NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Sandip Chakraborty

Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 40: Collective Signing (CoSi)

CONCEPTS COVERED

- Collective Signing
- Schnorr Multisignature
- PBFT as Collective Signing

KEYWORDS

- CoSi
- Multisignature

Collective Signing

- Method to protect “authorities and their clients” from undetected misuse or exploits

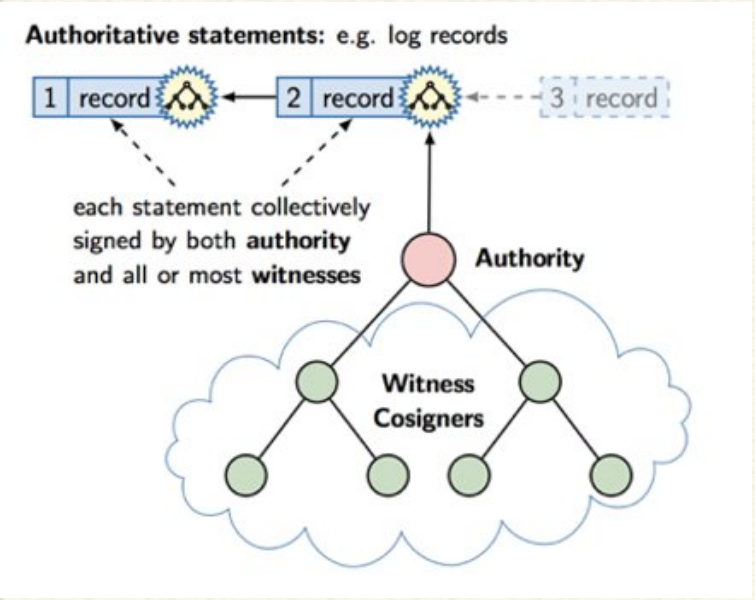
- A **scalable witness cosigning protocol** ensuring that every authoritative statement is validated and publicly logged by a diverse group of witnesses before any client accepts it

Syta, Ewa, *et al*. "**Keeping authorities "honest or bust" with decentralized witness cosigning**" *2016 IEEE Symposium on Security and Privacy (SP)*, 2016.

Collective Signing

- A statement *S* collectively signed by *W* witnesses assures clients that *S* has been seen, and not immediately found erroneous, by those *W* observers.

CoSi Architecture



- The leader organizes the witnesses in a tree structure – a scalable way of aggregating signatures coming from the children
- Three rounds of PBFT (pre-prepare, prepare and commit) can be simulated using two rounds of CoSi protocol

Schnorr Multisignature

- The basic CoSi protocol uses **Schnorr multisignatures**, that rely on a group *G* of prime order
  - *Discrete logarithmic problem is believed to be hard*

Schnorr Multisignature

- **Key Generation:**
  - Let G be a group of prime order r. Let g be a generator of G.
  - Select a random integer x in the interval $[0, r-1]$. x is the private key and g^x is the public key.
  - N signers with individual private keys $x_1, x_2, \ldots, x_N$, and the corresponding public keys $g^{x_1}, g^{x_2}, \ldots, g^{x_N}$

Schnorr Multisignature

- **Signing:**
  - Each signer picks up the random secret v_i, generates $V_i = g^{v_i}$
  - The leader collects all such V_i, aggregates them $V = \prod V_i$, and uses a hash function to compute a collective challenge $c = H(V||S)$. This challenge is forwarded to all the signers.
  - The signers send the response $r_i = v_i - cx_i$. The leader computes the aggregated as $r = \sum r_i$. The signature is (c, r).

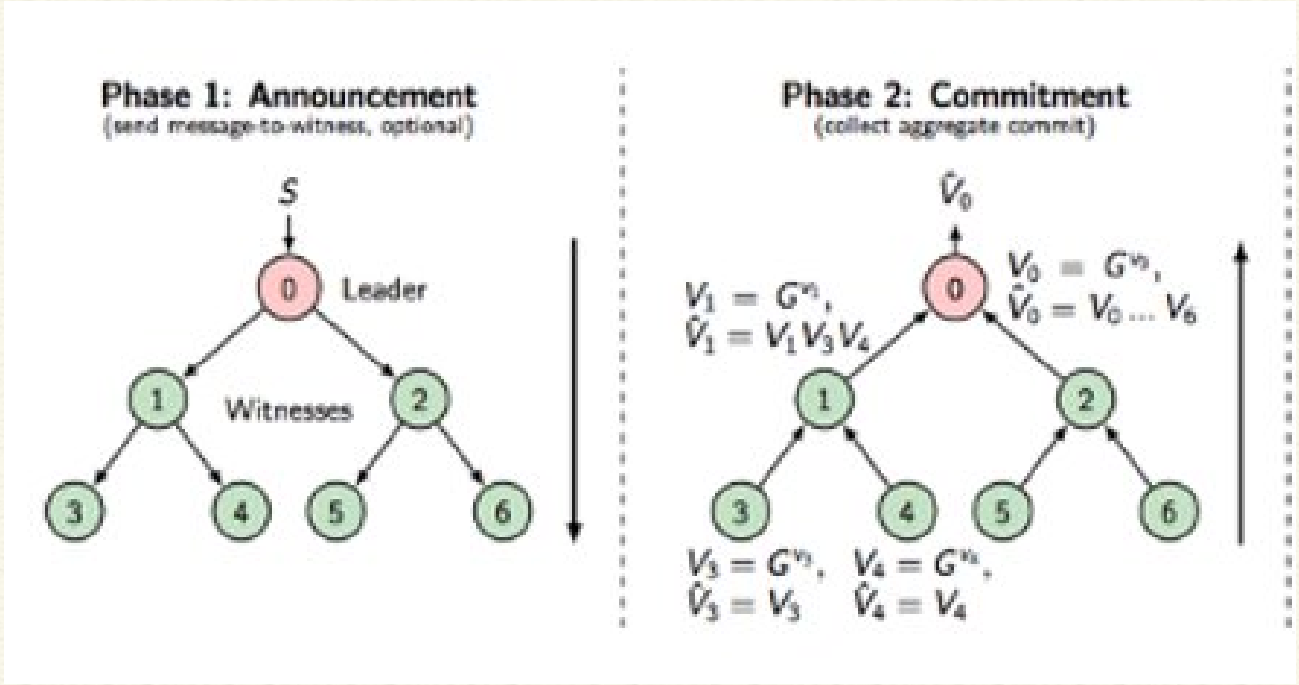
Schnorr Multisignature

- **Verification:**
  - The verification key is $y = \prod g^{x_i}$
  - The signature is (c, r), where $c = H(V||S)$ and $r = \sum r_i$
  - Let $V_v = g^r y^c$
  - Let $r_v = H(V_v||S)$
  - If $r_v = r$, then the signature is verified

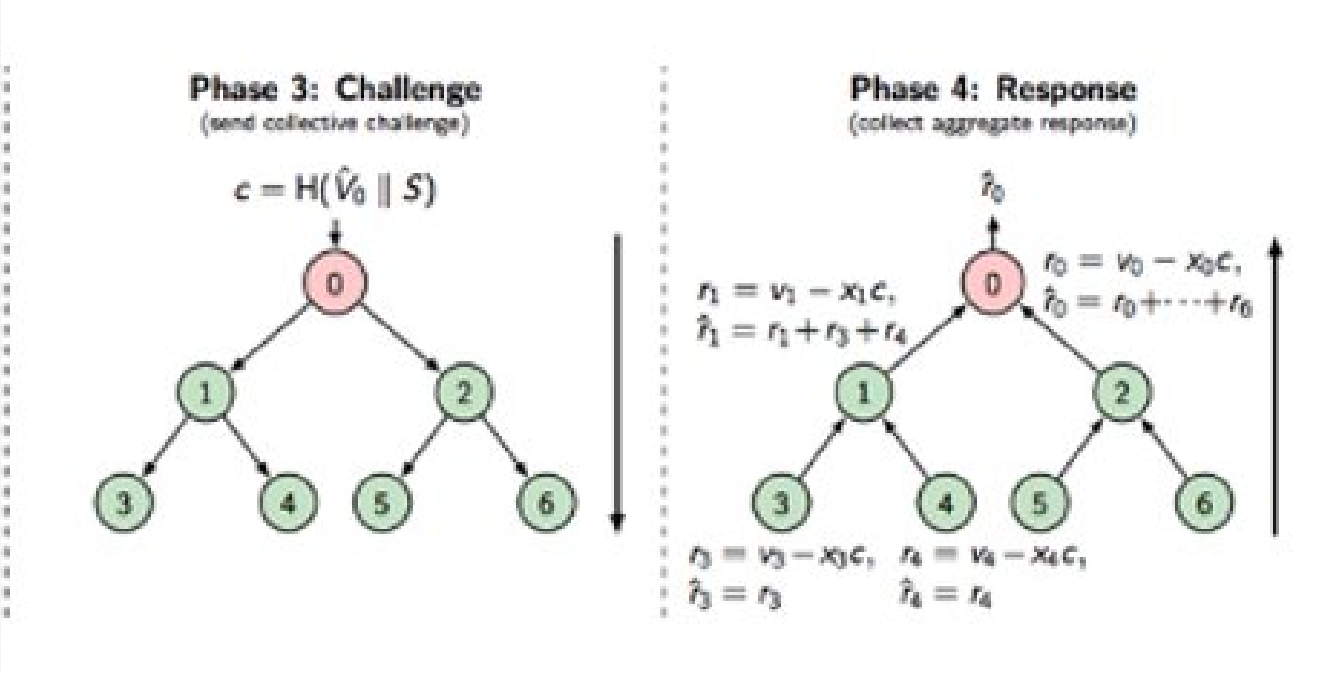
Schnorr Multisignature

- **Proof:**
  - The verification key is $y = \prod g^{x_i}$
  - The signature is (c, r), where $c = H(V||S)$ and $r = \sum r_i$
  - $V_v = g^r y^c = g^{\Sigma(v_i - cx_i)} \prod g^{cx_i} = g^{\Sigma(v_i - cx_i)} g^{\Sigma cx_i} = g^{\Sigma v_i} = \prod g^{v_i} = \prod V_i = V$
  - So, $r_v = H(V_v||S) = H(V||S) = r$

CoSi Protocol



CoSi Protocol



CoSi Protocol

- One CoSi round to implement PBFT's pre-prepare and prepare phases
- Second CoSi round to implement PBFT's commit phase
- Other multisignature methods are available
  - Boneh-Lynn-Shacham (BLS) Cryptography – uses Bilinear Pairing

Conclusion

- CoSi can be used to sign a message by multiple authorities collectively
  - Verification is easy – from the collective public key
- PBFT can be emulated using two rounds of CoSi
- Next, we'll see how CoSi can be used to design a scalable blockchain consensus


Thank
you