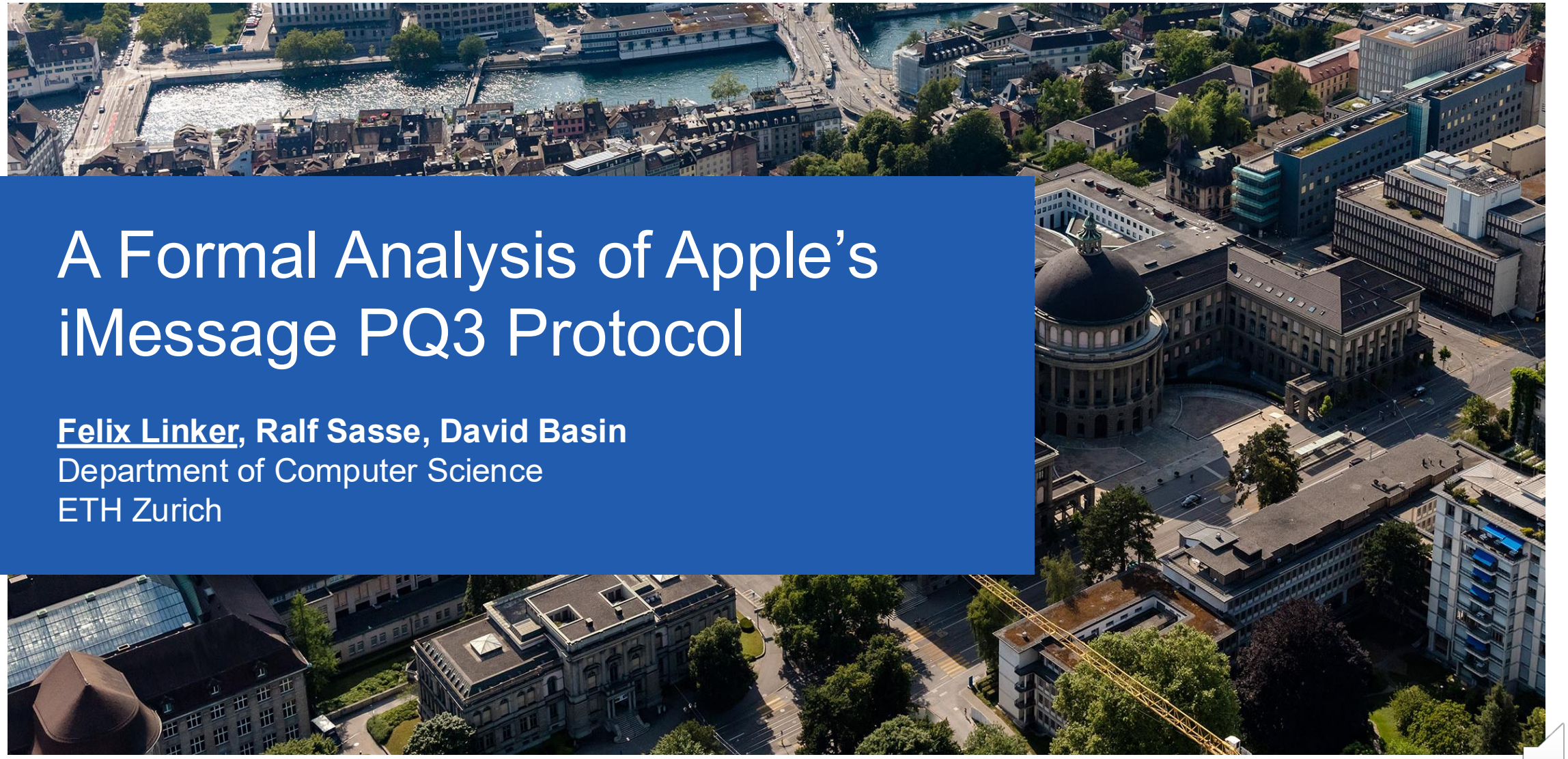
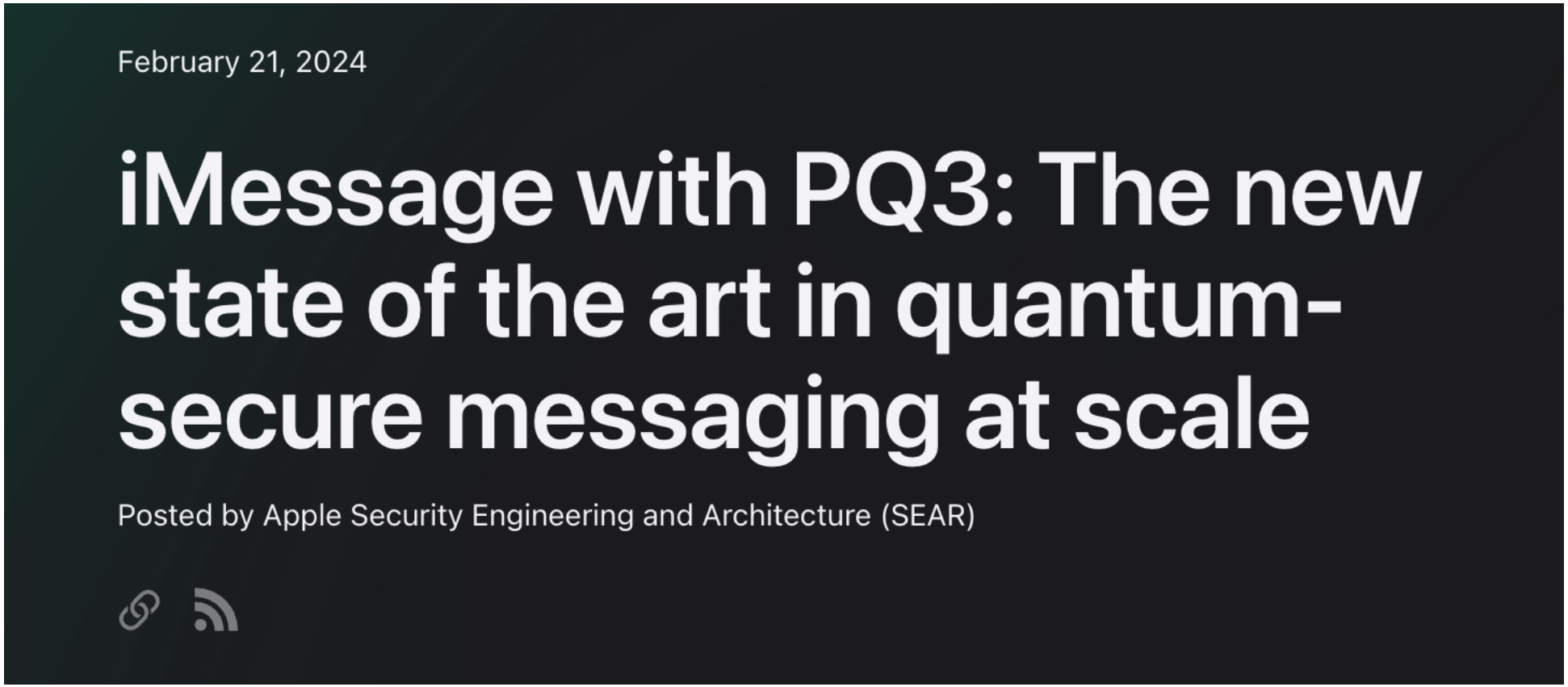
ETH zürich

Department of Computer Science

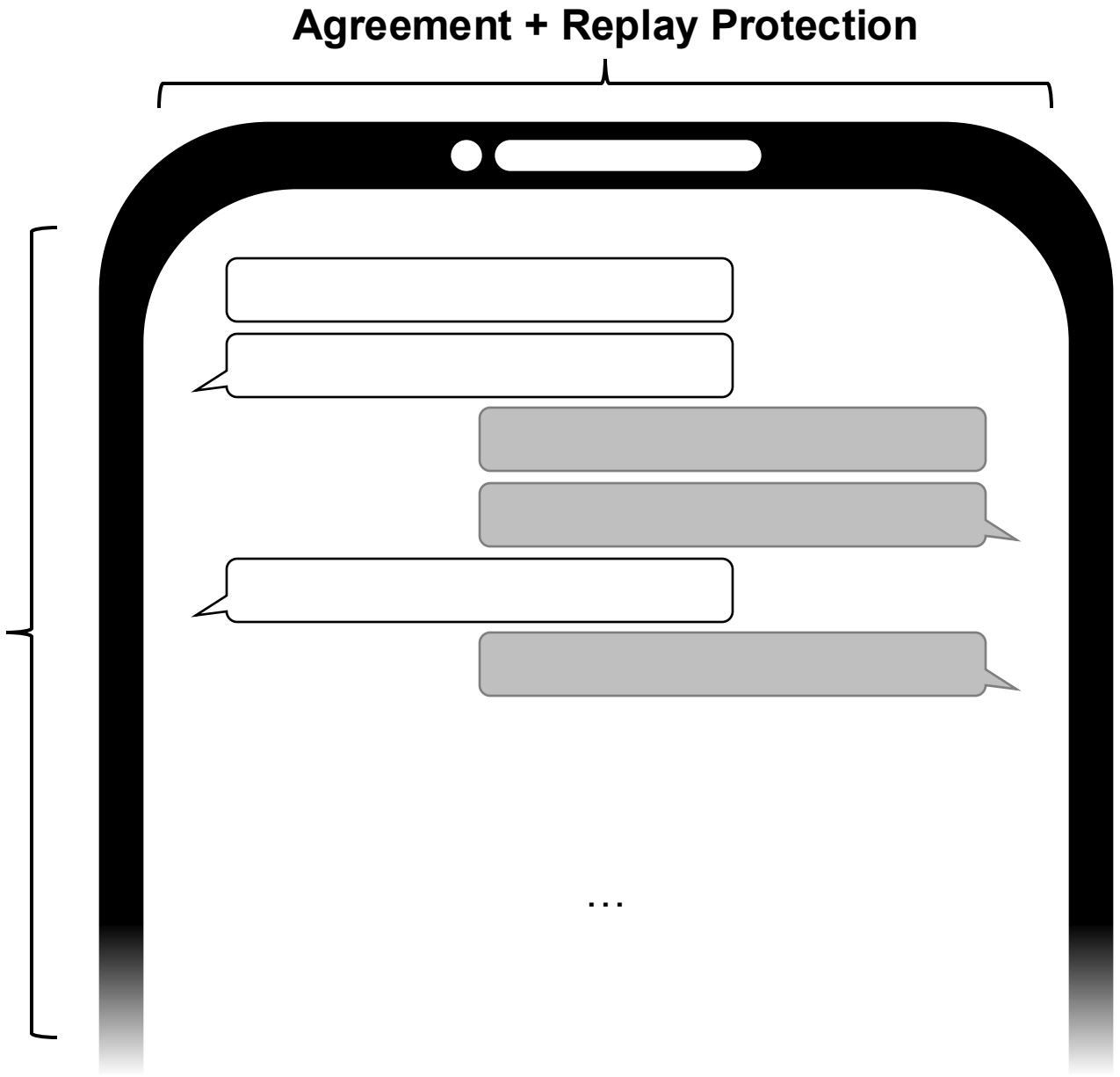


A Formal Analysis of Apple's iMessage PQ3 Protocol

Felix Linker, Ralf Sasse, David Basin
Department of Computer Science
ETH Zurich


February 21, 2024
iMessage with PQ3: The new state of the art in quantum-secure messaging at scale
Posted by Apple Security Engineering and Architecture (SEAR)

iMessage PQ3



Secrecy
Messages are confidential

Forward Secrecy
Previous messages remain confidential

Session secrets revealed

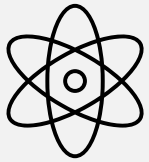
Post-Compromise Security
Recover secrecy

iMessage PQ3

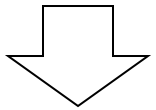
Adversary Capabilities

Active Network Adversary

"Harvest now, decrypt later"

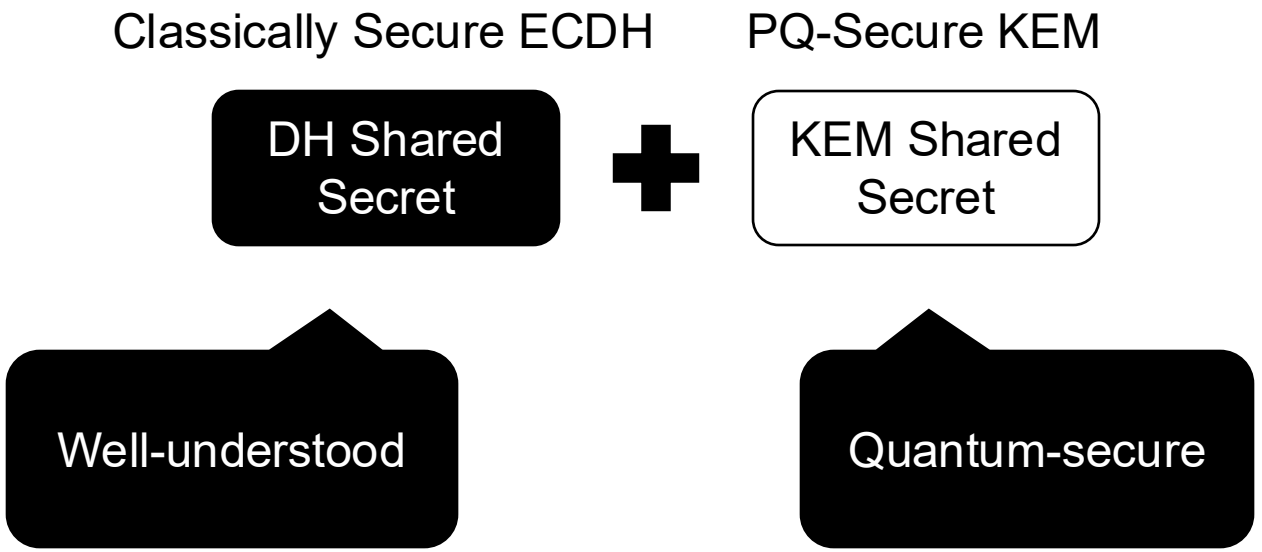


Can compromise any key

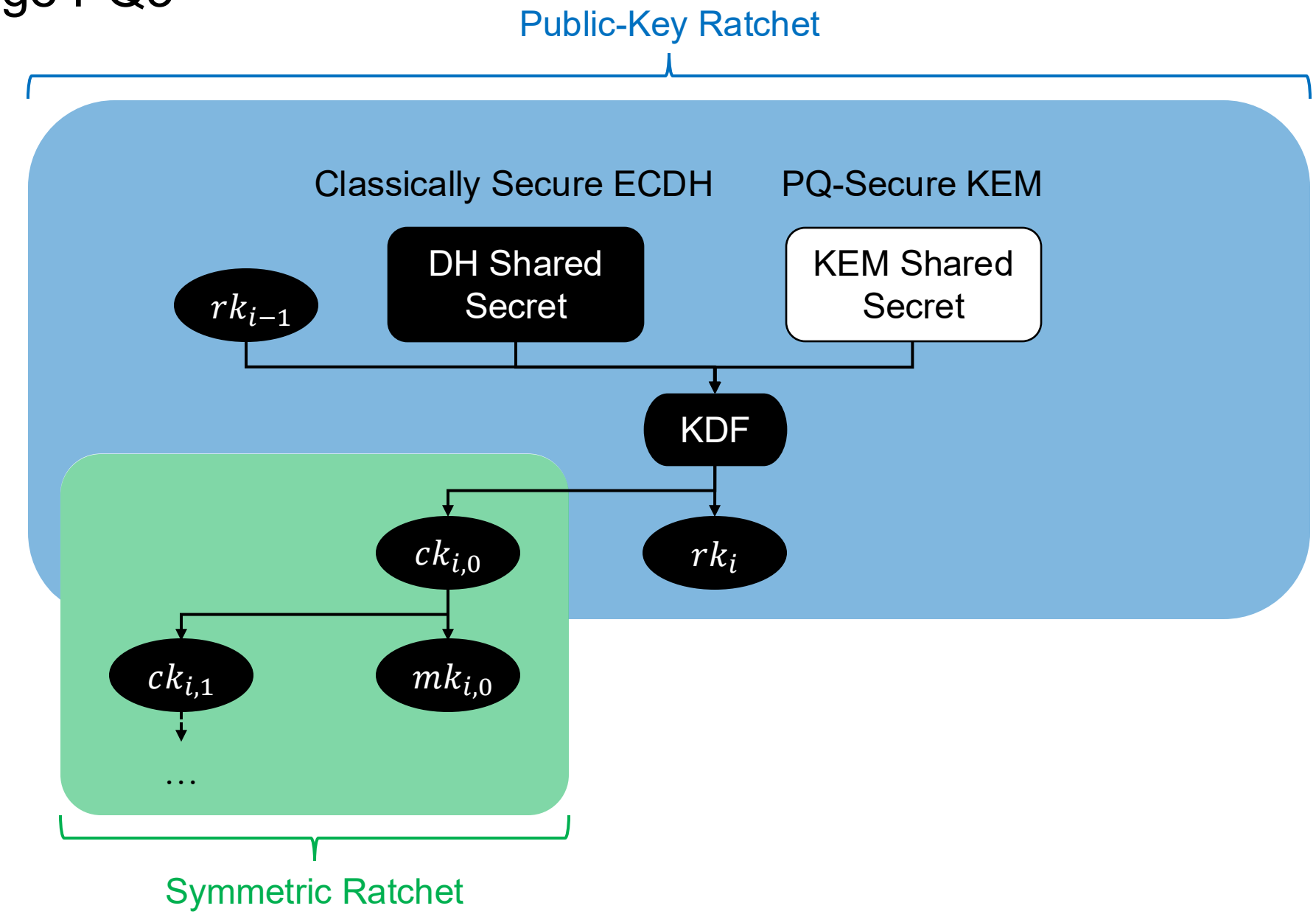


Passive quantum adversary

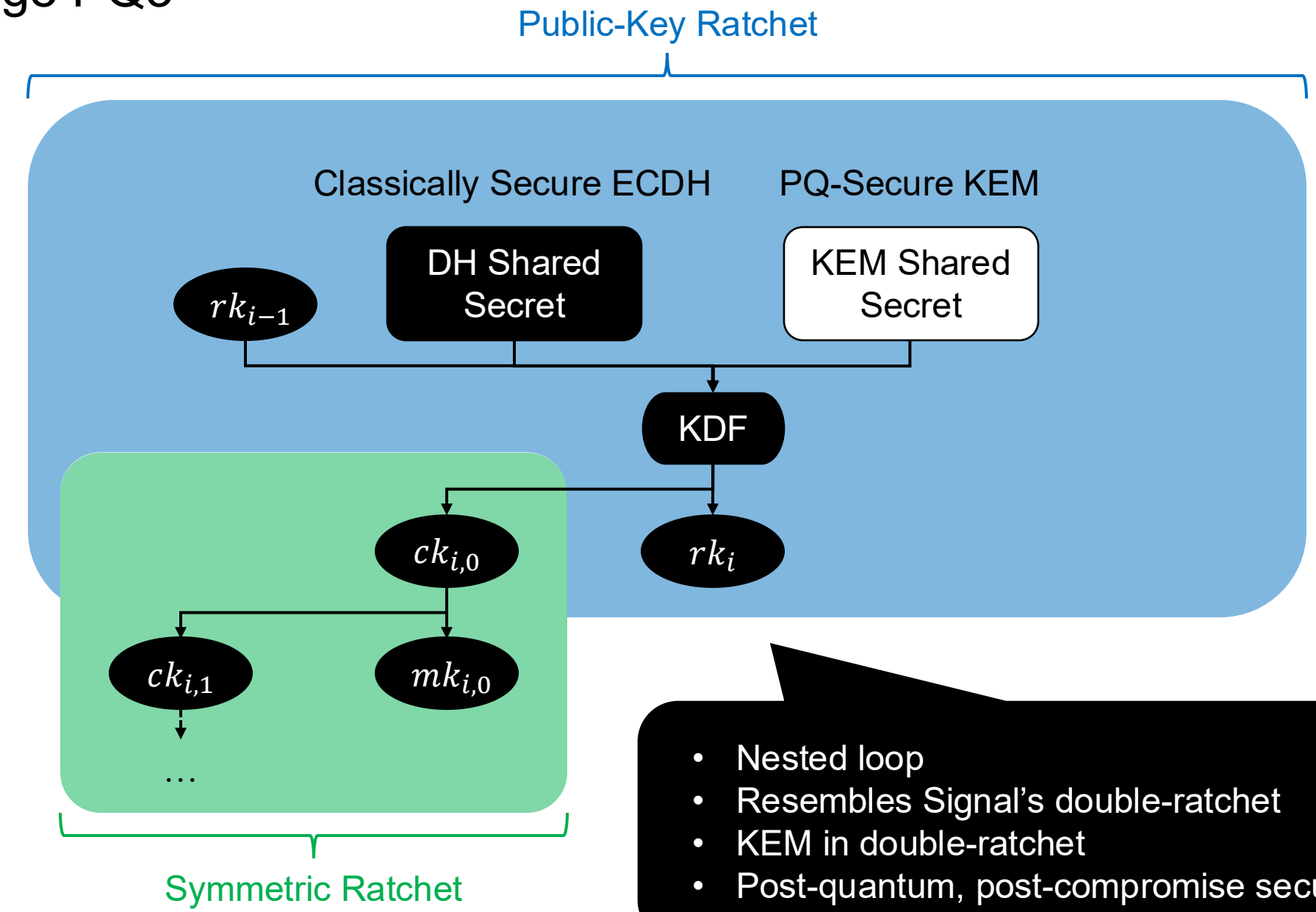
iMessage PQ3



iMessage PQ3

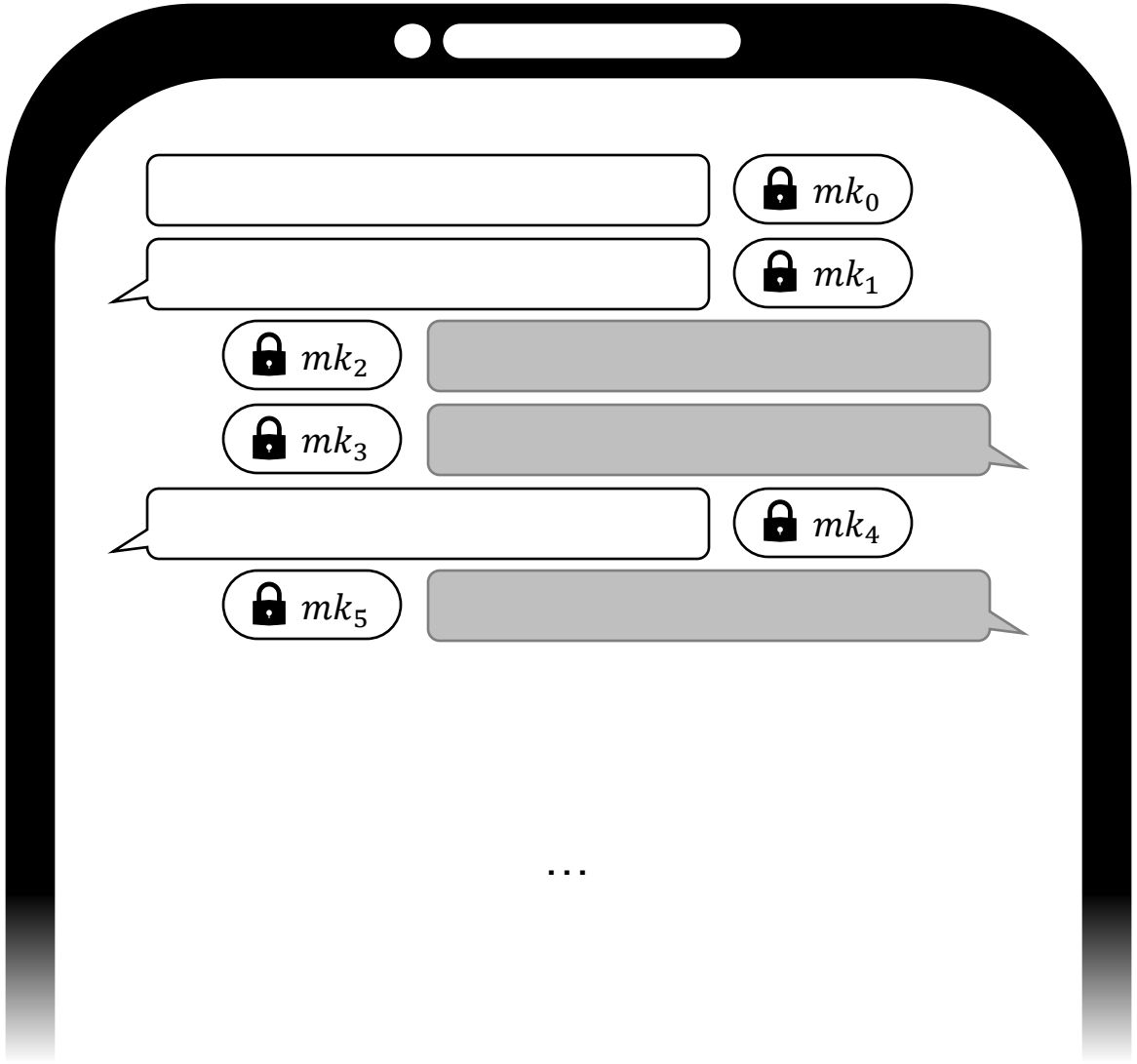


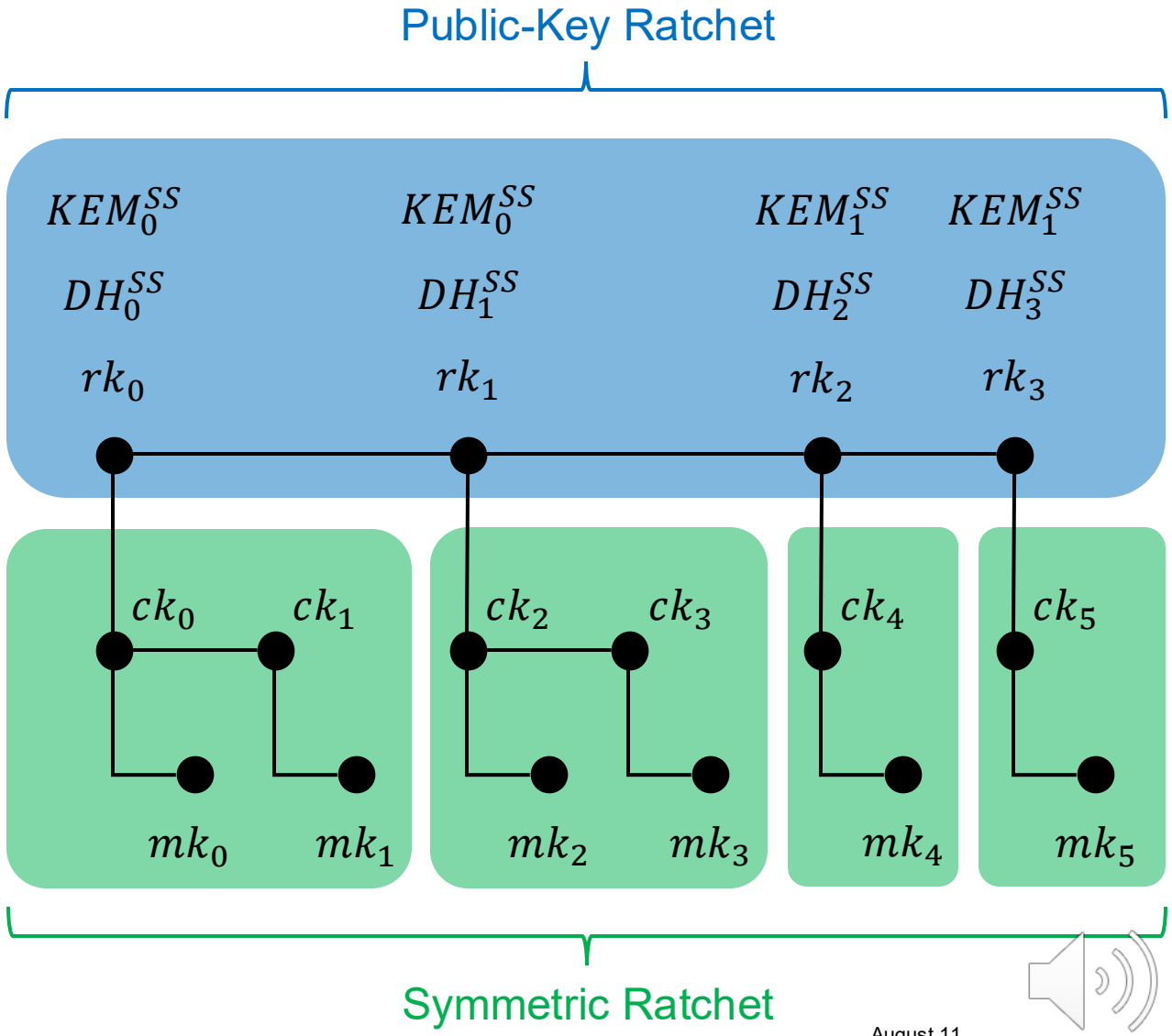
iMessage PQ3



- Nested loop
- Resembles Signal's double-ratchet
- KEM in double-ratchet
- Post-quantum, post-compromise security

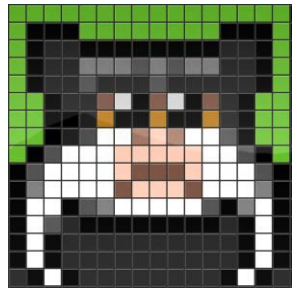
iMessage Double-Ratchet Protocol





Goals

- Understand security goals thoroughly
- **Verify** that iMessage meets security goals



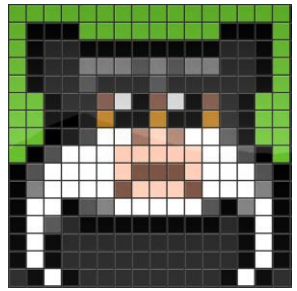
(“Tamarin” is also a monkey)

The Tamarin Prover

- …is a protocol verifier
- …uses constraint solving
- …operates in the symbolic model
- …has been used to verify TLS 1.3, 5G AKA, EMV

Goals

- Understand security goals thoroughly
- **Verify** that iMessage meets security goals

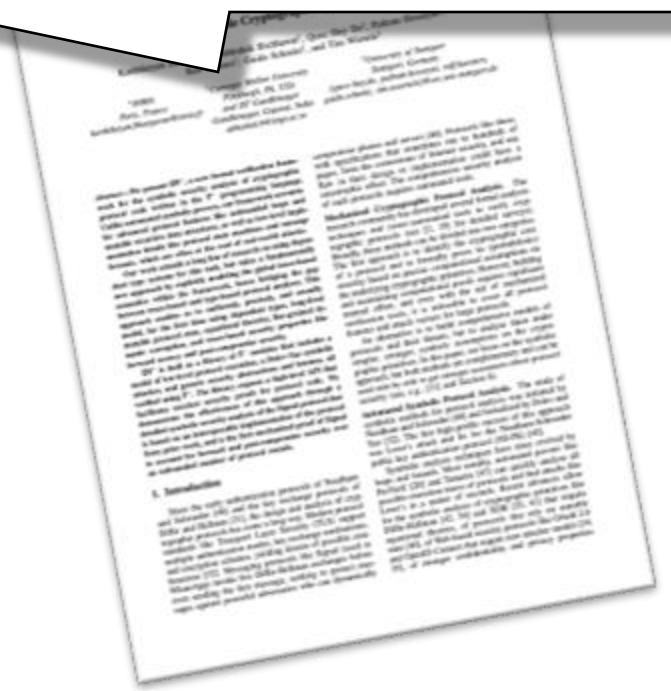


(“Tamarin” is also a monkey)

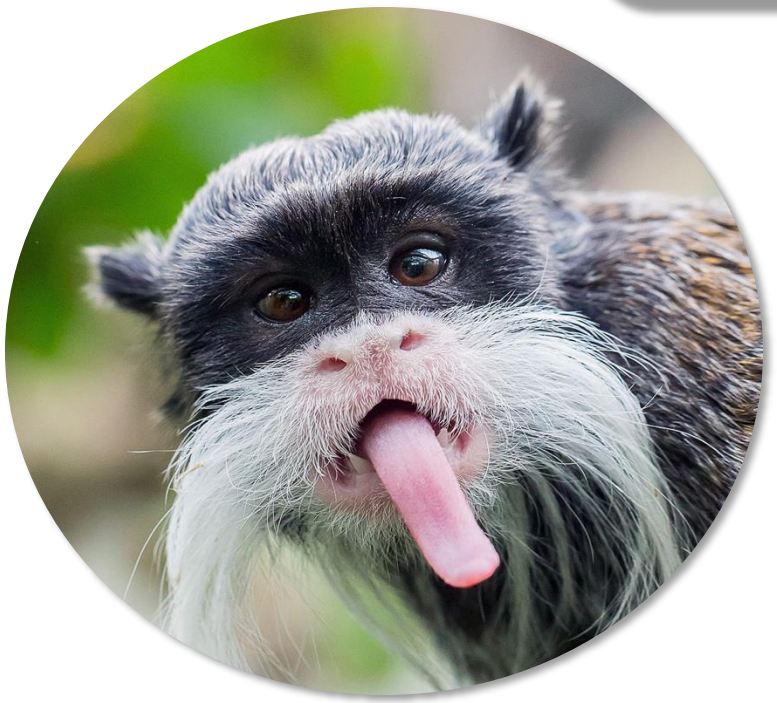
The Tamarin Prover

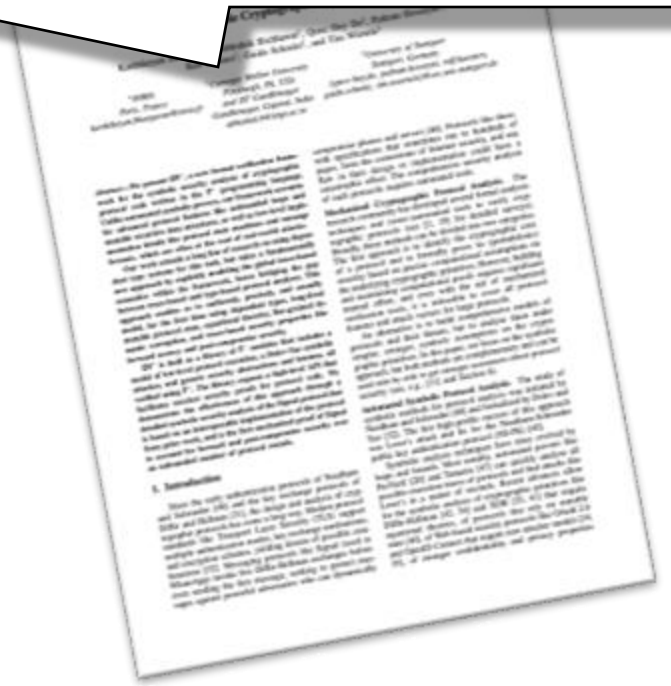
- a protocol verifier
- …ses constraint solving
- …operates in the symbolic model
- …has been used to verify TLS 1.3, 5G AKA, EMV

Unbounded (looping) protocols **like Signal** [...] are also **out of scope for symbolic provers**, without introducing artificial restrictions.



Unbounded (looping) protocols **like Signal** [...] are also **out of scope for symbolic provers**, without introducing artificial restrictions.





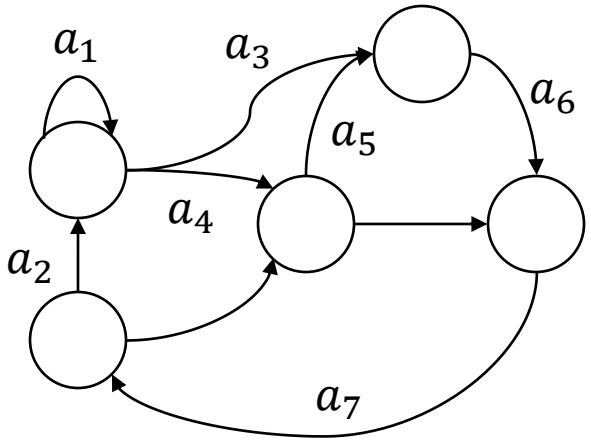
We prove iMessage secure – no abstractions*

We provide general proof methodology

The Tamarin Prover

Multiset-Rewriting Rules…

- Define labelled state transition system
- Model participant steps
- Model environment



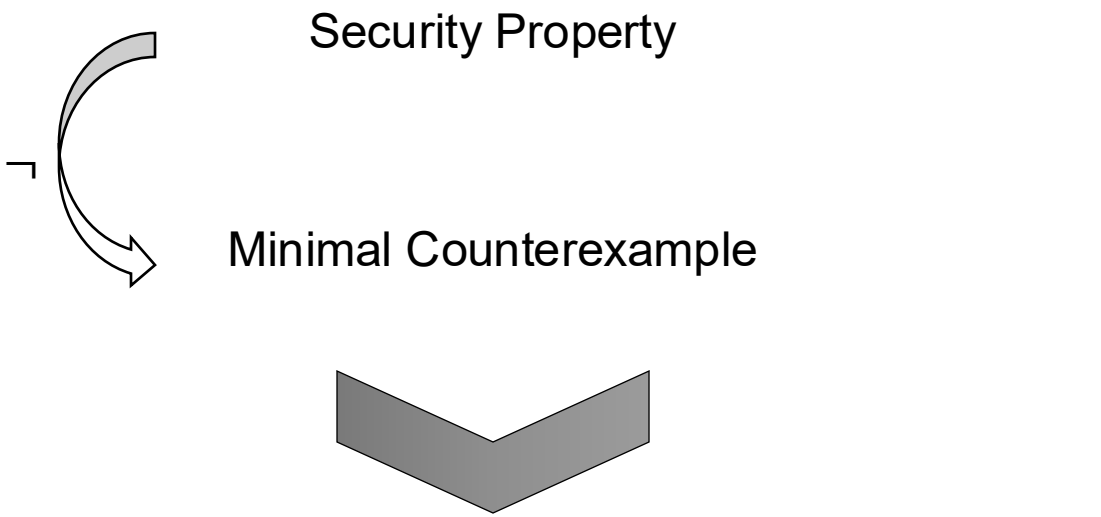
An Equational Theory…

- Defines cryptographic operations
- Defines adversary capabilities

```
verify(sign(m, sk), m, pk(sk)) = true

      sdec(senc(m, k), k) = m
```

The Tamarin Prover



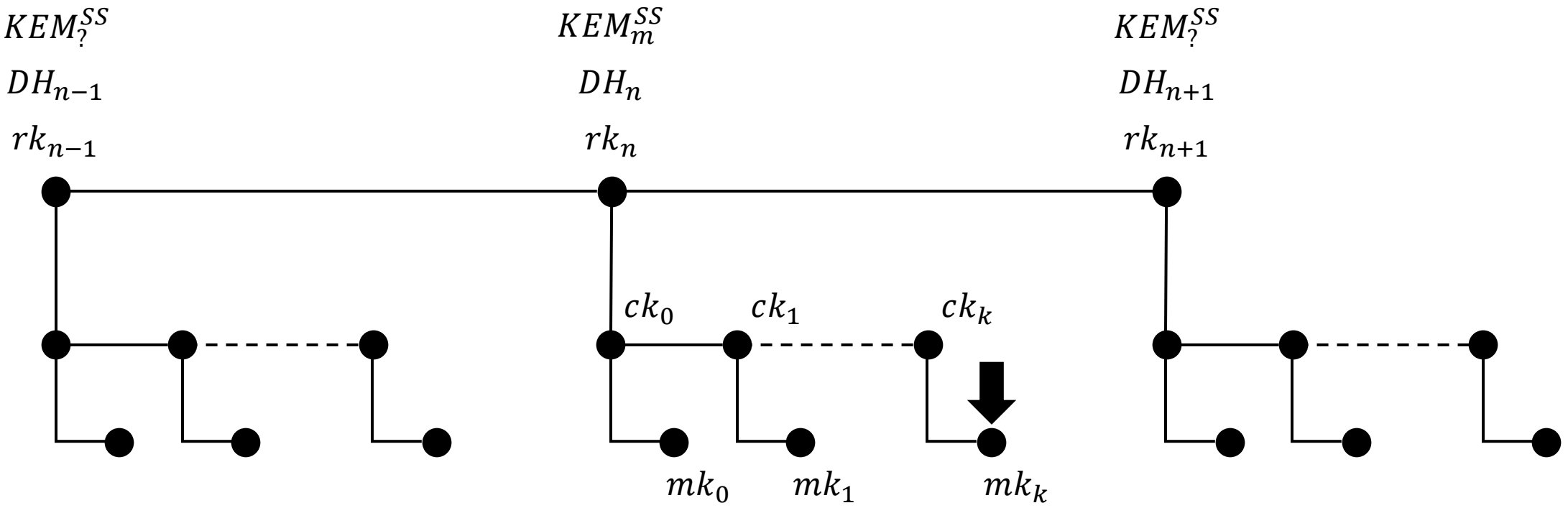
Formal Proofs

- Secrecy
  - Forward secrecy
  - Post-compromise security
- Agreement (authentication)
- Injective agreement (replay protection)

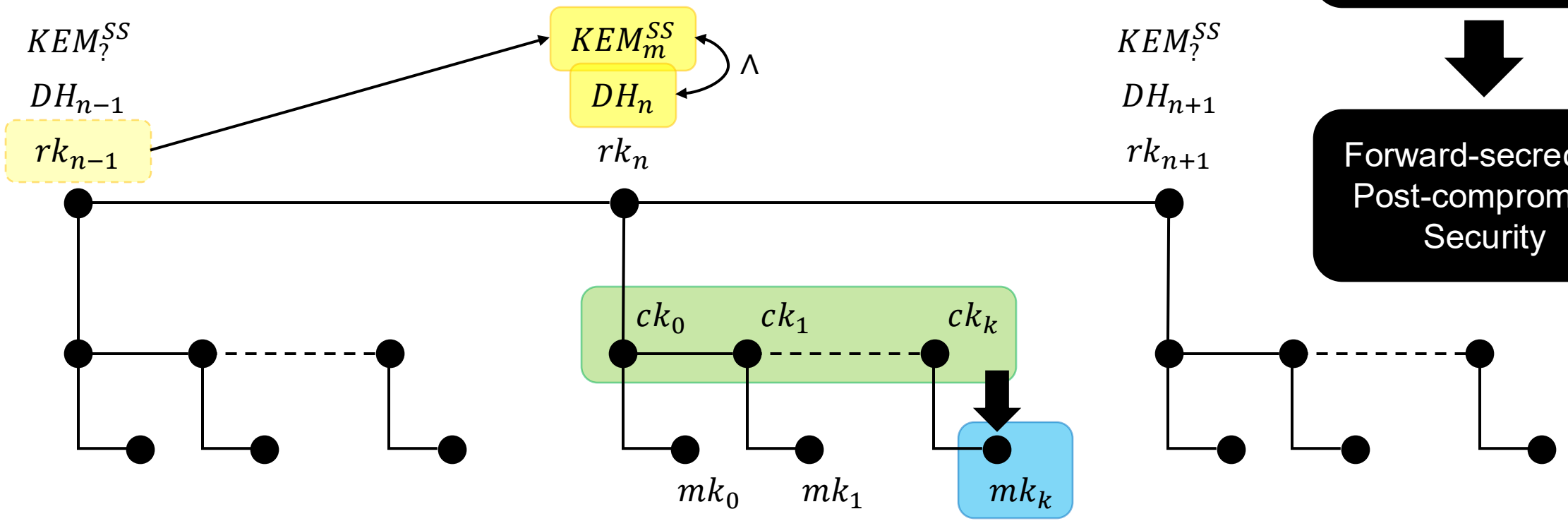
Formal Proofs

- **Secrecy**
  - **Forward secrecy**
  - **Post-compromise security**
- Agreement (authentication)
- Injective agreement (replay protection)

Secrecy


$KEM_?^{SS}$
DH_{n-1}
rk_{n-1}
KEM_m^{SS}
DH_n
rk_n
$KEM_?^{SS}$
DH_{n+1}
rk_{n+1}
ck_0
ck_1
ck_k
mk_0
mk_1
mk_k

Secrecy

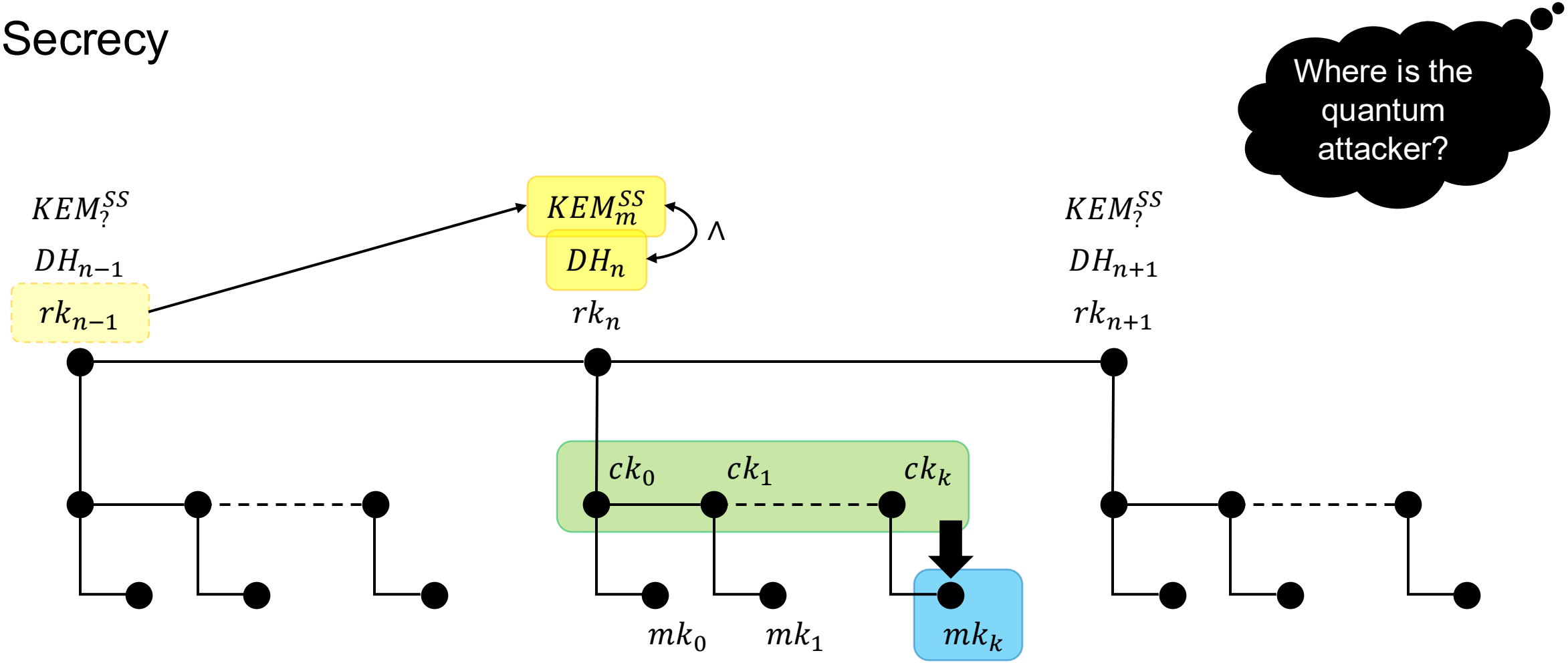


Adversary knows all other keys!

Forward-secrecy + Post-compromise Security

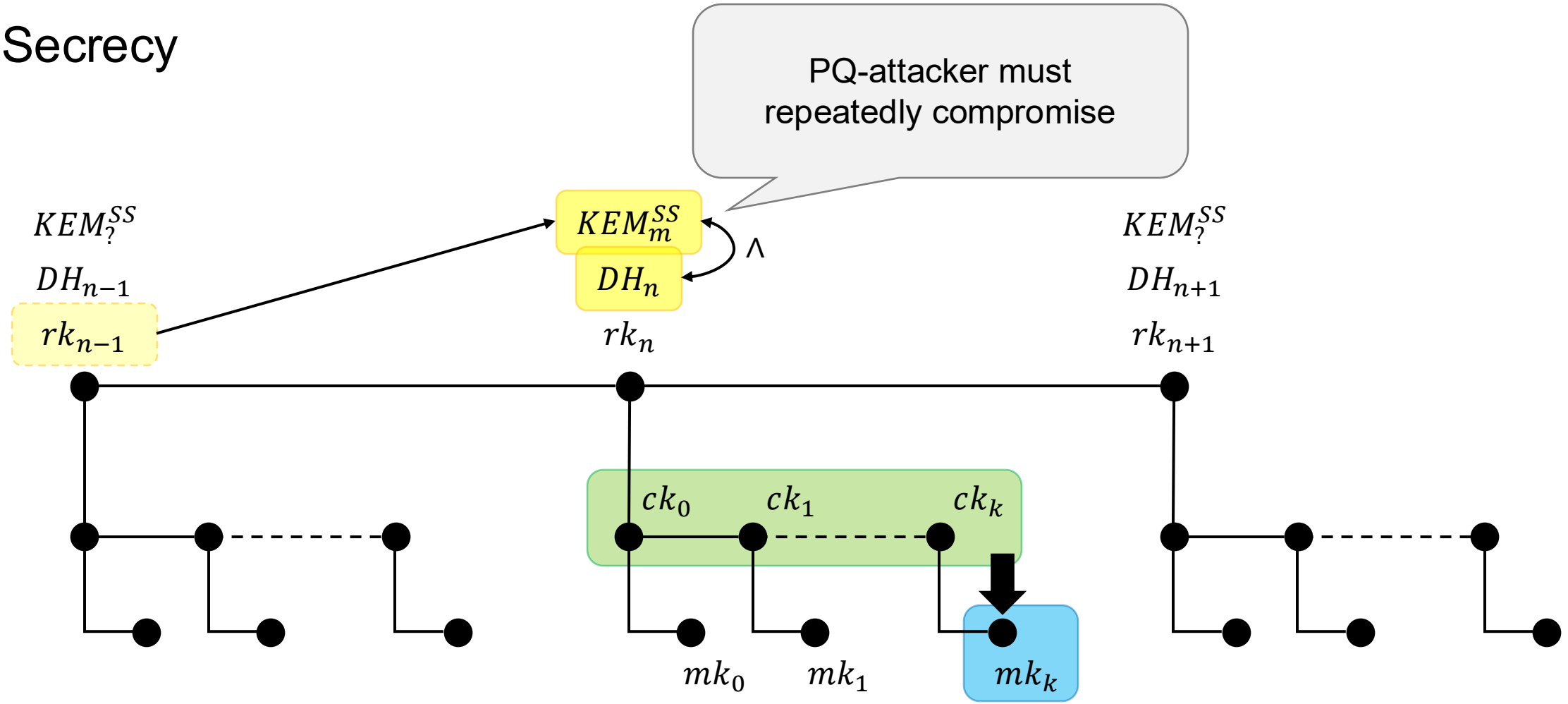
Messages are secret unless…  ∨  ∨ ∨ Signing key compromised

Secrecy



Messages are secret unless…  ∨  ∨ ∨ Signing key compromised

Secrecy



Messages are secret unless…  ∨  ∨ ∨ Signing key compromised

Proof Effort

- Proved 32 auxiliary lemmas
  - Checking all proofs takes ~2 days and up to 140 GB memory
- Estimate: 2.5 person months of work
  - Developed general proof methodology
  - We would be **much** quicker for other protocols now

Results

iMessage PQ3 is secure

- Formal security guarantees
- Refined specification

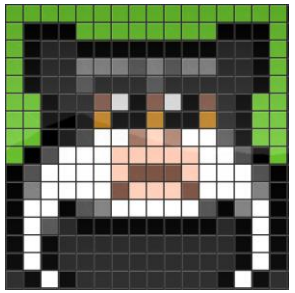
Tamarin can analyze complex protocols

- You should and can use it

Summary

We proved

- Secrecy
- Forward Secrecy
- Post-compromise Security
- Authentication
- Replay Protection

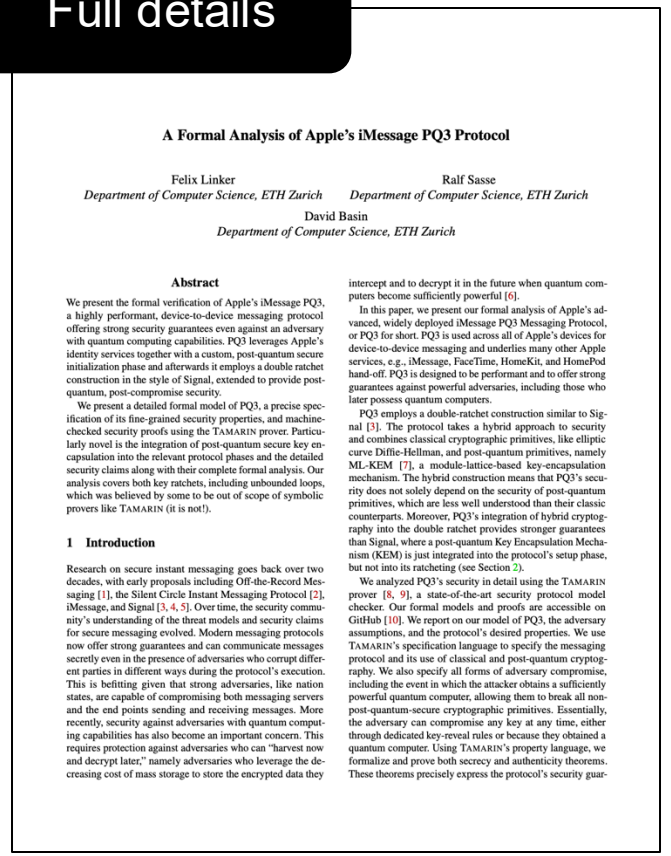


…using Tamarin

worked better than anticipated!

Tamarin can analyze complex protocols

Full details



A Formal Analysis of Apple's iMessage PQ3 Protocol

Felix Linker
Department of Computer Science, ETH Zurich

Ralf Sasse
Department of Computer Science, ETH Zurich

David Basin
Department of Computer Science, ETH Zurich

Abstract

We present the formal verification of Apple's iMessage PQ3, a highly performant, device-to-device messaging protocol offering strong security guarantees even against an adversary with quantum computing capabilities. PQ3 leverages Apple's identity services together with a custom, post-quantum secure initialization phase and afterwards it employs a double ratchet construction in the style of Signal, extended to provide post-quantum, post-compromise security.

We present a detailed formal model of PQ3, a precise specification of its fine-grained security properties, and machine-checked security proofs using the TAMARIN prover. Particularly novel is the integration of post-quantum secure key encapsulation into the relevant protocol phases and the detailed security claims along with their complete formal analysis. Our analysis covers both key ratchets, including unbounded loops, which was believed by some to be out of scope of symbolic provers like TAMARIN (it is not!).

1 Introduction

Research on secure instant messaging goes back over two decades, with early proposals including Off-the-Record Messaging [1], the Silent Circle Instant Messaging Protocol [2], iMessage, and Signal [3, 4, 5]. Over time, the security community's understanding of the threat models and security claims for secure messaging evolved. Modern messaging protocols now offer strong guarantees and can communicate messages secretly even in the presence of adversaries who corrupt different parties in different ways during the protocol's execution. This is befitting given that strong adversaries, like nation states, are capable of compromising both messaging servers and the end points sending and receiving messages. More recently, security against adversaries with quantum computing capabilities has also become an important concern. This requires protection against adversaries who can "harvest now and decrypt later," namely adversaries who leverage the decreasing cost of mass storage to store the encrypted data they intercept and to decrypt it in the future when quantum computers become sufficiently powerful [6].

In this paper, we present our formal analysis of Apple's advanced, widely deployed iMessage PQ3 Messaging Protocol, or PQ3 for short. PQ3 is used across all of Apple's devices for device-to-device messaging and underlies many other Apple services, e.g., iMessage, FaceTime, HomeKit, and HomePod hand-off. PQ3 is designed to be performant and to offer strong guarantees against powerful adversaries, including those who later possess quantum computers.

PQ3 employs a double-ratchet construction similar to Signal [3]. The protocol takes a hybrid approach to security and combines classical cryptographic primitives, like elliptic curve Diffie-Hellman, and post-quantum primitives, namely ML-KEM [7], a module-lattice-based key-encapsulation mechanism. The hybrid construction means that PQ3's security does not solely depend on the security of post-quantum primitives, which are less well understood than their classic counterparts. Moreover, PQ3's integration of hybrid cryptography into the double ratchet provides stronger guarantees than Signal, where a post-quantum Key Encapsulation Mechanism (KEM) is just integrated into the protocol's setup phase, but not into its ratcheting (see Section 2).

We analyzed PQ3's security in detail using the TAMARIN prover [8, 9], a state-of-the-art security protocol model checker. Our formal models and proofs are accessible on GitHub [10]. We report on our model of PQ3, the adversary assumptions, and the protocol's desired properties. We use TAMARIN's specification language to specify the messaging protocol and its use of classical and post-quantum cryptography. We also specify all forms of adversary compromise, including the event in which the attacker obtains a sufficiently powerful quantum computer, allowing them to break all non-post-quantum-secure cryptographic primitives. Essentially, the adversary can compromise any key at any time, either through dedicated key-reveal rules or because they obtained a quantum computer. Using TAMARIN's property language, we formalize and prove both secrecy and authenticity theorems. These theorems precisely express the protocol's security guar-

/usenixsecurity25/presentation/linker