ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1987

Seria: AUTOMATYKA z. 83 Nr kol. 888

Andrzej HŁAWICZKA

WIELOSYGNATUROWA RÓWNOLEGŁA ANALIZA USZKODZEŃ W SYSTEMIE CYFROWYM

Streszczenie. Artykuł przedstawia ideę równoległej wielosygnaturowej (k-sygnaturowej) analizy uszkodzeń w układach cyfrowych, w szczególności w jądrze mikrokomputera testowanego w trybie swobodnego obiegu przestrzeni adresowej (free run). W artykule opisano kilka technik realizacji takiej analizy za pomocą n-bitowego równoległego rejestru z wewnętrznym sprzężeniem zwrotnym liniowym. Udowodniono, że przy bardzo małym nakładzie kosztów sprzętu uzyskuje się prawdopodobieństwo wykrycia błędu równe $1-2^{-kn}$, jak również uzyskuje się możliwość wykrycia na dowolnym wejściu równoległego rejestru błędu grupowego o długości co najwyżej kn. Artykuł zakończono opisem kilku przykładów zastosowania wielosygnaturowej analizy.

1. WPROWADZENIE

Konwencjonalna jednosygnaturowa analiza mikrokomputerów przedstawiona w pracy [1] polega, zarówno w trybie testowania za pomocą swobodnego obiegu przestrzeni adresowej (free run), jak i w trybie testowania za pomocą pobudzania sterowanego programowo (software driven), na realizacji jednego pomiaru ciągu danych diagnostycznych w każdym testowanym punkcie, odczytaniu oddzielnych pojedynczych sygnatur związanych z testowanymi punktami i porównaniu ich z pojedynczymi sygnaturami wzorcowymi. Prawdopodobieństwo niewykrycia błędu w mierzonym ciągu zależy w takiej jednosygnaturowej analizie od długości stosowanego rejestru liniowego LFSR (Linear Feedback Shift Register) i również jest 2^{-n} [2]. Wydłużanie rejestru liniowego LFSR w celu zmniejszenia tego prawdopodobieństwa prowadzi do niepotrzebnej redundancji sprzętu pomiarowego [3-4]. Idea zwiększenia skuteczności detekcji błędów bez potrzeby wydłużania rejestru LFSR polega na realizacji kolejno kilku (k) pomiarów różnych ciągów tych samych danych diagnostycznych w każdym testowanym punkcie. Technika ta pod nazwą wielosygnaturowa analiza (kSA) została po raz pierwszy przedstawiona w pracach [3-4], następnie powtórzona pod nazwą technika MSA trzy lata później w pracy [5]. We wszystkich wymienionych pracach ograniczono się do realizacji techniki kSA w pojedynczych punktach kontrolnych systemu cyfrowego wykorzystując jednowejściowy, rejestr liniowy LFSR o stałym liniowym sprzężeniu zwrotnym. W pracach [3-4], a w ślad za nimi w pracy [5] rozważano szczególny przypadek techniki kSA w postaci dwusygnaturowej analizy realizowanej za pomocą wymuszania w testowanym punkcie takich dwóch róż-

Wyrażenie (1a) wykorzystamy do określenia skuteczności równoległej analizy sygnaturowej w naszym przykładzie, który obecnie skonkretyzujemy jeszcze bardziej. Weźmy rejestr MISR o wewnętrznym sprzężeniu liniowym opisany wielomianem pierwszym

$$p(x) = x^8 + x^7 + x^5 + x^3 + 1$$

Załóżmy następujące ciągi danych odczytywane z pamięci ROM na nie uszkodzonych liniach i oraz j magistrali danych w trybie swobodnego obiegu przestrzeni adresowej:

$$D_i = \ldots \overline{x\ y\ z\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ r\ w} \ldots$$

$$D_j = \ldots \overline{x\ y\ z\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ \underbrace{r\ w\ \ldots}_{t \text{ taktów pomiarowych}}$$

Strzałki oznaczają kierunek wprowadzania bitów ciągów D_i oraz D_j do rejestru MISR, natomiast x,y,z,r,w oznaczają bity o dowolnej wartości, jednak jednakowej w ciągu D_i oraz D_j w tym samym takcie pomiarowym. Ciąg danych, który pojawi się na liniach i oraz j w chwili zwarcia obu linii można opisać za pomocą ciągu:

$$Z = D_i \cdot D_j = \ldots 00000100001000 \ldots$$

W efekcie ciągi błędów, które w związku z tym pojawiają się na linii i oraz j są następujące:

$$E_i = Z \oplus D_i = \ldots\ \overset{876543210}{00011010100100} \ldots$$

$$E_j = Z \oplus D_j = \ldots\ 00000000000\underbrace{00\ldots}_{t \text{ taktów}}$$

Odpowiadające im wielomiany przedstawione są poniżej

$$e_i(x) = x^t(x^8 + x^7 + x^5 + x^3 + 1), \quad e_j(x) = 0 .$$

Podstawiając do wyrażenia (1a) otrzymane wielomiany uzyskujemy następujące dzielenie:

$$\frac{x^t(x^8 + x^7 + x^5 + x^3 + 1)x^i + 0 \cdot x^j}{x^8 + x^7 + x^5 + x^3 + 1} = x^{t+i} + \frac{0}{x^8 + x^7 + x^5 + x^3 + 1},$$

z którego wynika, że ciąg błędów nie zostanie wykryty w tym pomiarze. Przeprowadźmy więc w naszym przykładzie drugi pomiar sygnatury w trybie swobodnego obiegu przestrzeni adresowej, ale w taki sposób, że zmienione zostanie sprzężenie zwrotne MISR (np. na $p'(x) = x^8 + x^5 + x^3 + x+1$, który jest wielomianem pierwszym) lub obieg przestrzeni adresowej odbędzie się w przeciwnym kierunku. W pierwszym przypadku na podstawie (1a) otrzymujemy następujące wyrażenie niepodzielne:

$$\frac{x^t(x^8 + x^7 + x^5 + x^3 + 1)x^i + 0 \cdot x^j}{x^8 + x^5 + x^3 + x + 1}$$

Podobnie w drugim przypadku, w którym błąd $e_i'(x) = x^8 + x^5 + x^3 + x + 1$, otrzymujemy następujące niepodzielne wyrażenie:

$$\frac{x^t(x^8 + x^5 + x^3 + x + 1)x^i + 0 \cdot x^j}{x^8 + x^7 + x^5 + x^3 + 1}.$$

W obydwu przypadkach w drugim pomiarze ciąg błędów wymuszonych przez zwarcie linii i oraz j zostanie wykryty. Podobnych przykładów błędów wymuszonych realnymi uszkodzeniami (np. typu zwarcia wielu linii magistrali danych i niewykrytych w jednym pomiarze) można pokazać ogromną ilość.

Skuteczność wykrycia takich błędów zależy od podzielności wielomianu $e_z(x)$ przez $p(x)$. Można więc, zmieniając wielomian $e_z(x)$ albo wielomian $p(x)$, wpływać na ich wzajemną podzielność, a tym samym na skuteczność sygnaturowej analizy. Idea wielosygnaturowej równoległej analizy polega więc na zmianie wielomianu $e_z(x)$ albo wielomianu $p(x)$ w kolejnych pomiarach tych samych błędów.

Wprowadźmy następujące definicje:

Definicja 1 Analizą kRSA z użyciem różnych sprzężeń zwrotnych nazywać będziemy k-sygnaturową równoległą analizę uszkodzeń, realizowaną za pomocą k pomiarów tego samego ciągu błędnych słów przy użyciu rejestru MISR o innym sprzężeniu zwrotnym w każdym pomiarze.

Definicja 2 Analizą kRSA z użyciem różnych ciągów tych samych błędów nazywać będziemy k-sygnaturową równoległą analizę uszkodzeń realizowaną za pomocą k pomiarów ciągu błędnych słów generowanych w każdym pomiarze w innej kolejności i przy użyciu rejestru MISR o stałym sprzężeniu zwrotnym w każdym pomiarze.

Definicja 3 Paczką błędnych słów $\mathbb{E}$ (b,t) nazywać będziemy wycinek z ciągu m słów złożony z b słów, w którym mieszczą się wszystkie błędne słowa w ilości równej t i takie, że każde błędne słowo jest identyczne [6].

Załóżmy, że uszkodzenie testowanego układu cyfrowego wymusza na jego wyjściach w czasie testowania jedną z następujących paczek błędów:

$\mathbb{E}(m,1)$ dla $b = m$ oraz $t = 1$; $\mathbb{E}(kn,t)$ dla $b = k \cdot n$

oraz $1 \leqslant t \leqslant k \cdot n$; $\mathbb{E}(2^n - 1,2)$ dla $b = 2^n - 1$ oraz $t = 2$;

$\mathbb{E}(n,t)$ dla $b = n$ oraz $1 \leqslant t \leqslant n$.

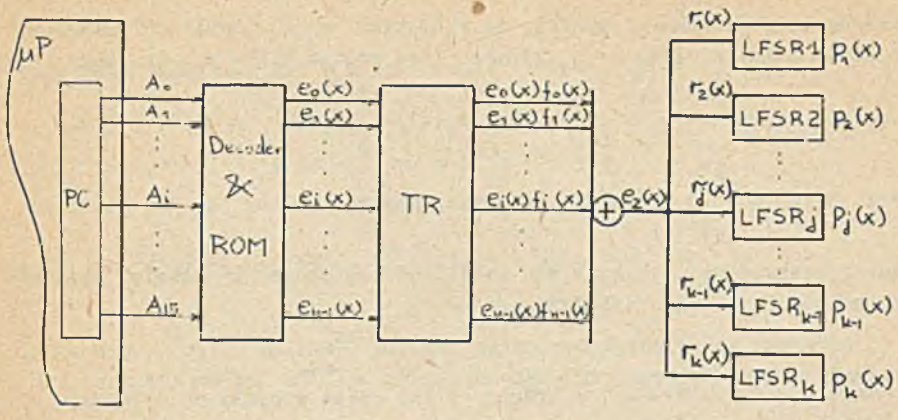
W następnych rozdziałach udowodniono, że analiza kRSA z użyciem różnych sprzężeń zwrotnych, reprezentowanych za pomocą k różnych wielomianów pierwotnych n-tego stopnia, wykrywa każdą paczkę błędów $\mathbb{E}(m,1)$, $\mathbb{E}(kn,t)$, $\mathbb{E}(2^n - 1,2)$ oraz umożliwia wykrywanie pozostałych błędów z prawdopodobieństwem $1-2^{-kn}$.
Udowodniono także, że analiza 2RSA z użyciem różnych ciągów tych samych błędów wykrywa każdą paczkę błędów $\mathbb{E}(m,1)$, $\mathbb{E}(2n,t)$, $\mathbb{E}(2^n-1,2)$ oraz umożliwia wykrywanie pozostałych błędów z prawdopodobieństwem $1-2^{-2n}$.

3. Analiza kRSA z użyciem różnych sprzężeń zwrotnych

Przeprowadzając jeden równoczesny pomiar tego samego ciągu błędnych słów za pomocą równolegle połączonych k rejestrów MISR każdy o innym sprzężeniu zwrotnym uzyskuje się taki sam efekt jak przy dokonywaniu k kolejnych pomiarów tego samego ciągu błędnych słów za pomocą tylko jednego rejestru MISR o ustawianym innym sprzężeniu zwrotnym w każdym kolejnym pomiarze. Można więc wielosygnaturową równoległą analizę np. uszkodzeń mikrokomputera w trybie swobodnego obiegu przestrzeni adresowej, realizowaną za pomocą rejestru MISR o zmiennym sprzężeniu zwrotnym zilustrować za pomocą schematu zastępczego przedstawionego na rys. 3. Na rysunku tym przetwornik TR jest przetwornikiem przekształcającym wielomiany $e_i(x)$ w wielomiany $e_i(x) \cdot f_i(x)$, k rejestrów LFSR o różnych sprzężeniach zwrotnych reprezentowanych wielomianami $p_1(x), p_2(x)\ldots, p_j(x)\ldots, p_k(x)$ odzwierciedla k kolejnych pomiarów, natomiast wielomian $e_z(x)$ ilustruje abstrakcyjny ciąg błędów wynikający z następującego wyrażenia:

$$e_z(x) = \sum_{i=0}^{n-1} e_i(x) \cdot f_i(x).$$

Ciąg błędów $e_z(x)$ jest niezależny od rodzaju wielomianu $p_j(x)$ i taki sam w każdym pomiarze. Efektem końcowym analizy kRSA z użyciem różnych sprzężeń zwrotnych jest więc k różnych dzieleń wielomianu $e_z(x)$ przez k



Rys. 3. Schemat zastępczy wielosygnaturowej równoległej analizy mikrokomputera w trybie swobodnego obiegu przestrzeni adresowej

Fig. 3. Substitutal scheme of multisignature parallel analysis of microcomputer in the free run mode of address space

różnych wielomianów $p_j(x)$ stopnia n dających w rezultacie zbiór k reszt w postaci wielomianów

$$r_1(x),\ r_2(x),\ldots,\ r_j(x),\ldots,\ r_k(x)\ .$$

<u>Lemat 1</u> Skuteczność detekcji uszkodzeń za pomocą jednosygnaturowej równoległej analizy przy użyciu rejestru MISR o wielomianie charakterystycznym $p'(x)$ stopnia $k \cdot n$ reprezentowanej dzieleniem wielomianu $e_z(x)$ przez $p'(x) = NWW\left[p_1(x), p_2(x), \ldots, p_j(x) \ldots p_k(x)\right]$ jest identyczna ze skutecznością analizy kRSA z użyciem różnych sprzężeń zwrotnych realizowanej za pomocą rejestru MISR o k różnych wielomianach charakterystycznych $p_1(x) \ldots p_2(x) \ldots p_j(x) \ldots p_k(x)$ każdy stopnia n.

<u>Dowód:</u>

O skuteczności detekcji błędu $e_z(x)$ decyduje podzielność wielomianu $e_z(x)$ przez wielomian charakterystyczny rejestru MISR. W związku z tym wystarczy udowodnić, że podzielność w obu wymienionych w lemacie przypadkach jest identyczna.

Każde z k dzieleń w analizie kRSA reprezentowane jest następującym wyrażeniem:

$$\frac{e_z(x)}{p_j(x)} = q_j(x) + \frac{r_j(x)}{p_j(x)} \quad \text{w którym} \quad j \in \left\{1, 2, \ldots, k\right\}, \quad \text{a } r_j(x)\ ,$$

jest wielomianem stopnia co najwyżej $n-1$.

Z własności podzielności wynika, że wielomian $e_z(x)$ podzielny równocześnie przez każdy wielomian $p_j(x)$ może mieć postać tylko następującą:

$$e_z(x) = q'(x)\mathrm{NWW}\left[p_1(x), p_2(x), \ldots, p_j(x), \ldots, p_k(x)\right] = q'(x).p'(x),$$

gdzie $p'(x) = \prod_{j=1}^{k} p_j(x)$ w przypadku, gdy wielomiany $p_j(x)$ są wielomianami pierwotnymi. Wniosek ten umożliwia zapisanie k dzieleń analizy kRSA za pomocą jednego dzielenia:

$$\frac{e_z(x)}{p'(x)} = q'(x) + \frac{r'(x)}{p'(x)},$$ w którym $r'(x)$ jest stopnia co najwyżej $k.n-1$. Ponieważ postać wielomianu $e_z(x)$ podzielnego przez $p'(x)$ w jednosygnaturowej równoległej analizie jest identyczna, dlatego lemat można uznać za udowodniony.

<u>Twierdzenie 1</u> Analiza kRSA przy użyciu różnych sprzężeń za pomocą rejestru MISR o wielomianach charakterystycznych pierwotnych $p_1(x), p_2(x), \ldots, p_j(x) \ldots, p_k(x)$ każdy stopnia n wykrywa każdą paczkę błędnych słów $\mathbb{E}(m,1)$, $\mathbb{E}(k.n,t)$, $\mathbb{E}(2^n-1,2)$.

<u>Dowód</u>:
Na podstawie lematu 1 należy udowodnić, że $e_z(x)$ jest niepodzielne przez wielomian $p'(x) = \mathrm{NWW}\left[p'(x), p_2(x), \ldots, p_k(x)\right] = \prod_{j=1}^{k} p_j(x)$ w przypadku wymienionych paczek błędów.
Założone paczki błędnych słów implikują następujące wielomiany

$e_i(x)$ oraz $e_z(x)$ dla dowolnie wybranych i :

$$\mathbb{E}(m,1) \Rightarrow e_i'(x) = x^w.a_i \Rightarrow e_z'(x) = x^w.\sum_{i=0}^{n-1} f_i(x).a_i,$$

gdzie $a_i = \begin{cases} 0 \text{ dla } e_i(x) = 0 \\ 1 \text{ dla } e_i(x) \neq 0 \end{cases}$

$$\mathbb{E}(k.n,t) \Rightarrow e_i''(x) = (x^g + \ldots + x^h + \ldots + x^w)a_i = x^w(x^{g-w} + \ldots + x^{h-w} + \ldots + 1).a_i,$$

gdzie $g-w < k.n; \Rightarrow e''_z(x) = x^w(x^{g-w}+..+x^{h-w}+..+1) \sum_{i=0}^{n-1} f_i(x).a_i,$

$$\mathbb{E}(2^n-1,2) \Rightarrow e''_i(x) = (x^h+x^w).a_i = x^w(x^{h-w}+1).a_i$$

gdzie $h-w \leqslant 2^n-1; \Rightarrow e''_z(x) = x^w(x^{h-w}+1).\sum_{i=0}^{n-1} f_i(x).a_i$

Wielomiany $x^w, (x^{g-w}+...+x^{h-w}+...1)$ są niepodzielne przez wielomian $p'(x)$ oraz wielomian $x^{h-w}+1$ jest niepodzielny przez dowolny wielomian pierwotny $p_j(x)$ oraz wielomian $\sum_{i=0}^{n-1} f_i(x).a_i$ stopnia co najwyżej n-1 jest niepodzielny przez $p'(x)$. W związku z tym twierdzenie zostało udowodnione.

Załóżmy obecnie, że każdy ciąg błędnych słów jest jednakowo prawdopodobny. Założenie to implikuje jednakowe prawdopodobieństwo wystąpienia ciągu błędów opisanego wielomianem $e_z(x)$ na wejściu każdego rejestru LFSR na rys. 3. W związku z tym prawdziwe jest następujące twierdzenie:

Twierdzenie 2 Prawdopodobieństwo niewykrycia ciągu błędnych słów o długości m w trakcie analizy kRSA przy użyciu różnych sprzężeń za pomocą rejestru MISR o wielomianach charakterystycznych $p_1(x), p_2(x), ..., p_j,(x), ..., p_k(x)$ każdy stopnia n jest równe 2^{-kn} dla $m \gg k.n$.

Dowód:

Opierając się na lemacie 1 ciągi błędów opisane wielomianem $e_z(x)$ będą niewykrywalne w trakcie analizy kRSA przy użyciu różnych sprzężeń, jeżeli wielomian $e_z(x)$ przyjmie postać następującego iloczynu:

$$e_z(x) = q'(x) \cdot p'(x)$$

Ponieważ wielomian $e_z(x)$ jest stopnia m+n-2 oraz wielomian $p'(x)$ jest stopnia k.n, dlatego stopień wielomianu $q'(x)$ jest równy m+n-2-kn. Ilość ciągów błędnych słów podzielnych przez $p'(x)$ jest liczbą niezerowych ilorazów opisanych wielomianem $g'(x)$ i wynikającą ze stopnia tego wielomianu. Natomiast ilość wszystkich ciągów błędnych słów wynika ze stopnia wielomianu $e_z(x)$.

Ostatecznie przyjmując, że jeden z ciągów słów nie zawiera w ogóle błędów, uzyskujemy następujący wzór określający poszukiwane prawdopodobieństwo:

$$P = \lim_{m \to \infty} \frac{2^{m+n-2kn}-1}{2^{m+n-2}-1} = 2^{-kn}$$

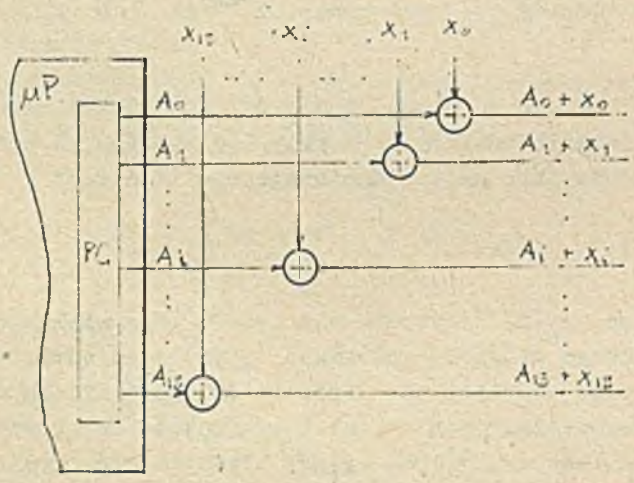
4. Analiza KRSA z użyciem różnych ciągów tych samych błędów

Stosując w trybie swobodnego obiegu przestrzeni adresowej generator testów w postaci licznika programów μP z blokiem bramek XOR (rys. 4) na każdej linii adresowej [3-4], można wymusić w k kolejnych pomiarach, za pomocą wektora $x = \langle x_0, x_1, \ldots x_i \ldots x_{15} \rangle$, na magistrali adresowej k różnych sekwencji adresów. W konsekwencji na magistrali danych pojawi się k różnych ciągów błędnych słów. Te ciągi błędnych słów można opisać zastępczo za pomocą następujących wielomianów:

$$e_{z1}(x), e_{z2}(x), \ldots, e_{zj}(x), \ldots, e_{zk}(x).$$

Zakładając, że w każdym z k powyższych pomiarów wielomian $p(x)$ charakterystyczny dla rejestru MISR jest identyczny, można każde z k kolejnych dzieleń takiej analizy KRSA zapisać za pomocą następującego wyrażenia:

$$\frac{e_{zj}(x)}{p(x)} = q'_j(x) + \frac{r'_j(x)}{p(x)} \quad \text{w którym} \quad j \in \{1, 2, \ldots, k\}$$



Rys. 4. Generator testów z blokiem bramek XOR umożliwiający generację k różnych sekwencji adresów w trybie swobodnego obiegu przestrzeni adresowej

Fig. 4. The generator with XOR block which enables generation of k different address sequences in the free run mode of address space

Ograniczymy naszą dalszą uwagę tylko do dwusygnaturowej równoległej analizy reprezentowanej dwoma dzieleniami ilustrującymi dwa pomiary - pierwszy przy wektorze $X = \langle 0,0,\ldots,0,\ldots,0 \rangle$ wymuszającym normalny obieg przestrzeni adresowej zgodny z pracą w przód licznika programów μr oraz drugi przy wektorze $X = \langle 1,1,\ldots,1,\ldots,1 \rangle$ wymuszającym odwrotny obieg przestrzeni adresowej podobny do pracy rewersyjnej licznika binarnego. Oznaczmy przez $e_{z1}(x)$ wielomian związany z ciągiem identycznych błędnych słów wymuszanych w pierwszym pomiarze na magistrali danych, natomiast przez $e_{z2}(x)$ wielomian związany z odwrotnym ciągiem tych samych błędnych słów wymuszanych w drugim pomiarze.

Umówmy się, że wielomian $w^+(x) = x^n\left[w_0+w_1x^{-1}+\ldots+w_nx^{-n}\right]$ nazywać będziemy wielomianem odwrotnym do wielomianu $w(x) = w_0+w_1x+\ldots+w_nx^n$, a także załóżmy następujące wielomiany:

$$w(x) \text{ jak wyżej } \quad z(x) = z_0+z_1x+\ldots+z_mx^m \quad \text{oraz}$$

$$v(x) = w(x).z(x) = w_0\cdot z_0+(w_0\cdot z_1+w_1\cdot z_0)x+\ldots+w_n\cdot z_m\cdot x^{n+m}$$

Wówczas prawdziwy jest następujący lemat [4-5].

<u>Lemat 2</u> Jeżeli $v(x) = w(x).z(x)$, to $v^+(x) = w^+(x).z^+(x)$

<u>Dowód</u>:

$$v^+(x) = x^{n+m}\left[w_0\cdot z_0+(w_0\cdot z_1+w_1\cdot z_0)\cdot x^{-1}+\ldots+w_n\cdot z_m\cdot x^{-(n+m)}\right]$$

natomiast

$$w^+(x).z^+(x) = x^n\left[w_0+w_1x^{-1}+\ldots+w_nx^{-n}\right].x^m\left[z_0+z_1x^{-1}+\ldots+z_mx^{-m}\right] =$$

$$= x^{n+m}\left[w_0z_0+(w_0\cdot z_1+w_1\cdot z_0)x^{-1}+\ldots w_n\cdot z_m\cdot x^{-(n+m)}\right] = v^+(x)$$

<u>Twierdzenie 3</u> Skuteczność detekcji uszkodzeń za pomocą analizy 2RSA z użyciem różnych ciągów tych samych błędnych słów opisanych wielomianami $e_{z1}(x)$ i $e_{z2}(x)$ i przy wykorzystaniu rejestru MISR z charakterystycznym wielomianem $p(x)$ stopnia n jest identyczna ze skutecznością analizy 2RSA z użyciem różnych sprzężeń rejestru MISR opisanych wielomianami charakterystycznymi $p(x)$ i $p^+(x)$ każdy stopnia n i przy użyciu tego samego ciągu opisanego przez $e_{z1}(x)$.

<u>Dowód</u>:

Skuteczność analizy 2RSA w pierwszym i drugim przypadku zależy od podzielności w następujących parach dzieleń reprezentujących oba rodzaje analiz 2RSA:

$$\frac{e_{z1}(x)}{p(x)}, \quad \frac{e_{z2}(x)}{p(x)} \quad \text{oraz} \quad \frac{e_{z1}(x)}{p(x)}, \quad \frac{e_{z1}(x)}{p^+(x)}$$

Ponieważ pierwsze dzielenie w obu parach jest identyczne, dlatego wystarczy udowodnić, że $e_{z1}(x)$ jest podzielne przez $p^+(x)$, jeżeli $e_{z2}(x)$ jest podzielne przez $p(x)$.

Na podstawie schematu zastępczego (rys. 3) można przedstawić pierwszy pomiar analizy 2RSA zużyciem różnych ciągów identycznych błędnych słów w postaci następującego wyrażenia:

$$\frac{e_{z1}(x)}{p(x)} = \frac{e(x)\sum_{i=0}^{n-1} x^i a_i}{p(x)} = q_i'(x) + \frac{r_i'(x)}{p(x)} \tag{2}$$

natomiast drugi pomiar w postaci następującego wyrażenia:

$$\frac{e_{z2}(x)}{p(x)} = \frac{e^+(x)\sum_{i=0}^{n-1} x^i a_i}{p(x)} = q_2'(x) + \frac{r_2'(x)}{p(x)} \tag{3}$$

gdzie: $e(x)$ $(e^+(x))$ jest wielomianem opisującym identyczne ciągi błędów na różnych wejściach rejestru MISR.
Mnożąc obie strony wyrażenia (3) przez $p(x)$ i zakładając podzielność $e_{z2}(x)$ przez $p(x)$ czyli $R\left[e_{z2}(x),\ p(x)\right] = r_2'(x) = 0$ otrzymujemy

$$e_{z2}(x) = e^+(x)\sum_{i=0}^{n-1} x^i a_i = q_2'(x)p(x) \tag{4}$$

Opierając się na lemacie 2 z wyrażenia (4) otrzymujemy wyrażenie

$$e_{z2}^+(x) = e(x)\sum_{i=0}^{n-1} x^{n-1-i}\ a_i = q_2'^+(x)p^+(x) \tag{5}$$

z którego wynika następujący wniosek:

$$R\left[e_{z2}(x), p(x)\right] = 0 \Rightarrow R\left[e(x)\sum_{i=0}^{n-1} x^{n-1-i} a_i,\ p^+(x)\right] = 0$$

Podobnie przy założeniu $r_1'(x) = 0$ z wyrażenia (2) wynika następujący wniosek:

$$R\left[e_{z1}(x), p(x)\right] = 0 \Rightarrow R\left[e(x)\sum_{i=0}^{n-1} x^i a_i, p(x)\right] = 0$$

Zauważmy, że $\deg \sum_{i=0}^{n-1} x^{n-1-i} a_i < \deg p^+(x)$ jak również $\deg \sum_{i=0}^{n-1} x^i a_i$ $\deg p^+(x)$.

Wynika z tego, że $R\left[\sum_{i=0}^{n-1} x^{n-1-i} a_i, p^+(x)\right] \neq 0$ jak również

$R\left[\sum_{i=0}^{n-1} x^i a_i, p^+(x)\right] \neq 0$ co pozwala zauważyć, że tylko podzielność $e(x)$ przez $p(x)$ i $p^+(x)$ decyduje o końcowych wnioskach. Ostatecznie można więc sformułować następujący wniosek

$$R\left[e(x) \sum_{i=0}^{n-1} x^{n-1-i} a_i, p^+(x)\right] = 0 \Rightarrow R\left[e(x) \sum_{i=0}^{n-1} x^i a_i, p^+(x)\right] = 0$$

z którego w sposób oczywisty wynika, że

$$R\left[e_{z2}(x), p(x)\right] = 0 \Rightarrow R\left[e_{z1}(x), p^+(x)\right] = 0$$

co kończy dowód twierdzenia.

Wniosek 1 Analiza 2RSA z użyciem dwóch różnych odwrotnych ciągów opisanych wielomianami $e_{z1}(x)$ i $e_{z2}(x)$ i przy wykorzystaniu rejestru MISR o wielomianie charakterystycznym pierwotnym $p(x)$ n-tego stopnia wykrywa każdą paczkę błędnych słów $E(m,1)$, $E(2n,t)$, $E(2^n-1,2)$.

Dowód:

Na podstawie lematu 1 parę dzieleń reprezentującą analizę 2RSA z użyciem różnych ciągów identycznych błędnych słów można zastąpić jednym następującym dzieleniem:

$$\frac{e_{z1}(x)}{p''(x)} = q''(x) + \frac{r''(x)}{p''(x)} \quad \text{w którym} \quad p''(x) = NWW\left[p(x), p^+(x)\right] \tag{6}$$

Wielomian $p''(x) = p(x)p^+(x)$ gdy oba wielomiany są pierwotne.
W związku z powyższym przy założeniu $k = 2$ opierając się na twierdzeniu 1 wniosek jest prawdziwy.

Wniosek 2 Prawdopodobieństwo niewykrycia ciągu błędnych słów o długości m w trakcie analizy 2RSA zużyciem różnych odwrotnych ciągów tych samych błędnych słów za pomocą rejestru MISR o wielomianie charakterystycznym $p(x)$ n-tego stopnia jest równe 2^{-2n} dla $m >> 2n$.

Podobne wnioski ale ograniczone do jednowejściowego rejestru liniowego LFSR (Linear Feedback Shift Register) zarówno ze sprzężeniem wewnętrznym jak i zewnętrznym można sformułować opierając się o prace wcześniejsze [4-5]

5. Ograniczenie stosowania analizy 2RSA z użyciem różnych ciągów

Przedstawione w poprzednim rozdziale wnioski nie uwzględniają tzw. symetrycznych ciągów błędów opisywanych zdefiniowanymi poniżej symetrycznymi wielomianami.

Definicja 4 Symetrycznym wielomianem $w(x)$ nazywać będziemy taki wielomian $w(x)$, który równy jest swojej postaci odwróconej $w^+(x)$.

Poniżej udowodniono, że wnioski 1 i 2 przestają obowiązywać w przypadku analizy 2RSA z użyciem symetrycznych ciągów tych samych błędów wymuszonych w TUC raz za pomocą pracy w przód generatora testów, a drugi raz za pomocą pracy wstecz tego samego generatora testów.

Lemat 3 Jeżeli $w(x)$ jest wielomianem symetrycznym, wówczas $w(x).x^l = w^+(x)x^i$
Dowód jest oczywisty.

Twierdzenie 4 Jeżeli w analizie 2RSA z użyciem różnych ciągów błędów wymuszonych przez generator testów pracujący raz w przód, a drugi raz w tył, w pierwszym pomiarze na wejściach rejestru MISR o wielomianie charakterystycznym $p(x)$ n-tego stopnia wystąpią tylko symetryczne ciągi błędów, wówczas analiza ta wykrywa tylko każdą paczkę błędnych słów $\mathbb{E}(m,1)$, $\mathbb{E}(n,t)$, $\mathbb{E}(2^{n-1},2)$, a prawdopodobieństwo niewykrycia pozostałych ciągów błędnych słów za pomocą wspomnianego rejestru MISR jest równe tylko 2^{-n} dla $m \gg n$.

Dowód:

Weźmy $e_{z1}(x) = \sum_{i=0}^{n-1} e_i(x)f_i(x)$ oraz $e_{z2}(x) = \sum_{i=0}^{n-1} e_i^+(x)f_i(x)$,

Opierając się na lemacie 1 parę dzieleń reprezentujących analizę 2RSA z użyciem różnych (odwrotnych) ciągów błędów można zastąpić jednym dzieleniem (6), w którym wielomian $p''(x) = NWW[p(x),p^+(x)] = p(x)p^+(x)$ jest wielomianem 2n-tego stopnia. Ponieważ każdy ciąg błędów $e_i(x)$ jest ciągiem symetrycznym, dlatego $e_i(x) = e_i^+(x)$, w związku z tym na podstawie lematu 3 można napisać, że $e_{z1}(x) = e_{z2}(x)$. W efekcie wielomian $p''(x)$ w dzieleniu (6) przyjmuje wartość $p''(x) = NWW[p(x),p(x)] = p(x)$. Wielomian $p(x)$ jest n-tego stopnia, co powoduje, że własności detekcyjne omawianej analizy 2RSA w zastosowaniu do symetrycznych ciągów błędów są takie same jak analizy 1 RSA.

Rozpatrując ciągi błędów w oderwaniu od modelu uszkodzeń TUC i przy założeniu jednakowego prawdopodobieństwa pojawienia się dowolnego ciągu błędów można udowodnić następujące twierdzenie:

Twierdzenie 5 Prawdopodobieństwo Ps wystąpienia bardzo długiego symetrycznego ciągu błędów o długości l jest równe 0.

Dowód:
Liczba M wszystkich możliwych ciągów błędów o długości l równa jest 2^l-1. Natomiast liczba N wszystkich możliwych symetrycznych ciągów błędów o długości l równa jest $2^{\frac{l}{2}}-1$.

W związku z powyższym prawdopodobieństwo

$$P_s = \lim_{l\to\infty} \frac{N}{M} = \lim_{l\to\infty} \frac{2^{\frac{l}{2}}-1}{2^l-1} = 0$$

Na podstawie twierdzenia 5 można by zlekceważyć wpływ symetrycznych ciągów błędów na skuteczność ich detekcji za pomocą analizy 2RSA z użyciem różnych (odwrotnych) ciągów błędów. Okazuje się jednak, że istnieją takie uszkodzenia w TUC, które wymuszają tylko symetryczne ciągi błędów. Udowodnimy obecnie realność występowania takich błędów,

Lemat 4 Każdy wielomian w(x) m-tego stopnia taki, że

$$w(x) = \sum_{i=0}^{\left[\frac{m}{2}\right]} a_i x^i + \sum_{i=0}^{\left[\frac{m-1}{2}\right]} a_i x^i = \sum_{i=0}^{\left[\frac{m}{2}\right]} a_i x^{m-i} + \sum_{i=0}^{\left[\frac{m}{2}\right]} a_i x^{m-i}, \text{ gdzie}$$

$\left[\frac{m}{2}\right]$ oznacza największą liczbę całkowitą $\leqslant \frac{m}{2}$, a

$\left[\frac{m-1}{2}\right]$ " " " " $\leqslant \frac{m-1}{2}$,

jest wielomianem symetrycznym w(x).

Dowód:

Wystarczy udowodnić, że $w^+(x) = w(x)$

$$w^+(x) = x^m\left[\sum_{i=0}^{\left[\frac{m}{2}\right]} a_i x^{-i} + \sum_{i=0}^{\left[\frac{m-1}{2}\right]} a_i x^{-(m-i)}\right] = \sum_{i=0}^{\left[\frac{m}{2}\right]} a_i x^{m-i} + \sum_{i=0}^{\left[\frac{m-1}{2}\right]} a_i x^i = w(x) \quad \square$$

Lemat 5 Jeżeli ciąg o długości m+1 na i-tym wyjściu nie uszkodzonego TUC jest ciągiem symetrycznym opisanym wielomianem w(x), to ciąg błędów wymuszonych na i-tym wyjściu uszkodzeniem typu s-z-0 lub s-z-1 jest symetrycznym ciągiem błędów.

Dowód:

Wielomiany $\sum_{i=0}^{m} 0.x^i = 0$ i $\sum_{i=0}^{m} x^i = D(x)$ opisują ciągi, które pojawiają się na wyjściu i-tym TUC w przypadku uszkodzeń odpowiednio s-z-0 i s-z-1.

Otrzymamy więc następujące ciągi błędów:

- dla s=z=0

$$e_0(x) = \underset{\circ}{w}(x) + 0 = w(x)$$

- dla s=z=1

$$e_1(x) = \underset{\circ}{w}(x)+D(x) = \sum_{i=0}^{\left\lceil \frac{m}{2} \right\rceil} (1+a_i)x^i + \sum_{i=0}^{\left\lceil \frac{m-1}{2} \right\rceil} (1+a_i)x^{m-i} = \overline{\underset{\circ}{w}(x)} \qquad \square$$

<u>Lemat 6</u> Jeżeli dwa ciągi o długości m=1 na a-tym oraz b-tym wyjściu nie uszkodzonego TUC są ciągami symetrycznymi opisanymi wielomianami odpowiednio $\underset{\circ}{w}_a(x)$ i $\underset{\circ}{w}_b(x)$, to ciąg błędów wymuszonych zwarciem wyjścia a z wyjściem b jest symetrycznym ciągiem błędów.

<u>Dowód</u>:

Jeżeli założymy, że

$$\underset{\circ}{w}_a(x) = \sum_{i=0}^{\left\lceil \frac{m}{2} \right\rceil} a_i x^i + \sum_{i=0}^{\left\lceil \frac{m-1}{2} \right\rceil} a_i x^{m-i} \quad \text{oraz}$$

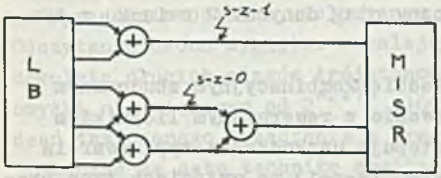
$$\underset{\circ}{w}_b(x) = \sum_{i=0}^{\left\lceil \frac{m}{2} \right\rceil} b_i x^i + \sum_{i=0}^{\left\lceil \frac{m-1}{2} \right\rceil} b_i x^{m-i}, \quad \text{to}$$

ciąg błędów wymuszony zwarciem linii a z linią b opisany będzie następującym wielomianem:

$$e(x) = \sum_{i=0}^{\left\lceil \frac{m}{2} \right\rceil} (a_i \cdot b_i) x^i + \sum_{i=0}^{\left\lceil \frac{m-1}{2} \right\rceil} (a_i \cdot b_i) x^{m-i}$$

Wielomian e(x) zgodnie z lematem 3 jest ciągiem symetrycznym $\underset{\circ}{e}(x)$ $\square$

Przykładem realnego nie uszkodzonego TUC, w którym występują symetryczne ciągi błędów jest dowolny liniowy układ kombinacyjny realizujący funkcję $S = A_i \oplus A_j \oplus \ldots \oplus A_k$ zbudowany z bramek XOR, którego wejścia podłączone są w czasie testowania do dowolnych wyjść i,j,....,k rewersyjnego licznika binarnego (rys. 5).



Rys. 5. Schemat blokowy testowania liniowego układu kombinacyjnego

Fig. 5. Block diagram of linear test of combination system

Udowodnimy to poniżej.

Zauważmy, że każdy wielomian $A_i(x) = x^k \cdot a_i(x) + a_i(x)$, gdzie $a_i(x)$ jest stopnia k-1 oraz $k=2^{n-1}$ opisuje ciąg binarny na i-tym wyjściu n-bitowego licznika binarnego.

Podobnie zauważyć można, że suma wielomianów $A_i(x)+D(x)$, gdzie $D(x)=1+x+\ldots+x^{k-1}+x^k\ldots+x^{2k-1}$ jest wielomianem odwrotnym $A_i^+(x)$, który opisuje negację ciągu binarnego na i-tym wyjściu licznika binarnego.

Na tej podstawie można udowodnić następujący lemat i twierdzenie.

<u>Lemat 7</u> Każdy wielomian $A_i(x)$ można przedstawić jako następującą sumę wielomianów:

$$A_i(x) = x^k a_i(x) + x^{k-1} a_i(\tfrac{1}{x}) + D(x^{k-1}) \quad \text{gdzie} \quad D(x^{k-1}) = 1+x+\ldots+x^{k-1} \qquad \square$$

Dowód jest oczywisty.

<u>Twierdzenie 6</u> Suma modulo dwa dwóch wielomianów $A_i(x)$ i $A_j(x)$ ilustrujących ciągi na dwóch dowolnych wyjściach i oraz j licznika binarnego jest wielomianem symetrycznym c(x).

<u>Dowód</u>:

Należy udowodnić, że $c^+(x) = c(x)$.

Zapiszmy na podstawie lematu 7, że

$$A_i(x) = x^k a_i(x) + x^{k-1} a_i(\tfrac{1}{x}) + D(x^{k-1})$$

oraz

$$A_j(x) = x^k a_j(x) + x^{k-1} a_j(\tfrac{1}{x}) + D(x^{k-1}).$$

Przyjmijmy, że

$$c(x) = A_i(x)+A_j(x) = x^k\left[a_i(x)+a_j(x)\right] + x^{k-1}\left[a_i(\tfrac{1}{x})+a_j(\tfrac{1}{x})\right] = x^k c(x) + x^{k-1} c(\tfrac{1}{x}).$$

Ostatecznie

$$c^+(x) = x^{2k-1}\left[x^{-k} c(\tfrac{1}{x}) + x^{-(k-1)} c(x)\right] = x^{k-1} c(\tfrac{1}{x}) + x^k c(x) = c(x) . \qquad \square$$

Z powyższego twierdzenia wynika, że na wyjściu każdej bramki XOR liniowego układu kombinacyjnego występuje symetryczny ciąg danych. W związku z tym ważne jest także poniższe twierdzenie.

Twierdzenie 7 Jeżeli w liniowym układzie kombinacyjnym zbudowanym z bramek XOR i połączonym w czasie testowania z rewersyjnym licznikiem binarnym pracującym w przód (wstecz) występują uszkodzenia typu zwarcia wyjść bramek XOR lub uszkodzenia typu s-z-0 (s-z-1) na wyjściach tych bramek, wówczas ciągi błędów wymuszonych tymi uszkodzeniami są ciągami symetrycznymi.
Dowód wynika z lematów 4, 5 i 6. □

Wniosek 3 W liniowych układach kombinacyjnych nie należy stosować analizy 2RSA z użyciem różnych (odwrotnych) ciągów tych samych błędów.
Dowód wynika z twierdzenia 4 i 6. □
Przykładem takich układów liniowych mogą być np. układy scalone TTL 7486 lub 74180.

6. Inne zastosowania analizy kRSA z użyciem różnych sprzężeń i lub różnych ciągów

Technika wielosygnaturowej analizy została przedstawiona w poprzednich rozdziałach głównie na przykładzie testowania mikrokomputerów w trybie swobodnego obiegu przestrzeni adresowej. Istnieje szereg innych jej zastosowań. Oto niektóre z nich.

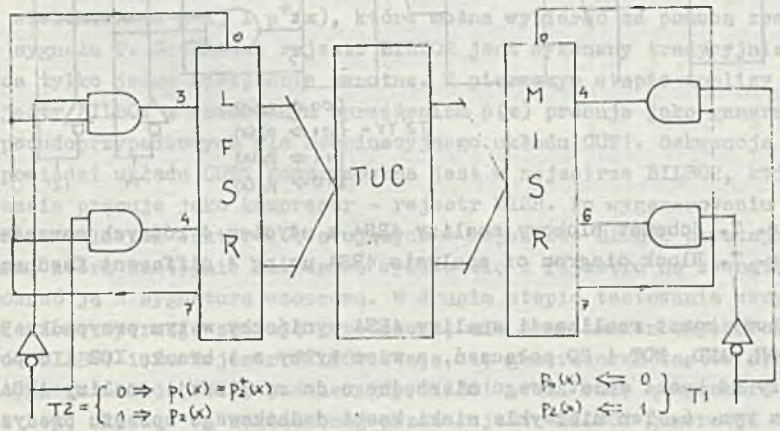
Technika analizy kSRA może być z powodzeniem zastosowana w trybie pobudzania sterowanego programowo, w którym programowy licznik może pracować w przód albo w tył umożliwiając tym samym realizację analizy 2RSA z użyciem różnych ciągów tych samych błędów. Analiza kRSA może być także zastosowana w mikrokomputerach z samotestowaniem, których przykładem jest Microbit [12], CRYSTALDIGRAF NC [14].

Omówienie w tej pracy głównie przykładu testowania mikrokomputerów nie przekreśla możliwości zastosowania analizy kRSA do testowania dowolnych urządzeń cyfrowych, a w szczególności wielowyjściowych układów kombinacyjnych w elementach scalonych VLSI z samotestowaniem, które obecnie są przedmiotem badań wszystkich liczących się w świecie laboratoriów cyfrowych. Twierdzenia i wnioski są tak sformułowane, że są ważne dla analizy kRSA realizowanej w dowolnym układzie cyfrowym. Gdy ciągi mierzone zawierają dodatkowo trzeci stan tzw. wysokiej impedancji, wówczas sprzęt pomiarowy dla techniki kRSA może być uzupełniony dodatkowymi środkami szczegółowo omówionymi w pracach [7-10].

Przykładem zastosowania techniki dwusygnaturowej analizy z użyciem różnych sprzężeń zwrotnych jest programowalny analizator sygnatur PAS 80 opisany w pracy [11], w którym z pulpitu operatora można zmieniać sprzę-

żenie zwrotne rejestru LFSR opisane wielomianem $p_1(x) = x^{16}+x^9+x^7+x^4+1$ na sprzężenie opisane wielomianem pierwotnym $p_2(x) = x^{16}+x^{10}+x^7+x^4+1$. Odczytanie dwóch sygnatur w kolejnych dwóch pomiarach umożliwia detekcję dowolnie długich ciągów trójstanowych z prawdopodobieństwem popełnienia omyłki nie większym od $2^{-2\cdot 16}\cdot 100\% = 0{,}2\cdot 10^{-9}\%$, czyli wykrywanie uszkodzeń testowanego urządzenia z prawdopodobieństwem 99,9999999997%.

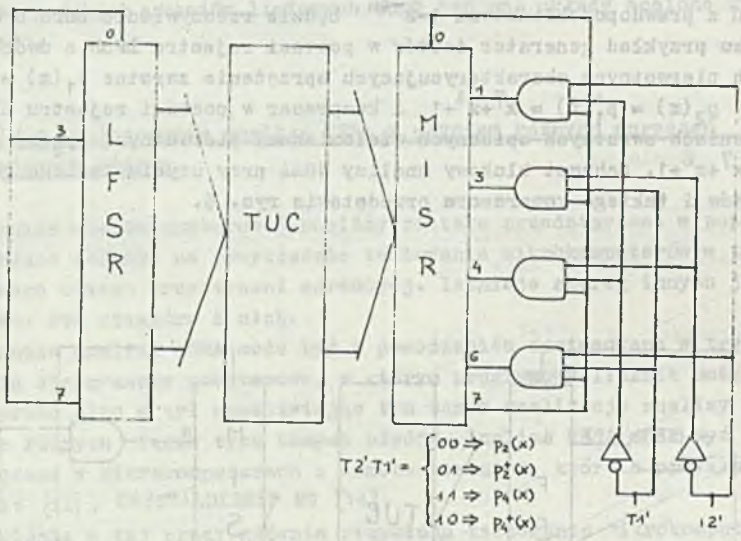
Łącząc ze sobą technikę analizy 2RSA z użyciem różnych sprzężeń i technikę analizy 2RSA z użyciem różnych ciągów tych samych błędów można uzyskać analizę 4RSA z użyciem jednocześnie różnych sprzężeń i różnych ciągów tych samych błędów. Jeżeli jako generatora testów wyczerpujących użyć rejestr LFSR o takich dwóch przełączanych sprzężeniach zwrotnych [4-5], że ciąg testów w drugim pomiarze będzie odwrotnością ciągu testów w pierwszym pomiarze, a jako kompresora użyć rejestr MISR o dwóch różnych sprzężeniach zwrotnych, wówczas koszt dodatkowego sprzętu umożliwiającego detekcję uszkodzeń z prawdopodobieństwem $1-2^{-4n}$ będzie rzeczywiście bardzo mały. Weźmy jako przykład generator testów w postaci rejestru LFSR o dwóch wielomianach pierwotnych charakteryzujących sprzężenie zwrotne $p_1(x) = x^7+x^3+1$ i $p_2(x) = p_1^+(x) = x^7+x^4+1$ i kompresor w postaci rejestru MISR o sprzężeniach zwrotnych opisanych wielomianami pierwotnymi $p_2(x)$ i $p_4(x) = x^7+x^6+1$. Schemat blokowy analizy 4RSA przy użyciu takiego generatora testów i takiego kompresora przedstawia rys. 6.



Rys. 6. Schemat blokowy analizy 4RSA przy użyciu jednocześnie różnych sprzężeń i różnych ciągów tych samych błędów

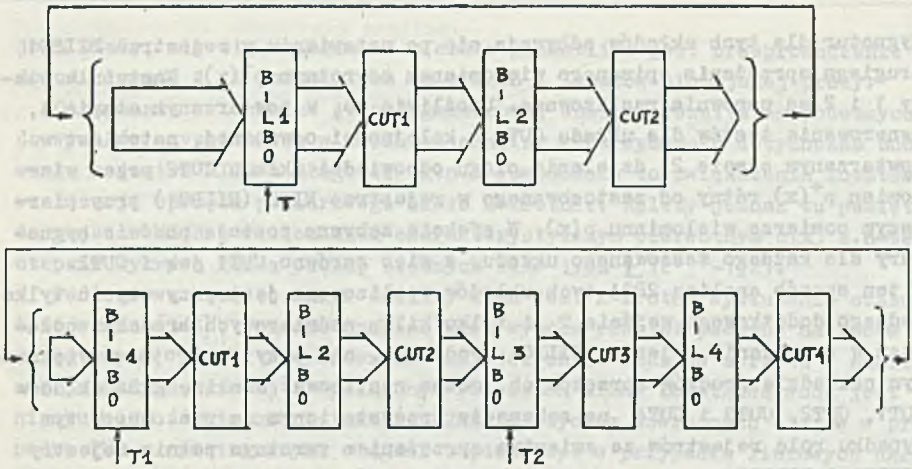
Fig. 6. Block diagram of analysis 4RSA using simultaneous different feedback and different sequences of the same faults

Dodatkowy koszt realizacji takiej techniki 4RSA wynosi w tym przykładzie 8 bramek XOR, AND, NOT i 14 połączeń, natomiast dodatkowy koszt realizacji techniki analizy jednosygnaturowej przy użyciu rejestru MISR o długości $4 \cdot n = 4 \cdot 7$ wyniósłby 21 przerzutników D, każdy złożony co najmniej z 6 bramek i 10 połączeń, co w sumie wyniosłoby 126 dodatkowych bramek i 210 dodatkowych połączeń. Porównania obu kosztów nie trzeba nawet komentować. Koszt dodatkowy takiej mieszanej techniki analizy 4RSA jest w wielu przypadkach także niższy od kosztu dodatkowego sprzętu niezbędnego do realizacji analizy 4RSA z użyciem czterech różnych sprzężeń zwrotnych. Weźmy jako przykład rejestr MISR ze sprzężeniami opisanymi wielomianami pierwotnymi $p_1(x) = p_2^+(x)$, $p_2(x)$, $p_3(x) = p_4^+(x)$ i $p_4(x)$ takimi samymi, jakie użyto w analizie 4RSA przedstawionej na rys. 6. Schemat blokowy analizy 4RSA przy użyciu takiego rejestru MISR przedstawia rys. 7.



Rys. 7. Schemat blokowy analizy 4RSA z użyciem 4 różnych sprzężeń
Fig. 7. Block diagram of analysis 4RSA using 4 different feedback

Dodatkowy koszt realizacji analizy 4RSA wyniósłby w tym przypadku 9 bramek XOR, AND, NOT i 20 połączeń, a więc byłby o 1 bramkę XOR i 6 połączeń droższy od koszt dodatkowego niezbędnego do realizacji analizy 4RSA podanej na rys. 6. Ten niezwykle niski koszt dodatkowego sprzętu predystynuje w niektórych przypadkach technikę analizy 4RSA z jednoczesnym użyciem różnych sprzężeń i różnych ciągów tych samych danych do wykorzystywania jej w elementach scalonych VLSI z samotestowaniem, w których każdy zbędny nakład sprzętu ma kolosalne znaczenie.



Rys. 8. Schemat blokowy analizy 2RSA w układach z rejestrem BILBO
Fig. 8. Block diagram of analysis 2RSA in system with BILBO register

Innym przykładem bardzo taniego sposobu zwiększania skuteczności równoległej analizy sygnaturowej są układy cyfrowe z samotestowaniem, wykorzystujące opisany w pracy [13] rejestr BILBO (Built-In Logic Block Observation). Rejestr ten umożliwia realizację analizy 2RSA przy użyciu zarówno dwóch różnych sprzężeń zwrotnych, jak i dwóch różnych (odwrotnych) ciągów tych samych błędów.

Przykłady takiego wykorzystania rejestru BILBO przedstawiono na rysunku 8. Rejestr BILBO1 (rys. 8a) zawiera dwa różne sprzężenia zwrotne opisane wielomianami $p(x)$ i $p^{+}(x)$, które można wybierać za pomocą zewnętrznego sygnału T. Natomiast rejestr BILBO2 jest wykonany tradycyjnie i posiada tylko jedno sprzężenie zwrotne. W pierwszym etapie analizy 2RSA rejestr BILBO1 z ustawionym sprzężeniem $p(x)$ pracuje jako generator testów pseudoprzypadkowych dla kombinacyjnego układu CUT1. Sekwencja słów-odpowiedzi układu CUT1 komprymowana jest w rejestrze BILBO2, który w tym czasie pracuje jako kompresor - rejestr MISR. Po wygenerowaniu wszystkich możliwych wektorów testujących w rejestrze BILBO2 powstaje sygnatura, którą następnie szeregowo wysuwa się z rejestru na zewnątrz, aby porównać ją z sygnaturą wzorcową. W drugim etapie testowania wszystkie wymienione operacje zostają powtórzone, ale przy zamienionych rolach rejestrów BILBO1 i 2. Rejestr BILBO2 staje się generatorem testów dla kombinacyjnego układu CUT2, podczas gdy BILBO1 pełni rolę kompresora odpowiedzi tego układu. Po zakończonej przez rejestr BILBO2 generacji testów uzyskana w rejestrze BILBO1 sygnatura zostaje z niego wysunięta, a następnie zweryfikowana. Te dwa etapy testowania miały dotąd charakter jednosygnaturowej analizy układów CUT1 i CUT2. Pomiary dwóch kolejnych

sygnatur dla tych układów odbywają się po ustawieniu w rejestrze BILBO1 drugiego sprzężenia opisanego wielomianem odwrotnym $p^+(x)$. Następnie etapy 1 i 2 są ponownie realizowane. Umożliwia to, w powtarzanym etapie 1, generowanie testów dla układu CUT1 w kolejności odwrotnej, natomiast w powtarzanym etapie 2 dzielenie ciągu odpowiedzi układu CUT2 przez wielomian $p^+(x)$ różny od zastosowanego w rejestrze MISR (BILBO1) przy pierwszym pomiarze wielomianu $p(x)$. W efekcie zebrane zostają po dwie sygnatury dla każdego testowanego układu, a więc zarówno CUT1 jak i CUT2. W ten sposób analiza 2RSA tych układów realizowana jest przy użyciu tylko jednego dodatkowego wejścia T i tylko kilku nadmiarowych bramek i połączeń w sprzężeniu rejestru BILBO1. Podobnie, ale przy dwukrotnie zwiększonym nakładzie środków sprzętowych, można realizować analizę 2RSA układów CUT1, CUT2, CUT3 i CUT4 na schemacie przedstawionym na rys. 8b. W tym wypadku rolę rejestrów ze zmiennym sprzężeniem zwrotnym pełnią rejestry BILBO1 i BILBO3.

7. Zakończenie

Technika wielosygnaturowej równoległej analizy uszkodzeń przedstawiona w tej pracy posiada istotną zaletę w porównaniu do techniki jednosygnaturowej analizy. Twierdzenie 1 i 2 (wnioski 1 i 2) wyraźnie wskazują, że analiza kRSA za pomocą rejestru MISR ze sprzężeniem wewnętrznym i o długości n umożliwia wykrywanie paczek błędnych słów $\mathbb{E}(k.n,t)$, $\mathbb{E}(m,1)$, $\mathbb{E}(2^n-1,2)$ oraz niewykrywanie pozostałych ciągów błędnych słów z częstotliwością 1 ciągu na $2^{k.n}$ ciągów. Tymczasem ten sam rejestr MISR o długości n w analizie jednosygnaturowej wykrywa tylko paczki błędnych słów $\mathbb{E}(n,t)$, $\mathbb{E}(m,1)$, $\mathbb{E}(2^n-1,2)$ oraz nie wykrywa pozostałych ciągów błędnych słów z częstotliwością większą o kilka rzędów, czyli około 1 ciągu na 2^n ciągów [6].

Tych samych rezultatów nie można uzyskać przy użyciu rejestru MISR z zewnętrznym sprzężeniem liniowym. Ten rejestr MISR, opisany w pracy [6] i [9], nie spełnia lematu 1, a w związku z tym i pozostałych twierdzeń i lematów tej pracy. Ciąg błędów $e_z(x)$ z wyrażenia 1, zgodnie z pracami [6] i [9], przyjmuje dla tego rejestru postać następującą:

$$\sum_{i=0}^{n-1} e_i(x).f_i(x) \quad \text{gdzie} \quad f_i(x) = \sum_{j=0}^{i} p_j x^{i-j}$$

Wyrażenie $f_i(x)$ jest w tym przypadku zależne od wielomianu $p_j(x)$ opisującego sprzężenie zewnętrzne rejestru MISR. W związku z tym w k różnych pomiarach dla różnych postaci wielomianu $p_j(x)$ ciąg błędów $e_z(x)$ nie

jest stały, ale się zmienia. W efekcie niemożliwe jest przeprowadzenie dowodu lematu 1 i pozostałych twierdzeń i lematów niniejszej pracy.

Otrzymanie w technice jednosygnaturowej analizy rezultatów podobnych do wyników uzyskiwanych w technice analizy kRSA wymagało dotychczas budowania rejestru MISR o długości k.n. Powodowało to zwiększenie kosztów realizacji sprzętu pomiarowego około k-krotnie. Należy jednak tu pamiętać, że rejestr MISR z wielomianem charakterystycznym pierwotnym p(x) k.n-tego stopnia wykrywa każdą paczkę błędnych słów typu $E(2^{k.n}-1,2)$.

Podstawową wadą techniki analizy kRSA jest k-krotne wydłużenie czasu testowania [3-4]. Ponadto analiza kRSA wymaga również pewnych nakładów sprzętowych, jednak nieporównanie mniejszych od kosztów sprzętu w analizie jednosygnaturowej z wydłużonym rejestrem MISR. Dodatkową wadą jest nieskuteczność stosowania analizy 2RSA z użyciem odwrotnych ciągów w przypadku TUC z symetrycznymi ciągami błędów, np. w przypadku liniowych układów kombinacyjnych.

Własności detekcyjne analizy kRSA omówiono w niniejszej pracy w oderwaniu od modelu uszkodzeń testowanego urządzenia. W pracy tej nie określono więc charakterystycznych uszkodzeń TUC, np. wąską próbą określenia takich uszkodzeń dla analizy jednosygnaturowej komputerów jest praca [13]. W dalszym ciągu otwarty jest więc problem określenia uszkodzeń charakterystycznych dla różnych TUC oraz mikrokomputera i wykrywanych na pewno za pomocą analizy kRSA.

LITERATURA

[1] Frohwerk A. Robert, Signature Analysis: A New Digital Field Service Method, Hewlett-Packard Journal, May 1977.

[2] Smith J.M .: Measures of the Effectiveness of Fault Signature Analysis, IEEE TC, vol, C-29, No 6, June 1980, pp. 510-514.

[3] Hławiczka A., Kubica H.: The Method of Increasing the Probability of Detecting Errors for Signature Analysis, Proceedings of International Conference on Fault Tolerant Systems Diagnostics, September 1981, Brno, pp. 273-277.

[4] Hławiczka A., Kubica H.: Sposób zwiększania prawdopodobieństwa i lokalizacji uszkodzeń techniką analizy sygnatur w systemach cyfrowych zwłaszcza mikrokomputerach, patent P-231306 z mocą od dnia 21.05.81.

[5] Hassan S.Z., Mc Cluskey E.J.: Increased Fault Coverage Through Multiple Signatures, Proc. of FTCS-14, June 1984, St. Cloud Hall, pp. 354--359.

[6] Hławiczka A.: Równoległa kompresja liniowa w analizie sygnaturowej uszkodzeń - Podstawy Teoretyczne. Archiwum Automatyki i Telemechaniki Nr 2 1988, a także Prace IPI PAN Nr 601, 1987.

[7] Hławiczka A.: Binary Implemented Compression of Multiple-Valued Data Serial Streams, Proc. of 14th ISMVL, May 1984, Winnipeg, Canada.

[8] Hławiczka A., Pach R.: Method for Compression of Serial Streams of Test Result Three State Data, Proc. of 6th International Conference on Fault-Tolerant Systems and Diagnostics, September 1983, Brno.

[9] Hławiczka A.: Compression of three-state data serial, streams by means of a parallel LFSR signature analyzer. IEEE Trans. Comput (USA) vol C-35, No 8, August 1986, pp. 732-741.

[10] Hławiczka A.: Binary Implemented Exhaustive Testing of Multi-Valued Logic Networks, Proc. of 16 th ISMVL, May 1986, Blacksburg, USA.

[11] Hławiczka A., Nowiński M.: Easy-To-Use Programmable Signature Analyzer PAS 80, Proc. of 6th Symposium on Reliability in Electronics RELECTRONIC 85, Budapest, August 1985, także po polsku w PAK nr 6 1985.

[12] Fasang Patrick P.: Microbit brings self-testing on board complex microcomputers, Elekctronics, March 10 1983, pp 116-119.

[13] Hławiczka A.: Fault Signature Effectiveness of Microconputer Address Bus, Electronics Letters 2nd August 1984 Vol. 20 Nr 16 pp. 645-646.

[14] Hławiczka A., Nikiel J.: Samotestowalne mikrokomputerowe urządzenie pomiarowe - CRYSTALDIGRAF NC, Elektronizacja (zaakceptowano do opublikowania).

PODZIEKOWANIE

Składam podziękowanie Prof. dr hab. inż. F. Wagnerowi, dr. J. Chojcanowi, dr. M. Nowińskiemu oraz mgr inż. K. Mostowskiemu za krytyczne uwagi, dzięki którym praca zyskała na wartości.

Recenzent: Prof. dr hab. inż. Ferdynand WAGNER

Wpłynęło do Redakcji 16.05.85 r.

МНОГОСИГНАТУРНЫЙ ПАРАЛЛЕЛЬНЫЙ АНАЛИЗ ОТКАЗОВ В ЦИФРОВОЙ СИСТЕМЕ

Р е з ю м е

В статье даётся иделя параллельнлгл многосигнатерного анализа (к - сигнатурного) отказов в цифровых системах, в частности в ядре микрокомпьютера опрашиваемого по схеме свободного обега адрессного пространства (фри ран). В статье представлено несколько способов провидения такого анализа при помощи n- битового параллельного регистра с внутренней линейной обратной связью. Доказано, что при небольших издержах на оборудование, получается вероятность обнаружения ошибки в виде $1 - 2^{2-kn}$, также открывается возможность обнаружения на любом входе параллельного регистра группой ошибки длиныне более kn. Статью закончено описанием нескольких примеров применения многосигнатурного анализа.

PARALLEL MULTISIGNATURE ANALYSIS OF FAULTS IN THE DIGITAL SYSTEM

S u m m a r y

The paper presents a scheme of the parallel multisignature (k-signature) analysis of digital circuits faults. In particular the multisignature analysis of microcomputer faults carried out in the free run mode using the Multi-Input Shift Register (MISR) with a length n has been discussed. Some techniques of such an analysis realization have been described. It has been proved that with very low additional hardware expenses a probability of error detection is obtained equal to $1-2^{-kn}$. as well as a possibility of n-burst erroneous bits detection inclued in the kn bits section of any sequence applied to any of inputs of the MISR. Finally, a few examples of using of the parallel multisignature analysis are given in the paper.