Biometric Security

BIRS-09

Ton Kalker

An interpretation of work by: Tanya Ignatenko (TUE),
Frans Willems (TUE)

First slide

- Topic:
  - new direction in secure biometry
  - Interesting mixture of signal processing, cryptography and information theory

- Overview
  - Biometry: strength and weaknesses
  - Cancelable biometrics
  - Secrets from common randomness
  - Biometric encryption
  - Fuzzy commitment
  - Optimal biometric encryption
  - Open questions

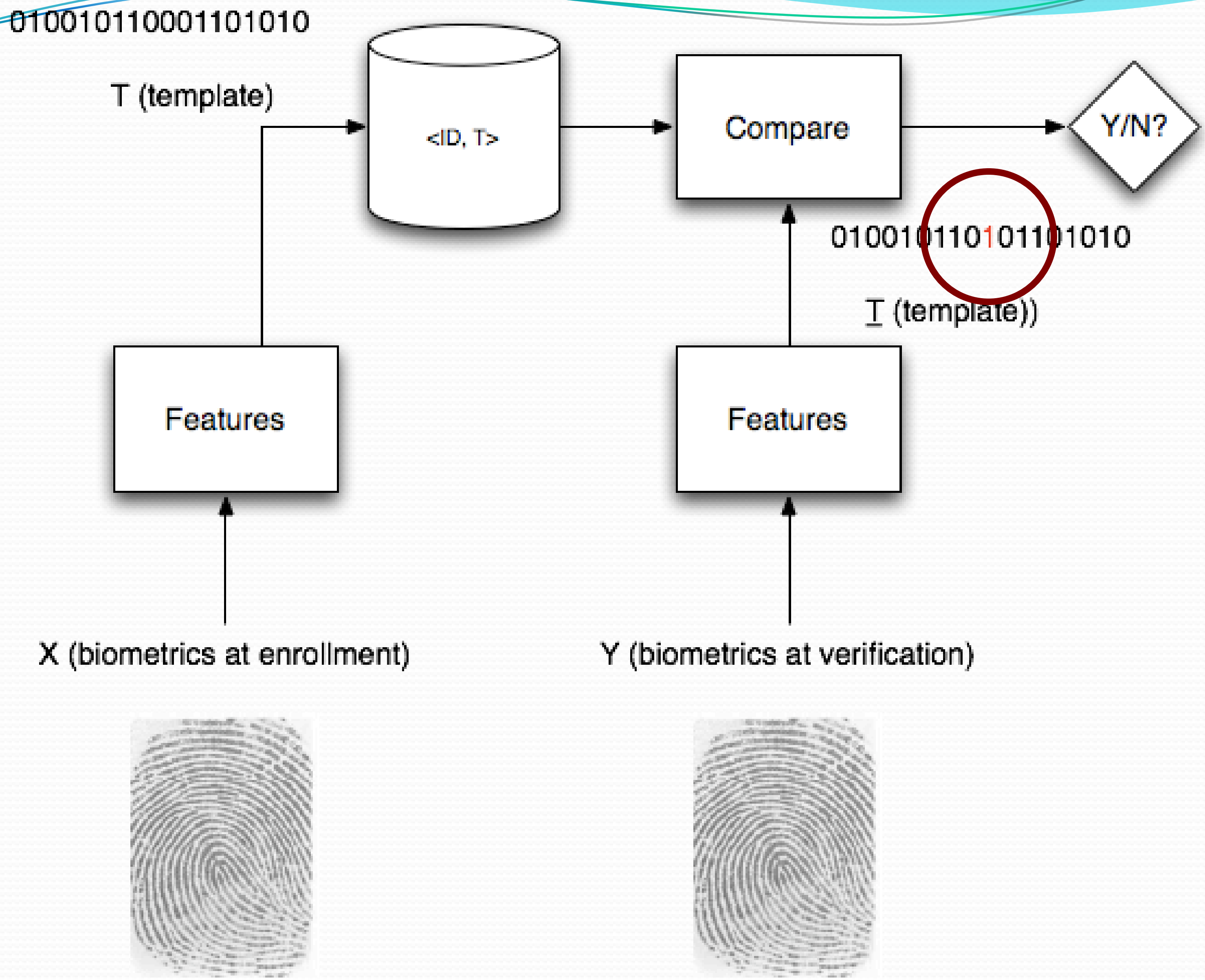
Biometry

- Authorization
  - Passwords: what you know
  - Biometry: who you are
- Interaction
  - Touch interfaces
    - Finger recognition
  - Personalization
    - Face recognition

Authorization by password

- Control mechanism
  - Database (DB) of (username, **hash**(password)) pairs
- PRO
  - DB entries do not leak PW
  - DB entries can be modified
- CON
  - PWs are hard to remember

Ignatenko, 2009


010010110001101010
T (template)
<ID, T>
Compare
Y/N?
010010110101101010
T (template))
Features
Features
X (biometrics at enrollment)
Y (biometrics at verification)

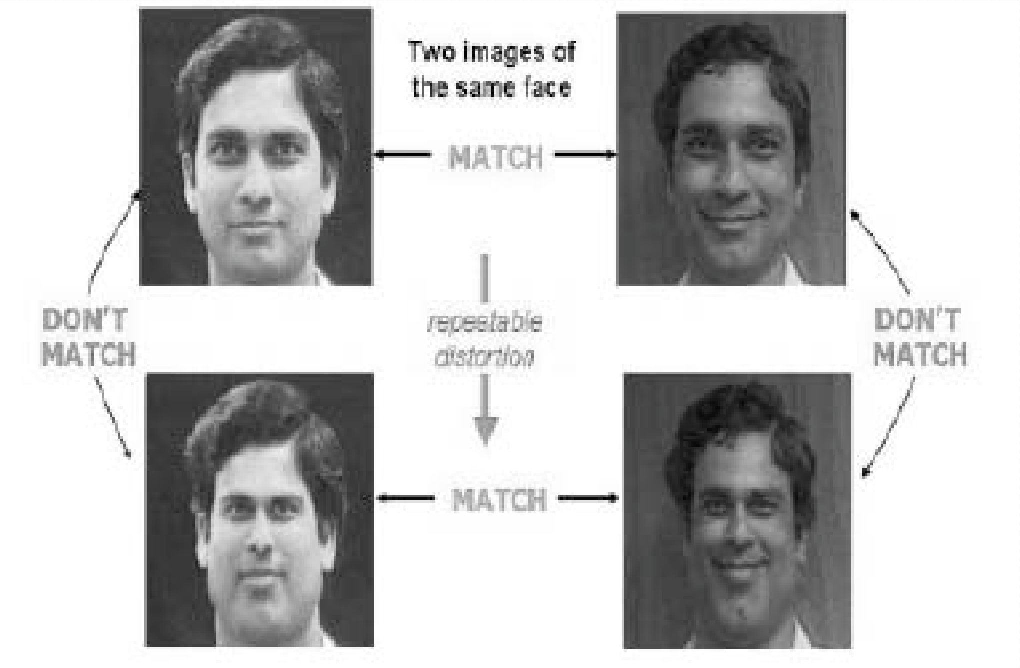
Biometric security

- Control mechanism
  - Database (DB) of (username, **hash**(T)) pairs?

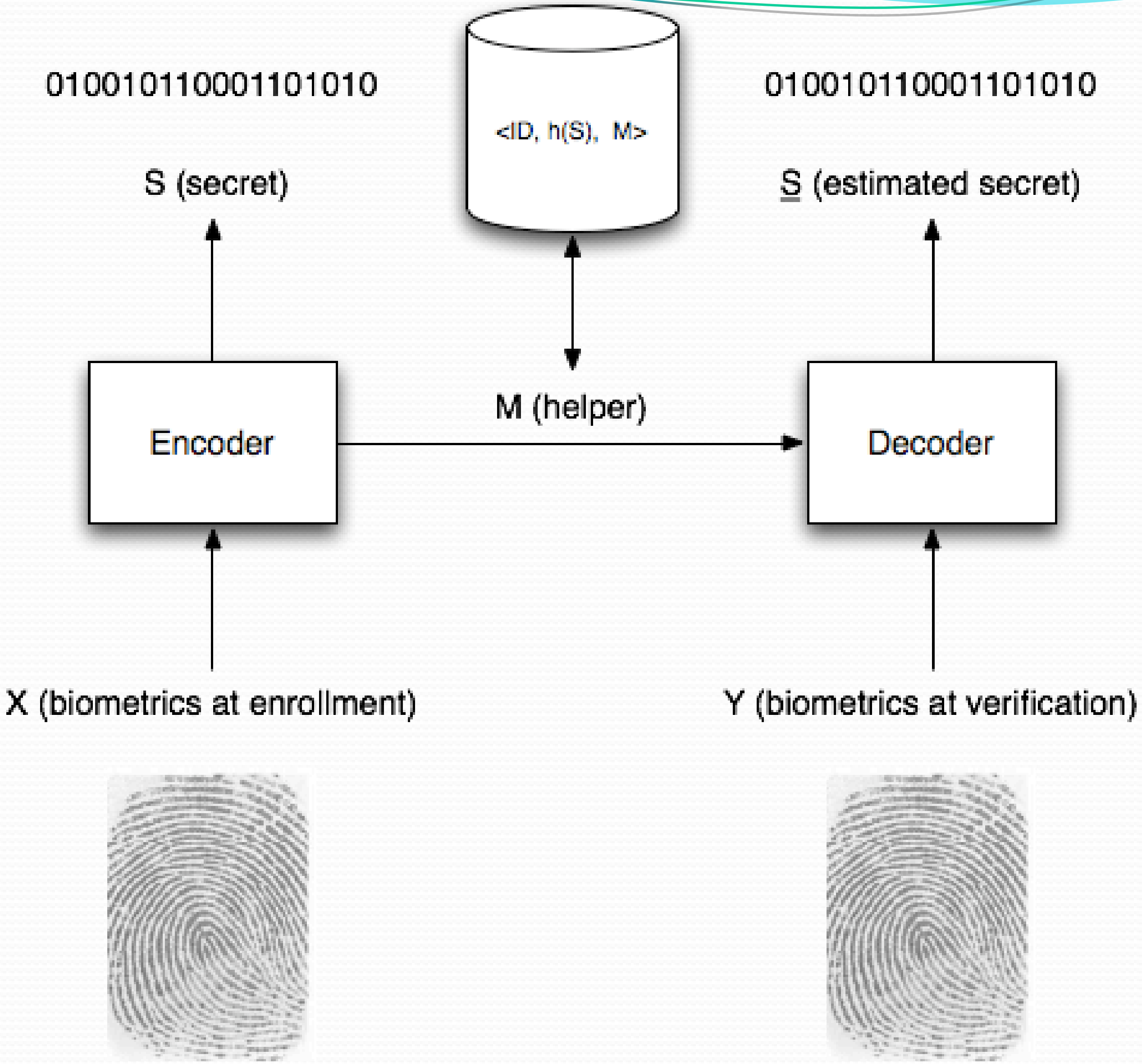
- But
  - Biometrics are fuzzy
  - Hash-functions cannot be used

- So
  - Store biometrics in unprotected form?
  - Renew biometrics when compromised?

Cancelable Biometrics



[Ratha et al., Generating Cancelable Fingerprint Templates, 2007, [2]]



010010110001101010
S (secret)
<ID, h(S), M>
010010110001101010
S (estimated secret)
Encoder
M (helper)
Decoder
X (biometrics at enrollment)
Y (biometrics at verification)

Performance parameters

- **Secrecy rate**: R_s = **log** (# secrets)/ biometric symbol

- **Security**: I(S;M) measuring leakage between helper M and secret S. **Should always be zero!**

- **Privacy rate**: R_b = I(X;M) measuring leakage between helper M and biometrics X

Common randomness (1)

- Theorem [Ahlswede & Cziszar, 1993, [1]]:
  - The maximum secrete key rate R_s that can be extracted **securely** from common randomness is given by R_s = **I(X;Y)**;
  - At maximum secrecy rate the entropy of the helper data M is given by **H(M) = H(X|Y)**
  - At maximum secrecy rate, **privacy leakage** is equal to H(M) = H(X|Y)

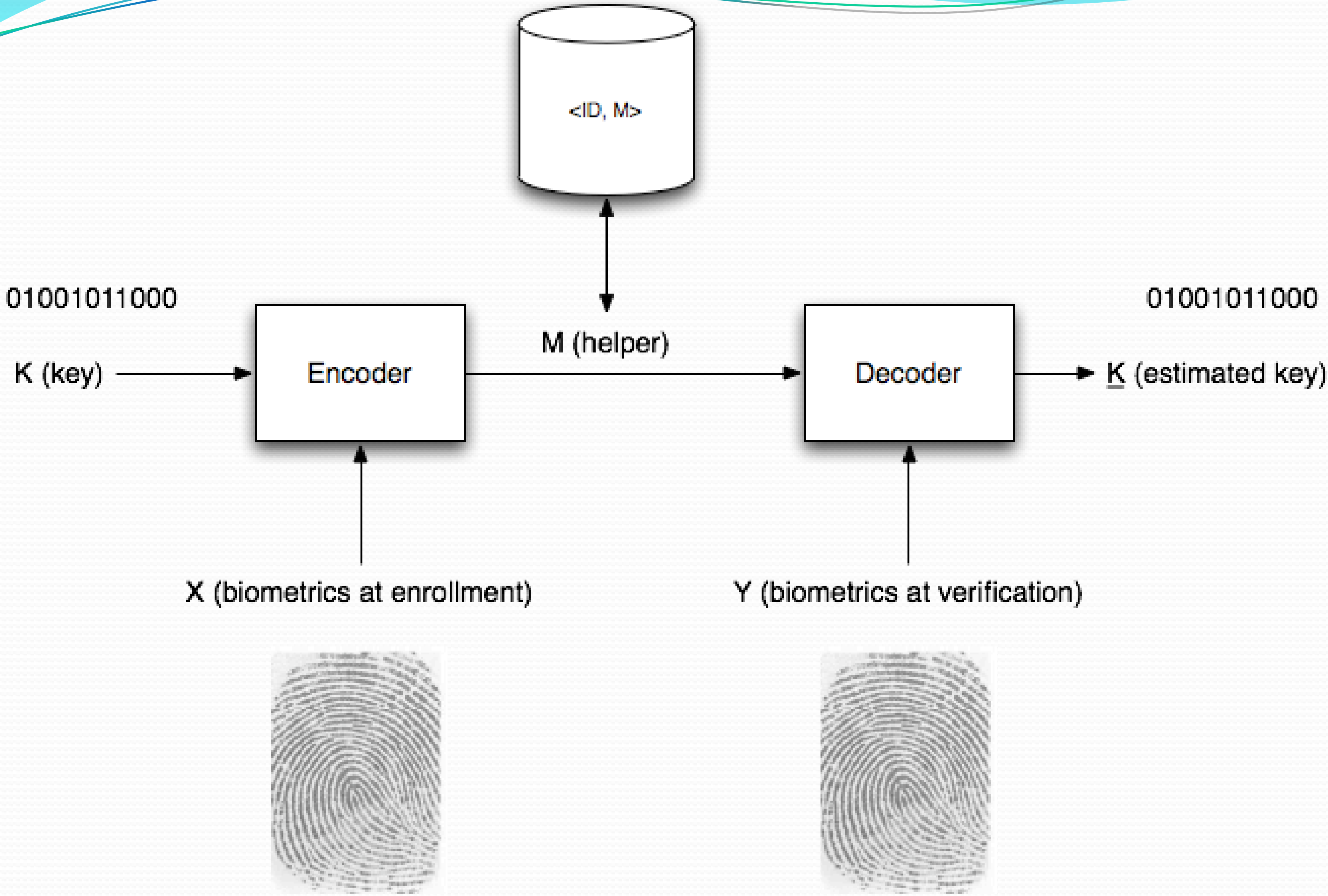
Common randomness (2)

- PRO
  - DB does not leak information on S
    - In information theoretic sense for M
    - In computational sense from h(S)
- CON
  - DB admits privacy leakage
    - In information theoretic sense
    - Can protection by computational cryptography be added?
  - DB entries cannot be changed!

Biometric encryption

- Binding a secret key to a biometric template
- PRO
  - No security leakage
  - Renewability
- CON
  - Privacy leakage

Chavoukian et al., White Paper on Biometric Encrytpion, 2007, [4]


<ID, M>
01001011000
K (key)
Encoder
M (helper)
Decoder
01001011000
K (estimated key)
X (biometrics at enrollment)
Y (biometrics at verification)

Biometric encryption

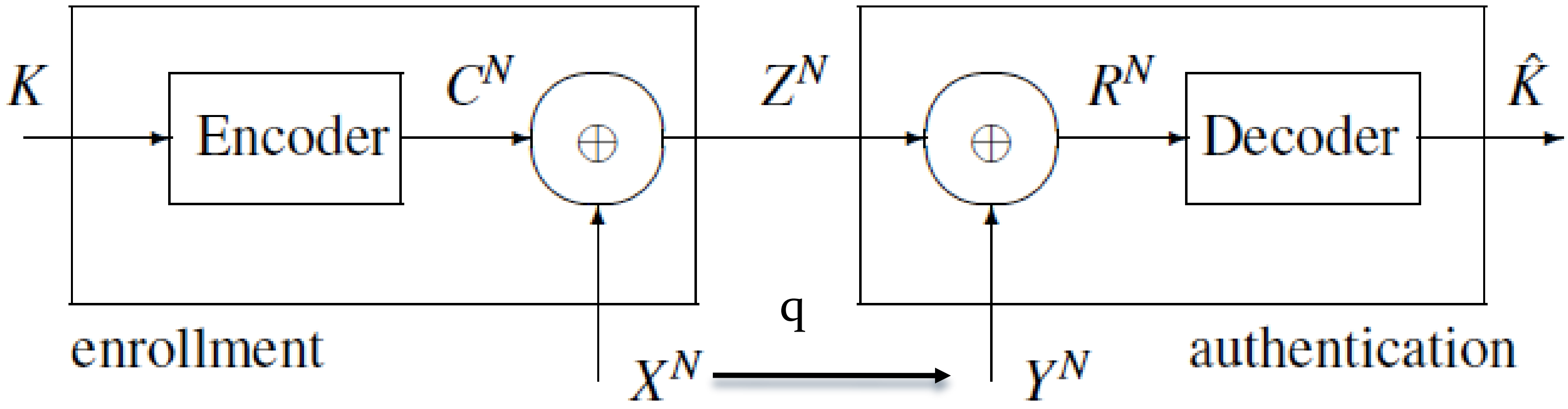
- Binding a secret key to a biometric template

- PRO
  - No security leakage
  - Renewability

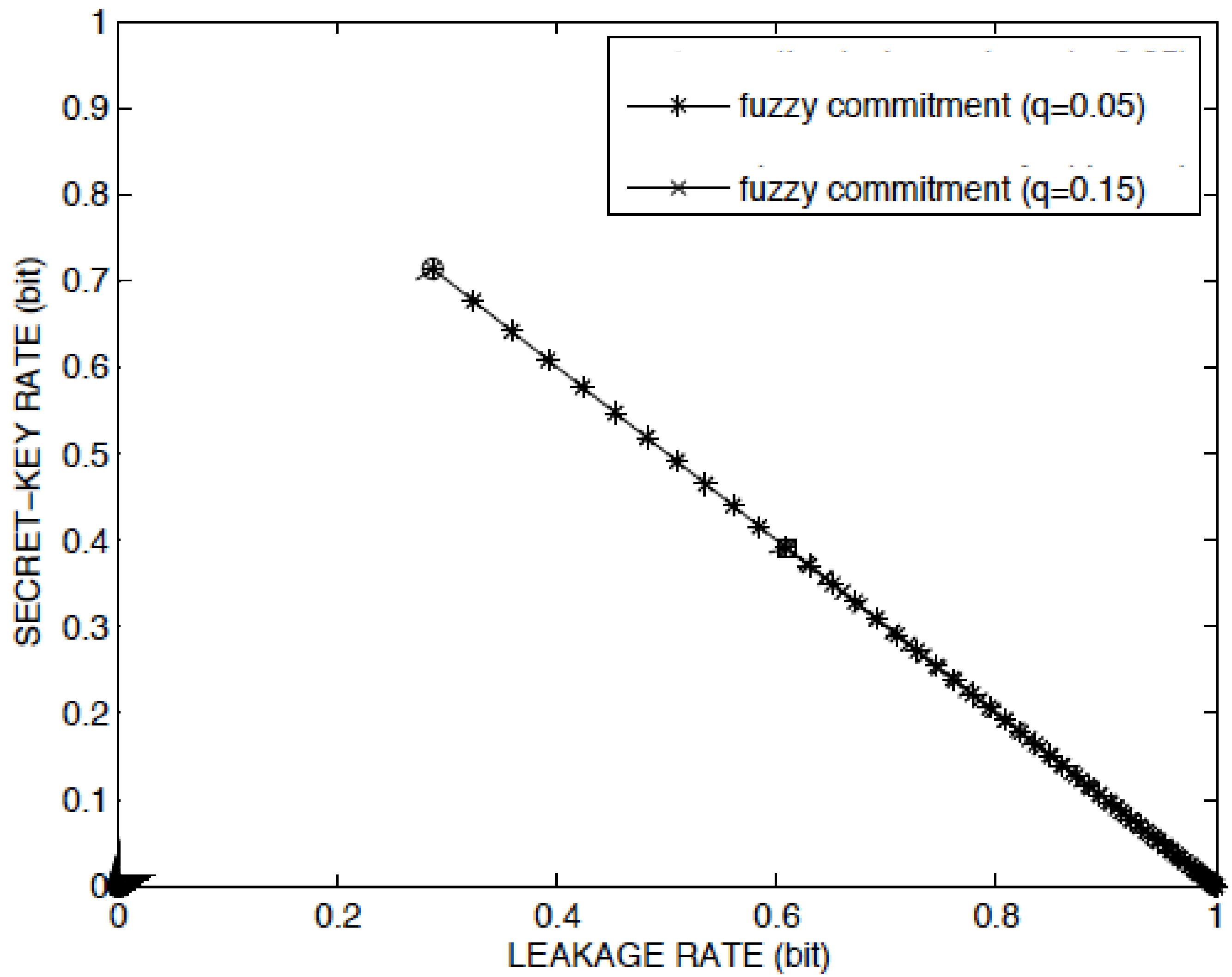
- CON
  - Privacy leakage

Chavoukian et al., White Paper on Biometric Encrytpion, 2007, [4]

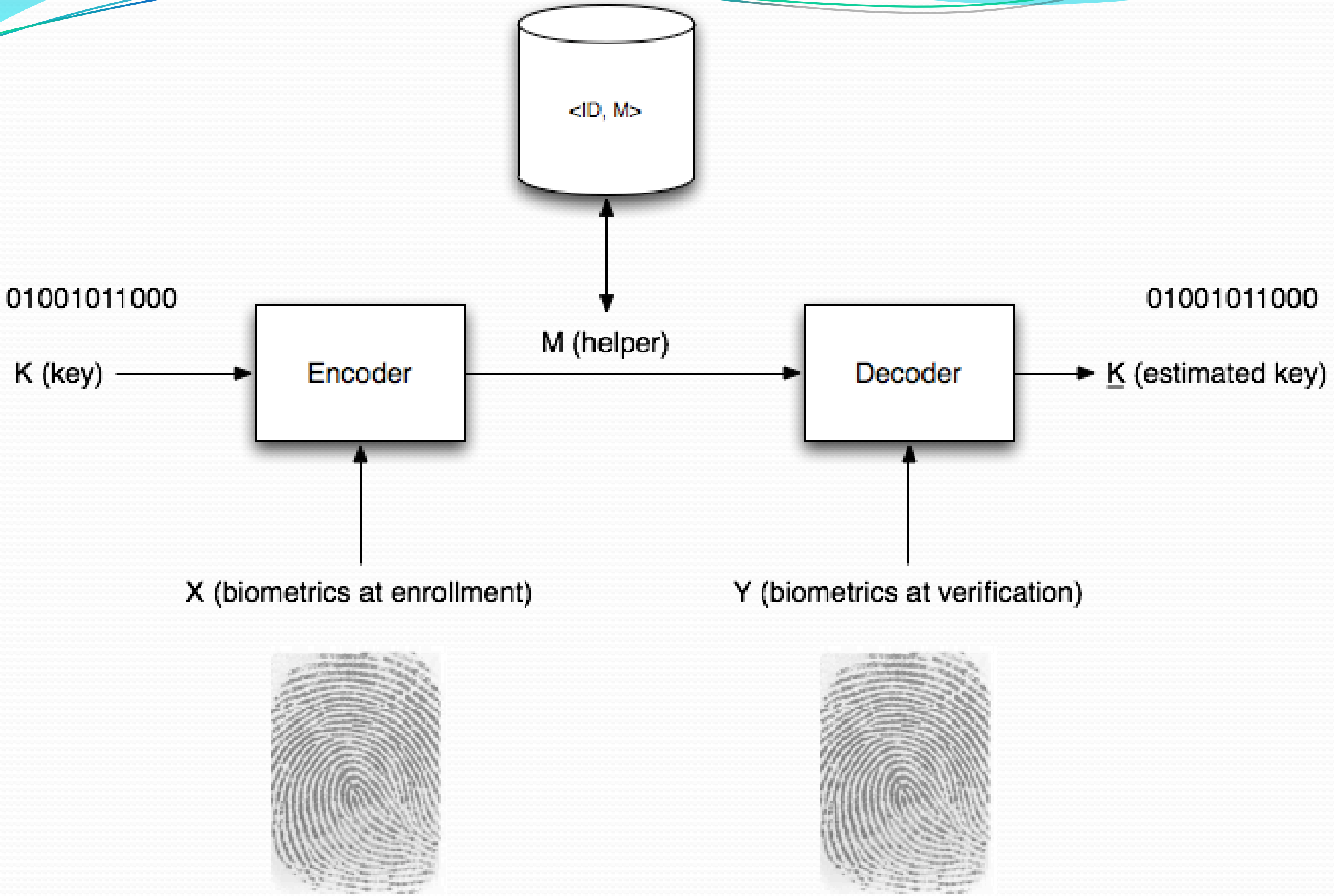
BE: Fuzzy Commitment



- Key rate R_k: $0 \le R_k \le 1 - h(q)$
- No security leakage: $I(K;Z) = 0$
- Privacy leakage: $R_b \ge 1 - R_k$



Ignatenko, 2009 [3]

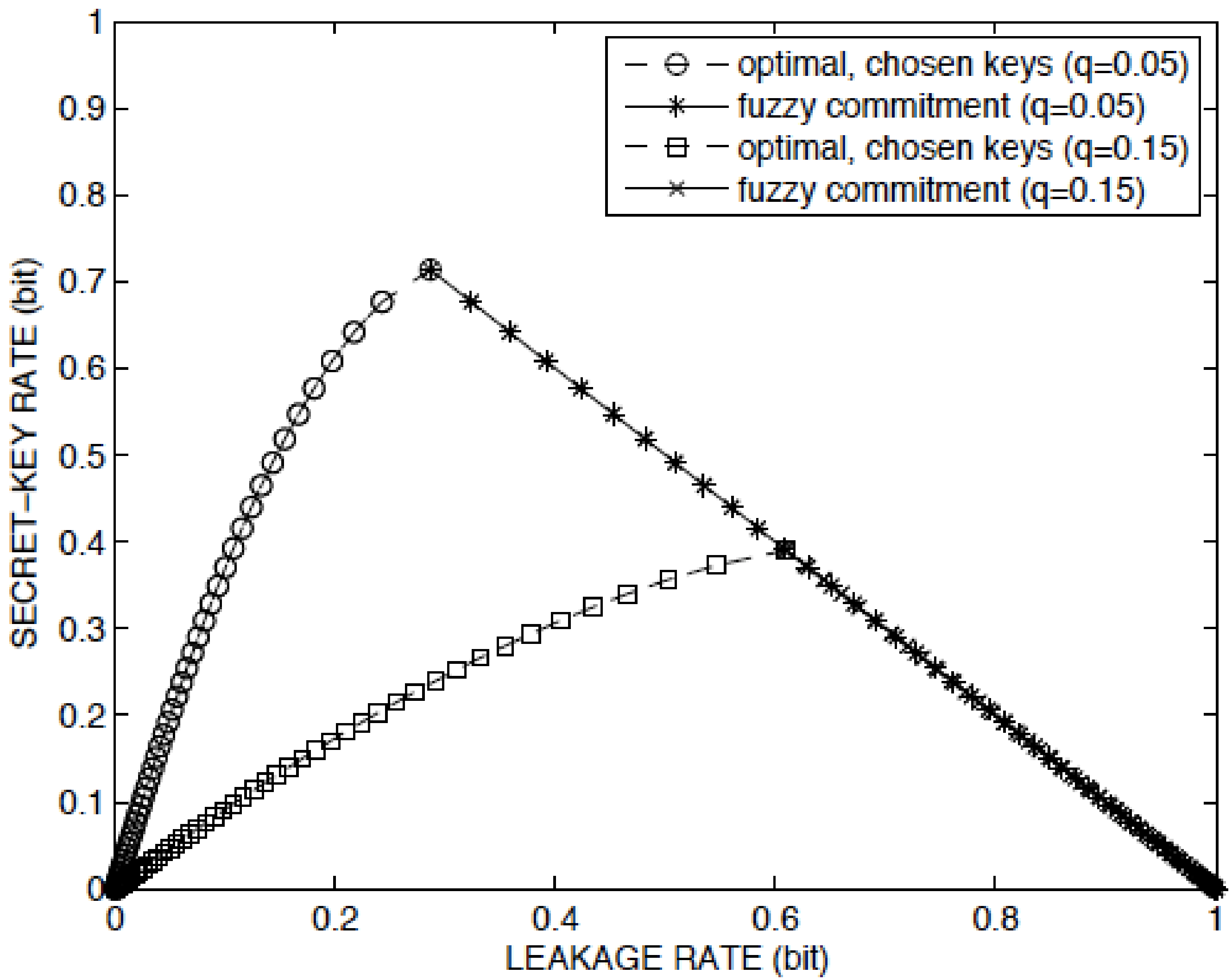

<ID, M>
01001011000
K (key)
Encoder
M (helper)
Decoder
01001011000
K (estimated key)
X (biometrics at enrollment)
Y (biometrics at verification)

Optimal Biometric Encryption

- Theorem (Ignatenko, 2009 [3]) The optimal relation between secret key rate and privacy leakage is given by
  - $R_k = I(U;Y)$
  - $R_b = I(U;X) - I(U;Y)$
  - $H(M) = I(U;X)$

  for some auxiliary random variable $U \rightarrow X \rightarrow Y$

- Proof: random binning argument



Ignatenko, 2009 [3]

Open questions

- Theory
  - Integration of computational and information theoretic security
  - Correlation in biometric data
- Theory to practice
  - Real biometric signals are not i.i.d.
  - Real biometric signals have finite length
  - Measuring entropy
  - Constructing codes

Bibliography

1. R. Ahlswede and I. Csiszár, “Common randomness in information theory and cryptography - part I: Secret sharing,” *IEEE Transactions on Information Theory,* vol. 39, pp. 1121–1132, July 1993.
2. N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, “Generating cancelable fingerprint templates,” *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 29, no. 4, pp. 561–572, April 2007
3. T. Ignatenko, Secret-Key Rates and Privacy Leakage in Biometric Systems, “Secret-Key Rates and Privacy Leakage in Biometric Systems”, Thesis, TUE, June 2009.
4. Ann Chavoukian and Alex Stoianov, “Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy”, White Paper IPC, http://www.ipc.ca, March 2007.