An Authentication Protocol with encrypted Biometric Data based on Bringer et. Al. [1]

Seminar Biometry & Security, Winter 2009/2010

Andreas Dresen, 23.11.2009

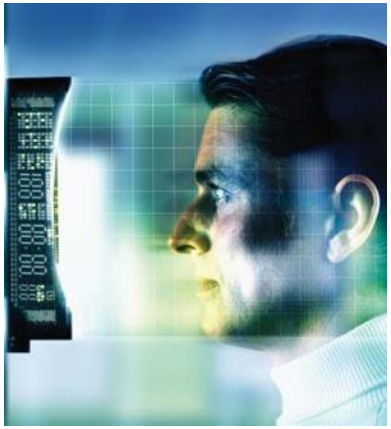
Content

- Motivation
- Biometric Authentication Protocol in general
- Components of encrypted Protocol
- Protocol with encrypted Biometric Data
- Security Analysis
- Summary

Motivation

- Enforce privacy of biometric data
- Obtain communication complexity; prevents eavesdropping
- Separation of biometric data and temporary data generated for authentication

Capturing of Biometric Data



[2]

Advantages & Disadvantages of Biometrics

- Advantages [3]:
  - Reduce password administration costs
  - Replace hard-to-remember passwords which may be shared or observed
  - Eliminate problems caused by lost IDs or forgotten passwords by using physiological attributes

- Disadvantages [4]:
  - Biometrics is an expensive security solution
  - For people affected with diabetes, the eyes get affected resulting in differences

Normal biometric-based recognition scheme

enrollment phase

- User U register a biometric template
- Therefore he has to measure any biometric data of his choice
- Template is stored in a database

verification phase

- A new biometric template is measured from U
- Compared to stored data via matching function
- Decision is made, if accepted or not

Security Model

- **Soundness**. An authentication scheme is sound if:
  - The Service Provider accept a request if the client sends (ID_i , b_i‘) in an authentication request, where b_i matches b_i‘ and b_i is the reference template of ID_i .
  - Else reject.

- **Identity Privacy:**
  - For any random username, the adversary don‘t get to know anything about the corresponding biometric template
  - The adversary cannot find a link between registrations

Security Model

- **Transaction Anonymity:**
  - The database cannot distinguish an authentication request of user U_{i_0} with one from user U_{i_1}

Goldwasser-Micali Scheme

- Step 1 (Key generation):
  - Security parameter 1^l as input
  - Generate two large prime numbers p and q, n = p * q
  - Also a non-residue x
  - Public key *pk* is (x,n)
  - Secret key *sk* is (p,q)

- Step 2 (Encryption):
  - Take a message m $\in \{0,1\}$ and *pk* as input
  - Output ciphertext c, where $c = y^2 x^m \bmod n$ and y is random from $\mathbb{Z}_n^*$

Goldwasser-Micali Scheme

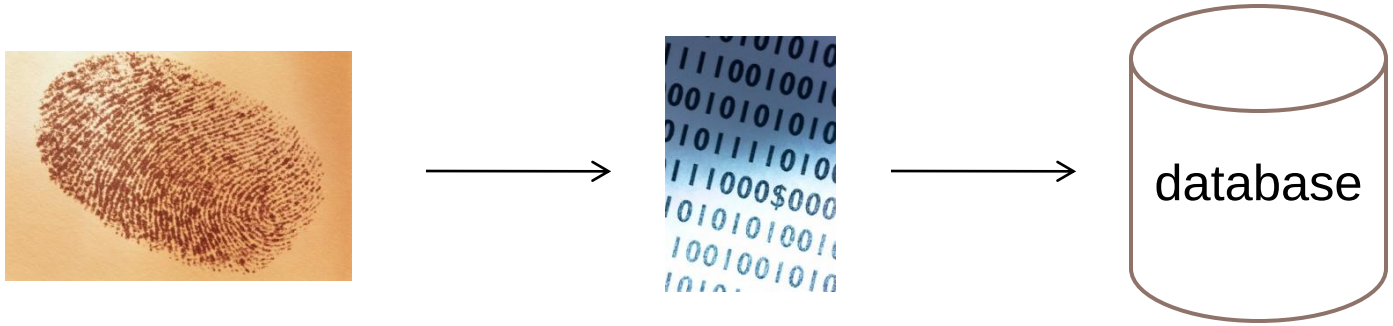
- Step 3 (Decryption):
  - Takes ciphertext c and private key as input
  - Output: message m
    - Where m = 0 if c is a quadratic residue
    - Otherwise m = 1

- Definition quadratic residue [5]:

  Let p be an odd prime. A number $a \subseteq Z_p^*$ is a ***quadratic residue*** if the equation $x^2 = a \pmod{p}$ has a solution for the unknown x.

Encrypted Sketches

- **<u>Problem:</u>** biometric data of enrollment phase is stored in databases
- **<u>Result:</u>** anybody can check membership of biometric data in the DB
- **<u>Idea:</u>** encrypt the biometric data before it is stored in the database



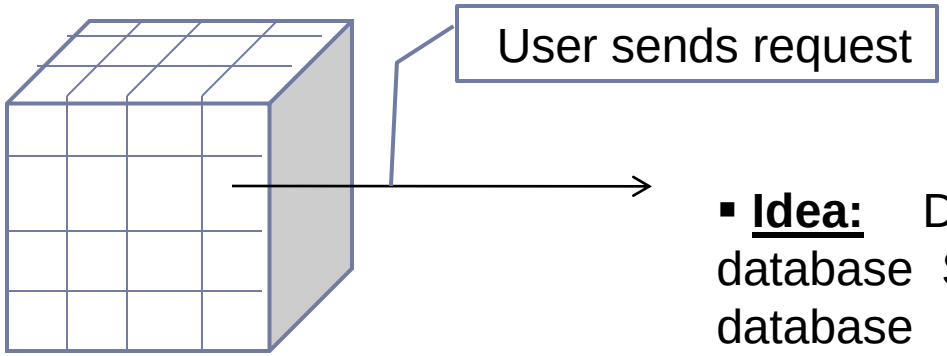
Encrypted Sketches

- The Service Provider (*SP*) generates a Goldwasser-Micali key pair and publishes public key *pk*
- [.] denotes a related Encryption Enc(. , pk)
- During enrollment:
  - User U_i registers with his biometric template b_i at *SP*
  - Then $P = SS_c(b_i) = c \oplus b_i$ is computed and [P] is stored in the *DB* for a random codeword c
  - *H*(c) is stored by *SP*, *H* a cryptographic hash function

Encrypted Sketches

- During authentication:
  - A new biometric template b‘ is captured and sent to *DB*
  - *DB* computes [P] x [b‘] = [c $\oplus$ b_i $\oplus$ b‘] = Z
  - Send Z to the *SP*
  - *SP* decrypts Z with private key *sk*
  - Decodes output c $\oplus$ b_i $\oplus$ b‘ to obtain c‘
  - Finally it checks $H(c') = H(c)$

Lipmaa‘s Protocol



Database seen as multidimensional array.

Entries are associated to a vector of index

- **<u>Idea:</u>** Decrease dimension of database S to construct a smaller database recursively till the last dimension

Don‘t send the whole index vector $(q_1, \ldots, q_\lambda)$.

Construct an index vector of dimension λ-1 as encryption of the index vector of dimension λ; repeat this λ times.

The λ times encryption of index vector $(q_1, \ldots, q_\lambda)$ is the answer to the request of the user.

Details in [1].

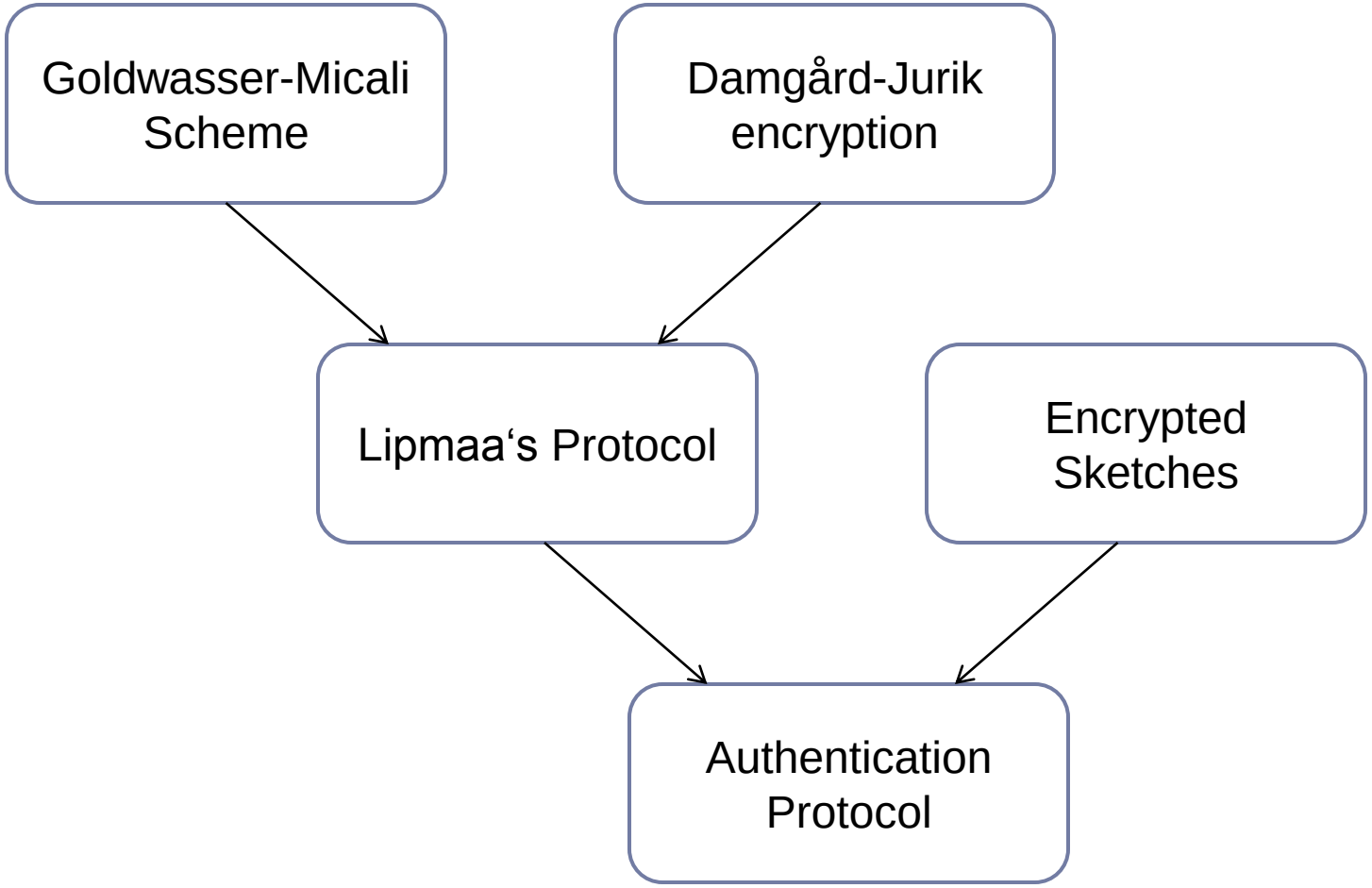
Lipmaa‘s Protocol

- How the user recovers the requested element:
  - The user has to decrypt λ times the element that he has got from the database.
  - Finally he will get the original vector $(q_1, \ldots, q_\lambda)$

    ⇒ The requested biometric template

- Request Privacy is achieved through semantic security of Damgård-Jurik cryptosystem.

Achieving an Authentication Protocol with Encrypted Biometric Data



Private Biometric Authentication Protocol with Secure Sketches

- Parameters:
  - *M* number of users in the database
  - Service Provider has two keys (pk_{GM} , sk_{GM}) and (pk_P ,sk_P)
  - Encryption denoted as [.] for GM and [[.]] for P.
  - Public keys published and secret keys stored inside *HSM*

  - Database stores *M* encrypted sketches and the corresponding biometric templates for every User U_i
  - Database also possesses the hash values $H(c_i)$

  - Dimension for Lipmaa is $\lambda = 1$ (for simplification)

Verification Phase

Encrypted via GM

Client *C*

database

Send a request with the Paillier's ciphertexts

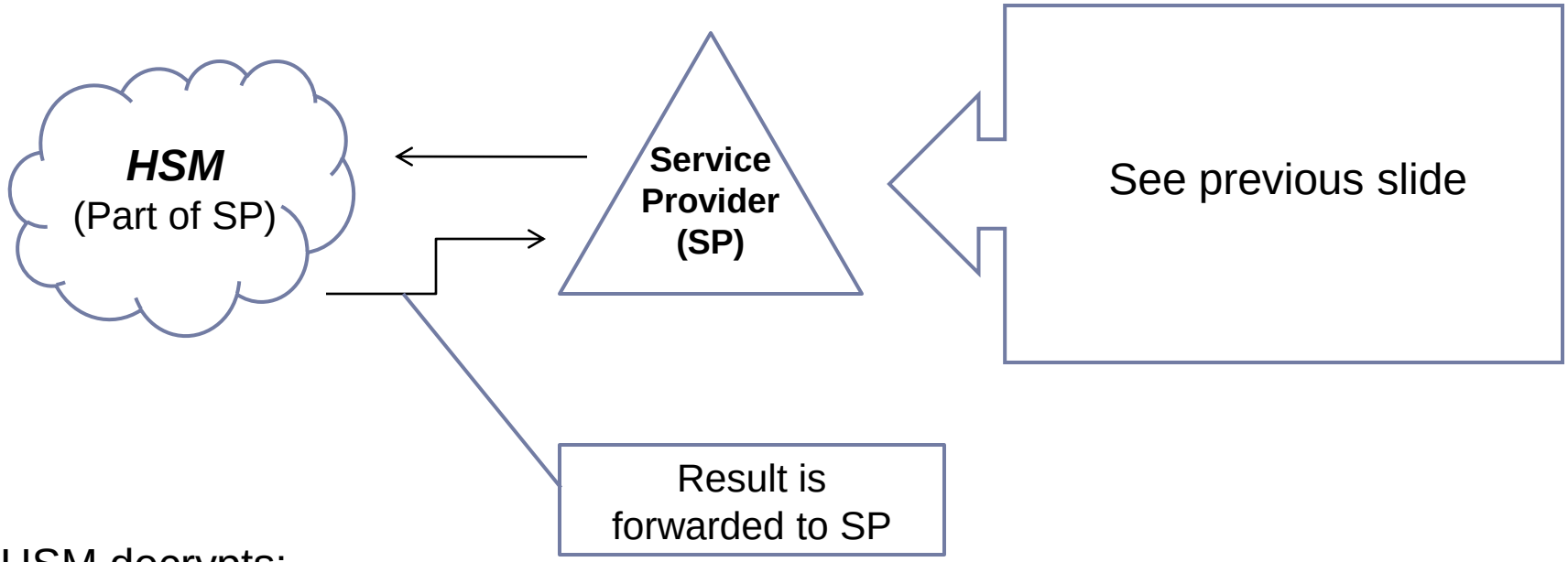
computes

$[[a_{i,u} \times [\pi_u (b')]]]$, for $u = 0, \ldots , l-1$

$[[a_{i,l}]]$, $a_{i,l} = H(c_i)$ (cryptographic hash function)

Service Provider (SP)

Verification Phase (continued)



HSM decrypts:

1. Paillier algorithm
2. Goldwasser-Micali algorithm to recover $SS_c(b_i) \oplus b'$ and $H(c_i)$.

Further it decodes $SS_c(b_i) \oplus b'$ to obtain a codeword c' and checks if $H(c') = H(c_i)$ to accept or reject the authentication

Security Analysis

- **Lemma 1 (Soundness) [1]:**
  - *The protocol is sound under Definition 1 if the involved Secure Sketch (SS_C, Rec_C) is sound and if the PIR protocol is sound.*

- Rely on efficiency of secure sketches
  - In this protocol, biometric data and sketches are always encrypted with a secure encryption scheme

⇨ An adversary cannot recover any template

Security Analysis

- **Lemma 2 (Identity Privacy) [1]:**
  - *Our scheme achieves identity privacy against a malicious service provider or a malicious database under the semantic security of the Goldwasser-Micali scheme, i.e. under the QR assumption.*

- It ensures identity privacy against non-colluding malicious service provider or database and any external adversary

Security Analysis

- **Transaction Anonymity (TA)**
  - There is no TA against the service provider because it can learn $H(c_i)$ for a request of User U_i
  - So you can track a specific user request in the future

- Countermeasure:
  - Renew regularly enrolled data
    i. Encrypted sketch
    ii. Corresponding hash value

Summary

- This protocol achieves biometric authentication while keeping the privacy of users
- During all computations, you deal with encrypted biometric data
- It is possible to integrate it into one of the best Private Information Retrieval scheme (Lipmaa)
- Lipmaa reduces also the communication complexity to $\mathcal{O}(\log^2 \mathrm{M})$
- One disadvantage:
  - Encryption of Goldwasser-Micali is done bit by bit

Thank you.

Sources

- [1]: J. Bringer and H. Chabanne. An Authentication Protocol with Encrypted Biometric Data. In S. Vaudenay, editor, AFRICACRYPT'08, volume 5023 of LNCS, pages 109–124. Springer, 2008.
- [2]: http://www.die-friedenskrieger.de/pics/biometrie.jpg
- [3]: http://www.questbiometrics.com/advantages-of-biometrics.html
- [4]: http://www.allpctips.com/technology/biometrics.htm
- [5]: http://highered.mcgraw-hill.com/sites/0070131511/student_view0/glossary_p-s.html