LE CHIP CARD

Le chiavi elettroniche diventano sempre più difficili da espugnare, ma è grazie a una nuova tecnologia che si arriva alla sicurezza completa: le chip card infatti assicurano una completa inespugnabilità di quanto protetto

Paola Sbrana - 1ª parte

Recentemente, anche in Italia si vedono sempre più applicazioni delle cosiddette chip-card, ovvero di quelle schedine simili a una carta da visita con sopra un piccolo chip. Una fra le prime fu senza dubbio la security-card che veniva rilasciata in cambio di un abbonamento ad alcuni circuiti di ricezione satellitare, poi ne abbiamo trovate alcune nel settore bancario ed infine ne troviamo sempre più frequentemente nel campo della sicurezza.

Cercheremo, quindi, con una piccola serie di articoli dedicati, di rispondere ai tanti quesiti che queste carte fanno porre ai nostri lettori, spiegando dapprima che cosa sono, come si utilizzano e dove si trovano, per terminare con un circuito di chiave elettronica ed un piccolo terminale portatile per la programmazione di alcune di queste.

I modelli principali

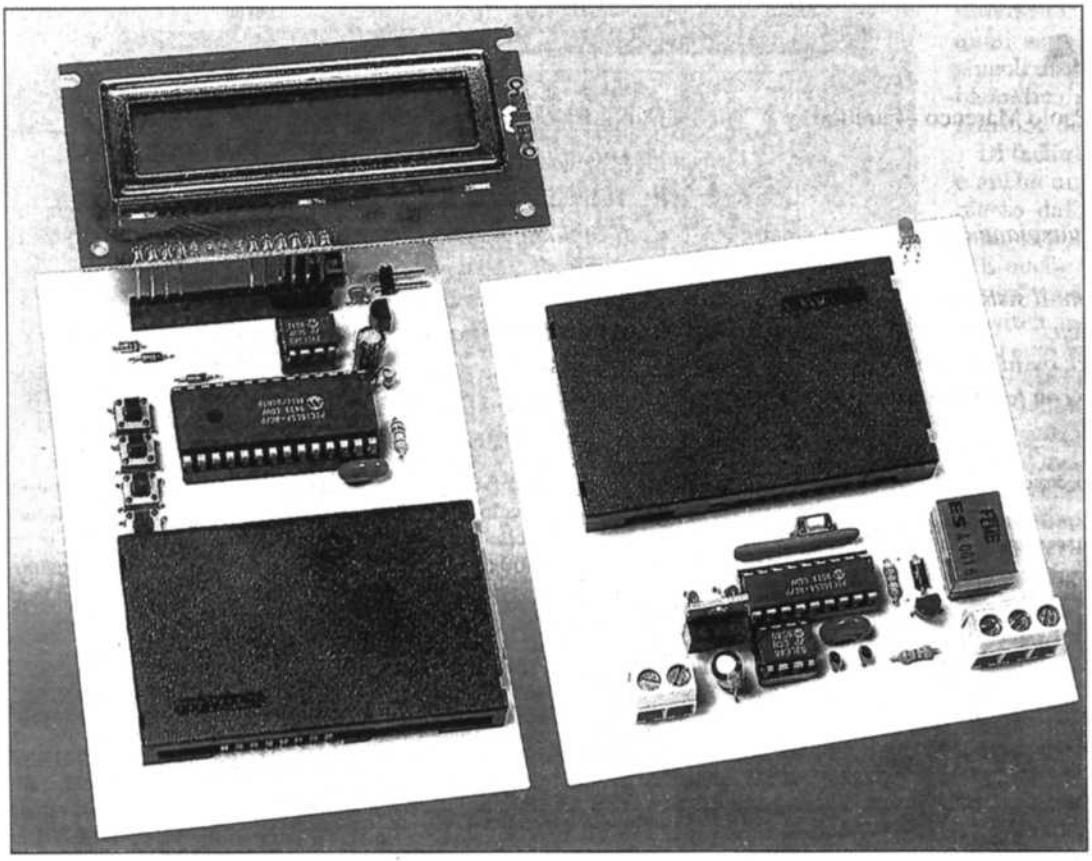
Prima di analizzare dettagliatamente il modello di carta che noi utilizzeremo, vediamo quante altre carte si trovano in commercio: innanzitutto, la prima distinzione che dobbiamo fare è la differenza tra una "vera" chip-card ed un'altra detta erroneamente chip-card, ma che non ha niente del chip inteso come circuito integrato. Esistono infatti carte che hanno al loro interno solamente memorie (di tipo PROM, EPROM o EEPROM, RAM), altre che abbinano alla memoria interna una "intelligenza" (periferiche di dialogo, contatori, PLD) ed infine altre che possiedono veri e propri microcontroller.

Le prime sono le più facili da trattare, ma anche le meno affidabili dal lato della sicurezza. Le altre invece vengono attualmente impiegate nei più svariati settori ed in special modo, le ultime sono prevalentemente sfruttate nel settore bancario.

Noi tratteremo le carte "intermedie", ovvero quelle che hanno al loro interno sia della memoria (di tipo prevalentemente EEPROM) sia alcune periferiche che le rendono intelligenti. Esistono molte carte appartenenti a questo segmento, con capacità di memoria da 256 byte a 8kb e con sistemi di accesso e di codifica da semplici a molto complessi.

Tanto per avere un'idea di che cosa troviamo sul mercato, diciamo che ci sono carte che vengono lette e scritte molte volte senza artifici particolari, mentre ce ne sono altre che possono essere sempre lette ma per essere riscritte è necessario eseguire una procedura iniziale abbastanza complessa con un codice di accesso (il classico PIN) preprogrammato. Dopo n tentativi di scrittura con codice errato, la carta si blocca e non permette più la riscrittura neanche con il codice corretto.

Ce ne sono, infine, alcune che necessitano del codice PIN anche per la sola lettura delle informazioni. Capite quindi quanto vasto sia questo settore e perché noi ci siamo dovuti orientare su di un solo tipo di queste carte, anche per consentire a tutti di comprendere bene il funzionamento e metterlo poi in pratica senza rischio di incomprensioni.



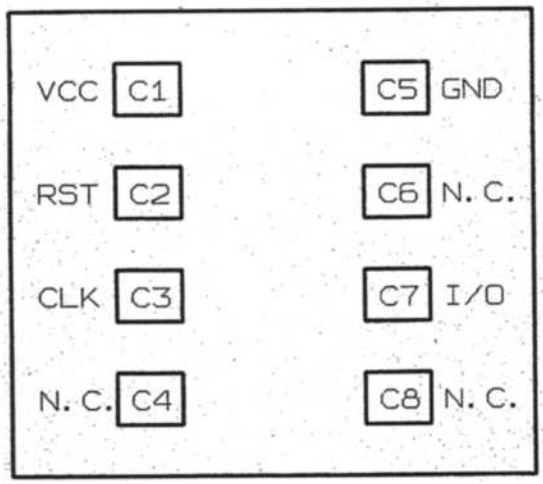


Figura 1. Piedinatura delle chip card SLE4432 e SLE4442

Le SLE4432 e 4443

Le carte che abbiamo individuato per i nostri scopi, sono le SLE4432 e SLE4442 della Siemens, gentilmente forniteci dalla Veron, una compagnia Olivetti Telemedia che si incarica di distribuirle in tutto il territorio nazionale.

Queste carte sono entrambe definite "intelligenti" in quanto hanno a bordo alcune periferiche e una di queste ha la protezione dalla scrittura non autorizzata. Le caratteristiche principali sono:

- Organizzazione di 256 x 8 byte in EEPROM.
- Indirizzamento diretto e sequenziale.
- Protezione irreversibile sulla scrittura dei primi 32 byte.

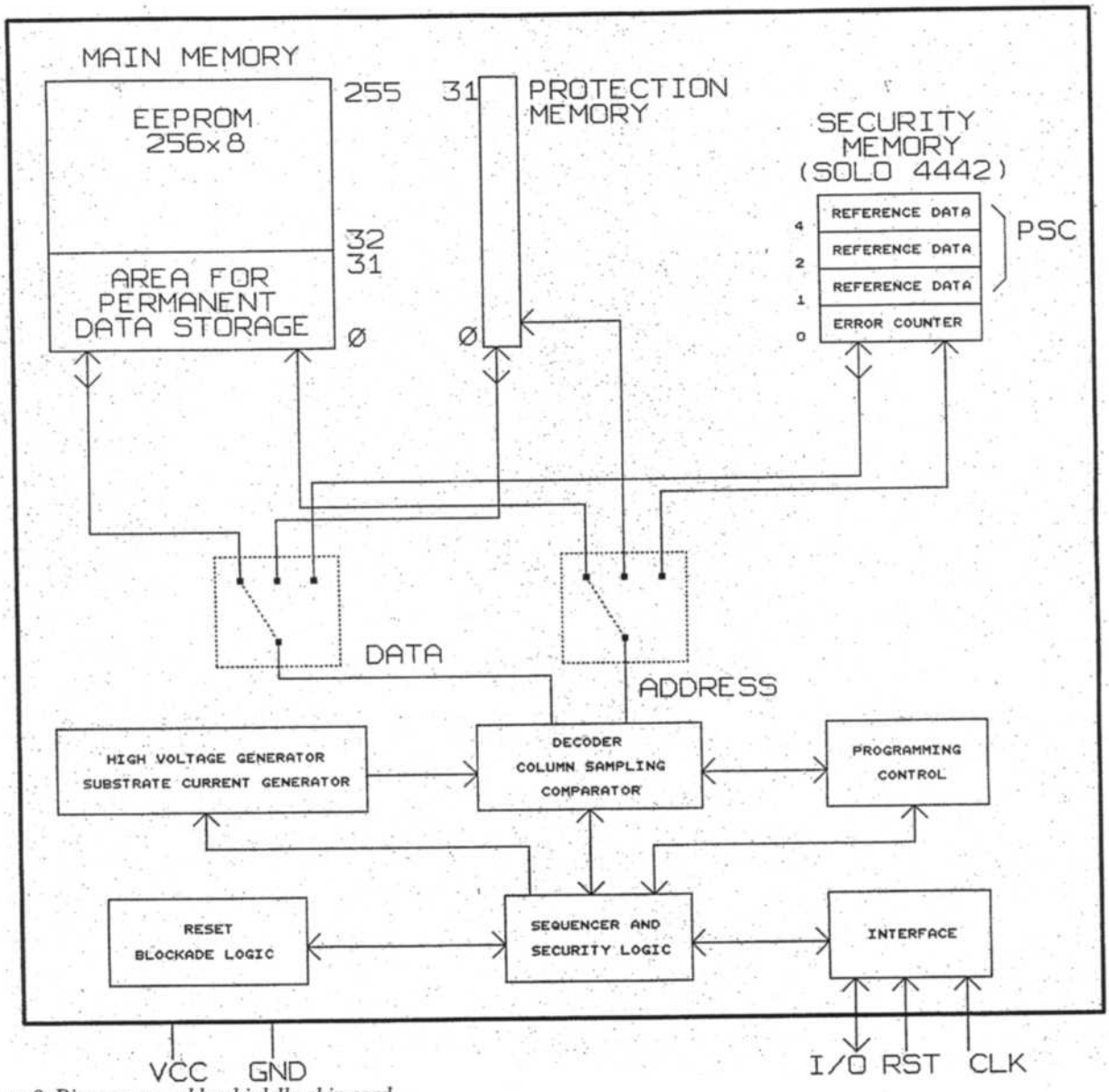


Figura 2. Diagramma a blocchi della chip-card

Figura 3. Schema di accesso alle due memorie

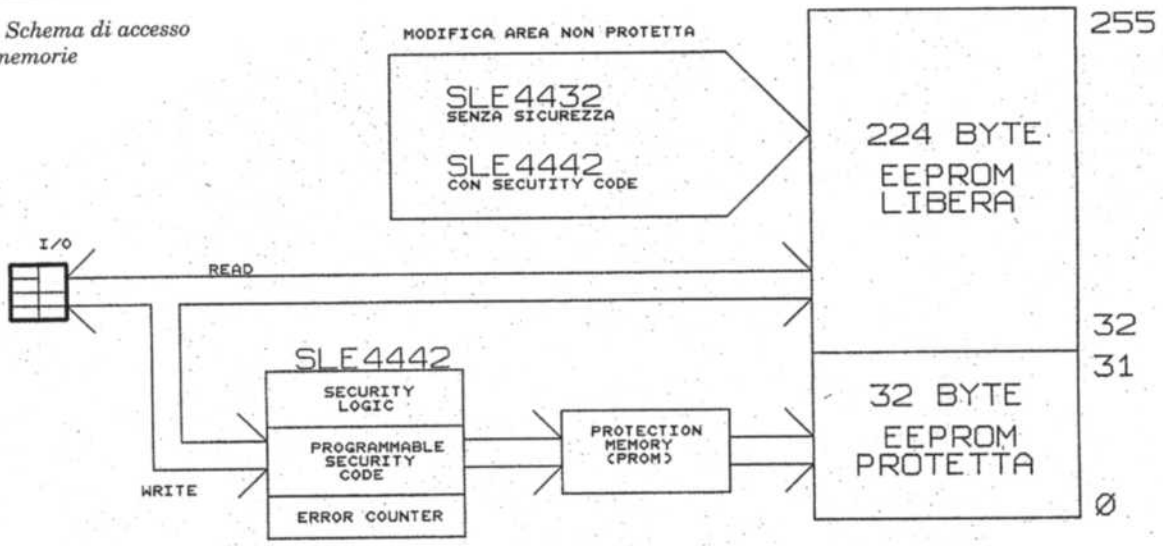
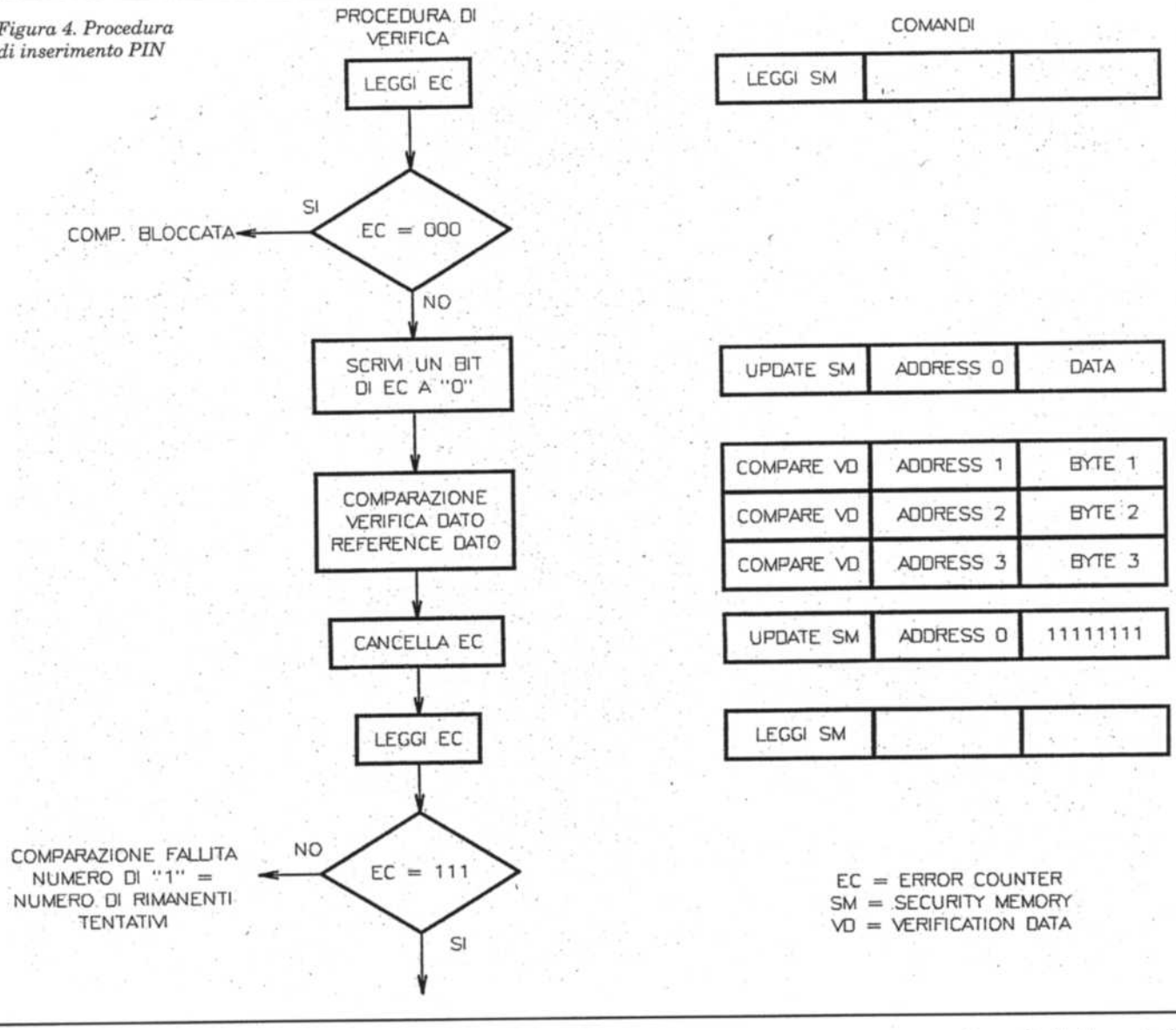


Figura 4. Procedura di inserimento PIN



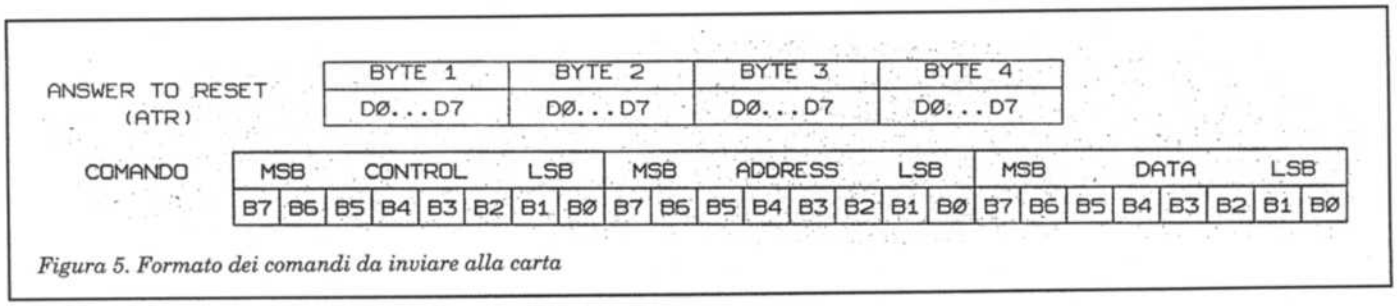


Figura 5. Formato dei comandi da inviare alla carta

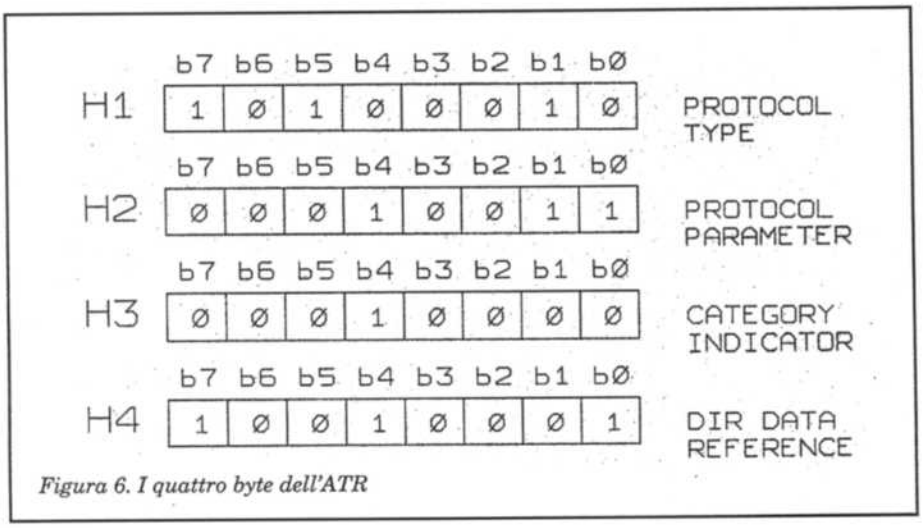


Figura 6. I quattro byte dell'ATR

- Protection memory di 32 byte.
- Protocollo a 2 fili (clock e dato).
- Fine delle operazioni indicato dalla carta.
- Answer-to-reset in accordo allo standard ISO 7816-3.
- Tempo di programmazione per byte: 5ms.
- Minimo numero di scritture: 10.000.
- Ritenzione dei dati per almeno 10 anni.
- Contatti e interfaccia seriale in accordo con lo standard ISO 7816 (trasmissione sincrona).
- Solo per la SLE4442: i dati possono essere variati solamente dopo i 3 byte del security code.

La nostra scelta di impiegare la serie SLE4432 è nata dal fatto che se è possibile leggere una carta è egualmente possibile copiarla, quindi non abbiamo ritenuto opportuno prendere in considerazione le SLE4442.

In accordo con lo standard ISO7816, in Figura 1 vediamo la piedinatura di tali carte. Il contatto C1 (VCC) deve essere connesso ad una tensione di alimentazione di 5 volt precisi.

Il contatto C2 (RST) corrisponde al terminale di reset. Il contatto C3 (CLK)e è la linea di clock e il contatto C7(I/O) quella dei dati.

Il C4, il C6 ed il C8 sono non connessi, mentre il contatto C5 (GND) è la massa.

Analizziamo ora lo schema a blocchi della chip-card aiutandoci con la Figura 2. Le linee di controllo entrano nel blocco INTERFACE e da qui vengono indirizzate ai vari blocchi interessati.

È presente un blocco di reset, uno per la generazione della tensione di programmazione della EEPROM, un controllore di programma, un decoder degli indirizzi ed infine l'area della memoria EEPROM.

Questa area è suddivisa in due blocchi funzionali:

- Il primo (dall'indirizzo 0 al 31 decimale) può essere protetto andando a scrivere sulla PROTECTION MEMORY, mentre sul secondo blocco (dall'indirizzo 32 al 255 decimale) è sempre possibile scrivere o leggere. Da notare che la PROTECTION MEMORY è di tipo PROM, quindi una volta scritta non potrà più essere riscritta, rendendo irrimediabilmente non riscrivibili anche i primi 32 byte della EEPROM. Questa la parte comune alle due carte SLE4432 e SLE4442.
- Ilsecondo, invece, ha in più il blocco detto SECUTITY MEMORY, ovvero un'area di 4 byte dove risiede un numero PIN di tre byte ed un contatore del numero di tentativi di accesso non permesso. Quando questo numero supero i tre consecutivi, la EEPROM non potrà più essere riscritta, ma soltanto letta. Si ricorda che l'inserimento del numero di PIN serve soltanto per l'accesso alla riscrittura della EEPROM e non alle operazioni di lettura.

In Figura 3 vediamo lo schema di accesso alle due memorie.

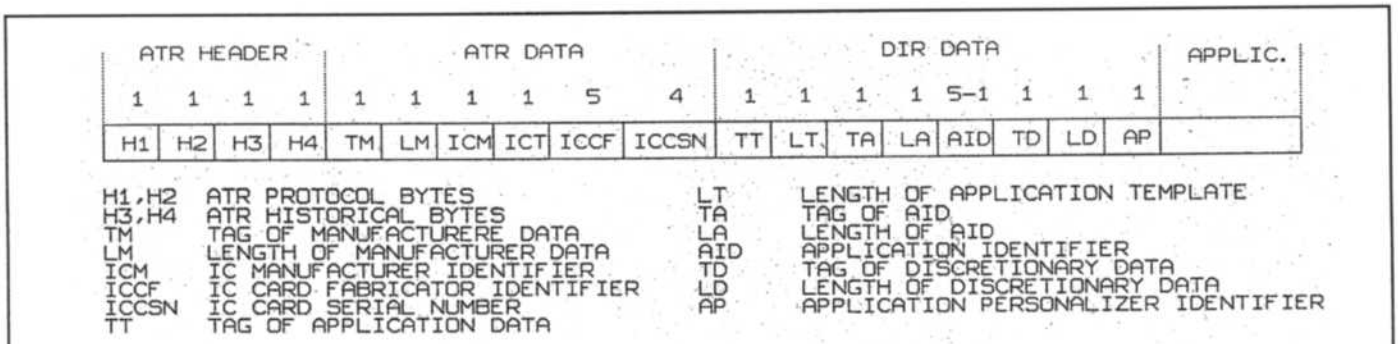


Figura 7. Informazioni contenute nei primi 32 byte

La procedura di verifica PIN

In Figura 4 abbiamo lo schema a blocchi della procedura per l'inserimento del PIN e la conseguente abilitazione della carta SLE4442 alla riscrittura: viene dapprima letto il contatore di errore, poi si va a vedere se questo è uguale a 000.

Se ciò accade, la comparazione è bloccata, viceversa si scrive a 0 un bit dell'error counter. Poi si passa alla comparazione dei tre byte del PIN e si cancella l'error counter. Infine, si legge nuovamente l'error counter e si vede se è uguale a 111. In caso positivo la comparazione è terminata positivamente, viceversa la carta rimane bloccata in riscrittura.

La procedura ATR

In accordo con lo standard ISO7816, le due carte, ad un ben preciso segnale di reset, "rispondono" quattro byte tramite la procedura detta Answer-To-Reset.

In Figura 5 troviamo i quattro byte inviati dalla carta all'ATR ed il formato tipico dei comandi che la carta si aspetta dopo un ATR: i primi otto bit detti CONTROL BYTE identificano il comando vero e proprio che la carta dovrà eseguire, il secondo byte detto ADDRESS BYTE indica l'indirizzo della locazione di memoria dove eseguire il comando ricevuto ed il terzo byte, detto DATA BYTE, consente il passaggio dei dati inerenti la locazione precedentemente indicata.

Tutti i byte sono inviati a partire dal bit meno significativo (LSB first).

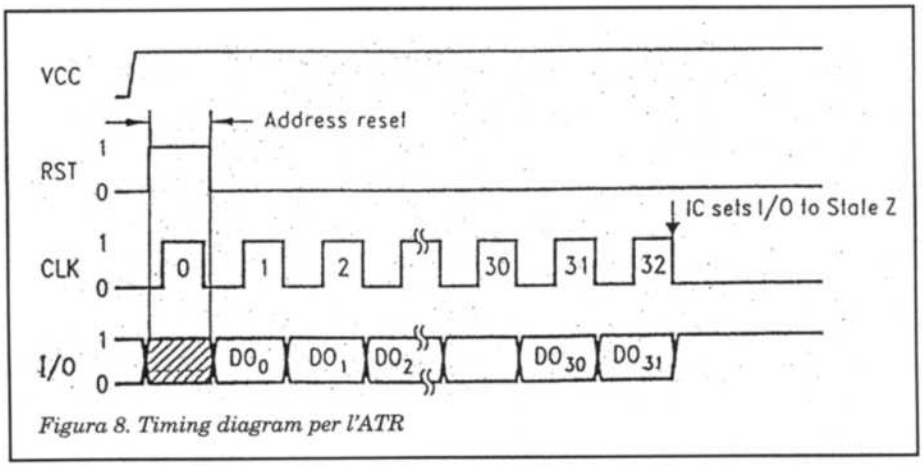


Figura 8. Timing diagram per l'ATR

In Figura 6 sono visibili i 4 byte dell'ATR: il primo (PROTOCOL TYPE) indica il tipo di protocollo impiegato, il secondo (PROTOCOL PARAMETER) indica i parametri per quel tipo di protocollo, il terzo (CATEGORY INDICATOR) indica la categoria di appartenenza ed il quarto (DIR DATA REFERENCE) ci da informazioni sui dati contenuti nella EEPROM.

In Figura 7, invece, vediamo come sono distribuite le informazioni nei primi 32 byte della memoria EEPROM.

Tutte queste informazioni, ricordiamo che sono proteggibili dalla riscrittura tramite la protezione della PROTECTION MEMORY, quindi per fare un esempio, un venditore di carte potrebbe inserire nei byte preposti il suo codice cliente e poi proteggere questa informazione da qualsiasi altra riscrittura (esempio data scadenza garanzia).

L'interfaccia con l'esterno

Per poter dialogare con il mondo esterno, queste carte necessitano di un'alimentazione a 5 volt (connettori VCC e GND), di un terminale di reset (RST), di un terminale di clock (CLK) e di uno per i dati (I/O). Il terminale di reset, viene per lo più usato solo nella fase iniziale di una transazione, per far partire la procedura ATR: in Figura 8 ne vediamo il timing diagram. A fronte di un impulso di reset lungo almeno la durata di un impulso di clock, la carta invia i 4 byte dell'ATR precedentemente visti, ovviamente sincronizzati con la linea del clock.

Una volta terminata la procedura ATR, la carta è pronta a ricevere comandi, nella forma vista prima. A ogni comando, come si vede chiaramente nella Figura 9, seguirà una risposta, sempre gestita dal segnale di clock.

Il prossimo mese vedremo un'applicazione pratica delle carte tipo SLE4432, realizzando una chiave elettronica con oltre 280 miliardi di combinazioni.

Le carte potranno essere acquistate sia vergini che già codificate.

Nel primo caso prossimamente presenteremo un programmatore per le sole SLE4432 della sola memoria EEPROM.

Si ringrazia la Veron Spa - Via Caldera, 21 - Milano per la collaborazione data nell'acquisizione delle informazioni citate. La Veron Spa è disponibile telefonicamente al numero 02/482151 per chiarimenti commerciali.

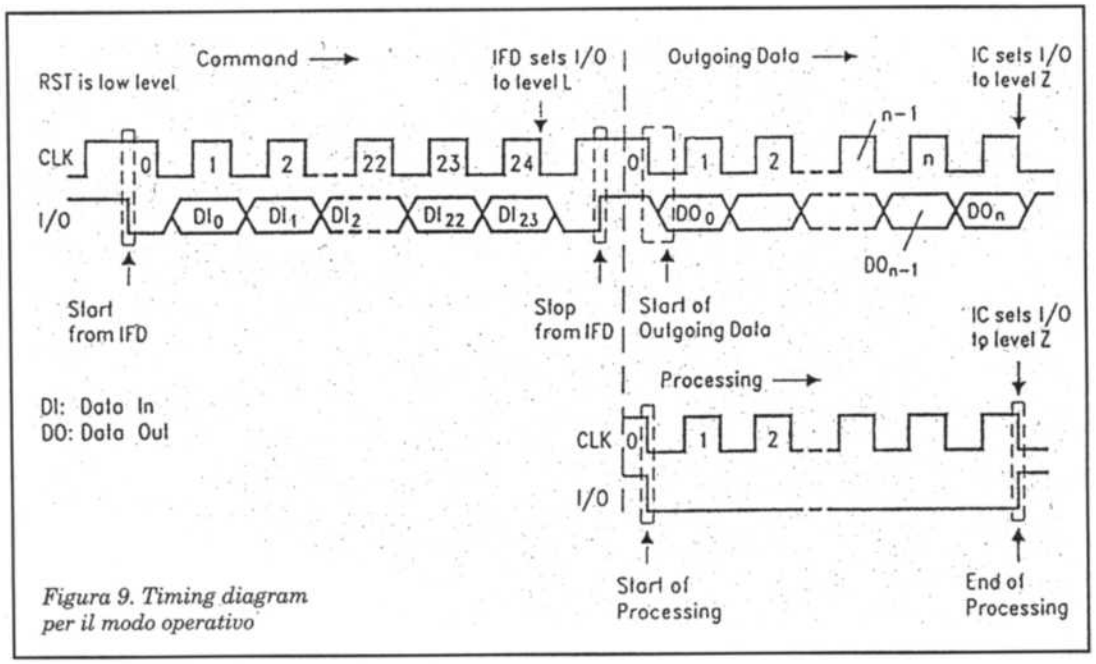


Figura 9. Timing diagram per il modo operativo

continua