Radio-Frequency Identification (RFID)

Exploration

IRISA
Embedded Security and Cryptography (EMSEC)

02/04/2015

Outline

Definition :

The contactless technology is a ’no touch’ technology where 2 entities create a communication channel by radiating electromagnetic waves. This communication channel can optionally be authenticated and encrypted.

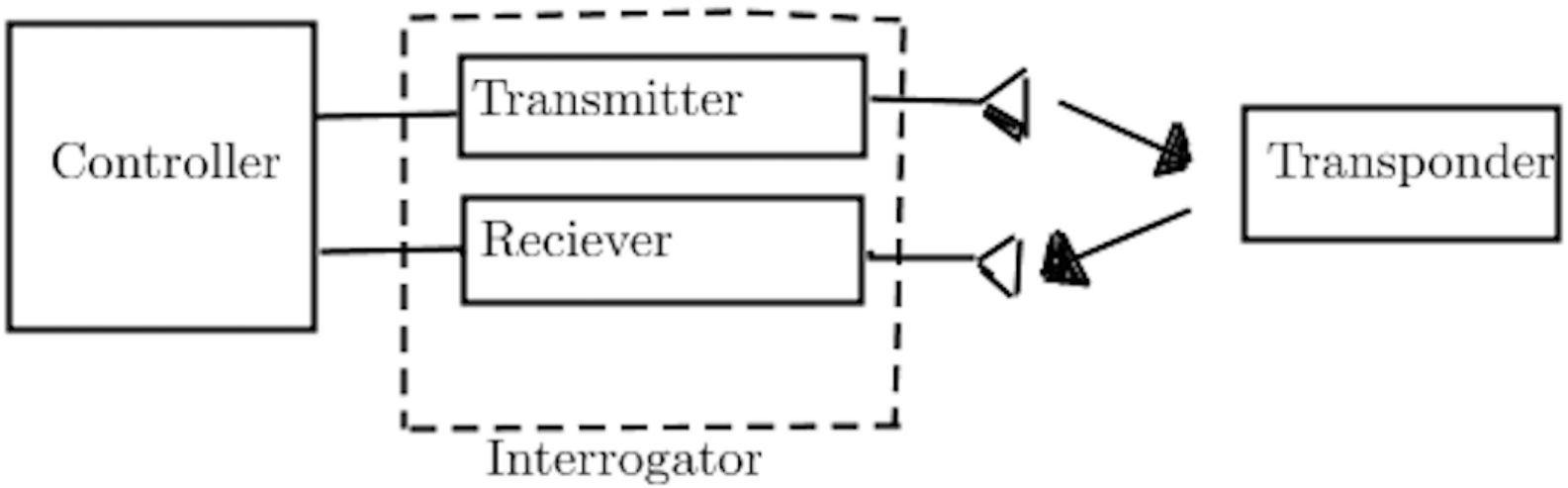
Some examples :

- Radio-Frequency Identification(RFID) technology.
- Near Field Communication(NFC) technology.
- Contactless SmartCards technology.
- Wi-Fi.

Definition :

- Radio-Frequency Identification technology allows devices called readers or interrogators to identify wirelessly objects or persons which/who hold what we call RFID tags (or transponders).
- RFID tags obtain power and/or exchange data from/with readers through electromagnetic waves resulting from the EM field created by the readers.

Definition :
Illustration of an RFID system

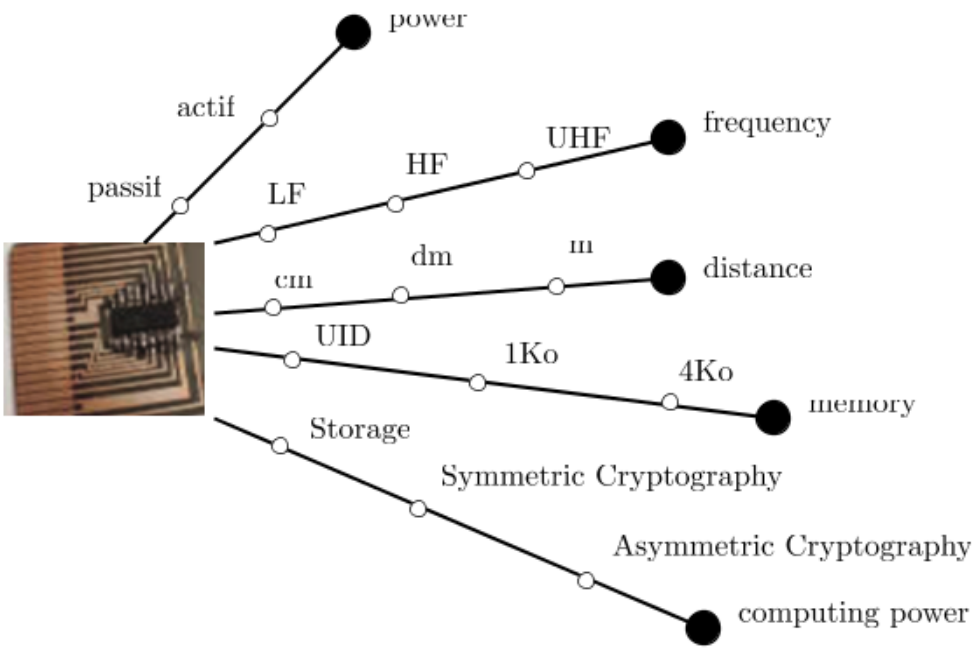


Transponders

- Small microchip with limited data storage, logical functionnality and processing capability.
- RF interface :
  - Antenna : allows the RFID tag to couple to an EM field to obtain power, or to communicate with the reader, or to do both.
  - Transmitter : modulate the signals for sending responses to readers.
  - Receiver : receive and demodulate signals received from readers.
- Examples : Mifare UltraLight, Mifare Desfire,..

Transponders

- RFID tags can be distinguished based on:



Transcievers

- RF interface :
  - Antenna : is an electrical device which converts electric currents into radio waves, and vice versa.
  - Transmitter : modulate the signals for sending requests to RFID tags.
  - Receiver : receive and demodulate signals received from tags.
- Control Unit :
  - Controls the communication between the backend system and the RFID tag.
  - Communicate with the backend system
- Examples : pn532, pn533 from NXP.

Backend Systems

- Manage the information related to the RFID tags : Every object's information is stored as a record in a database server, and the information on the tag attached to that object serves as a pointer to the record.
- The readers are connected to the backend systems through a secure channel.

Overview

Many standards exist for contactless technology interfaces in order to :

- Unify the architecture of RFID tags or contactless SmartCards.
- Enable an inter-industry communication.

Overview

We distinguish standards for :

- Proximity devices (ISO14443) :
  - 10 cm , HF (13,56 MHz).
  - It applies to RFID devices which may be type A and type B.
  - The main difference between these types concern modulation methods and protocol initialization procedures (layers 2 and 3).

Overview

We distinguish standards for :

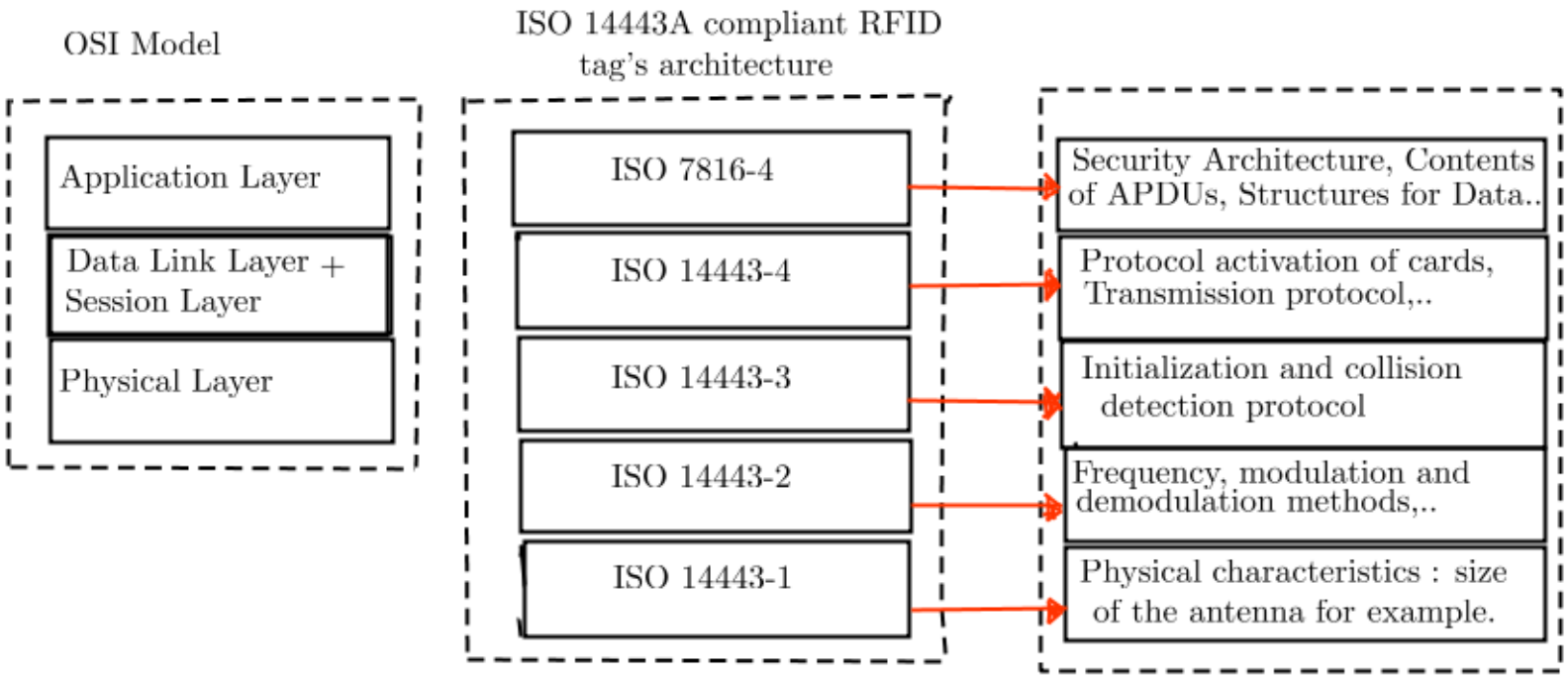
- Vicinity devices (ISO15693) :
  - 1m, HF(13,56 MHz).
  - It applies also to RFID devices, but applications where it is used differ from the ones where ISO14443 is used.

Overview

We distinguish standards for :

- Near Field devices (ISO18092) :
  - 10 cm, HF(13,56 MHz).
  - It is an extension of ISO14443 standard for peer-to-peer tags.

Architecture of an ISO 14443A compliant RFID tag



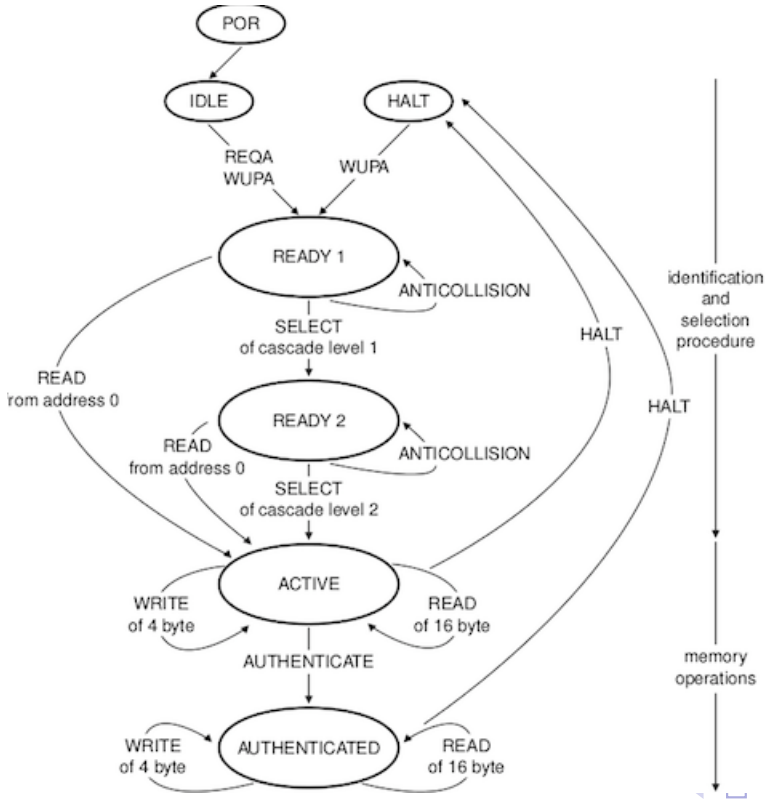
Architecture of an ISO 14443A compliant RFID tag

State Diagram

- An ISO 14443A compliant RFID tag (or PICC) is considered as a state machine where possible transitions from one state to another are caused by commands sent by the reader (or PCD):

Architecture of an ISO 14443A compliant RFID tag

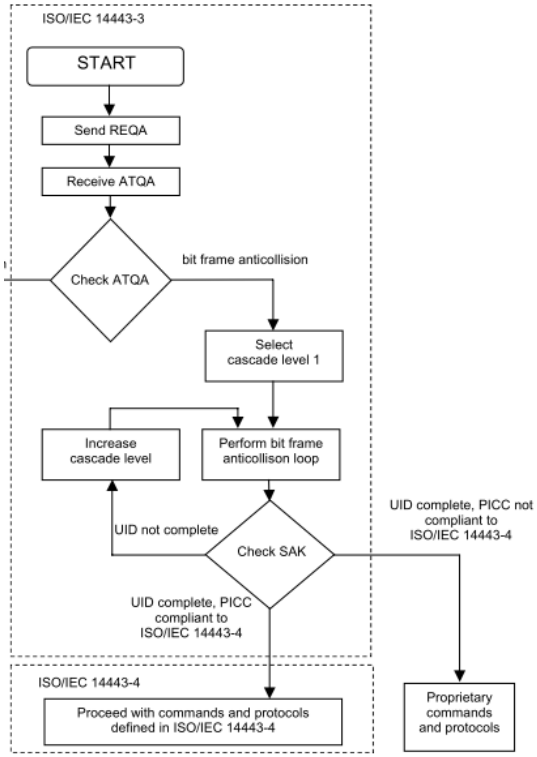
State Diagram



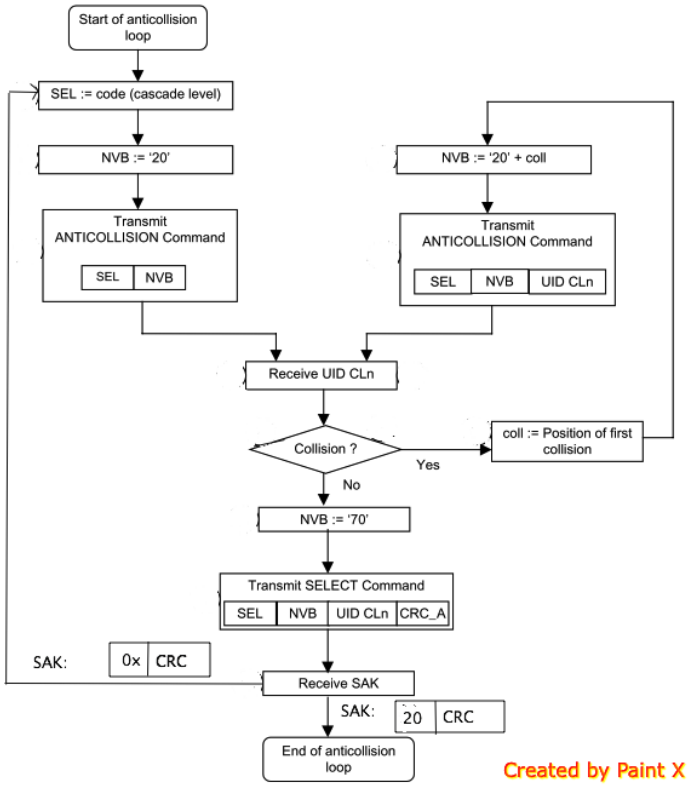
Description of ISO 14443A-3 layer

- Initialization and collision detection protocol.
- Definition of frame format and timing used during communication initialization and anticollision.

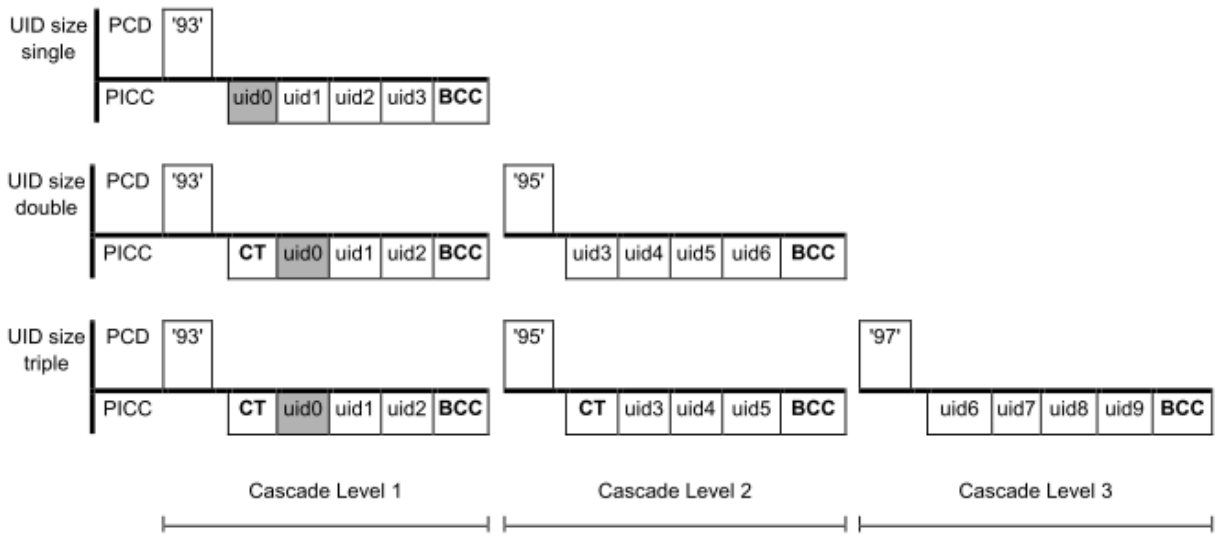
Description of ISO 14443A-3 layer :
Initialization and anti-collision protocol



Description of ISO 14443A-3 layer :
Initialization and anti-collision protocol



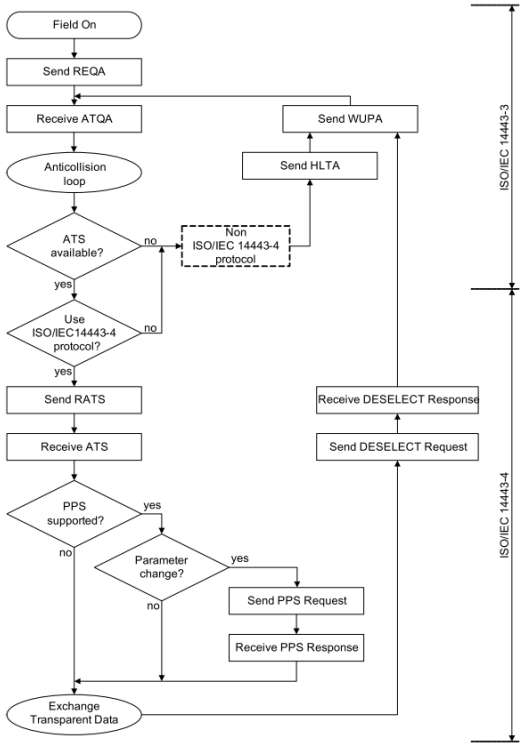
Description of ISO 14443A-3 layer :
Initialization and anti-collision protocol



Description of ISO 14443A-4 layer

- Activation protocol :
  - Description of activation protocol of PICCs supporting ISO 14443-4 standard.
  - Definition of frame format and timing used during communication activation.
- Transmission protocol :
  - Definition of frame format and timing during transmission of information between the PCD and the PICC.
  - Description of protocol operation.

Description of ISO 14443A-4 layer :
Activation protocol



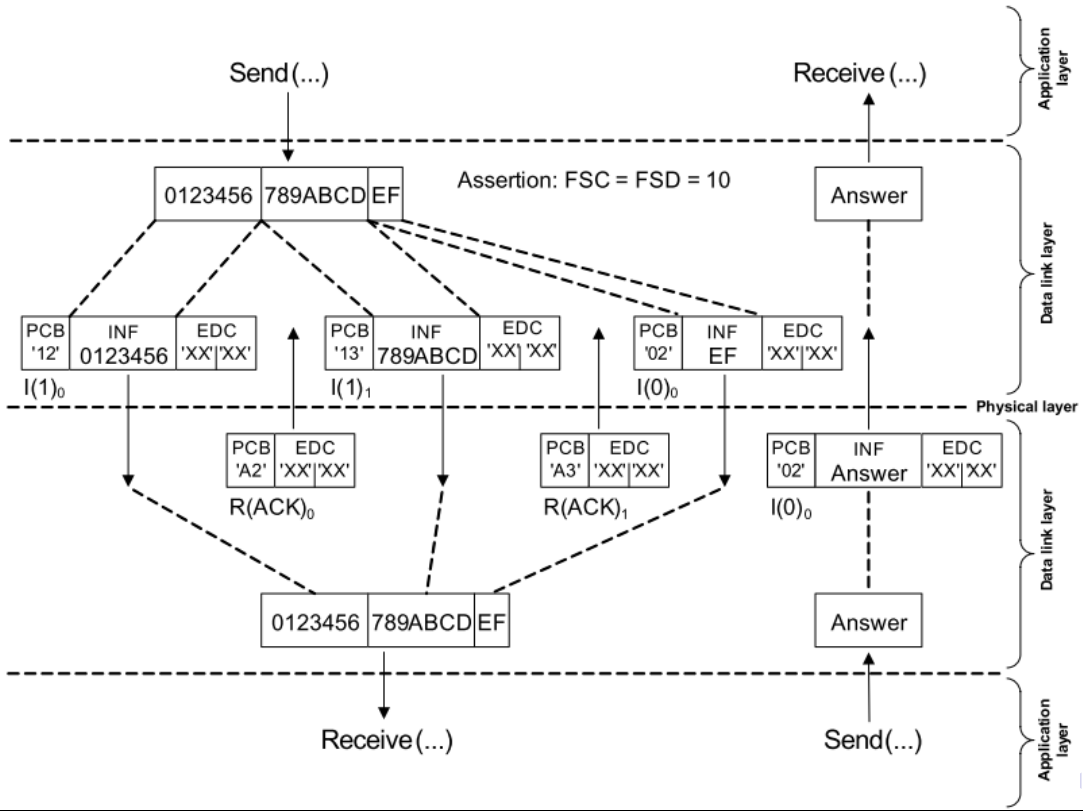
Description of ISO 14443A-4 layer :
Transmission protocol

- Communication between the PCD and the PICC is half-duplex : the PCD sends always a command and shall wait for the corresponding response from the PICC before sending another command.
- Protocol Data Unit : this layer uses blocks consisting of prologue field, information field and epilogue field.

Description of ISO 14443A-4 layer :
Transmission protocol

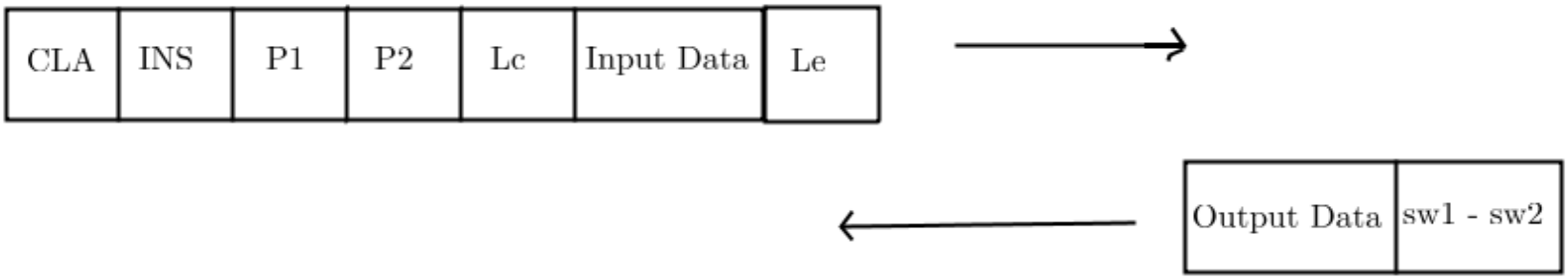
- Multi-activation : allows the PCD to communicate with several PICCs simultaneously.
- Chaining : allows the PCD or the PICC to transmit information that does not fit in a single block as defined by FSC or FSD respectively, by dividing the information into several blocks.

Description of ISO 14443A-4 layer :
Transmission protocol



Description of ISO 7816-4 layer

- Contents of command-response pairs :



- Structures for applications and data in the card : applications, directories, files.
- Security architecture : access rights, authentication, encryption..

Examples of products

http://open-nfc.org/documents/$PRE_NFC_0804-250%20NFC%20Standards$.pdf

Mifare UltraLight

- Memory organisation : 16 sectors of 4 bytes. Some sectors are read-only (UID sectors).
- Command set : In addition to commands defined by the standard, we find 2 commands : Read and Write.
- Access control : Lock bytes and OTP bytes.
- Cryptography : No cryptography features.

Mifare UltraLight C

- Memory organisation : 48 sectors of 4 bytes. Some sectors are read only (3DES key sectors).
- Command set : In addition to commands defined by the standard, we find 3 commands : Read, Write and Authenticate.
- Access control : Lock bytes, OTP bytes and 3DES authentication.
- Cryptography : 2 key 3DES encryption/decryption in CBC mode.

Mifare Desfire

- Memory organisation :
  - The Mifare Desfire card hold one root application (or directory).
  - The root directory can hold up to 28 applications.
  - Each application can hold up to 16 files of different size and type.
- Command set : In addition to commands defined by the standard, we find many other commands : Read, Write, Authenticate, CreateApplication, ChangeFileSettings,..etc

Mifare Desfire

- Access Control :
  - 16-byte key to control access to the root application.
  - Each directory is linked to a set of up to fourteen 16-byte definable keys :
    - One key to control access to the directory itself.
    - The other keys are used to define different levels of access rights on the sixteen files the directory may contain.

Mifare Desfire

- Cryptography :
  - DES or 2 key 3DES encryption (128-AES for Mifare Desfire EV1).
  - The Mifare Desfire card always performs the cryptographic operation "encipherment" on any received and sent data :
    - It uses the encipher cryptographic operation in "CBC send mode" (XOR before DES) to encrypt data.
    - It uses the encipher cryptographic operation in "CBC receive mode"(XOR after DES) to decrypt data received from the reader.

Mifare Desfire : Cryptography

- The reader always needs to perform the cryptographic operation "decipherment" on any received and sent data :
  - It uses the decipher cryptographic operation in "CBC send mode" to encrypt data.
  - It uses the decipher cryptographic operation in "CBC receive mode" to decrypt data received from the Mifare Desfire card.
- This particularity implicates that the developer can not fully rely on libraries to do the cryptographic operations automatically.

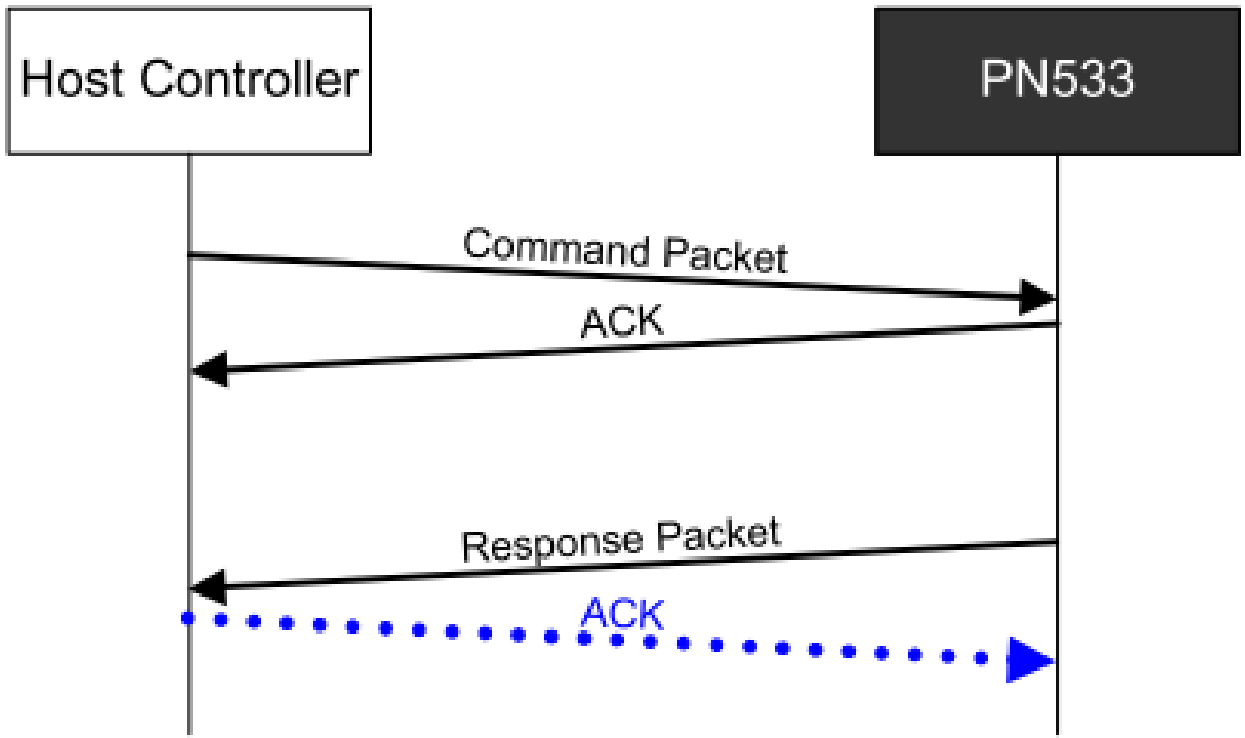
Mifare Desfire

- Security Features :
  - Data authenticity by 4 byte MAC.
  - Secure messaging by (3)DES encryption.

PN53x chips

- The PN53x chips have 2 interfaces : RF interface to communicate with the RFID devices and an USB interface to communicate with the host application.
- From the host application, the developer can send :
  - Commands to communicate with the chip itself: GetFirmwareVersion and RFConfiguration.
  - Commands to communicate with the RFID tag through the chip if the initiator mode is enabled : InDataExchange.
  - Commands to communicate with the reader through the chip if the target mode is enabled : TgGetData.

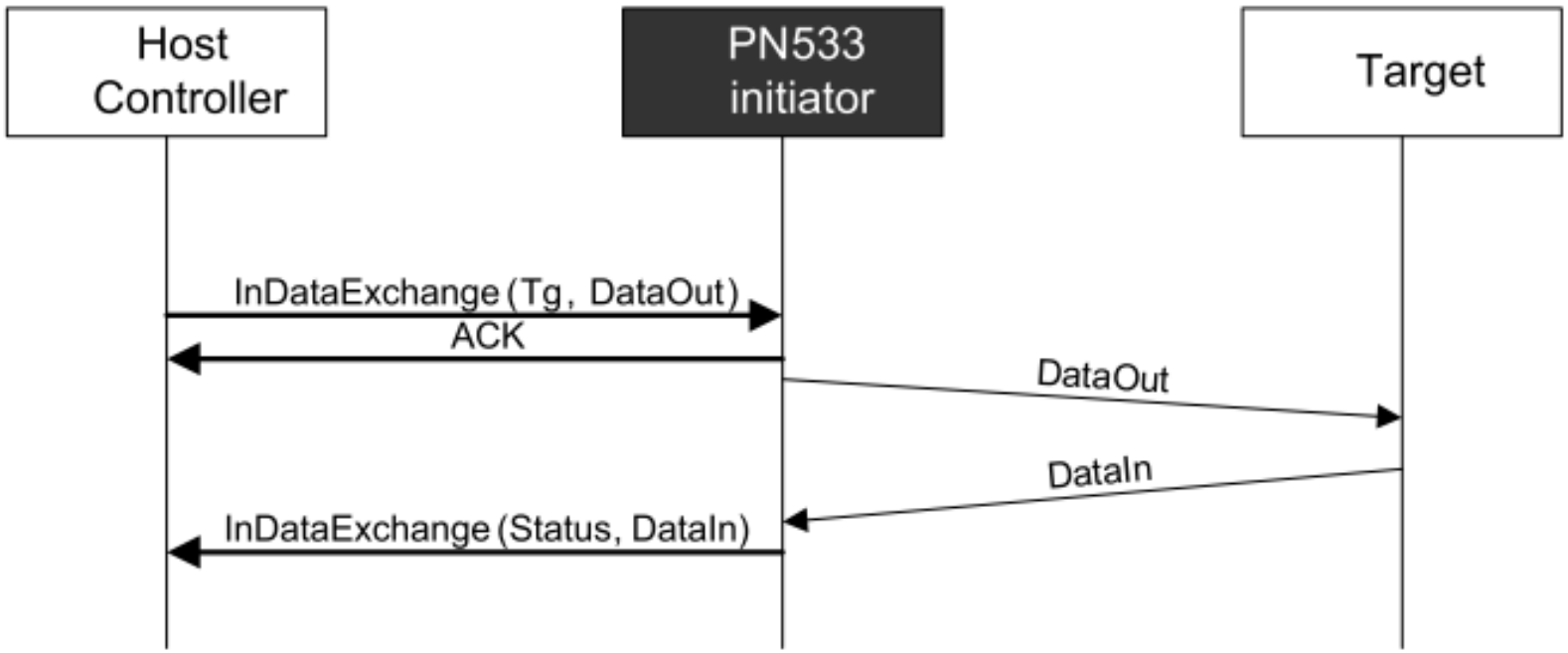
PN53x chips :
2 main communication models (1)



PN53x chips :
2 main communication models (1)

Example : GetFirmwareVersion
PC -> Chip : 00 00 ff 02 fe d4 02 2a 00 (Command)
Chip -> PC : 00 00 ff 00 ff 00 (ACK)
Chip -> PC : 00 00 ff 06 fa d5 03 33 02 07 07 e5 00 (Response)

PN53x chips :
2 main communication models (2)

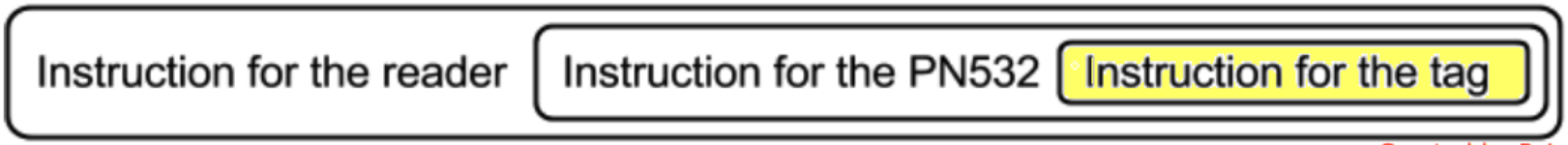


PN53x chips :
2 main communication models (2)

Example : InDataExchange
PC -> Chip : 00 00 ff 0c f4 d4 40 01 90 5a 00 00 03 00 00 00 00 fe 00(Command)
Chip -> PC : 00 00 ff 00 ff 00 (ACK)
Chip -> PC : 00 00 ff 05 fb d5 41 00 91 00 59 00 (Response)

Introduction

These tools aim to give a certain coverage of low-level chipset commands. Thus, the developer has to know the instructions to send to the RFID tags without regard to the pn53x chip commands or/and the reader commands.



pcsc-tools

- These tools allow the user to send and receive commands to and from the card.
- These tools don't provide a complete coverage of low-level commands since the user has to know :
  - The appropriate instruction to send to the reader,
  - The appropriate instruction to send to the pn53x chip,
  - And the appropriate instruction to send to the tag.
- Examples : pcsc-scan, scriptor , gscriptor.

pcsc-tools :

Example of use of «scriptor» with ACR122 reader and Mifare Classic card

- ACR122 is a PC-linked Contactless Cards reader.
- It embeds PN532 chip and provides a PCSC driver.
- It defines 2 main commands :

Command	Class	INS	P1	P2	Lc	Data In
Direct Transmit	0xFF	0x00	0x00	0x00	Number of Bytes to send	PN532_Contactless Command

Command	Class	INS	P1	P2	Le
Get Response	0xFF	0xC0	0x00	0x00	Number of Bytes to retrieve

pcsc-tools :

Example of use of «scriptor» with ACR122 reader and Mifare Classic card

How to poll the Mifare Classic card using ACR122 reader and «scriptor» tool :

```
Using T=0 protocol
Reading commands from STDIN
ff 00 00 00 04 d4 4a 01 00
> ff 00 00 00 04 d4 4a 01 00
< 61 0E : 0x0E bytes of response still available.
ff c0 00 00 0E
> ff c0 00 00 0E
< D5 4B 01 01 00 04 08 04 63 9B E4 E1 90 00 : Normal processing.
```

Libnfc

- Libnfc is a library written in C for NFC devices manipulation.
- It provides a complete coverage of low-level PN53x chip commands.
- It allows a high-level programming of applications designed for NFC devices.

Libnfc :

Example of use of Libnfc library with SCL3711 reader and Mifare Desfire

- SCL3711 is a PC-linked Contactless Cards reader. It embeds PN533 chip and provides a PCSC interface. It provides several commands.
- Example : How to poll the Mifare Desfire card using SCL3711 and Libnfc library :

```
debug   libnfc.chip.pn53x       InListPassiveTarget
debug   libnfc.chip.pn53x       No timeout
debug   libnfc.driver.pn53x_usb TX: 00 00 ff 04 fc d4 4a 01 00 e1 00
debug   libnfc.driver.pn53x_usb RX: 00 00 ff 00 ff 00
debug   libnfc.chip.pn53x       PN53x ACKed
debug   libnfc.driver.pn53x_usb RX: 00 00 ff 15 eb d5 4b 01 01 03 44 20 07 04 2f 39 c1 b6 1b 80 06 75 77 81 02 80 fd 00
The following (NFC) ISO14443A tag was found:
    ATQA (SENS_RES): 03  44
       UID (NFCID1): 04  2f  39  c1  b6  1b  80
      SAK (SEL_RES): 20
         ATS (ATR): 75  77  81  02  80
```

Libfreefare

- Libfreefare is a library written in C. It is based on Libnfc library and it aims to provide a convenient API for Mifare card manipulation.

Sniffing

- Defintion : Since the communication channel is public, an adversary can sniff the content of the communication between the PCD and the PICC.
- countermeasures : Encipherment.

Cloning

- Defintion : An adversary can copy the identifier and the data of a tag into another one.
- countermeasures : Authentication

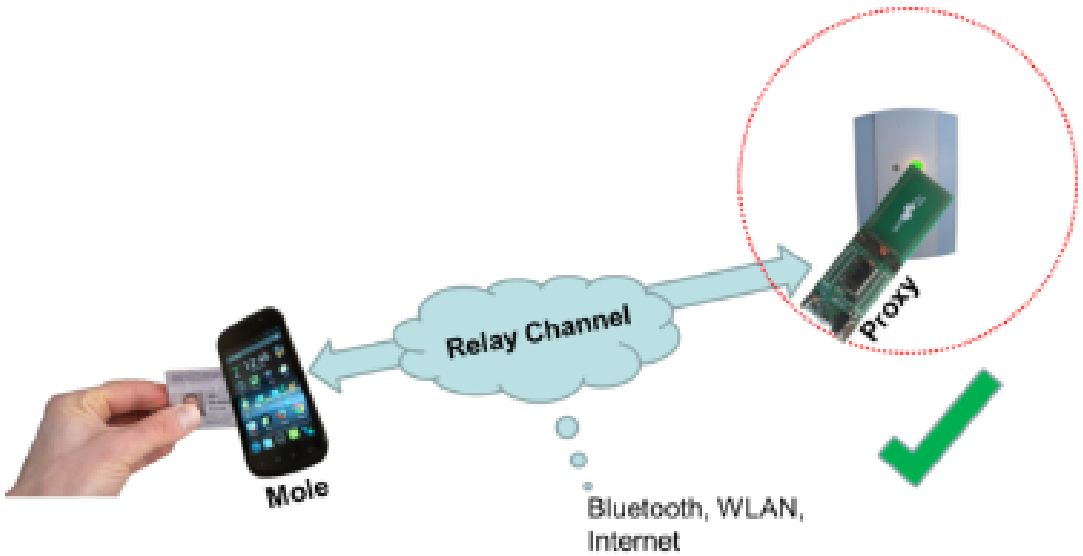
Denial Of Service

- Defintion : An adversary can use RFID jammers to disturb the electromagnetic waves by introducing an important electromagnetic noise. It can also tamper the data exchanged between the PICC and the PCD to defeat for example an authentication.
- countermeasures :

Relay attacks

- Definition :
  - Contactless card answers without the knowledge of its owner to any request it may receive from a reader.
  - An attacker can then relay information through a communication link between the card and a remote reader.
  - The reader will assume that the card and by implication the user, is in close vicinity and provide access to the complice of the attacker.
- countermeasures : Distance-bounding protocol if the legitimate tag is outside the neighborhood of the reader.

Relay attacks



Principle and objectives

- Distance-bounding protocol is a challenge-response protocol where the reader plays the role of a verifier and the card plays the role of the prover. This protocol aims :
  1. To convince the verifier that the prover knows the secret key.
  2. To convince the prover that the verifier knows the pre-shared secret key (optional).
  3. To convince the verifier that the prover he is communicating with is really in its neighborhood.

Principle and objectives

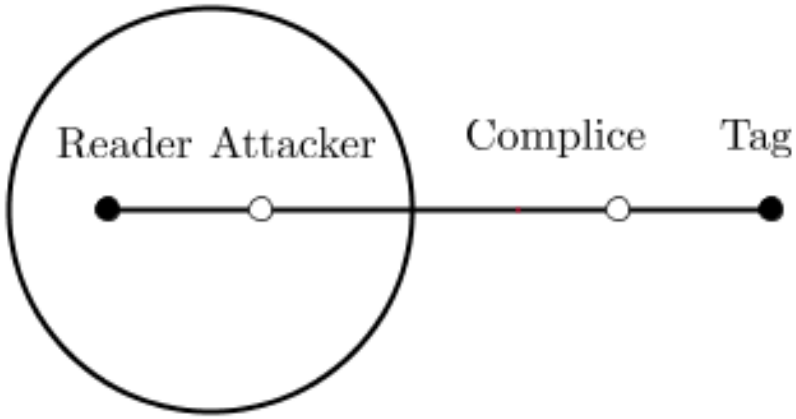
- To achieve goals 1 and 2, distance-bounding protocols use mutual authentication schemes.
- To achieve goal 3, distance-bounding protocols uses the RTT distance-estimation approach to check the distance between the verifier and the prover:
  - The verifier calculates the maximum distance $d_{max} = c.\frac{(t_m - t_d)}{2}$, where t_m is the round-trip-time and t_d is the processing time.
  - If $d_{max} > d_{standard}$, the verifier rejects the prover.
  - Since $t_m = 2.t_p + t_d$ and we know that $d = c.t_p$, the estimation is realistic if t_d is negligible.

Principle and objectives

- Distance-bounding protocols consist of 3 distinct phases :
  - Setup phase : The prover and the verifier exchange initial information used during the rest of the protocol.
  - Exchange phase :It consists of n rounds. In each round, the verifier sends challenges to the prover and measures the time from the moment he has sent a challenge to the moment the corresponding response is received.
  - Verification phase : The verifier checks the validitiy of the responses and the proximity of the prover.

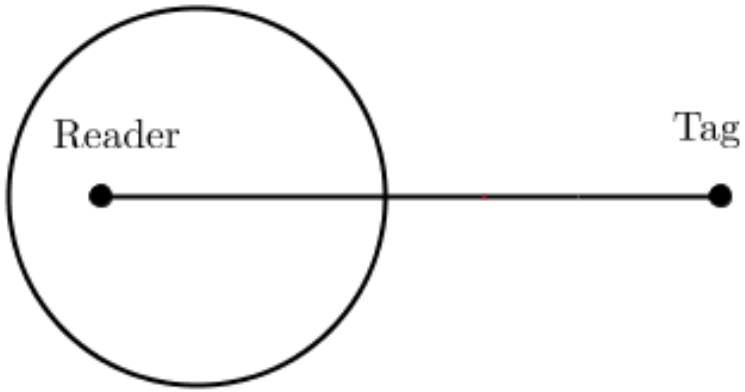
Attacks

- **Mafia fraud attack** is an attack where an attacker defeats a distance-bounding protocol using a MITM between the verifier and an honest prover located outside the neighborhood of the verifier.



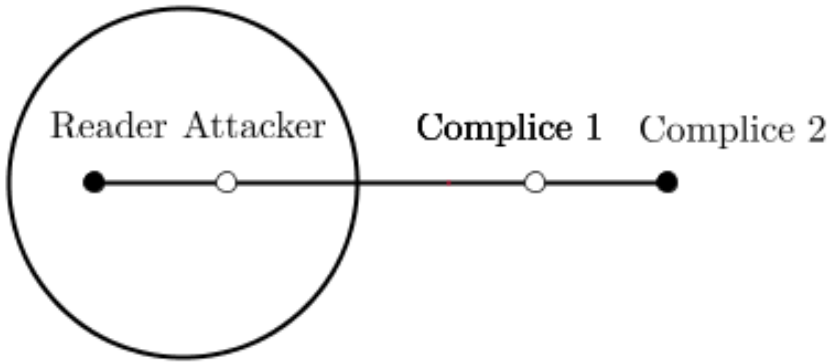
Attacks

- **Distance fraud attack** is an attack where a dishonest prover defeats a distance-bounding protocol without help of other entities located in the neighborhood of the verifier.



Attacks

- **Terrorist fraud attack** is an attack where an attacker defeats a distance-bounding protocol using a MITM between the verifier and a dishonest prover located outside the neighborhood of the verifier, such that the dishonest prover colludes with the attacker to deceive the verifier without revealing his secret key to the attacker.



Attacks

- The non-resistance of a distance-bounding protocol against mafia, distance and terrorist fraud attacks is the probability p of success of such attacks against that protocol :
  - $p(\textit{success}) = p(\textit{success at round } i)^n . p(\textit{signature is correct})$, where $p(\textit{success at round } i)$ is the probability that the response sent to the verifier is correct.

State of the art

Algorithm 1: Brands and Chaum's Protocol

Verifier (prover's public key K_v)		**Prover** (prover's private key K_s)
	$\xleftarrow{\text{Commit}(m_1 \,\|\| \ldots \,\|\| m_n)}$	$m_i \in_R \{0,1\}$
Pick $c_i \in_R \{0,1\}$ and Start Timer	$\xrightarrow{c_i}$	
Stop Timer	$\xleftarrow{r_i}$	$r_i = m_i \oplus c_i$
	$\xleftarrow{open,\ s}$	$open = \text{Open}(\text{Commit})$ $s = \text{Sign}_{K_s}(c_1 \| r_1 \| \ldots)$
Check r_i and $\Delta t_i \leq t_{\max}$ for $1 \leq i \leq n$, then Verify s		

Brands and Chaum's Distance-bounding protocol : Attacks

- Mafia fraud : The probability of success of mafia fraud attack on BC distance-bounding protocol is $\left(\frac{1}{2}\right)^n$.
- Distance fraud : The probability of success of distance fraud attack on BC distance-bounding protocol is $\left(\frac{1}{2}\right)^n$.
- Terrorist fraud : The probability of success of terrorist fraud attack on BC distance-bounding protocol is 1.

Algorithm 2: Hancke and Kuhn's Protocol

Verifier (secret K)		**Prover** (secret K)
Pick $N_V \in_R \{0,1\}^\delta$		Pick $N_P \in_R \{0,1\}^\delta$
	$\xrightarrow{N_V}$	
	$\xleftarrow{N_P}$	
$H = h(K, N_V, N_P)$		$H = h(K, N_V, N_P)$
$R^0 = H_1 \|\| H_2 \|\| \ldots \|\| H_n$		$R^0 = H_1 \|\| H_2 \|\| \ldots \|\| H_n$
$R^1 = H_{n+1} \|\| H_{n+2} \|\| \ldots \|\| H_{2n}$		$R^1 = H_{n+1} \|\| H_{n+2} \|\| \ldots \|\| H_{2n}$
Pick $c_i \in \{0,1\}$ and Start Timer	$\xrightarrow{c_i}$	
Stop Timer	$\xleftarrow{r_i}$	$r_i = R_i^{c_i}$
Check correctness of r_i and $\Delta t_i \leq t_{\max}$ for $1 \leq i \leq n$		

Hancke and Kuhn's Distance Bounding Protocol : Attacks

- Mafia fraud : The probability of success of mafia fraud attack on HK distance-bounding protocol is $\left(\frac{3}{4}\right)^n$.
- Distance fraud : The probability of success of distance fraud attack on HK distance-bounding protocol is $\left(\frac{3}{4}\right)^n$.
- Terrorist fraud : The probability of success of terrorist fraud attack on HK distance-bounding protocol is 1.

Algorithm 3: Swiss-knife Protocol

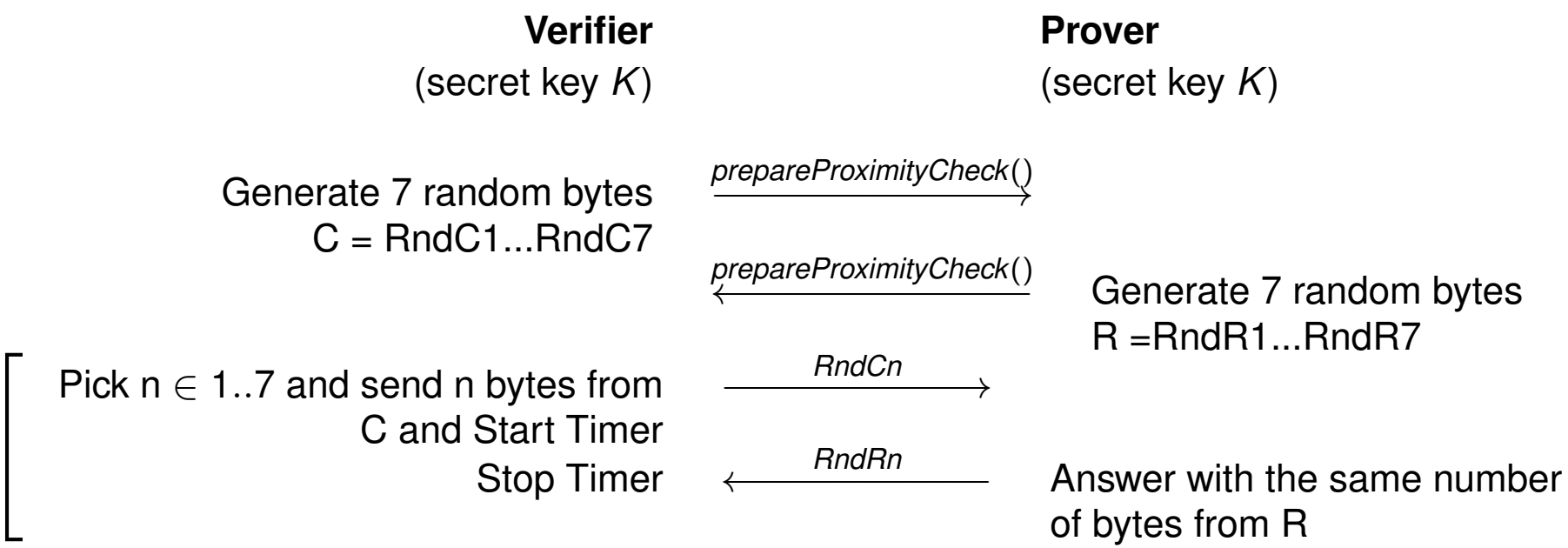
Verifier (secret K, constant C)		**Prover** (secret K, ID, constant C)
Pick $N_V \in_R \{0,1\}^\delta$ Pick a random D s.t. $\mathcal{H}(D) = n$		Pick $N_P \in_R \{0,1\}^\delta$ $a = f_K(C, N_P)$ $Z^0 = a, Z^1 = a \oplus K$
	$\xrightarrow{N_V, D}$	
		For $i = 1$ to n: $j =$ index of the next "1" in the binary representation of D. $R_i^0 = Z_j^0, R_i^1 = Z_j^1$
	$\xleftarrow{N_P}$	

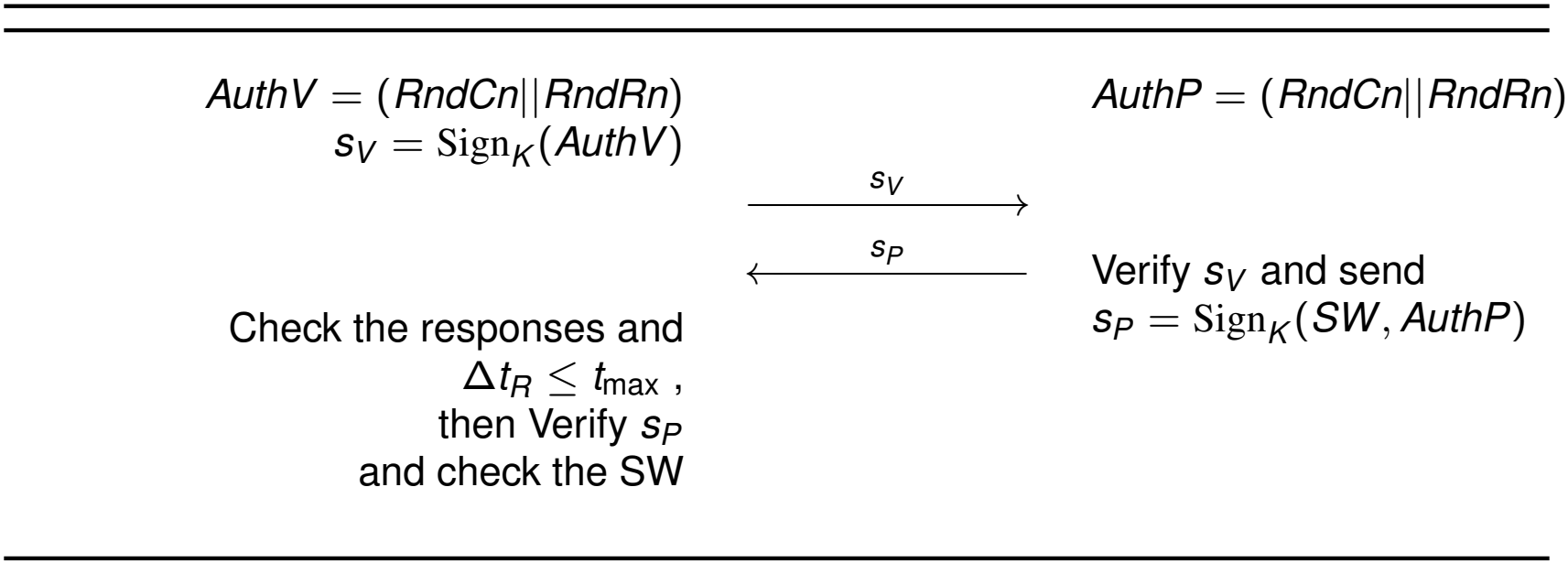
Pick $c_i \in_R \{0,1\}$ and Start Timer	$\xrightarrow{c'_i}$	
Stop Timer	$\xleftarrow{r_i}$	$r_i = R_i^{c'_i}$
	$\xleftarrow{T_B, c'_1, \ldots, c'_n}$	$T_B = f_K(c'_1, \ldots, c'_n, ID, N_V, N_P)$
Check ID via DB Compute R^0, R^1 Compute $err_C := \sharp\{i : c_i \neq c'_i\}$, $err_R := \sharp\{i : c_i = c'_i \wedge r_i \neq R_i{}^{c_i}\}$, $err_T := \sharp\{i : c_i = c'_i \wedge \Delta t_i > t_{\max}\}$. If $err_C + err_R + err_T \geq T$, then REJECT		
$T_A = f_K(N_P)$	$\xrightarrow{T_A}$	Compute and check T_A

Swiss-knife Distance Bounding Protoclol : Attacks

- Mafia Fraud : The probability of success of mafia fraud attack on SK distance-bounding protocol is $\left(\frac{1}{2}\right)^n$.
- Distance Fraud : The probability of success of distance fraud attack on SK distance-bounding protocol is $\left(\frac{1}{2}\right)^n$.
- Terrorist Fraud : The probability of success of terrorist fraud attack on SK distance-bounding protocol is $(1)^v . \left(\frac{3}{4}\right)^{n-v}$ if the attacker knows v bits of the key among the n bits used in the exchange phase. If the attacker knows 0 bits of the key, the probability is then equal to $\left(\frac{3}{4}\right)^n$.

Algorithm 4: Proximity Check Protocol




$AuthV = (RndCn||RndRn)$
$s_V = \mathrm{Sign}_K(AuthV)$
s_V
s_P
$AuthP = (RndCn||RndRn)$
Verify s_V and send
$s_P = \mathrm{Sign}_K(SW, AuthP)$
Check the responses and
$\Delta t_R \leq t_{\max}$,
then Verify s_P
and check the SW

Proximity check protocol : Attacks

Mafia fraud , distance fraud , and terrorist fraud attacks against the proximity check protocol depend on :

- How the RTT is measured .
- The strategy of the attacker.
- How the T_{max} is defined.

Conclusion : Next steps

- Understand the different timing parameters we find in the standards specification, the data sheets of the Mifare cards, and the manuals of contactless cards readers.
- Understand how readers control timing aspects on regular commands.
- Perform a relay attack on an ISO-14443 RFID tag.
- Perform time measurements to know the limits of relay attacks.

Some References

- Security of Distance-Bounding: A Survey. Avoine et al.
- Distance-Bounding Protocols. Brands and Chaum.
- An RFID Distance Bounding Protocol. Hancke and Kuhn.
- The Swiss-Knife RFID Distance Bounding Protocol. Kim et al.
- ISO 14443 specification.
- Cristina Onete presentations.
- Gildas Avoine presentations.
- Stephane Capmarti thesis.