Revocable Biometrics

Francisco Corella
fcorella@pomcor.com
Karen Lewison
kplewison@pomcor.com

Traditional Biometrics

Enrollment:

- Enrollment sample (raw data, e.g. bitmap) => Enrollment code (features) =>
- Template

Authentication:

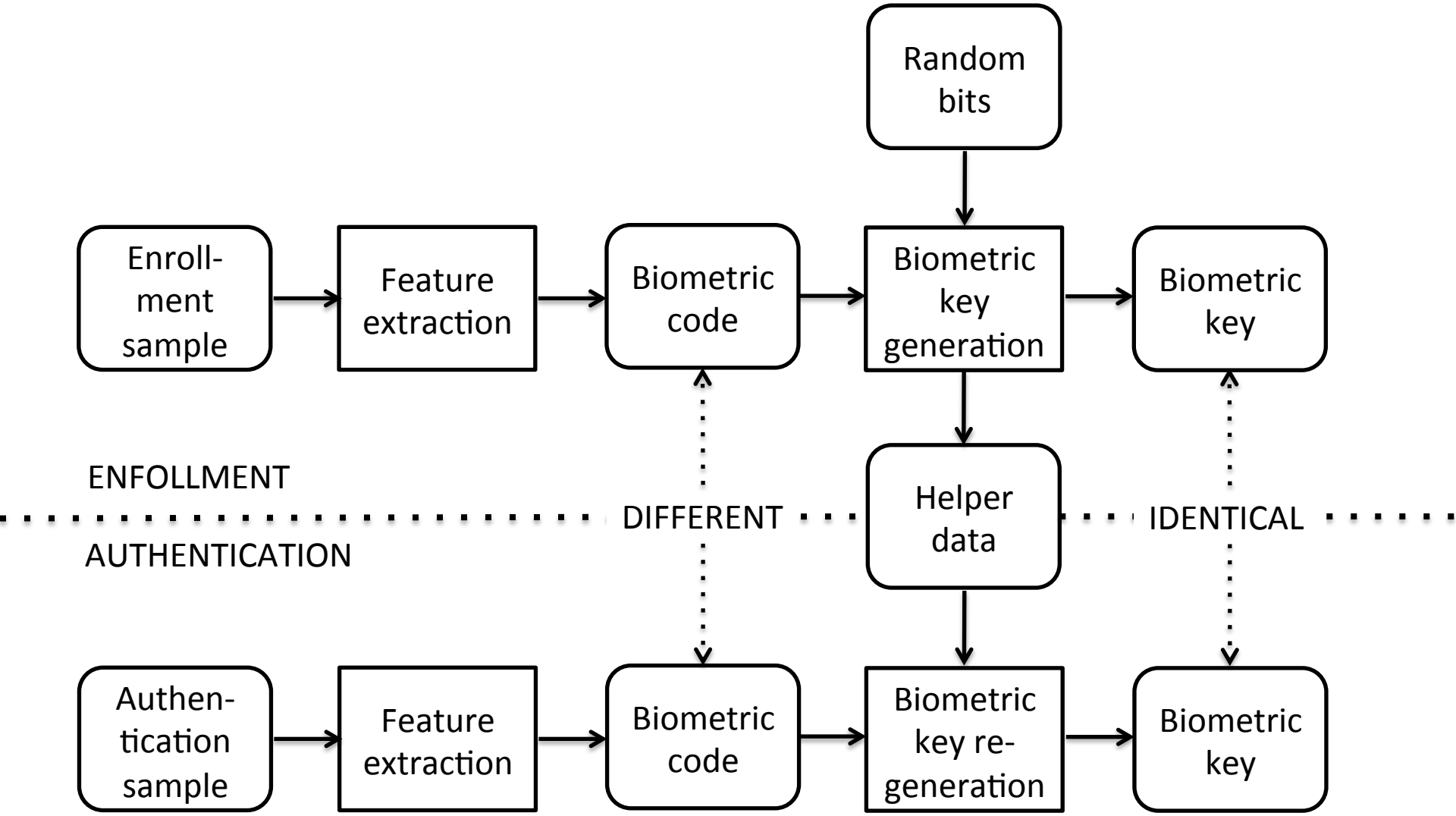
- Authentication sample => authentication code
- Match authentication code against template

Privacy Danger

- Template => sample that can be successfully matched against template
- Adversary who captures template can impersonate user
- User cannot recover from the compromise because the biometric credential is not revocable

Revocable Biometrics

- Enrollment
  - Enrollment sample (bitmap) => enrollment code (features)
  - Enrollment code + random bits => biometric key + helper data
  - Helper data is stored for use at authentication time
- Authentication
  - Authentication sample => authentication code
  - Authentication code + helper data => same biometric key if sample is genuine


Random bits
Enroll-ment sample
Feature extraction
Biometric code
Biometric key generation
Biometric key
ENFOLLMENT
DIFFERENT
Helper data
IDENTICAL
AUTHENTICATION
Authen-tication sample
Feature extraction
Biometric code
Biometric key re-generation
Biometric key

Revocable Biometrics, continued

- Biometric key can be used for authentication
  - As bearer token, or
  - As symmetric key that signs a challenge
- Biometric key and helper data can be revoked because they are randomized
- **AND**… no useful information can be obtained from the helper data

Revocable Biometrics Using Error Correction System

- Enrollment
  - Biometric key generated at random
  - Biometric key + redundancy => codeword
  - Enrollment sample => enrollment code
  - Enrollment code $\oplus$ codeword => helper data
- Authentication
  - Authentication sample => authentication code
  - Authentication code $\oplus$ helper data =
    authentication code $\oplus$ (enrollment code $\oplus$ codeword) =
    (authentication code $\oplus$ enrollment code) $\oplus$ codeword
    bits that differ $\oplus$ codeword
  - Error correction system can recover codeword if sample is genuine
  - Biometric key recovered by dropping redundancy from codeword

Best Result

- Hao, Anderson & Daugman, "Combining biometrics with cryptography effectively", IEEE Transactions on Computers 55(9), pages 1081-1088, 2006
  - Iris
  - 140-bit biometric key
- Reported experimental results:
  - 0.47% FRR
  - 0% FAR

Caveats

- Biometric key $\oplus$ helper data = biometric code
- Low entropy for modalities other than iris

Multifactor Authentication

- Low entropy for modalities other than iris can be addressed with MFA
- Example: 3FA
  - Biometric key
  - Password
  - Uncertified key pair

Enhanced 3FA

- Password deserves protection against security breach of a back-end database because it has intrinsic value if reused
- Joint hash method
  - Password hashed with public key and optionally with biometric key, rather than salt
  - Public key not stored in back-end
- Protocredential method
  - Password and biometric key not sent to back-end
  - Instead, they are used to regenerate an uncertified key pair from a protocredential

Thank you for your attention!

For more information:
Web site: pomcor.com
Blog: pomcor.com/blog

Francisco Corella
fcorella@pomcor.com
Karen Lewison
kplewison@pomcor.com

Any questions?