THAIS IDALINO, University of Ottawa

Efficient Unbounded Fault-Tolerant Aggregate Signatures Using Nested Cover-Free Families

Several applications deal with a large amount of data and digital signatures, such as outsourced databases, secure logging, sensor networks, etc. These applications require a way of saving on storage and communication, as well as a fast mechanism for verifying the signatures. We can solve these problems by using aggregate signature schemes, which combine all signatures into one. However, if at least one of the signatures is invalid, the entire aggregate is invalidated.

A fault-tolerant aggregate signature scheme is important for scenarios where we still want to identify the valid signatures and have the benefits of aggregation. This can be done by using d-cover-free families (d-CFFs) [1]. Given a bound d on the number of invalid signatures, the scheme can determine which signatures are invalid and guarantees a moderate increase on the size of the aggregate signature when there is an upper bound on the number n of signatures to be aggregated. However, for the case of unbounded n the constructions provided had a constant compression ratio, i.e. the signature size grew linearly with n. We propose a solution to the unbounded scheme with increasing compression ratio for every d, by proposing what we call a *nested family* of d-CFFs [2]. In particular, for $d = 1$ the compression ratio meets the information theoretical bound.

[1] Hartung, G., Kaidel, B., Koch, A., Koch, J., Rupp, A.: "Fault-tolerant aggregate signatures". In: PKC 2016.

[2] Idalino T. B., Moura L. "Efficient Unbounded Fault-Tolerant Aggregate Signatures Using Nested Cover-Free Families". IWOCA 2018.