

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.

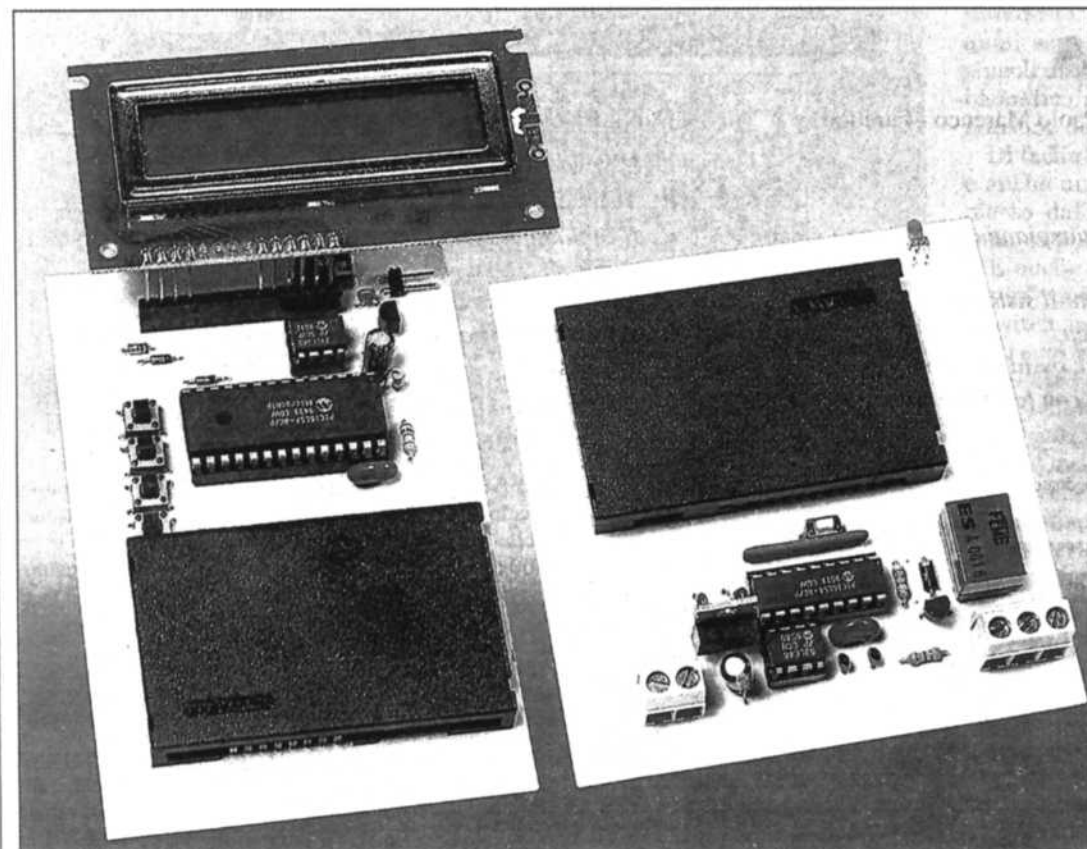
Le prime sono le più facili da trattare, ma anche le meno affidabili dal lato della sicurezza. Le altre invece vengono attualmente impiegate nei più svariati settori ed in special modo, le ultime sono prevalentemente sfruttate nel settore bancario.

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.



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 1.
Piedinatura
delle chip card
SLE4432
e SLE4442

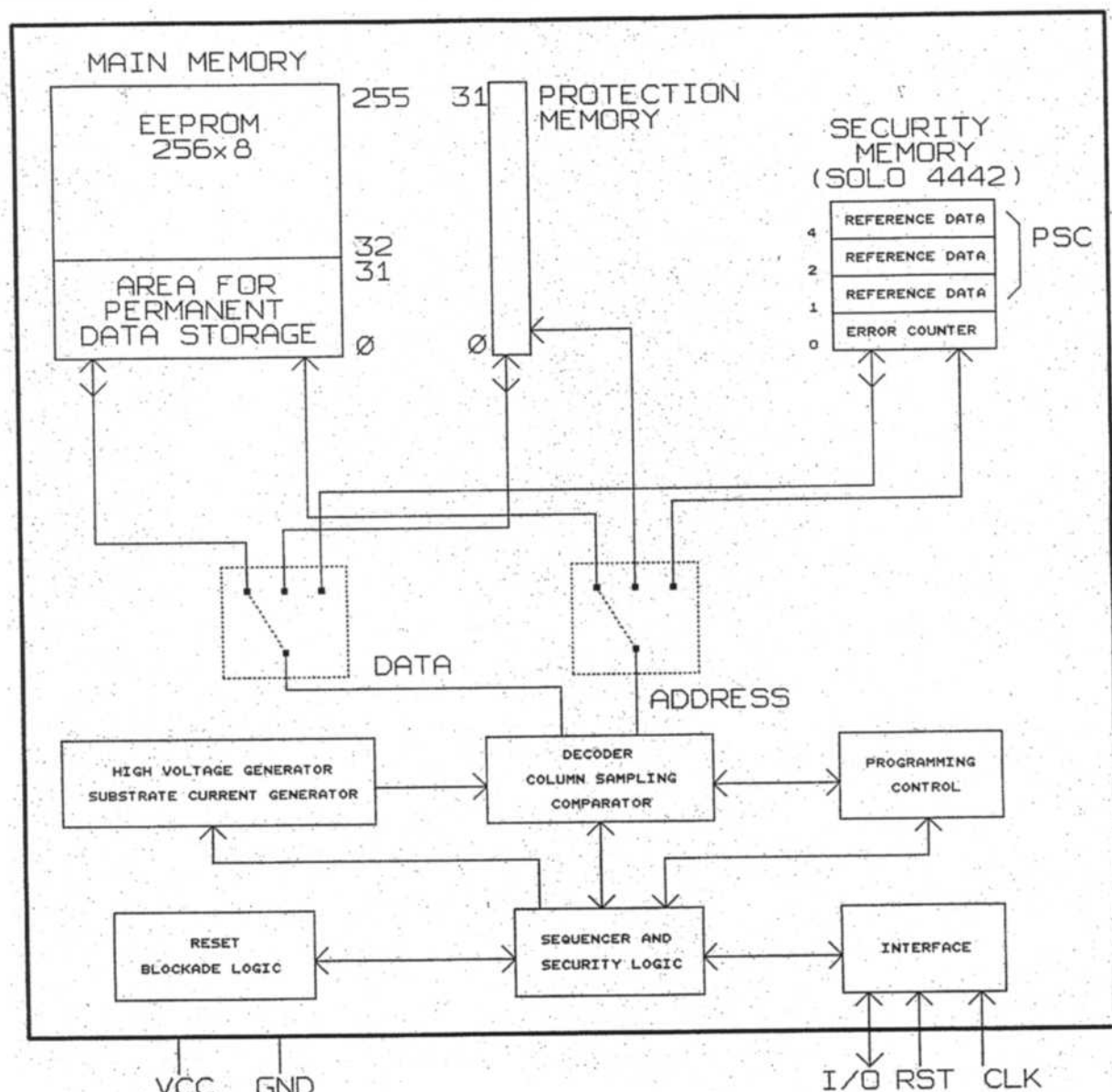
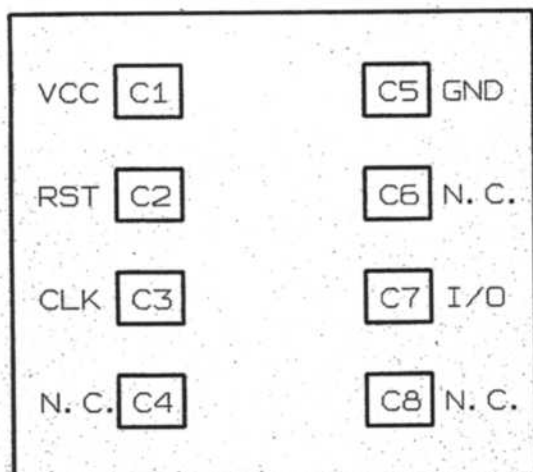


Figura 2. Diagramma a blocchi della chip-card

