Chair of Applied Cryptography
Prof. Sebastian Faust

TECHNISCHE UNIVERSITÄT DARMSTADT

Master's thesis proposal

Security Analysis of Chaum's eCash Protocol

Cryptocurrencies attracted attention with the emerge of Bitcoin in 2009 [5]. However, David Chaum came up with the idea of an electronic payment system already in 1983 [2]. His work includes some fundamental concepts like double spending protection and user anonymity still important for nowadays cryptocurrencies.

Although the eCash payment system from Chaum was deployed by several banks in the U.S. and Europe in the 1990s, a detailed description and cryptocraphic security analysis are still missing. There are some follow-up works by Chaum et al. [3], Schoenmakers [6], and Dreier et al. [4] but none of them includes a cryptographic proof of the eCash scheme. The main goal of this thesis is to fill this gap. Therefore, a detailed description of the eCash protocol, the design of a security model, and a security analysis of Chaum's protocol in this model should be part of the thesis.

There exist eCash systems that are proven to be secure, for example the one proposed by Brands [1]. Even if the security model from [1] cannot be used for the security analysis of Chaum's eCash protocol directly, it can serve as an inspiration.

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

1. Acquire a deep understanding of anonymous electronic payment systems and Chaum's eCash protocol in particular.
2. Compare Chaum's protocol with other existing electronic payment schemes (e.g. Brands).
3. Design a security model for anonymous electronic payment systems.
4. Formalize Chaum's eCash protocol and analyze its security within the previously designed model.

Prerequisites:

- interest in cryptocurrencies and provable security
- background in cryptography
- 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:

Benjamin Schlosser, S4|14, 3.2.17
benjamin.schlosser@crisp-da.de

References

[1] S. Brands. An efficient off-line electronic cash system based on the representation problem. Technical report, CWI Technical Report CS-R9323, 1993.

[2] D. Chaum. Blind signatures for untraceable payments. In *Advances in cryptology*, pages 199–203. Springer, 1983.

[3] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In *Conference on the Theory and Application of Cryptography*, pages 319–327. Springer, 1988.

[4] J. Dreier, A. Kassem, and P. Lafourcade. Formal analysis of e-cash protocols. In *2015 12th International Joint Conference on e-Business and Telecommunications (ICETE)*, volume 4, pages 65–75. IEEE, 2015.

[5] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2009.

[6] B. Schoenmakers. Basic security of the ecashtm payment system. *Course on Computer Security and Industrial Cryptography, LNCS*, 1528:338–352, 1997.