



# MitM Cryptanalysis of QARMAv2

Advisor: **Simon Gerhalter**




## Motivation

QARMAv2 is a redesign of the tweakable block cipher QARMA. The aim was to increase the security margins and allow longer tweaks, while keeping the latency and area comparable.

For a round reduced version of QARMA there exists a Demirci-Selçuk MitM (DM-MitM) attack. DM-MitM is a powerful technique, especially when the length of the key is bigger than the state size. Since QARMAv2 is similar to QARMA in many aspects, the designers of QARMAv2 argue that this type of attack does not pose a threat to the full version of QARMAv2. However, no dedicated DM-MitM cryptanalysis exists.

The goal of this thesis is to perform DM-MitM cryptanalysis on QARMAv2 and find out if the claim of the designers holds.

## Goals and Tasks

-  Get familiar with DM-MitM and QARMA(v2)
-  Analyse the previous attack on QARMA
-  Adapt the attack to QARMAv2

## Literature

- > [Y. Liu et al.](#)  
Improved Cryptanalysis of Reduced-Version QARMA-64/128  
[IEEE Access 2020](#)
- > [R. Avanzi et al.](#)  
The QARMAv2 Family of Tweakable Block Ciphers  
[IACR Trans. Symmetric Cryptol. 2023](#)  
<https://doi.org/10.46586/tosc.v2023.i3.25-73>

## Courses & Deliverables

- Introduction to Scientific Working**  
Short report on background  
Short presentation
- Bachelor Project**  
Project code and documentation
- Bachelor's Thesis**  
Project code  
Thesis  
Final presentation

## Recommended if you're studying

- CS
- ICE
- SEM

## Prerequisites

- > Interest in Symmetric Cryptography

## Advisor Contact

[simon.gerhalter@iaik.tugraz.at](mailto:simon.gerhalter@iaik.tugraz.at)