Privacy-preserving methods: multimedia and biometrics perspectives

S. Voloshynovskiy

http://sip.unige.ch/education/multimedia-security/

Lecture Outline

- Introduction: privacy and security in biometrics and multimedia
- Cryptographic approach
- Signal processing approach
- Hybrid approach

Information security

- Personal Identier Number (PIN): to control access to service, systems and information

- Subscriber Identity Module (SIM): access to mobile phones, to protect against illegal use of network

- Secure Socket Layer (SSL): to prevent eavesdropping on information exchanged between two terminals

Traditional cryptography

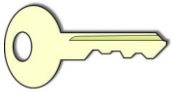
Cryptography: develops tools for protecting information and establishing secure interactions.

- Encryption: provides confidentially of information
- Authentication: verifies the identity

Note: The algorithms are public, therefore, the security of the schemes depends on the secrecy of a key owned by the legitimate parties.

Practical cryptography issues in our modern society:

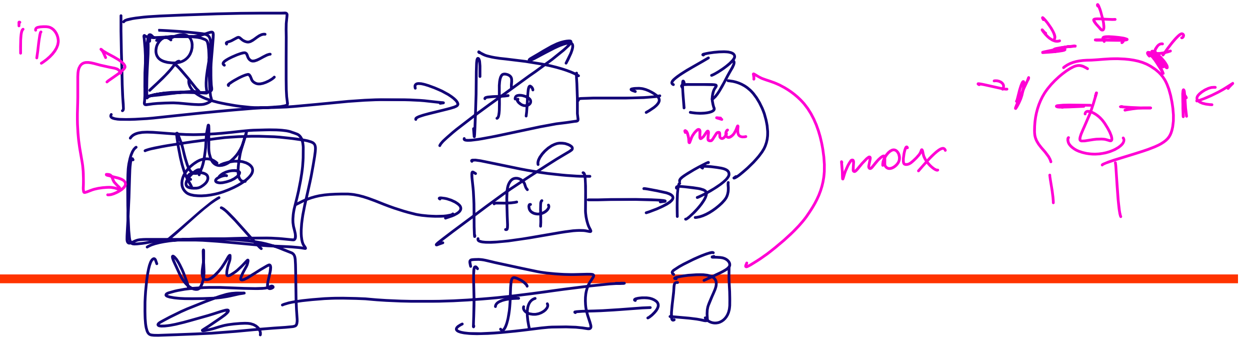
1 Key generation and distribution



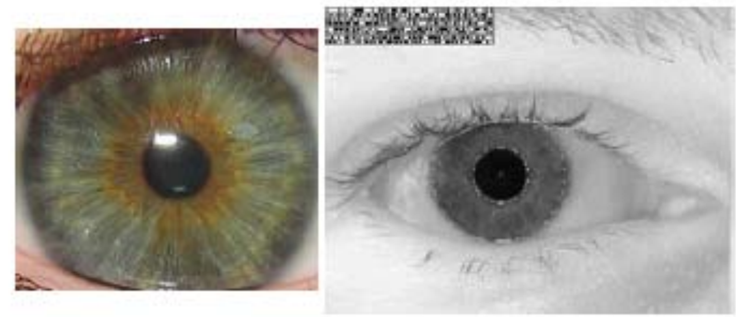
2 Safely storage: (mobile phones, bank tokens, smart cards, : : :)

3 Noisy observation: authentication based on something closely linked to physiological characters

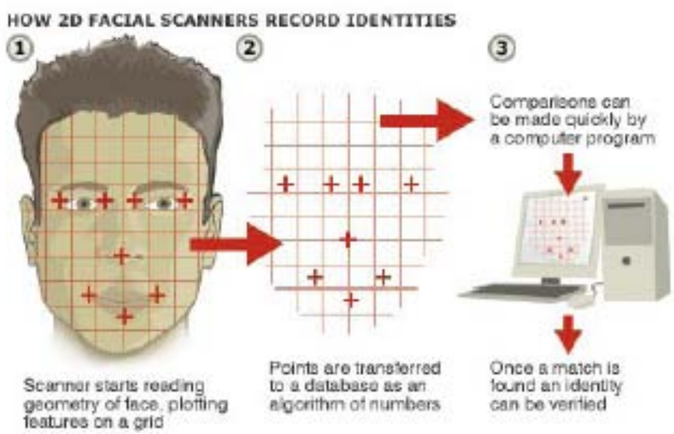
Biometrics



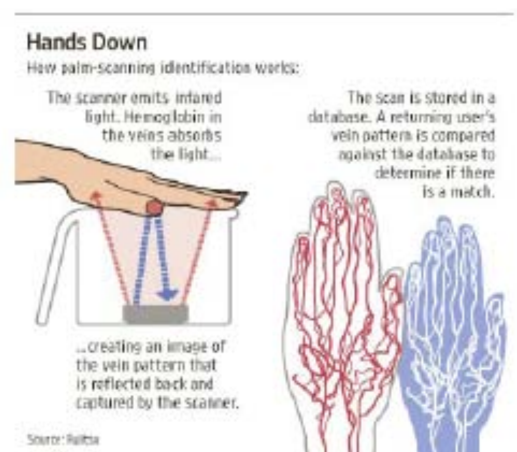
Fingerprint



Iris



Facial



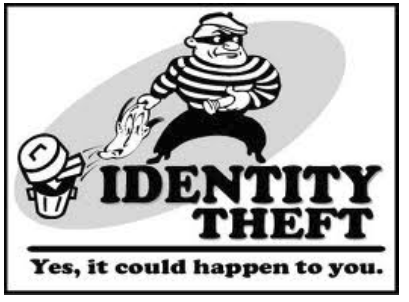
Palm vein

Biometrics: why to be protected?

A biometric template is a representation of a unique characteristic of an individual. It might also contain some information about diseases. Therefore, it contains privacy-sensitive information.

To abuse database:

- impersonation
- identity theft
- cross-database matching
- detectable pathologies
- … yet undiscovered attacks

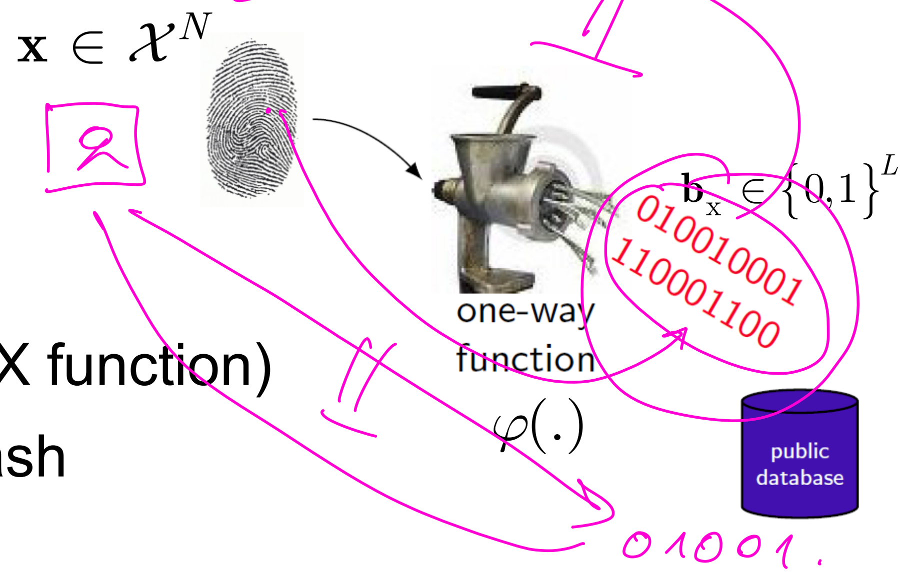


Note: biometric templates can not be "cancelable" because people have only ten fingers, two eyes, etc.

15:10.

Mutimedia security: cryptographic solution

- Main idea:
  - do not store date itself
  - store a one-way hash (non-invertible function like UNIX function)
  - for the same data, the same hash



Remark: the hash $\varphi(.)$ is assumed to be uninformative $\Rightarrow$ non-invertible.

(which is not true in information-theoretic sense).

$$\underbrace{I\left(X; h\left(X\right)\right) = 0}$$

This is not true, since $h(X)$ is a function of X!

B_x

$b_x = h(x)$

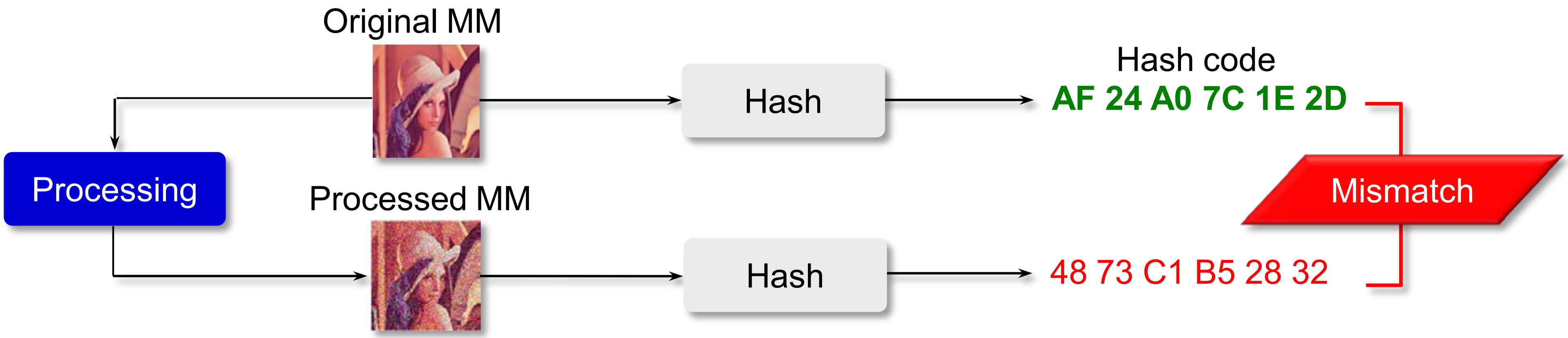
X Y

$I(x;y) = 0$ $I(x;y) > 0$

Mutimedia security: cryptographic solution

Why are traditional security tools not suitable for multimedia?

- Traditional *security*:
  - Cryptographic encryption (confidentiality of information)
  - Cryptographic hashes (authentication, trust, access control)
- Main concerns of classical crypto-based algorithms:
  - Sensitivity to noise and unintentional distortions in input data
  - Data handling in the encrypted domain



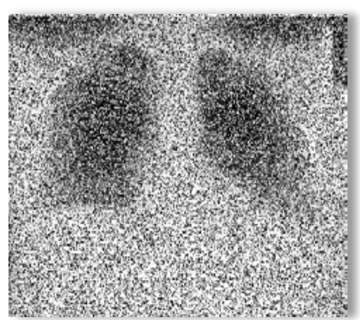
Mutimedia privacy: data «degradation»

Why are traditional privacy tools not suitable for multimedia?

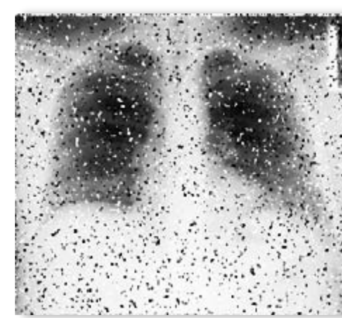
- Traditional *privacy protection* [1]:
  - Data owner (protect data): based on data degradation and randomization (noise addition, lossy compression, data removal, dim. reduction…)
  - Data user (protect requests): based on anonymization, randomized rules
- Main concerns of classical privacy preserving algorithms:
  - Reduction of accuracy (data utility)
  - Not very efficient against experienced attackers (sensitivity analysis)

Original

50% removed based on key



Median 9x9



Adaptive recovery

[1] C. Aggarwal and P. Yu, Privacy-Preserving Data Mining: Models and Algorithms, Spinger, 2008.

DINOv2.
SSL.

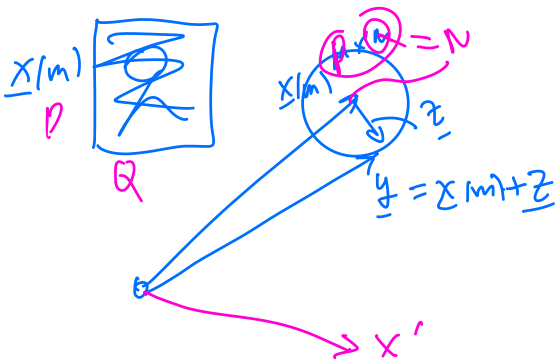
Signal processing approach: authentication

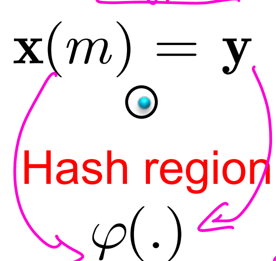
- Use hypothesis testing
- Handle noisy data $\Rightarrow$ extended decision region

$$\begin{cases} H_0 : \mathbf{y} = \mathbf{x}' + \mathbf{z}, \\ H_1 : \mathbf{y} = \mathbf{x}(m) + \mathbf{z}, \end{cases}$$

$$\mathbf{x}' \neq \mathbf{x}(m), \text{any } 1 \leq m \leq |\mathcal{M}|$$

8 Mio



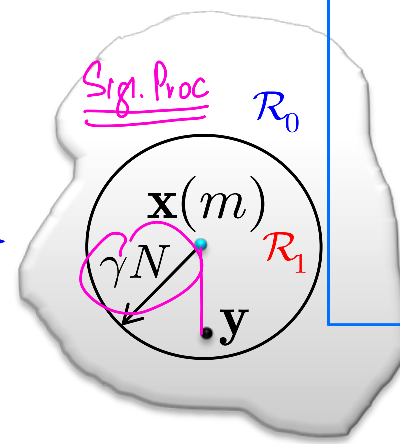


$\| x(m) - y \|_2^2 = 0$

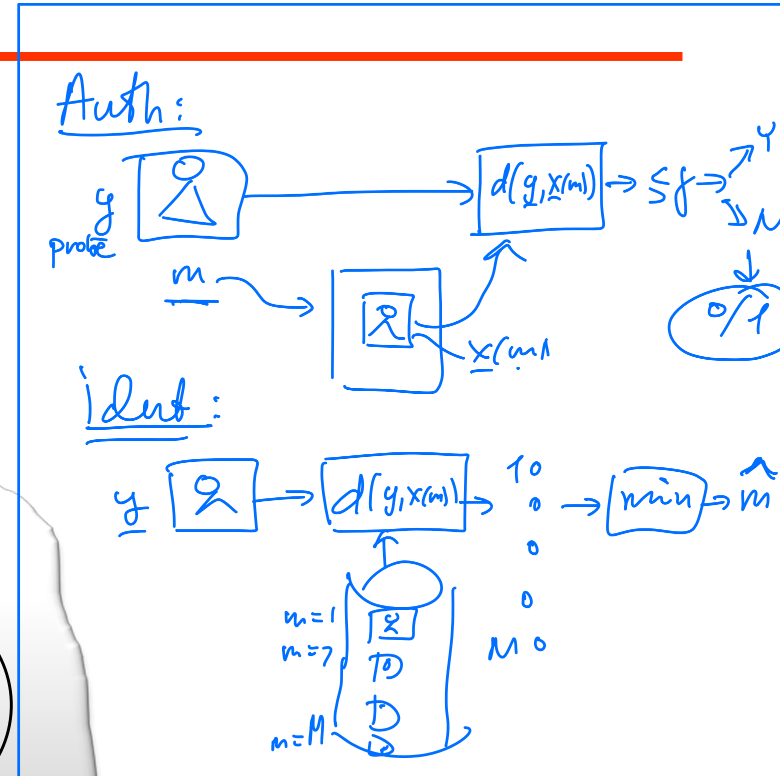
$\| \varphi(x(m)) - \varphi(y) \|_2^2 = 0$

$\neq$

$\Rightarrow$



Decision region



Gaussian assumption $\Rightarrow$ Euclidian distance $\equiv$ Sphere region

$$\mathcal{R}_1 : d^E\left(\mathbf{y}, \mathbf{x}(m)\right) = \left\|\mathbf{y} - \mathbf{x}(m)\right\|^2 \leq \gamma N \quad \Rightarrow \quad \mathcal{R}_1 : \mathbf{y}^T \mathbf{x}(m) \geq \gamma' N$$

$(a-b)^2 = a^2 - 2ab + b^2$

$\|y\|_2^2 - 2 y^T x(m) + \|x\|_2^2$

Signal processing approach: authentication

$$\color{red}{\mathcal{R}_1} : \boxed{\mathbf{y}^T \mathbf{x}(m)} \geq \gamma' N$$

x'

H_0: $\underline{x}^T \underline{x}(m)$, y^T

H_1: $x^T(m)\, \underline{x}(m) = \|\underline{x}(m)\|_2^2$

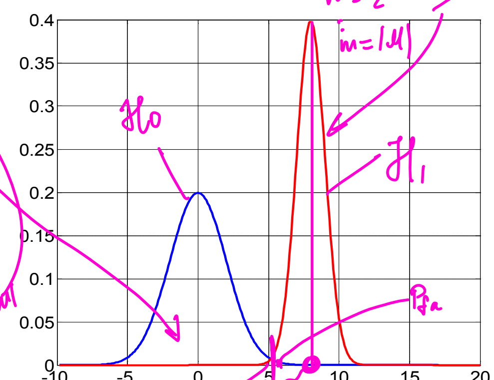
$(x^T(m)+z)\,\underline{x}(m)$

$= x^T(m)\,\underline{x}(m) + z^T \underline{x}(m)$

$\|x(m)\|_2^2$

m=1, m=2, m=|M|

z



H_0, H_1, P_{fa}, P_m

γ'

Bayes → P_e

N-P, fix P_{fa} → P_m.

$$\rho = \frac{\mathbf{y}^T \mathbf{x}(m)}{N}$$

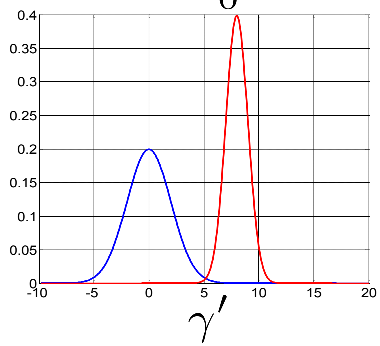
$$P_f = \Pr\left[\mathbf{y}^T \mathbf{x}(m) \geq \gamma' N \,\middle|\, H_0\right] - \text{probability of false accaptance}$$

$$P_m = \Pr\left[\mathbf{y}^T \mathbf{x}(m) < \gamma' N \,\middle|\, H_1\right] - \text{ probability of miss}$$

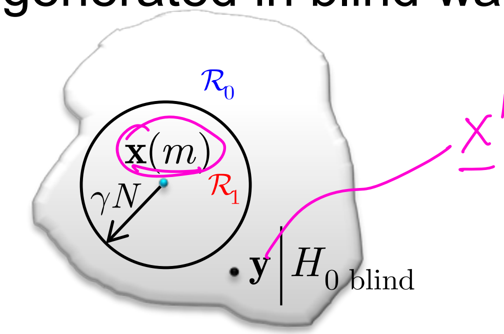
Signal processing approach: authentication

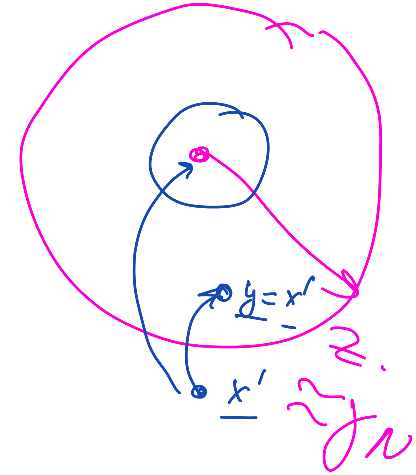
Blind attacks

- $\mathbf{x}'$ under H_0 was assumed to be generated in blind way



$$\rho = \frac{\mathbf{y}^T\mathbf{x}(m)}{N}$$



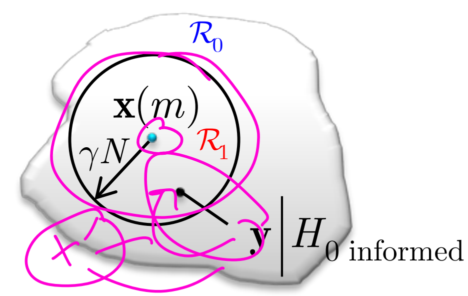


Informed attacks

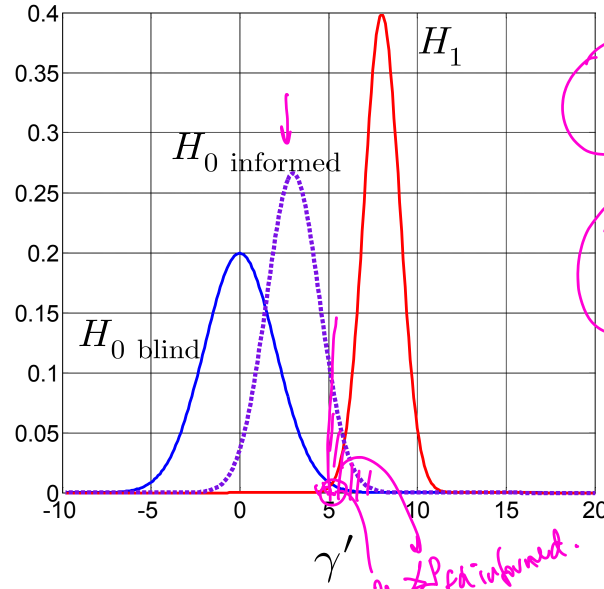
- Attacker can generate $\mathbf{x}'$ as close as possible to $\mathbf{x}(m)$, if it is disclosed!

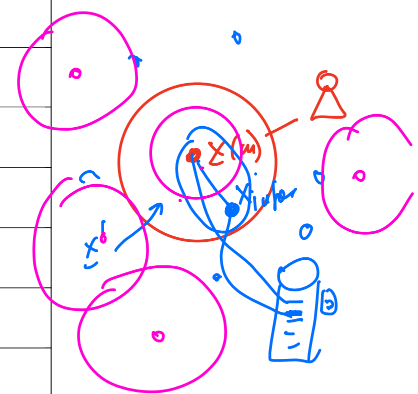
$$P_f = \Pr\left[\mathbf{y}^T\mathbf{x}(m) \geq \gamma' N \,\middle|\, H_0 \text{ blind}\right]$$

$$P_{sa} = \Pr\left[\mathbf{y}^T\mathbf{x}(m) \geq \gamma' N \,\middle|\, H_0 \text{ informed}\right] - \text{prob. of succ. attack}$$



Signal processing approach: authentication





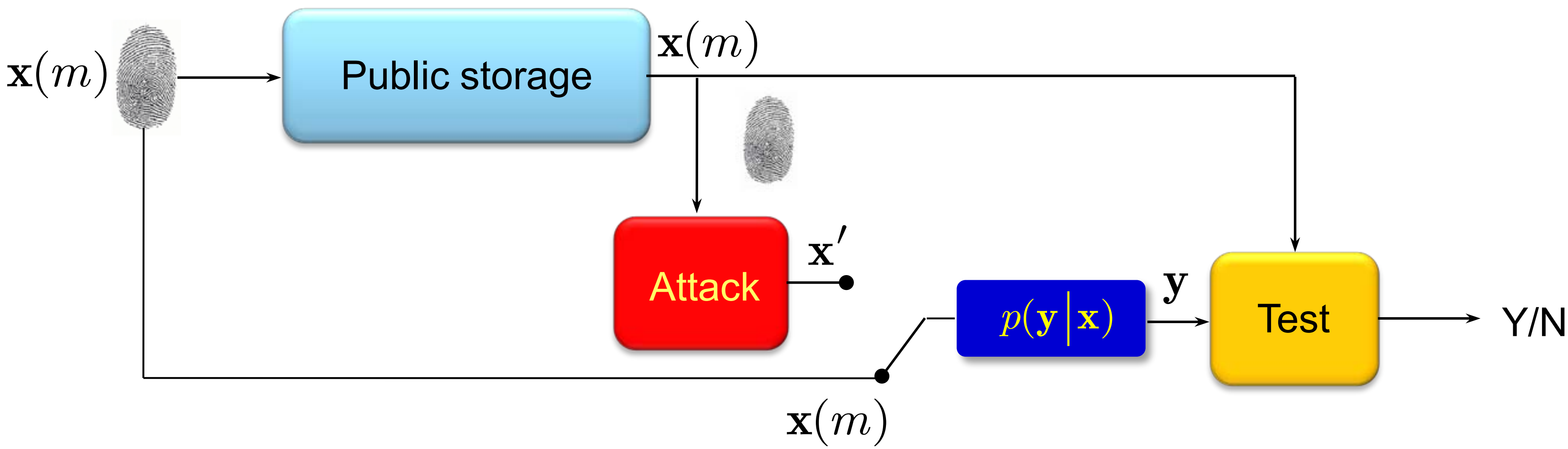
$$\rho = \frac{\mathbf{y}^T \mathbf{x}(m)}{N}$$

$$\boxed{P_{sa} \geq P_f}$$

Conclusion:

- the disclosure of $\mathbf{x}(m)$ is dangerous for the performance (security).

Signal processing approach: authentication



Open issues:

- $\mathbf{x}(m)$ is stored in the public domain
- no security
- no privacy

$\left.\begin{array}{l}\text{no security}\\ \text{no privacy}\end{array}\right\}$ $\mathbf{x}(m)$ can be used for various attacks

Signal processing approach: identification

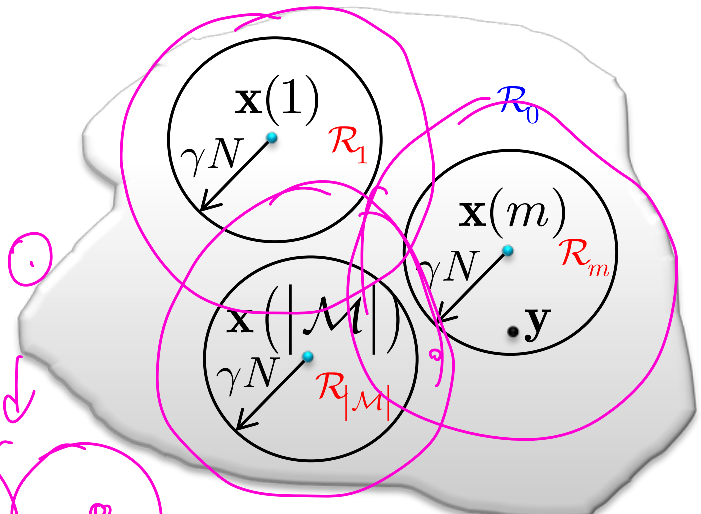
- M-ary hypothesis testing

$$
\begin{cases}
H_0 : \mathbf{y} = \mathbf{x}' + \mathbf{z}, \\
H_1 : \mathbf{y} = \mathbf{x}(1) + \mathbf{z}, \\
\vdots \\
H_{|\mathcal{M}|} : \mathbf{y} = \mathbf{x}\left(|\mathcal{M}|\right) + \mathbf{z},
\end{cases}
$$

$$\mathbf{x}' \neq \mathbf{x}(m), \text{any } 1 \leq m \leq |\mathcal{M}|$$

a

b $|\mathcal{M}|$



$$\hat{m} = \underset{1\leq m\leq|\mathcal{M}|}{\arg\min}\left(\left\|\mathbf{y}-\mathbf{x}(m)\right\|^2 \leq \gamma N\right)$$

$\to \hat{m}$

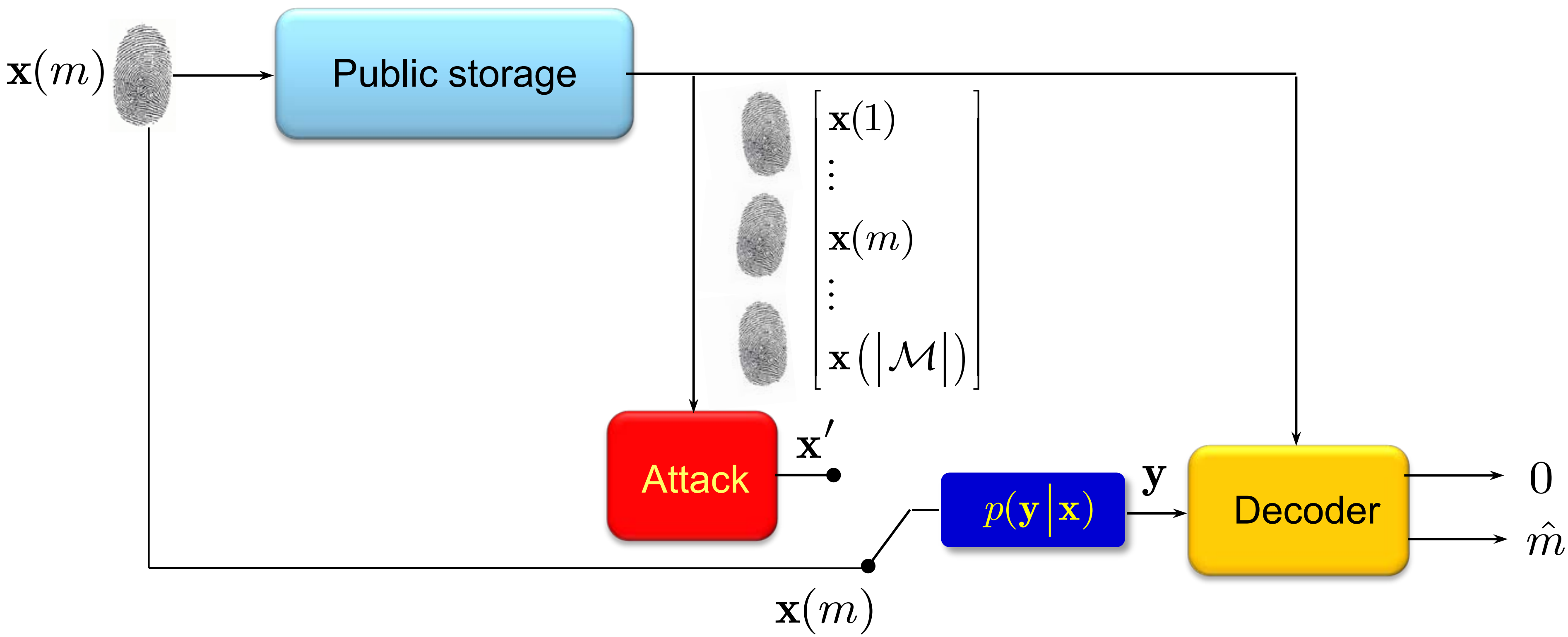
$\to \emptyset$

$$P_f = \Pr\left[\bigcup_{m=1}^{|\mathcal{M}|} \mathbf{y}^T\mathbf{x}(m) \geq \gamma' N \,\middle|\, H_{0\,\text{blind}}\right]$$

$$P_{sa} = \Pr\left[\bigcup_{m=1}^{|\mathcal{M}|} \mathbf{y}^T\mathbf{x}(m) \geq \gamma' N \,\middle|\, H_{0\,\text{informed}}\right]$$

$$P_{ic} = \Pr\left[\underbrace{\mathbf{y}^T\mathbf{x}(m) < \gamma' N}_{\text{miss}} \bigcup \underbrace{\bigcup_{m'\neq m}^{|\mathcal{M}|} \mathbf{y}^T\mathbf{x}(m') \geq \gamma' N}_{\text{missaccaptance}} \,\middle|\, H_m\right]$$

Signal processing approach: identification



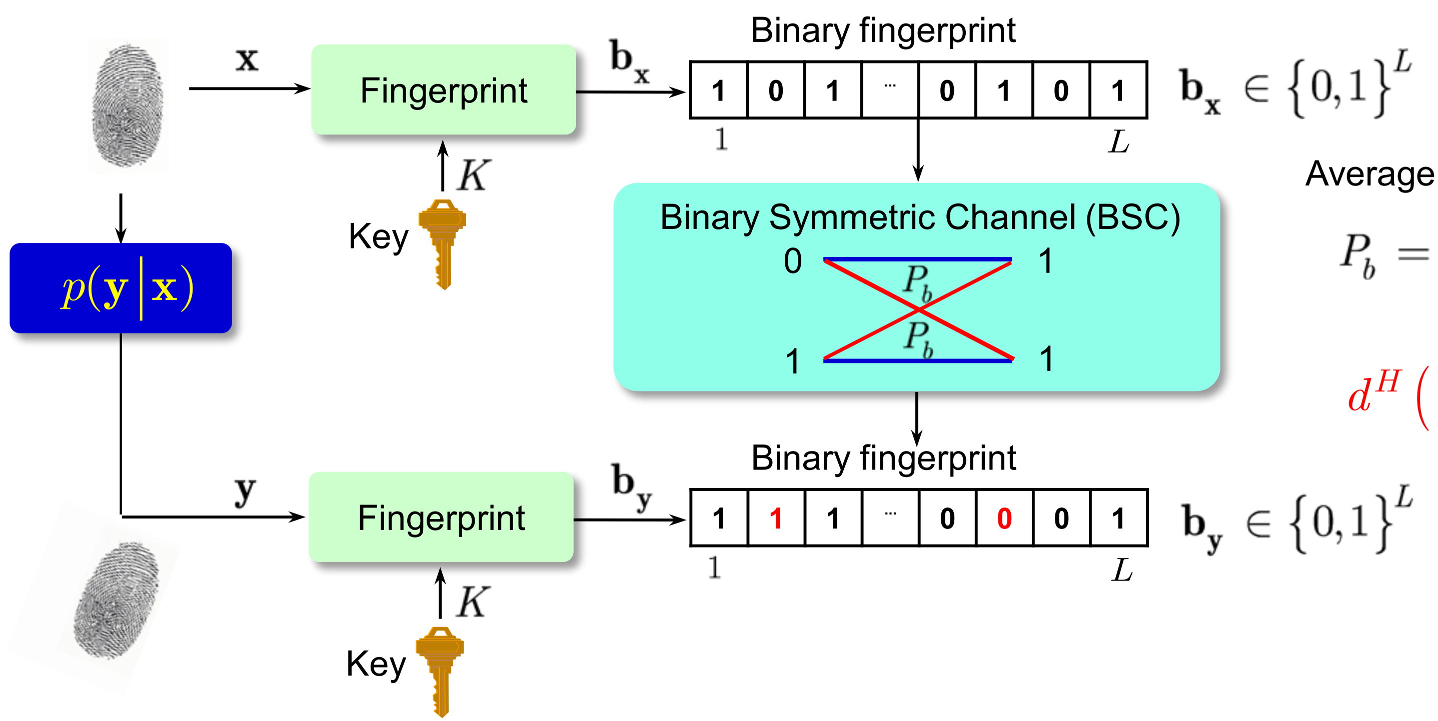
Open issues:

- all $\{\mathbf{x}(m)\}$ are stored in the public domain
- no security
- no privacy

$\left.\right\}$ $\mathbf{x}(m)$ can be used for various attacks

Signal processing approach: towards «robust hashing»

- If $\mathbf{x}(m)$ is open, the attacker can: (a) deduce privacy and (b) design attacks
- Robust hashing: an attempt to mimic crypto hashing but stay robust to signal processing (blur, noise, lossy compression, etc.) and geometric (affine, projective) distortions.



Average probability of bit error

$$P_b = \frac{1}{L}\sum_{i=1}^{L} \Pr\left[b_{x_i} \neq b_{y_i}\right]$$

$$d^H\left(\mathbf{b}_\mathbf{x}(m), \mathbf{b}_\mathbf{y}\right) \le \alpha L$$

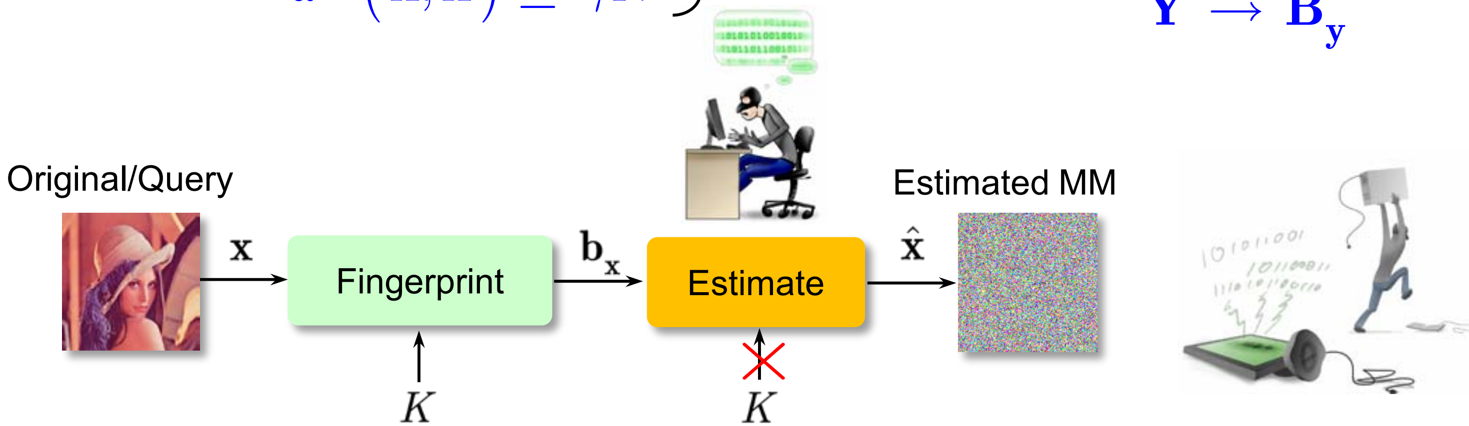
Signal processing approach: towards «robust hashing»

- Main assumptions:
  - Robust hashing is robust to some minor modifications
  - Robust hashing is non-invertible under
    - (a) unknown key
    - (b) known key

      such that $d^E\left(\mathbf{x}, \hat{\mathbf{x}}\right) \geq \gamma N$

This is possible due to loss of information

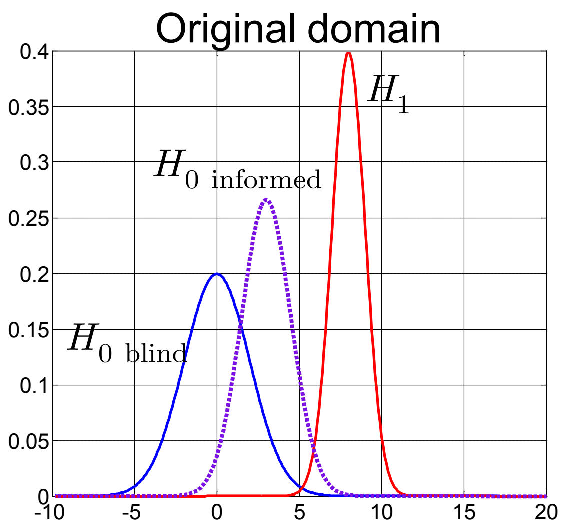
$$\mathbf{X} \rightarrow \mathbf{B}_\mathbf{x}$$
$$\mathbf{Y} \rightarrow \mathbf{B}_\mathbf{y}$$



Remark: authentication/identification based on $\left(\mathbf{B}_\mathbf{x}, \mathbf{B}_\mathbf{y}\right)$ is less accurate than based on $\left(\mathbf{X}, \mathbf{Y}\right)$

Signal processing approach: towards «robust hashing»

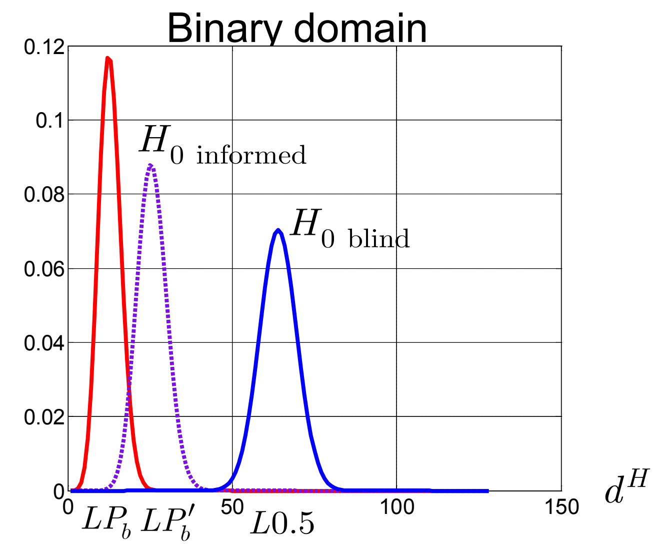
- Impact of reduction of dimensionality and binarization:
  - FP: $\mathcal{R}^N \times \mathcal{K} \rightarrow \{0,1\}^L$



$$\rho = \frac{\mathbf{y}^T \mathbf{x}(m)}{N}$$

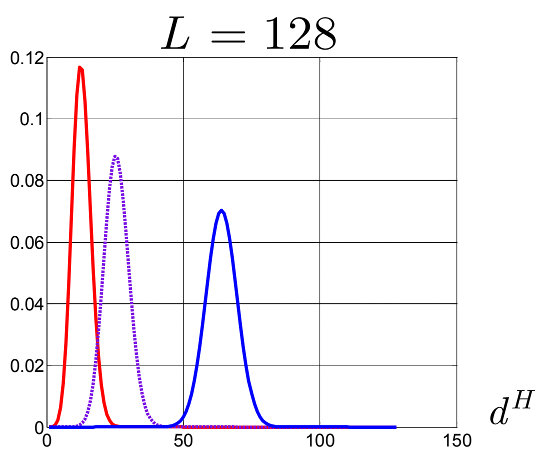
Fingerprinting

Loss of information

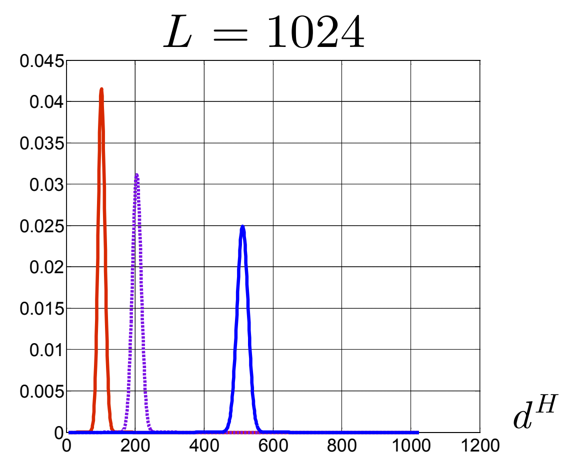


Hybrid solution

- Application of non-invertible transformations leads to the loss in performance
- One can compensate it by selecting longer L



Increase L $\Longrightarrow$



- In turn, longer L leads to better chances for image reconstruction!
- Problem: can one trade-off security/privacy – performance?

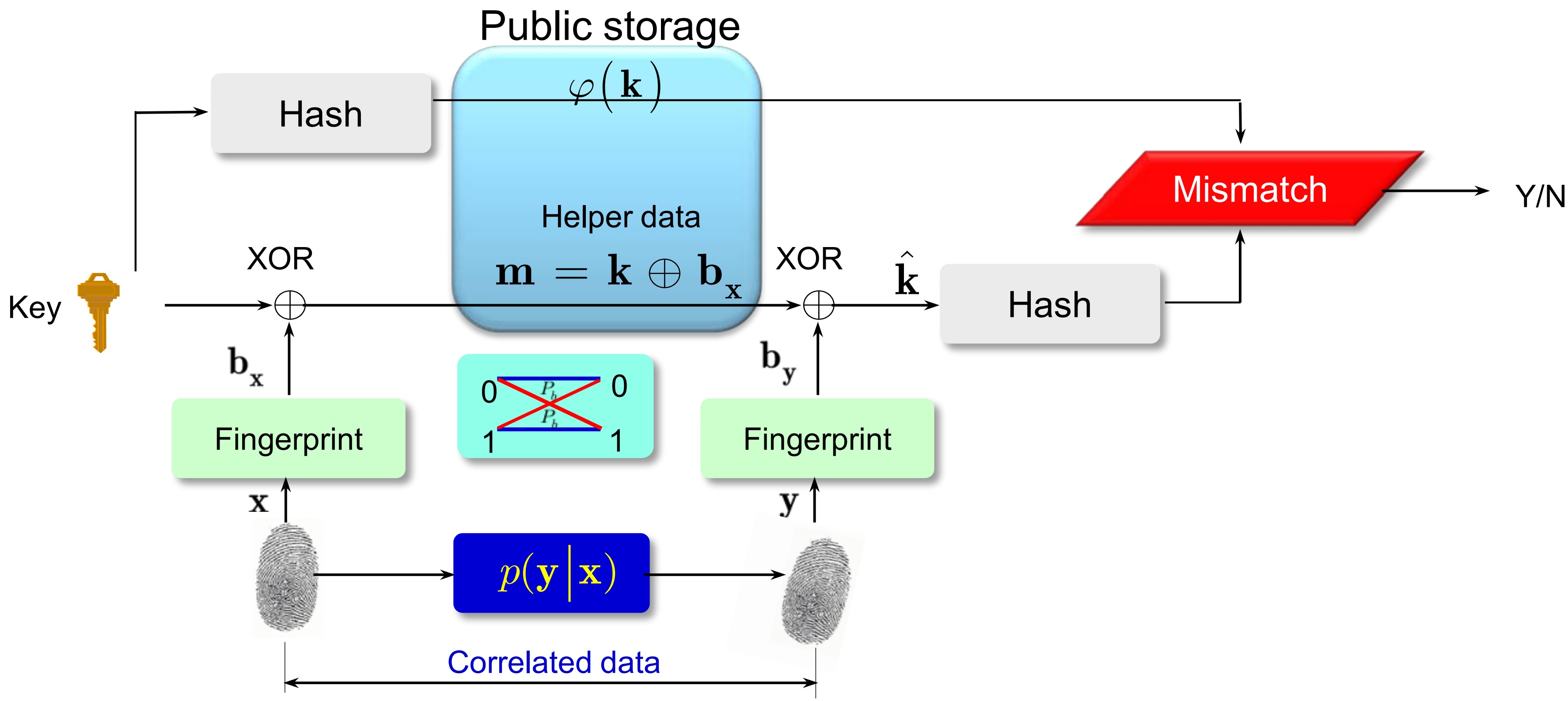
$\Rightarrow$ Solution: crypto + signal processing + coding

Hybrid solution: strategies

- Several methods (based on common idea):
  - fuzzy commitment
  - helper data

- Main strategy:
  - use additional helper data to correct errors
  - use a fact that $\mathbf{X}$ and $\mathbf{Y}$ are correlated as well as $\mathbf{B_x}$ and $\mathbf{B_y}$ for the hypothesis H_1 in authentication and the hypothesis H_m in identification

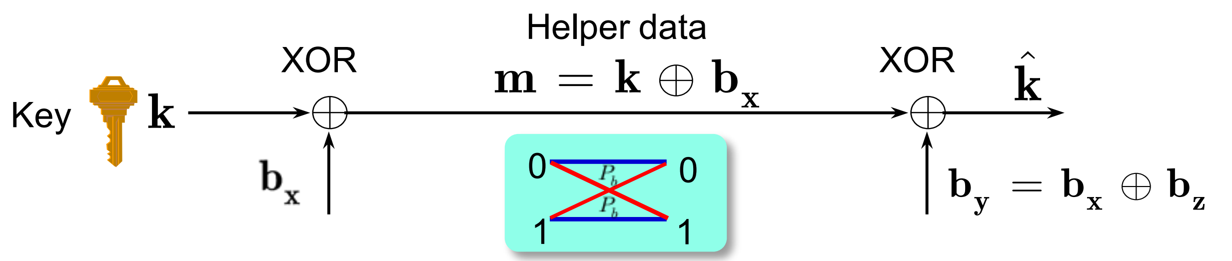
Hybrid solution: fuzzy commitment



- Idea:
  - $\mathbf{k}$ is used for every new session (i.i.d.) while $\mathbf{b_x}$ remains the same (non-renewable)
  - $\mathbf{b_x}$ is used to lock the key (even, if it is not i.i.d.) $\Rightarrow$ analog of one-time-pad

Hybrid solution: fuzzy commitment

- Open issues:

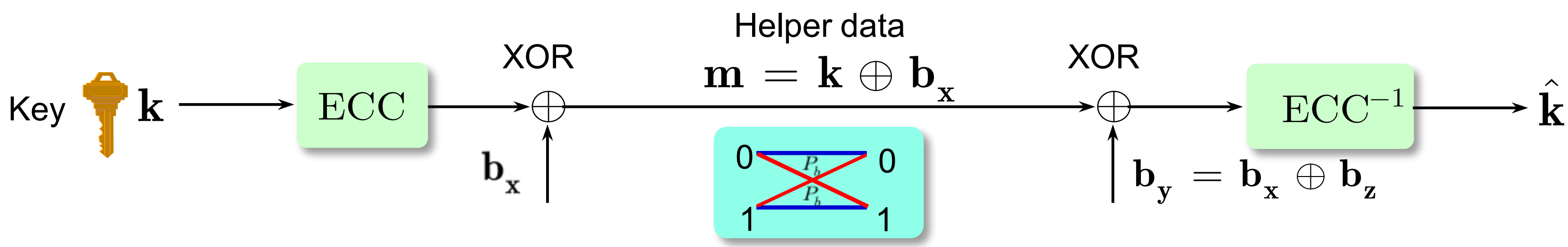


- In general case,
  - $\mathbf{b}_x \neq \mathbf{b}_y \quad \Rightarrow \quad$ residual error

$$\hat{\mathbf{k}} = \mathbf{k} \oplus \underbrace{\mathbf{b}_x \oplus \mathbf{b}_y}_{\mathbf{b}_z} = \mathbf{k} \oplus \mathbf{b}_z \Rightarrow \varphi(\mathbf{k}) \neq \varphi(\hat{\mathbf{k}})$$

- Idea:
  - add redundancy to $\mathbf{k}$ using error correction code to correct errors
  - redundancy is proportional to $\approx LH_2(P_b)$

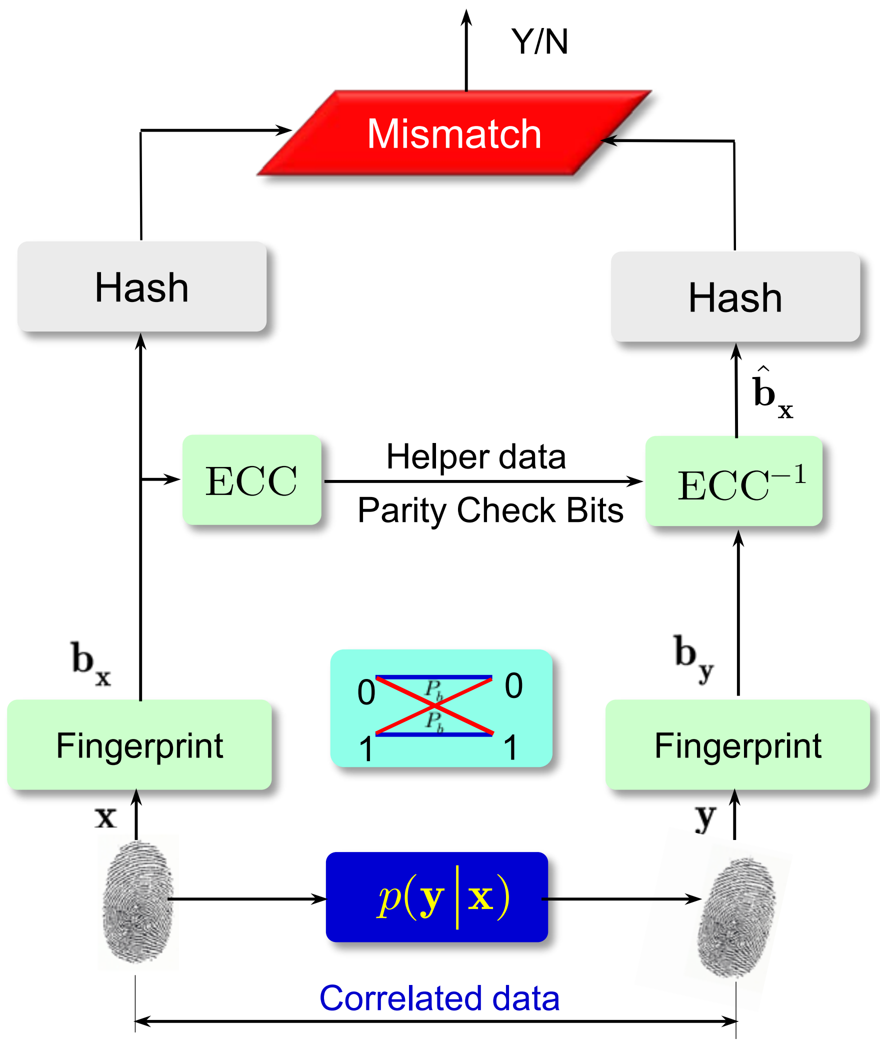
Hybrid solution: fuzzy commitment



- ECC^{-1} decoder corrects errors in $\mathbf{k} \oplus \mathbf{b_z}$
- Open issues:
  - $\mathrm{ECC}(\mathbf{k})$ is not anymore i.i.d.

    $\Rightarrow$ smaller entropy: easier to predict and attack
  - In addition $\mathbf{b_x}$ is not i.i.d., the attacks are possible against both!

Hybrid solution: helper data based systems



- Open issues:
  - redundancy is proportional to $\approx LH_2(P_b)$
  - However, these methods represent the state-of-the-art!
  - It is up to you to find something better.