An Authentication Protocol with Encrypted Biometric Data
AFRICACRYPT 2008

Julien Bringer and Hervé Chabanne

Sagem Sécurité

Work partially supported by french ANR RNRT project BACH

julien.bringer@sagem.com

2008, June 11th

Biometrics: the 3rd factor. Who I am

- allows authentication of one person and identification among a large set of persons;
- is unique, permanent, easy to use, non-transferable;

but. . .

Biometrics: the 3rd factor. Who I am

- cannot be chosen;
- cannot be modified if compromised;
- is public;

- is a personal data;
- is different at each measure.

Biometrics: the 3rd factor. Who I am

- cannot be chosen;
- cannot be modified if compromised;
- is public;

- is a personal data;
- is different at each measure.

How to manage *fuzzy* biometric authentication with privacy protection?

Model for a biometric system with a database

Entities:

- human user U_i who wants to authenticate himself with his biometric;
- sensor client $\mathcal{C}$ which measures biometric templates and checks their liveness;
- service provider $\mathcal{SP}$ possibly with an access to a *HSM* which manages the secret keys;
- database $\mathcal{DB}$ which stores enrolled biometric information.

$$U_i \longrightarrow \mathcal{C} \longrightarrow \mathcal{SP} \longleftrightarrow \mathcal{DB}$$

Model for a biometric system with a database

Entities:

- human user U_i who wants to authenticate himself with his biometric;
- sensor client $\mathcal{C}$ which measures biometric templates and checks their liveness;
- service provider $\mathcal{SP}$ possibly with an access to a *HSM* which manages the secret keys;
- database $\mathcal{DB}$ which stores enrolled biometric information.

$$U_i \longrightarrow \mathcal{C} \longrightarrow \mathcal{SP} \longleftrightarrow \mathcal{DB}$$

We assume $\mathcal{SP}$ and $\mathcal{DB}$ do not collude. $\mathcal{C}$ is always considered as honest.

Private biometric authentication

- $\mathcal{DB}$ stores information related to couples (ID_i, b_i),
- U_i presents its ID_i and a new measure b',
- $\mathcal{SP}$ wants to check whether b_i matches with b'.

To respect privacy, stored data and transactions must be secured.

Secure Sketches [Dodis-Reyzin-Smith'04]

Let $(\mathcal{H}, \mathrm{d})$ be a metric space. A secure sketch is a pair (SS, Rec) where

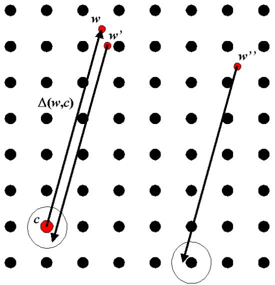
- $\mathsf{SS}(w)$, with $\mathsf{SS} : \mathcal{H} \rightarrow \{0,1\}^*$, does not leak too much about w,
- $\mathsf{Rec}(w', \mathsf{SS}(w)) = w$ if $d(w, w')$ small enough.

Allows to correct differences between measures but security should be improved by other means.

Code-offset construction [Juels-Wattenberg'98]

Given C a binary linear code, $(\mathrm{SS}_\mathrm{C}, \mathrm{Rec}_\mathrm{C})$ are defined by

- $\mathrm{SS}_\mathrm{C}(w)$ outputs $P = c \oplus w$, where $c \in_R C$;
- $\mathrm{Rec}_\mathrm{C}(w', P)$ decodes $w' \oplus P$ into a codeword c', and then outputs $c' \oplus P$.



An authentication protocol is achieved by storing $(P, H(c))$.

Goldwasser-Micali Scheme '82

Parameters

- p and q large primes, $n = pq$
- a non-residue x for which the Jacobi symbol is 1

Scheme

- $pk = (x, n)$ and $sk = (p, q)$
- $\text{Enc}(m, pk) = y^2 x^m$ for $m \in \{0, 1\}$ and $y \in_R \mathbb{Z}_n^*$
- $\text{Dec}(c, sk) = 0$ if $c = \square$, 1 otherwise.

Goldwasser-Micali Scheme '82

Properties

- IND-CPA under Quadratic Residuosity (QR) assumption
- homomorphic: $\mathrm{Dec}(\mathrm{Enc}(m, pk) \times \mathrm{Enc}(m', pk), sk) = m \oplus m'$

Generalization:
$\sqsubset m \sqsupset = (\mathrm{Enc}(m_0, pk), \ldots, \mathrm{Enc}(m_{l-1}, pk))$ for $m \in \{0, 1\}^l$

Authentication with encrypted sketches

1. Enrollment of the user U_i with b_i.
   - $\sqsubset P \sqsupset$ is stored in $\mathcal{DB}$ with $P = \mathsf{SS}_{\mathrm{C}}(b_i) = c \oplus b_i$
   - $H(c)$ is stored by $\mathcal{SP}$

Authentication with encrypted sketches

1. Enrollment of the user U_i with b_i.
   - $\sqsubset P \sqsupset$ is stored in $\mathcal{DB}$ with $P = \mathrm{SS}_{\mathrm{C}}(b_i) = c \oplus b_i$
   - $H(c)$ is stored by $\mathcal{SP}$
2. Authentication of U_i with b'
   - $\sqsubset b' \sqsupset$ is sent to $\mathcal{DB}$
   - $\mathcal{DB}$ computes $\sqsubset P \sqsupset \times \sqsubset b' \sqsupset = \sqsubset c \oplus b_i \oplus b' \sqsupset = Z$ and sends it to $\mathcal{SP}$
   - $\mathcal{SP}$ decrypts Z, decodes $c \oplus b_i \oplus b'$ into a codeword c' and checks if $H(c') = H(c)$.

Authentication with encrypted sketches

1. Enrollment of the user U_i with b_i.
   - $\sqsubset P \sqsupset$ is stored in $\mathcal{DB}$ with $P = \mathrm{SS}_{\mathrm{C}}(b_i) = c \oplus b_i$
   - $H(c)$ is stored by $\mathcal{SP}$
2. Authentication of U_i with b'
   - $\sqsubset b' \sqsupset$ is sent to $\mathcal{DB}$
   - $\mathcal{DB}$ computes $\sqsubset P \sqsupset \times \sqsubset b' \sqsupset = \sqsubset c \oplus b_i \oplus b' \sqsupset = Z$ and sends it to $\mathcal{SP}$
   - $\mathcal{SP}$ decrypts Z, decodes $c \oplus b_i \oplus b'$ into a codeword c' and checks if $H(c') = H(c)$.

$\Rightarrow$ encrypted data in $\mathcal{DB}$; $\mathcal{SP}$ obtains no information on biometric data

Private Information Retrieval

[Chor-Kushilevitz-Goldreich-Sudan'98]

A PIR protocol enables a user to retrieve a bit from a database.
When user asks for bit i,

- Soundness: the user retrieves the bit i
- User-Privacy: the database learns nothing about i

Symmetric PIR:

- Database-Privacy: the user learns nothing about other bits in the database

Private Information Retrieval

[Chor-Kushilevitz-Goldreich-Sudan'98]

A PIR protocol enables a user to retrieve a bit from a database.
When user asks for bit i,

- Soundness: the user retrieves the bit i
- User-Privacy: the database learns nothing about i

Symmetric PIR:

- Database-Privacy: the user learns nothing about other bits in the database

Private Block Retrieval

A PBR protocol enables a user to retrieve a block from a block-database.

Allows to reduce communication cost to poly-log complexity [Lipmaa'05,Gentry-Ramzan'05]

Paillier Cryptosystem '99

Parameters

- $n = pq$ an RSA integer, g of order n modulo n^2

Scheme

- $pk = (n, g)$ and $sk = \lambda(n)$ (λ Carmichael function)
- $\mathrm{Enc}(m, pk) = g^m r^n \mod n^2$ for $m \in \mathbb{Z}_n$ and $r \in_R \mathbb{Z}_n^*$
- $\mathrm{Dec}(c, sk) = \frac{L(c^{\lambda(n)} \mod n^2)}{L(g^{\lambda(n)} \mod n^2)} \mod n$ with $L(u) = \frac{u-1}{n}$

Properties

- IND-CPA under degree n decisional Composite Residue problem
- $\mathrm{Dec}(\mathrm{Enc}(m, pk) \times \mathrm{Enc}(m', pk) \mod n^2, sk) = m + m' \mod n$
- $\mathrm{Dec}(\mathrm{Enc}(m, pk)^k \mod n^2, sk) = km \mod n$

Generalization [Damgård-Jurik'01-03]

Length flexible encryption

For $m \in \mathbb{Z}_{n^s}^*$, $[\![m]\!]_s = (1+n)^m r^{n^s} \mod n^{s+1}$ with $r \in \mathbb{Z}_n^*$

Allows re-encryption of encrypted messages.

Used in Lipmaa's PIR to reduce the communication cost by working on a multidimensional $\mathcal{DB}$.

Successive re-encryptions lead to reduce progressively the size of the processed database and to obtain only the requested data at the end (after successive decryptions).

Identity Privacy

The adversary $\mathcal{A}$ plays the role of $\mathcal{DB}$ or $\mathcal{SP}$, and tries to learn some information from the enrolled data.

1. $\mathcal{A}_1$ generates a set $(i, ID_i, b_i^{(0)}, b_i^{(1)}, (ID_j, b_j)(j \neq i))$
2. The challenger randomly chooses a template $b_i^{(e)}$ for ID_i and simulates the enrollment phase for $(ID_i, b_i^{(e)})$ and all the (ID_j, b_j)
3. $\mathcal{A}_2$ lets the challenger to issue Verification queries on the sensor side
4. $\mathcal{A}_2$ outputs a guess e'

Transaction Anonymity

The adversary $\mathcal{A}$ plays the role of $\mathcal{DB}$, and tries to learn some information from the user.

1. $\mathcal{A}_1$ generates a set $\{(ID_j, b_j)\}$
2. The challenger simulates the enrollment phase for all the (ID_j, b_j)
3. $\mathcal{A}_2$ lets the challenger to issue Verification queries on the sensor side and outputs (i_0, i_1)
4. The challenger randomly chooses $e \in_R \{0, 1\}$ and issues a Verification query with input i_e
5. $\mathcal{A}_3$ lets the challenger to issue Verification queries on the sensor side and outputs a guess e'

Adaptation of the PIR User-Privacy property. The same is possible for Data-Privacy vs $\mathcal{SP}$.

Secure Biometric Authentication

A biometric authentication scheme must satisfy

- Soundness: $\mathcal{SP}$ will accept an authentication request of (ID_i, b') from $\mathcal{C}$ side iff b' and b are matching (biometric) data, except for a small probability
- Identity Privacy vs $\mathcal{DB}$ or $\mathcal{SP}$
- Transaction Anonymity vs $\mathcal{DB}$

Soundness: in practice, probability of failure depends of biometrics performances (FRR/FAR)

Overview

We want to combine encrypted secure sketches with PIR in an efficient and quite transparent way.

Overview

We want to combine encrypted secure sketches with PIR in an efficient and quite transparent way.

The idea is to combine two "compatible" encryption schemes to benefit from both homomorphic properties

$$[\![\sqsubset c \sqsupset]\!]_s^{\sqsubset w \sqsupset} = [\![\sqsubset c \sqsupset \times \sqsubset w \sqsupset]\!]_s = [\![\sqsubset c \oplus w \sqsupset]\!]_s$$

where $\sqsubset . \sqsupset$ stands for Golwasser-Micali encryption and $[\![.]\!]_s$ for Damgård-Jurik of length n^s

It allows us to embed information in a classical PIR request.

Parameters

- $\mathcal{SP}$ is associated to (pk_{GM}, sk_{GM}) and (pk_{DJ}, sk_{DJ}); secret keys are stored inside a *HSM*
- M users $U_1, \ldots, U_M$
- $\mathcal{DB}$ contains $a_i = (a_{i,0}, \ldots, a_{i,l-1}) = \sqsubset \mathrm{SS}_{\mathrm{C}}(b_i) \sqsupset$, for $i = 1, \ldots, M$, with $\mathrm{SS}_{\mathrm{C}}(b_i) = b_i \oplus c_i$ and b_i l-bits biometric template.
- $\mathcal{DB}$ stores also $a_{i,l} = H(c_i)$.

To simplify, we explain now the verification phase for $s = 1$, i.e. with Paillier and only one iteration in Lipmaa's PIR.

Verification Phase

Authentication of user U_i

1. $\mathcal{C}$ measures b', computes $\sqsubset b' \sqsupset$ and sends to $\mathcal{DB}$, $[\![\delta_k^u]\!]$, $k = 1, \ldots, M$, $u = 0, \ldots, l$ where $(\delta_k^0, \ldots, \delta_k^{l-1}, \delta_k^l) = (\sqsubset b' \sqsupset, 1)$ if $k = i$ and $(0, \ldots, 0)$ otherwise

Verification Phase

Authentication of user U_i

1. $\mathcal{C}$ measures b', computes $\sqsubset b' \sqsupset$ and sends to $\mathcal{DB}$, $[\![\delta_k^u]\!]$, $k = 1, \ldots, M$, $u = 0, \ldots, l$ where $(\delta_k^0, \ldots, \delta_k^{l-1}, \delta_k^l) = (\sqsubset b' \sqsupset, 1)$ if $k = i$ and $(0, \ldots, 0)$ otherwise
2. $\mathcal{DB}$ computes for $u = 0, \ldots, l-1$

$$[\![\sqsubset (\mathrm{SS}_{\mathrm{C}}(b_i) \oplus b')_u \sqsupset]\!] = [\![a_{i,u} \times \sqsubset (b')_u \sqsupset]\!] = \prod_{k=1}^{M} [\![\delta_k^u]\!]^{a_{k,u}}$$

and $[\![H(c_i)]\!] = [\![a_{i,l}]\!] = \prod_{k=1}^{M} [\![\delta_k^l]\!]^{a_{k,l}}$. Then sends everything to $\mathcal{SP}$

Verification Phase

Authentication of user U_i

1. $\mathcal{C}$ measures b', computes $\sqsubset b' \sqsupset$ and sends to $\mathcal{DB}$, $[\![\delta_k^u]\!]$, $k = 1, \ldots, M$, $u = 0, \ldots, l$ where $(\delta_k^0, \ldots, \delta_k^{l-1}, \delta_k^l) = (\sqsubset b' \sqsupset, 1)$ if $k = i$ and $(0, \ldots, 0)$ otherwise
2. $\mathcal{DB}$ computes for $u = 0, \ldots, l-1$

$$[\![\sqsubset (\mathrm{SS_C}(b_i) \oplus b')_u \sqsupset]\!] = [\![a_{i,u} \times \sqsubset (b')_u \sqsupset]\!] = \prod_{k=1}^{M} [\![\delta_k^u]\!]^{a_{k,u}}$$

   and $[\![H(c_i)]\!] = [\![a_{i,l}]\!] = \prod_{k=1}^{M} [\![\delta_k^l]\!]^{a_{k,l}}$. Then sends everything to $\mathcal{SP}$
3. HSM decrypts with sk_{GM}, sk_P to recover $\mathrm{SS_C}(b_i) \oplus b'$ and $H(c_i)$, decodes into c', checks if $H(c') = H(c_i)$ and forwards the result to $\mathcal{SP}$

PIR Performances

- With Paillier, communication cost linear in M
- Expandable to Lipmaa's protocol for a dimension λ with λ Damgård-Jurik encryption scheme $[\![.]\!]_s, \ldots, [\![.]\!]_{s+\lambda-1}$
  Communication cost in $O(\log^2 M)$

This combination is valid with all PIR based on a homomorphic scheme with a compatible group law (e.g. [Chang'04]).

Security / Privacy

- Soundness: if the PIR and $(\mathrm{SS}_{\mathrm{C}}, \mathrm{Rec}_{\mathrm{C}})$ are sound
- Identity Privacy: under QR assumption
- Transaction Anonymity vs $\mathcal{DB}$: if the PIR achieves User-Privacy

Transaction Anonymity vs $\mathcal{SP}$?

Needs to renew c_i after each Verification query
(or regularly to avoid long-term tracking)

Conclusion

We have described a new Biometric Authentication Scheme

- Improvement of a previous scheme presented at ACISP'07 [Bringer-Chabanne-Izabachène-Pointcheval-Tang-Zimmer]
- Preserves privacy of users
- Deals only with encrypted biometric data
  a new way to manage secure sketches with homomorphic encryption to enable a strict separation between biometric data and temporary data
- Uses a communication efficient PIR

Conclusion

We have described a new Biometric Authentication Scheme

- Improvement of a previous scheme presented at ACISP'07 [Bringer-Chabanne-Izabachène-Pointcheval-Tang-Zimmer]
- Preserves privacy of users
- Deals only with encrypted biometric data
  a new way to manage secure sketches with homomorphic encryption to enable a strict separation between biometric data and temporary data
- Uses a communication efficient PIR

Research issues

- Improve information rates (encryption)
- Improve computational cost

Thanks! Any question?