AN EFFICIENT PROTOCOL FOR PRIVATE IRIS-CODE MATCHING BY MEANS OF GARBLED CIRCUITS

Ying Luo, Sen-ching Samson Cheung[*]

Center for Visualization and Virtual Environments
University of Kentucky, USA

Tommaso Pignata, Riccardo Lazzeretti, Mauro Barni

Information Engineering Department
University of Siena, Italy

ABSTRACT

Biometric-based access control is receiving increasing attention due to its security and ease-of-use. However, concerns are often raised regarding the protection of the privacy of enrolled users. Signal processing in the encrypted domain has been proposed as a viable solution to protect biometric templates and the privacy of the users. In particular, several solutions have been proposed to protect the privacy of the biometric probe during the authentication process. In this paper we focus on privacy-preserving iris-based authentication. The main innovations compared to the prior art include: i) an iris masking technique that simplifies the operations on the encrypted data without sacrificing the recognition rate; ii) the adoption of a matching protocol based only on garbled circuits which offers longer term security over existing solutions based on homomorphic encryption or hybrid techniques. The computational and communication complexity of the on-line phase of the proposed protocol is extremely low, thus opening the way to its exploitation in practical applications.

***Index Terms*—** Private Iriscode Matching, Garbled Circuit, Biometric Authentication

1. INTRODUCTION

Due to their immutable and highly-discriminative characteristic, biometric signals such as faces, iris, and fingerprints are widely employed in access control system to authorize the users' membership. However, the widespread deployment of biometric access control system has raised serious concerns about the leakage of the individual's privacy. Since the biometrical signals are unique to each individual, the compromise of biometric signals in one system will directly endanger the security of other systems using the same biometric signals. To mitigate the concerns on the loss of privacy, it is imperative to process the biometric data in a privacy-preserving way.

One approach to protect the privacy of both the biometric server and the probe owner is to treat the matching process as an instance of Secure Function Evaluation (SFE) which guarantees the privacy of both the biometric gallery and the probe. The two prevailing approaches of implementing SFE are to use Garbled Circuits (GC) [1] and Homomorphic Encryption (HE) [2]. GC provides a generic implementation of any binary function by having one party prepared an encrypted boolean circuit, and another party obliviously evaluated the circuit without access to intermediate values. HE is an asymmetric public-key cipher that allows certain arithmetic operations such as addition to be directly performed on the encrypted data.

In this paper, we focus on using SFE to implement the iriscode matching process as described in [3]. The matching between two binary iriscodes is based on a combination of hamming distance and iris masks that remove erroneous parts of the codes. A customized SFE of iriscode was first proposed in [4] which is based on Paillier HE [5]. While HE is very efficient for large integer fields, iriscode matching consists of mostly binary operations and is conceptually more suitable for GC. Blanton et al. proposed a hybrid approach of GC and HE for iriscode and achieved a more efficient implementation [6]. Recent research efforts have significantly improve the efficiency of GC [7, 8]. Moreover, GC is likely to become a more efficient alternative than HE as GC theory relies almost exclusively on symmetric encryption and HE on asymmetric encryption. The former is characterized by shorter security parameters, which become more pronounced when we pass from short term to medium term and long term security [9]. As such, it is attractive to develop the iriscode matching by using only GC. In this paper, we demonstrate a computationally efficient GC-based iriscode matching algorithm. A novel contribution is the adoption of a simplified masking technique for iriscode which significantly reduces the complexity of the circuit.

The rest of the paper is organized as follows: Section 2 presents the overall design of a GC-based private iriscode matching system. The impact on privacy and efficiency of mask simplification in iriscode matching is explained in Section 3. Experiment results and discussions are presented in Section 4. We conclude this paper with prospect for the future work in Section 5.

2. GC-BASED IRISCODE MATCHING

In our proposed system, the biometric server, Bob, has an iris gallery which stores the iris features $\{X_1, \ldots, X_N\}$ of N members. X_i is a binary vector denoted as $(x_{i1}, \ldots, x_{in})$. The user, Alice, provides a probe $q = (q_1, \ldots, q_n)$ and evaluates the GC which produces a match if there exists at least an $i \in \{1, \ldots, N\}$ such that $d(q, X_i) < \epsilon$ for a similarity threshold ϵ. $d(q, X_i)$ is a modified Hamming Distance (HD) defined below:

$$d(q, X_i) := \frac{D(q, X_i)}{M(q, X_i)} = \frac{\| (q \otimes X_i) \cap mask_q \cap mask_{X_i} \|}{\| mask_q \cap mask_{X_i} \|} \tag{1}$$

In (1), $\otimes$ denotes XOR, $\cap$ AND, and $\| \cdot \|$ the norm of the binary vector. $mask_q$ and $mask_{X_i}$ are the corresponding binary masks that zero out the unusable portion of the irises due to occlusion by eyelids and eyelash, specular refections, boundary artifacts of lenses, or poor signal-to-noise ratio.

[*] Part of this material is based upon work supported by the National Science Foundation under Grant No. 1018241. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

We adopt the typical semi-honest adversary model in our system that Alice and Bob will faithfully follow the protocol but are free to extract additional information from the received data. Our protocols guarantee that only the final matching result could be shared by two parties. The biometric probe is protected from Bob and Bob's biometric database is kept secret from Alice under any polynomial-time attacks. We will not consider the attacks on the misuse of the biometric database, which is out of scope of this paper.

In our protocol, we use GC to implement the above framework. The basic principle of GC is described in [1] and we summarize it as follows: Bob first constructs a circuit for computing the final result of iriscode matching. After Alice receives the circuit, she uses 1-out-of-2 Oblivious Transfer (OT) [10] to input her probe and computes the output of the circuit without learning any intermediate values.

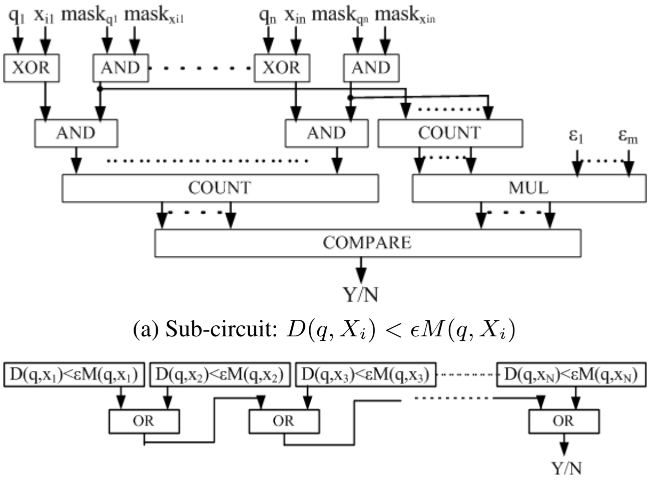
Figure 1(a) shows the circuit for private iris-code matching between the probe q and the entry X_i in the database. It uses the basic garbled circuits (XOR, AND, and MULtiplication), a COUNT circuit to compute the number of ones in its input [11], and a COMPARE circuit to check if the first input is lower than the second input [12]. Considering that the division in (1) is a complicated circuit [13] and multiplication involves fewer gates than division [14], we roll the denominator $M(q, X_i)$ of (1) into the similarity threshold ϵ and test whether $D(q, X_i) < \epsilon \cdot M(q, X_i)$ instead of $d(q, X_i) < \epsilon$. Since all computation should be computed over integers and ϵ is a decimal in the range $[0, 1]$, we scale up ϵ, which is multiplied by 2^m, to an integer in the range $[0, 2^m]$ before taking part in the multiplication circuit with $M(q, X_i)$. Also, $D(q, X_i)$ is left shifted by m bits so the real COMPARE checks the result of $D(q, X_i) \cdot 2^m < (\epsilon \cdot 2^m) \cdot M(q, X_i)$. In order to highlight the overall structure of the circuit, we hide the scale-up processing and use $D(q, X_i)$ and ϵ instead of $D(q, X_i) \cdot 2^m$ and $\epsilon \cdot 2^m$ in Figure 1(a).

The output of the sub-circuit $D(q, X_i) < \epsilon \cdot M(q, X_i)$ cannot be known by Bob in plaintext, otherwise, Bob will know the exact entry that matches the probe and reveal Alice's identity. In Figure 1(b), we use OR gates to connect the outputs of all COMPARE sub-circuits $D(q, X_i) < \epsilon \cdot M(q, X_i)$ for $i \in \{1, \ldots, N\}$ together. In the end, only the final output of all OR gates will be decoded and shared by two parties.

Since XOR gates can be evaluated for free without communication between two parties [7], only non-XOR gates are considered for complexity analysis. In the sub-circuit shown in Figure 1(a), a substantial number of gates are devoted to incorporate individual masks in the calculation – there are n AND gates used to compare the two masks and n AND gates for the actual masking, where n is the bit-length of the iriscode; a COUNT circuit is used to aggregate the number of non-zero common mask bits and a MUL circuit to combine the result with the similarity threshold. As such, any effort to minimize or even eliminate the variability among masks, without sacrificing the precision, can significantly reduce the complexity of the circuit. We explore the feasibility of such an approach in the next section.

3. SIMPLIFICATION OF IRIS MASKS

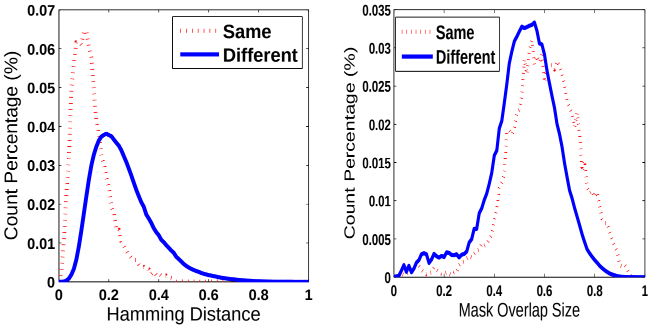
In this section, we will exploit the impact on privacy and efficiency of mask simplification in iriscode matching. Each iris-code consists of two parts: iris feature and mask. While the iris feature is confidential data, it is unclear if the mask itself contains enough sensitive information for identification. In [4], it is assumed that masks do not disclose identify information and are treated as public information. Such an approach can significantly reduce complexity as alluded in Section 2. Let us first check whether such an assumption is valid.



(a) Sub-circuit: $D(q, X_i) < \epsilon M(q, X_i)$

(b) Whole Circuit

Fig. 1. Circuit design for private iriscode matching



(a) Hamming Distances

(b) Masks Overlap Sizes

Fig. 2. Mask distance distributions

3.1. Privacy and similarity among iris masks

First, we inspect the relationship between masks and iris similarity. Li et al. have performed East-Asian/Caucasian classification based on the investigation of eyelashes, which make up most of the masks [15]. It has been shown that masks have inherent correlation, even though they only include the part of eyelashes close to the irises and cannot recover the original shape of the eyelashes. In this section, we test a hypothesis that masks from the same individual are similar to those from different individuals. If this hypothesis is accepted, there is no identity information leaked through masks and thus can be released to public.

We use CASIA-IrisV3-Lamp iris database for our similarity experiment [16]. To ensure that we begin with a good quality set of samples, we removes erroneous samples which cannot extract accurate iriscode based on the Matlab feature generation code from [17]. Finally, 3763 samples from 292 individuals are included in our dataset. $28,006$ pairs between the same individuals and $7,050,197$ pairs between different individuals are compared based on the normalized hamming distance (HD).

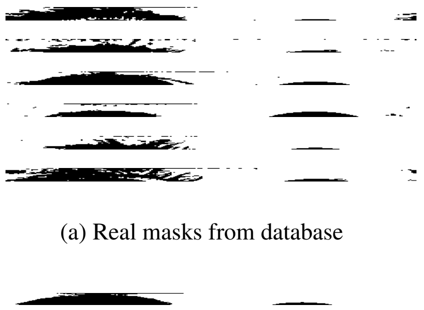
Figure 2(a) shows the distribution of these two types of HDs. We can easily find the distinct difference between the two distributions.

To further test if the difference between hamming distances from the same and different individuals are statistically significant, we utilize the distribution-free Wilcoxon Rank-Sum Test between these two samples [18, Ch.15]. The sample from the same indivuduals' HDs are labeled as X and the sample from different indivuduals' HDs as Y. Let u_1 and u_2 be the averages of X and Y respectively. The null hypotheses is $H_0 : u_1 - u_2 = 0$ and the alternative hypothesis is $H_a : u_1 - u_2 \neq 0$. When the samples from X and from Y are pooled into a combined sample of size $m + n$, these observations are sorted from smallest (rank 1) to largest (rank $m + n$). Then the sum of ranks of all samples from X is considered as our test statistic W, i.e. $W = \sum_{i=1}^{m} R_i$ where R_i is the rank for the i-th sample of X. Due to the large sample size, the distribution of the test statistic $z = (W - \mu_W)/\sigma_W$ can be approximated by a standard normal distribution if H_0 is true where

$$\begin{aligned} \mu_W &= \frac{m(m+n+1)}{2} = 9.91 \times 10^{10} \\ \sigma_W^2 &= \frac{mn(m+n+1)}{12} = 1.16 \times 10^{17} \end{aligned}$$

At the confident level of 99%, H_0 is rejected if either $z \geq 2.58$ or $z \leq -2.58$. In our experiments, $W = 5.19 \times 10^8$ which implies that $z = -288.91$. The null hypothesis is therefore rejected.

To further illustrate the difference, the distribution of mask overlap sizes, $\|mask_{\mathbf{x}} \cap mask_{\mathbf{y}}\|$, is shown in Figure 2(b). It shows that masks from the same individuals have larger overlap than from different individuals. This result can also be verified by Wilcoxon Rank-Sum Test, which is omitted here as it is essentially the same as the test of the HDs. Based on these two tests, we conclude that masks have inter-correlation among each individual, and therefore, should not be shared between Alice and Bob.



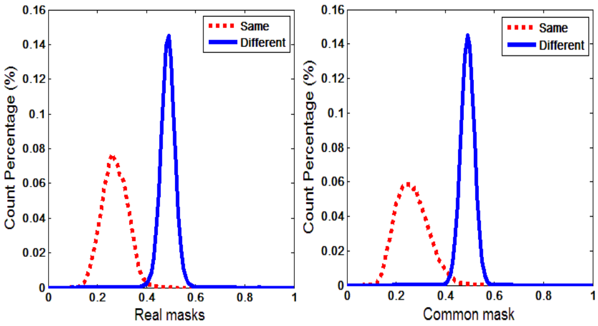
(a) Real masks from database

(b) Common mask

Fig. 3. Real masks and common mask

3.2. Common mask for all irises

Since the information of masks cannot be shared, we exploit a different approach to simplify the usage of masks. A typical mask contains information about eyelashes, eyelids, specular reflections, or other noise. Samples of masks from different individuals are shown in Figure 3(a). We can observe that there are a great deal of similarity among masks even from different individuals. Also, our earlier experiments depicted in Figure 2(a) indicate that there could be up to 50% bit difference even between masks from the same individual. As such, it is conceivable to use a common mask to replace individual masks without much loss in precision. As we have pointed out earlier, the use of a common mask can significantly reduce the complexity of our GC circuits. To test our hypothesis, we use the following method to derive the common mask: first, we pre-align all iriscodes in Bob's database, both features and masks, to the position which can get the minimum Hamming distance between every two pairs of the same individual. The common iris mask is set to '1' at all bit positions where the percentages of the pre-aligned masks being '1' at those positions exceed an empirically-determined threshold λ. The common mask obtained from the CASIA iris database is shown in Figure 3(b).



(a) Real masks

(b) Common mask

Fig. 4. HD distributions

Figure 4 shows the distribution of HDs using both real masks and the common mask. When $\epsilon = 0.41$, False Accept Rate (FAR) is 0.53% while False Reject Rate is 0.54% for the distribution computed with real masks. The best FAR and FRR is 1.44% and 1.47% at $\epsilon = 0.43$ for the distribution with the common mask, based on setting λ to 80%. We can see that the accuracy in the case of common mask is reduced by less than 1%.

Assuming the common mask is known to both Bob and Alice, the simplified GC sub-circuit for $D(q, X_i) < \epsilon M(q, X_i)$ is shown in Figure 5 and the whole circuit is the same as Figure 1(b). In Figure 5, we use MASK to denote the common mask and the blue-line block to highlight the gates that can be pre-computed. MASK_FILTER is a circuit which only accepts the iriscodes to participant to the matching processing with the set of corresponding masks. The performance of GC-based private iriscode matching with the simplified mask is demonstrated in Section 4.

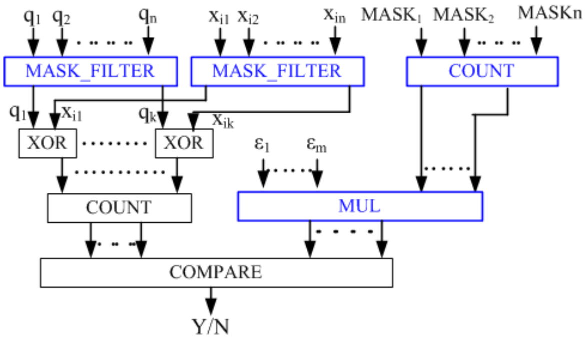


Fig. 5. Simplified GC sub-circuit for $D(q, X_i) < \epsilon M(q, X_i)$

4. EXPERIMENTS

All our experiment are written in Java and run on an Intel Core2 Duo CPU E8400 @3.00GHz 3.00GHz with 8GB RAM on 64-bit windows 7 Professional. We analyze the results using two sets of iriscodes – the length of an iriscode is $n = 2048$-bit based on the system by Daugman [3] and $n = 9600$-bit based on an open source iris recognition system in [17]. Note that circuit construction, circuit transmission and OT can be performed offline [10], we do not analyze the precomputation for circuit construction and circuit transmission since they are executed only once. We count the OT precomputation as the offline time since it needs to be done every time when our protocol is implemented. The OT offline time is independent of the size of biometric database but related to the length of the iriscode, as shown in Table 1. Table 1 also lists the total amount of non-XOR gates and runtime needed to implement the sub-circuit to test if $D(q, X_i) < \epsilon \cdot M(q, X_i)$, together to the total amount of data transmitted during the online computation. The results are derived by averaging the comparisons of 100 pairs of iriscodes in the database.

The performance of the totally GC-based private iris-code matching is quite efficient: when we adopt 80-bit security parameter, it takes 563 ms to compare two 2048-bit iris-codes with private iris features and masks. If the common mask is used, a speedup factor of up to 8.7 or 65 ms per comparison can be achieved. This is comparable to 14 ms as reported in [6] but with a pure GC implementation.

Considering that longer cyphertexts will be required to guarantee security with the rapid development in computational capability, we also list the processing time with the longer term security parameters (112 and 128 bits) in Table 1. The execution time is increased by 11% for the individual masks and 23% for the common mask. These are much smaller than the 62% increase for the hybrid protocol as reported in [19]. As such, our GC-only protocol is clearly preferred in the cases when longer term security is needed.

Table 1. Number of non-XOR gates, runtime (ms) and bandwidth (KB) based on different secure parameters (bit)

n-bit	# non -XOR	Sec Para.	OT Offline Time	Online Time		Overall Time	Band-width
				Alice	Bob		
Individual Masks							
2048	8349	80	19,767	40	108	563	571.5
		112	20,260	49	113	606	754.0
		128	20,425	61	109	608	845.7
9600	38654	80	90,744	102	508	2530	2655.0
		112	93,441	106	539	2769	3503.2
		128	92,736	128	557	2816	3828.5
Common Mask							
2048	2059	80	10,379	11	24	65	133.7
		112	10,396	11	29	74	176.5
		128	10,399	16	30	80	197.9
9600	9641	80	45,354	26	115	538	626.1
		112	45,431	28	119	545	826.5
		128	45,313	57	130	573	926.7

5. CONCLUSION

In this paper, we have developed an efficient GC protocol for private iriscode matching. A simplified mask scheme is designed to reduce the number of non-XOR gates used in the circuit. Such a design reduces the accuracy by less 1% but provides more than eight fold increase in performance. Our result is comparable to the current state-of-the-art implementation based on a hybrid protocol of GC and HE. Moreover, our GC-only protocol is more suitable than HE based approach as the computational complexity of GC circuits scales better for long-term security. However, one shortcoming of using GC is that the memory requirement of GC increases with the size of database. We are currently exploring to improve the memory requirement of GC with the incorporation of the technique proposed in [20], which makes GC scale to unlimited gates using a nearly constant amount of memory.

6. REFERENCES

[1] A. C. Yao, "Protocols for secure computations," in *Proceedings of the 23rd Annual IEEE Symposium on Foundations of computer science*, 1982.

[2] C. Fontaine and F. Galand, "A survey of homomorphic encryption for nonspecialists," *EURASIP Journal on Information Security*, vol. 2007, 2007.

[3] John Daugman, "How iris recognition works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 4, pp. 21–30, Jan. 2004.

[4] Y. Luo, S-C S. Cheung, and S. Ye, "Anonymous biometric access control based on homomorphic encryption," in *IEEE International Conference on Multimedia & Expo*, Cancun, Mexico, June 2009.

[5] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT ?9)*, vol. vol. 1592, pp. 223–238, May 1999.

[6] M. Blanton and P. Gasti, "Secure and efficient protocols for iris and fingerprint identification," Tech. Rep., Cryptology ePrint Archive, Report 2010/627, 2010. http://eprint.iacr.org, 2010.

[7] V. Kolesnikov and T. Schneider, "Improved garbled circuit: Free xor gates and applications," *Automata, Languages and Programming*, pp. 486–498, 2008.

[8] B. Pinkas, T. Schneider, N. Smart, and S. Williams, "Secure two-party computation is practical," *Advances in Cryptology–ASIACRYPT 2009*, pp. 250–267, 2009.

[9] E. Barker, W. Burr, A. Jones, T. Polk, S. Rose, M. Smid, and Q. Dang, "Recommendation for key management," *NIST special publication*, 2009.

[10] D. Beaver, "Precomputing oblivious transfer," *Advances in CryptologyCRYPT095*, pp. 97–109, 1995.

[11] M. Barni, J. Guajardo, and R. Lazzeretti, "Privacy preserving evaluation of signal quality with application to ecg analysis," in *Information Forensics and Security (WIFS), 2010 IEEE International Workshop on*. IEEE, 2010, pp. 1–6.

[12] V. Kolesnikov, A.R. Sadeghi, and T. Schneider, "Improved garbled circuit building blocks and applications to auctions and computing minima," *Cryptology and Network Security*, pp. 1–20, 2009.

[13] R. Lazzeretti and M. Barni, "Division between encrypted integers by means of garbled circuits," *The 2011 IEEE Intl. Workshop on Information Forensics and Security (WIFS'11)*, 2011.

[14] V. Kolesnikov, A.R. Sadeghi, and T. Schneider, "How to Combine Homomorphic Encryption and Garbled Circuits," *Signal Processing in the Encrypted Domain*, pp. 100–121, 2009.

[15] Y. Li, M. Savvides, and T. Chen, "Investigating useful and distinguishing features around the eyelash region," in *2008 37th IEEE Applied Imagery Pattern Recognition Workshop*. 2008, IEEE.

[16] T. Tan and Z. Sun, "Casia-irisv3," Tech. Rep., Chinese Academy of Sciences Institute of Automation, http://www.cbsr.ia.ac.cn/IrisDatabase.htm, 2005.

[17] L. Masek and P. Kovesi, "Matlab source code for a biometric identification system based on iris patterns," Tech. Rep., The School of Computer Science and Software Engineering, The University of Western Australia, 2003.

[18] J.L. Devore, "Probability and Statistics for Engineering and the Science, Brooks/Cole Pub," *Co., Monterey, California*, vol. 704, 1991.

[19] A.R. Sadeghi, T. Schneider, and I. Wehrenberg, "Efficient privacy-preserving face recognition," *Information, Security and Cryptology–ICISC 2009*, pp. 229–244, 2010.

[20] Y. Huang, D. Evans, J. Katz, and L. Malka, "Faster secure two-party computation using garbled circuits," in *USENIX Security Symposium*, 2011.