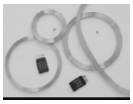
L'Autenticazione negli RFID

Giovanna Di Napoli	Giuseppina Elefante
Carmela Paolillo	Marco Volpe

Indice

RFID - Introduzione



La Radio Frequency Identification è una tecnologia che, sfruttando la radiofrequenza, permette l'identificazione (ossia il riconoscimento univoco) di un oggetto o di un essere vivente.

RFID - Funzionamento

• Alla base degli RFID ci sono i **tag**, detti anche **transponder**, ossia dei piccoli chip dotati di memoria e di un'antenna.

• Per leggere le informazioni contenute al loro interno si usano degli appositi lettori detti **reader.**

• Attraverso onde elettromagnetiche il reader comunica con il tag il quale, sfruttando l'energia ottenuta, restituisce al reader le informazioni volute.

RFID - Vantaggi

• I dati possono essere scambiati in entrambe le direzioni

• I tag sono resistenti agli agenti esterni e agli ambienti ostili

• Alcuni tag hanno una elevata capacità di memorizzazione

• La lettura può essere fatta a distanza entro un raggio d'azione che può variare da pochi centimetri ad alcuni metri

• Sui tag possono esserci dei sistemi di sicurezza (password e/o crittografia) che li proteggono da un uso malizioso

RFID – Storia – Anni 40

• I primi tag furono progettati per scopi militari in aiuto dei radar aerei.

• All'interno di una scatola sull'aereo vi era una ricetrasmittente (transponder) che rispondeva sulla stessa banda di frequenza del segnale radar.

• Il sistema era definito IFF (Identification Friend or Foe) e serviva per distinguere gli aerei amici da quelli nemici.

• Successivamente, al transponder venne associato un ID che permetteva di identificare quale fosse l'aereo amico.

RFID – Storia – Anni 50

• Inizia una forte sperimentazione in laboratorio ed una consistente ricerca di tipo teorico. R.F. Harrington è stato uno dei primi a studiare le capacità elettromagnetiche degli RFID

• Nascevano anche le prime società (Sensormatic, Checkpoint) che usavano la tecnologia RFID per sistemi di sorveglianza.

• Nascono i sistemi EAS (Electronic Article Surveillance) che usano tag di 1 bit per l'identificazione dei prodotti cosiddetti "taggati".

RFID – Storia – Anni 70

• Università e laboratori governativi intensificano la ricerca; i confini si allargano verso aree fino ad allora impensabili.

• Le nuove applicazioni miravano al riconoscimento di animali e veicoli, oltre all'automazione nel campo delle industrie.

• Veniva realizzata quella che, forse ancora oggi, è la più importante applicazione d'uso dei tag, ossia il pagamento elettronico dei pedaggi.

RFID – Storia – Anni 80 / 90

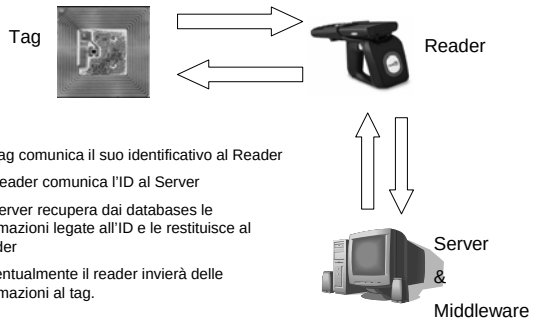
• Gli Stati Uniti diventano i maggiori produttori e consumatori di RFID.

• Le applicazioni RFID abbracciano ormai tutti i settori del commercio e dell'industria. Nasce la necessità di definire i primi standard di utilizzo.

• Nasce l'Auto-ID Center che raccoglie i più grandi ricercatori e studiosi del mondo RFID. Il suo scopo è quello di progettare l'infrastruttura e gli standard.

• L'EPCGlobal, nata da una costola dell'Auto-ID Center, ha il compito di interagire con utenti finali, produttori di hardware e software.

RFID – Elementi strutturali



• Il Tag comunica il suo identificativo al Reader

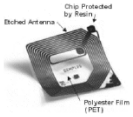
• Il Reader comunica l'ID al Server

• Il Server recupera dai databases le informazioni legate all'ID e le restituisce al Reader

• Eventualmente il reader invierà delle informazioni al tag.

RFID – Tag

• Un RFID tag consiste di un chip e di un'antenna. Un chip può conservare un numero seriale o altre informazioni.



• Il tag possiede una sua memoria interna tipo EEPROM. Il tipo di memoria identifica la modalità d'uso del tag.

• La dimensione dell'antenna limita il range di trasmissione e ricezione del tag

RFID – Tag Attivi

• Contengono una propria sorgente di alimentazione, di solito una batteria al litio.

• Possono avviare una comunicazione in quanto emettono continuamente un segnale

• Spesso hanno un elevato range di comunicazione (dieci o più metri)

• Hanno una memoria RAM interna piuttosto grande, dell'ordine di qualche KiloByte

• Hanno un costo che varia da 10 a 50 dollari, a seconda delle componenti.

RFID – Tag Passivi

• E' il tipo di transponder più diffuso. Non contiene alcuna batteria.

• Si alimenta tramite le onde elettromagnetiche che riceve dal reader.

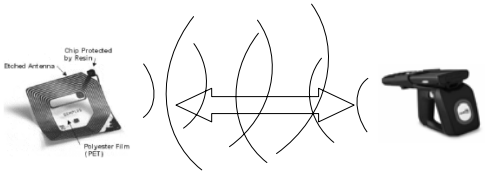
• Non può avviare una comunicazione ed ha un basso range di comunicazione.

• Per le tecnologie di cui dispone ha, in media, un costo inferiore al dollaro, in genere tra i 20 ed i 60 centesimi.

RFID – Tag SemiPassivi

• Hanno una batteria interna che permette loro di eseguire alcune operazioni (controllo potenza, operazioni logiche avanzate)

• Possono avviare una comunicazione con il reader oppure, nella maggior parte dei casi, essere silenti in attesa di un segnale



RFID – Tag - Modalità

Il tipo e la quantità di memoria contenuta ne definiscono la **modalità** di utilizzo:

Read Only
Il tag può essere interrogato in sola lettura. La capacità di memoria è minima. I tag passivi sono di solito read only

Read & Write
La memoria del tag può essere sia letta che scritta. La dimensione è dell'ordine di qualche KiloByte ed il loro costo è maggiore.

Write Once – Read Many
E' consentito scrivere all'interno del tag una sola volta, dopodichè la sua memoria è accessibile solo in lettura.

RFID – Tag - Classificazione

L'EPCGlobal Network, un'organizzazione dedita anche allo studio di applicazioni RFID, ha sviluppato una classificazione dei tag in base alle loro caratteristiche.

Classe	Caratteristiche
Classe 0	Tag passivi Read-Only
Classe I	Tag passivi con memoria utente e accesso con password
Classe II	Tag passivi ma con funzionalità aggiuntive (es. memoria secondaria, crittografia)
Classe III	Tag semi-passivi
Classe IV	Tag attivi

RFID – Tag – Frequenza di Banda

Intervallo	Raggio	Uso
125 – 134 kHz (LF)	Corto	Identificazione, Car Ignition
13.533 – 13.567 MHz (HF)	Corto/Medio	Smartcards, bibloteche
860 – 960 MHz (UHF)	Medio/Lungo	Supply Chain Tracking
2.400 – 2.483 GHz (VHF)	Lungo	Telepass

RFID – Reader

E' il dispositivo preposto sia alla lettura del tag che alla sua scrittura, ove questo sia possibile.

Il reader (anche "interrogator" o "lettore") si interfaccia anche con il database del sistema per recuperare le informazioni sul prodotto identificato dal tag.

RFID – Reader – Struttura

• ***Controller:*** è il cuore del reader. Gestisce la comunicazione con l'host. Traduce i comandi interni in segnali captabili dalle antenne dei tag.

• ***Network Interface:*** insieme di porte di comunicazione che permettono di collegare il reader all'host.

• ***Apparato ricetrasmettitore:*** permette di interfacciarsi in radiofrequenza con le antenne secondo una banda di frequenza prestabilita.

• ***Antenne:*** emettono fisicamente le onde elettromagnetiche captabili dai transponder. Nei reader più sofisticati vi possono essere più antenne ognuna adibita ad una particolare frequenza.

RFID – Reader – Tipologie

Non esiste una classificazione vera e propria dei reader. Tuttavia è possibile diversificarli in base alle componenti presenti al loro interno:

• ***Interfaccia di comunicazione***
Porte seriali: RS232
WireLan Ethernet: RJ 45
Wireless: WiFi, Bluetooth, ZigBee

• ***Frequenza di trasmissione-ricezione***
LF: Low Frequency, basso raggio d'azione
HF: High Frequency, medio raggio d'azione
UHF: Ultra High Frequency, elevata trasmissione
VHF: Very High Frequency, nell'ordine di GigaHertz

RFID – Reader – Tipologie

• ***Interfaccia di I/O***
Possibilità di collegarsi direttamente ad alcune periferiche quali **stampanti**, **altri lettori**, **sensori**, …

• ***Potenza di trasmissione***
Legata alla potenza effettivamente trasmissibile via radio. La limitazione viene posta, tra l'altro, anche dal paese in cui si opera e si va, in genere, da alcune **centinaia di mWatt** fino a oltre **4 Watt**.

RFID – Reader – Comunicazione

• Lo spazio in cui reader e tag possono comunicare è definito zona di interrogazione o "range".

• La comunicazione reader - tag deve essere libera da interferenze esterne che potrebbero alterare o anche annullare la connettività.

• All'interno di un range possono esistere più tag ma anche più reader. Per evitare sovrapposizioni di comunicazioni, occorre usare degli algoritmi di *anti-collisione*.

• Si acquisiscono i codici identificativi di tutti i tag presenti nel sistema e si fa in modo di organizzarli in maniera selettiva.

RFID – Tipologie di sistemi

A seconda della presenza di tag e reader in un ambiente, è possibile definire quattro tipologie di sistemi:

One-to-Many
Ossia un solo lettore per più tag (un piccolo negozio al dettaglio)

One-to-One
Un solo reader per un solo tag (la chiave di accensione di un'auto)

Many-to-One
Più reader per un solo tag (Telepass).

Many-to-Many
Più reader per più tag. (Biblioteche, magazzini, grandi negozi)

RFID – Applicazioni d'uso

Magazzini e punti vendita
Ogni prodotto è identificato univocamente da un tag, permettendo un miglior controllo delle merci e dei loro spostamenti.

Trasporti
I tag possono essere applicati anche sui mezzi di trasporto così come sul conducente. Altre applicazioni sono tag sui bagagli negli aeroporti o sulle chiavi di accensione delle auto

Tracciamento pratiche
Non molto in uso, ma nella burocrazia può aiutare ad automatizzare la ricerca in archivi cartacei e gestire meglio gli spostamenti delle pratiche dentro gli uffici.

RFID – Applicazioni d'uso

Biblioteche

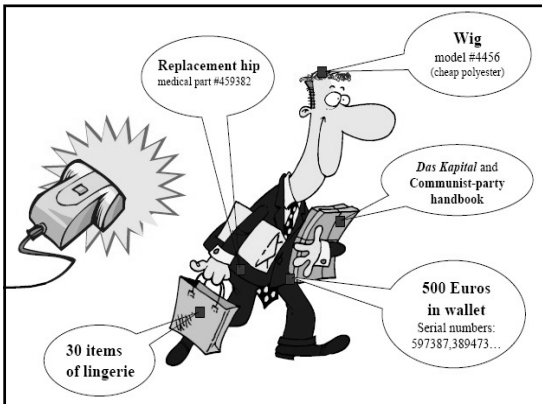
I tag sono posti su libri, video, CD, consentendo un controllo ed una gestione più accurata dei beni, sostituendo la lamina metallica che ne controlla solo l'eventuale uscita dalla biblioteca

Antitaccheggio

Una barriera posta all'uscita di un magazzino o di un negozio accerta che nessuna marce abbia varcato la soglia in maniera illecita.

RFID

Il Problema della Privacy



RFID – Il problema della Privacy

Ogni individuo in possesso di prodotti "taggati" rischia di essere anch'esso "taggato".

In base a ciò che possiede è possibile sapere:

- Dove si trova una persona in un dato momento (se è in prossimità di un reader)
- Quali sono le sue abitudini (cosa ha comprato)

In pratica è possibile tracciare una persona e controllarla come se avesse un occhio piazzato sopra di essa.

RFID – Il problema della Privacy

I sistemi RFID, originariamente, sono sistemi promiscui, cioè che rispondono a qualsiasi lettore tenti di interrogarli.

Le preoccupazioni principali riguardano la possibilità che la tecnologia possa essere utilizzata per violare la privacy del possessore degli oggetti "taggati"

In origine non c'erano grosse preoccupazioni da questo punto di vista. Ma la possibilità di crescita dei sistemi RFID pone tale problematiche al centro dell'attenzione.

RFID – Il problema della Privacy

Tutto questo non dovrebbe essere possibile, o quanto meno lo deve essere solo in determinate situazioni e attuabile solamente da agenzie di controllo o organi di legge

Per fare in modo che la privacy di una persona non venga lesa, occorre stabilire dei sistemi di sicurezza

RFID – Il problema della Privacy

Occorre dunque coinvolgere importanti considerazioni come *confidenzialità*, *integrita*, *disponibilità dei dati.*

Molte agenzie di controllo ritengono questi requisiti chiave per l'implementazione delle tecnologie RFID.

In particolare solo reader e personale autorizzati possono avere accesso alle informazioni contenute nei tag e nei database.

RFID – Il problema della Privacy

Ma tutto questo non basta. Esistono altri problemi legati agli attacchi che alcuni individui possono effettuare sui tag:

Counterfeiting
Falsificare o imitare un tag. Problema legato principalmente ai transponder posti sulle banconote.

Replay
Una trasmissione valida tra tag e reader viene ripetuta da un avversario che intercetta i dati e li ritrasmette.

Eavesdropping
Capacità di "origliare" una trasmissione tra tag e reader. Spesso è alla base del replay.

RFID – Privacy

Vi sono essenzialmente due grandi problemi da questo punto di vista:

• ***Tracking clandestino***, cioè la possibilità di seguire il segnale emesso da un tag e di collegarlo al suo possessore

• ***Inventorying***, cioè il riconoscimento di oggetti all'interno di uno store ottenibile tramite la lettura dei tag posti su di loro.

Il problema diventa sempre più serio quando le informazioni sui tag sono facilmente collegabili ai dati personali delle persone che li posseggono

RFID – Autenticazione

L'autenticazione nei sistemi RFID è il procedimento con il quale tag e reader dimostrano cioè di essere dispositivi legittimi.

Sorgono dei problemi quando reader legittimi vogliono raccogliere informazioni da tag non legittimi, in particolare da quelli contraffatti.

La duplicazione di dispositivi non protetti è piuttosto semplice e richiede di effettuare uno scanning del tag e poi di duplicarlo.

RFID – Autenticazione

Una soluzione per ridurre i rischi è quella di crittografare i dati nei tag, quelli che viaggiano nell'aria durante la trasmissione e quelli conservati nei tag.

L'approccio più generico e sicuro, però, è l'uso di protocolli standard di autenticazione già largamente usati nelle reti o nelle smart cards.

Tuttavia gran parte delle aziende preferiscono usare dei loro sistemi di autenticazione e non quelli consentiti dagli standard.

RFID – Scenari di Attacchi

Static Tag Data
Il tag emette un identificativo statico che non cambia mai (caso di molti tag attivi). Semplicemente tracciando quell'ID è possibile controllare l'oggetto o la persona proprietaria del tag.

No Access Control
Senza controllo degli accessi, un avversario può entrare in un sistema RFID, interrogare i tag e, usando dei meccanismi ausiliari quali ad esempio la videosorveglianza, legare più individui ad uno stesso tag.

RFID – Scenari di Attacchi

Write e Lock

- Il comando di "write" è un semplice bit che, se impostato ad '1', permette ad un reader di poter modificare la memoria del tag. Non è protetto da password
- Il comando di "lock" è anch'esso un bit che può assumere valore '0' o '1'. Se attivo, impedisce ad un reader di poter alterare la memoria del tag. È protetto da password a 48-bit

Tali comandi offrono protezione limitata. Un avversario potrebbe comunque alterare le informazioni dei tag.

Questo porterebbe ad avere un sistema RFID instabile ed inconsistente.

RFID – Scenari di Attacchi

Tag Password Management

Per un sistema RFID con molti tag esistono due approcci di gestione delle password:

1. Una sola password per blocchi di tag
2. Una password per ogni tag

Nel primo caso, la violazione della password comprometterebbe l'intero sistema. Pertanto occorre una modifica continua della password

Il secondo caso, invece, è più sicuro, ma costringerebbe il sistema a dover disporre di un meccanismo di selezione della password.

RFID

Tecniche di Autenticazione

RFID – Tecniche di autenticazione

Sono tre studi su tag RFID che utilizzano dei metodi avanzati di autenticazione:

1. La prima è una tecnica di crittografia poco espansiva, definita, minimalista, applicata su tag Low-Cost
2. La seconda è una tecnica di riconoscimento basata sul prodotto tra matrici
3. Il terzo studio è un'analisi di sicurezza eseguita su di un tag passivo avente al suo interno un sistema di cifratura privato.

RFID – Crittografia minimalista

Implementabile su tag di basso costo i quali hanno una memoria Read&Write.

Lo schema si basa sullo *Pseudonym throttling* in cui tag e reader conservano una lista di identificatori, o pseudonimi, che vengono utilizzati come chiavi di autenticazione.

Con il termine "Minimalista" si intende l'uso di operazioni crittografiche estremamente semplici, quali XOR Esclusivo e comparazione di stringhe, tali da non richiedere grossi sforzi computazionali



RFID – Crittografia minimalista

Il protocollo è basato su una mutua autenticazione. Vi sono tre liste di pseudonimi, $\{\alpha\}, \{\beta\}, \{\gamma\}$, che hanno dei compiti ben definiti:

- Ogni elemento di $\{\alpha\}$ serve ad avviare la procedura. Lo pseudonimo , selezionato dal tag ed inviato al reader, non ha valore di autenticazione, ma permetterà alle parti di decidere quali altri valori scegliere dai restanti due insiemi per completare la procedura.
- Ogni elemento di $\{\beta\}$ serve ad autenticare il reader al tag
- Infine ogni elemento di $\{\gamma\}$ serve ad autenticare il tag al reader.

RFID – Crittografia minimalista

Il sistema sembra semplice, ma per essere efficiente occorre che i valori che tag e reader trasmettono non siano sempre gli stessi.

Per risolvere il problema, i valori di α_i, β_i e γ_i vengono aggiornati usando delle chiavi one-time pad che il reader crea e trasmette al tag attraverso più sessioni di autenticazione.

Un avversario che ascolta una sola sessione di autenticazione, non sa quali possano essere i nuovi valori aggiornati di α_i, β_i e γ_i

RFID – Crittografia minimalista

Sia $k \in \{\alpha\} \cup \{\beta\} \cup \{\gamma\}$ un valore mantenuto all'interno del tag ed usato nell'ultima sessione. Consideriamo ora un parametro *m* ed un insieme di one-time pads: $\Delta_k = \{\delta_k^{(1)}, \delta_k^{(2)}, ..., \delta_k^{(m)}\}$ che tag e reader condividono

Il pad $\delta_k^{(1)}$ viene chiamato ***live pad*** e servirà ad aggiornare il valore di k
Cioè: $k \leftarrow k \oplus \delta_k^{(1)}$

Resta da vedere ora come viene aggiornato il vettore dei one-time pad attraverso le varie sessioni di autenticazione

RFID – Crittografia minimalista

Ad avvenuta autenticazione, il reader invia un vettore di nuovi pad generati casualmente: $\tilde{\Delta}_k = \{\tilde{\delta}_k^{(1)}, \tilde{\delta}_k^{(2)}, ..., \tilde{\delta}_k^{(m)}\}$

Nel vettore Δ_k il pad $\delta_k^{(1)}$ viene scartato. I restanti vengono spostati a sinistra di una posizione, mentre l'ultimo pad $\delta_k^{(m)}$ diventa una sequenza di zeri.

Infine si sovrascrive il vettore Δ_k con quello nuovo eseguendo degli XOR: $\delta_k^{(i)} = \delta_k^{(i)} \oplus \tilde{\delta}_k^{(i)}$, con 1 < i < m, operazione che un tag può eseguire senza problemi.

RFID – Crittografia minimalista

Il protocollo di autenticazione funziona in questo modo:

1. Il tag invia al reader il valore α_i
2. Una volta ricevuto α_i il reader verifica se lo pseudonimo è riferito a qualche tag. Se così, invia al tag il corrispondente valore di β_i per autenticarsi.
3. Il tag, a sua volta, per autenticarsi, manderà al reader la sua chiave di autenticazione γ_i, legata ai valori α_i e β_i
4. Ora che il processo di autenticazione è terminato, il reader genererà i nuovi one-time padding data da mandare al tag per l'aggiornamento dei suoi pseudonimi, eseguendo la procedura descritta precedentemente.

RFID – Crittografia minimalista

Tag		Reader
$d \leftarrow (c \bmod k) + 1$ $c \leftarrow c + 1$ $\alpha \leftarrow \alpha_d$	$\xrightarrow{\alpha'}$	Se è un valido pseudonimo per un dato tag T_x, allora: $i \in \{1,2,...k\}$ Seleziona un α non è piu valido *tag* $\leftarrow x$ $\beta' \leftarrow \beta_i$ $\gamma \leftarrow \gamma_i$ Altrimenti Autenticazione fallita
Se $\beta' \neq \beta_d$ allora Autenticazione fallita Altrimenti $\gamma' = \gamma_d$	$\xleftarrow{\beta'}$ $\xrightarrow{\gamma'}$	Se $\gamma' \neq \gamma$ o $\gamma' = \perp$ allora Autenticazione fallita Altrimenti Genera il nuovo insieme di pad $\tilde{\Delta}_k$ **Autenticazione Riuscita**
Aggiorna $(\Delta_k, \tilde{\Delta}_k)$ $\forall \kappa \in \{\alpha\}\{\beta\}\{\gamma\}$ $\kappa \leftarrow \kappa \oplus livepad(\Delta_k)$ $\forall \kappa \in \{\alpha\}\{\beta\}\{\gamma\}$	$\xleftarrow{\tilde{\Delta}_k}$	Aggiorna $(\Delta_k, \tilde{\Delta}_k)$ $\forall \kappa \in \{\alpha\}\{\beta\}\{\gamma\}$ $\kappa \leftarrow \kappa \oplus livepad(\Delta_k)$ $\forall \kappa \in \{\alpha\}\{\beta\}\{\gamma\}$

RFID – Crittografia minimalista

Il sistema è efficiente, ma ha alcune pecche.

Ogni comunicazione richiede la trasmissione di *3kl* bit, dove *l* è la lunghezza dei pad e *k* è il numero di pseudonimi.

Un attaccante capace di inserirsi nell'ultima fase del protocollo e di inviare falsi one-time pad al tag, potrebbe causare un Denial of service.

Infine, quando uno pseudonimo α_i viene usato, questi viene scartato e non più utilizzabile. Un successivo invio di α_i al reader renderebbe il tag inoperabile.

RFID – Tag senza Crittografia Estensiva

Il processo di autenticazione in questo protocollo non usa algoritmi o sistemi crittografici, ma semplici operazioni di **prodotti tra matrici**.

In un sistema RFID, ogni tag memorizza una coppia di matrici quadrate M_1 e M_2^{-1} di dimensione *p* x *p*.

Il reader mantiene le inverse di queste due matrici: M_2 e M_1^{-1}

Inoltre tag e reader condividono una chiave **K** di dimensione *rp* dove *r* è un fattore intero (generalmente indica il numero di tag presenti nel sistema).

RFID – Tag senza Crittografia Estensiva

La chiave **K** deve essere scelta in modo che il prodotto $X = K_i M_1$ sia unico per ogni 1< *i* < r.

Ad ogni sessione di autenticazione viene usata, da tag e reader, l'i-esima componente del vettore **K**, dove 1 < i < *r*.

$$M_1 \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix} \quad \text{X} \quad \begin{bmatrix} 0 & 1 & 0 & 1 \end{bmatrix} \quad K_i$$

RFID – Tag senza Crittografia Estensiva

Il processo di autenticazione viene avviato dal reader che invia un messaggio di "hello" al tag.

In questo messaggio è possibile che il reader indichi al tag quale delle r p-componenti di K selezionare. In ogni caso il tag selezionerà un 1 < *i* < r

Il tag, così, risponde inviando al reader: $X = K_i M_1$

RFID – Tag senza Crittografia Estensiva

Una volta inviato il vettore X, il tag avvia un timer alla fine del quale, se non avrà ricevuto alcuna risposta, bloccherà il processo.

Il reader riesce ad identificare il tag in base al vettore X calcolando $K_i = XM_1^{-1}$ A questo punto il reader genera una nuova chiave K_{new} sempre di lunghezza *p*.

Ora il reader computa due valori:

$Y = (K_1 \oplus K_1 \oplus ... \oplus K_r) M_2$

$Z = K_{new} M_2$

RFID – Tag senza Crittografia Estensiva

Nel momento in cui il tag riceve Y e Z, questi interrompe il suo timer, se non è già andato in timeout.

Il tag verificherà l'autenticità del reader eseguendo:

YM_2^{-1} per controllare l'esattezza di K

$K_{new} = ZM_2^{-1}$ per estrarre una nuova chiave da sostituire a K_i

RFID – Tag senza Crittografia Estensiva

Reader		**Tag**
Invia un messaggio di inizio sessione. Il messaggio potrebbe contenere il valore *i*.	hello, *i* →	Preso *i*, calcola: $X \leftarrow K_i M_1$ Avvia il timer
Identifica ed autentica il tag in base al valore di X Genera la nuova chiave K_{new} di taglia *p* Calcola: $Y \leftarrow (K_1 \oplus K_2 \oplus ... \oplus K_r) M_2$ $Z \leftarrow K_{new} M_2$	← X	
	Y, Z →	Ferma il timer Autentica il reader calcolando: $YM_2^{-1} = (K_1 \oplus K_2 \oplus ... \oplus K_r)$ Recupera la nuova chiave calcolando: $K_{new} \leftarrow ZM_2^{-1}$

RFID – Tag senza Crittografia Estensiva

La sicurezza del metodo sta nel riuscire a mantenere segrete le matrici e le loro inverse, viste che queste non vengono mai trasmesse.

Questo rende il protocollo sicuro ad attacchi *known-ciphertext*, il che è una buona garanzia per i sistemi RFID.

Un avversario non può nemmeno tracciare il tag in quanto non sa quale si stia autenticando al momento. Inoltre non può decodificare le comunicazioni (non conosce le matrici).

RFID – Analisi di Sicurezza di un DST

Il DST della Texas Instruments è un tag passivo inserito nelle chiavi di accensione delle auto come protezione dai furti.

È un tag al cui interno vi è un cipher la cui struttura completa non è mai stata resa nota, ma è stata in parte definita dal Dr. Ulrich Kaiser.

L'attacco mira al recupero della chiave crittografica contenuta nel cipher; per fare questo si è dovuto operare in due fasi:

1. Reverse Engineering: attraverso il quale si è cercato di recuperare la struttura completa del cipher

2. **KeyCracking**: si è attaccato il DST implementando il cipher recuperato in 16 FPGA (cluster riprogrammabili).

RFID – DST: Reverse Engineering

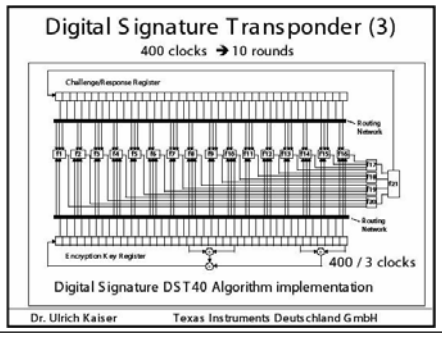
Il Kaiser cipher possiede due registri di 40-bit: uno per la chiave e l'altro per la challenge.

La funzione di crittografia, definita F, è formata da tre layer in ognuno dei quali sono presenti delle unità logiche chiamate **box**

L'output finale della funzione F occuperà i bit più a sinistra del registro di challenge.

Il DST come risposta alla challenge del reader, risponderà con i primi 24 bit del suo registro di challenge.

RFID – DST: Reverse Engineering



RFID – DST: Reverse Engineering

Vediamo ora come è costruita la funzione F

- Il primo layer contiene 16 box, chiamate ***f*-box**, ognuna delle quali prende tre bit dal registro di challenge e due da quello della chiave, o viceversa, e produce un solo bit di output
- Il secondo layer contiene quattro *f*-box, chiamate ***g*-box**, ognuna delle quali prende l'output di quattro *f*-box del primo layer e produce un bit.
- Il terzo layer è costituito da una solo *f*-box, chiamata ***h*-box**, che prende l'output delle *g*-box, e da in output due bit che saranno inseriti nelle posizioni più a sinistra dei bit di challenge.

RFID – DST: Reverse Engineering

Il DST40 è, in pratica un feedback shift register.

L'operazione di codifica avviene in più round: ad ogni round gli input del registro di challenge e della chiave passano attraverso le unità logiche.

L'output finale viene poi riportato (feedback) nel registro di challenge il quale viene spostato (shift) di determinati bit verso destra.

Inoltre, il registro della chiave viene aggiornato ciclicamente nel bit più significativo.

RFID – DST: Reverse Engineering

La fase di Reverse Engineering ha richiesto la realizzazione dei seguenti tasks:

- Determinare quanti bit costituiscono l'output della funzione F
- Individuare il Key Scheduling, ossia come e quando il registro della chiave viene aggiornato
- Individuare quali bit costituiscono gli input delle box
- Costruire le tabelle logiche per le box

RFID - DST RE: Output Funzione F

Lo studio sul DST è stato possibile utilizzando un kit di valutazione dello stesso in cui era possibile impostare alcuni parametri del tag

Si è iniziato con il fissare la chiave come una stringa di zeri, questo per annullare il key scheduling che secondo lo schema di Kaiser prevedeva delle operazioni di XOR

In questo modo è stato possibile rendere ogni ciclo di cifratura indipendente dall'altro.

RFID - DST RE: Output Funzione F

Data una challenge-response [C, R] del DST, il procedimento usato per determinare quanti fossero i bit di output di F è stato il seguente:

- Supposto che l'output di F fosse di un solo bit
- Sia C' il contenuto degli ultimi 39 bit del registro di challenge dopo una cifratura
- Il contenuto del registro di challenge poteva essere uno tra:

  $C_0 = 0 \mid C$

  $C_1 = 1 \mid C$

  dove | denota la concatenazione

RFID - DST RE: Output Funzione F

Se, ad esempio, C_0 fosse stato il valore "vero", allora la challenge-response [C_0, R_0] avrebbe avuto come risultato che $R_0 = R$, ma spostato di un bit in avanti

Usando questo test, applicato ogni volta su almeno due challenge-response, si è scoperto che l'output di F non era di un bit bensì di **due**.

Il passo successivo è stato quello di determinare il reale key scheduling.

RFID - DST RE: Key Scheduling

Il procedimento applicato in questa fase è identico a quello usato al passo precedente, ma stavolta applicato al registro della chiave.

Dallo schema di Kaiser si sapeva che la chiave veniva aggiornata ogni tre cicli, a partire dal secondo, eseguendo uno XOR tra alcuni bit del registro.

Eseguita una cifratura impostando una determinata chiave, veniva successivamente eseguita una secondo cifratura con una chiave aggiornata dopo sei cicli di cifratura.

RFID - DST RE: Key Scheduling

Eseguendo varie volte il test si è scoperto che la procedura di aggiornamento era la seguente:

- Ogni tre cicli di cifratura il registro della chiave viene spostato a destra di un bit.
- Il bit k_0 del registro della chiave veniva aggiornato calcolando:
  $k_0 = k_{39} \oplus k_{37} \oplus k_{20} \oplus k_{18}$

Dopo aver scoperto come vengono aggiornati i due registri, si passa a stabilire la rete di interconnessione del cipher

RFID - DST RE: Interconnessioni

C'erano due cose da stabilire per ogni box:

- Quali erano i bit di input
- Quali erano le funzioni booleane

La *h*-box è l'unica a produrre in output due bit e si sa che il suo input è dato dalle quattro *g*-box le quali, assieme alle *f*-box, producevano un solo bit di output.

Osservazione: l'alterazione di un bit di input alla *h*-box causava la produzione di al più due coppie distinte di valori

RFID - DST RE: Interconnessioni

Il test di esclusione per determinare quali gruppi di bit influissero sull'output delle quattro *g*-box era il seguente:

- Scegliere due bit appartenenti ai registri o di challenge o della chiave, diciamo b_1 e b_2, e di lasciare inalterati tutti gli altri bit
- Si controllava l'output della *h*-box per tutte le quattro possibili combinazioni di b_1 e b_2 e se ci fossero stati **più di due** differenti output, allora quei bit sicuramente non sarebbero stati connessi alla *g*-box

Tale test veniva eseguito per le altre *g*-box, dopo di che si passava alle *f*-box

RFID - DST RE: Interconnessioni

Sia B = $\{b_1, ..., b_5\}$ un insieme di cinque bit presi dai registri di challenge e della chiave (tre da uno e due dall'altro). Sia B' il set di tutti gli altri bit di quei registri.

Una *f*-box implementa una funzione booleana *z* su cinque bits di input.

Supponiamo che B sia l'input a questa *f*-box. Definiamo A_0 come il set di valori da assegnare ai bit in B tale che $z(b_1 \ldots b_5) = 0$, analogamente definiamo A_1 per $z(b_1 \ldots b_5) = 1$.

Osservazione: Fissato B, qualunque sia l'assegnamento dei valori di B', l'output della *f*-box non varierà mai.

RFID - DST RE: Interconnessioni

L'implementazione del test di esclusione è presto fatta.

- Si seleziona un set B di cinque bit per una data *f*-box.
- Successivamente si fissano tutti gli altri bit in B' nei registri di challenge e della chiave.
- Si itera su tutti i 32 possibili assegnamenti di B e si determinano A0 e A1 basandosi sull'output di h.
- Ora si cambia B'
- Se per tutti e 32 i tentativi i nuovi valori di A0 e A1 sono diversi, allora i bit scelti in B non sono quelli giusti per la f-box.

Si possono ora costruire le tabelle logiche per le varie box.

RFID - DST RE: Tabelle Logiche

Consideriamo una *f*-box. Preso il corrispondente set B e fissando i restanti bit in B', si itera per tutti i $2^5 = 32$ possibili valori di B.

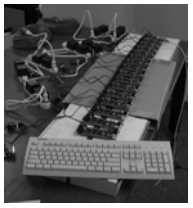
In questo modo la funzione F avrebbe prodotto due soli distinti output, uno di questi rappresentava il caso in cui la *f*-box produceva '0', e l'altro quando si aveva come output '1'.

In questo modo è stato possibile partizionare i 32 valori di input per B in due sottoinsiemi corrispondenti ai due possibili valori di output.

Lo stesso test viene eseguito anche per le *g*-box e per le *h*-box

RFID – DST: Key Cracker

Implementare il Key Cracker su software ed usando un cluster di 10 computer molto potenti avrebbe richiesto un tempo di ricerca di circa due settimane per scoprire la chiave giusta.



Per questo motivo si è reso necessario realizzare il cracker in Hardware usando degli FPGA, ossia dei circuiti programmabili, ognuno avente 32 core processors.

RFID – DST: Key Cracker

Si è utilizzato un array di 16 FPGA.

Il cracker agisce su due challenge-response. Se in un test si trova una corrispondenza con una coppia, lo si riesegue sulla successiva coppia.

Un solo FPGA trovava la chiave giusta in media dopo 12 ore. L'array di 16 FPGA riesce a recuperare cinque chiavi DST in meno di due ore.

RFID – Analisi di Sicurezza

Ovviamente il test eseguito mostra che la chiave di 40-bit non è sufficiente a proteggere il tag da attacchi.

C'è da considerare, però, che tale cipher è stato realizzato nel 1990, quando una chiave di tale dimensione forniva una buona sicurezza. E la struttura dei tag RFID non permette di avere capacità computazionali elevate.

Inoltre la struttura completa del cipher non è stata resa pubblica proprio per evitare che qualcuno potesse implementare in laboratorio l'intera procedura.

RFID

Protocolli Anti Collisione

RFID – Protocolli Anti Collisione

Si distinguono due grandi famiglie:

• ***Protocolli Deterministici***

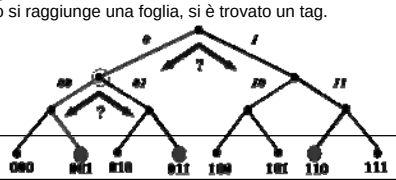
• ***Protocolli Probabilistici***

Esistono anche altri metodi realizzati da ricercatori e studiosi che fanno uso di tecniche crittografiche.

RFID – Protocolli Deterministici

Detti anche *Tree-Walking*

• Tutti gli ID statici dei tag di lunghezza fissa vengono organizzati in un albero di ricerca binario
• Un nodo alla profondità *d* è univocamente identificato dal prefisso $b_1b_2...b_d$
• Il reader inizia dalla radice ed esegue una visita in profondità. Al nodo $b_1b_2...b_d$ il reader interrogherà tutti i tag con quel prefisso
• I tag risponderanno con il *d*+1-esimo bit
• Quando si raggiunge una foglia, si è trovato un tag.



RFID – Silent Tree-Walking

• Per un avversario è più facile recuperare i segnali trasmessi dal reader al tag (forward range) che quelli dal tag al reader (backward range).

• Nel classico Tree-Walking è sufficiente che l'attaccante ascolti solo i segnali emessi dal reader per recuperare l'ID del tag.

• La versione **Silent** dell'algoritmo permette di nascondere ad estranei le informazioni trasmesse dal reader.

RFID – Silent Tree-Walking

• Due tag con lo stesso prefisso: $b_1 b_2$ e $b_1 \bar{b}_2$ condividono con il reader uno stesso segreto, ossia il loro prefisso b_1

• Quando il reader riceverà b_2 da un tag e $\bar{b}_2$ dall'altro, avrà una collisione.

• Per non svelare all'eavesdropper quale tag vuole identificare, il reader potrà mandare ai tag o $b_1 \oplus b_2$ o $b_1 \oplus \bar{b}_2$

• Di conseguenza un attaccante non saprà quale tag cercare perché solo nel backward range il tag invierà, in chiaro, il bit desiderato dal reader.

RFID – Protocolli Probabilistici

• L'accesso al canale di comunicazione è regolato da *time-slots*

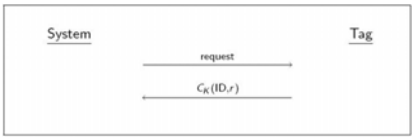
• Il reader decide il numero di slots da assegnare

• Ogni tag sceglie uno slot, occorre che vi siano almeno tanti slot quanti sono i tag, altrimenti si rischierebbero delle collisioni

• Il tag ha a disposizione un periodo di tempo per comunicare, dopodichè viene "zittito" dal reader il quale passa il controllo ad un altro tag.

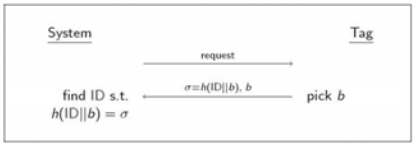
RFID – Altri Protocolli

Protocollo per Tag di Classe 1



• Il reader interroga il tag
• Il tag invia un'informazione al reader: il suo ID ed un valore *r* comune al reader, entrambi codificati secondo una chiave *K*
• Se il reader recupera *r*, ne fissa uno nuovo e lo comunica la tag
• Tag e reader possono dialogare

RFID – Altri Protocolli (Hash-Lock)



Noto anche come *Protocollo di Weis, Sarma, Rivest ed Engels*
• Il reader interroga il tag
• Il tag risponde con un valore pari all'hash del suo ID e di un valore *b* (o anche del solo valore *b*) che sia tag che reader dovrebbero sapere
• Il reader recupera il valore di *b* e lo restituisce al tag
• Questi accetta la comunicazione restituendo il proprio ID.

RFID

Applicazioni di Sicurezza

RFID – Applicazioni di Sicurezza

• Oltre ai protocolli di identificazione, occorre realizzare dei metodi che possano proteggere la comunicazione tra tag e reader

• Non esistono dei veri e propri standard, tuttavia ci sono alcuni algoritmi che hanno trovato un buon successo

• La maggior parte delle tecniche crittografiche usate sono di realizzazione privata, dunque non esiste una loro completa documentazione

RFID – Metodo Kill-tag

È il più semplice e diretto. Il tag viene ucciso e, dunque, le sue informazioni non possono più essere reperite.

Il comando “kill” avviene trasmettendo al tag una password di 8-bit che, una volta ricevuto, blocca **permanentemente** il transponder.

Questo garantisce soprattutto le persone dal fatto di non poter più essere tracciate, né di poter accedere a qualsivoglia informazione.

Tuttavia la lunghezza della password rende accessibile il tag ad un attacco a forza bruta che, con al più 256 tentativi, può riuscire a “spegnere” il tag.

RFID – Metodo Gabbia di Faraday

Il tag viene posto dentro un involucro metallico, composto per lo più da fogli di alluminio che avvolgono l’intero oggetto portatore del tag.

Il tag non può essere raggiunto da nessun contatto elettromagnetico. Dunque esso viene messo al sicuro da qualsiasi accesso, anche autorizzato.

Il metodo, nella sua praticità, si dimostra essere molto efficace verso tutti i tipi di attacchi, tranne verso l’antitaccheggio.

Ad esempio in un negozio un oggetto può essere posto dentro un sacchetto metallico per aggirare i lettori posti all’uscita.

RFID – Metodo Hash-Lock

Metodo che è alla base del protocollo, precedentemente mostrato, e realizzato da Weis, Sarma, Rivest ed Engels.

Permette di bloccare un tag in modo che esso si rifiuti di mostrare il proprio identificativo fino a quando un reader autorizzato non lo sblocchi.

Viene introdotto il concetto di **meta-ID**, l’hash di un valore numerico noto solo al sistema in cui agisce il tag.

Il **meta-ID** di ogni tag viene memorizzato in un database a cui può accedere solo un reader legittimo.

RFID – Metodo Hash-Lock

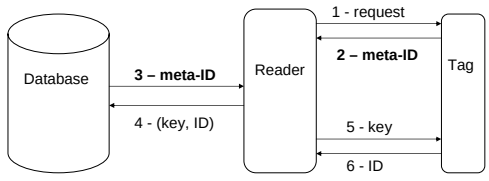
Il tag, ad ogni richiesta proveniente da un reader, risponderà sempre con il suo **meta-ID**.

Il reader legittimo invierà al database il **meta-ID** e questi gli fornirà la coppia formata dall’ID del tag e dal valore chiave.

RFID – Metodo Hash-Lock

Ora, il reader, per autenticarsi e per sbloccare il tag, invierà a questi il valore chiave.

Se è quello giusto, il tag si sbloccherà e gli invierà il suo ID che, se uguale a quello già in possesso del reader, permetterà alle parti di comunicare.



RFID – Metodo Hash-Lock

- Il metodo può rilevare eventuali tentativi di replay
- Un attaccante duplica il metaID di un tag, dopodichè lo invia ad un reader legittimo per l’identificazione.
- Il reader, tuttavia, non otterrà mai dall’attaccante il valore esatto dell’ID in quanto tale informazione non è stata recuperata.
- Resta però un ulteriore problema: il metaID di un tag può essere usato come identificativo alternativo per tracciare il comportamento del possessore del tag.
- Per evitare tale situazione, esiste una versione migliorata del metodo Hash-Lock chiamata **Randomized**

RFID – Metodo Randomized Hash-Lock

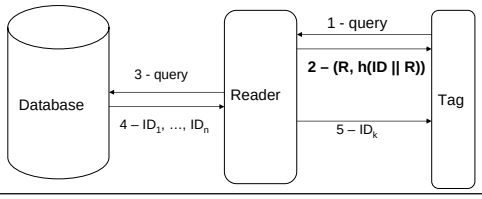
• All'interno del tag viene installato un generatore di numeri casuali che, ad ogni sessione di autenticazione, genera un valore R

• Il tag, poi, calcola l'hash del suo ID concatenato al valore R. Successivamente invia al reader la coppia (R, h(ID || R))

RFID – Metodo Randomized Hash-Lock

• Il reader ottiene dal database tutti gli ID del sistema e, per ognuno di questi, computa $h(ID_i || R)$, per tutti gli i possibili.

• Quando trova l'hash giusto, invia l'ID al tag, dimostrando la sua legittimità.



RFID – Metodo Randomized Hash-Lock

• Il metodo evita il problema della tracciabilità in quanto, ad ogni request, il tag invia una coppia (R, hash) diversa dalla precedente.

• Tuttavia sorgono due problemi: il primo è che tale metodo è utile per sistemi con un basso numero di tag in quanto, ad ogni request, il reader deve computare l'hash di tutti gli ID, operazione che può un tempo non indifferente.

• Inoltre, il metodo non prevede una mutua autenticazione visto che è solo il reader a legittimarsi, mentre il tag dà nessuna altra dimostrazione di sé.

RFID – Metodo Re-Encryption

• Questo metodo, realizzato da Juels e Pappu, prevede una cifratura a chiave pubblica dell'identificativo dei tag posti sulle banconote.

• Il sistema prevede la presenza di una coppia di chiavi, una pubblica PK e l'altra privata SK, stabilita dagli organi di legge.

• All'atto della distribuzione, l'ID del tag viene codificato con la chiave pubblica PK. Il nuovo valore può ora fungere da nuovo identificativo statico.

• Per evitare la tracciatura della banconota, lettori autorizzati possono re-codificare, usando PK, il valore presente sul tag.

RFID – Metodo Re-Encryption

• Solo agenzie governative di stato, in possesso della chiave privata SK, possono decodificare il valore presente sul tag.

• Questa possibilità permette solo ad agenzie autorizzate di tracciare i movimenti delle banconote e a nessun altro.

• Il livello di non tracciabilità delle banconote dipende esclusivamente dal tasso di re-cifratura dell'ID.

• Inoltre, i costi di installazione del cipher sul tag e l'utilizzo di lettori ottici potrebbero non essere indifferenti.

• Infine lettori non autorizzati potrebbero codificare il valore sul tag usando una coppia diversa di chiavi, rendendo la banconota irraggiungibile agli organi di controllo.

RFID – Metodo Active Jamming

Si utilizza un particolare dispositivo che emette interferenze elettromagnetiche volte ad annullare tutte le comunicazioni limitrofe.

Di conseguenza non può essere effettuata alcuna trasmissione da tag a reader e viceversa.

Tuttavia un'interferenza piuttosto elevata porterebbe alla rottura anche di altri sistemi RFID vicini, dove la segretezza non è una preoccupazione.

Per evitare tale problematica si utilizza il metodo del **blocker tag.**

RFID – Metodo Blocker Tag

Sviluppato da Ari Juels ed altri ricercatori RSA, permette di annullare la procedura di selezione tree-walking.

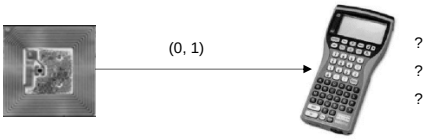
Un blocker tag è un normalissimo tag, ma che, interrogato dal reader, risponde in modo non standard, confondendo il lettore e bloccando la lettura di tutti gli altri tag.

I blocker tag vengono posti tra tag e reader o, comunque, in prossimità di uno dei tag appartenenti ad un sistema RFID.

RFID – Metodo Blocker Tag

Il metodo funziona solo per protocolli deterministici tree-walking, mentre è inapplicabile in tutti gli altri casi.

Quando, durante la lettura, il reader si trova ad aver letto fino ad un nodo B, il blocker tag, interrogato, trasmette contemporaneamente sia il bit '0' che il bit '1'.



RFID – Metodo Blocker Tag

Questa situazione induce il reader ad esplorare non un solo sottoalbero, ma entrambi.

L'ID di un tag, in genere, può essere di 64 o 128 bit, dunque l'albero può contare anche di 2^{128} foglie.

Un reader, per le sue caratteristiche, non è in grado di eseguire una ricerca così onerosa e, dunque, dopo un po' interrompe la ricerca.

Questo comportamento porta il blocker tag ad essere definito come **universal blocker tag**.

RFID – Metodo Blocker Tag

Per raffinare questa tecnica occorre considerare una proprietà dell'albero degli ID e cioè che tutti gli ID con lo stesso prefisso appartengono allo stesso sottoalbero.

In questo modo è possibile definire delle "**privacy zone**" all'interno delle quali può operare il blocker tag.

In pratica il blocker tag arresterà i processi di selezione solo per i tag che iniziano con un dato prefisso, per tutti gli altri prefissi il processo non si arresterà.

Un blocker tag di questo tipo si chiama "**selective blocker tag**".

RFID – Bibliografia

[1]: **RFID**, da Wikipedia: the Free Enciclopedia

[2]: **What is RFID**, da RFID Journal,

[3]: **The History of RFID Technology**, da RFID Journal,

[4]: **RFID: Eoluzione della Supply Chain**, di Ing. Daniele Maso, Universita degli Studi di Padova, Dipartimento di Ingegneria dell'Informazione, Tesi di Laurea in Ingegneria Elettronica, da Wikipedia: the Free Enciclopedia,

[5]: **The Basic of RFID Technology**, da RFID Journal,

[6]: **RFID System Components and Costs**, da RFID Journal,

[7]: **Information Security: Radio Frequency Identification Technology in the Federal Government**, from GAO – Report to Congressional Requesters, May 2005,

RFID – Bibliografia

[8]: **Tag a radiofrequenza**: Tag Attivi e Passivi, da SoftWork,

[9]: **Applicazioni Tipiche RFID**, da SoftWork,

[10]: **L'architettura di rete EPC**, di Enrico Cerroni, da i-dome.com: Dove l'ICT trova risposte, 22-12-2004,

[11]: **The EPC Network**, Dr. Mark Harrison, Associate Director Auto-ID Labs,

[12]: **L'architettura Tecnologica EPCGlobal**, for INDICOD-ECR, 12-10-2005,

[13]: **RFID & The EPC Network**, Ricardo Labiaga, Staff Engineer Sun Microsystems, Inc, 13-04-2004

[14]: **RFID Security**, prof. Dr. Heiko Kopse e prof. Hartmut Pohl, Information Security Technical Report Vol. 9, N.4, 15-02-2005

RFID – Bibliografia

[15]: **Privacy and Security in Library RFID Issues**, **Practices, and Architectures**, David Molnar e David Wagner, ACM Computer and Communications Security (CCS), 03-05-2004,

[16]: **Contact-Less Specificity in Term of Security and RFID Security**, Gildas Avoine, EPFL Lausanne Switzerland, Smart University, Sophia-Antipolis, September 2005,

[17]: **Passive RFID Security**, Kevin Mahaffey, for BlackHat –digital self defense, Luglio 2005

[18]: **Protecting Consumer Privacy**, RSA-Laboratories,

[19]: **Low-Cost RFID Systems**: **Confronting Security and Privacy**, Damith C. Ranasinghe, Daniel W. Engels, Peter H. Cole, for Auto-ID Labs Research Workshop, September 2004,

RFID – Bibliografia

[20]: **Minimalist Cryptography for Low-Cost RFID Tag**, Ari Juels, for RSA-Laboratories, in C. Blundo, ed., Security of Communication Networks (SCN), 2004,

[21]: **Security Analysis of a Cryptographically-Enabled RFID Device**, Steve Bono, Matthew Green, Adam Stubblefield, Ari Juels, Avi Rubin, Michael Szydlo, in P. McDaniel, ed., USENIX Security '05, pp. 1-16, 28-01-2005,

[22]: **The Blocker Tag: Selective Blocking of RFID Tag for Consumer Privacy**, Ari Juels, Ronald L. Rivest, Michael Szydlo, in V. Atluri, ed. 8th ACM Conference on Computer and Communications Security, pp. 103-111. ACM Press. 2003

[23]: **RFID Security without Extensive Cryptography**, Sindhu Karthikeyan, Mikhail Nesterenko, Computer Science Department of Kent State University, per SASN (Security of Ad Hoc and Sensor Networks), 07-11-2005

RFID – Bibliografia

[24]: **RFID Security and Privacy: A research Survey**, di Ari Juels, Condensed version to appear in 2006 in the IEEE Journal on Selected Areas in Communication, 28-09-2005,

[25]: **RFID Identificazione automatica a RadioFrequenza: tecnologia ed impatto sulla privacy**, di Gianni Bianchini, Progetto Winston Smith, E-Privacy 04, August 2004,

[26]: **RFID Technology, di Enrico Cerroni**, da i-dome.com: Dove l'ICT trova risposte, 13-12-2004,

[27]: **A Simple EPC Enterprise Model**, Kin Seong Leong, Mun Leng Ng, Auto-ID Labs, School of Electrical & Electronic Engineering,Universiy of Adelaide, 2004,

[28]: **"Progetto RFID": sviluppo e implementazione di un sistema di identificazione a radiofrequenza**, di Chiara De Dominicis, Università degli Studi di Brescia, Tesi di Laurea in Ingegneria per l'Informazione, AA 2004/2005,

RFID – Bibliografia

[29]: **Working Document on data protection issues related to RFID Technology**, for Data Protection Working Party, 19-01-2005,

[30]: **RFID Security and Privacy**, Christopher Soghoian, for SPAR Lab Seminar, 11-02-2003,

[31]: **Universal Immobilizer Crypto Engine**, Ulrick Kaiser, per la Quarta Conferenza su Advanced Encryption Standard (AES), 2004,

[32]: **RFID Privacy: An overview of Problems and Proposed Solutions**, di Simson L. Garfinkel, Ari Juels e Ravi Pappu, Security & Privacy Magazine, IEEE Publication Date: May-June 2005 Volume: 3, Issue: 3 On page(s): 34- 43

[33]: **Identificazione RFID**: **opportunità e timori**, da NetworkWorld, 30-11-2004,

[34]: **La sicurezza negli RFID**, di Aniello Coppeto, Università di Milano - Bicocca, Dipartimento di informatica sistemistica e comunicazione, 25-04-2006,

RFID – Bibliografia

[35]: http://www.rfidanalysis.org

[36]: http://www.ti-rfid.org