Chair of Applied Cryptography
Prof. Sebastian Faust

TECHNISCHE UNIVERSITÄT DARMSTADT

Master's thesis proposal

Formal treatment of Proof of Stake Wallets

In cryptocurrencies, it is crucial to securely store user's keys in order to protect user funds. Deterministic wallets is widely deployed as an essential tool for key management of cryptocurrency users. Usually deterministic wallets consists of two components. The public keys of the user are stored in a device which is most of the time online – this component is referred to as the *hot wallet*. While the secret keys are often stored in a device which mostly remains offline and referred as the *cold wallet*. Since reuse of public (secret) keys can lead to devastating attacks [Bit18], one of the key criteria of deterministic wallets is to ensure that freshly derived public (secret) keys are used for every payment. Such session public (secret) keys are derived via the deterministic key derivation algorithm run within the hot (cold) wallets.

Although such deterministic wallets have been prevalent since half a decade [Wik18], there have been almost no concrete security analysis of the same until last year [DFL19], where the authors presented a formalization of wallets and provided provable secure instantiations of deterministic wallets for a class of signature schemes with a certain rerandomizability property of the derived keys.

One inherent assumption in the design of the above mentioned deterministic wallet is that the underlying blockchain is based on a proof of work (PoW) based consensus algorithm [Nak09]. In such a PoW based consensus, parties, more precisely miners needs to solve a computational puzzle to mine the next block. Since PoW based blockchains require extensive amount of computational power, proof of stake (PoS) based consensus [Eth18] have been proposed as an alternative solution, where mining power corresponding to the amount of assets or 'staking keys' that a miner owns. In a PoS blockchain, every user is also a miner and needs to maintain two sets of keys - (1) payment keys which are similar to the PoW wallet (2) staking keys which are necessary to participate in the PoS consensus protocol. Protecting keys in a proof of stake wallet is even more crucial than its PoW wallet variant, since in such a wallet, loss of the staking keys can lead to a 51% attack that directly affects the underlying consensus. So it is not only harmful for the concerned user but also for the overall consensus.

Proof of stake wallets have recently been studied in a work [KKL], where the authors provide a formalization and some security analysis considering idealized signature schemes. However such a security analysis is not necessarily complete because it does not give concrete suggestions to the following question: Which class of signature schemes are practically suitable for such a PoS wallet and guarantee well defined security properties of the wallet?

The following main steps are planned as part of the thesis work:

1. Study the related work on proof of stake blockchain, particularly key management in proof of stake based blockchains.
2. Define a formal security model of proof of stake wallet, the security modeling of [DFL19] can be used as a reference.
3. Define security properties for a PoS wallet.
4. Provide provable secure instantiation of PoS Wallet using practically used signature schemes such as ECDSA, Schnorr or any other relevant variant.

Prerequisites:

- Strong background in cryptography, in particular provable security
- Some familiarity with cryptocurrencies is a plus
- good grades
- good working knowledge of written/oral English

If you are interested please send a short motivation 5-10 sentences and a transcript to the address given below.

Contact:

Poulami Das, S2|20, 315
poulami.das@tu-darmstadt.de

References

[Bit18] BitcoinExchangeGuide. CipherTrace Releases Report Exposing Close to $1 Billion Stolen in Crypto Hacks During 2018. `https://bitcoinexchangeguide.com/ciphertrace-releases-report-exposing-close-to-1-billion-stolen-in\_-crypto-hacks-during-2018/`, 2018.

[DFL19] Poulami Das, Sebastian Faust, and Julian Loss. A formal treatment of deterministic wallets. In *ACM SIGSAC Conference on Computer and Communications Security - CCS 2019*, pages 651–668. ACM, 2019.

[Eth18] Ethereum: Proof of Stake faqs (2018). `https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs`, 2018.

[KKL] Dimitris Karakostas, Aggelos Kiayias, and Mario Larangeira. Account management in proof of stake ledgers. In Clemente Galdi and Vladimir Kolesnikov, editors, *SCN 2020*.

[Nak09] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2009.

[Wik18] Bitcoin Wiki. BIP32 proposal. `https://en.bitcoin.it/wiki/BIP_0032`, 2018.