The Chair of Applied Cryptography is looking for student assistants for the following exciting projects!

**Brief background on wallets:** Payments over a cryptocurrency (such as Bitcoin or Ethereum), usually involve signing of a transaction using the sender’s secret key. On the other hand, the recipient of the payment publishes his/her own public key to receive the payment from the sender. Getting control over the secret key may lead to a complete theft of the money. So, it is essential to provide secure key management.

We offer the following two projects in the field of wallets:

1) **Implementation of a threshold wallet:** As the wallet contains the secret keys of the user, it may become an attractive target for attackers. One can solve this problem using threshold wallets. The key idea behind a threshold wallet is to split the wallet into two parts and store secret key shares in each of the respective parts. Another key difference of such wallets from the non-threshold variant is that now the signature will be generated using the secret key shares instead of using a single secret key. In this project, we want to implement and evaluate a threshold signature scheme to realize threshold wallets.

2) **Implementation of a wallet model:** Another way of securing a wallet is by splitting the wallet into two parts: a hot wallet and a cold wallet. A hot wallet is usually a device connected to the internet. For example, it can be thought of as a software in a mobile phone, where the public information related to payment transactions are stored. A cold wallet on the other hand is a device which is kept offline most of the time, storing the corresponding secret key related information. Hence, the cold wallet only needs to connect to the internet when the user wants to make a payment. The goal of this project is then to implement and evaluate such a model of hot/cold wallet which has been developed in our group.

Prerequisites:

- Good programming skills
- Background in cryptography

Contact for application/question:
poulami.das@tu-darmstadt.de
andreas.erwig@tu-darmstadt.de