QUAKE – Quantum Augmented KEM/DEM Encryption

B. Goncalves, A. Mashatan

Cybersecurity Research Lab, Ted Rogers School of Information Technology Management, Ryerson University

Research Funded by NXM Labs Inc.

Introduction / Motivation

As the **quantum age of computing approaches**, there is a definite **need for secure cryptographic algorithms against quantum attacks** that are expected to break nearly all current public-key cryptography. This becomes especially dangerous as the number of connected devices increases dramatically in the coming years.

However, it is **not a simple task to replace old algorithms** with new quantum resistant ones because of the following concerns:

- It would include **updating existing cryptographic infrastructure** which took nearly two decades to establish. There is then a risk that **during this process data may be vulnerable.**
- These new algorithms are still relatively **novel and future cryptanalysis may find quantum, or even classical, weaknesses**.

Background

Research Questions:

1. **Does there exist an encryption algorithm that provides security** against quantum attacks **that is also capable of minimalizing risks during a transition** away from classical algorithms?
2. If such an algorithm exists, **is it viable** to implement on lightweight devices such as Internet of Things (IoT) devices?

Methodology

To answer these questions we used both the theory of combiners and the theory of hybrid cryptography.

- **Combiners**: Algorithms which take different algorithms as input and produces a new cryptographic scheme.
- **Hybrid Cryptography**: Refers to Classical/Quantum hybrid cryptosystems. That is to say a cryptosystem that use both classical and quantum-resistant cryptographic components.

Implications

- Do more hybrid PKE combiners exist, and **how would new constructions compare** to **QUAKE?**
- **Do hybrid combiners for other protocols**, such as key exchange and distributed key generation, exist?
- Can the techniques used in **QUAKE** apply to these protocols? Can **QUAKE** itself be used to construct these protocols?

Results/Claims

1. We present a **new public-key encryption (PKE) combiner** that outputs **a hybridly secure PKE**, called **QUAKE**.
2. We prove its full security against adversaries in both the **Random Oracle Model and Quantum Random Oracle Model.**
3. In comparisons to similar works we rely on both **fewer and simpler assumptions.**

Results - QUAKE

Π.Enc(pk, ek, m):

1. $\delta \leftarrow_{\$} \{0, 1\}$
2. $(c, k) \leftarrow \mathrm{K.Encaps}(ek; \mathrm{Hash}_1(\delta))$
3. $c_{sym} \leftarrow \Pi^{sym}.\mathrm{Enc}(k, m \| \delta)$
4. $c_{asym} \leftarrow \Pi^{asym}.\mathrm{Enc}(pk, c_{sym}; \mathrm{Hash}_2(\delta))$
5. Send c, c_{asym}

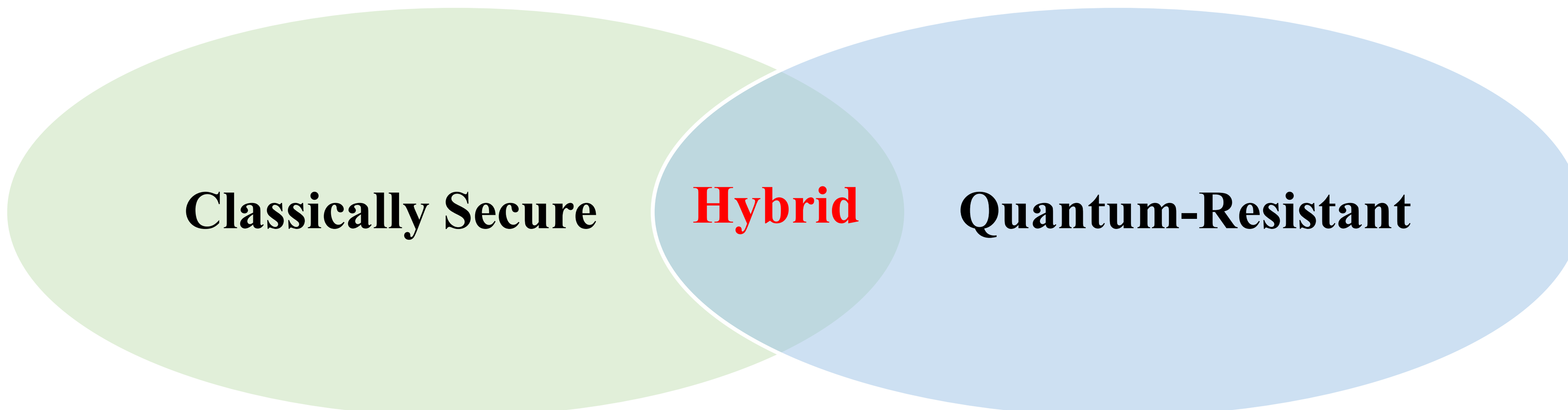

Figure 1 : Hybrid Cryptography

Discussions

Hybrid PKEs offer a solution to the challenges present when transitioning from classical to quantum-resistant algorithms.

QUAKE can be deployed on top of the current cryptographic infrastructure, including IoT devices and, thus, can **protect data now from a quantum future including the harvest now and decrypt later attack.**

QUAKE is also **compactly designed and efficient** allowing for future replacements. Old and new algorithms can be used and replaced as new attacks are developed and refined.

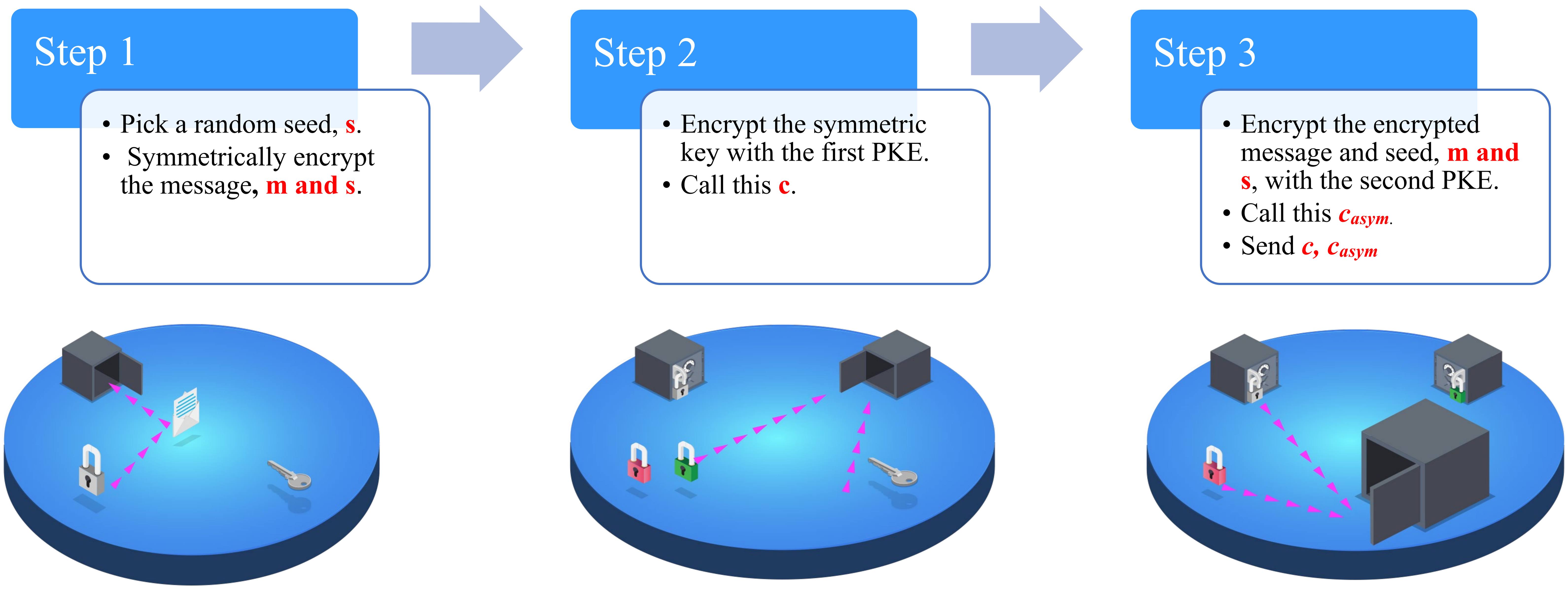

Figure 2 : QUAKE Encryption (Informal)

Ryerson University

TED ROGERS SCHOOL Information Technology Management

NSERC CRSNG

www.ryerson.ca/crl

NXM

CYBERSECURITY RESEARCH LAB