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

2003－CSEC－21 (12)
2003／5／16

認証局に対する 信頼仮定を 排除した 匿名 販売者-消費者 透かし方式

崔 在貴* ・ 櫻井 幸一+ ・ 朴 志煥*

あらまし：最近，Ju らによって，消費者は匿名でコンテンツを購入できるが，匿名性はコントロール可能である匿名販売者-消費者電子透かしプロトコルが提案されている．このプロトコルは，初めて電子透かしに匿名性を実現したものであるが，消費者の秘密鍵が露呈してしまう問題がある．さらに，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．本論文ではこの問題点を解決する．我々の提案手法では，離散対数問題が困難である限り，消費者の秘密鍵は露呈しない．また，我々は透かし認証局や他の機関に対する信頼を仮定しない．

An Anonymous Buyer-Seller Watermarking Without Trust Assumptions

Jae-Gwi Choi* · Kouichi Sakurai+ · Ji-Hwan Park*

Abstract: Digital watermarking scheme has been proposed as a method of copy protection and copy restraint for multimedia content. In copy restraint, a content owner (seller) inserts a unique watermark into a copy of the content before it is sold to a buyer. If the buyer distributes the unauthorized copies of the watermarked content, the buyer (a copyright violator) can be traced using a watermark detection algorithm. Recently, Ju et al., proposed an anonymous buyer-seller watermarking protocol, where a buyer can purchase contents anonymously, but anonymity control is provided. The significance of this protocol is that it first offered the anonymity of a buyer to watermarking schemes. But problems of this protocol are that the private key of a buyer can be exposed and whenever unauthorized copy is found, the three parties (the seller, the watermark certificate center, the judge) must all participate in the copyright violator identification process. In this paper, we propose a secure buyer-seller watermark protocol which can solve this problem. In the proposed scheme, the private key of a buyer will not be exposed if discrete logarithm problem is hard. Furthermore, we do not make any trust assumptions about the watermark certificate center or other authorities. Also, a seller can identify the copyright violator without the help of the watermark certificate center and the judge under robust watermarking schemes.

1．はじめに

新しいIT技術と電子商取引の急速な発展は安全な著作権保護の技術に対する強い要求をもたらしている．ディジタルデータの著作権保護に関するたくさんの研究が提案される．電子透かし方式はこれらの技術の中の一つである．これはディジタルデータについて所有権の挿入以外にコピー保護とコピー抑制の応用で使用される．コピー保護がどんな時点の後にもう以上ディジタルデータのコピーができないようにする反面，コピー抑制はディジタルデータを不正に配布した不正者を追跡する方法を提供する．特別に後者をフィンガープリントと用語で呼ぶ．フィンガープリントは各コン

* 釜慶大学校 情報保護学科．Department of Information Security, Pukyong national university, Busan, Korea.
+ 九州大学 大学院システム情報科学研究院．Faculty of Computer Science and Communication Engineering, Kyushu university, Fukuoka, Japan.

テンツにユニークなユーザ ID 情報を挿入して,コンテンツが不正配布された時,著作権違反者を追跡する. Pay-TV システム, マルチキャストコミュニケーションなどを用いた著作物の配布などに有用なブロードキャスト暗号は,センターが送信した暗号化コンテンツに対して,有効な鍵を持つ受信者のみがそのコンテンツを復号できる方式である. もし,認証を貰わない人 (pirate) が認証を貰った人(traitor)から復号鍵を受けたら, その復号器の中には認証を貰った人が検証できる情報が含まれている. この点で,各復号鍵が特定の復号器の所有者を追跡できる 透かしになる. これは, フィンガープリントの一種で,traitor tracing という名前で呼ばれている. このように,著作権保護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[8, 11]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 対称型だ. したがって,この透かしがある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. これは大きな問題点である.

・**非対称型手法**:対称型手法の問題は非対称型手法[2, 12]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出来ない.

・**匿名型手法**: 消費者のプライバシーを守るために,二つの技法[3, 5]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出来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]技法は高い計算量を必要とする secure two-party computation[4]を使ったので非効率で非実現的である. 最近に Ju らが,Memon・Wong の技法 (MW 技法) [12]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[5]. Ju らによる技法と MW による技法はで 結託攻撃に抵抗力が強い Cox の非可視的電子透かし[6]を使う. しかし Ju らの技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出来る. 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.

本論文では,我々は先ず Ju 技法の安全性に関する弱点を言及し,次に,この問題を解決した技法を提案する. 次の表に,以前の技法と我々の技法の特性を簡単に説明する. 表中の属性の定義は論文[5]にある.

	MW [12]	Ju [5]	Our Scheme
Anonymity	×	○	○
Unlinkability	×	○	○
No Framing	○	△*	○
No Reputation	○	△*	○
No two-party computation	○	○	○
Self-Operating identification	○	×	○
Trust Assumptions	○	○	×

*: 販売者と透かし認証局が共謀しなければ,該当機能を提供する.

- Anonymity: 消費者はコンテンツを匿名で買える.
- Unlinkability:二つのコンテンツがあったとき,それらのコンテンツを買ったのが同じ同一人物であるかを特定できない.
- No Framing:正当な消費者なら,悪意ある販売者または他の購入者て 著作権違反者で告訴されることは絶対にない.
- No Reputation: 告訴された消費者は販売者が自身のコンテンツを配布したと主張できない.
- Self-Operating identification:販売者は他人の助けを必要とせず著作権違反者の身元が知ることが出来る.
- Trust Assumptions:信頼センターはどんな不正もしないと仮定する.

本稿では, 2 章で Ju らの技法とそれの問題を, 3 章で我々の提案技法を説明する.

2. Ju 技法の概略

この技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,Ju らの論文と同じ表示を使う.

2.1. プロトコル

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

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暗号技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乗根だの物を証明するものである．ここには安全なverifiable暗号方法の存在を仮定する．検証されると，認証局は暗号文(C)が正確かにsk_B^*を暗号したものであると納得することが出来る．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．認証局は自分のテーブル$Table_{wa}$ 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形$(E_k(a \oplus b) = E_k(a) \oplus E_k(b))$だ．

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． $X'(= X \oplus V)$を透かし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．$E_{pk_B^*}(W)$ を復号しないで，二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，$\sigma(E_{pk_B^*}(W)) = E_{pk_B^*}(\sigma(W))$を満足する置換関数を捜す．透かし認証局によって使われた暗号アルゴリズム E の同型速成のため，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⊕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．

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，

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

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sk_B^*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．

2.2 分析

安全性分析：Juらの技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れたコンテンツとまったく同じな 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．

- ケースI． 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$Table_{wa}$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．

- ケースII． 販売者と判定者の共謀

論文[9]でJuらは,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,消費者だ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．後に販売者は彼のテーブルから得られた $C, Epk_B^*(X'')$ 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けるので,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．

効率性分析：Juらの技法は同型特性と Verifiable encryption[7]の特性を持つ公開鍵暗号アルゴリズムに基盤を置いている．この論文は MW技法と比べると安全な Verifiable encryption の存在に対する追加的な仮定を置いている．この論文で Juらは告訴された消費者の参加なしに不正配布者の特定可能にするため Verifiable encryption を利用している．しかし Verifiable encryption は安全なハッシュ関数[11, 14]などが要求される．

次の章で我々は追加要求がなく,さらに消費者の参加が不要であるプロトコルを提案する．

Ju らの技法のまた２つ目の次点は消費者の匿名性の保護に問題がある点である．大部分の匿名プロトコルは消費者の身元を一つの信頼センターだけが知ってあるので,消費者の身元露呈する可能性を低くしでる．しかしこの技法では透かし認証局と判定者は皆,消費者の匿名公開鍵とそれに対応する消費者の身元が分かるそのある．それにこの技法では判定者は任意の第 3 者ではなく必ず特定の人物で,不正配布者確認過程では消費者を除いたすべての人物が参加しなければならない．これは不正コピーが発見されられる度に他の人物は無条件に参加しなければならないので,該当する人物の大きな負担になりうる．

3. 提案方式

本章では認証局と判定者に対するどんな信頼仮定を必要とせず,不正配布者確認過程でも販売者一人で実行可能な消費者-販売者透かしプロトコルを提案する．

3.1 辞書段階

仮定：本章で Aliceは販売者で,Bobは消費者を表す．また本方式に使われるアルゴリズムは安全だと仮定する．

正義：透かし挿入過程は $X' = X \oplus W$ で 表示する,ここで,

- 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
- $sk_{A(B\,or\,wa)}$ ：Alice(Bob or 透かし認証局)の秘密鍵 $(pk_A = g^{sk_A})$

3.2. プロトコル

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_{wa} を使って sk_{B2}^* $(E_{pkw_a}(sk_{B2}^*))$ 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[1, 9, 10, 13]を遂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を秘密鍵復号して,Bob の公開鍵 pk_B を持って $pk_B^{*sk_{B2}^*} = pk_B \bmod p$ 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 プロトコル遂行のために 2 個の透かしを生成する． 認証局は次の多項式

$f(x) = \sum_{i=0}^{n} a_i x^i \pmod p$ を生成して

$f(i), i = \{0,1\}$,

$F(i) = pk_B \cdot (pk_B^*)^{a_0} (pk_B^*)^{a_i i_0} \cdots (pk_B^*)^{a_k i^k}$ を計算する．認証局は Bob の匿名公開鍵を持って $(f(i), F(i))$ を暗号化して（式(２)），これに対する署名を遂行する（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．

$$Enc - W_0 = E_{pk_B^*}(f(0) \,\|\, F(0))$$
$$Enc - W_1 = E_{pk_B^*}(f(1) \,\|\, F(1)) \qquad (2)$$

$$Sig_0 = sign_{sk_{wa}}(Enc - W_0 \,\|\, pk_B^*)$$
$$Sig_1 = sign_{sk_{wa}}(Enc - W_1 \,\|\, pk_B^*) \qquad (3)$$

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 個の透かしと認証局の署名を現わす.

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

Bobは 2個の透かしの中で 1個を選択して，ここで認証局は Bob がどんな透かしを選択したのか分からない．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.

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

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に対する確率と効率性に対する トレードオフである.

透かし挿入：ここから，簡略化のために $E_{pk_B^*}(f(i) \| F(i)), sig_i$ は w, s と記す．Bob は Alice に w, s, pk_B^* を送る．Alice は w が透かし認証局から検証受けた妥当な透かしように s を確認して，確認されれば，Alice はユニークな透かし V を生成してコンテンツに挿入する．ここで X を Bob が Alice から購買しようとするコンテンツだと置く．AliceはBobから受けた暗号化された透かしを変えること(置き換え)ためにランダム置き換え関数 σ を生成して，$\sigma(E_{pk_B^*}(W)) = E_{pk_B^*}(\sigma(W))$. を計算する．Alice はに 2 番目透かしを挿入する．Bob から受けた透かしが Bob の匿名公開鍵で暗号化されたが，同型属性を持った暗号アルゴリズムの特性の上 Alice は式(6)のようにここにまた他の透かしを挿入することができる.

$$\begin{aligned} E_{pk_B^*}(X'') &= E_{pk_B^*}(X') \oplus \sigma(E_{pk_B^*}(w)) \\ &= E_{pk_B^*}(X') \oplus E_{pk_B^*}(\sigma(w)) \\ &= E_{pk_B^*}(X' \oplus \sigma(w)) \end{aligned} \quad (6)$$

Alice はBobに $E_{pk_B^*}(X'')$ を送って，自分のテーブルに pk_B^*, V, σ, s, w を保存しておく．テーブルは Alice が販売した各コンテンツに対する各人物の情報を維持するレコードを意味する．Bob は Alice から受けたコンテンツを復号化して使う．Bob が挿入された透かしは知っているのが σ は分からないから $\sigma(w)$ を除くことができない.

不正配布者身元確認：不正配布物 (Y) が発見されれば，Alice は Y からユニークな透かし (U) を抽出する．堅固な透かし技法の場合，Alice は不正コピーから抽出した U と自分のテーブルに保存されたすべての透かしを比べて，一番高い相関性を持つ V を捜すでしょう．あったら，Alice は該当の消費者の匿名公開鍵が分かって，これを利用して w を抽出することができるでしょう．先に Alice は pk_B^* を持って計算した値 $E_{pk_B^*}(w)$ と Y から抽出した w を比べて w を検証する．2 個の値が一致すれば Alice は一人で著作権違反者を特定することができる．$pk_B = \frac{F(i)}{pk_B^{*f(i)}}$ もし Alice が w は抽出することができないか．V は捜すことができたら彼女は透かし認証局の助けを借りて該当の不正者の身元を確認することができる．もし U から抽出した V と関係が高い V を自分のテーブルで捜すことができなかったら，この過程は失敗に帰る.

3.3. 提案方式の分析

消費者と販売者の安全性：販売者と認証センターが共謀すると言っても，正当な消費者は絶対に著作権違反の罪で告訴されない．何故ならば w を挿入された Y を偽造するためには販売者は消費者の秘密鍵または消費者のユニークな透かしを知る必要があるからであるからだ．　本方式では認証センターでさえも消費者がどんな透かしを選択したのか分からない．したがって販売者は消費者のようなコピーを作ることができない．また離散代数問題が困難であれば，本提案方式ではどんな誰も消費者の秘密鍵を計算することができないので，消費者は安全にプロトコルを行うことができ，販売者やっぱりも(消費者が他人によって不正コピーが配布されたことを主張することができないので)不法配布物を見つければ著作権違反者を抽出することができる．もちろん提案方式でも透かし認証局は最小限消費者の匿名性に対する露呈はしないことを前提にする.

否認及偽造不可:本方式は販売者と透かし認証局が共謀をすると言っても,販売者は消費者のコピーのようなことを作ることができない.何故ならば透かし認証局も消費者がどんな透かしを選択したのか分かることができないし,消費者の秘密鍵は消費者以外には誰もわからないからだ.

自動著作権違反者確認:Ju らの技法が不正配布者の身元確認時,透かし認証局と判定者の助けを必要とする一方,本方式は他人の協力を必要としない.もし販売者が不正配布されたコピーから $w(=f(i)\|F(i))$ を正確に抽出することができたら,販売者は一人で著作権違反者の身元を確認することができる.もし正確な $w(=f(i)\|F(i))$ を抽出し出すことができなければ,販売者は透かし認証局の協力により不正配布者の身元を確認することができる.また本方式で判定者は任意の第三者は誰も判定者になることができる.

4. まとめ·今後の課題

販売者,消費者の権利と消費者の匿名を保護する為に,Ju らが匿名販売者-消費者電子透かしプロトコルを提案した.しかしこのプロトコルの問題は,消費者の秘密鍵が露呈してしまう可能性と,著作権違反者の確認(抽出)過程において全ての人物らが参加しなければならい.　本論で,我々はこの問題を解決した.さらに本提案方式は透かし認証局に関するどんな信頼仮定も必要ではない.

どんなケースの下においても,販売者一人で著作権位牌者の確認(抽出)できる匿名販売者-消費者電子透かしプロトコルに関する研究が今後に必要になると考えられる.

5. 謝辞

本研究は一部,「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] Bellare, M., Micali, S., "Non-Interactive Oblivious Transfer and Applications", Advances in Cryptology-CRYPTO'89, LNCS 435, Springer-Verlag, 1990, pp.544-557.

[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.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.

[5] Hak-Soo Ju, Hyung-Jeong Kim, Dong-Hoon Lee and Jong-In Lim., "An Anonymous Buyer-Seller Watermarking Protocol with 2002

[6] 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.

[7] 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.

[8] 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.

[9] Naor, M., Pinkas, B., "Oblivious Transfer and Polynomial Evaluation", 31th ACM Symposium on Theory of Computing, ACM, 1999, pp.245-254.

[10] 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.

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

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

[13] Rabin, M. O., "How to Exchange Secrets by Oblivious Transfer", Technical Memo TR-81, Aiken Computation Laboratory, 1981.