

HOMOMORPHIC LATTICE CRYPTOSYSTEMS FOR SECURE SIGNAL PROCESSING

Alberto Pedrouzo-Ulloa

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

apedrouzo@gts.uvigo.es juan.troncoso-pastoriza@epfl.ch fperez@gts.uvigo.es

Workshop on Monitoring PhD Student Progress. June 22-23, 2017

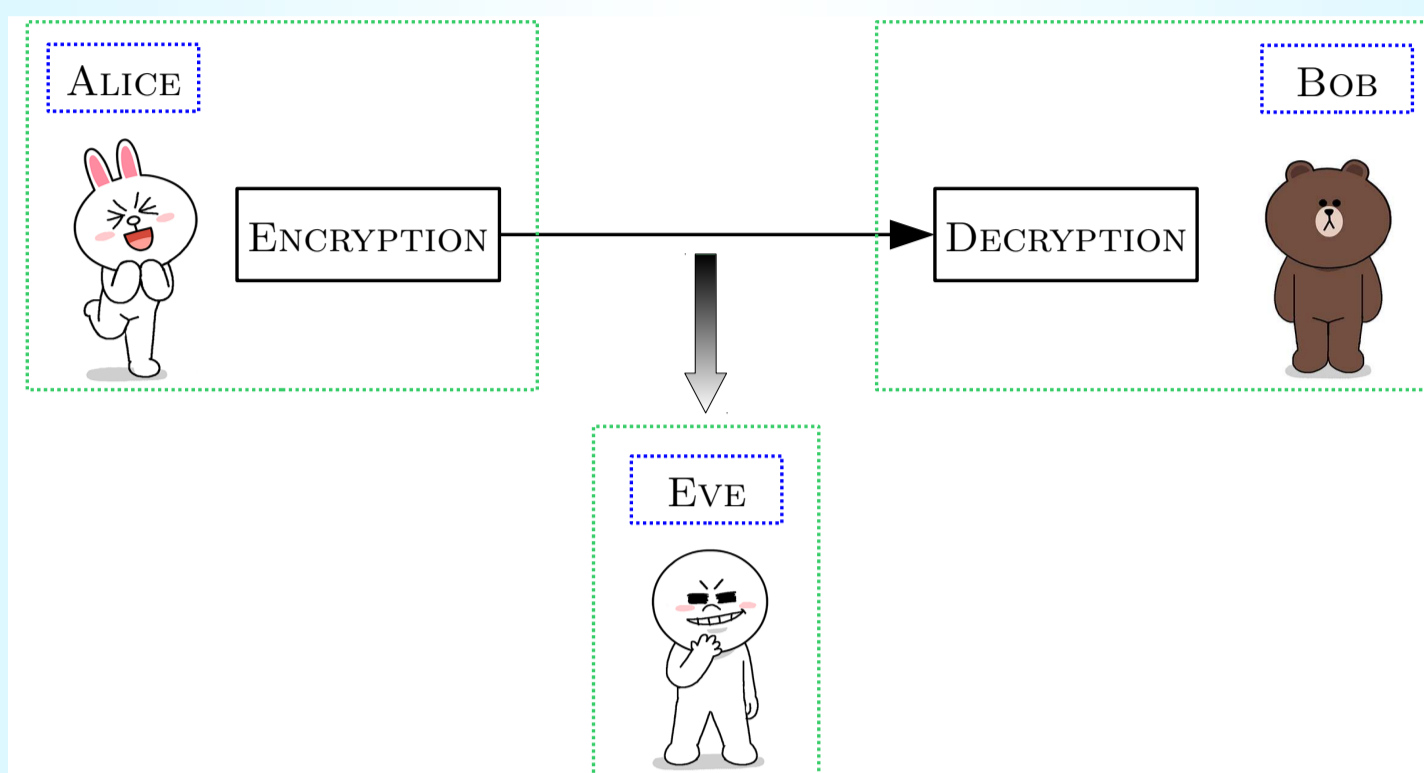
Universidade de Vigo

Signal Theory and Communications Department
University of Vigo
Spain



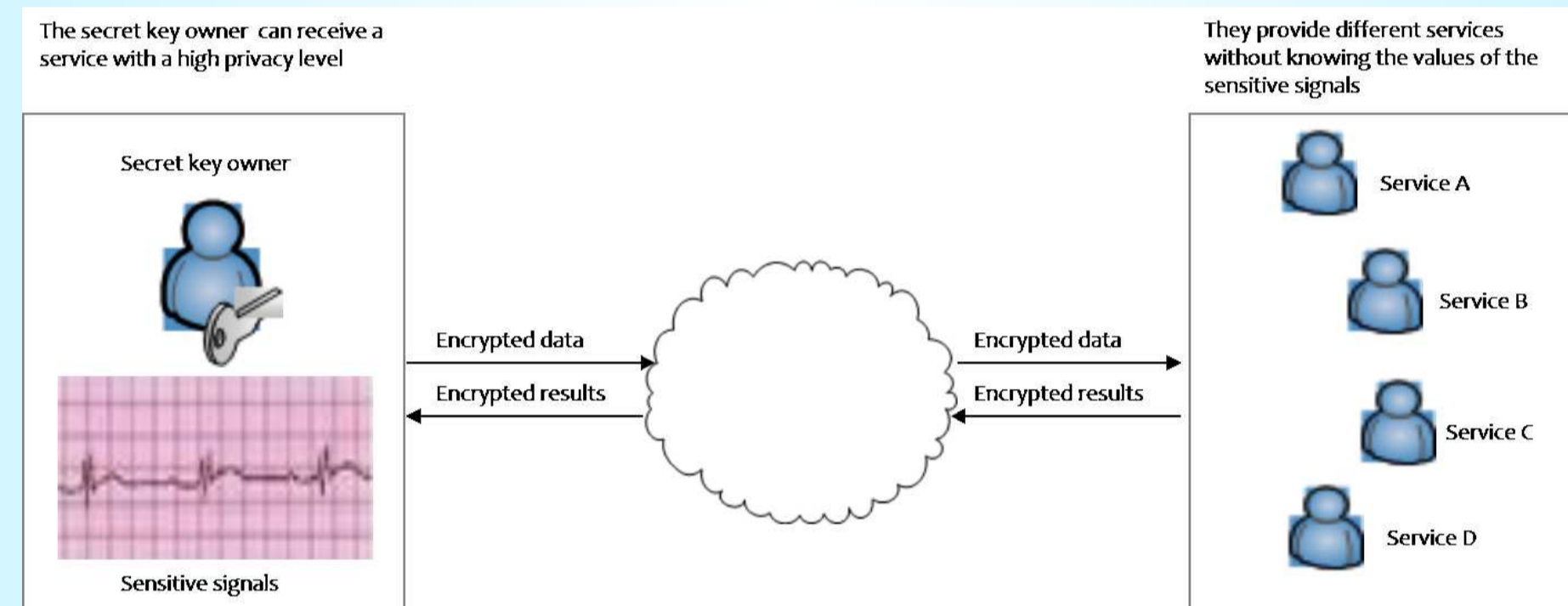
1. MOTIVATION OF THE WORK

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 trust in the outsourced environment.

This is the context where the SSP (Secure Signal Processing) is born.



SSP 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.

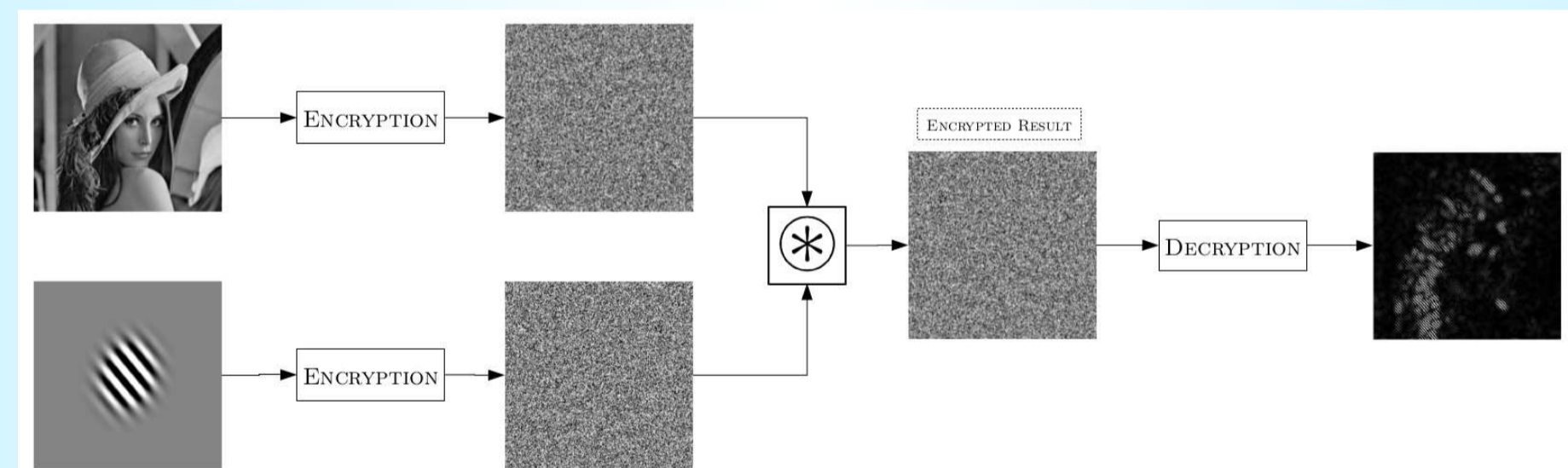
In this way, we can reduce the needed trust between the owner of the private data and the party operating on it. However, it is a very recent research topic with a lot of open problems!

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:

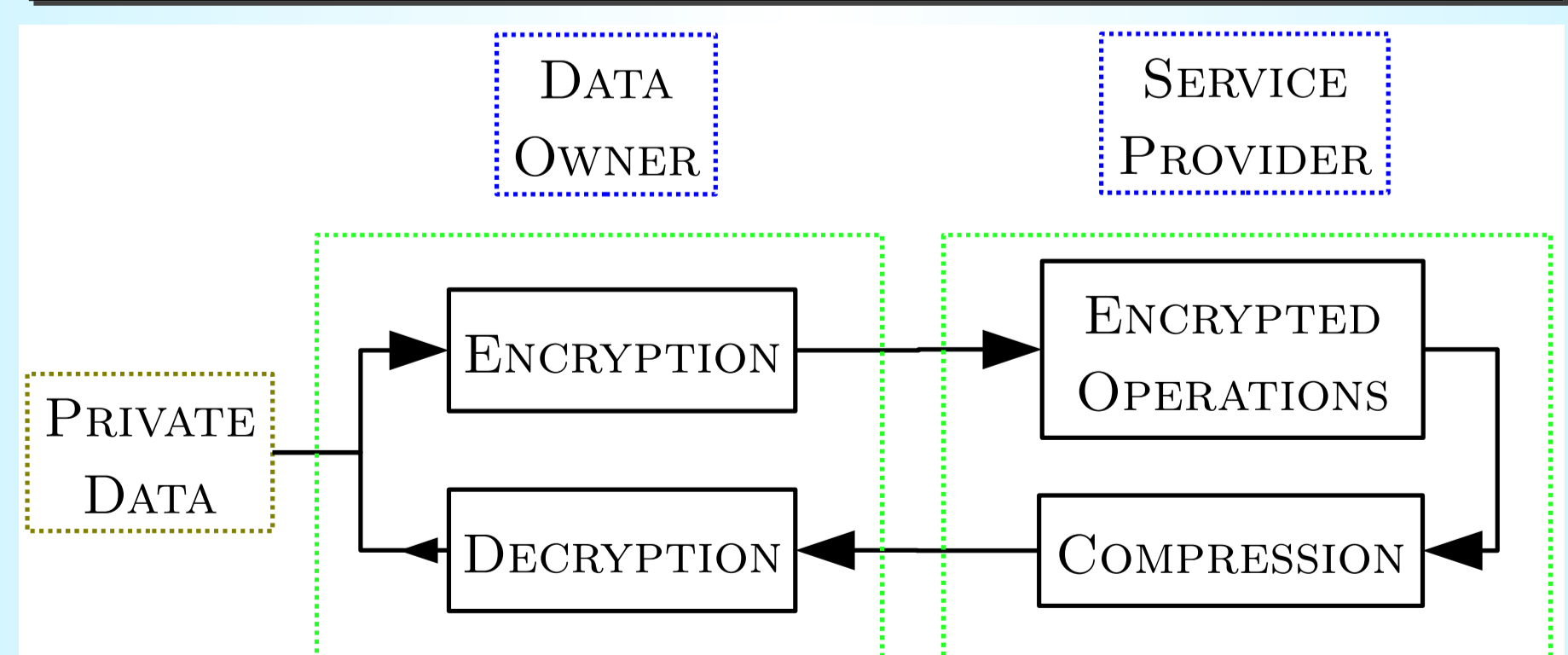
Privacy Protection when dealing with multidimensional signals.



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.

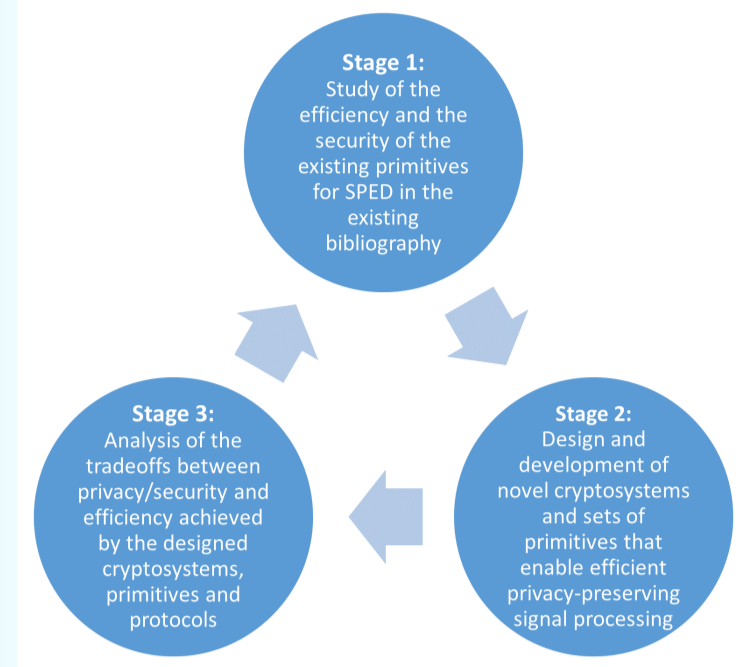


3. RESEARCH PLAN

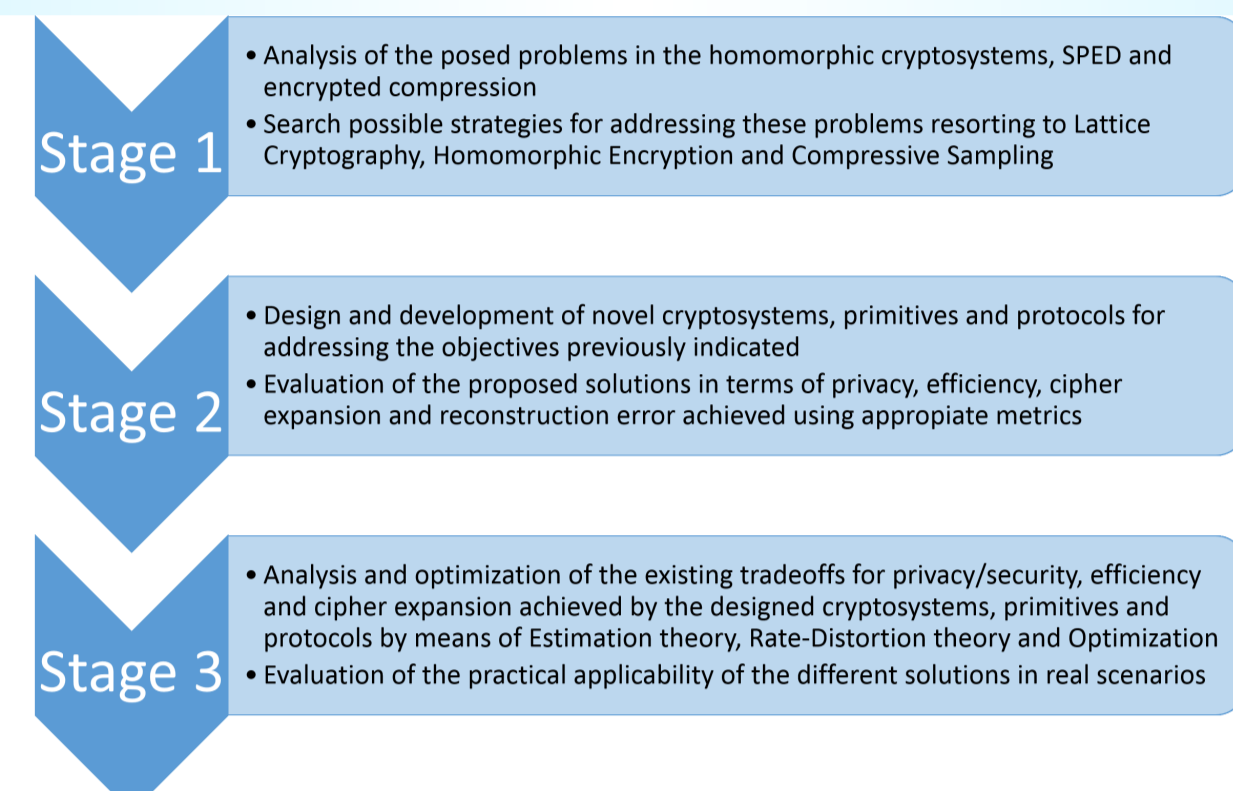
For reaching the aforementioned objectives, this Thesis is devoted to the research of both the theoretical and practical aspects of signal processing in the encrypted domain.

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.

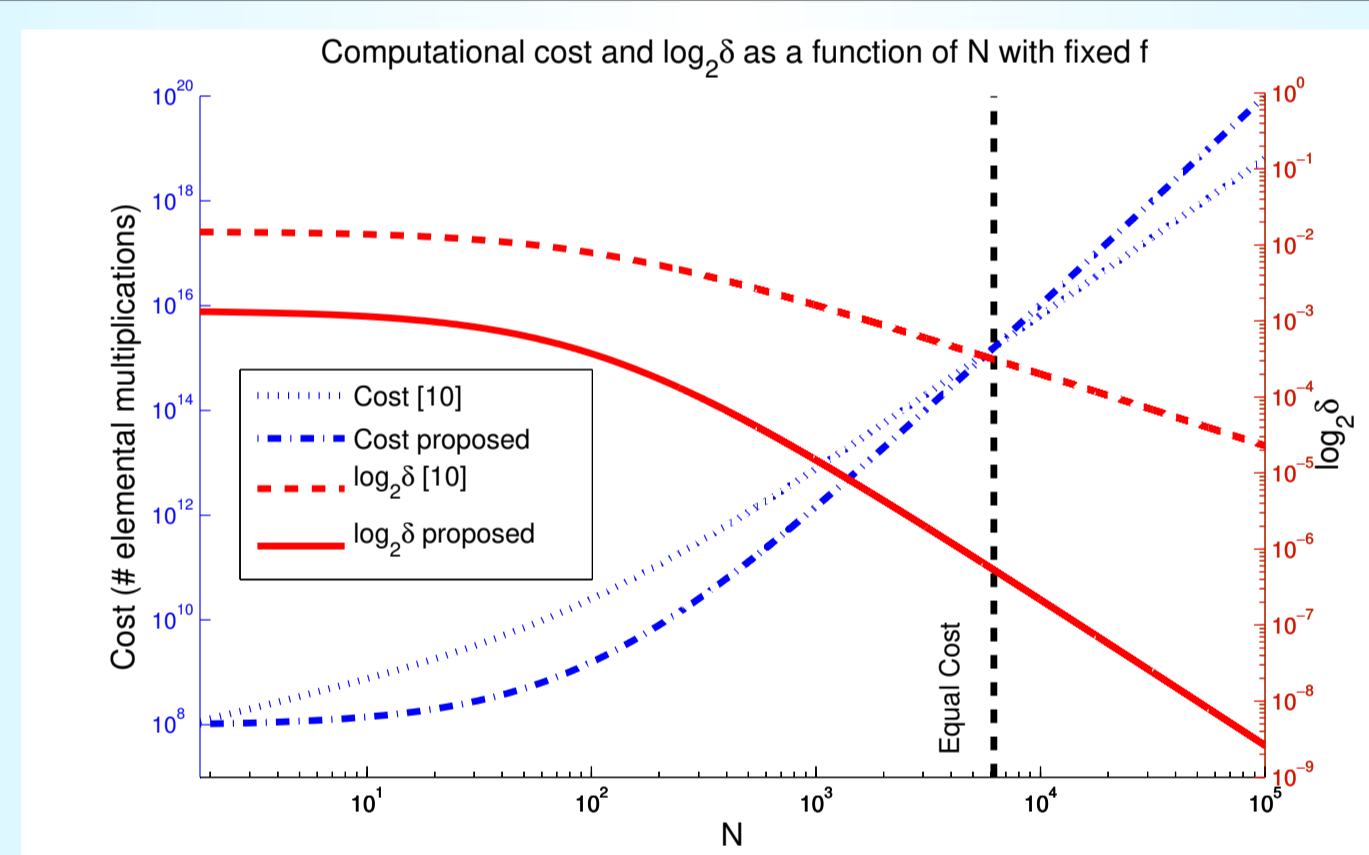


4. RESULTS AND DISCUSSIONS

i. PUBLISHED RESULTS

1. 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 ($F = 100, h = 8$).



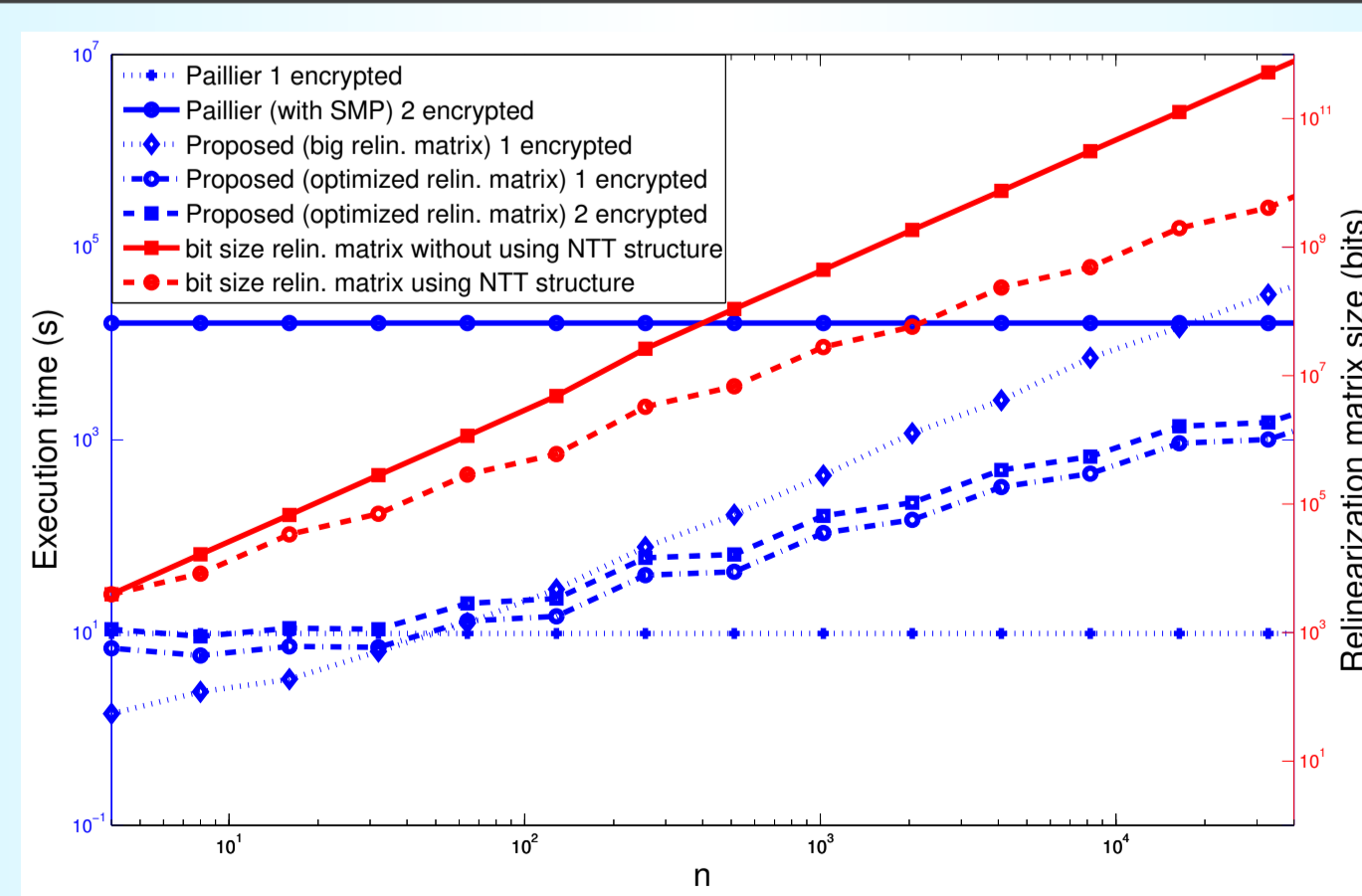
Comparison of the runtimes of the different cryptosystems for encrypted image filtering.

	$N = 1024$	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

2. 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.

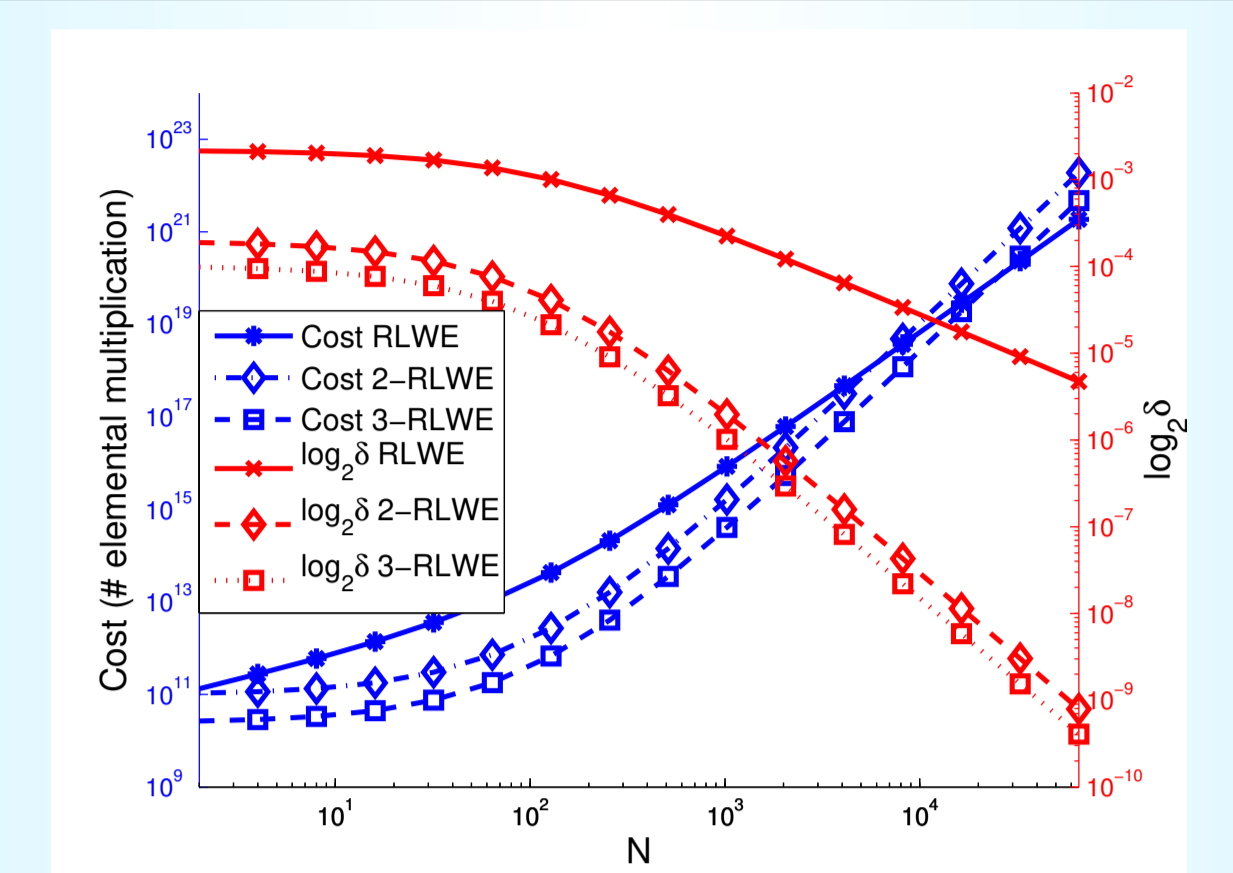
Comparison of the element-wise runtimes for different schemes ($N = 131072$).



ii. NEW RESULTS

1. A manuscript [6] detailing a new comprehensive and sound security proof for the hardness problem m -RLWE.
2. A manuscript [7] 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 ($I = 16, F = 100, h_{RLWE} = 64, h_{2-RLWE} = 8$).



3. We have proposed methods based on 2-RLWE [4] to efficiently perform unattended denoising operations on encrypted images.
4. We have proposed an encrypted genomic susceptibility test protocol [5], introducing optimizations as data packing and transformed processing.

iii. IN PREPARATION

We plan to submit one 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.

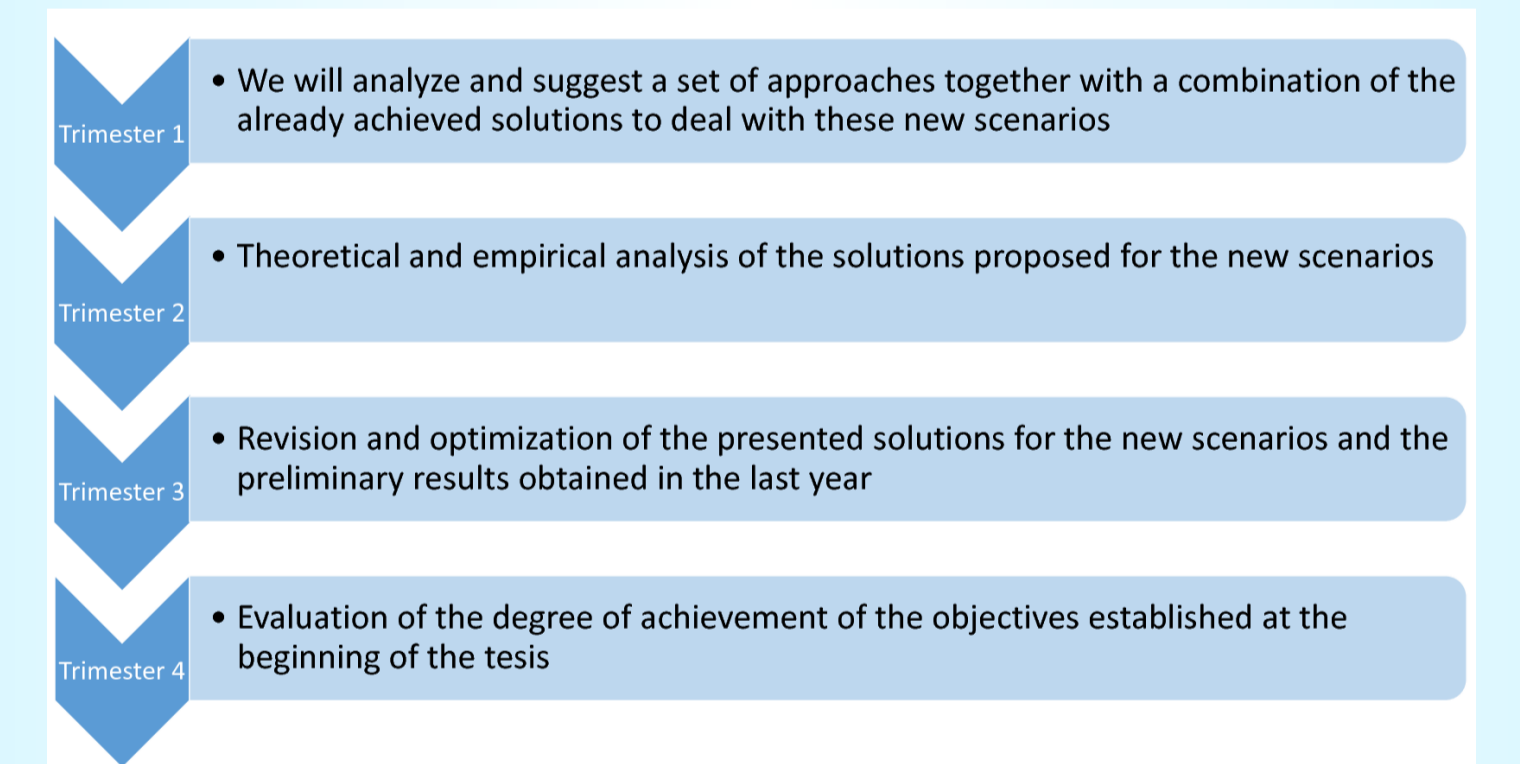
5. NEXT YEAR PLANNING

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

- For the first objective, we want to revise and submit the manuscript [6] which details the reduction of the m -RLWE problem from hard problems over lattices.
- For the second objective, we want to study the use of the developed tools to different scenarios (as the genomic and financial).
- Finally, with respect to the third objective, we will continue with the study of the encrypted compression analyzing the bounds for Rate-Distortion theory.

According to this plan, after finishing the manuscripts of the first and third point, we plan to submit them. Additionally, we envisage doing a stay during the next academic year.

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 Foundations for Secure Signal Processing," in *IEEE Trans. on Inf. Forensics and Security*, 2017.
- [4] A. Pedrouzo-Ulloa, J.R. Troncoso-Pastoriza, and F. Pérez-González, "Image Denoising in the Encrypted Domain," in *WIFS*, 2016.
- [5] J.R. Troncoso-Pastoriza, A. Pedrouzo-Ulloa, and F. Pérez-González, "Secure Genomic Susceptibility Testing based on Lattice Encryption," in *ICASSP*, 2017.
- [6] A. Pedrouzo-Ulloa, and J.R. Troncoso-Pastoriza, and F. Pérez-González, "On Ideal Lattices over the Tensor Product of Number Fields and Ring Learning with Errors over Multivariate Rings," *ArXiv e-prints*, 2016.
- [7] A. Pedrouzo-Ulloa, and J.R. Troncoso-Pastoriza, and F. Pérez-González, "Multivariate Cryptosystems for Secure Processing of Multidimensional Signals," *IEEE Trans. on Computers* (submitted).
- [8] P. Paillier, "Public-key Cryptosystems Based on Composite Degree Residuosity Classes," in *EUROCRYPT'99*, 1999.
- [9] K. Lauter, M. Naehrig, and V. Vaikuntanathan, "Can Homomorphic Encryption be Practical?," Crypt. ePrint Archive, Report 2011/405, 2011.
- [10] J.R. Troncoso-Pastoriza, and F. Pérez-González, "Secure Signal Processing in the Cloud," *IEEE Signal Processing Magazine*, 2013.