Low-Communication Byzantine Agreement and Succinct Arguments

Naman Kumar [1] Chaya Ganesh [2]

[1]*Chennai Mathematical Institute* [2]*Advisor, Indian Institute of Science*

The Byzantine Agreement Problem

The Setting

- n different divisions of the Byzantine army, each headed by a general, are camped outside an enemy city
- Must decide on a common plan of action: whether to attack at dawn
- The invasion will only be successful if **all** generals agree to attack
- To communicate, the generals use point-to-point messengers

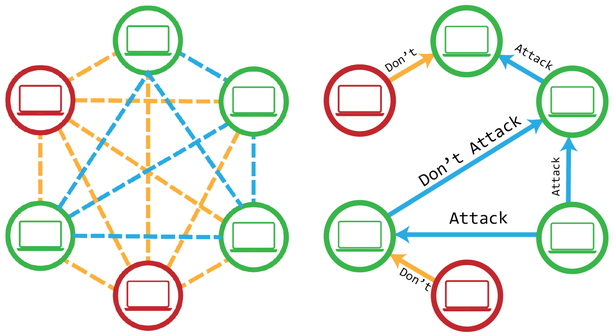

Figure 1. A typical byzantine fault setting. The red computers are 'traitors' and the yellow lines are compromised channels of communication. The green computers must agree on a 'plan of action,' say, a bit (whether to attack or not).

The Problem

- Some generals are traitors!
- They want to convince the army to adopt a **bad** plan
- Or they want to destabilize it by **convincing some generals to attack and some to abort**

Can we find a protocol that accomplishes the following?

- All honest generals agree on the same plan of action.
- A small number of traitors cannot cause the honest generals to adopt a bad plan.

The Problem: Can BA be Achieved with Low Communication?

We know that if $\#$ traitors $\geq n/3$ we **cannot** achieve BA.

Can BA *always* be achieved if the number of traitors is less than $n/3$? Yes.

Using cryptography, there are a number of secure BA protocols that manage to achieve full BA with less than $n/3$ traitors. The questions then become:

1. **What is the minimum amount of (a) total, and (b) per-party communication required to achieve full BA?**
2. **Do we require the presence of a trusted third party (separate from the generals/traitors) to set up some infrastructure which is used in the protocol?**

BA with $\tilde{O}(1)$ Per-Party Communication

1. Latest result by E. Boyle, R. Cohen and A. Goel achieves BA [1]
2. Per-party communication is $\tilde{O}(1)$ ie. **polylog in** n, where n is the number of parties
3. Using certain strong cryptographic assumptions, **a trusted third party is not required to achieve full BA**

Succinctly Reconstructed Digital Signatures (SRDS)

Signature Schemes

A mathematical protocol that verifies the authenticity of a message.

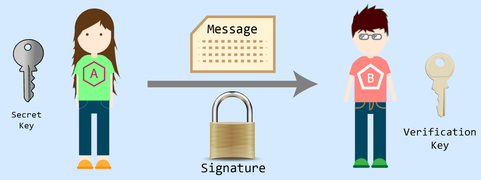

Figure 2. A digital signature scheme. With each message Alice sends a signature signed by her private key. If Bob's public verification key accepts, then the message was indeed sent by Alice.

SRDS

- The low-communication BA protocol of [1] relies on a primitive known as **Succinctly Reconstructed Digital Signatures (SRDS)**
- A signature which certifies that a **majority of parties** have agreed on a common message
- Assigns each party a secret key and then aggreggates generated signatures at each level

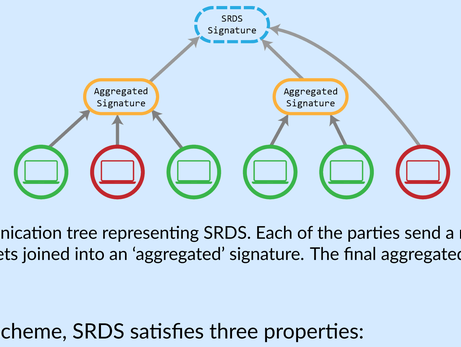

Figure 3. A communication tree representing SRDS. Each of the parties send a message and a signature, which gets joined into an 'aggregated' signature. The final aggregated signature is the SRDS signature.

As a signature scheme, SRDS satisfies three properties:

- **Succinctness:** The size of the signatures is small.
- **Robustness:** Enough honest parties can always create a signature on any message of their choice.
- **Unforgeability:** Traitors cannot create a false signature on a message.

Crucially: Can a SNARG be constructed using SRDS?

Succinct Arguments

1. A **Succinct Non-Interactive Argument of Knowledge (SNARG)** produces a short proof that some hard problem has a witness
2. The problem is out of Bob's computational reach
3. Alice can show to Bob that the problem has a witness with **low communication**

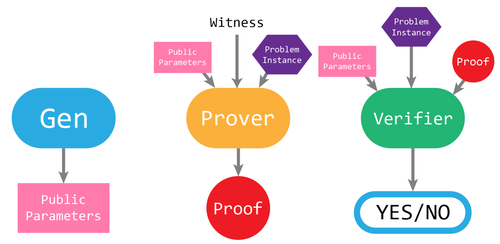

Figure 4. A succinct argument system. Alice feeds the prover algorithm a problem instance and receives a short proof. Bob can then run the verifier and check whether the proof is indeed correct.

SNARG Soundness

- A SNARG is only useful if an adversary cannot **forge a proof** for some problem instance that does not have a witness
- This property is called *soundness* and comes in two flavors:

1. **Non-adaptive Soundness**: If we give an adversary the public parameters and a problem instance for which there is no witness, then it cannot create a valid proof for that instance.
2. **Adaptive Soundness**: If we give an adversary the public parameters, then it cannot produce a valid proof for some problem instance of its choice, provided that the instance does not have a witness.

Falsifiability and Gentry-Wichs

Falsifiable Assumptions

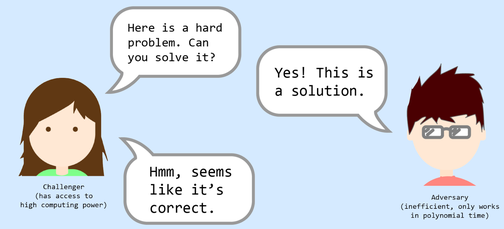

Figure 5. A falsifiable problem. If there exists an inefficient adversary that can solve the hard problem with non-negligible probability, then our assumption that the problem is hard will be proven to be false.

Examples of falsifiable assumptions in cryptography:

- Rivest-Shamir-Adleman (RSA) Assumption
- Learning with Errors (LWE) Assumption
- Decisional Diffie-Hellman (DDH) Assumption

Gentry-Wichs [2]

- Consider an **adaptively sound** SNARG
- Soundness must be **proven**
- Gentry-Wichs show that the proof cannot depend on any falsifiable assumption!
- In particular, simply **assuming soundness without proving it** is not falsifiable
- Makes reasoning about such SNARGs hard

If SRDS implies an adaptive SNARG, then SRDS cannot be based on falsifiable assumptions. Question: Can an adaptive SNARG be constructed using SRDS?

Results and Progress

Our progress has been on two fronts:

1. We believe that we have shown that SRDS implies a SNARG for a problem known as **Subset-Product**. The soundness of this scheme is *non-adaptive*. We are attempting to found out whether SRDS implies an adaptive SNARG - if this is the case, then SRDS is based on falsifiable assumptions.
2. We consider the basic structure and construction of SRDS which involves a very strong primitive known as PCD (proof carrying data) and attempt to see whether SRDS really does require such a strong condition to hold.

References

[1] Elette Boyle, Ran Cohen, and Aarushi Goel. Breaking the $o(\sqrt{n})$-bit barrier: Byzantine agreement with polylog bits per party, 2020.

[2] Craig Gentry and Daniel Wichs. Separating succinct non-interactive arguments from all falsifiable assumptions. Cryptology ePrint Archive, Paper 2010/610, 2010. https://eprint.iacr.org/2010/610.

namankumar@cmi.ac.in