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.

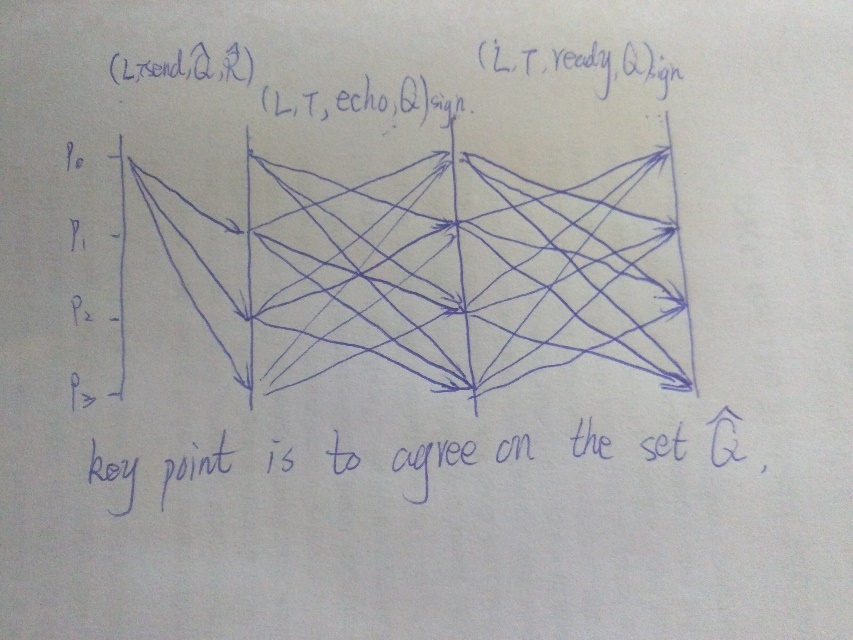
9.AVSS and HybridVSS use bivariate polynomials as they guarantee that the interpolated polunomials are of degree t or less.

6/9/2017

1. 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 and to make sure the same set is used across different views ! this is important.

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