Buyer-Seller Watermarking Protocols with Off-line Trusted Parties

Chun-I Fan, Ming-Te Chen, Wei-Zhe Sun


The final publication is available at http://inderscience.metapress.com
Outline

• Introduction
• Problems
• Our idea
• The proposed scheme
• Conclusions
Introduction

- Information hiding
  - Watermarks
  - Fingerprints
- Watermarks
  - Visible watermarks
  - Invisible watermarks
Introduction

Visible watermark (From HP)
Introduction

Invisible watermark
Introduction

• Homomorphic Encryption

\[ E(x) \theta E(y) = E(x \theta y) \]

Do not need to decrypt \( E(x) \) and \( E(y) \)
Introduction

• A traditional watermarking protocol

Buyer

A watermark,  
A purchase order

A digital content embedded  
with the buyer’s watermark

Seller
Problems

1. The buyer tracing problem
2. The buyer’s right problem
3. The binding problem
4. The anonymity problem
5. The dispute problem
The buyer tracing problem

Seller (Honest) → How to trace the distributor?

Buyer

Buyer

...
The buyer’s right problem

1. Make a duplicate copy of a content to frame buyer Y

2. How to prove that she/he is innocent to the TTP?
The binding problem

• Step 1

Buyer A’s content X

Seller (Malicious)

Watermark extraction algorithm

Watermark $W_A$ of buyer A

Original content A
The binding problem (cont.)

• Step 2

Watermark $W_A$ of buyer A

Another content Y (Never bought by buyer A)

Watermark insertion algorithm

Content Y with Watermark $W_A$

• Step 3

Content B with watermark $W_A$

Seller (Malicious)

Buyer A

frame
The anonymity problem

- After transaction, the seller or WCA may derive the link between buyer A and the digital content that A purchased.
The dispute problem

Buyer M (Malicious)
1. Distribute a digital content
2. Deny the distribution of the content

Seller

2. The content

TTP

How to solve the dispute?
Our idea

• Preliminary
  – Our idea solves the above four problems via
    • Signatures
    • An off-line trusted party
  – The anonymity problem is solved by
    • One-time keys
    • Separate the personal information of each buyer
Our idea (cont.)

<table>
<thead>
<tr>
<th>Buyer</th>
<th>ID</th>
<th>content</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Alice</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>Bob</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>John</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Buyer</th>
<th>ID</th>
<th>content</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Image</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>Mp3</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>Video</td>
<td></td>
</tr>
</tbody>
</table>

WCA Knows Buyer

Seller Knows Seller

Achieve the anonymity property
The proposed scheme

(1) Send out the purchase order
(2) Request for a valid watermark
(3) Return the watermark
(4) Forward the content

Buyer -> Seller

The WCA device
## Notation Definition

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( ARG )</td>
<td>The description of a purchase content</td>
</tr>
<tr>
<td>( X )</td>
<td>The original content without watermarks</td>
</tr>
<tr>
<td>( I_B )</td>
<td>The identity of the buyer</td>
</tr>
<tr>
<td>((e_B, d_B), (e_{WCA}, d_{WCA}))</td>
<td>The public-private key pairs of the buyer and WCA</td>
</tr>
<tr>
<td>((e_T, d_T))</td>
<td>A temporary public-private key pair of the buyer</td>
</tr>
<tr>
<td>( V )</td>
<td>Seller’s watermark</td>
</tr>
<tr>
<td>( \text{Sig}_k(\cdot) )</td>
<td>The signature function with key ( k )</td>
</tr>
<tr>
<td>( \oplus )</td>
<td>A watermark insertion operator</td>
</tr>
</tbody>
</table>
### Notation Definition (cont.)

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E_k(\cdot)$</td>
<td>The homomorphism encryption function with key $k$</td>
</tr>
<tr>
<td>$D_k(\cdot)$</td>
<td>The decryption function with key $k$</td>
</tr>
<tr>
<td>$Cert_{CA}(e_B)$</td>
<td>The certificate of the buyer issued by CA</td>
</tr>
<tr>
<td>WCA</td>
<td>Watermark Certificate Authority</td>
</tr>
<tr>
<td>The WCA device</td>
<td>A tamper-resistant device issued by WCA</td>
</tr>
</tbody>
</table>
The proposed scheme

$M_1 = \{e_T, ARG, \text{Sig}_{d_T}(e_T||\text{ARG})\}$

$M_2 = \{e_T, I_B, \text{Cert}_{CA}(e_B), \text{Sig}_{d_B}(e_T||I_B)\}$

$M_4 = \{\text{Sig}_{d_{WCA}}(e_T||E_{e_{WCA}}(W)||E_{e_T}(W)), E_{e_T}(W), E_{e_{WCA}}(W)\}$

$M_3 = E_{e_{WCA}}(M_2)$
# Efficiency

<table>
<thead>
<tr>
<th></th>
<th>Memo Wong</th>
<th>Lei</th>
<th>Zhang Fan</th>
<th>Choi</th>
<th>Ours</th>
</tr>
</thead>
<tbody>
<tr>
<td>The buyer tracing problem</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>The customer right problem</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>The binding problem</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>The anonymity problem</td>
<td>×</td>
<td>Δ</td>
<td>Δ</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>The dispute problem</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>Without on-line TTPs</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>✓</td>
</tr>
</tbody>
</table>

✓: total solved  ×: No solved  Δ: partially solved
Conclusions

• Our scheme can cope with above the five problems.

• It can fully protect the privacy of each buyer.
Q&A