

Blind signatures

Master's (or Bachelor's) Thesis

A blind signature is an interactive signing protocol between a user and a signer, such that: At the end of the protocol, the user gets a signature on its input message, while the signer learns nothing about that message. Moreover, the signature satisfies a weakened notion of unforgeability, namely, one-more unforgeability, i.e., it is impossible to produce more signatures than the number of (successful) blind signing interactions.

Blind signatures are an important primitive for privacy-preserving technologies. For example, by signing a random serial number, one already obtains a type of E-Cash or Privacy-Pass-like protocol. Moreover, blind signatures are closely related to (one-show) anonymous credentials, but are comparatively inflexible: In many situations, one needs to restrict the messages to satisfy certain guarantees modelled as satisfying a predicate $\phi(m) = 1$, but the signer must not learn anything more about m except $\phi(m) = 1$. This has recently been formalized as predicate blindness [FW24].

Another weakness of most efficient blind signatures, with the exception of pairing-based constructions, is that their security requires the programmable random oracle model (ROM). This is often inherited from the underlying signature schemes.

Scope of the work

This is not a specific thesis topic, but a general direction. Some concrete directions for this work are as follows:

- Survey and relate existing security notions for blind signatures.
- Modify the construction of [KR25] (or another candidate) to achieve stronger security or new, e.g., security in the non-programmable ROM or predicate blindness.
- Prove stronger security guarantees than known for some existing schemes, e.g. [KR25]. Or prove the impossibility that.

The thesis topic need not be restricted to the above questions. Any suitable question related to blind signatures is of interest.

Requirements

Following prior knowledge is helpful for the bachelor's thesis.¹

- Theoretical foundations of cryptography, provable security and security reductions are essential.
- Knowledge of Σ -protocols is very helpful, see [Dam10] or [BS23, Ch. 19].

Given advanced background knowledge from lectures or seminars, this topic can serve as a challenging Bachelor's thesis.

Contact

In case of interest or for further information, please contact Michael Kloß, michael.klooss@kit.edu.

¹It is customary to *cite the published versions* but **read the full version** of conference publications, found e.g., directly at the Cryptology ePrint Archive, via dblp, or other search engines. The shortened conference versions can be hard to follow.

References

- [BS23] Dan Boneh and Victor Shoup. *A Graduate Course in Applied Cryptography*. 2023. URL: <https://toc.cryptobook.us/>.
- [Dam10] Ivan Damgård. *On Σ -protocols*. 2010. URL: <https://cs.au.dk/~ivan/Sigma.pdf>.
- [FW24] Georg Fuchsbauer and Mathias Wolf. “Concurrently Secure Blind Schnorr Signatures”. In: 2024, pp. 124–160. DOI: 10.1007/978-3-031-58723-8_5.
- [KR25] Michael Kloöß and Michael Reichle. “Blind Signatures from Proofs of Inequality”. In: 2025, pp. 157–189. DOI: 10.1007/978-3-032-01887-8_6.