



May 20, 2025

Statement of supervisor on

„On security of practical adaptor signatures“ by Bc. Berenika Richterová

The thesis studies adaptor signatures—a cryptographic primitive that “locks” a digital signature to the knowledge of a witness to some hard relation—with a focus on the two schemes most relevant to cryptocurrencies, Schnorr and ECDSA.

Chapter 1 revisits Non-Interactive Zero-Knowledge (NIZK) proofs for equality of discrete logarithms and provides a detailed presentation of the Chaum-Pedersen construction in the Random Oracle Model. Then the author illustrates how such NIZK proofs underpin payment-related protocols. Chapter 2 recaps existing Schnorr- and ECDSA-based adaptor signatures, reviews the “robust” security framework of Aumayr et al. (ASIACRYPT 2021) and identifies where that framework fails for real-world ECDSA deployments. In particular, the author presents an attack that undermines the assumed hardness of the relation when unrestricted pre-signing queries are allowed. Chapter 3 introduces relaxed security notions (existential unforgeability, witness extractability, pre-signature adaptability) that fit the practical adaptor scheme for positive ECDSA and bypass the attack from Chapter 2. It is shown that the scheme satisfies the new notions under standard assumptions. Chapter 4 compares the cost of Schnorr- and ECDSA-based designs and sketches how the new definitions could be extended to allow for analysing Discreet Log Contracts (DLCs) on Bitcoin. The thesis ends with a concise conclusion highlighting open questions, such as formal security of full DLC constructions.

The author presents the following original results:

1. Inadequacy of robust definitions for ECDSA-based adaptor signatures:

The author exemplifies a deficiency of the robust notions of Aumayr et al. when applied to practical ECDSA-based adaptor signature. It is shown that a malicious party can turn a pre-signing oracle into a fixed Diffie–Hellman oracle and recover the signer’s key in roughly 2^{93} group operations on the secp256k1 curve.

2. Relaxed security notions enabling proofs of security:

The author presents new definitions and proofs of security for positive ECDSA-based adaptor signatures. The new definitions restrict the adversary’s access just enough to restore the hardness of discrete logarithm while still plausibly capturing intended applications; the author proves the practical ECDSA-based adaptor signature secure w.r.t. the new definitions.

3. Comparison of efficiency for the known proposals:

The author gives a concrete efficiency comparison across three adaptor-signature variants (Tables 4.1–4.3).

Overall, the thesis addresses a major gap in security of practical adaptor signatures. The studied ECDSA-based adaptor signatures are the predominantly deployed variant in practice, yet there was no proof of security for these schemes. The attack and follow-up refinements of security demand a good grasp of elliptic-curve cryptography and cryptographic security reductions.

The text is written well. The exposition is clear, and the results are technically solid with detailed proofs. The thesis cites the relevant sources and clearly positions its results against Aumayr et al. and other related work. Overall, the work clearly meets the expected scientific standard for a master thesis.

I recommend that the thesis be accepted and graded “excellent”.

Mgr. Pavel Hubáček, Ph.D.