Secure Signal Processing for Outsourced Face Verification

Biométrie, Indexation multimédia et Vie privée
6th October 2015
Paris (Telecom ParisTech)

AtlanTIC

Dr. Juan R. Troncoso Pastoriza
troncoso@gts.uvigo.es

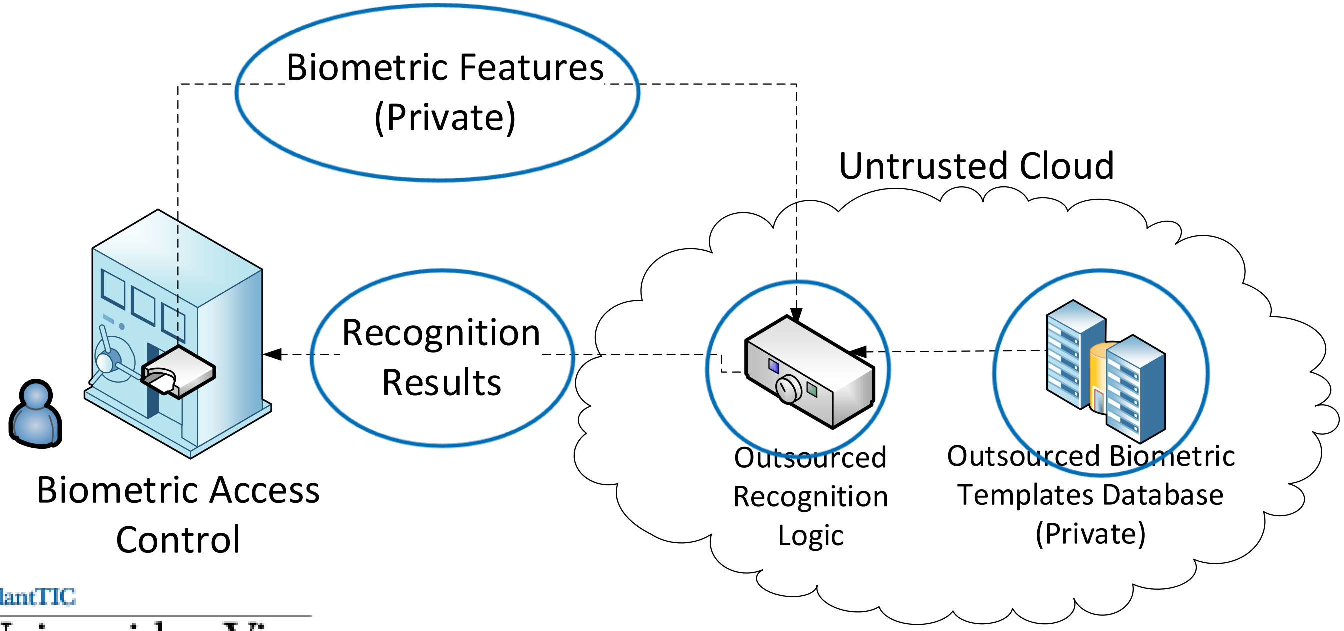
Outline

- Privacy in Outsourced Verification
- Template Protection
  - Cryptography-Based Alternatives
- Secure Signal Processing
  - Homomorphic Encryption: advances and limitations
- Encrypted Face Verification
  - Chronology and Recent Approaches
- Challenges for Privacy-Preserving Outsourced Face Verification

Privacy in Outsourced Verification

Privacy in Outsourced Biometrics

- Biometric vs traditional authentication
  - Universal, Reliable
  - Revocability, Security, Privacy
- Outsourced Biometric Recognition

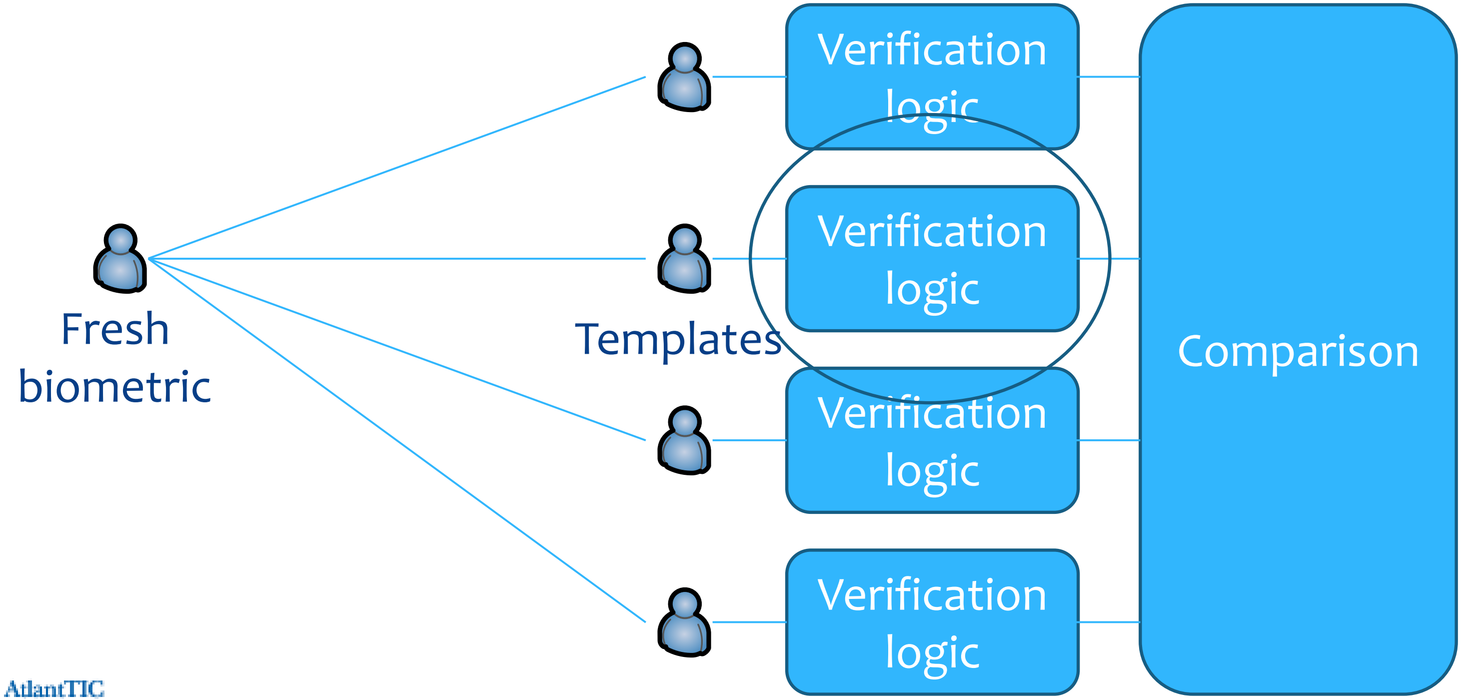


- Storage
- Communication
- Processing

AtlantTIC
Universida de Vigo

Privacy in Outsourced Biometrics

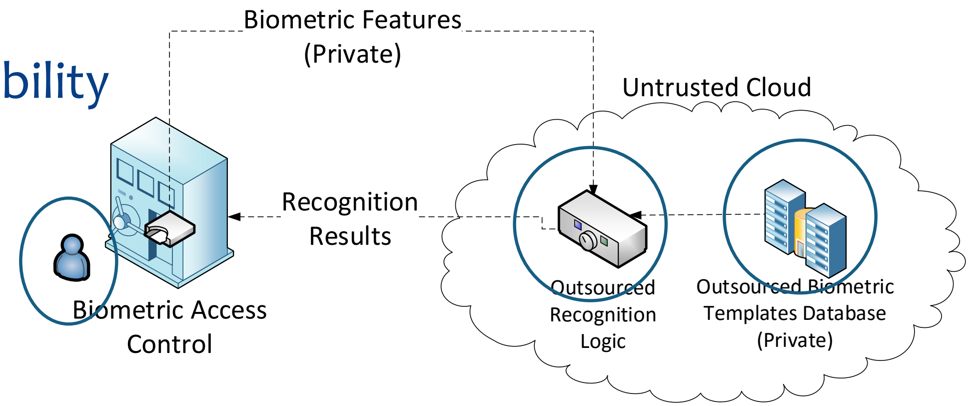
- Verification vs Identification
  - One-to-one: verification logic
  - One-to-many: verification logic + comparison



AtlantTIC
Universida de Vigo

Privacy in Outsourced Biometrics

- Secure Biometrics
  - Secure Encoding (biometric + key)
    - Irreversibility
    - Unlinkability
    - Renewability/Revocability
    - Privacy Leakage
  - Secure Matching
    - Performance



Template Protection

Cryptography-based alternatives

Template Protection

- Biometric template protection systems
  - Cancellable biometrics/feature transformation
    - Biohashing
  - Biometric cryptosystems/HDS
    - Key-binding (fuzzy commitments)
    - Key-generation (secure sketches)
- Characteristics
  - High entropy random sequence through key/salt
  - The helper data leak information about the biometric (privacy leakage)
- Assumptions
  - Public database
  - Verification in a trusted domain
  - Revocability based on key (two-factor)

Template Protection

- Comparison [RWSI13]

	Cancellable Biometrics	HDS	Secure Computation
Analysis framework	Signal Processing	Information Theory	Cryptography
Adversary	Bounded	Un/bounded	Bounded
Revocability	Yes	Two-factor	Yes
Storage	Low	Low	High
Overhead	Low	Low	High

- But we are trying to protect both templates and fresh query faces, keeping the verification logic outsourced
  - CB and HDS are not enough, SC does not account for SP

Secure Signal Processing

Efficient Privacy-preserving Solutions for Multimedia

Secure Signal Processing

- Secure Signal Processing (SSP) or Signal Processing in the Encrypted Domain (SPED)
  - Marriage of Cryptography and Signal Processing
  - Efficient Solutions for Privacy Problems in SP
- Traditional cryptography can protect data during communication or storage, but it cannot **prevent the access** to the data when they are sent to an **untrustworthy party**. Through advanced encryption techniques, SSP provides means to **process signals while they are encrypted**, without prior decryption and without the decryption key, thus enabling fully secure services like **Cloud computing over encrypted data**.

Secure Signal Processing

- Examples of services and outsourced processes with private or sensitive signals
  - eHealth: semi-automated diagnosis or decision support (MRI, ECG, DNA,…)
  - Social media / social data mining
  - Smart metering: use of fine-grained metered data
  - Banking and financial information
  - Large scale/big data processing with sensitive data (social data, personal information, business-critical processes)
  - **Biometrics:** outsourcing of authentication/identification processes (faces, fingerprints, iris)
- Current situation: *Non-proportional collection or usage leads to unjustified user profiling*
- SSP mission: enable secure services with
  - Integration of data protection supported by cryptographic techniques (efficient homomorphic processing, SMC, searchable encryption,…)
  - Versatile, flexible and efficient solutions combining cryptography and signal processing
  - No impairment for service providers

Privacy Tools from SSP

- Available SSP tools to produce privacy-preserving systems
  - SMC (Garbled Circuits)
  - Homomorphic Encryption (FHE, SHE)
  - Searchable Encryption and PIR
  - Secure (approximate) interactive protocols
  - Obfuscation mechanisms (diff. private)

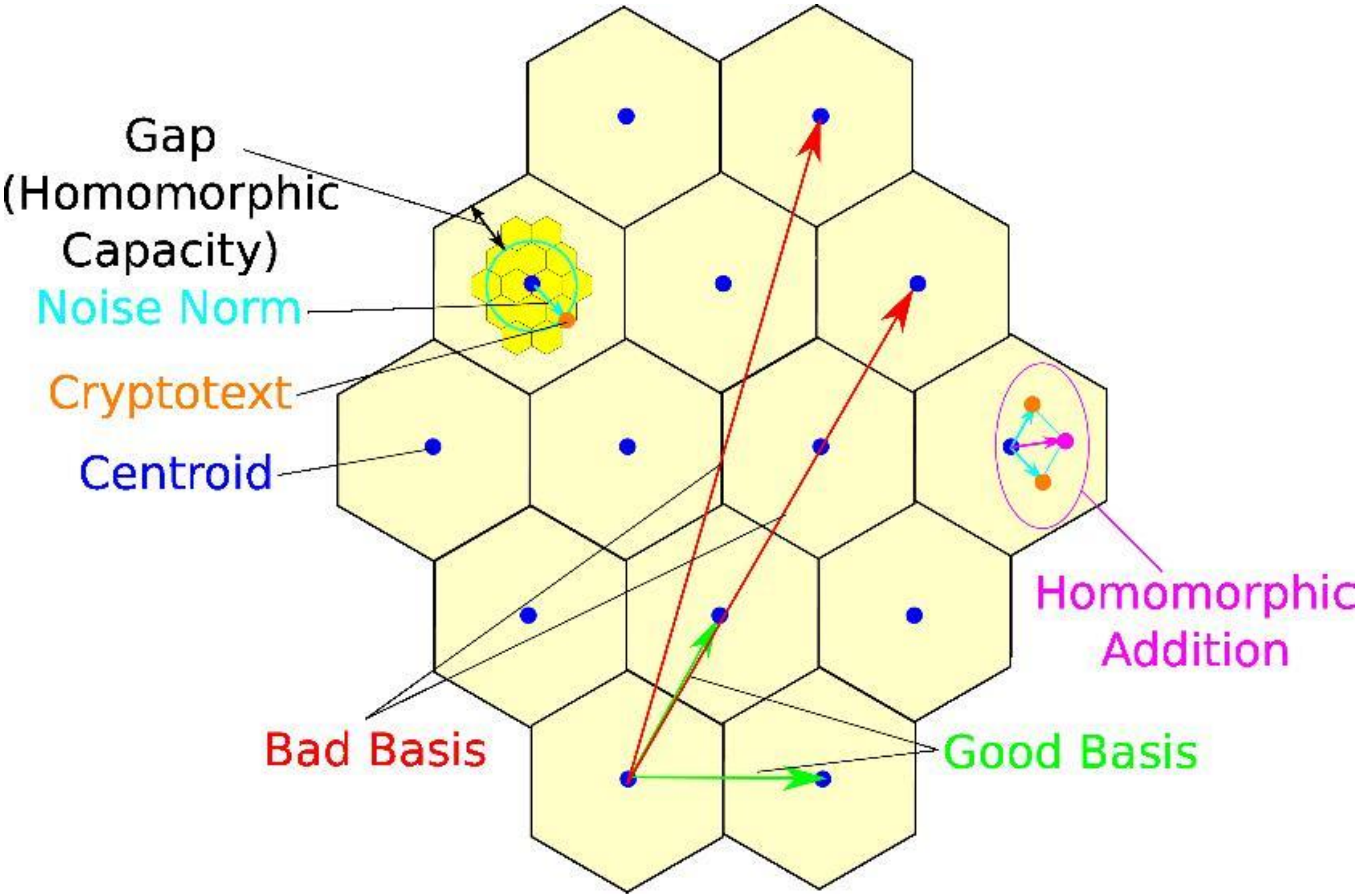
Homomorphic Encryption

- Fundamental idea (group homomorphisms)
  - $(P,+) \longrightarrow^{E_k} (C,\circ)$
  - $E_k(x+y) = E_k(x) \circ E_k(y)$
- Example: RSA (multiplicative)
  - $E_k(x) = x^e \ mod \ n$ $\qquad (P,\cdot) \longrightarrow^{E_k} (C,\cdot)$
  - $(x \cdot y)^e = (x^e) \cdot (y^e) \ mod \ n$
- Example: Paillier (additive)
  - $E_k(x) = (1 + x \cdot n) \cdot r^n \ mod \ n^2$ $\qquad (P,+) \longrightarrow^{E_k} (C,\cdot)$
  - $E_k(x+y) = E_k(x) \cdot E_k(y) \ mod \ n^2, E_k(x \cdot k) = E_k(x)^k \ mod \ n^2$
- Cryptosystems with semantic security

Homomorphic Encryption

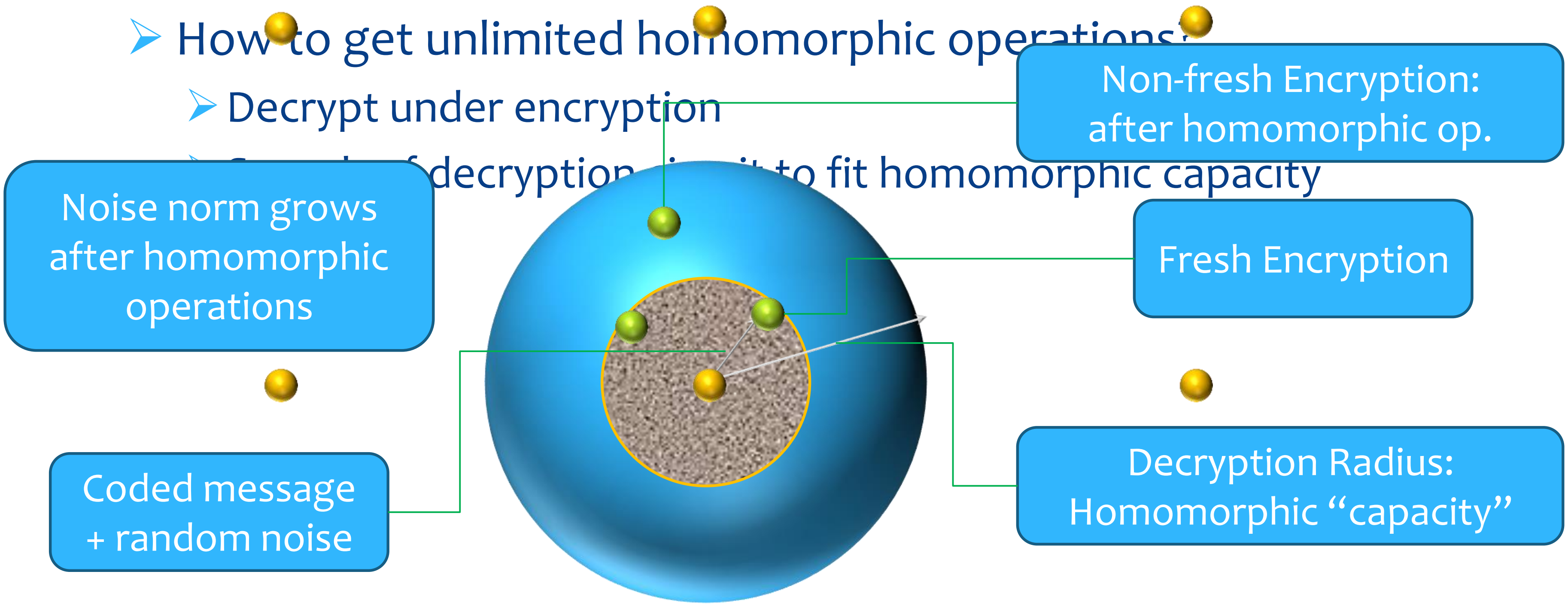
- Challenges
  - Computation overhead
  - Cipher expansion
  - Versatility (only additions or multiplications)
- Somewhat and Fully Homomorphic Cryptosystems (SHE/FHE)

Lattice Crypto and FHE/SHE



Gentry's Lattice-based SHE Cryptosystem

- Gentry's somewhat homomorphic cryptosystem [GH11]
  - Can execute a limited-depth circuit, binary inputs
  - How to get unlimited homomorphic operations?
    - Decrypt under encryption
    - ... decryption ... to fit homomorphic capacity

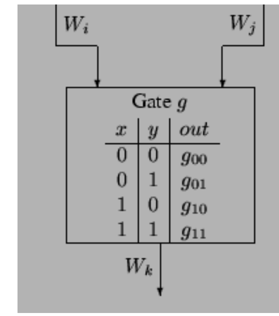


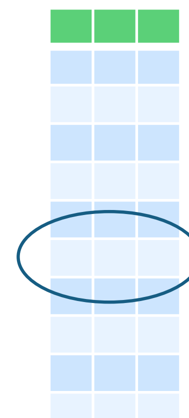
SHE vs FHE

- Bootstrapping is costly
- SHE is more efficient and a perfect candidate for SSP and simple verification logics
- A practical extension [TGP13]:
  - Works with non-binary plaintexts (increases fresh encryption norm)
  - Trades off full homomorphism for homomorphic capacity
  - Keeps key generation procedure
  - Negligible impact on decryption performance

SMC, PIR and OT

- SMC: Interactive protocols & binary evaluation (garbled circuits)
- Private Information Retrieval (PIR)
  - 1-out-of-N Oblivious Transfer (OT_1^N)
  - Alice asks for x_i from Bob's database of N elements
  - Bob sends x_i without knowing i





AtlantTIC
Universida de Vigo

Privacy Tools from SSP: Wrap-up

- There are only limited (secure) privacy homomorphisms known
- The limitations of HE can be tackled through interaction (non-colluding parties)
- Solutions for complex functions
  - Specific interactive protocols
  - Hybrid protocols homomorphic/*garbled circuits*
- Full Homomorphisms (allowing any function) are not practical… yet
  - Hot research topic in cryptography

Encrypted Face Verification

Chronology and Recent Approaches

Encrypted Face Verification

- Most representative examples of secure face verification
  - [EFGKLT09], [SSW10] Eigenfaces
  - [OPJM10] SCiFI, Set-distance
  - [TGP13] Gabor-based Euclidean distance
  - [YSKYK13] Hamming distance
  - [PTP15] Efficient Encrypted Image Filtering

Encrypted Face Verification

- [EFGKLT09]
  - Eigenfaces: PCA projection
    - Average face $\boldsymbol{\Psi}$ and Eigen-faces basis $\{\boldsymbol{u}_1, \dots, \boldsymbol{u}_K\}$
    - Projection of a face $\boldsymbol{\Gamma}^{ID}$: $\omega_i^{ID} = \boldsymbol{u}_i^T \cdot (\boldsymbol{\Gamma}^{ID} - \boldsymbol{\Psi}), i = 1, \dots, M$
    - Euclidean distance and threshold $\left\|\boldsymbol{\omega}^{fresh} - \boldsymbol{\omega}^{ID}\right\| < T$
  - Paillier encryptions (additively homomorphic)

$$\sum_{i=1}^{K} (\omega_i^{ID})^2 + \sum_{i=1}^{K} (-2\omega_i \omega_i^{ID}) + \sum_{i=1}^{K} \omega_i^2$$

$\boldsymbol{\Psi}$, $\{\boldsymbol{u}_1, \dots, \boldsymbol{u}_K\}$
$\{\boldsymbol{\omega}^1, \dots, \boldsymbol{\omega}^N\}$

$\boldsymbol{\Gamma}$ $E_k(\boldsymbol{\Gamma})$

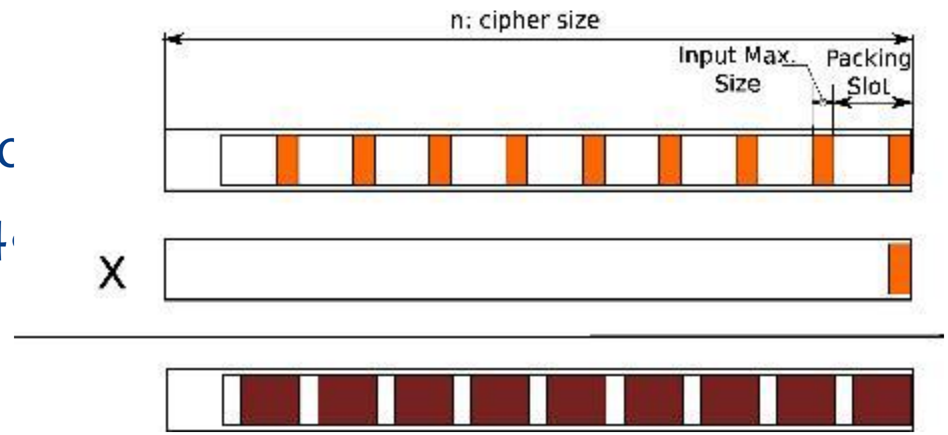
Projection: $E_k(\omega_i) = \prod_l \left(E_k(\Gamma_l) \cdot E_k(-\Psi_l)\right)^{u_{i,l}} \Big|_{i=1}^{K}$

Secure Product: $E_k(\omega_i^2)$

Distance: $E_k(d) = E_k\left(\sum_{i=1}^{K} (\omega_i^{ID})^2\right) \cdot \prod_{i=1}^{K} (E_k(\omega_i))^{-2\omega_i^{ID}} \cdot \prod_{i=1}^{K} E_k(\omega_i^2)$

Encrypted Face Verification

- [SSW10]
  - Minor improvement on prc
  - For mid-term security (204
  - ORL Database of Faces
    - 92x112=10304 pixels

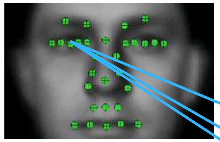


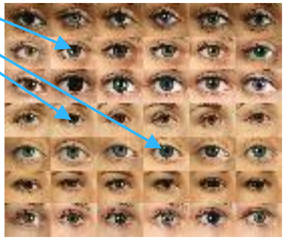
Computation [s]	Client	Server
Projection	0.60	17.43
Distance	16.87	1.52
Total	17.47	18.95

Communication	
Encrypted Face	5.03 MB
Distance	1.0 kB
Total	5.03 MB

Encrypted Face Verification

- SCiFI [OPJM10]
  - Redefines crypto-amenable face representation and logic
  - Face representation
    - Public database Y: parts defined as patches
      - p vocabularies of N parts (gallery)
    - Face: list of most similar patches per part: $s = (s^a, s^s)$
      - s^a: appearance: p sets of n vocabulary indices from Y
      - s^s: spatial: sets of n quantized distance to center
  - Matching logic:
    - Set distance between fresh biometric and template
    - Threshold defined per each user



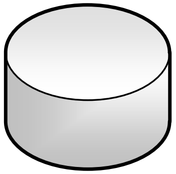


Encrypted Face Verification

- SCiFI verification:
  - Binary representation of the face vector s $= (s^a, s^s)$ (900 bits)
    - Hamming distance = Set distance $d_{max} = 180$

$E_k(\underbrace{1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 0}_{\omega})$

0 1 1 0 0 1 1 0 1 0



For each user $\omega^{ID} = (s^a, s^s), \tau$

$$E_k(d_H) = E_k\left(\sum_{i=1}^{900} \omega_i^{ID}\right) \cdot \prod_{\omega_i^{ID}=0} (E_k(\omega_i)) \cdot \left(\prod_{\omega_i^{ID}=1} (E_k(\omega_i))\right)^{-1}$$

Blind Haming distance: $E_k(d_H) \cdot E_k(r_i)$

$(d_H + r_i)\ mod\ (d_{max} + 1)$

$OT_1^{d_{max}+1}$

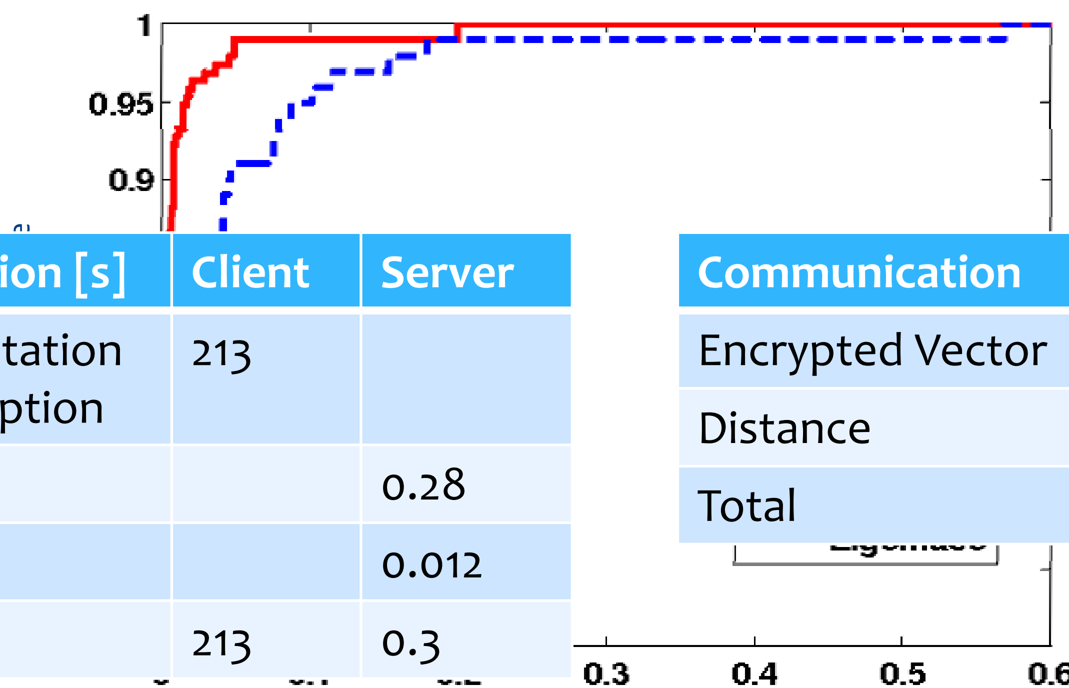
$$\begin{cases} 1\ if\ 0 \leq (d_H)\ mod\ (d_{max} + 1) \leq \tau^{ID} \\ 0 \quad otherwise \end{cases}$$

AtlantTIC
Universida de Vigo

Encrypted Face Verification

- SCiFi performance

ROC for FERET fc



False Positive Rate

Computation [s]	Client	Server
Precomputation And encryption	213	
Distance		0.28
OT		0.012
Total	213	0.3

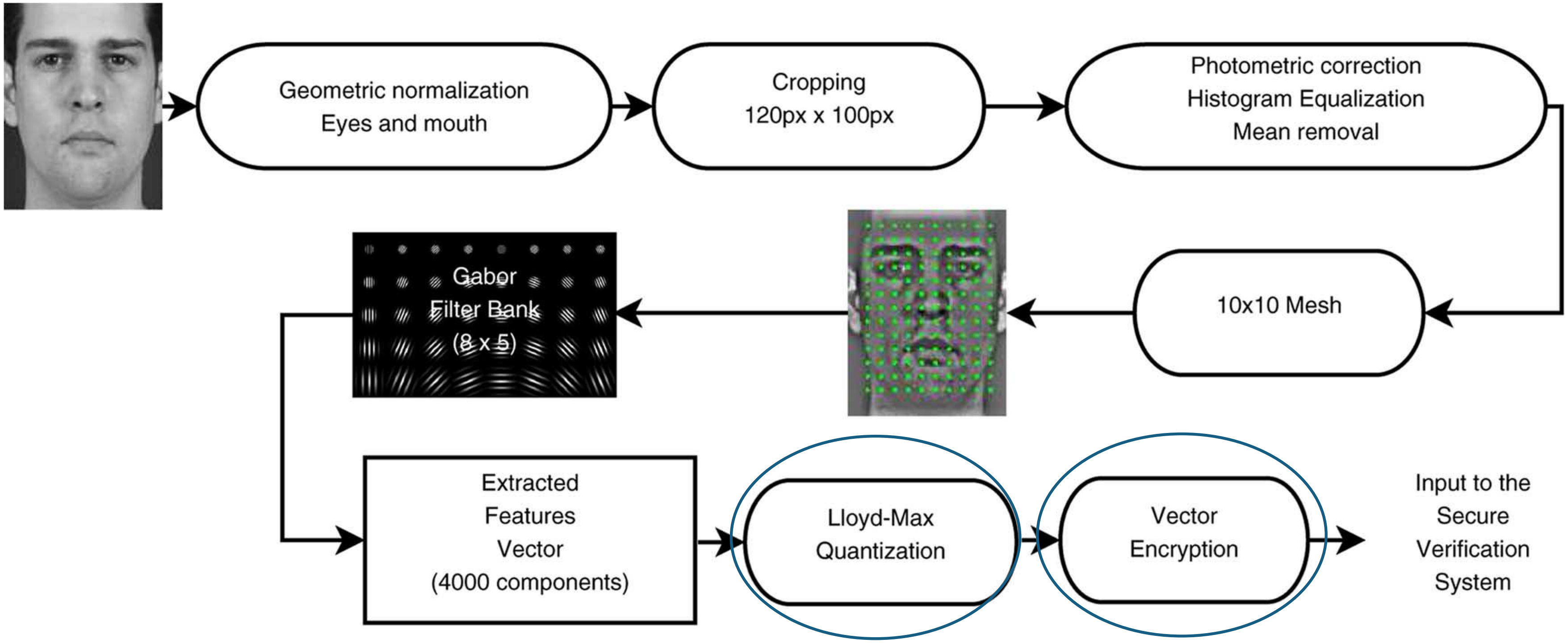
Communication	
Encrypted Vector	450 kB
Distance	1.0 kB
Total	451 kB

Encrypted Face Verification

- Encrypted verification, but
  - The server learns the whole template database
  - Enrolled users' faces can be reconstructed
  - Only the query face and the verification result is protected
- For an outsourced scenario:
  - Fully encrypted template database
  - Encrypted query faces
  - Minimum interaction rounds for the verification result
  - Lightweight client-side processing (encrypt-decrypt)

Fully Encrypted Face Verification

- [TGP13]
  - SHE with low plaintext cardinality
  - Non-linear optimal quantization of inputs
  - Compact and accurate statistical representation

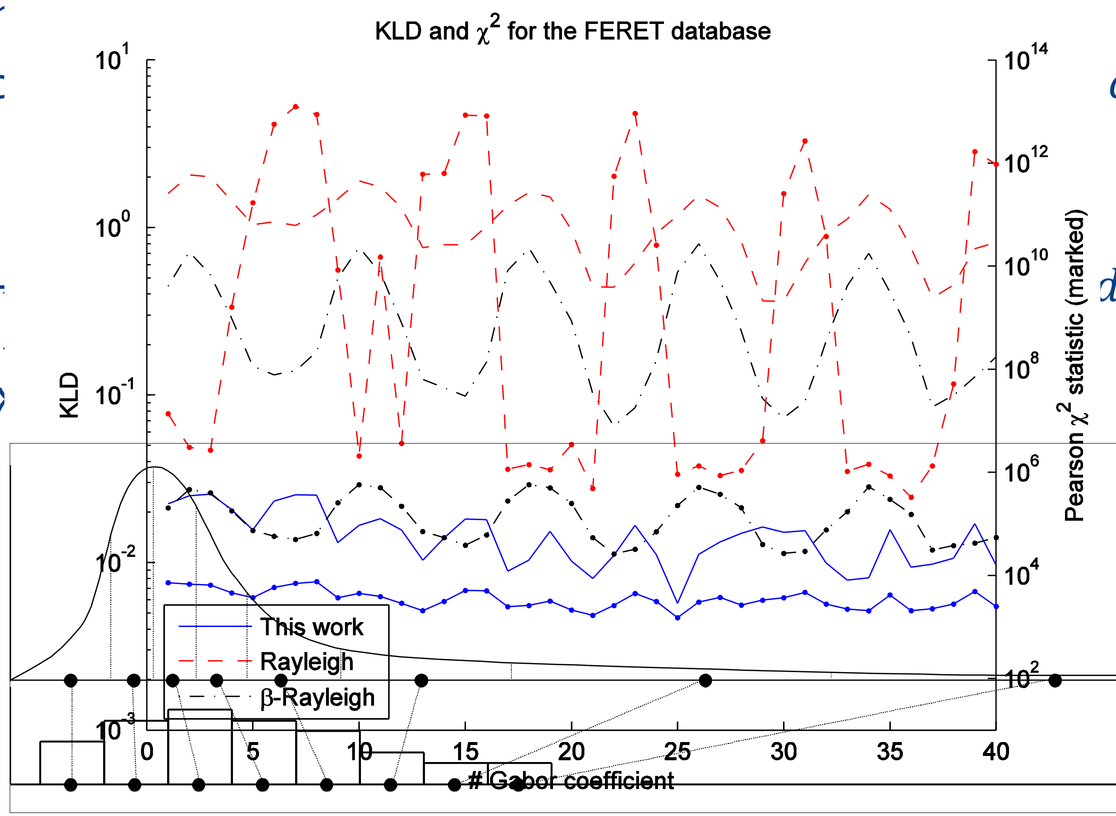


Fully Encrypted Face Verification

- [TGP13]
  - Input representation
    - Gabor m
    - Statistic $c_i)$
    - $f_{|G_i|}(x)$

$$\frac{c_i \beta_i}{2 \cdot x \cdot \Gamma\left(1/c_i\right.} \quad d\omega$$

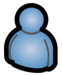
  - Lloyd-Ma



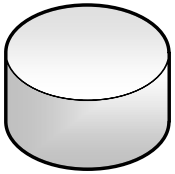
AtlantTIC
UniversidadeVigo

Fully Encrypted Face Verification

- [TGP13]
  - Verification
    - Soft score: weighed (SVM) Euclidean distance (degree-3 polynomial) - threshold
    - $\text{score}(\boldsymbol{g}, \boldsymbol{g}^{ID}) = \sum_{i=1}^{N_{tp}} \sum_{j=1}^{4000} \alpha_j \cdot \left(g_j - g_{i,j}^{ID}\right)^2 - Ntp \cdot \eta$
  - SHE for noninteractive calculation (extension of Gentry's)



$\boldsymbol{g}$ $\quad E_k(\boldsymbol{g})$



$E_k(\boldsymbol{\alpha}), E_k(\eta)$

For each user:

$\left\{E_k(\boldsymbol{g}_1^{ID}), \ldots, E_k(\boldsymbol{g}_{\boldsymbol{N_{tp}}}^{ID})\right\}$

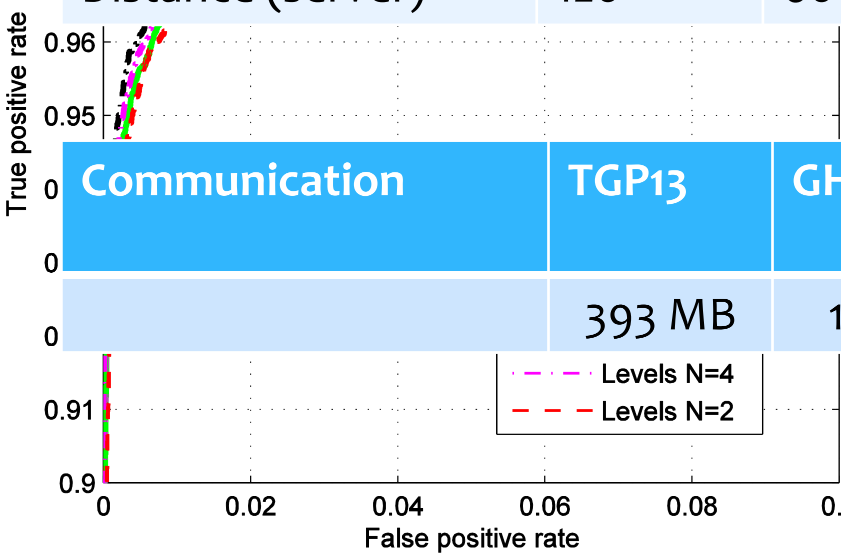
$$E_k(\text{score}) = \sum_{i=1}^{N_{tp}} \sum_{j=1}^{4000} E_k(\alpha_j) \cdot \left(E_k(g_j) - E_k(g_{i,j}^{ID})\right)^2 - Ntp \cdot E_k(\eta)$$

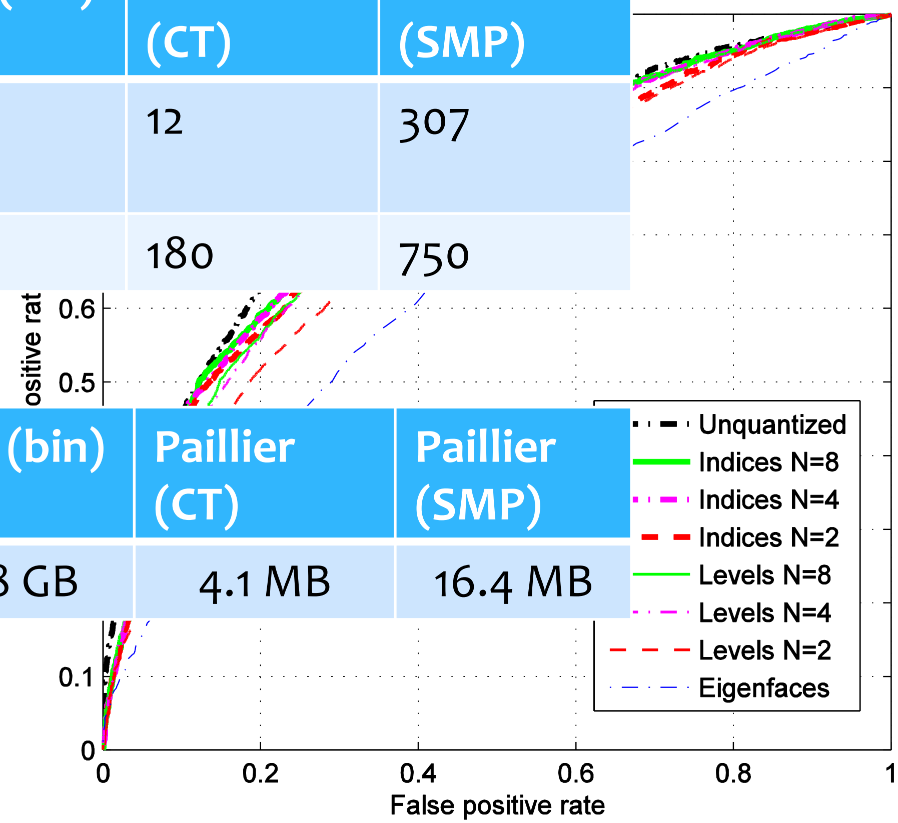
Fully Encrypted Face Verification

- [TGP13] performance

Computation [s]	TGP13	GH11 (bin)	Paillier (CT)	Paillier (SMP)
Encryption/ Decryption (client)	1.4	4.8	12	307
Distance (server)	120	6000	180	750

Communication	TGP13	GH11 (bin)	Paillier (CT)	Paillier (SMP)
	393 MB	1.18 GB	4.1 MB	16.4 MB





Fully Encrypted Face Verification

- [YSKYK13] improvement
  - Variant of GH11 with modified key generation
    - Encrypts polynomials, decrypts independent term
  - Packing inputs in SHE for Hamming distance
  - Input ve
    - $\mathrm{vEnc}_1($
    - $\mathrm{vEnc}_2($

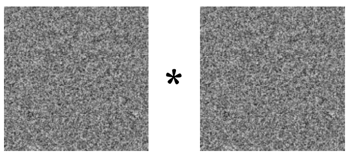
Efficiency	Yasuda HD
Computation	18.1 ms
Template size	19 kB

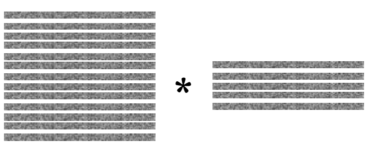
  - The product $\boldsymbol{c}$ of the two masked inputs has as i.t.
    - $c_0 = \sum_{i=0}^{2047} a_i \cdot b_i \bmod s$
  - Hamming distance: $d_H(\boldsymbol{a},\boldsymbol{b})$=$\sum_{i=0}^{2047}(a_i + b_i - 2a_i \cdot b_i)$
    - $C_1 = \sum_{i=0}^{2047} r^i \mod d,\ C_2 = -C_1 + 2 \mod d$
    - $ct_H = C_1 \cdot (-\mathrm{vEnc}_1(\boldsymbol{a}) + \mathrm{vEnc}_2(\boldsymbol{b})) + 2\,\mathrm{vEnc}_1(\boldsymbol{a}) \cdot (1 - \mathrm{vEnc}_2(\boldsymbol{b}))$

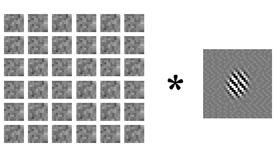
Feature extraction

- Except for Eigenfaces, only the verification logic (distance) has been outsourced
- Image pre-processing and feature extraction could also be outsourced
- Paillier only allows for linear projections
- Use of leveled SHE can improve on this
- [PTP15]: extension of RLWE to multivariate RLWE
  - Images represented as m-variate polynomials
  - 1 image = 1 encryption
    - Better cipher expansion
    - Better computational overhead
    - Better security

Encrypted image filtering with 2-RLWE



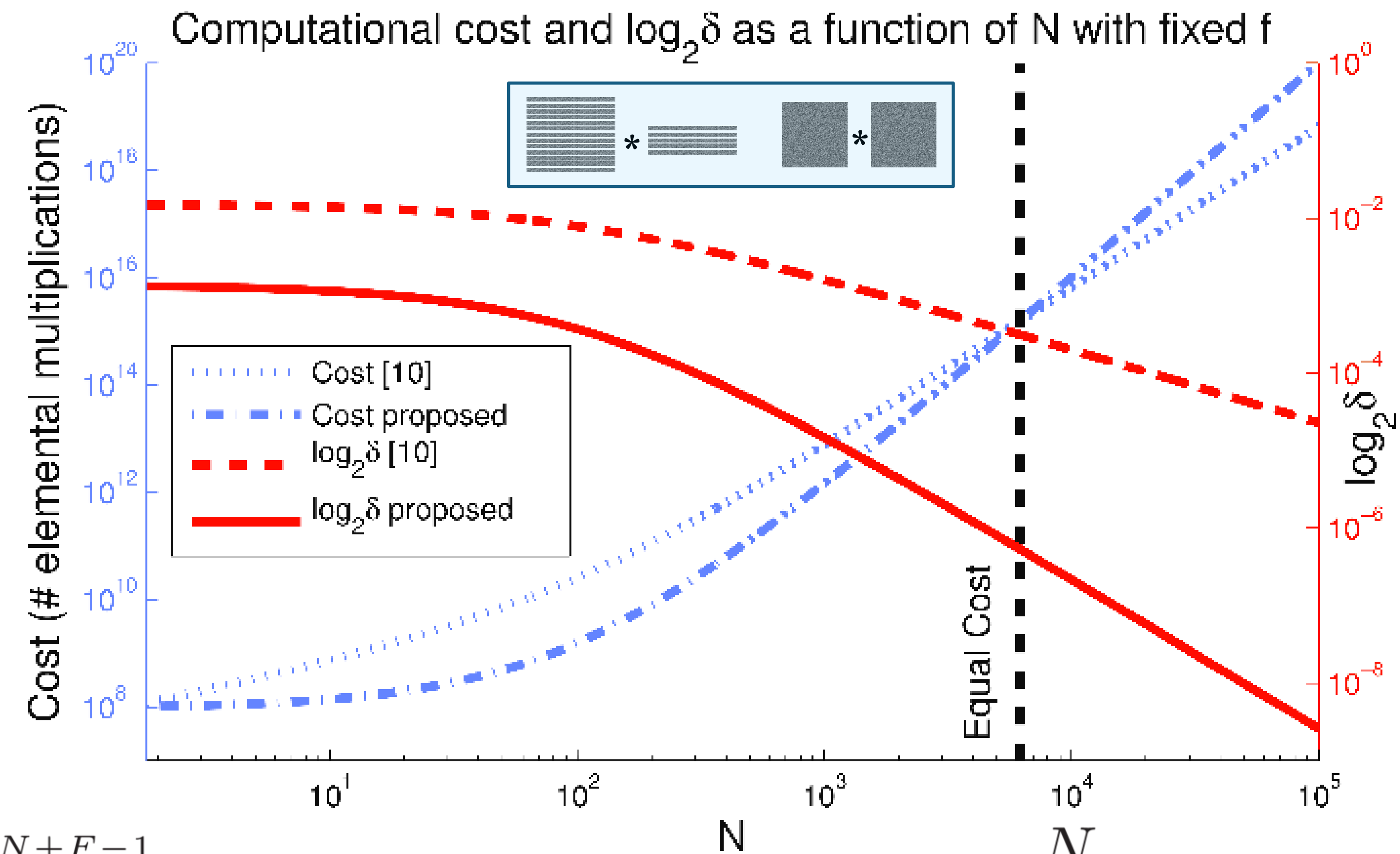




Encrypted filtering performance ($D = 1$, $t = 256$, $s = \sqrt{2\pi}$)

N	1014
Proposed cryptosystem	
n	1048576
$\lceil \log_2(q) \rceil$	52
Enc. image size (bits)	$1.09 \cdot 10^8$
δ	1.0000085
Encrypt. time (s)	4.127
Decrypt. time (s)	4.038
Conv. time (s)	8.047
Lauter cryptosystem ($h = 8$)	
n	8192
$\lceil \log_2(q) \rceil$	42
Enc. image size (bits)	$6.98 \cdot 10^8$
δ	1.00087
Encrypt. time (s)	7.122
Decrypt. time (s)	6.200
Conv. time (s)	134.719
Paillier cryptosystem (with 2048 bit modulus)	
Enc. image size ($bits$)	$4.21 \cdot 10^9$
Encrypt. time (s)	12852
Decrypt. time (s)	13107
Conv. time (s)	8205

Encrypted image filtering with 2-RLWE



$$\delta_{2-RLWE}^{\frac{N+F-1}{h}} \approx \delta_{Lauter}, \quad \mathrm{cost}_{2-RLWE} \approx \frac{N}{h^2 F}\mathrm{cost}_{Lauter}.$$

Conclusions

Challenges for SSP in Privacy-preserving Face Verification

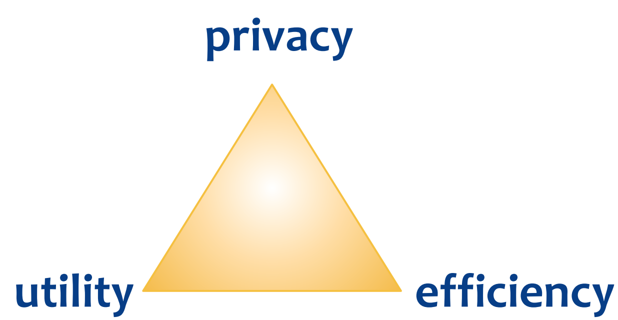
Challenges in SSP for Privacy-preserving Face Verification

- Signal representation (crypto-amenable)
  - Only integers or fixed point
  - Input quantization
  - Packing/pre-processing
- Versatility/Malleability (secure verification logic)
  - Simplifications: choice of distance and matching functions
    - Hamming, Euclidean, set-difference,…
  - Secure feature extraction
- Performance
  - Verification accuracy

AtlantTIC
Universidade Vigo

Challenges in SSP for Privacy-preserving Face Verification

- Efficiency
  - Use of SHE
  - Combination with interactive protocols
  - Lower cipher expansion and communication rounds
  - Lower computation overhead
- Security
  - Information-theoretic vs cryptographic
  - Malicious adversaries



References

- [JNN08] Anil K Jain, Karthik Nandakumar and Abhishek Nagar, Biometric Template Security, EURASIP Journal on Advances in Signal Processing 2008, 2008:579416
- [RU11] Christian Rathgeb , Andreas Uhl, A survey on biometric cryptosystems and cancelable biometrics, EURASIP Journal on Information Security, December 2011, 2011:3
- [LHPS15] Cai Li; Jiankun Hu; Pieprzyk, J.; Susilo, W., "A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion," in Information Forensics and Security, IEEE Transactions on , vol.10, no.6, pp.1193-1206, June 2015
- [DL15] Droandi, G.; Lazzeretti, R., "SHE based non interactive privacy preserving biometric authentication protocols," in Intelligent Signal Processing (WISP), 2015 IEEE 9th International Symposium on , vol., no., pp.1-6, 15-17 May 2015
- [IW14] Ignatenko, T.; Willems, F.M.J., "Privacy-leakage codes for biometric authentication systems," in Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on , vol., no., pp.1601-1605, 4-9 May 2014
- [BCP13] Bringer, J.; Chabanne, H.; Patey, A., "Privacy-Preserving Biometric Identification Using Secure Multiparty Computation: An Overview and Recent Trends," in Signal Processing Magazine, IEEE , vol.30, no.2, pp.42-52, March 2013
- [BDL15] Barni, M.; Droandi, G.; Lazzeretti, R., "Privacy Protection in Biometric-Based Recognition Systems: A marriage between cryptography and signal processing," in Signal Processing Magazine, IEEE , vol.32, no.5, pp.66-76, Sept. 2015
- [IW15] Ignatenko, T.; Willems, F.M.J., "Fundamental Limits for Privacy-Preserving Biometric Identification Systems That Support Authentication," in Information Theory, IEEE Transactions on , vol.61, no.10, pp.5583-5594, Oct. 2015

References

- [RWDI13] Rane, S.; Ye Wang; Draper, S.C.; Ishwar, P., "Secure Biometrics: Concepts, Authentication Architectures, and Challenges," in Signal Processing Magazine, IEEE , vol.30, no.5, pp.51-64, Sept. 2013
- [PRC15] Patel, V.M.; Ratha, N.K.; Chellappa, R., "Cancelable Biometrics: A review," in Signal Processing Magazine, IEEE , vol.32, no.5, pp.54-65, Sept. 2015
- [OPJM10] Osadchy, M.; Pinkas, B.; Jarrous, A.; Moskovich, B., "SCiFI - A System for Secure Face Identification," in Security and Privacy (SP), 2010 IEEE Symposium on , vol., no., pp.239-254, 16-19 May 2010
- [YSKYK13] Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama, Takeshi Koshiba, "Packed Homomorphic Encryption Based on Ideal Lattices and Its Application to Biometrics," Security Engineering and Intelligence Informatics, Volume 8128 of the series Lecture Notes in Computer Science pp 55-74, 2013
- [EFGKLT09] Z. Erkin, M. Franz, J.Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, "Privacy-preserving face recognition," in *Proc. PETS'09*, 2009, ser. Lecture Notes in Computer Science, no. 5672, pp. 235–253.
- [SSW10] A.-R. Sadeghi, T. Schneider, and I. Wehrenberg, "Efficient privacypreserving face recognition," in *Proc. ICISC 2009*, 2010, vol. 5984, ser. Lecture Notes in Computer Science, pp. 229–244, Springer.
- [GH11] C. Gentry and S. Halevi, "Implementing Gentry's fully-homomorphic encryption scheme," in *Proc. EUROCRYPT 2011*, 2011, vol. 6632, ser. Lecture Notes in Computer Science, pp. 129–148
- [BGV14] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) Fully Homomorphic Encryption without Bootstrapping," ACM Trans. Comput. Theory, vol. 6, no. 3, pp. 13:1–13:36, Jul. 2014.
- [LNV11] K. Lauter, M. Naehrig, and V. Vaikuntanathan, "Can Homomorphic Encryption be Practical?" Cryptology ePrint Archive, Report 2011/405, 2011, http://eprint.iacr.org/.

Further info

SSP Recent Publications (http://gpsc.uvigo.es)

- [PTP15] A. Pedrouzo-Ulloa, J.R. Troncoso-Pastoriza, and F. Pérez-González, “Multivariate Lattices for Encrypted Image Processing”, in IEEE ICASSP 2015
- [TC14] J.R. Troncoso-Pastoriza, S. Caputo, “Bootstrap-based Proxy Reencryption for Private Multi-user Computing”, IEEE WIFS 2014
- [TGP13] J. R. Troncoso-Pastoriza, D. González-Jiménez, and F. Pérez-González, “Fully Private Noninteractive Face Verification”, IEEE TIFS, vol. 8(7), 2013
- [ETLP13] Z. Erkin, J.R. Troncoso-Pastoriza, R. Lagendijk, and F. Pérez-González, “Privacy-Preserving Data Aggregation in Smart Metering Systems: An Overview”, IEEE SPM, vol. 30(2), 2013
- [TP13] J. R. Troncoso-Pastoriza and F. Pérez-González, “Secure Signal Processing in the Cloud: enabling technologies for privacy-preserving multimedia cloud processing”, IEEE SPM, vol. 30(2), 2013
- [TP11] J. R. Troncoso-Pastoriza and F. Pérez-González, “Secure Adaptive Filtering”, IEEE TIFS, vol. 6(2), 2011

Related Patents

- US Patents No. 8433925, 8837715, 8843762, 8972742
- US Patent Pending, No. 12/876229
- EPO Patent Pending, No. EP10175467

AtlantTIC
UniversidadeVigo

Secure Signal Processing for Outsourced Face Verification

Biométrie, Indexation multimédia et Vie privée
6th October 2015
Paris (Telecom ParisTech)

AtlantTIC

Dr. Juan R. Troncoso Pastoriza
troncoso@gts.uvigo.es
http://gpsc.uvigo.es/juan-ramon-troncoso-pastoriza