Seminar topics proposals

**1: HAWK: A Privacy-Preserving Smart Contract System**

**Introduction:** These days, along with blockchain technology, smart contracts have found intense interest in lots of practical applications. A smart contract is a mechanism involving digital assets and some parties, where the parties deposit assets into the contract and the contract redistributes the assets among the parties based on provisions of the smart contract and inputs of the parties.

Recently there have been valuable efforts to construct smart contract systems that can provide privacy-preserving payments and interconnections in the contracts. HAWK is one of decentralized smart contract systems that uses zk-SNARKs (zero-knowledge Succinct Non-interactive Arguments of Knowledge) to retain transactional privacy from the public’s view. Similar to privacy-preserving coins (e.g. Zerocash), HAWK does not store financial transactions in the clear on the blockchain, instead the system stores short (succinct) zero-knowledge proofs on the ledger.

The protocol of HAWK constructed from two main blocks, where one block is responsible for private money transfers and uses a variation of Zerocash (Zerocash is a known and efficient cryptocurrency that allows anonymous transactions), while the second part handles the required operations for a smart contract specified with HAWK.

**Task:** The task is to read, understand and present the article "HAWK: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts" available in [https://eprint.iacr.org/2015/675.pdf](https://eprint.iacr.org/2015/675.pdf).

**2: Private Proof-of-Stake Protocols**

**Introduction:** Bitcoin is the first well-known cryptocurrency where all transactions are linked together by public ledger. The key component in Bitcoin protocol (and many of the follow-up protocols) is the proof-of-work (PoW) puzzle solving. A miner can issue a new block only if it has solved a computationally difficult PoW challenge. The miner who finds the solution first, can issue the next block and she is rewarded in some coins. PoW protocols suffer from enormous energy consumption.

Proof-of-stake (PoS) protocols are one of the most promising alternative to the wasteful PoW protocols for consensus in distributed ledgers. In PoS protocols, individual parties have certain amount of stakes on the ledger (e.g. coins) and for deciding who will issue the next block, there is a randomized (but stake-based) leader election process. More stake a party has, more likely she will be elected as a leader for next block. During the leader election procedure, both the identity and the stake of stakeholders are disclosed which is incompatible with privacy-preserving cryptocurrencies such as Zerocash, Monero, etc.

Recently, Ganesh et al. proposed to add zero-knowledge proofs to the PoS protocols to guarantee the privacy of stakeholders; known as Private PoS (PPoS) protocols. They also presented a privacy-preserving version of a popular PoS protocol, Ouroboros Praos.

**Task:** The task is to read, understand and present the paper "Proof-of-Stake Protocols for Privacy-Aware Blockchains" which is going to be presented in Eurocrypt 2019, [https://eprint.iacr.org/2018/1105](https://eprint.iacr.org/2018/1105).