DKGnote

lu562

June 2017

1.Synchronous vs asynchronous:

Synchronous: time bounded

Asynchronous: number and type of message.

Deciding time bounds is a difficult problem. As klong as there is a time bound, a real-world adversary with knowledge of any time bounds used, can always slow dowm the protocols by delaying its messages to the verge of the time bounds.

2. weak synchronous assumption to provide liveness.

3.question: how to get N¿=3t+2f+1.

4.we also need to bound the number of crashes by a function d() otherwise the protocol execution time will be unbounded.

5.protocol statistics,uniformly bounded by T(k).

6.homomorphic commitments:

Two forms of commitments: Dlog commitment and Pedersen commitment. Dlog commitment: computational security unconditional share integrity. Pederson commitment: unconditional security computational intefrity under DLog assumtiom.(Why)

7.DKG:

Correctness cs weak correctness: uniformly randomness.

8.adaptive adversary vs static adversary.

9.AVSS and HybridVSS use bivariate polynomials as they guarantee that the interpolated polunomials are of degree t or less.

6/9/2017

hybridDKG

agreement in asynchronous system is difficult. It is difficult to differentiate between slow node and faulty node.

Use signature as a kind of proof.

How to deal with view change?

Use $\tilde{Q}$ and $\bar{Q}$ to make sure the same set is used across different views ! this is important.

Result of Hybrid DKG is not uniformly random because of Dlog. We can use Ped commitment instead.

6/10/2017

1.DKG

liveness: based on the liveness of reliable broadcast.

agreement: when everything is fine,according to agreeement property of reliable broadcast,if one honest node completes the protocol then all honest finally up nodes will eventually complete the protocol.If there is a view change,$\bar{Q}$ and$\bar{M}$ can make sure all nodes complete a reliable broadcast with the same $\bar{Q}$

wC: one point: Lagrange interpolation is homomorphic over addition.

wS:At the end of HybridDKG the adversary does not know at least one of the t + 1 shared secrets and as a result adversary cannot compute s.

Efficiency.

2.Uniform randomness of secret:

Result of Hybrid DKG is not uniformly random, which is due to using only Dlog commitments.

3.reliable broadcast:

a useful blog:https://misfra.me/2015/09/22/reliable-broadcast/

a note:https://people.cs.umass.edu/ arun/cs677/notes/Consensus.pdf