Let's stick together

Digitally ensuring physical proximity

Sjouke Mauw
University of luxembourg

(joint work with Rolando Trujillo-Rasua)

TouW Informatica Symposium, Amsterdam, November 19, 2016

University of Luxembourg

- Founded in 2003.
- Trilingual: French, German and English.
- $\sim$6000 students, $\sim$250 professors.
- Three faculties, three interdisciplinary centers.

TIMES HIGHER EDUCATION
WORLD UNIVERSITY RANKINGS

- Overall: 178
- Young universities (under 50 year): 14
- Most international universities: 2
- Computer science: 58

Outline

- Disruptive developments.
- From Physical to Digital.
  - Digital money
  - Electronic voting
  - Smart keys
- Achieving physical properties in a digital world.
  - Distance bounding
  - Grouping

Disruptive developments

- The world's largest taxi firm, Uber, owns no cars.
- The world's most popular media company, Facebook, creates no content.
- The world's most valuable retailer, Alibaba, carries no stock.
- And the world's largest accommodation provider, Airbnb, owns no property.

(Tom Goodwin)

Long-term trend on the path of disruption

From Physical to Digital

Examples

1. Digital money
2. Electronic voting
3. Smart keys
4. . . .

Example 1: Digital money

Long before bitcoin: DigiCash (ecash).

- 1983 ground breaking paper by David Chaum (Berkely, CWI).
- Idea based on blind signatures.
- 1990 founded company Digicash.
- Huge commercial interest, e.g., Bill Gates wanted to integrate ecash in every copy of Windows95 for 100 million dollars.
- 1998 DigiCash bankrupt alledgely due to mismanagement.
- Current focus on distributed digital currencies (e.g. BitCoin).

Traditional vs. digital money

Traditional money:

- Can be spent only once (transferrable object).
- Untraceable (object decoupled from owner).
- Unforgeable.

Digicash:

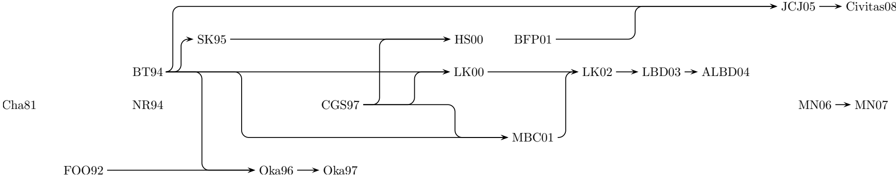
- Detection of double spending.
- Privacy and authentication through blind signatures.

Bitcoin:

- Block chain.
- Decentralized.

Example 2: Electronic voting

- 1981 first proposal of an electronic voting system that is end-to-end verifiable by David Chaum.
- Idea based on Mixes.
- Currently abundent collection of e-voting systems.
- Used in real elections (Estonia).



Traditional vs. electronic voting

Traditional voting:

- Privacy (voting booth, after voting ballot decoupled from voter).
- Auditable ((re-)counting ballots, observers).
- Voter can vote only once (authentication).
- No coercion (forbidden to take selfie in vote booth).

Electronic voting:

- Privacy (blind signatures, shuffling of votes through Mixes).
- Verifiability (bulletin board).
- No coercion (no digital receipt, last submitted vote counts).

Example 3: Smart keys

- From traditional keys to transponder keys to smart keys.

Traditional vs. smart keys

Traditional keys:

- Can’t open lock without key (next speaker will disagree).
- Key can’t be copied.
- Proximity.

Smart keys:

- Secrecy of cryptographic key.
- Authentication protocol to prove possession of key.
- Distance-bounding protocol.

Traditional vs. smart keys

Traditional keys:

- Can’t open lock without key (next speaker will disagree).
- Key can’t be copied.
- Proximity.

Smart keys:

- Secrecy of cryptographic key.
- Authentication protocol to prove possession of key.
- Distance-bounding protocol.

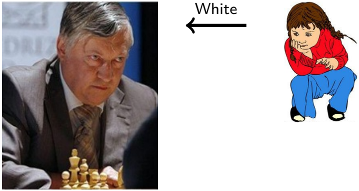
(Note: 1993 First distance-bounding protocol by David Chaum.)

Distance Bounding

- To prove proximity.
- E.g. to prevent relay attacks (man-in-the-middle attacks).

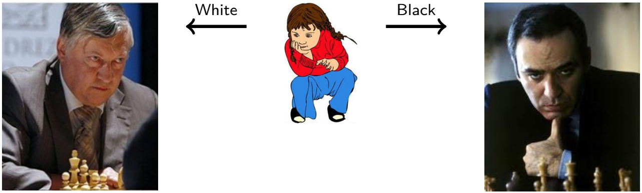
Relay attack: how to beat a grand master

Relay attack: how to beat a grand master



White

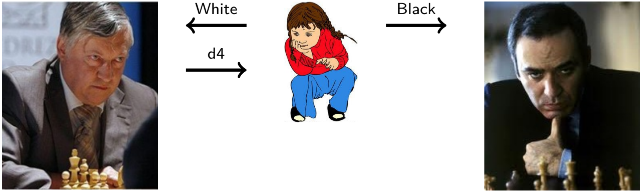
Relay attack: how to beat a grand master



White

Black

Relay attack: how to beat a grand master

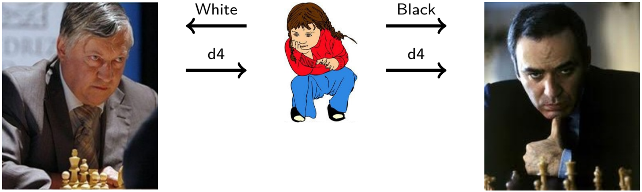


White

d4

Black

Relay attack: how to beat a grand master



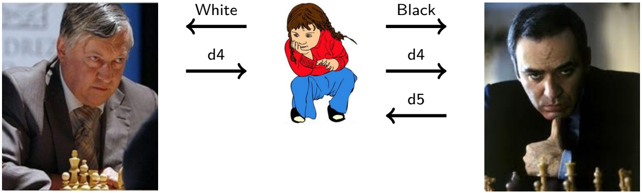
White

d4

Black

d4

Relay attack: how to beat a grand master



White

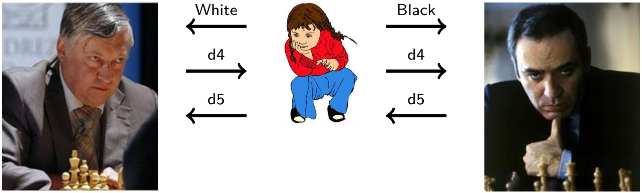
d4

Black

d4

d5

Relay attack: how to beat a grand master



White

d4

d5

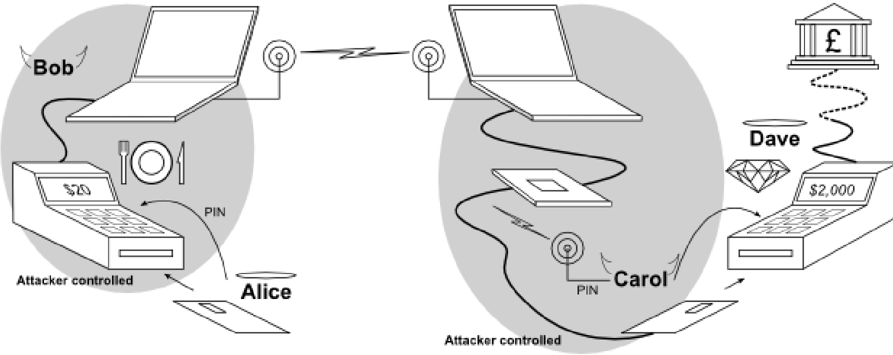
Black

d4

d5

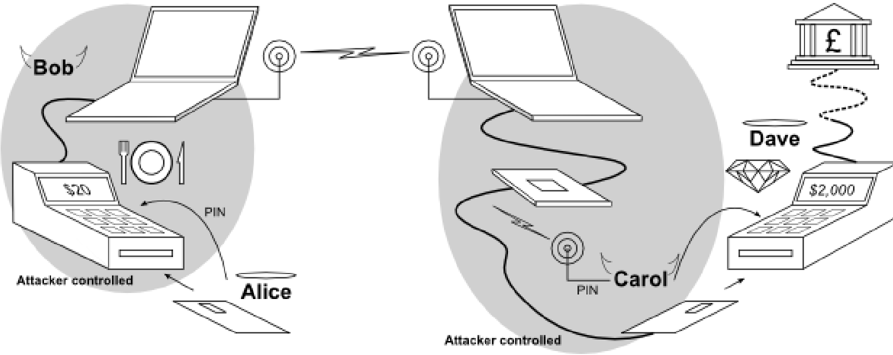
Chip & Pin relay attack

(Murdoch & Drimer 2007)



Chip & Pin relay attack

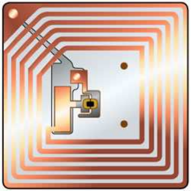
(Murdoch & Drimer 2007)

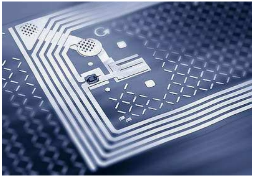


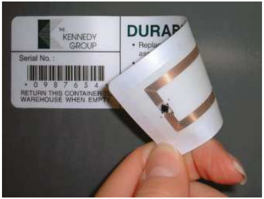
Many more practical attacks, e.g.

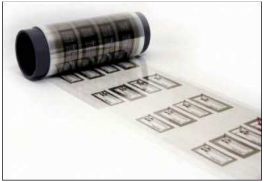
- Passive keyless entry and start systems used in modern cars (Francillon 2012)
- Google Wallet Relay Attack (Roland 2013)

RFID (Radio Frequency IDentification)









Properties of RFID

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

Problem: Relay attacks

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.

Problem: Relay attacks

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.

Note that relaying is not always an attack
(e.g. store-and-forward in communication network).

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.

Attacks on distance-bounding protocols

We will focus on, so-called, Mafia fraud attacks.

Definition (Mafia fraud)

A mafia fraud attack is an attack where an adversary defeats a distance bounding protocol using a man-in-the-middle between the reader and an honest tag located outside the neighborhood.

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~~

How to measure distance?

- Reader sends a challenge.
- Tag provides correct response.
- Reader measures the round-trip-time and accepts if this is “fast enough”.

How to measure distance?

- Reader sends a challenge.
- Tag provides correct response.
- Reader measures the round-trip-time and accepts if this is “fast enough”.

- RF communication at the speed of light.
- Need very short processing time at the tag (otherwise the adversary could overclock the tag).
- A timing error of 1 ns corresponds to a distance error of 15 cm.

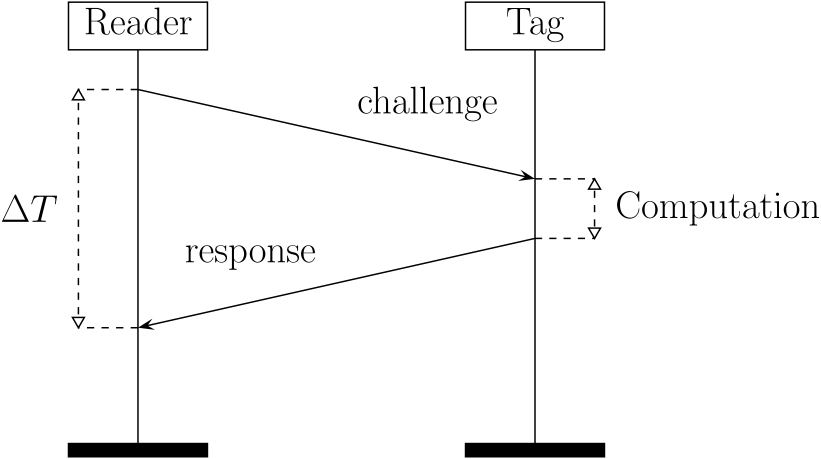
How to measure distance?

- Reader sends a challenge.
- Tag provides correct response.
- Reader measures the round-trip-time and accepts if this is "fast enough".

- RF communication at the speed of light.
- Need very short processing time at the tag (otherwise the adversary could overclock the tag).
- A timing error of 1 ns corresponds to a distance error of 15 cm.

- 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.

One challenge-response round



Hancke and Kuhn's proposal (2005)

P (Tag)
secret x

V (Reader)
secret x

Hancke and Kuhn's proposal (2005)

P (Tag)
secret x

V (Reader)
secret x

slow phase

fast phase

Hancke and Kuhn's proposal (2005)

P (Tag)
secret x

V (Reader)
secret x

slow phase

fast phase

Hancke and Kuhn's proposal (2005)

P (Tag)
secret x

V (Reader)
secret x

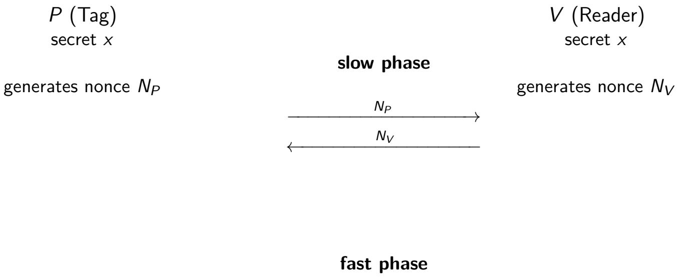
slow phase

generates nonce N_P

generates nonce N_V

fast phase

Hancke and Kuhn's proposal (2005)



P (Tag)
secret x

V (Reader)
secret x

slow phase

generates nonce N_P

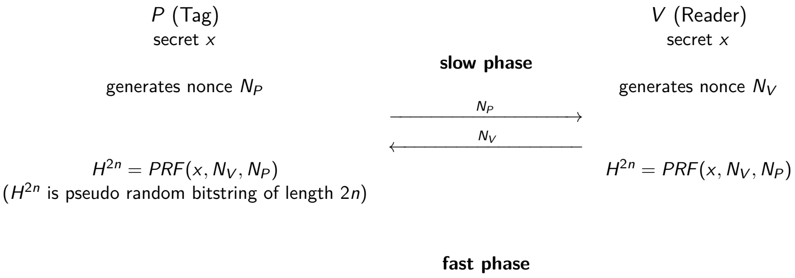
generates nonce N_V

$\xrightarrow{N_P}$

$\xleftarrow{N_V}$

fast phase

Hancke and Kuhn's proposal (2005)



P (Tag)
secret x

V (Reader)
secret x

slow phase

generates nonce N_P

generates nonce N_V

$\xrightarrow{N_P}$

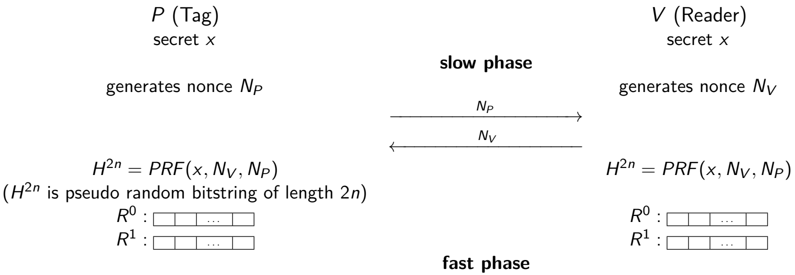
$\xleftarrow{N_V}$

$H^{2n} = PRF(x, N_V, N_P)$
(H^{2n} is pseudo random bitstring of length $2n$)

$H^{2n} = PRF(x, N_V, N_P)$

fast phase

Hancke and Kuhn's proposal (2005)



P (Tag)
secret x

V (Reader)
secret x

slow phase

generates nonce N_P

generates nonce N_V

$\xrightarrow{N_P}$

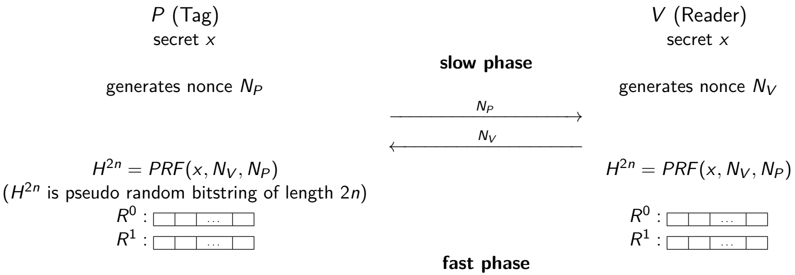
$\xleftarrow{N_V}$

$H^{2n} = PRF(x, N_V, N_P)$
(H^{2n} is pseudo random bitstring of length $2n$)
$R^0 : \boxed{}\boxed{}\boxed{\ldots}\boxed{}$
$R^1 : \boxed{}\boxed{}\boxed{\ldots}\boxed{}$

$H^{2n} = PRF(x, N_V, N_P)$
$R^0 : \boxed{}\boxed{}\boxed{\ldots}\boxed{}$
$R^1 : \boxed{}\boxed{}\boxed{\ldots}\boxed{}$

fast phase

Hancke and Kuhn's proposal (2005)



P (Tag)
secret x

V (Reader)
secret x

slow phase

generates nonce N_P

generates nonce N_V

$$\xrightarrow{N_P}$$

$$\xleftarrow{N_V}$$

$H^{2n} = PRF(x, N_V, N_P)$
(H^{2n} is pseudo random bitstring of length $2n$)

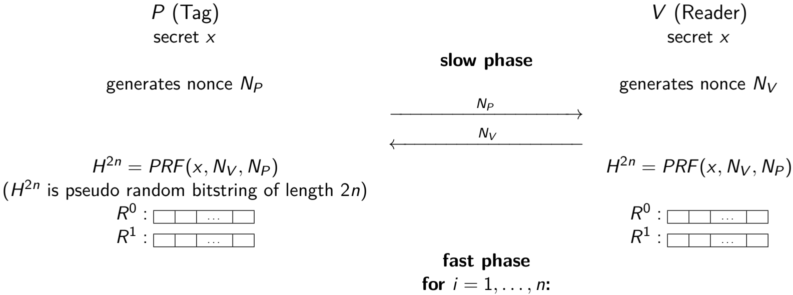
R^0 : □□ … □
R^1 : □□ … □

$H^{2n} = PRF(x, N_V, N_P)$

R^0 : □□ … □
R^1 : □□ … □

fast phase

Hancke and Kuhn's proposal (2005)



P (Tag)
secret x

V (Reader)
secret x

slow phase

generates nonce N_P

generates nonce N_V

$\xrightarrow{N_P}$

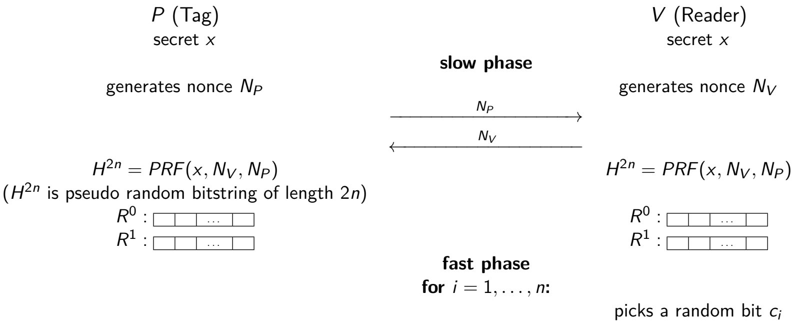
$\xleftarrow{N_V}$

$H^{2n} = PRF(x, N_V, N_P)$
(H^{2n} is pseudo random bitstring of length $2n$)
R^0 : □□ … □
R^1 : □□ … □

$H^{2n} = PRF(x, N_V, N_P)$
R^0 : □□ … □
R^1 : □□ … □

fast phase
for $i = 1, \ldots, n$**:**

Hancke and Kuhn's proposal (2005)



P (Tag)
secret x

V (Reader)
secret x

slow phase

generates nonce N_P

generates nonce N_V

$\xrightarrow{N_P}$

$\xleftarrow{N_V}$

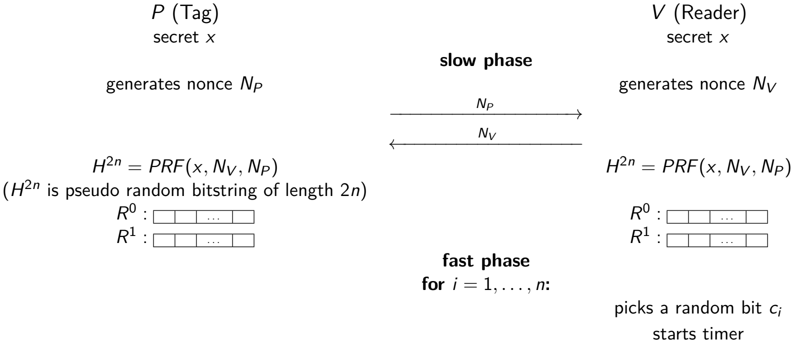
$H^{2n} = PRF(x, N_V, N_P)$
(H^{2n} is pseudo random bitstring of length $2n$)
R^0 : □□ ... □
R^1 : □□ ... □

$H^{2n} = PRF(x, N_V, N_P)$
R^0 : □□ ... □
R^1 : □□ ... □

fast phase
for $i = 1, \ldots, n$**:**

picks a random bit c_i

Hancke and Kuhn's proposal (2005)



P (Tag)
secret x

V (Reader)
secret x

slow phase

generates nonce N_P

generates nonce N_V

$\xrightarrow{N_P}$

$\xleftarrow{N_V}$

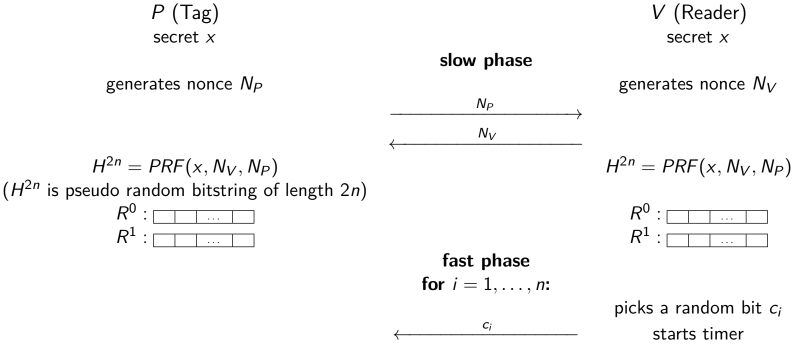
$H^{2n} = PRF(x, N_V, N_P)$
(H^{2n} is pseudo random bitstring of length $2n$)
R^0 : □□ … □
R^1 : □□ … □

$H^{2n} = PRF(x, N_V, N_P)$
R^0 : □□ … □
R^1 : □□ … □

fast phase
for $i = 1, \ldots, n$**:**

picks a random bit c_i
starts timer

Hancke and Kuhn's proposal (2005)



P (Tag)
secret x

V (Reader)
secret x

slow phase

generates nonce N_P

generates nonce N_V

$\xrightarrow{N_P}$

$\xleftarrow{N_V}$

$H^{2n} = PRF(x, N_V, N_P)$
(H^{2n} is pseudo random bitstring of length $2n$)
$R^0 : \boxed{}\boxed{}\boxed{\ldots}\boxed{}$
$R^1 : \boxed{}\boxed{}\boxed{\ldots}\boxed{}$

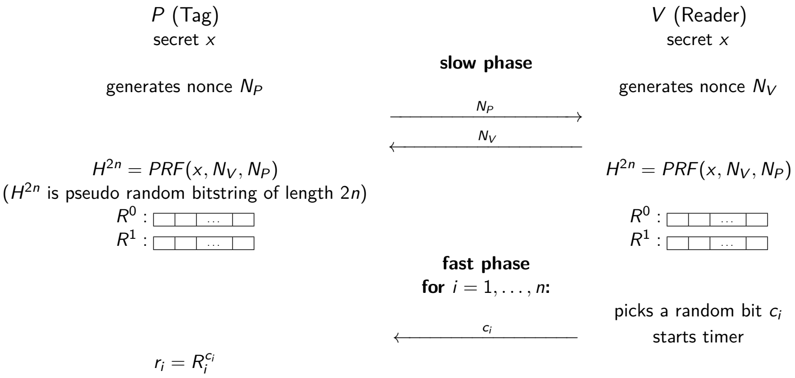
$H^{2n} = PRF(x, N_V, N_P)$
$R^0 : \boxed{}\boxed{}\boxed{\ldots}\boxed{}$
$R^1 : \boxed{}\boxed{}\boxed{\ldots}\boxed{}$

fast phase
for $i = 1, \ldots, n$**:**

picks a random bit c_i
starts timer

$\xleftarrow{c_i}$

Hancke and Kuhn's proposal (2005)



P (Tag)
secret x

V (Reader)
secret x

slow phase

generates nonce N_P

generates nonce N_V

$\xrightarrow{N_P}$

$\xleftarrow{N_V}$

$H^{2n} = PRF(x, N_V, N_P)$
(H^{2n} is pseudo random bitstring of length $2n$)

$H^{2n} = PRF(x, N_V, N_P)$

R^0 : $\boxed{}\boxed{}\boxed{\ldots}\boxed{}$

R^1 : $\boxed{}\boxed{}\boxed{\ldots}\boxed{}$

R^0 : $\boxed{}\boxed{}\boxed{\ldots}\boxed{}$

R^1 : $\boxed{}\boxed{}\boxed{\ldots}\boxed{}$

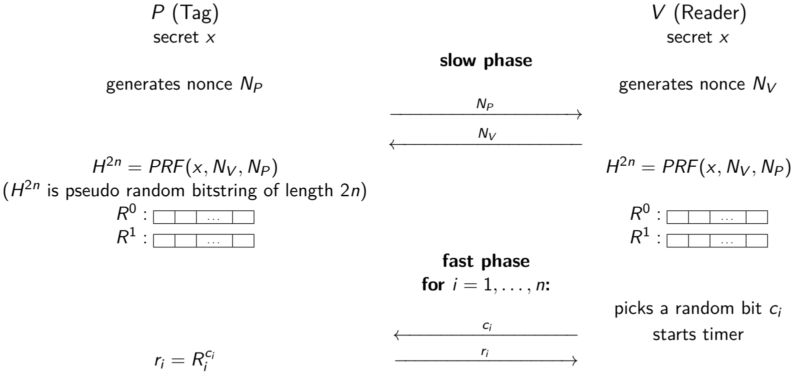
fast phase
for $i = 1, \ldots, n$**:**

picks a random bit c_i
starts timer

$\xleftarrow{c_i}$

$r_i = R_i^{c_i}$

Hancke and Kuhn's proposal (2005)



P (Tag)
secret x

V (Reader)
secret x

slow phase

generates nonce N_P

generates nonce N_V

$\xrightarrow{N_P}$

$\xleftarrow{N_V}$

$H^{2n} = PRF(x, N_V, N_P)$
(H^{2n} is pseudo random bitstring of length $2n$)

$H^{2n} = PRF(x, N_V, N_P)$

R^0 : $\boxed{}\boxed{}\boxed{\dots}\boxed{}$
R^1 : $\boxed{}\boxed{}\boxed{\dots}\boxed{}$

R^0 : $\boxed{}\boxed{}\boxed{\dots}\boxed{}$
R^1 : $\boxed{}\boxed{}\boxed{\dots}\boxed{}$

fast phase
for $i = 1, \dots, n$**:**

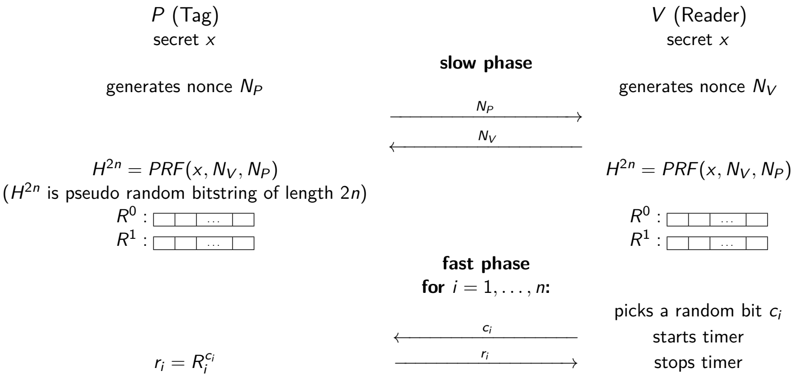
picks a random bit c_i
starts timer

$\xleftarrow{c_i}$

$r_i = R_i^{c_i}$

$\xrightarrow{r_i}$

Hancke and Kuhn's proposal (2005)



P (Tag)
secret x

V (Reader)
secret x

slow phase

generates nonce N_P

generates nonce N_V

$\xrightarrow{N_P}$

$\xleftarrow{N_V}$

$H^{2n} = PRF(x, N_V, N_P)$
(H^{2n} is pseudo random bitstring of length $2n$)

R^0 : ...
R^1 : ...

$H^{2n} = PRF(x, N_V, N_P)$

R^0 : ...
R^1 : ...

fast phase
for $i = 1, \dots, n$**:**

picks a random bit c_i

$\xleftarrow{c_i}$

starts timer

$r_i = R_i^{c_i}$

$\xrightarrow{r_i}$

stops timer

Random response attack

- Attacker is near the reader, so he can reply in time.
- But he doesn't know the correct responses.
- So sends random responses.
- Success probability for one round: $\frac{1}{2}$
- For n rounds: $\left(\frac{1}{2}\right)^n$
- E.g. for $n = 10$: 0.00098

Random response attack

- Attacker is near the reader, so he can reply in time.
- But he doesn't know the correct responses.
- So sends random responses.
- Success probability for one round: $\frac{1}{2}$
- For n rounds: $\left(\frac{1}{2}\right)^n$
- E.g. for $n = 10$: 0.00098

Can the attacker do better?

Pre-ask strategy

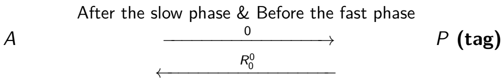
After the slow phase & Before the fast phase

Pre-ask strategy

After the slow phase & Before the fast phase

$A \qquad \xrightarrow{0} \qquad P$ **(tag)**

Pre-ask strategy

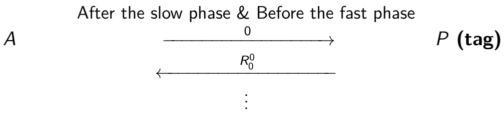


After the slow phase & Before the fast phase

A $\xrightarrow{0}$ P **(tag)**

$\xleftarrow{R_0^0}$

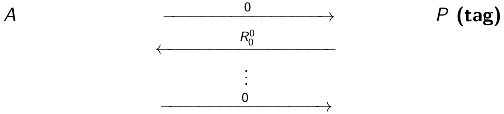
Pre-ask strategy



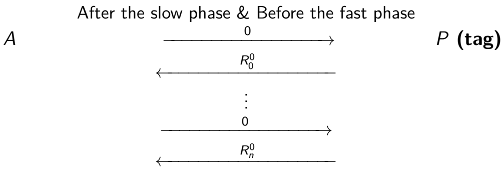
After the slow phase & Before the fast phase

Pre-ask strategy

After the slow phase & Before the fast phase



Pre-ask strategy



After the slow phase & Before the fast phase

A

P **(tag)**

$\xrightarrow{0}$

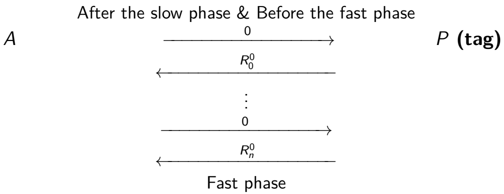
$\xleftarrow{R_0^0}$

$\vdots$

$\xrightarrow{0}$

$\xleftarrow{R_n^0}$

Pre-ask strategy



After the slow phase & Before the fast phase

A

P **(tag)**

0

R_0^0

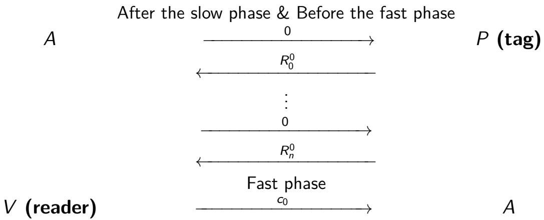
$\vdots$

0

R_n^0

Fast phase

Pre-ask strategy



After the slow phase & Before the fast phase

A $\xrightarrow{0}$ P **(tag)**

$\xleftarrow{R_0^0}$

$\vdots$

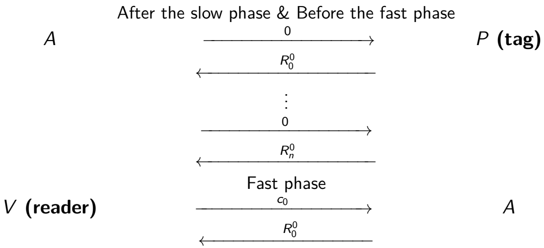
$\xrightarrow{0}$

$\xleftarrow{R_n^0}$

Fast phase

V **(reader)** $\xrightarrow{c_0}$ A

Pre-ask strategy



After the slow phase & Before the fast phase

A $\xrightarrow{0}$ P **(tag)**

$\xleftarrow{R_0^0}$

$\vdots$

$\xrightarrow{0}$

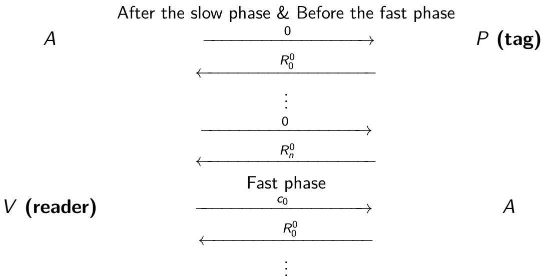
$\xleftarrow{R_n^0}$

Fast phase

V **(reader)** $\xrightarrow{c_0}$ A

$\xleftarrow{R_0^0}$

Pre-ask strategy



After the slow phase & Before the fast phase

A

P **(tag)**

0

R_0^0

⋮

0

R_n^0

Fast phase

V **(reader)**

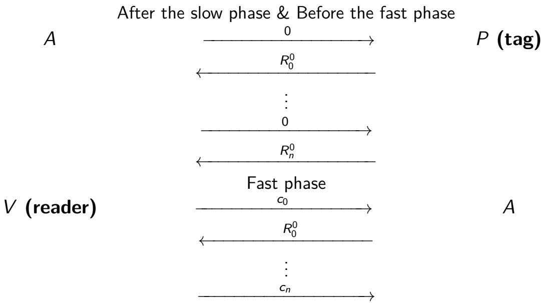
A

c_0

R_0^0

⋮

Pre-ask strategy



After the slow phase & Before the fast phase

A

P **(tag)**

0

R_0^0

$\vdots$

0

R_n^0

Fast phase

V **(reader)**

A

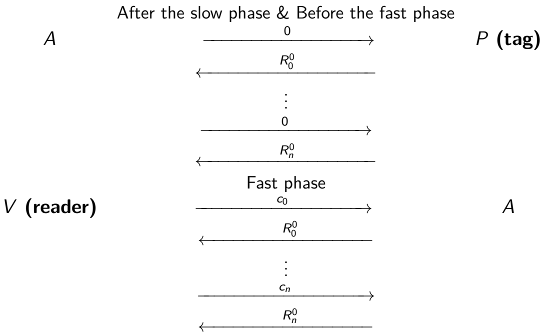
c_0

R_0^0

$\vdots$

c_n

Pre-ask strategy



After the slow phase & Before the fast phase

A

0

R_0^0

$\vdots$

0

R_n^0

P **(tag)**

Fast phase

V **(reader)**

c_0

R_0^0

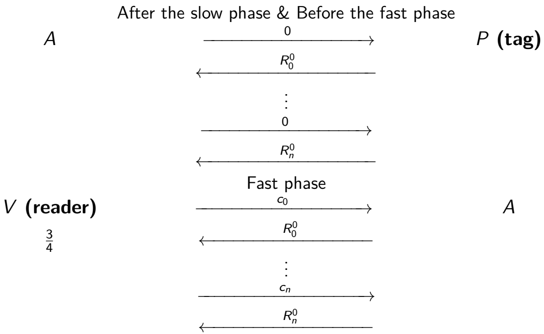
$\vdots$

c_n

R_n^0

A

Pre-ask strategy



After the slow phase & Before the fast phase

A $\xrightarrow{0}$ P **(tag)**

$\xleftarrow{R_0^0}$

$\vdots$

$\xrightarrow{0}$

$\xleftarrow{R_n^0}$

Fast phase

V **(reader)** $\xrightarrow{c_0}$ A

$\frac{3}{4}$

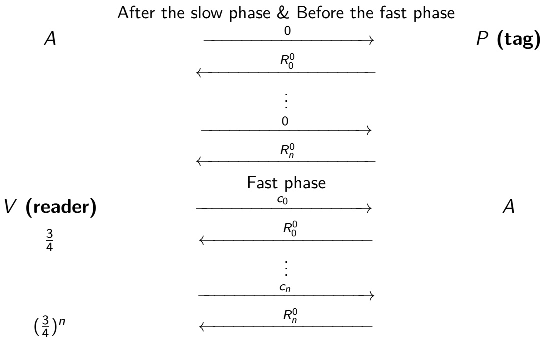
$\xleftarrow{R_0^0}$

$\vdots$

$\xrightarrow{c_n}$

$\xleftarrow{R_n^0}$

Pre-ask strategy



After the slow phase & Before the fast phase

A

P **(tag)**

0

R_0^0

$\vdots$

0

R_n^0

Fast phase

V **(reader)**

A

c_0

$\frac{3}{4}$

R_0^0

$\vdots$

c_n

$(\frac{3}{4})^n$

R_n^0

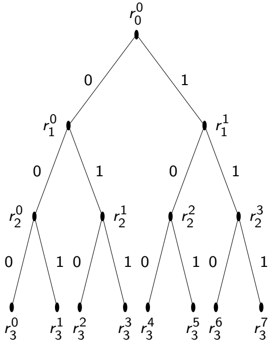
For $n = 10$: 0.056

Time to think

Can this protocol be improved?

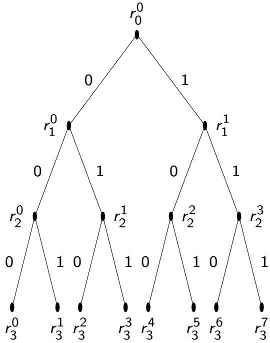
Avoine and Tchamkerten's proposal (2009)

V (reader)

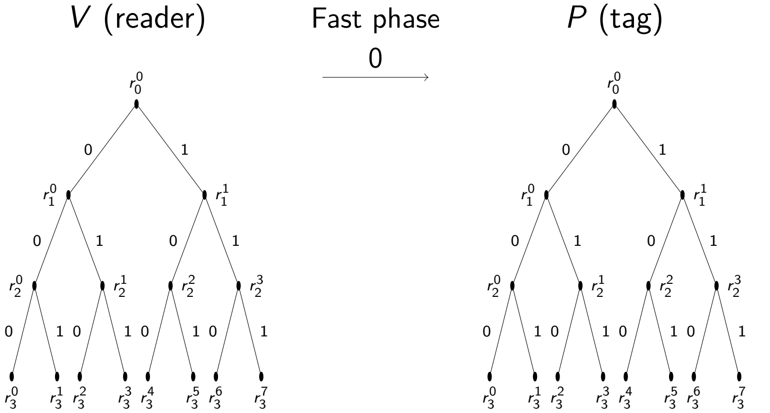


Fast phase

P (tag)



Avoine and Tchamkerten's proposal (2009)



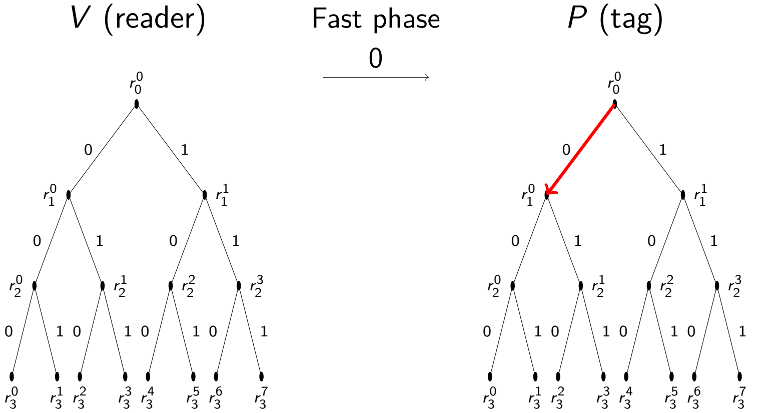
V (reader)

Fast phase

0

P (tag)

Avoine and Tchamkerten's proposal (2009)



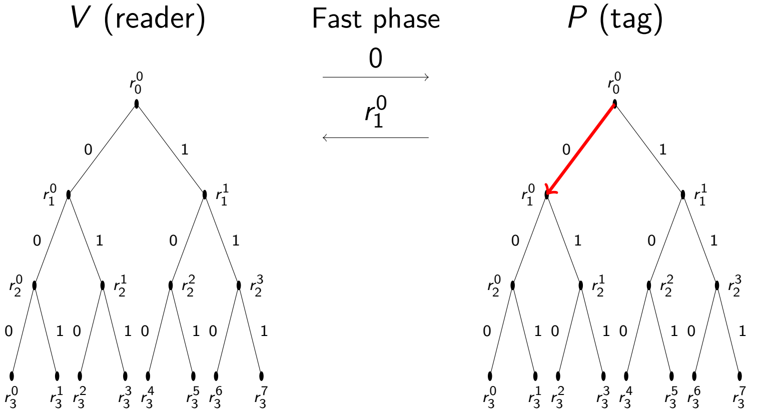
V (reader)

Fast phase

$$\xrightarrow{0}$$

P (tag)

Avoine and Tchamkerten's proposal (2009)



V (reader)

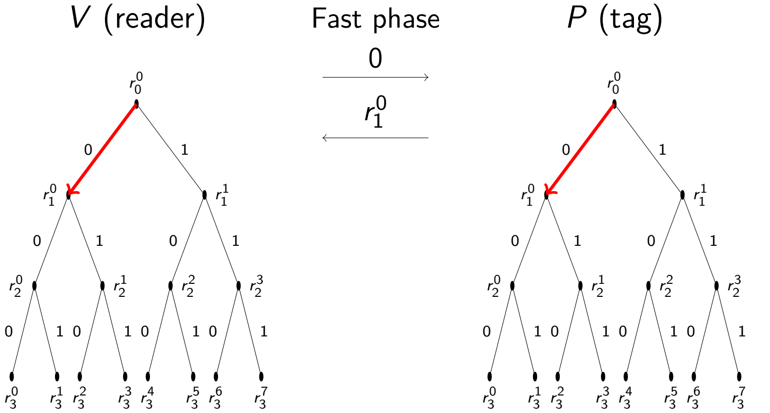
Fast phase

$\xrightarrow{0}$

$\xleftarrow{r_1^0}$

P (tag)

Avoine and Tchamkerten's proposal (2009)



V (reader)

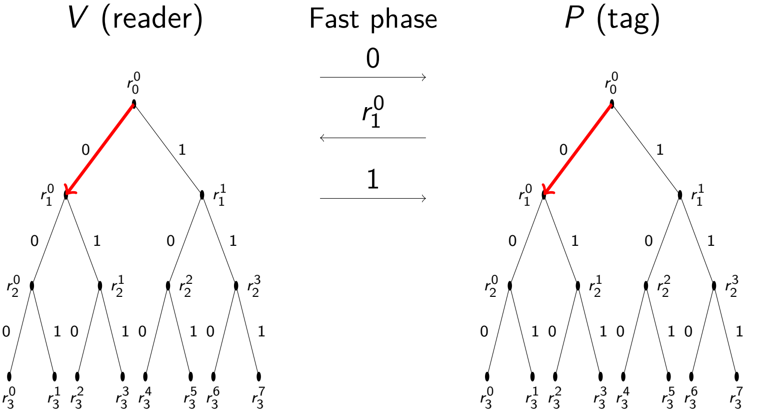
Fast phase

0

r_1^0

P (tag)

Avoine and Tchamkerten's proposal (2009)



V (reader)

Fast phase

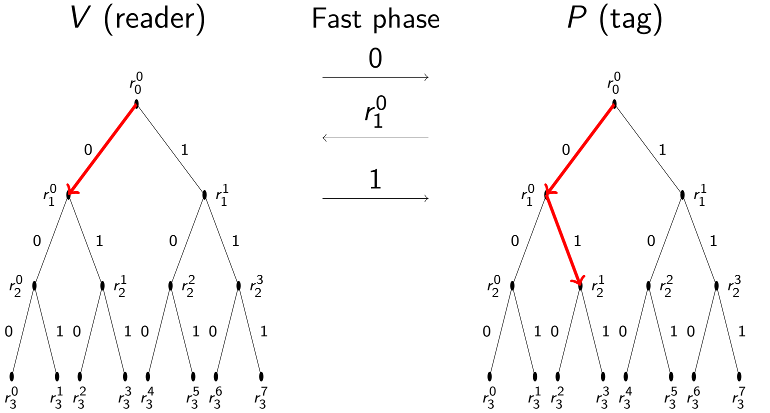
P (tag)

$$0 \longrightarrow$$

$$r_1^0 \longleftarrow$$

$$1 \longrightarrow$$

Avoine and Tchamkerten's proposal (2009)



V (reader)

Fast phase

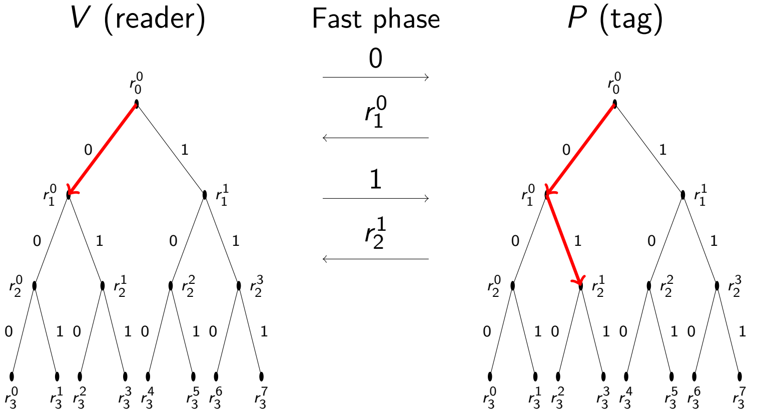
P (tag)

$\xrightarrow{0}$

$\xleftarrow{r_1^0}$

$\xrightarrow{1}$

Avoine and Tchamkerten's proposal (2009)



V (reader)

Fast phase

P (tag)

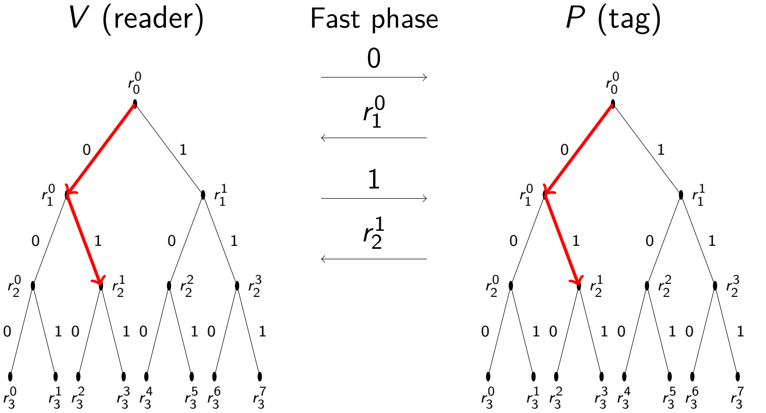
$0 \longrightarrow$

$r_1^0 \longleftarrow$

$1 \longrightarrow$

$r_2^1 \longleftarrow$

Avoine and Tchamkerten's proposal (2009)



V (reader)

Fast phase

P (tag)

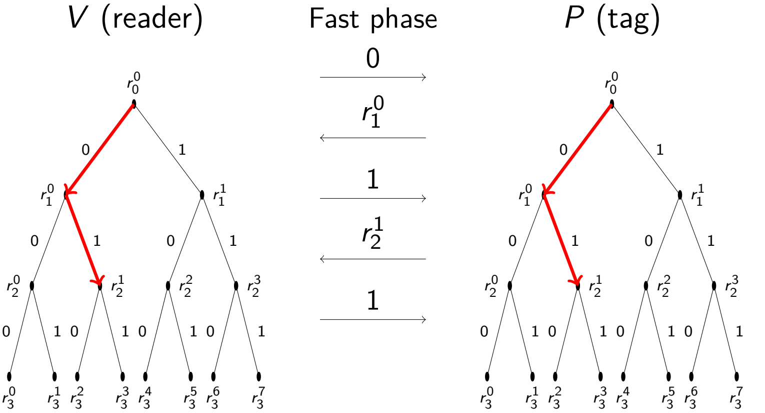
$$0 \longrightarrow$$

$$r_1^0 \longleftarrow$$

$$1 \longrightarrow$$

$$r_2^1 \longleftarrow$$

Avoine and Tchamkerten's proposal (2009)



V (reader)

Fast phase

P (tag)

$\xrightarrow{0}$

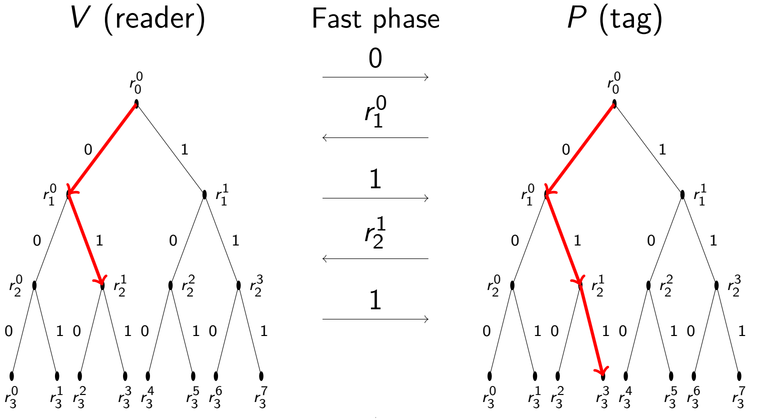
$\xleftarrow{r_1^0}$

$\xrightarrow{1}$

$\xleftarrow{r_2^1}$

$\xrightarrow{1}$

Avoine and Tchamkerten's proposal (2009)



V (reader)

Fast phase

P (tag)

$$0 \longrightarrow$$

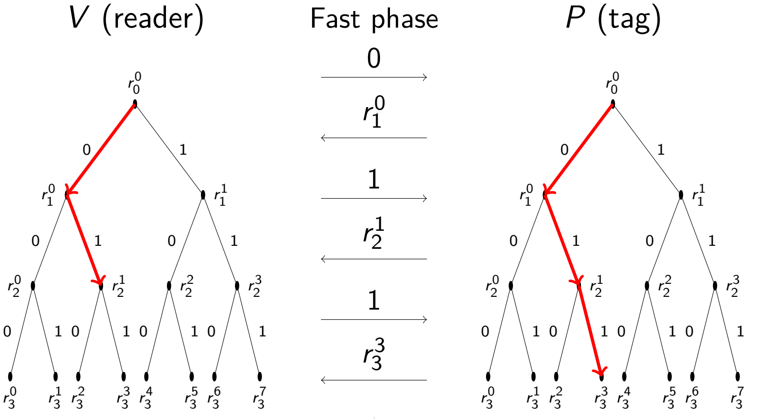
$$\longleftarrow r_1^0$$

$$1 \longrightarrow$$

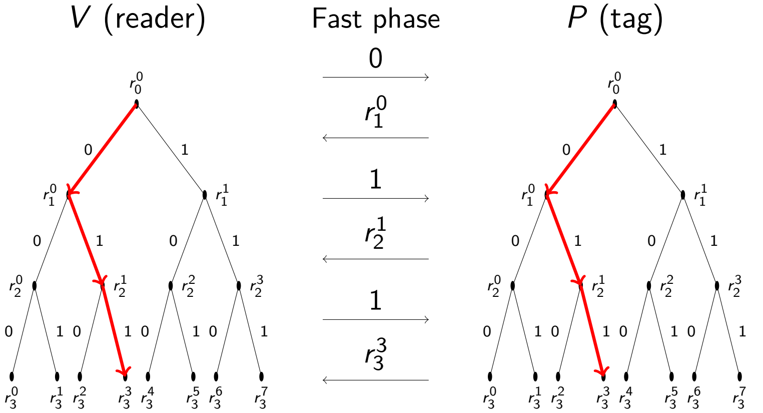
$$\longleftarrow r_2^1$$

$$1 \longrightarrow$$

Avoine and Tchamkerten's proposal (2009)



Avoine and Tchamkerten's proposal (2009)



V (reader)

Fast phase

P (tag)

$0 \longrightarrow$

$r_1^0 \longleftarrow$

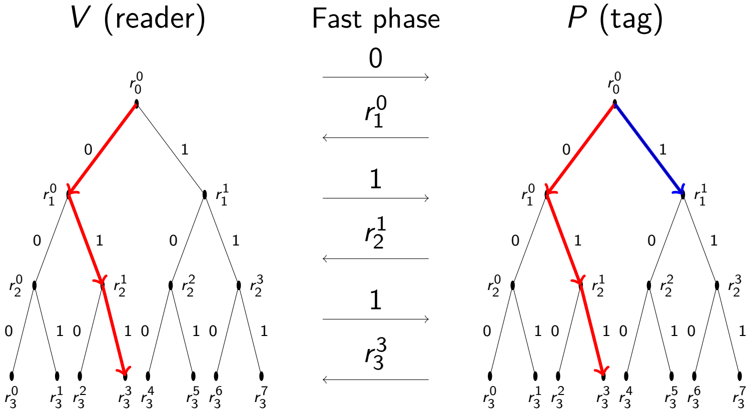
$1 \longrightarrow$

$r_2^1 \longleftarrow$

$1 \longrightarrow$

$r_3^3 \longleftarrow$

Avoine and Tchamkerten's proposal (2009)



V (reader)

Fast phase

P (tag)

$0 \longrightarrow$

$r_1^0 \longleftarrow$

$1 \longrightarrow$

$r_2^1 \longleftarrow$

$1 \longrightarrow$

$r_3^3 \longleftarrow$

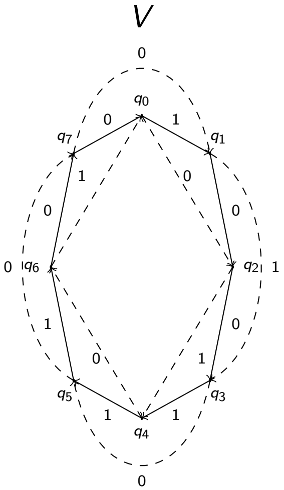
Security analyis

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

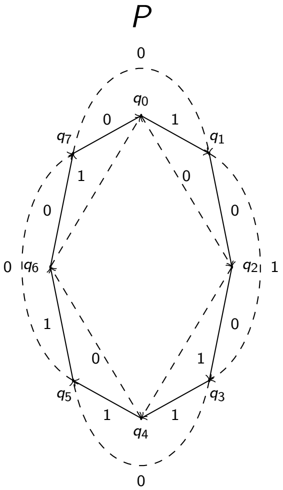
Security analyis

	Mafia Fraud	Memory usage
HK protocol	$\left(\frac{3}{4}\right)^n$	linear in number of rounds
AT protocol	$\frac{1}{2^n}(1+\frac{n}{2})$	exponential in number of rounds

Graph-based protocols

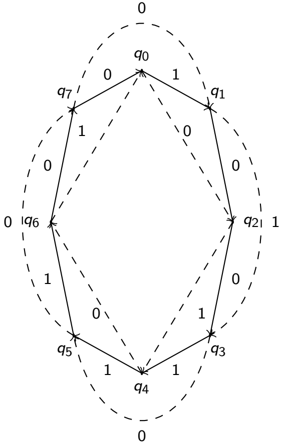


Fast phase



Graph-based protocols

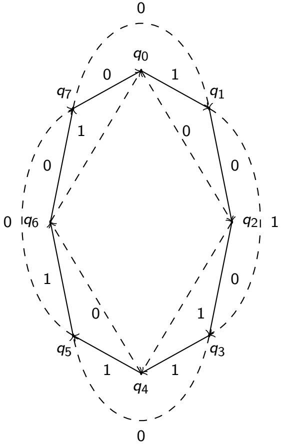
V



Fast phase

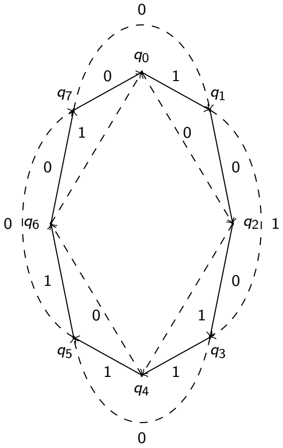
$\xrightarrow{0}$

P



Graph-based protocols

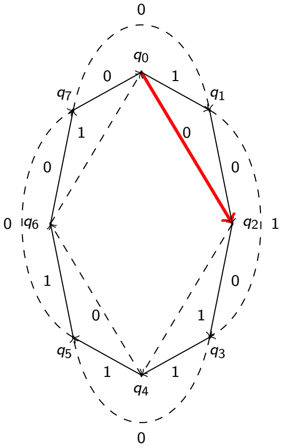
V



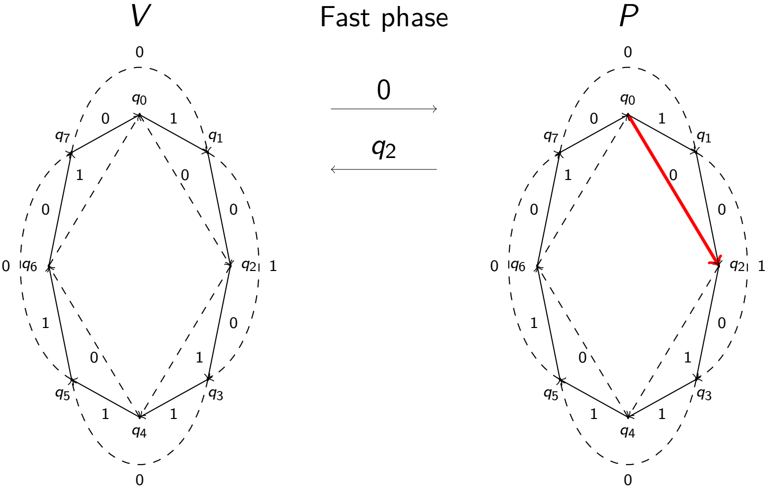
Fast phase

$\xrightarrow{0}$

P

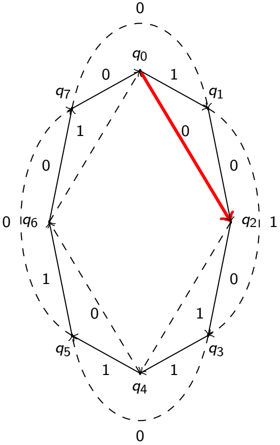


Graph-based protocols



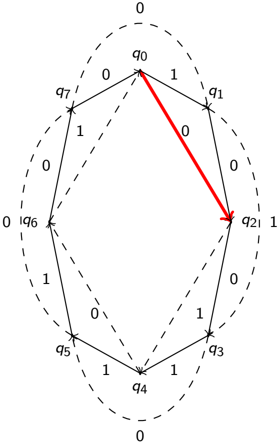
Graph-based protocols

V Fast phase P

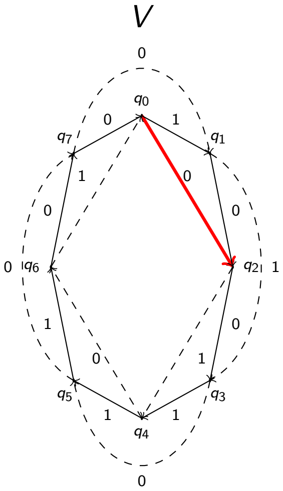


$$\xrightarrow{0}$$

$$\xleftarrow{q_2}$$



Graph-based protocols

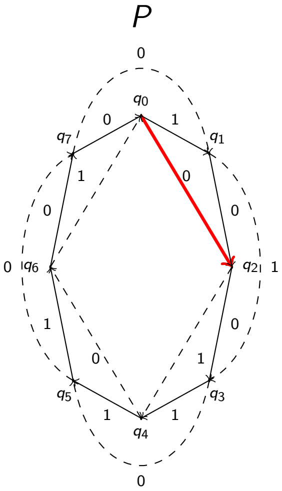


Fast phase

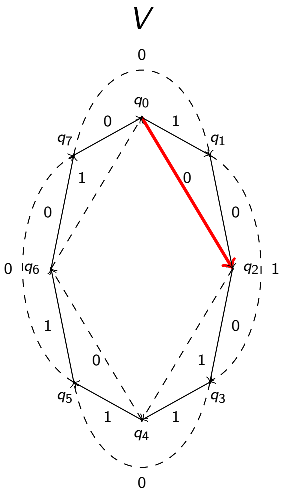
$$\xrightarrow{0}$$

$$\xleftarrow{q_2}$$

$$\xrightarrow{0}$$



Graph-based protocols

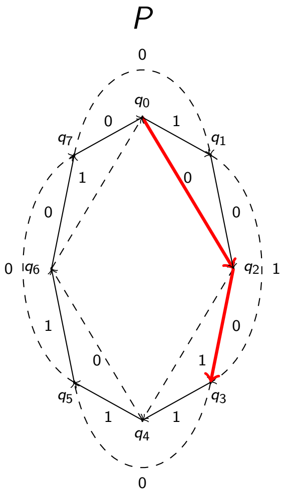


Fast phase

$$\xrightarrow{0}$$

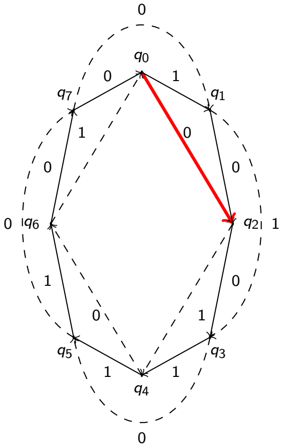
$$\xleftarrow{q_2}$$

$$\xrightarrow{0}$$



Graph-based protocols

V



Fast phase

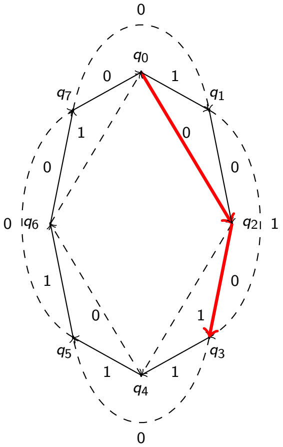
$\xrightarrow{0}$

$\xleftarrow{q_2}$

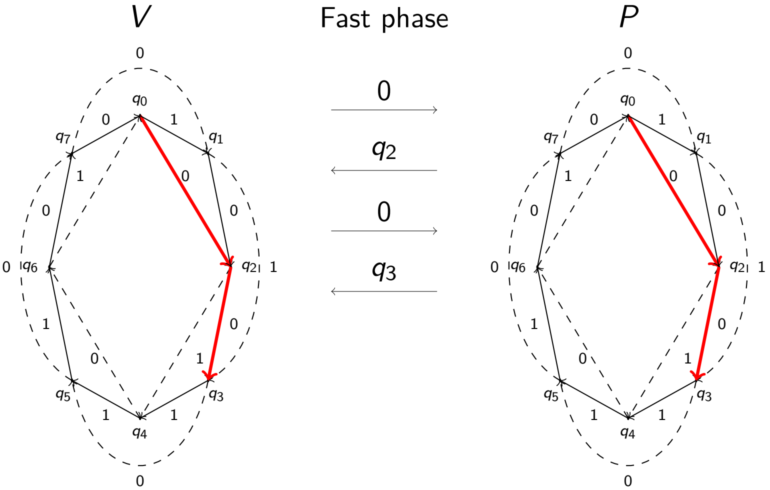
$\xrightarrow{0}$

$\xleftarrow{q_3}$

P



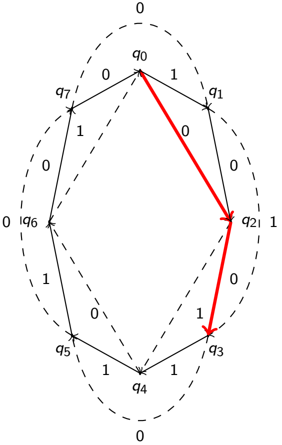
Graph-based protocols



Fast phase

Graph-based protocols

V



Fast phase

$$\xrightarrow{0}$$

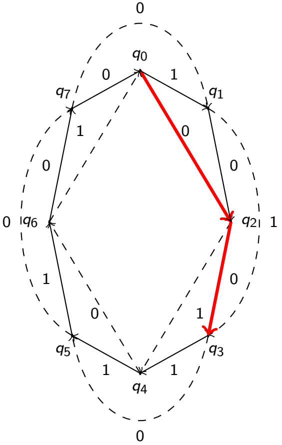
$$\xleftarrow{q_2}$$

$$\xrightarrow{0}$$

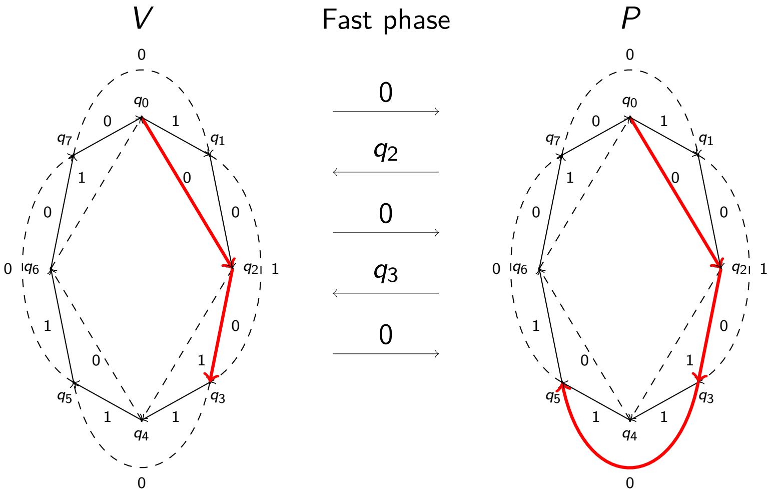
$$\xleftarrow{q_3}$$

$$\xrightarrow{0}$$

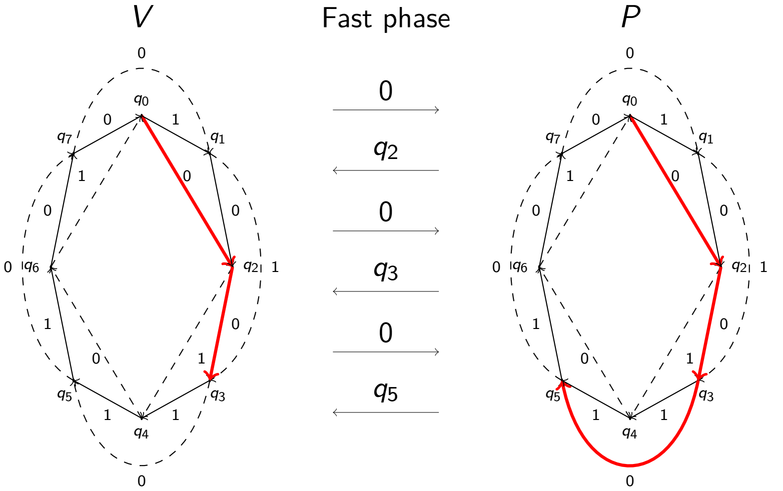
P



Graph-based protocols

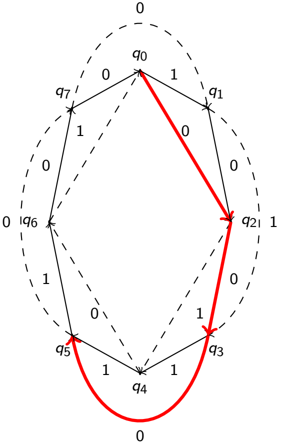


Graph-based protocols



Graph-based protocols

V



Fast phase

$\xrightarrow{0}$

$\xleftarrow{q_2}$

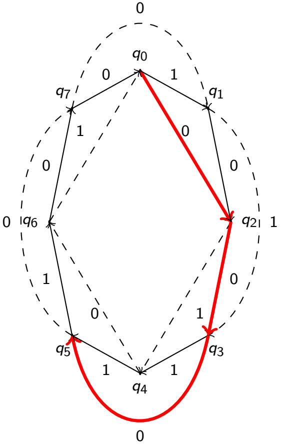
$\xrightarrow{0}$

$\xleftarrow{q_3}$

$\xrightarrow{0}$

$\xleftarrow{q_5}$

P



Questions with respect to distance bounding

1. Can we define the class of lookup-based distance-bounding protocols and perform a generic analysis for its elements.

2. Is there a graph-based protocol that beats AT: $\frac{1}{2^n}(1+\frac{n}{2})$?

3. Do we need an exponential memory to achieve $\frac{1}{2^n}(1+\frac{n}{2})$?

Questions with respect to distance bounding

1. Can we define the class of lookup-based distance-bounding protocols and perform a generic analysis for its elements. Yes, using finite automata
2. Is there a graph-based protocol that beats AT: $\frac{1}{2^n}(1 + \frac{n}{2})$?
3. Do we need an exponential memory to achieve $\frac{1}{2^n}(1 + \frac{n}{2})$?

Questions with respect to distance bounding

1. Can we define the class of lookup-based distance-bounding protocols and perform a generic analysis for its elements.
   Yes, using finite automata
2. Is there a graph-based protocol that beats AT: $\frac{1}{2^n}(1+\frac{n}{2})$?
   No, AT is optimal
3. Do we need an exponential memory to achieve $\frac{1}{2^n}(1+\frac{n}{2})$?

Questions with respect to distance bounding

1. Can we define the class of lookup-based distance-bounding protocols and perform a generic analysis for its elements.
   Yes, using finite automata
2. Is there a graph-based protocol that beats AT: $\frac{1}{2^n}(1 + \frac{n}{2})$?
   No, AT is optimal
3. Do we need an exponential memory to achieve $\frac{1}{2^n}(1 + \frac{n}{2})$?
   Yes, we do.

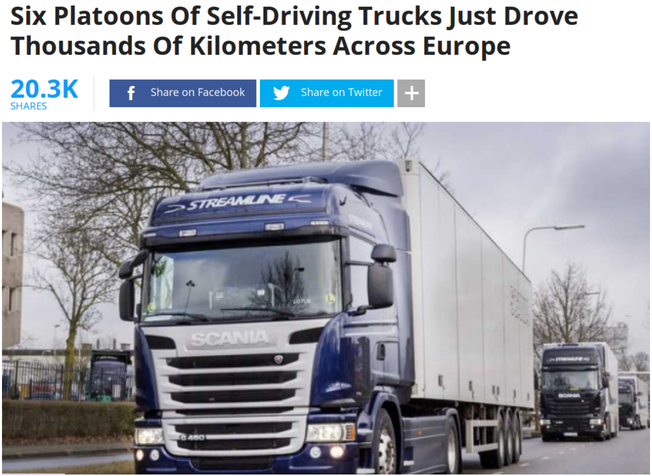
Questions with respect to distance bounding

1. Can we define the class of lookup-based distance-bounding protocols and perform a generic analysis for its elements.
   Yes, using finite automata
2. Is there a graph-based protocol that beats AT: $\frac{1}{2^n}(1+\frac{n}{2})$?
   No, AT is optimal
3. Do we need an exponential memory to achieve $\frac{1}{2^n}(1+\frac{n}{2})$?
   Yes, we do.
   But, we can approximate it without exponential memory.

Generalizing distance bounding: One-to-many

Generalizing distance bounding: Many-to-many

Platooning



Six Platoons Of Self-Driving Trucks Just Drove Thousands Of Kilometers Across Europe

Security challenges

- Secure communication
- Is everybody there? (distance bounding)
- No intruders? (authentication)
- What if objects are moving fast?
- What if the group is dynamic?

Security challenges

- Secure communication
- Is everybody there? (distance bounding)
- No intruders? (authentication)
- What if objects are moving fast?
- What if the group is dynamic?

We have studied published grouping protocols and the majority is flawed.

Security challenges

- Secure communication
- Is everybody there? (distance bounding)
- No intruders? (authentication)
- What if objects are moving fast?
- What if the group is dynamic?

We have studied published grouping protocols and the majority is flawed.
Current objective: distance-bounding grouping protocols.

- Requirements
- Design of novel protocols
- Formal verification

Summary

- Our physical technology has evolved such that security properties are obvious.
- With the transition to the digital world, these properties are not straightforwardly true.
- Don't forget that our physical world largely depends on trust, which is harder to achieve in the digital world.
- Practice: technology first, security later.
- Challenge to combine features (grouping, distance bounding).

ALL RIGHTS OF THE RECORD PRODUCER & OWNER OF THE WORK RECORDED RESERVED MADE IN AUSTRALIA BY FESTIVAL RECORDS PTY. LTD. PUBLIC PERFORMANCE,BROADCASTING & COPYING OF THIS RECORD PROHIBITED.
℗ 1976 Island Records Ltd.
LET'S
STICK TOGETHER
(LET'S WORK TOGETHER)
(Harrison) (United Artists)
A
K-6417
MX49277
(WIP-6307)
(2.59)
BRYAN FERRY
Produced by Chris Thomas and Bryan Ferry
for E.G. Records Ltd.
45

Thanks for your attention!