Analysis and verification of code-based key encapsulation mechanism BIKE in Maude

Víctor García
vicgarval@upv.es

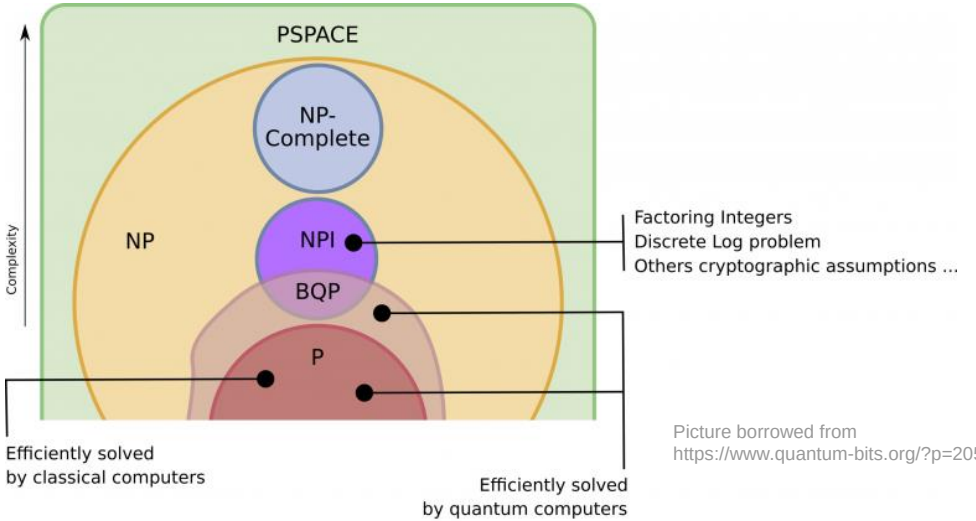
Santiago Escobar
sescobar@upv.es

Universitat Politècnica de València

VRAIN - Valencian Research Institute for Artificial Intelligence

Contents

- Threat of quantum computers
  - Shor's algorithm
  - Grover's algorithm



Picture borrowed from
https://www.quantum-bits.org/?p=2059

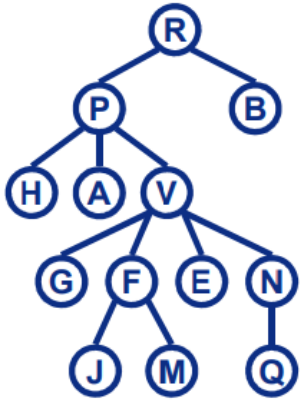
- Solution by the NIST with the Post-Quantum Cryptography project
  - Round 4 (2022): **BIKE**, Classic McEliece, HQC, SIKE

Types of security analysis

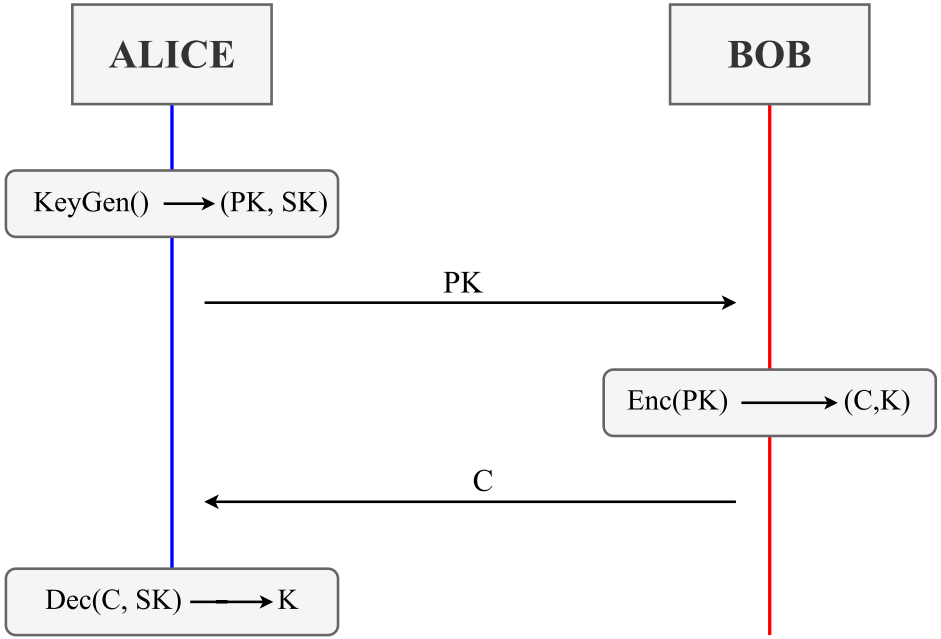
- Computational
  - Mathematical proofs and probabilities
  - Keys, messages,... are bit strings
  - Closer to reality, used by cryptographers
- Symbolic
  - Cryptographic primitives as black boxes
  - Keys, messages,… are symbols
  - Suitable for automation and easier to understand for non-experts of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

MaudE

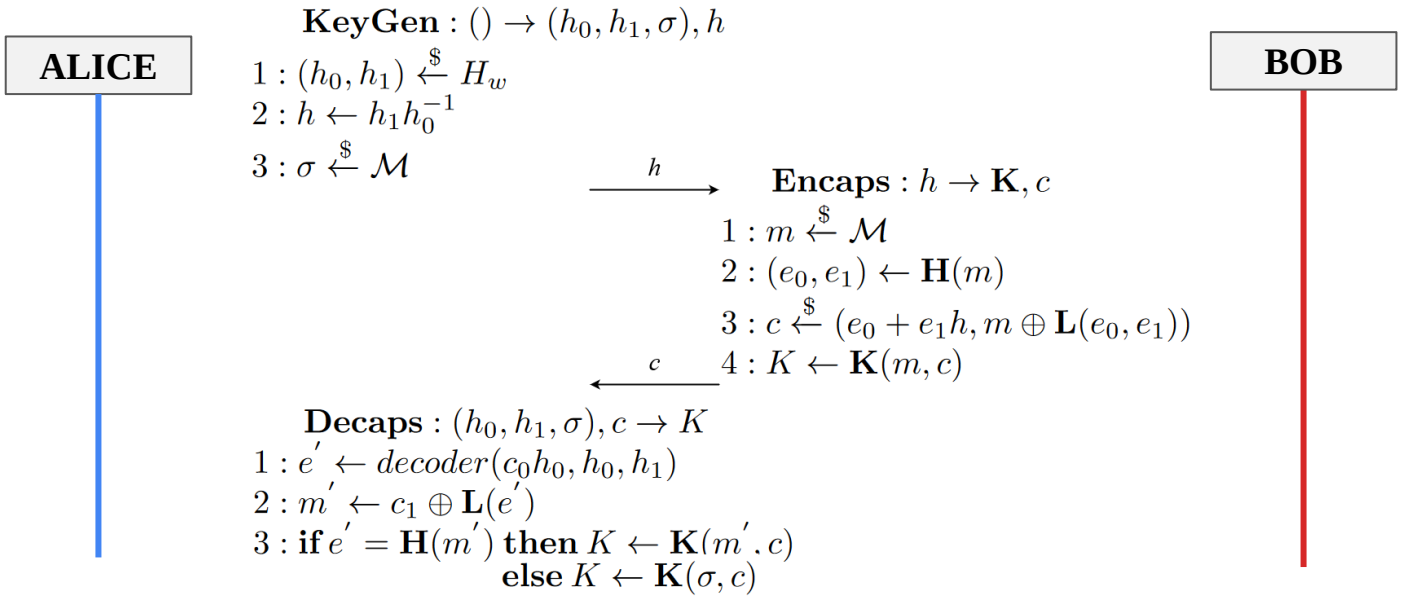
- Maude is a modelling, programming and verification language
- Explicit state model checking using *search* or LTL properties
- Origins at Stanford, California
- Project members
  - USA
  - Norway
  - Spain



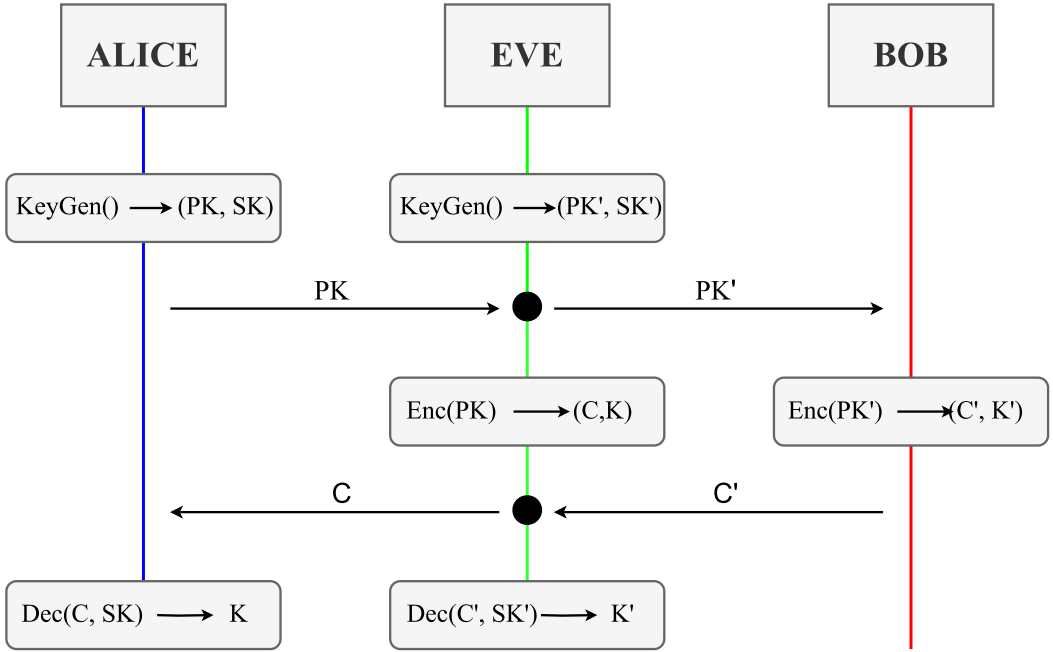
KEM behaviour



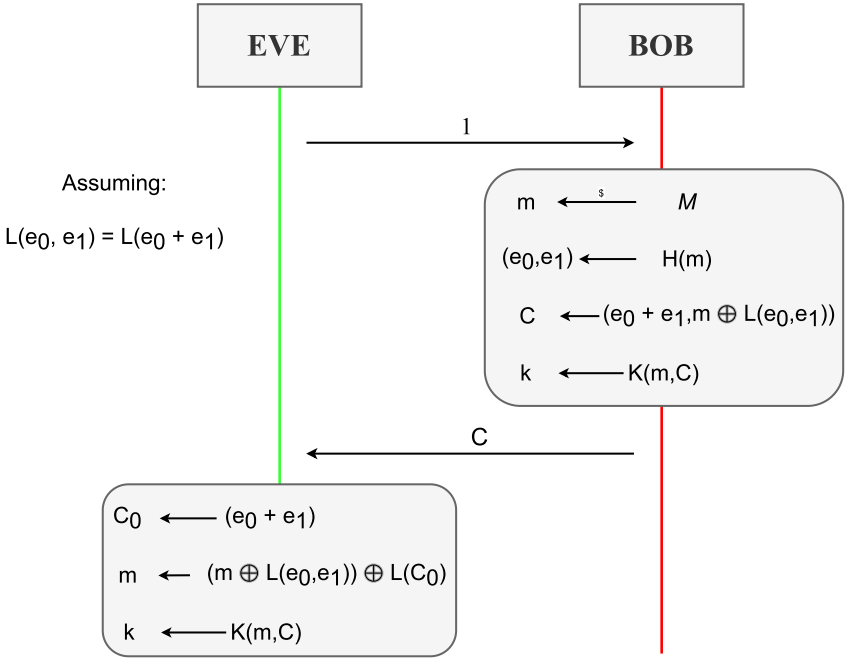
BIKE specification



Discovery of Man-In-The-Middle



Discovered key vulnerability



- Symbolic specification of BIKE using a formal framework
- Extended symbolic analysis
  - Verify its correctness with respect to the original protocol specification
  - Check three properties in Maude's LTL Model Checker
    - Key Sharing (LIVENESS)
    - FAIRNESS
    - SECURITY
- Found a MITM attack and a design vulnerability
  - Both can be fixed using authentication or integrity over messages
  - Design vulnerability can be avoided by checking insecure/weak keys before Enc