Biometric Crypto-Systems

Felix Baumann, Ravinder Sangar, Jonas Winkler

May 4, 2020

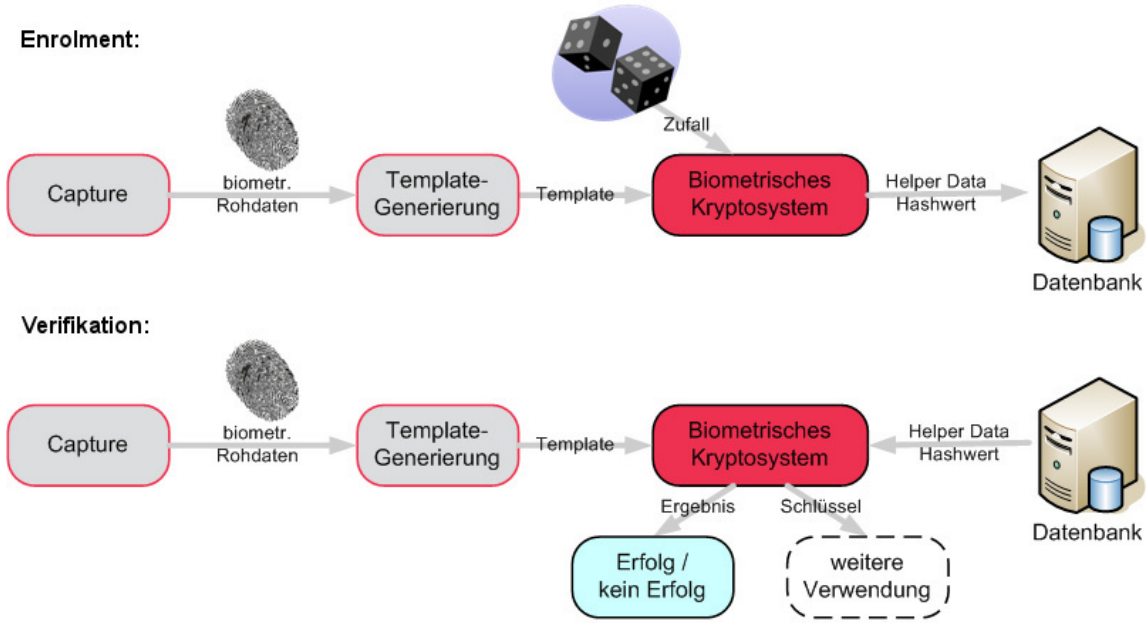
Inhalt

Biometrische Kryptosysteme

- Biometrische Daten sind biologische Messwerte, die Personen eindeutig identifizieren
- Bsp: Fingerabdruckscan, Gesichtserkennung, Irisscan
- Biometrische Kryptosysteme verbinden Kryptographie mit Biometrie

Quelle: *https://www.cancom.info/2019/03/gesichtserkennung-technologie/*

Funktionsweise

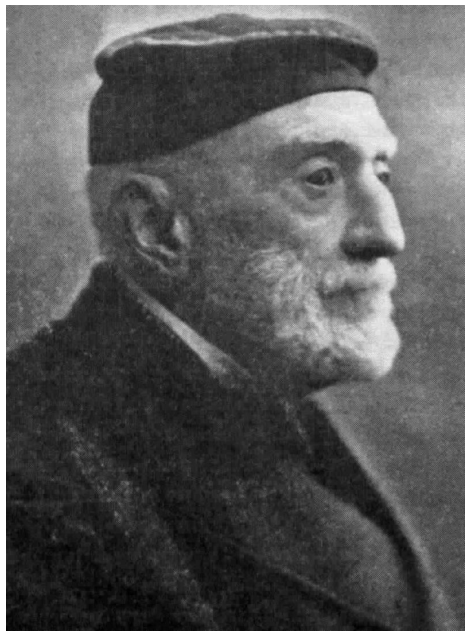


Quelle: *http://2014.kes.info/archiv/online/images/08-6-052-1-400.jpg*

Inhalt

Idee hinter Biometrie

- Erste Biometrie war der Fingerabdruck
- Vor 4000 Jahren wurde mit Fingerabdrücken unterzeichnet
- Henry Fauld fand heraus, dass Fingerabdrücke individuell sind



Quelle: *de.wikipedia.org*

Heutige Verwendung

- Fingerabdrücke werden heute in Forensik eingesetzt
- Gesichtserkennung bei einigen Smartphone und in Flughäfen
- Schlüssel für Gebäude werden von Fingerabdruckscane abgelöst
- Biometrischer Pass wird weltweit eingesetzt: Bild des Gesichts und 2 Fingerabdruckbilder

Quelle: *wikimedia.org*

Problematik

- Alle biometrischen Daten, die gesammelt wurden, können gehackt werden
- Biometrische Daten können nicht verändert werden, wie ein Passwort
- Duplikation von Daten: Fingerabdrücke können im Alltag unbemerkt abgenommen werden, Hochauflösende Fotos von Gesichtern

Biometric Template Protection

- biometrische templates keine Referenzdaten
- umgewandelt in protected templates
- reicht aus für Authentifizierung

Fuzzy commitment

- Commitment-Schema - 2 Eigenschaften:
  - *binding*-Eigenschaft
  - *hiding*-Eigenschaft
- $y = G(k, x)$
- ungefährer Schlüssel reicht zur Identifikation
- Messung: Hamming-Distanz

Fuzzy commitment

- Vorteile
  - Unschärfe - nötig für biometrische Authentifizierung
  - Biometrie kann sich minimal verändern
- Nachteile
  - weniger Sicherheit gegenüber anderen Commitments, da mit Unschärfen gearbeitet wird

Fuzzy Vault

- Fingerabdrücke sind nicht zu 100% reproduzierbar
- Konzept das Fehler tolleriert?

Fuzzy Vault

- Alice möchte wissen ob jemand ihre Interessen teilt
- Alice sichert Interessen in einem Save
- Bob hat ähnliche Interessen
- Bob kann den Save entsperren

LOCK

$X, R \rightarrow \emptyset$

$s \rightarrow p$

for $i = 1$ *to* t

$(a_i, p(a_i)) \rightarrow (x_i, y_i)$

$X \bigcup \{x_i\} \rightarrow X$

$R \bigcup \{(x_i, y_i)\} \rightarrow R$

for $i = t + 1$ *to* r

$x_i \in F - X$

$y_i \in F - \{(x_i, y_i\}$

$R \cup \{(x_i, y_i)\} \rightarrow R$

return R

UNLOCK

$Q \rightarrow \emptyset$

for $i = 1$ *to* t

$R \xrightarrow{b_i, \circ} (x_i, y_i)$

$Q \bigcup (x_i, y_i) \rightarrow Q$

$RS_{DECODE}(k, Q) \rightarrow s'$

return s'

Vor- und Nachteile

- Vorteile
  - Fehler der Sensoren/Finger werden tolleriert
  - Chaff-Points bestimmen die Sicherheit
- Nachteile
  - eventuell weniger Sicherheit gegenüber anderen Verschlüsselungssysteme bei wenigen Chaff-Points
  - Risiko für hohe Komplexität

Vielen Dank für Ihre Aufmerksamkeit