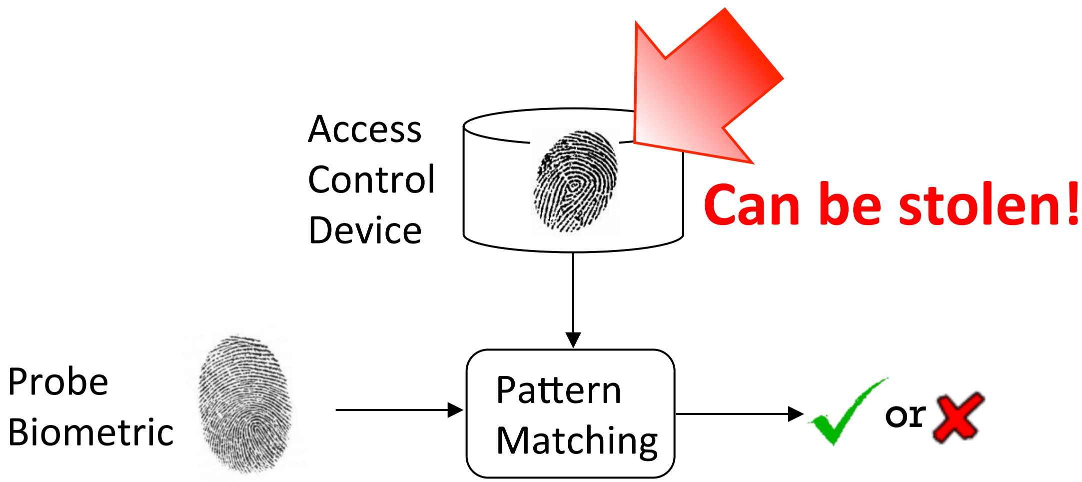
Performance Testing of Biometric Template Protection Schemes

ISO/IEC 30136

Shantanu Rane
MERL, Cambridge, MA.

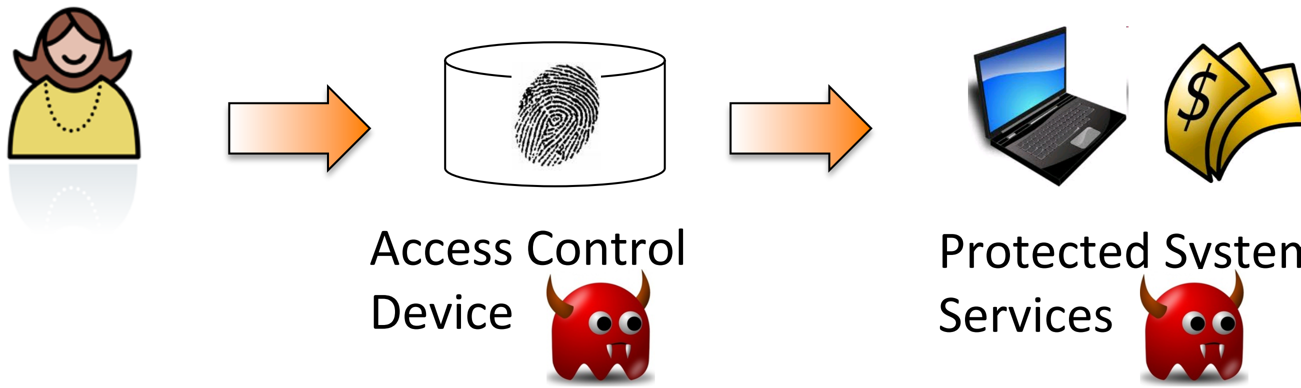
IBPC 2014, NIST, Gaithersburg, MD.

Conventional Biometric Recognition



- Reference biometric is often stored in the clear, OR
- Encrypted for storage but decrypted during comparison. Visible to attacker monitoring the authentication protocol.
- Biometrics cannot be canceled and renewed an unlimited number of times (unlike passwords).

What does an attacker stand to gain?

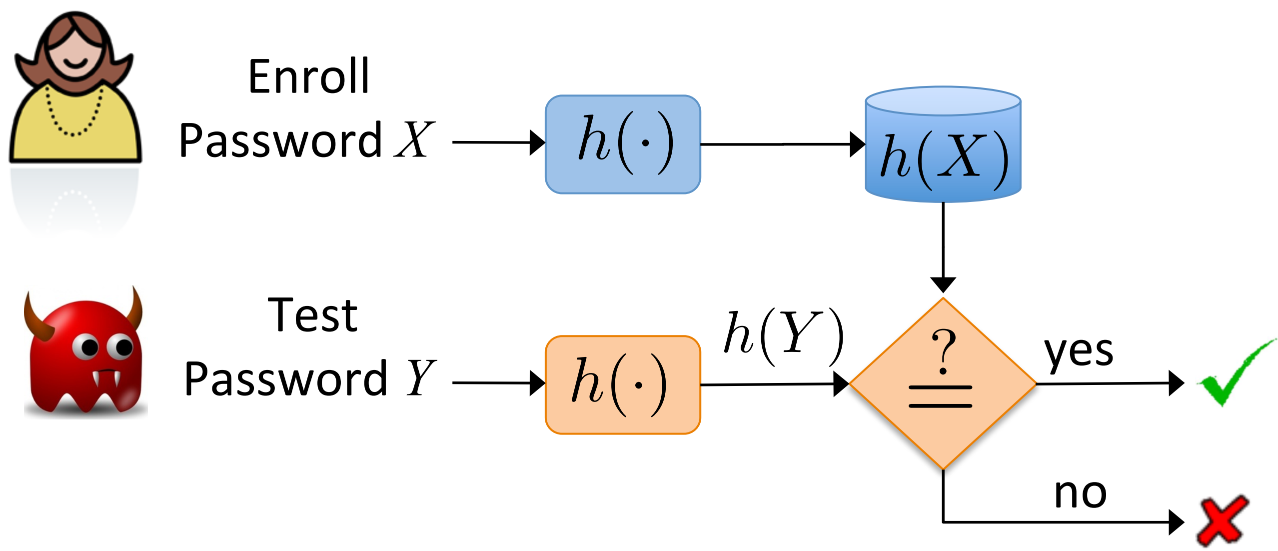


- Attacker discovers information about the biometric, an inherent property of the person.
- Attacker gains access to the system. E.g.
  - Sensitive files and data (Trade secrets)
  - Finances (Bank accounts)
  - Services (Gym, parking lot, etc.)
- **Distinct notions**: One does not necessarily imply the other!

Outline

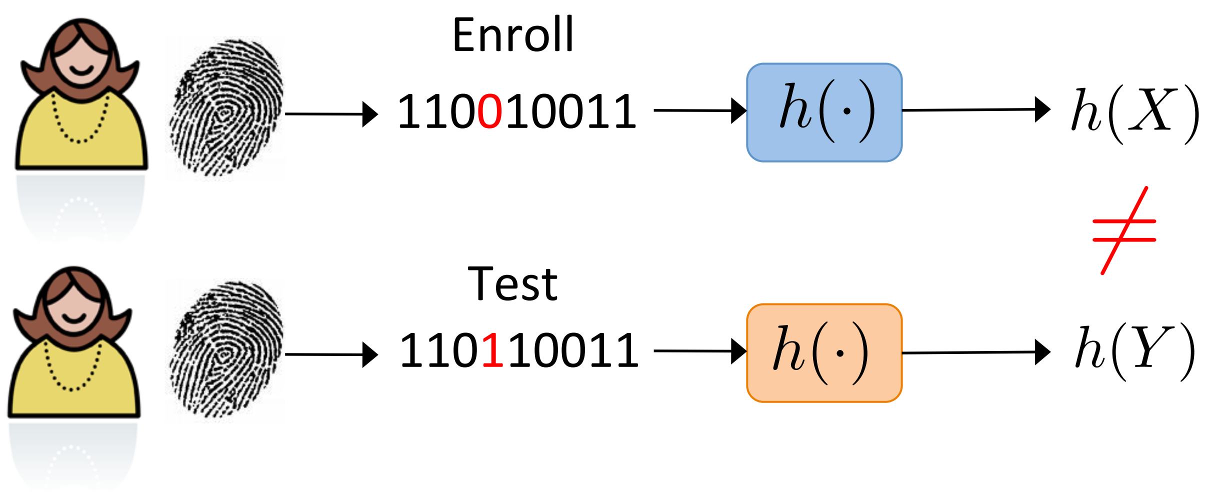
- What is biometric template protection?
- How to evaluate performance of template protection systems?
- One example: Fuzzy commitment
- Why is standardization necessary?
- A brief history of ISO/IEC WD 30136

Can cryptographic hashes be used to secure biometrics?



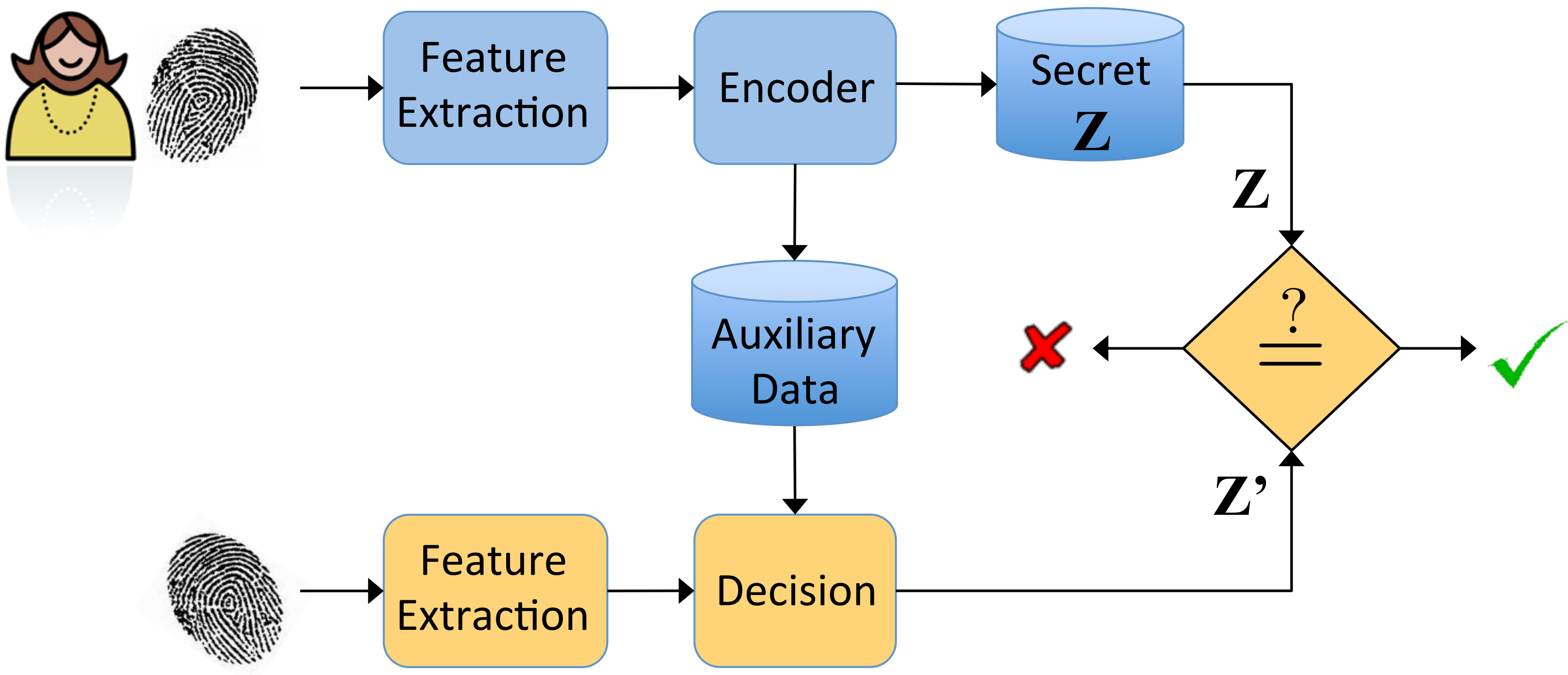
- At enrollment, computer stores a cryptographic hash (e.g. SHA 256, MD5) of a password, not the password itself.
- Authentication involves comparison of hashes.

Biometrics are noisy, Hashes don't work.



- Biometrics are inherently noisy, exact matches are impossible. E.g., Fingerprints vary from measurement to measurement due to dust, oil, dryness, pressure, misalignment, injury, etc.
- Even legitimate biometrics generate vastly different hashes.

Biometric Template Protection



- Enrolment (blue) process results in two items
  - A secret called a Pseudonymous Identifier
  - Auxiliary data, which leaks little or no info about biometric
- Decision process attempts to extract secret from test biometric and auxiliary data. Can use cryptographic hashes for the secret.

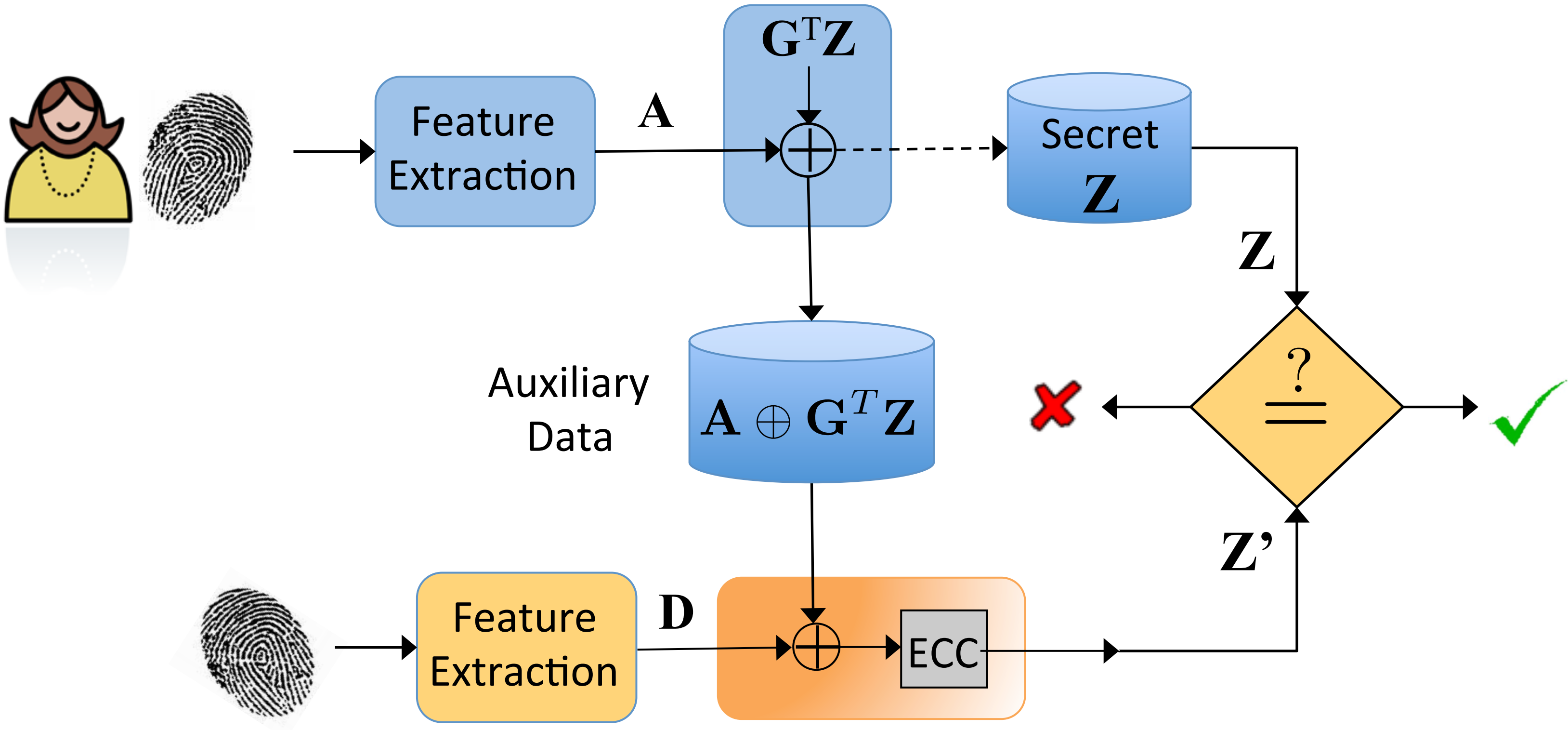
How to Evaluate Template Protection Systems?

- How often does the system **falsely reject** a genuine user?
- How often does the system **falsely accept** somebody else?
- How well does the system preserve **secrecy** of protected data?
- Is the stored template **irreversible**, i.e., how difficult is it for an attacker to recover the biometric from the template?
- How much **storage** do the templates require?
- Can an attacker combine two or more templates to gain an advantage (**unlinkability**)?
- How many templates can one extract from a given biometric (**diversity**)?

Concepts and Examples of Metrics

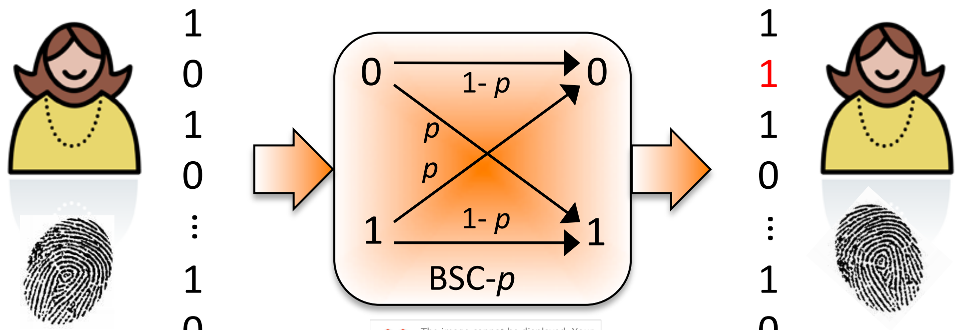
• Missed detection	False Non-Match Rate (FNMR)
• False acceptance	False Match Rate (FMR)
• Secrecy	Successful Attack Rate (SAR)
• Irreversibility	# Bits of Privacy Leakage
• Storage	# Bits
• Unlinkability, Diversity, Revocability, …	?

Fuzzy Commitment



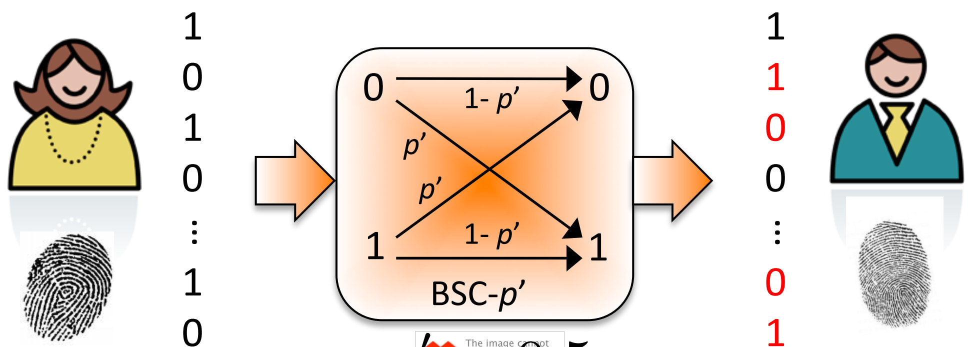
- Enrolment: Choose k-bit secret $\mathbf{Z}$, and derive a ECC codeword. Perturb the codeword with biometric $\mathbf{A}$ to obtain auxiliary data.
- Decision module tries to cancel out the perturbation using $\mathbf{D}$. Does not succeed completely as $\mathbf{D}$ is a noisy version of $\mathbf{A}$.
- Noise bits $\mathbf{A} \oplus \mathbf{D}$ removed by ECC decoding to return $\mathbf{Z}$.

Modeling differences between biometrics



$$0 \le p \ll 0.5$$

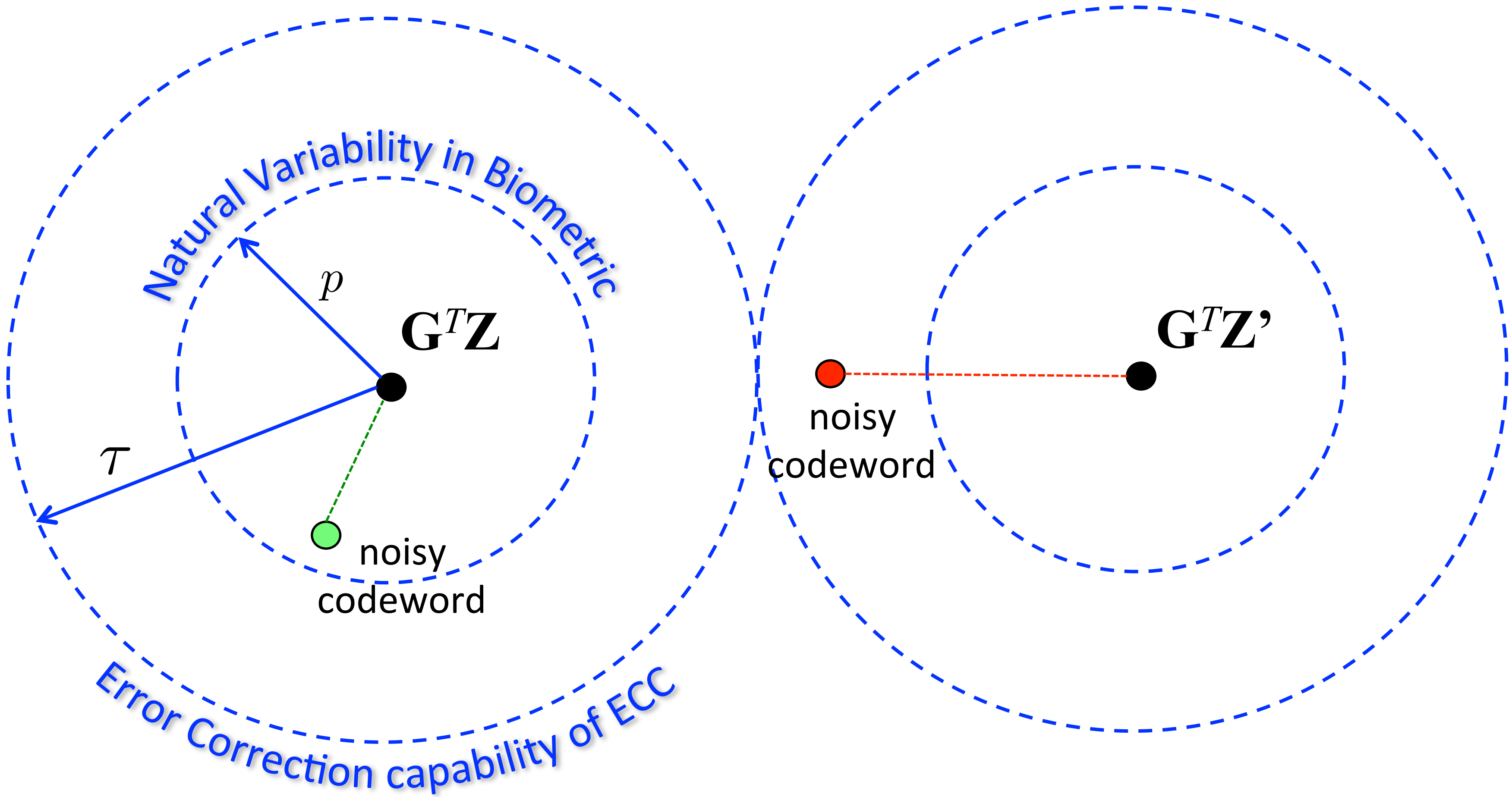
- Features extracted from the same user are similar, hence modeled by a less noisy channel.



$$p' \approx 0.5$$

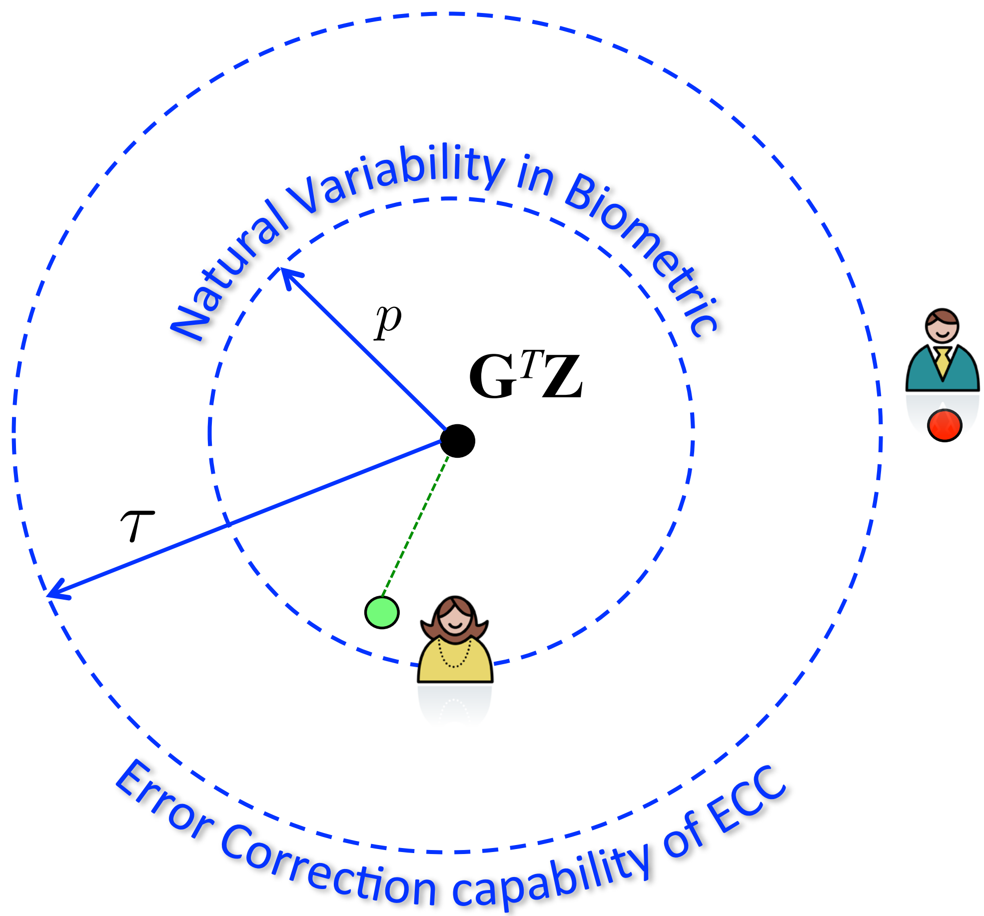
- Features extracted from a different user are dissimilar, hence modeled by a very noisy channel.

False Non-Match Rate (FNMR)



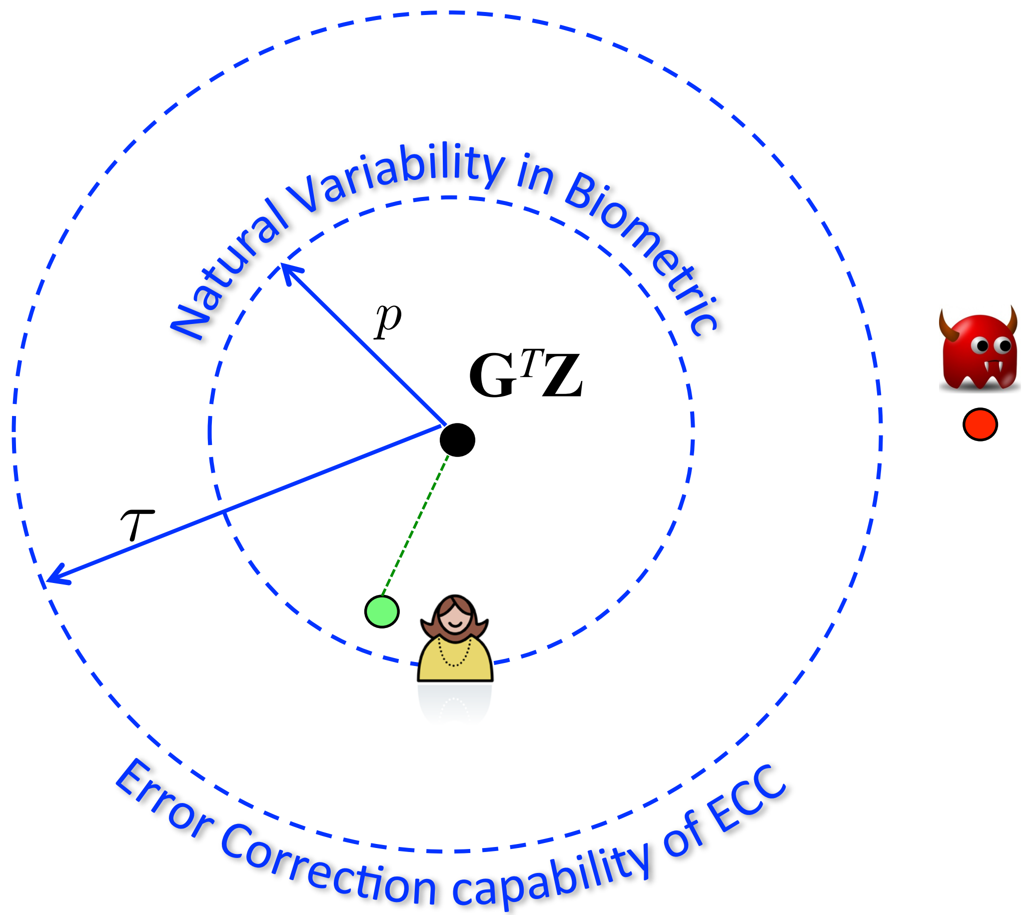
FNMR depends on the natural variability in the biometric features and the strength of the error correcting code.

False Match Rate (FMR), OR Probability of Successful Attack by an *Uninformed* Adversary



FMR also depends on the variability in the biometric features, and the strength of the error correcting code

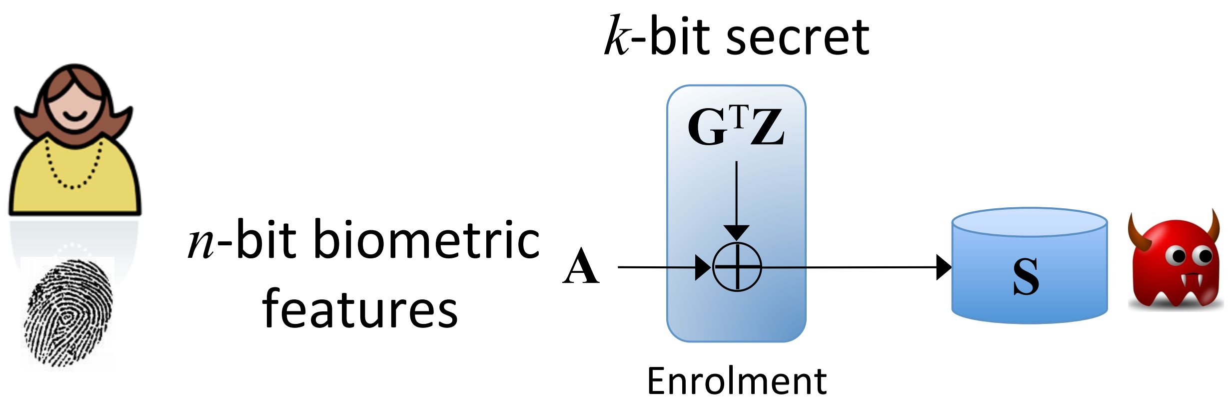
Probability of Successful Attack by an *Informed* Adversary



SAR is at least as large as the FMR, and can be larger if adversary

- Obtains side information about enrolled users
- Uses knowledge of system parameters to synthesize attack biometric

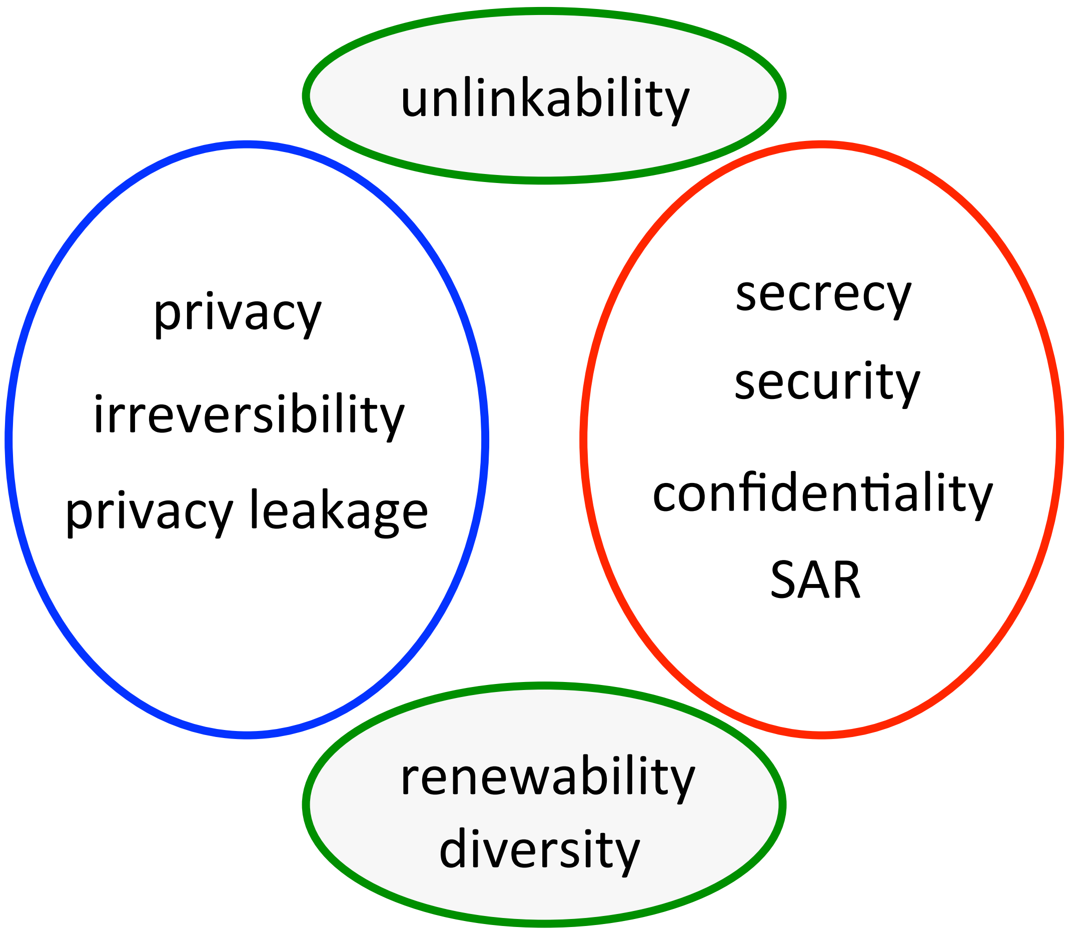
Privacy Leakage



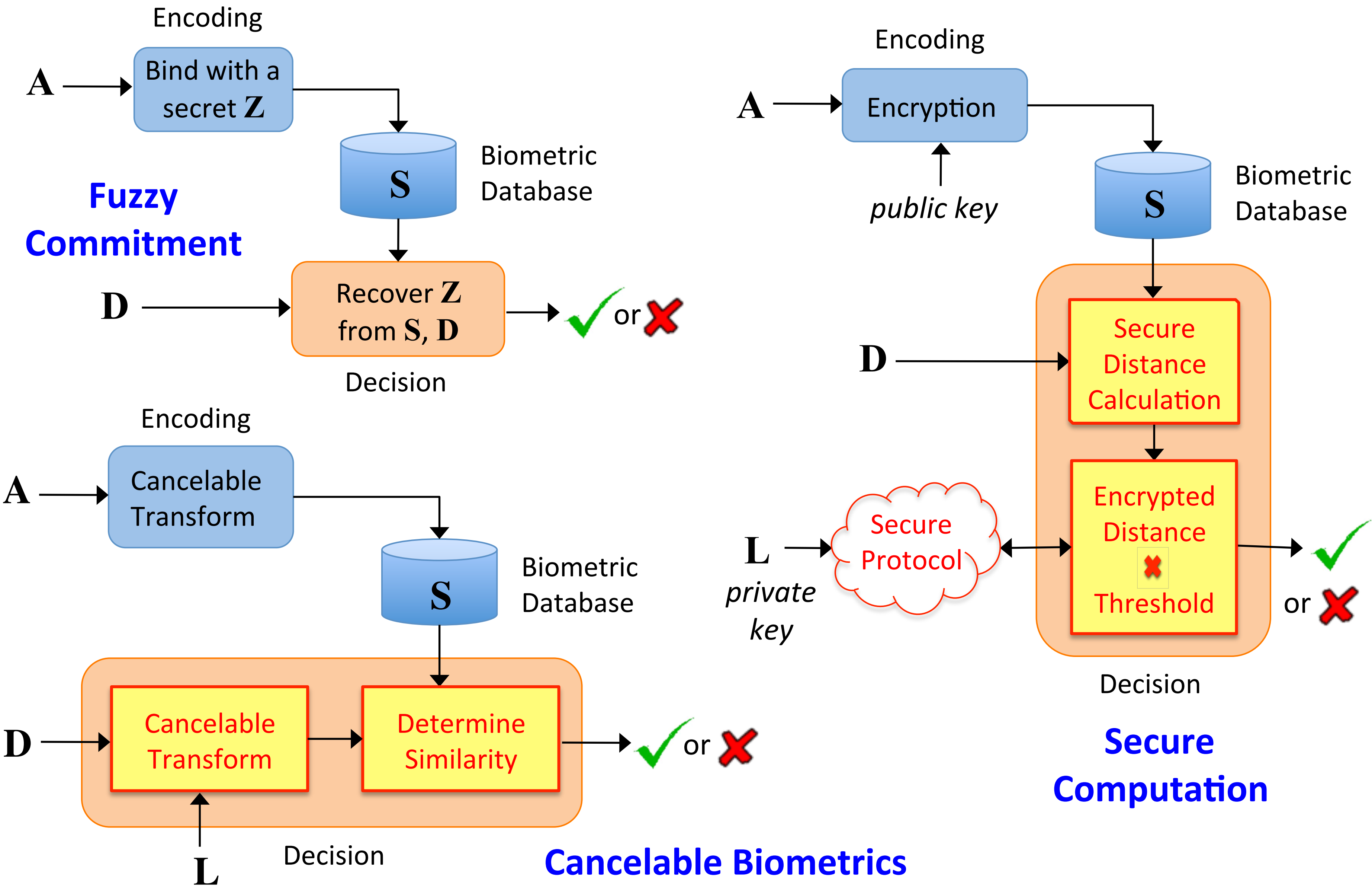
- # of possible biometric feature vectors is 2^n
- But # of possible secrets is only 2^k
- Hence # of bits leaked about the biometric is $n-k$
- Each time an adversary hacks into the auxiliary database, he will discover $n-k$ bits.

Why is standardization necessary?
(1) A vocabulary for security and privacy

Vast academic literature, but need consensus on the concepts and definitions of the quantities being measured.



Why is standardization necessary?
(2) Extending metrics to many architectures



Why is standardization necessary?
(3) Metrics depend on attack models

- **Naïve model:** Adversary only tries to succeed in biometric recognition without any side information.
- **Kerckhoffs' Principle:** Adversary knows all essential details of the template protection algorithm, and implementation parameters, but not the secrets or keys.
- **Stronger adversary:** Adversary knows all essential details of the template protection algorithm, implementation parameters, and a subset of secrets or keys.
- Adversary can be computationally **bounded** or **unbounded**.

- Any reported metrics must also specify the models under which they apply.

A brief history of ISO/IEC 30136

- 2010 Melaka SC37 meeting, USNB Informative Presentation, Incorporated into WG5 Roadmap
- **2011 SC27 24725 Standard on Biometric Information Protection**
- 2011 Phuket SC37 meeting, JPNB Informative Presentation
- 2012 Paris SC37 meeting, New Work Item Proposal, USNB
- **2013 Winchester SC37 meeting, NWIP approved, US/JP Co-editors Comments invited on 1st WD of ISO/IEC 30136.**
- 2014 Darmstadt SC37 meeting, Comments invited on 2nd WD
- 2014 Purdue SC37 meeting, …

Summary

- Template protection enables biometric recognition without directly storing biometric features in the enrolment database.
- In addition to traditional performance metrics, there is a need for metrics that specify how strongly the systems deter attacks on
  - individuals biometric data
  - data/services enabled by the recognition systems
- The goal of ISO/IEC WD30136 is to specify metrics, and evaluation methodologies for template protection architectures.

Bibliography

- [JW 1999] A. Juels and M. Wattenberg, “A fuzzy commitment scheme,” in Proc. ACM Conf. on Computer and Communications Security, Nov. 1999, pp. 28–36.
- [LHP 2011A] L. Lai, S. W. Ho, and H. V. Poor, “Privacy-security tradeoff in biometric security systems–Part I: Single use case,” IEEE Trans. Information Forensics and Security, vol. 6, no. 1, pp. 122–139, Mar. 2011.
- [IW 2012] T. Ignatenko and F. M. J. Willems, “Biometric security from an information-theoretical perspective,” Foundations and Trends in Communications and Information Theory, vol. 7, no. 2-3, pp. 135–316, Feb. 2012.
- [SYZBBNP 2012] K. Simoens, B. Yang, X. Zhou, F. Beato, C. Busch, E. Newton, and B. Preneel, “Criteria towards metrics for benchmarking template protection algorithms,” in Proc. IAPR International Conference on Biometrics (ICB), New Delhi, India, Mar. 2012, pp. 498–505.
- [N 2008] K. Nandakumar. (Ph.D. Thesis). “Multibiometric systems: fusion strategies and template security.” ProQuest Publishing, 2008.
- [TNG 2004] A. Teoh, D. Ngo, and A. Goh. "Biohashing: two factor authentication featuring fingerprint data and tokenised random number." Pattern recognition 37.11 (2004): 2245-2255.
- [ISO 24745] SC27 IT Security Techniques, ISO/IEC 24745: Biometric Information Protection.International Standards Organization, 2011.

Bibliography

- [RCB 2001] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Systems Journal, vol. 40, no. 3, pp. 614–634, 2001.
- [WRDI 2012] Y. Wang, S. Rane, S. C. Draper, and P. Ishwar, "A theoretical analysis of authentication, privacy and reusability across secure biometric systems," IEEE Trans. Information Forensics and Security, vol. 7, no. 6, pp. 1825–1840, Dec. 2012.
- [**R**WDI 2013] S. Rane, Y. Wang, S. C. Draper, and P. Ishwar, "Secure Biometrics: Concepts, Authentication Architectures, and Challenges" IEEE Signal Processing Magazine, Sep. 2013.

Q & A

rane@merl.com