Politechnika Poznańska
Wydział Informatyki
Katedra Inżynierii Komputerowej

Rekonfigurowalny hybrydowy generator chaotyczny dla kryptografii sprzętowej

Streszczenie rozprawy doktorskiej

Michał Melosik

Promotor główny: Wiesław Marszałek
Rutgers University, NJ, USA

Promotor pomocniczy: Paweł Śniatała
Politechnika Poznańska

Poznań, 2017

Spis treści

Rozdział 1

Wstęp

1.1 Obszar badań

Projektowanie kryptograficznych systemów wbudowanych wymaga uwzględnienia wzajemnych powiązań między informatyką i elektroniką. Szczególną rolę zaczyna odgrywać inżynieria komputerowa scalająca ze sobą zagadnienia związane z architekturą sprzętową systemów wbudowanych przy jednoczesnym uwzględnieniu wybranych aspektów warstwy programowej. Ze względu na specyfikę systemów wbudowanych trudno jest jednoznacznie wskazać gdzie zacierają się granice między elektroniką a informatyką. Przy obecnym rozwoju technologicznym dyscypliny te ściśle się przenikają a ich rozdzielenie w zaawansowanych systemach nie jest już możliwe. System operacyjny oraz oprogramowanie narażone są na działanie złośliwego oprogramowania takiego jak wirusy lub trojany. Problem ten można rozwiązać zapewniając ochronę w postaci oprogramowania antywirusowego. Innym rozwiązaniem często stosowanym w urządzeniach mobilnych jest przeniesienie najbardziej newralgicznych modułów bezpieczeństwa do warstwy sprzętowej. Realizacja sprzętowa dotyczy głównie kluczowych modułów bezpieczeństwa takich jak generatory liczb losowych lub algorytmy kryptograficzne. Podejście takie w podstawowym założeniu miało gwarantować ochronę przed działaniem złośliwego oprogramowania. W ostatnich dziesięciu latach pojawiły się nowe zagrożenia w postaci ataków z całkowitym pominięciem systemu operacyjnego i oprogramowania urządzenia mobilnego. Ten specyficzny rodzaj zagrożenia określany jest terminem trojanów sprzętowych (ang. *hardware trojans*) [1–4].

Zgodnie z definicją podaną w [1] za trojan sprzętowy uważa się: *"dodatkowy obwód lub zmianę (parametrów, połączeń) wprowadzoną do układu z wrogim zamiarem, która nie może zostać wykryta w ramach podstawowego procesu testowania."*

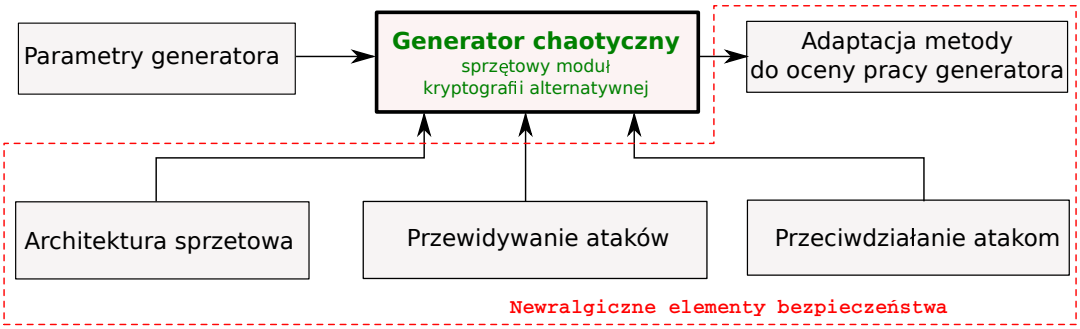
Trojany sprzętowe zmniejszają poziom bezpieczeństwa całego systemu bez ingerencji w warstwę oprogramowania. Bagatelizowanie trojanów sprzętowych może skutkować dokonaniem ataków sprzętowych, praktycznie niewykrywalnych dla użytkownika końcowego.

Nowe formy zagrożeń wymusiły poszukiwanie interdyscyplinarnych metod bezpieczeństwa takich jak kryptografia kwantowa i chaotyczna. Pomimo intensywnych badań w zakresie kryptografii kwantowej nie udało się opracować takich modułów kwantowych, które pozwalałby na bezpośrednia integrację z układem ASIC (ang. *Application Specific Integrated Circuit*) lub strukturą matrycy FPGA (ang. *Field-Programmable Gate Array*) [5]. W odróżnieniu od kryptografii kwantowej, moduły kryptografii chaotycznej mogą zostać poddane miniaturyzacji - nawet do rozmiarów układów scalonych [6, 7]. Aktualne obszary badań nad kryptografią chaotyczną skupiają się nad oceną poziomu jej bezpieczeństwa, wykrywaniem i eliminacją czynników zagrożeń umożliwiających przeprowadzenie ataku sprzętowego [8, 9]. Szczególnie kluczowe znaczenie zyskują badania w zakresie podatności wprowadzania trojanów sprzętowych do generatorów chaotycznych. Do tej pory w badaniach nad generatorami chaotycznymi używanymi w kryptografii nie została podjęta próba oceny zagrożenia ze strony trojanów sprzętowych [10, 11]. Nie jest również znana żadna koncepcja zapobiegania tego typu zagrożeniom.

1.2 Cel i zakres pracy

W ramach prowadzonych badań należy dokonać selekcji najbardziej newralgicznych elementów bezpieczeństwa w tradycyjnym generatorze chaotycznym tak jak pokazano na rysunku 1.1. Badania przedstawione w pracy oparte są na symulacjach komputerowych z wykorzystaniem środowisk: *Matlab, RStudio, Mentor Graphics SystemVision, LTSpice* oraz *AnnadigmDesigner*. Ze względu na teoretyczno-koncepcyjny charakter pracy dla warstwy sprzętowej zakłada się użycie tylko matrycy FPAA (ang. *Field Programmable Analog Array*). Badania zostały podzielone na cztery etapy:

- adaptacja metod do oceny dynamiki chaotycznej generowanej sekwencji binarnej,
- zdefiniowanie problemów bezpieczeństwa w wybranych sprzętowych generatorach chaotycznych,
- opracowanie koncepcji struktury hybrydowej generatora chaotycznego,
- analiza porównawcza bezpieczeństwa hybrydowego generatora chaotycznego z generatorem kwantowym,



Rysunek 1.1: Wymogi generatora chaotycznego jako sprzętowego modułu kryptografii alternatywnej.

Do tej pory w badaniach nad zastosowaniem obwodów chaotycznych w kryptografii problem trojanów sprzętowych nie był rozpatrywany. Tym samym brak jest skutecznego rozwiązania zapewniającego generację sygnałów chaotycznych w przypadku ataku sprzętowego. Rosnąca potrzeba zapewnienia bezpieczeństwa systemów wbudowanych potwierdza potrzebę podjęcia pogłębionych badań w tym zakresie.

Rozdział 2

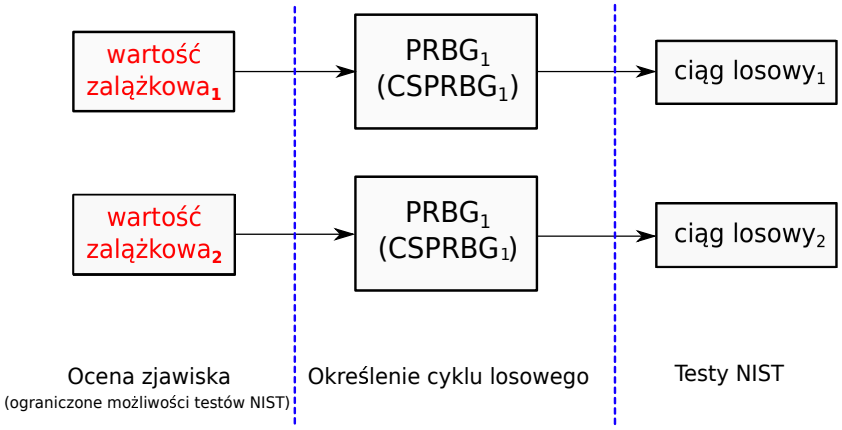
Kryptografia w systemach wbudowanych

2.1 Podstawowe wymogi bezpieczeństwa

Obecnie prawie każdy system kryptograficzny posiada zintegrowany generator pseudolosowy dla zapewnienia bezpiecznego procesu kryptograficznego. Struktury zastosowanego generatora uzależnione są od wolnych zasobów w warstwie sprzętowej. Do najbardziej znanych generatorów należą A5/1 [12] oraz Fortuna [13]. Sprzętowe moduły kryptograficzne przed implementacją w docelowej infrastrukturze elektronicznej powinny zostać poddane ocenie pod kątem spełnienia kilku niezależnych kryteriów bezpieczeństwa. Dla generatorów losowych kryteria te można podzielić na trzy grupy [14]:

- analizę losowości,
- badanie źródła wartości zalążkowej,
- analizę fizycznej budowy modułu kryptograficznego pod kątem jego podatności na ataki sprzętowe.

W większości praktycznych rozwiązań ocena bezpieczeństwa generatorów losowych sprowadzana jest niestety tylko do pierwszej grupy. Ocena losowości dokonywana jest w oparciu o zestaw piętnastu testów statystycznych NIST badających ciągi o długości nie mniejszej niż 1 milion bitów [15]. Należy zwrócić uwagę, że pakiet z testami NIST został przygotowany tak aby użytkownik zwolniony był z konieczności posiadania specjalistycznej wiedzy eksperckiej z zakresu podstaw matematycznych dla każdej ze stosowanych metod statystycznych. Uzyskanie pozytywnych wyników dla kilkunastu testów potwierdza losowy charakter badanej



Rysunek 2.1: Zależność sekwencji pseudolosowej od wartości zalążkowej inicjującej niezmienny generator pseudolosowy.

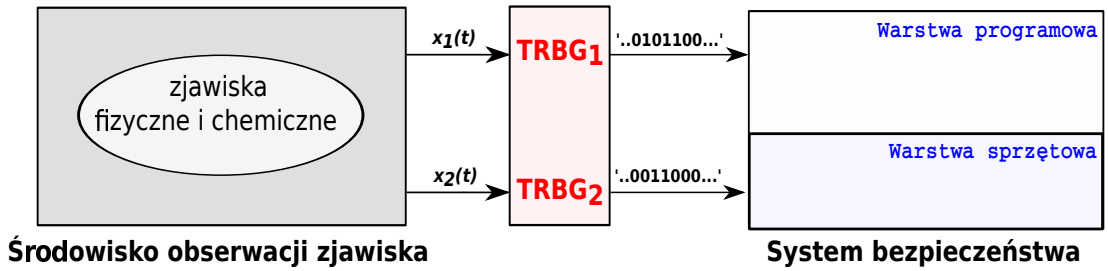
sekwencji. Mimo powszechnego stosowania metody opartej na testach statystycznych NIST wykazano w [16] ze nie zawsze uzyskane wyniki można traktować wiarygodnie.

Drugim kryterium jest badanie źródła wartości zalążkowych przez ocenę jego entropii. Zgodnie z [17] ocena poziomu entropii może być używana zamiennie w stosunku dla metody opartej na testach statystycznych NIST.

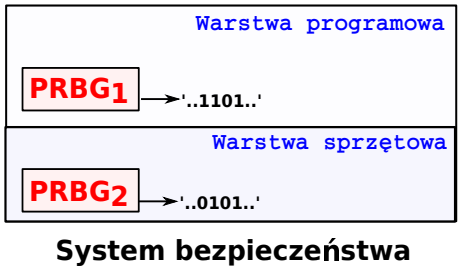
Bezpieczeństwo w kryptografii sprzętowej uwarunkowane jest również sposobem fizycznej realizacji konkretnych układów. Kluczowa staje się analiza struktury układu pod względem ilości zastosowanych źródeł entropii oraz sposobu ich realizacji. Zgodnie z [13, 18] zaleca się, aby generatory sekwencji losowych nie były ograniczone tylko do jednego źródła entropii. Układy w kryptografii sprzętowej z jednym źródłem losowości cechują się niskim poziomem bezpieczeństwa - istnieje (często tylko domniemane) ryzyko możliwości wrogiego oddziaływania na źródło entropii. Na rysunku 2.1 przedstawiono znaczenie doboru nieprzewidywalnej wartości zalążkowej w celu generacji unikatowej sekwencji losowej. Wielokrotne użycie tej samej wartości zalążkowej skutkować będzie generowaniem takiego samego ciągu losowego w następnym cyklu pracy generatora pseudolosowego. Do tej pory znane ataki na generatory pseudolosowe dotyczyły możliwości przewidywania ich okresu [19, 20]. Biorąc pod uwagę schemat z rysunku 2.1 skuteczniejszym atakiem może okazać się bezpośrednia modyfikacja generatora zalążkowego.

2.2 Ograniczenia technologiczne

Wybór generatora losowego dla konkretnego systemu wbudowanego uzależniony jest od czasu potrzebnego do wygenerowania odpowiedniej sekwencji losowej [13]. Rejestracja ciągów



(a)



(b)

Rysunek 2.2: Generacja ciągu prawdziwie i pseudolosowego w systemach wbudowanych.

losowych pochodzących z obserwacji procesu fizycznego może być procesem długotrwałym. Ograniczenia technologiczne dotyczące natury zjawiska uniemożliwią miniaturyzację i integrację generatorów prawdziwie losowych z układami mikroelektronicznymi [5].

Na rysunku 2.2 przedstawiono schemat formowania binarnej sekwencji losowej tworzonej z obserwacji zjawiska fizycznego. W obserwowanych zjawiskach rejestrowane są sygnały ciągłe - rysunek 2.2(a). Przy użyciu odpowiedniej funkcji formującej (komparatora wartości) tworzona jest binarna sekwencja losowa. Poziom progowy w komparatorze ustalany jest tak aby uzyskać możliwie największy poziom entropii. W generatorach prawdziwie losowych (ang. *True Random Bit Generator*) podczas formowania sekwencji binarnej powstają przedziały z nadmiarem tych samych wartości (ang. *bias*). Eliminacja przedziałów tych dokonywana jest przez zastosowanie ekstraktora losowości (czerwony blok na rysunku 2.2(a)). Złożone zaplecze do obserwacji zjawiska w kontekście kryptograficznych urządzeń mobilnych nie znajduje praktycznego zastosowania ze względu na rozmiary aparatury oraz specyfikę samego zjawiska. Uzasadnione w systemach wbudowanych staje się użycie innych generatorów pozwalających na ich bezpośrednią integrację z systemem wbudowanym. Uwarunkowania współczesnych cyfrowych systemów transmisji, układów zabezpieczenia danych, wymuszają stosowanie generatorów pseudolosowych, w których ciąg losowy formowany jest stosunkowo szybko bez specjalistycznych wymagań związanych ze środowiskiem obserwacji oraz aparatury rejestracyjnej.

Rozdział 3

Ocena bezpieczeństwa generatorów chaotycznych

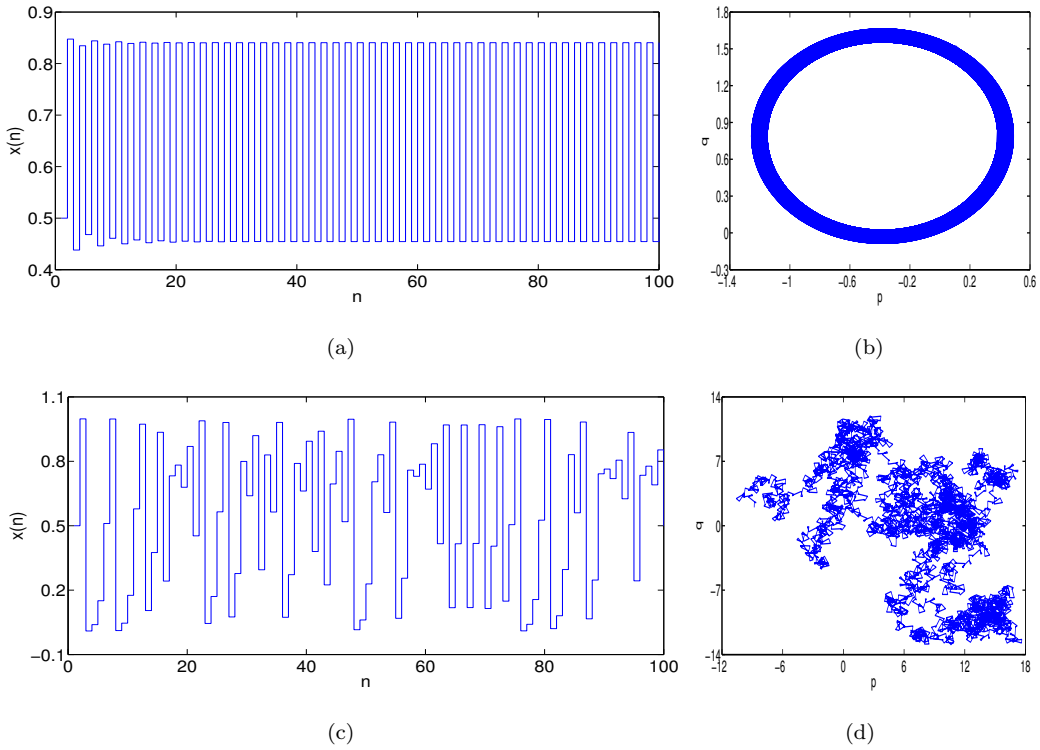
3.1 Chaos w sekwencjach binarnych

Test 0-1 do detekcji chaosu jest stosunkowo nowym aparatem matematycznym używanym do wykrywania dynamiki chaotycznej dla wektora wartości pochodzącego z systemu dla którego model matematyczny nie jest znany [21]. Wyniki reprezentowane są w postaci numerycznej (liczba rzeczywista K z przedziału [0,1]) oraz graficznej (dwuwymiarowa reprezentacja specjalnych zmiennych dynamicznych p_c i q_c - przykładowa reprezentacja dla wyników otrzymanych z równania logistycznego została przedstawiona na rysunku 3.1). W przypadku wykrycia sekwencji regularnej wartość liczby K jest bliska 0. Dla sekwencji chaotycznej wartość K dąży do 1. Obliczanie wartości K dokonywane jest przy użyciu jednej z dwóch niezależnych metod: regresji lub korelacji. Dla sekwencji $\{N_k\}$, $k = 0, \ldots, \overline{N} - 1$, zmienne p_c i q_c są obliczane zgodnie z poniższymi zależnościami dla losowo wybranej liczby c z przedziału $(0, \pi)$

$$p_c(n) = \sum_{j=0}^{n} N_j cos[(j+1)c], \quad q_c(n) = \sum_{j=0}^{n} N_j sin[(j+1)c] \tag{3.1}$$

gdzie $n = 0, \ldots, \overline{N} - 1$ [22]. Dla uzyskanych zmiennych dynamicznych p_c i q_c dokonuje się obliczenia przesunięcia średnio kwadratowego $M_c(n)$, $n = 0, 1, \ldots, n_{cut}$, dla p_c i q_c z rekomendowaną wartością $n_{cut} \approx (\overline{N} - 1)/10$

$$M_c(n) = \lim_{\overline{N} \to \infty} \frac{1}{\overline{N} - 1} \sum_{j=0}^{\overline{N}-1} [p_c(j+n) - p_c(j)]^2 + [q_c(j+n) - q_c(j)]^2. \tag{3.2}$$



Rysunek 3.1: Odpowiedź układu opartego na równaniu logistycznym dla różnych wartości parametru μ w równaniu logistycznym: (a)-(b) $\mu = 3{,}39$ oraz (c)-(d) $\mu = 3{,}99$.

W metodzie regresji należy wyznaczyć asymptotyczny współczynnik wzrostu K_c dla przesunięcia średnio kwadratowego zgodnie z zależnością

$$K_c = \lim_{n\to\infty} \frac{log\, M_c(n)}{log\, n}. \tag{3.3}$$

Stosując natomiast metodę korelacji należy utworzyć dwa osobne wektory $\xi = (0, 1, 2, \ldots, n_{cut})$ oraz $\Delta = (M_c(0), M_c(1), M_c(2), \ldots, M_c(n_{cut}))$. Współczynnik korelacji K_c obliczany jest zgodnie z zależnością

$$K_c = corr(\xi, \Delta) \equiv \frac{cov(\xi, \Delta)}{\sqrt{var(\xi) var(\Delta)}} \tag{3.4}$$

gdzie *cov* i *var* oznaczają odpowiednio kowariancję i wariancję. W obu metodach powyższe kroki są powtarzane dla N_c losowych wartości c z przedziału $(0, \pi)$. Zgodnie z [22] zaleca się aby $N_c = 100$. Ostateczna wartość K obliczana jest jako mediana N_c wartości liczb K_c. Jeżeli $K \approx 1$ wtedy uznaje się wektor $\{N_k\}$ jako chaotyczny. Uzyskanie wyniku $K \approx 0$ wskazuje natomiast na wykrycie sekwencji regularnej - niechaotycznej.

W pracy przedstawiono nową metodę rozwiązania problemu nadpróbkowania sygnałów chaotycznych z czasem ciągłym. Metoda ta oparta jest na kryterium częstotliwościowym i została porównana ze znanym kryterium miary informacji wzajemnej.

Rozdział 4

Ataki sprzętowe w kryptografii chaotycznej

4.1 Zakres bezpieczeństwa sprzętowego

W literaturze wyróżnia się dwie grupy ataków sprzętowych - z użyciem metod inwazyjnych i nieinwazyjnych [23]. Pierwsza związana jest z fizyczną ingerencją w strukturę np. układu scalonego. Druga grupa ataków dotyczy aktywacji podukładu w obwodzie scalonym, matrycy FPGA lub obwodzie drukowanym, którego umieszczenie odbyło się w sposób nieautoryzowany. W literaturze przedmiotu nie została opisana uniwersalna metoda zabezpieczania warstwy sprzętowej systemów wbudowanych przed atakami sprzętowymi.

Firma IBM zaproponowała podział na sześć poziomów bezpieczeństwa sprzętowego systemów wbudowanych [23, 24]:

1. **Poziom zerowy:** brak technik zabezpieczających w module sprzętowym. Moduł posiada swobodny dostęp do swojej struktury umożliwiający tym samym dokonanie nieautoryzowanych modyfikacji.

2. **Poziom niski:** zastosowano proste techniki zabezpieczające, które mogą zostać pominięte przy pomocy podstawowej aparatury laboratoryjnej. Całkowita wysokość nakładów finansowych potrzebnych na przeprowadzenie ataku nie przekracza $1000.

3. **Poziom średnio-niski:** moduł wykazuje odporność na proste ataki wymagające niskich nakładów finansowych. Przeprowadzenie skutecznego ataku wymaga zastosowania minimalnego zakresu wiedzy eksperckiej oraz specjalistycznych umiejętności. Całkowity koszt pozwalający na przeprowadzenie ataku nie przekracza $10 000.

4. **Poziom średni:** skuteczność ataku uzależniona jest od wiedzy eksperckiej oraz specjalistycznych informacji z zakresu funkcjonowania układu. Przeprowadzenie ataku musi zostać dokonane w warunkach specjalistycznego laboratorium układów mikroelektronicznych. Poniesione nakłady finansowe przekraczają $100 000.

5. **Poziom średnio-wysoki:** do przeprowadzenia ataku konieczna jest dogłębna analiza wszystkich mechanizmów zabezpieczających zintegrowanych w układzie. W analizie mechanizmów zabezpieczających konieczne jest wykorzystanie wysoko specjalistycznej aparatury z dedykowanym zapleczem laboratoryjnym. Szacowane nakłady finansowe oscylują w granicach $1 000 000. Skuteczność ataku zależy od dobrze skoordynowanej współpracy wielu ekspertów posiadających specjalistyczną wiedzę z zakresu wykorzystywanego zaplecza laboratoryjnego, struktury modułu, funkcji jego przeznaczenia oraz zastosowanych mechanizmów ochrony.

6. **Poziom wysoki:** układ wykazuje całkowitą odporność na wszystkie znane ataki sprzętowe. Aby dokonać nieautoryzowanego ataku zespół ekspertów z różnych dziedzin (elektroniki, informatyki, inżynierii komputerowej, telekomunikacji, fizyki, matematyki) musi opracować nowe nieznane do tej pory skuteczne scenariusze ataków. Badania nad możliwościami przeprowadzenia skutecznego ataku mogą wiązać się z koniecznością konstrukcji nowej dedykowanej aparatury. Skuteczność przeprowadzeniu ataku jest niepewna.

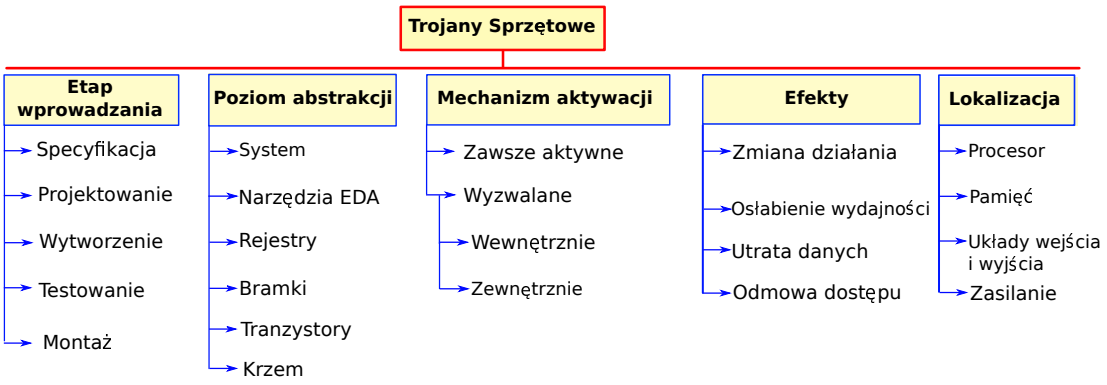
Niezależna klasyfikacja bezpieczeństwa sprzętowego związana ściśle z układami kryptograficznymi została opracowana przez NIST [23, 25]. Klasyfikacja wyróżnia cztery poziomy o zróżnicowanym zabezpieczeniu modułów kryptograficznych:

1. **Poziom 1:** spełnione minimalne wymagania w zakresie zapewnienia bezpieczeństwa modułu kryptograficznego. Zastosowane mechanizmy obronne nie gwarantują skutecznego bezpieczeństwa sprzętowego.

2. **Poziom 2:** poprawa poziomu bezpieczeństwa z poziomu 1 przez zastosowanie dodatkowych wymogów uwzględniających specjalną osłonę lub plombę zabezpieczającą przed dokonaniem nieautoryzowanej modyfikacji w układzie.

3. **Poziom 3:** zwiększona ochrona przed fizyczną ingerencją w układ zapobiegająca dostępowi do newralgicznych elementów struktury modułu.

4. **Poziom 4:** najwyższy możliwy poziom bezpieczeństwa. Odporność na ataki zapewniona jest dzięki zastosowaniu specjalnej osłony modułu kryptograficznego pozwalającej na wykrycie jakiejkolwiek ingerencji w układ.



Rysunek 4.1: Podział i klasyfikacja trojanów sprzętowych według [26].

4.2 Trojany w generatorach chaotycznych

Ogólny podział trojanów sprzętowych w literaturze został dokonany ze względu na pięć kryteriów zgodnie z rysunkiem 4.1 [26]. Szczególny problem bezpieczeństwa systemów elektronicznych bezpośrednio na poziomie obwodu drukowanego został po raz pierwszy opisany dopiero w roku 2015 na łamach *IEEE Design and Tests* [27]. W kontekście generatorów binarnych sekwencji chaotycznych niebezpieczeństwo wprowadzania trojanów na etapie montażu zostało przedstawione w [28]. Bezpieczeństwo obwodów drukowanych jest obecnie jednym z kluczowych wyzwań w projektowaniu sprzętowego systemów wbudowanych [1]. Obwody chaotyczne stosowane jako generatory wartości zalążkowych nie były do tej pory analizowane w literaturze pod kątem podatności na oddziaływanie trojanów sprzętowych. Weryfikacja poprawności ich działania odbywa się podczas etapu testowania w idealnych warunkach laboratoryjnych [11]. Znane badania laboratoryjne do tej pory nie podejmowały analizy konsekwencji modyfikacji struktury obwodów i jej wpływu na różnorodność generowanych sekwencji zalążkowych. W idealnych warunkach testowych obwód chaotyczny będzie zachowywał się prawidłowo. Dopiero jego montaż w urządzeniu docelowym może zostać powiązany z jednoczesnym umieszczeniem lub aktywacji trojanu wcześniej zintegrowanego z obwodem drukowanym.

W pracy przedstawiono nowe modele trojanów sprzętowych wprowadzone do obwodu chaotycznego Chua w realizacji Matsumoto oraz obwodu LMT (*Lindberg-Murali-Tamasevicius*) [29]. Atak sprzętowy w tych generatorach skutkuje zanikiem właściwości chaotycznych oraz generowaniem sygnałów okresowych. Dodatkowo dokonano analizy synchronizacji obwodów Chua jako metody ataku powielającego użycie takich samych wartości zalążkowych. Dla generatora chaotycznego opartego na równaniu logistycznym opracowano model trojanu sprzętowego zmniejszającego precyzję w arytmetyce stałoprzecinkowej. Jako metodę wykrywania obecności trojanów z powodzeniem użyto testu 0-1.

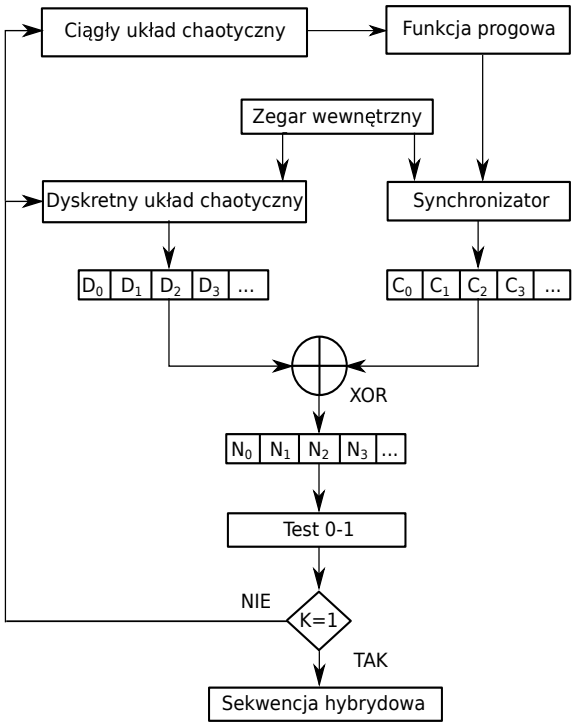
Rozdział 5

Hybrydowy generator chaotyczny

5.1 Konfiguracja modułowa

Analiza zagrożeń ze strony różnorodnych trojanów sprzętowych opisanych w rozdziale 4 stanowi podstawę do podjęcia próby opracowania koncepcji generatora chaotycznego nowego typu o strukturze hybrydowej przystosowanej do implementacji jako system rekonfigurowalny. Typowe generatory chaotyczne używane jako źródła entropii w generatorach pseudolosowych wykorzystują tylko jeden niezależny obwód chaotyczny. Takie podejście pod względem bezpieczeństwa jest niewystarczające. Sekwencja generowana przez pojedynczy generator czasu ciągłego może zostać zsynchronizowana z innym generatorem chaotycznym. Przypadek ten stwarza możliwość ponownego wykorzystania tej samej wartości zalążkowej przez PRBG. Natomiast użycie samego niezależnego generatora chaotycznego czasu dyskretnego może skutkować powstaniem okresowości sygnału nawet dla bardzo długich sekwencji [16]. Problemy te wymagają opracowania właściwego mechanizmu ochronnego.

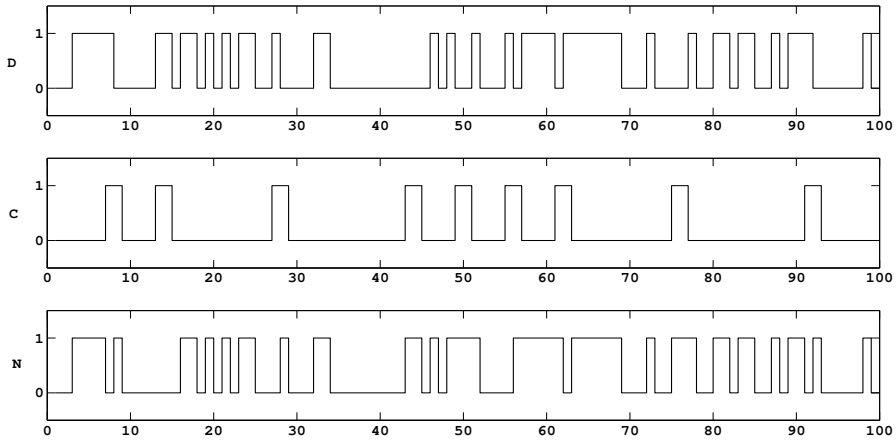
Na rysunku 5.1 przedstawioną strukturę nowego hybrydowego generatora chaotycznego. Do zastosowania jako generatory ciągłe przewidziano obwody Chua, Rösslera, Lorenza, układ z oscylacjami mieszanymi MMO (ang. mixed-mode oscillations), a jako dyskretne generatory Henona, Tinkerbella, Lozi, Gingerbreadmen oraz Bakera. Najprostszym w bezpośredniej realizacji cyfrowej jest układ oparty na równaniu logistycznym. Implementacja hybrydowego generatora chaotycznego na etapie procesu wdrożeniowego może zostać podzielona na trzy kategorie:



Rysunek 5.1: Koncepcja hybrydowego generatora chaotycznego.

- niezależna realizacja modułów w analogowych układach reprogramowalnych FPAA oraz cyfrowych układach reprogramowalnych FPGA,
- wytworzenie w technologii CMOS układu ASIC zawierającego na jednym podłożu krzemowym układ analogowy i cyfrowy opracowany jako niezależny IPCore,
- realizacja mieszana programowo-sprzętowa, w której moduł analogowy zostaje realizowany sprzętowo, a cyfrowy jest typową realizacją programową symulującą sprzętowe operacje arytmetyczne w zapisie stałoprzecinkowym.

Trzecia kategoria jest najbardziej uniwersalna. Dla przypadku, w którym część programowa jest celem ataku moduł analogowy na matrycy FPAA będzie odpowiedzialny za minimalizację negatywnych skutków. Dodatkowo zastosowanie matrycy FPAA uniemożliwia dokonanie nieautoryzowanych zmian w strukturze analogowego obwodu chaotycznego.



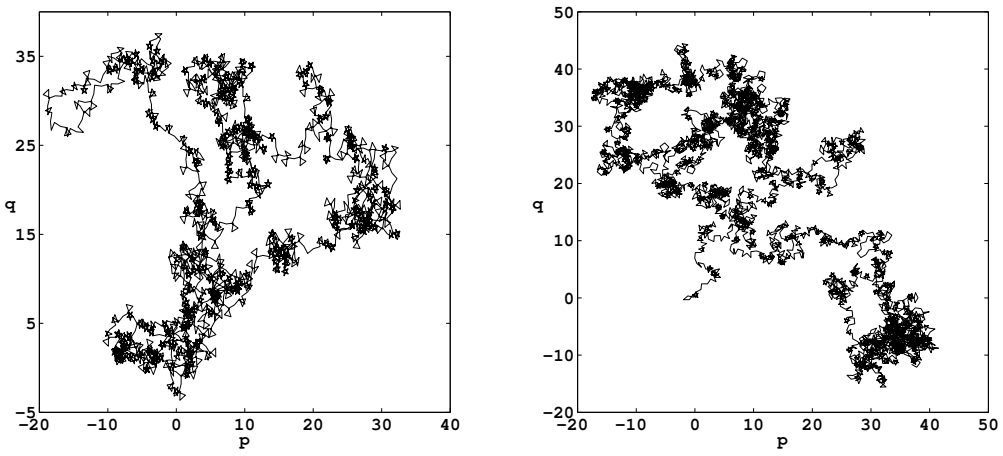
Rysunek 5.2: Sekwencje bitów chaotycznych D, C oraz N dla obwodu Chua.

5.2 Hybrydowa sekwencja chaotyczna

W modelu hybrydowym nowa sekwencja chaotyczna tworzona jest z dwóch binarnych sekwencji chaotycznych generowanych niezależnie przez moduł analogowy i cyfrowy. Mieszanie wektorów D i C z rysunku 5.1 w celu utworzenia sekwencji N odbywa się przez zastosowanie operacji XOR. Wiarygodne bezpieczeństwo tej operacji znane jest w kryptografii m.in. z procesu szyfrowania z kluczem jednorazowym (ang. *one time pad*). Test 0-1 interpretuje sekwencję bitów N jako chaotyczną gdyż $K = 0{,}9984$. Na rysunku 5.2 przedstawiono wyniki symulacyjne (100 pierwszych bitów) Wektor D powstaje z rejestracji bitów na konkretnej pozycji bitu w reprezentacji stałoprzecinkowej kolejnych wartości równania logistycznego. Zastosowanie reprezentacji stałoprzecinkowej w programie komputerowym zapewnia możliwość odtworzenia działania w warstwie sprzętowej na matrycach FPGA.

5.2.1 Odporność parametrów generatora cyfrowego

Zakładając wystarczająco dokładną precyzję obliczeniową w części cyfrowej podtrzymującą właściwości chaotyczne generatora opartego na równaniu logistycznym nadal istnieje możliwość wpływania na zmianę zachowania układu przez wprowadzenie trojanu zmieniającego wartość parametru μ w równaniu logistycznym $x(n+1) = \mu x(n)[1 - x(n)]$. Trojan dokonujący zmian bezpośrednio w rejestrze bitów przechowującym wartość μ jest trudny w wykryciu ze względu na jego minimalne wymagania sprzętowe, a skutkiem jego aktywności jest dokonanie trwałej rekonfiguracji generatora opartego na równaniu logistycznym przez zmianę wartości parametru na przykład z $\mu = 3{,}99$ na $\mu = 3{,}50$. Zmiana taka powoduje przejście generatora z trybu chaotycznego w tryb regularny. Na rysunku 5.3 pokazano wykresy zachowania zmiennych dynamicznych $p_c - q_c$ dla sekwencji hybrydowej w zależności od zmian



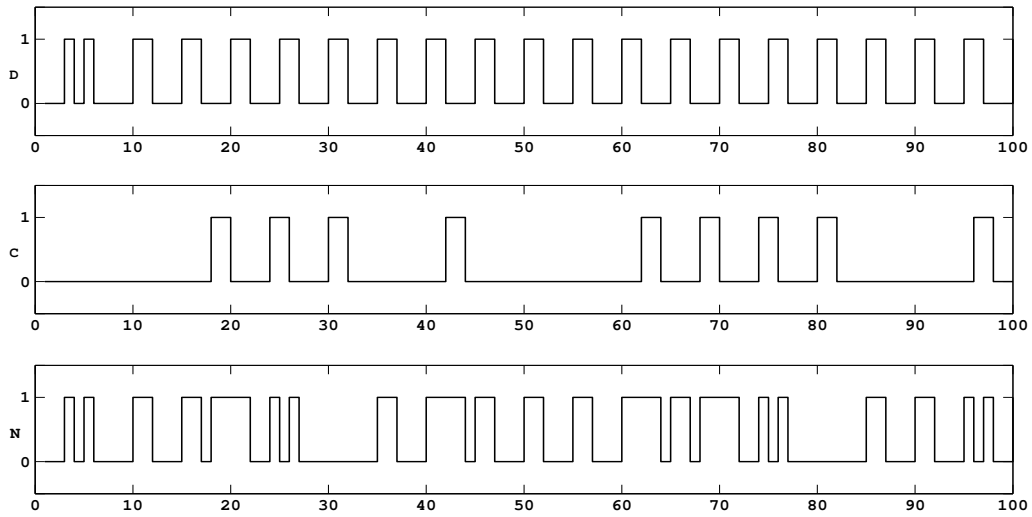
(a) (b)

Rysunek 5.3: Wyniki testu 0-1 dla hybrydowej sekwencji chaotycznej z parametrem $\mu = 3{,}50$ (a) i $\mu = 3{,}99$ (b).

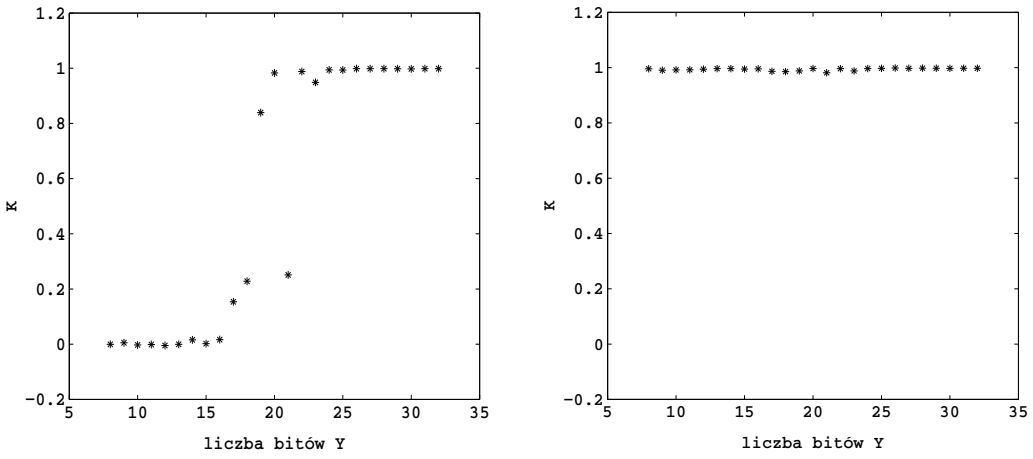
wartości parametru μ w module cyfrowym hybrydowego generatora chaotycznego z ciągłymi i dyskretnymi sekwencjami wejściowymi. Wyniki testu 0-1 wynoszą odpowiednio K=0,9974 dla rysunku (a) i K=0,9984 dla rysunku (b). Analiza wyników testu 0-1 wskazuje, że aktywność trojanu dokonującego rekonfiguracji wartości parametrów generatora nie wpływa na utratę właściwości chaotycznych w sekwencji N.

5.2.2 Odporność dokładności obliczeniowej

Na rysunku 5.4 widoczny jest skutek ataku zmniejszającego dokładność obliczeniową w sekwencji bitów przeznaczonych do reprezentacji części ułamkowej wartości dyskretnych w układzie opartym na równaniu logistycznym. W wyniku ataku sprzętowego nastąpiła redukcja do 12 bitów części ułamkowej. Zamiast oczekiwanej sekwencji chaotycznej o dużej różnorodności w występowaniu bitów w wektorze D układ generuje regularny (periodyczny) wektor z wartościami 0 i 1. Algorytm formowania hybrydowej sekwencji chaotycznej zapewnia podtrzymanie generowania nieprzewidywalnej sekwencji chaotycznej przez utworzenie ciągu N ze względu na operację mieszania $N = D\ (XOR)\ C$. Analiza sekwencji z rysunku 5.4 pokazuje, że nawet w przypadku ataku sprzętowego na jeden z modułów składowych modelu hybrydowego końcowa sekwencja chaotyczna charakteryzuje się nieprzewidywalnością i pozwala na użycie jej jako wartości zalążkowej w generatorach pseudolosowych. Na rysunku 5.5 zostały przedstawione wyniki testu 0-1 dla sekwencji N tworzonej z połączenia regularnej sekwencji



Rysunek 5.4: Poprawna (bezpieczna) praca generatora hybrydowego w przypadku działania trojanu (okresowa sekwencja D).



(a) (b)

Rysunek 5.5: (a) Oddziaływanie trojanu zmniejszającego liczbę bitów Y w generatorze opartym na równaniu logistycznym. (b) Podtrzymanie właściwości chaotycznych w generatorze hybrydowym mimo oddziaływania trojanu.

D oraz chaotycznej sekwencji C. Sekwencja D została wygenerowana z modułu cyfrowego będącego pod wpływem trojanu zmniejszającego precyzje obliczeniową. Pomimo oddziaływania trojanu zmniejszającego liczbę bitów Y poniżej 20 końcowa sekwencja N wykazuje dynamikę chaotyczną. Interpretacja uzyskanych wyników symulacyjnych potwierdza odporność dokładności obliczeniowej na ataki dokonywane przy użyciu trojanów sprzętowych.

Rozdział 6

Ocena bezpieczeństwa modelu hybrydowego

6.1 Poziom bezpieczeństwa sprzętowego

Opracowaną koncepcję hybrydowego generatora chaotycznego należy odnieść do klasyfikacji poziomów bezpieczeństwa sprzętowego omówionej w rozdziale 4.1. Według podziału zaproponowanego przez IBM model hybrydowy posiada cechy poziomu średniego.

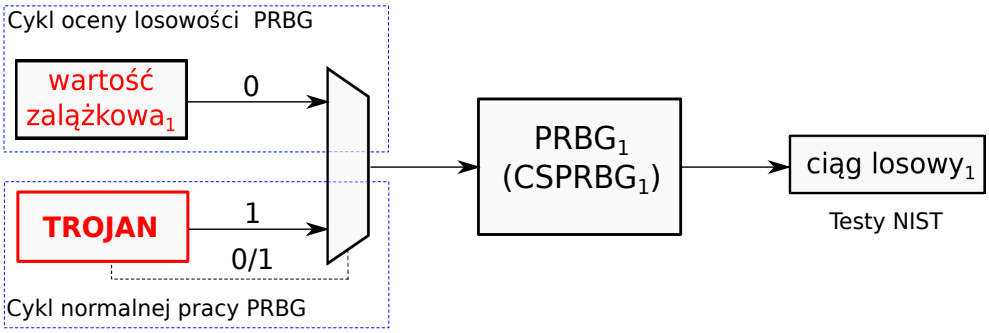
*"**IBM - Poziom Średni:** skuteczność ataku uzależniona jest od wiedzy eksperckiej oraz specjalistycznych informacji z zakresu funkcjonowania układu. Przeprowadzenie ataku musi zostać dokonane w warunkach specjalistycznego laboratorium układów mikroelektronicznych. Poniesione nakłady finansowe nie przekraczają $100 000."*

Dokonanie jakichkolwiek manipulacji w obu modułach wymaga specjalistycznego zaplecza laboratoryjnego - analizatorów stanów logicznych, programatorów układów FPGA, środowiska EDA (ang. *Electronic Design Automation*) dla programowania matryc FPGA i FPAA oraz stosownych licencji.

Według klasyfikacji NIST model hybrydowy generatora chaotycznego wykazuje cechy trzeciego poziomu bezpieczeństwa:

*"**NIST - Poziom 3:** zwiększona ochrona przed fizyczną ingerencją w układ zapobiegająca przed dostępem do newralgicznych elementów struktury układu."*

Analizując opisane w literaturze generatory chaotyczne jako moduły wspomagające kryptografię sprzętową warto zwrócić uwagę, że do tej pory nie przeprowadzono pogłębionych



Rysunek 6.1: Problem wiarygodnej oceny poziomu losowości generatora wartości zalążkowych.

badań w kontekście ich bezpieczeństwa sprzętowego [11, 30, 31].

6.2 Ograniczenia w rejestracji danych do oceny losowości

Użycie generatorów TRBG (ang. *True Random Bit Generator*) we współczesnych systemach wbudowanych jest nieefektywne (ze względu na powolna dynamikę używanych zjawisk [13,18]). Proces generacji sekwencji losowych spowalniałby cały system czyniąc go całkowicie niepraktycznym dla użytkownika końcowego. Używanie generatorów PRBG (ang. *Pseudo Random Bit Generator*) zapewnia jednoczesną szybką transmisję i płynny proces kryptograficzny. Wartości zalążkowe formowane są głównie ze źródeł o wolnej dynamice zachodzenia procesów. Ograniczenia te w odniesieniu do rzeczywistych systemów wbudowanych są szczególnie istotne, a konsekwencje z nich wynikające nie były brane pod uwagę w badaniach nad zastosowaniem obwodów chaotycznych w kryptografii sprzętowej [10, 11]. W realnych warunkach nie jest możliwa rejestracja w trybie ciągłym sekwencji bitów o rozmiarze kilkunastu *Gb* i ich jednoczesna ocena w czasie rzeczywistym testami statystycznymi. Spowodowałby to wydłużenie całego procesu kryptograficznego i transmisyjnego z ułamków sekundy nawet do kilku godzin.

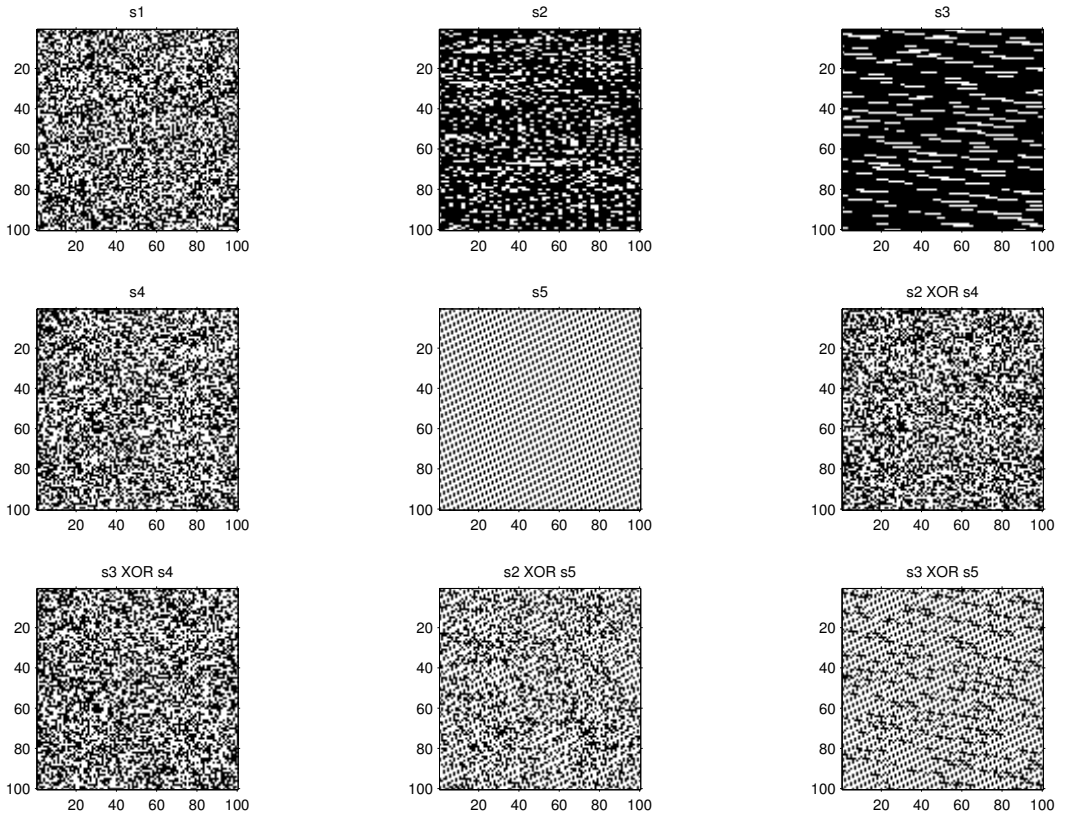
Na rysunku 6.1 pokazano ogólny schemat, w którym trojan w generatorze pseudolosowym pozostaje nieaktywny na etapie testów. Bez analizy podatności na oddziaływanie ze strony trojanów sprzętowych nie można zagwarantować poprawnej pracy obwodów chaotycznych w systemie wbudowanym w kolejnych przedziałach czasu. W tym kontekście nie można wykluczyć obecności trojanu, który w momencie weryfikacji sekwencji generatora pseudolosowego testami statystycznymi pozostanie w stanie nieaktywnym. Po zakończonym procesie weryfikacji aktywność trojanu może powodować utratę losowości, zaburzając prawidłowe funkcjonowanie generatora zalążkowego. Badania przeprowadzone w ramach pracy pokazują, że zapobieganie atakom na generator zalążkowy jest istotnym wyzwaniem dla kryptografii.

Tabela 6.1: Źródła sekwencji bitów poddane ocenie programem *ent*.

Sekwencja *sn*	Źródła
s1	**QUANTIS (sekwencja odniesienia z najwyższą entropią)**
s2	bity chaotyczne z systemu Lorenza
s3	bity chaotyczne z obwodu Chua
s4	bity chaotyczne D (dla 32 bitów cz. ułamk. równania logistycznego)
s5	bity chaotyczne D (dla 10 bitów cz. ułamk. równania logistycznego)
s6	sekwencja s2 XOR sekwencja s4
s7	sekwencja s3 XOR sekwencja s4
s8	sekwencja s2 XOR sekwencja s5
s9	sekwencja s3 XOR sekwencja s5

6.3 Model hybrydowy a źródła kwantowe

Ocena właściwości losowych hybrydowego generatora chaotycznego dla sekwencji mniejszych niż $1Gb$ danych nie jest możliwa przy zastosowaniu testów statystycznych NIST. Jako kryterium pomocnicze w ocenie losowej natury sekwencji chaotycznej zaproponowano metodę porównawczą z kwantowym źródłem losowym. Hybrydowa sekwencja chaotyczna o długości 10000 bitów została porównana z sekwencją o takiej samej długości uzyskanych z generatora kwantowego. Porównanie poziomu losowości sekwencji chaotycznych ze źródłem kwantowym do tej pory nie zostało zaproponowane w literaturze. Ocena poziomu losowości została dokonana przy użyciu pakietu *ent* [32]. Jako kwantowe źródło odniesienia użyto generatora prawdziwie losowego QUANTIS (model USB-4m) szwajcarskiej firmy ID Quantique [33]. W badaniach wykorzystano generator kwantowy o numerze seryjnym 163109A410 posiadający indywidualny certyfikat potwierdzający prawdziwą losowość generowanych sekwencji. Tabela 6.1 zawiera oznaczenia badanych ciągów bitów s1 do s9, przy czym sekwencja s1 jest źródłem odniesienia otrzymanym z generatora QUANTIS. Dodatkowo każdy ciąg został przedstawiony na wykresie różnorodności występowania 10 000 bitów zgrupowanych w 100 wierszach (rysunek 6.2). Wykresy s6 (s2 XOR s4) oraz s7 (s3 XOR s4) są zbliżone do sekwencji odniesienia s1. Wykres różnorodności występowania bitów uzyskany z równania logistycznego s4 z 32 bitową reprezentacją części ułamkowej również wskazuje nieprzewidywalność w występowaniu bitów 0 oraz 1. W przypadku zmniejszenia precyzji w reprezentacji liczby rzeczywistej do 10 bitów sekwencji Y w układzie opartym na równaniu logistycznym widać sekwencję regularną. Wykresy różnorodności występowania dla sekwencji bitów uzyskanych z obwodów Chua i Lorenza nie wykazują nieprzewidywalności. W sekwencjach s2 i s3 dominują przedziały z



Rysunek 6.2: Wykres różnorodności występowania 10000 bitów w sekwencjach $s1$-$s9$.

dużym nadmiarem bitów o tej samej wartości. Długość regularnych ciągów w sekwencjach s2 i s3 zależy od poziomu funkcji progowej w komparatorze, metody rejestracji bitów oraz zegara użytego w tym procesie. Bez względu na dobór poziomu progowego oraz częstotliwość zegara rejestrującego systemy chaotyczne z czasem ciągłym zawsze wykazywać będą nadmiar przedziałów z bitami tej samej wartości.

Wykresy sekwencji s9 (s3 XOR s5) pokazują, że zastosowanie operacji XOR w hybrydowym generatorze chaotycznym wprowadza minimalną nieprzewidywalność. Analiza losowości pakietem *ent* (tabela 6.2) wskazuje, że sekwencje s2 (bity chaotyczne z generatora Lorenza) oraz sekwencja s3 (bity chaotyczne z generatora Chua) cechują się znacznie niższym poziomem entropii niż oczekiwana wartość 8 - występuje tutaj dominacja bitów tej samej wartości. Poprawa poziomu entropii dla sekwencji s2 i s3 mogłaby zostać uzyskana dopiero po zastosowaniu korekcji von Neumanna. Sekwencja s4 (bity chaotyczne z układu opartego na równaniu logistycznym) wykazuje bardzo dobry poziom losowości dla odpowiednio dużej precyzji w reprezentacji liczby rzeczywistej. Należy ponownie podkreślić, że każdy układ chaotyczny realizowany cyfrowo osiąga okresowość przy analizie bardzo długich sekwencji liczbowych [16]. Tym samym w sekwencji s4 istnieje ryzyko powtarzania jednakowych sekwencji ze względu

Tabela 6.2: Wyniki 6 testów z pakietu *ent* dla sekwencji $s1$-$s9$

sn	Entropia	Komp. %	χ^2 wart.; %	AMV	MC π %	SCC
s1	**7,869559**	**1**	**213,91; 95**	**127,4415**	**1,07**	**0,005292**
s2	3,884870	51	36200,14; 0,01	62,4149	21,87	0,119915
s3	1,829749	77	162993,87; 0,01	39,1188	27,32	0,111901
s4	7,850575	1	263,07; 50	131,5946	4,81	0,051919
s5	2,845031	64	44492,49; 0,01	181,7886	44,22	0,037565
s6	7,851689	1	251,59; 50	129,7392	2,06	0,013551
s7	7,837249	2	270,84; 25	131,6376	2,67	0,043232
s8	6,266494	21	5044,32; 0,01	155,7672	16,14	0,102282
s9	4,512645	43	22535,47; 0,01	166,5360	32,67	0,073107

na reprezentację stałoprzecinkową liczb rzeczywistych. Innym zagrożeniem jest wielokrotne użycie tej samej wartości początkowej x_0 skutkujące powtarzaniem generowania tej samej sekwencji chaotycznej. Szczególnie interesujące obserwacje dotyczące poziomu losowości występują w dwóch przypadkach:

- **bez oddziaływania trojanów sprzętowych:**
  Sekwencje s6 oraz s7 wykazują bardzo dobry poziom losowości w porównaniu do sekwencji odniesienia s1, nie wymagają zastosowania korekcji von Neumnna oraz nie są narażone na powstanie okresowości ze względu na skończoną precyzję w reprezentacji liczb rzeczywistych w module cyfrowym generatora hybrydowego.

- **z oddziaływaniem trojanów sprzętowych (sekwencje s8 i s9):**
  Działanie potencjalnych trojanów sprzętowych może ograniczać się tylko w przypadku zmniejszenia dokładności obliczeniowej na matrycy FPGA w wyniku redukcji bitów w sekwencji Y reprezentujących część ułamkową. Wyniki dla sekwencji s8 i s9 należy ocenić jako akceptowalne gdyż mimo obecności trojanu sprzętowego wprowadzone zostają bity zaburzające sekwencję regularną. Zwiększa się tym samym szansa na eliminację identycznych wartości zalążkowych używanych w generatorze pseudolosowym do momentu potencjalnego wykrycia ataku sprzętowego.

Ograniczenia w rejestracji bitów na potrzeby analizy testami NIST wymuszają konieczność użycia programu *ent* oraz zastosowanie analizy porównawczej w celu określenia odporności generatora hybrydowego na ataki w warstwie sprzętowej.

Rozdział 7

Oryginalne osiągnięcia pracy

W pracy przedstawiono koncepcję rozwiązania problemu podatności generatorów chaotycznych na trojany sprzętowe. Do oryginalnych osiągnięć w badaniach nad bezpieczeństwem sprzętowym kryptografii chaotycznej w ramach pracy należy zaliczyć:

1. Adaptację testu 0-1 do wykrywania aktywności trojanów w obwodach chaotycznych.
2. Analizę podatności obwodów chaotycznych na działanie trojanów sprzętowych.
3. Opracowanie hybrydowego generatora chaotycznego.
4. Analizę porównawczą poziomu losowości generatora hybrydowego z losowym generatorem kwantowym.

Uzyskane osiągnięcia stanowią bazę potencjalnych przyszłościowych prac wdrożeniowych. Opracowanie ogólnej teorii i koncepcji hybrydowego generatora chaotycznego pozwala na wykorzystanie uzyskanych wyników badań do dalszych prac nad bezpieczeństwem współczesnych systemów wbudowanych.

Bibliografia

[1] Swarup Bhunia, Michael S Hsiao, Mainak Banga, Seetharam Narasimhan. Hardware Trojan attacks: threat analysis and countermeasures. *Proceedings of the IEEE*, 102(8):1229–1247, 2014.

[2] Nisha Jacob, Dominik Merli, Johann Heyszl, Georg Sigl. Hardware Trojans: current challenges and approaches. *IET Computers & Digital Techniques*, 8(6):264–273, 2014.

[3] Masoud Rostami, Farinaz Koushanfar, Ramesh Karri. A primer on hardware security: models, methods, and metrics. *Proceedings of the IEEE*, 102(8):1283–1295, 2014.

[4] Subhasish Mitra, H-S Philip Wong, Simon Wong. The Trojan-proof chip. *IEEE Spectrum*, 52(2):46–51, 2015.

[5] Thomas Symul, SM Assad, Ping K Lam. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Applied Physics Letters*, 98(23):231103, 2011.

[6] Jose M Cruz, Leon O Chua. An IC chip of Chua's circuit. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, 40(10):614–625, 1993.

[7] Octavio A Gonzales, Gunhee Han, José Pineda de Gyvez, Edgar Sánchez-Sinencio. Lorenz-based chaotic cryptosystem: a monolithic implementation. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 47(8):1243–1247, 2000.

[8] Gonzalo Alvarez, Shujun Li. Breaking an encryption scheme based on chaotic baker map. *Physics Letters A*, 352(1):78–82, 2006.

[9] Fatih Özkaynak, Sırma Yavuz. Security problems for a pseudorandom sequence generator based on the Chen chaotic system. *Computer Physics Communications*, 184(9):2178–2181, 2013.

[10] Ljupco Kocarev, Shiguo Lian. *Chaos-Based Cryptography: Theory, Algorithms and Applications*, wolumen 354. Springer, 2011.

[11] Mustak E Yalcin, Johan AK Suykens, Joos Vandewalle. True random bit generation from a double-scroll attractor. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 51(7):1395–1404, 2004.

[12] Imran Erguler, Emin Anarim. A modified stream generator for the gsm encryption algorithms A5/1 and A5/2. *13th European Signal Processing Conference*, strony 1–4. IEEE, 2005.

[13] Robert McEvoy, James Curran, Paul Cotter, Colin Murphy. Fortuna: cryptographically secure pseudo-random number generation in software and hardware. *Irish Signals and Systems Conference*. IET, 2006.

[14] Recommendation for random number generation using deterministic random bit generators. http://dx.doi.org/10.6028/NIST.SP.800-90Ar1, 2006.

[15] Statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf, 2009.

[16] KJ Persohn, Richard J Povinelli. Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation. *Chaos, Solitons & Fractals*, 45(3):238–245, 2012.

[17] A Beirami, H Nejati, WH Ali. Zigzag map: a variability-aware discrete-time chaotic-map truly random number generator. *Electronics Letters*, 48(24):1537–1538, 2012.

[18] Christof Paar, Jan Pelzl. *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, Berlin, 2009.

[19] Alex Biryukov, Adi Shamir, David Wagner. Real time cryptanalysis of A5/1 on a pc. *International Workshop on Fast Software Encryption*, strony 1–18. Springer, 2000.

[20] Patrik Ekdahl, Thomas Johansson. Another attack on A5/1. *IEEE Transactions on Information Theory*, 49(1):284–289, 2003.

[21] Michał Melosik, Wiesław Marszałek. On the 0/1 test for chaos in continuous systems. *Bulletin of the Polish Academy of Sciences Technical Sciences*, 64(3):521–528, 2016.

[22] Georg A Gottwald, Ian Melbourne. On the implementation of the 0–1 test for chaos. *SIAM Journal on Applied Dynamical Systems*, 8(1):129–145, 2009.

[23] Mohammad Tehranipoor, Cliff Wang. *Introduction to hardware security and trust*. Springer Science & Business Media, 2011.

[24] Dennis G. Abraham, George M. Dolan, Glen P. Double, James V. Stevens. Transaction security system. *IBM Systems Journal*, 30(2):206–229, 1991.

[25] Security requirements for cryptographic modules. https://doi.org/10.6028/NIST.FIPS.140-2, 2011.

[26] Ramesh Karri, Jeyavijayan Rajendran, Kurt Rosenfeld, Mohammad Tehranipoor. Trustworthy hardware: Identifying and classifying hardware trojans. *Computer*, 43(10):39–46, 2010.

[27] Swaroop Ghosh, Abhishek Basak, Swarup Bhunia. How secure are printed circuit boards against trojan attacks? *IEEE Design & Test*, 32(2):7–16, 2015.

[28] Michał Melosik, Wiesław Marszałek. Using the 0-1 test for chaos to detect hardware trojans in chaotic bit generators. *Electronics Letters*, 52(11):919–921, 2016.

[29] Erik Lindberg, Krishnamurthy Murali, Arunas Tamasevicius. The smallest transistor-based nonautonomous chaotic circuit. *IEEE Transactions on Circuits and Systems. Part 2: Express Briefs*, 52(10):661–664, 2005.

[30] Paweł Dąbal, Ryszard Pełka. A chaos-based pseudo-random bit generator implemented in FPGA device. *14th International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS)*, strony 151–154. IEEE, 2011.

[31] Wafaa S Sayed, Ahmed G Radwan, Ahmed A Rezk, Hossam AH Fahmy. Finite precision logistic map between computational efficiency and accuracy with encryption applications (https://doi.org/10.1155/2017/8692046). *Complexity*, 2017.

[32] Wen-Kai Yu, Shen Li, Xu-Ri Yao, Xue-Feng Liu, Ling-An Wu, Guang-Jie Zhai. Protocol based on compressed sensing for high-speed authentication and cryptographic key distribution over a multiparty optical network. *Applied optics*, 52(33):7882–7888, 2013.

[33] ID QUANTIQUE SA, http://www.idquantique.com/, 2017.