Hello everyone!

Shashank Agrawal and myself (Srini Raghuraman) would like to would like to share a new result on key-value commitments that we published in Asiacrypt recently (ia.cr/2020/1161). The talk given at the conference describing the construction can be found here: https://bit.ly/3w2GFCf.

The details of the construction can be found in the paper linked above, with the concrete description, appearing on page 22, also reproduced here for ease.

[

Screen Shot 2021-06-07 at 1.50.08 PM

986×1402 171 KB

](https://ethresear.ch/uploads/default/original/2X/3/3ad1d82b80b9c690581302a341b5a9a214995b8b.png)

Our commitment scheme KVaC (pronounced 'quack') allows one to commit to any number of key-value pairs and prove efficiently that a certain pair(s) is contained in the commitment. In particular, the commitment and the proofs consist of just two and three group elements respectively (in groups of unknown order like RSA/class groups). Verifying and updating proofs involves just a few group exponentiations, and so does additive updates to values.

We believe that KVaC could be a very good commitment scheme for building stateless clients. We found out that Verkle tries with Kate commitments are being considered for this purpose, so here we compare the two.

KVaC vs KZG (Kate) commitments

Similarities

- Both have very short commitments and proofs.
- Both support short multiproofs too: one can prove that the commitment contains several values with a proof whose size is the same as the one for a single value.

Pros of KVaC

- Kate relies on a trusted setup while KVaC doesn't (if class groups are used). In Kate, the size of trusted parameters limits the number of values that could be committed.
- KVaC is a key-value commitment, a more general primitive than vector commitments. So KVaC could enable more use-cases than Kate.
- In KVaC, inserting new key-value pairs or updating the value of an existing pair is very efficient (just a few group operations in either case). The cost of these operations in Kate is not clear.

Cons of KVaC

- KVaC operates in groups of unknown order while Kate is defined in elliptic-curve groups. So group operations will be faster in Kate and the elements will be shorter. (However, verification in Kate involves pairings which tend to be expensive.)
- Commitment and proofs in Kate consist of just one group element whereas they consist of two and three group elements, respectively, in KVaC.

Merkle Trees and Commitments

KVaC could be used in a Merkle Tree like fashion just as Kate commitments. In other words, KVaC could be a replacement for Kate in Verkle Tries. In particular, just as proofs for different commitments could be combined in a clever way for Kate, one could also combine proofs from different KVaC commitments to produce a short proof for all the values.

We would be happy to discuss more! Looking forward to many conversations on this