Bio-Cryptosystem for Authentication

Dr. Rajarshi Pal
Assistant Professor
Institute for Development and Research in Banking Technology (IDRBT)
Hyderabad, India

Outline

- Authentication (User)
- Cryptosystem for Authentication
- Bio-cryptosystem
  - Protecting cryptographic key using biometrics
  - Cryptographic key generation using biometrics

User Authentication

Authentication Factors

- Knowledge Factor
  - Password, PIN, Challenge Response, Security Question
- Ownership Factor
  - ID card, token (software/hardware), Mobile number, mobile phone, MAC Address, PC
- Inherence Factor
  - Signature, Fingerprint, retinal pattern, voice and other biometric identifiers

Bad Password Management: Equifax Argentina Case

- Identified on September, 2017
- One of Equifax Argentina's web portal had the following user name and password:

User name: admin

Password: admin

- Using the above credentials one can access to records of 14000 customers and more than 100 staff members.

Password Vulnerabilities

- Social Engineering Attack (Phishing, Vishing etc)
- Shoulder Surfing Attack
- Exploiting multiple use of the password
- Database breaches
- Malware (keylogger, screenlogger)
- Rainbow table attack
- Guessing
  - Based on user
  - Dictionary attack
  - Brute force attack

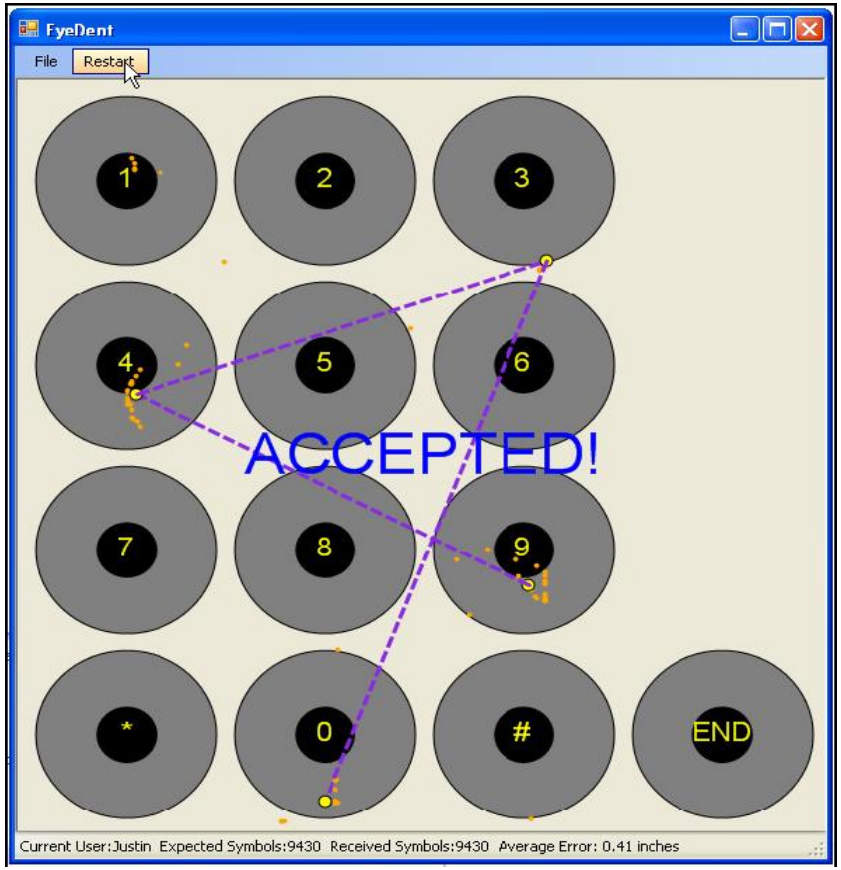
ZeuS

- First identified in July 2007.
- The most successful Banking Trojan of last decade.
- Capabilities???
  - Everything that you ‘remember’ on a computer.
  - Any keystroke you enter on a keyboard.
  - If you use virtual keypad, every time you click left mouse button, it takes a screenshot.
  - Modifies website’s code before it is shown in the browser. It can ask other information like PIN, for example.
  - Will steal your security keys (which may be specific to a website), in order to digitally sign on behalf of you.

Alternate Forms of Passwords

- Graphical passwords

Gaze Based Password



- A. Tiwari and R. Pal, “Gaze Based Graphical Password Using Webcam”, ICISS 2018

Authentication Tokens: Something You Have

- Problems with normal OTPs send over a communication channel
  - Hijacking the OTP
- Token based solutions for One-Time Passwords
  - Counter-based OTPs
  - Clock-based OTPs

Physical Types of Tokens

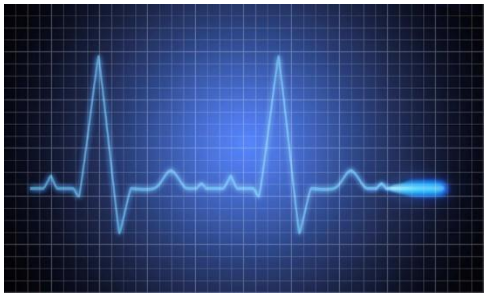
- Disconnected
- Connected
  - Smart card based
  - USB Based
- Contactless (RFID, NFC)
- Device Token

Biometrics: Something You Are

- Measuring Physical Traits
  - Fingerprints
  - Hand geometry
  - Retina
  - Iris
  - Face
  - Heartbeat
- Measuring Behavioral Traits
  - Speaker recognition
  - Written signature
  - Keystroke dynamics

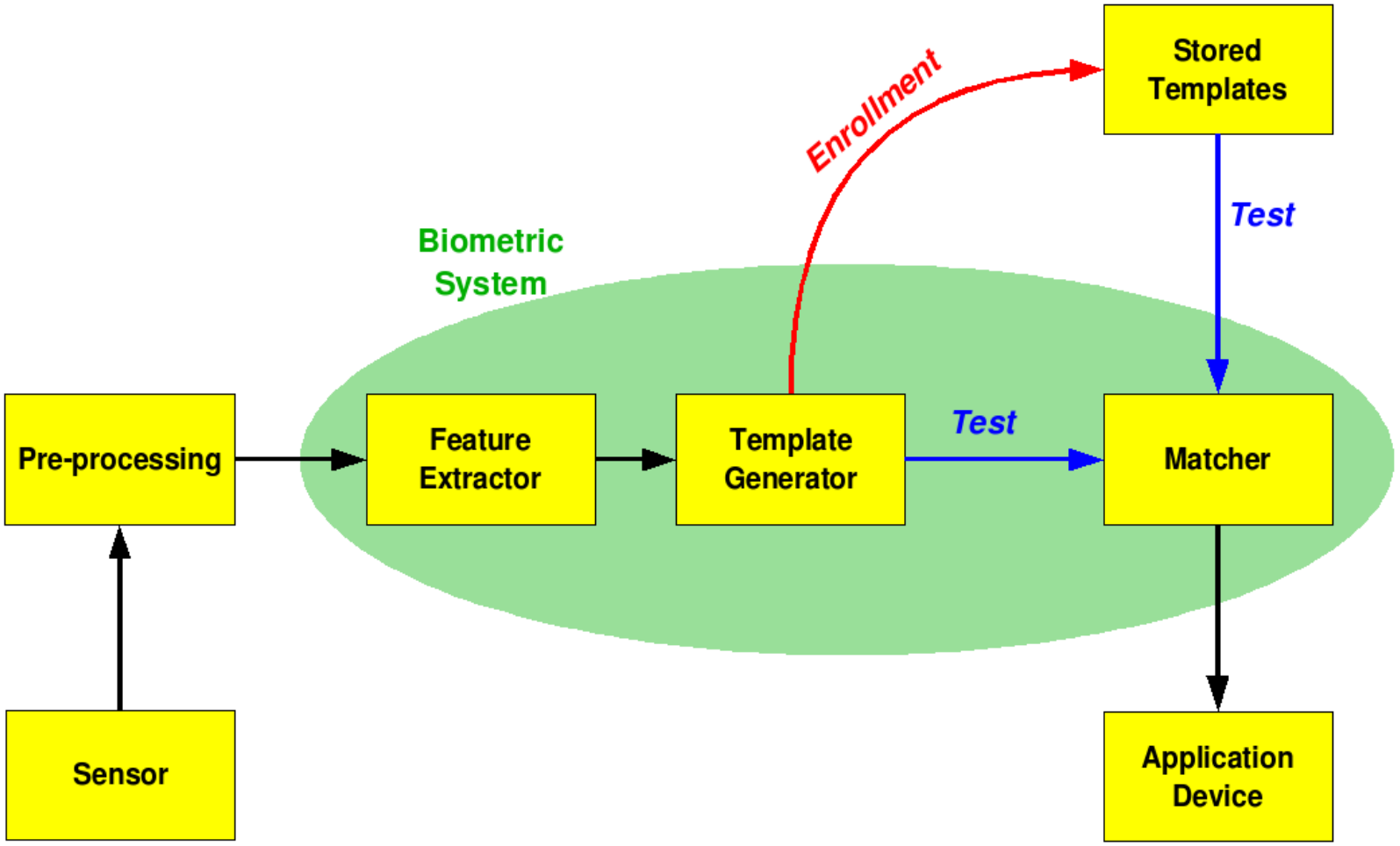
12

Heartbeat Recognition



- Authenticates the user verifying purchases
  - RBC Royal Bank
  - TD Bank

How Biometric Works



14

Problems with Biometrics

- Problem of matching biometric reading
  - Has changed over time or injured
  - Presented in an unusual fashion
  - Dirt or noise is present
- Faking biometric
  - https://www.heise.de/video/artikel/iPhone-5s-Touch-ID-hack-in-detail-1966044.html (Chaos Computer Club video (2013))
  - Infrared light enabled liveness detection for fingerprints on smartphones is available with selected models.
  - Similarly, liveliness detection technologies for face or iris recognition on mobile devices have also come up.

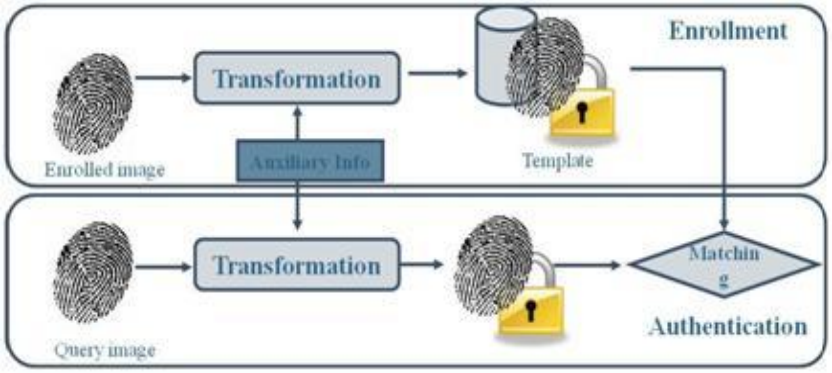
Recorded Voice can Divulge Your Identity

- Smartphones record everything you say to it http://www.telegraph.co.uk/technology/news/11434754/Why-your-smartphone-records-everything-you-say-to-it.html
- Companies may not be selling them; But it is a lucrative business proposition – where is the guarantee?
- Several third party applications ask so much permissions – specifically, microphone and camera permissions (be careful!)
- Even how can we be sure that the biometric information is stored securely at the backend.

Problems with Biometrics

- Sniffing or stealing biometric data (too dangerous!!!)
  - 5.6 million fingerprint record have been stolen from Office of Personnel Management (OPM) of U.S. military. (2013) https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/?utm_term=.af8d5771265a
  - Solution: cancelable biometric

Cancellable Biometric Should have been the Way



Authentication Factors

Factor	Benefits	Weakness	Examples
Something you know	Cheap to implement, portable	Sniffing attacks, either easy to guess or hard to remember	Passwrod, PIN
Something you have	Hard to abuse	Expensive, Can be lost or stolen, Risk of hardware failure, Not always portable	Token, Smart card, secret data embedded in a file or device, Mechanical key
Something you are	Portable	Expensive, Replay threats, Privacy risks, Characteristics can't be changed, False rejection of legitimate users, Characteristic can be injured	Fingerprint, Eye scan, Voice recognition, Photo ID

19

Two-factor and Multi-factor Authentication

- Use of two or more of the authentication factors – categorized as knowledge, ownership and inherence

ZitMo (Zeus-in-the-mobile)

- First detected on September 2010.
- Capability: can forward the text messages to attacker's mobile.
- How does it work?
  - Cyber criminals use PC based ZeuS to steal data to access online banking and mobile number.
  - The victim's mobile phone receives a text message with a request to install an updated security certificate, or some other necessary software. However, the link in the message will actually lead to mobile version of ZeuS.
  - The attacker can use the stolen credentials to intiate financial transactions from the compromised account.
  - Bank sends a code to the client's mobile phone.
  - ZitMo forwards this text message with the code to the attacker's phone.
  - Attacker uses the code to complete the transaction.

FakeToken.A

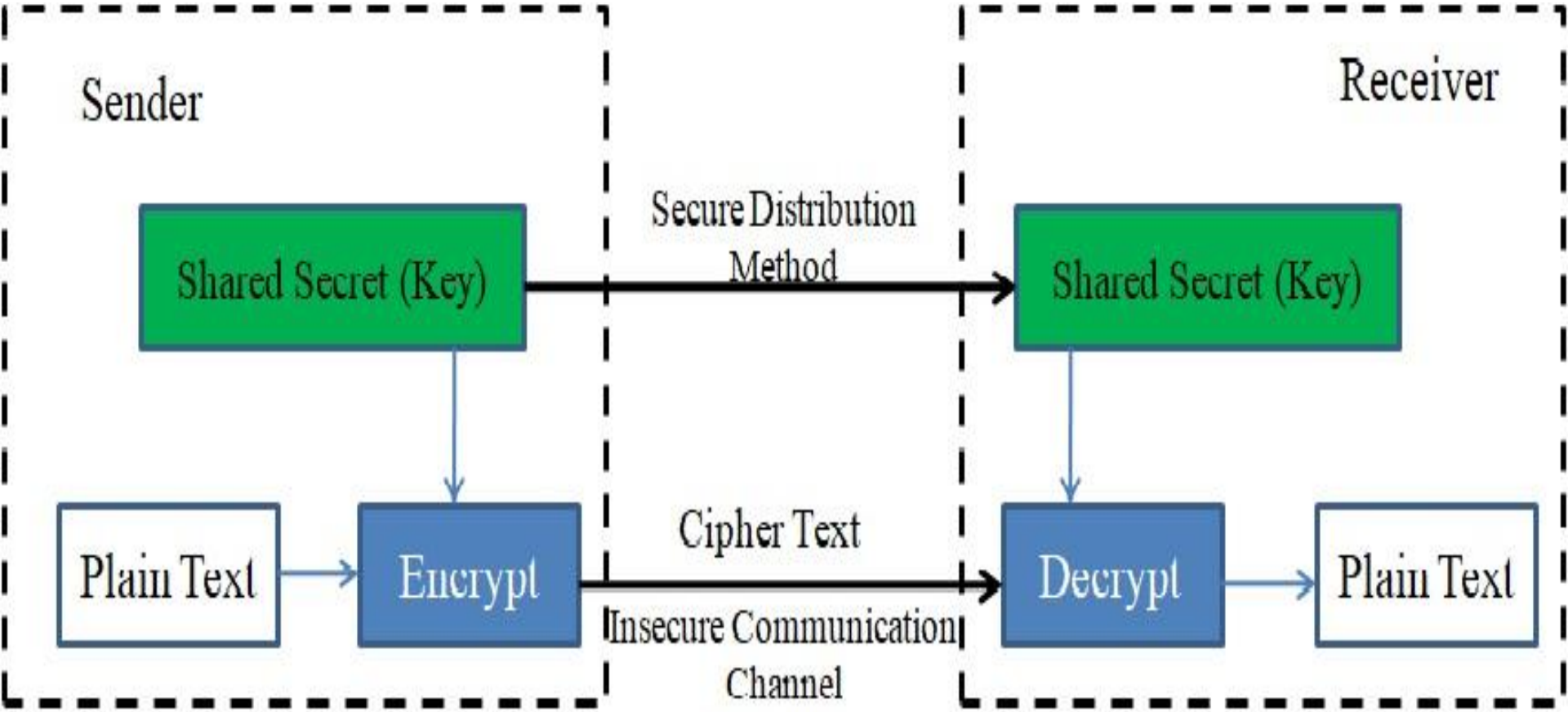
- Operation is similar to Zeus/ZitMo duo.
- Additionally, gathers the following information
  - IMEI
  - IMSI
  - Phone model
- New version FakeToken.q is more powerful (discovered in August 2017)
  - Displays fake user interface (look and feel will be similar to targeted app) where victims are encouraged to enter data
  - Steal incoming SMS codes (Do you want to deliver OTP over voice?)
  - Records voice calls coming from/made to certain numbers and sends the recorded file to the attacker.
- Few other Mobile Banking Malwares can even initiate the transaction from the compromised device.

Cryptosystem for Authentication

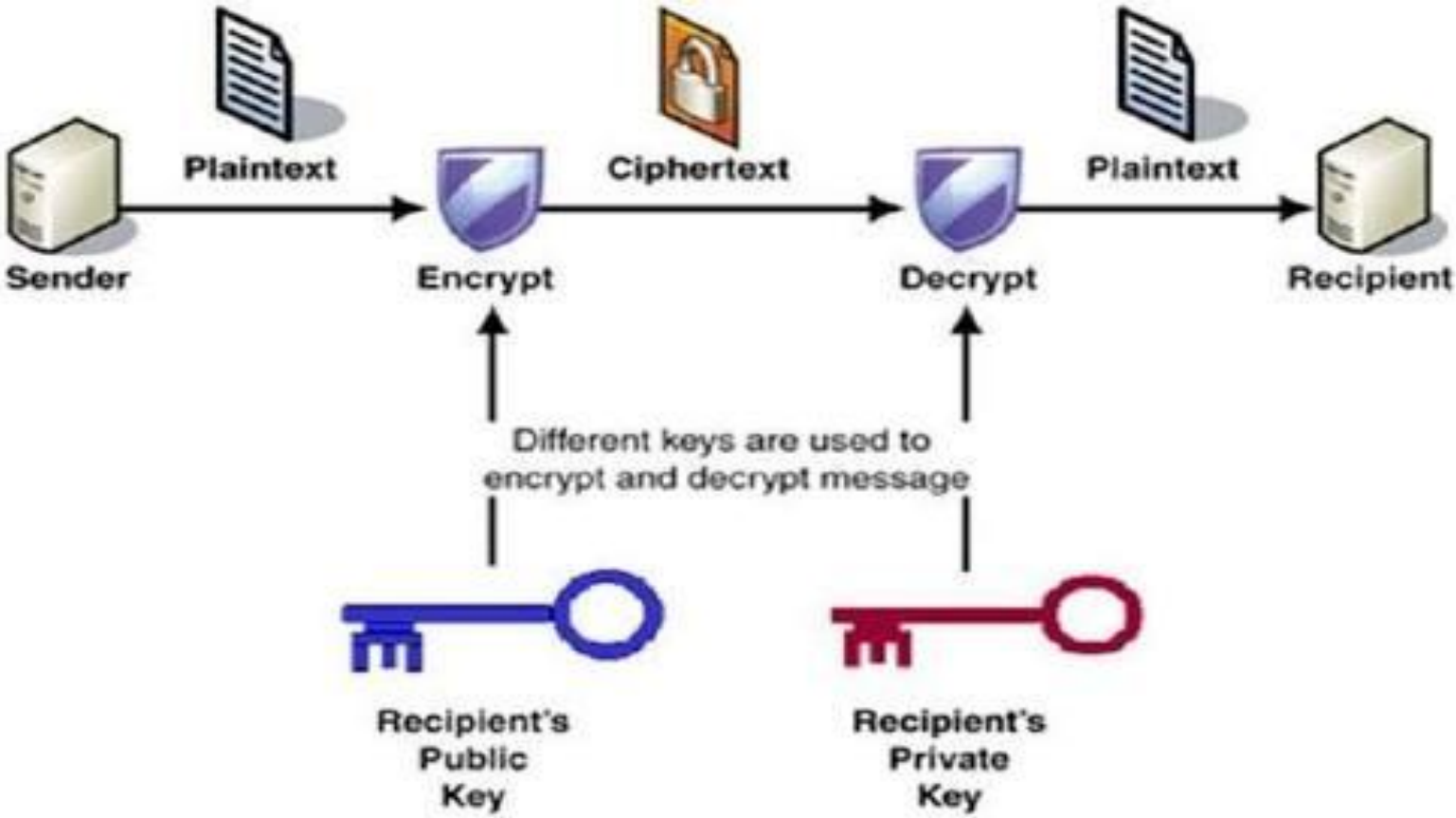
Need for Cryptographic Techniques

- Confidentiality
- Integrity
- Availability

Symmetric-Key Cryptography



Asymmetric-Key Cryptography

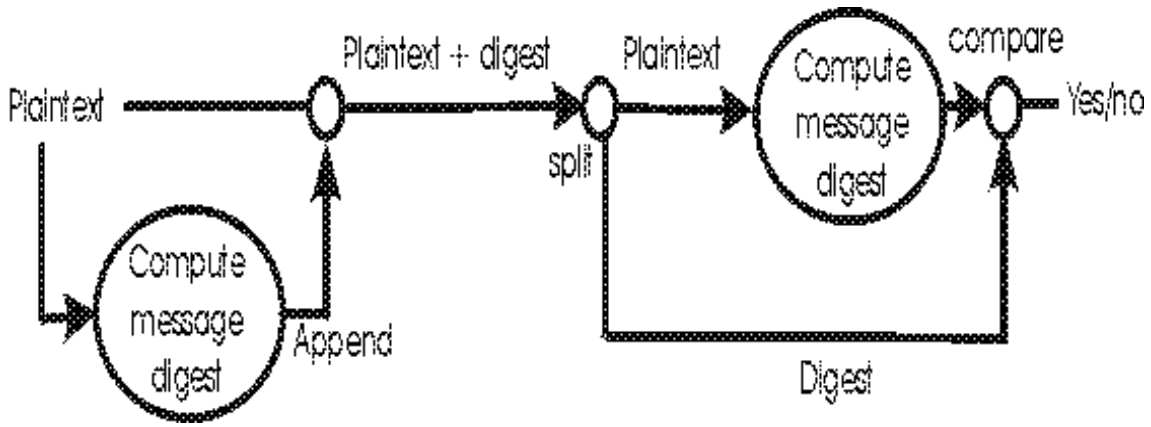


Symmetric or Asymmetric Ciphers???

- Asymmetric-key cryptography is much slower then symmetric-key cryptography.
- For encipherment of messages (usually large), symmetric-key cryptographic is needed.
- What is the use of asymmetric-key cryptography?

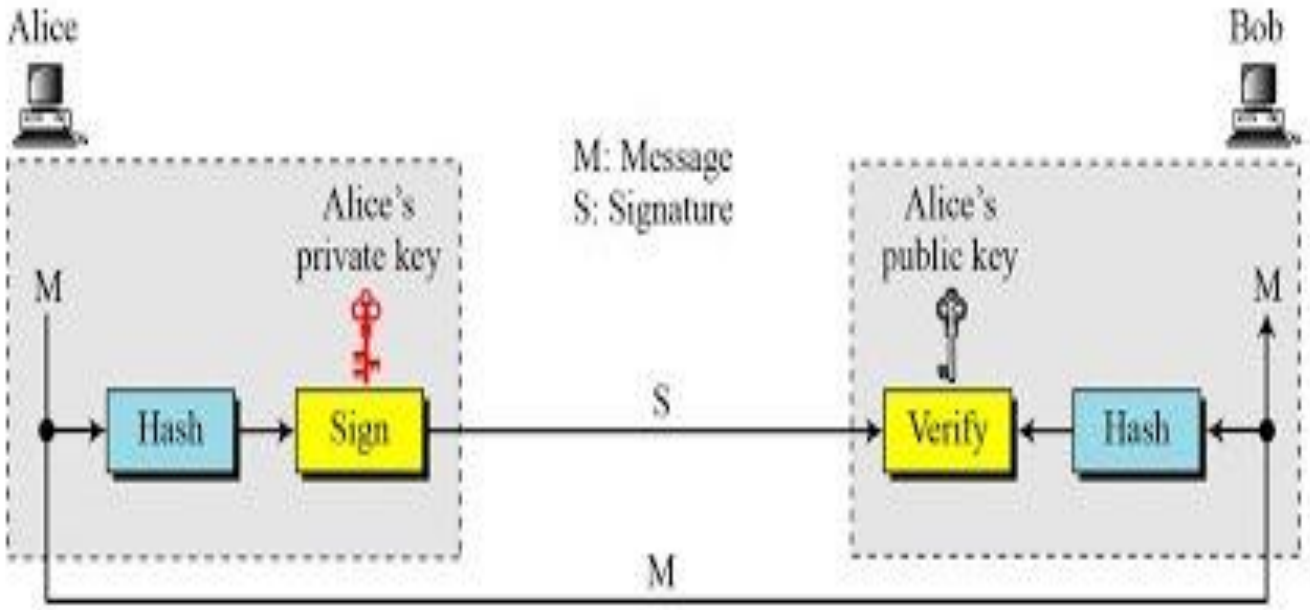
- Asymmetric-key cryptography is needed for authentication, digital signatures, and secret-key exchanges.

Message Integrity



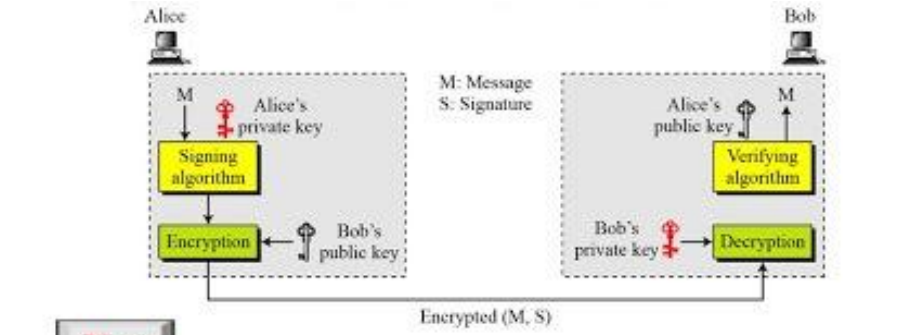
28

Digital Signature



Services Provided by Digital Signature

- Sender Authentication
- Message Integrity
- Non-repudiation (How is it achieved?)
- Confidentiality



Note

A digital signature does not provide privacy. If there is a need for privacy, another layer of encryption/decryption must be applied.

13.17

Basic Prerequisite for the Digital Signature to Work

- The private key must remain private.
- The public key owner must be verifiable.

- How will you verify the owner of the public key?

Protecting Private Key

- Minimize access
  - Computer with private keys should have minimal external connections
  - Minimize the number of users who have access to the private keys
- Physical security
  - Cryptographic hardware (HSM)
  - Store the key in a secure external device (smart card or some other security token)

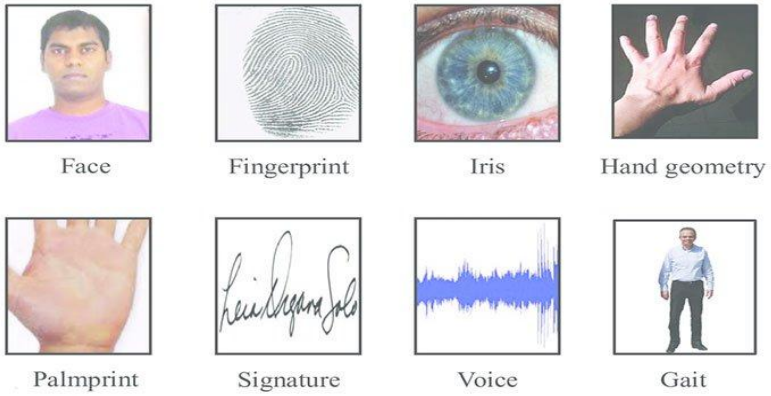
Bio-cryptosystem

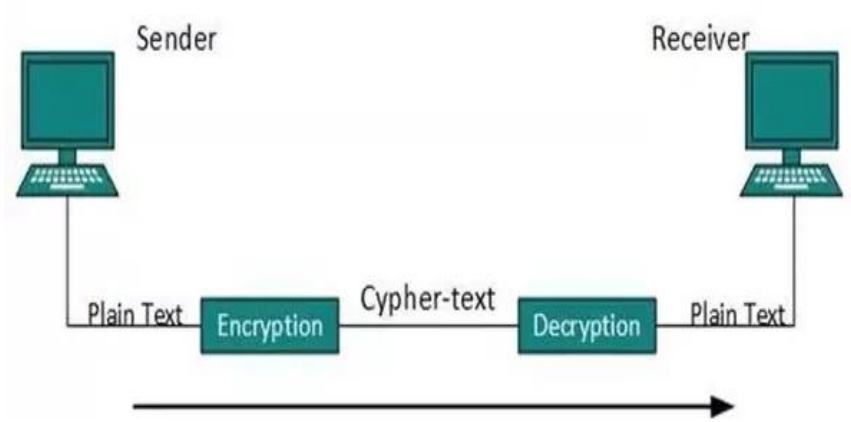
Bio-cryptosystem

Bio - Cryptosystem

=

Biometrics + Cryptography





Bio-cryptosystem

In general, there are three ways to integrate biometrics and cryptography

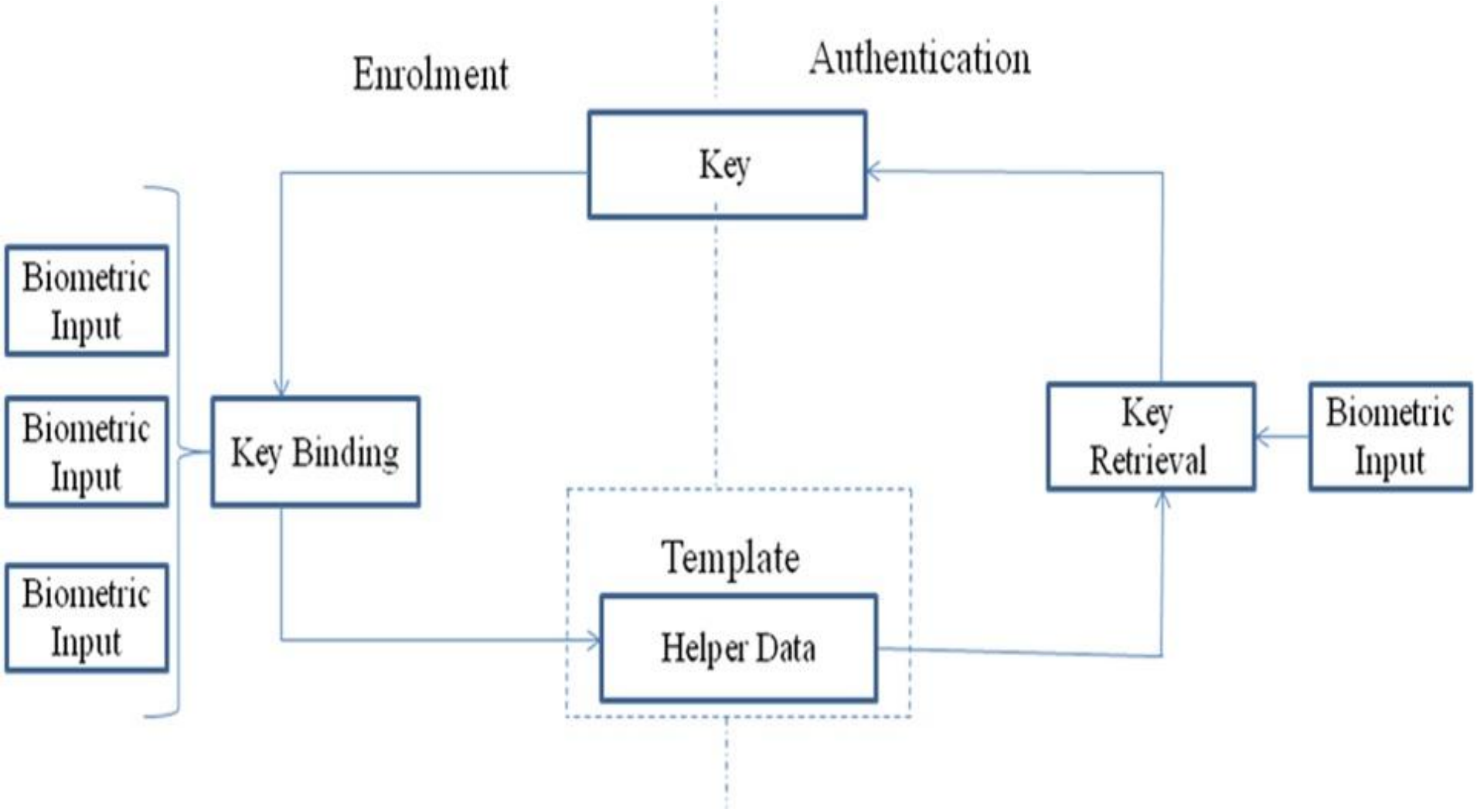
- Key Release
- Key Binding
- Key Generation

- Key release is to release the cryptographic key based on biometric authentication
- Key binding is to protect cryptographic key using biometrics.
- Key generation is to generate cryptographic key directly from the biometric features.

Key Release

- In the key release scheme, key release mechanism and biometric template matching are completely decoupled.
- The biometric template and cryptographic key are stored in a smart card or token or in computer as separate entities.
- To release the cryptographic key, stored biometric and query biometric are compared.
- The key is released only on the successful biometrics matching.
- In this bio-cryptosystems, biometric template is stored and it is, again, vulnerable to attacks.

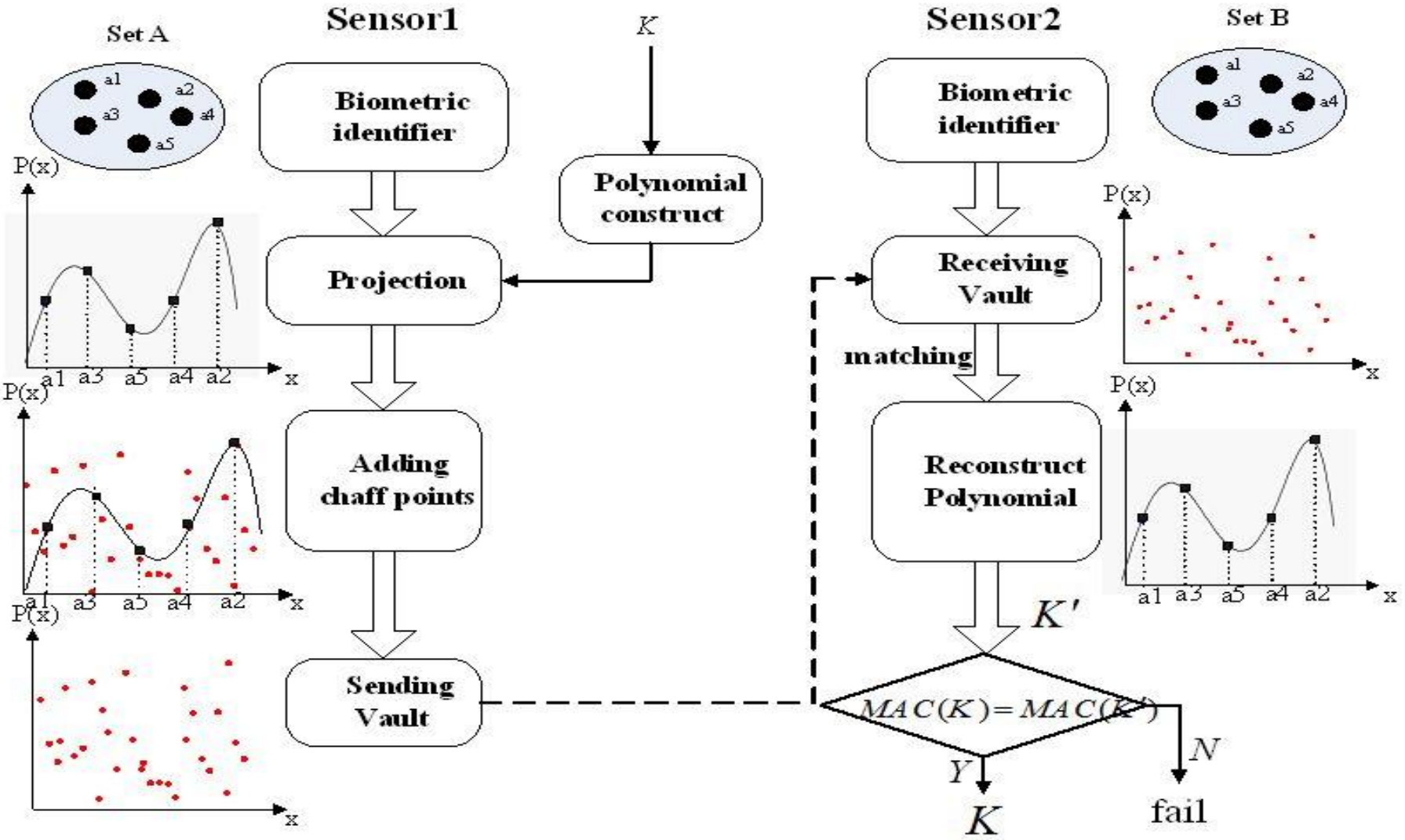
Key Binding


Enrolment
Authentication
Key
Biometric Input
Biometric Input
Biometric Input
Key Binding
Key Retrieval
Biometric Input
Template
Helper Data

Key Binding

- There are two techniques in key binding scheme
    - Fuzzy Vault
    - Fuzzy Commitment
- Error Correcting Codes (ECC) are used to correct the biometric invariance errors.

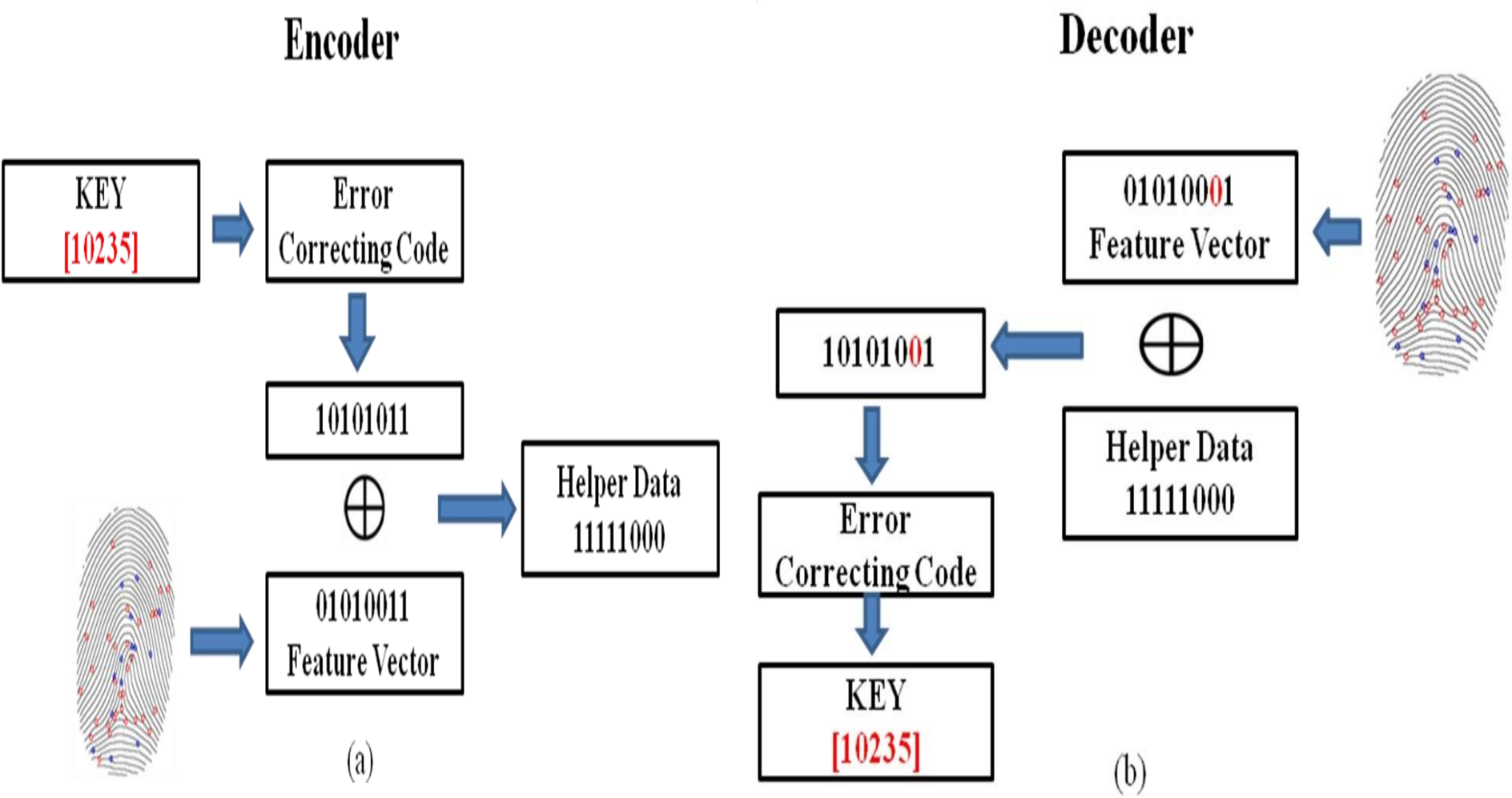
Fuzzy Vault


Set A
Sensor1
K
Sensor2
Set B
a1
a2
a3
a4
a5
Biometric identifier
Polynomial construct
Projection
Adding chaff points
Sending Vault
Biometric identifier
Receiving Vault
matching
Reconstruct Polynomial
K'
MAC(K)=MAC(K')
Y
N
K
fail
P(x)
x

Fuzzy Vault

- A. Juels and M. Sudan, “A fuzzy vault scheme”, Proc. of IEEE International Symposium on Information Theory, 2002.
  - Polynomial p of a single variable x encodes the secret key k (i.e., in its coefficients)
  - Evaluations of p on the elements of A (derived from biometric template)
  - A number of random chaff points are introduced
- Dang et al, “Cancellable fuzzy vault with periodic transform for biometric template protection”, IET Biometrics, 2016.
- Dang et al, “Chaff pint generation mechanism for improving fuzzy vault security”, IET Biometrics, 2016.
  - Chaff points are also generated using biometrics and secret key
  - Chaff points are also verified after generation of the key

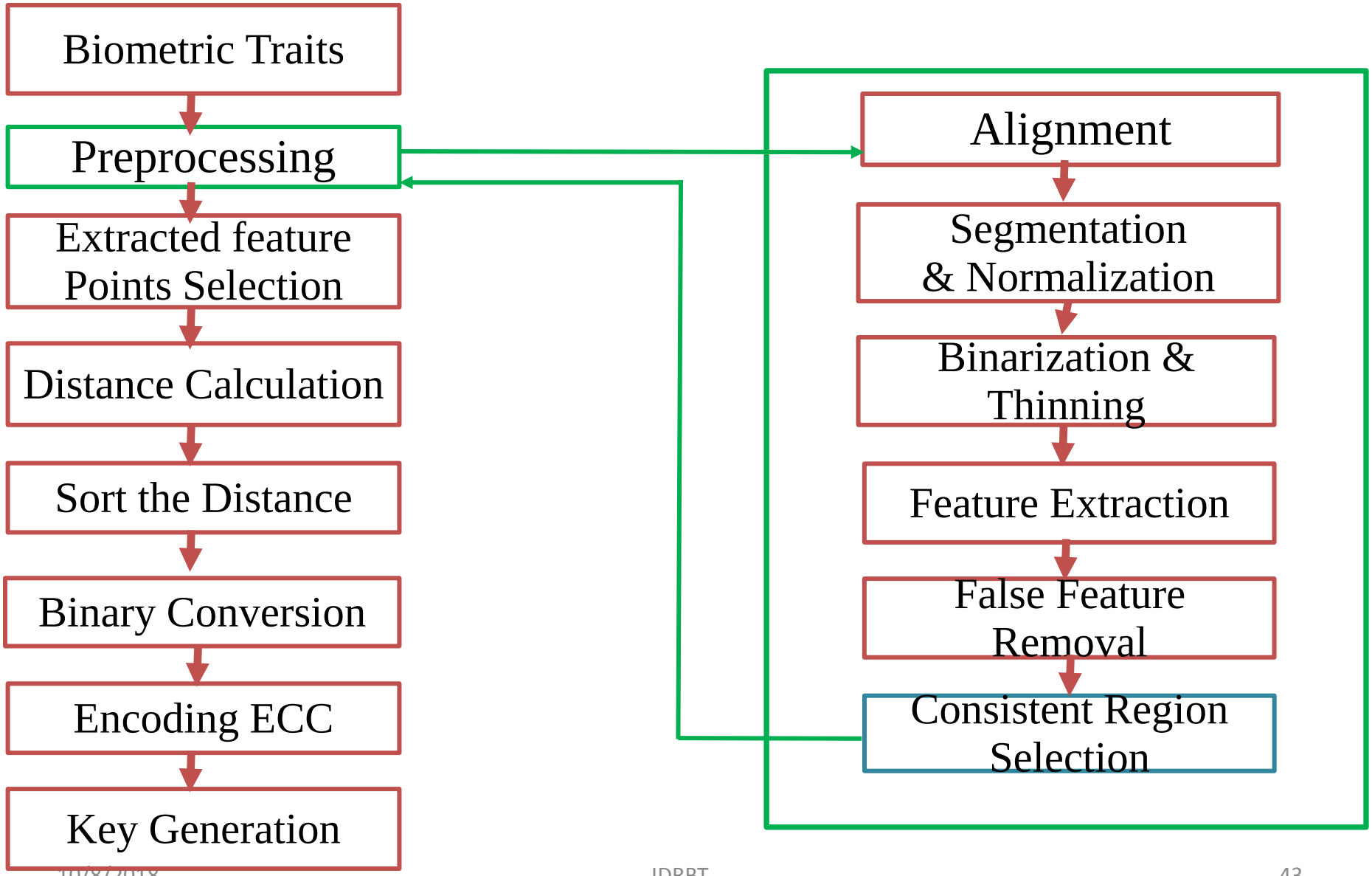
Fuzzy Commitment



Fuzzy Commitment

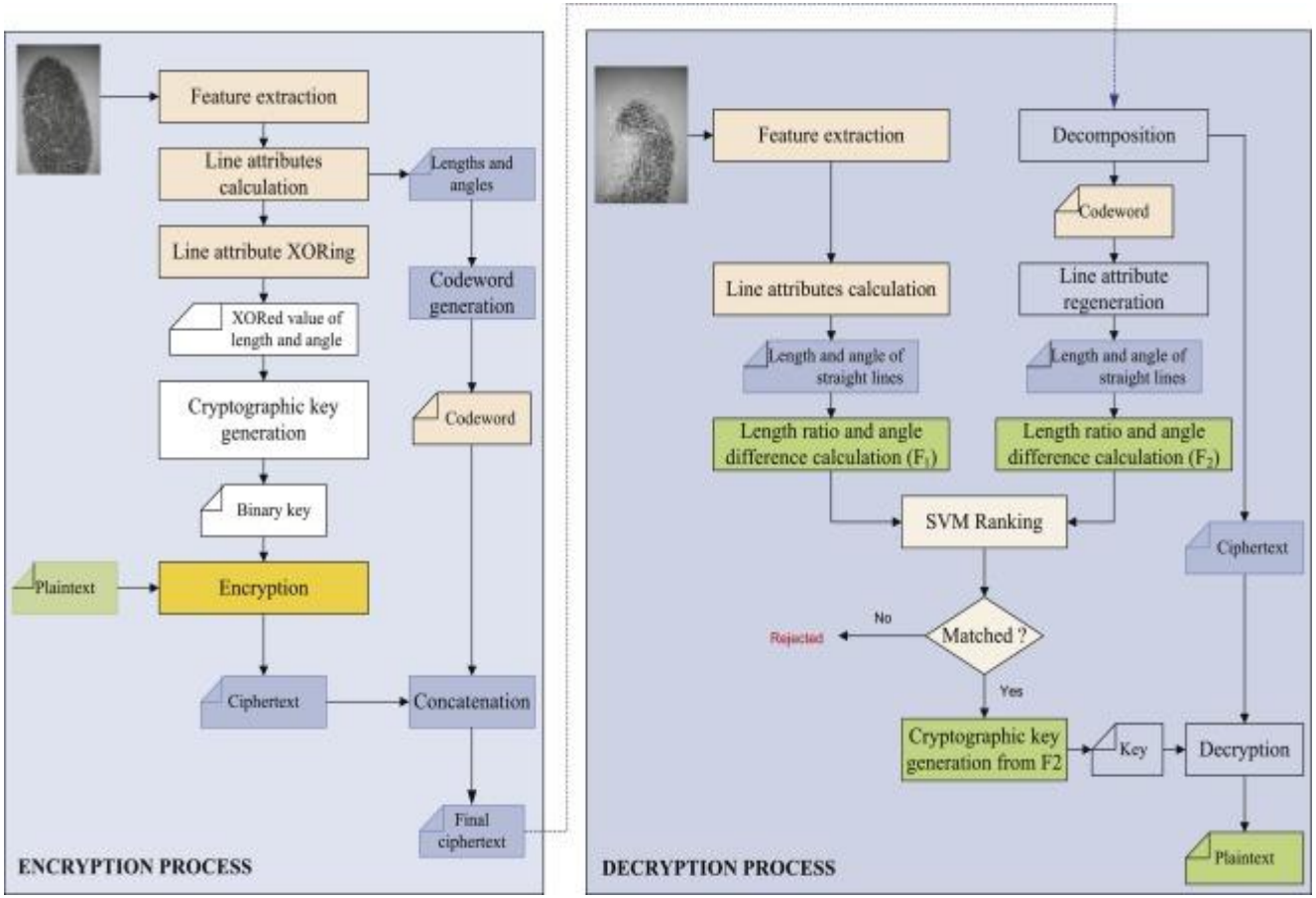
- A. Juels and M. Wattenberg, “A fuzzy commitment scheme”, Proc. Of 6th ACM Conference on Computer and Communications Security, 1999.
- Adamovic et al, “Fuzzy commitment scheme for generation of cryptographic keys based on iris biometrics”, IET Biometric, 2017.
  - Drawback of existing schemes: knowing either one (biometric or the key), can reveal the other
  - Interleaving (random shuffling) the iris code (using a pseudorandom key)

Key Generation Schemes



Key Generation Schemes

- Gaurang Panchal, Debasis Samanta, “A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its applications to Storage Security”, *Computers and Electrical Engineering, Elsevier,* 2018.



Issues and Challenges

- The fundamental challenge of biometric systems is alignment issue.
- Biometric data is naturally noisy. Hence, error correction codes are used to tackle these noises in a biometric based cryptographic systems.
- Securing biometric features is another important challenge, because biometric data are not extremely secret. Example, fingerprints of an individual can be easily taken from the object which he/she touches.
- Some of the common potential attacks against biometric cryptosystems are attack via record multiplicity, masquerade attack, attacks on error correcting codes, brute force attack, chaff elimination and false acceptance attack.

Conclusion

- Bio-cryptosystem techniques do not require to store the key or the biometric.
- It pulls up the advantages of possession factor and the inherence factor – hence, a powerful way of authentication.
- Still need to go long way till adoption by Industry

Thank You

Email: PRajarshi@idrbt.ac.in