JISBD 2025 QuantumX Track

Formalization and analysis of the post-quantum signature scheme FALCON with Maude

Víctor García[1] (vicgarval@upv.es)
Santiago Escobar[1] (sescobar@upv.es)
Kazuhiro Ogata[2] (ogata@jaist.ac.jp)

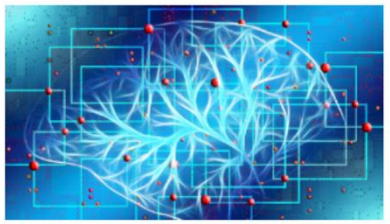
[1]Universitat Politècnica de València (UPV), Camí de Vera, s/n, 46022 València, Valencia, Spain

[2]Japan Advanced Institute of Science and Technology (JAIST), Ishikawa 923–1292, Japan

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UNIVERSITAT POLITÈCNICA DE VALÈNCIA
UPV VRAIN

Who we are

Research Groups



Automata, Formal Languages and its Applications (ALFA)

Language Engineering and Pattern Recognition (ELiRF)

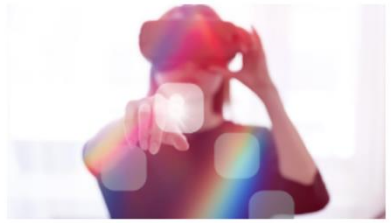
Extensions of Logic Programming (ELP)

Software Production Methods (PROS)

Machine Learning and Language Processing (MLLP)

Information Technology and Artificial Intelligence (GTI-IA)

Multi-paradigm Software Technology (MiST)



Interactive Tehnologies Lab (VertexLit)

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

∋

VRAIN

UPV

Valencian Research Institute for Artificial Intelligence

Extensions of Logic Programming

- Research lines:
  - Industrial Formal Methods,
  - Cryptographic Protocol Analysis,
  - Robust Evaluation of AI Capabilities,
  - Data Science Methodologies and Automation,...
- Members in numbers:
  - 6 (+1) Full Professors
  - 7 Associate Professors
  - 4 Assistant Professors
  - ~17 students (PhD + Collaborators)

About me

- 3rd year PhD Student in Computer Science
- Formal Methods applied to the security of protocols and systems
- Two main research areas:
  - Post-Quantum protocols
  - Protocol Dialects (Moving Target Defence)

(LinkedIn)

FAVPQC (2021 - 2023)

- Formal Analysis and Verification of Post-Quantum Cryptographic Protocols
- Four partners (cryptographers and formal methods collaboration)
- Use of **Maude-NPA** or similar tools

(Web)

EIG CONCERT JAPAN
Connecting and Coordinating European Research and Technology Development with Japan

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

JAIST
JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY
1990

ONDOKUZ MAYIS UNIVERSITY

UNIVERSITÉ DE ROUEN NORMANDIE

Now, about the paper

*"**Formalization** and **analysis** of the post-quantum signature scheme **FALCON** with **Maude**"*

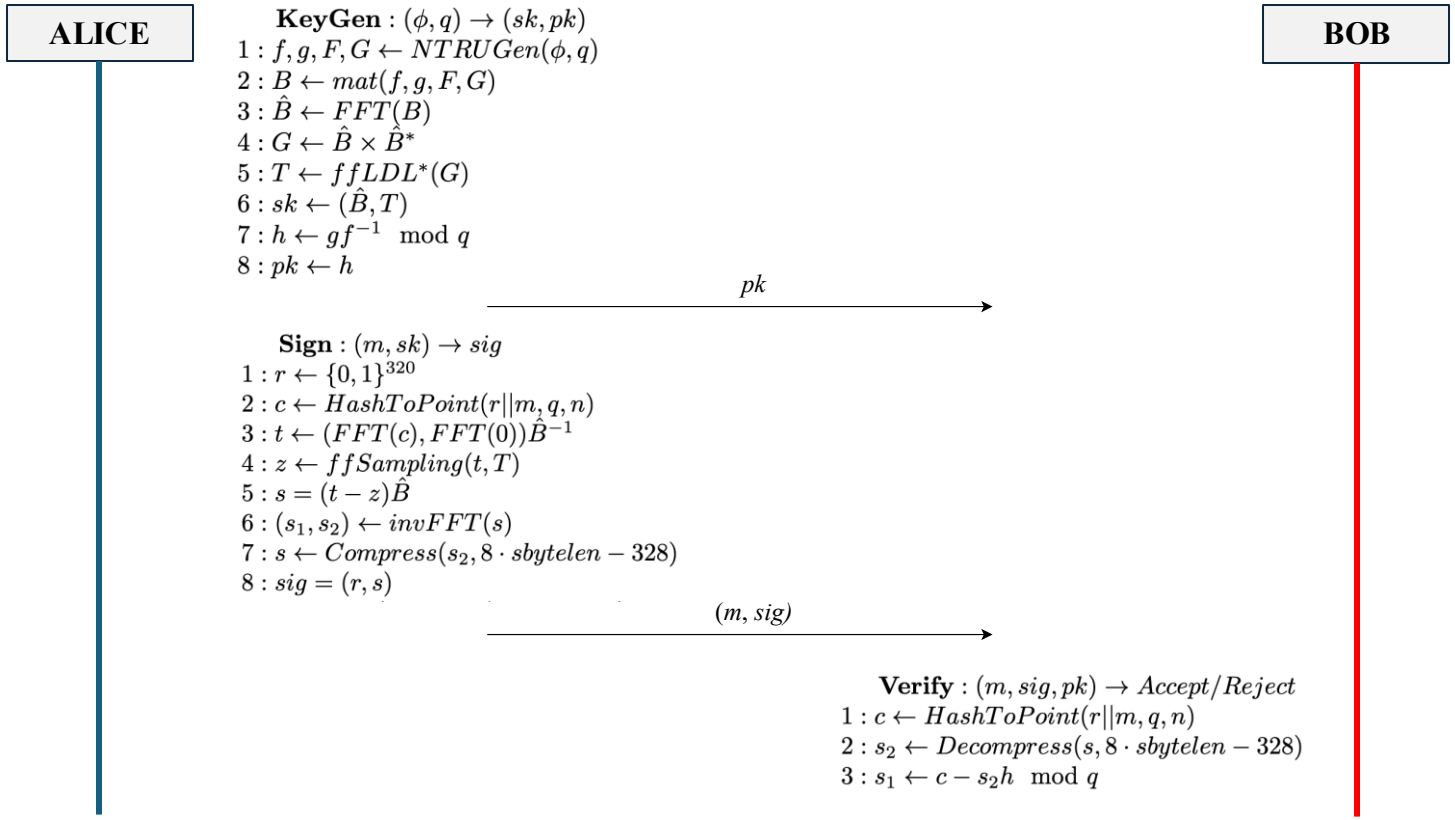
On formalization and analysis

Approaches to security analysis

- **Computational**
  - Mathematical proofs and probabilities
  - Keys, messages,… are bit strings
  - Closer to reality, used by cryptographers
- **Symbolic**
  - Cryptographic primitives as black boxes
  - Keys, messages,… are symbols
  - Suitable for automation and easier to understand for non-experts of cryptography

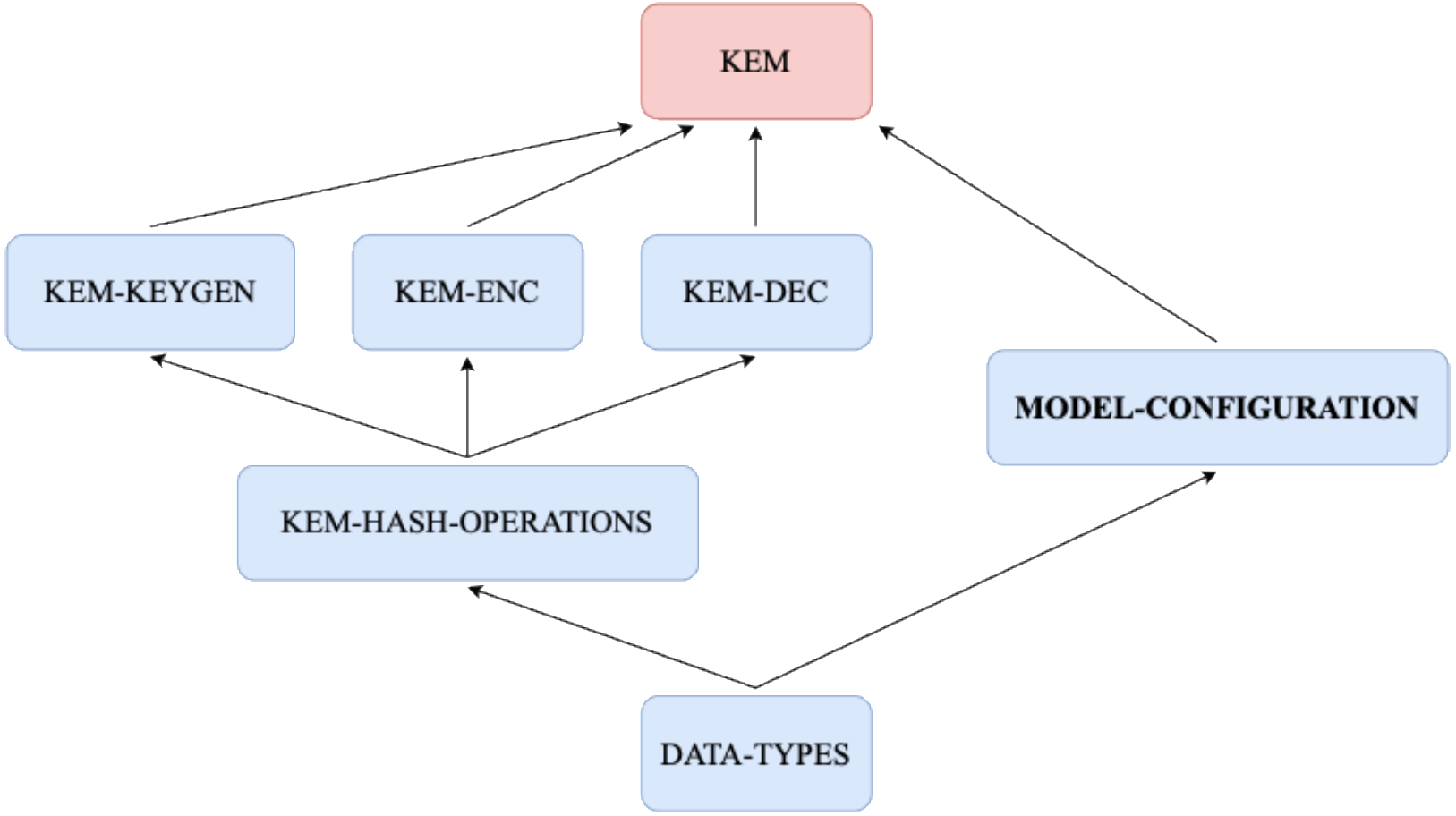
What is FALCON?

Falcon is a signature scheme based on lattices to sign and verify messages.



Framework

MoudEE



Results

- We have built a symbolic model with our reusable framework
- We have proven the following interesting properties for DSA
  - Integrity
  - Non-Repudiation
  - Authentication
- If no authentication is given to the channel, a Man-In-The-Middle attack could happen

Questions, comments, opinions, ...

Contact us!

Víctor García

(vicgarval@upv.es)

Santiago Escobar

(sescobar@upv.es)