Black-box accumulation (BBA) is a building block allowing a privacy-preserving implementation of “point collection” and “redemption”, which can be used to implement certain forms of mobile payments, incentive systems (e.g. loyalty programs) and the like. It was first introduced in [JR16], and a line of work [Har+17; Hof+20] improved the security guarantees and/or efficiency of such schemes. The works [Blö+19; Bob+20] generalize the setting to updatable anonymous credentials (UAC), while also extending the security guarantees. An anonymous credential can be seen as a digital identification card which protects the privacy of its owner. It allows proving that the credential satisfies a policy, e.g. that the owner is older than 65, without revealing additional information. Updatability allows to update an attribute, for example a stored value, in an interaction. Naive implementations, such as showing/issuing a plain signature on the data, are very harmful to privacy.

Scope of the work

The first lattice-based BBA scheme is BABL [Fal+21]; it generally follows the blueprint from its group-based counterparts [JR16; Har+17; Hof+20; Blö+19], but requires some adaptions. The main objective of this thesis is to investigate possible efficiency improvements of lattice-based BBA/UAC constructions by using (1) ring- or module-LWE/SIS assumptions and (2) recent advances in efficient lattice-based zero-knowledge proofs and oblivious resp. blind signatures.

As a first step, familiarity with the general template of BBA (and UAC schemes) is important, see [Har+17; Hof+20] for BBA, and [Blö+19; Bob+20] for UAC. The BABL scheme from [Fal+21] is an example of how to adapt BBA to the lattice setting. A useful introduction and survey for lattices-based cryptography is [Pei16]. Following works can serve as starting points for the (recently improved) lattice primitives:

- Lattice-based ZK: The state-of-the-art protocol is [LNP22]. Previously, the works [BLS19; Yan+19] were common choices. Familiarity with the commitment scheme of [Bau+18] helps to comprehend these works.
- Lattice-based signatures with efficient protocols: The works [Agr+21; JRS22; LNP22a; PK22] offer forms of (partially) blind or oblivious signature schemes. However, other useful works or approaches may exist.

The goals for the thesis are as follows:

1. Get familiar with BBA/UAC (and BABL for the lattice setting) and do a literature search for efficient suitable building blocks (from recent advances in lattice-based primitives).
2. Employ these lattice-based primitives to construct a more efficient, provably secure BBA scheme and estimate its efficiency (computation and communication).
3. Use ring- or module-LWE/SIS-based primitives to further improve upon BABL which builds on plain LWE/SIS.
4. Optional: Extend the scheme with desirable features from the UAC setting, such as tracing, blacklisting, and so on. Define and prove security of these modifications.
5. Optional: Implement a prototype of this scheme.

To find open access and/or full versions of the cited papers, use dblp.

Requirements

Following prior knowledge is helpful for the master’s thesis:

- Good familiarity and knowledge of basic cryptography, including zero-knowledge and the simulation paradigm for real-ideal notions of security and privacy. Familiarity with Σ-protocols is helpful.
- Familiarity with lattice-based cryptography from seminars or otherwise is very useful.

Please take into account that learning lattice-based cryptography imposes a steep learning curve on this topic.

Contact

In case of interest or for further information, please contact Laurin Benz, laurin.benz@kit.edu and Michael Kloß, michael.klooss@kit.edu.
References


