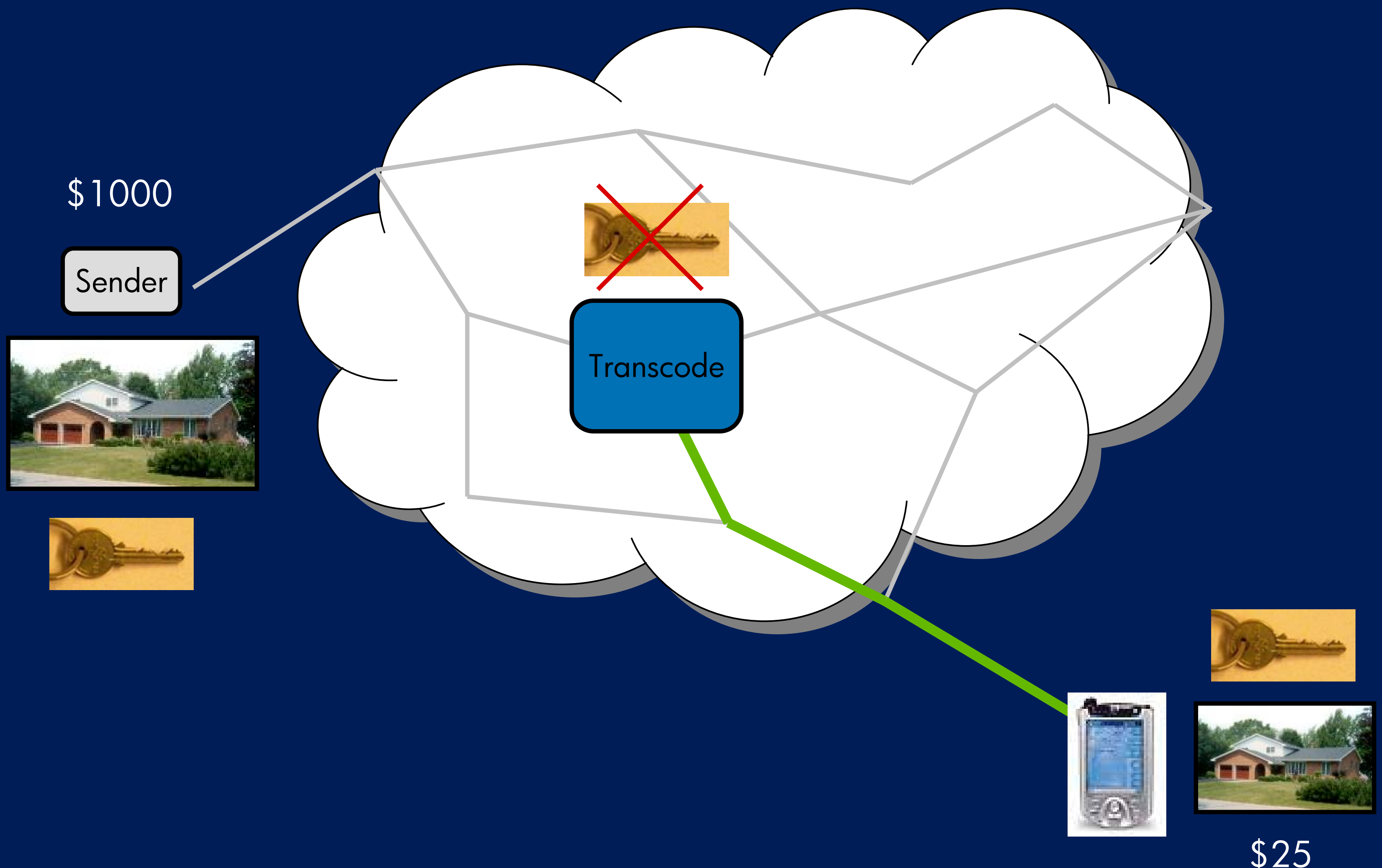
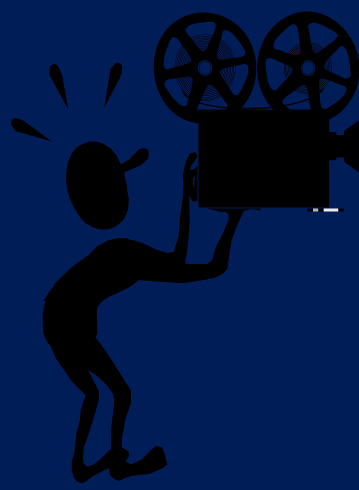
Secure Media Processing

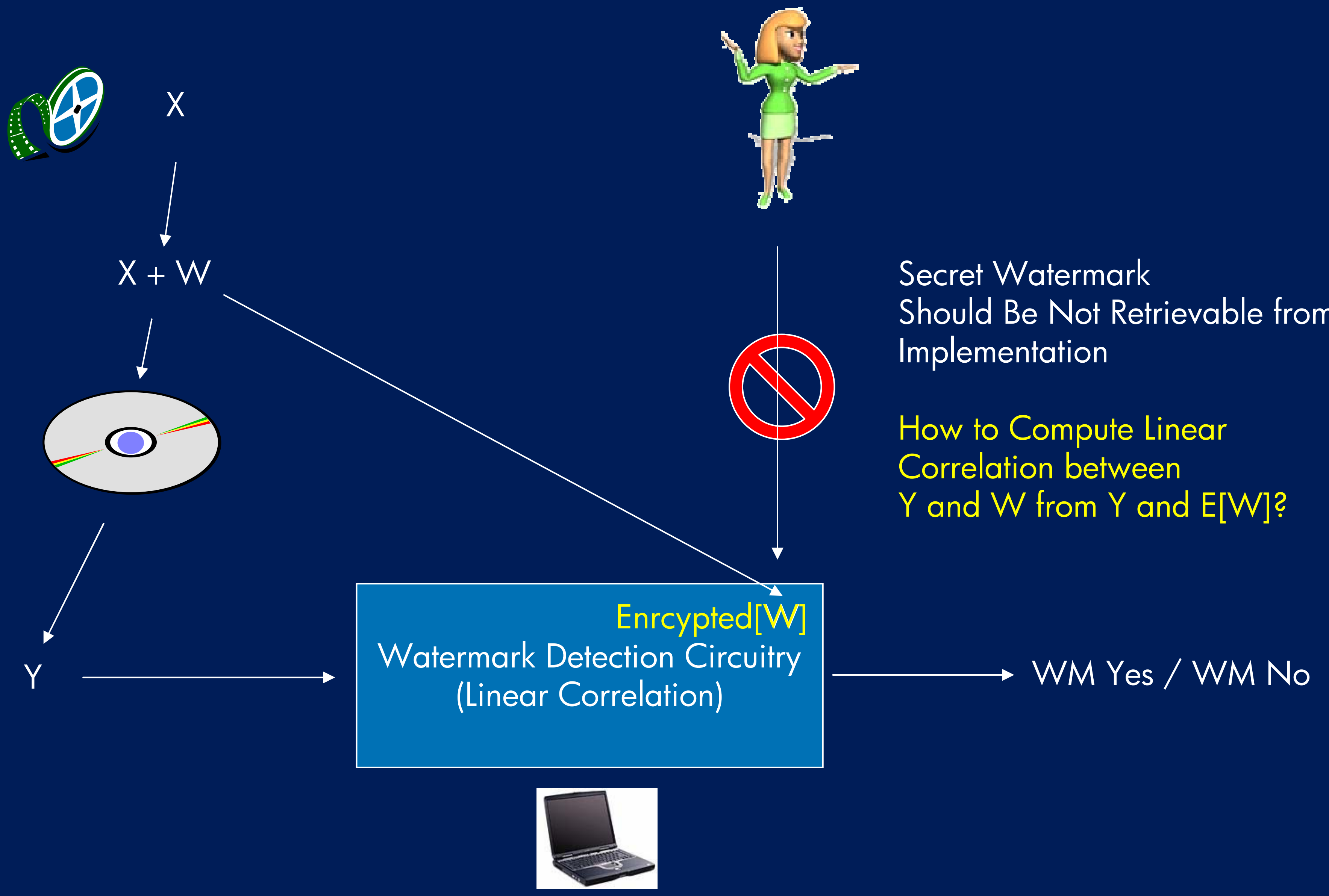
BIRS, July 2005, Banff

Ton Kalker


$1000
Sender
Transcode
$25

+ Play Control / Forensic Watermark W




X
X + W
Secret Watermark
Should Be Not Retrievable from
Implementation
How to Compute Linear
Correlation between
Y and W from Y and E[W]?
Enrcypted[W]
Watermark Detection Circuitry
(Linear Correlation)
Y
WM Yes / WM No

Secure Media Processing

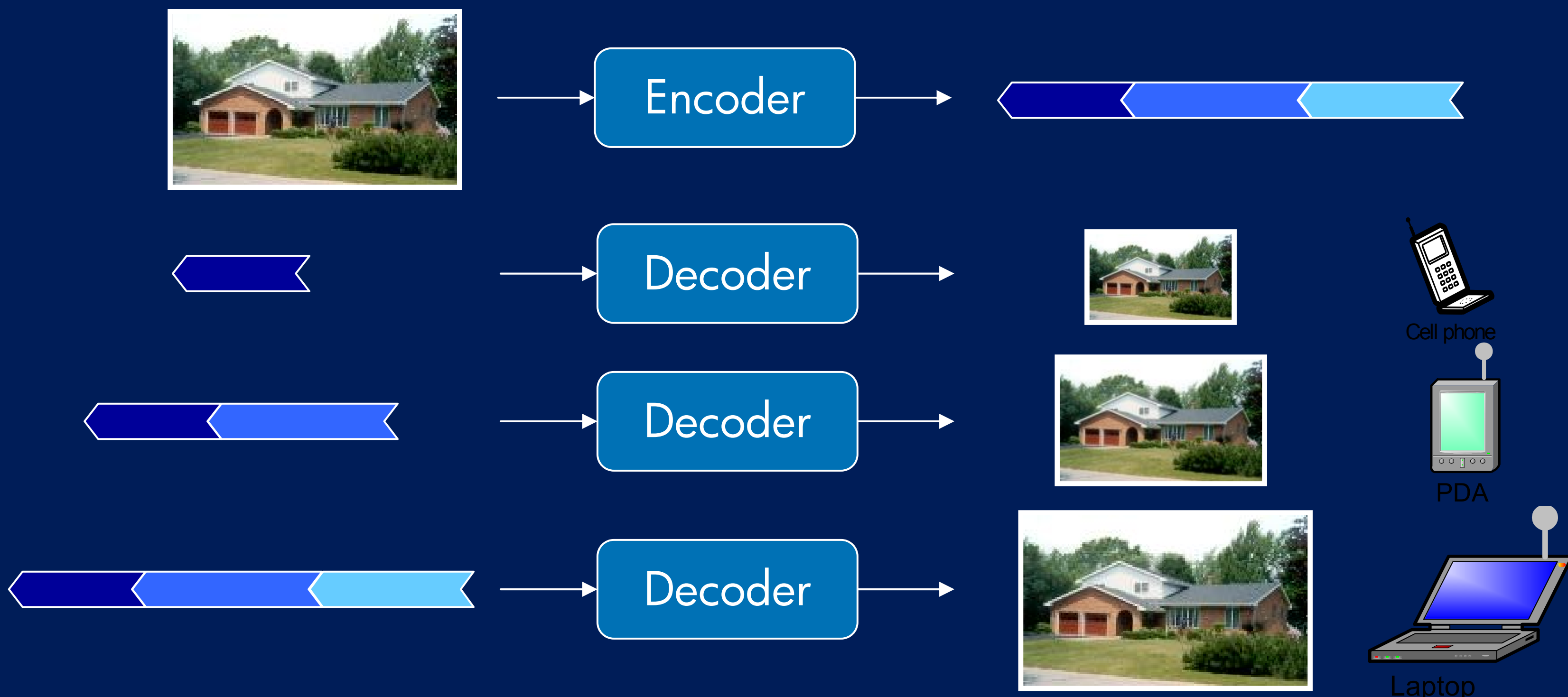
- Two examples of
  - signal processing
  - of encrypted data
  - without access to decryption/encryption keys
    - Transcoding
    - Correlation (watermark detection)
- Context
  - Non-trusted environment
  - Limited computing resources
- Other examples
  - Querying encrypted data
  - Compression of 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



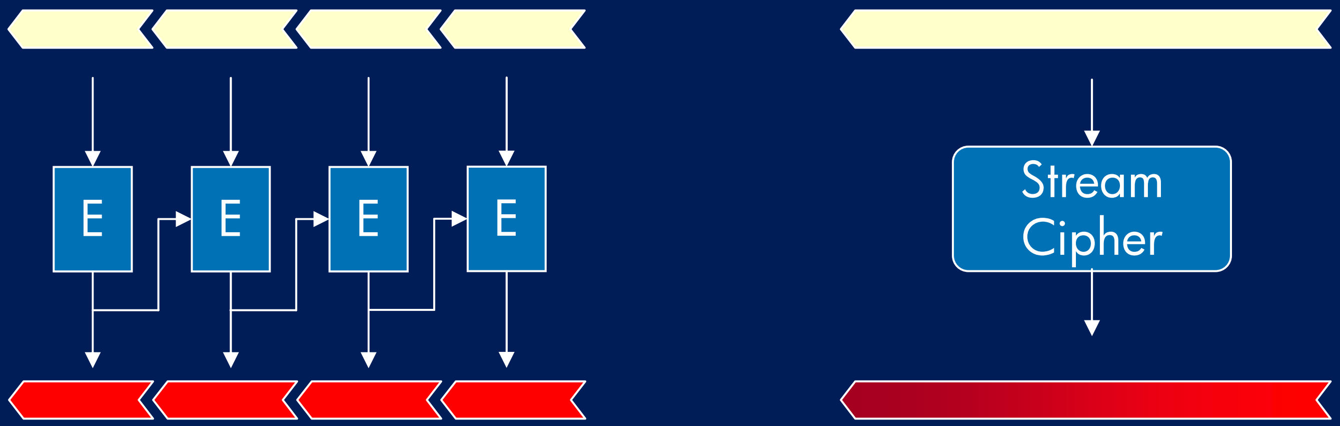
Key features of scalable coding

- 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



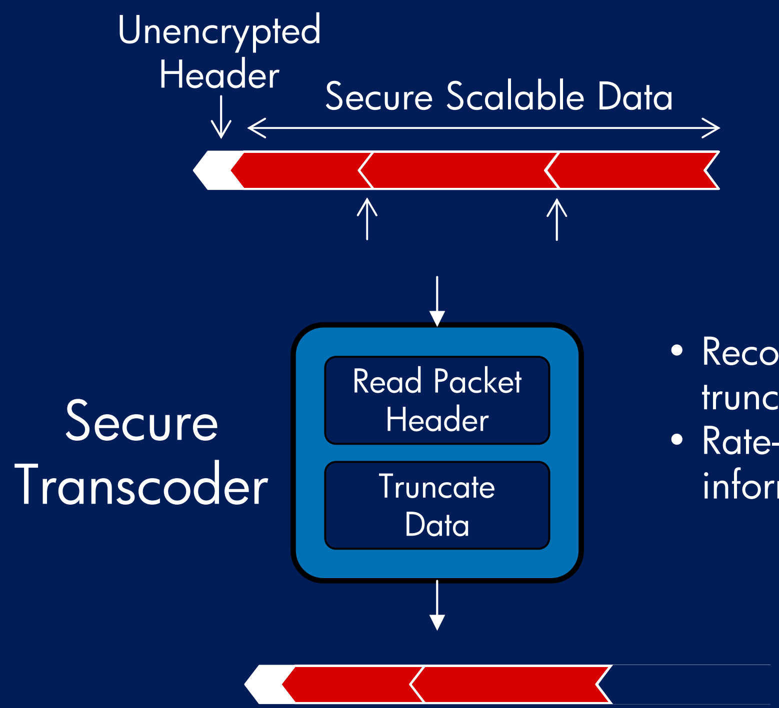
Cipher block chains

Stream ciphers

Key features of progressive encryption

- Earlier bits fed into later bits
- Only need earlier segments to decrypt

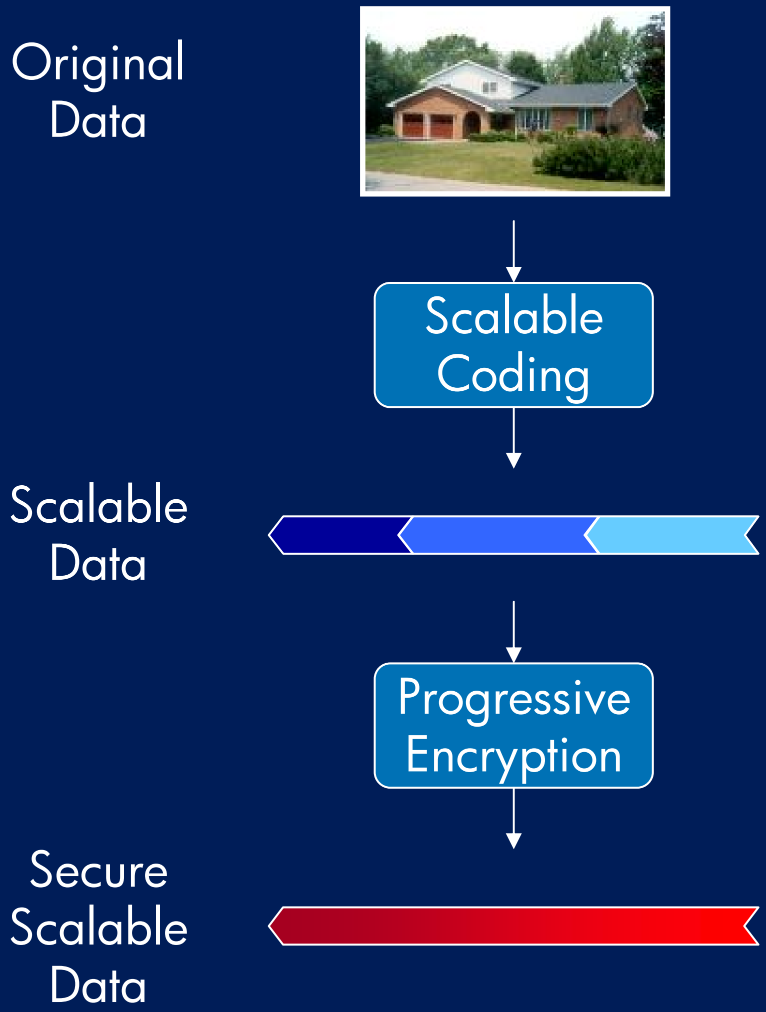
Formatting – Expose Truncation Information



- Recommended truncation points
- Rate-Distorsion information

(John Apostolopolous, Susie Wee) ©

Secure Transcoding



Approach:

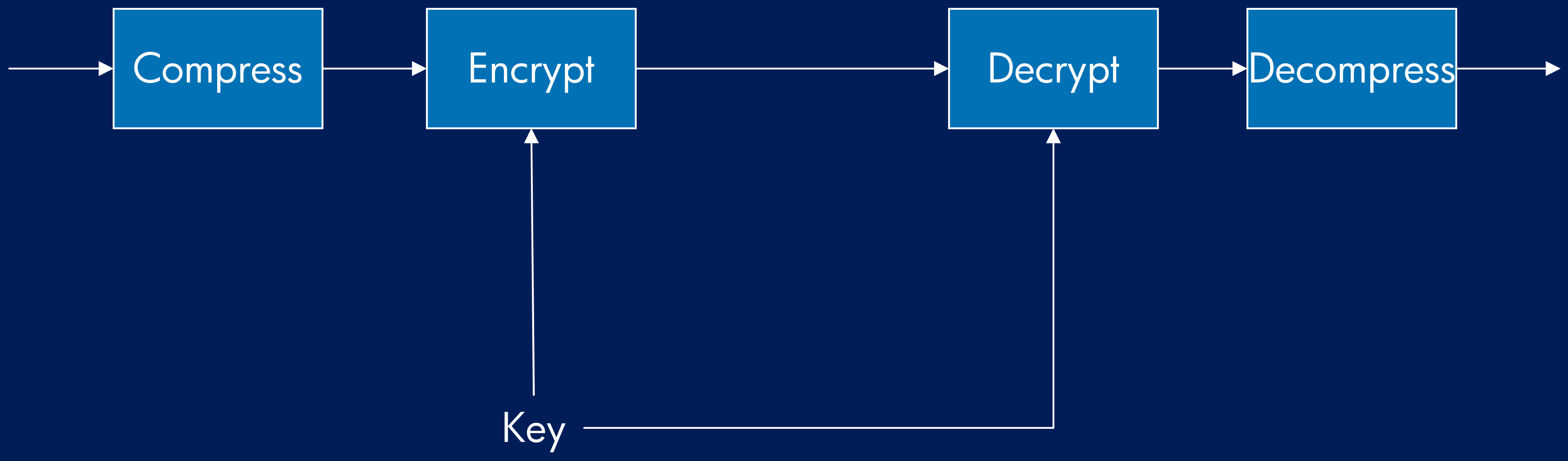
- Combine scalable coding & progressive encryption

Result:

- Secure Scalable Data

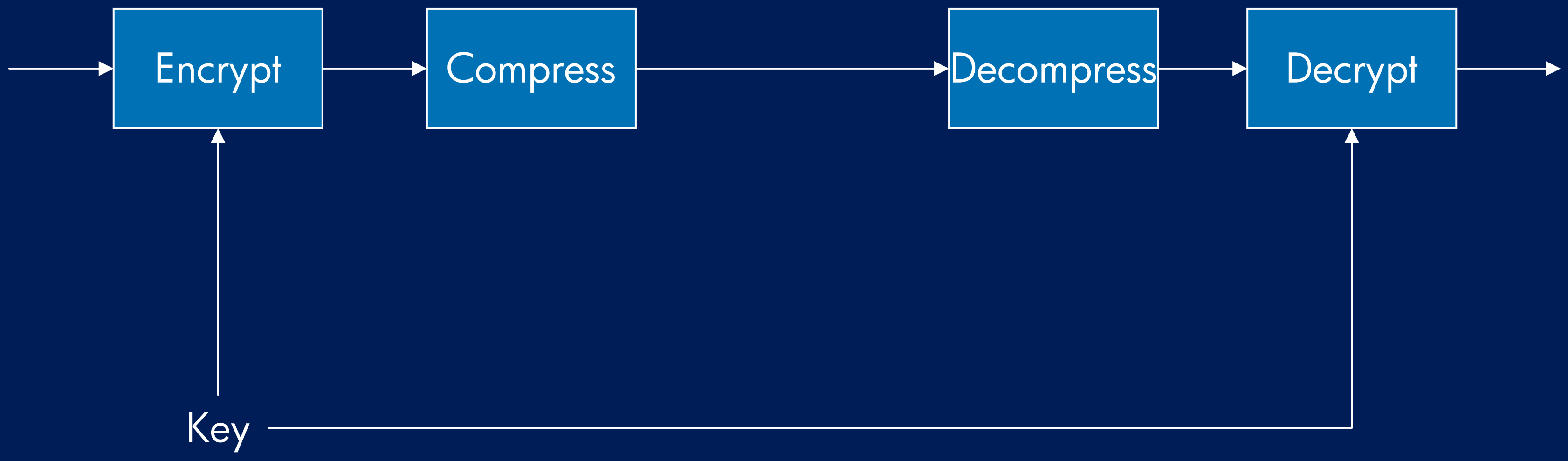
Compressing Encrypted Data

Standard Approach



(Ramchandran et al.) ©

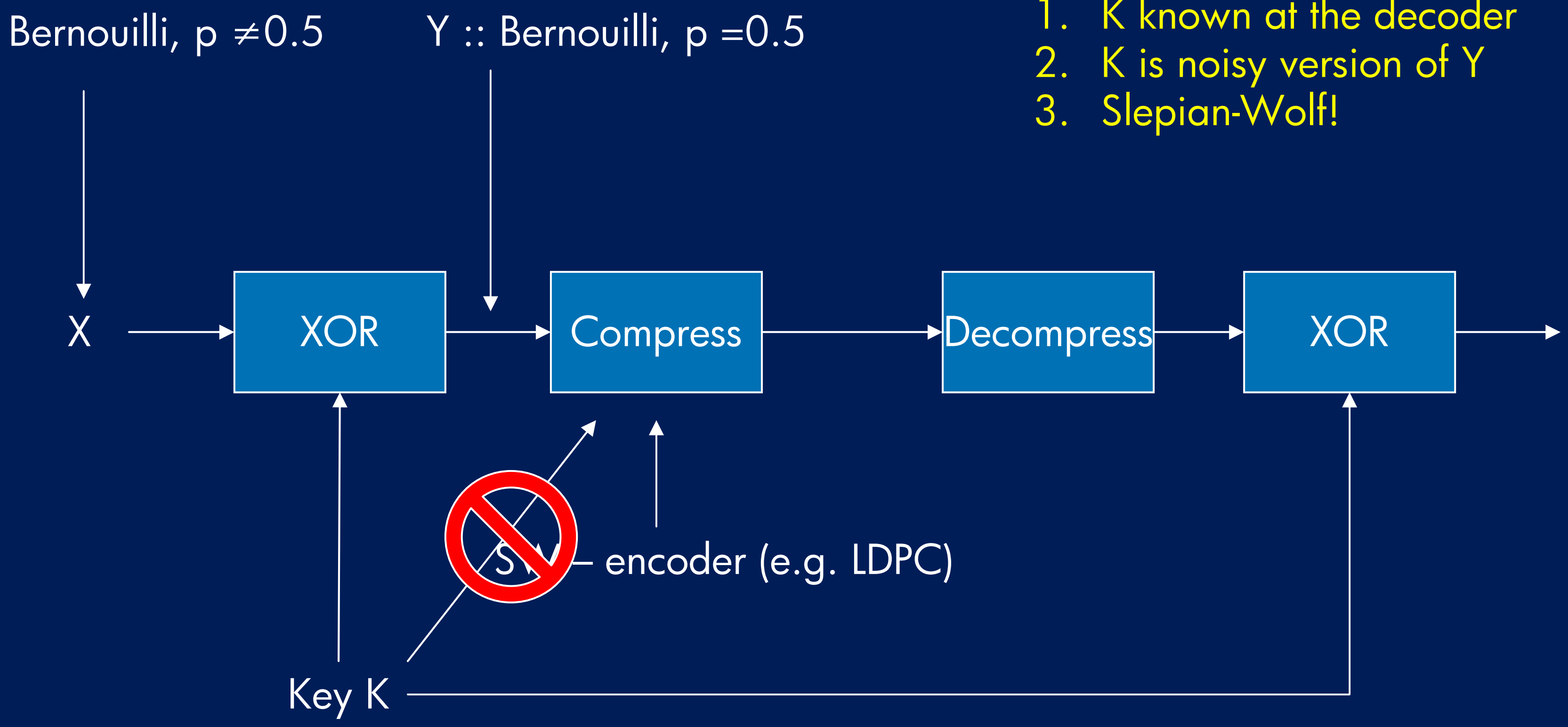
Non-Standard Approach



(Ramchandran et al.) ©

Coding with Side-Information -- Slepian-Wolf

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



(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,x) :: multiplicative structure on invertible elements of $\mathbb{Z}$ mod N

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

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

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

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

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?

$$<Y,W>^2 / <Y,Y> = (\Sigma\, w_i\, y_i)^2 \;/\; (\Sigma\, y_i\, y_i) \geq T$$

Y → E[W] Watermark Detection Circuitry (Linear Correlation) → WM Yes / WM No

Blinding of Watermark Sequence

- Known protocols require E to be component-wise
  - $E[W] = \{E[w_1], ..., E[w_n]\}$
  - 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 $R = \{r_1, ..., r_n\}$
    - R pseudo-random
    - $E[R,W] = \{E[r_1,w_1], ..., E[r_n,w_n]\}$
    - Blinding compensates for limited value set

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
    - $UZ_{10} = \{1, 3, 7, 9\}$
    - 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)

$$E[r,w] = h^r g^w \pmod{N}$$

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

Homomorphic Blinding

- The previously defined scrambling function preserves arithmetic structure

$$E[r_1,w_1] * E[r_2,w_2] = E[r_1 + r_2, w_1 + w_2]$$

$$(h^{r1}g^{w1})*(h^{r2}g^{w2}) = h^{r1+r2}\, g^{w1+w2}$$

- Algebraic consequence :

$$E[r,w]^m = E[m*r,m*w]$$

- Homomorphic property
  - addition in clear-text $\rightarrow$ multiplication in cipher-text
  - multiplication in clear-text $\rightarrow$ exponentiation in cipher-text

Correlation in the encrypted domain

Processing followed by scrambling

- $E[R,W]^{Y} =$

$$\prod E[r_i, w_i]^{y_i} =$$

$$E[\Sigma\ r_i y_i,\ \Sigma\ w_i y_i] =$$

$$E[\langle R,Y\rangle,\ \langle Y,W\rangle]$$

Scrambling followed by processing

Squared Correlation in the encrypted domain

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

$$<Y,W>^2 / <Y,Y> = (\Sigma\, w_i\, y_i)^2 \;/\; (\Sigma\, y_i\, y_i) \geq T$$

- Squared correlation needed: $<Y,W>^2 = \Sigma\, y_i\, y_j\, w_i\, w_j$
- Provide scrambled version of $W \otimes W$, i.e. $\{w_i\, w_j\}$, in stead of $W = \{w_i\}$
- Watermark detection circuit computes

$$E[R,W \otimes W]^{Y \otimes Y} = E[<R, Y \otimes Y>, <Y,W>^2] = E[S,C]$$

Y

$E[W \otimes W]$

Watermark Detection Circuitry
(Linear Correlation)

WM Yes / WM No

Hostile environment computations

- Compute normalization factor

$$A = \langle Y,Y \rangle * T$$

- Compute squared correlation

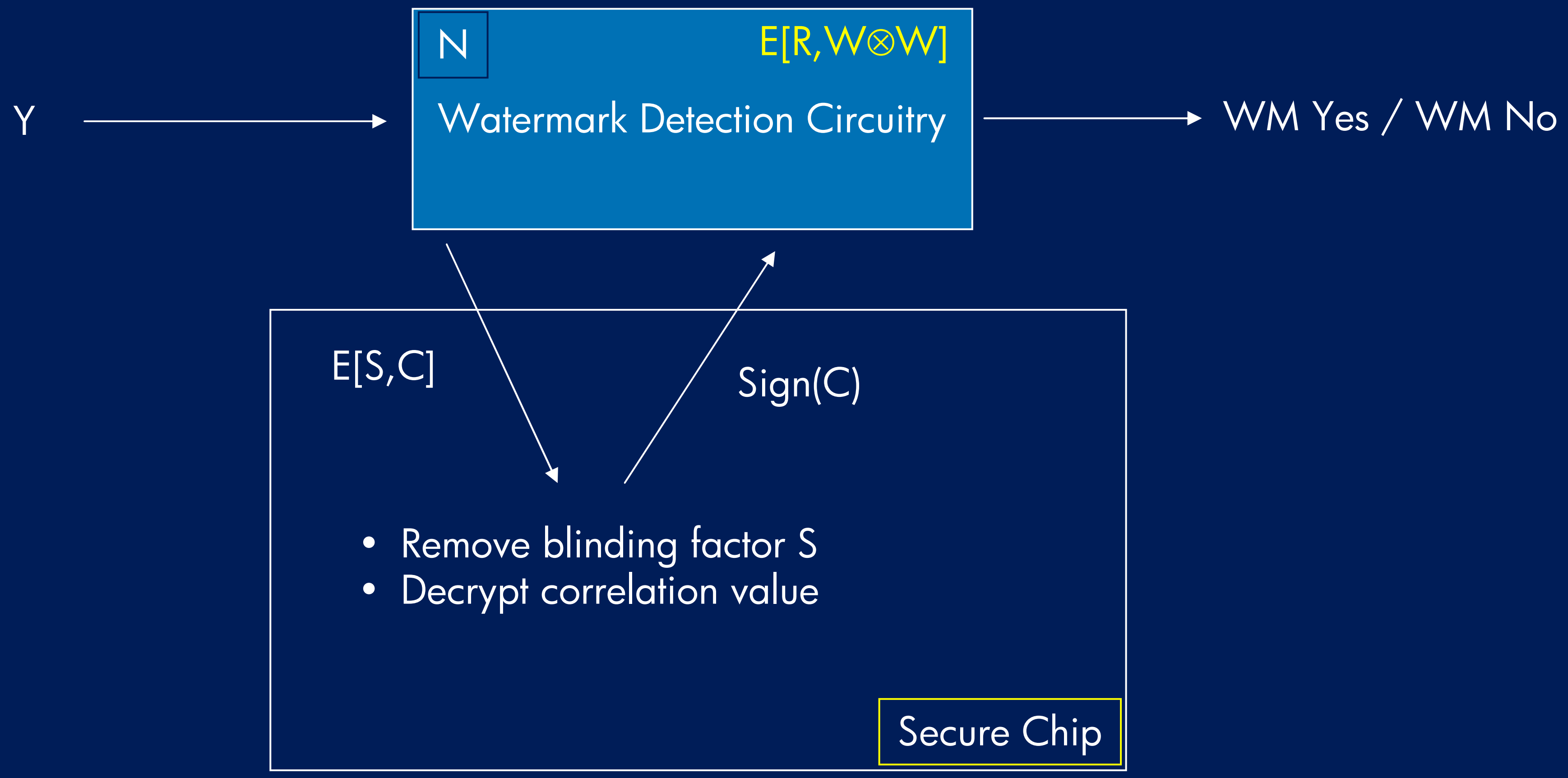
$$B = E[R, W \otimes W]^{Y \otimes Y} = E[\langle R, Y \otimes Y \rangle, \langle Y,W \rangle^2]$$

- 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



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

$$E[r,x] = h^r g^x$$

- Blinding factor removal

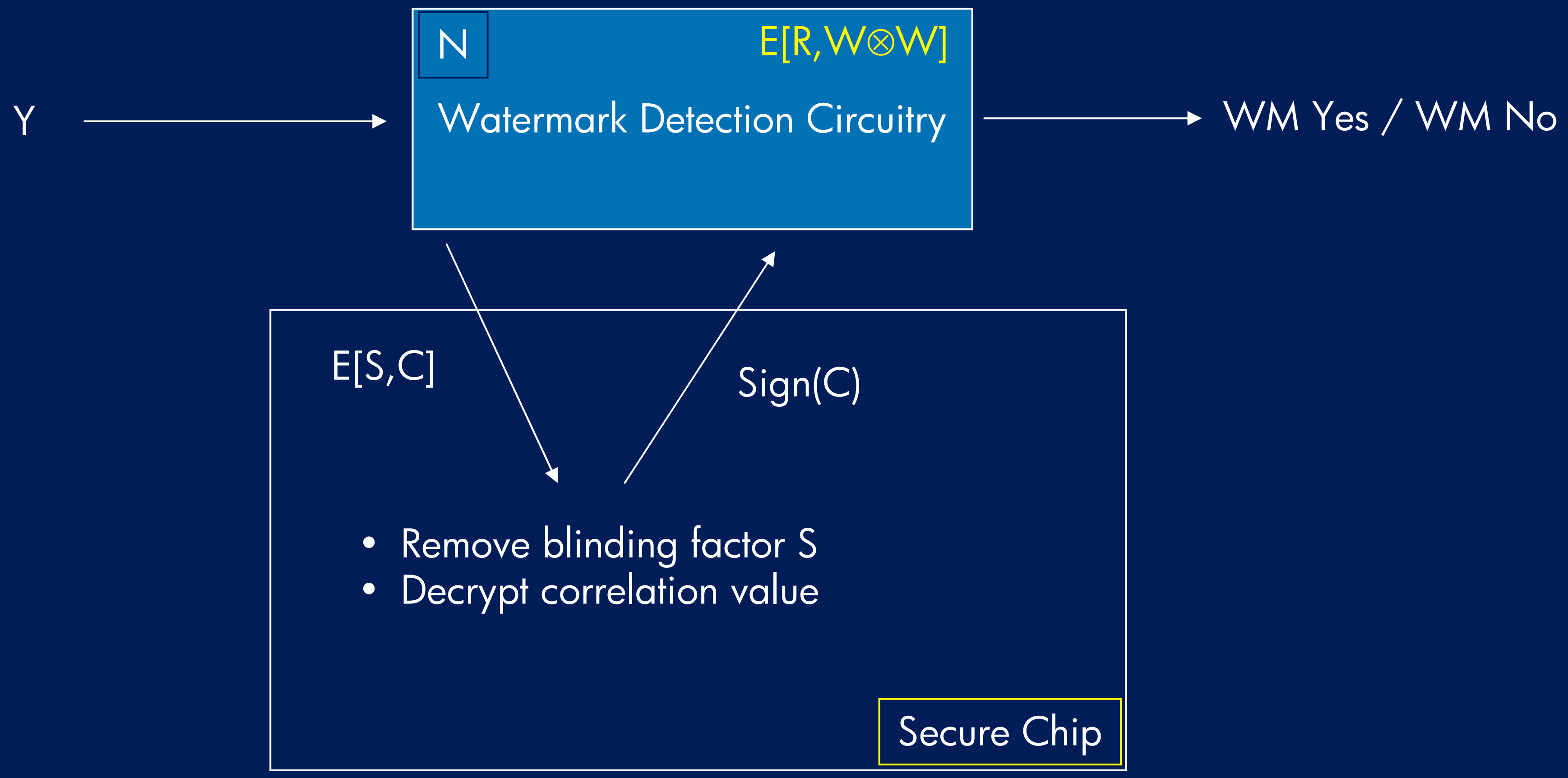
$$(h^r g^x)^M = g^{xM}$$

- Special g makes Discrete Logarithmic problem easy

$$g^{xM} \rightarrow x$$

Secure Assistance

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



Summary

- Secure Media processing
- Three examples
  - Exposing data structures
  - Exploiting distributed knowledge
  - Structure preserving encryption
- Looking ahead
  - More relevant problems?
  - More approaches?