A Generalized Framework for Privacy and Security Assessment of Biometric Template Protection

Xuebing Zhou

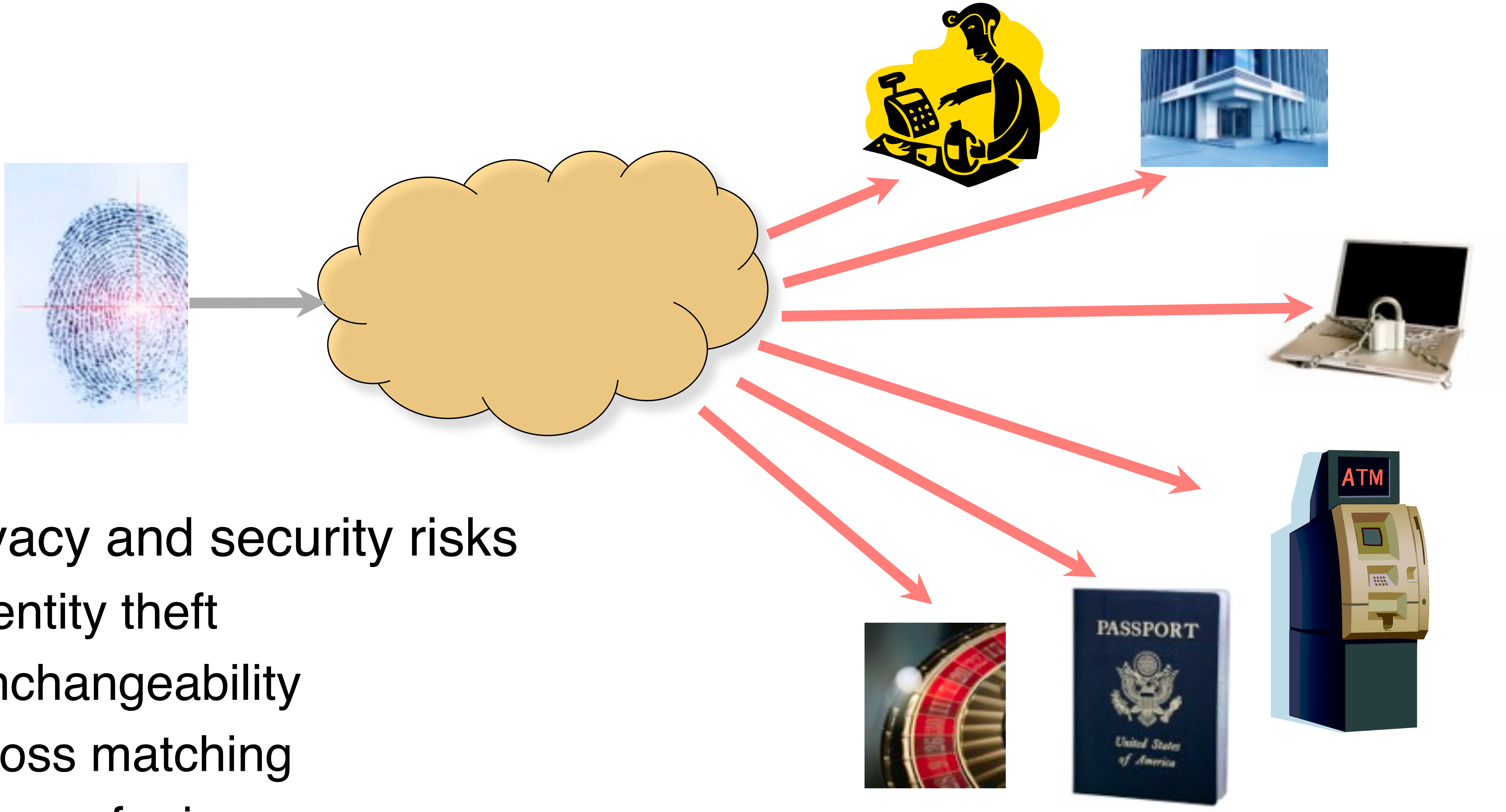
CASED - Center for Advanced Security Research Darmstadt
Hochschule Darmstadt

Gaithersburg, March 09, 2012

Content

- Biometric template protection
- How to assess biometric template protection
  the systematic evaluation framework
- Assessment of different systems
- Conclusions
- Future work

Biometric Systems



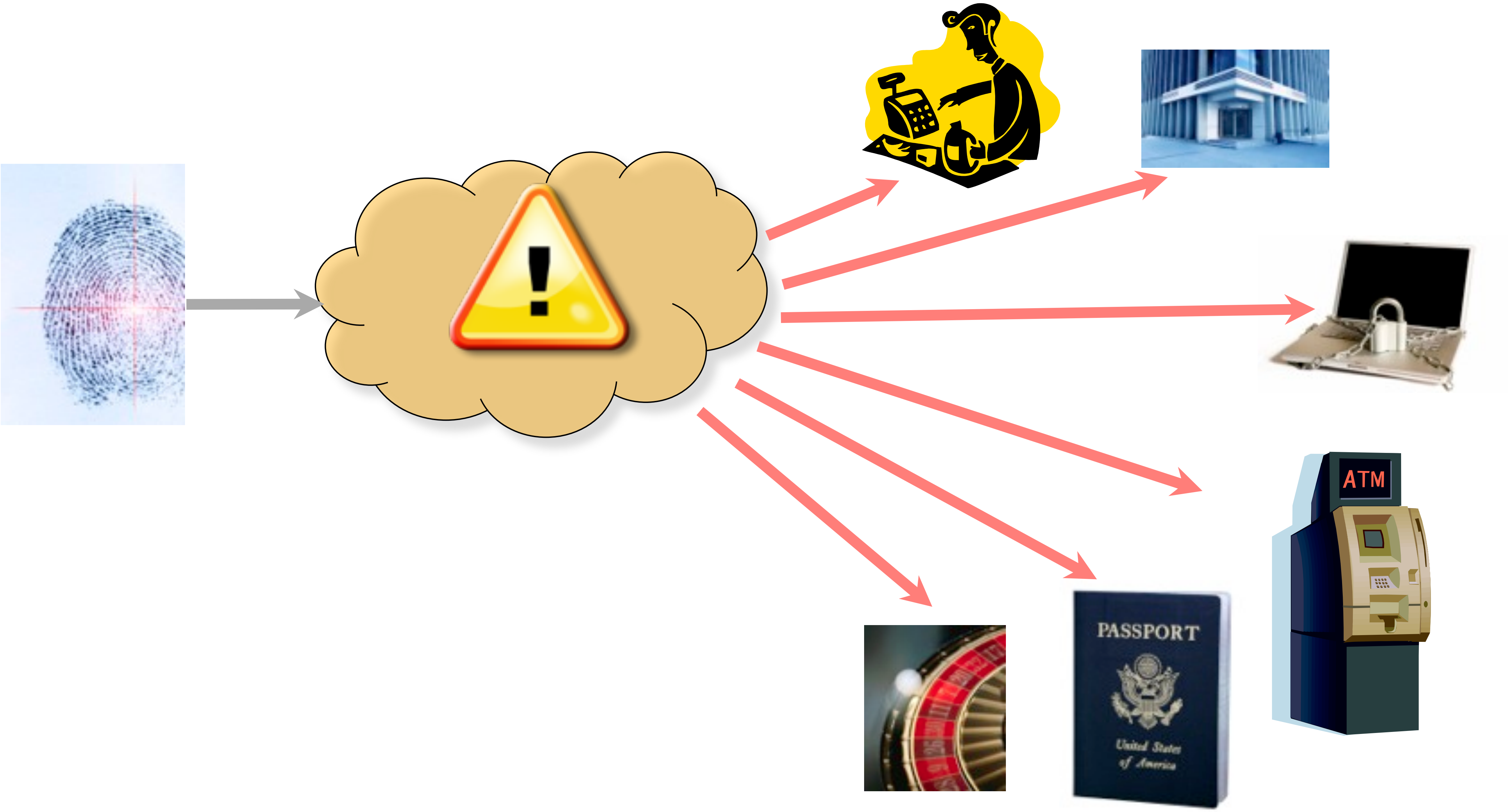
- Privacy and security risks
  - Identity theft
  - Unchangeability
  - Cross matching
  - Harm of privacy

Biometric Systems

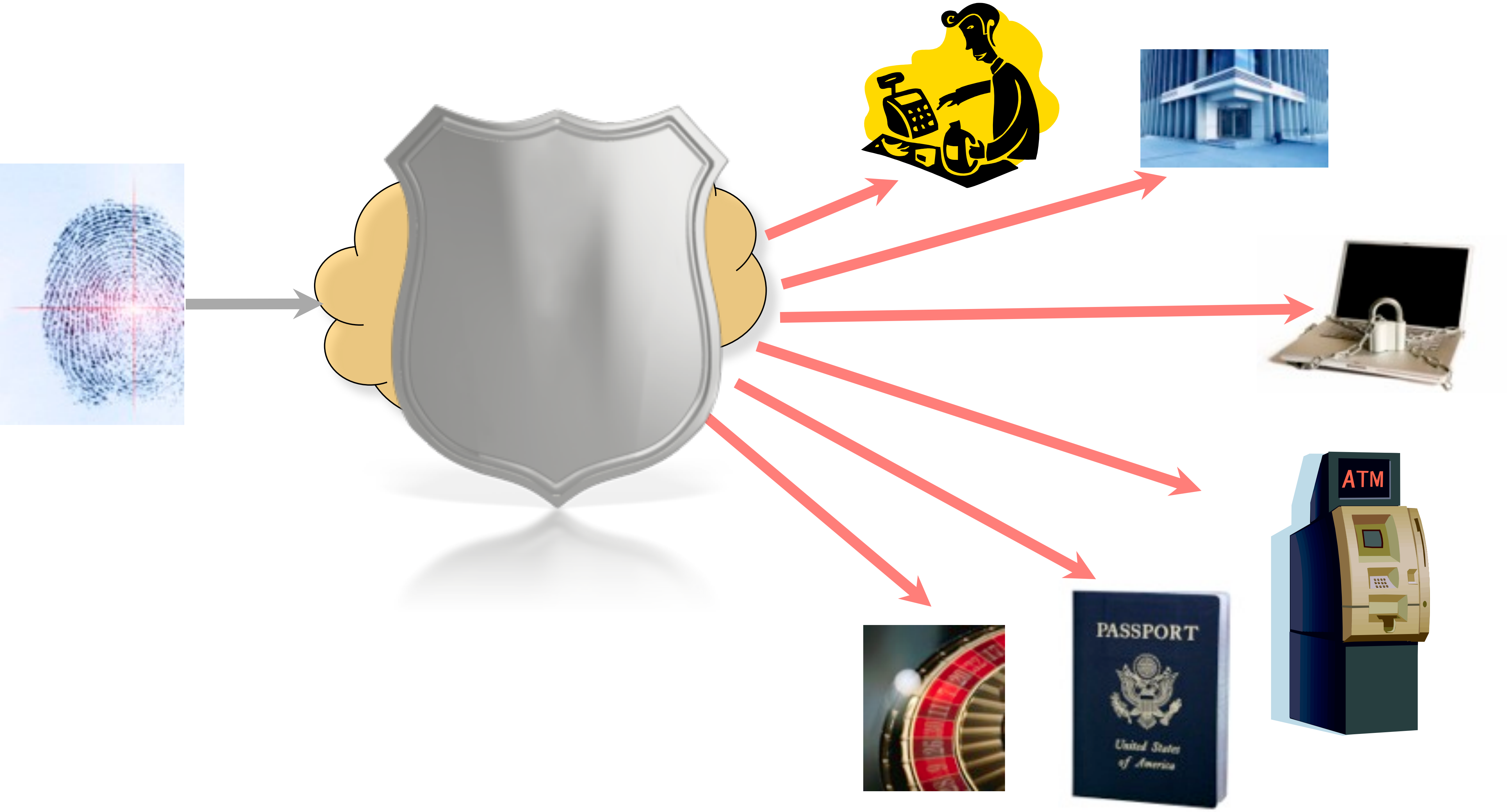
ATM
PASSPORT
United States of America

- Privacy and security risks
  - Identity theft
  - Unchangeability
  - Cross matching
  - Harm of privacy

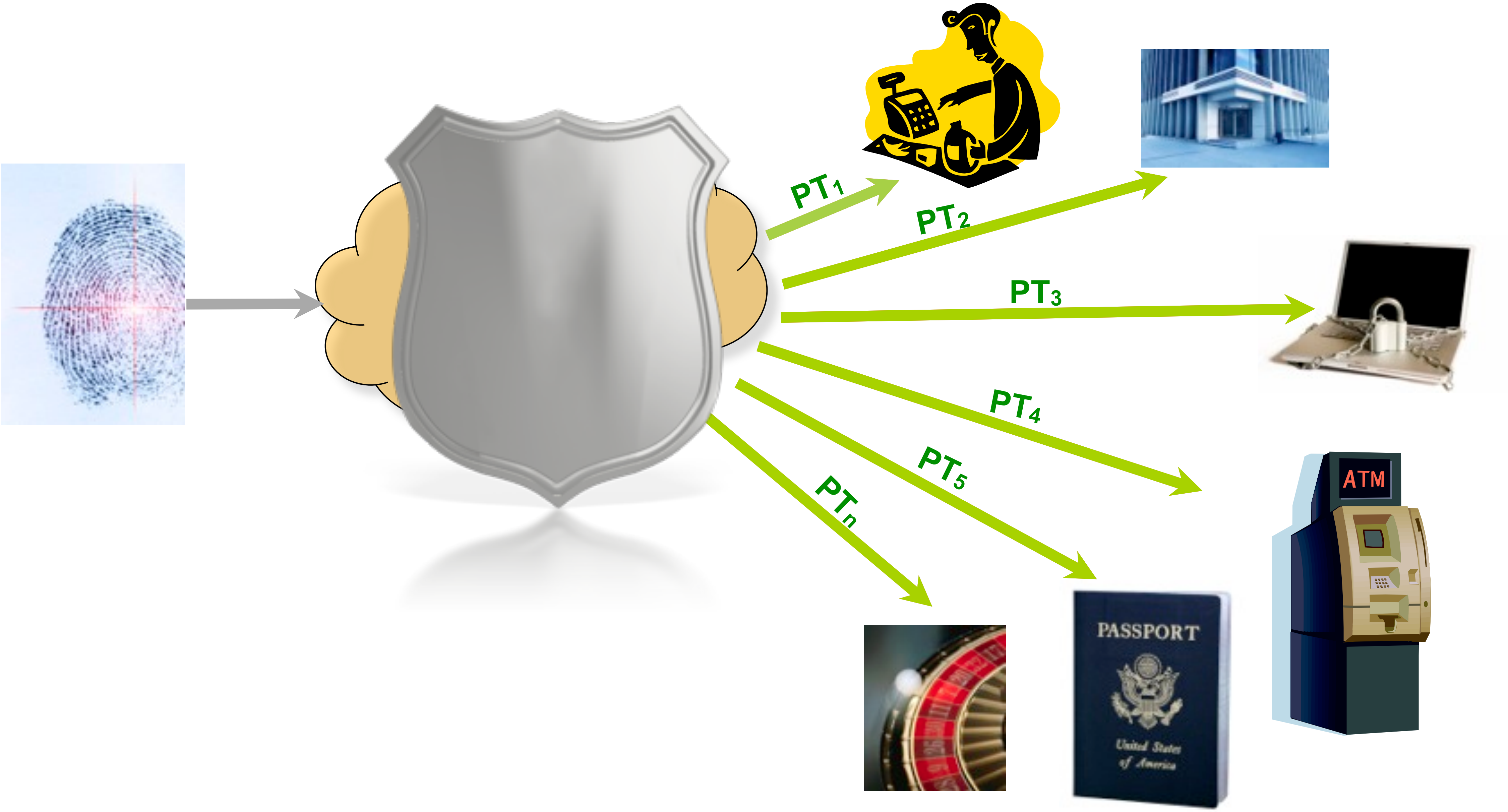
Biometric Template Protection



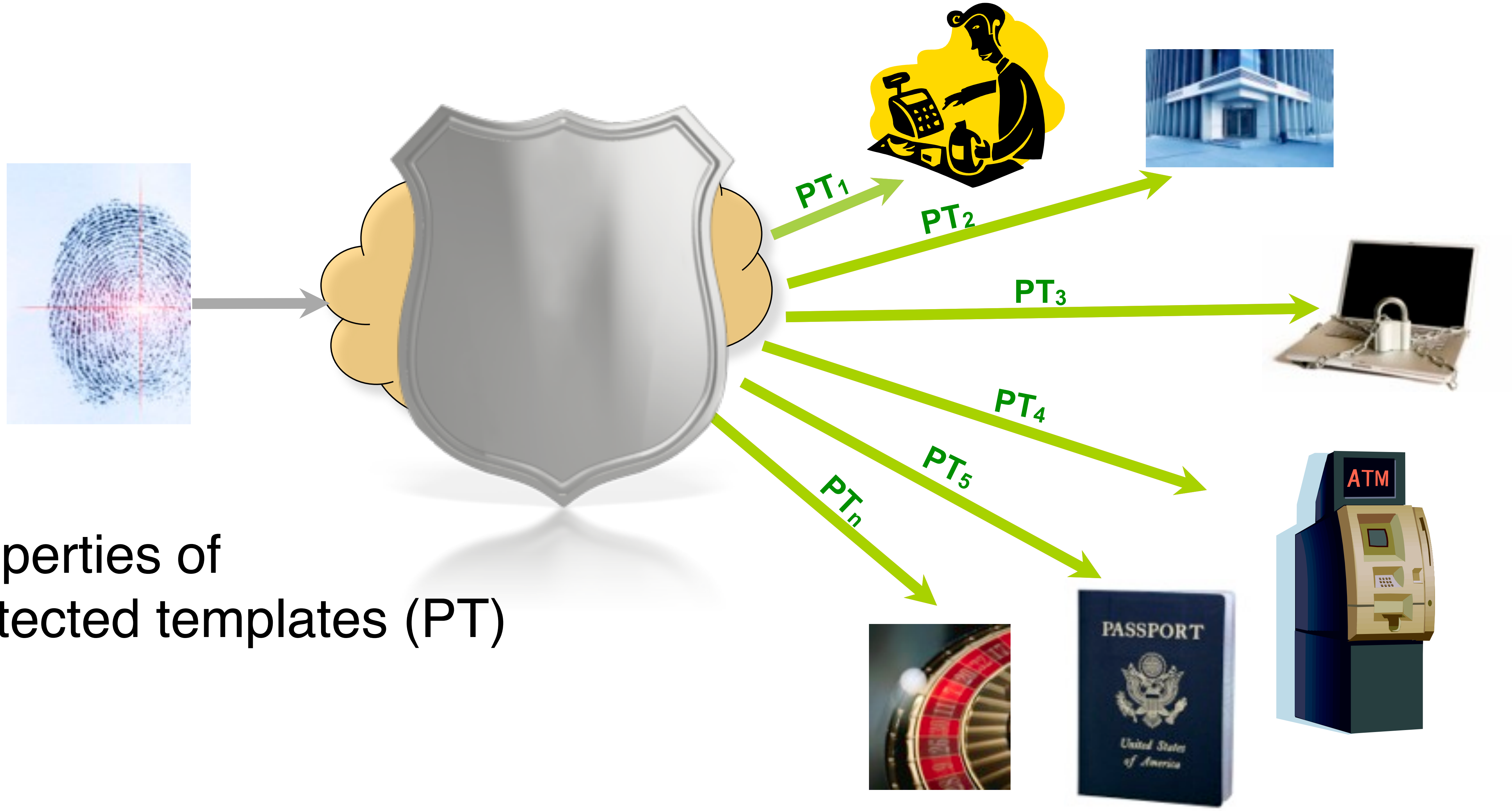
Biometric Template Protection



Biometric Template Protection

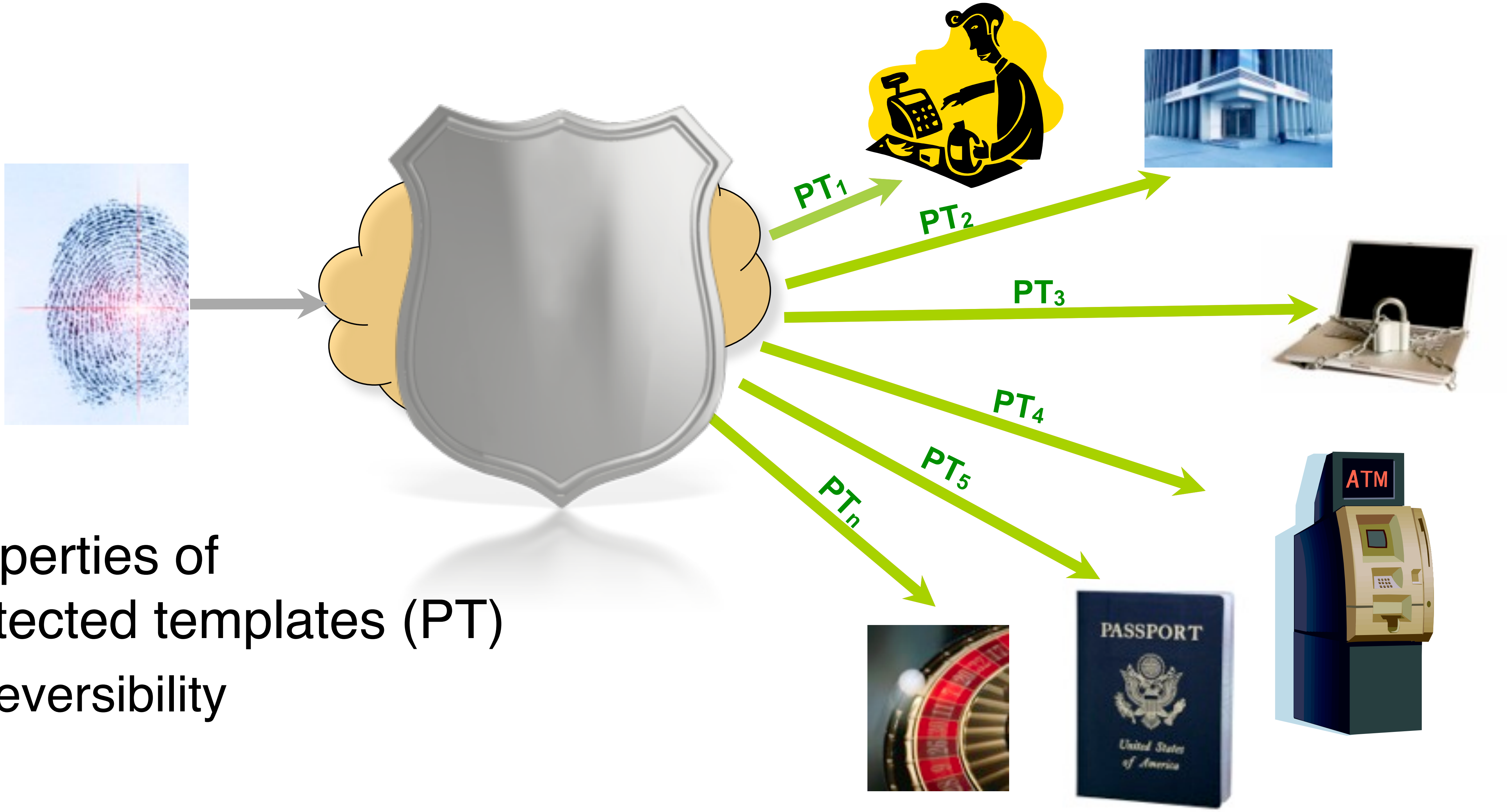


Biometric Template Protection



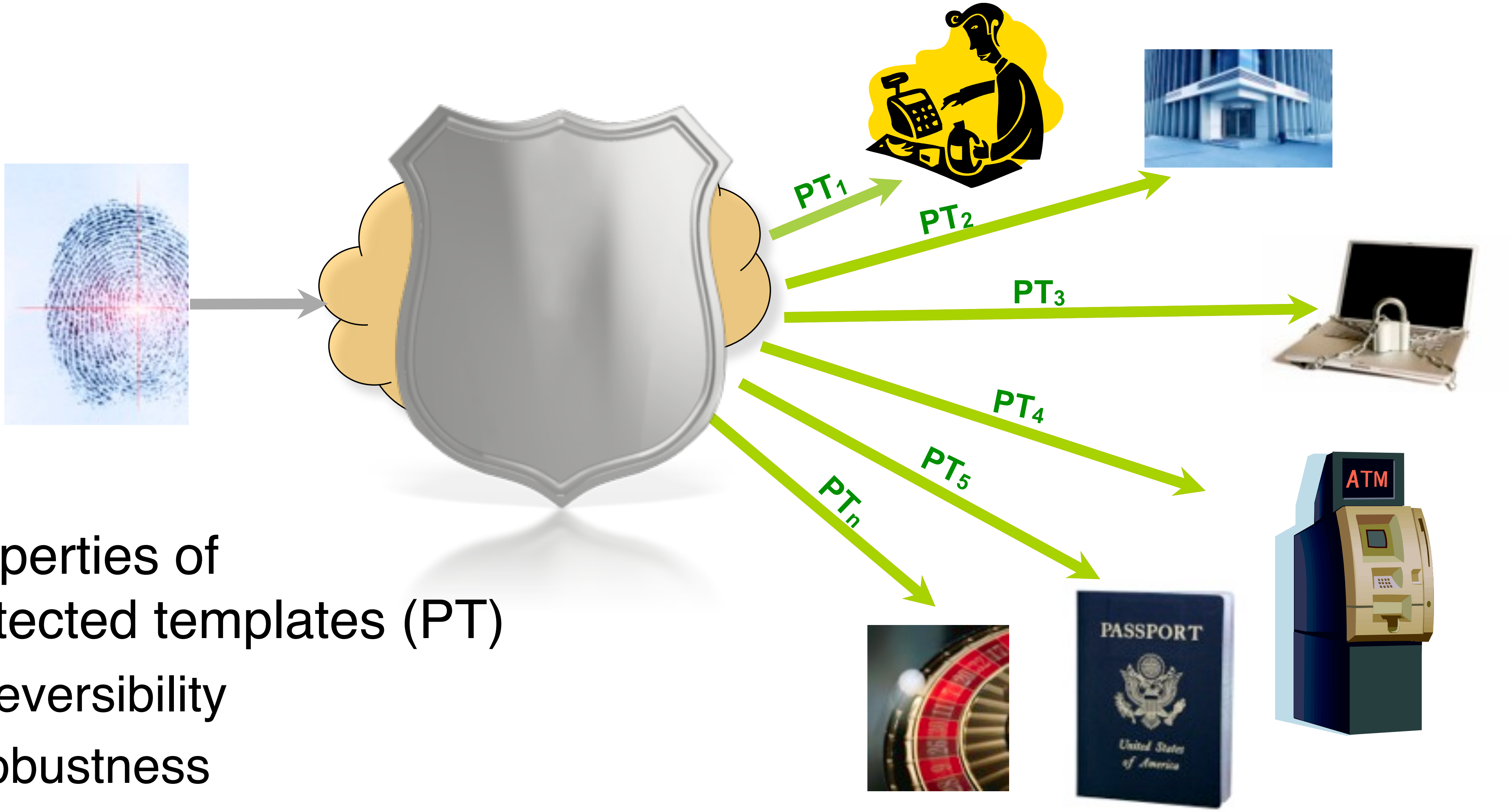
- Properties of protected templates (PT)

Biometric Template Protection



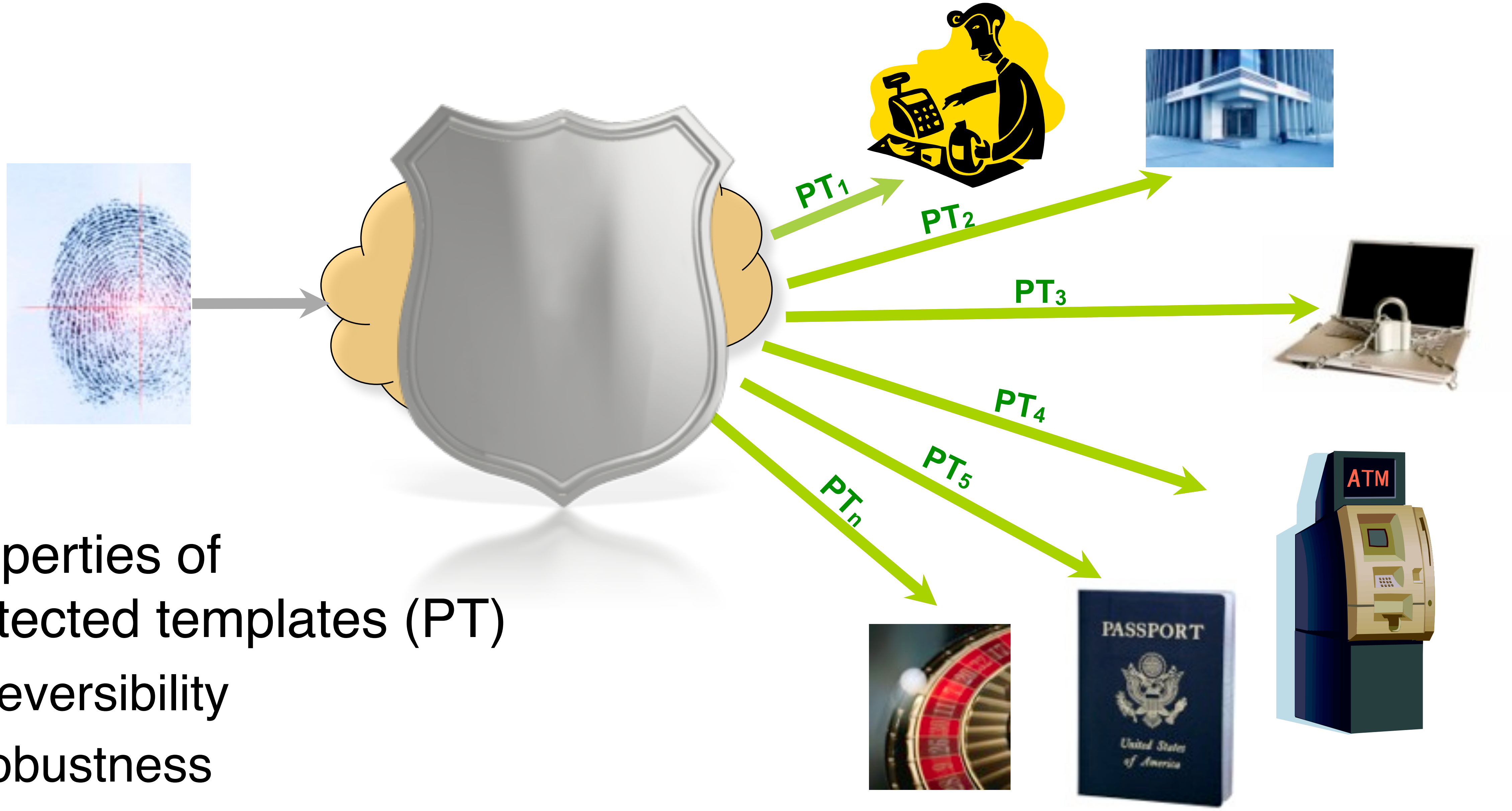
- Properties of protected templates (PT)
  - Irreversibility

Biometric Template Protection



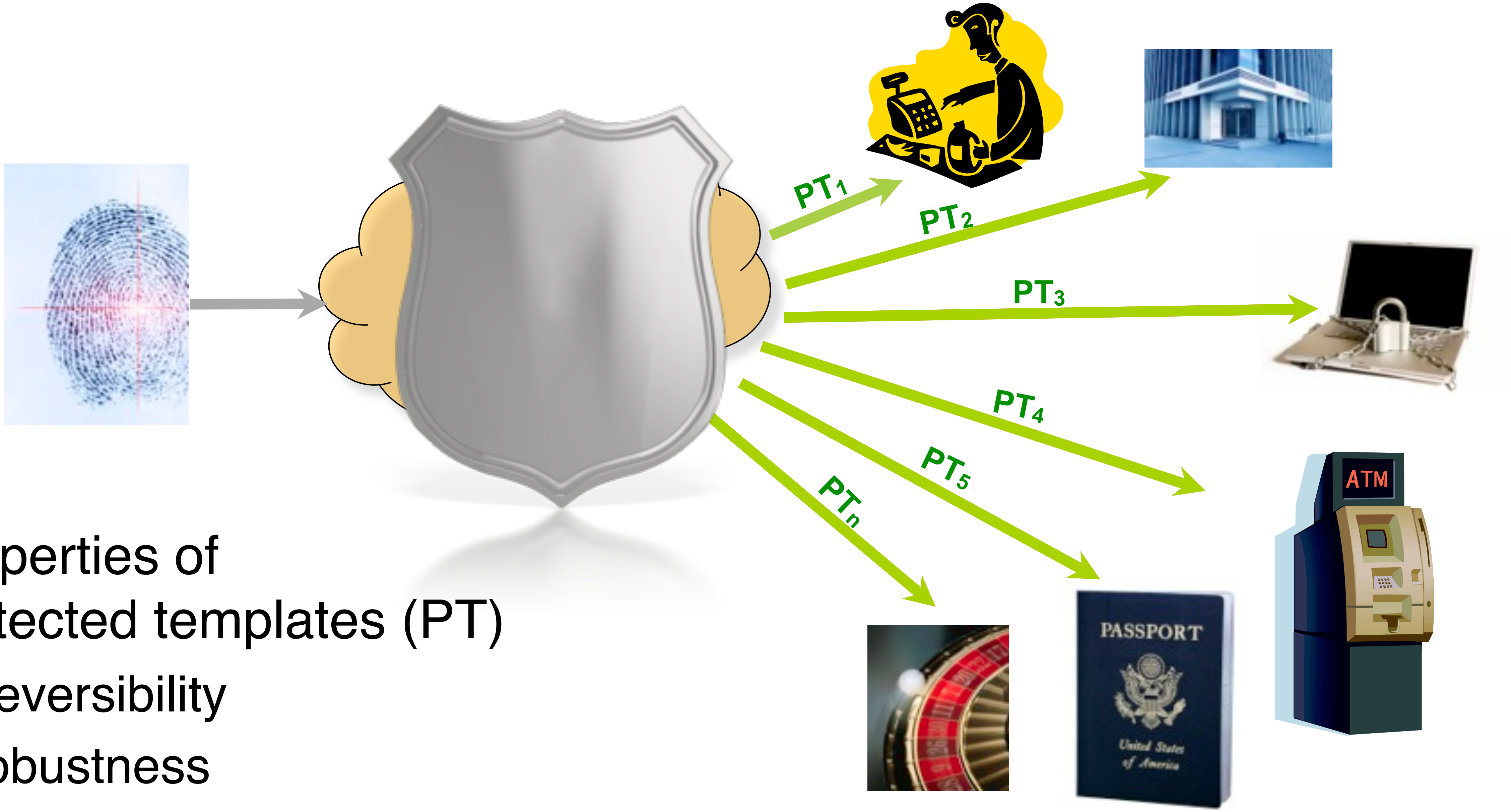
- Properties of protected templates (PT)
  - Irreversibility
  - Robustness

Biometric Template Protection



- Properties of protected templates (PT)
  - Irreversibility
  - Robustness
  - Diversity

Biometric Template Protection

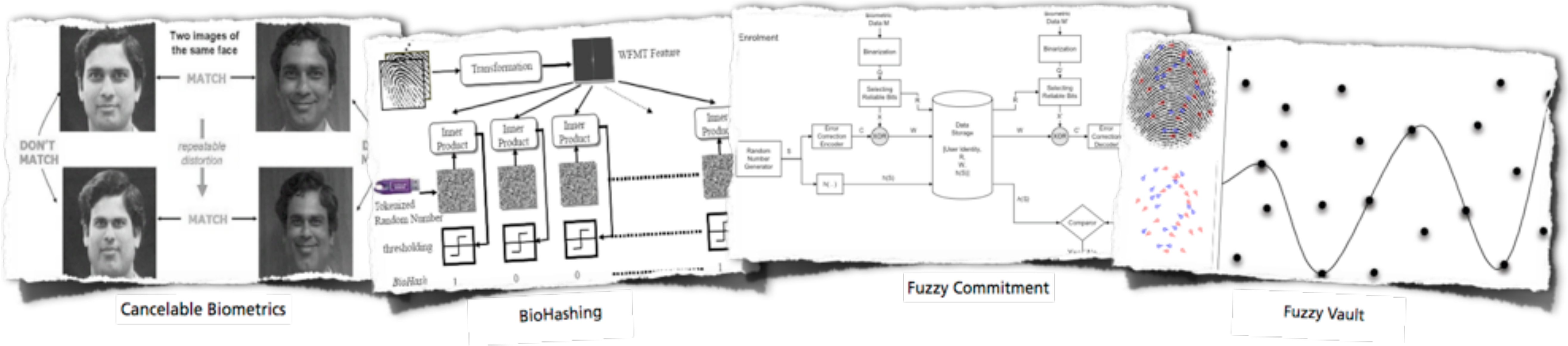


- Properties of protected templates (PT)
  - Irreversibility
  - Robustness
  - Diversity
  - Unlinkability

State of the Art of Template Protection

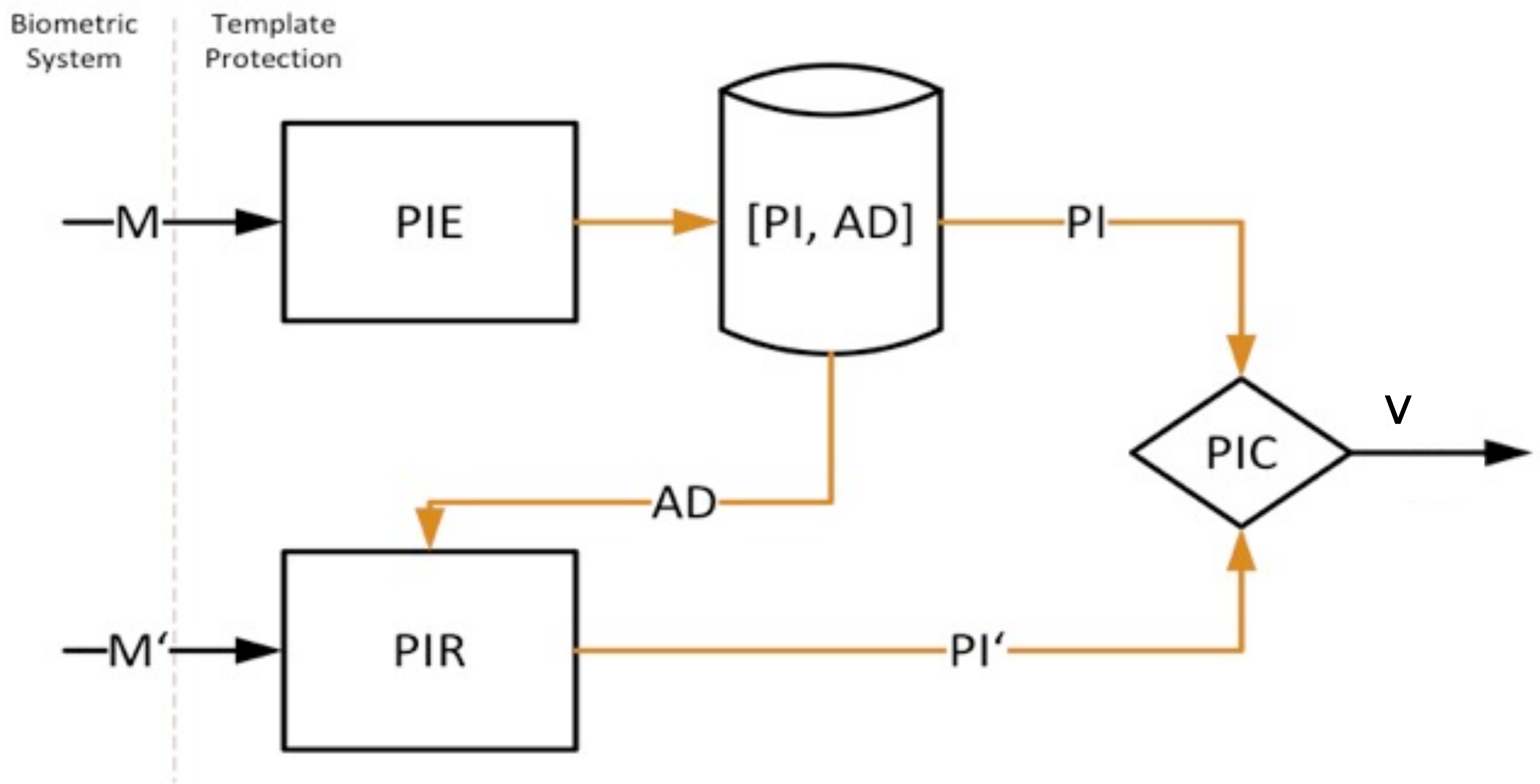
- Transformation-based algorithms
  - Biometric salting
    - Biometric encryption [Soutar99, Savvides04, Takaragi07 etc.]
    - Biohashing [Teoh04, Teoh09, Ao09 etc.]
  - Cancelable biometrics [Ratha01, Zuo08, Bolle09 etc.]

- Biometric cryptosystems
  - Fuzzy extractor [Dodis03]
    - Fuzzy commitment scheme [Juels99]
    - Helper data scheme [Tuyls04]
    - Fuzzy vault scheme [Juels02]
  - Quantization index modulation [Linnartz03, Buhan08]



Biometric Template Protection

ISO Architecture*



- Pseudonymous Identifier Encoder *(PIE)*: *[PI, AD] = PIE(M)*, *M* is observed biometric data in enrolment
- Pseudonymous Identifier Recorder *(PIR)*: *[PI'] = PIR(M', AD)*, *M'* is probe biometric data
- Pseudonymous Identifier Comparator *(PIC)*: *v = PIC (PI , PI')*, *v* is comparison result
- Stored protected template *[PI, AD]*, where *PI* is pseudonymous identifier and *AD* is auxiliary data

** ISO/IEC 24745 (2011) Information technology - Security techniques - Biometric Information protection*

How to Assess Template Protection

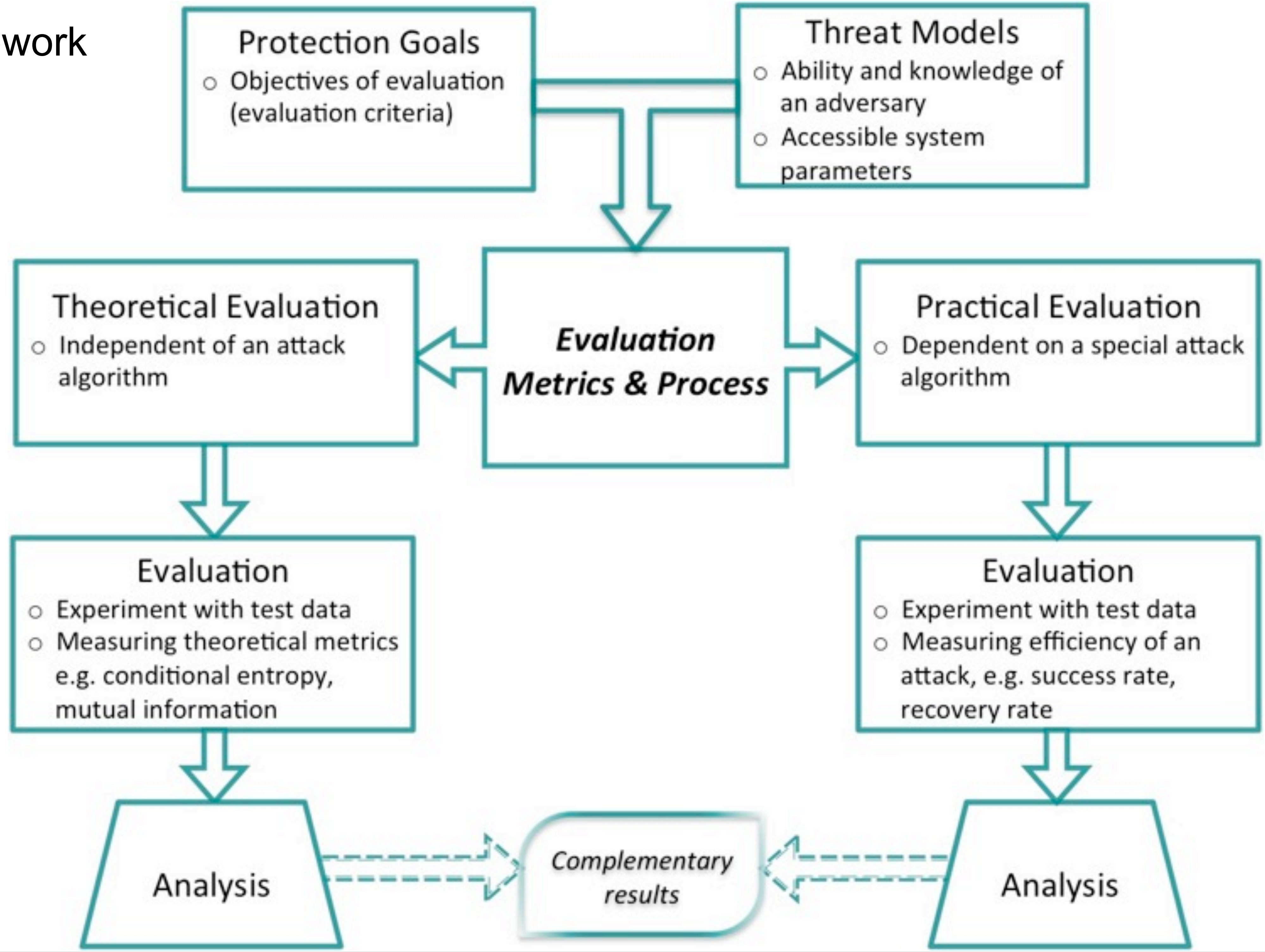
- Protection goals - Evaluation criteria
  - Security of *PI*: Hardness to find an M^* ("pre-image" of *PI*), which can pass *PI*- verification process
  - Privacy protection ability:
    - Irreversibility: Hardness to find an M^*, which is very close to the original M
    - Privacy leakage: Information about M contained in protected templates
  - Unlinkability:
    - Cross matching: Personal identifiable information contained in protected templates
    - Leakage amplification: Additional information about M or pre-image of *PI* gained when combining protected templates of the same subject

How to Assess Template Protection

- Threat models - description of an adversary
  - Naive Model: Adversary has no information about the system
  - Advanced Model: Adversary has full knowledge of the algorithm (Kerckhoffs' principle) and properties of biometric data
  - Collision Model: Adversary owns a large amount of biometric data and can exploit inaccuracies of the biometric system
- Distribution of biometric features
  - Important a priori information for an adversary
  - Essential for security and privacy assessment

How to Assess Template Protection

Evaluation framework

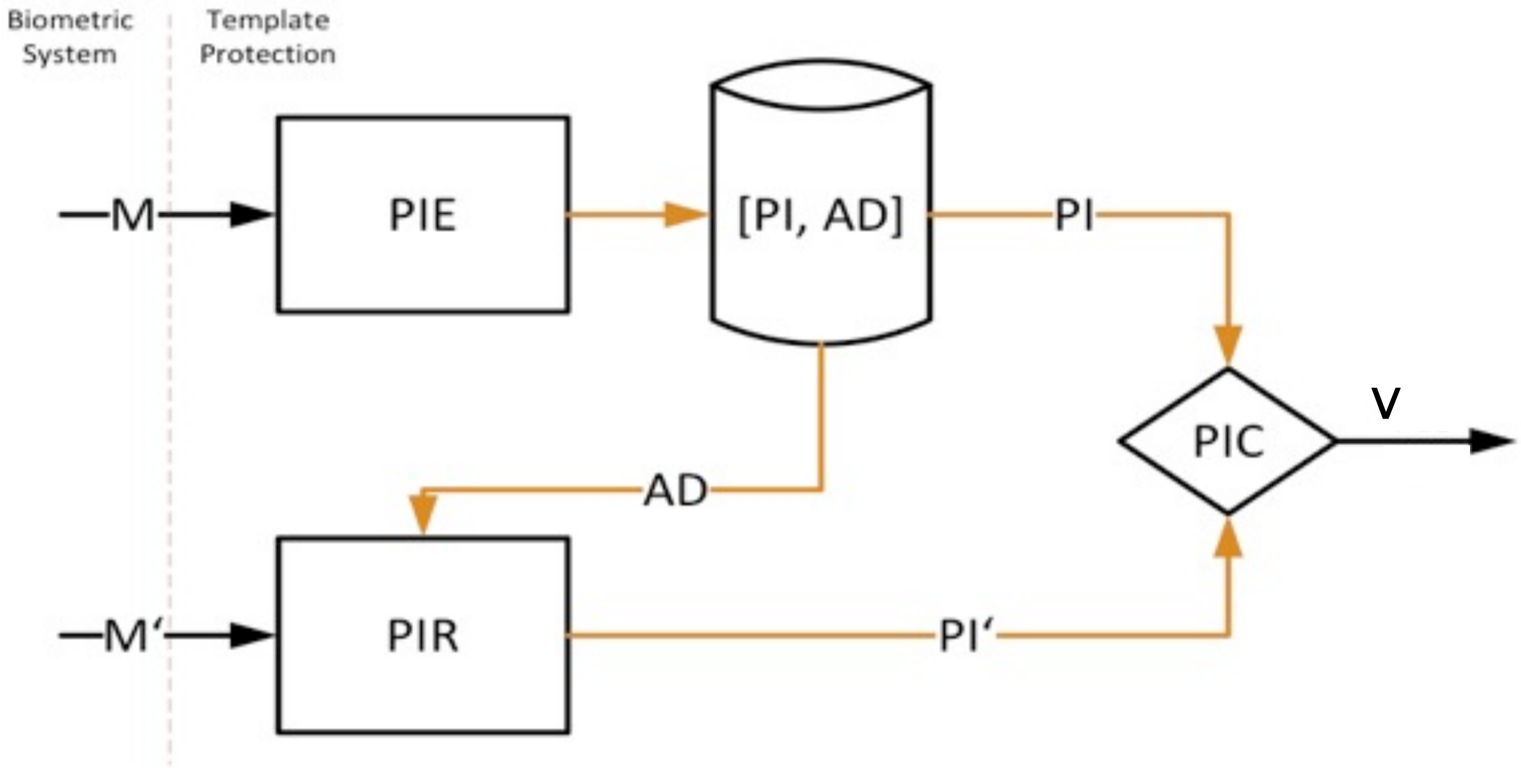

Protection Goals
○ Objectives of evaluation (evaluation criteria)
Threat Models
○ Ability and knowledge of an adversary
○ Accessible system parameters
Theoretical Evaluation
○ Independent of an attack algorithm
Evaluation Metrics & Process
Practical Evaluation
○ Dependent on a special attack algorithm
Evaluation
○ Experiment with test data
○ Measuring theoretical metrics e.g. conditional entropy, mutual information
Evaluation
○ Experiment with test data
○ Measuring efficiency of an attack, e.g. success rate, recovery rate
Analysis
Complementary results
Analysis

How to Assess Template Protection

- Definition of security:
  - Let $A(AD, PI)=[M', PI']$ be a reconstruction function, where $PI'=PIR(M', AD)$. T_A is the computational time required in one reconstruction and n is the average number of reconstructions needed to get a $[M', PI']$ such that $PIC(PI,PI')=1$ for a positive authentication result.
  - Then, a template protection algorithm is (T, ε)**- *secure***, if for all A

$$T_A \geq T$$

$$\log_2 n \geq \varepsilon$$

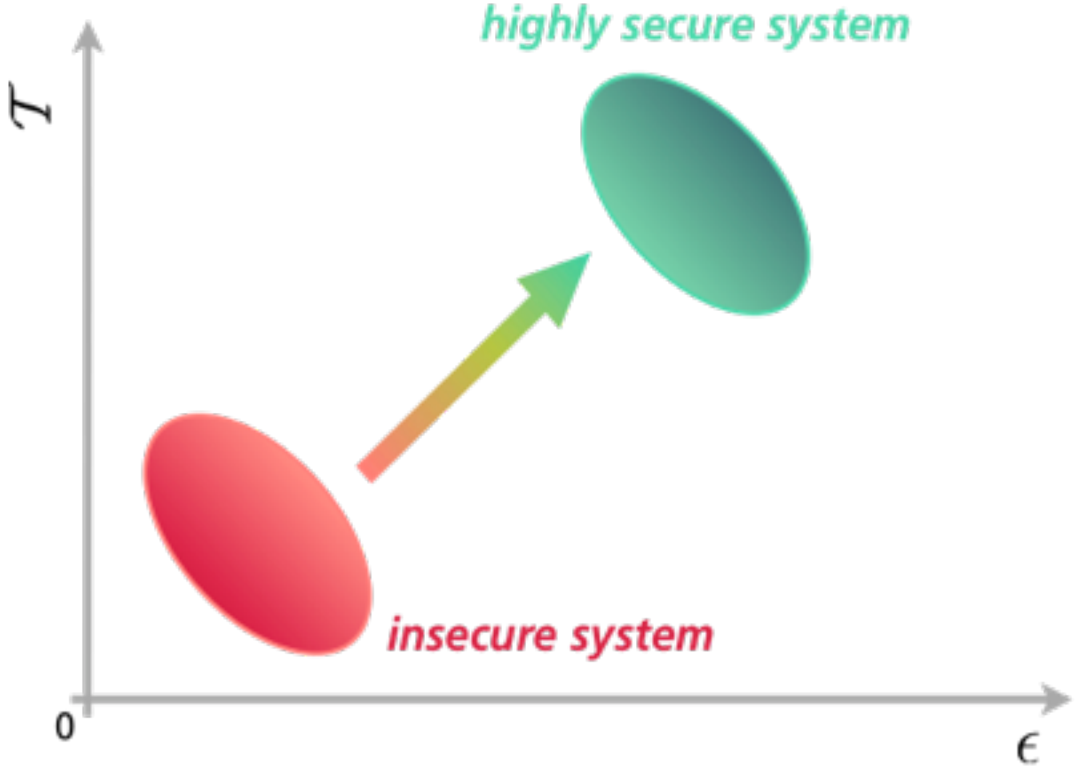


How to Assess Template Protection

- Definition of security:
  - Let $A(AD, PI)=[M', PI']$ be a reconstruction function, where $PI'=PIR(M', AD)$. T_A is the computational time required in one reconstruction and n is the average number of reconstructions needed to get a $[M', PI']$ such that $PIC(PI,PI')=1$ for a positive authentication result.
  - Then, a template protection algorithm is (T, ε)**- secure**, if for all A

$$T_A \geq T$$

$$\log_2 n \geq \varepsilon$$



How to Assess Template Protection

- Definition of security:
  - Let $A(AD, PI)=[M', PI']$ be a reconstruction function, where $PI'=PIR(M', AD)$. T_A is the computational time required in one reconstruction and n is the average number of reconstructions needed to get a $[M', PI']$ such that $PIC(PI,PI')=1$ for a positive authentication result
  - A template protection algorithm is $(\boldsymbol{T}, \boldsymbol{\varepsilon})$**- *secure***, if for all A

$$T_A \geq T$$

$$\log_2 n \geq \varepsilon$$

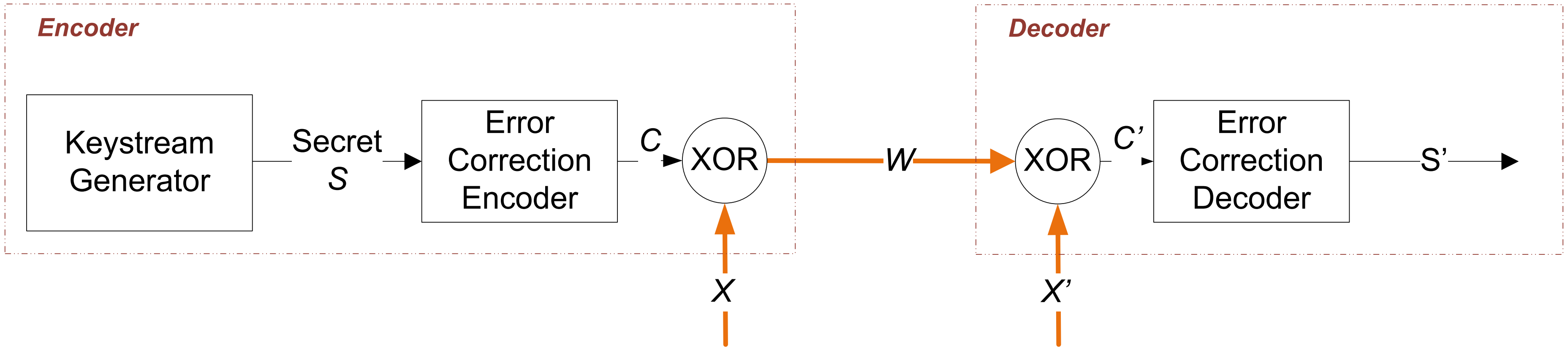
- Definition of privacy:
  - Let $A(AD, PI)=[M', PI']$ be a reconstruction function, where $PI'=PIR(M', AD)$. T_A is the computational time required in one reconstruction; for a given threshold t, n is the average number of reconstructions needed to get a $[M', PI']$ such that for a distance function $dist(M, M')<t$
  - A template protection algorithm is $(\boldsymbol{t}, \boldsymbol{T}, \boldsymbol{\varepsilon})$**- *preserving***, if for all A

$$T_A \geq T$$

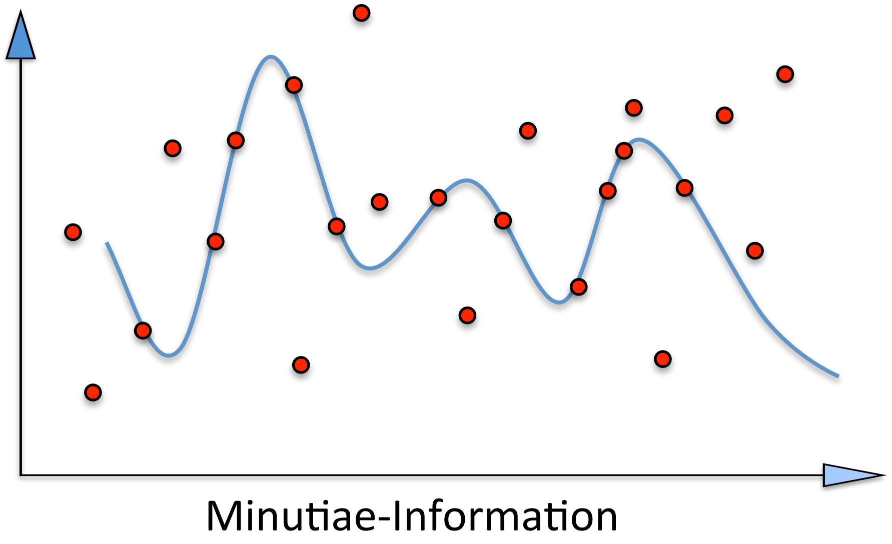
$$\log_2 n \geq \varepsilon$$

Assessment of Different Protected Systems

- The fuzzy commitment scheme for 3D face recognition
- The fuzzy commitment scheme for iris recognition



- The fuzzy vault algorithm for fingerprint recognition



Assessment of Different Protected Systems

- Security assessment

		Naive Model		Advanced Model		Collision Model	
System	L_S	$\varepsilon = L_S - 1$	T	ε	T	$\varepsilon = -\log_2(FAR)$ $FAR@FRR$	**Ranking**
3D Face Fuzzy Commitment	71 bit	70	$O(1)$	11.13	$O(1)$	6.48 1.12%@19.97%	🙁
Iris Fuzzy Commitment	72 bit	71	$O(1)$	14.25	$O(1)$	7.41 0.59%@22.74%	😐
*Fingerprint Fuzzy Vault**	128 bit	127	$O(1)$	34.54	$O(n \log^2(n))$	13.29 0.01%@9%	🙂

* "Fingerprint-Based Fuzzy Vault: Implementation and Performance", Nandakumar, Jain and Pankanti, IEEE Trans. on Info. Forensics and Security, 2007

Assessment of Different Protected Systems

CASED

- Privacy protection ability in the advanced model:
  - High privacy leakage, which can cause cross matching and leakage amplification
  - Irreversibility is measured with the privacy definition for t=0. It shows computational complexity to retrieve the original biometric features

System	L_S	Privacy leakage	Irreversibility	
			ε	T
3D Face Fuzzy Commitment	71 bit	77.5 bit	74.2 bit	$O(1)$
Iris Fuzzy Commitment	72 bit	4311 bit	14.25 bit	$O(1)$
*Fingerprint Fuzzy Vault**	128 bit	892.59 bit	34.54 bit	$O(n \log^2(n))$

* "Fingerprint-Based Fuzzy Vault: Implementation and Performance", Nandakumar, Jain and Pankanti, IEEE Trans. on Info. Forensics and Security, 2007

Assessment of Different Protected Systems

- Unlinkability in the advanced model:
  - Cross matching is a serious problem
  - It should be avoided to use any personal identifiable information in the systems
  - Additionally, the privacy leakage is unavoidable in these system due to error tolerance, but it should be minimized

System	Cross matching	Leakage Amplification
3D Face Fuzzy Commitment	☹ EER=5%	😐 no feasible attack yet
Iris Fuzzy Commitment	☹ EER =16.34%	🙂
*Fingerprint Fuzzy Vault**	☹ no assessment in the paper	☹ no assessment in the paper

* "Fingerprint-Based Fuzzy Vault: Implementation and Performance", Nandakumar, Jain and Pankanti, IEEE Trans. on Info. Forensics and Security, 2007

Conclusions

- The framework is useful to detect vulnerabilities of the existing algorithms
- The framework enables rigorous assessment, which is important and necessary for the development of template protection
- All the protection goals need to be taken into account
- Threat models are the important prerequisites. Security and privacy protection ability of a system can be overestimated, if unrealistic assumption is made
- Unique and measurable metrics such as the metrics used in the security and privacy definitions, are necessary for ranking of different algorithms

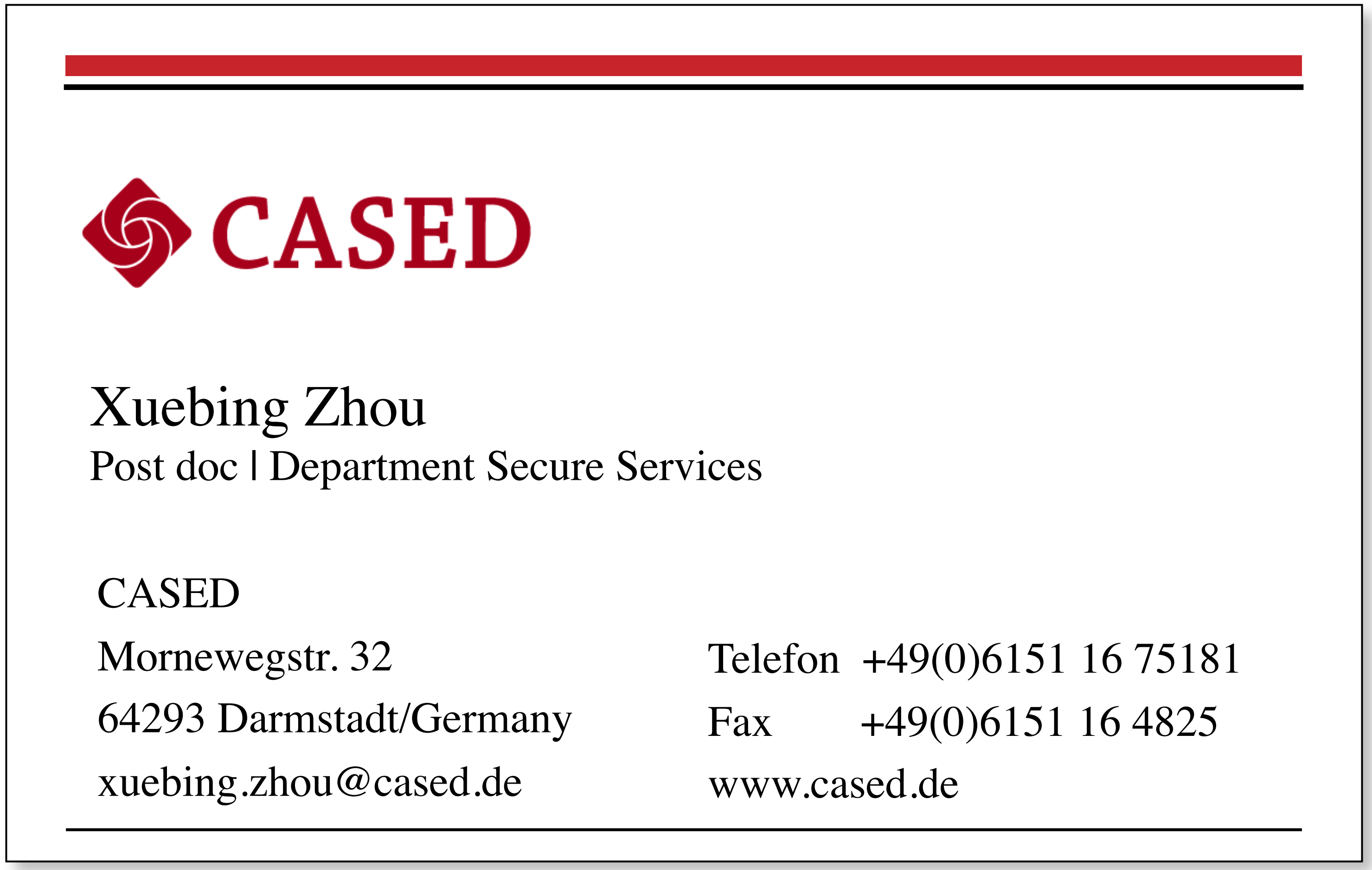
Future Work

- Universal and constructive criteria, which can guarantee security and privacy performance of template protection
- An extended evaluation including both security and recognition performance
- Benchmarking and certification for template protection

References

- Zhou, Xuebing: “Privacy and Security Assessment of Biometric Template Protection”, PhD thesis, Technische Universität Darmstadt, Germany, 2011

- Zhou, Xuebing; Kuijper, Arjan; Busch, Christoph: Cracking Iris Fuzzy Commitment In: IEEE the International Conference on Biometrics (ICB 12), 2012
- Zhou, Xuebing; Kuijper, Arjan; Veldhuis, Raymond; Busch, Christoph: Quantifying Privacy and Security of Biometric Fuzzy Commitment In: IEEE the International Joint Conference on Biometrics (IJCB 11), 2011



Xuebing Zhou
Post doc | Department Secure Services

CASED
Mornewegstr. 32
64293 Darmstadt/Germany
xuebing.zhou@cased.de

Telefon +49(0)6151 16 75181
Fax +49(0)6151 16 4825
www.cased.de