Attacks on Privacy-Preserving Biometric Authentication

Aysajan Abidin, Elena Pagnin, Aikaterini Mitrokotsa

Chalmers University of Technology, Gothenburg, Sweden
{aysajan.abidin, elenap, aikmitr}@chalmers.se

Abstract. Biometric authentication based on facial image, fingerprint, palm print, iris, retina, or veins are becoming increasingly popular. However, compromised biometric templates, indeed, may lead to serious threats to identity and their inherent irrevocability makes this risk even more serious. Because of such serious privacy implications the need for *privacy-preserving biometric authentication protocols* is of utmost importance. Recently, Yasuda *et al.* [1, 2] proposed two efficient privacy-preserving biometric authentication using packed homomorphic encryption based on ideal lattices and on ring learning with error. We review these protocols and analyse their security against *malicious* internal adversaries.

Yasuda *et al.* [1, 2] have proposed two packed homomorphic encryption schemes based, respectively, on ideal lattices and on ring-LWE (ring-learning-with-errors). Let $\mathsf{vE}_1(\cdot)$ be the type 1 packed encryption, and $\mathsf{vE}_2(\cdot)$ the type 2 packed encryption. Let A and B be bitstrings of length N. Then, $\mathsf{ct}_H = C\mathsf{vE}_1(A) + C'\mathsf{vE}_2(B) - 2\mathsf{vE}_1(A)\mathsf{vE}_2(B)$ corresponds to an encryption of the Hamming distance between A and B, for suitable chosen constants C and C'. In particular, $\mathsf{vE}_1(A)\mathsf{vE}_2(B)$ provides an encryption of the inner product between A and B. Both protocols involve three entities (a client server $\mathcal{C}$, a computation server $\mathcal{CS}$ and an authentication server $\mathcal{AS}$) and are composed of three phases:

– ***Setup Phase:*** $\mathcal{AS}$ generates the public key pk and the secret key sk for the SHE schemes, and distributes only pk to both $\mathcal{C}$ and $\mathcal{CS}$.

– ***Enrolment Phase:*** $\mathcal{C}$ generates a feature vector A from the client's biometric readings, computes $\mathsf{vE}_1(A)$, and sends it with client's ID to $\mathcal{CS}$, who then stores $\mathsf{vE}_1(A)$ and ID in its database $\mathcal{DB}$.

– ***Authentication Phase:*** $\mathcal{C}$ generates a feature vector B from the client's fresh biometric readings, computes $\mathsf{vE}_2(B)$, and sends it with the client's ID to $\mathcal{CS}$. Then, $\mathcal{CS}$ retrieves the template $\mathsf{vE}_1(A)$ corresponding to ID from $\mathcal{DB}$, computes $\mathsf{ct}_H$and sends ct_H to $\mathcal{AS}$. Subsequently, $\mathcal{AS}$ decrypts ct_H with the secret key sk to obtain the Hamming distance $\mathsf{HD}(A, B)$. Finally, $\mathcal{AS}$ returns the authentication result YES (resp. NO) to $\mathcal{C}$ if $\mathsf{HD}(A, B) \leqslant \tau$ (resp., otherwise), where τ is a pre-defined threshold.

We briefly describe the attack algorithms that could be employed when $\mathcal{C}$ (Algorithm 1) and $\mathcal{CS}$ (Algorithm 2) are malicious. Note that Algorithm 1 can also be employed by a compromised $\mathcal{CS}$. In the attack algorithm descriptions, $\mathcal{C} \xrightarrow{A} \mathcal{CS}$ denotes $\mathcal{C}$ sends A to $\mathcal{CS}$.

Algorithm 1 Center search attack

Input: $B = B_1, \cdots, B_N$ (fresh)
Output: $A = A_1, \cdots, A_N$ (reference)
for $i = 1$ to N: **do**
  $D \leftarrow \overline{B_1}, \ldots, \overline{B_i}, B_{i+1}, \ldots, B_N$
  $\mathcal{C} \xrightarrow{\mathsf{vE}_2(D)} \mathcal{CS}$
  $\mathcal{CS} \xrightarrow{\mathsf{ct}_H} \mathcal{AS}$
  if rejected **then**
    break
  end if
end for
for $i = 1$ to N: **do**
  $\mathcal{C} \xrightarrow{\mathsf{vE}_2(D_1,\ldots,\overline{D_i},D_{i+1},\ldots,D_N)} \mathcal{CS}$
  $\mathcal{CS} \xrightarrow{\mathsf{ct}_H} \mathcal{AS}$
  if accepted **then**
    $A_i \leftarrow \overline{D_i}$
  else
    $A_i \leftarrow D_i$
  end if
end for

Algorithm 2 Cheating attack

Input: $\mathsf{vE}_1(A)$
Output: $A = A_1, \cdots, A_N$
Initialise: $A = 0_1 0_2 \cdots 0_N$
for $i = 0$ to $N - \tau$: **do**
  $D \leftarrow 1_1 \cdots 1_{\tau+i}\, 0_{\tau+i+1} \cdots 0_N$
  $\mathcal{CS} \xrightarrow{\mathsf{vE}_1(A)\mathsf{vE}_2(D)} \mathcal{AS}$
  if rejected **then**
    break
  end if
end for
$i' \leftarrow \tau + i$; $A_{i'} \leftarrow 1$
for $i = 1$ to $i' - 1$: **do**
  $D \leftarrow 1_1 \cdots 1_{i-1}\, 0_i\, 1_{i+1} \cdots 1_{i'} 0 \cdots 0_N$
  $\mathcal{CS} \xrightarrow{\mathsf{vE}_1(A)\mathsf{vE}_2(D)} \mathcal{AS}$
  if accepted **then**
    $A_i \leftarrow 1$
  end if
end for
for $i = i' + 1$ to N: **do**
  $D \leftarrow 1_1 \cdots 1 0_{i'} \cdots 0 1_i 0 \cdots 0_N$
  $\mathcal{CS} \xrightarrow{\mathsf{vE}_1(A)\mathsf{vE}_2(D)} \mathcal{AS}$
  if rejected **then**
    $A_i \leftarrow 1$
  end if
end for

We reviewed two recently proposed privacy-preserving biometric authentication protocols and presented two attack algorithms. The center search attack (Algorithm 1) enables to recover a reference biometric template using a fresh acceptable template. The second attack (Algorithm 2) allows the recovery of reference templates of arbitrary users. Both attacks require a number of authentication attempts that is linear in N (*i.e.* the length of the biometric template) to fully recover a reference template.

Acknowledgements: This work was partially supported by the FP7-STREP project "BEAT: Biometric Evaluation and Testing", grant number: 284989.

References

1. Yasuda, M., Shimoyama, T., Kogure, J., Yokoyama, K., Koshiba, T.: Packed homomorphic encryption based on ideal lattices and its application to biometrics. In: Security Engineering and Intelligence Inf. Volume 8128 of LNCS. (2013) 55–74
2. Yasuda, M., Shimoyama, T., Kogure, J., Yokoyama, K., Koshiba, T.: Practical packing method in somewhat homomorphic encryption. In: DPM/SETOP. Volume 8147 of LNCS. (2013) 34–50