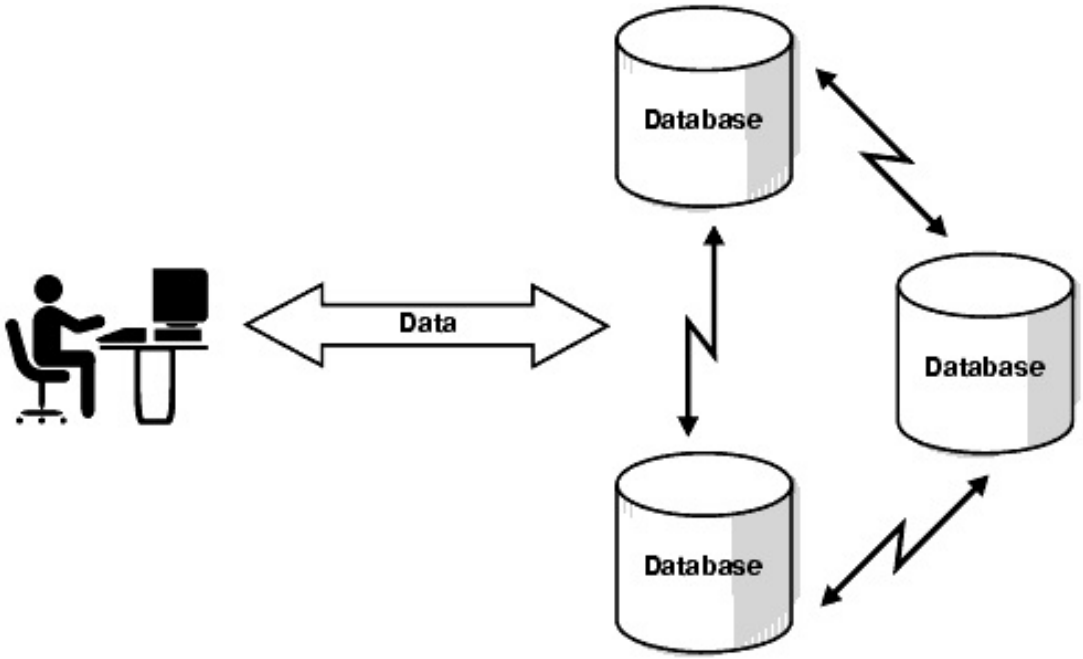
On the Composition of Athenticated Byzantine Agreement

Markos-Spyridon Epitropou

NTUA

February 6, 2012

Introduction



Byzantine Generals Problem

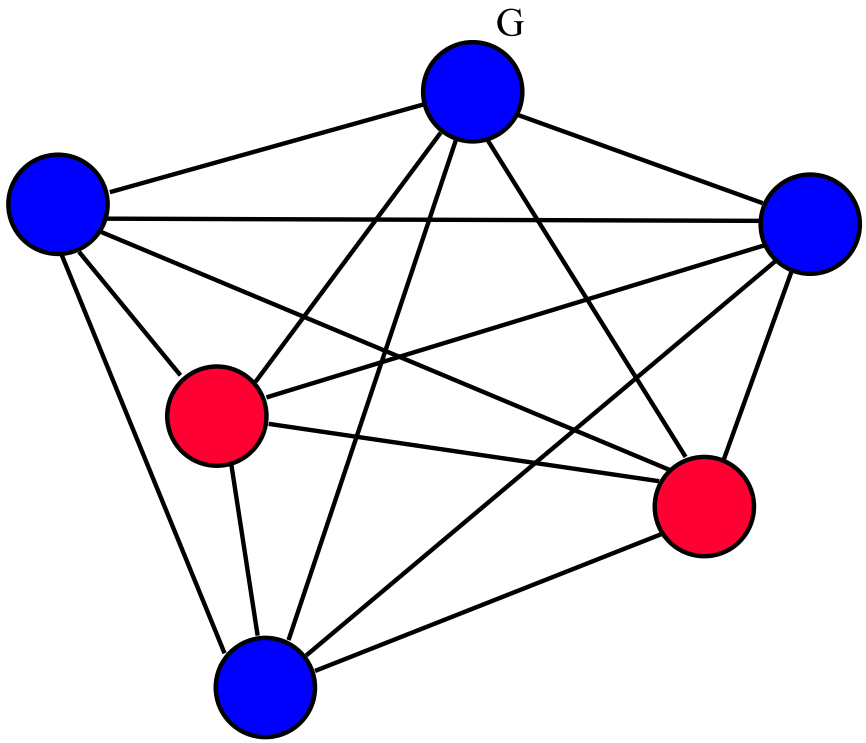
Definition 1

Let $P_1, \ldots, P_{n-1}$ and $G = P_n$ be n parties and let G be the designated party with input x. In addition there is an adversary who may corrupt up to t of the parties including the special party G. A protocol solves the Byzantine Generals problem if the following two properties hold (except with negligible probability):

1. Agreement: All honest parties ouput the same value.
2. Validity: If G is honest, then all honest parties output x.

We denote such a protocol by $BG_{n,t}$.

Byzantine Generals Problem



- faulty: RED
- non-faulty: BLUE

Byzantine Agreement Problem

Definition 2

Let $P_1, \ldots, P_{n-1}$ be n parties, with associated inputs $x_1, \ldots, x_n$. In addition there is an adversary who may corrupt up to t of the parties. Then, a protocol solves the Byzantine Agreement problem if the following two properties hold (except with negligible probability):

1. Agreement: All honest parties output the same value.
2. Validity: If $\max(n - t, \lfloor n/2 \rfloor + 1)$ of the parties have the same input value x and follow the protocol specification, then all honest parties output x.

Byzantine Generals $\Leftrightarrow$ Byzantine Agreement

Byzantine Generals $\Leftrightarrow$ Byzantine Agreement

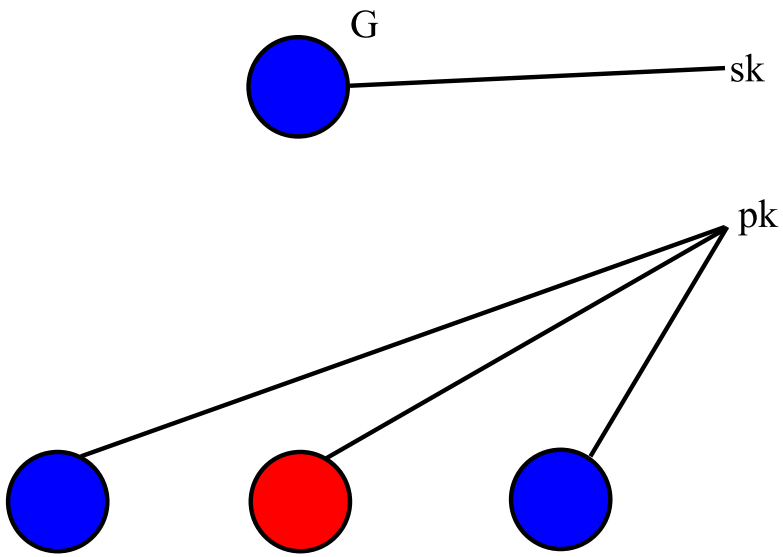
- Byzantine Generals $\Rightarrow$ Byzantine Agreement
  Every player broadcasts his value and then decides on the majority of the values received

Byzantine Generals $\Leftrightarrow$ Byzantine Agreement

- Byzantine Generals $\Rightarrow$ Byzantine Agreement
  Every player broadcasts his value and then decides on the majority of the values received
- Byzantine Agreement $\Rightarrow$ Byzantine Generals
  G broadcasts his value to all players and then all players decide on the same value using a Byzantine Agreement Protocol

Authenticated Model

- G sends a message $M = (m, sign_{sk}(m))$
- P_i verifies every message she receives $(Ver_{pk}(M))$



Composition of Protocols

- Parallel Composition
- Concurrent Composition
- Sequential Composition

Proposition

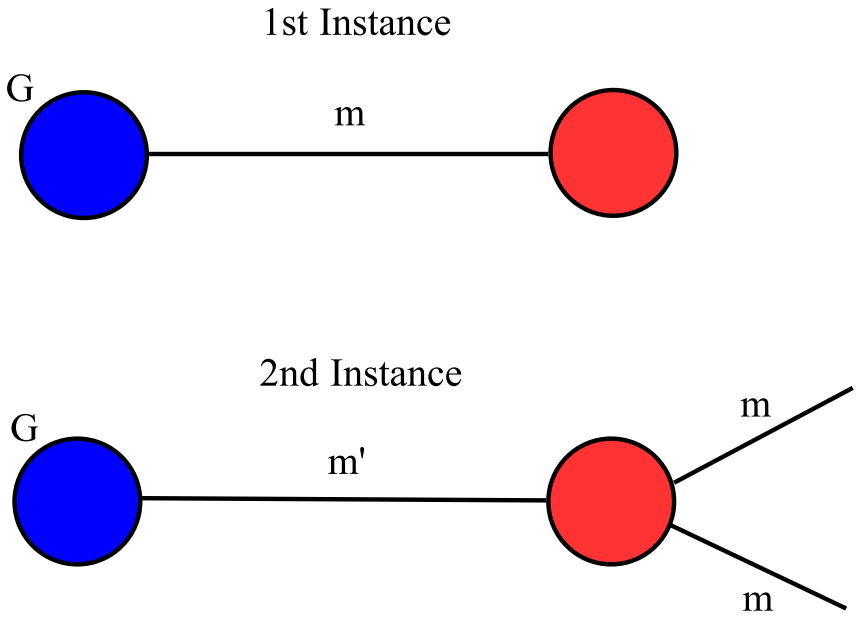
Any protocol Π for Byzantine Generals (or Agreement) in the standard model, remains secure under concurrent composition.

Impossibility Results

Secure Protocols

Composition	Standard Model	Authenticated Model
Stand-Alone	$t < n/3$	$t \leq n$
Concurrent	$t < n/3$	?
Sequential	$t < n/3$	?

Parallel Composition



Faulty party sends false value m at 2nd instance

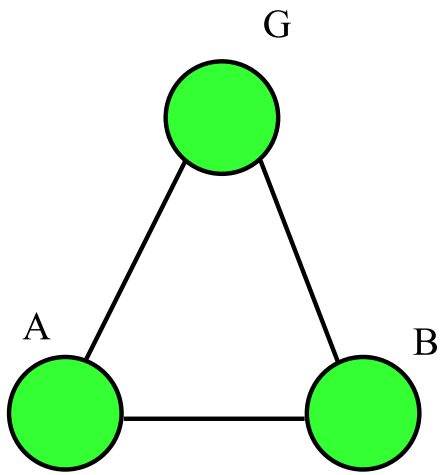
Parallel Composition

Theorem

No protocol for authenticated Byzantine Agreement that composes in parallel (even twice) can tolerate n/3 or more faulty parties.

Parallel Composition

Proof:



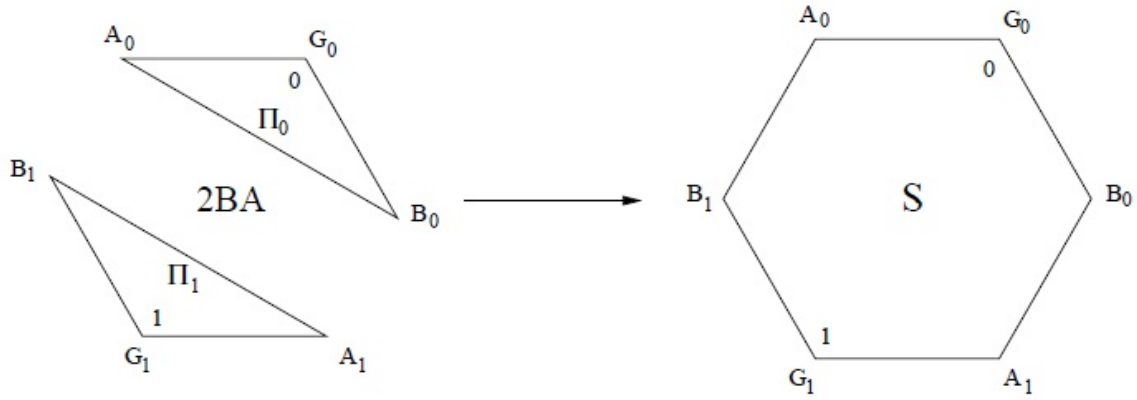
Lemma

There exists no protocol for authenticated Byzantine Agreement for three parties, that composes in parallel (even twice) and can tolerate one faulty party.

Parallel Composition

G, A: non-faulty

B: faulty



Claim 1

Except with negligible probability, parties G_0 and A_0 halt within rounds(Π) steps and output 0 in the system S.

Parallel Composition

Claim 1

Except with negligible probability, parties G_0 and A_0 halt within rounds(Π) steps and output 0 in the system S.

Claim 2

Except with negligible probability, parties G_1 and B_1 halt within rounds(Π) steps and output 1 in the system S.

Claim 3

Except with negligible probability, parties A_0 and B_1 halt within rounds(Π) steps and output the same value in the system S.

Concurrent Composition

Corollary

No protocol for authenticated Byzantine Agreement that composes concurrently (even twice) can tolerate n/3 or more faulty parties.

Sequential Composition

r rounds of 2 parallel executions of the protocol can be perfectly simulated in 2r sequential executions of the same protocol

Theorem

Let Π be a deterministic protocol for authenticated Byzantine Generals that terminates within r rounds of communication and remains secure under sequential composition for 2r or more executions. Then Π can tolerate at most $t < n/3$ statically corrupted parties.