

The Poulidor Distance-Bounding Protocol

Rolando Trujillo-Rasua¹ Benjamin Martin² Gildas Avoine²

¹Universitat Rovira i Virgili
Catalonia, Spain

²Université catholique de Louvain
Belgium

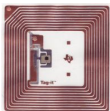
RFIDSec 2010



Outline

- 1 Motivation
- 2 Protocols
- 3 Our Proposal
- 4 Comparison
- 5 Conclusions

Authentication in RFID



secret k

response $R_k(Q)$

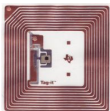


secret k

query Q

verifies $R_k(Q)$

Authentication in RFID



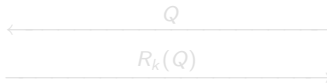
secret k



secret k

query Q

response $R_k(Q)$



verifies $R_k(Q)$

Authentication in RFID

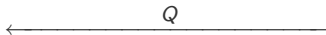


secret k



secret k

query Q



response $R_k(Q)$



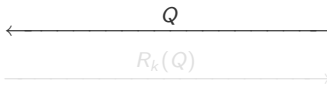
verifies $R_k(Q)$

Authentication in RFID



secret k

response $R_k(Q)$

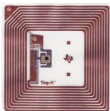


secret k

query Q

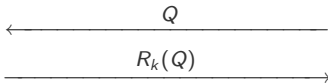
verifies $R_k(Q)$

Authentication in RFID



secret k

response $R_k(Q)$

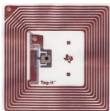


secret k

query Q

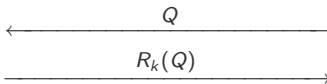
verifies $R_k(Q)$

Authentication in RFID



secret k

response $R_k(Q)$

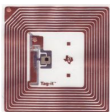


secret k

query Q

verifies $R_k(Q)$

Authentication in RFID



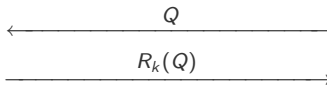
secret k



secret k

query Q

response $R_k(Q)$



verifies $R_k(Q)$

Assumption

The prover is close to the verifier during the execution of the protocol.

Relay attack

Mafia fraud



$R_k(Q)$

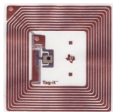


query Q

$R_k(Q)$ Ok ?

Relay attack

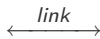
Mafia fraud



$R_k(Q)$



\tilde{V}



\tilde{P}



query Q



$R_k(Q)$ Ok ?

Relay attack

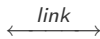
Mafia fraud



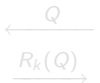
$R_k(Q)$



\tilde{V}



\tilde{P}



query Q

$R_k(Q)$ Ok?

Relay attack

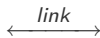
Mafia fraud



$R_k(Q)$



\tilde{V}



\tilde{P}

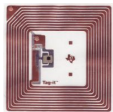


query Q

$R_k(Q)$ Ok?

Relay attack

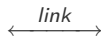
Mafia fraud



$R_k(Q)$



\tilde{V}



\tilde{P}

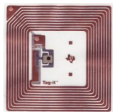


query Q

$R_k(Q)$ Ok?

Relay attack

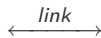
Mafia fraud



$R_k(Q)$



\tilde{V}



\tilde{P}

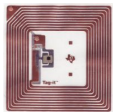


query Q

$R_k(Q)$ Ok?

Relay attack

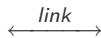
Mafia fraud



$R_k(Q)$



\tilde{V}



\tilde{P}



query Q

$R_k(Q)$ Ok?

Relay attack

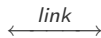
Mafia fraud



$R_k(Q)$



\tilde{V}



\tilde{P}



query Q



$R_k(Q)$ Ok?

Relay attack

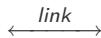
Mafia fraud



$R_k(Q)$



\tilde{V}



\tilde{P}



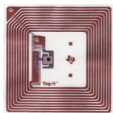
query Q



$R_k(Q)$ Ok?

Relay attack

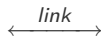
Mafia fraud



$R_k(Q)$



\tilde{V}



\tilde{P}

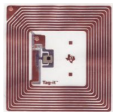


query Q

$R_k(Q)$ Ok?

Relay attack

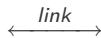
Mafia fraud



$R_k(Q)$



\tilde{V}



\tilde{P}



query Q

$R_k(Q)$ Ok ?



Relay attack

Mafia fraud



$R_k(Q)$



\tilde{V}



\tilde{P}



query Q

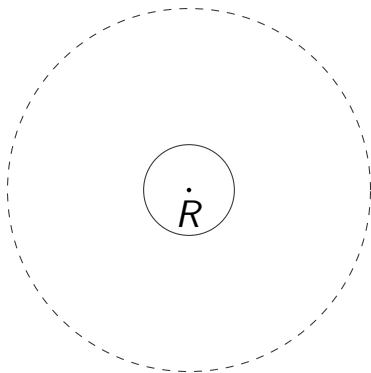
$R_k(Q)$ Ok?

How to defeat the attack?

The verifier could measure the distance between him and the prover.

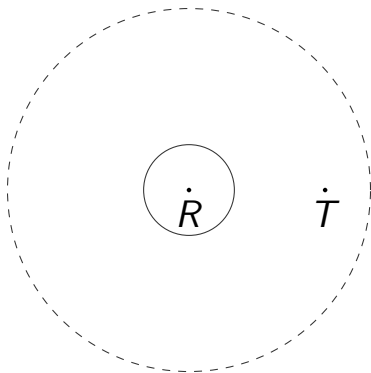
Relay attack

Distance fraud



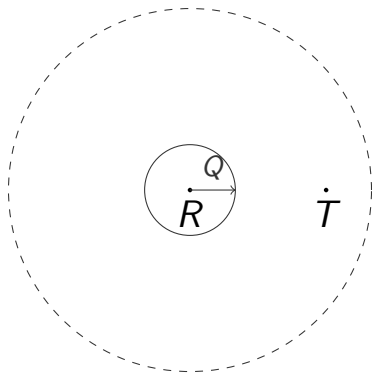
Relay attack

Distance fraud



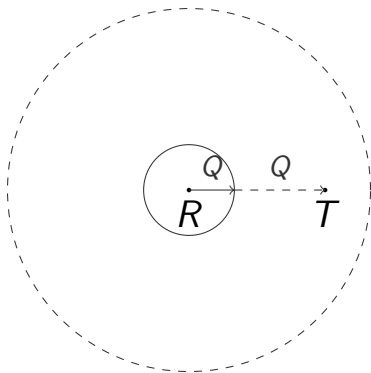
Relay attack

Distance fraud



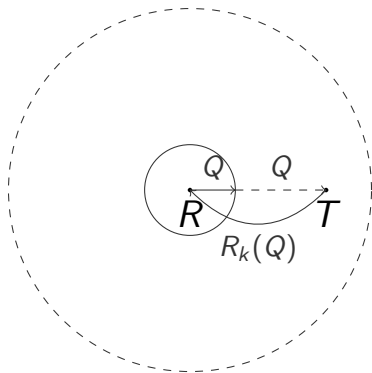
Relay attack

Distance fraud



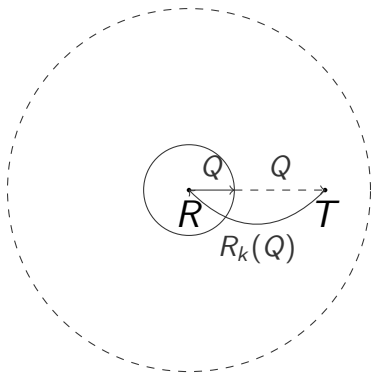
Relay attack

Distance fraud



Relay attack

Distance fraud



How to defeat the attack?

The verifier could measure the distance between him and the prover.

Solutions

Distance Bounding Protocol

Definition (Distance Bounding)

A *distance bounding* is a process that consists of an authentication combined with a distance-checking, where the considered property is an upper-bound on the distance between the two parties.

Solutions

Distance Bounding Protocol

Definition (Distance Bounding)

A *distance bounding* is a process that consists of an authentication combined with a distance-checking, where the considered property is an upper-bound on the distance between the two parties.

How to measure the distance ?

The verifier could measure the time spent during an exchange between him and the prover.

Solutions

Challenges

General Challenge

A distance-bounding should resist to both frauds (mafia fraud and distance fraud) using low computational resources (memory and time) at least in the tag side.

Solutions

Challenges

General Challenge

A distance-bounding should resist to both frauds (mafia fraud and distance fraud) using low computational resources (memory and time) at least in the tag side.

- Trade-off prob. vs computation complexity (e.g. Brands-Chaum).

Solutions

Challenges

General Challenge

A distance-bounding should resist to both frauds (mafia fraud and distance fraud) using low computational resources (memory and time) at least in the tag side.

- Trade-off prob. vs computation complexity (e.g. Brands-Chaum).
- Trade-off prob. vs memory (e.g. Avoine-Tchamkarten).

Solutions

Challenges

General Challenge

A distance-bounding should resist to both frauds (mafia fraud and distance fraud) using low computational resources (memory and time) at least in the tag side.

- Trade-off prob. vs computation complexity (e.g. Brands-Chaum).
- Trade-off prob. vs memory (e.g. Avoine-Tchamkarten).
- Trade-off prob. vs symbol size (bits) (e.g. Munilla-Peinado).

Solutions

Challenges

General Challenge

A distance-bounding should resist to both frauds (mafia fraud and distance fraud) using low computational resources (memory and time) at least in the tag side.

- Trade-off prob. vs computation complexity (e.g. Brands-Chaum).
- Trade-off prob. vs memory (e.g. Avoine-Tchamkarten).
- Trade-off prob. vs symbol size (bits) (e.g. Munilla-Peinado).
- Trade-off mafia fraud vs distance fraud (e.g. Kim-Avoine).

Solutions

Contributions

Contributions

- We introduce the concept of distance-bounding protocols based on graphs.
- We propose a new distance-bounding protocol based on a particular graph that ensures a good trade-off between memory, distance fraud resistance, mafia fraud resistance, and computation complexity.

Previous Protocols

Hancke and Kuhn

P

secret x

V

secret x

slow phase

fast phase

Previous Protocols

Hancke and Kuhn

P

secret x

V

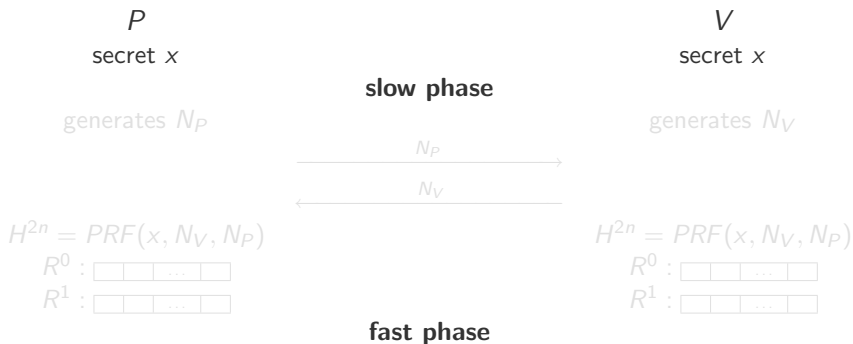
secret x

slow phase

fast phase

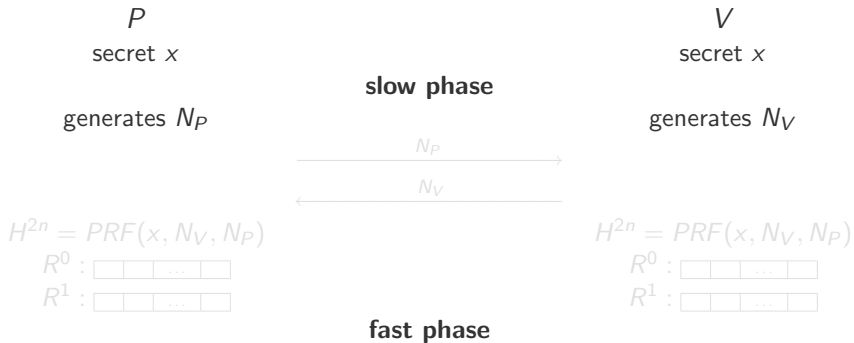
Previous Protocols

Hancke and Kuhn



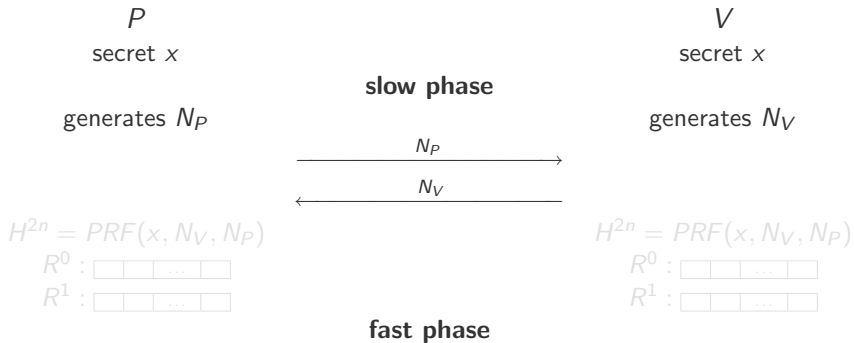
Previous Protocols

Hancke and Kuhn



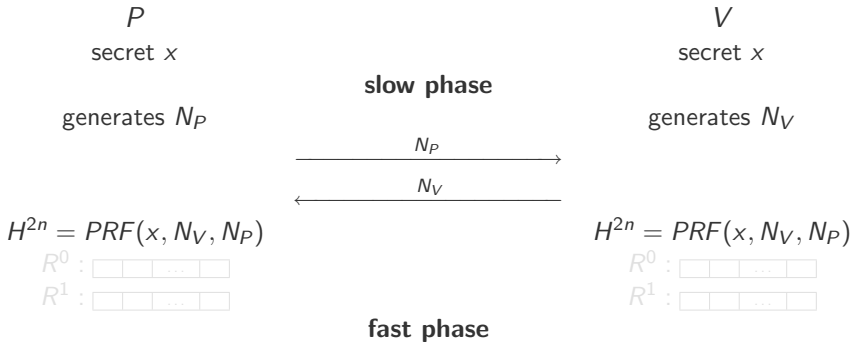
Previous Protocols

Hancke and Kuhn



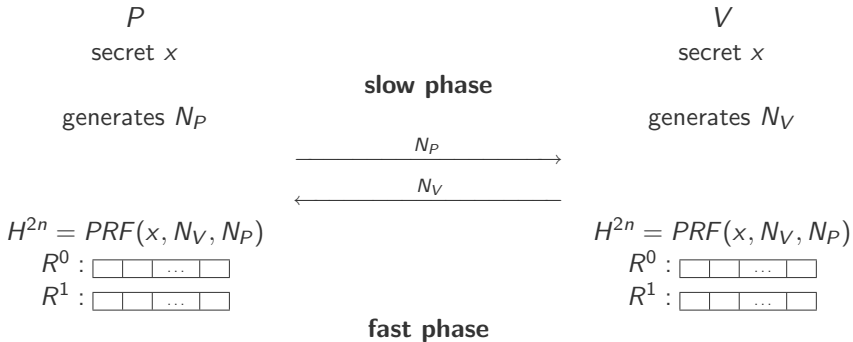
Previous Protocols

Hancke and Kuhn



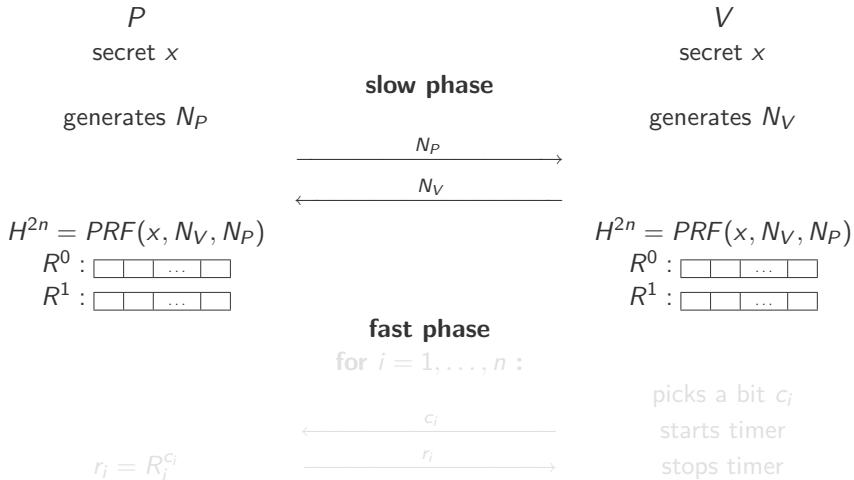
Previous Protocols

Hancke and Kuhn



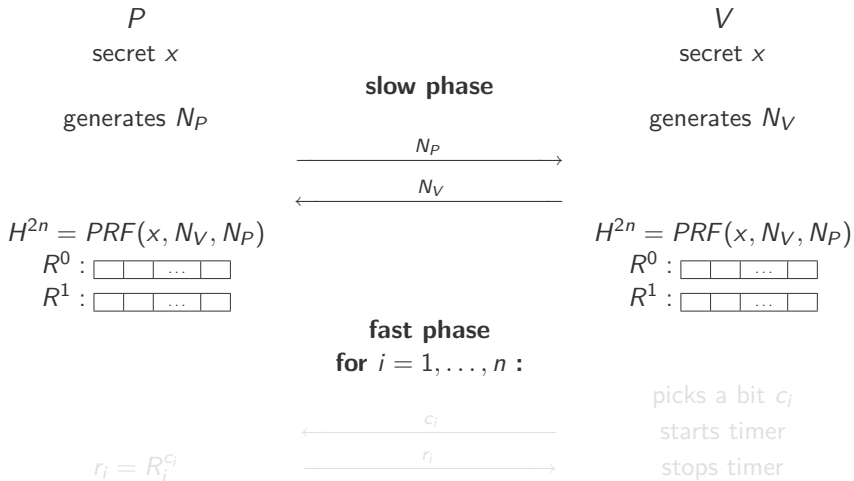
Previous Protocols

Hancke and Kuhn



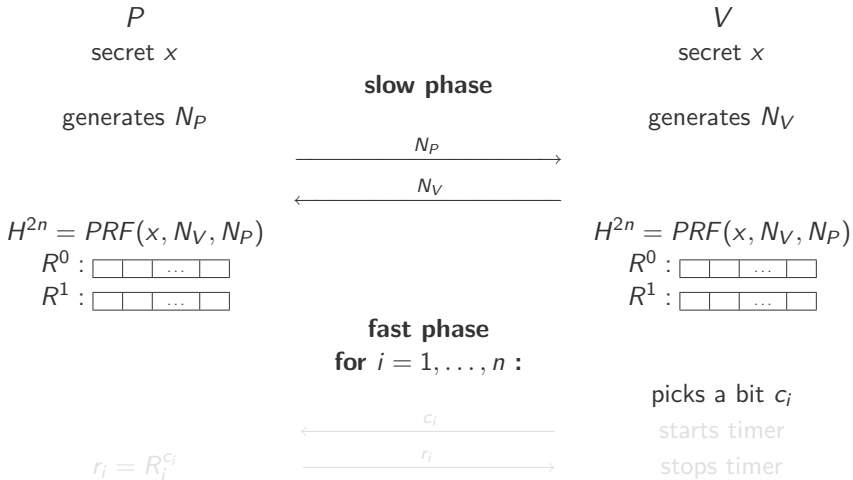
Previous Protocols

Hancke and Kuhn



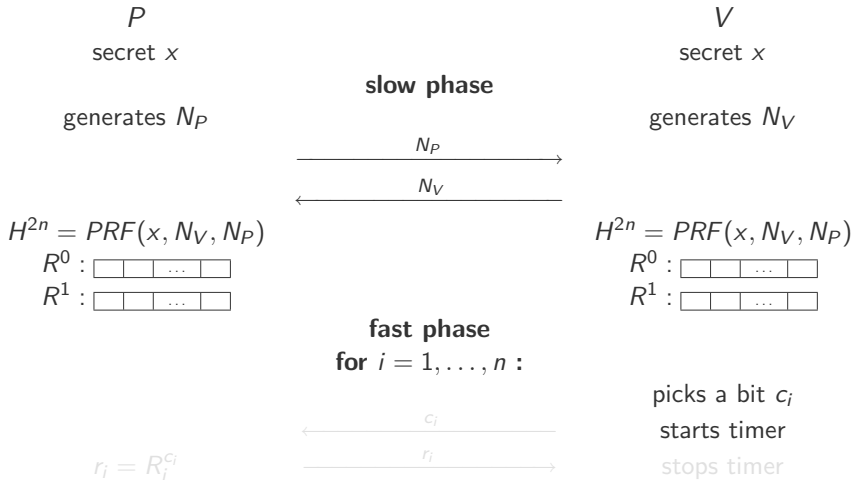
Previous Protocols

Hancke and Kuhn



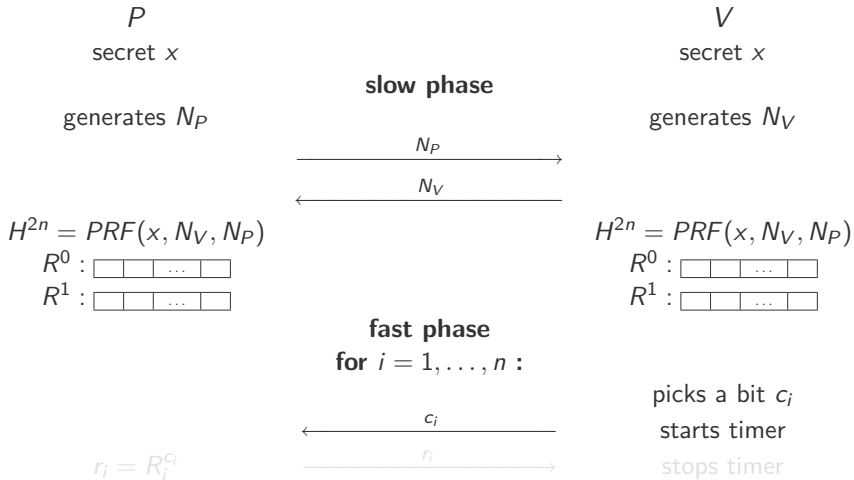
Previous Protocols

Hancke and Kuhn



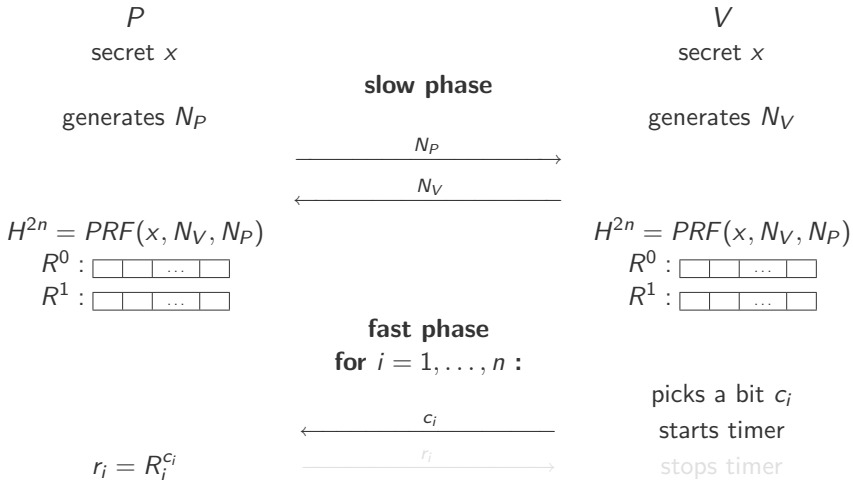
Previous Protocols

Hancke and Kuhn



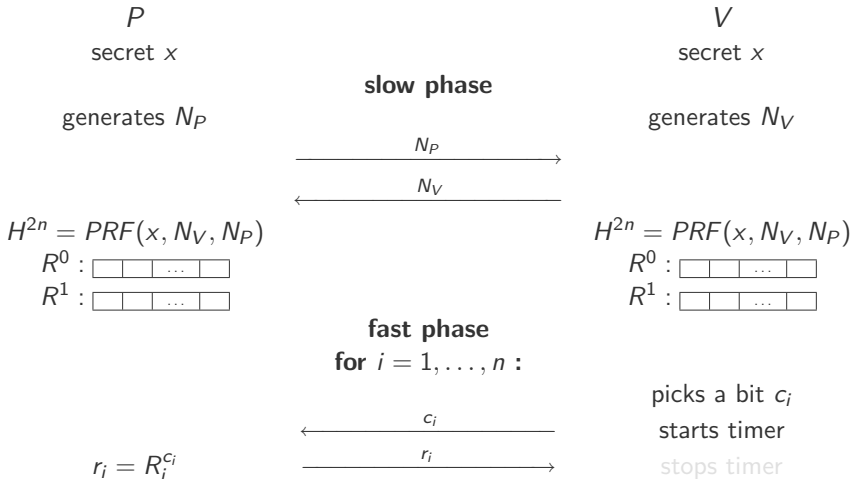
Previous Protocols

Hancke and Kuhn



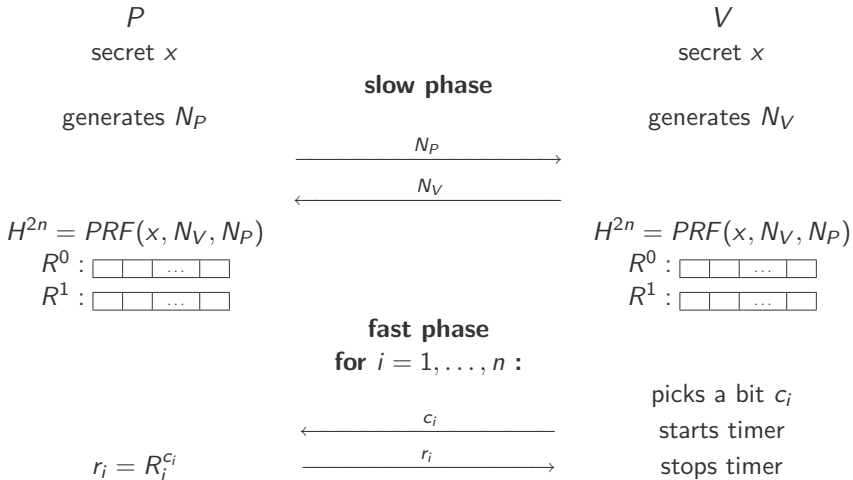
Previous Protocols

Hancke and Kuhn



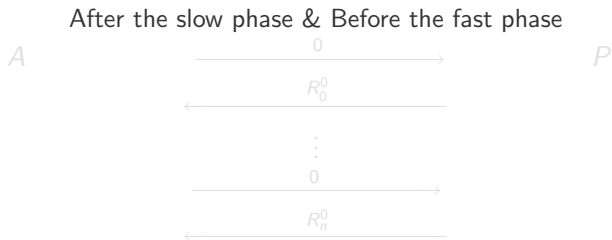
Previous Protocols

Hancke and Kuhn



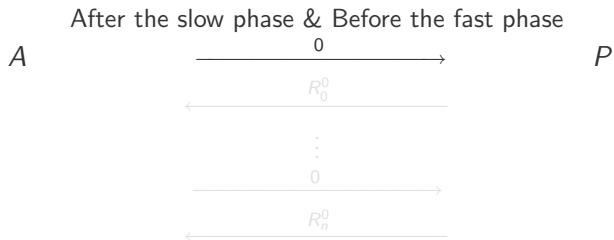
Adversary strategy

Pre-ask Strategy



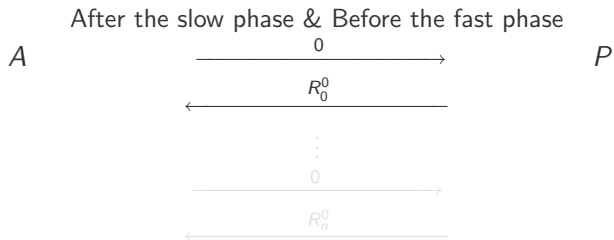
Adversary strategy

Pre-ask Strategy



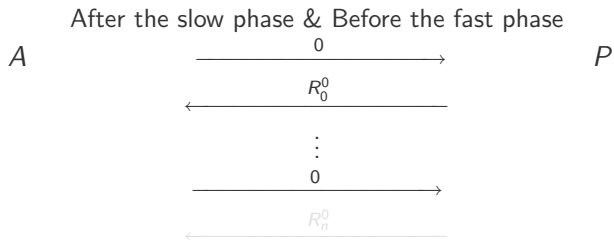
Adversary strategy

Pre-ask Strategy



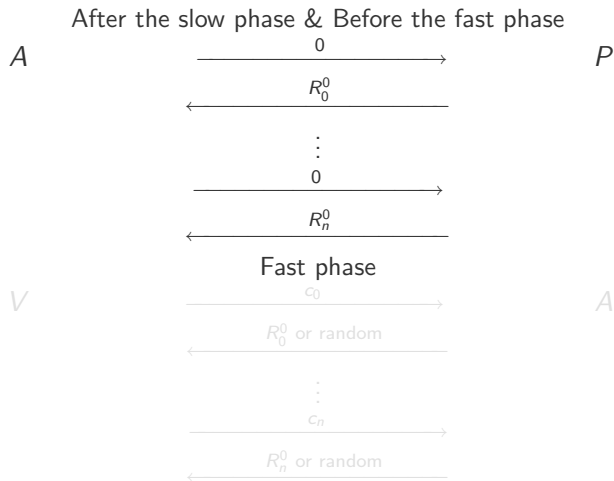
Adversary strategy

Pre-ask Strategy



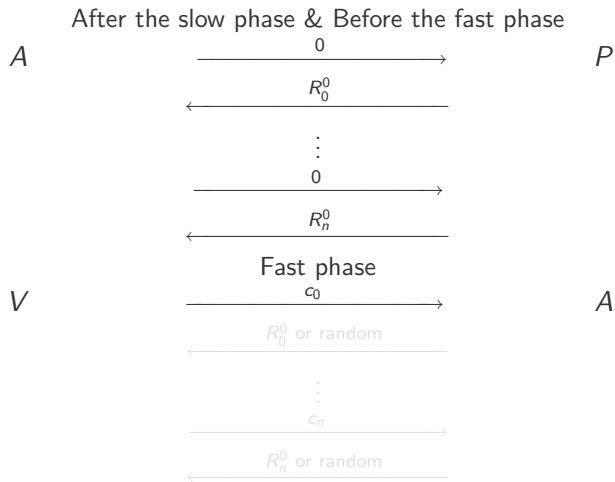
Adversary strategy

Pre-ask Strategy



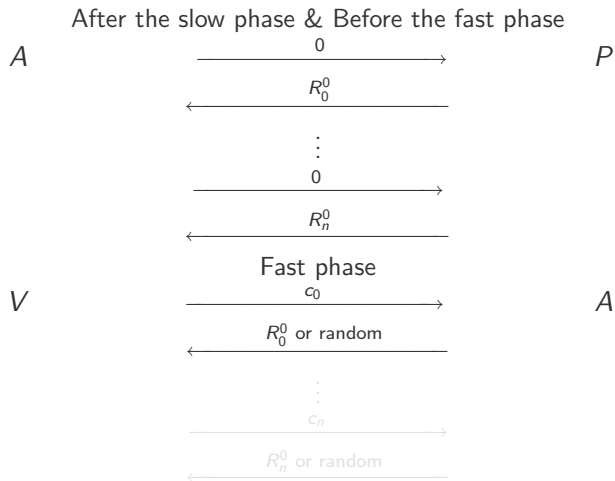
Adversary strategy

Pre-ask Strategy



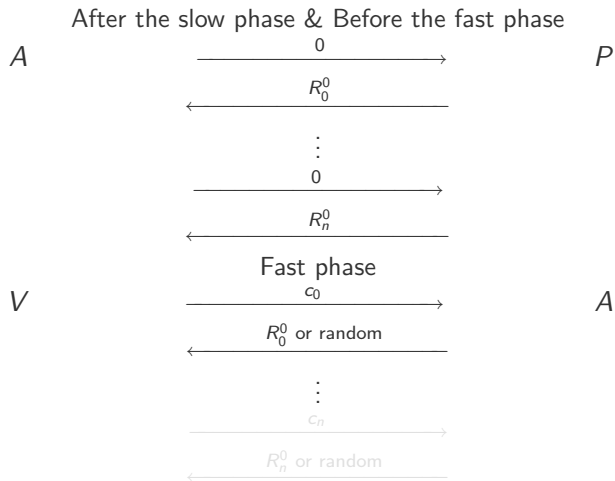
Adversary strategy

Pre-ask Strategy



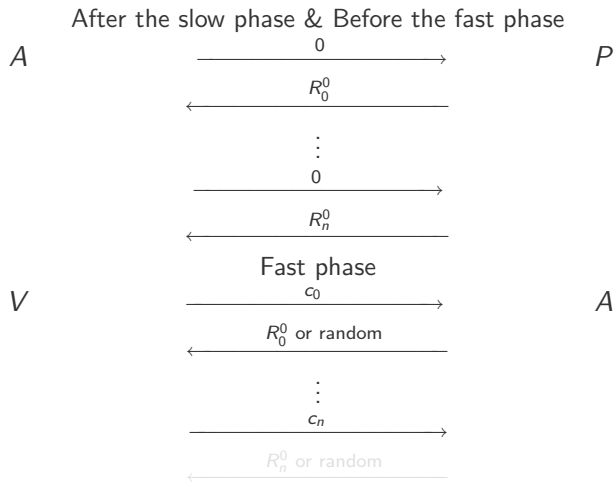
Adversary strategy

Pre-ask Strategy



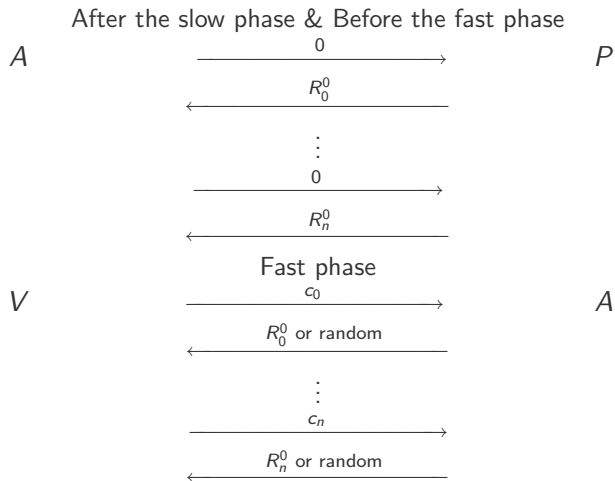
Adversary strategy

Pre-ask Strategy



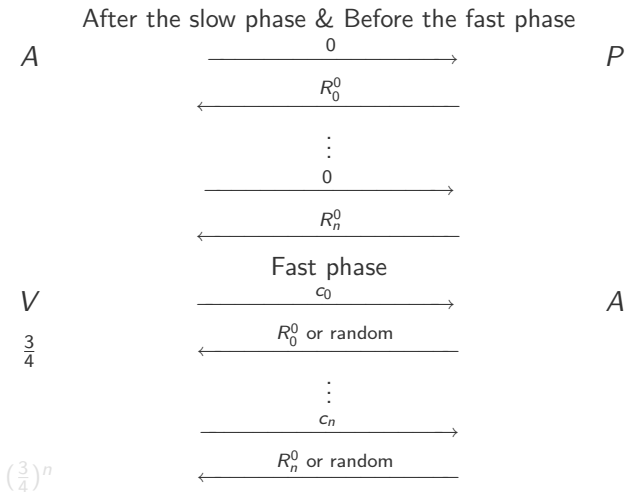
Adversary strategy

Pre-ask Strategy



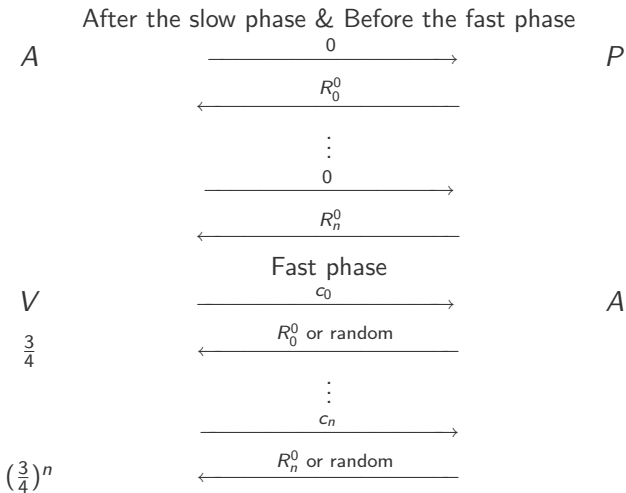
Adversary strategy

Pre-ask Strategy



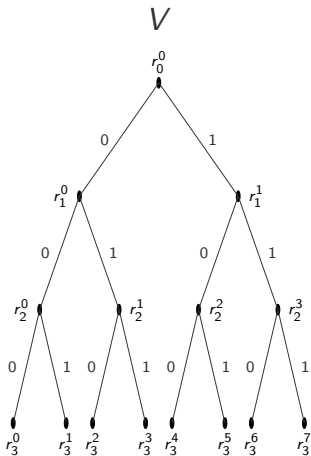
Adversary strategy

Pre-ask Strategy

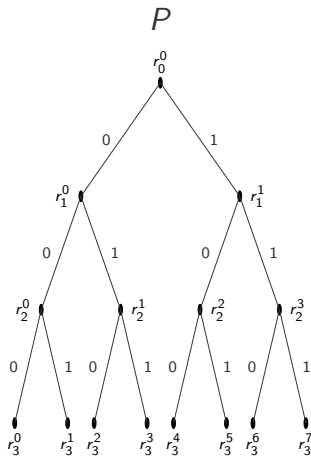


Previous Protocols

Avoine and Tchamkerten

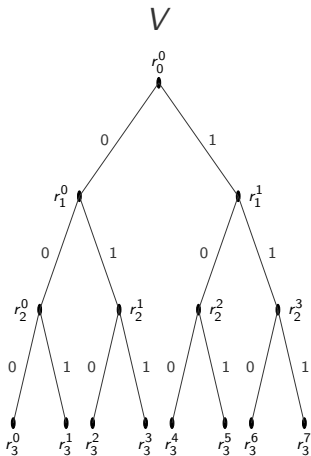


Fast phase



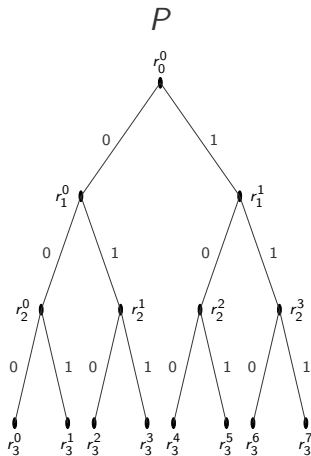
Previous Protocols

Avoine and Tchamkerten



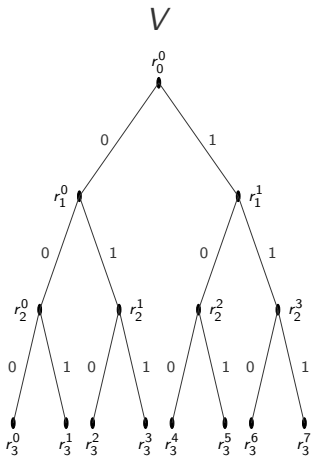
Fast phase

0 →



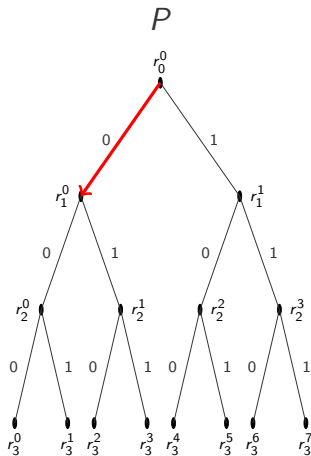
Previous Protocols

Avoine and Tchamkerten



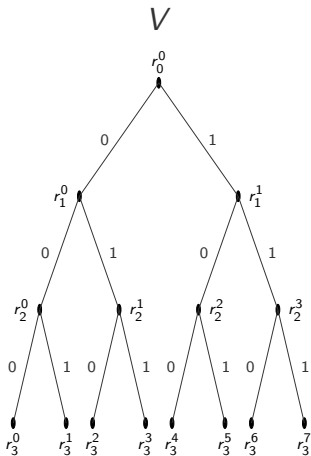
Fast phase

$0 \rightarrow$

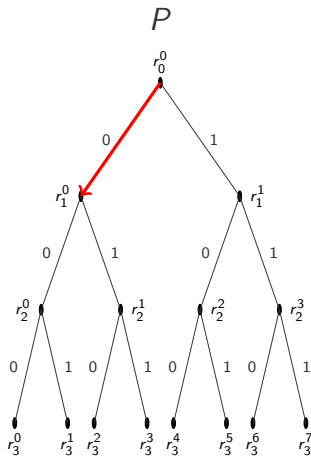
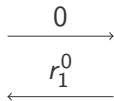


Previous Protocols

Avoine and Tchamkerten

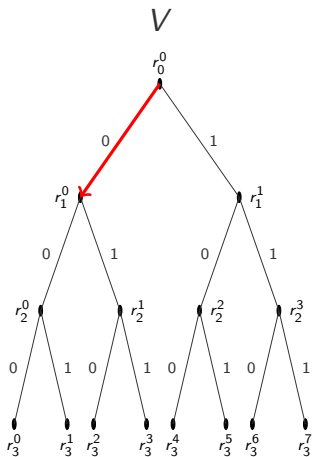


Fast phase

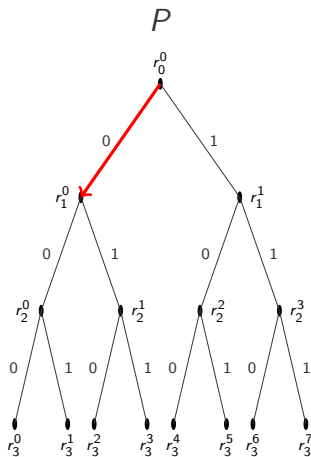
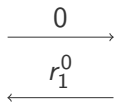


Previous Protocols

Avoine and Tchamkerten

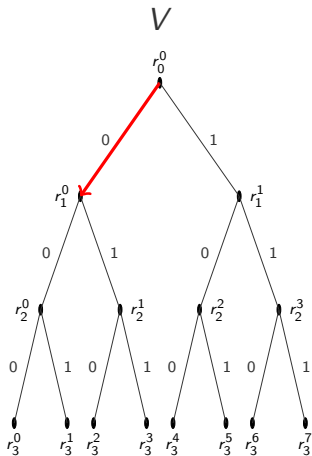


Fast phase

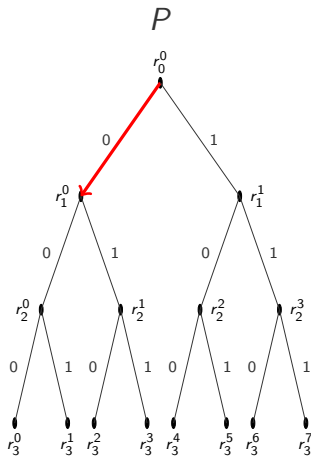
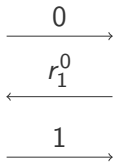


Previous Protocols

Avoine and Tchamkerten

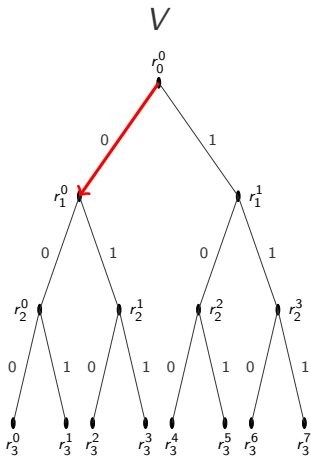


Fast phase

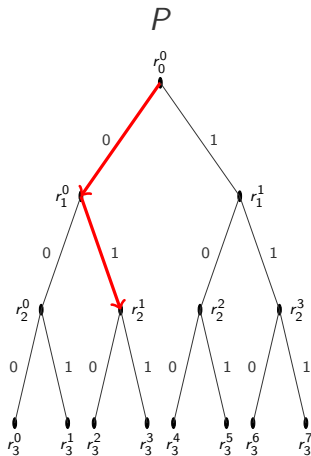
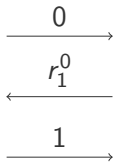


Previous Protocols

Avoine and Tchamkerten

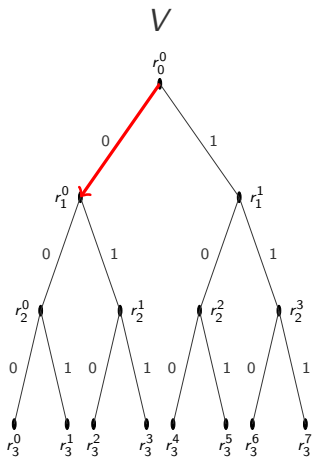


Fast phase

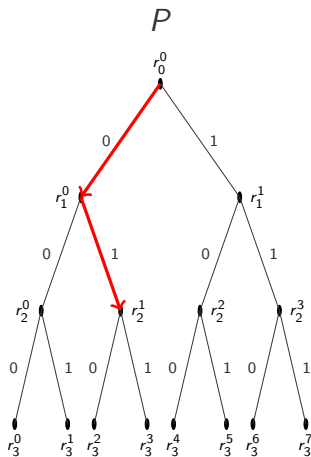
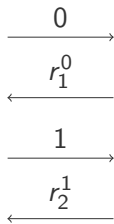


Previous Protocols

Avoine and Tchamkerten

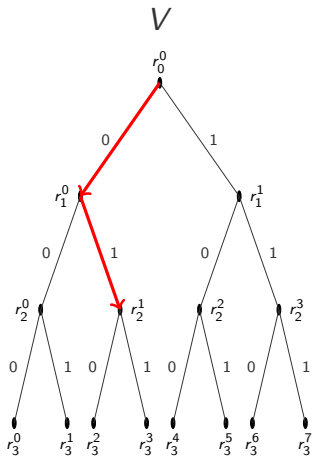


Fast phase

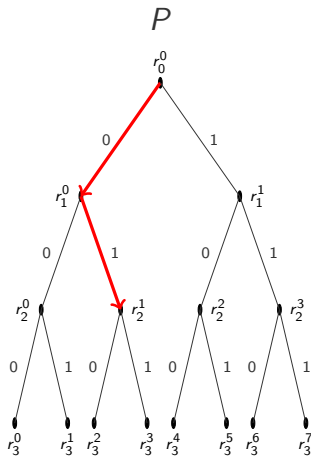
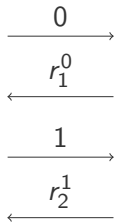


Previous Protocols

Avoine and Tchamkerten

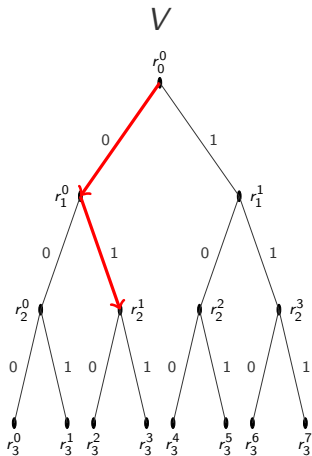


Fast phase

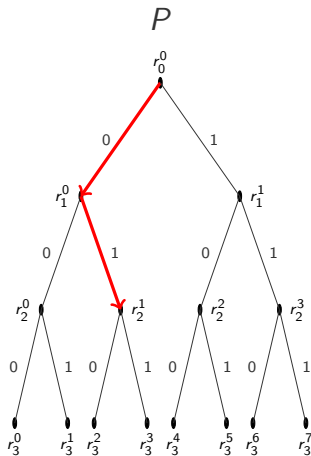
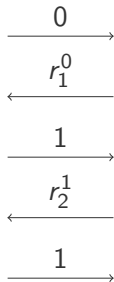


Previous Protocols

Avoine and Tchamkerten

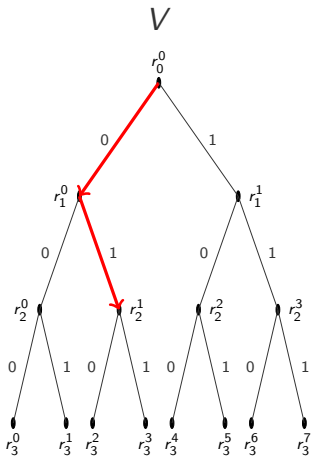


Fast phase

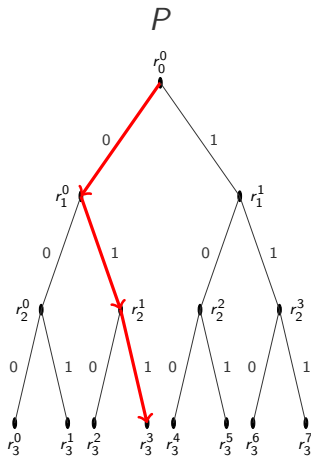
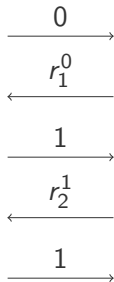


Previous Protocols

Avoine and Tchamkerten

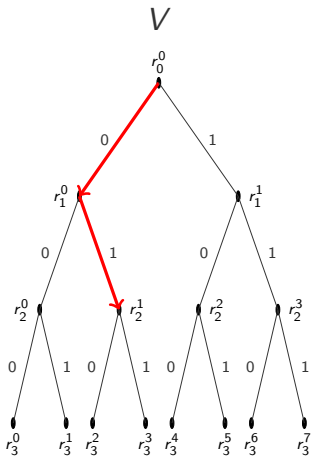


Fast phase

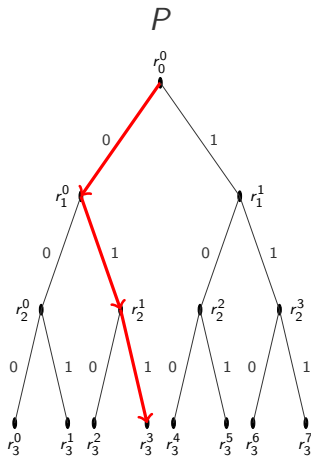
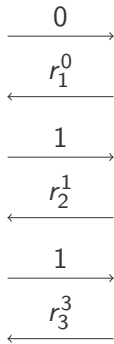


Previous Protocols

Avoine and Tchamkerten

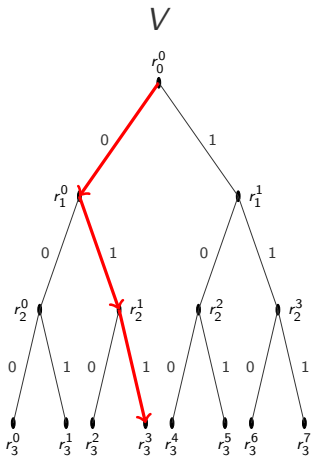


Fast phase

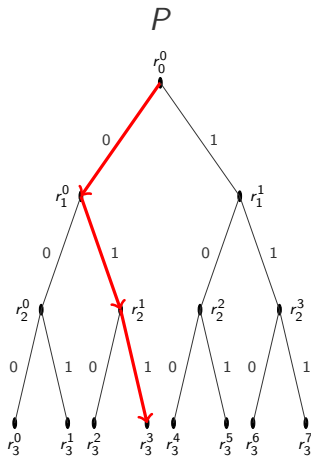
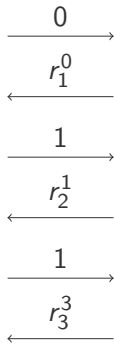


Previous Protocols

Avoine and Tchamkerten

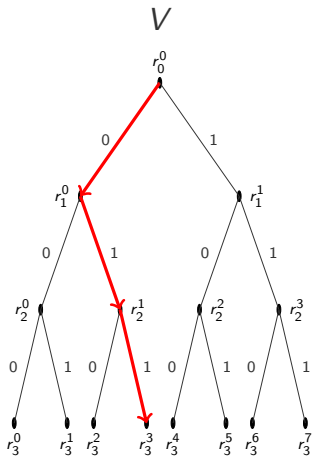


Fast phase

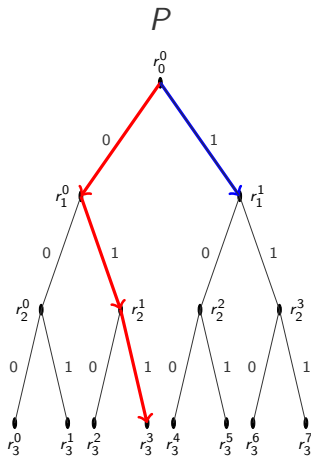
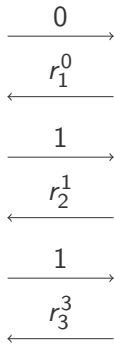


Previous Protocols

Avoine and Tchamkerten

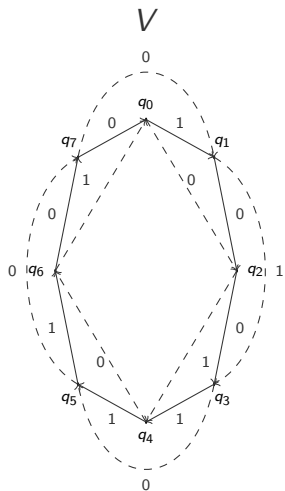


Fast phase

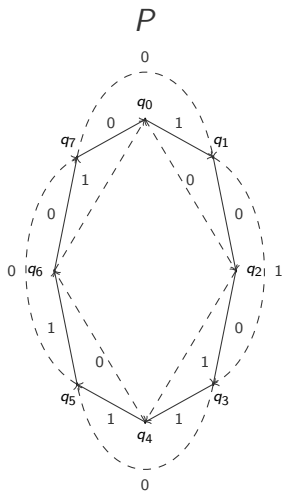


Graph-based Protocols

Our Proposal

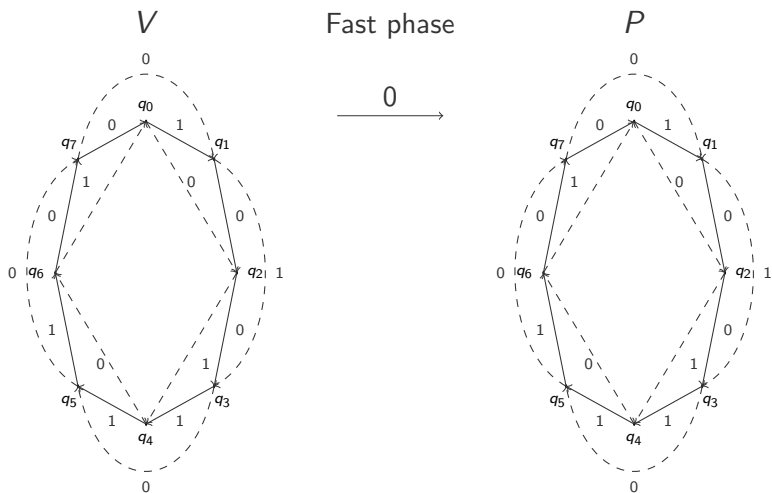


Fast phase



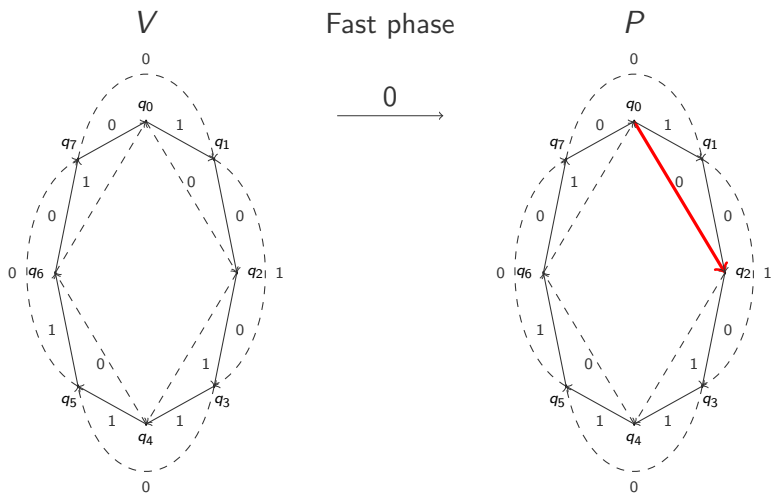
Graph-based Protocols

Our Proposal



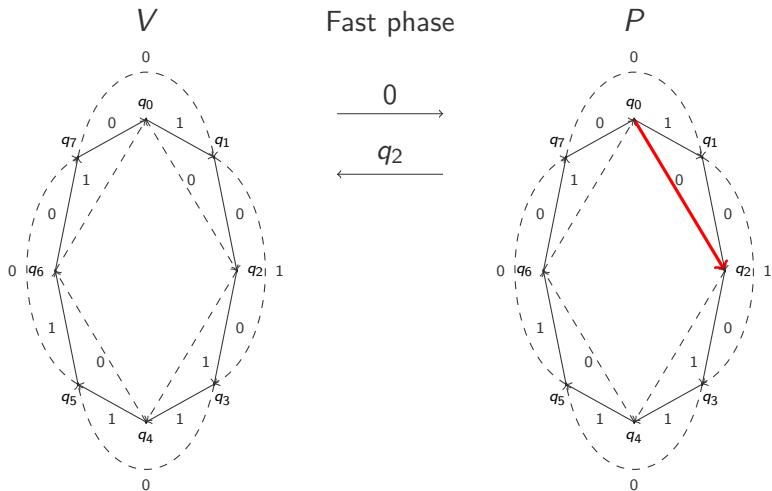
Graph-based Protocols

Our Proposal



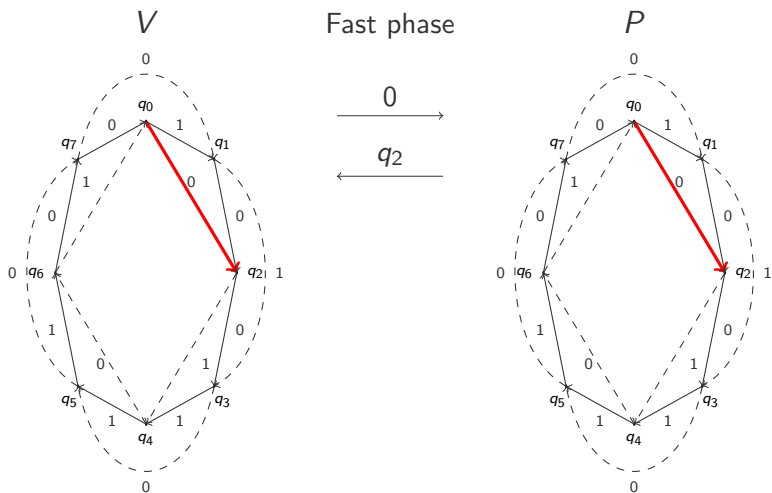
Graph-based Protocols

Our Proposal



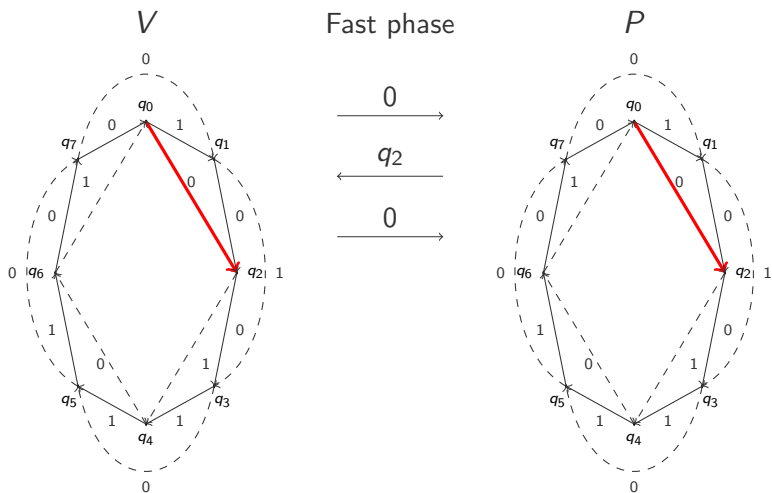
Graph-based Protocols

Our Proposal



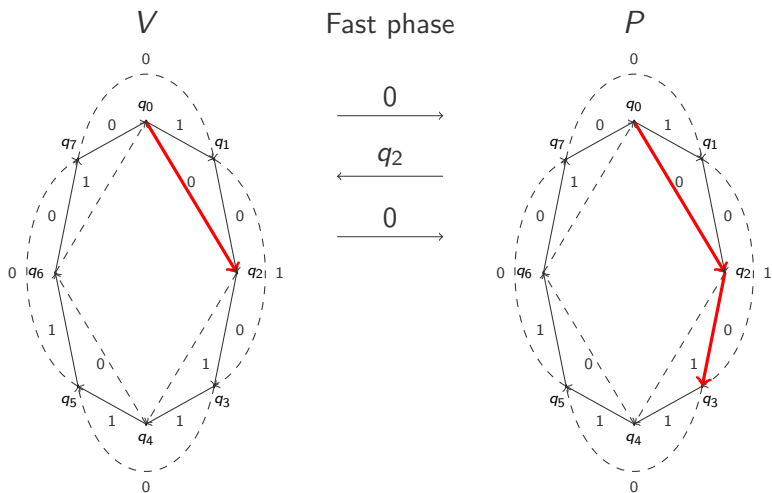
Graph-based Protocols

Our Proposal



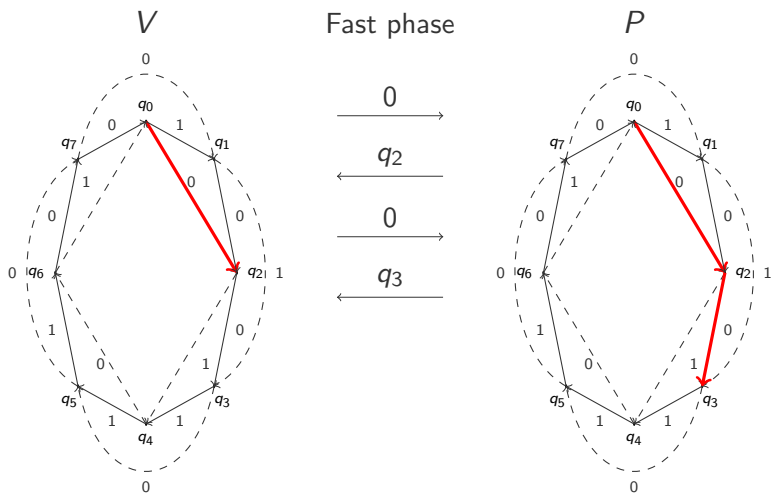
Graph-based Protocols

Our Proposal



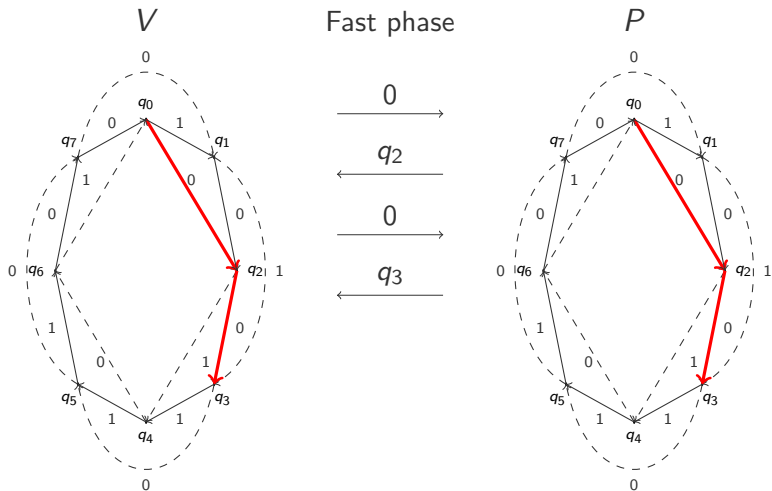
Graph-based Protocols

Our Proposal



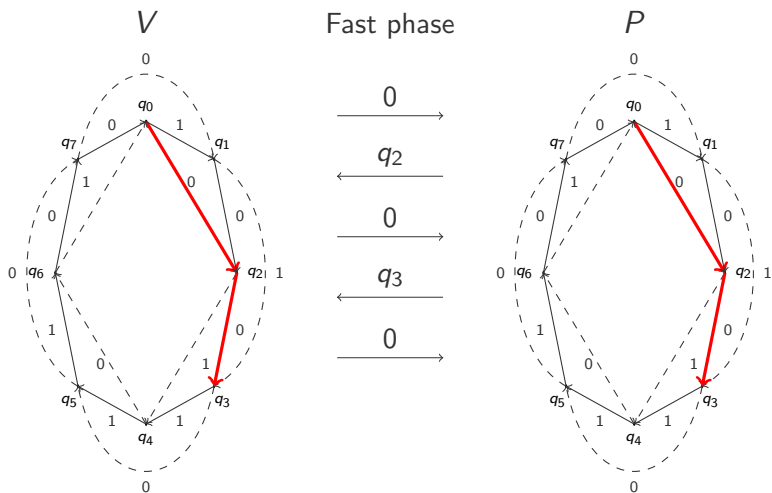
Graph-based Protocols

Our Proposal



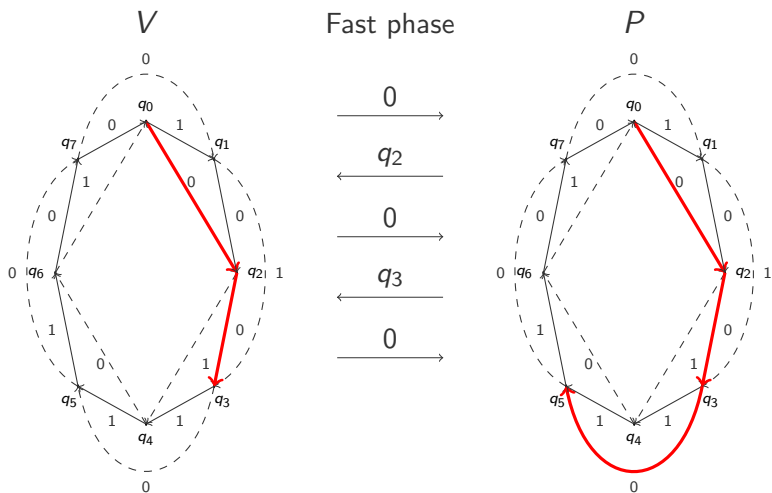
Graph-based Protocols

Our Proposal



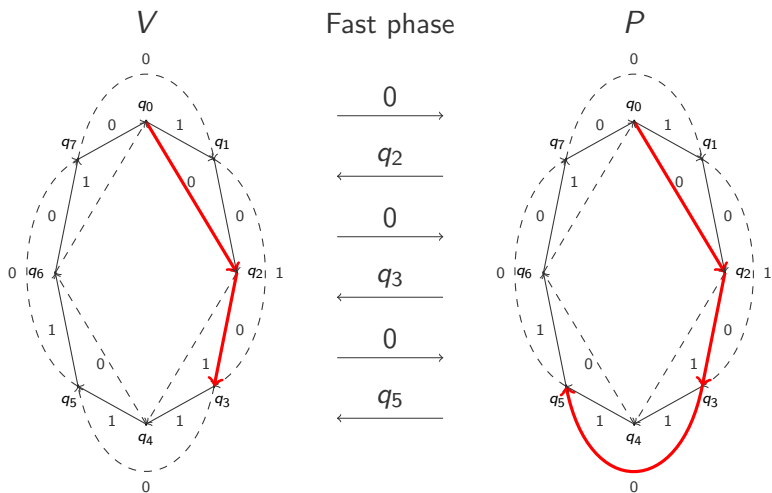
Graph-based Protocols

Our Proposal



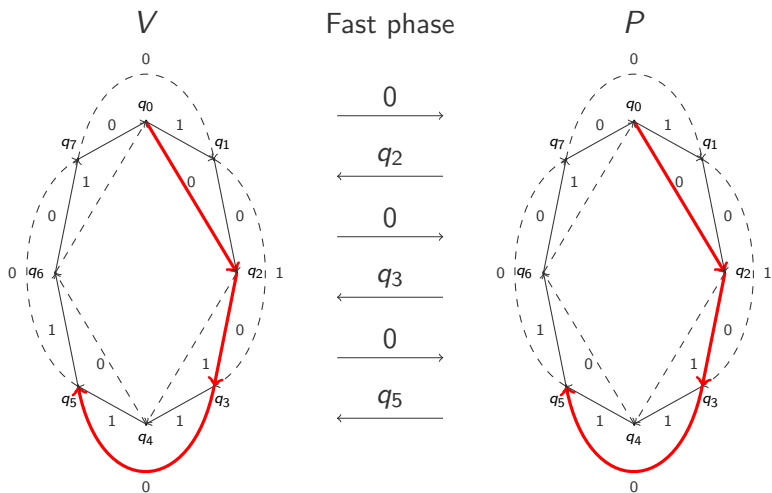
Graph-based Protocols

Our Proposal



Graph-based Protocols

Our Proposal



Comparison

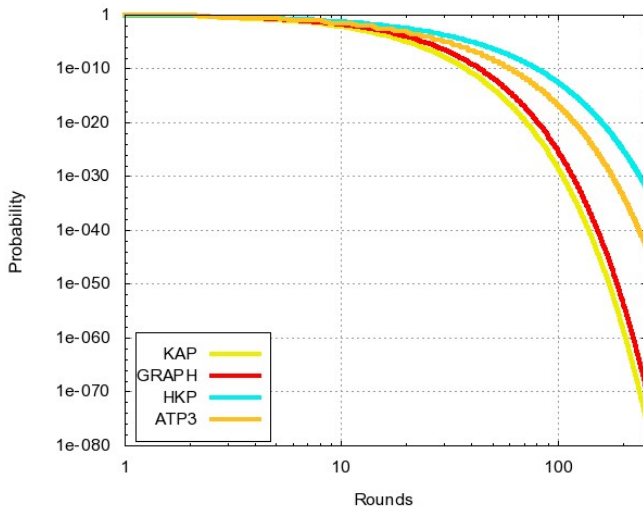
Table

- Hancke and Kuhn Protocol (HKP).
- Kim and Avoine Protocol (KAP).
- Avoine and Tchamkerten Protocol (ATP and ATP3).
- Our Graph-based Protocol (GRAPH).

	Memory	Mafia Fraud	Distance Fraud
HKP	$2n$	$\left(\frac{3}{4}\right)^n$	$\left(\frac{3}{4}\right)^n$
KAP	$4n$	This Paper	$\left(\frac{3}{4} + \frac{p_d}{4}\right)^n$
ATP	$2^{n+1} - 2$	$\left(\frac{1}{2}\right)^n \left(\frac{n}{2} + 1\right)$	Upper Bounded
ATP3	$\frac{14n}{3}$	$\left(\frac{1}{2}\right)^n \left(\frac{5}{2}\right)^{\frac{n}{3}}$	$(0.3999)^{\frac{n}{3}}$
GRAPH	$4n$	This Paper	Upper Bounded

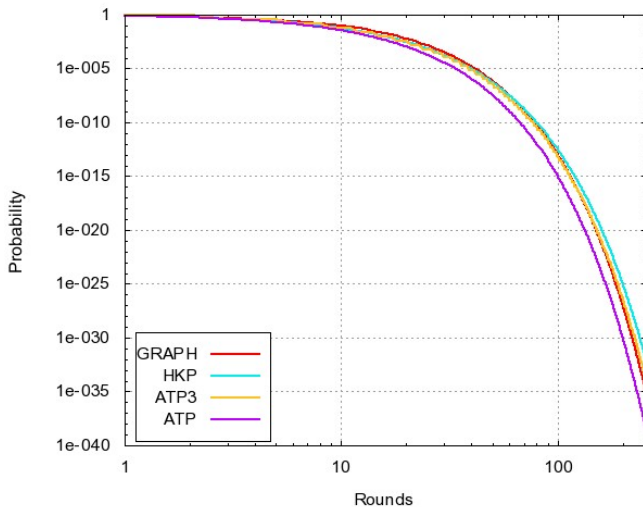
Comparison

Mafia Fraud



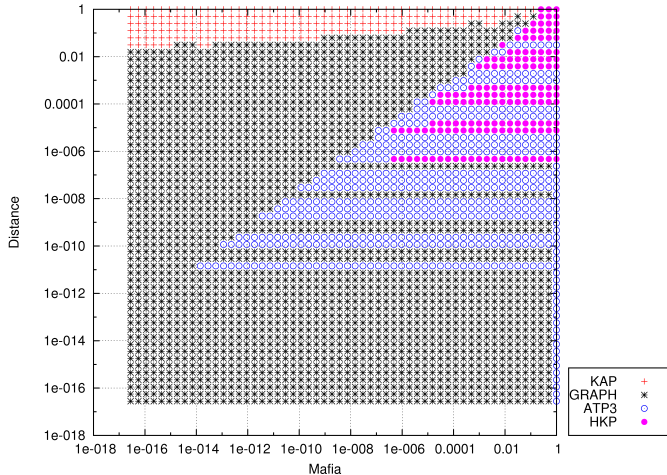
Comparison

Distance Fraud



Comparison

Distance Fraud



Discussion

- To know if there are graph-based protocols that behave still better.
- To know if it is possible to use a node twice.
- To find the exact distance fraud probability of success for the graph-based protocol.

Thanks