RFID Security and the Mifare Classic

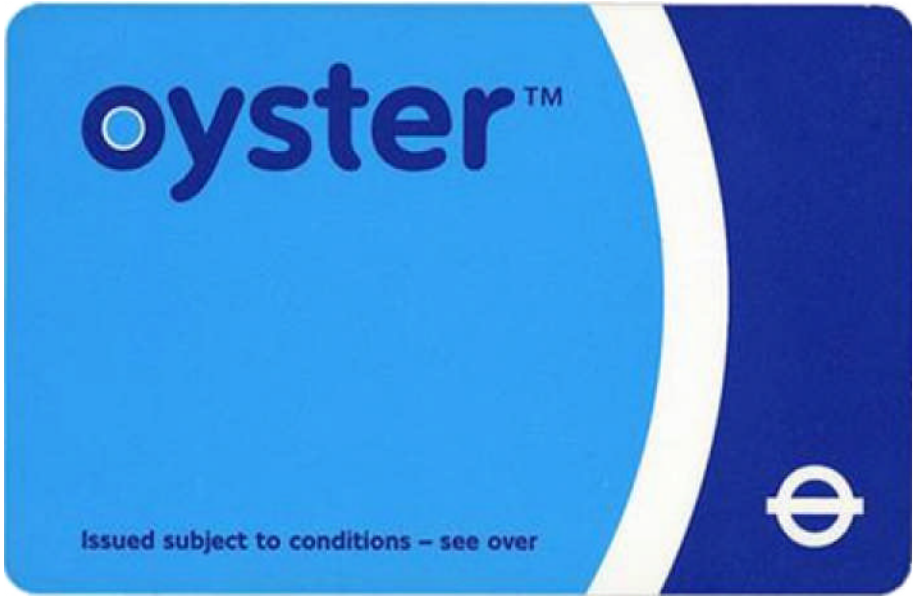
Peter van Rossum

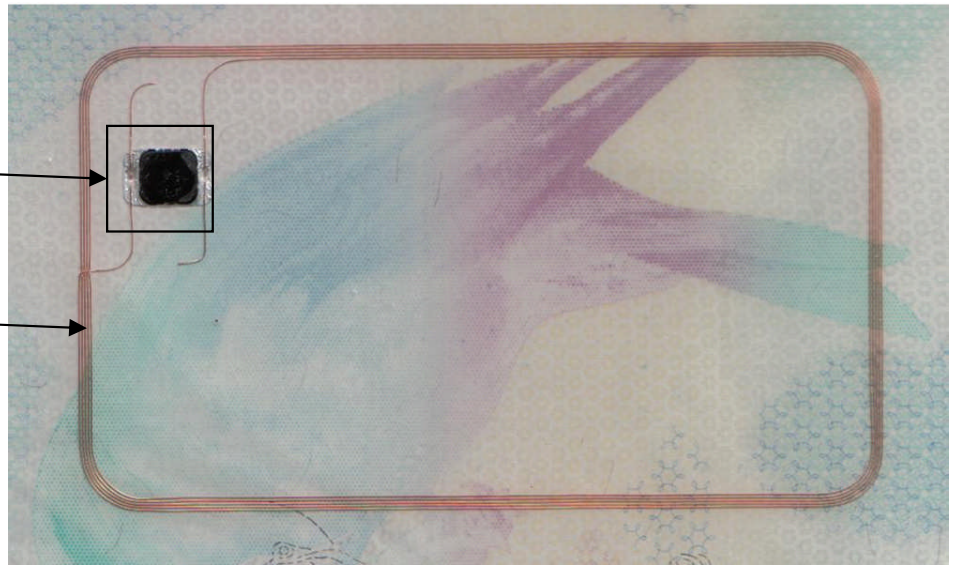
Radboud University Nijmegen

RFID

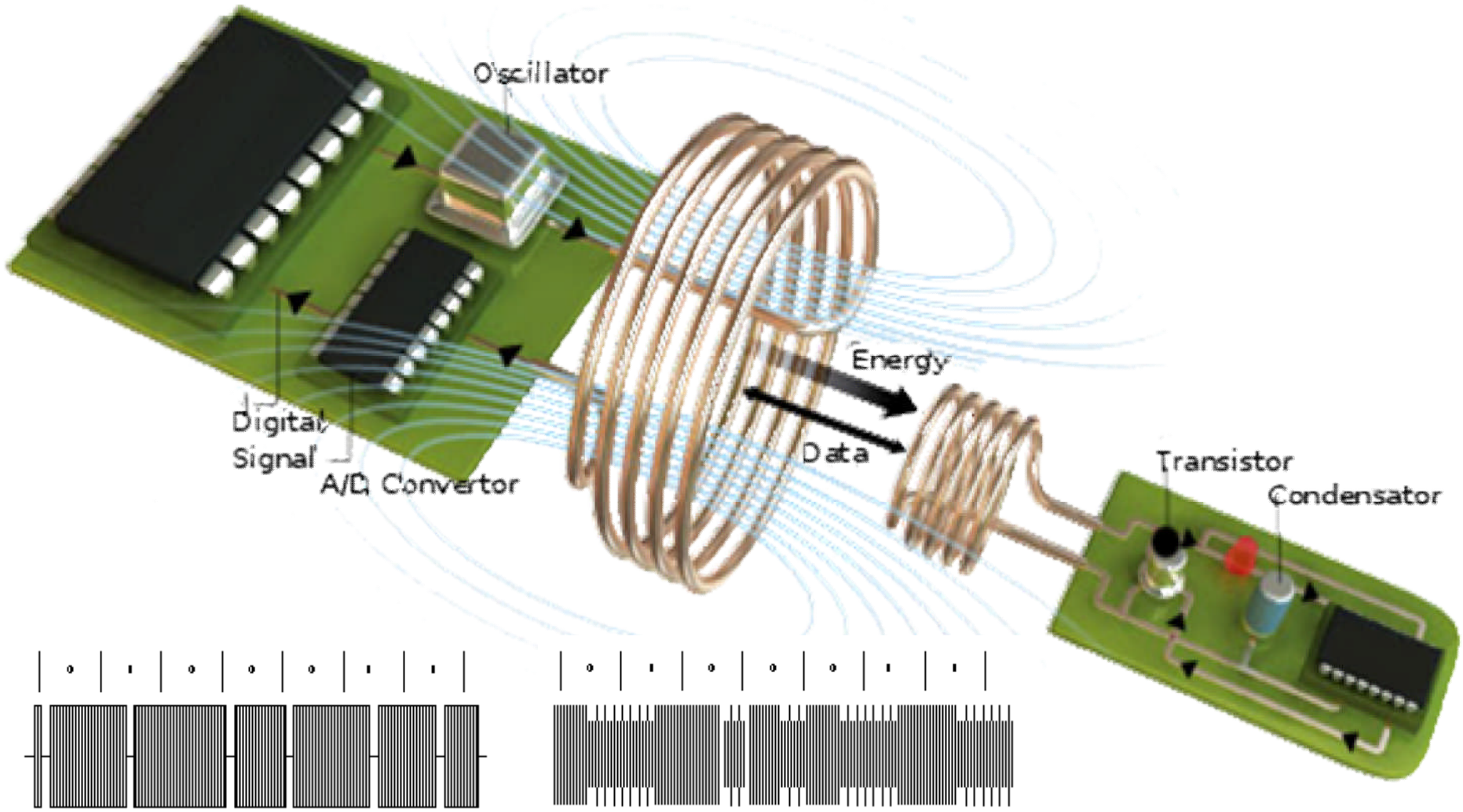
RFID


ov-chipkaart
klantenservice 0900-0980
www.ov-chipkaart.nl
GVB


oyster™
Issued subject to conditions – see over


RFID Chip
Antenna

RFID Technology

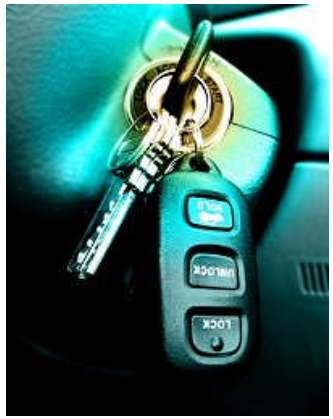


Reader to tag signal
- Dropping field
- Modified Miller Encoding

Tag to reader signal
- Modulating field
- Manchester Encoding

RFID Applications

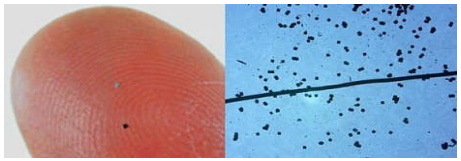
Identify friend or foe (1942)



Car keys

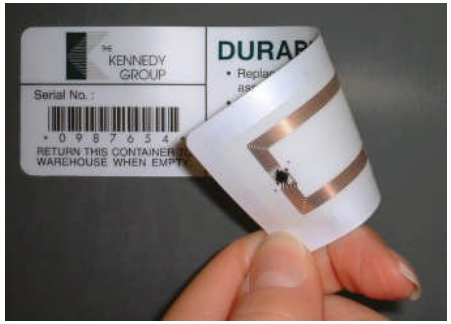
Public transport ticketing

Electronic passport



RFID Powder

Access control



Supply chain management

Anti-theft

Event ticketing

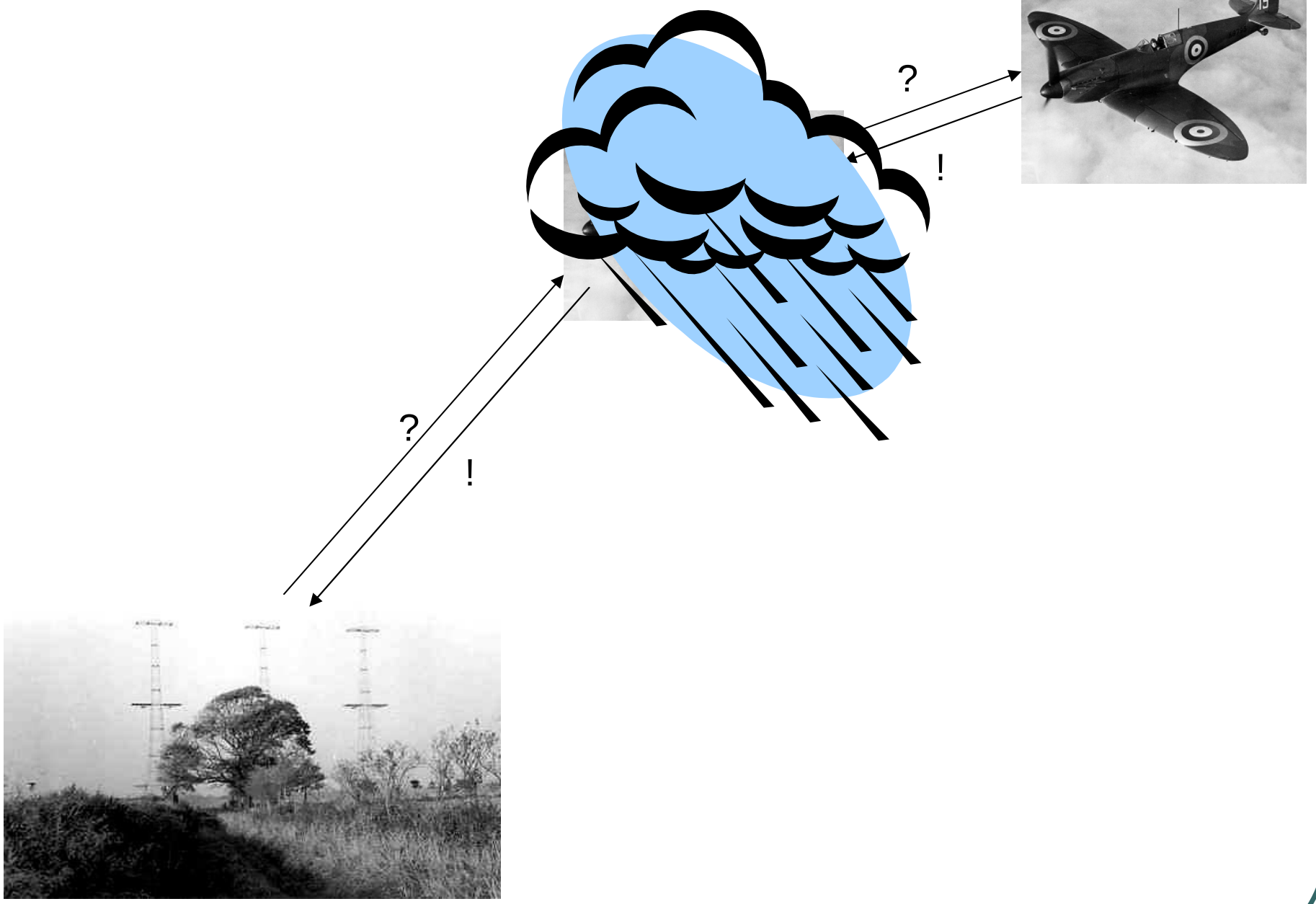
RFID Security

- RFID = Radio Frequency Identification
- More properly authentication
- Contactless smartcards
  - data storage, computational capabilities
  - confidentiality
  - integrity

RFID Security

- Relay attack
- Replay attack
- Cryptanalytic attack
- Tracing attack
- …

RFID Security – Relay Attack



RFID Security – Relay Attack

- Wireless communication
- No link between authenticating object (tag) and service receiver (tag holder)
  - Attacker A initiates service
  - Attacker A **relays** queries to tag to attacker B
  - Attacker B sends queries to victim's tag
  - Attacker B **relays** answers back to attacker A
  - Attacker A answers queries
- Countermeasures
  - Second authentication channel
  - Distance bounding protocols

RFID Security – Replay Attack

- Parking at Radboud University / UMC
  - Access control: wireless employee card
  - No authentication protocol at all
    - Card sends uid; back-end checks authorization

- Attack
  - Eavesdrop signal from car (card) to barrier
  - Replay signal to gain entry
  - (only works when original car has left; more effective to eavesdrop signal from a departing car)

RFID Security – Replay Attack

- No clock
- Weak randomness
  - Attacker **intercepts** communication between tag and reader
  - Attack **replays** communication at a later time
- Countermeasures (standard)
  - Challenge-response authentication (needs clock, randomness, or some other form of “freshness”)

RFID Security – Crypto Attacks

- Low energy
- Low computational capacity
- Cheap to manufacture
- Fast enough to operate
  - Weak cryptography
  - Attacker can break encryption scheme

RFID Security – Tracing Attack

- Used for identification
- Anti-collision phase
  - Attacker can recognize people based on the RFID tags they are carrying

RFID Security

- No clock, weak randomness
  → replay attacks
- Low computational capacity
  → cryptanalytic attacks
- Wireless
  → relay attacks
- Used for identification
  → tracking attacks (privacy)

Mifare Classic

Mifare Classic

- Many standards for RFID
  - ISO14443A: Mifare (NXP)
  - ISO14443B: CryptoRF (Motorola/Atmel)
  - ISO14443C: Felica (Sony)
  - ISO14443D: (OTI)
  - ISO14443E: (Cubic)
  - ISO14443F: Legic (KABA)
  - ISO15693: Tag-IT (Texas Instruments)

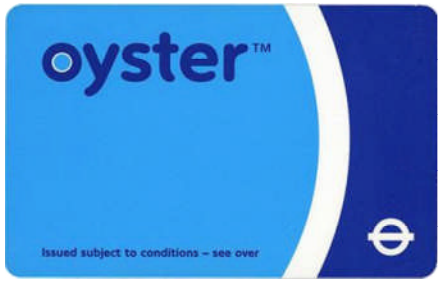
  - Typically describe physical and data-link layers (typically not cryptographic features)

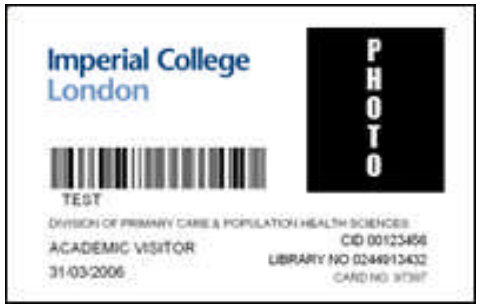
Mifare Classic

- Many chips in the Mifare (ISO14443A) family
  - Mifare Ultralight
  - Mifare Classic
  - Mifare DESFire
  - Mifare Plus
  - Mifare EV1
  - Mifare SMART MX
- Most popular: Mifare Classic
  - over 1 billion sold
  - over 200 million in use
  - 80% of contactless smartcard market

Mifare Classic Applications

- Public transport ticketing systems
- Access control
- Wireless payment systems





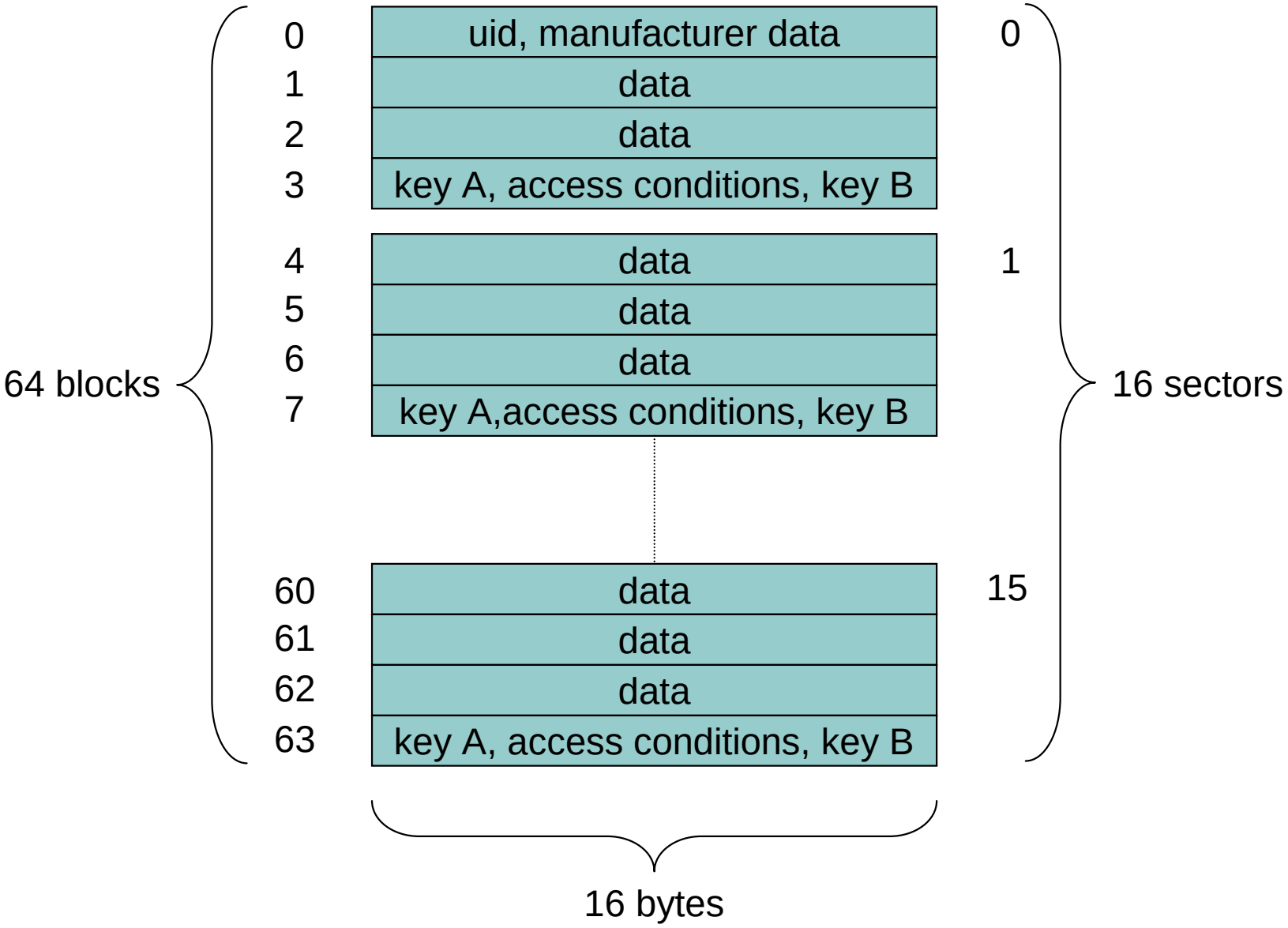
Timeline

Jun 06	RU	Start of development of Ghost for ISO 14443-A (Mifare) emulation
Nov 07	RU	Functional ISO14443-A (Mifare) emulation
Dec 07	CCC, VA	Presentation: reverse engineered encryption of Mifare Classic: CRYPTO1
Feb 08	RU	Media report: cloning Mifare Ultralight (single-use OV-chipkaart)
Feb 08	TNO	Report on OV-chipkaart: fraud unlikely, advanced equipment needed, 2 year respite
Mar 08	RU	Reverse engineered CRYPTO1 & authentication protocol
Mar 08	RU	Key recovery using intercepted traffic or communication with reader
Apr 08	RHUL	Report on OV-chipkaart: fraud likely, replace cards, design open&modular
Jun 08	NXP	Lawsuit against RU to stop publication
Jul 08	Court	Publication allowed: potential damage due to flaws in chip, not publication
Oct 08	RU	Publication at ESORICS
Nov 08	RU	Card-only key recovery of Mifare Classic
Dec 08	RU	Attack possible using commercially available (cheap) hardware

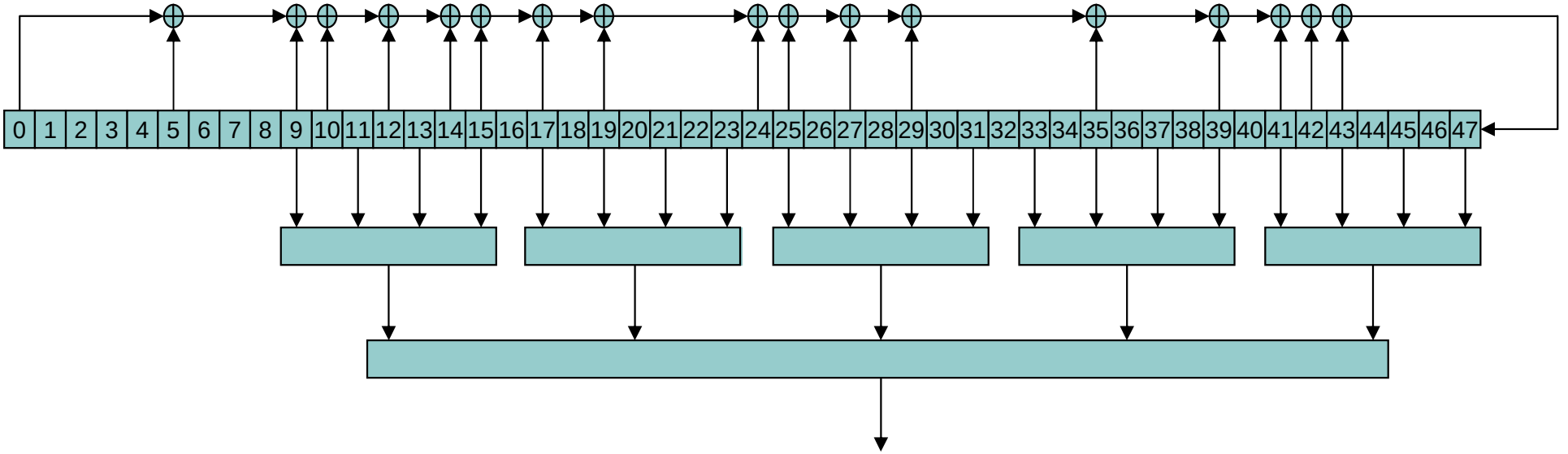
Timeline

2004	Fudan	Sale of fully functional Mifare Classic clones
2006	Angstrom	(Rumour) Mifare Classic reverse engineered and CRYPTO1 broken
Jun 06	RU	Start of development of Ghost for ISO 14443-A (Mifare) emulation
Nov 07	RU	Functional ISO14443-A (Mifare) emulation
Dec 07	CCC, VA	Presentation: reverse engineered encryption of Mifare Classic: CRYPTO1
Feb 08	RU	Media report: cloning Mifare Ultralight (single-use OV-chipkaart)
Feb 08	TNO	Report on OV-chipkaart: fraud unlikely, advanced equipment needed, 2 year respite
Mar 08	RU	Reverse engineered CRYPTO1 & authentication protocol
Mar 08	RU	Key recovery using intercepted traffic or communication with reader
Apr 08	RHUL	Report on OV-chipkaart: fraud likely, replace cards, design open&modular
Jun 08	NXP	Lawsuit against RU to stop publication
Jul 08	Court	Publication allowed: potential damage due to flaws in chip, not publication
Oct 08	RU	Publication at ESORICS
Nov 08	RU	Card-only key recovery of Mifare Classic
Dec 08	RU	Attack possible using commercially available (cheap) hardware

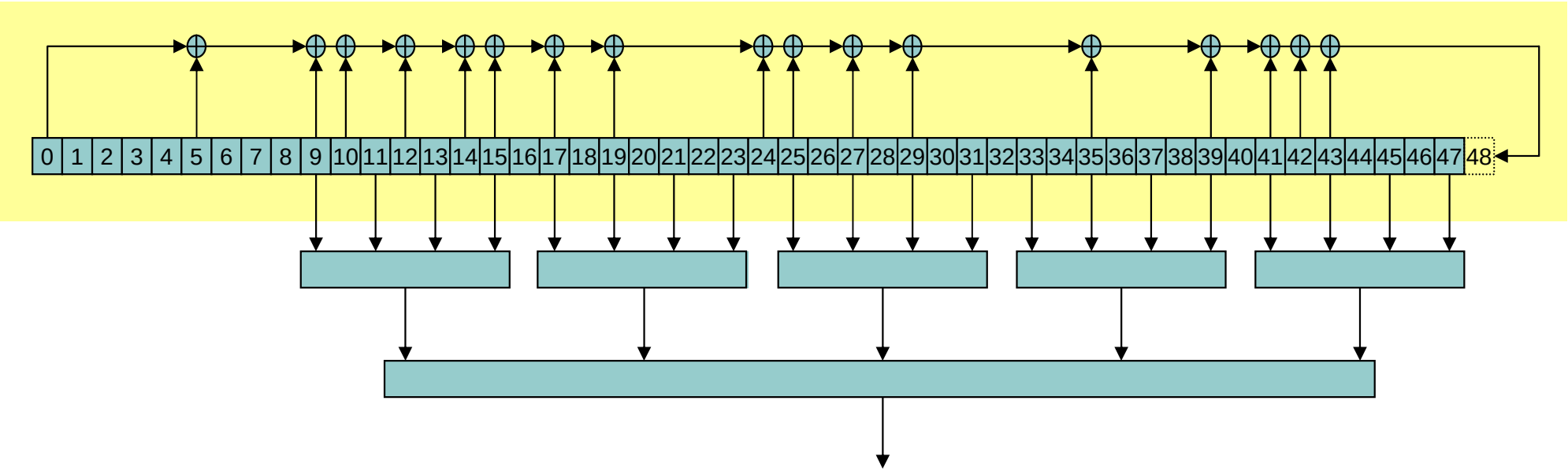
Mifare Classic: structure



CRYPTO1


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47

CRYPTO1: LFSR



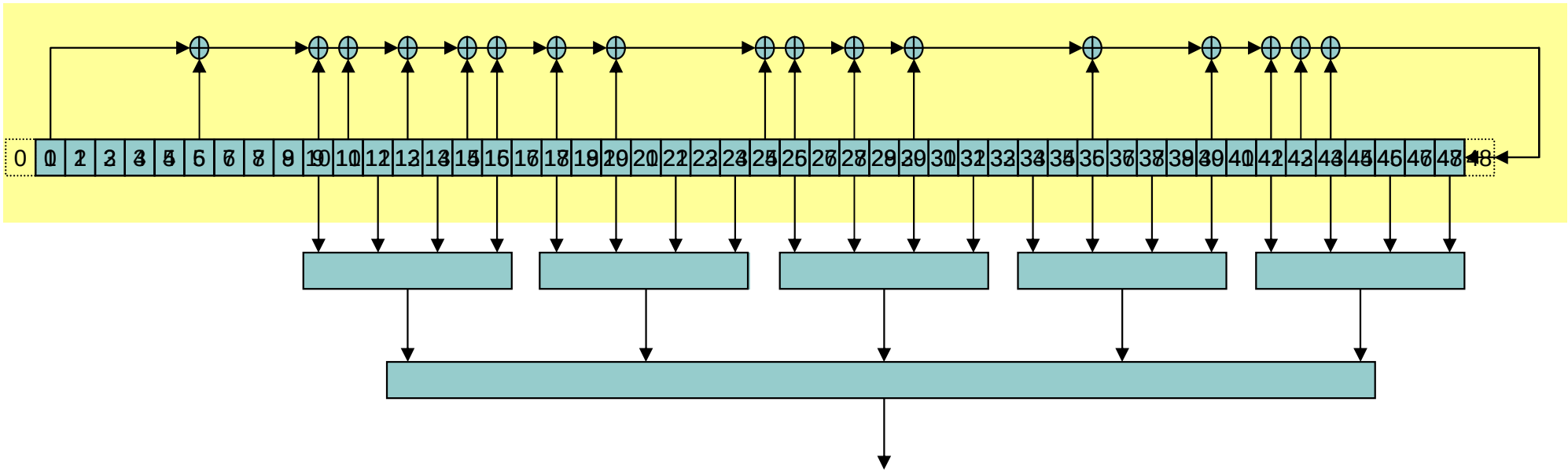
Feedback:

$$L(x_0,x_1,\ldots,x_{47}) := x_0+x_5+x_9+x_{10}+x_{12}+x_{14}+x_{15}+x_{17}+x_{19}+x_{24}+x_{25}+x_{27}+x_{29}+x_{35}+x_{39}+x_{41}+x_{43}$$

LFSR stream:

$$a_{i+48} := L(a_i,a_{i+1},\ldots,a_{i+47}) \quad \square i \square \mathbb{N}$$

CRYPTO1: LFSR



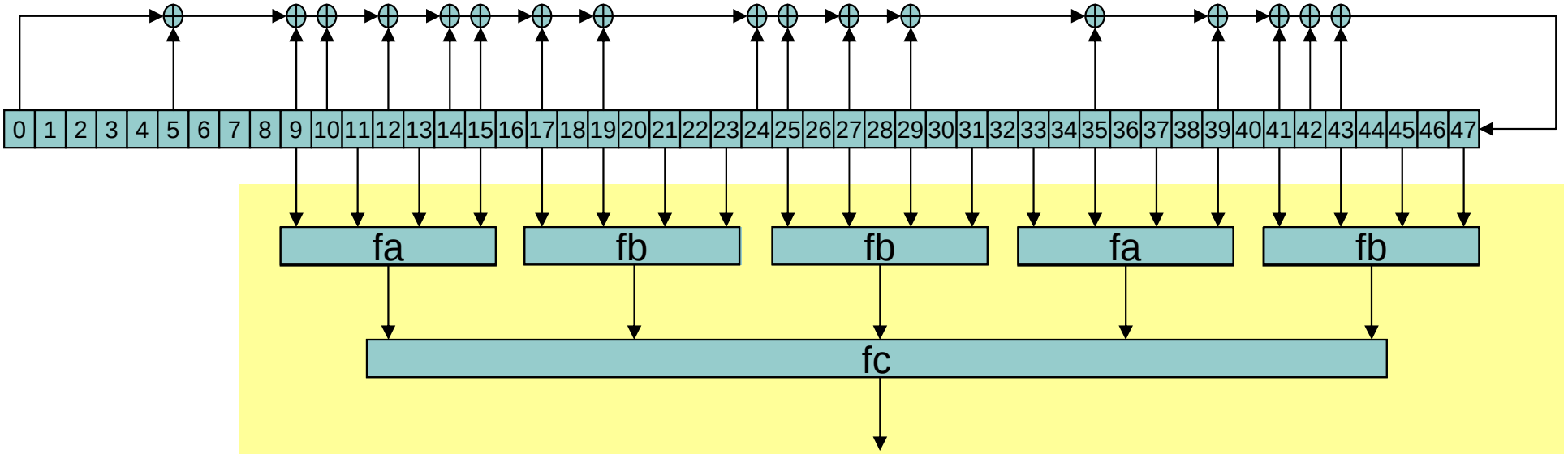
Feedback:

$$L(x_0,x_1,\ldots,x_{47}) := x_0+x_5+x_9+x_{10}+x_{12}+x_{14}+x_{15}+x_{17}+x_{19}+x_{24}+x_{25}+x_{27}+x_{29}+x_{35}+x_{39}+x_{41}+x_{43}$$

LFSR stream:

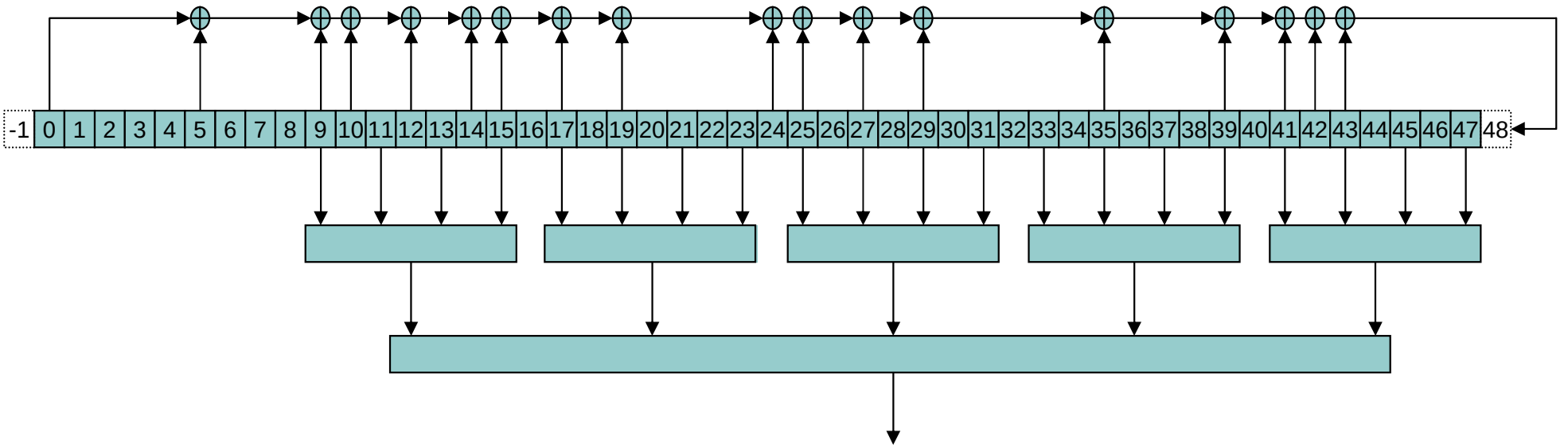
$$a_{i+48} := L(a_i,a_{i+1},\ldots,a_{i+47}) \quad \square i \square \mathbb{N}$$

CRYPTO1: filter function



fa				fb				fc							
0000	1	1000	0	0000	1	1000	1	00000	1	01000	1	10000	1	11000	0
0001	1	1001	1	0001	1	1001	0	00001	1	01001	1	10001	1	11001	0
0010	1	1010	1	0010	0	1010	1	00010	0	01010	0	10010	1	11010	1
0011	0	1011	0	0011	0	1011	1	00011	0	01011	0	10011	0	11011	0
0100	0	1100	0	0100	1	1100	0	00100	1	01100	0	10100	1	11100	0
0101	0	1101	1	0101	0	1101	0	00101	1	01101	0	10101	0	11101	0
0110	1	1110	0	0110	1	1110	0	00110	0	01110	1	10110	1	11110	1
0111	1	1111	0	0111	1	1111	0	00111	1	01111	1	10111	0	11111	0

CRYPTO1



Feedback:

$L(x_0,x_1,\ldots,x_{47}) := x_0+x_5+x_9+x_{10}+x_{12}+x_{14}+x_{15}+x_{17}+x_{19}+x_{24}+x_{25}+x_{27}+x_{29}+x_{35}+x_{39}+x_{41}+x_{43}$

LFSR stream:

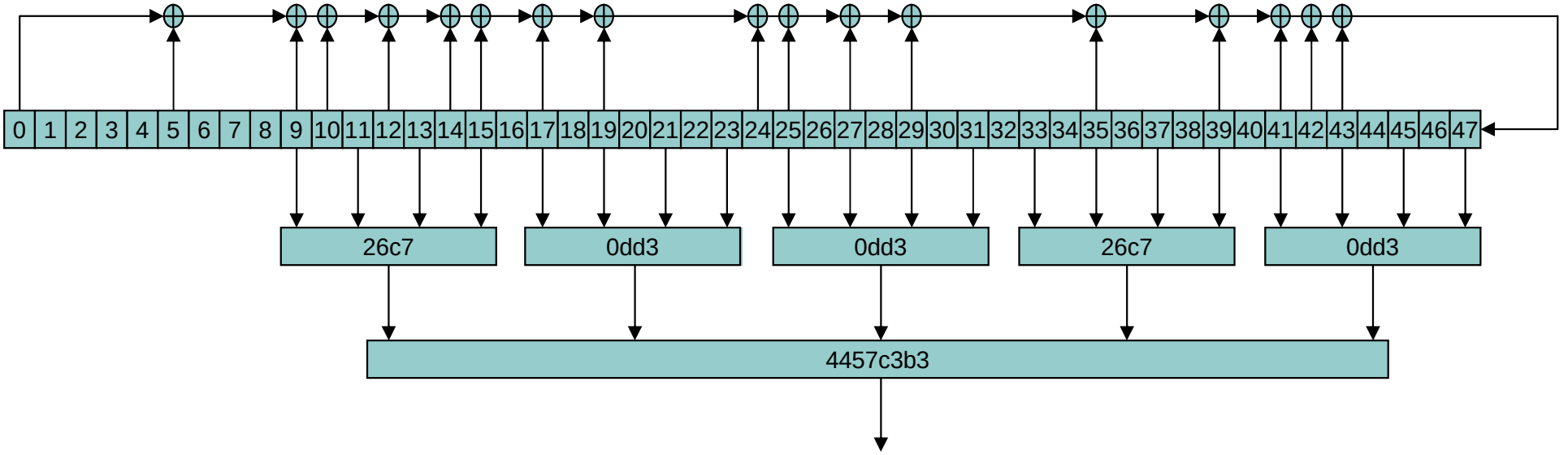
$a_{i+48} := L(a_i,a_{i+1},\ldots,a_{i+47})$ □i□ℕ

(actually a bit more complicated because of the initialization)

Keystream:

$b_i := f(a_{i+9},a_{i+11},\ldots,a_{i+47})$ □i□ℕ

CRYPTO1



Feedback:

$$L(x_0,x_1,\ldots,x_{47}) := x_0+x_5+x_9+x_{10}+x_{12}+x_{14}+x_{15}+x_{17}+x_{19}+x_{24}+x_{25}+x_{27}+x_{29}+x_{35}+x_{39}+x_{41}+x_{43}$$

LFSR stream:

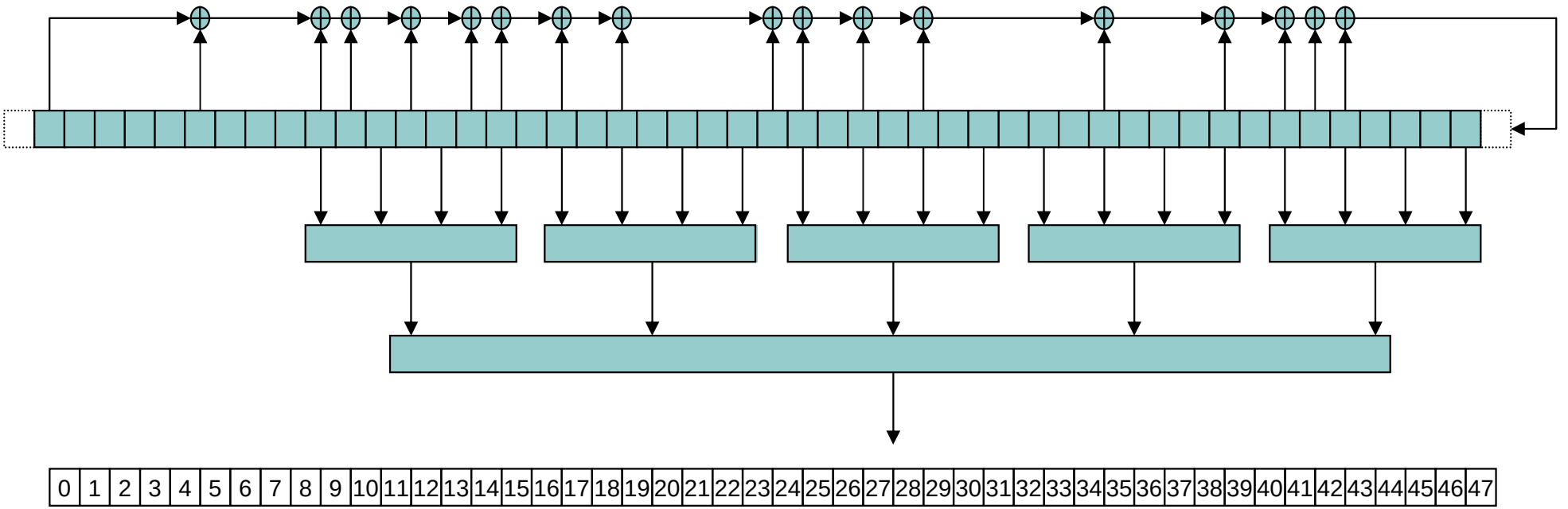
$$a_{i+48} := L(a_i,a_{i+1},\ldots,a_{i+47}) \quad \square i \square \mathbb{N}$$

(Actually a bit more complicated because of the initialization)

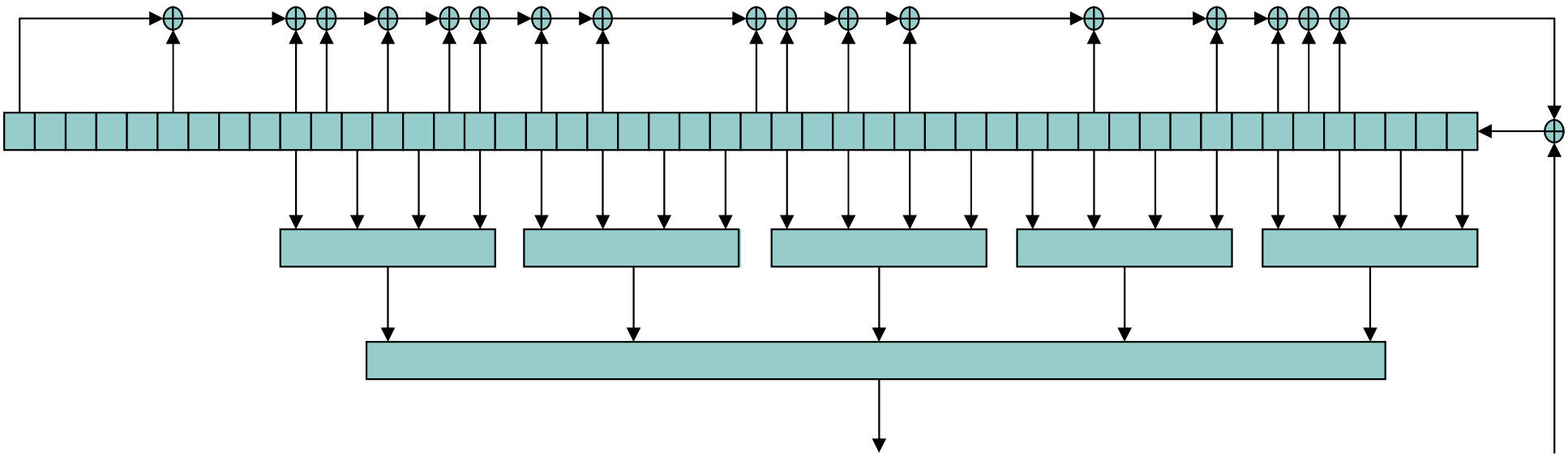
Keystream:

$$b_i := f(a_{i+9},a_{i+11},\ldots,a_{i+47}) \quad \square i \square \mathbb{N}$$

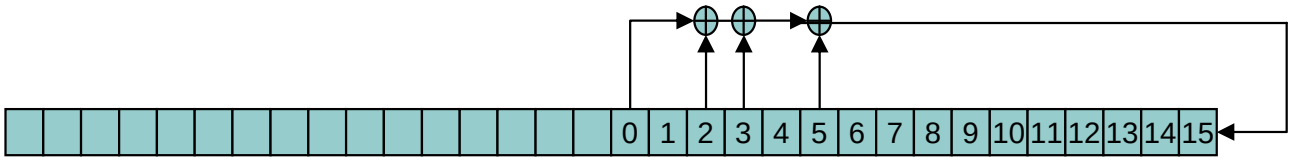
CRYPTO1


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47

CRYPTO1



CRYPTO1: random number generator



32 bit nonces

16 bit internal state

period $2^{16} - 1 = 65535$

Feedback:

$L_{16}(x_0,x_1,\ldots,x_{15}) := x_0+x_2+x_3+x_5$

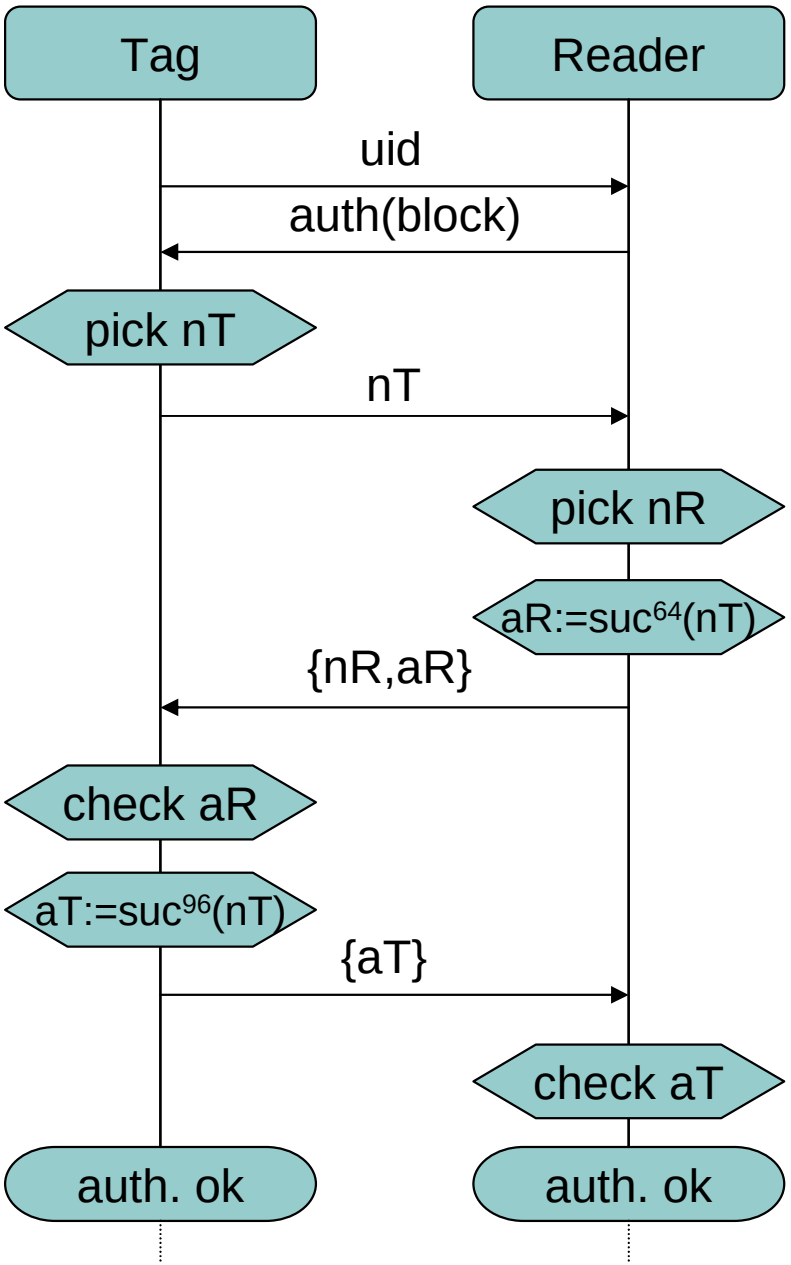
Successor:

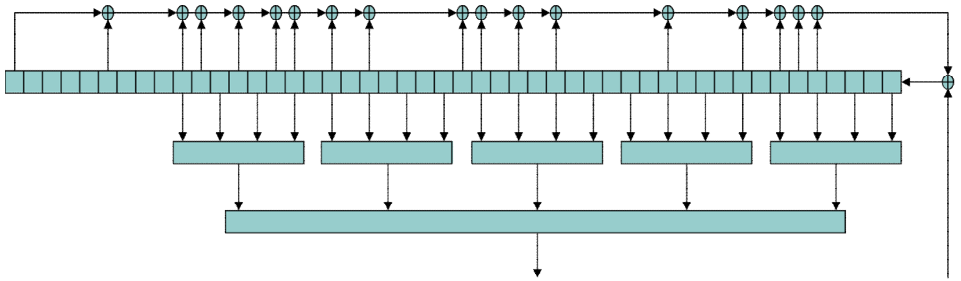
$suc(x_0,x_1,\ldots,x_{31}) := (x_1,x_2,\ldots,x_{30},L_{16}(x_{16},x_{17},\ldots,x_{31}))$

Distance:

$d((x_0,x_1,\ldots,x_{31})(y_0,y_1,\ldots,y_{31})) := \min \{ n \in \mathbb{N} \mid suc^n(x_0,x_1,\ldots,x_{31}) = (y_0,y_1,\ldots,y_{31})$

CRYPTO1: authentication & initialization





LFSR stream:

Initial state of the LFSR is the key

$a_i := k_i$ $\quad i \in [0,47]$

Shift nT + uid into the LFSR

$a_{i+48} := L(a_i,\ldots,a_{i+47}) + nT_i + uid_i \quad i \in [0,31]$

Shift nR into the LFSR

$a_{i+48} := L(a_i,\ldots,a_{i+47}) + nR_i \quad i \in [32,63]$

After authentication, LFSR keeps shifting

$a_{i+48} := L(a_i,\ldots,a_{i+47}) \quad i \in [64, \infty)$

Keystream:

$b_i := f(a_{i+9},a_{i+11},\ldots,a_{i+47}) \quad i \in \mathbb{N}$

Mifare Classic: trace

Step	Sender	Ciphertext	Plaintext	Meaning
01	R		26	request type A
02	T		04 00	answer request
03	R		93 20	select
04	T		2a 69 8d 43 8d	uid
05	R		93 70 2a 69 8d 43 8d	select(uid)
06	T		08 b6 dd	Mifare Classic 1k
07	R		60 04 d1 3d	auth(block 4)
08	T		3b ae 03 2d	tag nonce (nT)
09	R	c4 94 a1 d2 6e 96 86 42		rdr nonce (nR) & resp (aR)
10	T	84 66 05 9e		tag response (aT)
11	R	7d de a6 b3		
12	T	e7 ee e3 ab 0f 89 bb ed 44 b1 91 ce ef 8a 4d ce		

Mifare Classic: trace

Step	Sender	Ciphertext	Plaintext	Meaning
01	R		26	request type A
02	T		04 00	answer request
03	R		93 20	select
04	T		2a 69 8d 43 8d	uid
05	R		93 70 2a 69 8d 43 8d	select(uid)
06	T		08 b6 dd	Mifare Classic 1k
07	R		60 04 d1 3d	auth(block 4)
08	T		3b ae 03 2d	tag nonce (nT)
09	R	c4 94 a1 d2 6e 96 86 42	bb 03 1f 2d 7f cf 34 c3	rdr nonce (nR) & resp (aR)
10	T	84 66 05 9e	86 9d bb d5	tag response (aT)
11	R	7d de a6 b3	30 04 cd d1	read(block 4)
12	T	e7 ee e3 ab 0f 89 bb ed 44 b1 91 ce ef 8a 4d ce	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cd ea	contents

CRYPTO1: weaknesses

- 48 bit internal state
  - enables brute force attack
- weak random number generator
  - enables known plaintext attack
- 16 bit random number generator
  - enables replay attack
- evenly distributed taps of f
  - enables inverting of the one-way function f
- simple LFSR structure
  - enables unshifting the internal state
- consequences
  - intercepted communication can (quickly) be decrypted
  - key can be recovered from just a reader

Mifare Classic: further weaknesses

- weak random number generator sync with time
  - enables chosen plaintext attack
- reader nonces determine 32 bits of the internal state
  - enables chosen ciphertext attack against card
- mixing of data link and encryption layers
  - one-time pad used twice: information leakage
- encrypted error message sent when authentication fails
  - information leakage
- consequences
  - keys can be recovered from just a card
  - card can be wirelessly cloned

Mifare Classic: consequences

- Attacks:
  - Read/modify state of card
    - Store/restore state of card
    - (Wirelessly) clone a card
- Defenses:
  - Back-end checks

Mifare Classic is less secure than bar codes or magnetic stripe cards

CRYPTO1: (in)security

Why being open about security makes us all safer in the long run

Bruce Schneier
The Guardian, Thursday August 7 2008
Article history

London's Oyster card has been cracked, and the final details will become public in October. NXP Semiconductors, the Philips spin-off that makes the system, lost a court battle to prevent the researchers from publishing. People might be able to use this information to ride for free, but the sky won't be falling. And the publication of this serious vulnerability actually makes us all safer in the long run.

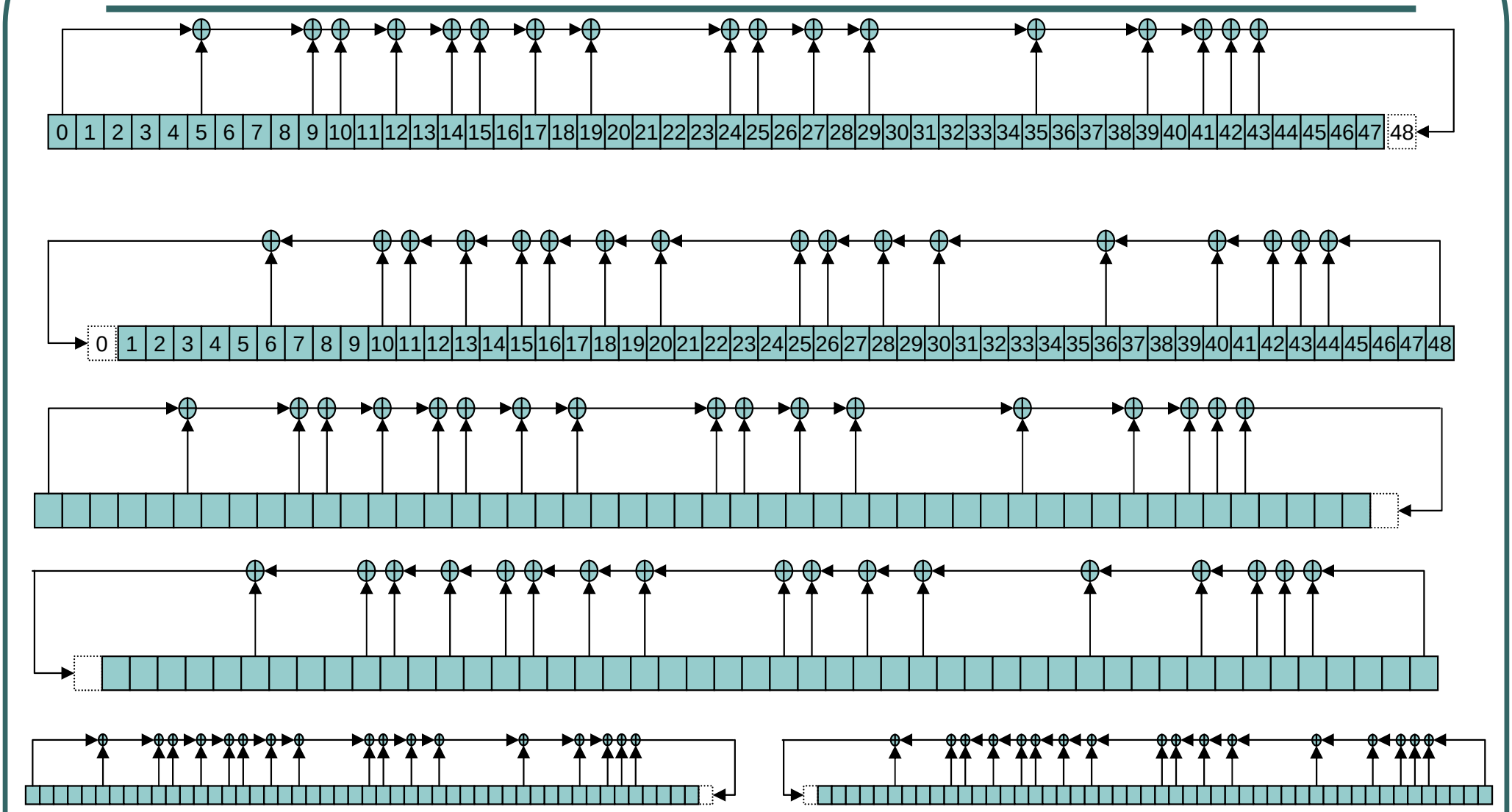
Here's the story. Every Oyster card has a radio-frequency identification chip that communicates with readers mounted on the ticket barrier. That chip, the "Mifare Classic" chip, is used in hundreds of other transport systems as well — Boston, Los Angeles, Brisbane, Oslo, Amsterdam, Taipei, Shanghai, Rio de Janeiro — and as an access pass in thousands of companies, schools, hospitals, and government buildings around Britain and the rest of the world.

> The security of Mifare Classic is terrible. This is not an exaggeration; it's kindergarten cryptography. Anyone with any security experience would be embarrassed to put his name to the design. NXP attempted to deal with this embarrassment by keeping the design secret.

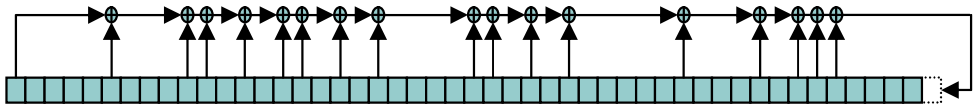
The group that broke Mifare Classic is from Radboud University Nijmegen in the Netherlands. They demonstrated the attack by riding the Underground for free, and by breaking into a building. Their two papers (one is already online) will be published at two

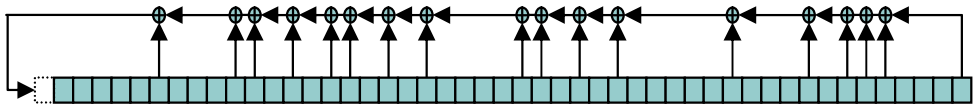
References

- Akerlof. *The Market for Lemons: Quality Uncertainty and the Market Mechanism.* The Quarterly Journal of Economics 84(3), 488-500. 1970.
- Garcia et al. *Dismantling Mifare Classic*. Proceedings of ESORICS 2008. Lecture Notes in Computer Science 5283. 97-114. 2008.
- De Koning Gans et al. *A Practical Attack on the Mifare Classic*. Proceedings of CARDIS 2008. Lecture Notes in Computer Science 5189. 267-282. 2008.


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48

CRYPTO1: Unshifting the LFSR





Feedback:

$$L(x_0,x_1,\ldots,x_{47}) := x_0+x_5+x_9+x_{10}+x_{12}+x_{14}+x_{15}+x_{17}+x_{19}+x_{24}+x_{25}+x_{27}+x_{29}+x_{35}+x_{39}+x_{41}+x_{43}$$

LFSR stream:

Initial state of the LFSR is the key

$a_i := k_i$ $\quad i \in [0,47]$

Shift nT + uid into the LFSR

$a_{i+48} := L(a_i,\ldots,a_{i+47}) + nT_i + uid_i \quad i \in [0,31]$

Shift nR into the LFSR

$a_{i+48} := L(a_i,\ldots,a_{i+47}) + nR_i \quad i \in [32,63]$

After authentication, LFSR keeps shifting

$a_{i+48} := L(a_i,\ldots,a_{i+47}) \quad i \in [64, \infty)$

Keystream:

$b_i := f(a_{i+9},a_{i+11},\ldots,a_{i+47}) \quad i \in \mathbb{N}$

Inverting feedback:

$$R(x_1,\ldots,x_{47},x_{48}) := x_5+x_9+x_{10}+x_{12}+x_{14}+x_{15}+x_{17}+x_{19}+x_{24}+x_{25}+x_{27}+x_{29}+x_{35}+x_{39}+x_{41}+x_{43}+x_{48}$$

$$R(x_1,\ldots,x_{47},L(x_0,x_1,\ldots,x_{47})) = x_0$$

Inverting LFSR stream:

Unshift LFSR until end of authentication

$a_i = R(a_{i+1},\ldots,a_{i+48}) \quad i \in [64, \infty)$

Unshift nR from the LFSR

$a_i = R(a_{i+1},\ldots,a_{i+48}) + nR_i \quad i \in [32,63]$

$= R(a_{i+1},\ldots,a_{i+48}) + \{nR\}_i + b_i$

$= R(a_{i+1},\ldots,a_{i+48}) + \{nR\}_i + f(a_{i+9},\ldots,a_{i+47})$

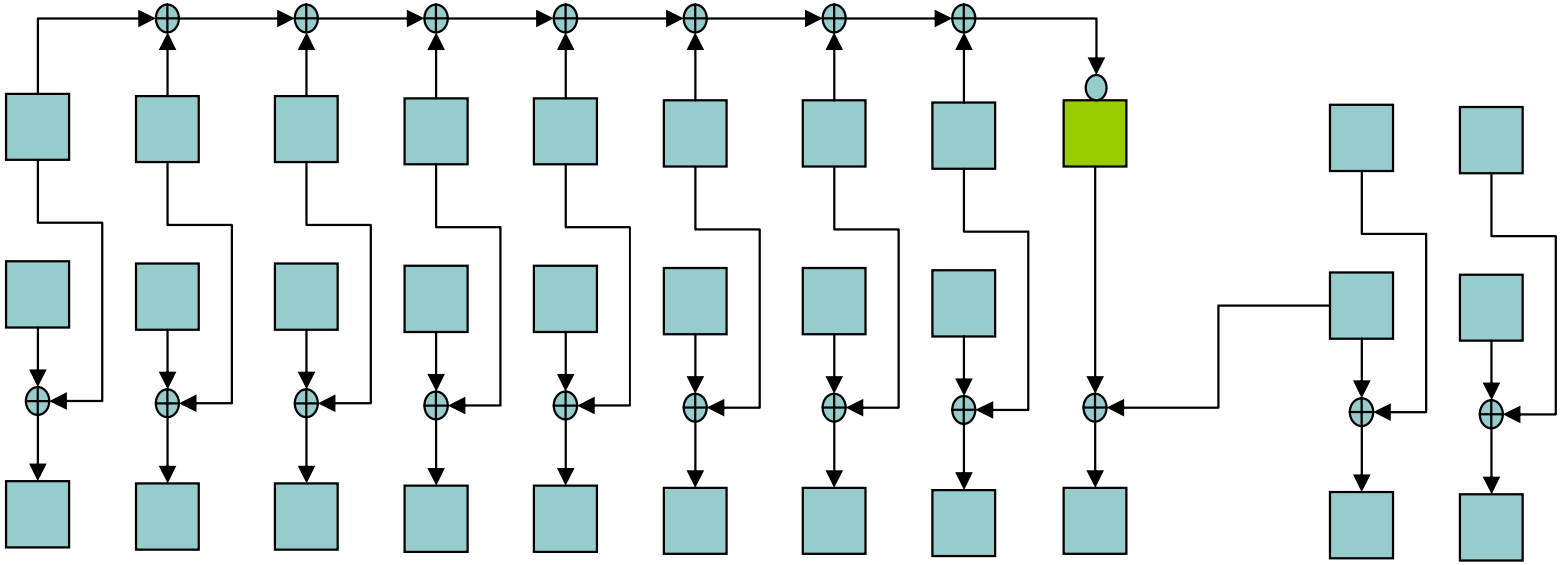
Shift nT + uid into the LFSR

$a_i = R(a_{i+1},\ldots,a_{i+48}) + nT_i + uid_i \quad i \in [0,31]$

Key is the initial state of the LFSR

$k_i = a_i \quad i \in [0,47]$

Mifare Classic: Parity Trouble



What to do?

- Openness vs. secrecy
  - of design
  - of problems

What to do? Openness/secrecy of design

- Openness +/-
  - + Customer can judge himself
  - + Mistakes detected earlier
  - – Bad guys know more
  - + Design may (will?) leak anyway

    (Kerckhoff's Principle: Security [of a cryptographic scheme] should not depend on secrecy [of the scheme], but only on the secrecy of the key)
  - + Designer make better effort

What to do? Openness/secrecy of design

- Secrecy +/-
  - + Slows down bad guys
  - – No (or little) critical feedback
  - – Absolute trust required in (claimed) professionality
    - - Unclear mix with marketing
    - - Independent evaluations secret as well
  - –/+ Own weaknesses/mistakes stay hidden
  - + Protection of intellectual property

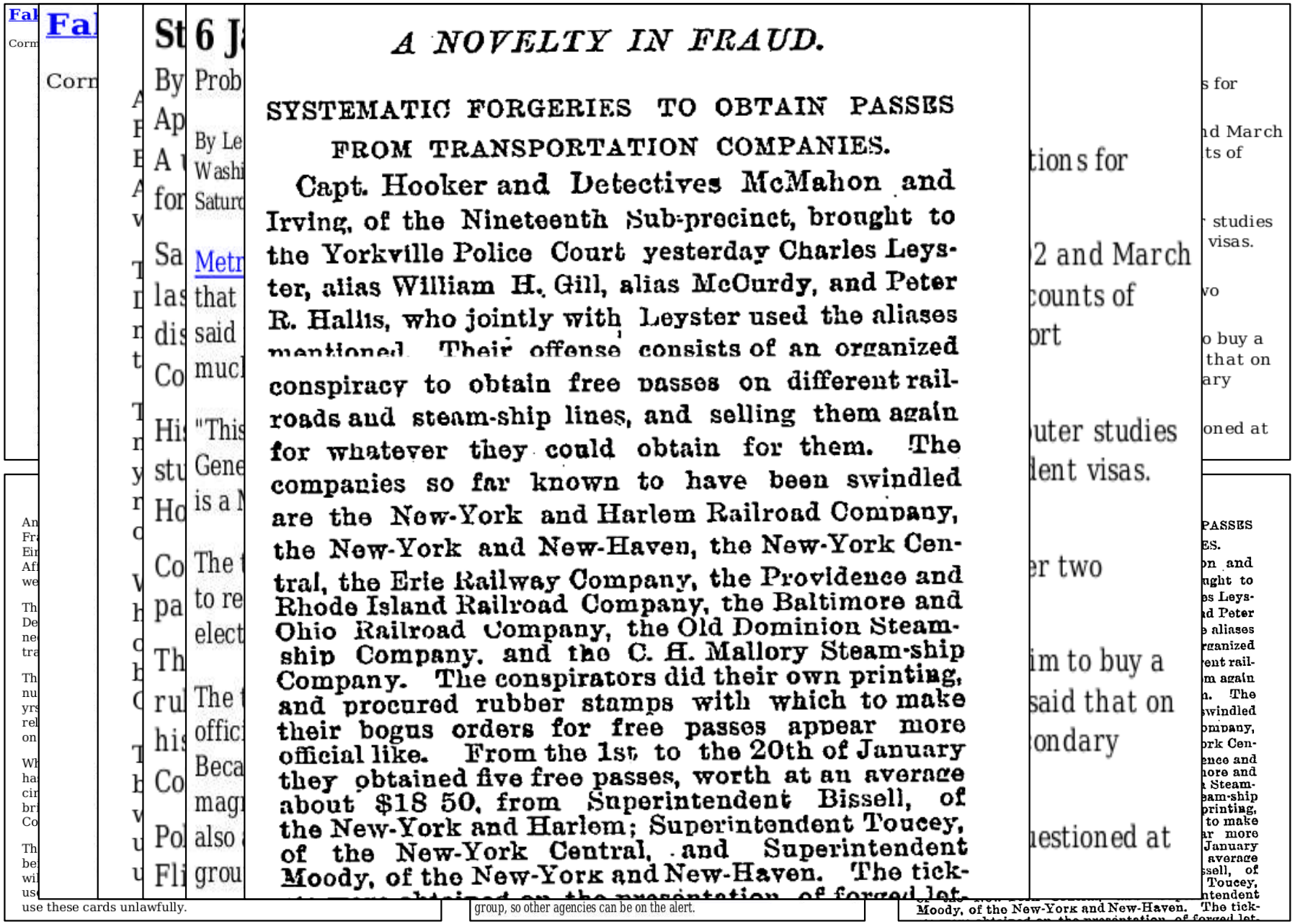
Openness in practice

- Cryptographic algorithms
  - Good ones are nearly always open
  - (Corrolary: secret ones are nearly always poor)
- System architecture
  - Mostly open
- Software
  - Often closed, but opening up via open source
- Hardware
  - Hardly ever open

What to do? Openness/secrecy of problems

- Strategy RU: responsible disclosure
  - 02/08: Warning (to NXP, government): additional measures needed; minister of internal affairs made problems public
    Only claim what we can actually demonstrate
  - 10/08: Publication after delay of 7 months
    All details, but no reference implementation
- Strategy NXP: damage control
  - 03/08: Customer chooses cheapest chip
  - 07/08: Publication irresponsible
  - 10/08: Don’t use Classic for new applications
- Strategy system integrators (TLS, TFL, …): protect investment
  - 03/08: Attack not feasible
  - 07/08: Fraud detected in back-end; no fraud detected so far
  - 10/08: No criminal business case

“No Criminal Business Case”?



A NOVELTY IN FRAUD.

SYSTEMATIC FORGERIES TO OBTAIN PASSES FROM TRANSPORTATION COMPANIES.

Capt. Hooker and Detectives McMahon and Irving, of the Nineteenth Sub-precinct, brought to the Yorkville Police Court yesterday Charles Leyster, alias William H. Gill, alias McCurdy, and Peter R. Hallis, who jointly with Leyster used the aliases mentioned. Their offense consists of an organized conspiracy to obtain free passes on different railroads and steam-ship lines, and selling them again for whatever they could obtain for them. The companies so far known to have been swindled are the New-York and Harlem Railroad Company, the New-York and New-Haven, the New-York Central, the Erie Railway Company, the Providence and Rhode Island Railroad Company, the Baltimore and Ohio Railroad Company, the Old Dominion Steam-ship Company, and the C. H. Mallory Steam-ship Company. The conspirators did their own printing, and procured rubber stamps with which to make their bogus orders for free passes appear more official like. From the 1st to the 20th of January they obtained five free passes, worth at an average about $18 50, from Superintendent Bissell, of the New-York and Harlem; Superintendent Toucey, of the New-York Central, and Superintendent Moody, of the New-York and New-Haven. The tick-

“No Criminal Business Case”?

Fake Dublin Bus ticket scam uncovered

Cormac Murphy of the Herald writes:

> Fraudsters have been using forged bus and Luas tickets to evade public transport fares, it emerged today.
>
> Dublin Bus launched a full-scale probe when the scam was uncovered, leading to the arrest of a number of suspects.
>
> A man has already been fined €300 in court for using a fake pass, while other cases are pending.
>
> The con centred on the ‘Combi’ 30-day pass worth €98 which was advertised for sale at a price of €50 on the Gumtree website earlier this year.
>
> The pass is valid on all Dublin Bus vehicles and Luas trams.
>
> The forgeries look almost exactly like the real ones, though they are not recognised by validating machines on buses.
>
> The fraud was exposed when an employee of the bus company was going through ‘standard fares’ — or fines — issued to passengers.
>
> Mark Kelly, an area manager with the semi-state’s revenue protection unit, came across a fine issued to a woman for not having her Dublin Bus identification card with her.
>
> He told the Herald he thought it odd that she would pay €98 for a Combi ticket and then not even carry her free ID.
>
> Mr Kelly kept the ticket with him and within 24 hours had it checked out. It proved to be a forgery.
>
> Dublin Bus officers then discovered an ad on Gumtree for a 30-day bus and Luas pass at a cut-price €50.

Student ran transport scam

By Daniella Miletic
April 20, 2005

A university student faked dozens of transport concession card applications for foreign students at $80 a time, a court was told yesterday.

Samuel Tang, 23, of Forest Hill, conducted the scam between early 2002 and March last year, using a fake school stamp. He pleaded guilty yesterday to 54 counts of dishonestly obtaining student concession cards from the Public Transport Corporation.

His friend Elizabeth Hancock told the County Court that Tang, a computer studies student at Monash University, wanted to help Chinese students on student visas. Holders of such visas are ineligible for travel concession cards.

County Court judge Julie Nicholson heard that students would hand over two passport photos and $80. Tang received $4320 over the two years.

The court heard that a friend Tang visited in 2001 in China advised him to buy a rubber stamp with a school's name on it. Tang's lawyer, Geoff Martin, said that on his return to Melbourne, Tang bought a stamp reading "Bayswater Secondary College". He then gained clients through word of mouth.

Police were alerted after an application that Tang had stamped was questioned at Flinders Street station and the person submitting the application fled.

Travel Card Fraud Detected

An Garda Sï¿½ochï¿½na, primarily through the Garda Bureau of Fraud Investigation, and in conjunction with Dublin Bus, Bus Eireann, Iarnrod Eireann & the Department of Social & Family Affairs, have been engaged in an investigation for a number of weeks.

The fraud involved false Travel Passes which are issued by the Department of Social & Family Affairs to persons with special needs. Passes entitle the bearer and an accompanying person free travel throughout the country on all public transport facilities.

The Garda investigation involved the interviewing of a significant number of people, culminating in the arrest of a male, aged 33 yrs. from the Dublin area. He has been charged with offences relating to this matter and is due before the Courts at 10.30a.m. on 10/02/06 at Dublin District Court No. 46.

While the source of these fake cards and the distribution network has now been dismantled, there are a number of fake cards still in circulation. The Garda investigation is continuing with a view to bringing those with fake cards in their possession before the Courts.

The introduction of a new Travel Pass Card System is currently being examined by the Department of Social & Family Affairs. This will significantly aid detection in the event of fake cards being used. It is a serious criminal offence to have in your possession or use these cards unlawfully.

6 Jailed In Metro Farecard Scheme

Probe Searches For 'Mr. Big'

By Lena H. Sun
Washington Post Staff Writer
Saturday, July 19, 2008; B01

Metro Transit Police have arrested six people in an elaborate fare card scam that has so far netted the agency $16,000 worth of stolen Farecards, officials said yesterday. The investigation is ongoing, and officials do not know how much the counterfeit operation has cost the agency.

"This was a sophisticated operation to defraud a public agency," Metro General Manager John B. Catoe Jr. said at a news conference. "We think there is a Mr. Big, and that's who we would like to find."

The thieves traded in counterfeit paper Farecards in Metro Farecard machines to receive legitimate ones, or used the counterfeit ones to add value to electronic SmarTrip cards, officials said.

The thieves also sold some of the legitimate cards on the street at half-price, officials said. Metro is investigating whether the cards were also sold online. Because many transit agencies have similar fare collection systems -- a magnetic strip that is electronically read by a Farecard machine -- Metro has also alerted the American Public Transportation Association, a major industry group, so other agencies can be on the alert.

A NOVELTY IN FRAUD.

SYSTEMATIC FORGERIES TO OBTAIN PASSES FROM TRANSPORTATION COMPANIES.

Capt. Hooker and Detectives McMahon and Irving, of the Nineteenth Sub-precinct, brought to the Yorkville Police Court yesterday Charles Leyster, alias William H. Gill, alias McCurdy, and Peter R. Hallis, who jointly with Leyster used the aliases mentioned. Their offense consists of an organized conspiracy to obtain free passes on different railroads and steam-ship lines, and selling them again for whatever they could obtain for them. The companies so far known to have been swindled are the New-York and Harlem Railroad Company, the New-York and New-Haven, the New-York Central, the Erie Railway Company, the Providence and Rhode Island Railroad Company, the Baltimore and Ohio Railroad Company, the Old Dominion Steamship Company, and the C. H. Mallory Steam-ship Company. The conspirators did their own printing, and procured rubber stamps with which to make their bogus orders for free passes appear more official like. From the 1st to the 20th of January they obtained five free passes, worth at an average about $18 50, from Superintendent Bissell, of the New-York and Harlem; Superintendent Toucey, of the New-York Central, and Superintendent Moody, of the New-York and New-Haven. The tick-

Challenge

- Technological
  - Better cryptography (fast and small and cheap)
  - Better privacy protection (at least random uid)
  - Modular design
  - Open design
- Economical
  - There should be incentive for manufacturers to produce secure technology and for system integrators to use secure technology
    - Customer demand (requires customer knowledge)
    - Adequate reviewing (requires openness)
    - Accountability

Questions? / Remarks?