

引用格式:杨雄,张晓惠. 基于全同态加密的人脸特征密文认证系统[J]. 微电子学与计算机,2020,37(9):56-61. [YANG X, ZHANG X H. Face feature ciphertext authentication system based on fully homomorphic encryption[J]. Microelectronics & Computer,2020,37(9):56-61.]

基于全同态加密的人脸特征密文认证系统

杨 雄,张晓惠

(福州大学 至诚学院计算机工程系,福州 福建 350002)

摘 要: 随着人脸识别系统的广泛采用,基于人脸识别的身份认证系统必须充分考虑用户人脸特征的安全性. 为防止人脸特征泄漏,人脸特征不能以明文形式进行操作和存储. 针对此问题,设计了基于全同态加密的人脸特征密文认证系统,该系统在加密域中进行人脸特征匹配,同时数据库中保存的是人脸特征模板的同态密文,整个系统无需解密人脸特征模板就可完成认证. 系统实现部分借助了微软的开源简单加密算法函数库,并进一步探索了一种批处理和降维的方案,以权衡人脸匹配的准确性和计算复杂性. 基于人脸基准数据库(LFW、IJB-A、IJB-B、CASIA)的测试结果表明,基于全同态加密的人脸特征密文认证是可行的,能够基本满足真实应用场景的需求.

关键词: 全同态加密;人脸特征;SEAL

中图分类号: TP3 **文献标识码:** A **文章编号:** 1000—7180(2020)09—0056—06

Face feature ciphertext authentication system based on fully homomorphic encryption

YANG Xiong,ZHANG Xiao-hui

(Dept. of Computer Engineering, Zhicheng College of Fuzhou University, Fuzhou 350002, China)

Abstract: With the widespread adoption of face recognition systems, identity authentication systems based on face recognition must fully consider the security of user face features. To prevent face feature leakage, face features cannot be manipulated and stored in clear text. Aiming at this problem, a face-character ciphertext authentication system based on fully homomorphic encryption is designed. The system performs face feature matching in the encrypted domain. At the same time, the database stores the homomorphic ciphertext of the face feature template. The whole system Authentication can be done without decrypting the face feature template. The system implementation part relies on Microsoft's open source simple encryption algorithm library, and further explores a batch and dimension reduction scheme to balance the accuracy and computational complexity of face matching. The test results based on face reference database (LFW, IJB-A, IJB-B, CASIA) show that face-based ciphertext authentication based on fully homomorphic encryption is feasible and can basically meet the needs of real application scenarios.

Key words: fully homomorphic encryption;face feature;SEAL

1 引言

泛的应用,然而这种技术的广泛部署使用也使其成为恶意攻击的首选目标之一. 针对人脸识别系统最直接的攻击点之一就是人脸模板数据库. 因此,若将

近几年人脸识别技术在各种场景中都得到了广

人脸特征以明文形式直接存储于数据库中,会严重影响注册用户的隐私和认证系统的安全性^[1-2].为提高人脸识别系统的安全性可使用密码系统来保护人脸模板数据库并对加密的人脸特征数据执行匹配操作.然而,通用加密方案不支持在加密域中进行模板匹配所需的基本算术运算.另一方面,同态加密系统是一类特殊的密码系统,能够支持对加密数据进行基本的算术运算^[3-6].

前沿的人脸匹配方法都是基于深度神经网络的技术,这些方法依赖于卷积神经网络模型^[7-9]提出人脸特征.因此,要确保从此类模型中提取的人脸特征能够在加密域中进行安全匹配.关键技术障碍在于全同态加密的计算复杂性,尤其是乘法运算^[10].

本文基于全同态加密方案 Fan-Vercauteren^[11]提出了一种更高效的解决方案,探索了使用全同态加密的人脸模板进行人脸匹配的实用性.

2 基于全同态加密的人脸特征密文认证方案设计

一个典型的人脸识别系统包括了由已注册用户的人脸特征所构成的人脸模板数据库 $X = \{x_1, x_2, \dots, x_n\}$. 当用户进行身份认证时,需要从摄像头采集的人脸图像中提取当前人脸特征 y ,将 y 与其数据库中的人脸模板 X 进行匹配操作,匹配结果即为 y 和 X 之间的相似程度.将 y 和 X 之间的相似度定义为:

$$\begin{aligned} d(x, y) &= 1 - \frac{x^T y}{\|x\| \|y\|} \\ &= 1 - \tilde{x}^T \tilde{y} = 1 - \sum_{i=1}^d \tilde{x}_i \tilde{y}_i \end{aligned} \quad (1)$$

式中, $\tilde{x} = \frac{x^T}{\|x\|}$, d 为所提取的人脸特征维度.

从公式(1)可知,人脸的匹配过程包含了 d 组向量的乘法和 d 组向量的加法.

为了防止用户个人信息的泄露,则需要对 y 和 X 做加密处理,可通过定义一个参数化函数将人脸模板 z 进行空间变换: $\epsilon(z) = f(z; \theta_e)$, 其中 $f(\cdot; \theta_e)$ 为带参数 θ_e 的空间变换函数;同时 $z = g(\epsilon(z); \theta_d)$, 其中 $g(\cdot; \theta_d)$ 为带参数 θ_d 的空间反变换函数.使用空间变换函数的目的是为了保证原始人脸特征 z 的安全性,但同时也必须允许在转换后的空间中进行模板匹配而不会损失精度,即:

$$\begin{aligned} d(\epsilon(x), \epsilon(y)) &= d(f(x; \theta_e), f(y; \theta_e)) \\ &\approx d(x, y) \end{aligned} \quad (2)$$

2.1 用户注册和身份认证协议

本节描述基于全同态加密系统实现空间转换功能的用户注册和身份认证协议.考虑具有两个实体的场景:一个设备和一个数据库.

2.1.1 注册协议

在注册阶段,标识为 c 的用户需要执行如下步骤:

- (1) 生成一对公私密钥对,其中公钥为 θ_e ,私钥为 θ_d ,每个用户可拥有独立的公私密钥对;
- (2) 将公钥 θ_e 保存到数据库中;
- (3) 采集用户 c 的多张人脸图像并提取每张图像的人脸特征值 $X_c = \{x_1^c, x_2^c, \dots, x_{n_c}^c\}$, 其中 n_c 为该用户注册时所使用的人脸样本数量;
- (4) 使用公钥 θ_e 加密用户的样本人脸特征值,将加密的多个人脸模板与该用户身份标签一起保存到数据库中.

注册后数据库中添加了新注册用户加密后的人脸模板、公钥 θ_e 和用户标识,私钥 θ_d 则保存于设备中.注册过程如图1所示.

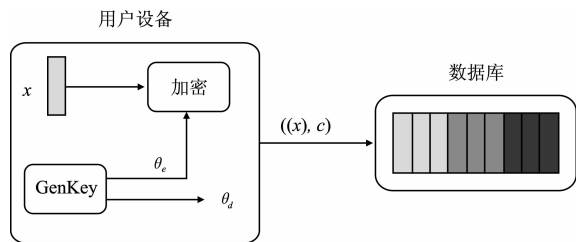


图1 用户注册过程

2.1.2 身份认证协议

在此阶段,设备将通过以下步骤对用户进行身份认证:

- (1) 采集待认证用户的人脸图像并提取其特征值 y ;
- (2) 使用公钥 θ_e 加密人脸特征值,使用的公钥 θ_e 可能与 θ_e^c 不同;
- (3) 将加密后的人脸特征值和待认证用户的声称身份 c' 同时发送给数据库,倘若使用的公钥 θ_e 与 θ_e^c 不同,那么公钥 θ_e 也需要发送给数据库.此时,在数据库中还需要执行密钥交换操作;
- (4) 计算加密模板 $\epsilon(y)$ 与数据库中用户 c' 的所有加密人脸特征模板之间的相似度 $d(\epsilon(y), \epsilon(x) c'_k)$,并将该相似度值返回给客户端;
- (5) 最后,在设备上通过私钥 θ_d 对相似度值进行解密后即可获取身份认证的结果,完成用户身份的验证.身份认证过程如图2所示.

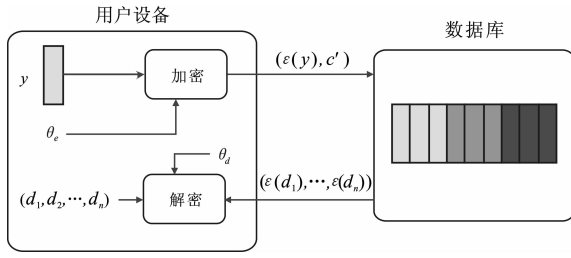


图2 用户身份认证注册过程

2.2 Fan-Vercauteren 方案

在 FV 方案中,任意数字 t (整数或有理数) 都必须先在环 R 中编码: $R_t = \frac{Z_t[x]}{x^n + 1}$, 然后才能够进行加密, 也意味着加密的数字在环中被编码为整数多项式. 令 λ 为安全参数, ω 是分解整数的基, $l = \log_{\omega} q$ 表示将整数 q 分别为 l 个部分. 在 FV 方案使用私钥 θ_d 、公钥 θ_e 和对加密数据进行乘法所必需的密文计算公钥 θ_{ev} . 该方案在加密整数上进行密钥生成、加法和乘法操作的具体步骤如下:

(1) GenKey(λ)

在 R_2 上随机选取一个元素作为私钥 $\theta_d \leftarrow R_2$, 接着在 R_q 上随机选取一个元素 $\alpha \leftarrow R_q$, 同时在高斯分布 X 上随机选取一个差错 $e \leftarrow X$, 通过计算

$\theta_e = ([-(\alpha \theta_d + e)]_q, \alpha)$ 获得一对公钥和私钥 (θ_e, θ_d) .

(2) GenEvKey(θ_d, ω)

令 $i \in \{0, \dots, l\}$, 在 R_q 上随机选取元素 $\alpha_i \leftarrow R_q$, 同时在高斯分布 X 上随机选取差错 $e_i \leftarrow X$, 通过计算 $\theta_{ev} = ([-(\alpha_i \theta_d + e_i) + \omega^i \theta_d^2]_q, \alpha_i)$ 得到密文计算公钥.

(3) Encrypt(m, θ_e)

为了加密消息 $m \in R_t$, 在 R_2 上随机选取一个元素 u , 同时在高斯分布 X 上随机选取两个差错 $e_1, e_2 \leftarrow X$, 计算密文 $ct = ([m + \theta_e[0]u + e_1]_q, [\theta_e[1]u + e_2]_q)$

(4) Decrypt(ct, θ_d)

根据密文 ct , 利用私钥 θ_d 计算出 $m' = [\frac{t}{q}[ct[0] + ct[1]\theta_d]]$.

(5) Add(ct_0, ct_1)

输入两个密文 ct_0 和 ct_1 , 通过计算 $(ct_0[0] + ct_1[0], ct_0[1] + ct_1[1])$ 求得这两个密文的和 $ct_0 + ct_1$.

(6) Multiply(ct_0, ct_1)

输入两个密文 ct_0 和 ct_1 , 通过如下计算求得这

两个密文的乘积 $ct_0 \times ct_1$:

$$c_0 = [\frac{t}{q}(ct_0[0] ct_1[0])]_q$$

$$c_1 = [\frac{t}{q}(ct_0[0] ct_1[1] + ct_0[1] ct_1[0])]_q$$

$$c_2 = [\frac{t}{q}(ct_0[1] ct_1[1])]_q$$

$$c_2 = \sum_{i=0}^l c_2^{(i)} \omega^i$$

那么计算:

$$c'_0 = c_0 + \sum_{i=1}^l \theta_{ev}[i][0] c_2^i$$

$$c'_1 = c_1 + \sum_{i=1}^l \theta_{ev}[i][1] c_2^i$$

得到 (c'_0, c'_1) 即为这两个密文的乘积 $ct_0 \times ct_1$.

使用上述算法使得人脸匹配能够在加密域中执行. 公式(1)中描述的人脸相似度可在加密域中描述为:

$$d(x, y) = 1 - g(\sum_{i=1}^d \epsilon(x_i) \epsilon(y_i), \theta_d) \quad (3)$$

那么对加密数据上计算内积则分别需要 d 次的加密乘法运算和 $d-1$ 次的加密加法运算. 但由于每次对加密数据的乘法运算量很大, 导致在加密域中计算人脸相似度的速度非常缓慢, 尤其在人脸特征高维度表示的场景下该问题会进一步加剧.

2.3 高效的全同态人脸匹配

尽管上述算法可直接用于人脸匹配, 但它的高计算要求无法满足实际部署应用的要求. 对于 512 维的人脸特征模板和 128 位的安全等级, 使用此算法需要每加密模板 16.5 MB 的存储空间和每对模板 0.7 秒的匹配时间. 为此, 本文使用了以下几种方案来解决这些限制. 首先, 提出了一种在环 R 中对人脸特征进行编码的量化方案; 接着, 使用了批处理技术, 利用中国剩余定理将向量编码为一个明文多项式, 以单个同态乘法的代价实现多个同态乘法, 从而能够显著提升计算效率. 最后, 利用经典的降维算法进一步减轻全同态人脸匹配的计算负担.

2.3.1 人脸特征编码

全同态加法和乘法的计算效率主要取决于选择用来表示多项式环 R_t 内人脸特征原始数值的编码方案. 为了保持同构计算的完整性, 所选的编码方案需要确保同构运算之后的值范围仍在环内. 因此, 将人脸特征原始值编码为基数 ω 的两位十进制整数: $\text{Encoding}(a) = \text{sign}(a)(a_{n-1}x^{n-1} + \dots + a_1x + a_0)$

(4)

此编码方案可以表示 $-(w^n - 1) \leq a \leq (w^n - 1)$ 范围内的任意整数.

2.3.2 批处理

加密人脸匹配的主要瓶颈是计算人脸计算相似度时所需的全同态乘法次数. Brakerski^[12] 提出了一种可针对数字向量进行同态加密和解密的技术, 而不是每次仅使操作单个数字. 该技术利用中国剩余定理 (Chinese Remainder Theorem, CRT) 将 n 个数编码到同一个多项式上. 对于给定模为 t 的 $2n$ 次本原单位根有:

$$x^n + 1 = (x - \epsilon)(x - \epsilon^3) \cdots (x - \epsilon^{2n-1}) \bmod t$$

当 t 为许多小素数的乘积时, 即 $t = \prod_{i=1}^k p_i$, 其中 $p_1, p_2, \dots, p_k$ 为不同的素数, 那依据中国剩余定理可对环 R_t 进行分解. 通过对每个素数进行模运算, 并使用 CRT 可获得给定素数乘积的计算结果. 由于对于这些素数的计算是彼此独立的, 所以这些计算是可以并行完成的.

给定两个向量 x 和 y , 可简单地将两个向量的和与内积转换为加密向量对应元素的加法和乘法的计算. 通过将 k 个数批处理到单个加密块中, 可在单次计算操作的时间成本内完成 k 次同态加法或乘积运算. 因此, 随着一次批处理数量的增加, 可显著提高计算效率. 但该方案的主要缺点是无法访问加密后向量中的各个元素, 导致无法计算元素之和. 此限制可以通过 Gentry^[13] 提出的循环旋转 $l = \log_w q$ 次并累加向量元素从而获得加密向量元素之和. 此过程的算法描述如下所述:

```
1: Function EncryptInnerProduct( $m, m'$ )
2:  $\epsilon(x) \leftarrow f(x, \theta_e)$ 
3:  $\epsilon(y) \leftarrow f(y, \theta_e)$ 
4:  $ct \leftarrow \text{Multiply}(\epsilon(x), \epsilon(y))$ 
5: for  $i = \{0, \dots, l\}$  do
6:    $ct \leftarrow ct + K_{g_i}(ct)$ 
7: end for
8: return  $ct$ 
```

通过循环旋转计算点积和的过程如图 3 所示.

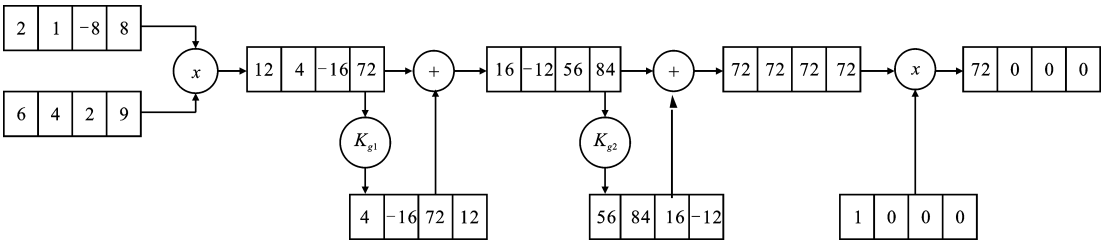


图 3 循环旋转计算点积和

2.3.3 降维

在加密域进行人脸匹配的高计算成本除了全同态乘法的高计算成本外, 还与高维度的人脸特征密切相关. 前者在一定程度上是通过批处理方案来解决, 但还是需要通过减少人脸特征维数来减轻计算负担. 本文使用经典的主成分分析法做为降维方案.

3 系统仿真测试

本文目的在于探索基于全同态加密进行人脸匹配的实用性和有效性, 因此在系统仿真测试中基于复杂度不同的多个数据集 (LFW、IJB-A、IJB-B 和 CASIA) 上分别使用基于深度神经网络的人脸模型 FaceNet 和 SphereFace 进行测试.

本文系统使用 C++ 语言在 Centos 7 上开发, 测试处理器为 Intel Core I5-6600, 同态加密算法采用微软开源的简单加密算法函数库 (Simple Encrypted Arithmetic Library, SEAL), 所有实验测

试均为单线程实现. SEAL 使用标准 C++ 编写的, 没有外部依赖关系. 目前 SEAL 库中已经支持的同态运算操作包括取反 (Negate)、加法 (Add)、累加 (AddMany)、减法 (Sub)、乘法 (Multiply)、累乘 (MultiplyMany)、平方 (Square)、幂方 (Exponentiate)、密文上加明文 (AddPlain)、密文上乘明文 (MultiplyPlain).

在进行人脸匹配实验之前, 需要先确定人脸匹配安全性和正确性所需的参数. 表 1 显示了不同参数 (n, q 和 t) 下人脸特征维数对全同态加密人脸匹配的计算复杂度的影响.

从表 1 可知, 在未使用批处理时, 即使最快的基于全同态加密的人脸匹配速度也要比非加密人脸匹配慢 1 000 倍以上. 但是, 批处理可以显著提高速度和节约内存.

在 Troncoso-Pastoriza 等人提出的基于 FHE 的人脸匹配方案中, 对于 512 维的人脸特征, 每个模板需要 48.7 MB 内存, 每对匹配大约需要 12.8 秒.

表 1 不同安全参数下维度对时间和内存的影响

安全等级/位	维	非同态加密		参数			批处理		未批处理	
		时间/ μ s	Mem/kB	n	t /位	q	时间/ms	Mem/kB	时间/ms	Mem/MB
128	64	0.44	2.0	128	110	40 961	0.25	2.0	9.66	0.25
	128	0.89	4.0	256	110	40 961	0.59	4.0	38.64	1.0
	512	3.48	16.0	1 024	110	40 961	2.45	16.0	624.07	16.5
	1 024	7.49	32.0	2 048	110	40 961	5.80	33.0	2 547.42	66.0
	1024	7.49	32.0	4 096	110	40 961	11.42	66.0	5 139.97	131.0
192	64	0.44	0.44	128	77	40 961	0.25	2.0	9.64	0.25
	128	0.89	0.89	256	77	40 961	0.55	4.0	38.33	1.0
	512	3.48	3.48	1 024	77	40 961	2.50	16.0	617.79	16.5
	1 024	7.49	7.49	2 048	77	40 961	5.35	33.0	2 545.38	66.0
	1 024	7.49	7.49	4 096	77	40 961	11.54	66.0	5 104.68	131.0

相比之下,本方案的测试结果表明,使用本文的 FHE 框架在加密域上进行人脸匹配不仅可以提供 128 至 192 位的高安全性,而且在小型人脸数据库上能够提供实时匹配.

进一步,由于本方案中全同态加密先对人脸特征值编码为整数后才进行操作,因此针对人脸特征值的编码分别设计了三种不同的量化方案,其编码精度分别为 0.1、0.01 和 0.0025.并在基准人脸数据集(LFW、LJB-A、LJB-B、CASIA)上分别使用了两种模型 FaceNet 和 SphereFace 进行人脸匹配实验.实验结果评估以未加密的人脸特征匹配性能作为基准,表 2 中列出了错误接受率 FAR 分别为 0.01%、0.1% 和 1.0% 时的正确接受率 TAR.

从表 2 可知,编码精度为 0.002 5 时其正确率能够达到未加密人脸特征的水准.因此,在提供人脸

模板保护、防止信息泄漏和保护用户隐私的同时,基于全同态人脸的匹配可达到与原始人脸特征匹配的性能.最后实验结果也表明,使用经典 PCA 的降维方法后,其性能不仅可与原始高维人脸特征持平,而且可提高全同态人脸的匹配效率.

4 结束语

本文探讨了使用全同态加密来保护人脸模板数据库的实用性.首先,利用了一个批处理方案,实现了在一次乘法运算中执行了多个同态乘法,进一步利用降维方案,显著提高了计算效率.对于 512 维的人脸特征,能够达到每个加密模板仅需要 16 KB 的存储空间和匹配一对加密模板 0.02 秒的时间.多个基准数据集的实验结果表明,全同态加密对于在加密域中进行精确人脸匹配是一种可行的实用解决方案,既保护了用户的隐私,又防止了信息泄漏.

表 2 人脸识别准确率(TAR @FAR in %)

数据集	方法	128 维 FaceNet			64 维 PCA FaceNet			512 维 SphereFace			64 维 PCA SphereFace		
		0.01%	0.1%	1%	0.01%	0.1%	1%	0.01%	0.1%	1%	0.01%	0.1%	1%
LFW	NO FHE	84.06	94.56	98.65	83.99	94.46	98.63	90.49	96.74	99.11	88.41	95.80	98.87
	FHE(2.5×10^{-3})	84.05	94.56	98.65	83.99	94.46	98.62	90.49	96.74	99.11	88.38	95.80	98.87
	FHE(1.0×10^{-2})	83.89	94.53	98.62	83.85	94.44	98.58	90.46	96.73	99.11	88.38	95.80	98.87
	FHE(1.0×10^{-1})	78.82	92.58	98.35	78.18	92.55	98.31	84.78	94.72	98.64	84.32	94.38	98.69
LJB-A	NO FHE	23.13	45.92	70.26	20.13	44.07	68.71	7.27	30.40	67.89	6.81	28.92	67.59
	FHE(2.5×10^{-3})	23.12	45.91	70.25	20.08	44.04	68.66	7.27	30.40	67.89	6.81	28.92	67.59
	FHE(1.0×10^{-2})	22.83	45.78	70.17	19.92	44.01	67.81	7.25	30.39	67.66	6.80	28.92	67.45
	FHE(1.0×10^{-1})	19.82	42.74	68.37	17.54	42.04	66.11	7.20	30.00	65.23	6.68	27.43	66.40
LJB-B	NO FHE	25.77	48.31	74.47	24.95	47.80	73.58	7.86	31.27	69.83	7.13	29.72	69.79
	FHE(2.5×10^{-3})	25.75	48.28	74.46	25.06	47.78	73.44	7.86	31.27	69.82	6.85	29.70	69.69
	FHE(1.0×10^{-2})	25.71	48.21	74.44	24.90	46.97	73.20	7.80	31.20	69.75	6.85	29.69	69.52
	FHE(1.0×10^{-1})	23.75	46.08	72.87	22.79	45.80	73.02	7.49	30.92	67.45	6.80	29.60	69.45
CASIA	NO FHE	70.98	84.70	93.29	70.85	84.69	93.28	86.48	90.81	93.83	82.87	89.07	92.80
	FHE(2.5×10^{-3})	70.98	84.70	93.29	70.85	84.69	93.28	86.47	90.81	93.83	82.78	89.04	92.78
	FHE(1.0×10^{-2})	70.96	84.68	93.28	70.92	84.62	93.26	86.47	90.80	93.81	82.74	89.00	92.77
	FHE(1.0×10^{-1})	70.82	84.66	93.25	70.78	84.59	93.22	83.21	89.49	93.05	78.82	87.29	92.16

参考文献:

- [1] MAI G C, CAO K, YUEN P C, et al. On the Reconstruction of Face Images from Deep Face Templates [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2019, 41(5): 1188-1202.
- [2] LIU Z, PING L, WANG X, et al. Deep Learning Face Attributes in the Wild [C]//International Conference on Computer Vision. Santiago: IEEE, 2015: 3730-3738.
- [3] FONTAINE C, GALAND F. A Survey of Homomorphic Encryption for Nonspecialists [J]. EURASIP Journal on Information Security, 2007(1): 1-10.
- [4] ZHAO Q S, ZENG Q K, LIU X M, et al. Verifiable Computation Using Re-randomizable Garbled Circuits [J]. Journal of Software, 2019, 30(2): 209-225.
- [5] LIN Z J, XU C X, W X F, et al. Application of (Full-y) Homomorphic Encryption for Encrypted Computing Models [J]. Journal of Cryptologic Research, 2017(6): 596-610.
- [6] YU L Z, LIN G X, JIE G Y, et al. Survey on Homomorphic Encryption Algorithm and Its Application in the Privacy-Preserving for Cloud Computing [J]. Journal of Software, 2018, 29(7): 1830-1851.
- [7] TAIGMAN Y, YANG M, RANZATO M, et al. DeepFace: Closing the Gap to Human-Level Performance in Face Verification [C]//Computer Vision and Pattern Recognition. Columbus: IEEE, 2014: 1701-1708.
- [8] SCHROFF F, KALENICHENKO D, PHILBIN J. FaceNet: A unified embedding for face recognition and clustering [C]//Computer Vision and Pattern Recognition. Boston: IEEE, 2015: 815-823.
- [9] LIU W Y, WEN Y D, YU Z D, et al. SphereFace: Deep Hypersphere Embedding for Face Recognition [C]//Computer Vision and Pattern Recognition. Hawaii: IEEE, 2015: 6738-6746.
- [10] TRONCOSO PASTORIZA J R, GONZALEZ JIMENEZ D, PEREZ GONZALEZ F. Fully Private Noninteractive Face Verification [J]. IEEE Transactions on Information Forensics and Security, 2013, 8(7): 1101-1114.
- [11] FAN J F, FREDERIK VERCAUTEREN. Somewhat Practical Fully Homomorphic Encryption [C]//Practice and Theory in Public Key Cryptography. Darmstadt: Springer, 2012: 1-16.
- [12] BRAKERSKI Z, GENTRY C, HALEVI S. Packed ciphertexts in LWE-based homomorphic encryption [M]. Berlin: Springer, 2013.
- [13] GENTRY C, HALEVI S, SMART N P. Fully Homomorphic Encryption with Polylog Overhead [C]//Theory and Applications of Cryptographic Techniques. Washington DC: Springer, 2012: 465-482.

作者简介:

杨雄男, (1986-), 硕士, 高级工程师. 研究方向为云计算、嵌入式应用.

张晓惠(通讯作者)女, (1984-), 硕士, 讲师. 研究方向为人工智能、网络安全. E-mail: 83789047@163.com.

(上接第55页)

- [3] FOUQUE P A, HOFFSTEIN J, LYUBASHEVSKY V, et al. Falcon: Fast-Fourier lattice-based compact signatures over NTRU [EB/OL]. [2019-12-01]. <https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/Falcon.zip>.
- [4] HOWE J, ORDER T, KRAUSZ M, et al. Standard lattice-based key encapsulation on embedded devices [J]. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018(3): 372-393.
- [5] KARMAKAR A, MERA J M B, ROY S S, et al. Saber on ARM cca-secure module lattice-based key encapsulation on ARM [J]. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018(3): 243-266.
- [6] ALBRECHT M R, HANSER C, HOLLER A, et al. Learning with errors on RSA co-processors [J]. IACR Cryptology ePrint Archive, 2018: 425.
- [7] SAARINEN M J O, BHATTACHARYA S, GARCI-A-MORCHON O, et al. Shorter messages and faster post-quantum encryption with Round5 on Cortex M [J]. IACR Cryptology ePrint Archive 2018: 723.
- [8] ORDER T, SPEITH J, HOLTGEN K, et al. Towards practical microcontroller implementation of the signature scheme Falcon [C]//International Conference on Post-Quantum Cryptography. [s. l.]. 2019: 65-80.

作者简介:

郭丽敏女, (1986-), 硕士, 工程师. 研究方向为密码芯片安全. E-mail: guolimin@fmsh.con.cn.

刘丹男, (1981-), 硕士, 工程师. 研究方向为密码芯片安全.

王立辉男, (1982-), 博士, 高级工程师. 研究方向为密码芯片安全.

李清女, (1968-), 硕士, 教授级高级工程师. 研究方向为集成电路设计开发.

俞军男, (1968-), 硕士, 教授级高级工程师. 研究方向为集成电路设计开发.