Universidade Vigo
Signal Theory and
Communications
Department
University of Vigo
Spain

Homomorphic Lattice Cryptosystems for Secure Signal Processing

Alberto Pedrouzo-Ulloa

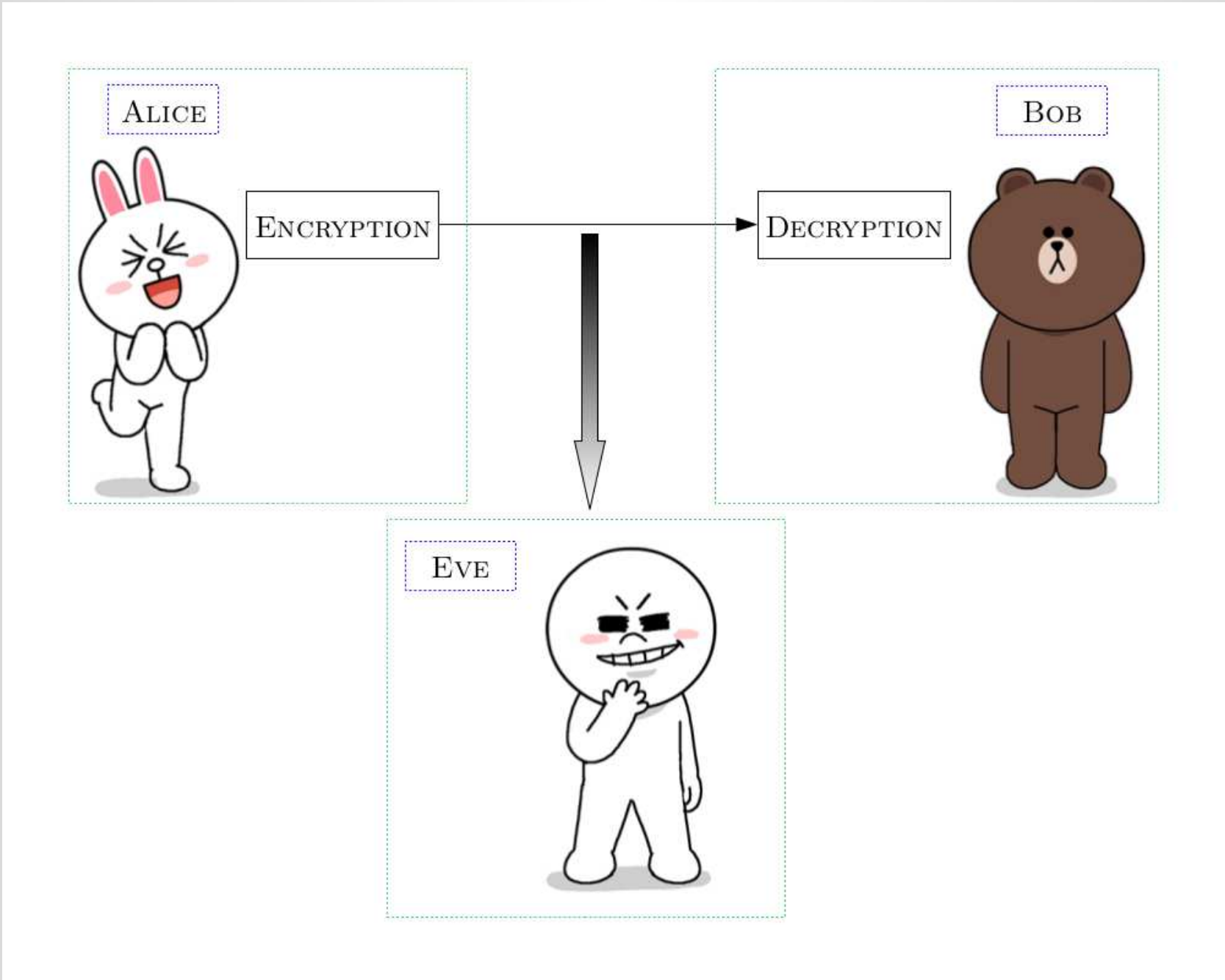
Advisors: Juan Ramón Troncoso-Pastoriza and Fernando Pérez-González

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

Workshop on Monitoring PhD Student Progress. June 16, 2015

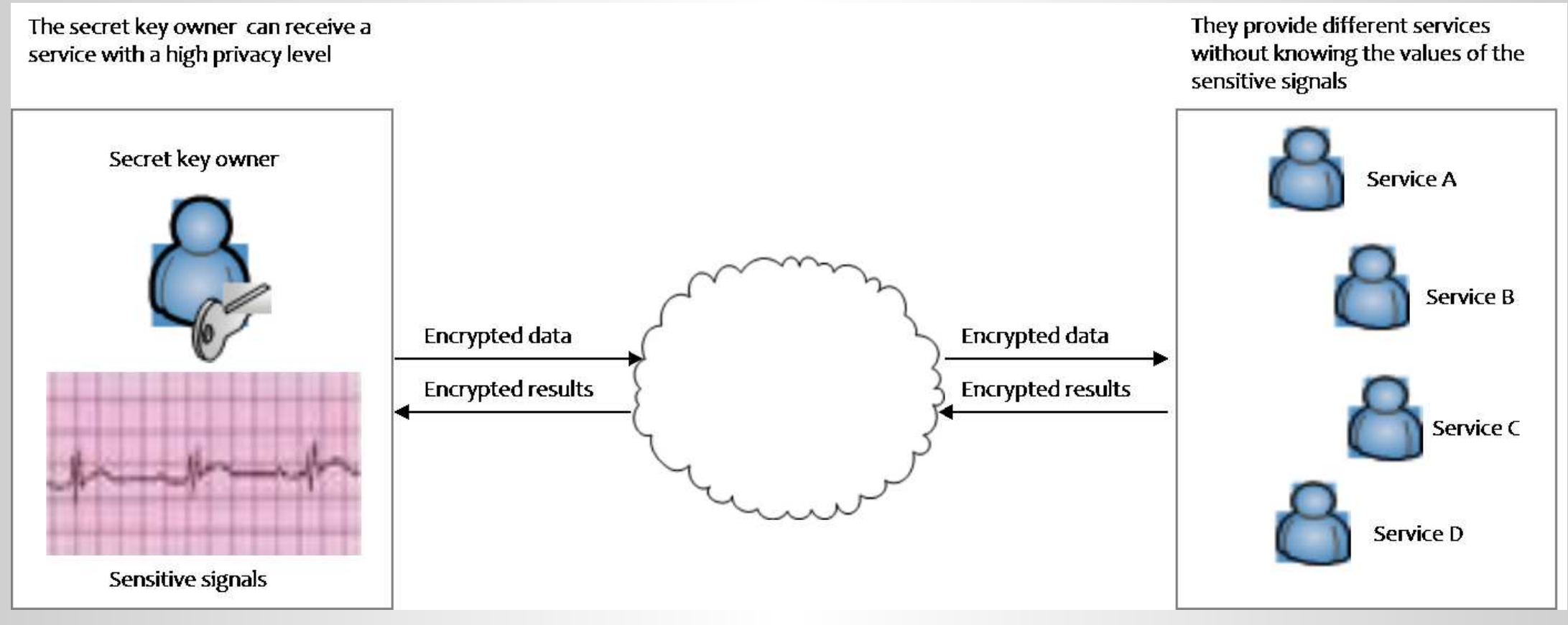
1. Motivation of the Work

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



However, there are many signal processing applications where the use of the previous methods is not enough. For example, 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.


The secret key owner can receive a service with a high privacy level
They provide different services without knowing the values of the sensitive signals
Secret key owner
Sensitive signals
Encrypted data
Encrypted results
Encrypted data
Encrypted results
Service A
Service B
Service C
Service D

SPED is typically defined as the marriage between Signal Processing and Cryptography and its main goal is to be able to operate with encrypted data.

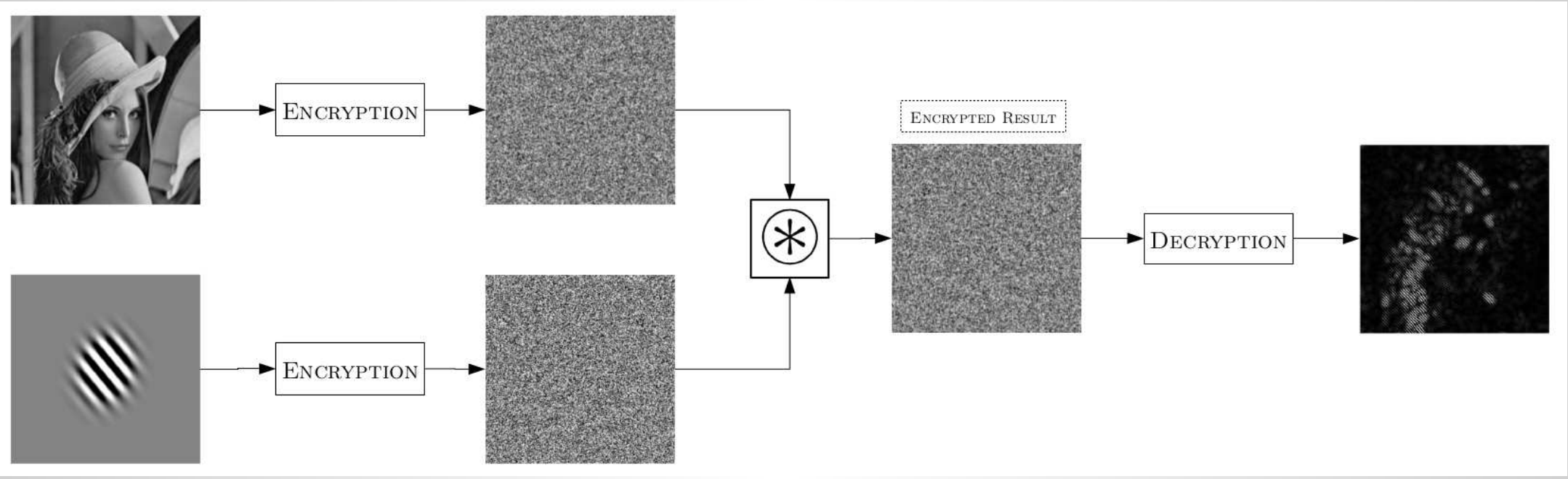
In this way, we can reduce the needed confidence between the owner of the private data and the party operating on it. However, **it is a very recent research topic with a lot of open problems!**

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:

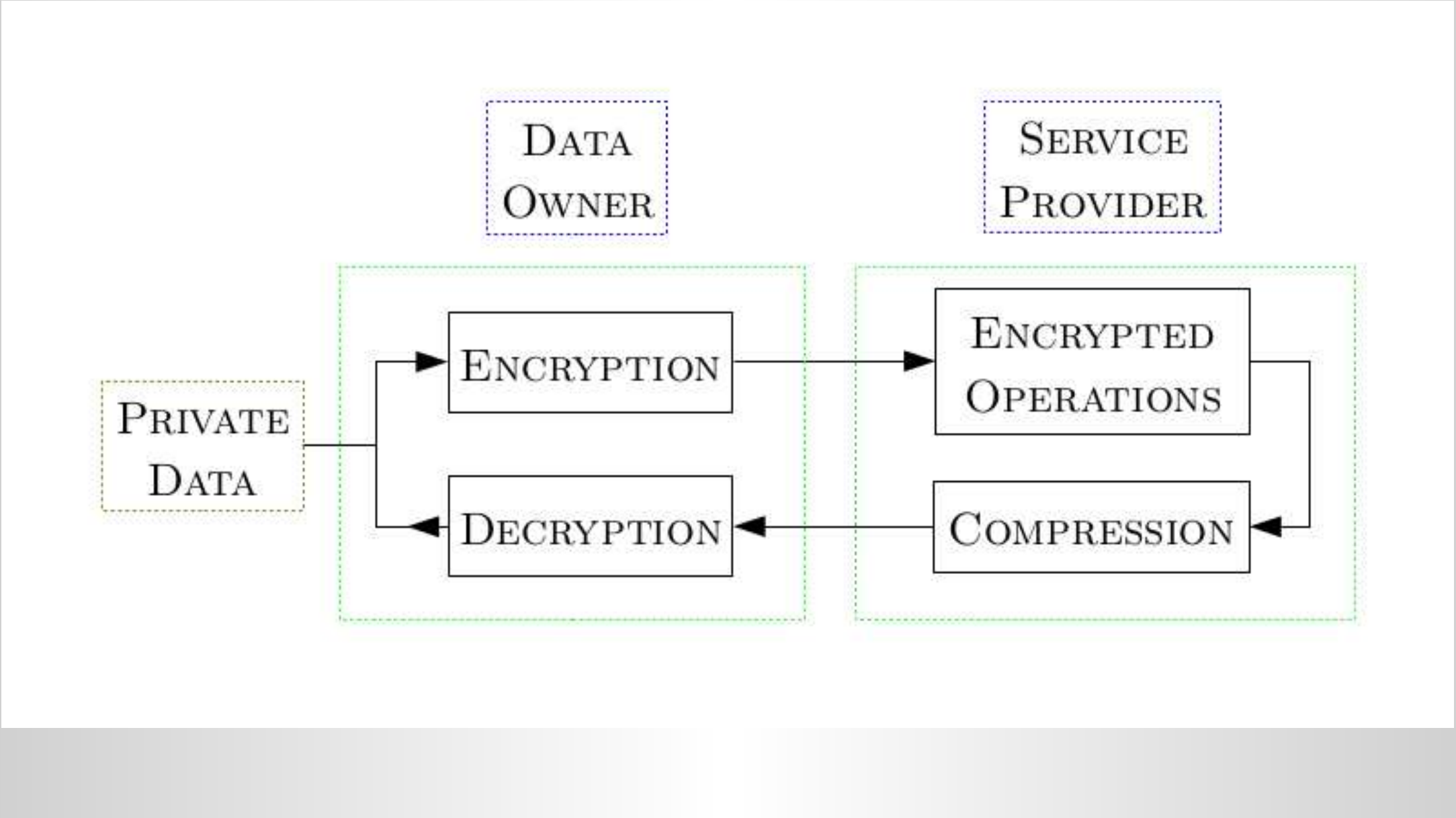
Privacy Protection when dealing with multidimensional signals.



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.

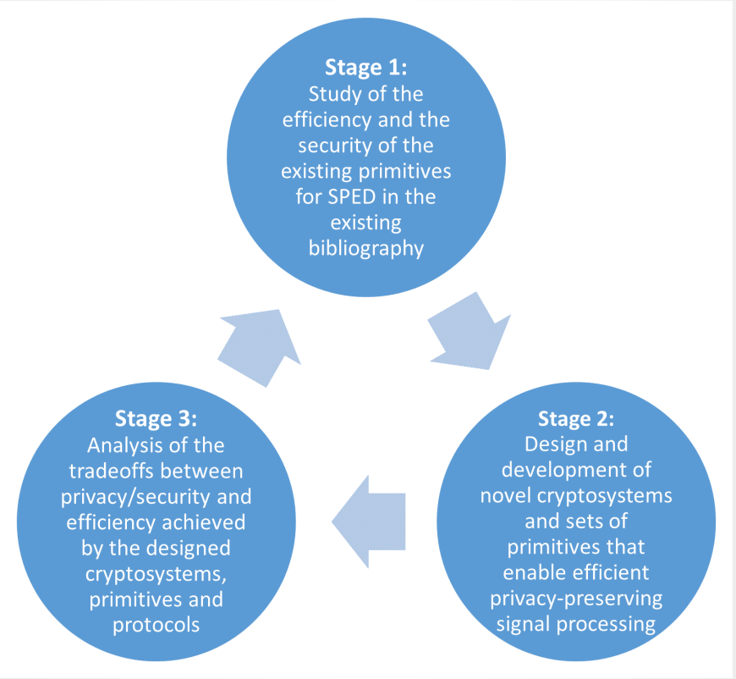


3. Research Plan

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.

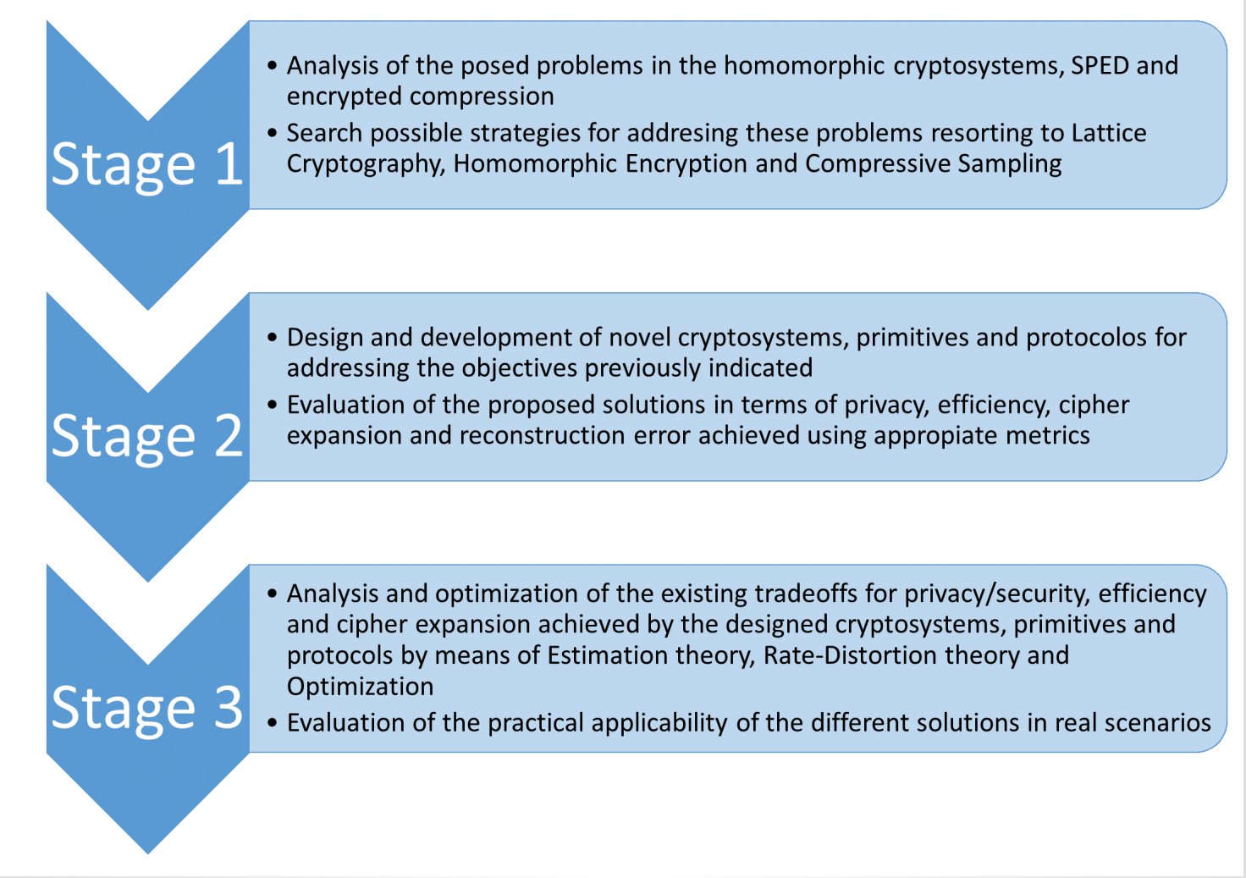


Stage 1: Study of the efficiency and the security of the existing primitives for SPED in the existing bibliography

Stage 2: Design and development of novel cryptosystems and sets of primitives that enable efficient privacy-preserving signal processing

Stage 3: Analysis of the tradeoffs between privacy/security and efficiency achieved by the designed cryptosystems, primitives and protocols

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



Stage 1
- Analysis of the posed problems in the homomorphic cryptosystems, SPED and encrypted compression
- Search possible strategies for addresing these problems resorting to Lattice Cryptography, Homomorphic Encryption and Compressive Sampling

Stage 2
- Design and development of novel cryptosystems, primitives and protocolos for addressing the objectives previously indicated
- Evaluation of the proposed solutions in terms of privacy, efficiency, cipher expansion and reconstruction error achieved using appropiate metrics

Stage 3
- Analysis and optimization of the existing tradeoffs for privacy/security, efficiency and cipher expansion achieved by the designed cryptosystems, primitives and protocols by means of Estimation theory, Rate-Distortion theory and Optimization
- Evaluation of the practical applicability of the different solutions in real scenarios

4. Results and Discussions

Regarding the first objective, **there is no prior work that exploits image structure** to design a low-expansion and efficient encrypted image processing solution.

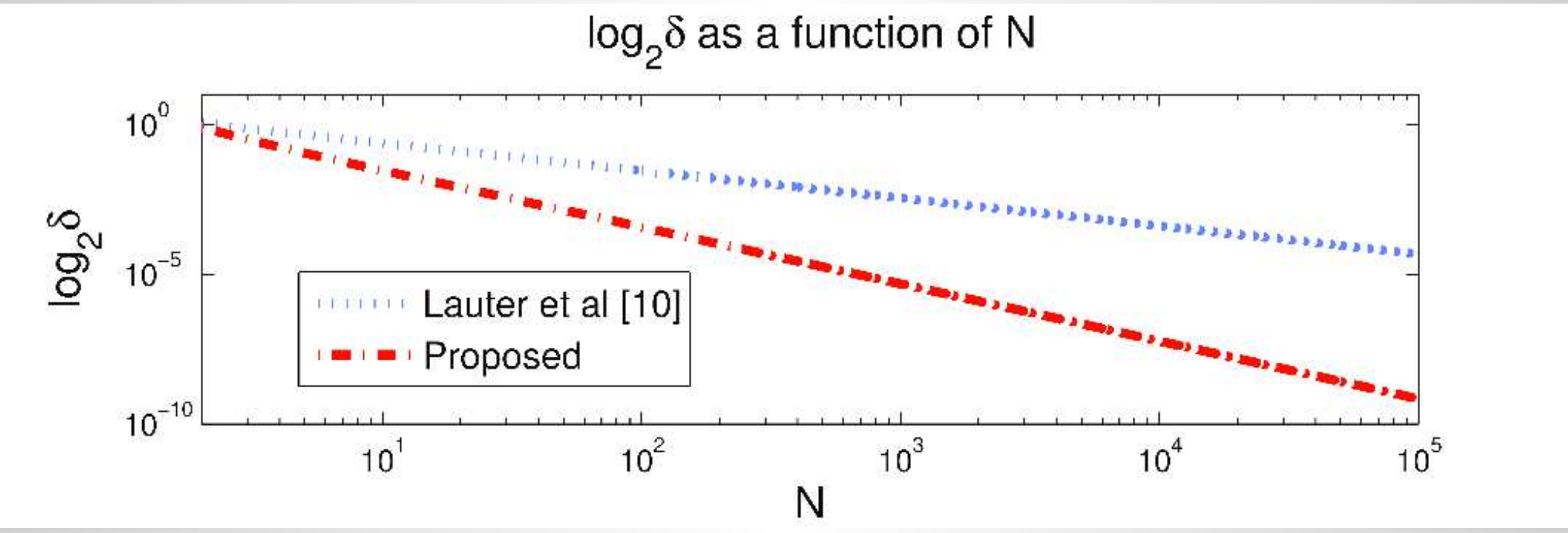
Additive homomorphic schemes like Paillier's [2], have been extensively used for implementations of typical signal processing primitives. However, **all the previous solutions that use Paillier cryptosystem [2] present a high cipher expansion** (ratio between cipher size and clear text size).

So we have proposed:

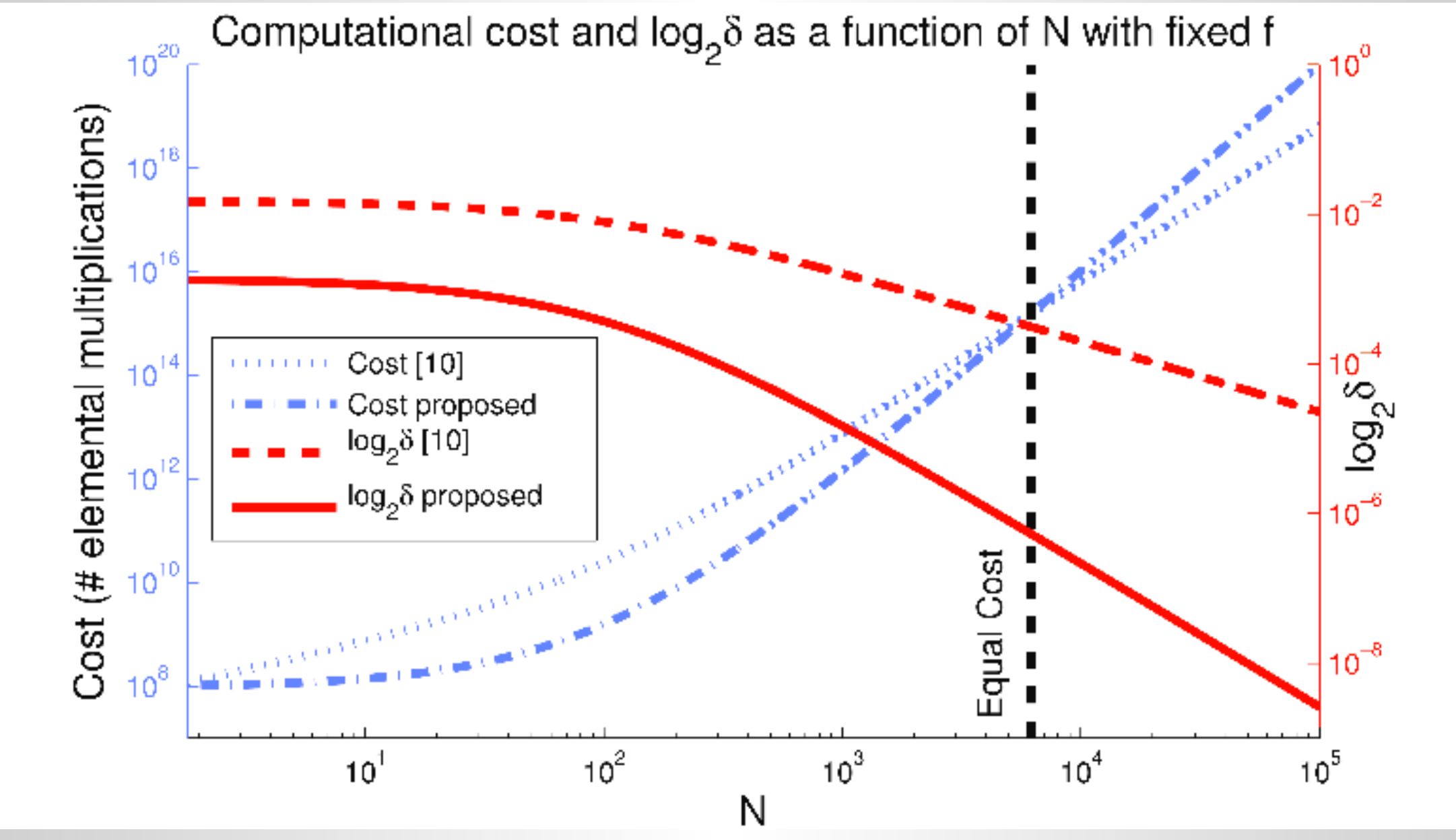
- **A new hardness problem m-RLWE that exploits the polynomial structure of lattice-based schemes** and their relation with images to **enable very efficient encrypted image operations with a high security and low cipher expansion [1]**.
- A cryptosystem that extends the RLWE based cryptosystem proposed in [5] to the m-RLWE problem. We choose Lauter's scheme due to its efficiency, but any other RLWE-based cryptosystem can be extended to the m-RLWE problem by following the introduced procedure in [1].

Below, there are several figures and a table that allow us to compare our results with the previous State of the Art when working with images.

Comparison of the security for encrypted image correlation (equal cost, $h = 2$).



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	118	246	502	1014
Proposed cryptosystem				
n	16384	65536	262144	1048576
$\lceil \log_2(q) \rceil$	43	46	49	52
Enc. image size (bits)	$1.4 \cdot 10^6$	$6.03 \cdot 10^6$	$2.57 \cdot 10^7$	$1.09 \cdot 10^8$
δ	1.00045	1.00012	1.000032	1.0000085
Encrypt. time (s)	0.031	0.144	0.673	4.127
Decrypt. time (s)	0.029	0.137	0.649	4.038
Conv. time (s)	0.058	0.275	1.299	8.047
Lauter cryptosystem ($h = 8$)				
n	1024	2048	4096	8192
$\lceil \log_2(q) \rceil$	37	39	40	42
Enc. image size (bits)	$8.94 \cdot 10^6$	$3.93 \cdot 10^7$	$1.64 \cdot 10^8$	$6.98 \cdot 10^8$
δ	1.0062	1.0037	1.0017	1.00087
Encrypt. time (s)	0.062	0.258	1.248	7.122
Decrypt. time (s)	0.038	0.214	1.053	6.200
Conv. time (s)	0.737	4.342	22.206	134.719
Paillier cryptosystem (with 2048 bit modulus)				
Enc. image size ($bits$)	$5.7 \cdot 10^7$	$2.48 \cdot 10^8$	$1.03 \cdot 10^9$	$4.21 \cdot 10^9$
Encrypt. time (s)	174	756	3150	12852
Decrypt. time (s)	205	819	3277	13107
Conv. time (s)	111	483	2011	8205

Our proposed cryptosystem improves on cipher expansion, security and efficiency the previous schemes

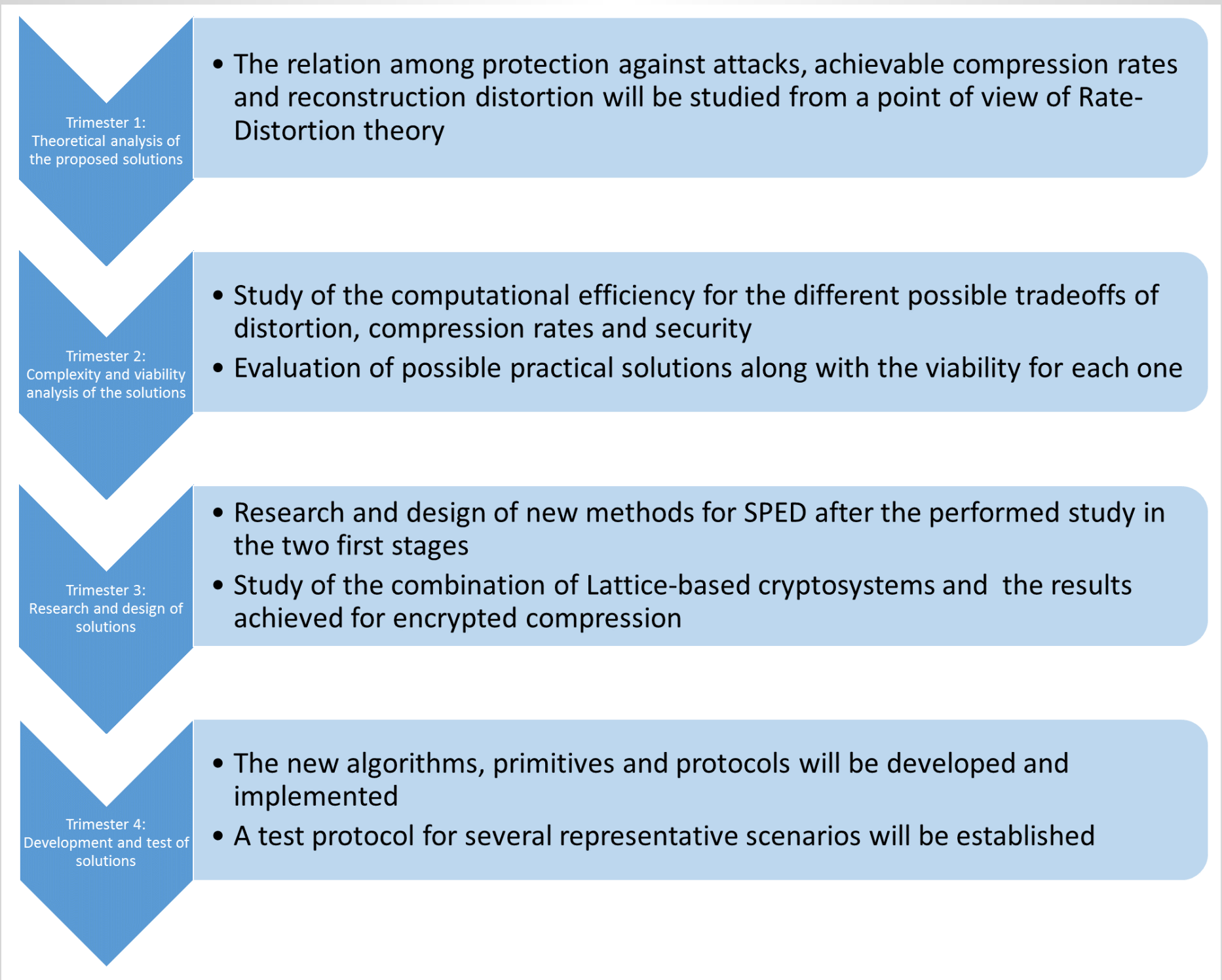
5. Next Year Planning

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

1. Concerning the first objective, **we want to generalize the results obtained in [1]** for performing very efficient encrypted operations between sets of multidimensional signals.
2. For the second objective, **we will cover the study of several novel efficient encrypted operations belonging to the field of signal processing (e.g., filtering, different types of signal transforms, matrix operations, etc.)**.
3. Finally, with respect to the third objective, we will follow the **study of the encrypted compression analyzing the bounds for encrypted compression from a point of view of Rate-Distortion theory [6]**.

We also plan to submit two journal papers during the next year. A paper that extends the results of [1] and other paper that covers part of the second objective.

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



Trimester 1: Theoretical analysis of the proposed solutions
- The relation among protection against attacks, achievable compression rates and reconstruction distortion will be studied from a point of view of Rate-Distortion theory

Trimester 2: Complexity and viability analysis of the solutions
- Study of the computational efficiency for the different possible tradeoffs of distortion, compression rates and security
- Evaluation of possible practical solutions along with the viability for each one

Trimester 3: Research and design of solutions
- Research and design of new methods for SPED after the performed study in the two first stages
- Study of the combination of Lattice-based cryptosystems and the results achieved for encrypted compression

Trimester 4: Development and test of solutions
- The new algorithms, primitives and protocols will be developed and implemented
- A test protocol for several representative scenarios will be established

6. References

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

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

[3] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," in *Proceedings of ACM STOC'09*. ACM, 2009, pp. 169–178.

[4] 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.

[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] T.M. Cover, and J.A. Thomas, "Elements of Information Theory," Wiley-Interscience, 2006.

[7] J.R. Troncoso-Pastoriza, and F. Pérez-González, "Secure Signal Processing in the Cloud: Enabling technologies for privacy-preserving multimedia cloud processing," *Signal Processing Magazine, IEEE*, vol.30, no.2, pp. 29–41, March 2013.