I.J. Cox, J.Kilian, T.Leighton, and T.Shamnon, "Secure spread spectrum watermarking for image, audio and video", *IEEE Transactions on Image Processing*, vol.6, no 12, pp.1673-1678, 1997.

[9] J.Camenisch and I.Damgard, "Verifiable encryption and applications to group signatures and signatures sharing", *Technical Report RS 98-32, Brics*, Department of Computer Science, University of Aarhus, Dec.1998.

[10] Jae-Gwi Choi, Kouichi Sakurai and Ji-Hwan Park, "An Anonymous Buyer-Seller Watermarking Without Trust Assumptions", IPSJ SIG Technical Report, 2003, p71-76.

[11] L.Qian and K.Nahrstedit, "Watermarking schemes and protocols for protecting rightfuk ownership and customer's rights", *J.Visual Commun. Image Represent*, vol. 9, pp.194-210, Sept. 98.

[12] Naor.M, Pinkas,B, "Oblivious Transfer and Polynomial Evaluation",31th ACM Symposium on Theory of Computing, ACM,1999.

[13] N.Asokan, Birgit Baum-Waidner, Matthias Schunter and Michael Waidner, "Optimistic fair exchange of digital signatures", *IEEE Journal on selected Areas in communication*, 18(4), pp.591-610, Apr.2000.

[14] Neal.R.Wanger, "Fingerprinting", *IEEE Symposium on Security and Privacy*, 1983.

[15] N.Memon and P.W.Wong, "A Buyer-Seller Watermarking Protocol", *IEEE Transactions on image processing,* vol.10, no. 4, April 2001.

[16] Weiliang Zhao, Vijay Varadharajan and Yi Mu, "A secure Mental Poker Protocol Over the internet", Australasian Information Security Workshop 2003. *Conference in Research and Practice in Information Technology, Vol.21*, 4.Feb.2003.