Sublinear-Round Byzantine Agreement under Corrupt Majority

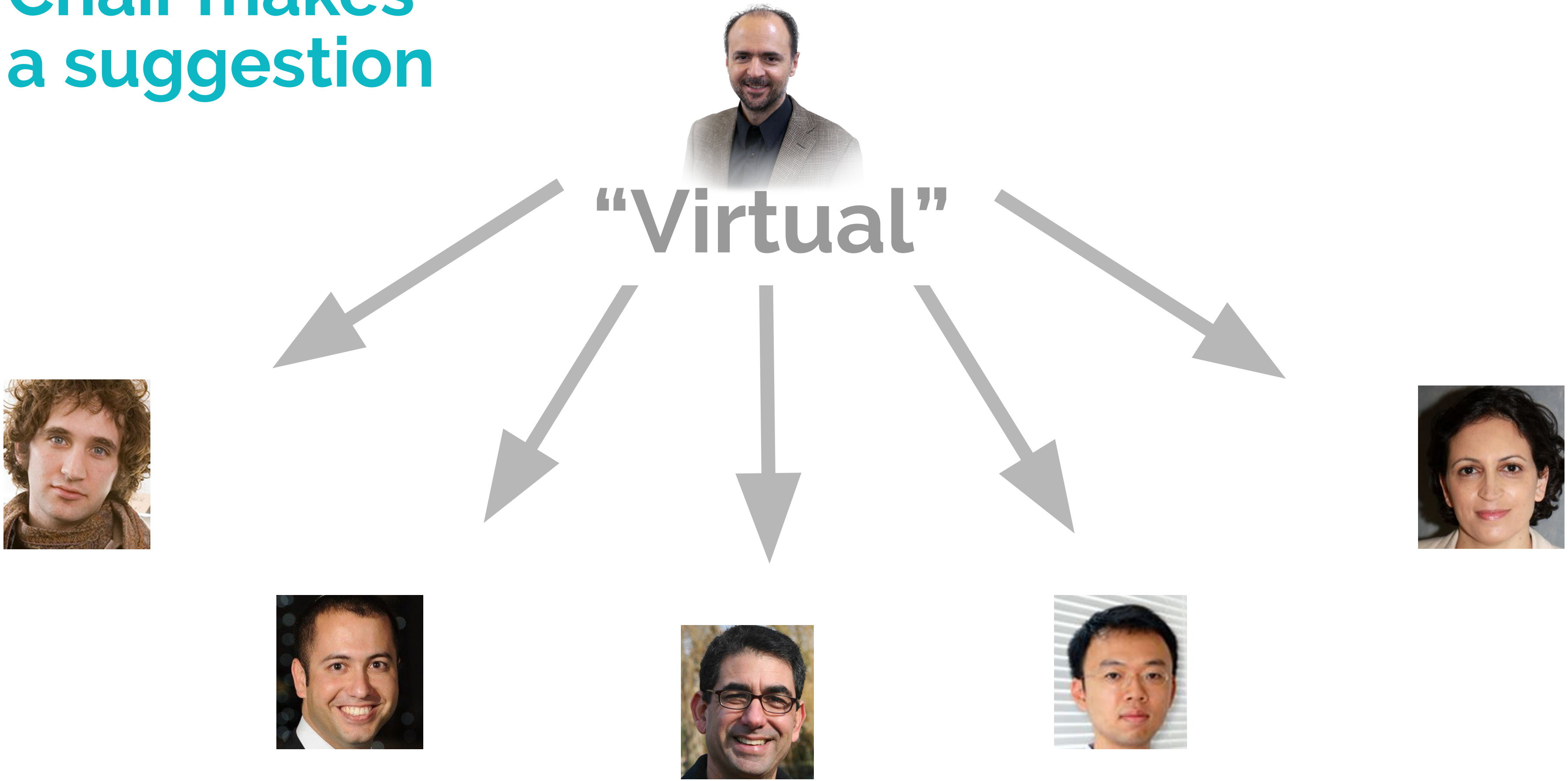
Elaine Shi @ Cornell

Joint with T-H. Hubert Chan (HKU) & Rafael Pass (Cornell)

PKC'2021

Virtual or Physical?

Chair makes a suggestion



Everyone discusses

Everyone decides

Virtual

Virtual

Virtual

Virtual

Virtual

Virtual

Some are unhappy

(e.g., had papers rejected from pkc)

Consistency

happy players agree on decision

Validity

if chair happy, agree on chair’s suggestion

Byzantine Broadcast

[Lamport'82]

Consistency

happy players agree on decision

Validity

if chair happy, agree on chair's suggestion

Byzantine Broadcast

f: number of corrupt players

Corrupt majority

f+1 rounds

[DS'83]

Byzantine Broadcast

Corrupt majority

f+1 rounds

[DS'83]

Deterministic lower bound

≥ f+1 rounds

[DS'83]

Byzantine Broadcast

Honest majority

Expected O(1) rounds

[FM'97]

Corrupt majority

f+1 rounds

[DS'83]

Deterministic lower bound

≥ f+1 rounds

[DS'83]

Can we achieve sublinear rounds under corrupt majority (with randomization) ?

Honest majority

Expected O(1) rounds

[FM'97]

Corrupt majority

f+1 rounds

[DS'83]

Deterministic lower bound

≥ f+1 rounds

[DS'83]

Can we achieve sublinear rounds under corrupt majority (with randomization) ?

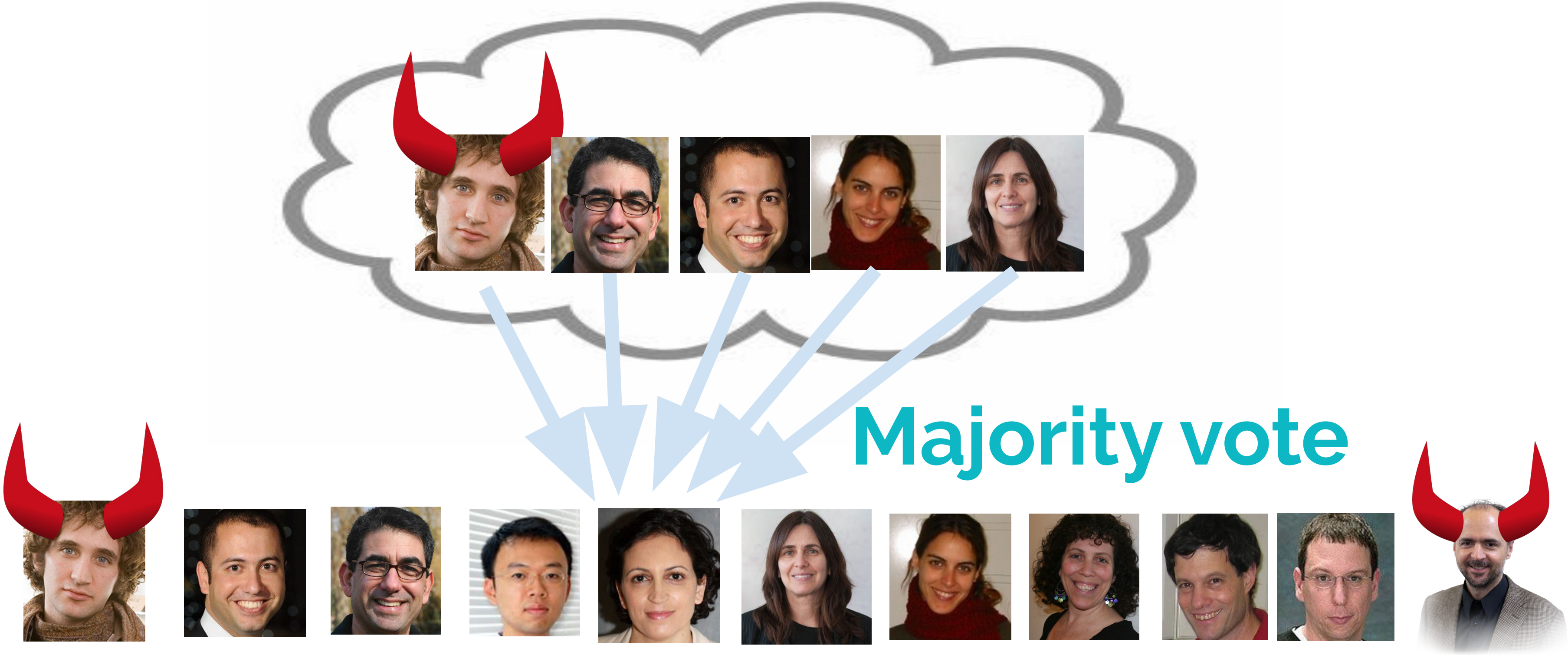
Honest majority	Corrupt majority	Corrupt majority	Deterministic lower bound
Expected O(1) rounds [FM'97]	**Expected Θ(2f-n) rounds** [GKKO'07, FN'09]	**f+1 rounds** [DS'83]	**≥ f+1 rounds** [DS'83]

Can we achieve sublinear rounds under corrupt majority (with randomization) ?

Can we achieve sublinear rounds under corrupt majority (with randomization) ?

- Hard even for static corruption
- Folklore committee election fails

Folklore committee election



Folklore committee election

Corrupt majority: majority voting fails

Can we achieve sublinear rounds under corrupt majority (with randomization) ?

- Hard even for static corruption
- Nothing known for 51% corrupt

Our Result

Assume trusted setup and standard hardness assumptions, there exists poly-log round BB even in the presence of 99.9% weakly adaptive corruptions.

See paper for a more generalized statement.

Challenge 1

Convey decision to those outside the committee

Adaptive corruption of the committee

Challenge 2

1. Dolev-Strong among the committee
2. Non-committee-members participate as non-voters

b r : bit b with r sigs from distinct s including 

committee size: C = polylog(λ)

b r : bit b with r sigs from distinct s including 

committee size: C = polylog(λ)

Round 0:  multicasts b 1

b r : bit b with r sigs from distinct s including 

committee size: C = polylog(λ)

Round 0:  multicasts b 1

Round r = 1.. C:

Committee:

if committee member j sees b r

if b not in E_j : add b to E_j, multicasts b (r + 1) b r : bit b with r sigs from distinct s including 

committee size: C = polylog(λ)

Round 0:  multicasts b 1

add its own sig

Round r = 1.. C:

Committee:

if committee member j sees b r

if b not in E_j : add b to E_j, multicasts b (r + 1) b r : bit b with r sigs from distinct s including 

committee size: C = polylog(λ)

Round 0:  multicasts b 1

Round r = 1.. C:

Committee:

if committee member j sees b r

if b not in E_j : add b to E_j, multicasts b (r + 1)

Finally: player j outputs elem in E_j if its size is 1, else output 0

Lemma 1: if in round **$r < C$**, honest player j has b in its E_j, then in round **$r+1$**, every honest player i has b in E_i

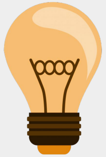
Lemma 2: if in round **C**, honest player j has b in its E_j, then in round **C**, every honest player i has b in E_i

b r : bit b with r sigs from distinct s including 

committee size: C = polylog(λ)

Phase 0:  multicasts b 1

Phase r = 1.. C:

Relay round (everyone): 

if player i sees b r

if b not in E_i : add b to E_i , multicast b r

Voting round (committee):

if committee member j sees b r

if b not in E_j : add b to E_j, multicasts b (r + 1)

Finally: player j outputs elem in E_j if its size is 1, else output 0

Challenge 1

Convey decision to those outside the committee

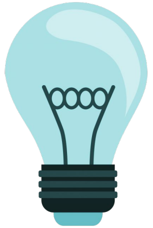
Adaptive corruption of the committee

Challenge 2

Adaptive corruption of the committee

Challenge 2

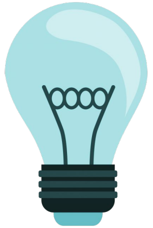
- Secret committee election
- Reveal membership on voting



Player j is member of the b-committee iff

Player j itself: $\rho, \Pi = \mathrm{VRF}(sk_j, b)$

$\& \ \rho < D$



Player j is member of the b-committee iff

Player j itself: $\rho, \Pi = \mathrm{VRF}(sk_j, b)$
$\& \ \rho < D$

Everyone else: $\mathrm{VRF.Vf}(pk_j, b, \rho, \Pi) = 1$
$\& \ \rho < D$

Membership in the two committees decided **independently**

Player j itself: $\rho, \Pi = VRF(sk_j, b)$ & $\rho < D$

Everyone else: $VRF.Vf(pk_j, b, \rho, \Pi) = 1$ & $\rho < D$

b r : bit b w/ r votes from distinct s including 

committee size: C = polylog(λ)

Phase 0:  multicasts b 1

Phase r = 1.. polylog(λ):

Relay round:

if player i sees b r

if b not in E_i : add b to E_i , multicast b r

Voting round:

if player j sees b r and is member of b-committee:

if b not in E_j : add b to E_j, multicasts b (r + 1)

Finally: player j outputs elem in E_j if its size is 1, else output 0

Open Questions and Ongoing Work

- Can we achieve **expected constant rounds** with corrupt majority?

  https://eprint.iacr.org/2020/590

- Can we achieve a similar result in the **strongly adaptive** model?

Thank you!

runting@gmail.com