Lightweight Cryptography

Alfredo De Santis

Dipartimento di Informatica
Università di Salerno

ads@unisa.it

http://www.di-srv.unisa.it/~ads

Ottobre 2019

Algoritmi cifratura

La maggior parte sono stati progettati per computer desktop

Non ci sono grandi vincoli

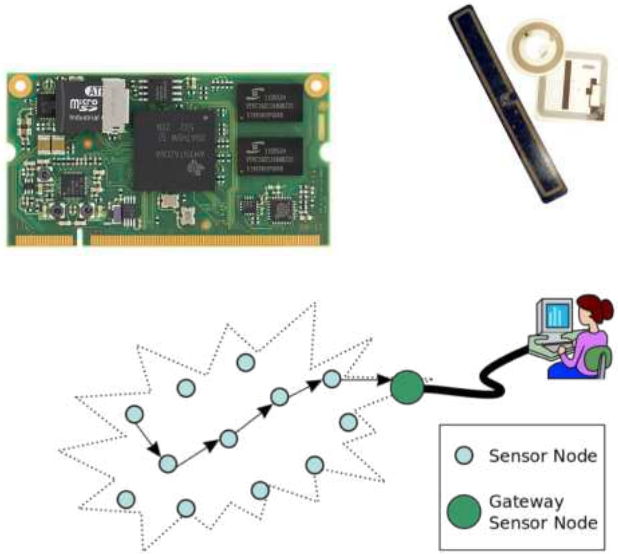
Cryptography

Crittografia convenzionale

- Server, Desktop,
- Tablet, Smartphone

Lightweight Cryptography

- Sistemi embedded
- RFID, Sensor Network



Sistemi embedded

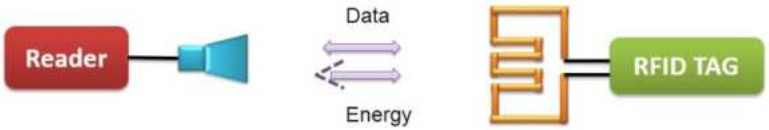
Sistemi a microprocessore per determinate applicazioni (special purpose). Non progettato per essere programmato dall'utente finale.

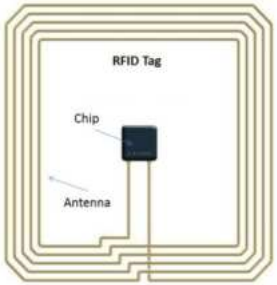
PC dedicati all'automazione industriale e il controllo di processo, Bancomat, terminali POS, stampanti, fotocopiatrici, Termostati, condizionatori, forni a microonde, lavatrici, TV, …

RFID

- Radio-Frequency Identification
- Uno dei metodi per Automatic Identifying and Data Capture (AIDC)
- Identificazione e/o memorizzazione automatica di informazioni inerenti ad oggetti, animali o persone
- Applicazioni:

Passaporti, bigliettazione elettronica, Carte di credito, logistica magazzini e trasporti, controllo presenze ed accessi, tracciamento, assistenza e manutensione, identificazione animali, monitoraggio raccolta rifiuti, sistemi di allarme, …

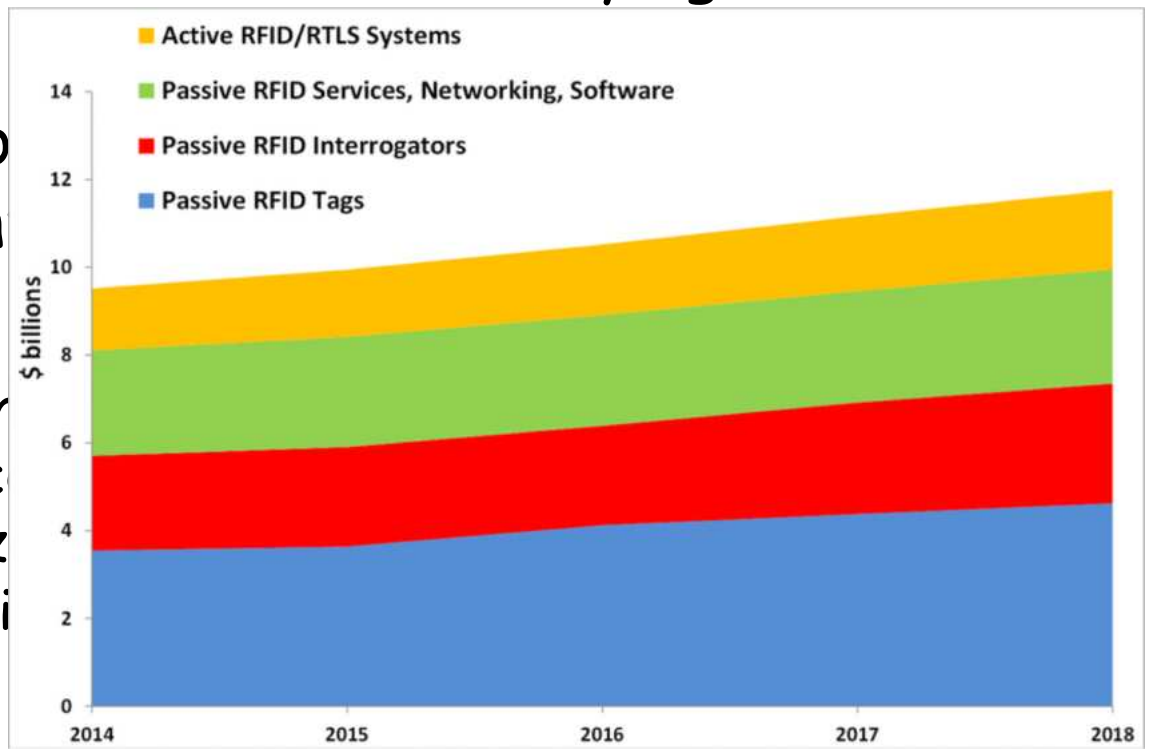




RFID

- Radio-Frequency Identification
- Uno dei metodi per Automatic Identifying and Data Capture (AIDC)
- Identificazione e/o informazioni ineren
- Applicazioni:

Passaporti, bigliettazior magazzini e trasporti, c tracciamento, assistenz monitoraggio raccolta ri

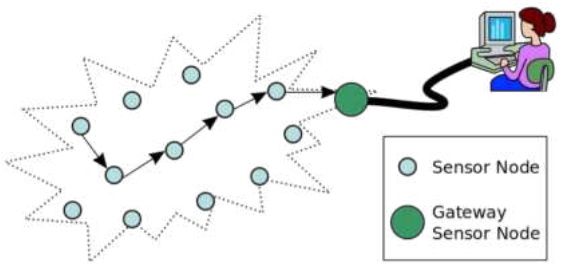


Total RFID Market in US$ billions

https://www.idtechex.com/research/reports/rfid-forecasts-players-and-opportunities-2017-2027-000546.asp

Sensor Network

Rete di sensori dedicati per monitorare e memorizzare dati dell'ambiente e organizarli ad una locazione centrale.

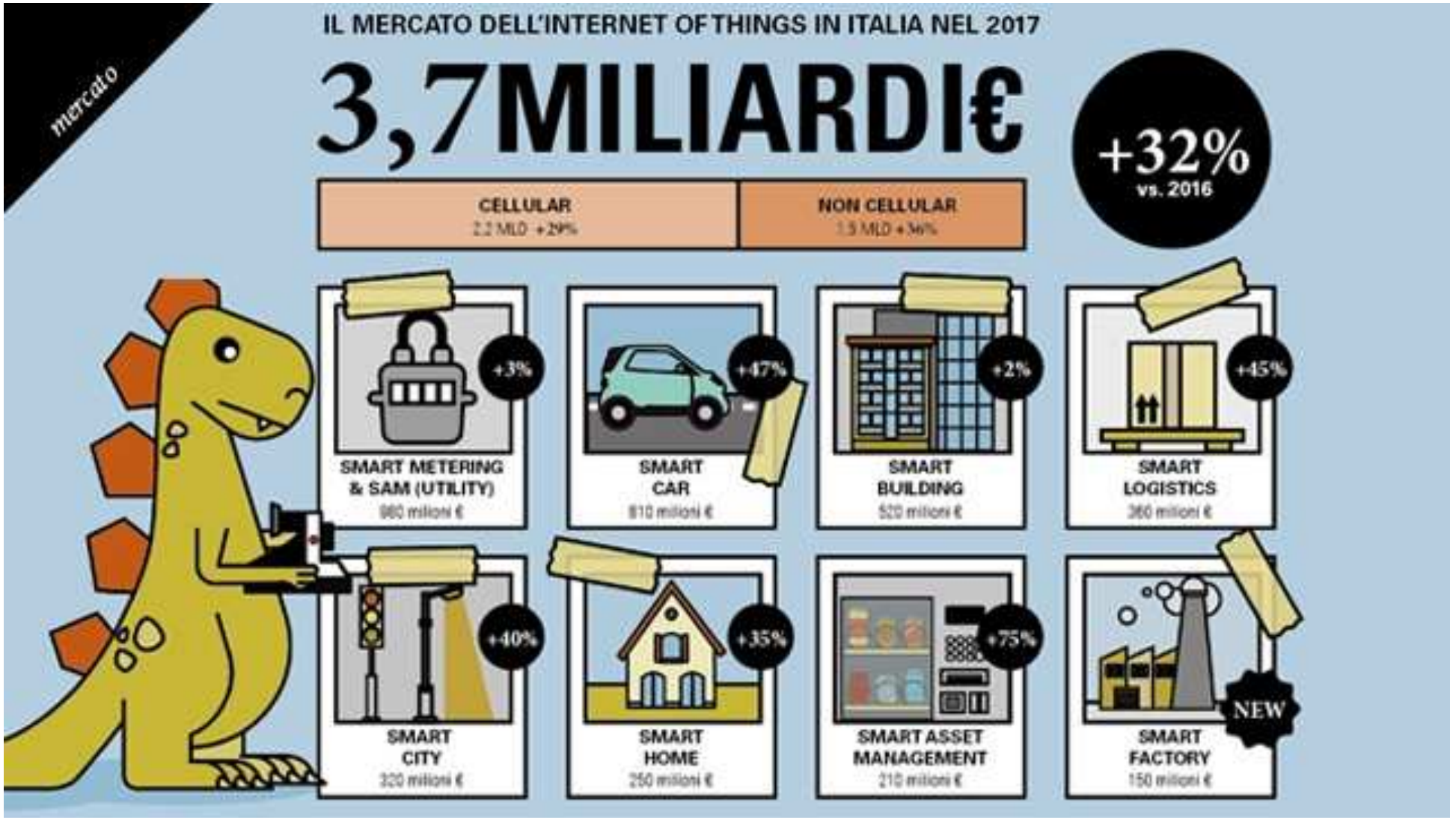


Applicazioni:

Monitoraggio aree (ad es. militari), monitoraggio inquinamento aria, monitoraggio acqua, monitoraggio medico, monitoraggio costruzioni edili, …

IoT

- Evoluzione della rete di oggi: smart object connessi
- Previsione Gartner: nel 2020 ci saranno 26 miliardi di oggetti connessi a livello globale
- Previsione ABI Research: più di 30 miliardi


mercato
IL MERCATO DELL'INTERNET OF THINGS IN ITALIA NEL 2017
3,7MILIARDI€
+32%
vs. 2016
CELLULAR
2,2 MLD +29%
NON CELLULAR
1,5 MLD +36%
+3%
SMART METERING & SAM (UTILITY)
960 milioni €
+47%
SMART CAR
810 milioni €
+2%
SMART BUILDING
520 milioni €
+45%
SMART LOGISTICS
360 milioni €
+40%
SMART CITY
320 milioni €
+35%
SMART HOME
250 milioni €
+75%
SMART ASSET MANAGEMENT
210 milioni €
NEW
SMART FACTORY
150 milioni €

Applicazioni

access control

secure e-passport

automatic pay-toll

inventory control

pet identification

tags for medicines

supermarket checkout counters

Necessità di autenticazione e confidenzialità

The Reader need to be sure the tag is not counterfeit

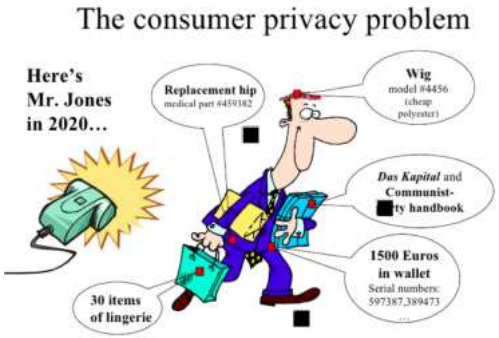
" … anti-counterfeiting tags for medicines"

anti-counterfeiting tags for medicines

The Tag need to be sure the Reader is a legal one

" … supermarket checkout counters"

supermarket checkout counters



Vincoli

Hardware

- Grandezza ASIC/FPGA, potenza, energia, latenza

Software

- Grandezza del codice, memoria, velocità, energia

Tool necessari

- Primitive lightweight
  - Cifrari a blocchi
  - Funzioni Hash
- Protocolli lightweight e ultralightweight
  - Authenticated encryption schemes
  - Authentication protocols

Tool necessari

- Primitive lightweight
  - Cifrari a blocchi
  - Funzioni Hash
- Protocolli lightweight e ultralightweight
  - Authenticated encryption schemes
  - Authentication protocols

Vediamo due cifrari a blocchi

Simon and Speck

Sviluppati da National Security Agency (NSA)

Resi pubblici nel giugno 2013

https://eprint.iacr.org/2013/404.pdf

https://csrc.nist.gov/csrc/media/events/lightweight-cryptography-workshop-2015/documents/presentations/session1-shors.pdf

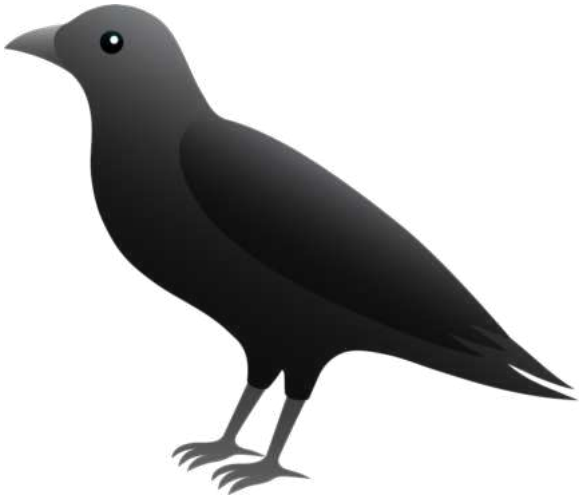
Specialista e generalista

Koala

- Specialista: la dieta consiste quasi esclusivamente di foglie di eucalipto

Corvo americano

- Generalista: molto adattabile



Specialista e generalista

- Specialista: richiedono un ambiente stabile

- Generalista: si adattano all' ambiente che cambia

Specialista e generalista

- Molti algoritmi sono specialisti, cioè ottimizzati per particolari piattaforme

- Meglio generalista:
  - progettati per essere semplici e flessibili
  - con buone prestazioni su molte piattaforme esistenti (ed anche future)

Simon e Speck

Funzione di round semplice

- Iterata quanto necessario per la sicurezza
- Invece, AES usa funzione di round complessa iterata poche volte

Simon e Speck

Simon

Ottimizzato per implementazioni hardware

Speck

Ottimizzato per implementazioni software

Simon e Speck: parametri

Famiglia di 10 algoritmi

Lunghezza blocco	Lunghezza chiave
32	64
48	72, 96
64	96, 128
96	96, 144
128	128, 192, 256

Notazione: **Simon2n/mn**, con n = 16,24,32,48,64

Es., Simon64/128

Simon: operazioni

Famiglia di 10 algoritmi

Lunghezza blocco	Lunghezza chiave
32	64
48	72, 96
64	96, 128
96	96, 144
128	128, 192, 256

Operazioni di Simon2n su parole di n bit

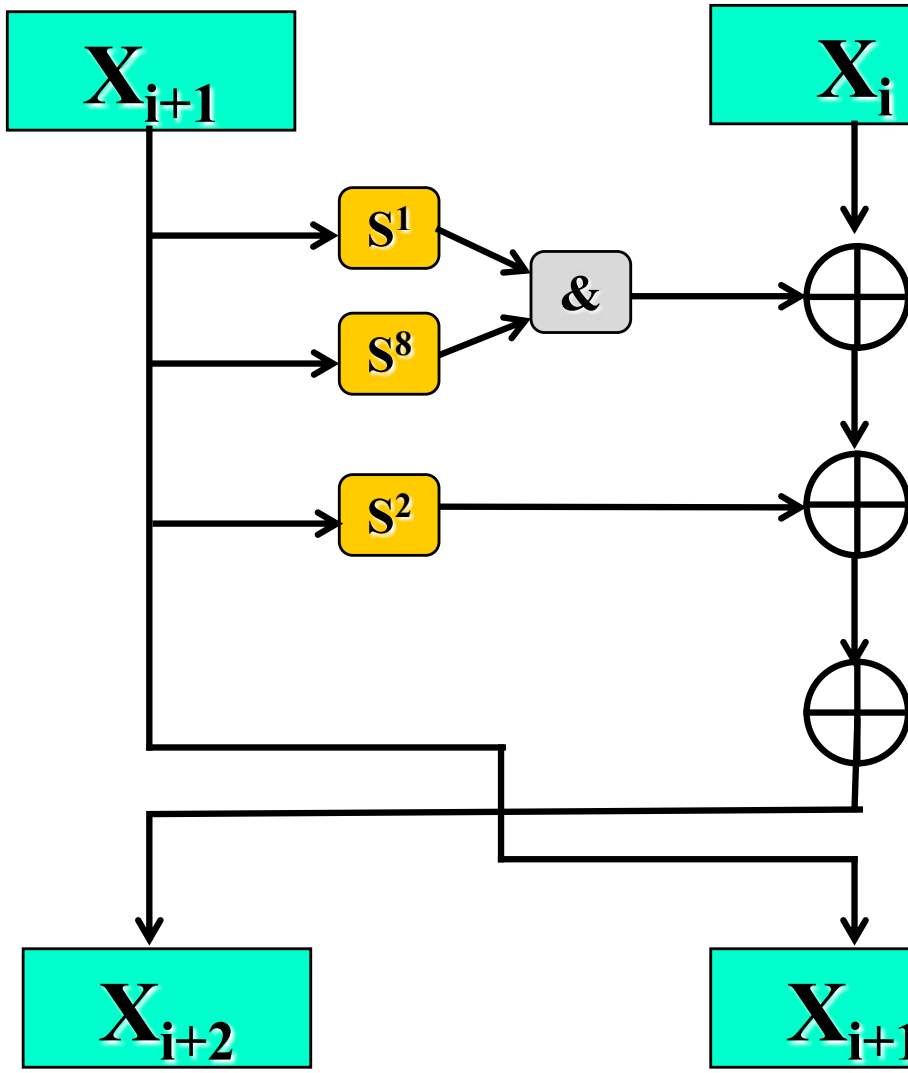
- S^i shift circolare a sx di i bit
- & AND logico
- $\oplus$ XOR

Simon: numero iterazioni

Famiglia di 10 algoritmi

Lunghezza blocco	Lunghezza chiave	Numero iterazioni
32	64	32
48	72	36
	96	36
64	96	42
	128	44
96	96	52
	144	54
128	128	68
	192	69
	256	72

Simon: struttura round



S^i shift circolare a sx di i bit

& AND logico

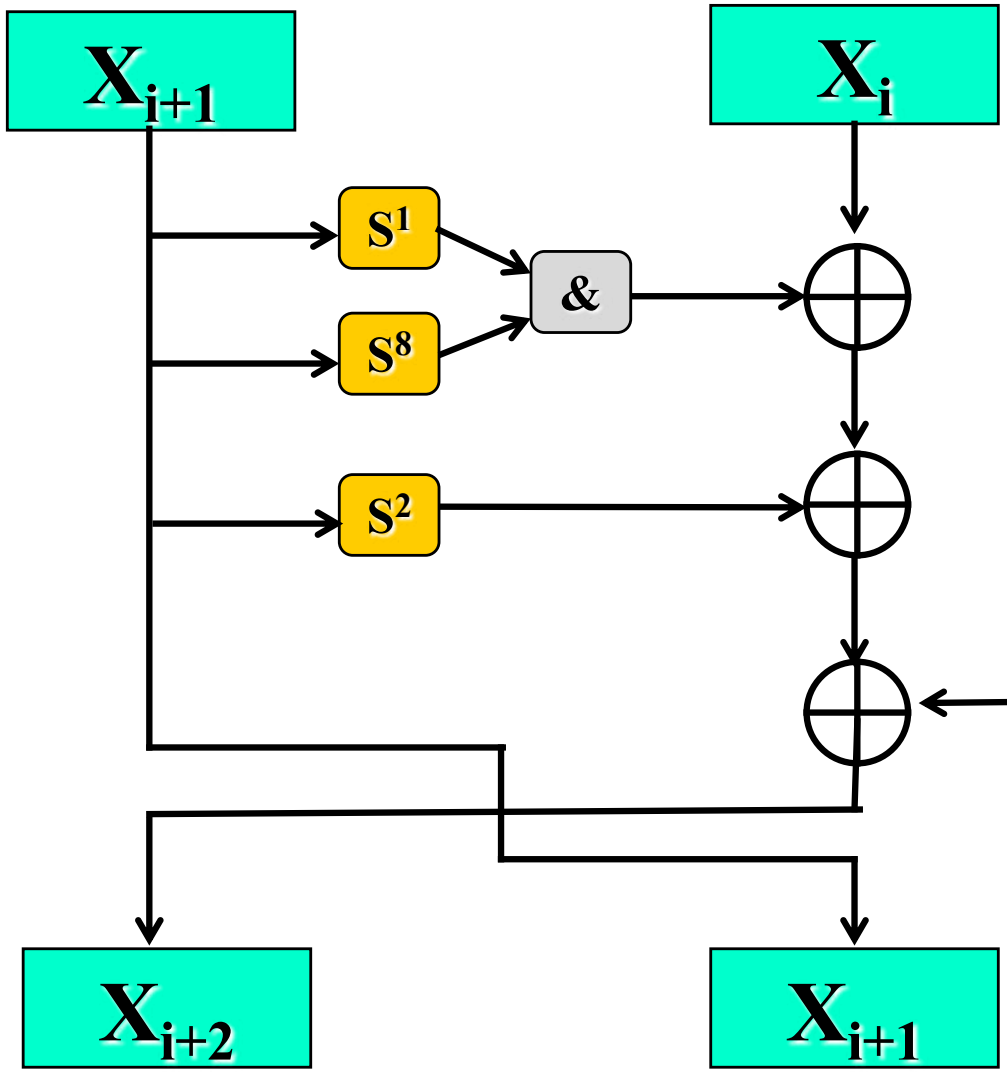
sottochiave

Cifrario di Feistel

Simon

Round:

$X_{i+2} \leftarrow X_i \oplus (S^1 X_{i+1} \,\&\, S^8 X_{i+1}) \oplus S^2 X_{i+1} \oplus k_i$



S^i shift circolare a sx di i bit

& AND logico

sottochiave

Cifrario di Feistel

Simon: pseudocodice cifratura

Testo in chiaro (x,y)

for i = 0...T-1

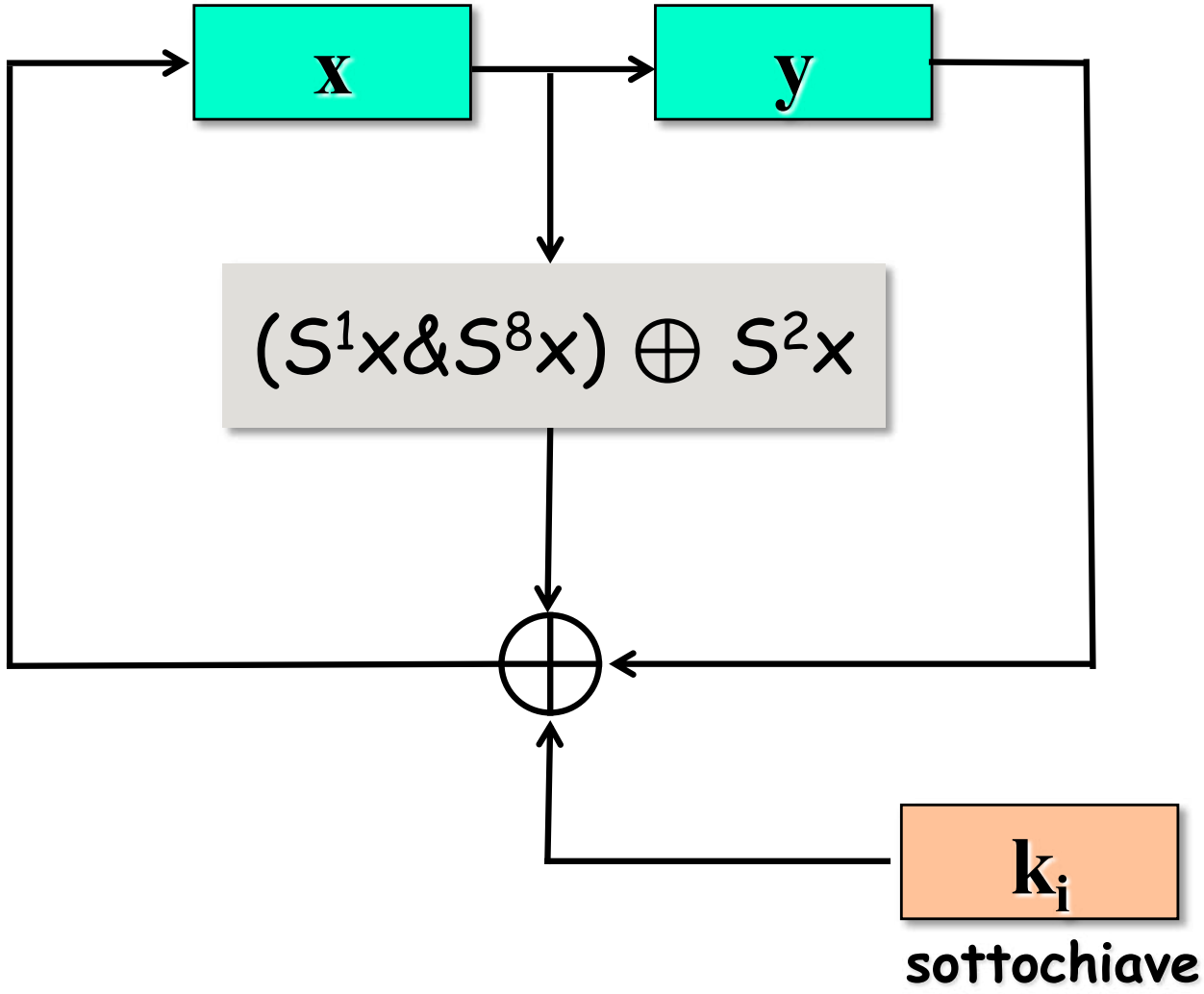
$tmp \leftarrow x$

$x \leftarrow y \oplus (S^1x \& S^8x) \oplus S^2x \oplus k[i]$

$y \leftarrow tmp$

end for

Simon: registri hardware



Simon: decifratura

Esercizio

- Chiarire come si decifra
- Scrivere lo pseudocodice per la decifratura

Speck: operazioni

Famiglia di 10 algoritmi

Lunghezza blocco	Lunghezza chiave
32	64
48	72, 96
64	96, 128
96	96, 144
128	128, 192, 256

Operazioni di Speck2n su parole di n bit

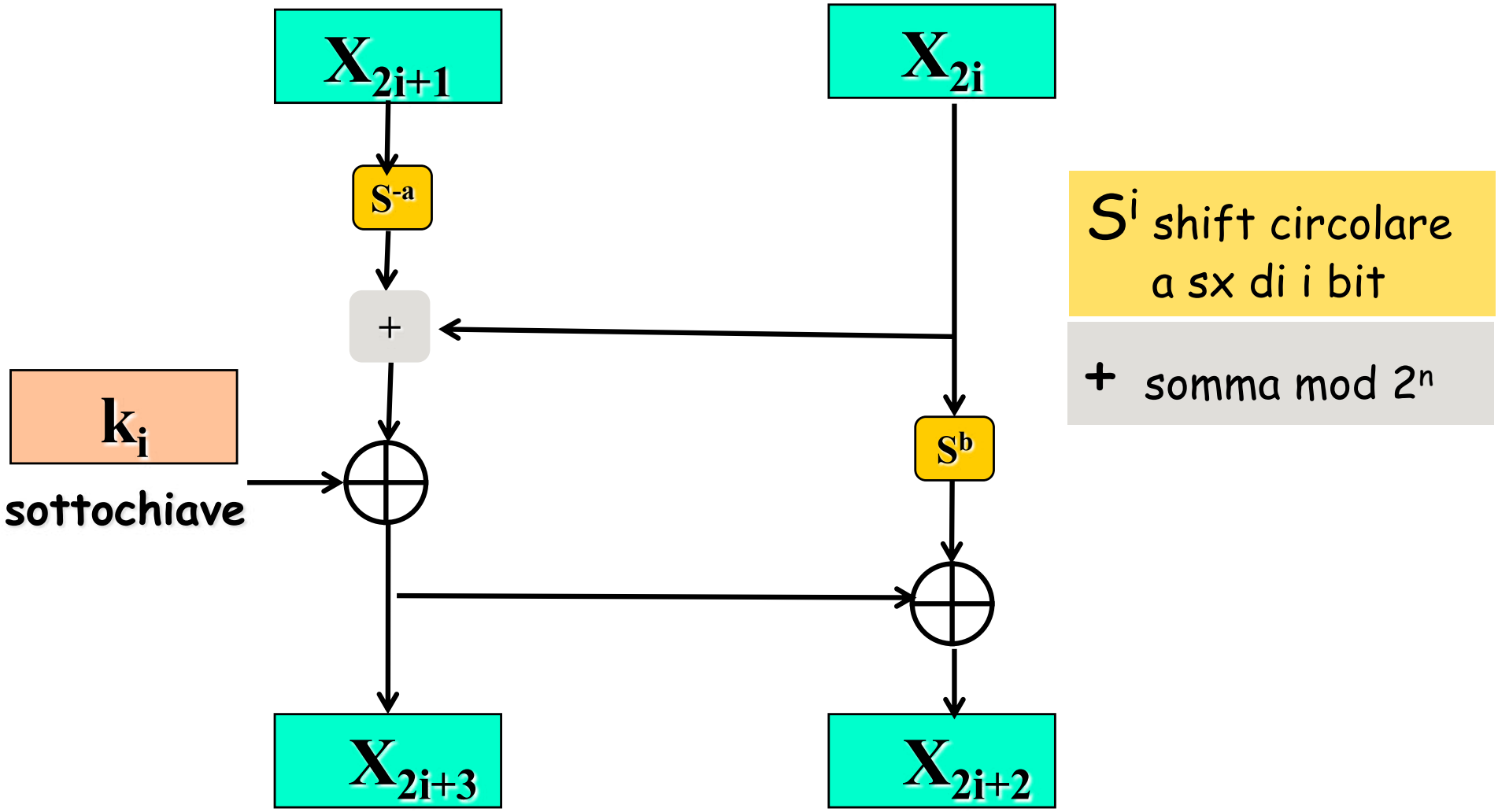
- S^i shift circolare a sx di i bit
- $+$ somma modulo 2^n
- $\oplus$ XOR

Speck: numero iterazioni

Famiglia di 10 algoritmi

Lunghezza blocco	Lunghezza chiave	Numero iterazioni Simon	Numero iterazioni Speck
32	64	32	22
48	72	36	22
	96	36	23
64	96	42	26
	128	44	27
96	96	52	28
	144	54	29
128	128	68	32
	192	69	33
	256	72	34

Speck: struttura round



Speck: bit shiftati

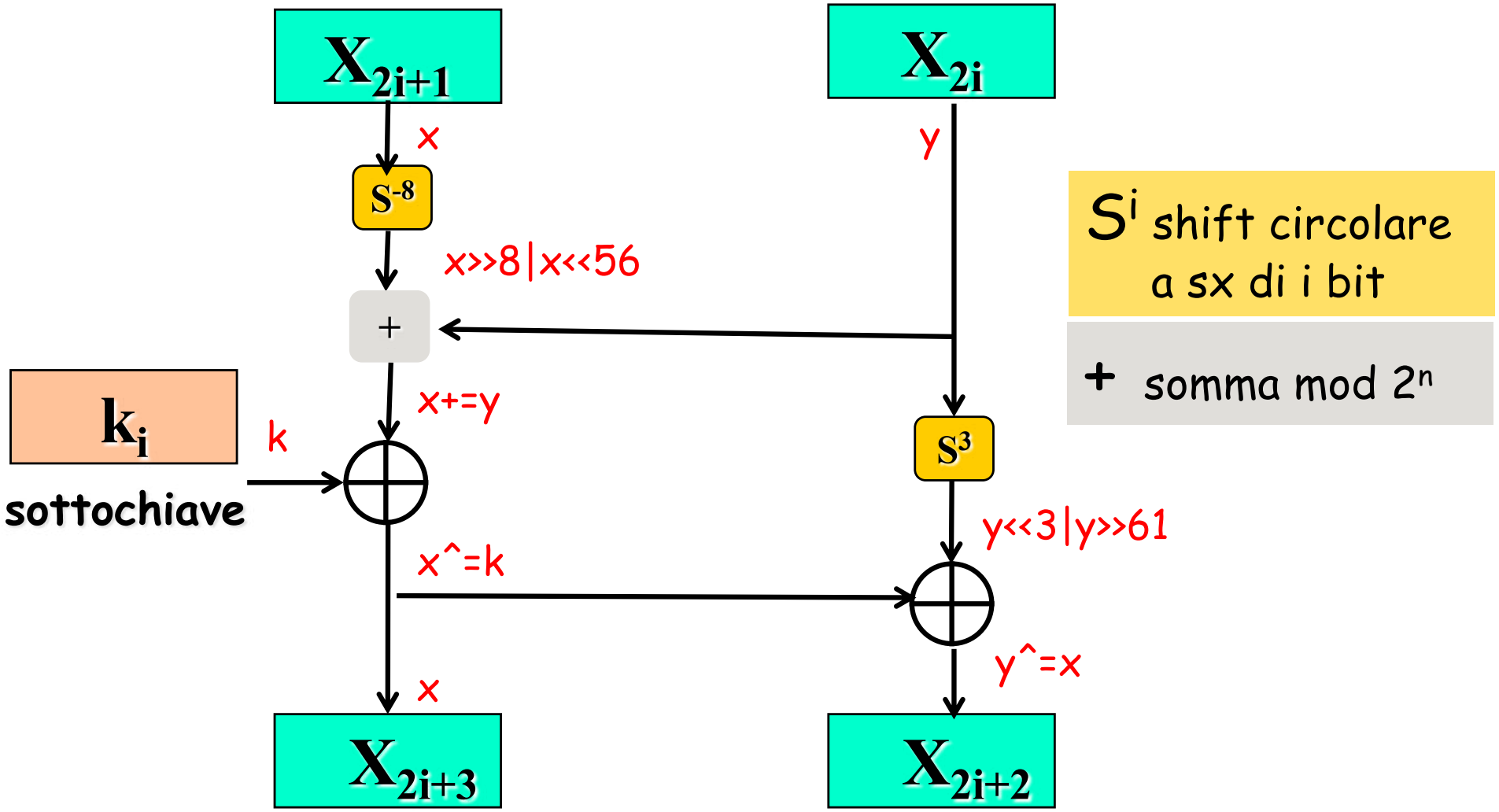
Lunghezza blocco	Lunghezza chiave	a	b
32	64	7	2
48	72	8	3
	96	8	3
64	96	8	3
	128	8	3
96	96	8	3
	144	8	3
128	128	8	3
	192	8	3
	256	8	3

SPECK 128/128: codice C

```
#define R(x,y,k)x=x>>8|x<<56,x+=y,x^=k,y=y<<3|y>>61,y^=x
void E(uint64_t *T,uint64_t *K){for(int i=0;i<32;){R(T[1],*T,*K);R(K[1],*K,i++);}}
```

SPECK 128/128: struttura round

#define R(x,y,k)x=x>>8|x<<56,x+=y,x^=k,y=y<<3|y>>61,y^=x



Speck: decifratura

Esercizio

- Chiarire come si decifra
- Scrivere lo pseudocodice per la decifratura

Simon e Speck

Simon

- Meglio per app hardware puro

Speck

- Meglio per app software puro
- Evita di fare copie di parole

Standard ISO

- Cifrari molto criticati dai delegati di diversi paesi (Germania, Giappone, Israele,…)
- Rifiutati come ISO standard, giugno 2018

International Organization for Standardization

ISO is an independent, non-governmental international organization with a membership of 162 national standards bodies.

Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.

You'll find our Central Secretariat in Geneva, Switzerland.

ISO has published 22368 International Standards and related documents, covering almost every industry, from technology, to food safety, to agriculture and healthcare. ISO International Standards impact everyone, everywhere.

https://www.iso.org

REUTERS

WORLD NEWS SEPTEMBER 21, 2017 / 7:03 AM / A YEAR AGO

Distrustful U.S. allies force spy agency to back down in encryption fight

Joseph Menn

8 MIN READ

SAN FRANCISCO (Reuters) - An international group of cryptography experts has forced the U.S. National Security Agency to back down over two data encryption techniques it wanted set as global industry standards, reflecting deep mistrust among close U.S. allies.

https://www.reuters.com/article/us-cyber-standards-insight/distrustful-u-s-allies-force-spy-agency-to-back-down-in-encryption-fight-idUSKCN1BW0GV

CYBER SECURITY | Back to Home

NSA: Our Crypto Is Good. ISO: No Thanks Though

ED TARGETT EDITOR
27TH APRIL 2018

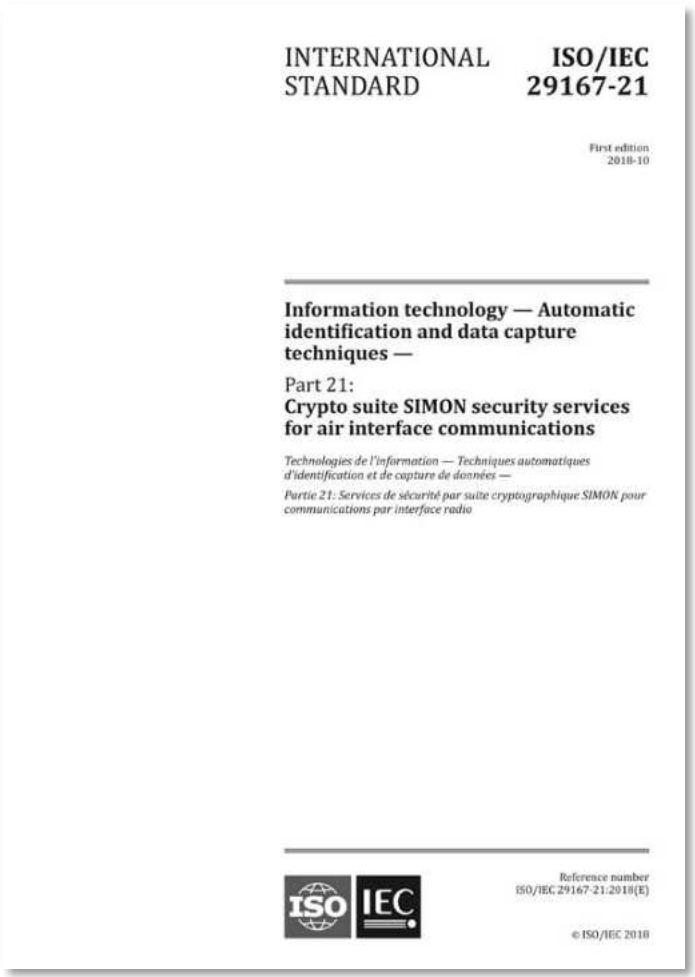
+ INCREASE / DECREASE TEXT SIZE −

SIMON and SPECK made public in 2013; critics fear backdoors.

https://www.cbronline.com/news/iso-nsa

Standard ISO (ottobre 2018)

Crypto suite per ISO/IEC 18000 air interfaces standards
for radio frequency identification (RFID) devices



INTERNATIONAL STANDARD **ISO/IEC 29167-21**

First edition
2018-10

Information technology — Automatic identification and data capture techniques —

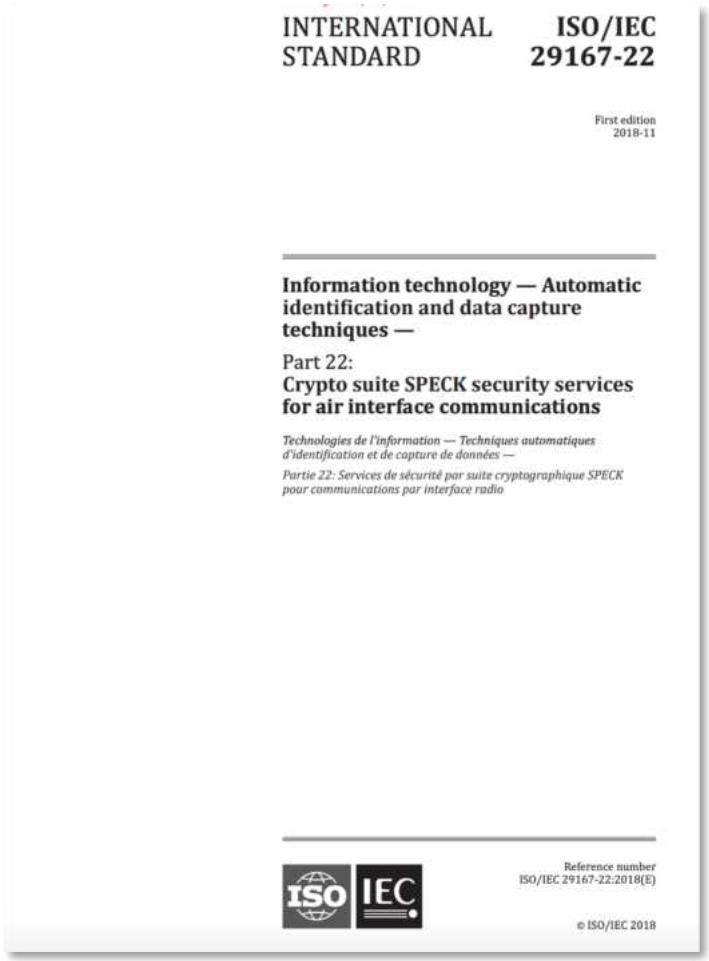
Part 21:
Crypto suite SIMON security services for air interface communications

Technologies de l'information — Techniques automatiques d'identification et de capture de données —

Partie 21: Services de sécurité par suite cryptographique SIMON pour communications par interface radio

Reference number
ISO/IEC 29167-21:2018(E)

© ISO/IEC 2018



INTERNATIONAL STANDARD **ISO/IEC 29167-22**

First edition
2018-11

Information technology — Automatic identification and data capture techniques —

Part 22:
Crypto suite SPECK security services for air interface communications

Technologies de l'information — Techniques automatiques d'identification et de capture de données —

Partie 22: Services de sécurité par suite cryptographique SPECK pour communications par interface radio

Reference number
ISO/IEC 29167-22:2018(E)

© ISO/IEC 2018

NIST lightweight crypto standardization process

- First Lightweight Cryptography Workshop at NIST, July 20-21, 2015
- Second Lightweight Cryptography Workshop at NIST, Oct 17-18, 2016
- Request for Nominations for Lightweight Cryptographic Algorithms, Aug 27, 2018
  - Submission deadline March 29, 2019
- NIST announces 56 candidates for Round 1, Apr 18, 2019
- NIST announces 32 candidates for Round 2, Aug 30, 2019
- Third Lightweight Cryptography Workshop at NIST, Nov 4-6, 2019

https://csrc.nist.gov/projects/lightweight-cryptography

National Institute of Standards and Technology
U.S. Department of Commerce

Bibliografia

NISTIR 8114: Report on Lightweight Cryptography, March 2017
https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf

SIMON and SPECK Ciphers for the IoT, July 2015
https://csrc.nist.gov/csrc/media/events/lightweight-cryptography-workshop-2015/documents/presentations/session1-shors.pdf

NIST Lightweight Cryptography
https://csrc.nist.gov/projects/lightweight-cryptography

Domande?