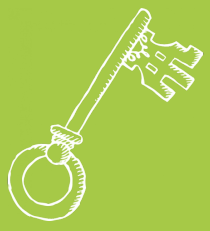


Masked PAKE Implementation using Mithril as a KEM

Advisor: **Selim Kirbiyik**

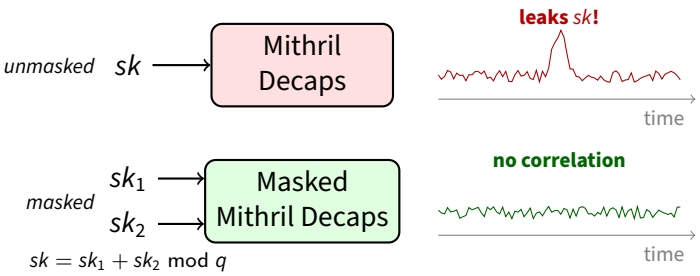
Motivation

Attackers can learn about a secret being computed by measuring the power it takes to compute a function. Hence, having masked implementations of algorithms is crucial. Password Authenticated Key Exchange protocols are useful in establishing more secure session keys before there is an authenticated channel available. Concrete use cases include wireless networks and identification cards.

In this topic, you will explore performant masked implementation of PAKE scheme using Mithril as the Key Encapsulation Mechanism. Mithril is a new KEM algorithm that is similar in construction to SABER and ML-KEM (formerly Kyber).

Goals and Tasks

- Understand Mithril KEM scheme
- Identify the vulnerable procedures
- Implement an efficient masked implementation



Abstract view of masked versus unmasked implementation.

Literature

- J. Renes et al.
  Radical Ring-LWR: Efficient Key Encapsulation and Signatures from Structured Rounding
  2026
- M. Green
  Let's Talk about PAKE
  2018
  blog . cryptographyengineering . com / 2018/10/19/lets-talk-about-pake/

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☑ CS ☑ ICE

Prerequisites

- Interest in secure implementations
- Programming (Cortex-M4 Assembly, C/C++, Python)

Advisor Contact

selim.kirbiyik@tugraz.at