# Fully Private Non-interactive Face Verification

Juan Ramón Troncoso-Pastoriza, Daniel González-Jiménez, Fernando Pérez-González

***Abstract*—Face recognition is one of the foremost applications in computer vision, which often involves sensitive signals; privacy concerns have been lately raised and tackled by several recent privacy-preserving face recognition approaches. Those systems either take advantage of information derived from the database templates or require several interaction rounds between client and server, so they cannot address outsourced scenarios.**

**We present a private face verification system that can be executed in the server without interaction, working with encrypted feature vectors for both the templates and the probe face. We achieve this by combining two significant contributions: a) a novel feature model for Gabor coefficients' magnitude driving a Lloyd-Max quantizer, used for reducing plaintext cardinality with no impact on performance; b) an extension of a quasi-fully homomorphic encryption able to compute, without interaction, the soft scores of an SVM operating on quantized and encrypted parameters, features and templates. We evaluate the private verification system in terms of time and communication complexity, and in verification accuracy in widely known face databases (XM2VTS, FERET and LFW). These contributions open the door to completely private and non-interactive outsourcing of face verification.**

***Index Terms*—Privacy, Biometrics, Face Verification, Complexity, Full Homomorphic Encryption, Gabor Coefficients, Generalized Gaussian, Gabor Magnitude, Statistical Model, Quantization**

## I. Introduction

FACE recognition is an important and active area of research [3] whose interest has increased in recent years because of theoretical and application-driven motivations. Due to the sensitivity of the involved biometric signals, privacy has shown to be a serious concern when working with digital imagery, especially for those systems that must process, recognize or classify face images (*visual privacy* [4]).

There are several aspects that must be taken into account when dealing with biometric signals (faces, irises, fingerprints,...), like *revocability*, *performance* and *security/privacy* [5]. *Revocability* copes with the impossibility of reissuing the biometric information if it gets compromised; the *performance* of the original system should not be degraded by the template protection system. Finally, *security* and *privacy* are crucial aspects that deal with concealing the private biometrics so that they are not disclosed to unauthorized parties. These signals are intrinsically linked to the identity of an individual; hence, their disclosure to an attacker may not only leak information like age, gender or race (harming user privacy), but it may also be used for unauthorized impersonation of that individual (harming system security).

There are two groups of biometric template protection techniques proposed so far [5]: those based on *feature transformation* (e.g., biohashing) apply a transformation function parameterized by a random key to the biometrics before storing them on the database; matching is run on the transformed domain. Conversely, *biometric cryptosystems* or *helper data-based methods* (e.g., secure sketches, fuzzy commitments, fuzzy vaults) extract a key from the biometric features and some auxiliary (helper) data. The latter should leak a negligible amount of information about the biometric, as it is stored at the recognition server or publicly available. Matching is performed by checking the validity of the key extracted from the query biometric and the helper data.

All these systems construct a high entropy random sequence related to the biometric features through a cryptographic key or random salt. The secrecy of this key provides unlinkability, while revocability is achieved through the regeneration of the random sequence by choosing a different salt or key. But all these approaches disclose a *noisy* (quantized) version of the biometric features to the server that stores them. This version is not fully independent of the original features; it reveals some information about the latter, called privacy leakage [6].

An alternative formulation of privacy-preserving biometric systems aims at either computational or statistical secrecy about the biometric features through the use of Signal Processing in the Encrypted Domain (SPED) techniques. These involve semantically secure cryptosystems, homomorphic processing and multiparty computation protocols (like garbled circuits). SPED builds secure recognition protocols for which unauthorized parties cannot infer any information that they are not allowed to, so the main concern is privacy and performance. This is the framework to which this work belongs.

### A. Private Outsourced Face Verification Scenario

In a privacy-aware face recognition scenario, a user presents his/her face for matching against a database of enrolled clients, to find the corresponding identity. There are two possibilities:

- *Verification* (one-to-one): The server tests whether the query features match the database templates for the identity claimed by the user.

J.R. Troncoso-Pastoriza is with the Signal Theory and Communications Department, University of Vigo, Vigo 36310, SPAIN, e-mail: troncoso@gts.uvigo.es

D. González-Jiménez is with the Galician Research and Development Center in Advanced Telecommunications (GRADIANT), Vigo 36310, SPAIN, e-mail: dgonzalez@gradiant.org

Prof. F. Pérez-González is with the Signal Theory and Communications Department, University of Vigo, Vigo 36310, SPAIN, with the Galician Research and Development Center in Advanced Telecommunications (GRADIANT), Vigo 36310, SPAIN, and with the Dept. of Electrical and Computer Engineering, University of New Mexico, Albuquerque, NM, USA, e-mail: fperez@gts.uvigo.es

Part of this work has been presented at IEEE ICASSP 2010 [1] and at IEEE ICIP 2012 [2]

- *Identification* (one-to-many): The server has to find in the template database the identity that best matches the query features (if there is any).

The identification scenario involves running several verifications and later carrying out a comparison to choose the best match. In this work, we address the **private non-interactive verification scenario**, leaving aside the last comparison step, as it is not yet possible to perform that step non-interactively in an efficient way.

We assume that the database and the verification process are outsourced to an untrusted environment (e.g., a cloud). For the sake of clarity, we can give an exemplifying use-case, depicted in Fig. 1: a biometric access control system with high security requirements, whose sensor nodes cannot store the whole database of authorized users. This database is outsourced to an untrusted cloud storage and processing provider. Due to privacy concerns, the query faces must not be disclosed to the cloud. In turn, the sensor device at the facility may be a tamper-proof device, and it may have access to some private information before producing the verification answer. All the database information comes from the same facility, so all the records of the database are protected with the same encryption/decryption key pair, embedded in the tamper-proof sensor devices. It must be noted that keeping per-user keys to encrypt each record is also possible in the verification scenario we address, but it could not be straightforwardly translated into the identification one, as homomorphic operations typically work only on values encrypted with the same key (see [7]).

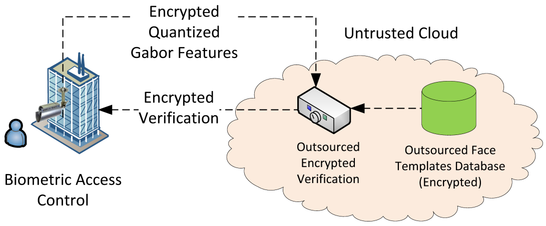


Fig. 1. Secure Outsourced Face Verification Scenario.

Regarding the attack and threat model in this scenario, we deal with semi-honest adversaries; i.e., the parties do not deviate from the protocol, but they may be curious and try to infer some information about the transcript. Coping with malicious adversaries, able to perform spoofing or replay attacks, would require additional mechanisms that fall out of the scope of this work.

### B. Related Work

There have been several proposals of efficient privacy-preserving solutions in biometric recognition, most of them in an **identification scenario**. Erkin *et al.* [8] and Sadeghi *et al.* [9] combine additive homomorphic encryption and garbled circuits. Both works focus on private face identification using Eigenfaces [10], which projects faces onto a PCA (Principal Component Analysis) subspace. Luo *et al.* [11] propose an anonymous biometric access control (ABAC) system for iris-based biometric identification using Paillier encryptions [12] and an interactive Hamming distance calculation. Osadchy *et al.* [13] design a novel face identification system using cryptography-amenable primitives like Hamming distance, to facilitate the design of the corresponding secure protocol. Barni *et al.* [14] present a secure fingerprint-based authentication system comprising three elements: a bank of Gabor filters for clear-text feature extraction; a secure Euclidean distance computation protocol, and a "*less than*" interactive secure protocol. Finally, Upmanyu *et al.* [15] use RSA's multiplicative homormorphism, and tune the tradeoff between identification accuracy versus security by increasing the communication complexity and the client-side computation load; non-linear operations are performed either as clear-text operations at the server, or approximated with interactive circuits.

### C. Our Contributions

Our formulation clearly differs from prior SPED-based works: they assume that the server is a trusted party with clear-text access to the biometric database, so they do not truly protect the privacy of the enrolled users in an outsourced verification scenario. Cloud-based services are being increasingly adopted, but, without appropriate measures, biometric privacy is a barrier for them. Thus, their need for effective privacy-preservation is essential [16]. This work addresses this problem, enabling the use of cloud-based services for biometric verification. We impose the following requirements: a) fully encrypted template database and query faces (total privacy); b) no interaction rounds for providing the verification result, and c) restrict the processing done by the client to encryption and decryption, so that lightweight client devices can engage in the secure verification protocol.

On top of a baseline Gabor-based face verification algorithm [17], we make two significant contributions that must be combined to reach a fully non-interactive solution: a) an efficient extension of Gentry's *somewhat* homomorphic cryptosystem [18], able to run the whole verification algorithm in the encrypted domain, and b) a non-linear quantization for Gabor features that achieves a great plaintext cardinality reduction. These two elements jointly enable the implementation of our non-interactive private system in an untrusted environment.

The closest related work is that of Barni *et al.* [14], which uses encrypted quantized Gabor features for fingerprint recognition. Besides the different scenario and our ability to work with encrypted query biometrics *and* encrypted templates, our work presents the advantage of homomorphically calculating low-degree polynomial functions, not being limited to Hamming distance or linear projections. Conversely, the server in [14] needs auxiliary values to compute an Euclidean distance, and it would also need interaction rounds for each multiplication if the database were encrypted. Finally, the quantization in [14] is linear, while we are proposing a non-linear Lloyd-Max quantization driven by our model for Gabor magnitudes.

With respect to [1], [2], here we provide a coherent and integrated vision of the two elements that comprise our privacy-preserving solution, with a more comprehensive explanation of the cryptosystem extension and a new security discussion; we employ more rigorous goodness-of-fit measures to validate the developed Gabor magnitudes model, and we also enhance our verification algorithm with different pre-normalization techniques and the use of a Support Vector Machine (SVM) classifier together with a more extensive and homogeneous experimental validation including more databases.

### *D. Notation and Structure*

Matrices and column vectors are respectively represented as uppercase and lowercase boldface letters, while random variables are represented as uppercase letters; $[a]_d$ represents the reduction of $a \bmod d$; vector notation $\boldsymbol{a} = [a_0, \ldots, a_{n-1}]$ and polynomial notation $a(x) = \sum_{i=0}^{n-1} a_i \cdot x^i$ will be used indistinctly when appropriate. Finally, $(a(x))$ represents the ideal generated by the polynomial $a(x)$, and $[\![x]\!]$ (resp. $[\![\boldsymbol{x}]\!]$) represents the encryption of $x$ (resp. of the elements of $\boldsymbol{x}$).

The rest of the paper is organized as follows: Section II presents our Gabor feature extraction process. Section III introduces and evaluates the used statistical model and quantization for Gabor coefficients magnitude. Section IV reviews fully homomorphic cryptosystems and presents the proposed extension and its homomorphic capacity. Section V shows the application of both contributions to a fully-private non-interactive face verification scenario, and evaluates its performance figures in widely known test face databases. Finally, Section VI discusses the security aspects of the extended cryptosystem, and Section VII draws some conclusions and future research lines.

## II. Gabor Features Extraction

Gabor filters have received great attention for face processing [19] due to biological reasons and because of their optimal resolution in both frequency and spatial domains [20].

One of the drawbacks of Gabor features [17] is their huge storage requirements. In this work, we take one step further in the reduction of the representation length needed for an efficient recognition, addressing the cardinality requirements that the encryption system presented in Section IV-C poses. In order to minimize the volume of data, we discard the phase information and use a novel statistical characterization to model magnitudes of Gabor coefficients [1], under the assumption that both real and imaginary parts are generalized Gaussian distributed with circular symmetry, and we propose two different quantizations, using levels and indices (cf. Section III-B). Some recent approaches showed the benefits of keeping Gabor phase for effective recognition [21], [22], but no clear improvements over magnitudes have been obtained on difficult scenarios (e.g. see [22]). Furthermore, magnitude-based systems can work, as in our case, with sparse points, while phase-based approaches require a dense filtering, producing feature vectors of large dimensionality. In any case, we aim at showcasing our secure system on a baseline polynomial verification function working with input signals of reduced cardinality and dimensionality.

Fig. 2 depicts our feature extraction process. It comprises a geometric normalization—so that eyes and mouth are in fixed positions—, cropping the faces to a common size ($120 \times 100$ pixels), and a photometric correction (histogram equalization and local mean removal). Afterwards, a bank of 40 Gabor filters [17] (8 orientations and 5 spatial frequencies per orientation) is applied to each node of a $10 \times 10$ grid superimposed to the image of the face. The outputs are Lloyd-Max quantized and encrypted prior to their transmission to the secure verification system.

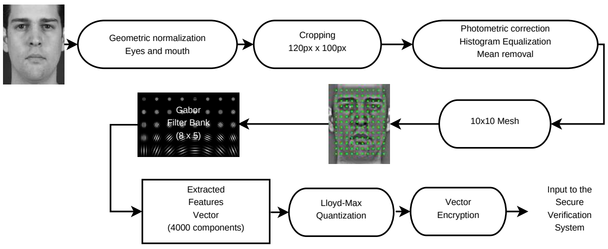


Fig. 2. Preprocessing, feature extraction and encryption steps performed at the client for our setup.

The next section presents our feature model, fit to the magnitudes of the "Extracted Features Vector" coefficients (Fig. 2), and used for optimal data compression at the "Lloyd-Max quantization" step in order to discretize the inputs and to reduce the plaintext cardinality prior to encryption.

## III. Theoretical Model for the magnitude of Gabor Coefficients

Generalized Gaussian (GG) distributions are a good fit for peaky and heavy-tailed random variables; examples of GG-modeled variables can be found in coefficients of many transforms, like DCT (Discrete Cosine Transform) or Wavelets [23], [24], and, especially, the marginals of Gabor coefficients [17]. A GG variable has the following density

$$f_{GG}(x) = \frac{\beta \cdot c}{2\Gamma(\frac{1}{c})} \cdot e^{-|\beta x|^c}, \quad \beta = \frac{1}{\sigma}\sqrt{\frac{\Gamma(\frac{3}{c})}{\Gamma(\frac{1}{c})}},$$

where $\Gamma(.)$ is the Euler Gamma function $\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} \cdot dt$, $\beta$ is a scale parameter, inversely proportional to the standard deviation $\sigma$ of the variable, and $c$ is a shape parameter (see [1], [17], [25] for further details). To the best of our knowledge, there is only a previous approach to modeling Gabor coefficients magnitude, proposed in [26], through the so called $\beta$-Rayleigh distribution, a generalization of the Rayleigh distribution with a shape factor $\beta$. Unfortunately, a $\beta$-Rayleigh-distributed magnitude cannot be obtained from GG marginals, so this model misses a connection with current models, which assume GG distributed real and imaginary parts.

We derive now our model for Gabor magnitudes. Let $g_i \in \mathbb{C}$ be one of the Gabor coefficients extracted from a face, and $gr_i, gi_i \in \mathbb{R}$ its real and imaginary parts, respectively. Both real and imaginary parts follow Generalized Gaussian marginals with the same parameters $(c, \sigma)$ [17]. We have observed that the phase of $g_i$ is approximately uniform, meaning that the distribution of each $g_i$ presents circular symmetry. Actually, independent bidimensional generalized Gaussian variables are not circularly symmetric (unless they are Gaussian, $c = 2$), and consequently $gr_i$ and $gi_i$ are not independent. In order to assimilate this dependency, we propose a doubly stochastic model for Gabor coefficients in which real and imaginary parts are marginally GG, but locally independent, identically distributed (i.i.d.) Gaussian with a non-constant deviation across locations and subjects (see [1] for further details).

For each coefficient $G_i$, we express $G_i = (C_i + j \cdot D_i) \cdot S_i$, where $C_i$ and $D_i$ are two independent Gaussian $\mathcal{N}(0,1)$, and $S_i$, independent of $C_i$ and $D_i$, is a non-negative random variable that models the non-constant deviation, such that $C_i S_i$ and $D_i S_i$, which model respectively the real and imaginary marginals of a Gabor coefficient, are Generalized Gaussians. As $S_i$ does not affect the phase, $C_i S_i$ and $D_i S_i$ preserve the circular symmetry. This model covers all the observed properties of Gabor coefficients, and allows us to calculate an accurate distribution for their magnitudes, for which we need to determine the distribution of $S_i$: it is the Gaussian transform [27] of a Generalized Gaussian variable (GTGG):

$$f_{S_i}(s^2) = \frac{1}{s^2}\sqrt{\frac{\pi}{2s^2}}\left(\mathcal{F}^{-1}\left(f_{G_i}(\sqrt{j\omega})\right)\right)_{t=\frac{1}{2\sigma^2}},$$

where $\mathcal{F}^{-1}$ represents the inverse Fourier Transform.

Then, the modulus of $G_i$ will be given by

$$|G_i| = \underbrace{\sqrt{C_i^2 + D_i^2}}_{R_i} \cdot S_i,$$

being $R_i = \sqrt{C_i^2 + D_i^2}$ Rayleigh distributed. We can obtain the density of a Gabor magnitude, represented as the product of a Rayleigh and an independent GTGG variable:

$$\begin{aligned} f_{|G_i|}(x) &= \int_0^\infty f_{S_i}(\sigma^2)\frac{x}{\sigma^2}e^{-\frac{x^2}{2\sigma^2}}\,d\sigma^2 \\ &= \int_0^\infty \frac{1}{\sqrt{2\pi}\sigma^2}\left(\int_{-\infty}^\infty \frac{\beta_i \cdot c_i}{2\Gamma(\frac{1}{c_i})}e^{-\beta_i^{c_i}(j\omega)^{c_i/2}+j\frac{\omega}{2\sigma^2}}\,d\omega\right)\cdot \\ &\quad \frac{x}{\sigma^2}e^{-\frac{x^2}{2\sigma^2}}\,d\sigma. \end{aligned}$$

Reversing the order of the integrals, we finally get

$$\begin{aligned} f_{|G_i|}(x) =& \frac{c_i\beta_i}{2\cdot\Gamma(\frac{1}{c_i})\cdot x}\cdot \\ & \int_0^\infty \left[\frac{\cos(\frac{3}{2}\tan^{-1}(\frac{\omega}{x^2}) - \beta^{c_i}\omega^{c_i/2}\sin(\frac{\pi c_i}{4}))}{(x^4+\omega^2)^{\frac{3}{4}}}\cdot \right. \\ & \left. e^{-\beta^{c_i}\cos(\frac{\pi c_i}{4})\omega^{c_i/2}}\right]d\omega. \end{aligned} \tag{1}$$

This integral can be numerically evaluated for a given pair $(c_i, \beta_i)$, obtaining a more peaky and heavy-tailed pdf than the Rayleigh (see [1], [25] for further details).

### A. Parameter Estimation and Goodness of Fit

We estimate the parameters $c, \sigma$ for our model using data from three known biometric face databases XM2VTS [28], FERET [29], and LFW [30]; we employ maximum likelihood (ML) estimation, using the numerical calculation of the pdf, Eq. (1). We get a perfect agreement between our model and the GG-marginals estimated parameters (see [1], [25] for details).

For evaluating the goodness of fit, we use two measures: the Kullback-Leibler divergence [31] (KLD) and Pearson's $\chi^2$ statistic. The KLD provides a measure of the statistical distance between two discrete distributions with probability functions $P$ and $Q$, and is given by

$$KLD(P,Q) = \sum_{i=0}^{K-1} P(i)\log\left(\frac{P(i)}{Q(i)}\right),$$

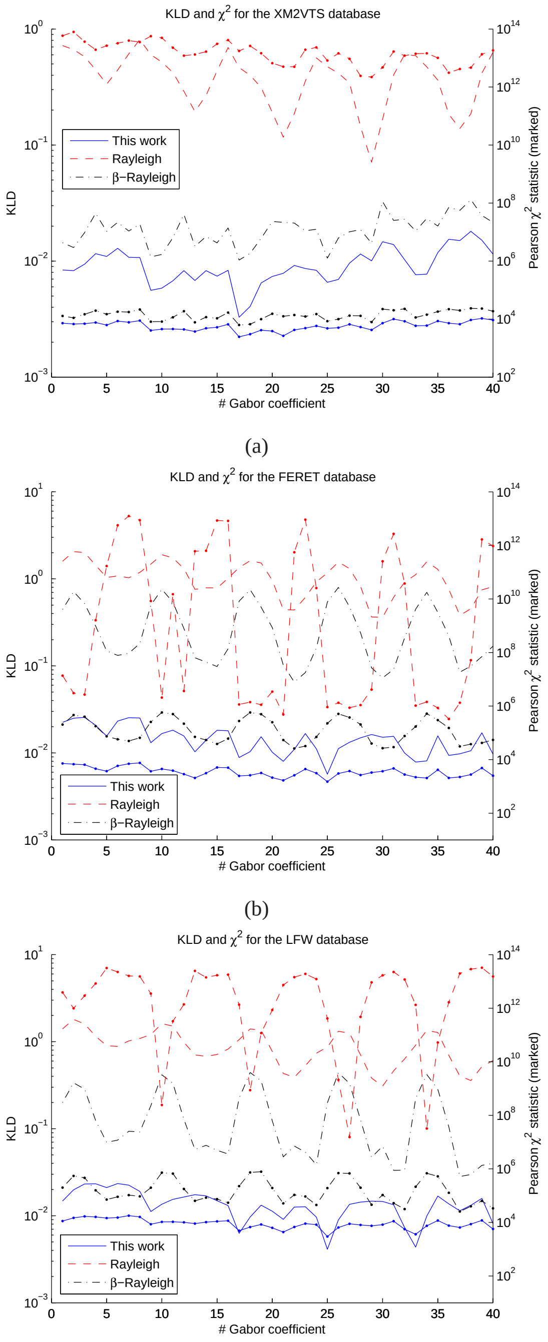
where $K$ stands for the number of possible values of the discrete distribution. The KLD is also proportional to the $G$ statistic ($G = 2N \cdot KLD(P,Q)$, for $N$ observations), widely used in biometrics for hypothesis testing. Additionally, Pearson's $\chi^2$ statistic for a sample with $N_i$ observations for each possible value ($N = N_0 + N_1 + \ldots + N_{K-1}$) and a theoretical distribution $Q$ can be calculated as

$$\chi^2 = \sum_{i=0}^{K-1}\frac{(N_i - N\cdot Q(i))^2}{N\cdot Q(i)}.$$

Both Pearson's statistic and the $G$ statistic have a $\chi^2$ distribution with $K-1$ degrees of freedom, which can be used for hypothesis testing and for calculating the confidence interval for the event that the observations be derived from the distribution $Q$. As we are working with actual data, our model is not intended to capture all the noise sources and uncertainty in the observed signal, but to present a better fit than previously used models. To this end, we show next that both the KLD and Pearson's statistic for our model are significantly lower than for previously used distributions for Gabor magnitudes.

In order to calculate both the KLD and Pearson's $\chi^2$ statistic, we discretize the theoretical pdf in $K$ intervals ($K \in [512, 1024]$) and compare it to the empirical discrete pdf given by the histogram of the actual data. Fig. 3 shows the KLD and Pearson's statistic calculated for XM2VTS, LFW and FERET databases for our model compared to two distributions: Rayleigh, equivalent to considering Gaussian i.i.d. real and imaginary part for the Gabor coefficients, and $\beta$-Rayleigh [26]. For the three databases, our model gives a much better fit than the Rayleigh, especially for the coefficients with a lower shape factor, which are farther apart from the Gaussian model. Fig. 3 also shows the pseudoperiodic effect on $c$ when varying the orientation [17]. This produces that the calculated statistics for the Rayleigh have minima at those coefficients with shape factors closest to $c = 2$. In any case, as shape factors are always in the range $(0.5, 1.5)$, our model will always yield a better fit than the Rayleigh model.

Additionally, the improvement on the fit provided by our model is much more noticeable for the LFW and the FERET databases. This is due to XM2VTS's samples be taken within controlled conditions, thus presenting a limited set of poses and illuminations; on the other extreme, LFW yields a much richer variety of poses, expressions and illuminations on lower quality images, producing a heavier-tailed distribution for the magnitude of the coefficients that is harder to approximate with a $\beta$-Rayleigh. These heavy tails are very well fitted by our model, corroborating that the original assumptions on which it is grounded are fulfilled by the three databases.



(a)

(b)

(c)

Fig. 3. KLD (non-marked lines) and $\chi^2$ statistic (marked lines) for Gabor magnitudes modeled as Eq. (1), Rayleigh and $\beta$-Rayleigh [26] for the XM2VTS (a), the (b) FERET, and the LFW (c) databases.

### B. *Optimal Quantization of Biometric Data*

The presented model has interest in itself, and there are many applications that can benefit from its use. Our target here is the minimization of the plaintext cardinality of the involved magnitudes; this is necessary for the encrypted private system to effectively handle the full face verification without any interaction. Hence, we apply our model for optimal coefficient quantization using a Lloyd-Max quantizer [32]. When an accurate distribution of the to-be-quantized variables is given, this quantizer achieves minimum mean squared error (MSE) for a fixed number $N_L$ of representative levels.

A Lloyd-Max strategy was also used in [17] for independently quantizing the real and imaginary parts of Gabor coefficients. If the phase information is discarded for verification, it is more appropriate to directly quantize the magnitudes instead. Hence, our choice gets a more significant storage reduction, so we expect to achieve similar performance with less representative levels. Additionally, the quantization in [17] and [1] uses a number $N_L$ of centroids for each coefficient, preserving the real values of the corresponding levels as the output quantizations. This strategy allows for a storage reduction in a clear-text system: only the (integer) indices of the corresponding quantization levels and the mapping from the indices to the real levels have to be stored. However, this mapping has to be applied to recover the quantizations before operating on them; an encrypted system that has to work with integer-valued numbers cannot translate this quantization into an actual reduction in plaintext size. Instead, we propose the use of integer quantization indices, as a more suitable strategy for the encrypted system, i.e., all the involved variables are mapped to integer numbers with a very low cardinality (the number of quantization levels). Additionally, the use of indices involves a nonlinear scaling of all the coefficients in such a way that, after scaling, the resulting centroids are arranged in equidistant bins, as shown in Fig. 4. This also produces an inherent normalization, reducing coefficients with high variance and amplifying those with low variance, and fixing the range for all the coefficient indices.

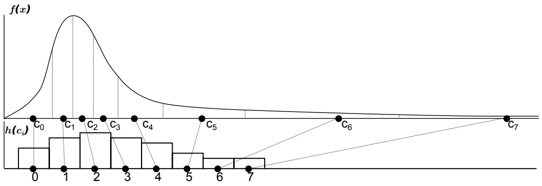


Fig. 4. Qualitative diagram showing the non-linear scaling produced by the use of integer quantization indices (lower graph) instead of the real values of the quantization centroids for Lloyd-Max quantization (upper graph).

Section V-A will validate the achieved performance results for a given cardinality reduction in the integrated system. Before that, we will introduce the second essential block of our secure verification scheme, which is fed by quantized coefficient levels: our extended homomorphic cryptosystem.

## IV. Extending Gentry's Fully Homomorphic Cryptosystem

We take one of the latest versions of Gentry's bootstrappable fully homomorphic cryptosystem (GH11 [18]). The cryptosystem is GGH-type (Goldreich-Goldwasser-Halevi) based on ideal lattices. We firstly give a brief explanation of GGH cryptosystems in general and GH11 in particular, and then present our extension. We refer the interested reader to [16], [25] for a more detailed description of GGH cryptosystems.

### A. *GGH Cryptosystems*

Given a lattice $L$ with shortest nonzero vector length $\lambda_1(L)$, the rationale behind GGH cryptosystems lies in choosing two bases with different *correction radii*. The *correction radius* of a basis can be defined as the norm of the shortest error vector that, added to a lattice point, cannot be corrected using that basis (as it falls outside the parallelepiped—Voronoi region—defined by the reduction modulo the basis). This radius is upper bounded by the inner radius of the lattice, defined as $\frac{\lambda_1}{2}$, that is, half the shortest distance between two lattice points; this bound yields the maximum correction *capacity* a lattice can achieve, depending on the basis. *Good bases* yield almost spherical Voronoi regions, with a correction radius approaching the inner radius of the lattice; bad bases have a very small correction radius and poor correction capabilities. This fact is used in GGH cryptosystems to choose the keys:

- $\boldsymbol{B}_{sk}$ constitutes the secret key; it is a *good basis*: it allows to efficiently solve certain instances of the closest-vector problem in the lattice, and its correction radius is large enough. The basis vectors are short and almost-orthogonal.
- $\boldsymbol{B}_{pk}$ ($\boldsymbol{B}$ from now on) constitutes the public key; it is a *bad basis*: solving the closest vector problem in $L$ using $\boldsymbol{B}$ is algorithmically hard. $\boldsymbol{B}$ is usually chosen as the Hermite Normal Form (HNF) of the lattice, as it can be efficiently computed from any other basis, it has a very small correction radius (asymptotically zero with growing dimensions), and the LLL algorithm (the most widely known lattice reduction algorithm, by Lenstra, Lenstra and Lovasz [33]) is particularly slow [34] for the HNF.

Encryption and decryption are analogous to channel noise addition and error correction in a digital communication system, with the peculiarity that the information resides in the induced channel errors. Encryption $\boldsymbol{c}$ of a message $m$ consists in the addition of a correctable error vector $\boldsymbol{e}$ ($||\boldsymbol{e}||_2 < \frac{\lambda_1(L)}{2}$), that encodes $m$, to a point in the lattice. Decryption stands for error correction, and it can only be done with a good basis like $\boldsymbol{B}_{sk}$, by recovering the error vector $\boldsymbol{e}$ as $\hat{\boldsymbol{e}} = \boldsymbol{c} \bmod \boldsymbol{B}_{sk}$.

### B. GH11 Cryptosystem

The *somewhat homomorphic* scheme presented by Gentry and Halevi [18] uses a principal-ideal lattice $J$, generated by a polynomial $v(x)$ ($\boldsymbol{v}$ in vector notation) with $t$-bit signed random integer coefficients, in the ring of polynomials modulo $f_n(x) \doteq x^n + 1$. The HNF must have the following structure:

$$\boldsymbol{B}^T = HNF(J) = \begin{pmatrix} d & 0 & 0 & & 0 \\ -r & 1 & 0 & & 0 \\ -[r^2]_d & 0 & 1 & & 0 \\ & & & \ddots & \\ -[r^{n-1}]_d & 0 & 0 & & 1 \end{pmatrix},$$

where $d$ can be defined as the resultant of the polynomials $v(x)$ and $f_n(x)$, and $r$ is a root of $f_n(x) \bmod d$. $\boldsymbol{B}$ is the *public-key* encryption matrix, completely determined by the pair of integers $(d, r)$, while the private key is given by $v(x)$ and its scaled (modulo $f_n(x)$)-inverse $w(x)$ (i.e., $v(x) \times w(x) = d \bmod f_n(x)$); only one of the coefficients of $\boldsymbol{w}$, denoted by $w_i$, is required for the decryption procedure.

As defined, this cryptosystem is *quasi*-homomorphic under addition and multiplication, that are directly mapped from the crypto-text ring (errors with respect to lattice points) to the clear-text ring. This homomorphism is limited, as both operations are only correctly mapped when the error lies within the same Voronoi region of the lattice $L$ after applying the operation. For reaching a full homomorphism, Gentry proposes to *squash* the decryption circuit so that it can be homomorphically executed. Hence, it is possible to *bootstrap*[1] a fresh encryption from a degraded one, effectively achieving a full homomorphism, at the cost of additional security assumptions.

Instead of bootstrapping the decryption circuit, we propose to trade this full homomorphic capacity for the ability to execute low to medium-degree polynomials before the cipher gets corrupted enough to lose data. Hence, we use the cryptosystem as a quasi-fully homomorphic scheme, while we improve on the allowed cardinality of the plaintext as shown in the next section. These two contributions together produce a very versatile cryptosystem for non-interactive secure processing.

### C. Proposed Extension to GH11 Cryptosystem

GH11 cryptosystem can only deal with binary numbers in $(\mathbb{Z}_2, +, \cdot)$; i.e., the homomorphic ring operations are *and* and *xor* gates. This means that a simple arithmetic circuit with non-binary numbers needs a high amount of binary homomorphic operations; each of them increases the noise within the Voronoi region of the lattice, until they wrap up producing a decoding error. This sets a limit to the depth of a homomorphically executable polynomial, which has been empirically calculated by Gentry and Halevi [18].

In this section we provide an extension to the plaintext-size, allowing for homomorphic additions and multiplications in $(\mathbb{Z}_{2^k}, +, \cdot)$ (powers of two are chosen for convenience). Additionally, we give a theoretical lower bound on the maximum number of executable multiplications, that also supports Gentry's empirical study for $\mathbb{Z}_2$. Our extension seeks to enhance the efficiency of arithmetic non-interactive operations and decrease the cipher expansion rate. Furthermore, the key generation process does not need to be changed[2], so the same keys can be used for the binary cryptosystem and for the proposed extension. A sketch of the proposed encryption and decryption operations is shown in Algorithm 1.

*1) Encryption:* In Gentry's original cryptosystem, the encryption operation of a bit $b \in \mathbb{Z}_2$ uses a random noise vector $\boldsymbol{u} \in \{0, \pm 1\}^n$. Each element $u_i$ is chosen as 0 with probability $q$ and $\pm 1$ with probability $(1-q)/2$ each ($q$ is a security parameter). We extend encryption for dealing with $m \in \mathbb{Z}_{2^k}$

$$\boldsymbol{a} = 2^k \boldsymbol{u} + m \cdot \boldsymbol{e}_1; \quad \boldsymbol{c} = \boldsymbol{a} \bmod \boldsymbol{B} = [a(r)]_d \cdot \boldsymbol{e}_1,$$

where $\boldsymbol{e}_1$ is the first vector of the canonical basis. The vector $\boldsymbol{c}$, as in the original construction, has only one non-zero component, representative of the encryption:

$$c = [a(r)]_d = [m + 2^k \sum_{i=0}^{n-1} u_i r^i]_d.$$

[1] For more details on squashing and bootstrappable fully homomorphic cryptosystems we refer the reader to [18], [35].

[2] See [18] for details on the key generation process.

**Algorithm 1** Proposed Encryption and Decryption

**Parameters:**
$q$: probability of a zero in the random salt vector
$k$: maximum bit size of the plaintext space elements
$(r, d)$: encryption key
$(w_i, d)$: decryption key
$n$: lattice dimensionality

| **Encryption** | **Decryption** |
|---|---|
| Input: plaintext $m \in \mathbb{Z}_{2^k}$<br>Output: ciphertext $c \in \mathbb{Z}_d$<br>1) Generate random vector $\boldsymbol{u} \in \{0, \pm 1\}^n$ with probability distribution $\{(1-q)/2, q, (1-q)/2\}$ for the values $\{-1, 0, 1\}$.<br>2) Calculate the ciphertext $c = [a(r)]_d = [m + 2^k \sum_{i=0}^{n-1} u_i r^i]_d$. | Input: ciphertext $c \in \mathbb{Z}_d$<br>Output: plaintext $m \in \mathbb{Z}_{2^k}$<br>Get the plaintext $m = [c \cdot w_i]_d w_i^{-1} \bmod 2^k$ |

The complexity of encrypting a $k$-bit number is the same as for encrypting a bit in the original system. Furthermore, the security in terms of Birthday-type attacks is not altered either, as the noise vector has the same entropy; hence, given a security level $\lambda$, $q$ may still be chosen such that

$$2^{(1-q)n} \left( \begin{array}{c} n \\ qn \end{array} \right) > 2^{2\lambda}.$$

A discussion about the security of the extended cryptosystem can be found in Section VI.

*2) Decryption:* For the decryption, the original scheme uses an optimized procedure that only needs one of the odd coefficients of $\boldsymbol{w} \bmod d$, denoted by $w_i$. Adapting that procedure, our decryption for a $k$-bit message $m$ becomes

$$m = [c \cdot w_i]_d w_i^{-1} \bmod 2^k.$$

The difference with respect to the original decryption is the product by $w_i^{-1} \bmod 2^k$. GH11 requires $w_i$ to be odd; due to our choice of powers of two for extended plaintexts, $w_i^{-1}$ exists if $w_i$ is odd, so we impose no additional requirement for the key generation process, and the added decryption complexity is negligible compared to modulo $d$ operations.

### *D. Homomorphically Achievable Polynomial Degree*

After presenting our extended cryptosystem, it is essential to measure its homomorphic capacity, in order to predict if it can execute the face verification function. With this target, we derive now a theoretical upper bound on the maximum achievable polynomial degree that the cryptosystem can evaluate with an arbitrarily bounded probability of incurring on decryption errors. We will first bound the probability of incorrect decryption for successive homomorphic multiplications.

Incorrect decryption may only happen when the error vector added to a lattice point lies outside the Voronoi region of the used lattice. This condition boils down to $||\boldsymbol{a}^T \boldsymbol{W}||_\infty < d/2$, where $\boldsymbol{W}$ is the rotation basis that generates $(w(x))$, having in each row the coefficients of $w(x) \cdot x^i \bmod f_n(x)$. Due to the structure of $\boldsymbol{W}$ (a circulant matrix with negated lower triangular part), we can bound

$$\begin{aligned} ||\boldsymbol{a}^T \boldsymbol{W}||_\infty \le & ||\boldsymbol{a}||_\infty ||\boldsymbol{W}||_\infty \\ & = \max_i(|a_i|) \cdot \sum_{i=0}^{n-1} |w_i| \le \sum_{i=0}^{n-1} |w_i| \sum_{i=0}^{n-1} |a_i| < d/2 \\ & \Rightarrow ||\boldsymbol{a}^T \boldsymbol{W}||_\infty < d/2. \end{aligned}$$

The number of non-zero elements ($Nz_j$) of a chosen $\boldsymbol{u}_j$ follows a Binomial distribution $Nz_j \sim Bi(n, 1-q)$. In a fresh encryption, each of these elements has magnitude $2^k$, while the message is $|m| < 2^k$. Hence, $\sum_{i=0}^{n-1}(|a_i|) < 2^k(1 + Nz_j)$.

Conversely, after a multiplication between two ciphertexts $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ (in the polynomial quotient ring $\mathbb{Z}_d[x]/(f_n(x))$), the resulting point must also be within the Voronoi region. The product of two polynomials modulo $f_n(x)$ is equivalent to a cyclic convolution of their coefficient vectors (with a sign change for the overlapped subvector). Let $\boldsymbol{c}_2$ be a fresh encryption; thus, it has the same absolute value ($2^k$) for all the non-zero coefficients of the used random $\boldsymbol{u}$. Consequently, the $l_1$-norm of the resulting coefficient vector of the product of a given ciphertext $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ is upper-bounded by $||\boldsymbol{c}_1||_1 \cdot 2^k(1 + Nz_2)$. In general, we have that, after $n_m$ successive products of a cipher by fresh encryptions,

$$||\boldsymbol{a}_{n_m}^T \boldsymbol{W}||_\infty \le \left( \sum_{l=0}^{n-1} |w_l| \right) \prod_{i=0}^{n_m} 2^k (1 + Nz_i).$$

Hence, we can bound the probability of decryption error

$$\begin{aligned} & P[\text{dec error}] = P[||\boldsymbol{a}^T \boldsymbol{W}||_\infty \ge d/2] \le \\ & P\left[ \underbrace{\sum_{i=0}^{n_m} \log(1 + Nz_i)}_{N_{n_m}} \ge \log\left( \frac{d}{2^{k(n_m+1)+1} \sum_{l=0}^{n-1} |w_l|} \right) \right], \end{aligned}$$

where $N_{n_m}$ is a random variable with bounded support ($N_{n_m} \in [0, (n_m + 1)\log(n+1)]$). Thus, it may happen that for a low number of dimensions and few multiplications the probability of decryption error be zero. Nevertheless, $q$ is chosen such that $(1-q) \ll 1$, for high enough $n$ (like the commonly used $n$ even for short-term security), so the error probability will not get to be identically zero in any case. Furthermore, the pdf of $N_{n_m}$ will present a narrower bell as $n$ or $n_m$ increase, so by virtue of the Central Limit Theorem (CLT), $N_{n_m}$ can be accurately approximated by a Gaussian variable with parameters

$$\begin{aligned} \mu_{n_m} = & (n_m + 1)\mu \doteq (n_m + 1) \sum_{i=0}^{n} \log_2(1 + i) \left( \begin{array}{c} n \\ i \end{array} \right) (1-q)^i q^{n-i}, \\ \sigma_{n_m}^2 = & (n_m + 1)\sigma^2 \\ \doteq & (n_m + 1) \sum_{i=0}^{n} (\log_2(1 + i) - \mu)^2 \left( \begin{array}{c} n \\ i \end{array} \right) (1-q)^i q^{n-i}, \end{aligned}$$

that will provide a very accurate approximation near the bell and an overestimation of the decryption error probability in the tails, due to the bounded support of $N_{n_m}$.

We may then bound the maximum number of bits to which we can extend the ciphertext for allowing a given number $n_m$

TABLE I
LOWER BOUND ON THE MAXIMUM NUMBER OF PRODUCTS AND GENTRY'S EMPIRICALLY OBTAINED MAXIMUM DEGREE POLYNOMIAL AS A FUNCTION OF $t$, WITH $n = 128$.

| $t$ | 64 | 128 | 256 | 384 |
|---|---|---|---|---|
| Lower bound | 10 | 22 | 46 | 69 |
| Empirical [18] | 13 | 33 | 76 | 128 |

of successive multiplications with a given probability of error $p_e$ using the $Q$ function[3]

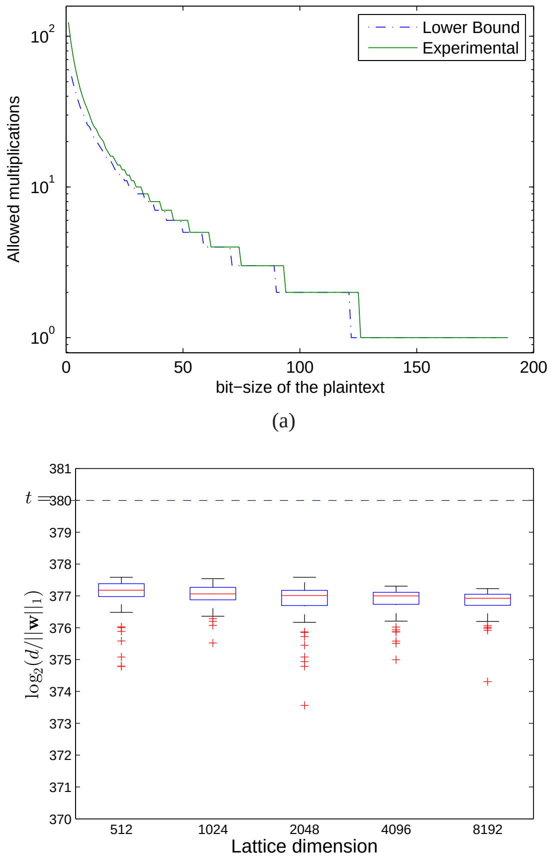
$$k_{max} = \left\lfloor \frac{\log_2(d/||\boldsymbol{w}||_1) - 1}{n_m + 1} - \mu - \frac{Q^{-1}(p_e)\sigma}{\sqrt{n_m + 1}} \right\rfloor. \quad (2)$$

As expected, the maximum number of bits decreases when increasing $n_m$, and it is heavily influenced by the quotient $d/||\boldsymbol{w}||_1$, representing the effective radius of the Voronoi region. It can be shown that the choice of $t$ (bit-size of the coefficients of $v(x)$) determines the maximum value of this quotient; the proof is obtained by expressing $v(x)w(x) = d \bmod f_n(x)$ in vector notation and using the Hölder inequality:

$$d = \boldsymbol{v}^T[w_0, -w_{n-1}, \ldots, -w_1]^T \leq ||\boldsymbol{v}||_\infty ||\boldsymbol{w}||_1 < 2^t ||\boldsymbol{w}||_1$$
$$\Rightarrow \frac{d}{||\boldsymbol{w}||_1} < 2^t.$$

Hence, for a good lattice, the maximum correctable noise norm (decryption radius) will be close to $t$ bits (cf. Fig. 5b). Substituting $\log_2(d/||\boldsymbol{w}||_1)$ by $t$ in Eq. (2), we get an estimation of the maximum plaintext bit-size for correct decryption after a given number of multiplications for a generic good lattice. Reciprocally, the inverse of this expression yields the maximum number of affordable multiplications with a bounded decryption error. It must be noted that $n_s$ consecutive homomorphic additions can increase at most in $\log_2(n_s)$ bits the size of the $\infty$-norm of the noise vector; in fact, Eq. (2) can take this into account by subtracting $\log_2(n_s)$ from $t$. Hence, when determining the maximum degree of a polynomial run on freshly encrypted variables, the maximum number of multiplications is the limiting factor. Gentry and Halevi provide an approximation of the maximum degree $deg$ of an elementary symmetric polynomial evaluated on $m$ encrypted binary variables, bounding the decryption radius by the approximated Euclidean norm of the polynomial output: $2^t \geq c^{deg}\sqrt{\binom{m}{deg}}$. However, for large $m$ this expression overestimates the effect of additions: as the combinatorial number of summed monomials grows above the lattice dimensionality, they cannot be considered independent anymore. Table I shows the validity of our bound compared to the experimental results by Gentry.

Fig. 5a represents the number of sequential products with new fresh ciphers before a decryption error occurs (for $n = 512$, $t = 380$ and $q = 1 - 20/512$, picking the minimum of 1000 trials), and our lower bound for $p_e = 10^{-4}$. The bound is fairly conservative for small plaintexts that allow for a high amount of products, as it is a worst-case bound, but it becomes tight for medium-to-high $k$, even when the Gaussian approximation in those cases provides an overestimation of the decryption error. We also obtained very similar results with bigger lattices, due to two facts: a) the quotient $\log_2(d/||\boldsymbol{w}||_1)$ is almost constant for random lattices (see Fig. 5b), and b) the binomial distribution barely changes with high $n$ for a fixed rate $(1 - q)n$.



(a)

(b)

Fig. 5. (a) Minimum number of multiplications (Eq. (2)) without decoding error after 1000 trials as a function of $k$ and (b) quotient $\log_2(d/||\boldsymbol{w}||_1)$ for random lattices of several dimensions with fixed $t = 380$.

## V. Fully Private Non-Interactive Face Verification

The combination of the quantization strategy of Section III together with the extended cryptosystem presented in Section IV provides an efficient and accurate solution for a fully private outsourced face verification scenario (see Section I-A). Algorithm 2 shows a sketch of the proposed protocol.

Unlike previous works [1], our system uses the integer indices of quantized coefficients instead of the actual quantized values. This allows for a hugely reduced plaintext size without much degradation in system performance (cf. Section V-A), and benefits from an inherent normalization of the jets, as the Lloyd-Max quantization already performs a nonlinear normalization (cf. Section III-B). The verification algorithm can be

[3] The $Q$ function can be defined as

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-u^2/2} du$$

based either on average correlation (cosine distance) or on average Euclidean distance; both can be efficiently calculated in the encrypted domain, and there are no statistically significant differences in verification performance between both distances. Actually, the proposed cryptosystem could work with other $l$-norms, whenever $l$ fits within the homomorphic capacity for a given bit size of the quantized inputs. This enables the use of the homomorphic cryptosystem for many verification functions without any intermediate decryption, i.e., in a fully non-interactive way.

In the *enrollment phase*, the presented feature vectors are encrypted and stored in a central database for later use as templates; each user may have up to $N_{tp}$ templates. The verification threshold $\eta$ is a system parameter also kept encrypted. We employ a linear-kernel Support Vector Machine (SVM [36]), previously trained on local distances, that produces a weight vector $\boldsymbol{\alpha}$, resulting from the linear combination of the support vectors $\{\boldsymbol{s}_j\}_{j=1}^{M-1}$

$$\text{score}_{SVM}(\boldsymbol{x}) = \sum_{j=0}^{M-1} \beta_j \boldsymbol{s}_j^T \cdot \boldsymbol{x} - \eta = \boldsymbol{x}^T \underbrace{\sum_{j=0}^{M-1} \beta_j \boldsymbol{s}_j}_{\boldsymbol{\alpha}} - \eta; \quad (3)$$

the score is classified as *true* if it is non-negative, and as *false* otherwise. For each pair of compared feature vectors $\boldsymbol{a}$ and $\boldsymbol{b}$, if the input to the SVM is chosen as $x_j = (a_j - b_j)^2$. The effect of the weight vector $\boldsymbol{\alpha}$ is to produce a weighted Euclidean distance $\text{dist}(\boldsymbol{a}, \boldsymbol{b}) = \sum_{i=0}^{N-1} \alpha_i \cdot (a_i - b_i)^2$ as the verification score. In the *verification phase*, a user presents an ID to be matched together with the encrypted quantization indices $\hat{\boldsymbol{g}}$ of his/her Gabor features vector. The database holder homomorphically calculates the encryption of the *soft* score

$$\text{soft\_score}(\hat{\boldsymbol{g}}^{(id)}, id) = \sum_{i=0}^{N_{tp}-1} \text{dist}(\boldsymbol{g}_i^{(id)}, \hat{\boldsymbol{g}}^{(id)}) - N_{tp}\eta,$$

that is returned as the output of the verification process. It must be noted that more involved kernels like RBF (Radial Basis Functions) or sigmoid have not shown a net improvement in the performance of this kind of verification systems, and they would add too much complexity to a non-interactive private solution. Using the proposed linear SVM adds little computation complexity to the non-weighted original approach (the number of products is doubled), while considerably enhancing the verification accuracy (cf. Section V-A).

As a last remark, a hard score may be required for some applications. We will not consider that case explicitly in this work, as we are testing the raw performance of the extended cryptosystem in a fully non-interactive outsourced scenario. In any case, the private implementation of the last comparison step needed for providing a hard score ($[\text{soft\_score}(\hat{\boldsymbol{g}}^{(id)}, id) \geq 0]$) could be easily produced, by adapting one of the many interactive comparison protocols available for an additive homomorphic cryptosystem(e.g., see [8, Section 5]). This adaptation must take into account that for performing a statistically blinding decryption—necessary for the intermediate steps of the protocol—the cipher must support the encryption of numbers with a length $\kappa$ bits higher than the input coefficients and results; hence, for normal values of the security parameter $\kappa$ ($\kappa \approx 70$ bits) and typical working magnitudes (around $20$ bits for this application, thanks to the proposed quantization), the extended cryptosystem will need to cope with $\sim 90$ bits clear-text sizes. With this capacity, it will be able to support at least two correct consecutive homomorphic products, Eq. (2); this is enough for calculating a weighted Euclidean distance.

**Algorithm 2** Proposed Secure Outsourced Verification Protocol

**Database preparation ($\mathcal{A}$):**

1) Calculate the weight vector $\boldsymbol{\alpha}$ and threshold $\eta$ for the desired operation point.
2) Encrypt existing database vectors and $\boldsymbol{\alpha}$ and $\eta$.
3) Send encryptions $\llbracket \boldsymbol{\alpha} \rrbracket$ and $\llbracket \eta \rrbracket$ to $\mathcal{B}$.

**Enrollment:**

| $\mathcal{A}$ | $\mathcal{B}$ |
|---|---|
| 1) Obtain a new identifier $id$ for the user.<br>2) Extract the feature vector $\boldsymbol{g}^{(id)}$ for the new user.<br>3) Encrypt $\llbracket \boldsymbol{g}^{(id)} \rrbracket$.<br>4) Send $\llbracket \boldsymbol{g}^{(id)} \rrbracket$ and $id$ to $\mathcal{B}$. | 5) If an entry associated to $id$ does not exist, create a new entry.<br>6) Store the encrypted $\llbracket \boldsymbol{g}^{(id)} \rrbracket$ as a new template for $id$ at the database. |
| 7) Return the identifier $id$ to the user. | |

**Verification:**

| $\mathcal{A}$ | $\mathcal{B}$ |
|---|---|
| 1) Obtain the identifier $id$ for the user.<br>2) Extract the feature vector $\hat{\boldsymbol{g}}^{(id)}$ for the presented user face.<br>3) Encrypt $\llbracket \hat{\boldsymbol{g}}^{(id)} \rrbracket$.<br>4) Send $\llbracket \hat{\boldsymbol{g}}^{(id)} \rrbracket$ and $id$ to $\mathcal{B}$. | 5) Retrieve the stored encrypted $N_{tp}$ templates for $id$: $\{\llbracket \boldsymbol{g}_i^{(id)} \rrbracket\}_{i=0}^{N_{tp}-1}$.<br>6) Calculate the encrypted score homomorphically as $\llbracket \text{score}\left(\hat{\boldsymbol{g}}^{(id)}, id\right) \rrbracket = \sum_{i=0}^{N_{tp}} \sum_{j=0}^{M-1} \llbracket \alpha_j \rrbracket \cdot \left(\llbracket g_{i,j}^{(id)} \rrbracket - \llbracket \hat{g}_j^{(id)} \rrbracket\right)^2 - N_{tp} \llbracket \eta \rrbracket$;<br>7) Return the encrypted $\llbracket \text{score}\left(\hat{\boldsymbol{g}}^{(id)}, id\right) \rrbracket$ to $\mathcal{A}$. |
| 8) Decrypt score $\left(\hat{\boldsymbol{g}}^{(id)}, id\right)$.<br>9) Check whether score $\left(\hat{\boldsymbol{g}}^{(id)}, id\right) > 0$.<br>10) Report verification result to the user. | |

We will now evaluate the presented secure verification system in terms of verification performance and efficiency.

### A. Face Verification Performance

In order to evaluate the impact of data quantization on system performance, we conducted experiments on the XM2VTS [28], the FERET [29], and the LFW [30] databases. We are not aiming at improving the verification rate of state-of-the-art classifiers, but showing instead that the presented optimal quantization driven by our accurate feature model does not hinder the verification performance of the system. Hence, we have used baseline verification methods (similar to the ones in [1], [17]) to better show the actual effects of quantization. We also compare our proposal of a weighted

Euclidean distance (Eq. (3)) as verification function with the results obtained without any additional weighting on the quantized coefficients [2]. The SVM provides improved results with a very little complexity overhead, also in a suitable configuration for the privacy-preserving implementation.

For the three databases, we plot the obtained ROC (Receiver Operating Characteristic) curve and report the verification accuracy $\mu = 1 - (FAR + FRR)/2$ at the EER (Equal Error Rate), where FAR and FRR stand for *False Acceptance Rate* and *False Rejection Rate* respectively. We present the comparison for three quantization strategies with a set of $N_L = \{2, 4, 8\}$ levels, with and without weighting:

- Independently quantizing the real and imaginary parts of the complex coefficients [17]. We use $N_L$ for the number of levels for quantizing the absolute value of the real and imaginary parts, in such a way that $2(1 + \log_2(N_L))$ bits are actually needed for each quantized coefficient (sign bit plus two quantizations per coefficient).
- Quantizing the magnitudes of coefficients [1].
- Using integer quantization indices instead of actual quantized values for our model (proposed in this work).

The two first strategies also comprise an additional prenormalization step such that each 40-coefficient jet for each localization has unit norm.

*a) XM2VTS database:* Experiments on XM2VTS were performed following configuration I of the Lausanne protocol [28]. The XM2VTS database contains mainly frontal face images recorded on 295 subjects (200 clients, 25 evaluation impostors, and 70 test impostors) during four sessions taken at one-month intervals. The database is divided into three sets: training, evaluation and test. The training set (3 images per user) was used to estimate model parameters ($c$ and $\sigma$), and calculate the quantization centroids. The evaluation set was used to estimate EER thresholds, and train the linear SVM classifier for providing the weight vector. Finally, the ROC is obtained from the separate test set.

*b) The Facial Recognition Technology (FERET) Database:* The Facial Expression (`fafb`) subset of the FERET database [29] contains a gallery of 1196 frontal images, with one image per person, and a probe set with 1195 images of the same people, obtained a few seconds after the gallery ones with a different expression. The standard FERET verification test [29] checks every possible pair of faces from gallery and probe set together, reporting the resulting ROC. For quantization in our tests, we took the model parameters $c$ and $\sigma$ and the centroids estimated from the LFW database *view 1*. As FERET does not provide a standardized division between evaluation and test set, for testing the proposed linear SVM we performed a 5-fold cross validation with equal-size disjoint subsets taken from gallery and probe.

*c) Labeled Faces in the Wild (LFW) database:* The LFW database [30] (we used the *funneled version*) is a more challenging dataset that contains 13,233 face images which have several compound problems (imperfect localizations, in-plane rotations, non-frontal poses, low resolution, non-frontal illumination, varying expressions...). The images were obtained by running an automatic face detector on images collected from the Internet. The LFW database is organized into two *views*: we used *view 1* to estimate model parameters and quantization centroids; it comprises two subsets, one for training, and one for testing. The training set consists of 1100 pairs of matched images and 1100 pairs of mismatched images. The test set consists of 500 pairs of matched and 500 pairs of mismatched images. *View 2* is organized in 10 disjoint folds; the experiments on this dataset were carried out following the *image restricted* paradigm, and performance was reported on *view 2* using the 10-fold, leave-one-out cross-validation scheme described in [30].

*1) Verification Performance Results:* Fig. 6 and Table II present the ROC and the verification accuracy $\mu$ for verification on the three databases, comparing the different quantization strategies for $N_L = \{2, 4, 8\}$ levels.

Our model with the indices-based quantization strategy significantly outperforms the independent real-imaginary quantization [17] and the level-based magnitude quantization [1] in all the configurations and databases. The proposed model produces a much better fit, and the indices-based quantization, with its non-linear scaling eliminates some non-informative noise and preserves much more useful information for verification in less bits. Taking XM2VTS results as a reference, our strategy gets a cardinality reduction factor of $4$ with respect to [17] for the same performance. Moreover, the use of the SVM weights with our strategy not only recovers the original performance, but surpasses it, with a considerable performance boost in both XM2VTS and FERET, while the unweighted systems [2] show an absolute gap of 1% and 0.5% respectively.

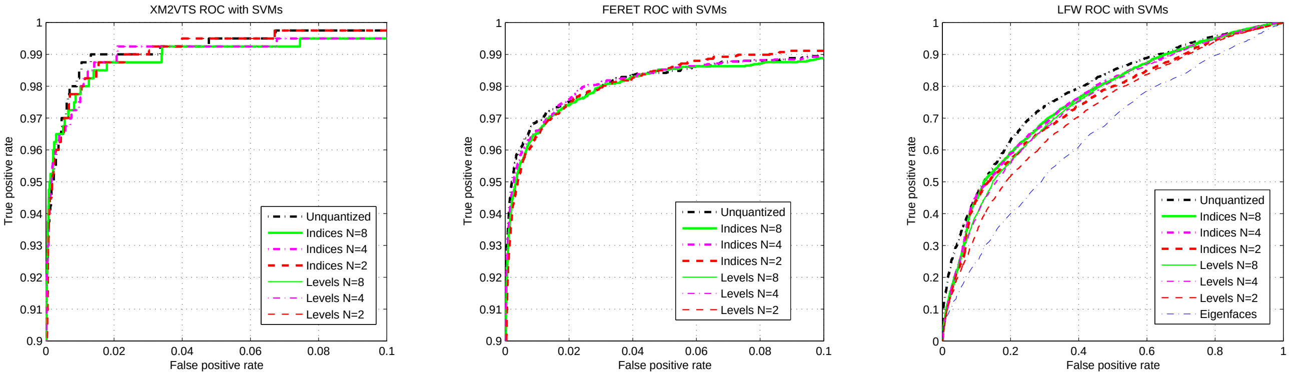
For the more challenging LFW database, there is a gap of 2.6% from original performance for our system, slowly recovered with increasing $N_L$; in any case, it again performs better than prior quantization strategies. Finally, for FERET and LFW, the results for Eigenfaces (used in prior privacy-preserving face identification works) are publicly available, so we have also shown them in Table II for comparison. The performance achieved with Eigenfaces in LFW is worse than baseline V1-like models [37] ($\approx 64\%$), while our system with SVM performs better than other baseline Gabor-based schemes ($\approx 68\%$ for V1-like+ models in LFW), and a $9\%$ and $\sim 5\%$ over Eigenfaces in LFW and FERET respectively.

*2) Quantization of SVM weighting coefficients:* For any of the studied databases, it is worth noting that the weighting coefficients must be also quantized before being used in the encrypted private system. We have checked that these coefficients $\{\alpha_i\}_{i=0}^{N-1}$ approximately follow a Gaussian distribution with a mean close to zero; their histogram for XM2VTS is shown in Fig. 7. Actually, these coefficients come from the sum of the signed—almost independent—coefficients of the support vectors, hence converging to a Gaussian due to the CLT. The number of obtained weight samples (4000 per database) is not enough for a reliable hypothesis testing for Gaussianity, but their quantization is not so critical as for the Gabor features. In fact, applying a Lloyd-Max quantizer based on this Gaussian fit, we found that using two levels (i.e., preserving just the sign of each $\alpha_i$) the impact on the verification performance is negligible (around $0.1 - 0.2\%$ in the three databases).

This system, in which all the involved values are integers with a very low cardinality is the one that we use in this

TABLE II
VERIFICATION ACCURACY $\mu$ (%) FOR THE QUANTIZED AND UNQUANTIZED VERIFICATION SYSTEM ON THE THREE STUDIED DATABASES. EIGENFACES RESULTS ARE SHOWN FOR COMPARISON ON FERET AND LFW.

| Database | | XM2VTS | | | | FERET | | | | | LFW | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $N_L$ | | 2 | 4 | 8 | Orig. | 2 | 4 | 8 | Orig. | Eigenf. | 2 | 4 | 8 | Orig. | Eigenf. |
| No SVM | [17] | 89.04 | 92.30 | 92.59 | 95.45 | 94.27 | 95.62 | 95.87 | 97.06 | 93.00 | 61.40 | 62.77 | 63.77 | 65.93 | 60.00 |
| | [1] (levels) | 91.06 | 92.28 | 92.55 | | 95.29 | 95.36 | 95.70 | | | 61.63 | 62.83 | 63.73 | | |
| | Proposed | 94.39 | 94.80 | 94.60 | | 96.63 | 96.63 | 96.54 | | | 65.73 | 65.90 | 65.73 | | |
| SVM | [17] | 96.38 | 97.67 | 97.58 | 96.64 | 95.15 | 95.59 | 96.41 | 97.64 | | 64.93 | 67.67 | 68.23 | 72.10 | |
| | [1] (levels) | 96.83 | 97.66 | 97.96 | | 96.14 | 96.39 | 96.35 | | | 63.53 | 67.13 | 67.57 | | |
| | Proposed | 96.47 | 98.07 | 98.37 | | 97.68 | 97.77 | 97.62 | | | 67.90 | 69.03 | 69.53 | | |



(a)

(b)

(c)

Fig. 6. ROC curves for the proposed verification system on the studied databases: XM2VTS (a), FERET (b), and LFW (c), with the use of a linear kernel SVM. Due to the good performance, for XM2VTS and FERET, the shown probability range is reduced to ease visibility.

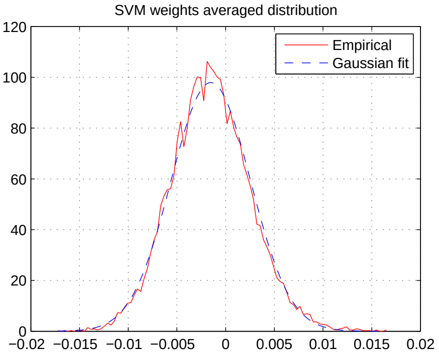


Fig. 7. SVM weights distribution for quantized XM2VTS.

work as the basis for our non-interactive privacy-preserving face recognition protocol.

### B. Complexity Analysis

In order to test the efficiency of our work, we implemented the extended cryptosystem and applied it for privately calculating the weighted Euclidean distance between a pair of quantized Gabor feature vectors. We choose the $N_L = 8$ indices quantization for its good compromise between clear-text cardinality and verification performance. The lattice size is fixed to $n = 2048$ dimensions, with $t = 380$ and $q = 1-20/n$, for a security parameter of $\lambda \approx 70$. We work with 4000-dimensional Gabor vectors for each face ($10\times 10$ localizations, 8 orientations and 5 scales) with 3-bit coefficients. Calculating the weighted Euclidean distance between two vectors thus needs two multiplications per pair of values, 3999 additions and one subtraction. Hence, starting from 8-level coefficients and 4-level weights, the resulting score is correctly represented using $\lceil \log_2(4000 \cdot 2 \cdot 8^2 \cdot 4)\rceil = 21$ bits (19 bits without weights), so we use $k = 22$ bits for the extended cryptosystem. Accounting for the $\log_2(4000) = 11.97$ bits of decrease for the effective decryption radius, Eq. (2) yields 13 supported consecutive multiplications, so the extended cryptosystem can perfectly cope with the distance calculation, with an arbitrarily bounded probability of incurring on decryption errors.

Our C++ implementation uses GMP[4] and NTL[5] libraries. We tested the time efficiency without any kind of parallelization in one core of an Intel i5 at 3.30GHz with 8GB of RAM. Table III shows the efficiency figures for the proposed algorithm compared to the expected running times of a *traditional* implementation based on an additive homomorphism (2048-bit modulus Paillier [12]), with either clear-text templates and weights (PaillierCT, partial privacy) and with encrypted templates and weights (PaillierE, total privacy using interactive multiplication protocols). In both Paillier-based systems the client provides the encryptions of both his/her face coefficients and their squared value, in the most favorable case for Paillier's homomorphism. The original GH11 using binary circuits for addition and multiplication needs one bootstrapping circuit after each multiplication gate to provide valid outputs; without them, the verification circuit exceeds the homomorphic capacity and produces erroneous outputs. Taking into account that the verification circuit involves around $3.2 \cdot 10^5$ products, and each bootstrapping circuit takes around 8 seconds in our test machine, GH11 would take *almost one month* for executing one verification. Hence, we report the execution times of GH11 *without the needed bootstrapping circuits* just as a reference.

[4] GNU MultiPrecision Arithmetic Library, http://gmplib.org
[5] Number Theory Library, http://www.shoup.net/ntl/

TABLE III
CLIENT AND SERVER (HP) TIMES AND NEEDED COMMUNICATION FOR THE PRIVATE VERIFICATION WITH AND WITHOUT SVMS.

| Execution times | No SVMs | | | | SVMs | | | |
|---|---|---|---|---|---|---|---|---|
| | Client | | Server | Communication | Client | | Server | Communication |
| | Cipher | Decrypt | (HP) | | Cipher | Decrypt | (HP) | |
| Proposed | 1.4 s | $1.5 \cdot 10^{-3}$ s | $5.9 \cdot 10^{1}$ s | 393 MB | 1.4 s | $1.5 \cdot 10^{-3}$ s | $1.2 \cdot 10^{2}$ s | 393 MB |
| GH11 (binary) | 4.5 s | $2.9 \cdot 10^{-1}$ s | $5.5 \cdot 10^{3}$ s | 1.18 GB | 4.5 s | $2.9 \cdot 10^{-1}$ s | $6.0 \cdot 10^{3}$ s | 1.18 GB |
| PaillierCT | $1.2 \cdot 10^{1}$ s | $4.4 \cdot 10^{-3}$ s | $9.9 \cdot 10^{1}$ s | 4.1 MB | $1.2 \cdot 10^{1}$ s | $4.4 \cdot 10^{-3}$ s | $1.8 \cdot 10^{2}$ s | 4.1 MB |
| PaillierE | $1.7 \cdot 10^{1}$ s | $3.3 \cdot 10^{1}$ s | $4.2 \cdot 10^{2}$ s | 10.2 MB | $2.3 \cdot 10^{1}$ s | $6.7 \cdot 10^{1}$ s | $7.5 \cdot 10^{2}$ s | 16.4 MB |

Our extension makes the system feasible in terms of bandwidth and processing time: the use of homomorphic operations in $\mathbb{Z}_{2^k}$ instead of $\mathbb{Z}_2$ reduces the server computation time in almost two orders of magnitude (furthermore, GH11 does not provide a correct output without the needed deciphering circuits), while the bandwidth is divided by a factor of three.

In terms of computational efficiency, the extended cryptosystem clearly improves on Paillier-based ones, even the system working with clear-text templates. The load for the client decreases in one order of magnitude with respect to Paillier, while the server's load is almost halved. This is due to the lighter homomorphic operations compared to Paillier's, even when working with larger ciphertexts. Conversely, the transferred encryptions for the proposed system are roughly one order of magnitude higher than for encrypted Paillier templates, due to the larger expansion factor that lattice cryptosystems like GH11 present. This is the main fact that constrains the performance of the homomorphism; our extension advances in this path, reducing the expansion factor and greatly increasing the efficiency of the operations performed non-interactively at the server. Furthermore, in an outsourced system that processes private data the initial bandwidth is not critical: the more operations that can be performed *unattendedly*, the more versatile and powerful the system becomes.

## VI. SECURITY CONSIDERATIONS

In this section we briefly make some considerations about the security of the proposed extension to Gentry's cryptosystem and the privacy-preserving face verification system.

We have already pointed out that the same Birthday attack security as the original GH11 cryptosystem is kept (see Section IV-C1). Regarding the dimensionality $n$ of the lattice $L$ and the hardness of finding the closest lattice vector without a good basis, it directly involves the $\gamma$-BDDP [38] (Bounded Distance Decoding Problem): given a vector $\boldsymbol{c}$, a lattice point must be found, knowing that there is at least one lattice point $\boldsymbol{p} \in L$ at a distance $\text{dist}(\boldsymbol{p}, \boldsymbol{c}) \leq \det(L)^{1/n}/\gamma$, with $\gamma > 1$. The best known algorithms for solving the $\gamma$-BDDP have exponential time-complexity in $n/\log\gamma$.[6] Our extension increases the radius of the noise in fresh encryptions with respect to the original [18]: approximately $2^k\sqrt{(1-q)\cdot n}$ for our extension, against $2\sqrt{(1-q)\cdot n}$ for the encryptions in [18]. Consequently, we increase the gap between the message vectors and the noise vectors by the same amount that we reduce the gap between the noise vectors and the boundaries of the Voronoi cell of the lattice. Hence, as we are not changing the structure of the lattice generated by $\boldsymbol{B}$, we are essentially keeping constant $\gamma$ for the $\gamma$-BDDP in our extended cryptosystem, just trading homomorphic capacity by an increased space for plaintexts[7].

Additionally, the performance of the presented system is really promising, as the execution times are comparable to those obtained with a Paillier-based system. The main drawback for even higher-dimensional lattices is the increase in the size of the keys, that imposes a very high bandwidth for transferring the encryptions. In this sense, there are two research directions targeted at alleviating this problem, and they are related to reducing either the size of the keys [39], or the cipher expansion; our work falls under the second category.

Regarding the security of the private face verification protocol, the semantical security of the underlying cryptosystem makes the whole protocol secure for semi-honest adversaries in the random oracle model. The only information that a semi-honest attacker may learn from the execution of the protocol is the verification soft score. This is indeed a piece of information that can be used (by a malicious attacker) in an oracle attack for extracting the information of a template for a given user, or the information for the used weight vector. If we want to restrict this kind of attacks limiting the given information to just one bit (a binary verification result), we can resort to one of the many interactive comparison protocols present in the literature (cf. Section V), like those used by Erkin *et al.* [8] or Sadeghi *et al.* [9]. This would involve a final interactive step that is not desired in an autonomous outsourced system. The development of non-interactive comparison protocols using fully-homomorphic encryptions is one of the open research lines that will follow this work.

## VII. CONCLUSIONS

In this paper we propose a fully private non-interactive face verification system that involves two novel contributions: a) an extension of Gentry's fully homomorphic cryptosystem that allows for non-interactively computing low to medium-degree polynomials with inputs of small plaintext cardinality; b) an optimal quantization strategy for Gabor-based face features, based on a novel statistical model for Gabor magnitudes. Only when combined, these two contributions enable the execution of the whole verification algorithm with non-interactive homomorphic operations.

We show that the developed model for Gabor magnitudes presents a better fit than previous models, and test the perfor-

[6] We refer the interested reader to the discussion in [38] by Gama and Nguyen, about the feasibility of the $\gamma$-BDDP in $n$ dimensional lattices with $n \in [100, 400]$.

[7] We thank Prof. Carlos Aguilar Melchor for insightful discussions on the security of our extended cryptosystem.

mance of the Lloyd-Max quantized system in XM2VTS [28], FERET [29] and LFW [30] databases, obtaining much better results than those achieved with other previously used distributions and quantization strategies, and considerable savings in storage. Our model opens a wide range of applications of independent interest, besides the presented data compression.

Additionally, the proposed extended cryptosystem trades homomorphic decryption capacity for high gains in efficiency when executing low to medium degree polynomials; this is only possible when working with compressed input features. The developed extension is the core of the proposed non-interactive fully-private outsourced face verification system, that is able to calculate a weighted $l$-norm distance between high-dimensional quantized and encrypted Gabor face features. Hence, our contribution enables the secure use of untrusted Cloud verification services.

Several future research lines can be highlighted: a) specifying the homomorphic decryption circuit for our extended cryptosystem; b) achieving other ways of reducing the cryptosystem cipher expansion while keeping the good homomorphic properties; this can be tackled by either increasing the plaintext size or decreasing the public key size for bigger lattices; finally, c) providing a non-interactive solution for comparison and other nonlinear operations that cannot be directly mapped by the nonbinary homomorphism is also challenging.

## VIII. Acknowledgments

We thank Prof. Nigel P. Smart and Prof. Carlos Aguilar Melchor, for their helpful comments and advise on the security of fully homomorphic cryptosystems. We also thank Enrique Argones-Rúa and Esteban Vázquez for their comments on the use and evaluation of the FERET database.

This work was partially funded by Xunta de Galicia under projects "Consolidation of Research Units" 2010/85, SAFECLOUD (ref. 09TIC014CT), SCALLOPS (ref. 10PXIB322231PR) and VISAGE (ref. 10TIC008CT), by the Spanish Ministry of Science and Innovation under project DYNACS (ref. TEC2010-21245-C02-02/TCM), COMONSENS (ref. CSD2008-00010) of the CONSOLIDER-INGENIO 2010 Program, and PRISMED (ref. IPT-2011-1076-900000) of the INNPACTO 2011 Subprogram, and by the Fundación Pedro Barrié de la Maza under project SCAPE.

## References

[1] J. R. Troncoso-Pastoriza, D. González-Jiménez, and F. Pérez-González, "A new model for Gabor Coefficients' Magnitude in Face Recognition," in *IEEE ICASSP 2010*. Dallas, USA: IEEE, March 2010.

[2] J. R. Troncoso-Pastoriza and F. Pérez-González, "Fully Homomorphic Faces," in *IEEE ICIP*. IEEE, 2012, pp. 2657–2660.

[3] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face Recognition: A Literature Survey," *ACM Computing Surveys*, vol. 35, no. 4, pp. 399–458, 2003.

[4] A. Senior and S. Pankanti, *Privacy Protection and Face Recognition*, 236 Gray's Inn Road — Floor 6 London — WC1X 8HL — UK, 2011, pp. 671–692.

[5] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric Template Security," *EURASIP J. Adv. Signal Process*, vol. 2008, pp. 113:1–113:17, Jan. 2008.

[6] T. Ignatenko and F. M. J. Willems, "Biometric Systems: Privacy and Secrecy Aspects," *IEEE Trans. on Information Forensics and Security*, vol. 4, no. 4, pp. 956–973, December 2009.

[7] A. López-Alt, E. Tromer, and V. Vaikuntanathan, "On-the-Fly Multiparty Computation on the Cloud via Multikey Fully Homomorphic Encryption," in *STOC'12*, 2012.

[8] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, "Privacy-Preserving Face Recognition," in *PETS'09*, ser. Lecture Notes in Computer Science, no. 5672, 2009, pp. 235–253.

[9] A.-R. Sadeghi, T. Schneider, and I. Wehrenberg, "Efficient Privacy-Preserving Face Recognition," in *ICISC 2009*, ser. Lecture Notes in Computer Science, vol. 5984. Springer, 2010, pp. 229–244.

[10] M. Turk and A. Pentland, "Eigenfaces for Recognition," *J. Cognitive Neuroscience*, vol. 3, pp. 71–86, January 1991.

[11] Y. Luo, S. c. S. Cheung, and S. Ye, "Anonymous Biometric Access Control Based on Homomorphic Encryption," in *IEEE International Conference on Multimedia and Expo, ICME 2009*, 2009, pp. 1046–1049.

[12] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," in *EUROCRYPT'99*, ser. Lecture Notes in Computer Science, vol. 1592. Springer, 1999, pp. 223–238.

[13] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich, "SCiFI - A System for Secure Face Identification," in *IEEE Symposium on Security & Privacy*, May 2010, pp. 239–254.

[14] M. Barni, T. Bianchi, D. Catalano, M. D. Raimondo, R. D. Labati, P. Failla, D. Fiore, R. Lazzeeretti, V. Piuri, A. Piva, and F. Scotti, "A Privacy-Compliant Fingerprint Recognition System Based on Homomorphic Encryption and Fingercode Templates," in *IEEE Intl. Conference on Biometrics: Theory Applications and Systems*, 2010, pp. 1–7.

[15] M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. V. Jawahar, "Blind Authentication: A Secure Crypto-Biometric Verification Protocol," *IEEE Trans. on Information Forensics and Security*, vol. 5, no. 2, pp. 255–268, June 2010.

[16] J. R. Troncoso-Pastoriza and F. Pérez-González, "Secure Signal Processing in the Cloud: Enabling Technologies for Privacy-Preserving Multimedia Cloud Processing," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 29–41, March 2013.

[17] D. González-Jiménez, F. Pérez-González, P. Comesaña-Alfaro, L. Pérez-Freire, and J. Alba-Castro, "Modeling Gabor Coefficients via Generalized Gaussian Distributions for Face Recognition," in *ICIP*, 2007.

[18] C. Gentry and S. Halevi, "Implementing Gentry's Fully-Homomorphic Encryption Scheme," in *EUROCRYPT 2011*, ser. Lecture Notes in Computer Science, vol. 6632, 2011, pp. 129–148.

[19] Á. Serrano, I. Martín de Diego, C. Conde, and E. Cabello, "Recent Advances in Face Biometrics with Gabor Wavelets: A Review," *Pattern Recognition Letters*, vol. 31, no. 5, pp. 372–381, 2010.

[20] J. G. Daugman, "Complete Discrete 2D Gabor Transforms by Neural Networks for Image Analysis and Compression," *IEEE Trans. on Acoustics, Speech and Signal Processing*, vol. 36, no. 7, pp. 1169–1179, July 1988.

[21] J. Zhu, D. Cao, S. Liu, Z. Lei, and S. Z. Li, "Discriminant Analysis with Gabor Phase for Robust Face Recognition," in *Proceedings of The 5th IAPR International Conference on Biometrics (ICB 2012)*, New Delhi, India, 2012.

[22] S. Xie, S. Shan, X. Chen, and J. Chen, "Fusing Local Patterns of Gabor Magnitude and Phase for Face Recognition," *IEEE Trans. on Image Processing*, vol. 19, no. 5, pp. 1349–1361, 2010.

[23] J. Hernández, M. Amado, and F. Pérez-González, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure," *IEEE TIP*, vol. 9, no. 1, pp. 55–68, January 2000, special Issue on Image and Video Processing for Digital Libraries.

[24] M. Do and M. Vetterli, "Wavelet-Based Texture Retrieval Using Generalized Gaussian Density and Kullback-Leibler Distance," *IEEE TIP*, vol. 11, no. 2, pp. 146–158, 2002.

[25] J. R. Troncoso-Pastoriza, "Encrypted Domain Processing for Signal Processing Applications," Ph.D. dissertation, University of Vigo, Vigo, Spain, April 2012. [Online]. Available: http://webs.uvigo.es/gpscuvigo/sites/default/files/publications/jr_troncoso_thesis.pdf

[26] D. González-Jiménez, E. Argones-Rúa, F. Pérez-González, and J. Alba-Castro, "Modeling Magnitudes of Gabor Coefficients: the $\beta$-Rayleigh Distribution," in *ICIP*, 2009.

[27] T. I. Alecu, S. Voloshynovsky, and T. Pun, "The Gaussian Transform," in *EUSIPCO'05*, 2005.

[28] K. Messer, J. Matas, J. Kittler, J. Luettin, and G. Maitre, "XM2VTSDB: The Extended M2VTS Database," *AVBPA*, pp. 72–77, March 1999.

[29] H. Moon and P. Phillips, "The FERET verification testing protocol for face recognition algorithms," in *IEEE Intl. Conf on Automatic Face and Gesture Recognition*, apr 1998, pp. 48–53.

[30] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, "Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments," University of Massachusetts, Tech. Rep. 07-49, 2007.

[31] T. Cover and J. Thomas, *Elements of Information Theory*. John Wiley & Sons, New York, 1991.

[32] J. Max, "Quantizing for Minimum Distortion," *IRE Trans. on Information Theory*, vol. IT-6, pp. 7–12, 1960.

[33] A. K. Lenstra, H. W. Lenstra, and L. Lovsz, "Factoring Polynomials with Rational Coefficients," *Mathematische Annalen*, vol. 261, pp. 515–534, 1982.

[34] D. Micciancio, "Improving Lattice based Cryptosystems using the Hermite Normal Form," in *Cryptography and Lattices Conference — CaLC 2001*, ser. Lecture Notes in Computer Science, J. Silverman, Ed.,

vol. 2146. Providence, Rhode Island: Springer-Verlag, March 2001, pp. 126–145.

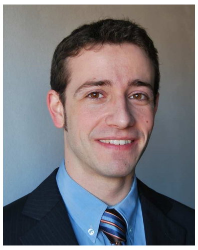
[35] C. Gentry, “A fully homomorphic encryption scheme,” Ph.D. dissertation, Stanford University, 2009.

[36] V. N. Vapnik, *The Nature of Statistical Learning Theory*, 2nd ed. Springer, 2000.

[37] N. Pinto, J. Dicarlo, and D. Cox, “Establishing Good Benchmarks and Baselines for Face Recognition,” in *IEEE ECCV*, 2008, faces in ’Real-Life’ Images Workshop.

[38] N. Gama and P. Q. Nguyen, “Predicting Lattice Reduction,” in *EUROCRYPT 2008*, ser. Lecture Notes in Computer Science, vol. 4965. Springer, 2008.

[39] J.-S. Coron, A. Mandal, D. Naccache, and M. Tibouchi, “Fully Homomorphic Encryption over the Integers with Shorter Public Keys,” in *Advances in Cryptology - CRYPTO11*, ser. Lecture Notes in Computer Science, vol. 6841, 2011, pp. 487–504.



**Juan Ramón Troncoso-Pastoriza** received the M.S. degree in Telecommunications Engineering from the University of Vigo, Vigo, Spain, in 2005, when he also received the National Best Graduate Student Award from the Spanish Ministry of Education and Science. In 2012, he received the Ph.D. in Telecommunications Engineering and the Best Ph.D. Thesis Award from the University of Vigo.

He has been working at the Signal Theory and Communications Department in the University of Vigo since 2005 as an Associate Researcher. Between 2006 and 2007 he visited the Information and Systems Security Department at Philips Research Europe (The Netherlands). He has participated in several National and European projects related to information security and privacy protection, an area in which he has authored numerous papers in international journals and conferences and filed several international patent applications.

His research interests include secure signal processing, privacy protection, multimedia security and image modeling.

**Daniel González-Jiménez** received the Telecommunication Engineer degree from the University of Vigo, Spain, in 2003 and the PhD (European mention) from the University of Vigo in 2008. He received the COETG/AETG award for the best doctoral thesis applied to the ICT sector in 2009.

Daniel joined GRADIANT in 2008, where he currently co-leads the Multimodal Information Area. Daniel has a strong record of R&D projects involving face processing and biometrics, including the Biosecure Network of Excellence. He has published more than 25 conference and journal papers, and 2 book chapters in audiovisual analysis, machine learning and data fusion. His current research interests include biometrics and face processing, affective computing, object detection and tracking, and scene understanding.

**Prof. Fernando Pérez-González** (M90-SM09) received the Telecommunication Engineer degree from the University of Santiago, Santiago, Spain in 1990 and the Ph.D. from the University of Vigo, Vigo, Spain, in 1993, also in Telecommunication Engineering. He joined the faculty of the School of Telecommunication Engineering, University of Vigo, as an assistant professor in 1990 and is currently Professor in the same institution. During 2009-2011 he was the holder of the Prince of Asturias Endowed Chair on Information Science and Technology at the University of New Mexico (UNM), where he is now Research Professor. Since 2007 he is the founding Executive Director of the Galician Research and Development Center in Advanced Telecommunications (GRADIANT).

His research interests lie in the areas of digital communications, adaptive algorithms, robust control, digital watermarking and information forensics and security. He has coauthored several international patents related to watermarking for video surveillance, integrity protection of printed documents, fingerprinting of audio signals, and digital terrestrial broadcasting systems. Prof. Pérez-González has co-authored over 50 papers in leading international journals and more than 140 conference papers. He has been the principal investigator of the University of Vigo group which participated in several European projects, including CERTIMARK, ECRYPT and REWIND. From 2007-2010 he was Manager of the Spanish National R&D Plan on Electronic and Communication Technologies, Ministry of Science and Innovation. Prof. Pérez-González served as Associate Editor of IEEE SIGNAL PROCESSING LETTERS (2005-2009) and the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY (2006-2010). Currently, he is Associate Editor of the LNCS TRANSACTIONS ON DATA HIDING AND MULTIMEDIA SECURITY, and the EURASIP INTERNATIONAL JOURNAL ON INFORMATION FORENSICS AND SECURITY.