Systemy identyfikacji bezstykowej, część 2

We współczesnym świecie coraz częściej zachodzi potrzeba identyfikacji osób oraz towarów. Przy stale rosnącej liczbie tych operacji oraz ciągle zwiększającym się wymaganiom co do bezpieczeństwa systemów identyfikacyjnych, przestają już wystarczać metody tradycyjne. Metody oparte na nalepkach z drukiem termicznym lub kodami kreskowymi (znakowanie towarów) oraz wszelkie inne oparte na hasłach, PIN–ach czy odręcznych podpisach muszą być zastąpione nośnikiem informacji bardziej odpornym na próby oszukania, bardziej niezawodnym, pozwalającym na odczyt i weryfikację informacji szybciej i z większą wiarygodnością.

Elementy

W ofercie firmy STMicroelectronics są dostępne dwie rodziny elementów do systemów identyfikacji bezstykowej: krótkiego zasięgu oraz dalekiego zasięgu. W pierwszej grupie mamy następujące elementy:

- SR176,
- SRIX512,
- SRIX4K.

Cechą wspólną tych układów jest zgodność z normą ISO14443. Wszystkie dysponują jednym sposobem modulacji sygnału do i z karty. Jest to odpowiednio ASK 10% oraz BPSK na częstotliwości 847,5 kHz. Układy posiadają odpowiednio 176, 512 oraz 4096 bitów pamięci EEPROM. Za wyjątkiem układu SR176, pozostałe gwarantują milion cykli zapis/odczyt. Mapę pamięci SR176 pokazano na **rys. 7.** Pierwsze 4 bloki zawierają 64–ro bitowy identyfikator UID. Jest on nadawany przez producenta w trakcie testów finalnych. UID nie może być modyfikowany przez użytkownika. Następne 11 bloków zawiera pamięć E^2PROM z możliwością permanentnego zabezpieczenia przed modyfikacją. Ostatni blok zawiera rejestr kontrolny OTP LOCK_REG informujący o stanie zabezpieczenia wszystkich bloków oraz miejsce na 4–ro bitowy identyfikator nadawany w trakcie inicjalizacji karty po tym jak znajdzie się ona w zasięgu pola czytnika. Na **rys. 8** pokazano mapę pamięci SRIX4K. Pierwsze 5 bloków zawiera kasowalne pola binarne OTP.

W trakcie standardowego zapisu można jedynie zmienić ich stan z 1 na 0. Odwrotna operacja nie przynosi żadnego skutku. Zanim omówimy sposób kasowania bitów OTP przejdźmy do omówienia bloków 5 i 6. Zawierają one dwa niezależne 32–bitowe liczniki, które można jedynie dekrementować. Stanem końcowym jest stan, w którym wszystkie bity są skasowane (równe 0). Od tego momentu żaden rozkaz nie jest w sta-

Block Address	MSB b15	16-bit block b8 b7	LSB b0	Description
0	UID0			64-bit UID ROM
1	UID1			
2	UID2			
3	UID3			
4	User Area			Lockable EEPROM
5	User Area			
6	User Area			Lockable EEPROM
7	User Area			
8	User Area			Lockable EEPROM
9	User Area			
10	User Area			Lockable EEPROM
11	User Area			
12	User Area			Lockable EEPROM
13	User Area			
14	User Area			Lockable EEPROM
15	OTP_LOCK_REG	Reserved	Chip_ID	

Rys. 7. Mapa pamięci SR176

Block Address	MSB b31	b24 b23	32-bit block b16 b15	b8 b7	LSB b0	Description
0	32 bits Boolean Area					Resetable OTP bits
1	32 bits Boolean Area					
2	32 bits Boolean Area					
3	32 bits Boolean Area					
4	32 bits Boolean Area					
5	32 bits binary counter					Count down Counter
6	32 bits binary counter					
7	User Area					Lockable EEPROM
8	User Area					
9	User Area					
10	User Area					
11	User Area					
12	User Area					
13	User Area					
14	User Area					
15	User Area					
16	User Area					EEPROM
...	User Area					
127	User Area					

255	OTP_LOCK_REG	ST Reserved	Fixed Chip_ID (Option)	System OTP bits

UID0	64 bits UID Area	ROM
UID1		

Rys. 8. Mapa pamięci SRIX4K

nie zmienić ich wartości. Najstarsze 11 bitów licznika pod adresem 6 jest używane przy okazji jako *reload timer* do kasowania kasowalnych pól OTP. Jeśli którykolwiek z tych bitów zostanie zmieniony, to następna operacja zapisu bloku od 0 do 4 (kasowalnych pola OTP) zostanie poprzedzona skasowaniem zapisywanego pola. W takim przypadku jest możliwe przejście z 0 do 1. Ponieważ *reload timer* ma 11 bitów, to kasowalne pola OTP można kasować 2047 (2^{11}–1) razy. Bloki od 7 do 15 zawierają pamięć E^{2}PROM z możliwością trwałego zabezpieczenia przed modyfikacją (jak w SR176). Bloki od 16 do 127 zawierają zwykłą pamięć E^{2}PROM bez możliwości zabezpieczenia. Znaczenie pól systemowych oraz UID jest identyczne jak w SR176.

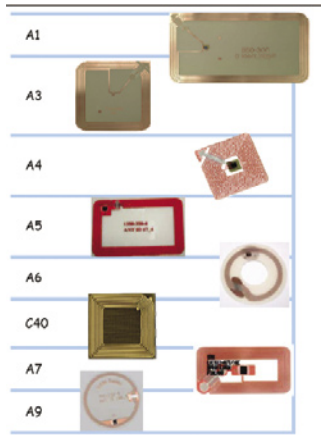
Element SRIX512 nie posiada pamięci pod adresami od 16 do 127. Pozostałe bloki mają takie samo znaczenie jak w SRIX4K. Identyfikator *Chip_ID* jest 8–bitowy i może być wpisany przez użytkownika.

W grupie elementów dalekiego zasięgu znajdują się dwa typy: LRI64 oraz LRI512. Obydwa elementy są zgodne z normą ISO 15693. Strukturę pamięci pierwszego z nich pokazano na **rys. 9**. Pierwsze 8 bloków zawiera 64–bitowy unikalny identyfikator. Jego najstarszy bajt zawsze jest równy 0xE0. Kolejny równy 0x02 identyfikuje producenta (STMicroelectronics). Po nich następuję unikalna 48–bitowa liczba. Rejestr AFI (*Application Family Identifier*) pod adresem 8 zawiera jednokrotnie zapisywalny przez użytkownika identyfikator aplikacji. Przykładowo AFI=0x50 oznacza aplikacje medyczne, 0xC0 – bilety bagażowe, itd. Bajt DSFID zawiera dodatkowe informacje na temat organizacji pamięci i może być wykorzystywany w trakcie inicjalizacji wielu kart w zasięgu czytnika. Bajty od 10 do 14 są przeznaczone dla użytkownika i mogą być jednokrotnie zapisane dowolną informacją. Po tej operacji zostają trwale zabezpieczone przed modyfikacją. Element LRI512 różni się od LRI64 wielkością pamięci przeznaczonej dla użytkownika oraz jej rodzajem. Tutaj dla użytkownika jest przeznaczone 16 bloków po 32 bity pamięci E^{2}PROM (100 kcykli zapis/odczyt). Każdy z nich może być permanentnie zabezpieczony przed modyfikacją. Rejestr DSFID nie występuje w tym elemencie.

Zarówno elementy SR jak i LR występują w kilku wariantach pakowania. Oczywiście dostępne są także bez obudowy, tzn.

Block Addr	0 1 2 3 4 5 6 7
0	UID 0
1	UID 1
2	UID 2
3	UID 3
4	UID 4
5	UID 5 = IC_ID
6	UID 6 = 02h
7	UID 7 = EOh
8	AFI (WORM Area)
9	DSFID (WORM Area)
10	WORM Area
11	WORM Area
12	WORM Area
13	WORM Area
14	WORM Area

Rys. 9. Mapa pamięci układu LRI64

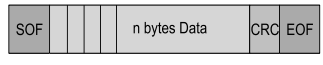


Rys. 10. Wygląd formatów kart

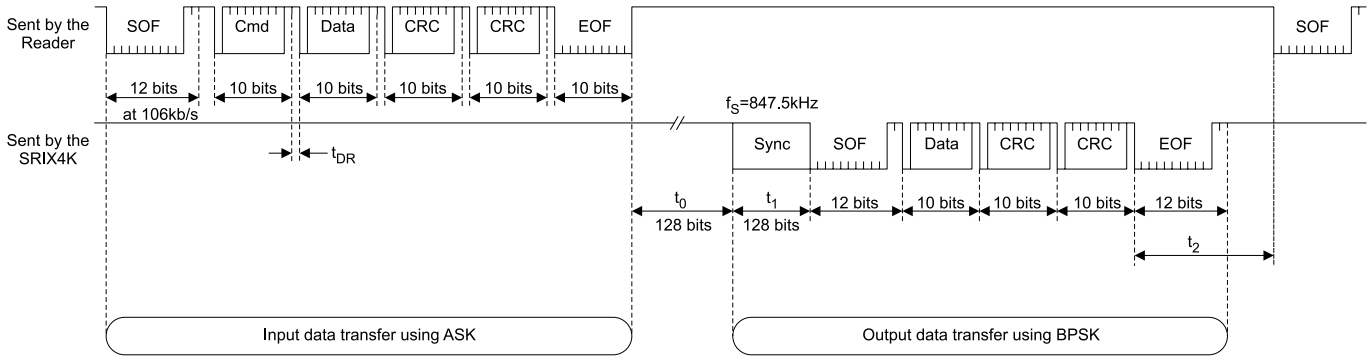
jako krążek krzemu ze strukturami (tzw. *wafer*). Struktury scalone razem z anteną (*inlay*) występują w 9 formatach:

- typ A1: 45x75mm (format karty kredytowej),
- typ A3: 38x38 mm,
- typ A4: 15x15mm,
- typ A5: 42x65 mm,
- typ A6: Ø35 mm (okrągły, dla elementów LR),
- typ C40: 28x28 mm (antena złocona),
- typ A7: 20x40 mm,
- typ A9: Ø35 mm (okrągły, dla elementów SR).

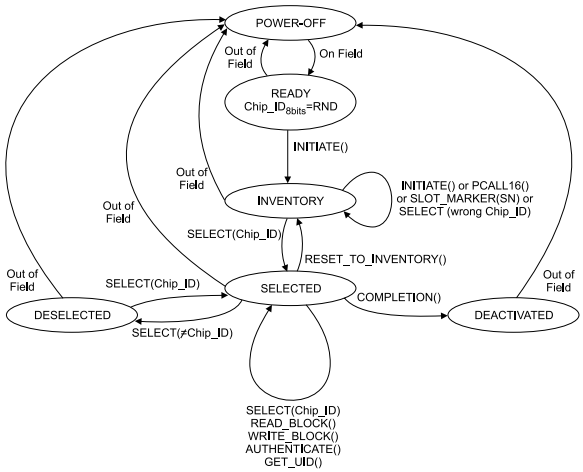
Dodatkowo elementy mogą występować na folii samoprzylepnej lub zwykłej



Rys. 11. Format ramki



Rys. 12. Kompletna transmisja do i z karty typu SR



Rys. 13. Graf działań karty SRIX4K

(do zalaminowania). Na **rys. 10** pokazano wygląd wymienionych formatów kart. Z przyczyn ekonomicznych nie wszystkie kombinacje elementów, formatów i typów folii są w danej chwili w produkcji.

Protokół komunikacji

Każda transmisja jest ograniczona znacznikami SOF – EOF. Kodowanie tych znaczników różni się w zależności od normy, a także może się różnić dla znaczników wysyłanych do i z karty. Znacznik SOF w przypadku kart LR zawiera także sposób kodowania ramki (1 z 4 lub 1 z 256).

Treść zawarta pomiędzy znacznikami SOF a EOF zależy od bardzo wielu parametrów, np. kierunku transmisji (do, czy z karty), rodzaju karty (SR czy LR), rodzaju komendy, itd. W każdym przypadku bity wysyłane są w kolejności od najmłodszego do najstarszego. Format ramki pokazano na **rys. 11**, a przebieg transmisji na przykładzie elementu SR – na **rys. 12**. W tabeli **tab. 3** zebrano komendy akceptowane przez karty LR. W **tab. 4** zebrano komendy akceptowane przez karty SR.

W celu wyjaśnienia sposobu działania karty na **rys. 13** zamieszczono graf działań dla karty SRIX4K. Stanem wyjściowym jest POWER–OFF (brak zasilania). Po pojawieniu się pola czytnika i krótkiej zwłoce na inicjalizację karta przechodzi do stanu READY. W tym stanie karta generuje losowy numer *Chip_ID*. Ponieważ jest to numer 8–bitowy, to teoretycznie w zasięgu czytnika może przebywać do 256 kart. Jednakże z uwagi na powtarzanie się numerów *Chip_ID*, realna wartość wynosi około 50. Dla porównania karty LRI posługują się 64 bitowym identyfikatorem UID i w związku z tym w zasięgu czytnika może przebywać do 2^{64} kart.

W stanie READY karta czeka na początek procedury *anti–collision*. Dokonywane jest to poprzez komendę INITIATE. Na skutek tej komendy karta generuje nowy *Chip_ID* i zwraca go. Takie rozwiązanie przyspiesza pracę, gdy tylko jedna karta jest w zasięgu czytnika. W takim przypadku po otrzymaniu nowego *Chip_ID* czytnik może od razu wykonać komendę SELECT i przełączyć kartę do trybu SELECTED. Gdy jednak w zasięgu czytnika znajduje się więcej kart, ich odpowiedzi nakładają się i powstaje kolizja. W tym momencie należy wysłać do kart komendę PCALL16. Powoduje ona wygenerowanie losowe nowej wartości dla najmłodszych 4 bitów *Chip_ID*. Starsza część pozostaje nie zmieniona. Te 4 młodsze bity nazywane są CHIP_SLOT_NUMBER.

Tab. 3. Komendy kart LR

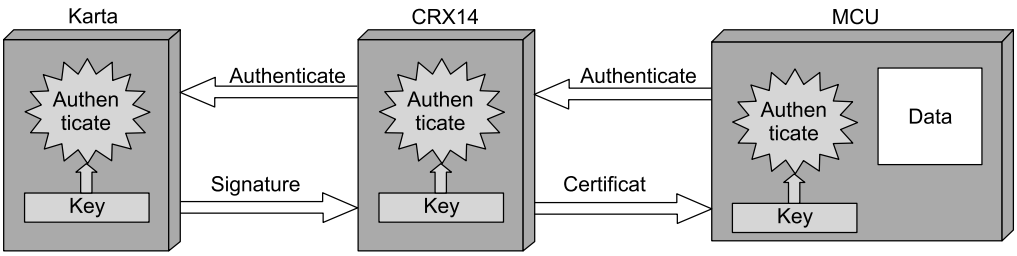
Polecenie	LRI512	LRI64	Opis
Inventory	+	+	Start procedury anti–collision*
Stay Quiet	+	+	Wejście w stan nieaktywny
Read Single Block	+	+	Odczyt bloku pamięci
Write Single Block	+	+	Zapis bloku pamięci
Lock Block	+		Zabezpieczenie bloku przez modyfikacją
Select	+		Wejście w stan SELECTED**
Reset to Ready	+		Powrót do stanu READY***
Write AFI	+		Zapis rejestru AFI
Lock AFI	+		Zabezpieczenie rejestru AFI przed modyfikacją
Activate EAS	+		Ustaw bit EAS****
De–activate EAS	+		Skasuj bit EAS
POOL EAS	+		Wszystkie karty z ustawionym EAS generują sygnał modulowany
Get System Info		+	Wyślij informacje: AFI, UID, DSFID, rozmiar pamięci, itd.

* – wyjaśnione poniżej
** – stan, w którym może przebywać tylko jedna karta w zasięgu czytnika. Ułatwia adresowanie kart, ponieważ nie trzeba podawać jej UID
*** – stan, w którym przebywają pozostałe karty. W celu wysłania rozkazu do konkretnej karty trzeba podać jej UID
**** – *Electrical Articles Surveillance*

Tab. 4. Komendy kart SR

Polecenie	SR176	SRIX512	SRIX4K	Opis
READ_BLOCK	+	+	+	Odczyt bloku EEPROM
WRITE_BLOCK	+	+	+	Zapis bloku EEPROM*
INITIATE	+	+	+	Start procedury anti–collision
SELECT	+	+	+	Wejście w stan SELECTED
COMPLETION	+	+	+	Wyjście ze stanu SELECTED
PROTECT_BLOCK	+			Zabezpieczenie bloku EEPROM
GET_PROTECTION	+			Kontrola stanu zabezpieczenia bloku
PCALL16		+	+	Część procedury anti–collision
SLOT_MARKER		+	+	Część procedury anti–collision
RESET_TO_INVENTORY		+	+	Wyjście ze stanu SELECTED
AUTHENTICATE		+	+	Kontrola legalności karty**
GET_UID		+	+	Zwraca UID

* – w przypadku kart SRIX512/4K można dodatkowo zabezpieczyć blok przed modyfikacją
** – skrótowo opisana poniżej



Rys. 14. Algorytm autoryzacji karty

Teraz karty, których CHIP_SLOT_NUMBER=0000_b wysyłają w odpowiedzi swój *Chip_ID*. Jeśli nie ma kolizji, to czytnik zapamiętuje ten numer i wysyła do karty komendę SELECT. Karta zostaje zidentyfikowana. Jeśli jednak nastąpiła kolizja czytnik wysyła komendę SLOT_MARKER(N), gdzie N jest liczbą od 0001_b do 1111_b. Karta porównuje swój CHIP_SLOT_NUMBER z wartością N. Jeśli są zgodne, to wysyła w odpowiedzi swój *Chip_ID*. Na komendy PCALL16 oraz SLOT_MARKER(N) nie odpowiadają karty wybrane komendą SELECT. Komendę SLOT_MARKER(N) można wywoływać dla kolejnych wartości N. W momencie osiągnięcia $N=1111_b$ można wykonać następny rozkaz PCALL16. Po każdej komendzie, na którą odpowiedziała tylko jedna karta (nie ma kolizji) zapamiętujemy jej *Chip_ID* i wprowadzamy ją w stan SELECTED. Komenda SELECTED z numerem *Chip_ID* nie zgodnym z daną kartą przenosi ją do stanu DESELECTED, ale jej *Chip_ID* nie ulega zmianie. Po pewnym czasie (zależnym od liczby kart znajdujących się w zasięgu czytnika) wszystkie karty są w stanie DESELECTED, a czytnik zna ich *Chip_ID*. W tej chwili komenda SELECT(*Chip_ID*) wprowadza kartę o *Chip_ID* zgodnym w stan SELECTED, przenosząc tym samym inne karty w stan DESELECTED. W stanie SELECTED możliwe są operacje zapisu/odczytu bloku pamięci E²PROM. Dopuszczalne jest także wykonanie komendy COMPLETION wprowadzającej w stan DEACTIVATED, czyli wyłączenie karty. Inną możliwością jest autoryzacja karty – AUTHENTICATE.

Autoryzacja

Elementy, w nazwie których występuje litera X (np. SRIX4K), są wyposażone dodatkowo w algorytm pozwalający na jednoznaczną autoryzację karty. Ponieważ algorytm jest chroniony patentem, to jego szczegółowy opis jest udostępniany klientom po podpisaniu umowy NDA (*Non Disclosure Agreement*). Poniżej zawarto jedynie ogólne założenia algorytmu.

Na **rys. 14** pokazano przepływ informacji pomiędzy procesorem (MCU), układem dekodującym (CRX14) a kartą. Warte zauważenia jest, że każda transmisja jest kodowana. Komunikacja pomiędzy MCU a czytnikiem odbywa się po magistrali I²C. Tą drogą jest wysyłana komenda AUTHENTICATE, następnie czytnik wysyła tę komendę do karty. Po otrzymaniu od karty opdpowiedzi jest ona porównywana z obliczoną wewnętrznie i odsyłana do MCU.

Na podstawie materiałów firmy STMicroelectronics przygotował:

Jerzy Baratowicz (ST)