A class of precomputation-based distance-bounding protocols

Jorge Toro-Pozo
University of Luxembourg

(joint work with Sjouke Mauw and Rolando Trujillo-Rasua,
to appear at Euro S&P 2016)

Nancy, France. March 16, 2016

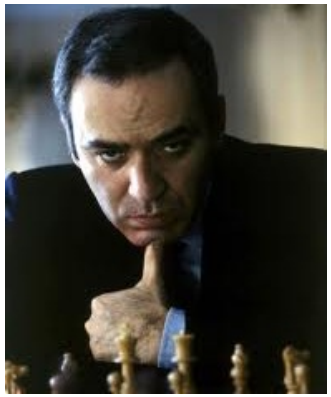
Relay attack: how to beat a grand master

White

Relay attack: how to beat a grand master

White

Black

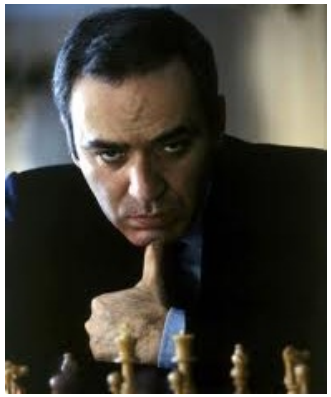


Relay attack: how to beat a grand master

White

d4

Black



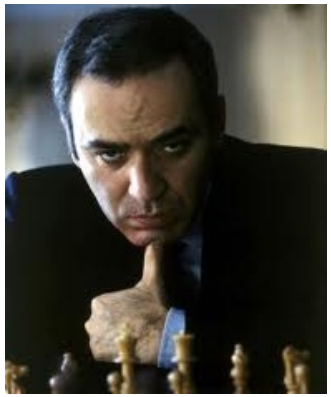
Relay attack: how to beat a grand master

White

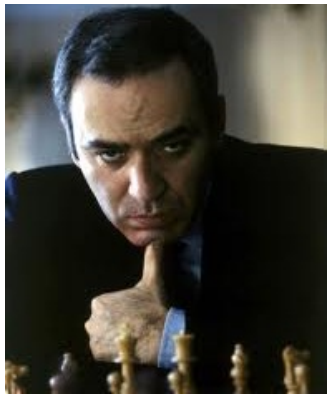
d4

Black

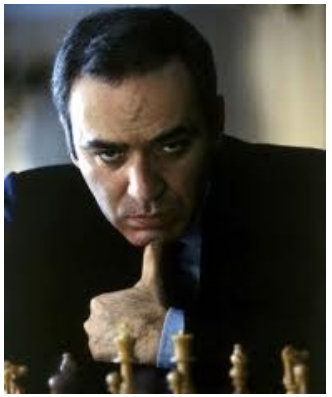
d4



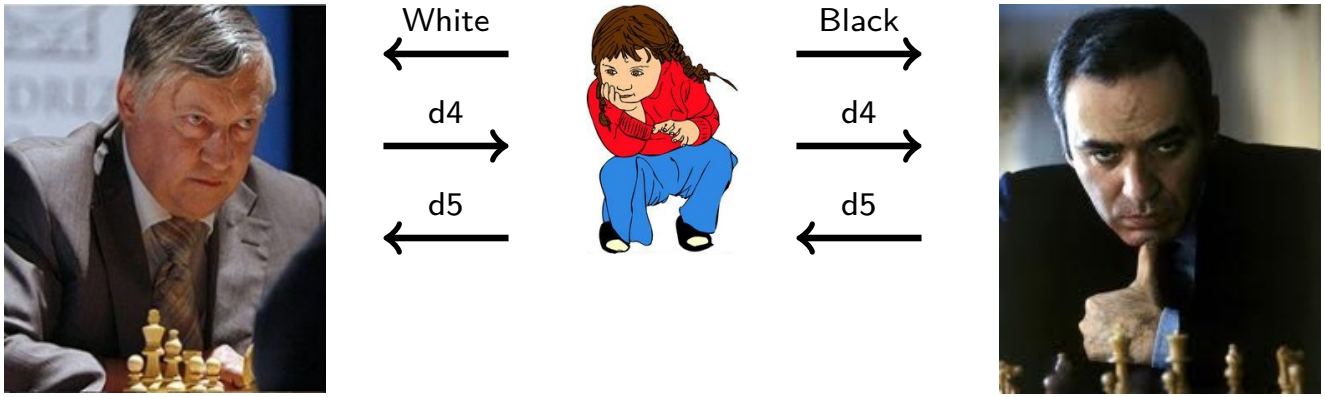
Relay attack: how to beat a grand master



Relay attack: how to beat a grand master



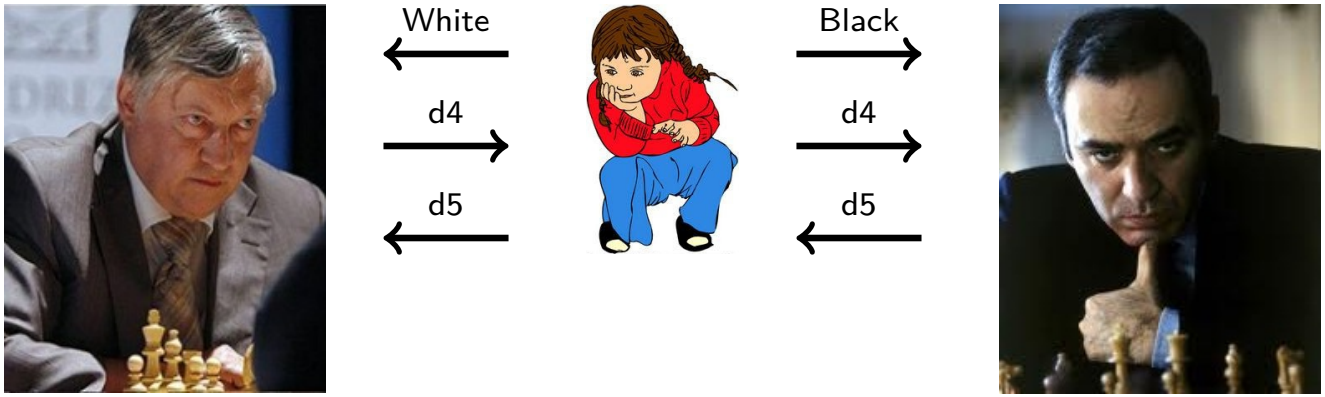
Relay attack: how to beat a grand master



Definition (Relay attack)

A relay attack is a man-in-the-middle attack where the adversary manipulates the communication by only relaying the verbatim messages between reader and the tag.

Relay attack: how to beat a grand master



Definition (Relay attack)

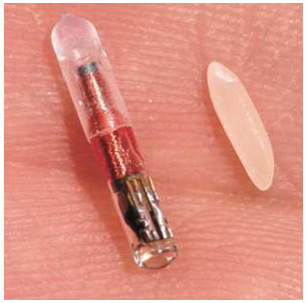
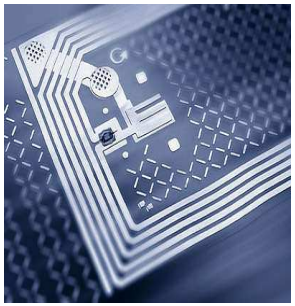
A relay attack is a man-in-the-middle attack where the adversary manipulates the communication by only relaying the verbatim messages between reader and the tag.

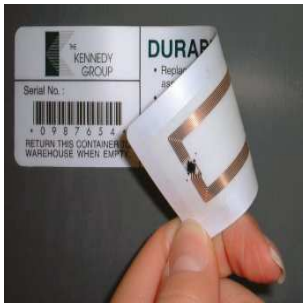
Solution: distance bounding protocols

Definition (Distance Bounding)

A distance bounding protocol is an authentication protocol that in addition checks the distance between tag and reader. The computed distance is an upper-bound on their actual distance.

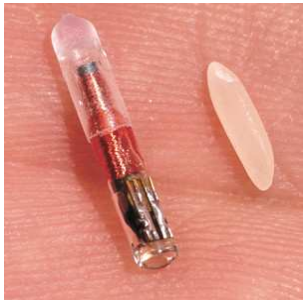
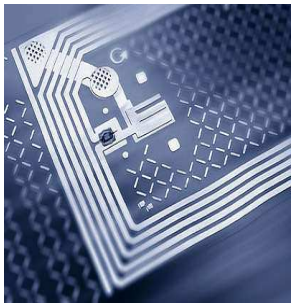
Radio Frequency Identification - RFID

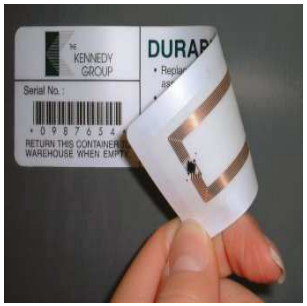






- Communication is contactless.
- Line-of-sight is not necessary.
- Messages are broadcast.
- Limited resources (memory, processor speed, energy, interaction time).

Radio Frequency Identification - RFID

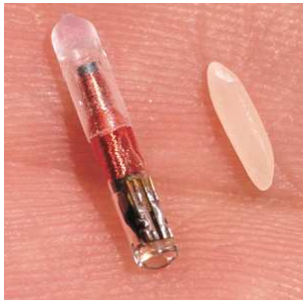
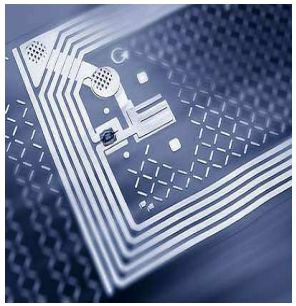






- Communication is contactless.
- Line-of-sight is not necessary.
- Messages are broadcast.
- Limited resources (memory, processor speed, energy, interaction time).

- Tags respond to the reader's requests without explicit agreement of their holder

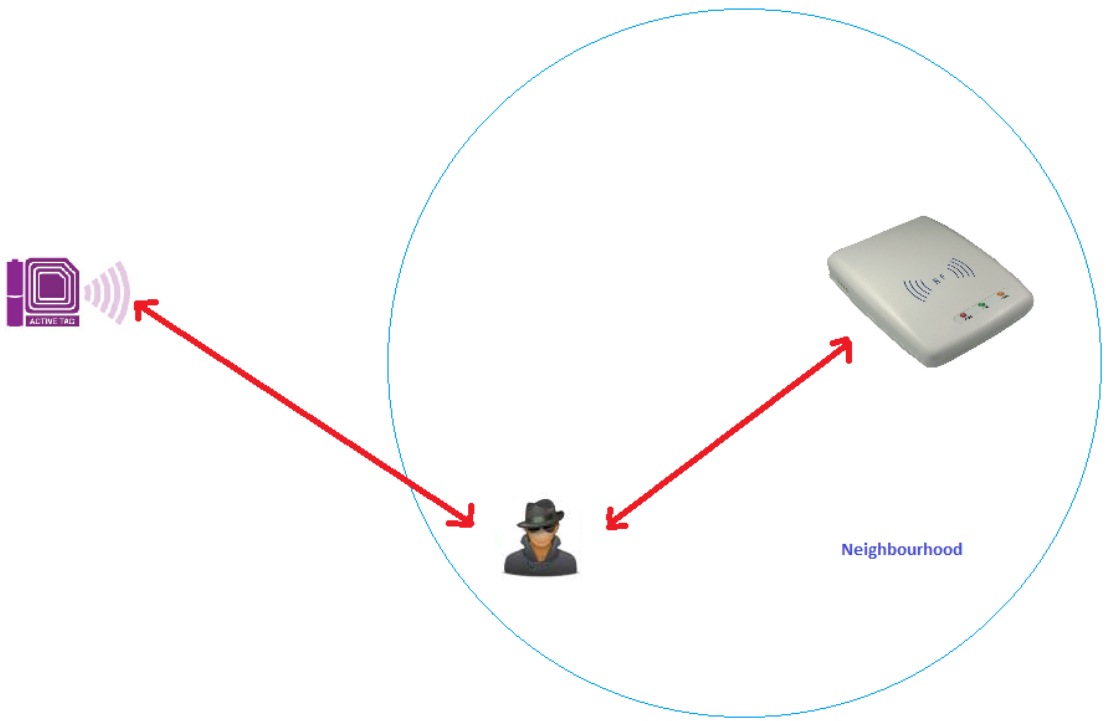
Radio Frequency Identification - RFID

- Communication is contactless.
- Line-of-sight is not necessary.
- Messages are broadcast.
- Limited resources (memory, processor speed, energy, interaction time).
- Tags respond to the reader's requests without explicit agreement of their holder

Distance bounding protocols are vulnerable

Mafia-fraud attacks

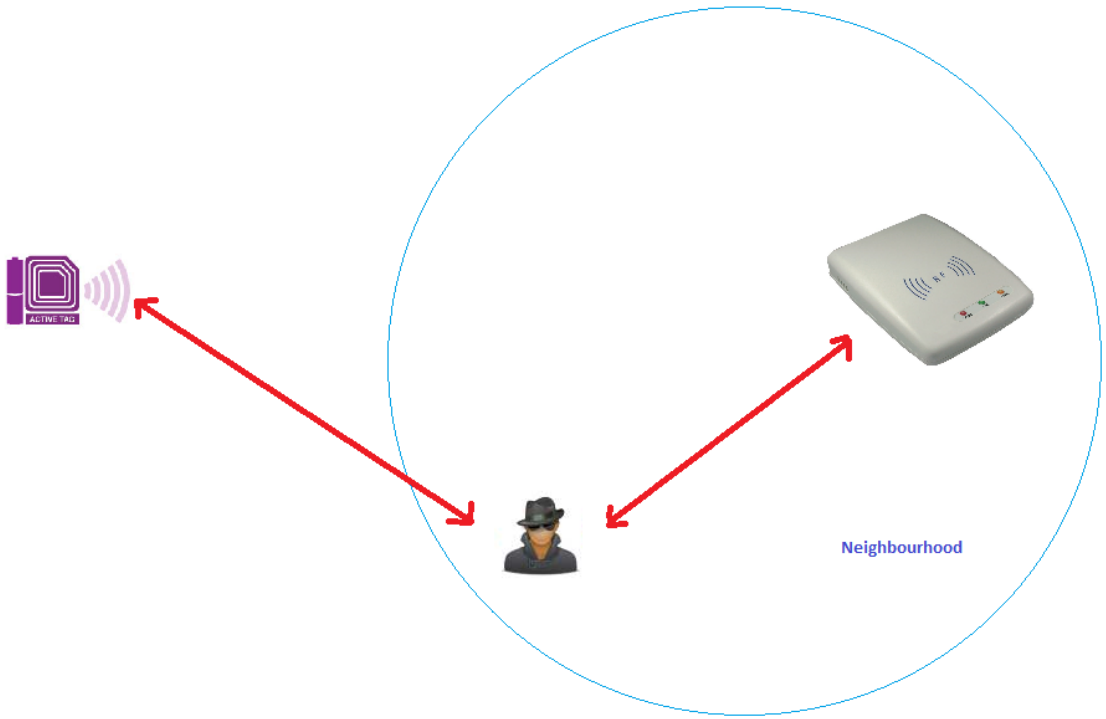


... and also to other attacks, e.g.

- distance fraud
- terrorist fraud
- distance hijacking

Distance bounding protocols are vulnerable

Mafia-fraud attacks



... and also to other attacks, e.g.

- distance fraud
- terrorist fraud
- distance hijacking

A few distance bounding protocols

- Brands and Chaum (Fiat-Shamir)
- Brands and Chaum (Schnorr)
- Brands and Chaum (signature)
- Bussard and Bagga
- CRCS
- Hancke and Kuhn
- Hitomi
- KA2
- Kuhn, Luecken, Tippenhauer
- MAD
- Meadows et al. for $F(\cdots) = \langle NV, NP \oplus P \rangle$
- Munilla and Peinado
- Noise resilient MAD
- Poulidor
- Reid et al.
- Swiss-Knife
- Tree
- WSBC+DB
- WSBC+DB Noent

Many of them have been broken

- ~~Brands and Chaum (Fiat-Shamir)~~
- ~~Brands and Chaum (Schnorr)~~
- ~~Brands and Chaum (signature)~~
- Bussard and Bagga
- ~~CRCS~~
- Hancke and Kuhn
- Hitomi
- KA2
- ~~Kuhn, Luecken, Tippenhauer~~
- ~~MAD~~
- ~~Meadows et al. for $F(\cdots) = \langle NV, NP \oplus P \rangle$~~
- Munilla and Peinado
- ~~Noise resilient MAD~~
- Poulidor
- Reid et al.
- Swiss-Knife
- Tree
- ~~WSBC+DB~~
- ~~WSBC+DB Noent~~

Some common principles

- Are composed by two phases:
  - Slow phase: generation of random values, exchange of parameters, preparation of data structures.
  - Fast phase: 1-bit messages, tag performs at most lookup/and/xor/...; repeat this n times.
- Need very short processing time at the tag (otherwise the adversary could overclock the tag).

Some common principles

- Are composed by two phases:
  - Slow phase: generation of random values, exchange of parameters, preparation of data structures.
  - Fast phase: 1-bit messages, tag performs at most lookup/and/xor/...; repeat this n times.
- Need very short processing time at the tag (otherwise the adversary could overclock the tag).
- Perform the authentication during the fast phase.

Some common principles

- Are composed by two phases:
  - Slow phase: generation of random values, exchange of parameters, preparation of data structures.
  - Fast phase: 1-bit messages, tag performs at most lookup/and/xor/...; repeat this n times.
- Need very short processing time at the tag (otherwise the adversary could overclock the tag).
- Perform the authentication during the fast phase.
- Do not have a final slow phase.

Some common principles

- Are composed by two phases:
  - Slow phase: generation of random values, exchange of parameters, preparation of data structures.
  - Fast phase: 1-bit messages, tag performs at most lookup/and/xor/...; repeat this n times.
- Need very short processing time at the tag (otherwise the adversary could overclock the tag).
- Perform the authentication during the fast phase.
- Do not have a final slow phase.

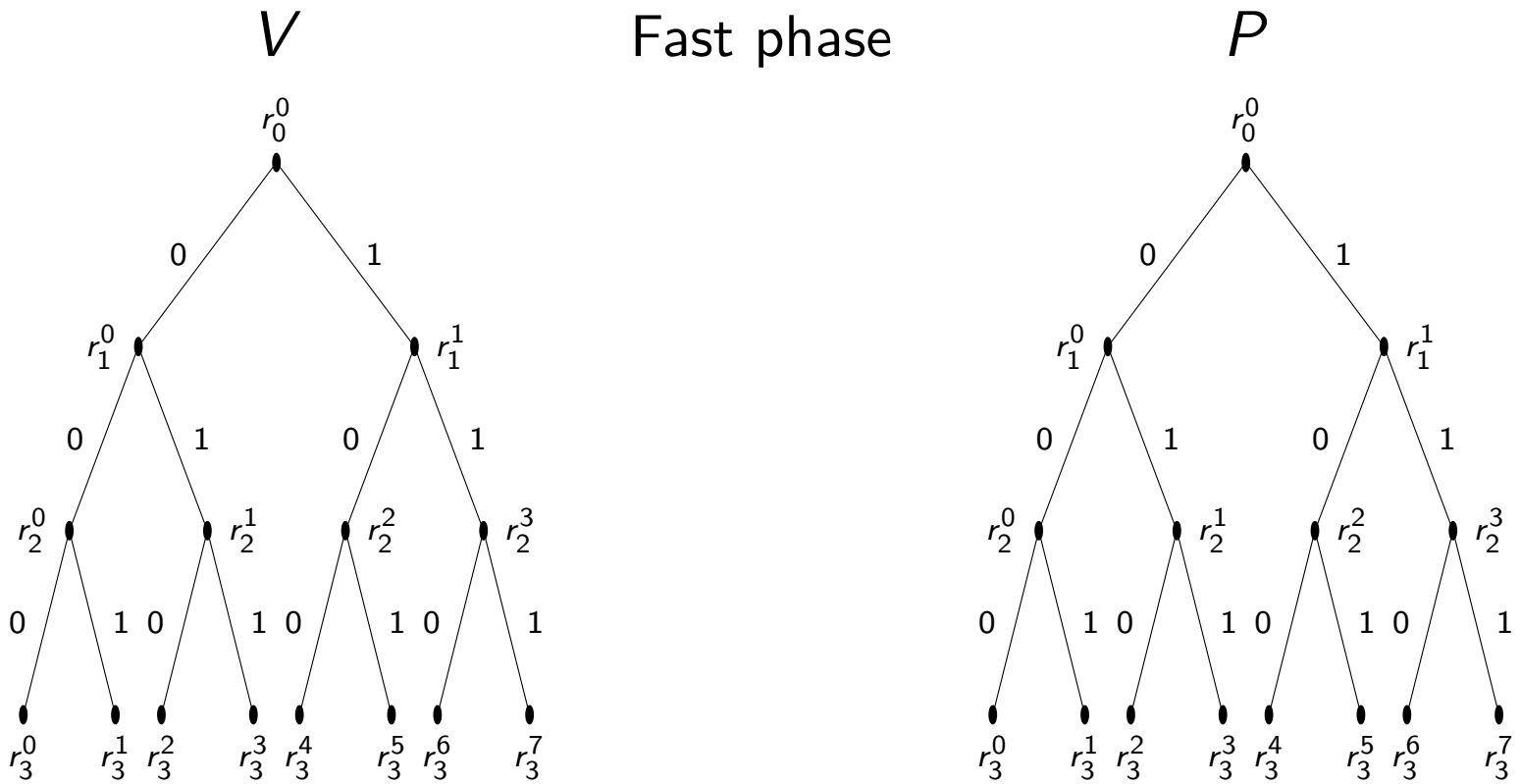
We call them Lookup-based protocols

Some common principles

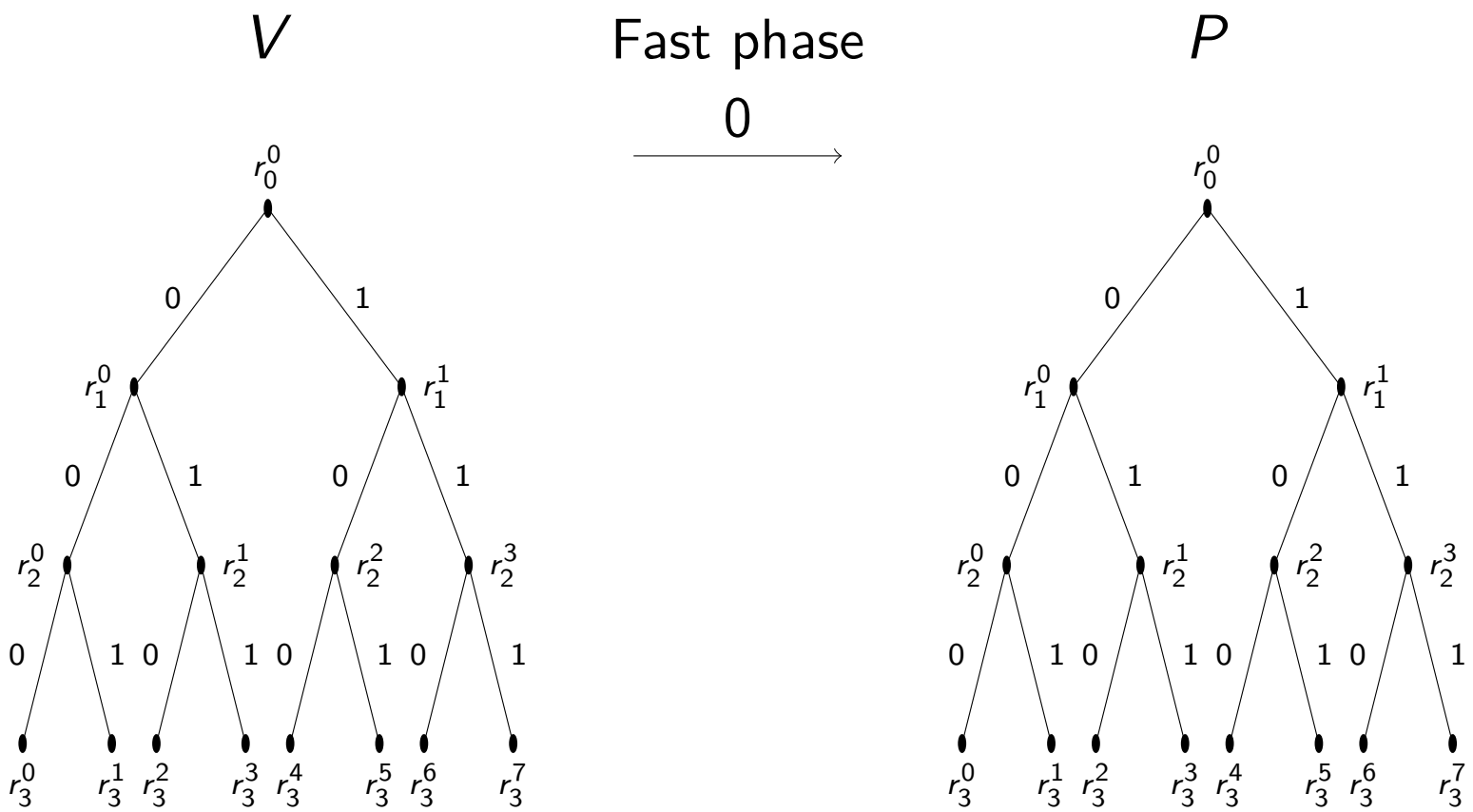
- Are composed by two phases:
  - Slow phase: generation of random values, exchange of parameters, preparation of data structures.
  - Fast phase: 1-bit messages, tag performs at most lookup/and/xor/...; repeat this n times.
- Need very short processing time at the tag (otherwise the adversary could overclock the tag).
- Perform the authentication during the fast phase.
- Do not have a final slow phase.

We call them Lookup-based protocols

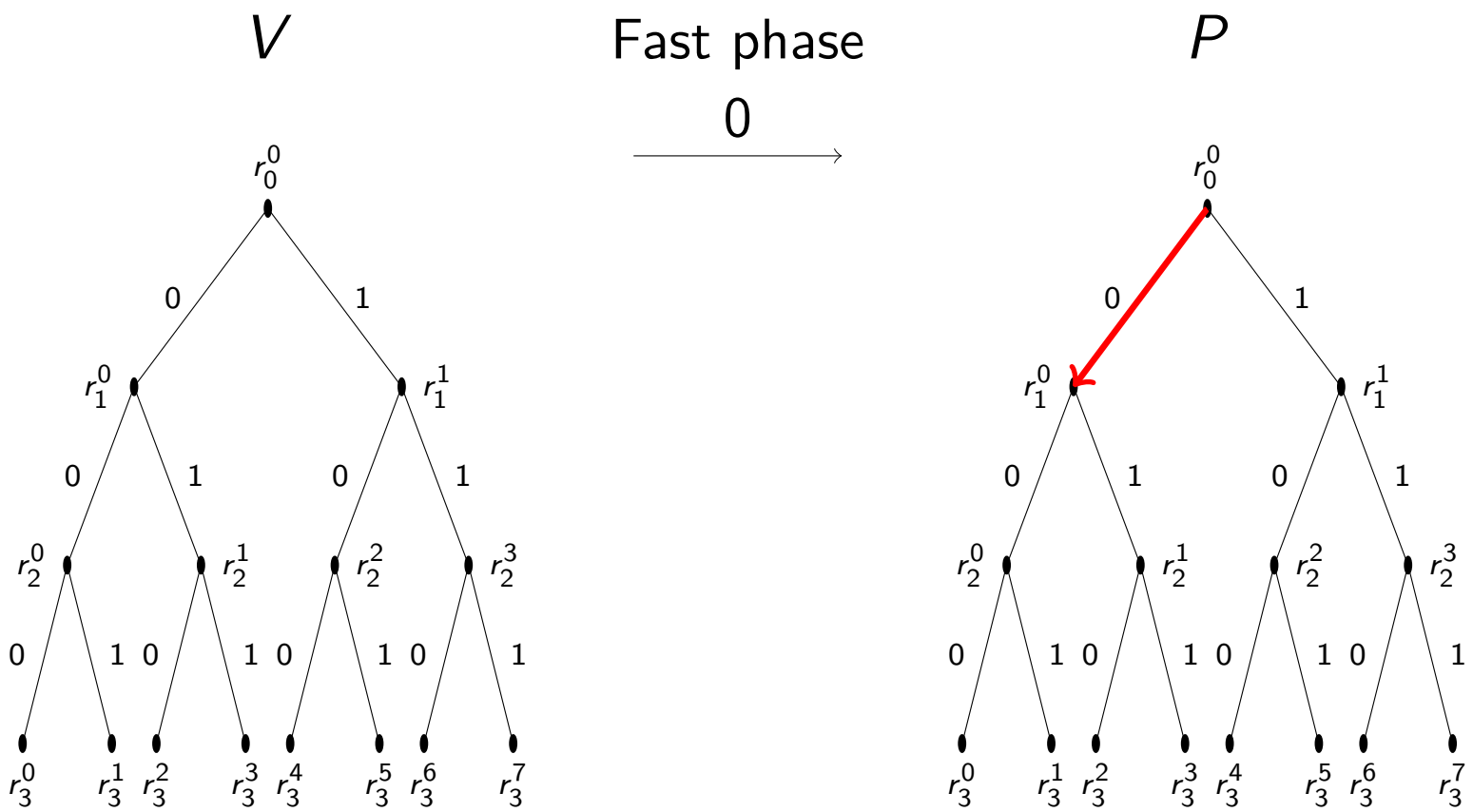
Avoine and Tchamkerten's proposal (2009)



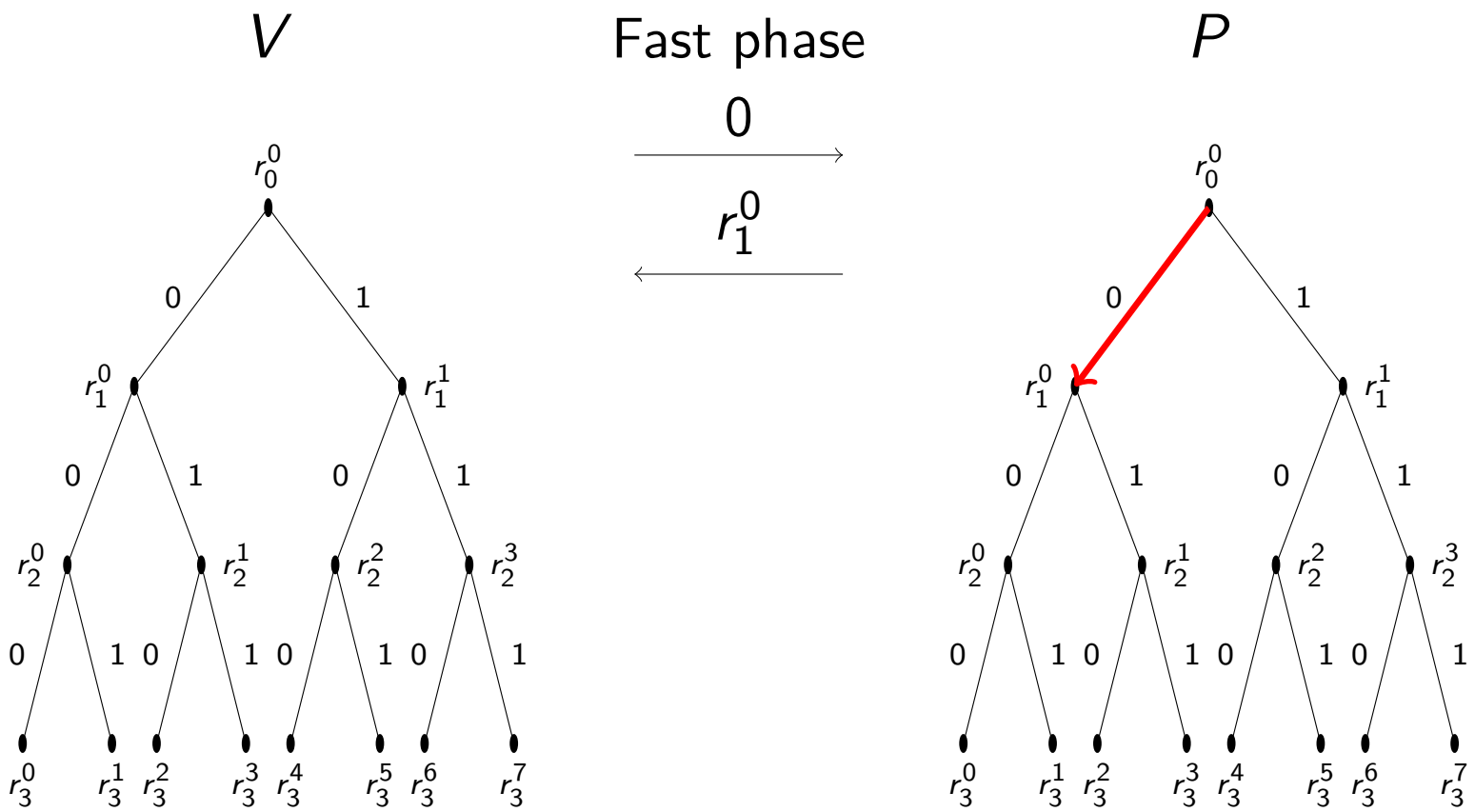
Avoine and Tchamkerten's proposal (2009)



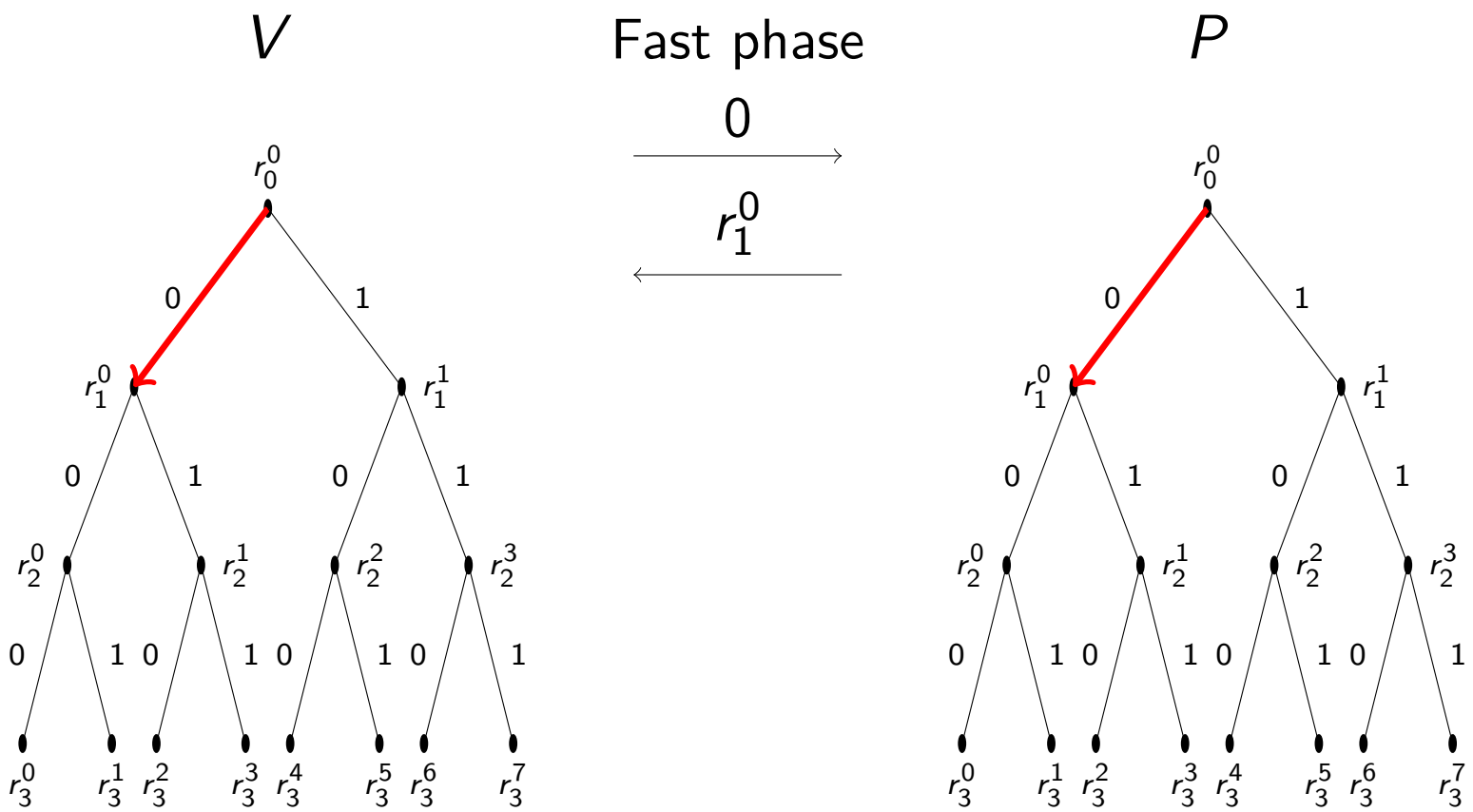
Avoine and Tchamkerten's proposal (2009)



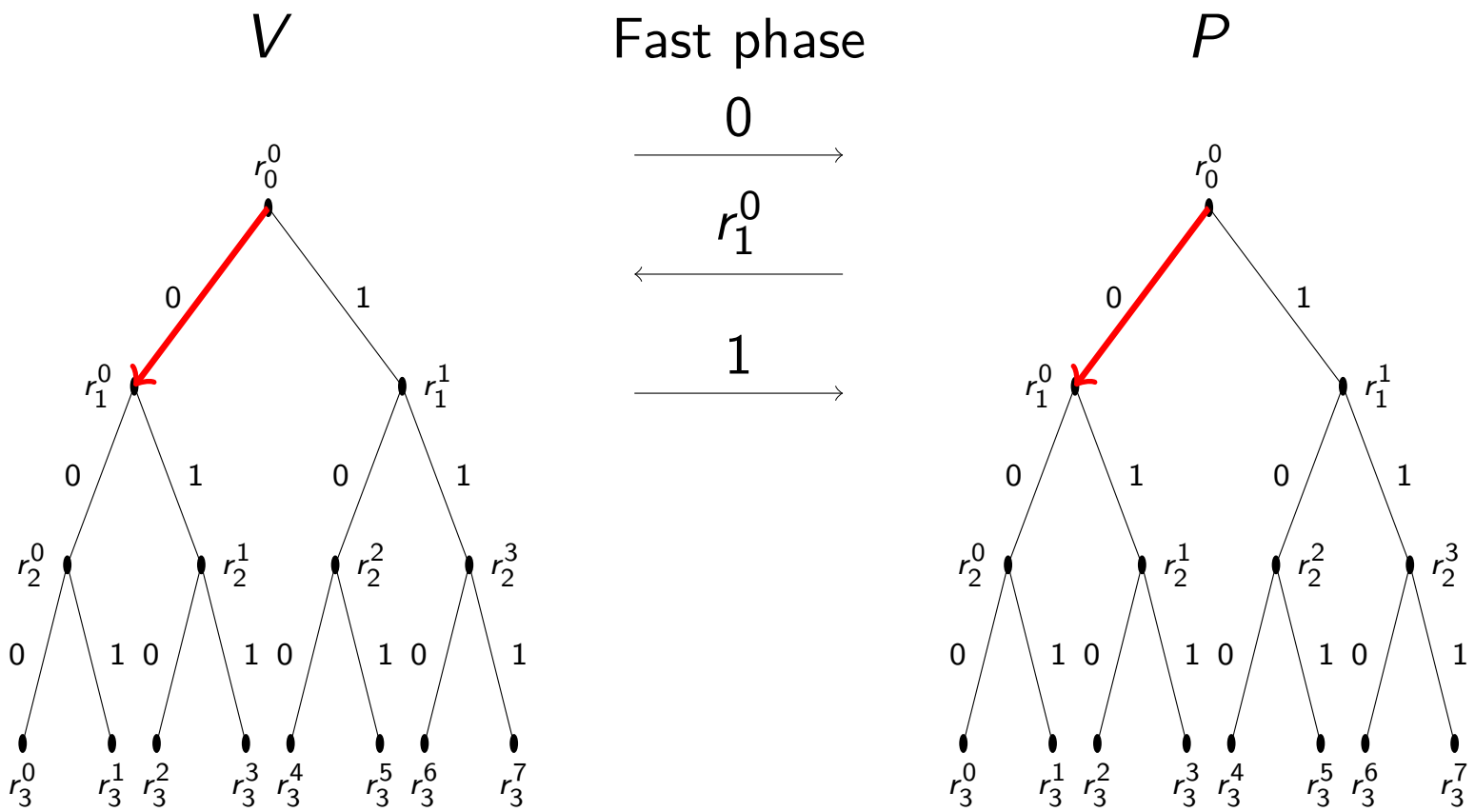
Avoine and Tchamkerten's proposal (2009)



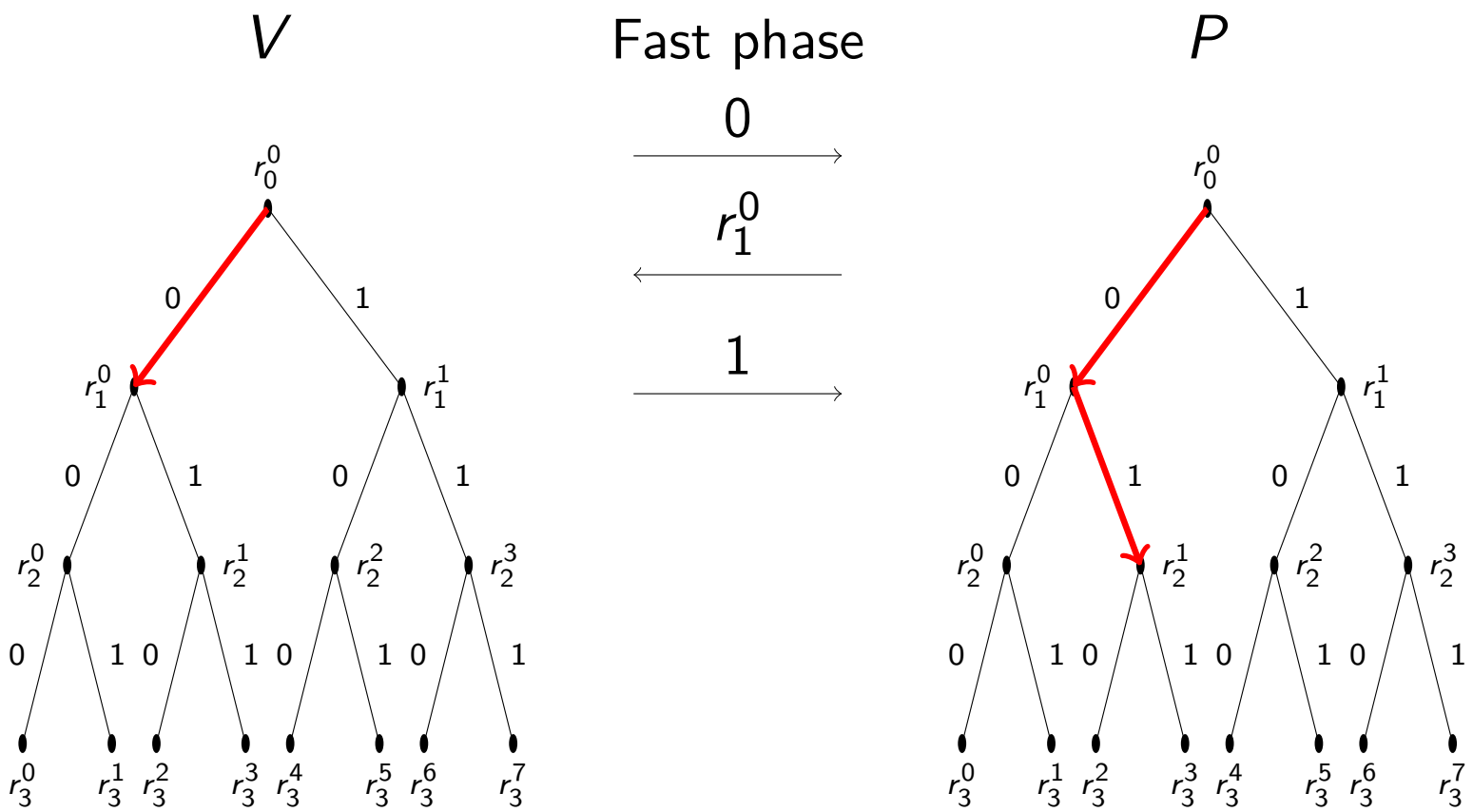
Avoine and Tchamkerten's proposal (2009)



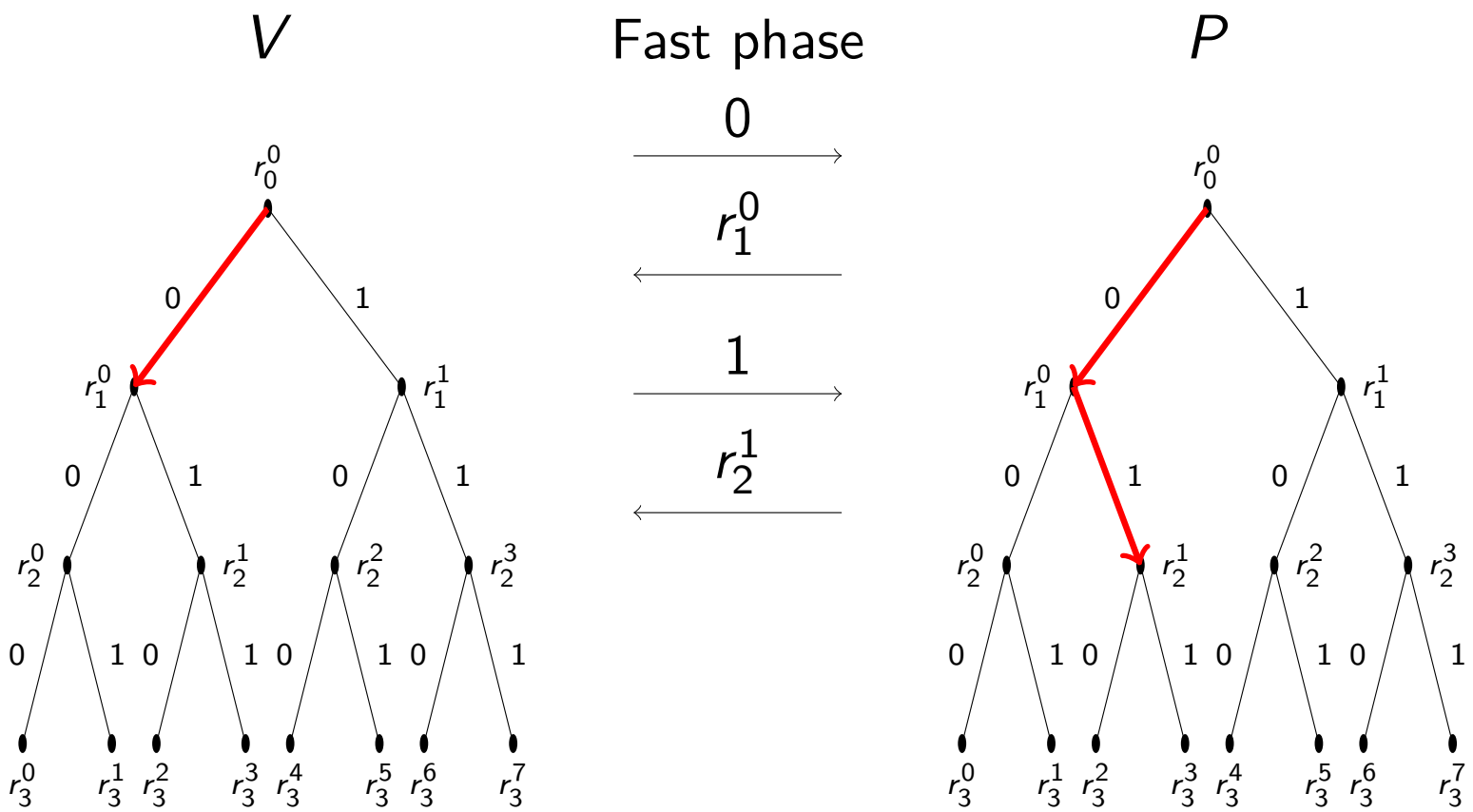
Avoine and Tchamkerten's proposal (2009)



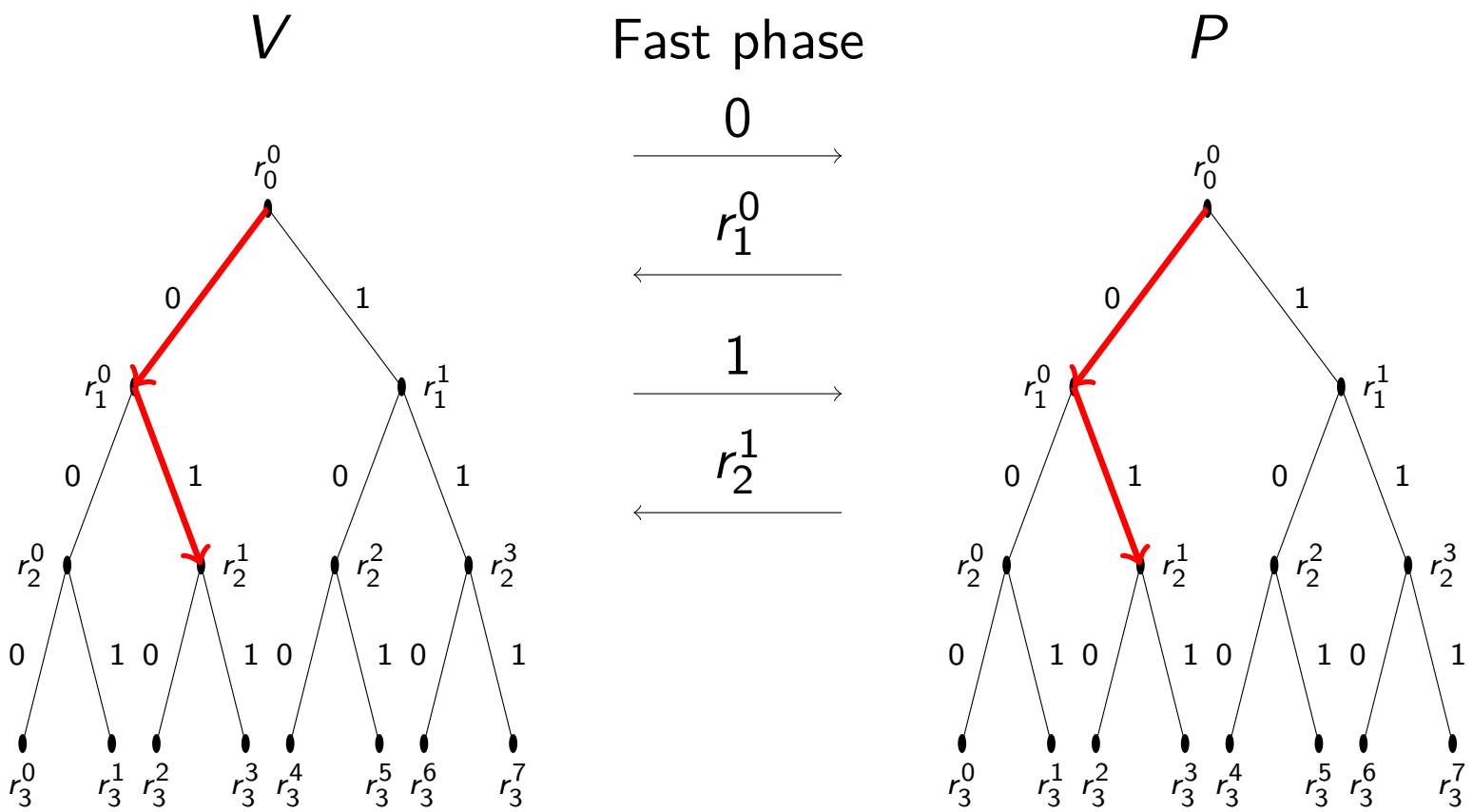
Avoine and Tchamkerten's proposal (2009)



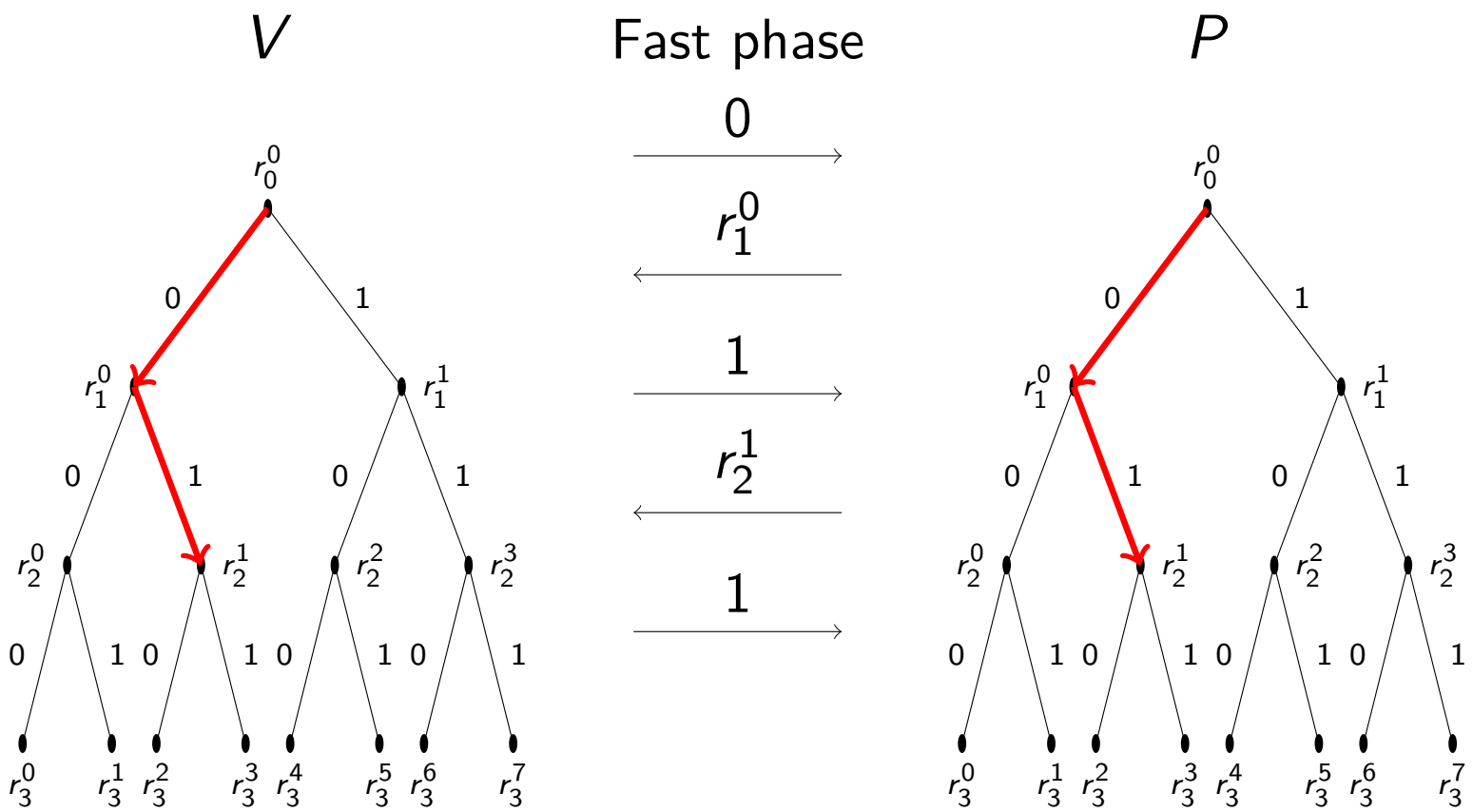
Avoine and Tchamkerten's proposal (2009)



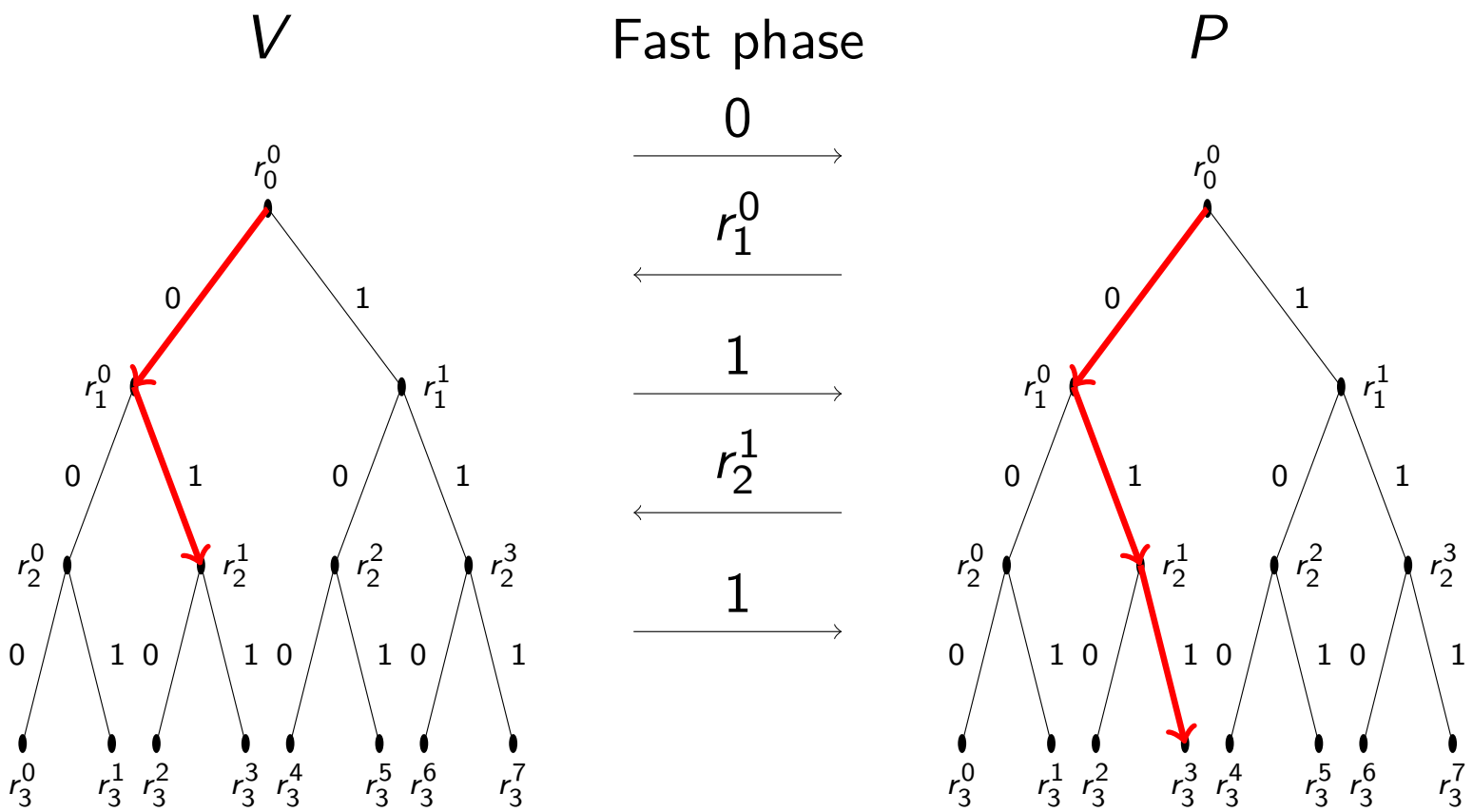
Avoine and Tchamkerten's proposal (2009)



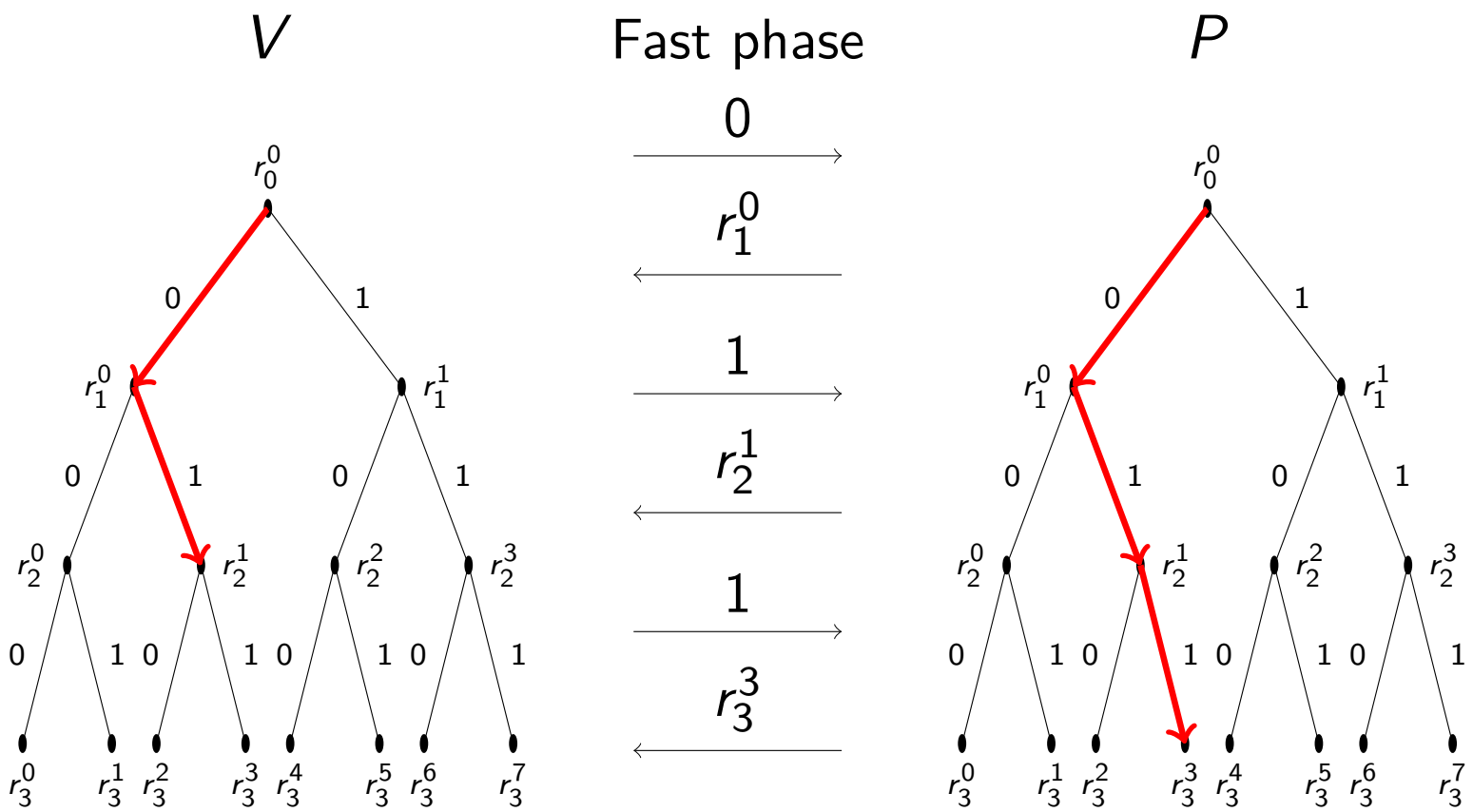
Avoine and Tchamkerten's proposal (2009)



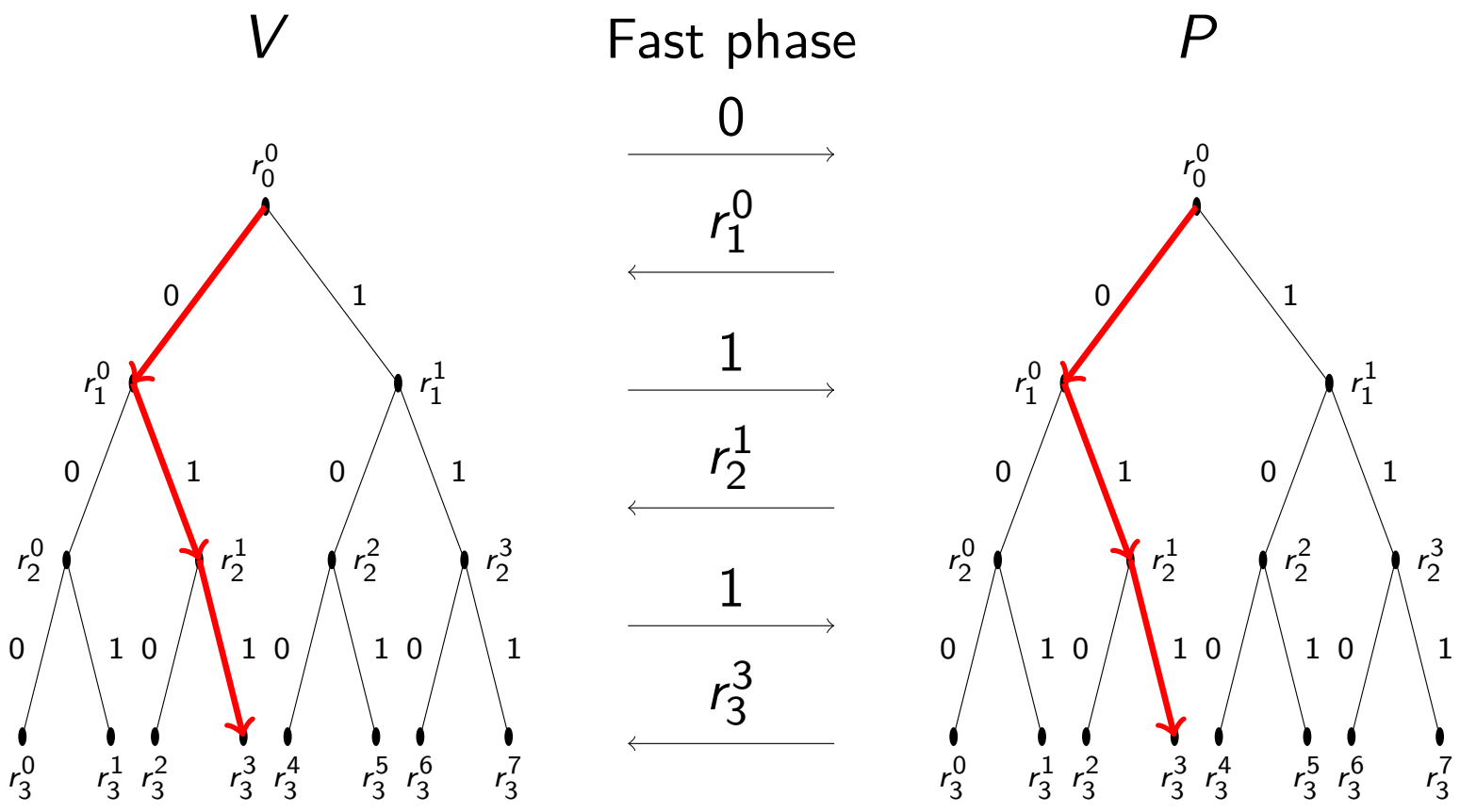
Avoine and Tchamkerten's proposal (2009)



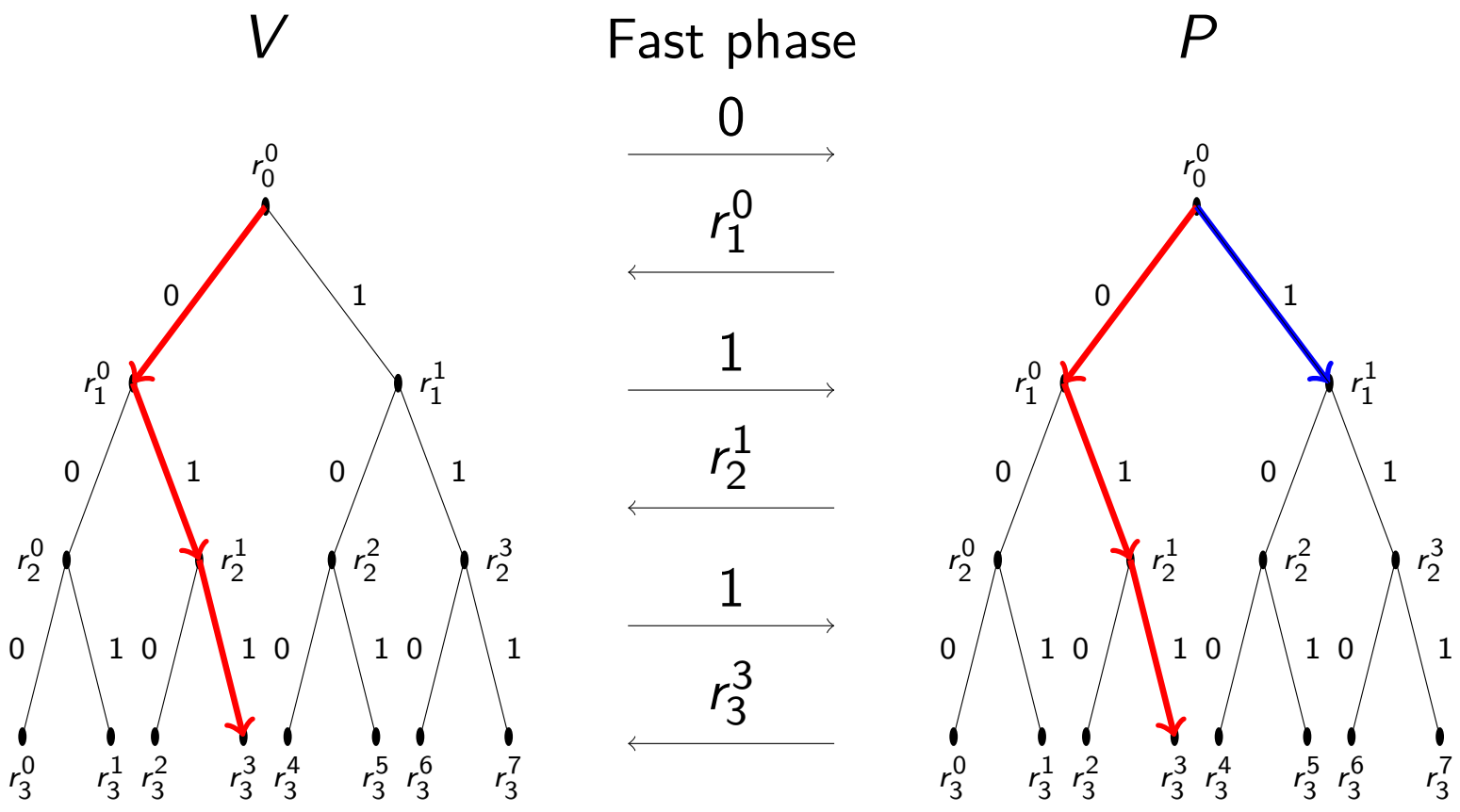
Avoine and Tchamkerten's proposal (2009)



Avoine and Tchamkerten's proposal (2009)



Avoine and Tchamkerten's proposal (2009)



Two well-known lookup-based protocols

	Mafia Fraud	Memory usage
HK protocol	$\left(\frac{3}{4}\right)^n$	$O(n)$
AT protocol	$\frac{1}{2^n}(1+\frac{n}{2})$	$O(2^n)$

- HK is simple, low cost requirements, but not good in security

Two well-known lookup-based protocols

	Mafia Fraud	Memory usage
HK protocol	$\left(\frac{3}{4}\right)^n$	$O(n)$
AT protocol	$\frac{1}{2^n}(1+\frac{n}{2})$	$O(2^n)$

- HK is simple, low cost requirements, but not good in security
- AT is the most secure existing DBP, but it requires exponential memory

Two well-known lookup-based protocols

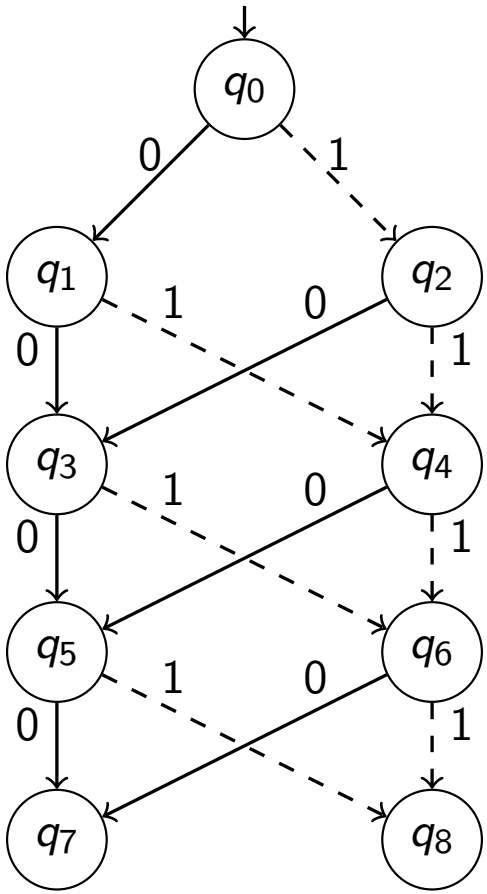
	Mafia Fraud	Memory usage
HK protocol	$\left(\frac{3}{4}\right)^n$	$O(n)$
AT protocol	$\frac{1}{2^n}(1+\frac{n}{2})$	$O(2^n)$

- HK is simple, low cost requirements, but not good in security
- AT is the most secure existing DBP, but it requires exponential memory

Questions

1. Can we model this class of lookup-based protocols and perform a generic analysis for its elements?
2. Does it exist a lookup-based protocol better than AT?
3. Do we need an exponential memory to achieve $\frac{1}{2^n}(1 + \frac{n}{2})$?

The model: Finite Automata



An example of HK protocol with 4 rounds.

Properties: lower bound

Theorem

The probability value $\frac{1}{2^n}\left(1+\frac{n}{2}\right)$ *is a tight lower bound on the resistance to mafia fraud of lookup-based distance-bounding protocols with n rounds.*

So, we can't do better than AT in lookup-based protocols.

Properties: lower bound

Theorem

The probability value $\frac{1}{2^n}\left(1+\frac{n}{2}\right)$ *is a tight lower bound on the resistance to mafia fraud of lookup-based distance-bounding protocols with n rounds.*

So, we can't do better than AT in lookup-based protocols.

Note that if we allow strong crypto and an extra phase, we can achieve $\frac{1}{2^n}$ (Brands & Chaum 1993).

Properties: lower bound

Theorem

The probability value $\frac{1}{2^n}\left(1+\frac{n}{2}\right)$ *is a tight lower bound on the resistance to mafia fraud of lookup-based distance-bounding protocols with n rounds.*

So, we can't do better than AT in lookup-based protocols.

Note that if we allow strong crypto and an extra phase, we can achieve $\frac{1}{2^n}$ (Brands & Chaum 1993).

Properties: generic calculation of security

We introduce the uniformity number $u \in \{1, \ldots, n\}$ of a protocol. The higher u, the harder it is for the attacker to predict the state of the protocol.

Theorem

Let P be a lookup-based distance-bounding protocol with uniformity number u for $n > 0$ rounds. Then the success probability of a mafia-fraud attack is R_n, where $R_0 = 1$ and

$$R_i = \frac{1}{2^i} + \sum_{j=0}^{i-1} \frac{R_{i-j-1}}{2^{j+\min(u,j+1)+1}},$$

This indeed instantiates to $\left(\frac{3}{4}\right)^n$ for HK and to $\frac{1}{2^n}\left(1 + \frac{n}{2}\right)$ for AT.

Properties: generic calculation of security

We introduce the uniformity number $u \in \{1, \ldots, n\}$ of a protocol. The higher u, the harder it is for the attacker to predict the state of the protocol.

Theorem

Let P be a lookup-based distance-bounding protocol with uniformity number u for $n > 0$ rounds. Then the success probability of a mafia-fraud attack is R_n, where $R_0 = 1$ and

$$R_i = \frac{1}{2^i} + \sum_{j=0}^{i-1} \frac{R_{i-j-1}}{2^{j+\min(u,j+1)+1}},$$

This indeed instantiates to $\left(\frac{3}{4}\right)^n$ for HK and to $\frac{1}{2^n}(1 + \frac{n}{2})$ for AT.

Properties: optimality implies exponential memory?

Do we need exponential memory to achieve AT's security ?

- We think so, but still don't have a formal proof

Properties: optimality implies exponential memory?

Do we need exponential memory to achieve AT's security ?

- We think so, but still don't have a formal proof
- We think our automata-based model will allows us to prove it

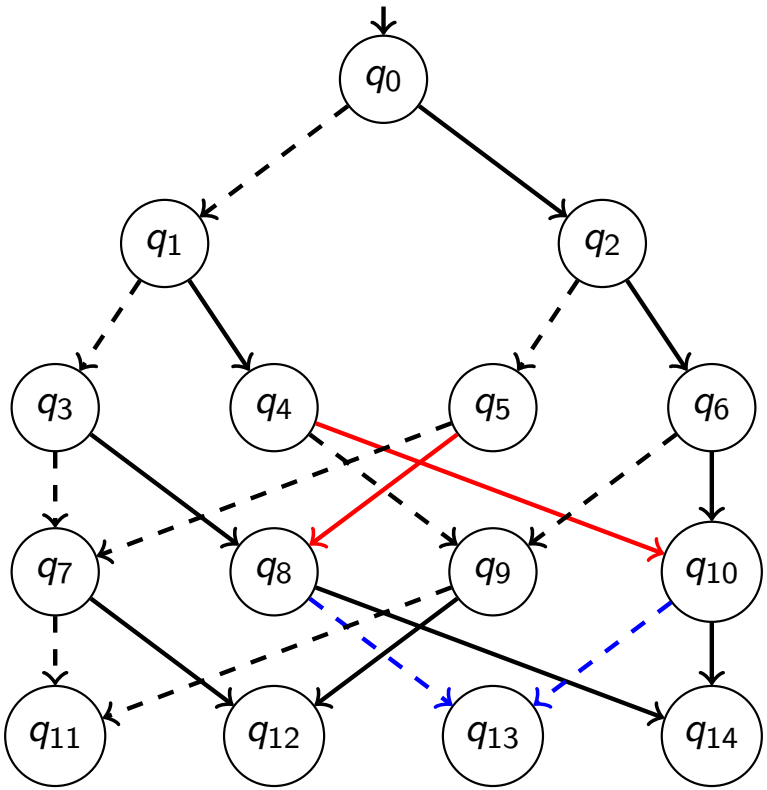
Properties: optimality implies exponential memory?

Do we need exponential memory to achieve AT's security ?

- We think so, but still don't have a formal proof
- We think our automata-based model will allows us to prove it

Our proposed protocol

The uniform protocols: an example of a 2-uniform protocol



- Approximates $\frac{1}{2^n}(1 + \frac{n}{2})$
- They required linear space.
- The uniformity value u is pre-defined

Security and memory usage analysis

	Mafia Fraud	Memory usage
HK protocol	$\left(\frac{3}{4}\right)^n$	$O(n)$
u-Uniform	$R_n(u) \xrightarrow[u \to n]{} \frac{1}{2^n}(1+\frac{n}{2})$	$O(2^u \times n)$
AT protocol	$\frac{1}{2^n}(1+\frac{n}{2})$	$O(2^n)$

Conclusions

- Better understanding and generic treatment of lookup-based distance-bounding protocols.
- Fundamental results on security and memory usage.
- Novel family of protocols that approximates optimality with low costs in memory.

- Can we extend our results to a larger class of protocols?
- What is the resistance of lookup-based protocols to distance fraud, terrorist frauds, etc.?
- Can we generalize the various types of fraud into one notion?
- Can we provide a causality-based definition of distance bounding (as opposed to time/space based)?

Conclusions

- Better understanding and generic treatment of lookup-based distance-bounding protocols.
- Fundamental results on security and memory usage.
- Novel family of protocols that approximates optimality with low costs in memory.

- Can we extend our results to a larger class of protocols?
- What is the resistance of lookup-based protocols to distance fraud, terrorist frauds, etc.?
- Can we generalize the various types of fraud into one notion?
- Can we provide a causality-based definition of distance bounding (as opposed to time/space based)?

Thanks for your attention

jorge.toro@uni.lu
http://satoss.uni.lu/members/jorge/