Homomorphic Lattice Cryptosystems for Secure Signal Processing

Alberto Pedrouzo-Ulloa

Advisors: Juan Ramón Troncoso-Pastoriza and Fernando Pérez-González

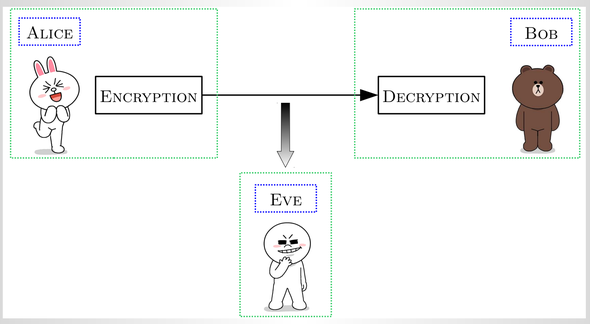
{apedrouzo,troncoso,fperez}@gts.uvigo.es

Universidad de Vigo
Signal Theory and Communications Department
University of Vigo
Spain

Workshop on Monitoring PhD Student Progress. June 13, 2016

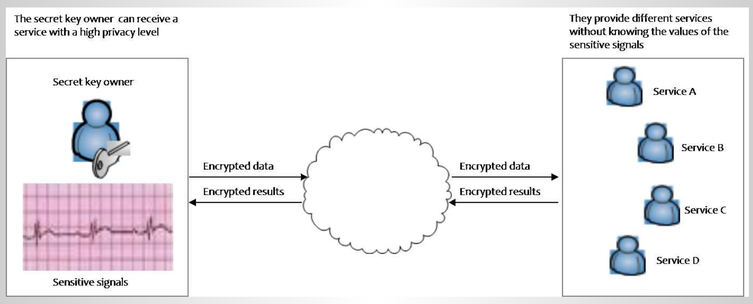
1. Motivation of the Work

Traditionally, cryptographic techniques have been used for preserving the privacy of the communications among several parties in the presence of adversaries.



If the scenarios dealing with sensitive signals involve outsourcing the data, the privacy problems increase, as currently the privacy guarantees for the data owner are mainly based on her confidence on the outsourced environment.

This is the context where the **SPED (Signal Processing in the Encrypted Domain)** is born.



SPED is typically presented as the result of the joint efforts of the cryptographic community and signal processing community, being its main goal to be able to operate with encrypted data.

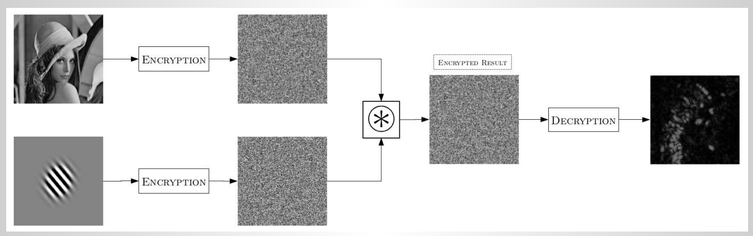
In this way, we can reduce the needed confidence between the owner of the private data and the party operating on it. However, **it is a very recent research topic with a lot of open problems!**

2. Thesis Objectives

The main objective during the development of this PhD Thesis is to **advance the State of the Art for privacy protection when dealing with sensitive signals in untrustworthy environments**.

Specifically, the three main objectives are the following:

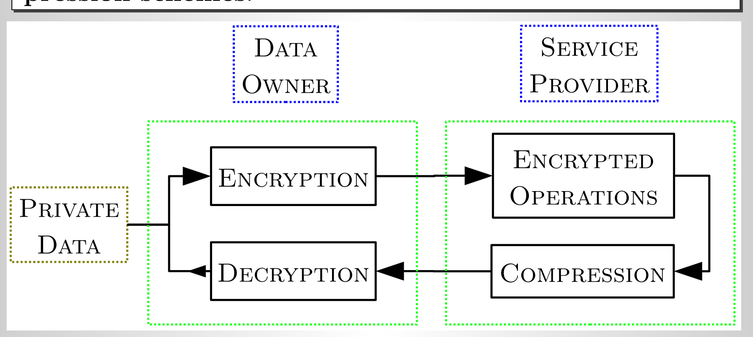
Privacy Protection when dealing with multidimensional signals.



Design of new primitives and protocols for encrypted signal processing.

Some applications	
Biometric recognition	Recommender systems
Videosurveillance	Collaborative filtering
e-Health	Smart Grids
Social media sharing	Cloud Computing

Security analysis and development of encrypted compression schemes.

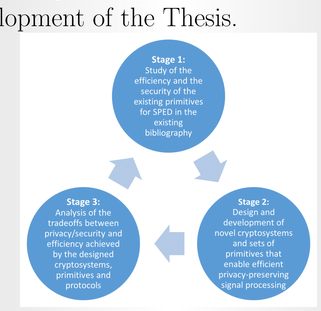


3. Research Plan

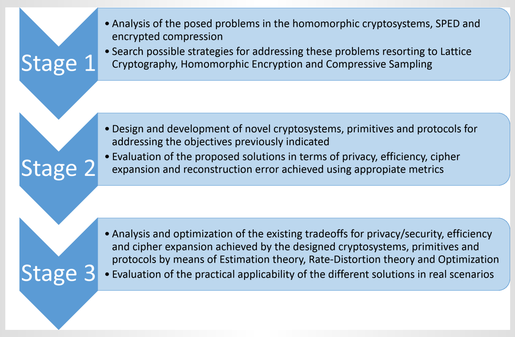
For reaching the aforementioned objectives, **this Thesis will be devoted to the research of both the theoretical and practical aspects of signal processing in the encrypted domain**.

The research activities will comprise methodologies and procedures taken from Lattice Cryptography, Homomorphic Encryption, Estimation theory, Optimization, Compressive Sampling and Rate-Distortion theory.

Therefore, the interdisciplinary grounds of this field will drive the main phases in the development of the Thesis.



The envisioned methodology for addressing the identified research problems in **this Thesis follows the next iterative steps**.

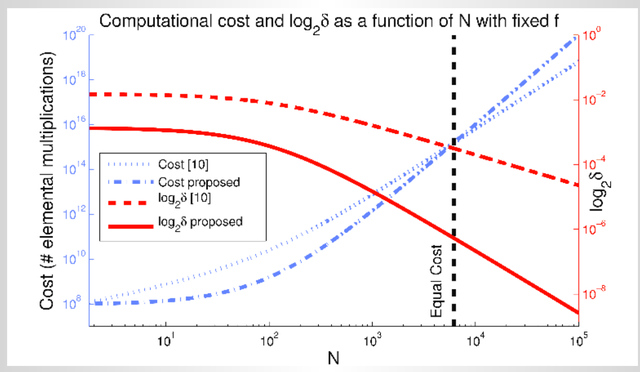


4. Results and Discussions

i. First Results

Regarding the first objective, **we have proposed a cryptosystem** which bases its security on a new hardness problem called m-RLWE (multivariate Ring Learning with Errors) [1, 2]. **It enables very efficient encrypted operations on multidimensional signals** with both a high security and a low cipher expansion.

Comparison of the cost and security for encrypted image filtering ($F = 100$, $h = 8$).



Comparison of the runtimes of the different cryptosystems for encrypted image filtering.

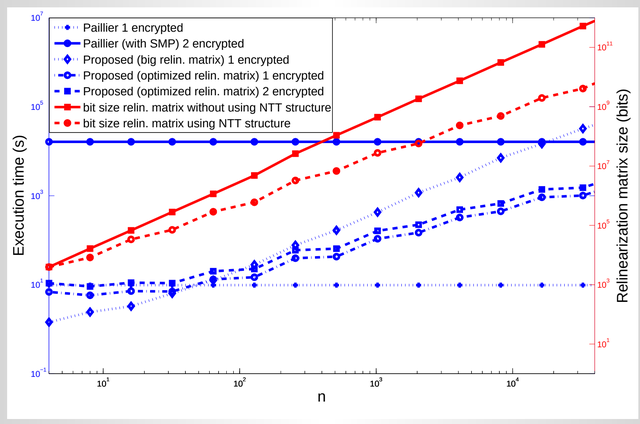
$N = 1024$	Paillier	Lauter	Proposed
Enc. image size (bits)	$4.21{\cdot}10^9$	$6.98{\cdot}10^8$	$1.09{\cdot}10^8$
δ		1.00087	1.0000085
Encrypt. time (s)	12852	7.122	4.127
Decrypt. time (s)	13107	6.200	4.038
Conv. time (s)	8205	134.719	8.047

Our proposed cryptosystem improves on cipher expansion, security and efficiency w.r.t the previous schemes

ii. New Results

In order to cover the second objective, **we have developed a novel and comprehensive set of primitives to efficiently process encrypted signals** [3]. Among this set of encrypted operations we enable filtering, generalized convolutions, matrix-based processing or error correcting codes. **The main focus is on unattended processing** where no interaction from the client is needed.

Comparison of the element-wise runtimes for different schemes ($N = 131072$).



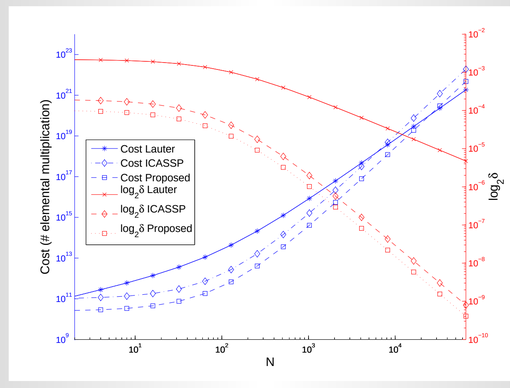
Additionally, in order to work with the previous applications, other basic encrypted primitives are compared in [3] to the previous state of the art. For example, **for the execution of an encrypted cyclic convolution or an encrypted transform like the NTT** (Number Theoretic Transform) **our proposals are several orders of magnitude more efficient than previous solutions**.

iii. In Preparation

We plan to submit three manuscripts collecting the ongoing work which cover the first and third objectives, for which we already have preliminary results.

1. A manuscript that extends the results of [1] and allows us to perform operations between sets of multidimensional signals (3-D images, video, ...) more efficiently. **The new results allow us to compute encrypted block processing algorithms on multidimensional signals in an unattended way**.

Cost and security for encrypted image filtering ($I = 16$, $F = 100$, $h_{Lauter} = 64$, $h_{ICASSP} = 8$).



2. A manuscript detailing **a new comprehensive and sound security proof for the hardness problem m-RLWE** presented in [1].
3. A manuscript summarizing the advances in encrypted compression, detailing **several algorithms to efficiently compress ciphertexts and work with compressed encryptions**, allowing an effective reduction on cipher expansion.

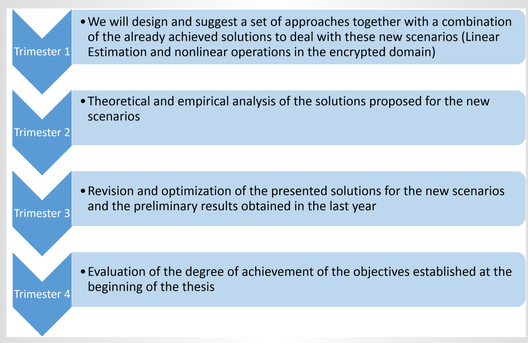
5. Next Year Planning

Regarding the specific planning for the next year, we have the following main points:

1. We want to continue the study of the topics considered on the previously mentioned manuscripts which cover the first and third objectives.
2. For the second objective, we want to study two new scenarios: a) **a primitive for encrypted linear estimation** and its possible practical application using measurements from several sensors, and b) **a novel set of fully unattended nonlinear operations in the encrypted domain** trying to avoid the use of communication protocols, that is, without the intervention of the secret key owner in the middle of the process.
3. Finally, with respect to the third objective, we will continue with the **study of the encrypted compression analyzing the bounds for encrypted compression from a point of view of Rate-Distortion theory**.

According to this plan, after finishing the manuscripts of the first point, we plan to submit them. Additionally, we envisage the preparation of two manuscripts covering the two scenarios described in the second point.

For achieving the previous objectives, we will follow the guidelines indicated in the methodology section of the Research Plan document.



6. References

[1] A. Pedrouzo-Ulloa, J.R. Troncoso-Pastoriza, and F. Pérez-González, "Multivariate Lattices for Encrypted Image Processing," in *ICASSP*, 2015.

[2] A. Pedrouzo-Ulloa, J.R. Troncoso-Pastoriza, and F. Pérez-González, "Multivariate Ring Learning with Errors," University of Vigo, Tech. Rep., September 2014.

[3] A. Pedrouzo-Ulloa, J.R. Troncoso-Pastoriza, and F. Pérez-González, "Number Theoretic Transforms for Secure Signal Processing," in *IEEE Trans. on Inf. Forensics and Security* (submitted).

[4] P. Paillier, "Public-key Cryptosystems Based on Composite Degree Residuosity Classes," in *EUROCRYPT'99*. 1999, pp. 223–238.

[5] K. Lauter, M. Naehrig, and V. Vaikuntanathan, "Can Homomorphic Encryption be Practical?," Cryptology ePrint Archive, Report 2011/405, 2011, http://eprint.iacr.org/.

[6] J.R. Troncoso-Pastoriza, and F. Pérez-González, "Secure Signal Processing in the Cloud," *Signal Processing Magazine, IEEE*, vol.30, no.2, pp. 29–41, March 2013.