Seminar topics proposals

1: A subversion-resistant SNARK  
MSc or PhD level

Introduction: Non-Interactive Zero-Knowledge proofs (NIZKs) are a popular and powerful building block in designing various cryptographic protocols including verifiable computation systems, anonymous credentials, signature of knowledges, privacy-preserving cryptocurrencies (such as Zerocoin, Zcash) and multi-party computation. Due to efficiency reasons, recently Zero Knowledge Succinct Non-Interactive ARguments of Knowledge (zk-SNARKs) have greatly accelerated to deploy in real practical systems.

A negative point regard to zk-SNARKs is that they need a one-time setup phase which needs to be done by a trusted third party which is not desired in some cases. Recently there was a question of what happens when the CRS (Common Reference String) has been subverted? More precisely, can we still guaranty soundness and zero-knowledge if CRS elements are subverted?

In ASIACRYPT 2016, Bellare, Fuchsbauer and Scafuro showed the first negative and positive results in this direction, proving that it is impossible to achieve subversion soundness and subversion zero knowledge at the same time. In ASIACRYPT 2017, Abdolmaleki et al. showed how to make Groths zk-SNARK (the state-of-the-art one) for Circuit-SAT from EUROCRYPT 2016 computationally knowledge-sound and perfectly composable subversion ZK with minimal changes.

Task: The task is to read, understand and present the article "A subversion-resistant SNARK" from ASIACRYPT 2017 [ABLZ17].

2: Zcash: Decentralized Anonymous Payments from Bitcoin  
MSc or PhD level

Introduction: Bitcoin is the first well-known cryptocurrency where all transactions are linked together by public ledger. However payments are conducted between pseudonyms, but it is shown that Bitcoin cannot offer strong confidentiality and privacy and it is possible to link all transaction of a target user and violate his/her privacy. To deal with such privacy concerns, several solutions have been proposed which one of those solutions is Zcash. More precisely, Zcash uses zero-knowledge Succinct ARgument of Knowledges (zk-SNARKs) to provide much more anonymous transactions by hiding payment’s origin, destination and the amount.

Task: The task is to read, understand the procedure of construing Zcash and present the article "Zcash: Decentralized Anonymous Payments from Bitcoin" from IEEE Security and Privacy Symposium 2014, [BCGG+14].

3: An Empirical Analysis of Anonymity in Zcash  
BSc, MSc or PhD level

Introduction: As discussed in second topic, Zcash is a cryptocurrency designed to provide anonymous transactions by hiding payment’s origin, destination and the amount of transaction. In a recent empirical research, Kappos et al. [USENIXSECURITY18] tested the anonymity of deployed version of Zcash. They evaluate anonymity of Zcashs transactions from different point of views including its transparent transactions to the interactions with and within its main privacy feature, a shielded pool that acts as the anonymity set for users wishing to spend coins privately. Based on their result, it can be concluded that in some cases it is possible to shrink Zcash’s anonymity set considerably by developing some heuristics based on identifiable patterns of usage.

Task: The task is to read, and give an overview form their analysis given in the article "An Empirical Analysis of Anonymity in Zcash" from proceedings of the 27th USENIX Security Symposium, [KYMM18].