EEE-6561 Fundamentals of Biometric Identification

April 18th, 2018

Lecture #19: Biometric Template Protection

Damon L. Woodard, Ph.D.
Dept. of Electrical and Computer Engineering
dwoodard@ece.ufl.edu

Biometric Template Protection

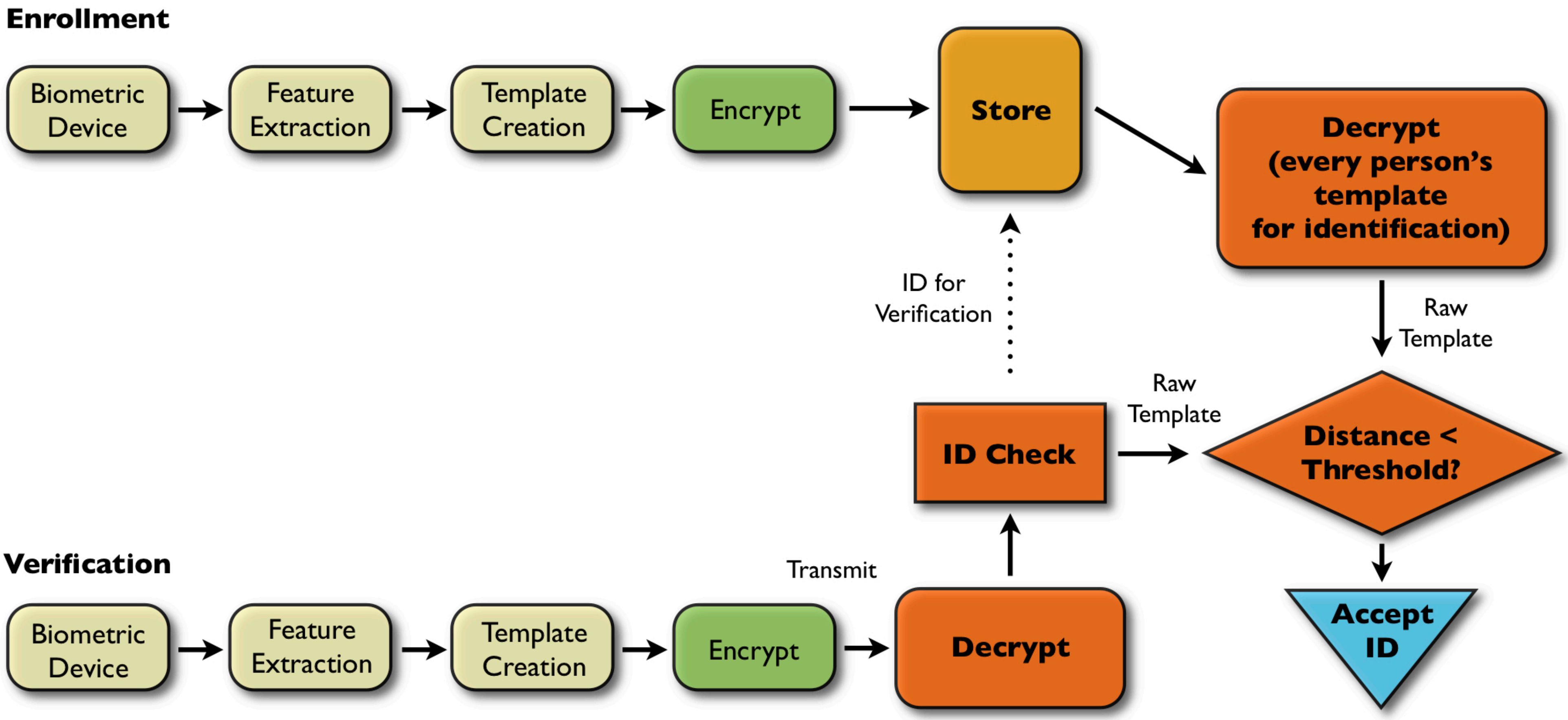
Hashing/Crypto great for passwords

Hire Only IEEE Members	1fc486d4b30dd490e044e40a35b6535c
Fire Only IEEE Members	53cc18345f93c390c7469e38c126a13f
Hire Only IEE Members	dfa9d634376d51d311ee55d40722950c

Minor Change results is radically different crypto string
(no match)

What does this suggest about potential for Biometrics?

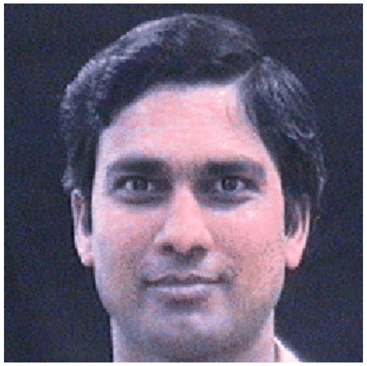
Standard cryptography as a weak solution

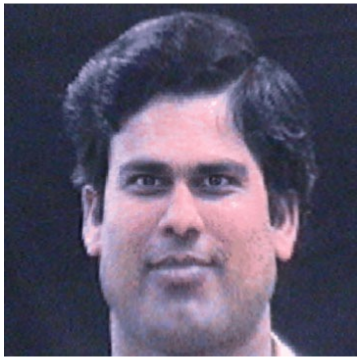


Cancelable biometrics: Non-invertible transforms

Very early work in face template protection by IBM

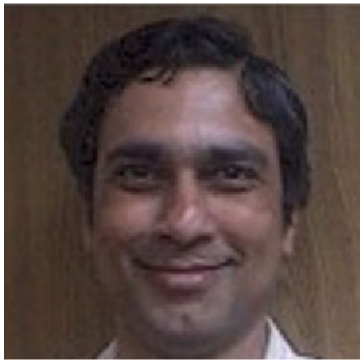
Original Image 1

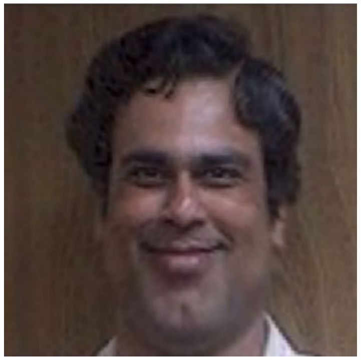




Intentional Distortion

Original Image 2





Same Intentional Distortion

N. Ratha, J. Connell, and R. Bolle. Enhancing Security and Privacy in Biometrics- based Authentication Systems. IBM Systems Journal, 40(3):614-634, 2001.

Basic revocability requirements

- Match while encoded
    - Tokens are matched in their secure encoded form, without decoding/decrypting.
- Cryptographically secure
    - Prevent recovery of individual identity or data that matches against another of the user’s tokens.

Basic Revocability Requirements

- Non-linkable revocability
  - Transform biometric data, such that an individual's biotokens made with different keys do not match and are not linkable.
  - The number of distinct non-matching forms must be extremely large (e.g., number of allowed integers)
  - Ideally protect from linking biotokens across uses of the same application at different time.

Basic Revocability Requirements

- How do we “revoke” a template?
    - Work in this area must address what it means and what is a process to revoke and reissue
- Reissue must be simple/easy/cost effective
- If re-issue means people must re-enroll, no company will “revoke”
- Ideally should support per-transaction tokens that are revoked after a single use

Security Basics for Template Protection

Template Protection as a Solution

- Protect the Privacy and Security of the Biometric Features
- Revoke and re-issue biometric templates like a password or credit card #
- Match in an encoded space
- Prevent linking across databases (solve the biometric dilemma)
- Prevent the doppelganger attack (multi-factors)

“Getting this right has been much more challenging than we first thought.” – Fabian Monrose

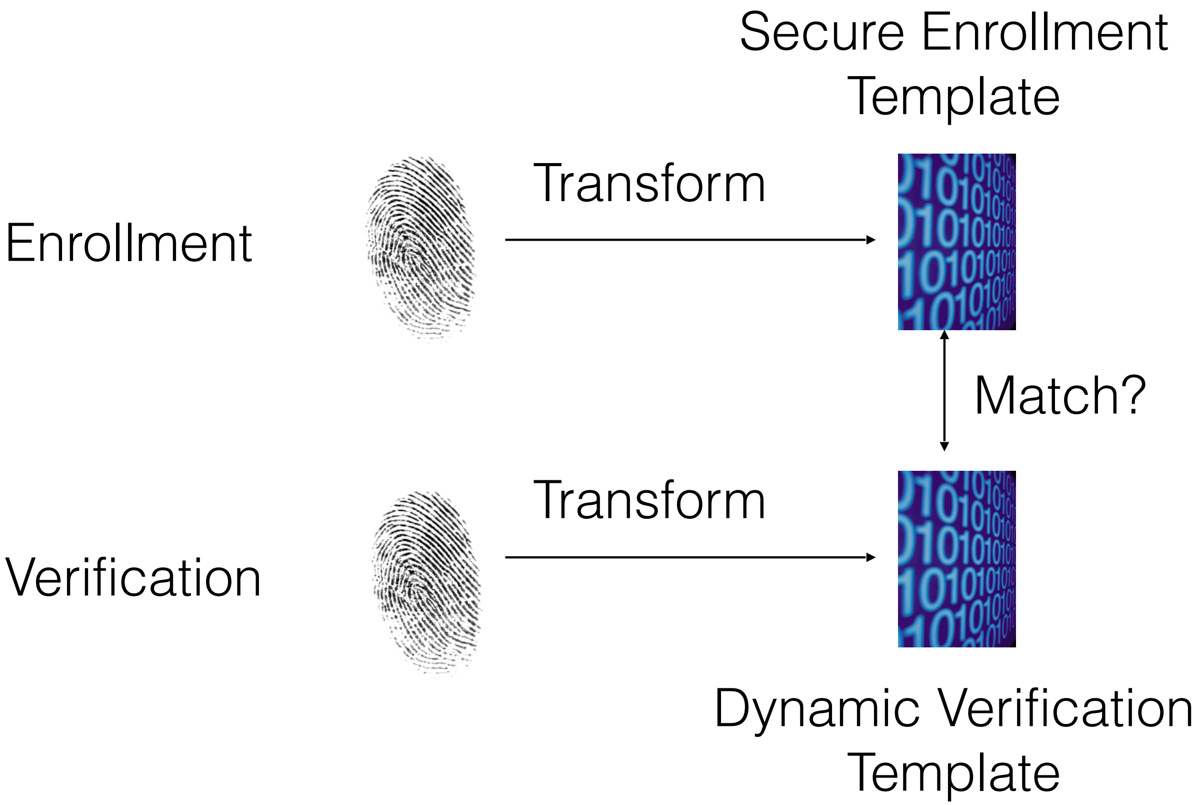
General Categories

- Straight feature protection encrypt feature
- Key-generating
- Key-binding

A. Jain, K. Nandakumar and A. Nagar, “Biometric Template Security”, in EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics, 2008

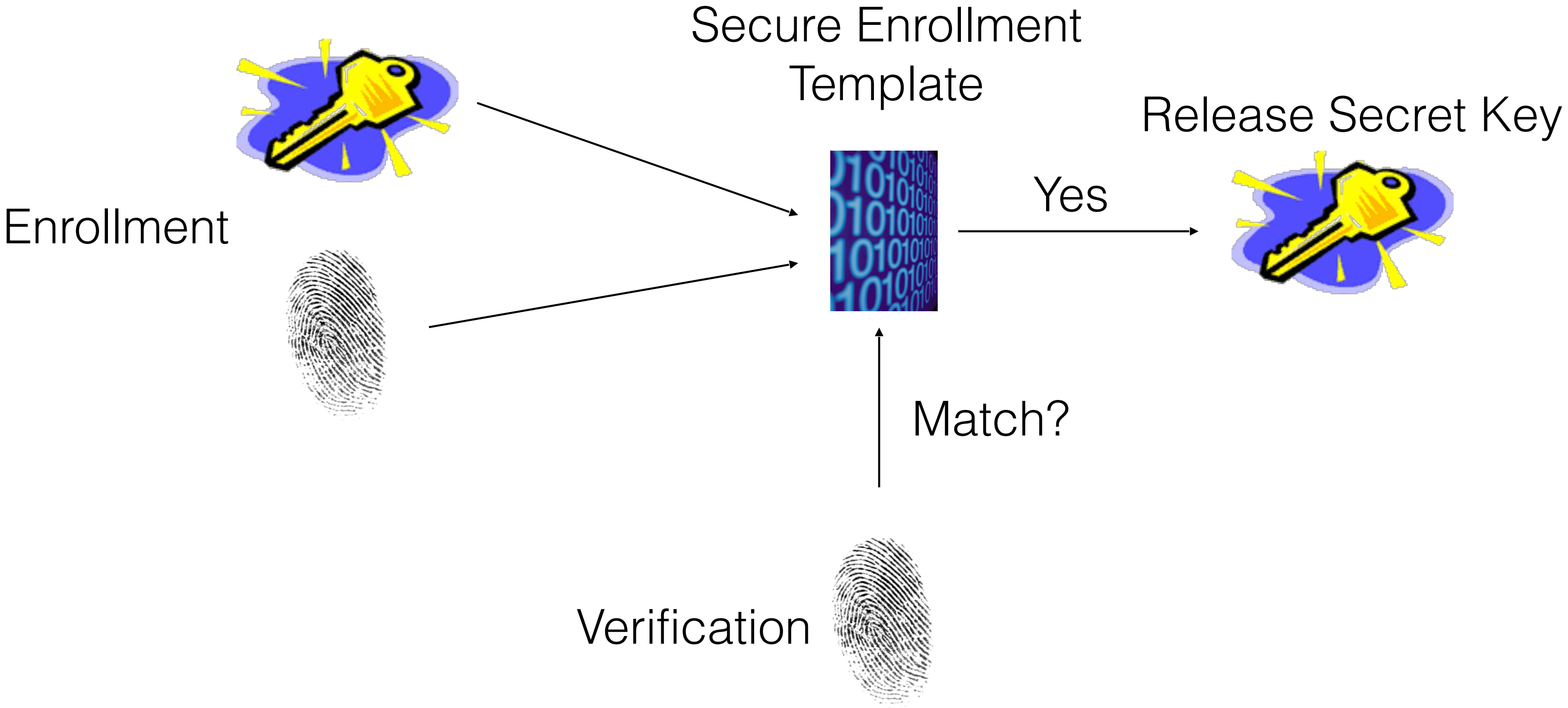
Straight Feature Protection

Simply protect the original biometric features using some transformation that allows matching in encoded space



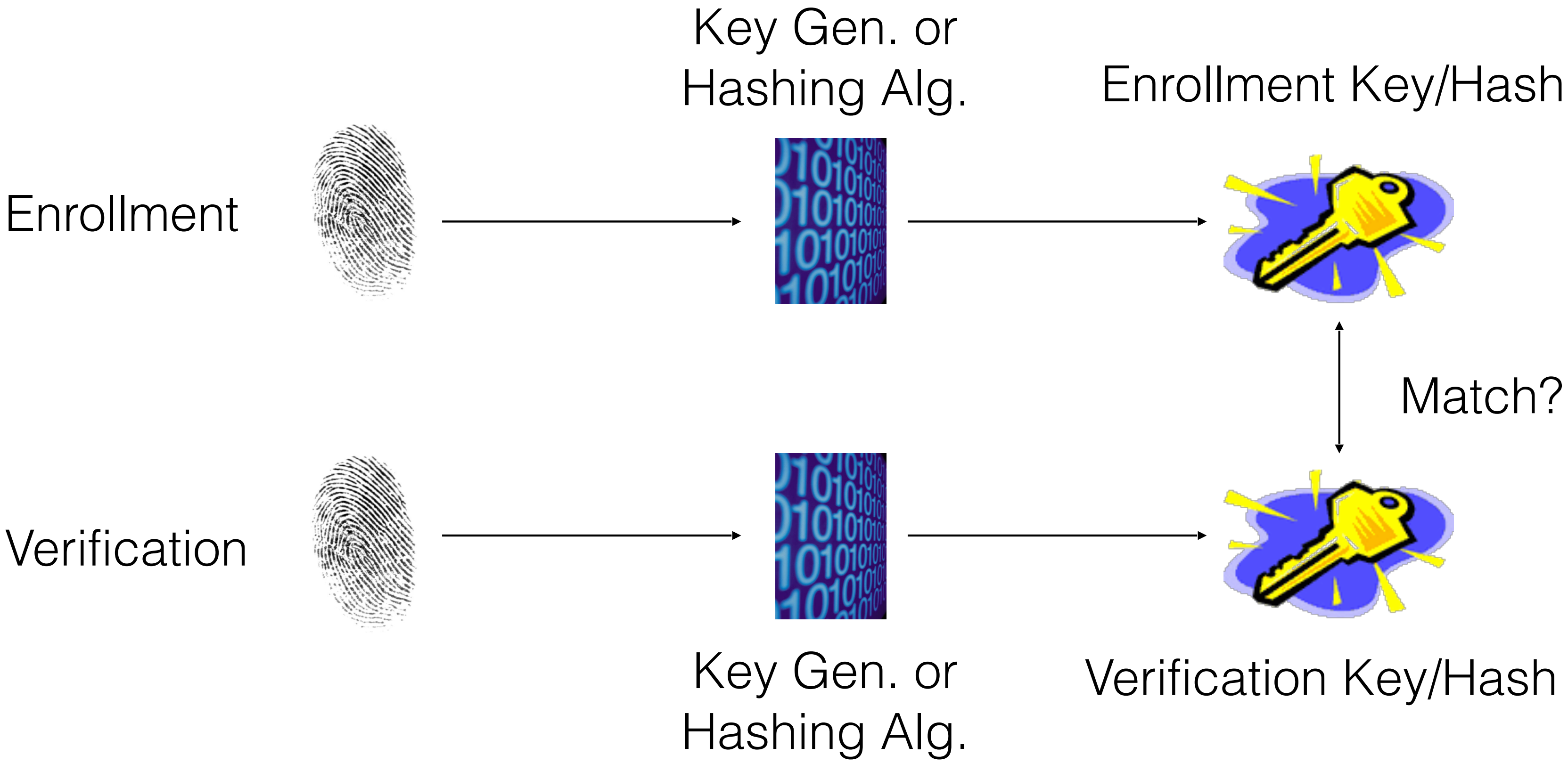
Key-binding

Biometric cryptosystem that binds key data with the biometric data



Key-generating

Biometric cryptosystem that derives a key from the biometric data

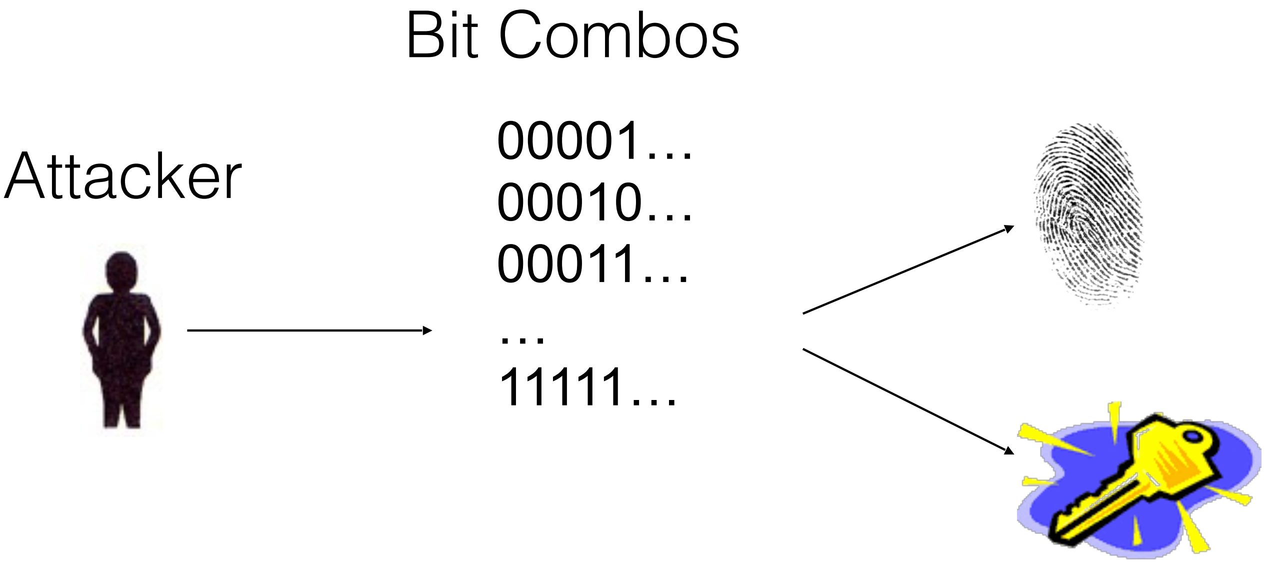


Attacks Against Secure Template Protection Technologies

- Basic Brute Force
- Correlation Attack
- Known Key Attack
- Doppelganger Attack
- Hill Climbing

Basic Brute Force

- Attacker tries every possible bit combination till they guess the correct original feature data or key
  - Need a way to test each bit combo

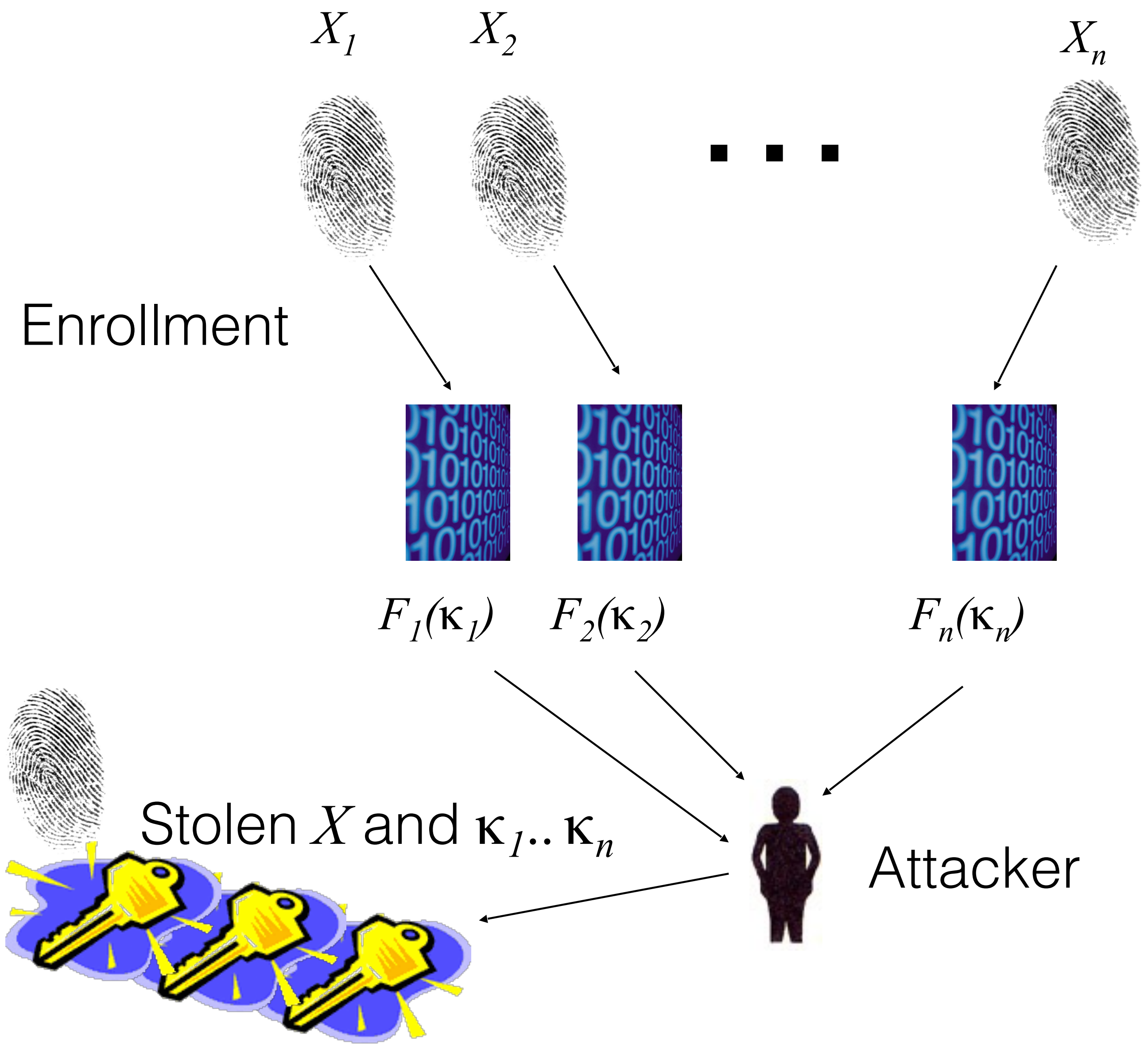


Bit Combos

Attacker

00001…
00010…
00011…
…
11111…

Correlation Attack



X_1 X_2 … X_n

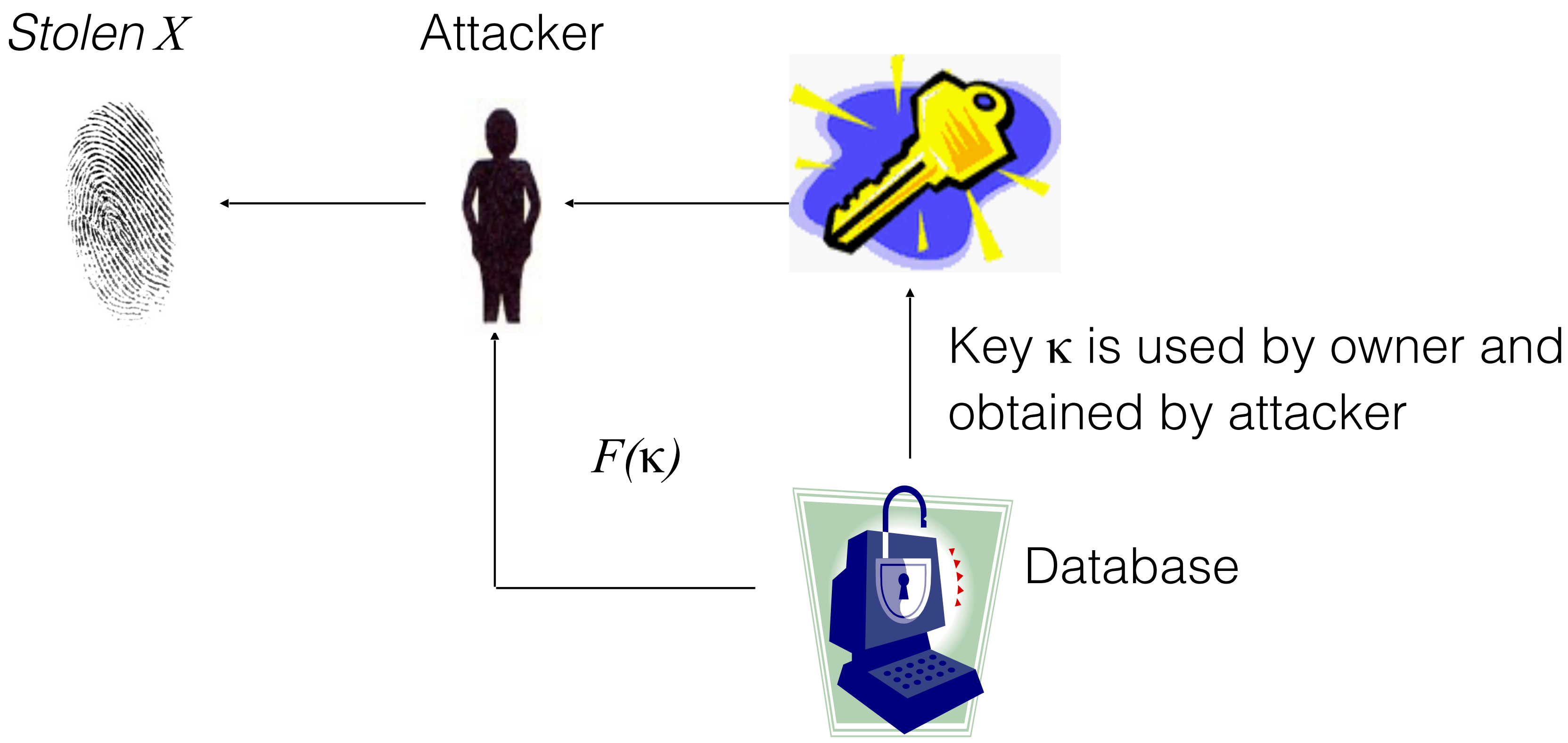
Enrollment

$F_1(\kappa_1)$ $F_2(\kappa_2)$ $F_n(\kappa_n)$

Stolen X and $\kappa_1 .. \kappa_n$

Attacker

Known Key Attack



Stolen X

Attacker

Key κ is used by owner and obtained by attacker

$F(\kappa)$

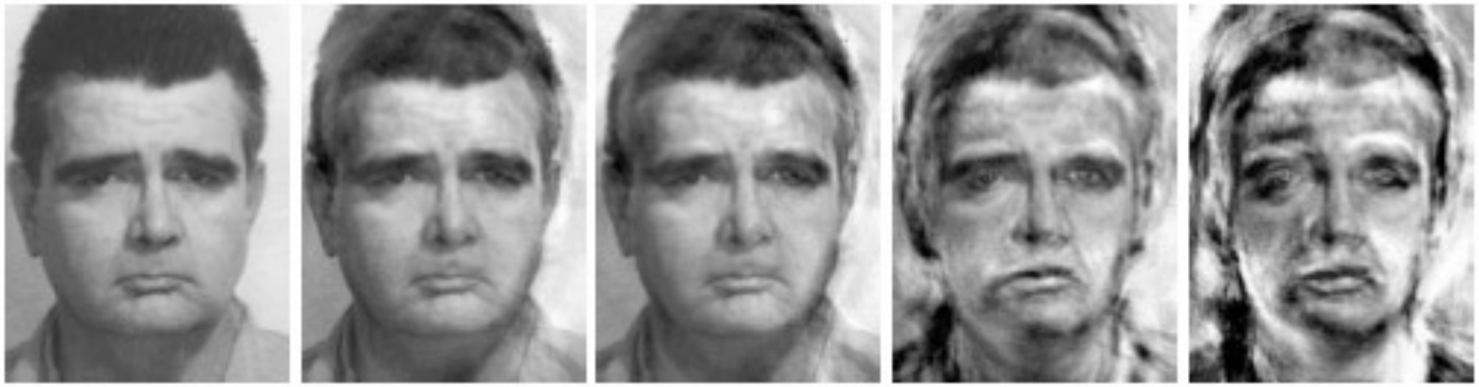
Database

The Doppelganger Threat

- If the FAR is 1 in *X*, then an attacker can try more than *X* different prints
- Lots of public data available!
  - Fingerprint: NIST DB 14, NIST DB 29, FVC 2002, FVC 2004 …
  - Face: MBGC, FRGC, FVT, FERET…
  - Think of this as a biometric dictionary attack

Hill Climbing

- Requires less than brute-force effort to recover an embedded secret
- Provides an estimate of the enrollment image



In an iterative fashion, modifications are made to the input, and those that increase the match score are retained.

Questions?

Slide Credits

Material used from Introduction to Biometrics text authors Arun Ross and Anil Jain as well as Walter Scheirer