Secure Media Processing

BIRS, July 2005, Banff

Ton Kalker
+ Play Control / Forensic Watermark W
Secret Watermark Should Be Not Retrievable from Implementation

How to Compute Linear Correlation between Y and W from Y and E[W]?

Watermark Detection Circuitry (Linear Correlation)

Y

X

X + W

Enrypted[W]

WM Yes / WM No
Secure Media Processing

• Two examples of
  – signal processing
  – of encrypted data
  – without access to decryption/encryption keys
    • Transcoding
    • Correlation (watermark detection)

• Context
  – Non-trusted environment
  – Limited computing resources

• Other examples
  – Querying encrypted data
  – Compression of encrypted data
  – …

• Theme: secure processing of media
Introduction to Secure processing methods

• Three examples

• Exposing data structure
  – Trancoding (Apostolopolous et al.)

• Exploiting distributed knowledge
  – Compressing encrypted data (Ramchandran et al.)

• Structure preserving cryptography
  – Secure watermark detection (Katzenbeisser et al.)

• ...

Secure Transcoding
Make Transcoding Easy -- Scalable coding

Key features of scalable coding

- Embedded bitstream: Quality depends on amount of decoded data
- Only need earlier segments to decode

(John Apostolopolous, Susie Wee) ©
Adapt Encryption -- Progressive encryption

Progressive Encryption: class of algorithms that encrypt data sequentially

Key features of progressive encryption
- Earlier bits fed into later bits
- Only need earlier segments to decrypt

(John Apostolopolous, Susie Wee) ©
Formatting – Expose Truncation Information

- Recommended truncation points
- Rate-Distortion information

Secure Transcoder

Unencrypted Header

Secure Scalable Data

Read Packet Header

Truncate Data

(John Apostolopolous, Susie Wee) ©
Secure Transcoding

Approach:
- Combine scalable coding & progressive encryption

Result:
- Secure Scalable Data

(John Apostolopolous, Susie Wee) ©
Compressing Encrypted Data
Standard Approach

- Compress
- Encrypt
- Decrypt
- Decompress

Key

(Ramchandran et al.) ©
Non-Standard Approach

(Ramchandran et al.) ©
Coding with Side-Information -- Slepian-Wolf

- Bernouilli, $p \neq 0.5$
- $Y ::$ Bernouilli, $p = 0.5$

1. $K$ known at the decoder
2. $K$ is noisy version of $Y$
3. Slepian-Wolf!

(XOR) → Compress → Decompress → XOR

Key $K$

encoder (e.g. LDPC)

(Ramchandran et al.) ©
Structure Preserving Cryptography
Homomorphic Encryption

- Let $(M,+)$ and $(C,+)$ be two algebraic groups
  - example
    - $(M,+)$ :: additive structure on $\mathbb{Z}$ mod $N$
    - $(C,\times)$ :: multiplicative structure on invertible elements of $\mathbb{Z}$ mod $N$

- Let $C = (M,C,K,E,D)$ be a crypto-system on $M$ and $C$

- $C$ is called **homomorphic** when the encryption function $E$ (and decryption function $D$) preserve the algebraic structures on $M$ and $C$, i.e.

$$E[k,m_1] + E[k,m_2] = E[k,m_1 + m_2]$$

(Katzenbeisser, Kalker) ©
Homomorphic Encryption

• Example
  - Take \((M,+)\) and \((C,+)\) as before

\[ E[k,m] = k^m \]

• Some facts
  - Homomorphic encryption systems that preserve \((+,-,x,/\) are not secure
    • Intuition: if encryption preservation preserves too much structure, security is lost
  - There exist homomorphic encryption systems that preserve \((+,-,x)\)
    • Intuition: rich homomorphic encryption systems do exist however

(Katzenbeisser, Kalker) ©
A Simple Watermarking System

• Original signal X
  - \( X = \{x_1, x_2, \ldots, x_n\} \)

• Watermark signal W
  - \( W = \{w_1, w_2, \ldots, w_n\}, w_i = \pm 1 \)

• Marked signal Y
  - \( Y = X + W \)

• Watermark detection (with threshold T)
  - Large normalized correlation between Y and W or not?

\[
\frac{\langle Y, W \rangle^2}{\langle Y, Y \rangle} = \frac{\left(\sum w_i y_i\right)^2}{\left(\sum y_i y_i\right)} \geq T
\]

(Katzenbeisser, Kalker) ©
Watermark Detection Circuitry (Linear Correlation)

Y → E[W] → WM Yes / WM No

(Katzenbeisser, Kalker) ©
Blinding of Watermark Sequence

- Known protocols require $E$ to be component-wise
  - $E[W] = \{E[w_1], \ldots, E[w_n]\}$
  - Deterministic scrambling methods will not work
  - Example:
    - $w \in \{-1, 1\}$, then $E[w] \in \{E[-1], E[1]\}$
    - $W$ can be estimated from binary valued $E[W]$ up to sign!
    - value set of $W$ too limited
  - $E$ randomized with blinding vector $R = \{r_1, \ldots, r_n\}$
    - $R$ pseudo-random
    - $E[R,W] = \{E[r_1,w_1], \ldots, E[r_n,w_n]\}$
    - Blinding compensates for limited value set

(Katzenbeisser, Kalker) ©
Homomorphic Blinding

- **Example scrambling function**
  - $N$ large integer
  - $h, g$ generators of units in $\mathbb{Z}_N$ (invertible integers modulo $N$)
    - $h, g$ have inverse modulo $N$ and powers of $h, g$ generate all units
  - **Example**
    - $N = 10$
    - $U_{\mathbb{Z}_{10}} = \{1, 3, 7, 9\}$
    - generators 3 ($3, 3^2 = 9, 3^3 = 7, 3^4 = 1$) or 7 ($7, 9, 3, 1$)
- Then define $E[r,w]$ by (blinded El Gamal)

$$E[r,w] = h^r g^w \text{ (mod } N)$$

- $E[r,w]$ is easy to compute
- $E[r,w]$ difficult (impossible) to invert
- **Example**
  - $E[r,w] = 3^r 7^w \text{ (mod } 10)$

(Katzenbeisser, Kalker) ©
Homomorphic Blinding

- The previously defined scrambling function preserves arithmetic structure

\[ E[r_1, w_1] \times E[r_2, w_2] = E[r_1 + r_2, w_1 + w_2] \]

\[ (h^{r_1}g^{w_1}) \times (h^{r_2}g^{w_2}) = h^{r_1+r_2} g^{w_1+w_2} \]

- Algebraic consequence:

\[ E[r, w]^m = E[m\times r, m\times w] \]

- Homomorphic property
  - addition in clear-text → multiplication in cipher-text
  - multiplication in clear-text → exponentiation in cipher-text

(Katzenbeissner, Kalker) ©
Correlation in the encrypted domain

- $E[R,W]^Y = \prod E[r_i, w_i]^{y_i} = E[\Sigma r_i y_i, \Sigma w_i y_i] = E[<R,Y>, <Y,W>]$
Squared Correlation in the encrypted domain

- Watermark detection (with threshold T)
  - Large normalized correlation between Y and W or not?

\[
\frac{\langle Y, W \rangle^2}{\langle Y, Y \rangle} = \frac{(\sum w_i y_i)^2}{(\sum y_i y_i)} \geq T
\]

- Squared correlation needed: \( \langle Y, W \rangle^2 = \sum y_i y_j w_i w_j \)

- Provide scrambled version of \( W \otimes W \), i.e. \( \{w_i w_j\} \), in stead of \( W = \{w_i\} \)

- Watermark detection circuit computes

\[
\]

(Katzenbeisser, Kalker) ©
Watermark Detection Circuitry (Linear Correlation)

$E[W \otimes W]$

WM Yes / WM No
Hostile environment computations

• Compute normalization factor

\[ A = \langle Y, Y \rangle^* T \]

• Compute squared correlation

\[ B = E[R,W \otimes W]^Y \otimes ^Y = E[\langle R, Y \otimes Y \rangle, \langle Y, W \rangle^2] \]

• Compute normalized correlation

\[ E[\langle R, Y \otimes Y \rangle, C] = E[S,C] = B / A \]
Secure Assistance

- Bulk computations in hostile environment
- Interpretation of outcome in trusted environment

(Watermark Detection Circuitry)

Y \( \rightarrow \) \( E[R,W \otimes W] \rightarrow \) WM Yes / WM No

N

Watermark Detection Circuitry

E[S,C]

Sign(C)

- Remove blinding factor S
- Decrypt correlation value

Secure Chip

(Katzenbeisser, Kalker) ©
Paillier encryption

- Paillier encryption system
  - Removal of blinding factor
  - Retrieval of correlation value

- El Gamal encryption with well-chosen parameters
  - N well-chosen large integer
  - h, g generators of units in $\mathbb{Z}_N$ (invertible integers modulo N)

- Blinding and encryption
  $$E[r, x] = h^rg^x$$

- Blinding factor removal
  $$E^r = E[r, h^rg^x] = h^r g^x$$

- Special g makes Discrete Logarithmic problem easy
  $$g^x \rightarrow x$$

(Katzenbeisser, Kalker) ©
Secure Assistance

- Bulk computations in hostile environment
- Interpretation of outcome in trusted environment

Watermark Detection Circuitry

$E[R,W\otimes W]$

Y

Secure Chip

N

$E[S,C]$

Sign(C)

- Remove blinding factor $S$
- Decrypt correlation value

WM Yes / WM No

(Katzenbeisser, Kalker) ©
Summary

• Secure Media processing

• Three examples
  - Exposing data structures
  - Exploiting distributed knowledge
  - Structure preserving encryption

• Looking ahead
  - More relevant problems?
  - More approaches?