Background on RFID security

Our contribution

Security analysis

Conclusion&Future work

Secret Shuffling: A Novel Approach to RFID Private Identification

Claude CASTELLUCCIA, Mate SOOS

INRIA team PLANETE, INRIA Rhône-Alpes

September 5, 2010

Claude CASTELLUCCIA, Mate SOOS

< □ ▶ < 部 ▶ < き ▶ くき ▶ き 少へで cret Shuffling: A Novel Approach to RFID Private Identific:

Security analysis

Conclusion&Future work

Table of Contents

Background on RFID security Identification, Authentication...

Our contribution

Protocol Packets Number of packets per identification Algorithm to find the tag

Security analysis

Breaking the anonymity?! Algorithm to attack Threshold phenomenon Security rating

Conclusion&Future work

<ロト < 団ト < 臣 > < き> < き> き のへで scret Shuffling: A Novel Approach to RFID Private Identific

Identification, Authentication, Private communication

What and why?

• Identification: Helps to choose the correct key(certificate, etc.) to authenticate the other party

Claude CASTELLUCCIA, Mate SOOS

< □ > < ⑦ > < 差 > < 差 > 差 の Q @ cret Shuffling: A Novel Approach to RFID Private Identific

What and why?

- Identification: Helps to choose the correct key(certificate, etc.) to authenticate the other party
- Authentication: Helps to be sure who we are talking to



< □ ▶ < 部 ▶ < き ▶ くき ▶ き 少へで cret Shuffling: A Novel Approach to RFID Private Identific:

What and why?

- Identification: Helps to choose the correct key(certificate, etc.) to authenticate the other party
- Authentication: Helps to be sure who we are talking to
- Private communication: Helps to hide messages' content

Our solution is a private identification solution. Private identification solutions until now:

< □ ト < 部 ト < き ト < き ト 差 のへで cret Shuffling: A Novel Approach to RFID Private Identific

What and why?

- Identification: Helps to choose the correct key(certificate, etc.) to authenticate the other party
- Authentication: Helps to be sure who we are talking to
- Private communication: Helps to hide messages' content

Our solution is a private identification solution. Private identification solutions until now:

• Hash-lock based: tree-like, synchronisation-type, mixed

What and why?

- Identification: Helps to choose the correct key(certificate, etc.) to authenticate the other party
- Authentication: Helps to be sure who we are talking to
- Private communication: Helps to hide messages' content Our solution is a private identification solution. Private

identification solutions until now:

- Hash-lock based: tree-like, synchronisation-type, mixed
- Intelligent systems outside the tag: non-authorised readers are not permitted to send identification requests. E.g. RFID blocker tag

What and why?

- Identification: Helps to choose the correct key(certificate, etc.) to authenticate the other party
- Authentication: Helps to be sure who we are talking to
- Private communication: Helps to hide messages' content Our solution is a private identification solution. Private identification solutions until now:
 - Hash-lock based: tree-like, synchronisation-type, mixed
 - Intelligent systems outside the tag: non-authorised readers are not permitted to send identification requests. E.g. RFID blocker tag
 - Ultra-lightweight crypto-primitives: lightweight implementations of ECC, AES, and totally new primitives (e.g. Vajda&Buttyán)

Security analysis

Conclusion&Future work

Protocol description

Protocol setup:

Each tag has a constant, random K long key, k_i, that is a unique bitstring(k_i[1]...k_i[K]) for each tag T_i

Claude CASTELLUCCIA, Mate SOOS

<ロト < 置 > < 差 > く 差 > 差 の Q @ scret Shuffling: A Novel Approach to RFID Private Identific

Protocol description

Protocol setup:

- Each tag has a constant, random K long key, k_i, that is a unique bitstring(k_i[1]...k_i[K]) for each tag T_i
- The reader knows all tag's keys

Claude CASTELLUCCIA, Mate SOOS

《□▷《圖▷《콜▷《콜▷ 콜 ∽잇솏(~ cret Shuffling: A Novel Approach to RFID Private Identifica

Protocol description

Protocol setup:

- Each tag has a constant, random K long key, k_i, that is a unique bitstring(k_i[1]...k_i[K]) for each tag T_i
- The reader knows all tag's keys
- There are far less tags, n, in the system than there are possible keys, $2^K \!\!: n \ll 2^K$

Protocol description

Protocol setup:

- Each tag has a constant, random K long key, k_i, that is a unique bitstring(k_i[1]...k_i[K]) for each tag T_i
- The reader knows all tag's keys
- There are far less tags, n, in the system than there are possible keys, $2^K \!\!: n \ll 2^K$

TAG

How it works:

READER



<ロト < 部 > < き > くき > き の Q () ecret Shuffling: A Novel Approach to RFID Private Identifica

Conclusion&Future work

Description of a packet

Description of a packet:

• Consists of *L* number of indexes from the key of the tag. Each index can be either inverted or not. No indexes are repeated

Claude CASTELLUCCIA, Mate SOOS

< □ ト < 部 ト < 注 ト < 注 ト 注 の へ C ecret Shuffling: A Novel Approach to RFID Private Identifi

Description of a packet

Description of a packet:

- Consists of *L* number of indexes from the key of the tag. Each index can be either inverted or not. No indexes are repeated
- Has the following interesting property: $\sum_{j=1}^{L} k_i [a_j] \oplus b_j = L/2 \text{ where } a_j \xleftarrow{r} [1, K] \text{ is a random index,}$ and $b_j \xleftarrow{r} \{0, 1\}$ is a random bit $b_j \xleftarrow{r} \{0, 1\}$

Security analysis

Conclusion&Future work

Description of a packet



Claude CASTELLUCCIA, Mate SOOS

< □ ▷ < 큔 ▷ < 분 ▷ < 분 ▷ 분
 Shuffling: A Novel Approach to RFID Private Identification

Security analysis

Conclusion&Future work

Description of a packet

From a computational complexity point of view:

• The packet is a constraint satisfaction problem (specifically, a linear pseudo-boolean constraint satisfaction problem)

Claude CASTELLUCCIA, Mate SOOS

ecret Shuffling: A Novel Approach to RFID Private Identifi

(ロ) (同) (E) (E) (E)

Description of a packet

From a computational complexity point of view:

- The packet is a constraint satisfaction problem (specifically, a linear pseudo-boolean constraint satisfaction problem)
- The packet is an L/2-in-L LSAT problem

Claude CASTELLUCCIA, Mate SOOS

《□▷《冊▷《불▷《불▷ 불 ∽)<</p>
Cret Shuffling: A Novel Approach to RFID Private Identification

Description of a packet

From a computational complexity point of view:

- The packet is a constraint satisfaction problem (specifically, a linear pseudo-boolean constraint satisfaction problem)
- The packet is an L/2-in-L LSAT problem
- These problems are equivalent and NP-hard (Shaefer's dichotomy theorem)

Security analysis

Conclusion&Future work

Number of packets per identification

How many packets will let the reader identify the tag?

• Number of solutions possible for the reader: n

Claude CASTELLUCCIA, Mate SOOS

Conclusion&Future work

Number of packets per identification

How many packets will let the reader identify the tag?

- Number of solutions possible for the reader: n
- One packet reduces the solution space by a factor of

$$R \approx \frac{\left(\begin{array}{c} K \\ L/2 \end{array}\right)^2}{\left(\begin{array}{c} 2 * K \\ L \end{array}\right)}$$

Conclusion&Future work

Number of packets per identification

How many packets will let the reader identify the tag?

- Number of solutions possible for the reader: n
- One packet reduces the solution space by a factor of

$$R \approx \frac{\left(\begin{array}{c} K\\ L/2 \end{array}\right)^2}{\left(\begin{array}{c} 2 * K\\ L \end{array}\right)}$$

• We want to reduce the solution space to 0 - the only possible solution must be the *inherent* solution, i.e. k

Conclusion&Future work

Number of packets per identification

How many packets will let the reader identify the tag?

- Number of solutions possible for the reader: n
- One packet reduces the solution space by a factor of

$$R \approx \frac{\left(\begin{array}{c} K\\ L/2 \end{array}\right)^2}{\left(\begin{array}{c} 2 * K\\ L \end{array}\right)}$$

- We want to reduce the solution space to 0 the only possible solution must be the *inherent* solution, i.e. k
- The number of packets needed for a given false positive rate is then: $fp\approx \frac{log(fp/n)}{log(R)}$

<ロ>> < 団> < 団> < 三> < 三> < 三> < 三> < 三> へのへ cret Shuffling: A Novel Approach to RFID Private Identific

Conclusion&Future work

Number of packets per identification

How many packets will let the reader identify the tag?

- Number of solutions possible for the reader: n
- One packet reduces the solution space by a factor of

$$R \approx \frac{\left(\begin{array}{c} K\\ L/2 \end{array}\right)^2}{\left(\begin{array}{c} 2 * K\\ L \end{array}\right)}$$

- We want to reduce the solution space to 0 the only possible solution must be the *inherent* solution, i.e. k
- The number of packets needed for a given false positive rate is then: $fp\approx \frac{log(fp/n)}{log(R)}$
- For fp = 0.1, i.e. for 90% identification chance, if K = 400, L = 10 and n = 1 million, P = 13

Security analysis

Conclusion&Future work

Graphic example

From the point of view of the size of the solution space:

• Reader's point of view:





Security analysis

Conclusion&Future work

Graphic example

From the point of view of the size of the solution space:

• Reader's point of view:



• Attacker's point of view:



<ロト < @> < き> くき> き のへで scret Shuffling: A Novel Approach to RFID Private Identific:

Security analysis

Conclusion&Future work

Algorithm to find the tag

What is the difference between a reader and an attacker?

• Caching n = 1 million keys takes as much as storing the keys

Claude CASTELLUCCIA, Mate SOOS

<ロ>> < 母> < き> < き> < き> こ き つくの scret Shuffling: A Novel Approach to RFID Private Identific

Algorithm to find the tag

What is the difference between a reader and an attacker?

- Caching n = 1 million keys takes as much as storing the keys
- Caching 2^K keys in memory is impossible

Caching:

Claude CASTELLUCCIA, Mate SOOS

《ロ》《郡》《臣》《臣》 臣 のへで ret Shuffling: A Novel Approach to RFID Private Identifica

Algorithm to find the tag

What is the difference between a reader and an attacker?

- Caching n = 1 million keys takes as much as storing the keys
- Caching 2^K keys in memory is impossible

Caching:

• Pre-construct look-up lists for all key's indexes:



Claude CASTELLUCCIA, Mate SOOS

《□▶ 《큔》 《茎》 《茎》 볼 ∽) 옷 (은 ecret Shuffling: A Novel Approach to RFID Private Identifica

Algorithm to find the tag

What is the difference between a reader and an attacker?

- Caching n = 1 million keys takes as much as storing the keys
- Caching 2^K keys in memory is impossible

Caching:

• Pre-construct look-up lists for all key's indexes:



• Go through the look-up table for the indexes in the packet, and calculate the shown sum for each packet. The tag that has L/2 for all packets is the one that is sending them

Conclusion&Future work

What do we mean by breaking the anonymity

We use Juels and Weis' "strong privacy" model:

* The attacker has q as a query limit and c as a calculation limit

Claude CASTELLUCCIA, Mate SOOS

<ロト < 理ト < 速ト < きト き のへで scret Shuffling: A Novel Approach to RFID Private Identific

What do we mean by breaking the anonymity

We use Juels and Weis' "strong privacy" model:

- * The attacker has q as a query limit and c as a calculation limit
- 1 Give the attacker all n tags, let him query them without surpassing the q query limit

Claude CASTELLUCCIA, Mate SOOS

< □ ト < 部 ト < 臣 ト < 臣 ト ミ の Q ペ cret Shuffling: A Novel Approach to RFID Private Identifica

- st The attacker has q as a query limit and c as a calculation limit
- $1\,$ Give the attacker all n tags, let him query them without surpassing the q query limit
- $2\,$ Let the attacker do calculations within the limit of $c\,$

- * The attacker has q as a query limit and c as a calculation limit
- $1\,$ Give the attacker all n tags, let him query them without surpassing the q query limit
- $2\,$ Let the attacker do calculations within the limit of $c\,$
- 3 Let the attacker select 2 tags, \mathcal{T}_A and \mathcal{T}_B

- st The attacker has q as a query limit and c as a calculation limit
- 1 Give the attacker all n tags, let him query them without surpassing the q query limit
- $2\,$ Let the attacker do calculations within the limit of $c\,$
- 3 Let the attacker select 2 tags, \mathcal{T}_A and \mathcal{T}_B
- 4 Secretly and randomly select one of the two, let's call it \mathcal{T}_C

- * The attacker has q as a query limit and c as a calculation limit
- 1 Give the attacker all n tags, let him query them without surpassing the q query limit
- $2\,$ Let the attacker do calculations within the limit of $c\,$
- 3 Let the attacker select 2 tags, \mathcal{T}_A and \mathcal{T}_B
- 4 Secretly and randomly select one of the two, let's call it \mathcal{T}_C
- 5 Let the attacker query \mathcal{T}_C without surpassing the q query limit

- * The attacker has q as a query limit and c as a calculation limit
- 1 Give the attacker all n tags, let him query them without surpassing the q query limit
- $2\,$ Let the attacker do calculations within the limit of $c\,$
- 3 Let the attacker select 2 tags, \mathcal{T}_A and \mathcal{T}_B
- 4 Secretly and randomly select one of the two, let's call it \mathcal{T}_C
- 5 Let the attacker query \mathcal{T}_C without surpassing the q query limit
- 6 Let the attacker do calculations within the limit of c

We use Juels and Weis' "strong privacy" model:

- st The attacker has q as a query limit and c as a calculation limit
- 1 Give the attacker all n tags, let him query them without surpassing the q query limit
- $2\,$ Let the attacker do calculations within the limit of $c\,$
- 3 Let the attacker select 2 tags, \mathcal{T}_A and \mathcal{T}_B
- 4 Secretly and randomly select one of the two, let's call it \mathcal{T}_C
- 5 Let the attacker query \mathcal{T}_C without surpassing the q query limit
- 6 Let the attacker do calculations within the limit of c
- 7 The attacker must tell if $\mathcal{T}_C = \mathcal{T}_A$ or $\mathcal{T}_C = \mathcal{T}_B$ with sufficient probability

ecret Shuffling: A Novel Approach to RFID Private Identifica

◆□ ▶ ◆□ ▶ ◆ □ ▶ ◆ □ ▶ ● □ ● ● ● ●

Security analysis ○●○○○○ Conclusion&Future work

Best attacker strategy

 Since all tags are totally independent, only the two pre-selected ones will be examined, i.e. T_A and T_B

Claude CASTELLUCCIA, Mate SOOS

< □ ▷ < 큔 ▷ < 볼 ▷ < 볼 ▷ 볼 ∽ Q (~ cret Shuffing: A Novel Approach to RFID Private Identifica

Security analysis ○●○○○○ Conclusion&Future work

Best attacker strategy

- Since all tags are *totally independent*, only the two pre-selected ones will be examined, i.e. T_A and T_B
- Query only one of the two tags $(\mathcal{T}_A, \mathcal{T}_B)$ for q/2 queries, e.g. \mathcal{T}_A , and obtain packets Run_A

Claude CASTELLUCCIA, Mate SOOS

< □ > < 部 > < き > く き > き のへで cret Shuffling: A Novel Approach to RFID Private Identific

Conclusion&Future work

Best attacker strategy

- Since all tags are totally independent, only the two pre-selected ones will be examined, i.e. T_A and T_B
- Query only one of the two tags $(\mathcal{T}_A, \mathcal{T}_B)$ for q/2 queries, e.g. \mathcal{T}_A , and obtain packets Run_A
- Query \mathcal{T}_C for q/2 queries, and obtain the packets Run_C

Claude CASTELLUCCIA, Mate SOOS

《□▷《冊▷《불▷《불▷ 불 ∽)<</p>
Cret Shuffling: A Novel Approach to RFID Private Identification

Conclusion&Future work

Best attacker strategy

- Since all tags are *totally independent*, only the two pre-selected ones will be examined, i.e. T_A and T_B
- Query only one of the two tags $(\mathcal{T}_A, \mathcal{T}_B)$ for q/2 queries, e.g. \mathcal{T}_A , and obtain packets Run_A
- Query \mathcal{T}_C for q/2 queries, and obtain the packets Run_C
- Find the solution to the constraint satisfaction problem defined by the packets $Run_A \cup Run_C$

Security analysis ○●○○○○ Conclusion&Future work

Best attacker strategy

- Since all tags are *totally independent*, only the two pre-selected ones will be examined, i.e. T_A and T_B
- Query only one of the two tags $(\mathcal{T}_A, \mathcal{T}_B)$ for q/2 queries, e.g. \mathcal{T}_A , and obtain packets Run_A
- Query \mathcal{T}_C for q/2 queries, and obtain the packets Run_C
- Find the solution to the constraint satisfaction problem defined by the packets $Run_A \cup Run_C$
- If the solution is UNSAT, then the two tags must be different packets sent by T_A always have solution k_A

Conclusion&Future work

Best attacker strategy

- Since all tags are *totally independent*, only the two pre-selected ones will be examined, i.e. T_A and T_B
- Query only one of the two tags $(\mathcal{T}_A, \mathcal{T}_B)$ for q/2 queries, e.g. \mathcal{T}_A , and obtain packets Run_A
- Query \mathcal{T}_C for q/2 queries, and obtain the packets Run_C
- Find the solution to the constraint satisfaction problem defined by the packets $Run_A \cup Run_C$
- If the solution is UNSAT, then the two tags must be different packets sent by T_A always have solution k_A
- If the solution is SAT, then:

<ロト 4 団ト 4 団ト 4 茎ト 4 茎ト 茎 のへで cret Shuffling: A Novel Approach to RFID Private Identific;

Security analysis ○●○○○○ Conclusion&Future work

Best attacker strategy

- Since all tags are *totally independent*, only the two pre-selected ones will be examined, i.e. T_A and T_B
- Query only one of the two tags $(\mathcal{T}_A, \mathcal{T}_B)$ for q/2 queries, e.g. \mathcal{T}_A , and obtain packets Run_A
- Query \mathcal{T}_C for q/2 queries, and obtain the packets Run_C
- Find the solution to the constraint satisfaction problem defined by the packets $Run_A \cup Run_C$
- If the solution is UNSAT, then the two tags must be different packets sent by T_A always have solution k_A
- If the solution is SAT, then:
 - Either $\mathcal{T}_A \neq \mathcal{T}_C$ BUT we did not gather enough packets to show they are different

ecret Shuffling: A Novel Approach to RFID Private Identifica

Conclusion&Future work

Best attacker strategy

- Since all tags are *totally independent*, only the two pre-selected ones will be examined, i.e. T_A and T_B
- Query only one of the two tags $(\mathcal{T}_A, \mathcal{T}_B)$ for q/2 queries, e.g. \mathcal{T}_A , and obtain packets Run_A
- Query \mathcal{T}_C for q/2 queries, and obtain the packets Run_C
- Find the solution to the constraint satisfaction problem defined by the packets $Run_A \cup Run_C$
- If the solution is UNSAT, then the two tags must be different packets sent by T_A always have solution k_A
- If the solution is SAT, then:
 - Either $\mathcal{T}_A \neq \mathcal{T}_C$ BUT we did not gather enough packets to show they are different
 - OR $T_A = T_C$. if we have gathered enough for sure, we can safely say this. 'Enough' in this context is defined as P_{att}

◆□▶ ◆□▶ ◆三▶ ◆三▶ ● ○ ○ ○

Security analysis ○○●○○○ Conclusion&Future work

Algorithm to attack

Best algorithm to attack the system:

• There are specialized solvers to find a solution to the problem described by the packets (LPBC solvers). But, these are slow for multiple reasons

Claude CASTELLUCCIA, Mate SOOS

《ロ》《澄》《登》《登》 をきり き のへの cret Shuffling: A Novel Approach to RFID Private Identifi

Security analysis ○○●○○○ Conclusion&Future work

Algorithm to attack

Best algorithm to attack the system:

- There are specialized solvers to find a solution to the problem described by the packets (LPBC solvers). But, these are slow for multiple reasons
- There are solvers to find a solution to general SAT problems (i.e. $a \lor \overline{b} \lor c \lor ...$). Packets must be converted to this representation. These solvers are fast

Claude CASTELLUCCIA, Mate SOOS

< □ ▷ < 큔 ▷ < 분 ▷ < 분 ▷ 분 - 위역() cret Shuffling: A Novel Approach to RFID Private Identifica

Security analysis ○○●○○○ Conclusion&Future work

Algorithm to attack

Best algorithm to attack the system:

- There are specialized solvers to find a solution to the problem described by the packets (LPBC solvers). But, these are slow for multiple reasons
- There are solvers to find a solution to general SAT problems (i.e. a ∨ b̄ ∨ c ∨ ...). Packets must be converted to this representation. These solvers are fast

We decided on Minisat (best of the 2005&2006 SAT competition). It is fast, open-source and readily modifiable

Threshold phenomenon

There is a so-called threshold phenomenon for all NP-hard problems. This states that when solving a *randomly* generated SAT problem, there are three phases in terms of the number of constraints:

• Solution is fast to find, chance to find one is nearly 100%

Claude CASTELLUCCIA, Mate SOOS

Threshold phenomenon

There is a so-called threshold phenomenon for all NP-hard problems. This states that when solving a *randomly* generated SAT problem, there are three phases in terms of the number of constraints:

- Solution is fast to find, chance to find one is nearly 100%
- After a certain point, the chance to find solution changes very rapidly from 100% to 0%, and at the same time, the difficulty to find a solution jumps to very high levels. This is the *threshold point*.

Threshold phenomenon

There is a so-called threshold phenomenon for all NP-hard problems. This states that when solving a *randomly* generated SAT problem, there are three phases in terms of the number of constraints:

- Solution is fast to find, chance to find one is nearly 100%
- After a certain point, the chance to find solution changes very rapidly from 100% to 0%, and at the same time, the difficulty to find a solution jumps to very high levels. This is the *threshold point*.
- After the threshold point, the chance to find a solution is almost 0%, but if there exists a solution (or if it does not), it becomes exponentially easier to find it (or find that it does not exist respectively) in respect to the number of constraints.

< □ ▶ < 部 ▶ < 茎 ▶ < 茎 ▶ 茎 のへで cret Shuffling: A Novel Approach to RFID Private Identific

Graphically



Claude CASTELLUCCIA, Mate SOOS

・ロト ・回ト ・ヨト ・ヨト

æ

Graphically



The attacker can only use the right side of the graph

Claude CASTELLUCCIA, Mate SOOS

・ロト ・回ト ・ヨト ・ヨト

Э

Security analysis

Conclusion&Future work

Results

100	200	400	1000
$1.47e2~{ m s}$	$3.17e11~{ m s}$	$1.46e28~{ m s}$	$1.46e78~{ m s}$
$3.33e1~{ m s}$	$7.41e5 \; \mathrm{s}$	$3.67e14~{ m s}$	$4.49e40~{\rm s}$
$6.31e0~{ m s}$	$4.54e3~{ m s}$	$2.35e9~{ m s}$	$3.27e26 \mathrm{~s}$
$4.27e0~{\rm s}$	$6.37e2~{ m s}$	$1.42e7~{ m s}$	$1.57e20~{ m s}$
$4.02e0~{\rm s}$	$4.87e2~{\rm s}$	$7.15e6~{ m s}$	$2.27e19~{ m s}$
$5.34e0~{ m s}$	$7.31e1~{ m s}$	$1.37e4~{ m s}$	$9.01e10~{ m s}$
$1.00e1 \; \mathrm{s}$	$7.28e1~{ m s}$	$3.86e3~{ m s}$	$5.74e8~{ m s}$
	100 1.47e2 s 3.33e1 s 6.31e0 s 4.27e0 s 4.02e0 s 5.34e0 s 1.00e1 s	$\begin{array}{c cccc} 100 & 200 \\ \hline 1.47e2 \ {\rm s} & 3.17e11 \ {\rm s} \\ 3.33e1 \ {\rm s} & 7.41e5 \ {\rm s} \\ 6.31e0 \ {\rm s} & 4.54e3 \ {\rm s} \\ 4.27e0 \ {\rm s} & 6.37e2 \ {\rm s} \\ 4.02e0 \ {\rm s} & 4.87e2 \ {\rm s} \\ 5.34e0 \ {\rm s} & 7.31e1 \ {\rm s} \\ 1.00e1 \ {\rm s} & 7.28e1 \ {\rm s} \end{array}$	$\begin{array}{c ccccc} 100 & 200 & 400 \\ \hline 1.47e2 \ {\rm s} & 3.17e11 \ {\rm s} & 1.46e28 \ {\rm s} \\ 3.33e1 \ {\rm s} & 7.41e5 \ {\rm s} & 3.67e14 \ {\rm s} \\ 6.31e0 \ {\rm s} & 4.54e3 \ {\rm s} & 2.35e9 \ {\rm s} \\ 4.27e0 \ {\rm s} & 6.37e2 \ {\rm s} & 1.42e7 \ {\rm s} \\ 4.02e0 \ {\rm s} & 4.87e2 \ {\rm s} & 7.15e6 \ {\rm s} \\ 5.34e0 \ {\rm s} & 7.31e1 \ {\rm s} & 1.37e4 \ {\rm s} \\ 1.00e1 \ {\rm s} & 7.28e1 \ {\rm s} & 3.86e3 \ {\rm s} \end{array}$

Table: Time to break the anonymity

Claude CASTELLUCCIA, Mate SOOS

<ロ>< 団>< 団>< 臣>< 注>< 注>< 注</td>

Conclusion&Future work

Conclusion&Future work

 We have developed an RFID privacy solution that is suitable for cheap tags

Claude CASTELLUCCIA, Mate SOOS

Conclusion&Future work

- We have developed an RFID privacy solution that is suitable for cheap tags
- The developed protocol's fundamentals are such that it can potentially be a foundation for many protocols to come

Claude CASTELLUCCIA, Mate SOOS

<ロト < 部ト < 注ト < 注ト 注 の Q ペ cret Shuffling: A Novel Approach to RFID Private Identifica

Conclusion&Future work

- We have developed an RFID privacy solution that is suitable for cheap tags
- The developed protocol's fundamentals are such that it can potentially be a foundation for many protocols to come
- We are at the moment developing an improvement of the presented protocol

Claude CASTELLUCCIA, Mate SOOS

< □ ▷ < 큔 ▷ < 분 ▷ < 분 ▷ 분 < 옷
 Cret Shuffling: A Novel Approach to RFID Private Identification

Background on RFID security

Our contribution

Security analysis

Conclusion&Future work

Thank you for your time

Are there any questions?

Claude CASTELLUCCIA, Mate SOOS

< □ > < 큔 > < 큔 > < 글 > < 글 > 트 의 < 관 > 트 의 < ↔