Efficient attacks and real-world provable security

Dr. Alexander W. Dent

Real-world provable security

- Two years ago, I presented a seminal result on the use of provable security in the real world.

Theorem **An experimental subject that has had their hands "cruelly" "hacked" off using a "rusty" machete is still able to pick up objects with probably 1/4.**

Corollary **An experimental subject whose hands have been removed with unsanitary implements can pick objects up almost always.**

Real-world provable security

- Two years ago, I presented a seminal result on the use of provable security in the real world.

Theorem **An experimental subject that has had their hands "cruelly" "hacked" off using a "rusty" machete is still able to pick up objects with probably 1/4.**
Corollary **An experimental subject whose hands have been removed with unsanitary implements can pick objects up almost always.**

- I used to believe that community's lack of interest was due to nepotism and intrigue.
- Now I understand that it's because proof had "turgid notation and 'game hopping'".

Real-world provable security

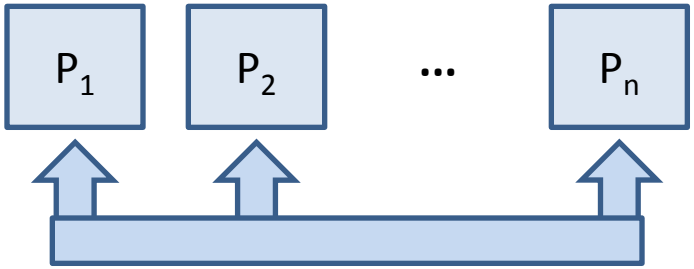
<u>Informal Theorem</u> War. (Huh?) What is it good for? Nothing.

Real-world provable security

<u>Informal Theorem</u> War. (Huh?) What is it good for? Nothing.

<u>Theorem</u> There is no black-box construction the produces anything good from war with a non-negligible probability (assuming a separation between mortals and divine creatures).

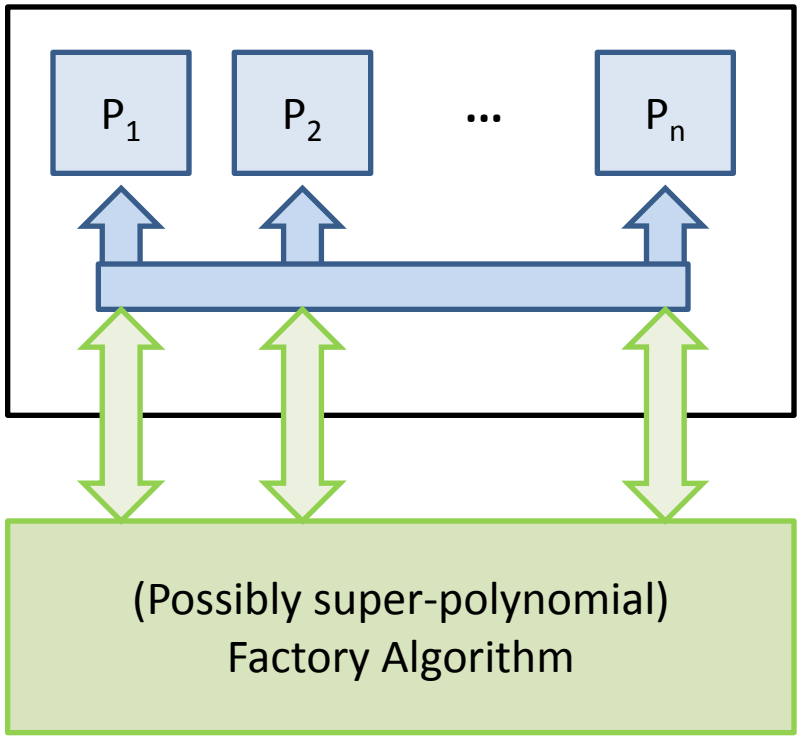
Real-world provable security



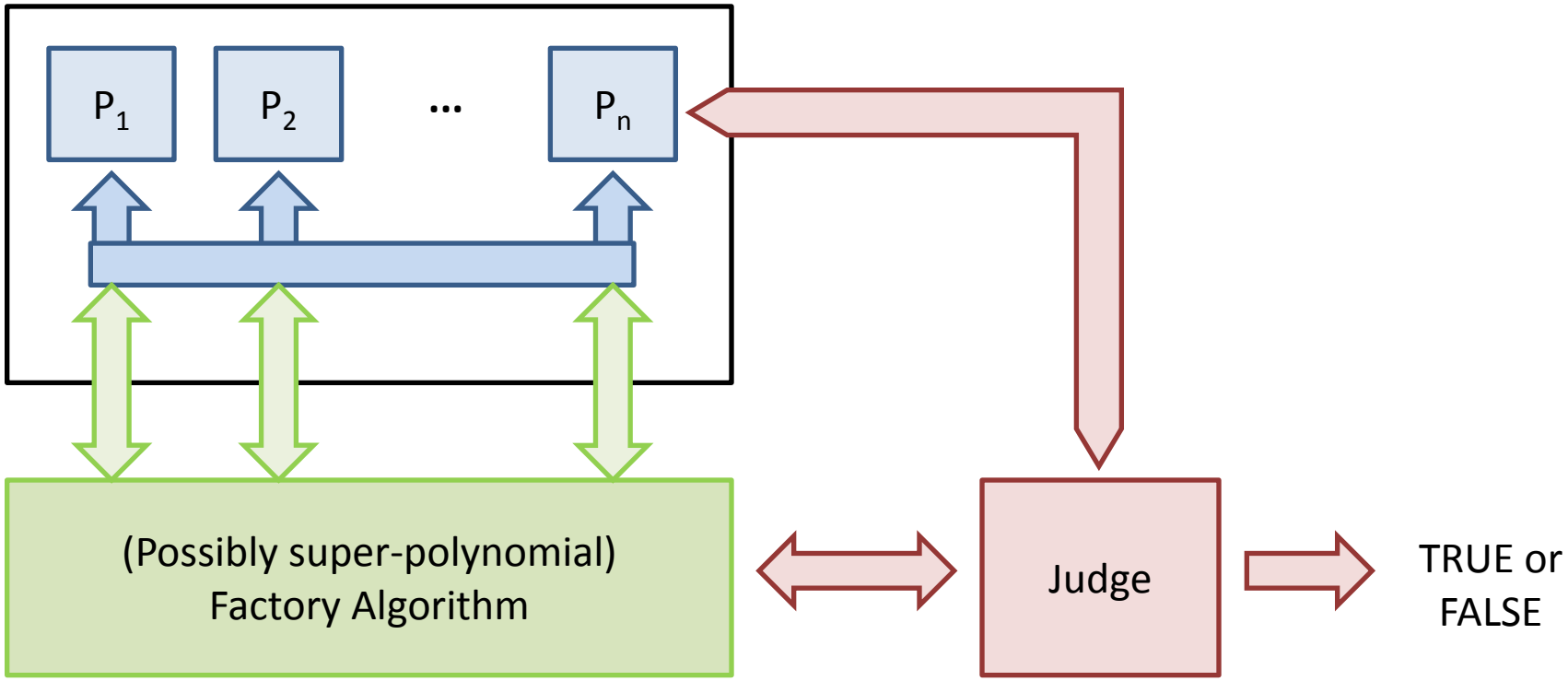
<u>War</u> An n-party multiparty protocol that is designed to output n-1 parties.

(n > 1 – no suicide here).

Real-world provable security

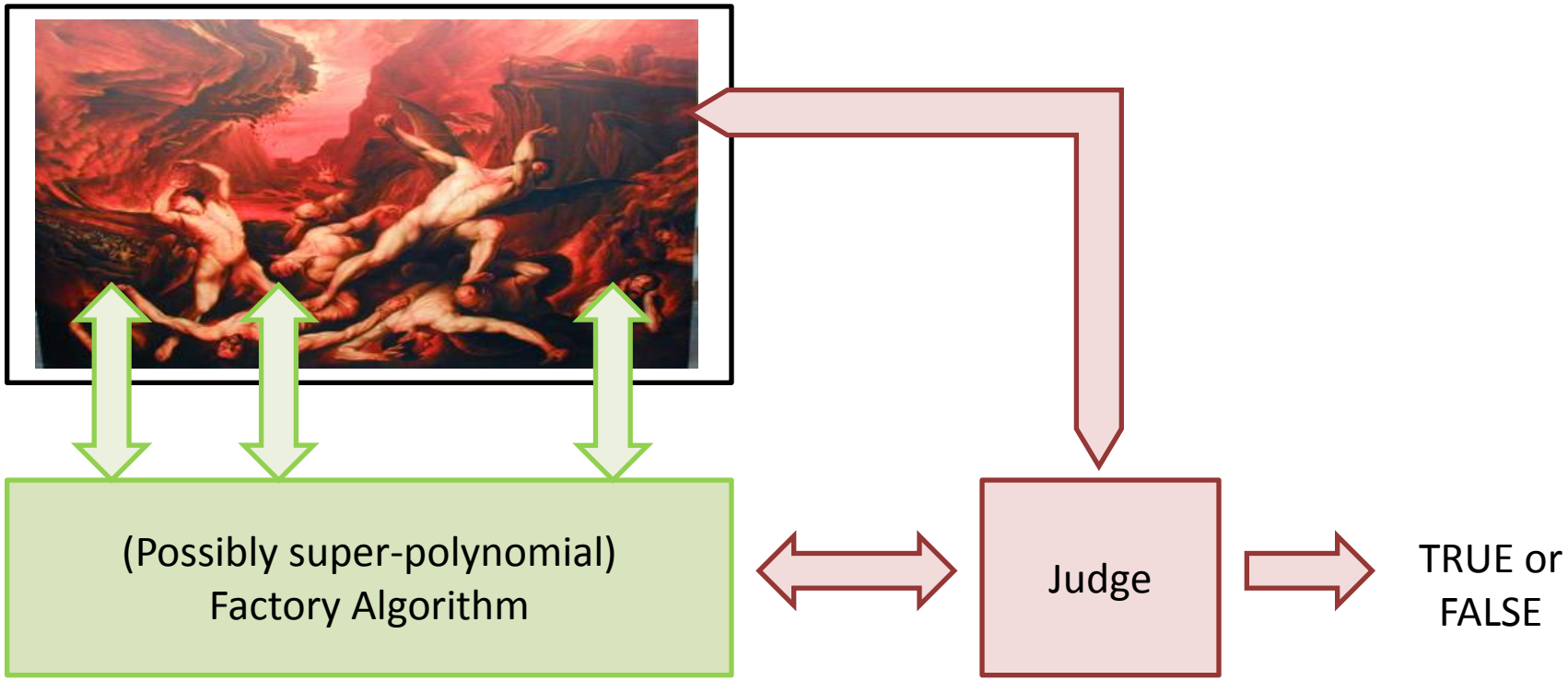


Real-world provable security



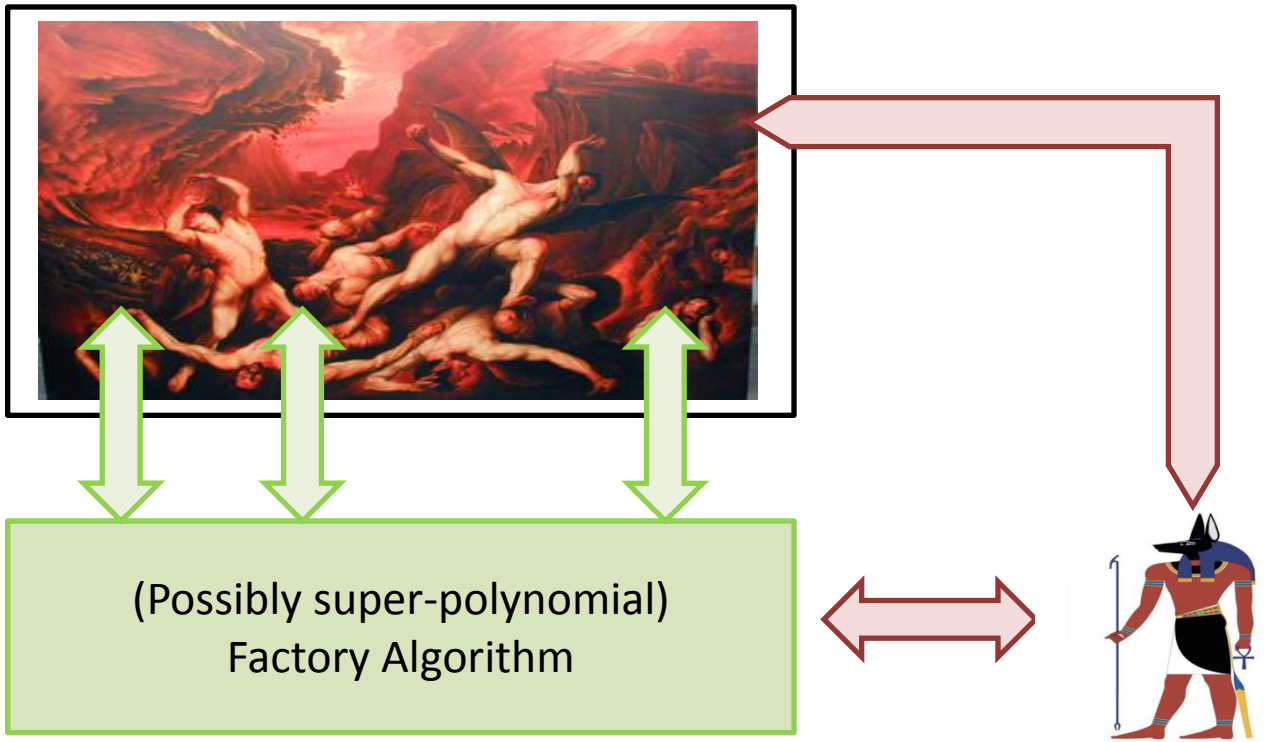
- Profiteer model – judge can interact with all parties.
- Factory output declared “good” if there exists a PPT judge will output TRUE.

Real-world provable security



- Using our assumption that divine creatures exist, we can replace the arbitrary war with an ideal war, i.e. Armageddon.

Real-world provable security



- The judge will now output TRUE with negligible probability because there is only a negligible chance of a judge surviving any form of divine intervention.

Real-world provable security

- High performance experiments are in progress and are scheduled to finish (assuming no power outages) on December 21st 2012.