Universidade Vigo
Signal Theory and Communications Department
University of Vigo
Spain

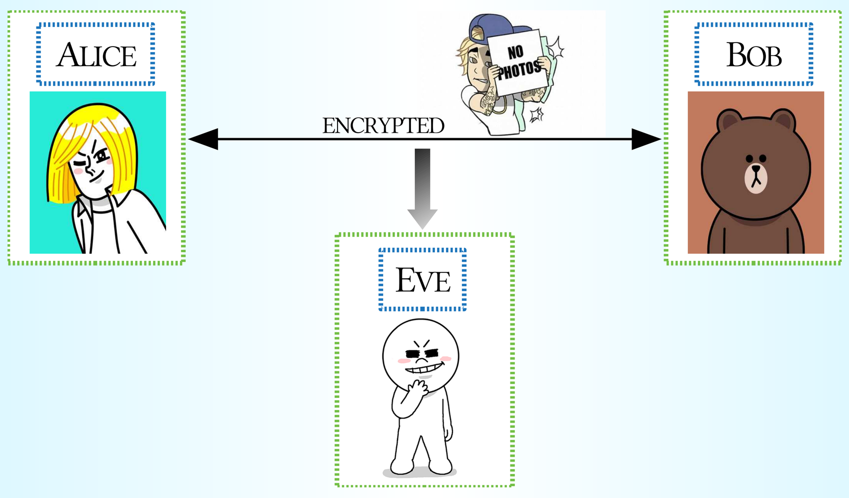
Homomorphic Lattice Cryptosystems for Secure Signal Processing

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

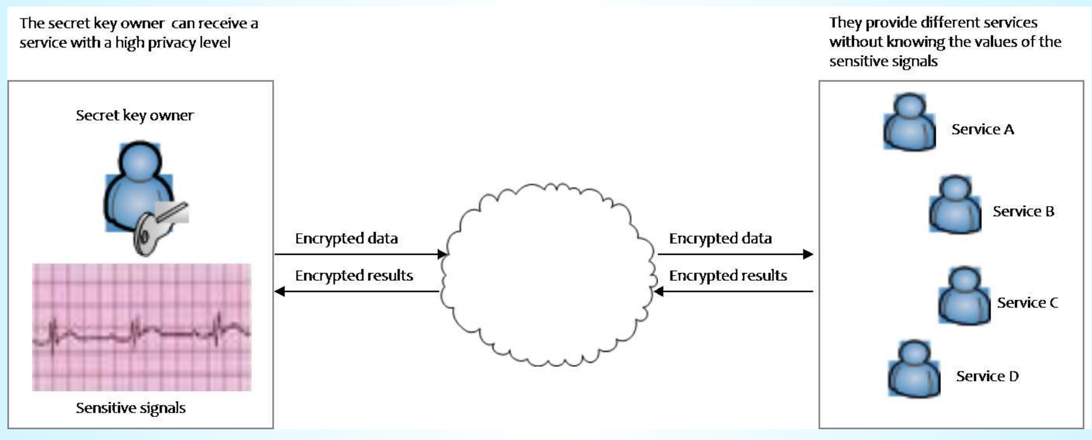
Workshop on Monitoring PhD Student Progress. June 14-15, 2018

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.

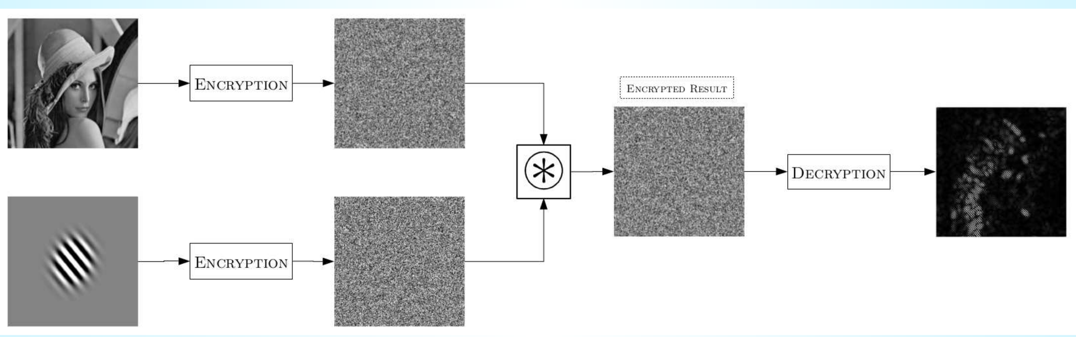


SSP is typically presented as the result of the joint efforts of the cryptographic community and signal processing community, being its main goal to be able to operate with encrypted data.
In this way, we can reduce the needed trust between the owner of the private data and the party operating on it. 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:

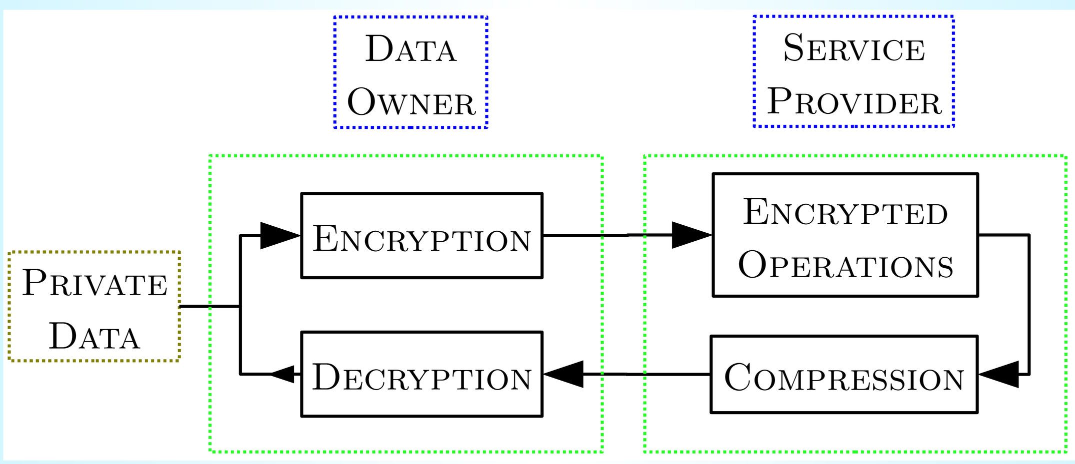
Privacy Protection when dealing with multidimensional signals.



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

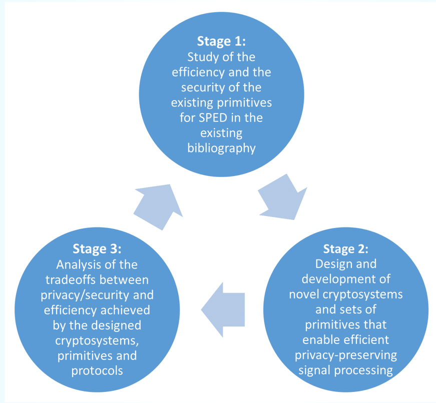
Security analysis and development of encrypted compression schemes.



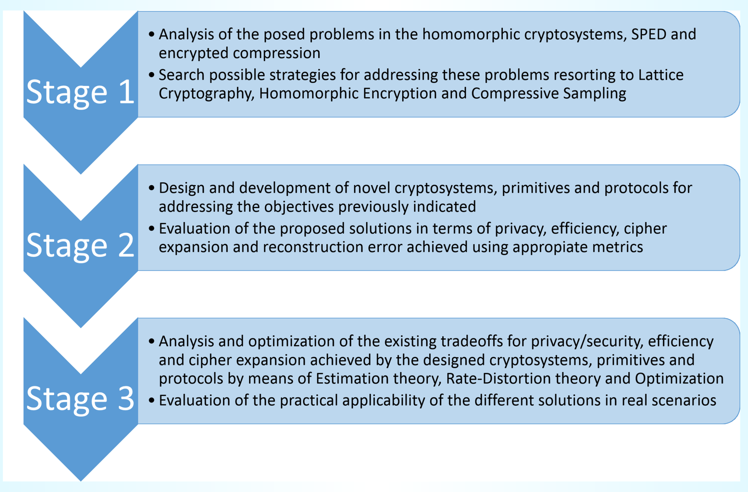
3. Research Plan

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 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 drive the main phases in the development of the Thesis.



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

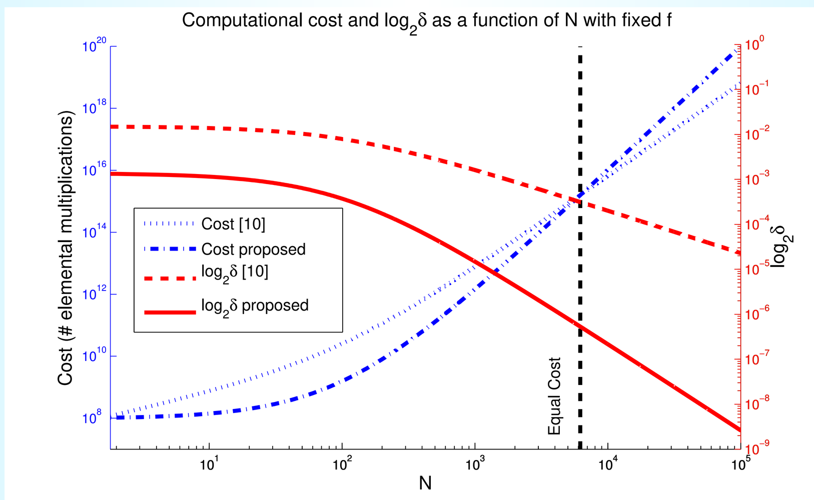


4. Results and Discussions

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



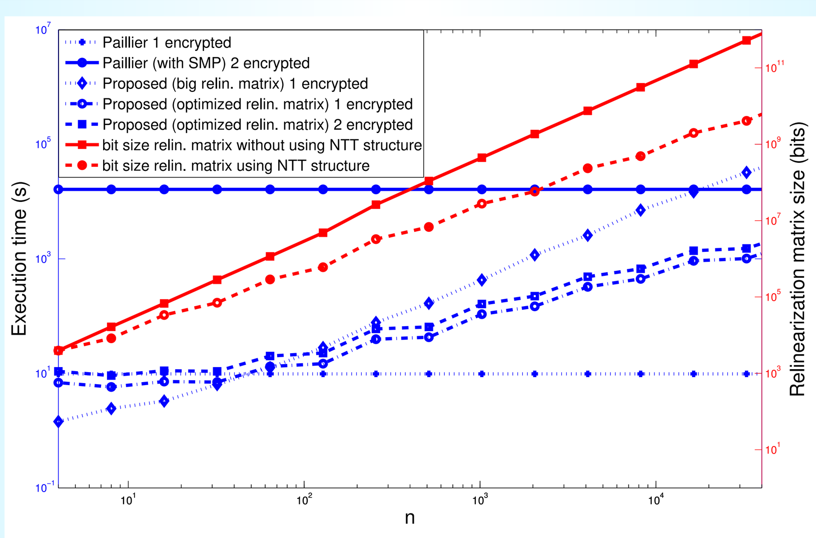
Comparison of the runtimes of the different cryptosystems for encrypted image filtering.

$N = 1024$	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 ($N = 131072$).

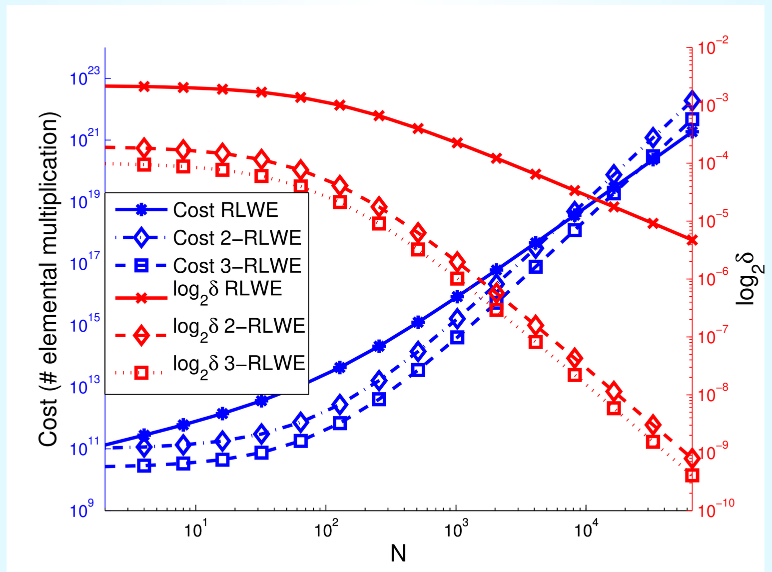


3. We have proposed methods based on 2-RLWE [4] to efficiently perform **unattended denoising operations on encrypted images**.
4. We have proposed an encrypted genomic susceptibility test protocol [5], introducing **optimizations as data packing and transformed processing**.

ii. Further 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 enables performing operations between sets of multidimensional signals (3-D images, video, ...) more efficiently. **The new results enable computing encrypted block processing algorithms on multidimensional signals in an unattended way**.

Cost and security for encrypted image filtering ($l = 16$, $F = 100$, $h_{RLWE} = 64$, $h_{2-RLWE} = 8$).



iii. h2020 project witdom

The WITDOM project has developed innovative technical solutions for secure and privacy-preserving processing of genomic and financial data in untrusted environments. We plan to submit the obtained results to the appropiate security and privacy venues.
Two patent applications (for genomic and financial applications) have been filed in the European Patent Office as a result of the work done in WITDOM.

iv. In Preparation

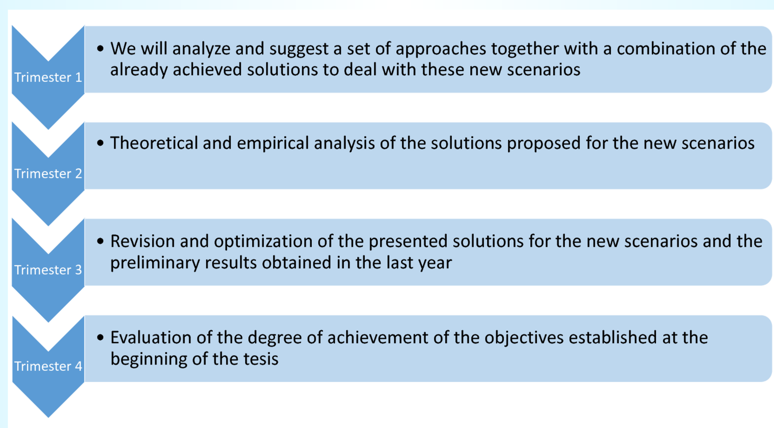
We plan to submit one manuscript summarizing the advances in encrypted compression, detailing **several algorithms to efficiently compress ciphertexts and work with compressed encryptions**, allowing an effective reduction on cipher expansion.

5. Next Year Planning

The main objective for the next year is to finish all the pending studies, together with the analysis and improvement of the results which have been already achieved.
Regarding the specific planning for the next year, we have the following main points:

1. To revise and submit all the pending works.
2. To collect and write all the results obtained during the thesis for its corresponding defense.

According to this plan, after fulfilling all the compulsory activities established by the PhD programme, the PhD defense is intended for the end/beginning of 2018/2019.
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*, 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 Ring Learning with Errors over the Tensor Product of Number Fields," *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," *ArXiv e-prints*, 2017.