Assumptions in Groups of Hidden Order

Bachelor’s or Master’s Thesis

Groups of hidden order, also called groups of unknown order (GUO) are cryptographic groups where the computation of the group order is supposedly hard. This alone is often insufficient, and further assumptions are made on top of this. The prime example of a GUOs are RSA groups: Factorization is equivalent to computing (a multiple of) the group order. Yet, most applications additionally require the RSA assumption, which is not known to be equivalent to factoring. The power of GUOs comes from their ability enable arguing (homomorphically) over the integers. For example, the map \( H_N: \mathbb{Z} \to \mathbb{Z}_N, \ H(m) = g^m \) is a collision-resistant homomorphic hash function for integers. That is \( H(x + y) = H(x) \cdot H(y) \). Homomorphic primitives are a powerful tool for many constructions.

While RSA groups (or generalizations, such as Paillier or Damgård–Jurik) satisfy almost all plausible security properties of interest, they have an important drawback in many applications, in particular zero-knowledge proofs. When using them as part of a common reference string, they require trusted setup. Untrusted setup, i.e., simply interpreting any random string as group description and/or group element, is much preferable since it is easier to obtain in practice. An alternative to RSA groups are class groups of imaginary quadratic orders. They can have transparent setup and presumably, their group order is also hard to compute. However, only weaker forms of the RSA assumption can possibly hold, since it is easy to compute square roots.

Scope of the work

The thesis should take a closer look at groups of hidden order, assumptions used in GUOs and their relations. This can be done from a general point of view, but class groups of imaginary quadratic orders are of particular interest. Related papers are [DF02, CPPT17]. Some basic questions are:

1. Construct a generic group model (GGM)\[Sho97; DK02; Mau05; LR06\] which captures GUOs where, e.g., \( \epsilon \)-th roots, can be efficiently computed. Prove that common assumptions hold in this model. Use [MPZ20, Zha22] to put the modelling in perspective.
2. Prove security of the assumptions in [Cou+22, Appendix A.3] in the generic model. Show that Lemma A.13 (4]) holds in the generic model without assuming \( C(k) \)-roughness [DF02].
3. Extend the setting and security to attacks with preprocessing, see [CK18].

Another (much harder, less clear) direction of interest are possible implications or distinctions between assumption due to the (im)possibility of invertible sampling.

1. Investigate the effects of (im)possibility of invertible sampling and the (im)possibility of modelling this generically.
2. Investigate whether invertible sampling could be possible in class groups of imaginary quadratic orders. (This requires a strong mathematical background, may be very hard, and you will be on your own.)

To find open access (full) versions of the cited papers, use dblp or academic search engines.

Requirements

Following prior knowledge is helpful for the bachelor’s or master’s thesis.

- This topic is “more mathematical”. Good mathematical understanding will be helpful.

Contact

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

References


