Modelling and verification of post-quantum key encapsulation mechanisms using Maude

Víctor García[1], Santiago Escobar[1], Kazuhiro Ogata[2], Sedat Akleylek[3,4], Ayoub Otmani[5]

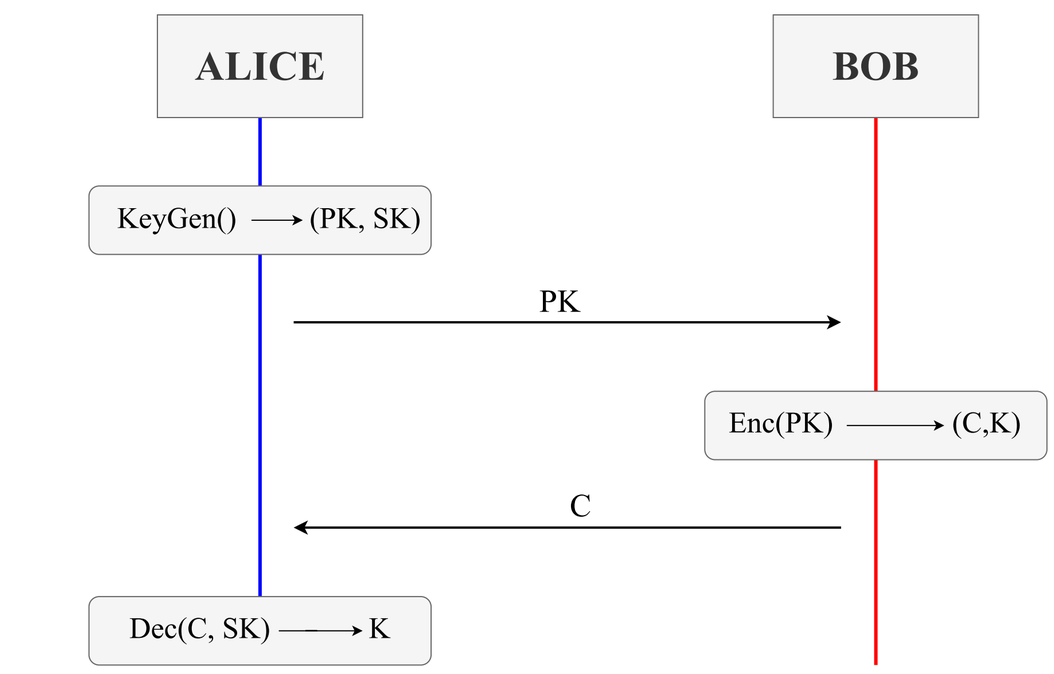
[1]VRAIN, Universitat Politècnica de València, Spain
[2]Japan Advanced Institute of Science and Technology, Japan
[3]Ondokuz Mayis University, Turkey
[4]University of Tartu, Estonia
[5]University of Rouen Normandie, France

Motivation

- Research in the quantum field endangers the security provided by classic cryptography.
- Wide range of candidates in the PQC project by NIST. From **KEMs** to DSAs.
- How can we analyze the security of the proposed schemes in a semi-automatic way? The answer is this work.

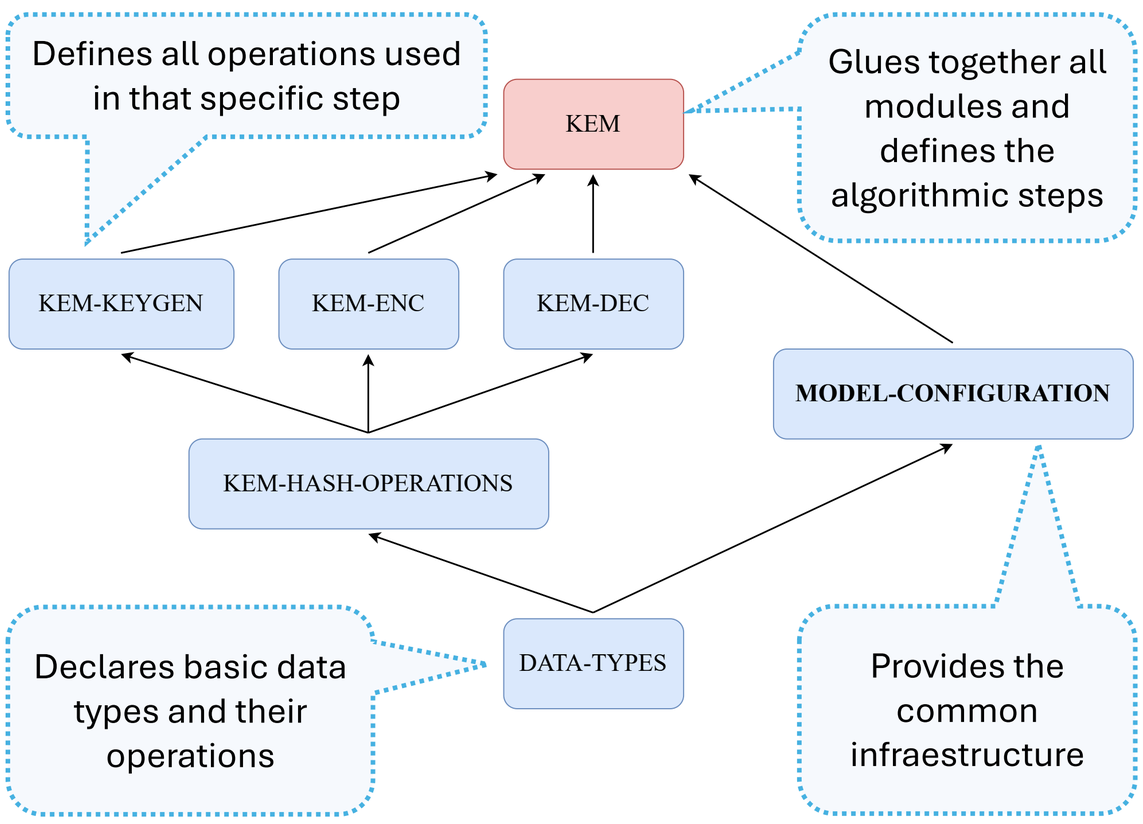
Key Encapsulation Mechanisms

A Key Encapsulation Mechanism's primary goal is to securely share a key between two network participants where channels are not safe from intruders. We selected **KYBER** (*lattice-based*), **BIKE** and **Classic McEliece** (both *code-based*).



Framework

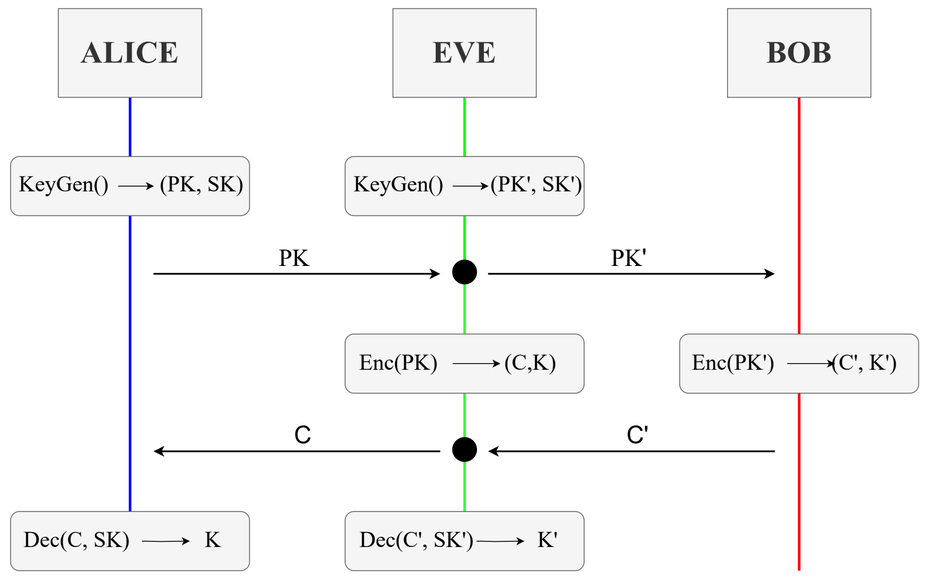
We propose a framework that eases the specification of KEMs in an intuitive **modular** way, providing a **reusable** network infrastructure for **different kinds** of KEMs.



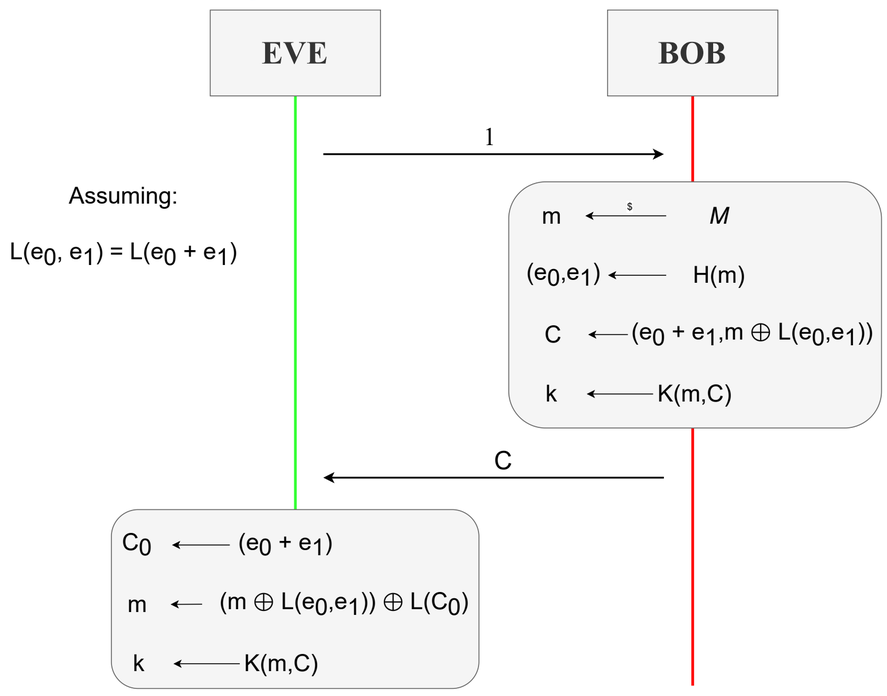
Experiments

Our symbolic analyses discover a Man-In-The-Middle attack for the three KEMs and a vulnerability regarding weak keys in BIKE. We also perform model checking of three properties.

Man-In-The-Middle Attack



BIKE's Vulnerability



Model Checking

PROPERTY	DESCRIPTION	RESULT
SECRECY	No participant learns the secret key of another one in any possible trace of execution.	✗
KEY SHARING	Whenever two participants want to share a key, they eventually do so.	✓
FAIRNESS	Whenever two participants want to share a key, they do so infinitely many often.	✓

Conclusion

We propose a framework for the symbolic analysis of KEMs and use it to analyse KYBER, BIKE and Classic McEliece. We prove the presence of a MITM attack on the three KEMs and a vulnerability on BIKE. A solution to the MITM attack is to use some form of authentication or integrity, e.g. digital signature algorithms. For the vulnerability, a check to avoid weak keys during encapsulation fixes the problem.

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Víctor García and Santiago Escobar were supported by INCIBE's Chair funded by the EU-NextGenerationEU through the Spanish government's Plan de Recuperación, Transformación y Resiliencia.