A Report of Malta Research Stay

Peter Spacek

Content

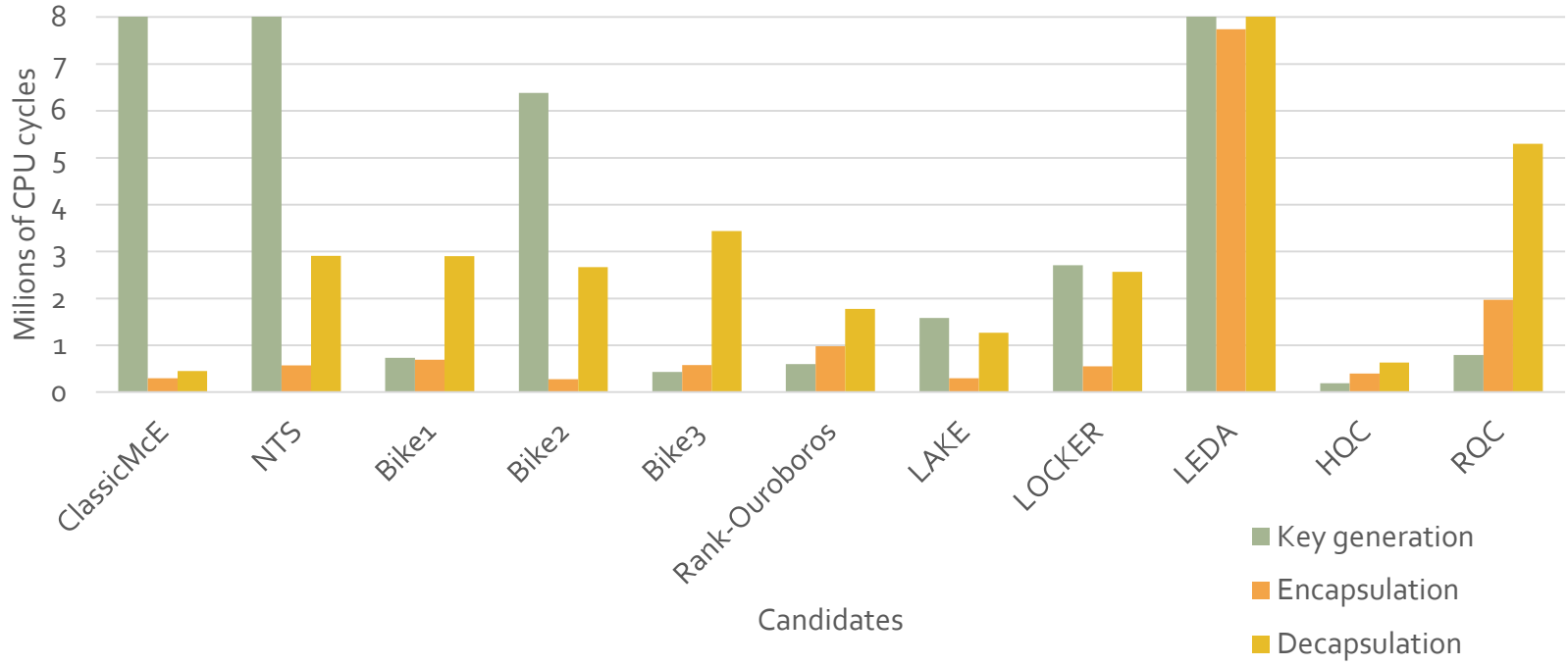
- Dissertation work
- TLS
- Collaboration with University of Malta
- Experiment
- Results
- Future work

Research topics

Dissertation goals

- Research in post-quantum key establishment
- (Quantum) secure TLS like protocol
  - Review quantum secure algorithms
  - Implementation level
  - Robustness against malware
  - Quantum secure algorithms in embedded devices

NIST code-based cadidates for KEM

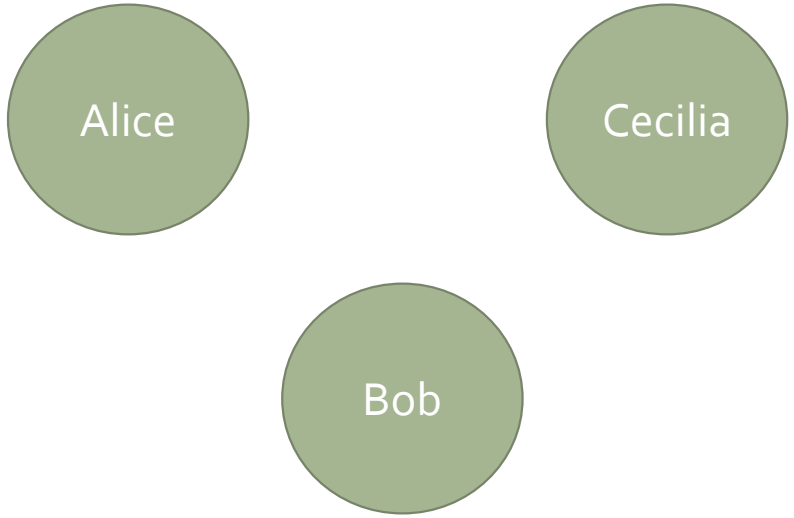


My research and the project

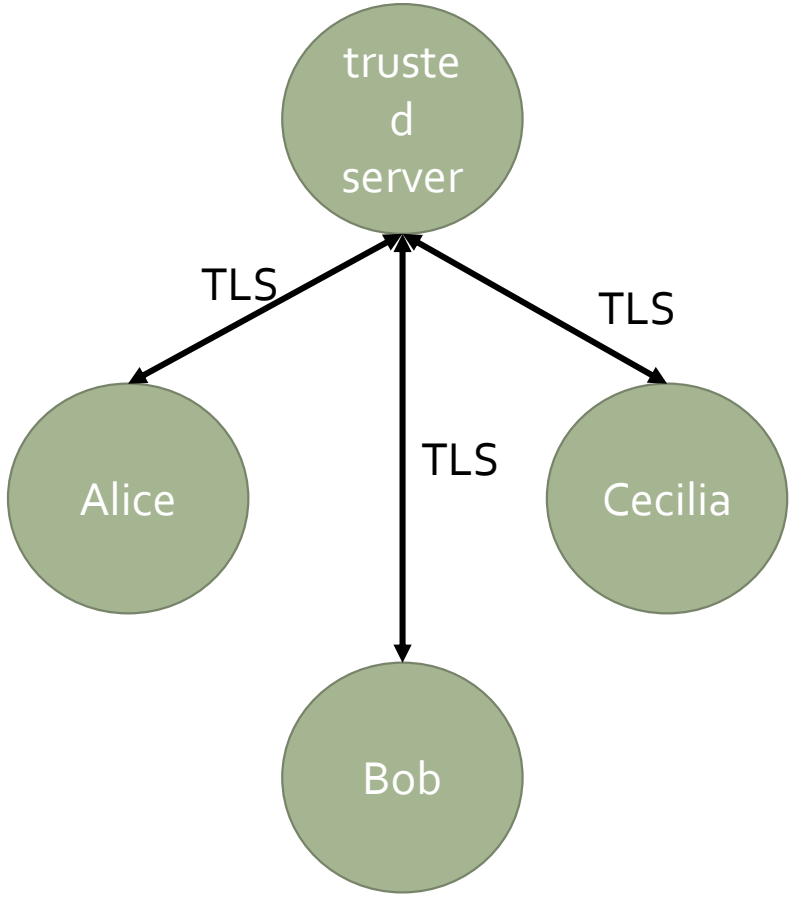
- Two models for secure group communication:

- Purpose-built protocol
  - Purpose-built Group Key Establishment
- Client-Server protocol
  - TLS like quantum secure protocol

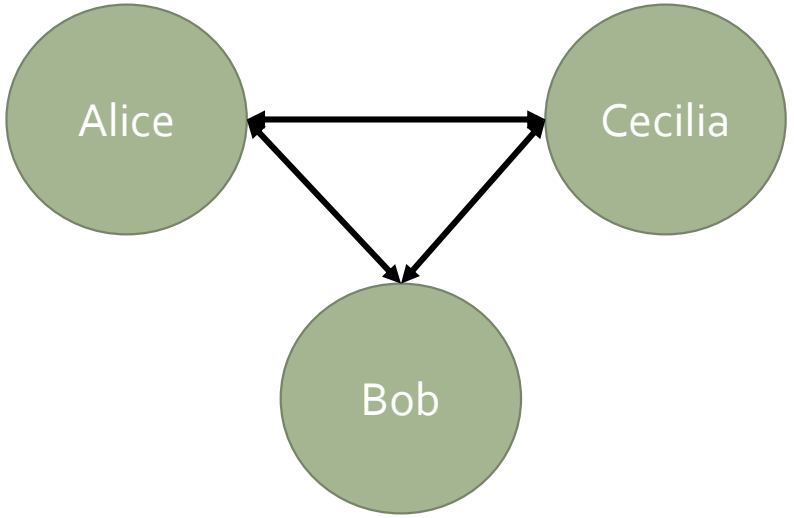
Group Key establishment – simple scenario



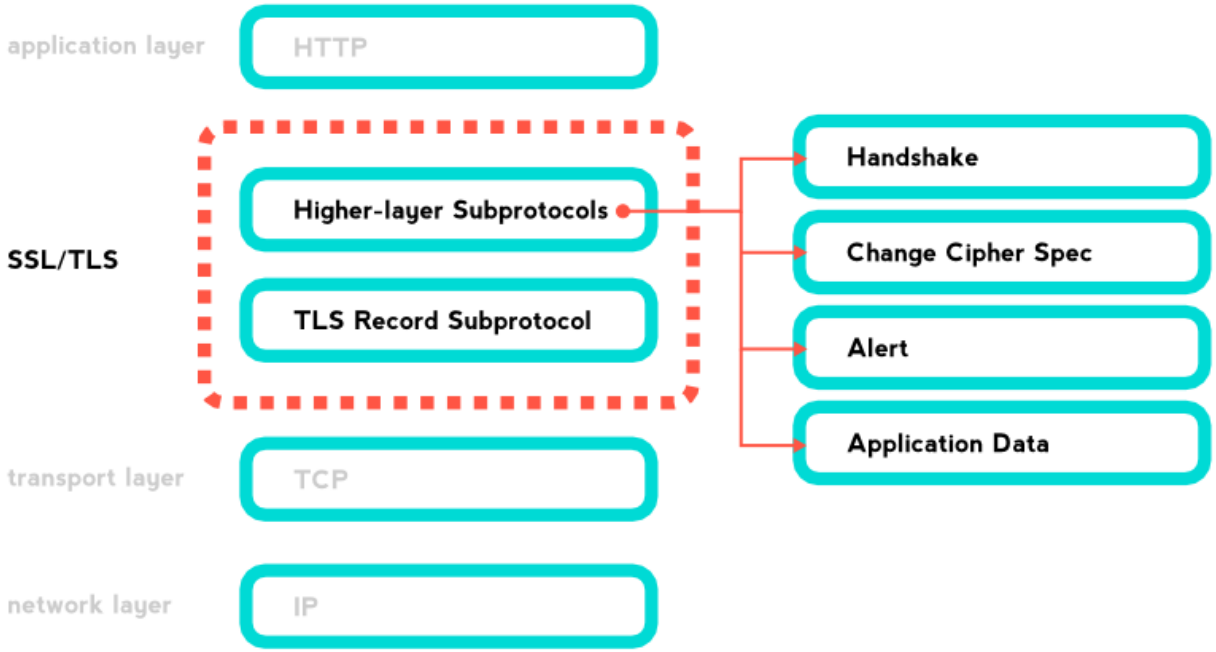
Group Key establishment – simple scenario



Group Key establishment – simple scenario



Client server communication - TLS

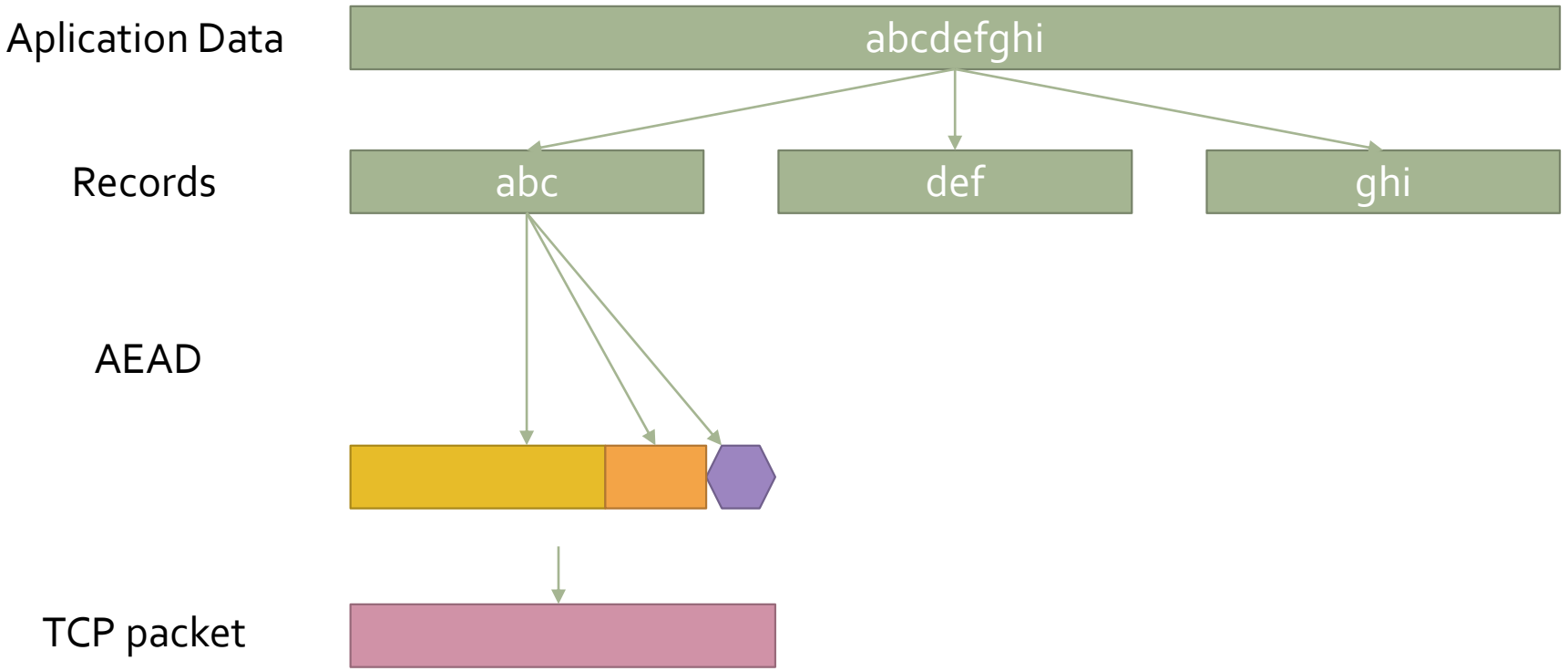


Post-Quantum TLS (Handshake)

- *Eric Crockett, Christian Paquin and Douglas Stebila*
- TLS key exchange for post-quantum cryptography
- liboqs librar

- *Dimitrios Sikeridis, Panos Kampanakis and Michael Devetsikiotis*
- Post-Quantum Authentication in TLS 1.3

Record


Aplication Data
abcdefghi
Records
abc
def
ghi
AEAD
TCP packet

Collaboration with University of Malta

Collaboration with University of Malta

- Enhance security of protocols using
  - HSM
  - RV
- Learn how to work with SeCube
  - Experiment with implementation of algorithm
  - Experiment in malware resistance
- High level Runtime Verification in protocol security

The experiment

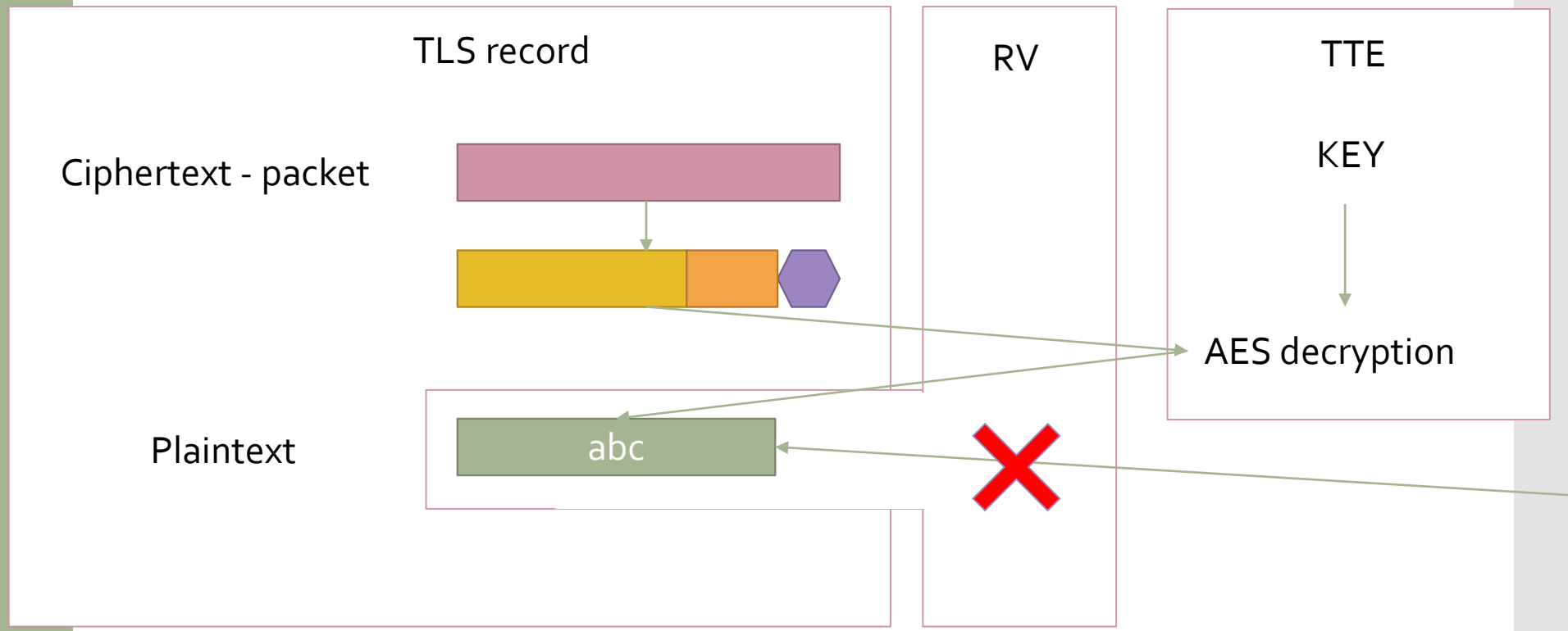
- Analytical security != operational security

- Breaking the cipher is too expensive
- Attacker trying access sensitive data in host

- Use specialized hardware (TEE) to isolate sensitive processes
- Place monitors at strategic points

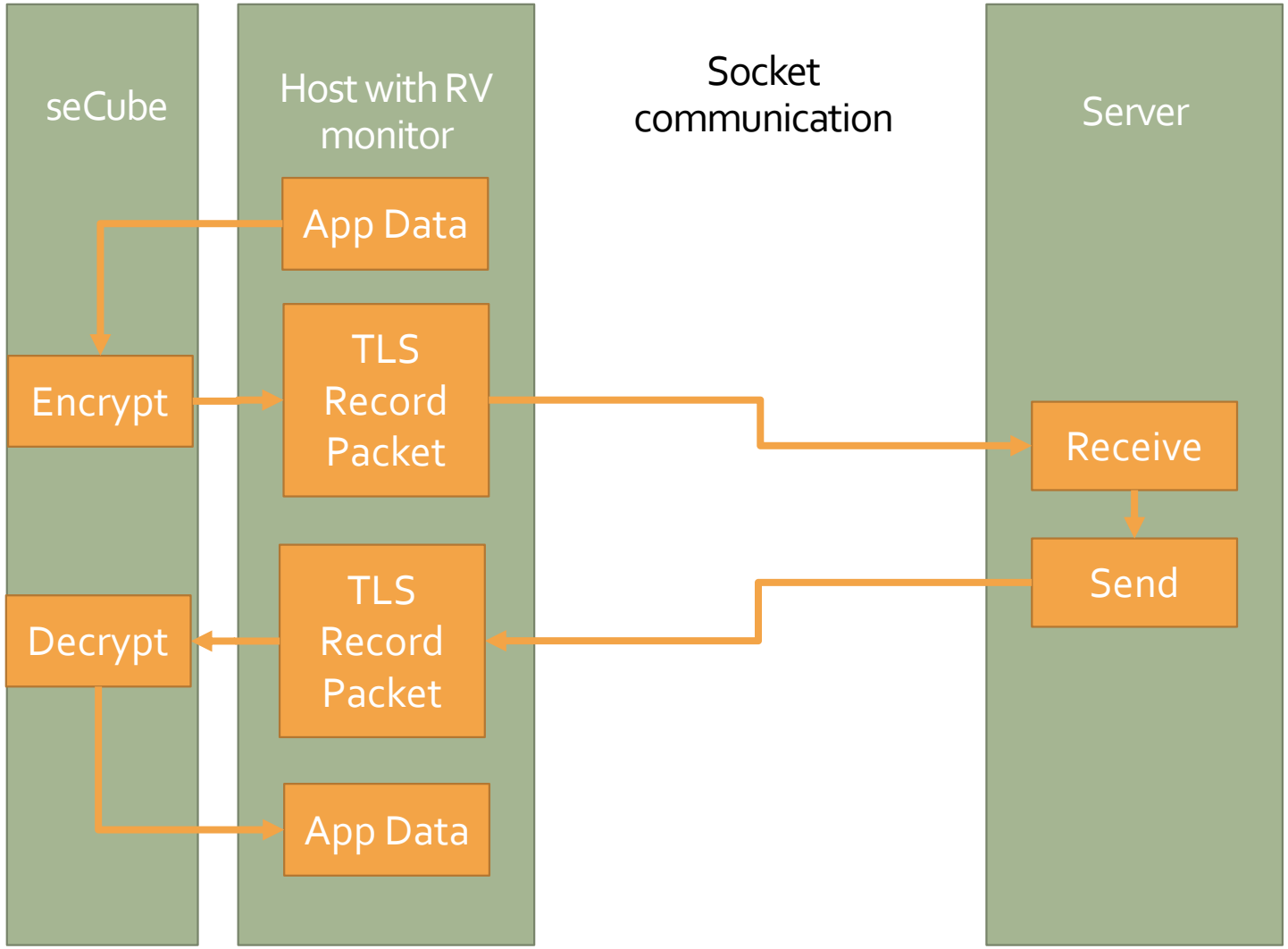
- Location – TLS record

Experiment objectives



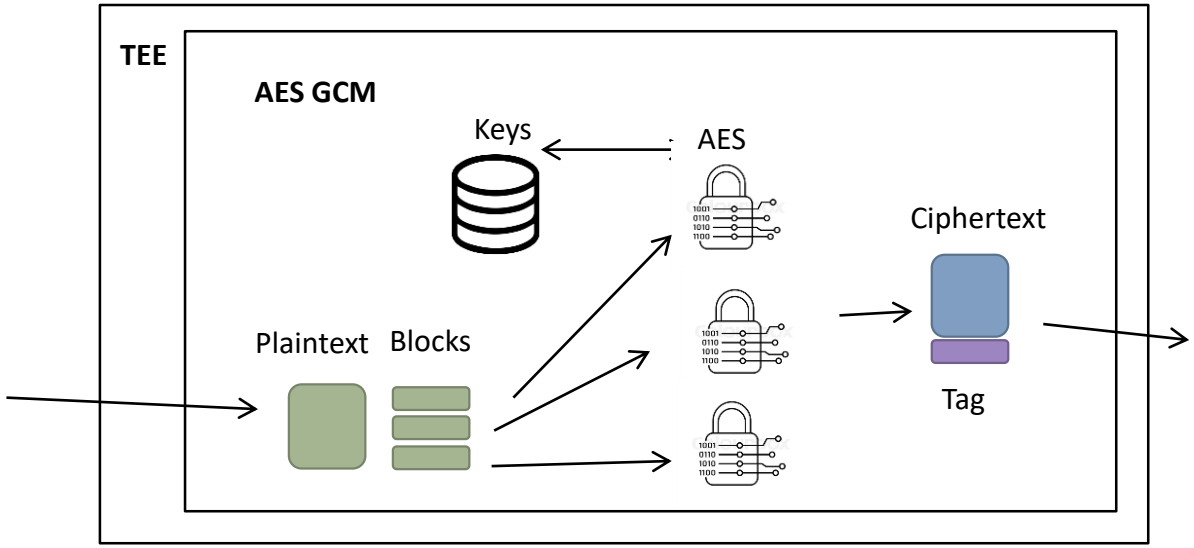
Results

TLS simulation



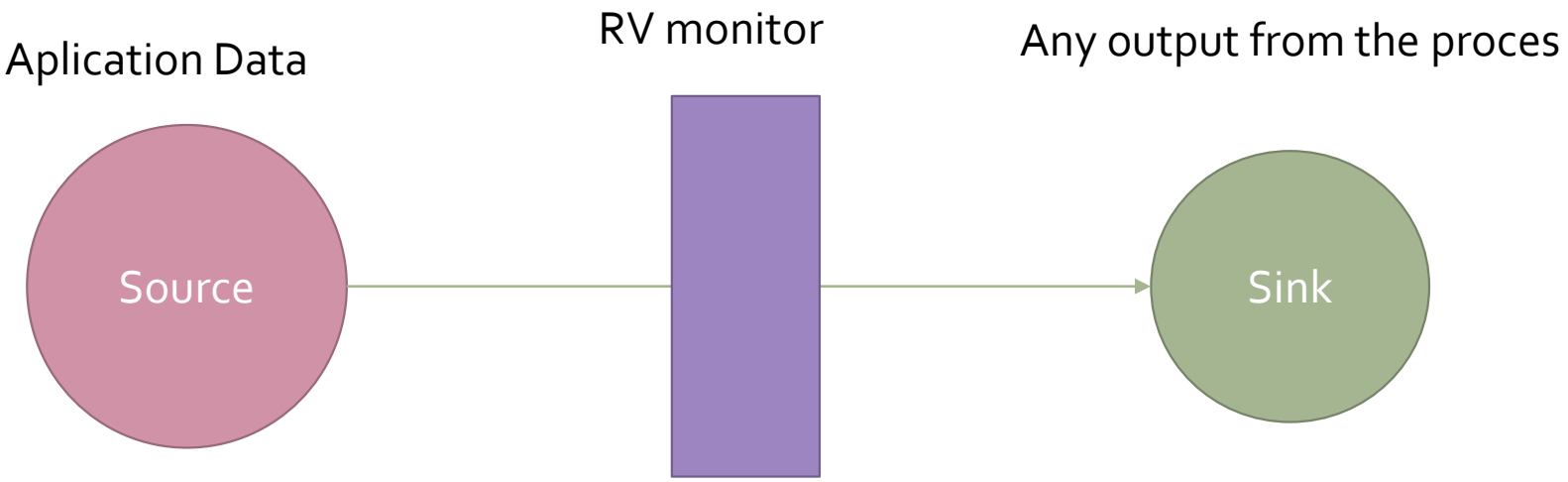
seCube - AES - GCM

- TLS 1.3 Record – AEAD
- AES in GCM mode implementation in seCube



RV monitor

- Hooked functions call
- Log function calls from source to sink



Malware simulation

- Malware stealing plaintext
- Output to network, pipe and file

- RV monitor detecting plaintext leakage

Results for GAKE

- Workshop in Malta
- Enhancing security with HSM
- Using RV to detect malware activity

Future work

- Full seCube TLS
- seCube quantum-resistant TLS

- Smartcard - defence against fyz. attacks
- Acceleration with FPGA

Conclusion

- Securing communication on several levels
  - Strong ciphers – GCM-AES
    - strong for implementation level, side channel attacks - seCube
  - Hiding the keys in TEE – seCube
  - Robustness against malware – seCube + RV

Thank you for your attention

This work is supported by the NATO Science for Peace and Security Programme through project G5448 Secure Communication in the Quantum Era .