Załącznik 2

Warszawa, 9 kwietnia 2018

Autoreferat
Wykorzystanie zjawisk niestałościowych w generacji liczb losowych

1. Imię i nazwisko:

Piotr Zbigniew Wieczorek

2. Posiadane dyplomy, stopnie naukowe

1. Stopień naukowy doktora nauk technicznych w dyscyplinie elektronika, Politechnika Warszawska, Wydział Elektroniki i Technik Informacyjnych, 2011 r. Tytuł rozprawy: „Modelowanie i optymalizacja metastabilności układów przerzutnikowych"

2. Tytuł zawodowy magistra inżyniera, Politechnika Warszawska, Wydział Elektroniki i Technik Informacyjnych, Instytut Systemów Elektronicznych, 2006 r. Tytuł pracy: „System do pomiaru subnanosekundowych odcinków czasu"

3. Informacja o dotychczasowym zatrudnieniu w jednostkach naukowych

2016 - obecnie, adiunkt, z-ca dyrektora Instytutu Systemów Elektronicznych ds. nauczania na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej

2012 - 2016 adiunkt, Politechnika Warszawska, Instytut Systemów Elektronicznych

2008 - 2012 asystent, Politechnika Warszawska, Instytut Systemów Elektronicznych

2007 - 2008 asystent, Uniwersytet Warmińsko-Mazurski, Katedra Fizyki i Biofizyki

4. Wskazanie osiągnięcia wynikającego z art. 16 ust. 2 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz. U. nr 65, poz. 595 ze zm.)

A. Tytuł osiągnięcia naukowego

Osiągnięciem naukowym opracowanym po otrzymaniu stopnia naukowego doktora, stanowiącym znaczący wkład w rozwój dyscypliny naukowej Nauk Technicznych w dziedzinie Elektronika i zgłaszanym jako podstawa mojej aplikacji o nadanie stopnia naukowego doktora habilitowanego jest cykl publikacji i wynalazków pod wspólnym tytułem „*Wykorzystanie zjawisk niestałościowych w generacji liczb losowych*".

B. Lista publikacji (autor/autorzy, tytuł/tytuły publikacji, rok wydania, nazwa wydawnictwa)

PUBLIKACJE WCHODZĄCE W SKŁAD OSIĄGNIĘCIA NAUKOWEGO[1]

A1. **Wieczorek Piotr Z.**, Gołofit Krzysztof: True Random Number Generator Based on Flip-Flop Resolve Time Instability Boosted by Random Chaotic Source, w: IEEE Transactions on Circuits and Systems I – Regular Papers, vol. 63, nr 7, 2017, ss. 1043-1054, DOI:10.1109/TCSI.2017.2751144,
swój wkład w tę publikację oceniam na 70%, MNiSW: 35, IF: 2,407

A2. **Wieczorek Piotr Z.**: Lightweight TRNG Based on Multiphase Timing of Bistables, w: IEEE Transactions on Circuits and Systems I – Regular Papers, vol. 63, nr 7, 2016, ss. 1043-1054, DOI:10.1109/TCSI.2016.2555248
MNiSW: 35, IF: 2,407

A3. **Wieczorek Piotr Z.**: True random number generator resistant to frequency injection attacks, w: Electronics Letters, vol. 51, nr 5, 2015, ss. 384-386, DOI:10.1049/el.2014.4030,
MNiSW: 20, IF: 0,854

A4. **Wieczorek Piotr Z.**: An FPGA Implementation of the Resolve Time-Based True Random Number Generator With Quality Control, w: IEEE Transactions on Circuits and Systems I – Regular Papers, vol. 61, nr 12, 2014, ss. 3450-3459, DOI:10.1109/TCSI.2014.2338615
MNiSW: 35, IF: 2,403

A5. **Wieczorek Piotr Z.**, Gołofit Krzysztof: Dual-Metastability Time-Competitive True Random Number Generator, w: IEEE Transactions on Circuits and Systems I – Regular Papers, vol. 61, nr 1, 2014, ss. 134-145, DOI:10.1109/TCSI.2013.2265952
swój wkład w tę publikację oceniam na 70%, MNiSW: 35, IF: 2,403

A6. **Wieczorek Piotr Z.**, Gołofit Krzysztof: Metastability Occurrence Based Physical Unclonable Functions for FPGAs, w: Electronics Letters, vol. 50, nr 4, 2014, ss. 281-283, DOI:10.1049/el.2014.0143
swój wkład w tę publikację oceniam na 70%, MNiSW: 25, IF: 1,023

A7. **Wieczorek Piotr Z.**: Dual-Metastability FPGA-Based True Random Number Generator, w: Electronics Letters, vol. 49, nr 12, 2013, ss. 744-745, DOI:10.1049/el.2012.4126
MNiSW: 25, IF: 1,068

B8. **Wieczorek Piotr Z.**: Secure TRNG with Random Phase Stimulation, w: Proc. SPIE. 10445, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2017 / Romaniuk Ryszard, Linczuk Maciej Grzegorz (red.), vol. 10445, 2017, SPIE, ISBN 9781510613546, ss. 104452A-1-104452A-7 DOI:10.1117/12.2280979
MNiSW: 15

B9. **Wieczorek Piotr Z.**, Wieczorek Zbigniew: Influence of radiation on metastability-based TRNG, w: Proc. SPIE. 10445, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2017 / Romaniuk Ryszard, Linczuk Maciej Grzegorz (red.), vol. 10445, 2017, SPIE, ISBN 9781510613546, ss. 1044529-1-1044529-7 DOI:10.1117/12.2280978
swój wkład w tę publikację oceniam na 70%, MNiSW: 15

PRZYZNANE PATENTY KRAJOWE WCHODZĄCE W SKŁAD OSIĄGNIĘCIA NAUKOWEGO

P1. **Wieczorek Piotr Z.**, Gołofit Krzysztof: Arbiter, Wynalazek, Zaakceptowany, Numer zgłoszenia: P.401520, Numer patentu/prawa: 224925, Data zgłoszenia: 08-11-2012, Data udzielenia (decyzji): 24-08-2016
swój wkład w ten wynalazek oceniam na 60%, MNiSW: 30

P2. **Wieczorek Piotr Z.**, Gołofit Krzysztof: Generator metastabilnościowych interwałów czasowych, Wynalazek, Zaakceptowany, Numer zgłoszenia: P.401521, Numer patentu/prawa: 225186, Data zgłoszenia: 08-11-2012, Data udzielenia (decyzji): 01-09-2016
swój wkład w ten wynalazek oceniam na 60%, MNiSW: 30

[1] Publikacje z listy A oznaczono jako A[numer], publikacje w materiałach pokonferencyjncych oznaczono jako B[numer], przyznane patenty krajowe P[numer], natomiast zgłoszenia patentowe potwierdzone oznaczono jako ZP[numer]. Zdecydowałem się na umieszczenie zgłoszeń ze względu na ich bezpośredni związek z osiągnięciem i komercjalizację w ramach tzw. preinkubacji w programie Bridge Alfa.

P3. **Wieczorek Piotr Z.**, Gołofit Krzysztof: Układ fizycznie nieklonowalnej funkcji, Wynalazek, Zaakceptowany, Numer zgłoszenia: P.407108, Numer patentu/prawa: 223881, Data zgłoszenia: 07-02-2014, Data udzielenia (decyzji): 04-03-2016
swój wkład w ten wynalazek oceniam na 60%, MNiSW: 30

P4. Gołofit Krzysztof, **Wieczorek Piotr Z.**: Metastabilnościowy generator losowy (1), Wynalazek, Zaakceptowany, Numer zgłoszenia: P.401522, Numer patentu/prawa: 225187, Data zgłoszenia: 08-11-2012, Data udzielenia (decyzji): 01-09-2016
swój wkład w ten wynalazek oceniam na 50%, MNiSW: 30

P5. Gołofit Krzysztof, **Wieczorek Piotr Z.**: Metastabilnościowy generator losowy (2), Wynalazek, Zaakceptowany, Numer zgłoszenia: P.401523, Numer patentu/prawa: 225188, Data zgłoszenia: 08-11-2012, Data udzielenia (decyzji): 01-09-2016
swój wkład w ten wynalazek oceniam na 40%, MNiSW: 30

P6. Gołofit Krzysztof, **Wieczorek Piotr Z.**: Metastabilnościowy generator losowy (3), Wynalazek, Zaakceptowany, Numer zgłoszenia: P.401519, Numer patentu/prawa: 225185, Data zgłoszenia: 08-11-2012, Data udzielenia (decyzji): 01-09-2016
swój wkład w ten wynalazek oceniam na 40%, MNiSW: 30

POTWIERDZONE ZGŁOSZENIA PATENTOWE KRAJOWE WCHODZĄCE W SKŁAD OSIĄGNIĘCIA NAUKOWEGO

ZP1. **Wieczorek Piotr Z.**, Gołofit Krzysztof: Generator losowy (1), Wynalazek, Zgłoszenie potwierdzone, Numer zgłoszenia: P.422488, Data zgłoszenia: 08-08-2017

ZP2. **Wieczorek Piotr Z.**, Gołofit Krzysztof: Generator losowy (2), Wynalazek, Zgłoszenie potwierdzone, Numer zgłoszenia: P-422484, Data zgłoszenia: 08-08-2017

ZP3. **Wieczorek Piotr Z.**, Gołofit Krzysztof: Generator losowy (3), Wynalazek, Zgłoszenie potwierdzone, Numer zgłoszenia: P-422485, Data zgłoszenia: 08-08-2017

ZP4. **Wieczorek Piotr Z.**, Gołofit Krzysztof: Generator fizycznie niekopiowanych kluczy kryptograficznych (1), Wynalazek, Zgłoszenie potwierdzone, Numer zgłoszenia: P-422486, Data zgłoszenia: 08-08-2017

ZP5. **Wieczorek Piotr Z.**, Gołofit Krzysztof: Arbiter (2), Wynalazek, Zgłoszenie potwierdzone, Numer zgłoszenia: P-422478, Data zgłoszenia: 08-08-2017

ZP6. **Wieczorek Piotr Z.**, Gołofit Krzysztof: Generator metastabilnościowych interwałów czasowych (2), Wynalazek, Zgłoszenie potwierdzone, Numer zgłoszenia: P-422477, Data zgłoszenia: 08-08-2017

ZP7. **Wieczorek Piotr Z.**, Gołofit Krzysztof: Metastabilnościowy generator losowy (4), Wynalazek, Zgłoszenie potwierdzone, Numer zgłoszenia: P-422481, Data zgłoszenia: 08-08-2017

ZP8. **Wieczorek Piotr Z.**, Gołofit Krzysztof: Metastabilnościowy generator losowy (5), Wynalazek, Zgłoszenie potwierdzone, Numer zgłoszenia: P-422482, Data zgłoszenia: 08-08-2017

ZP9. **Wieczorek Piotr Z.**, Gołofit Krzysztof: Metastabilnościowy generator losowy (6), Wynalazek, Zgłoszenie potwierdzone, Numer zgłoszenia: P-422479, Data zgłoszenia: 08-08-2017

ZP10. Gołofit Krzysztof, **Wieczorek Piotr Z.**: Metastabilnościowy generator losowy (7), Wynalazek, Zgłoszenie potwierdzone, Numer zgłoszenia: P-422480, Data zgłoszenia: 08-08-2017

ZP11. Gołofit Krzysztof, **Wieczorek Piotr Z.**: Generator fizycznie niekopiowanych kluczy kryptograficznych (2), Wynalazek, Zgłoszenie potwierdzone, Numer zgłoszenia: P-422487, Data zgłoszenia: 08-08-2017

ZP12. Gołofit Krzysztof, **Wieczorek Piotr Z.**: Generator losowy (4), Wynalazek, Zgłoszenie potwierdzone, Numer zgłoszenia: P-422490, Data zgłoszenia: 08-08-2017

ZP13. Gołofit Krzysztof, **Wieczorek Piotr Z.**: Generator losowy (5), Wynalazek, Zgłoszenie potwierdzone, Numer zgłoszenia: P-422491, Data zgłoszenia: 08-08-2017

ZP14. Gołofit Krzysztof, **Wieczorek Piotr Z.**: Generator losowy (6), Wynalazek, Zgłoszenie potwierdzone, Numer zgłoszenia: P-422489, Data zgłoszenia: 08-08-2017

C. Omówienie celu naukowego ww. prac i osiągniętych wyników wraz z omówieniem ich ewentualnego wykorzystania

Działalność naukową związaną ze zjawiskami niestałościowymi, w szczególności – badaniem i wykorzystaniem tych zjawisk w układach programowalnych rozpocząłem w 2012 r. po obronie doktoratu w 2011 r. W ramach doktoratu i studiów doktoranckich zajmowałem się optymalizacją układów przerzutnikowych pod kątem maksymalnej częstotliwości pracy. W 2012 roku zostałem zatrudniony na stanowisku adiunkta w Zespole Analogowych Układów Elektronicznych Zakładu Układów i Systemów Elektronicznych w Instytucie Systemów Elektronicznych Politechniki Warszawskiej, pod kierownictwem prof. Leszka Opalskiego. Prace zespołu koncentrowały się wtedy głównie na modelowaniu analogowych układów elektronicznych. Wówczas moje zainteresowania skupiły się na opisie symbolicznym i behawioralnym bloków układów programowalnych, ze szczególnym uwzględnieniem wpływu zjawisk niestałościowych (głównie szumowych) i zjawisk wynikających z opisu dynamiki bloków analogowych na pracę tych układów. Wpływ tego typu zjawisk jest zwykle pomijany przez projektantów układów cyfrowych, zwłaszcza gdy zagadnienie projektowania sprowadza się do zautomatyzowanej syntezy z wykorzystaniem języku opisu sprzętu np. VHDL. Projektanci starają się projektować układy w ten sposób by niepożądane zjawiska nie występowały, tj nie zaburzały pracy bloków cyfrowych, czy nie pogarszały drastycznie parametrów takich jak: średni czas pomiędzy błędami (ang. 'Mean Time Between Failure' – MTBF), czy stopa błędów (ang. 'Bit Error Rate' – BER) w obróbce danych i jej transmisji. Niestety rozważania nad wpływem szumu fazowego, opóźnień deterministycznych linii wewnątrz układów programowalnych i innych zjawisk o podłożu analogowym, stają się istotne jedynie gdy projektowany układ cyfrowy nie spełnia założonych przez projektanta wymagań. Okazuje się jednak, że wymienione zjawiska mają niezwykle istotne zastosowania w generacji liczb losowych przy zastosowaniu układów stricte cyfrowych, m.in. na potrzeby kryptografii, czy uwierzytelniania sprzętowego. Możliwość integracji układów wykorzystujących zjawiska o podłożu analogowym w blokach cyfrowych odpowiedzialnych za np. szyfrowanie algorytmami AES (ang. 'Advanced Encryption Standard') czy DES (ang. 'Data Encryption Standard') w układach programowalnych, umożliwia stworzenie wydajnych narzędzi istotnych z punktu widzenia dziedziny, jaką jest bezpieczeństwo informacji. W swojej działalności skupiłem się na wydajnym generowaniu ciągów losowych liczb na potrzeby tworzenia kluczy kryptograficznych o dowolnej długości oraz ciągów liczb do uwierzytelniania sprzętowego. Uwierzytelnianie takie jest stosunkowo nową dziedziną, przy czym u jej podstaw leży założenie, iż urządzenie generujące klucz nie posiada fizycznej kopii klucza, a jest on jedynie tworzony na potrzeby autoryzacji. W dalszej części autoreferatu omawiam podstawowe typy układów, które projektowałem i badałem w trakcie ostatnich kilku lat, stanowią one cel naukowy mojej działalności po doktoracie. Układy te, to rodzina generatorów liczb losowych oraz bloki generujące klucze kryptograficzne. W kolejnym punkcie opisuję te układy nawiązując do literatury.

C.1 Generatory liczb prawdziwie losowych i fizycznie niekopiowalne funkcje – wprowadzenie

Generacja ciągów zmiennych losowych jest niezwykle istotna z punktu widzenia współczesnych technik i algorytmów komputerowych m.in. w kryptografii (tworzenie kluczy publicznych i prywatnych), sieciach komputerowych, metodach uwierzytelniania sprzętowego, metodach statystycznych (Monte-Carlo), a także w zabezpieczaniu układów kryptograficznych przed atakami „Side Channel" (SCA) [21]. Do niedawna (lata 90'te) najbardziej popularnymi źródłami liczb o akceptowalnych właściwościach statystycznych były generatory pseudolosowe (ang. 'Pseudo Random Number Generators' – PRNG). W istocie generatory te tworzą ciągi deterministyczne (i powtarzalne) jednak ich tzw. właściwości lokalne, mierzone wynikami testów statystycznych charakterystycznych dla generatorów losowych, dają satysfakcjonujące wyniki [7]. W układach PRNG zarówno rozkłady generowanych liczb (zwykle jednostajne) jak ich momenty – mimo determinizmu PRNG – są prawidłowe. Należy jednak pamiętać, iż z punktu widzenia globalnych właściwości bardzo długich ciągów liczbowych (w pojedynczej realizacji lub wielu realizacji), układ PRNG jest przewidywalny, a jego entropia zależy tylko i wyłącznie od entropii źródła początkowego stanu układu. Pomimo oczywistych niebezpieczeństw związanych z przewidywalnością PRNG stosowano je masowo m.in. w szyfrowaniu połączeń internetowych. Prowadziło to, do tego, że przeciętne szyfrowane połączenie WWW mogła „złamać" niepowołana osoba w przeciągu 30 min [23]. Co ciekawe generatory PRNG są w dalszym ciągu stosowane w układach „System on Chip" (SoC) i związanym z nimi tzw. „Internetem Rzeczy" (ang. 'Internet of Things' – IoT). Ostatnie doniesienia przedstawione w pracy Taeill Yoo i in. [29] wskazały na możliwość predykcji 700 bajtowych ciągów binarnych generowanych przez generator PRNG systemu operacyjnego Google Brillo, z prawdopodobieństwem sięgającym 0,9 przy złożoności obliczeniowej $5,2{\times}2^{40}$. Świadczy to, o realnym zagrożeniu ujawnienia kluczy generowanych przez PRNG systemu na urządzeniach IoT. Biorąc pod uwagę rosnącą popularność IoT w urządzeniach codziennego

użytku (sprzęcie mobilnym, urządzeniach gospodarstwa domowego itp.), ryzyko związane z ujawnieniem szyfrowanej transmisji jest poważne. Rozwiązaniem tego problemu jest stosowanie generatorów tzw. liczb prawdziwie losowych wykorzystujących metody sprzętowe generacji ciągów liczbowych. W układach tego typu, źródłem entropii jest zjawisko fizyczne – szum termiczny, śrutowy, zjawisko kwantowe lub inny proces stochastyczny, zamiast deterministycznego algorytmu [4]. Generatory tego typu określane są mianem generatorów liczb prawdziwie losowych (ang. 'true random number generator' – TRNG). Są to układy szczególnie pożądane z punktu widzenia bezpieczeństwa informacji. Nie ma bowiem algorytmu ani opisu symbolicznego wiążącego n-ty i n+1 element sekwencji takiego generatora. Znaczną część prac składających się na mój dorobek poświęciłem opisowi teoretycznemu, projektowaniu i konstrukcji takich generatorów TRNG.

Oprócz generatorów PRNG stosowano także do niedawna (koniec lat 90-tych) generatory liczb prawdziwie losowych, wykorzystujące sygnał analogowy jako źródło losowości. Sygnał ten reprezentował proces stochastyczny wynikający ze zjawisk fizycznych, a dopiero po odpowiedniej obróbce nadawał się do tworzenia ciągów binarnych. Rozwiązania tego typu wymagały integracji układów analogowych odpowiadających za wyodrębnienie zjawiska losowego z układami cyfrowymi, które próbkowały losowy sygnał analogowy i dokonywały ewentualnej korekcji tzw. korektorami lub dekorelatorami. Poważną wadą tych rozwiązań była konieczność kontroli procesu stochastycznego (np. szumu termicznego) i utrzymywanie stałych warunków pracy układu analogowego [3, 9].

Obecnie popularne stały się rozwiązania TRNG wykorzystujące następujące zjawiska:
— szum fazowy (jitter) generatorów pierścieniowych [6, 22, 20],
— metastabilność w układach przerzutnikowych [23, 24, 7],
— praca chaotyczna [5, 26, 17].
W ramach prac po doktoracie włożyłem wkład w rozwój trzech wymienionych typów TRNG, a moje publikacje z tej tematyki cieszą się znacznym zainteresowaniem międzynarodowego środowiska naukowców. Wiele istniejących rozwiązań wykorzystujących metastabilność bazuje na niepewności stanu stabilnego układu przerzutnikowego wprowadzonego w otoczenie równowagi metastabilnej [25, 8]. Rozwiązania takie wymagają zwykle projektowania „full custom", są wrażliwe na zmiany parametrów fizycznych (temperatury, zasilania), często należy w nich stosować zaawansowane metody przetwarzania strumienia wyjściowego (ang. 'bit-stream post-processing') lub stabilizacji warunków pracy [24, 11]. Koronnym przykładem takiego rozwiązania jest generator TRNG wykorzystujący metastabilność w układach przerzutnikowych, stosowany w procesorach firmy Intel (począwszy od architektury Ivy Bridge). Niewątpliwym osiągnięciem wchodzącym w skład mojej działalności po doktoracie było zaprojektowanie i opisanie na gruncie teorii serii generatorów TRNG nie bazujących na losowości stanu układu bistabilnego. Rozwiązania te są niejako rozwinięciem koncepcji zaproponowanej przez firmę Intel. W opracowanych generatorach wykorzystuję ciągłą zmienną losową czasu odpowiedzi układu przerzutnikowego, zamiast zmiennej losowej dyskretnej stanu stabilnego przerzutnika. Zaletą tego rozwiązania jest większa entropia czasu odpowiedzi, w porównaniu do rozwiązania z losowym stanem układu bistabilnego oraz większa odporność na zmiany warunków pracy. Rozwiązanie to uzyskało status patentu krajowego w Urzędzie Patentowym RP w kilku możliwych wariantach implementacyjnych. Otrzymałem także finansowanie na badania nad układami TRNG tego typu, w postaci dwóch grantów dziekańskich.

Generatory TRNG wykorzystujące szum fazowy generatorów pierścieniowych (ang. 'ring oscillators' – RO) są dość popularne, jednakże nie są pozbawione wad. Pomimo łatwości implementacji w układach programowalnych CPLD (ang. 'Complex Programmable Logic Device') czy FPGA (ang. 'Field Programmable Gate Array') posiadają szereg wad eliminujących je z zastosowań masowych, należą do nich m.in. znaczny pobór mocy wywołany znacznymi częstotliwościami przełączania elementów aktywnych tworzących generator pierścieniowy, ryzyko występowania zjawiska synchronizacji fazowej (tzw. 'frequency lock-up') oraz podatność na tzw. ataki „wstrzykiwania energii" (ang. 'frequency injection attacks'), które drastycznie zmniejszają entropię takiego generatora [12]. Opracowałem kilka konstrukcji generatorów liczb prawdziwie losowych, które wykorzystują szum fazowy generatorów pierścieniowych. Rozwiązania te są konstrukcjami wielostopniowymi (hybrydowymi), w których szum fazowy (ang. 'jitter') wykorzystałem pośrednio jako źródło stanu początkowego dla kolejnego stopnia wykorzystującego np.: nieokreśloność stanu układu bistabilnego lub pracę chaotyczną. Pokazałem także, na drodze modelowania numerycznego w środowisku Matlab (Simulink) oraz eksperymentalnie, większą odporność rozwiązań hybrydowych na ataki wstrzykiwania energii ('frequency injection') i zmiany parametrów pracy niż w jednostopniowych rozwiązaniach konwencjonalnych [A1], [A2], [B8].

Ciekawą alternatywą dla generatorów bazujących na niestałości stanu układów bistabilnych i metastabilności, czy też szumie fazowym generatorów pierścieniowych, są generatory chaotyczne. Należy wszakże rozróżnić dwie podstawowe grupy chaotycznych generatorów liczb losowych:

— generatory opisane mapą chaosu zapisaną w układzie cyfrowym [10, 5, 26],
— generatory, których mapa chaosu wynika z opisu analogowych układów elektronicznych [17, 2].
Oba powyższe rozwiązania chaotyczne posiadają niższą entropię uzyskiwaną z pojedynczego bitu niż rozwiązania bazujące na niestałości stanu układów bistabilnych (metastabilności) czy próbkowaniu szumu fazowego generatorów pierścieniowych [A1]. Układy generatorów opisane mapą chaosu zapisaną w układzie cyfrowym są łatwe w implementacji, jednakże generowane przez nie ciągi liczbowe są deterministyczne, periodyczne i ściśle zależą od warunku początkowego i arytmetyki układu cyfrowego [5]. Nie są to więc generatory TRNG, lecz PRNG. Z kolei wadą generatorów chaotycznych z analogowymi układami elektronicznymi jest konieczność implementacji mapy chaotycznej w analogowym układzie scalonym, lub układzie z elementami dyskretnymi. Jednakże ten ostatni typ generatorów należy zaliczyć do generatorów TRNG, z powodu korzystnego wpływu zjawisk szumowych układów analogowych na pracę chaotyczną (tzw. „efekt motyla"). W trakcie prac nad układami do losowego pobudzania układów przerzutnikowych sygnałami o zmiennym położeniu zboczy aktywnych, zaproponowałem własną odmianę układu chaotycznego opisaną w [A1]. Układ ten wykorzystuje generatory pierścieniowe o zmiennej ścieżce propagacji i jest opisany liniową mapą chaotyczną. Niewątpliwą innowacją w zaproponowanym przez mnie rozwiązaniu układu chaotycznego jest to, że zmienną stanu układu jest czas, a dokładnie odległość pomiędzy dwoma zboczami aktywnymi na jego wyjściach. Dzięki wykorzystaniu czasu jako zmiennej stanu, ten typ chaotycznego generatora TRNG można zaimplementować w układach cyfrowych asynchronicznych, przy jednoczesnym zachowaniu pracy chaotycznej niedeterministycznej. Wynika to z tego, iż zmienna stanu jaką jest czas może osiągać dowolne wartości z określonego przedziału, w przeciwieństwie do rozwiązań generatorów chaotycznych, w których zmienną stanu jest wartość logiczna przerzutnika lub rejestru. Przedstawione rozwiązanie zostało zgłoszone jako wynalazek w urzędzie patentowym RP [ZP4], [ZP11] oraz trwają prace nad jego komercjalizacją w programie Bridge Alfa.

Ciągi liczb generowane przez opisane uprzednio układy wykorzystywane są m.in do tworzenia kluczy kryptograficznych. Właściwości ciągów generowanych przez TRNG powinny być niezależne od egzemplarza układu czy elementu, w którym zaimplementowano generator. Jednakże istnieje pewna klasa układów, których zadaniem jest generacja powtarzalnych ciągów liczbowych w konkretnym egzemplarzu układu i generacja niepowtarzalnych ciągów liczbowych w różnych egzemplarzach układu. Układy takie wykorzystywane są do realizacji tzw. fizycznie niekopiowalnych funkcji (ang. 'physically unclonable function' – PUF), których zadaniem jest tworzenie różnych ciągów binarnych (lub całych liczb) w różnych egzemplarzach układów (ang. 'inter-class variation') i identycznych ciągów w konkretnych egzemplarzu (ang. 'zero intra-class variation'). Istotną cechą układów z zaimplementowaną funkcją niekopiowalną jest brak jakiejkolwiek informacji (klucza) zapisanej w strukturze układu. Fizycznie niekopiowalne funkcje (PUF) są idealnym narzędziem do uwierzytelniania sprzętowego układów elektronicznych, tj. mikroprocesorów, układów CPLD lub FPGA, wymagają jednak wykorzystania losowych zjawisk zachodzących w procesie produkcyjnym układu (rozrzutów produkcyjnych międzyeglemplarzowych), różnicujących poszczególne egzemplarze tego samego typu układu, jak i odpowiednich mechanizmów pozyskiwania informacji o takich rozrzutach. Fizycznie niekopiowalne funkcje wykorzystują mierzalne elektrycznie rozrzuty parametrów fizycznych, takie jak: napięcie progowe tranzystorów lub całych bramek, czasy propagacji w bramkach lub połączeniach wewnątrz układu, czasy podtrzymania/ustalania przerzutników, stany początkowe komórek pamięci SRAM po inicjalizacji, różnice w częstotliwości generowanych przebiegów generatorów pierścieniowych, wynikające z różnych pojemności bramkowych i prądów drenów, itp [14, 27, 19]. Istotnym problemem w realizacji układów PUF jest implementacja niezawodnej metody powtarzalnego i niedestrukcyjnego odczytu parametrów podlegających rozrzutom. Ponadto ważne jest, by ciągi liczbowe generowane przez PUF w obrębie jednego układu pozostawały niezmienne wraz ze zmianami warunków pracy m.in. napięcia zasilania i temperatury. W ramach prac wchodzących w skład zgłaszanego osiągnięcia naukowego, opracowałem koncepcję układu PUF, bazującego na rozrzutach czasów ustalania w przerzutnikach typu D w układach FPGA. Przeprowadzone badania wskazały, że możliwe jest rozróżnianie egzemplarzy układów FPGA na podstawie różnych czasów ustalania mierzonych przez wewnętrzny układ dystrybucji zegara tzw. Digital Clock Menager (DCM) [A6]. Jestem także współautorem innej koncepcji PUF bazującej na różnych trajektoriach układów chaotycznych w tzw. zakresie chaosu deterministycznego. W rozwiązaniu tym klucz kryptograficzny pozyskiwany jest z trajektorii układu chaotycznego w trakcie tzw. chaosu deterministycznego, bezpośrednio po inicjalizacji układu. Różnica w trajektoriach w tym zakresie pracy wynika z rozrzutów parametrów elementów aktywnych tworzących złożone struktury makrocel (w układach CPLD) lub tzw. slice'ów (w układach FPGA), a w minimalnym stopniu wynika z obecności zjawisk szumowych. Oba wymienione rozwiązania, tj. bazujące na czasach ustalania przerzutników D i chaosie deterministycznym zostały zgłoszone jako wynalazki w Urzędzie Patentowym RP.

Najogólniej cel naukowy prac realizowanych w ramach osiągnięcia naukowego mogę streścić i podzielić na trzy części:

— opis teoretyczny, propozycję i implementację nowych topologii generatorów liczb prawdziwie losowych (TRNG) bazujących na niestałości czasu odpowiedzi układów przerzutnikowych, szumie fazowym i zjawiskach chaotycznych,

— opis i konstrukcję nowych układów fizycznie niekopiowalnych/nieklonowalnych funkcji (PUF) bazujących na rozrzutach czasów propagacji w układach programowalnych i fazy deterministycznej chaosu liniowego,

— prace nad bezpieczeństwem układów w tym nad zmniejszeniem podatności układów TRNG i PUF na ataki wstrzykiwania energii, podsłuchu ulotu elektromagnetycznego lub gwałtowne zmiany parametrów roboczych.

Ponadto wymienione prace wymagały rozbudowy instrumentarium badawczego, co wiązało się z samodzielnym konstruowaniem dedykowanych układów elektronicznych. W kolejnych podpunktach omówię szczegółowo każdą z części wchodzącą w skład osiągnięcia naukowego.

C.2 Opis teoretyczny, propozycja i implementacja nowych topologii generatorów liczb losowych

Swoje prace nad wykorzystaniem zjawisk niestałościowych do generacji liczb losowych rozpocząłem od badań niestałości czasu odpowiedzi układów bistabilnych. W pracy [A5] zaproponowałem opis rozkładu prawdopodobieństwa $P(T_{pd})$ czasu odpowiedzi t_{pd} układu bistabilnego pracującego w otoczeniu punktu równowagi chwiejnej (tzw. metastabilnej), w funkcji odstępu δ czasowego pomiędzy zboczami aktywnymi sygnałów danych i zegara (D i Clock) lub zapisującego i kasującego (Reset i Set). Rozkład ten ma wartość oczekiwaną $E(T_{pd})$ w przybliżeniu równą katalogowemu czasowi odpowiedzi układu przerzutnikowego, jest skośny i przy założeniu pewnych uproszczeń w opisie elementów aktywnych (inwerterów, tablic LUT lub makrocel) może być opisany równaniem (1), które zaproponowałem w [A5]:

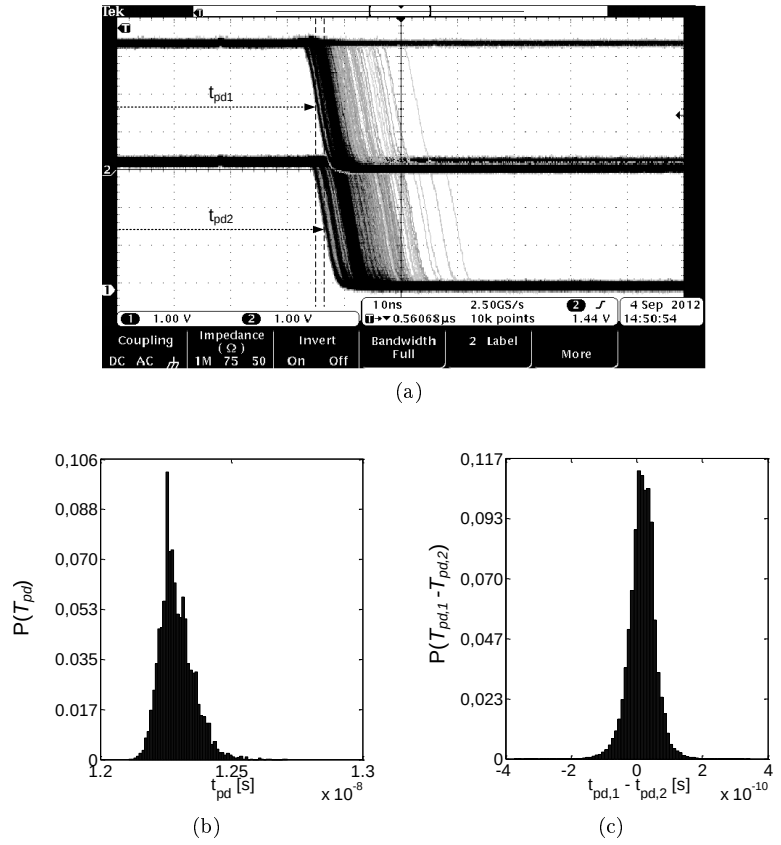
$$P(T_{pd}) = \frac{1}{\sigma\sqrt{2\pi}} \frac{\tau}{\tau_1} \cdot e^{\frac{-T_{pd}}{\tau_1}} \cdot e^{-\tau e^{\frac{(-\frac{T_{pd}}{\tau_1}+\delta_1-\delta)^2}{2\sigma^2}}}, \tag{1}$$

gdzie δ_1 to taki interwał między zboczami aktywnymi sygnałów danych i zegara (lub Reset i Set), które prowadzą do losowego stanu na wyjściu przerzutnika po osiągnięciu stanu stabilnego, tj. gdy $t_{pd} \to \infty$, σ to parametr reprezentujący napięciowy szum termiczny elementów aktywnych przerzutnika wyrażony w woltach, a τ i τ_1 to stałe czasowe wynikające z parametrów dynamicznych elementów aktywnych objętych pętlą dodatniego sprzężenia zwrotnego. W modelu (1) przyjęto, że szum napięciowy elementów aktywnych układu przerzutnikowego ma rozkład normalny.

Zaproponowany przeze mnie model (1) opisujący $P(T_{pd})$ dobrze przybliża rzeczywisty rozkład zmiennej losowej czasu propagacji układu przerzutnikowego i pozwala na opis T_{pd} jako źródła prawdziwie losowego w generatorze TRNG. Niestety parametry statystyczne (1) silnie zależą od parametrów roboczych układu przerzutnikowego, co utrudnia zastosowanie T_{pd} w bliskim otoczeniu punktu równowagi chwiejnej, jako źródła entropii w generatorze TRNG. Okazuje się jednak, że zastosowanie różnicy dwóch niezależnych zmiennych losowych $T_{pd,1}$ i $T_{pd,2}$ opisanych przez (1), z dwóch przerzutników pracujących w podobnych warunkach, pozwala na uzyskanie zmiennej losowej o symetrycznym rozkładzie gęstości prawdopodobieństwa, o wartości oczekiwanej zbliżonej do zera. Dla zobrazowania tej koncepcji na rys. 1a przedstawiłem oscylogramy odpowiedzi uzyskanych na wyjściach dwóch przerzutników umieszczonych w jednym układzie scalonym. Na rys. 1b pokazałem rozkład $P(T_{pd})$ uzyskany z czasów odpowiedzi jednego z przerzutników opisany przez (1) uzyskany w układzie FPGA (rodzina Spartan 3E), natomiast na rys. 1c rozkład będący różnicą dwóch niezależnych zmiennych losowych $T_{pd,1}$ i $T_{pd,2}$.

Rozkład $P(T_{pd,1} - T_{pd,2})$ został opisany na gruncie teorii w pracy [A5], a metoda jego generacji zastrzeżona w [P2] i [ZP6], natomiast w pracach [A4] i [A7] wykorzystano właściwość $P(T_{pd,1} - T_{pd,2})$ polegającą na zerowych wartościach oczekiwanej i skośności. Okazuje się, że przez zastosowanie odpowiedniego układu arbitrażu zastrzeżonego w [P1], [ZP5] możliwa jest wydajna i szybka klasyfikacja zdarzeń zachodzących, gdy $T_{pd,1} - T_{pd,2} > 0$ albo $T_{pd,1} - T_{pd,2} \leq 0$. Z kolei obciążenie rozkładu jedynek i zer logicznych generowanych przez układ arbitrażu jest z oczywistych względów zbliżone do zera i w niewielkim stopniu zależy od temperatury lub napięcia zasilającego układ TRNG.

Mechanizm generacji zmiennej losowej T_{pd} wymaga uzyskania takiego interwału δ aby odchylenia standardowe $\sigma(T_{pd})$ oraz $\sigma(T_{pd,1} - T_{pd,2})$ były wystarczające do dyskryminacji zdarzeń $T_{pd,1} - T_{pd,2} > 0$

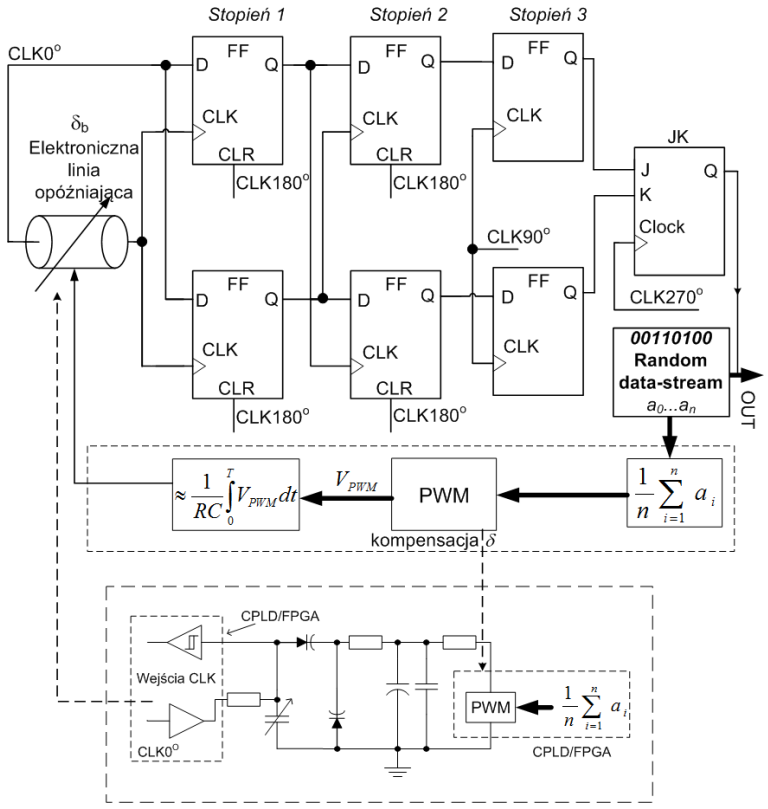


Rysunek 1: Czasy odpowiedzi dwóch układów przerzutnikowych w jednym układzie scalonym (a) oraz empirycznie uzyskane rozkłady gęstości prawdopodobieństwa: (b) $P(T_{pd})$ oraz (c) $P(T_{pd,1} - T_{pd,2})$

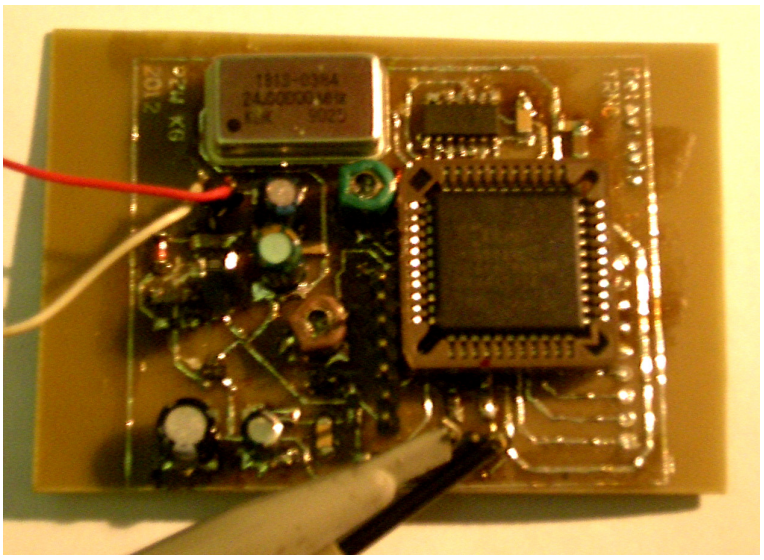
albo $T_{pd,1} - T_{pd,2} \leq 0$ przez układ arbitrażu. W tym celu konieczna jest precyzyjna kontrola odstępu δ pomiędzy zboczami aktywnymi sygnałów sterujących układami bistabilnymi. Ponadto interwał δ wymaga adaptacji, gdyż podlega on rozrzutom wewnątrz- i między-układowym (ang. 'intra-class variation' i 'inter-class variation'), a czasy propagacji sygnałów w układach programowalnych zmieniają się w funkcji temperatury i zasilania, co dokładnie opisałem w pracy [A2]. Uzyskanie $\sigma(T_{pd,1} - T_{pd,2})$ odpowiedniego dla danego układu arbitrażu wymaga zastosowania układu programowalnej linii opóźniającej. W pracy [A5] zaproponowałem rozwiązanie wykorzystujące analogową linię opóźniającą z diodami pojemnościowymi (warikapami), a w [P4]-[P6], [ZP6]-[ZP10] wspólnie z dr. inż. K. Gołofitem zastrzegliśmy różne warianty topologiczne tego rozwiązania. Na rys. 2a przedstawiłem ogólną koncepcję rozwiązania TRNG podzielonego na trzy stopnie wraz z przykładowym blokiem adiustacji (kompensacji) δ. Z kolei na rys. 2b przedstawiłem zrealizowany prototyp układu z rys. 2a z analogową linią opóźniającą i warikapami.

W rozwiązaniu przedstawionym na rys. 2a pierwszy stopień odpowiedzialny jest za uzyskanie $P(T_{pd,1} - T_{pd,2})$, z kolei kolejne stopnie pełnią funkcję arbitra i układu tworzącego wyjściowy ciąg binarny $a_0...a_n$. W publikacji [A4] i [A7] zaproponowałem rozwiązanie wykorzystujące cyfrowy menedżer dystrybucji sygnału zegarowego układu FPGA (ang. 'Digital Clock Menager' – DCM), do kompensacji δ, zamiast bloku analogowej linii opóźniającej z diodami pojemnościowymi. W ten sposób możliwa stała się integracja całego układu z rys. 2a w jednym układzie FPGA, a rozdzielczość linii opóźniającej osiągnęła 18 ps i 40 ps, odpowiednio w układach Spartan 3 i Spartan 6.

Koncepcja przedstawiona na rys. 2a posiada bardzo prosty mechanizm kompensacji δ wykorzystujący uśrednianie $a_0...a_n$ do sterowania układem modulacji wypełnienia impulsów (ang. 'Pulse Width Modulation' – PWM). Zadaniem układu PWM jest z kolei wytwarzanie napięcia stałego do sterowania warikapami w linii opóźniającej zmieniającej δ. Mechanizm ten niestety nie jest pozbawiony wad, czego skutkiem jest występowanie chwilowego obciążenia ciągu $a_0...a_n$, które prowadzi do konieczności stosowania tzw. korekcji Von-Neumanna [28]. Problem ten występuje także w rozwiązaniu opisanym w [A7], w którym zamiast analogowej linii opóźniającej wykorzystałem układ DCM. Z kolei zastosowanie korekcji ciągu $a_0...a_n$ prowadzi do spadku i fluktuacji przepustowości (ang. 'bitrate' lub 'throughput'), co opisano

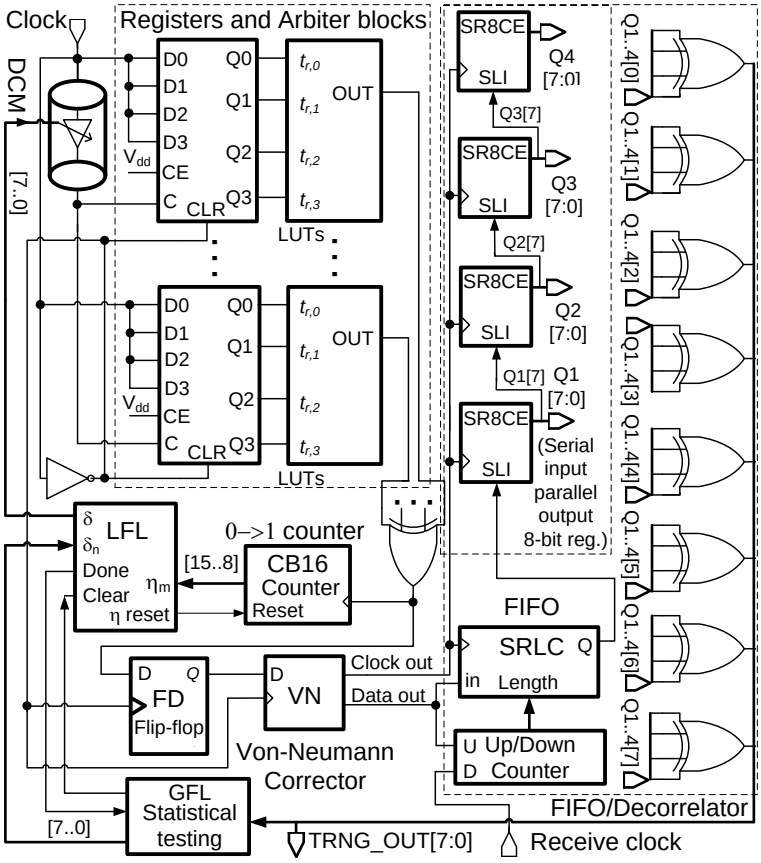


(a)



(b)

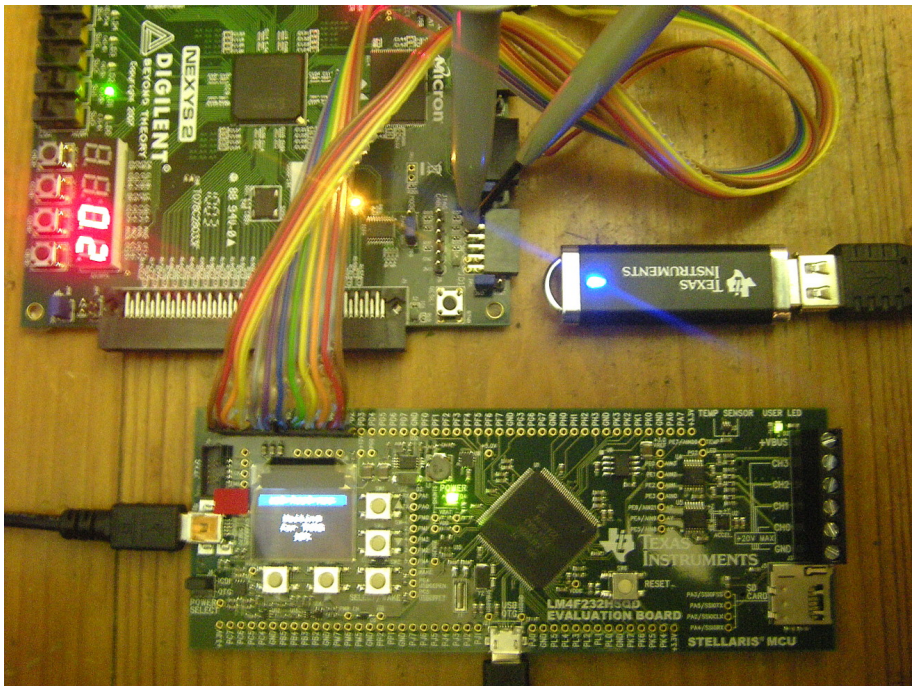
Rysunek 2: Układ TRNG wykorzystujący różnicę $T_{pd,1} - T_{pd,2}$ wraz z systemem arbitrażu, układem linii opóźniającej i automatycznej adiustacji δ: (a) schemat blokowy; (b) prototyp z analogową linią opóźniającą opisany w [A5] i opatentowany.



Rysunek 3: Układ TRNG z podwójnym blokiem adiustacji (kompensacji) δ, tj LFL i GFL

w [A5]. W związku z tym zaproponowałem rozbudowany mechanizm dwustopniowej kompensacji lokalnej (ang. 'local feedback loop' – LFL) i globalnej (ang. 'global feedback loop' – GFL) interwału δ w układzie TRNG. Rozwiązanie to zostało opisane w artykule [A4] i pozwala na utrzymanie stałej przepustowości, właściwie niezależnie od warunków zewnętrznych, zasilania oraz typu i egzemplarza układu scalonego, w którym zaimplementowano TRNG. Schemat blokowy tego rozwiązania zamieściłem na rys. 3.

W układzie TRNG przedstawionym na rys. 3 zintegrowano wszystkie funkcje w pojedynczym układzie scalonym FPGA, tj. blok adiustacji δ przez DCM, zwielokrotniony blok generacji $P(T_{pd,1} - T_{pd,2})$, blok arbitrażu, bloki LFL oraz GFL oraz kolejkę FIFO o adaptacyjnie zmienianej długości. W rozwiązaniu tym blok LFL dokonuje poszukiwania takiej wartości δ (optymalizacji), aby uzyskać maksymalną entropię ciągu binarnego, chwilę po inicjalizacji układu TRNG (np. uruchomienia zasilania). Po wykonaniu optymalizacji δ, blok LFL przestaje być aktywny, za to blok GFL dokonuje ciągłej korekty δ w otoczeniu ± 40 ps w trakcie normalnej pracy układu TRNG. Korekta w trakcie pracy GFL przeprowadzana jest na podstawie testów χ^2 obliczanych na 40 kB ciągach $a_0 ... a_n$. Testy χ^2 są przeprowadzane na bieżąco (ang. 'on the fly'), dzięki czemu zaproponowane przeze mnie rozwiązanie zapewnia bardzo wysoką jakość ciągów binarnych mierzoną testami Diehard i NIST [18, 13] pierwszego i drugiego poziomu [16, 15]. Z powodu bardzo dobrych właściwości, rozwiązanie przedstawione na rys. 3 wymagało zastosowania specjalnej metodyki badania ciągów $a_0 ... a_n$, aby w ogóle możliwa była ocena wpływu warunków zewnętrznych (zasilania i temperatury) na pracę układu. W tym celu napisałem skrypty w środowisku Matlab do przeprowadzania automatycznych testów statystycznych (Kołmogorowa - Smirnowa i χ^2) na p-wartościach zwracanych przez testy Diehard i NIST. Dopiero takie „hybrydowe" (dwupoziomowe) testy pozwoliły na analizę wpływu czynników zewnętrznych na parametry losowe ciągów $a_0 ... a_n$. Należy nadmienić, że testy dwupoziomowe wykonywałem na zbiorach danych sięgających pojedynczych GB, co wiązało się z koniecznością szybkiej akwizycji danych z układu TRNG zaimplementowanego w FPGA. W tym celu samodzielnie oprogramowałem w języku C platformę TM4C123G firmy Texas Instruments, która zapisywała na bieżąco dane z układu FPGA na przenośnym dysku USB. Na rys. 4 przedstawiłem



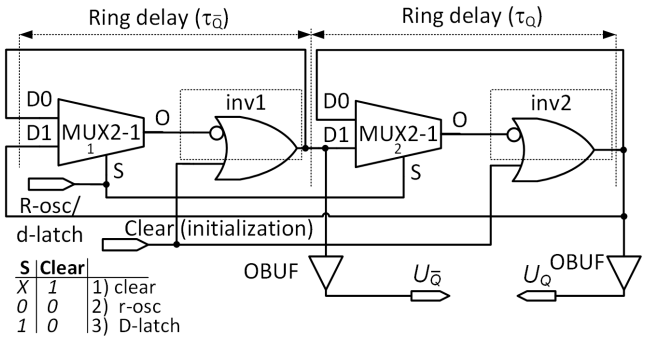
Rysunek 4: Zestaw TM4C123G dołączony do platformy Digilent 2 zapisujący dane z TRNG utworzonego w układzie Spartan na platformie Nexys 2

zaprogramowany przez mnie zestaw TM4C123G w trakcie akwizycji ciągów binarnych, dołączony do platformy z układem Spartan z TRNG przedstawionym na rys. 3.

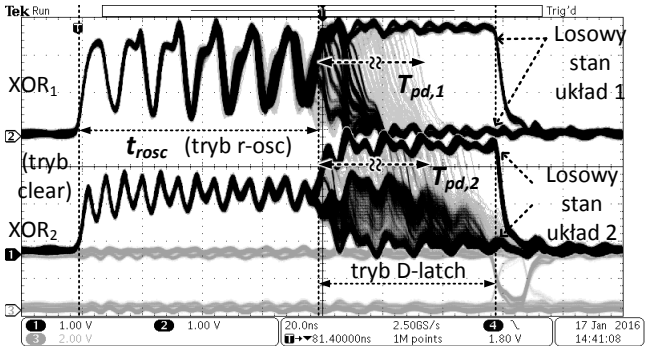
Częstym problemem występującym w układach TRNG jest asynchroniczna generacja kolejnych wyrażeń ciągu $a_0...a_n$. Przyczyną tej właściwości jest stosowanie układów korekcji, jak np. wspomniany już korektor Von-Neumanna, który zwraca kolejne wartości wyjściowe na podstawie wartości par wejściowych a_0a_1, a_2a_3, a_4a_5, ..., $a_{n-1}a_n$. Rozkład czasów pomiędzy kolejnymi losowymi bitami na wyjściu korektora Von-Neumanna ma rozkład Poissona, co omówiłem w artykule [A4]. Jeśli znana jest wartość oczekiwana czasów pomiędzy generacją kolejnych bitów wyjściowych korektora (na podstawie rozkładu Poissona), możliwe jest oszacowanie minimalnej długości kolejki FIFO, która przy założonym minimalnym BER, zapewni strumień danych wyjściowych (losowy ciąg binarny) TRNG o stałej przepustowości. W pracy [A4] zaproponowałem sposób wyznaczania długości kolejki FIFO i sposób synchronizacji danych wyjściowych z korektora Von-Neumanna.

Wymienione dotychczas rozwiązania wymagają stosowania linii opóźniających, co znacząco zwiększa zasoby potrzebne do konstrukcji generatora losowego TRNG. W pracy [A2] zaproponowałem rozwiązanie alternatywne, które do wytworzenia odpowiedniej δ wykorzystuje generatory pierścieniowe włączane i wyłączane przed generacją właściwego bitu losowego. Zaletą tego rozwiązania przedstawionego na rys. 5 jest mała ilość zasobów (ang. 'footprint'), a także korzystny wpływ szumu fazowego generatorów pierścieniowych na losowość uzyskiwanych zdarzeń na wyjściu układu bistabilnego.

Istotą rozwiązania przedstawionego na rys. 5. jest możliwość pracy w trzech trybach, tj., przygotowania/kasowania (ang. 'clear'), trybie oscylacyjnym dwóch niezależnych generatorów pierścieniowych (ang. 'Ring Oscillators' – *r-osc*) i trybie zatrzasku (ang. 'D-Latch'); zależnie od bitów sterujących wejściami *S* oraz *Clear*. Po fazie przygotowania/kasowania układ przełączany jest przez automat skończony do pracy w trybie *r-osc*, po czym po uzyskaniu odpowiedniego szumu fazowego i koherencji zboczy narastających przełączany jest w tryb *D-Latch*. W zaproponowanym rozwiązaniu, zależnie od sygnałów sterujących dochodzi do zmiany ścieżek pętli sprzężenia zwrotnego, oraz zamiany pracy samowzbudnej (niestabilnej) w sekcjach aktywnych z inwerterami i multiplekserami (odpowiednio MUX2-1_1 i inv1 oraz MUX2-1_2 i inv2) na pracę autonomiczną stabilną (w $t \to \infty$). Przykładowe implementacje tego rozwiązania, które zrealizowałem zarówno w układach CPLD (z rodziny CoolRunnerII) jak i FPGA (z rodziny Spartan 6



Rysunek 5: Koncepcja generatora liczb prawdziwie losowych wykorzystującego generatory pierścieniowe i układ bistabilny



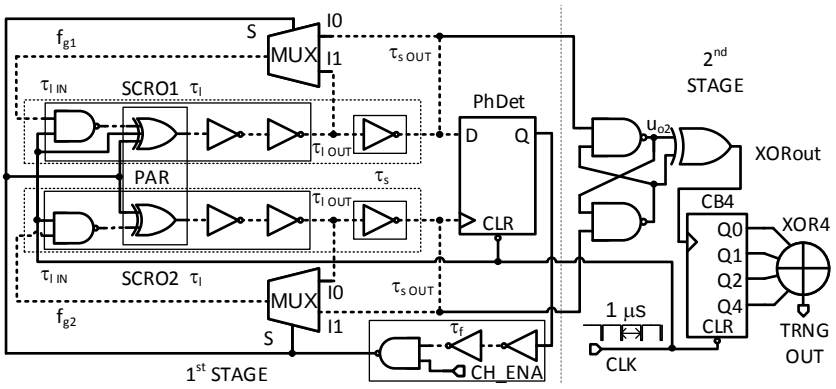
Rysunek 6: Przebiegi na wyjściach układu w kolejnych, następujących po sobie fazach

i Artix), wykazały wysoką zgodność zachowania tego rozwiązania z opisem teoretycznym, który zamieściłem w artykule [A2]. W celu ułatwienia zrozumienia przedstawionej koncepcji, na rys. 6 zamieściłem przebiegi uzyskane z dwóch identycznych układów przedstawionych na rys. 5, których wyjścia U_Q i $U_{\bar{Q}}$ dołączone zostały do dwuwejściowych bramek XOR (tj. $XOR_1(U_{Q,1}, U_{\bar{Q},1})$ i $XOR_2(U_{Q,2}, U_{\bar{Q},2})$).

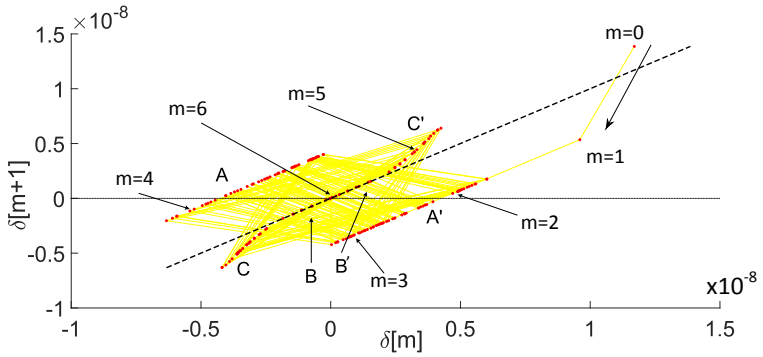
Sygnały na wyjściach obu bramek XOR wskazują na występowanie okresowych koincydencji (koherencji fazy) U_Q i $U_{\bar{Q}}$ w trybie *r-osc* układu. Z kolei zwiększające się rozmycie oscylogramów, wraz ze wzrostem czasu pracy w tym trybie (t_{rosc}), związane jest z błądzeniem przypadkowym fazy. Przejście z pracy oscylacyjnej tj., przełączenie między trybami *r-osc* i *D-Latch* prowadzi do inicjalizacji pracy autonomicznej układu bistabilnego (zatrzasku D-latch) z losowym warunkiem początkowym. Skutkuje to uzyskaniem losowego czasu odpowiedzi T_{pd}, losowego stanu końcowego układu (układów) bistabilnych, oraz losową liczbą gasnących oscylacji w trybie zatrzasku. Zaprezentowane przeze mnie rozwiązanie posiada zatem kilka źródeł entropii, które mogą być wykorzystane do generacji ciągów $a_0...a_n$, co czyni je konkurencyjnym w odniesieniu do rozwiązań przedstawionych w [23, 1]. Ponadto niezwykle mała ilość wykorzystywanych zasobów pozwala na wykorzystanie go w układach Internetu rzeczy (ang. 'Internet of Things' – IoT), czy rozwiązaniach systemów jednoukładowych (ang. 'System on Chip' – SoC), w których istotna jest oszczędność takich zasobów jak np. DCM.

Przedstawione rozwiązanie pomimo pozornej prostoty jest niezwykle złożone w opisie. W celu opisu behawioralnego układu z rys. 5 skonstruowałem algorytmy w środowisku Matlab do obliczania równań różniczkowych stochastycznych z opóźnieniami (ang. 'Stochastic Differential Delay Equations' – SDDE), dzięki którym uzyskałem wyniki opublikowane w [A2]. Należy nadmienić, iż na realizację wymienionych prac otrzymałem trzeci grant dziekański pt. „Rozwój badań nad źródłami prawdziwie losowymi odpornymi na nieinwazyjne ataki wstrzykiwania energii".

Rozwiązania tzw. lekkich (ang. 'lightweight') modułów kryptograficznych, w tym generatorów liczb prawdziwie losowych stały się ostatnio niezwykle popularne. Dlatego postanowiłem rozwijać koncepcje układów TRNG o małym zapotrzebowaniu na zasoby. Kolejne zaproponowane przeze mnie rozwiązanie (wspólnie z dr. inż. Krzysztofem Gołofitem), jest rozwiązaniem hybrydowym z dwoma źródłami (stopniami) entropii, tj. chaotycznym i oscylacyjnym metastabilnościowym. Rozwiązanie to zostało



Rysunek 7: Uproszczony schemat blokowy generatora hybrydowego

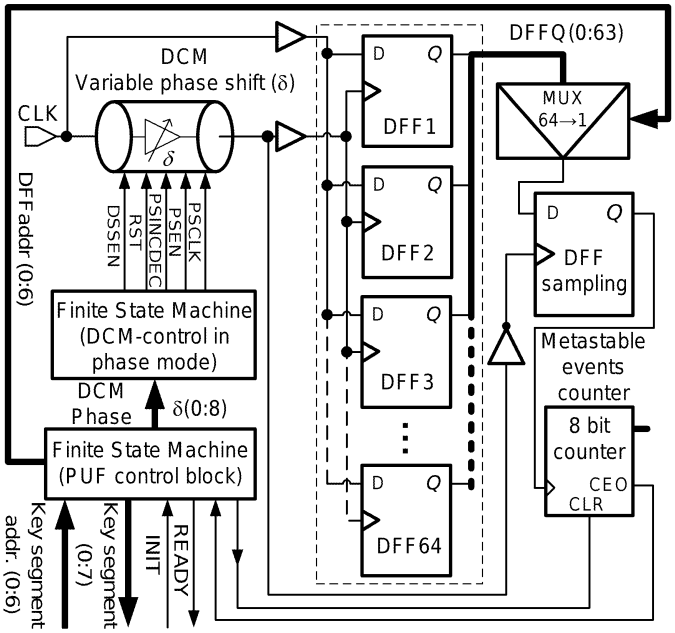


Rysunek 8: Mapa chaosu zaproponowanego układu z generatorami SCRO

szczegółowo opisane w artykule [A1] wraz z niezbędnym aparatem matematycznym, zaś uproszczony schemat blokowy układu zamieściłem na rys. 7. Rozwiązanie to zostało zgłoszone w kilku wariantach topologicznych do Urzędu Patentowego RP w [ZP1]-[ZP4], [ZP12]-[ZP14] i potwierdzone.

W rozwiązaniu tym, zaproponowałem wykorzystanie specjalnych generatorów pierścieniowych z przełączalną ścieżką propagacji (ang. 'switchable chain ring oscillators' – SCROs), których zadaniem jest generacja przebiegów na wejściach detektora fazy (PhDet). W systemie na rys. 7 układ detektora PhDet dokonuje korekty fazy na podstawie odległości między zboczami aktywnymi na wyjściach SCRO1 i SCRO2. Ponieważ ścieżki propagacji w SCRO1 i SCRO2 ulegają jedynie dyskretnym zmianom z $\tau_l + \tau_s$ na τ_l i odwrotnie, w układzie nigdy nie jest możliwe uzyskanie stanu równowagi fazowej. Ponadto, dzięki występowaniu nieciągłości stanów logicznych w trakcie przełączania ścieżek propagacji w SCRO1 i SCRO2, przy odpowiednio dobranych opóźnieniach τ_s, τ_l i τ_f dochodzi do pracy chaotycznej o dość ciekawej mapie, przedstawionej na rys. 8. Dla ułatwienia na mapie na rys. 8 oznaczyłem początkowe punkty ($m \in [0, 6]$) trajektorii fazowej.

Niewątpliwą zaletą omawianego rozwiązania jest to, że zgodnie z mapą przedstawioną na Rys. 8, zmienną stanu systemu jest interwał δ (czas). Ten sam interwał może zostać wykorzystany do stymulacji arbitra lub układu bistabilnego do generacji binarnego ciągu losowego $a_0 ... a_n$, co zostało opisane w artykule [A1]. Co ciekawe δ jest zmienną o wartościach ciągłych, w kolejnych n dyskretnych krokach pracy układu, czyli przełączeniach ścieżek propagacji w SCRO1 i SCRO2. Wg aktualnej wiedzy jest to jedyny układ w literaturze światowej, który pozwala na generację ciągłej zmiennej losowej w cyfrowym układzie chaotycznym. Ta konkretna właściwość sprawia, że rozwiązanie opisane wspólnie z dr inż. K. Gołofitem może zostać zaimplementowane w dowolnym układzie programowalnym klasy CPLD lub FPGA. Na rys. 8 oznaczono dodatkowo zakresy pracy układu chaotycznego (jest ich w sumie 6, tj. A, B, C oraz A', B', C', dla odpowiednio ujemnych i dodatnich interwałów δ). W artykule [A1] wyjaśniłem także ograniczenia entropii takiego układu na gruncie teorii grafów w powiązaniu z tymi zakresami pracy.



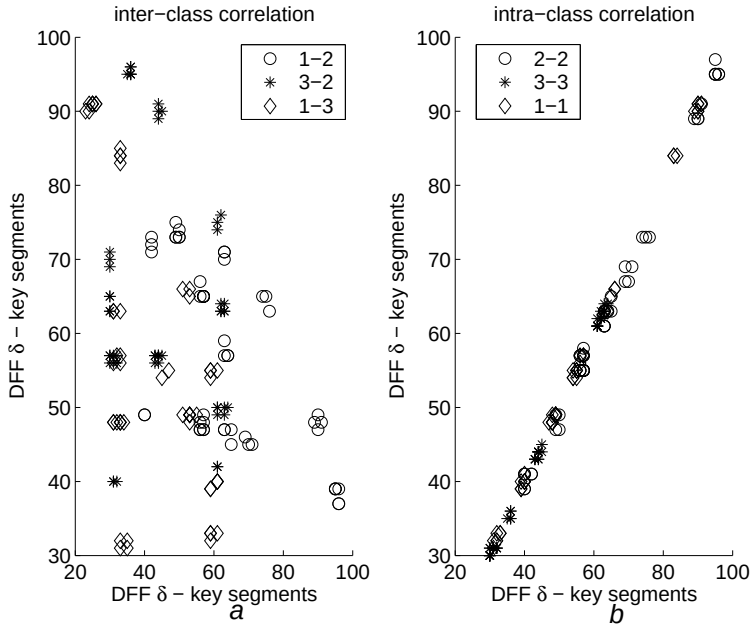
Rysunek 9: Schemat blokowy PUF w układzie FPGA

C.3 Opis i konstrukcja nowych układów fizycznie niekopiowalnych funkcji

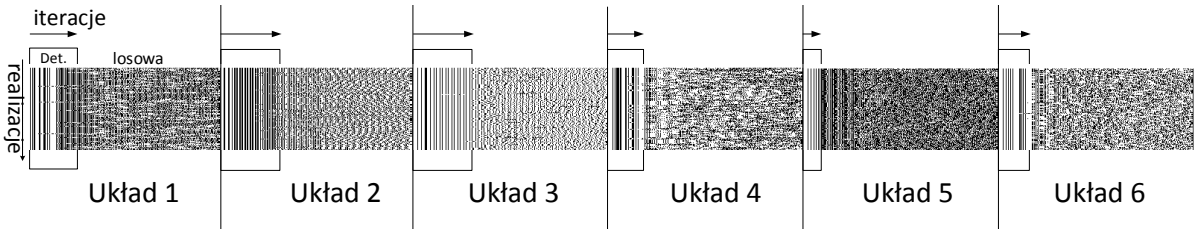
Atrakcyjną alternatywą dla uwierzytelniania sprzętu są fizycznie niekopiowalne funkcje PUF. Klasyczne metody uwierzytelniania sprzętu wymagają przechowywania kopii klucza wewnątrz układu, który ma zostać poddany uwierzytelnieniu, po dołączeniu do innego systemu. W rozwiązaniach PUF nie istnieje zapisana kopia klucza wewnątrz urządzenia, a klucz jest tworzony zgodnie z zapotrzebowaniem, zwykle na podstawie wewnątrzukładowych parametrów fizycznych podlegających rozrzutom międzyegzemplarzowym. Nie jest zatem możliwe wydobycie klucza na zewnątrz urządzenia, gdyż nie istnieje on w jego wnętrzu. Istotną właściwością PUF jest generowanie różnych kluczy przy podawaniu różnych pobudzeń (tzw. wektorów inicjalizujących). Oznacza to, że PUF wytwarza taki sam klucz w obrębie konkretnego egzemplarza układu, pod warunkiem, że będzie pobudzany w ten sam sposób, tj. tym samym wektorem inicjalizującym.

Wspólnie z dr. inż. Krzysztofem Gołofitem zaproponowałem rozwiązanie PUF, w którym klucz tworzony jest na podstawie rozrzutów parametrów przerzutników typu D w układzie FPGA. Parametrem podlegającym rozrzutowi jest tu zakres odległości zboczy aktywnych, przy których dochodzi do powstawania błędów na wyjściu przerzutnia typu D (ang. 'D Flip-Flop' – DFF). Rozwiązanie to zostało opatentowane w Urzędzie Patentowym RP [P3]. Okazuje się, że właściwie każdy przerzutnik typu D w układzie FPGA (DFF) posiada inny dozwolony czas ustalania (t_{su}), wystarczy zatem oszacować jego średnie wartości dla wybranego zestawu przerzutników (zestaw ten jest jednocześnie wektorem inicjalizującym PUF) i użyć ich do konstrukcji klucza. W rozwiązaniu, które opisałem w artykule [A6] pomiar t_{su} odbywa się poprzez iteracyjne zmniejszanie odstępu pomiędzy zboczami aktywnymi na wejściach danych i zegara wybranego przerzutnika D. Za zmianę tego odstępu odpowiedzialny jest blok DCM układu FPGA Spartan 6. W momencie, w którym dochodzi do powstawania stanów logicznych niezgodnych z tabelą prawdy przerzutnika, interwał ($\delta = min\, t_{su}$) zadawany przez DCM zostaje zapisany w pamięci układu FPGA jako zmienna 8-bitowa. Procedura ta jest powtarzana dla założonego zestawu przerzutników. Zestaw ten wybrany przez n-elementowy wektor inicjalizujący odpowiada generacji n segmentów klucza PUF. Na rys. 9 zamieściłem schemat blokowy rozwiązania zaproponowanego w artykule [A6].

Cały system przedstawiony na rys. 9 może być zintegrowany w układzie FPGA. W trakcie inicjalizacji układu dochodzi do ustalenia wektora inicjalizacji, poprzez wybór zbioru przerzutników typu D ($DFF_1 ... DFF_{64}$) przez automat sterujący PUF. Zadaniem drugiego automatu jest iteracyjne sterowanie modułem DCM, tak by możliwe było zbadanie interwału ($\delta = min\, t_{su}$) wybranego zestawu przerzutników. Odpowiedź układu PUF przedstawionego na rys. 9 i polega ona na iteracyjnym wysłaniu ośmiobitowych segmentów kodu (interwałów $\delta = min\, t_{su}$ wybranych przerzutników). Segmenty te tworzą ciąg



Rysunek 10: Regresja segmentów klucza: (a) brak zależności pomiędzy segmentami klucza PUF w różnych egzemplarzach układu FPGA, (b) wysoka korelacja segmentów klucza dla tych samych wektorów inicjalizujących.



Rysunek 11: Ciągi zer (białe piksele) i jedynek (czarne piksele) uzyskanych w sześciu różnych układach, kolejne wiersze odpowiadają kolejnym realizacjom. Strzałki wskazują na czas pracy chaotycznej deterministycznej w każdym z sześciu układów.

zmiennych losowych, różny dla różnych wektorów inicjalizujących i egzemplarzy układów FPGA. Na rys. 10b. przedstawiłem wykresy obrazujące korelację zmiennych losowych generowanych (segmentów klucza kryptograficznego) w tym samym układzie FPGA, dla tych samych wektorów inicjalizujących (ang. 'intra-class correlation'). Z kolei wykres na rys. 10a wskazuje na brak korelacji generowanych segmentów dla tych samych wektorów inicjalizujących w różnych egzemplarzach układu FPGA tego samego typu (ang. 'inter-class correlation').

Istotnym problemem w implementacji PUF jest wydobycie informacji o minimalnych różnicach parametrów fizycznych elementów aktywnych układu elektronicznego. W trakcie badań nad układem chaotycznym, który opisałem w artykule [A1], okazało się, że początkowe, deterministyczne kroki trajektorii fazowej zależą głównie od rozrzutów elementów aktywnych bloków SCRO1 i SCRO2, natomiast minimalny wpływ na ten zakres pracy chaotycznej mają zjawiska szumowe. Możliwe jest zatem tworzenie kluczy PUF w oparciu o trajektorie układu chaotycznego opisanego w [A1]. Rozwiązanie problemu pozyskiwania kluczy w początkowej fazie tzw. chaosu deterministycznego układu z rys. 7 rozwiązał dr inż. Krzysztof Gołofit wspólnie ze mną, a rozwiązanie to zostało zgłoszone i potwierdzone przez Urząd Patentowy RP [ZP4], [ZP11]. Układ PUF oparty o trajektorię tzw. chaosu deterministycznego został opisany w artykule „Chaos-based Physical Unclonable Functions", który jest w trakcie recenzji. Przykładowe ciągi binarne, uzyskiwane w sześciu różnych egzemplarzach układu tego samego typu, przedstawiłem na rys. 11.

Białe i czarne piksele na rys. 11 odpowiadają generacji odpowiednio zer i jedynek przez wyjście Q układu PhDet (na rys. 7). Początkowy zakres pracy chaotycznej w każdym z egzemplarzy układu FPGA ma właściwości deterministyczne (powtarza się w kolejnych realizacjach, tj. kolejnych wierszach), co przejawia się powtarzalnością ciągów binarnych między realizacjami. Dopiero po upływie pewnej, zależnej od egzemplarza układu liczby iteracji (porównań fazy SCRO1 i SCRO2), dochodzi do pracy chaotycznej niedeterministycznej, obserwowanej jako różne kombinacje pikseli w różnych realizacjach (wierszach). Zgodnie ze wstępnymi badaniami przeprowadzonymi przeze mnie i dr. inż. K. Gołofita, możliwe jest wykorzystanie czasu pracy chaotycznej deterministycznej lub trajektorii tego zakresu pracy do tworzenia segmentów kluczy kryptograficznych.

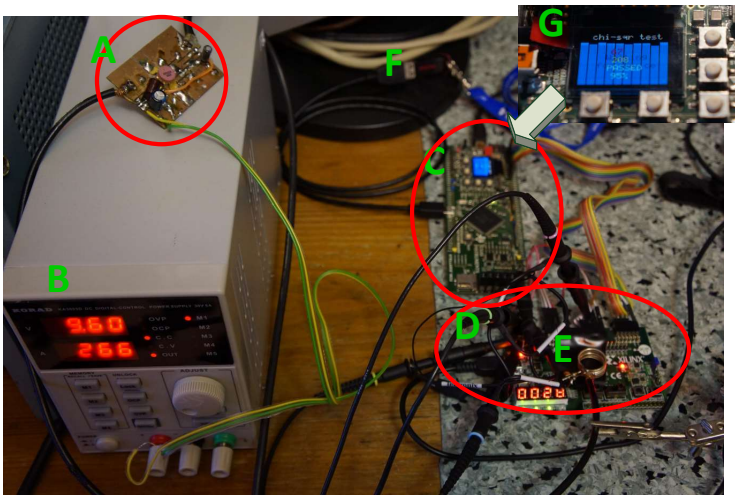
C.4 Bezpieczeństwo generatorów liczb losowych i fizycznie niekopiowalnych funkcji

Układy odpowiedzialne za generację ciągów losowych, czy to TRNG czy PUF, są krytycznymi elementami systemów odpowiedzialnych za bezpieczeństwo informacji. Stąd konieczność takiego ich konstruowania, by nie były podatne na tzw. ataki, a w szczególności ataki elektromagnetyczne [12]. W publikacjach [A1], [A2], [A3], [B8] szeroko omawiam bądź to modelowanie wpływu ataku na zachowanie generatora TRNG, bądź eksperymenty polegające na tzw. atakach częstotliwościowych. W pracy [B8] przedstawiłem łatwy w implementacji układ generatora liczb prawdziwie losowych. Nowością w tym rozwiązaniu jest przeprowadzanie samodiagnostyki, na podstawie której układ sam dobiera rozmiar łańcucha generatorów pierścieniowych, tak by losowy ciąg binarny charakteryzował się najmniejszym obciążeniem rozkładu. Pokazałem m.in. wpływ ataku radiowego (częstotliwościowego) na szum fazowy generatorów pierścieniowych tego generatora. Okazuje się, że posiadając informację o przybliżonej częstotliwości oscylacji własnych generatorów pierścieniowych, można przy zastosowaniu nadajnika odpowiedniej mocy wraz z anteną pętlową, zsynchronizować pracę generatorów pierścieniowych zaimplementowanych wewnątrz układu CPLD lub FPGA. Prowadzi to do drastycznego (blisko dwudziestokrotnego wg. danych opublikowanych w [B8]) spadku wariancji fazy, co przekłada się na zmniejszenie rozmiaru zbioru generowanych kluczy. Jednakże przedstawione w [B8] połączenie hybrydowe dwóch źródeł entropii, tj. generatorów pierścieniowych wraz z przerzutnikiem pracującym w otoczeniu równowagi metastabilnej poprawia parametry statystyczne generatora poddanego atakowi częstotliwościowemu.

Przeprowadzenie ataków częstotliwościowych omówionych w artykułach [A1], [A2], [A3], [B8] wymagało konstrukcji stanowiska pozwalającego na:
— precyzyjne zadawanie mocy sygnału atakującego,
— precyzyjne zadawanie częstotliwości sygnału atakującego,
— testy statystyczne 'on-the-fly' ciągów generowanych przez generatory poddawane atakom.
Na rys. 12 przedstawiłem skonstruowane przeze mnie stanowisko do ataków częstotliwościowych drogą radiową. Stanowisko składa się z: (A) pięciowatowego wzmacniacza mocy sygnału RF o paśmie pracy $30\,MHz \ldots 100\,MHz$, (B) zasilacza, (C) oprogramowanego przeze mnie systemu wbudowanego TM4C123G firmy Texas Instruments do testów diagnostycznych ciągów binarnych, (D) badanego układu z zaimplementowanym generatorem TRNG, (E) wąskopasmowej anteny pętlowej własnej konstrukcji, (F) nośnika danych z interfejsem USB, (G) wyświetlacza OLED, pokazującego bieżące wyniki testów χ^2 oraz histogramu liczb ośmiobitowych tworzonych na bieżąco z ciągów binarnych $a_0 ... a_n$.

Opisane stanowisko było kilkukrotnie wykorzystywane, m.in. do badań nad konstrukcją generatora liczb prawdziwie losowych, całkowicie odpornego na ataki elektromagnetyczne. Rozwiązanie to opublikowałem w artykule [A3], gdzie pokazałem, że nie tylko generatory TRNG wykorzystujące układy pierścieniowe narażone są na wpływ zewnętrznych fal elektromagnetycznych. Okazuje się, że rozwiązania wykorzystujące losowość stanu końcowego układu bistabilnego (metastabilność) są także podatne na wpływ zewnętrznego sygnału radiowego. Odpowiednia synchronizacja impulsów radiowych z wewnętrznym zegarem układu TRNG może w znaczący sposób wpłynąć na przewidywalność ciągów binarnych. Pokazałem, że współczynnik korelacji dla ciągów binarnych pochodzących z generatora TRNG wykorzystującego losowość stanu przerzutnika (podobne rozwiązanie zaproponował Intel), może sięgać nawet 0,3. Oznacza to, drastyczny spadek liczności zbioru generowanych kluczy.

W związku z powyższym zaproponowałem rozwiązanie generatora losowego, w którym zbocza sygnału zegarowego doprowadzanego do struktury TRNG w FPGA zostają doszumione w dziedzinie czasu (ang. 'dithering'). W tym celu wykorzystałem dodatkowy blok DCM, którego jedynym zadaniem jest losowe przesuwanie momentu pojawienia się zbocza na wejściach zegarowych DFF. Za losowy rozkład położenia zbocza zegarowego odpowiada generator pseudolosowy LFSR z ziarnem losowym pochodzącym z zabezpieczanej struktury generatora TRNG. W tym rozwiązaniu nie możliwe jest określenie momentu



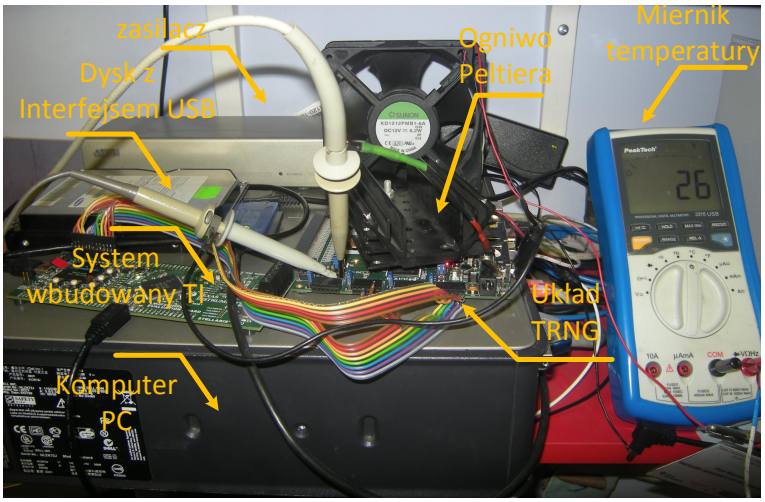
Rysunek 12: Stanowisko do ataków częstotliwościowych

zapisu danych do układów przerzutnikowych, nie jest zatem możliwe celowe wpływanie na ich zawartość. Ewentualne błędy wywołane wpływem fal radiowych z atakującego generatora będą miały charakter losowy, a więc nie wpłyną na współczynnik korelacji pomiędzy sygnałem ataku częstotliwościowego, a wyjściowym ciągiem binarnym. Przeprowadzone badania, opisane w [A3] wskazały na sześciokrotny spadek współczynnika korelacji pomiędzy sygnałem atakującym, a wyjściowym ciągiem binarnym przy wykorzystaniu zaproponowanej przeze mnie techniki.

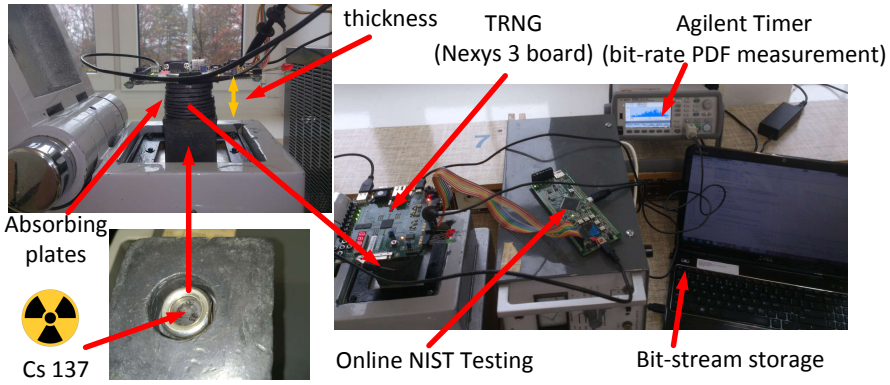
Badania nad atakami częstotliwościowymi wykazały także znaczną odporność chaotycznego rozwiązania (przedstawionego na rys. 7), w porównaniu z rozwiązaniami konwencjonalnymi z generatorami pierścieniowymi czy układami bistabilnymi. Wyniki tych badań przedstawiłem w artykule [A1]. Przyczyna kilkukrotnie mniejszej podatności tego układu jest dokładnie taka sama, jak w układzie opisanym w [A3], a wynika z rozmycia czasowego momentu generacji losowego bitu. Jednakże w układzie chaotycznym zaproponowanym na rys. 7, nie jest konieczne stosowanie dodatkowych bloków DCM wprowadzających jitter zbocza zegarowego, gdyż zmienną stanu opisującą zaproponowany układ chaotyczny jest czas. Nieokreśloność momentu generacji losowego bitu w rozwiązaniu z rys. 7 jest więc jego immanentną cechą.

Badania nad bezpieczeństwem generatorów losowych wymagają także sprawdzenia wpływu zmian temperatury otoczenia na parametry generowanych ciągów. Ponieważ generatory TRNG lub funkcje PUF zwykle wymagają określonego zakresu pracy elementów aktywnych (lub całych bloków logicznych), to zmiany temperatury mogą zaburzyć parametry wpływające na proces stochastyczny kluczowy dla generacji losowych bitów. Parametrem takim może być np. interwał δ, moment koherencji zboczy aktywnych generatorów pierścieniowych, poziom napięcia progowego czy czas propagacji bramek. Niestety każdy z tych parametrów zależy pośrednio od temperatury, dlatego w artykułach [A1], [A2], [A5], [A6] przedstawiłem zależności empiryczne, ugruntowane teoretycznie, które wyjaśniają wpływ temperatury na takie parametry TRNG, jak przepustowość czy entropia. W celu weryfikacji tych zależności skonstruowałem stanowisko pomiarowe przedstawione na rys. 13. Stanowisko to składa się z testowanego układu np. TRNG, ogniwa Peltiera przykręcanego wraz z radiatorem do badanego układu, regulatora temperatury sterowanego przez komputer PC, miernika temperatury i systemu wbudowanego do zapisu ciągu binarnego na dysku twardym przez port USB.

Innym nurtem badań nad źródłami losowości wykorzystywanymi w TRNG i PUF była weryfikacja wpływu obecności promieniowania jonizującego na pracę tych źródeł. W tym celu wspólnie z prof. dr hab. Zbigniewem Wieczorkiem skonstruowałem stanowisko do badania wpływu promieniowania jonizującego na generację liczb losowych. Na rys. 14 przedstawione jest stanowisko składające się ze źródła promieniotwórczego (izotop Cezu 137); płyt ołowiowych absorbujących promieniowanie – pozwalających na regulację natężenia promieniowania przenikającego przez strukturę układu np. TRNG; badanego układu TRNG; systemu wbudowanego do testowania statystycznego generowanych ciągów; czasomierza (ang. 'timer') do pomiaru czasów pomiędzy kolejnymi generowanymi bitami losowymi i analizy histogramu tych czasów oraz komputera PC.



Rysunek 13: Stanowisko do badania wpływu temperatury na parametry układów TRNG i PUF



Rysunek 14: Stanowisko do badań wpływu promieniowania jonizującego na generację liczb losowych TRNG

W artykule [B9] wskazałem, że analiza statystyczna zdarzeń na wyjściu przerzutnika pracującego w otoczeniu równowagi chwiejnej może być wykorzystana do oceny poziomu promieniowania w otoczeniu układu elektronicznego. Ponadto pokazałem znaczący wpływ promieniowania γ na losowość pracy układów przerzutnikowych w układach FPGA z rodziny Spartan 6. W publikacji [B9] potwierdziłem zależność pomiędzy natężeniem promieniowania mierzonym zliczeniami licznika scyntylacyjnego a częstością (przepustowością) generowanych losowych bitów na wyjściu TRNG. Ponadto wskazałem na wpływ promieniowania jonizującego na p-wartości testów NIST przeprowadzonych na ciągach generowanych przez TRNG.

C.5 Podsumowanie

W podsumowaniu chciałbym podkreślić, że wymienione trzy aspekty badawcze moich prac składające się na osiągnięcie naukowe, tj.: konstrukcja generatorów liczb losowych (TRNG) i funkcji niekopiowalnych (PUF) oraz badania podatności tych układów na ataki elektromagnetyczne, są wynikiem konsekwentnej i głównie samodzielnej pracy. Wyniki badań składające się na wskazane osiągnięcie są pracami jedno lub dwuautorskimi, których jestem pierwszym autorem. Opublikowanie prac wymagało ode mnie samodzielnego planowania eksperymentów, konstruowania stanowisk badawczych i układów elektronicznych, umiejętności programistycznych, konstruowania algorytmów obliczeniowych i opisu matematycznego układów. Moje najważniejsze osiągnięcia na tym polu to:

— konstrukcja prototypu generatora TRNG opartego na układzie CPLD z układem kompensacji PWM [A5];
— opracowanie algorytmów optymalizacji przepustowości i jednostajności generowanych rozkładów (LFL i GFL) [A4];
— konstrukcja prototypu generatora TRNG opartego na układzie FPGA z systemem automatycznej regulacji długości kolejki FIFO i podwójnym mechanizmem kompensacji punktu pracy (GFL i LFL) [A4];
— konstrukcja prototypu generatora TRNG opartego na układzie FPGA wykorzystującego układ DCM do ustalania warunków pracy [A7];
— konstrukcja bezpiecznego generatora TRNG odpornego na ataki częstotliwościowe, wykorzystującego modulację fazy sygnałów zegara i danych [A3];
— konstrukcja prototypu generatora TRNG opartego na układzie CPLD CoolRunnerII i FPGA Spartan 6 wykorzystującego inicjalizację szumem fazowym [A2];
— konstrukcja bezpiecznego generatora TRNG odpornego na ataki częstotliwościowe, wykorzystującego różnicę chwilowych faz synchronizowanych generatorów pierścieniowych o regulowanej długości pierścienia [B8];
— konstrukcja bezpiecznego generatora TRNG odpornego na ataki częstotliwościowe, wykorzystującego źródło chaotyczne, którego zmienną stanu jest czas [A1];
— implementacja fizycznie niekopiowalnej funkcji (PUF) do uwierzytelniania układów programowalnych [A6];
— implementacja fizycznie niekopiowalnej funkcji (PUF) wykorzystującej zakres chaosu deterministycznego [ZP4], [ZP11];
— opis matematyczny w środowisku Matlab generatorów TRNG stochastycznymi równaniami różniczkowymi z opóźnieniami (SDDE) [A2];
— opis matematyczny funkcji gęstości prawdopodobieństwa opisującej warunek początkowy układów bistabilnych pobudzanych szumem fazowym generatora pierścieniowego [A2];
— implementacja algorytmu RC5 w układzie FPGA na potrzeby testów podatności układów na ataki częstotliwościowe;
— konstrukcja wzmacniacza mocy w.cz. i anteny pętlowej do ataków częstotliwościowych [A1];
— zestawienie systemu pomiarowo-kontrolnego do badania właściwości dynamicznych układów programowalnych w różnych temperaturach pracy;
— zestawienie stanowiska do badania wpływu promieniowania jonizującego na pracę losową układów przerzutnikowych w układach FPGA [B9];
— opracowanie skryptów automatycznej akwizycji i obróbki danych z oscyloskopów Tektronix DPO 3012 i Rigol DS-6062 w środowisku Matlab oraz skryptów do testowania statystycznego (Kołmogorowa - Smirnowa i χ^2) danych uzyskanych z narzędzi testowych NIST i Diehard [A5];

— opracowanie skryptów do automatycznej akwizycji i obróbki danych z czterokanałowego oscyloskopu Tektronix MSO 3024 w środowisku Matlab oraz skryptów do badania współczynnika korelacji ciągów binarnych.

Dzięki powyższym osiągnięciom znacząco rozwinąłem dziedzinę konstrukcji generatorów losowych i układów uwierzytelniania sprzętowego z wykorzystaniem PUF w kraju. Zagadnienia badawcze, którymi się zajmuję oraz moje doświadczenie zostały już częściowo wykorzystane w realizacji prac dyplomowych studentów oraz w uruchomieniu nowego przedmiotu na Wydziale Matematyki i Nauk Informacyjnych PW. Przedmiot ten prowadzony zarówno w języku polskim jak i angielskim traktuje o tematyce układów i systemów wbudowanych. Zainteresowanie dziedziną, którą rozwijam przejawiają także krajowe firmy i instytucje jak np. firma FastLogic z Łodzi (wspólny wniosek do NCBiR związany z realizacją zintegrowanych modułów kryptograficznych zawierających TRNG i PUF) czy Polski Instytut Badań i Rozwoju Inwestycji - PIBiR w ramach Funduszu Bridge Alfa.

Literatura

[1] Advanced security features of Intel vPro technology. *Intel Technology Journal*, 12, December 2008.

[2] A. Beirami, H. Nejati, and W.H. Ali. Zigzag map: a variability-aware discrete-time chaotic-map truly random number generator. *Electronics Letters*, 48(24), November 2012.

[3] Milos Drutarovský and Galajda Pavol. A robust chaos-based true random number generator embedded in reconfigurable switched-capacitor hardware. *Radioelektronika, 2007. 17th International Conference*, pages 1–6, 2007.

[4] Michael Epstein, Laszlo Hars, Raymond Krasinski, Martin Rosner, and Hao Zheng. Design and implementation of a true random number generator based on digital circuit artifacts. In Colin Walter, editor, *Cryptographic Hardware and Embedded Systems - CHES 2003*, volume 2779 of *Lecture Notes in Computer Science*, pages 152–165. Springer Berlin / Heidelberg, 2003.

[5] Michael François, David Defour, and Christophe Negre. A fast chaos-based pseudo-random bit generator using binary64 floating-point arithmetic. *Informatica*, 38, June 2014.

[6] J. D. Golic. New methods for digital generation and postprocessing of random data. *IEEE Transactions on Computer-Aided Design*, 55(10):1217–1229, 2006.

[7] Hisashi Hata and Shuichi Ichikawa. FPGA implementation of metastability-based true random number generator. *IEICE Transactions on Information and Systems*, E95.D(2):426–436, 2012.

[8] Jens U. Horstmann, Hans W. Eichel, and Robert L. Coates. Metastability behavior of CMOS ASIC flip-flops in theory and test. *IEEE Journal of Solid-State Circuits*, 24(1):146 – 157, February 1989.

[9] Benjamin Jun and Paul Kocher. The Intel random number generator. *White Paper Prepared for Intel Corporation, Cryptography Research*, April 1999.

[10] Tin Ni Ni Kyaw and Akio Tsuneda. New sets of binary functions for generating orthogonal codes with negative auto-correlation based on bernoulli chaotic map. *International Conference on Information and Communication Technology Convergence (ICTC)*, 2016.

[11] Mehrdad Majzoobi, Farinaz Koushanfar, and Srinivas Devadas. FPGA-based true random number generation using circuit metastability with adaptive feedback control. In *Proceedings of the 13th International Conference on Cryptographic Hardware and Embedded Systems*, pages 17–32, 2011.

[12] A. Theodore Markettos and Simon W. Moore. The frequency injection attack on ring-oscillator-based TRNGs. *CHES 2009*, pages 317–330, 2009.

[13] G. Marsaglia. The Marsaglia random number CDROM including the Diehard battery of tests of randomness. October 2008.

[14] Vyas S. Patterson M. Sabotta C. Jones P. Mills, A. and J. Zambreno. Design and evaluation of a delay-based FPGA physically unclonable function. *2012 IEEE 30th Int. Conf. Computer Design (ICCD), Montreal, QC, Canada*, pages 143–146.

[15] F. Pareschi , R. Rovatti, and Gianluca Setti. On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution. *IEEE Transactions on Information Forensics and Security*, 7(2):491–502, April 2012.

[16] F. Pareschi, R. Rovatti, and Gianluca Setti. Second-level NIST randomness tests for improving test reliability. In *IEEE International Symposium on Circuits and Systems. ISCAS 2007*, pages 1437 – 1440, May 2007.

[17] A. Rodriguez-Vazques, M. Delgado, S. Espejo, and J. L. Huertas. Switched-capacitor broadband noise generator for CMOS VLSI. *Electronics Letters*, 27(21), October 1991.

[18] Andrew Rukhin, Juan Soto, and James Nechvatal. A statistical test suite for random and pseudorandom number generators for cryptographic applications. *National Institute of Standards and Technology*, (800-22), April 2010.

[19] A. Sadr and M Zolfaghari-Nejad. Weighted hamming distance for PUF performance evaluation. *Electronics Letters*, (49):1376–1378, 2013.

[20] D. Schellekens, B Preneel, and I. Verbauwhede. FPGA vendor agnostic true random number generator. In *Proc. Intl. Conf. Field Programmable Logic And Applications (FPL 2006)*. IEEE, August 2006.
[21] Martin Simka, Milos Drutarovský, Viktor Fischer, and Fayolle Jacques. Model of a true random number generator aimed at cryptographic applications. In *2006 IEEE International Symposium on Circuits and Systems. ISCAS 2006. Proceedings.*, pages 5619–5622, 2006.
[22] B. Sunar, W. J. Martin, and D. R. Stinson. A provably secure true random number generator with built-in tolerance to active attack. *IEEE Transactions on Computer-Aided Design*, 56(1):109–119, 2007.
[23] Greg Taylor and George Cox. Behind Intel's new random-number generator. *IEEE Spectrum*, September 2011.
[24] Carlos Tokunaga, David Blaauw, and Travor Mudge. True random number generator with a metastability-based quality control. *Journal of Solid-State Circuits*, 43(1):404 – 611, January 2008.
[25] Stephen H. Unger. Hazards, critical races, and metastability. *IEEE Transactions on Computers*, 44(6):754 – 768, 1995.
[26] Jose Luis Valtierra Sánchez de la Vega and Esteban Tlelo-Cuautle. Simulation of piecewise-linear one-dimensional chaotic maps by verilog-a. *IETE Technical Review*, 32(4), July 2015.
[27] I. Verbauwhede and R. Maes. Physically unclonable functions: manufacturing variability as an unclonable device identifier. *ACM Great Lakes Symp. VLSI, Lausanne, Switzerland*, pages 455–460, 2011.
[28] J. Von Neumann. Various techniques used in connection with random digits. Monte Carlo methods. *Nat. Bureau Standards*, 12:36–38, 1951.
[29] Taeill Yoo, Ju-Sung Kang, and Yongjin Yeom. Recoverable random numbers in an internet of things operating system. *Entropy*, 2017.

5. Omówienie pozostałych osiągnięć naukowo-badawczych

5.1 Pozostałe publikacje [2]

A10. Starecki Tomasz, **Wieczorek Piotr Z.**: A High Sensitivity Preamplifier for Quartz Tuning Forks in QEPAS (Quartz Enhanced PhotoAcoustic Spectroscopy) Applications, w: Sensors, vol. 17, nr 11, 2017, ss. 1-15, DOI:10.3390/s17112528
swój wkład w tę publikację oceniam na 50%, MNiSW: 30, IF: 2,677

A11. Justyna Szczygieł, **Wieczorek Piotr Z.**, Drozd-Sokołowska Joanna, Michałek Piotr, Mazurkiewicz Łukasz, Legatowicz-Koprowska Marta, Walczak Ewa, Jędrzejczak Wiesław W., Dwilewicz-Trojaczek J., Grzybowski J.: Impaired right ventricle function as predictor of early mortality in patients with light-chain cardiac amyloidosis assessed in the cardiology department, w: Polish Archives of Internal Medicine – Polskie Archiwum Medycyny Wewnętrznej, nr 127 (12), 2017, ss. 854-864, DOI:10.20452/pamw.4135
swój wkład w tę publikację oceniam na 30%, MNiSW: 30, IF: 2,191

A12. Smyk Bogdan, **Wieczorek Piotr Z.**, Zadernowski Ryszard: A method of concentration estimation of trienes, tetraenes, and pentaenes in evening primrose oil, w: European Journal of Lipid Science and Technology, vol. 113, nr 5, 2011, ss. 592-596 DOI:10.1002/ejlt.201000418
swój wkład w tę publikację oceniam na 30%, MNiSW: 27, IF: 2,162

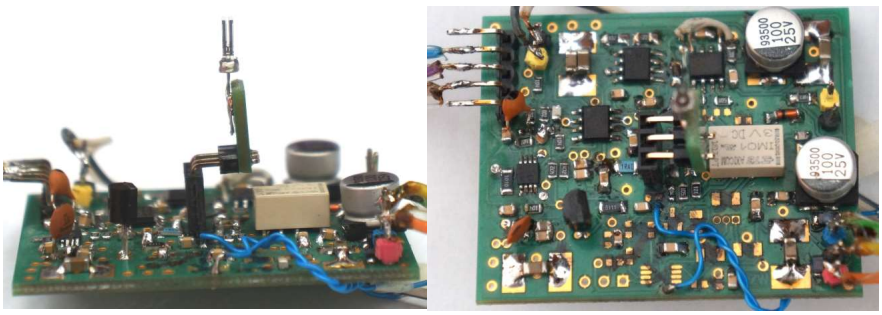
B13. Żbik Mateusz, **Wieczorek Piotr Z.**: Versatile subnanosecond laser diode driver, w: Proc. SPIE. vol.10031, 2016, SPIE ,100311F-1-100311F-9, DOI:10.1117/12.2249375
swój wkład w tę publikację oceniam na 40%, MNiSW: 15

B14. Rybaniec Radosław, **Wieczorek Piotr Z.**: Measuring and Minimizing Interrupt Latency in Linux-Based Embedded Systems, w: Proc. SPIE. vol. 8454, 2012, 84540Y-1-84540Y-6, DOI:10.1117/12.2000230
swój wkład w tę publikację oceniam na 30%, MNiSW: 15

B15. Szczygieł Justyna, Michałek Piotr, Drozd-Sokołowska Joanna, **Wieczorek Piotr Z.** [i in.]: sST-2 i GDF-15 jako nowoczesne markery kardiologiczne w amyloidozie serca z łańcuchów lekkich, w: Acta Haematologica Polonica, vol. 48, nr Supl. 1, 2017, ss. 65-66
swój wkład w tę publikację oceniam na 20%, MNiSW: 14

B16. **Wieczorek Piotr Z.**, Opalski Leszek J.: Nieliniowe modelowanie czasu rozwiązania w układach zatrzasków typu D, w: Elektronika- konstrukcje, technologie, zastosowania, SIGMANOT, nr 12, 2011, ss. 36-38
swój wkład w tę publikację oceniam na 70%, MNiSW: 6

[2] Publikacje z listy A oznaczono jako A[numer], Publikacje z listy B lub publikacje w materiałach pokonferencyjncych krajowych i zagranicznych oznaczono jako B[numer], referaty konferencyjne oznaczono jako C[numer]



Rysunek 15: Zaprojektowany i wykonany przeze mnie układ niskoszumnego wielostopniowego przedwzmacniacza fotoakustycznego. Zdjęcie wykonano w dwóch płaszczyznach w celu lepszego zobrazowania rezonatora kwarcowego (ang. 'Quartz Tuning Fork') i reszty urządzenia.

C17. Smyk Bogdan, **Wieczorek Piotr Z.**, Zadernowski R.,: Sprzężone kwasy tłuszczowe w olejach roślinnych, w Materiały: XV Jubileuszowego Ogólnopolskiego Sympozjum Spektroskopowego, Poznań „Zastosowanie metod spektroskopowych w badaniu materiałów i związków chemicznych", 2011, Str. 99
swój wkład w tę publikację oceniam na 30%

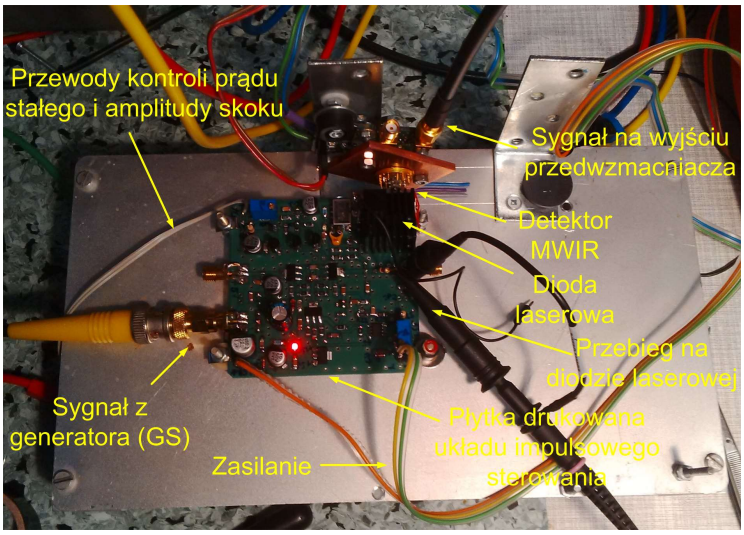
C18. Szczygieł Justyna, Michałek Piotr, Drozd-Sokołowska Joanna, **Wieczorek Piotr Z.** [i in.]: Soluble suppression of tumorigenicity 2 (sST2) and growth differentiation factor 15 (GDF-15) help to identify patients with light-chain amyloidosis in the cardiology department, w International Symposium on Amyloidosis, Japonia 2018, referat zaproszony przyjęty
swój wkład w tę publikację oceniam na 20%

W trakcie mojego zatrudnienia na Politechnice Warszawskiej aktywnie uczestniczyłem w pracach i projektach badawczych nie związanych bezpośrednio z osiągnięciem naukowym. Projekty te bazowały jednak na mojej wiedzy z dziedziny układów elektronicznych lub modelowaniu matematycznym procesów i zjawisk, którą także wykorzystywałem w osiągnięciu naukowym.

W trakcie zatrudnienia w Katedrze Fizyki i Biofizyki UWM zdobyłem podstawową wiedzę w dziedzinie technik spektroskopowych. Dzięki temu prawie dekadę później mogłem włączyć się w prace nad rozwojem techniki spektroskopowej, jaką jest fotoakustyka. W publikacji [A10] wraz z prof. Tomaszem Stareckim pokazałem, że stosowanie wzmacniaczy transimpedancyjnych w detekcji sygnału fotoakustycznego z rezonatorów kwarcowych nie jest optymalnym rozwiązaniem. W tym celu przeprowadziłem analizę szumową stosowanych w fotoakustyce typów przedwzmacniaczy, tj. transimpedancyjnych i ładunkowych i porównałem je ze wzmacniaczami napięciowymi. Ponadto przeprowadziłem badania różnych topologii wzmacniaczy w połączeniu z rezonatorami kwarcowymi w celu ekstrakcji ich parametrów teorioobwodowych. Porównanie zastępczych modeli teorioobwodowych wzmacniaczy wskazało na bezzasadność stosowania wzmacniaczy transimpedancyjnych. Skonstruowałem także (przedstawiony na rys. 15) wielostopniowy niskoszumny różnicowy wzmacniacz napięciowy i wykonałem pomiary jego parametrów elektrycznych. Zaproponowana koncepcja wykazuje lepsze właściwości szumowe od dotychczas publikowanych w literaturze.

Zaproponowana przeze mnie koncepcja przedwzmacniacza fotoakustycznego nie jest jedyną aktywnością związaną z szeroko rozumianą spektroskopią. W pracach [A12] i [C17] opisano metodę wyznaczania stężeń mieszaniny tłuszczów na podstawie widma spektroskopowego w zakresie UV-VIS. Za wyznaczanie stężeń na podstawie widm odpowiedzialny był program komputerowy, którego jestem twórcą. Program ten wykorzystywał zbiory uczące czystych związków (tłuszczów), po czym na podstawie analizy widma mieszaniny dokonywał estymaty stężeń w oparciu o regresję wielowymiarową.

Wiedza matematyczna, w tym związana z modelowaniem statystycznym, okazała się przydatna nie tylko w opisie zjawisk losowych i generacji liczb losowych. W pracach [A11], [B15] i [B18] wykorzystałem swoją wiedzę z modelowania rozkładów gęstości prawdopodobieństwa i stosowania modeli statystycznych. Byłem m.in. odpowiedzialny za analizę statystyczną wyników medycznych. Wyniki badań dotyczyły analizy śmiertelności pacjentów chorych na amyloidozę oraz wpływu parametrów biologicznych, takich jak: poziom troponiny T, peptydu NT-proBNP, wieku pacjentów czy markerów kardiologicznych, takich



Rysunek 16: System do charakteryzacji detektorów MWIR HgCdTe

jak sST-2 i GDF-15 na przeżywalność. W pracach [A11], [B15] i [B18] wskazano m.in. na ciekawą zależność wieku pacjentów oraz funkcji skurczowej serca (TAPSE, RV i EF) i śmiertelności. Wykazano także, że sST-2 i GDF-15 mogą być wartościowymi markerami w rozpoznawaniu amyloidozy serca u pacjentów z kardiomiopatią restrykcyjną.

W trakcie prac nad tzw. osiągnięciem naukowym uczestniczyłem także aktywnie w latach 2013-1015 w projekcie: „*Integracja detektorów podczerwieni chłodzonych termoelektrycznie lub pracujących w temperaturze otoczenia z szerokopasmowym układem odbiorczym*", w ramach tzw. Programu Badań Stosowanych (PBS) Narodowego Centrum Badań i Rozwoju. W projekcie brałem udział w zadaniach 2 i 4 (wspólnie z dr hab. inż. Wojciechem Wiatrem i dr hab. inż. Leszkiem Opalskim, prof. PW), które dotyczyły odpowiednio analizy toru odbiorczego detektorów podczerwieni i modelowania detektorów oraz dedykowanych przedwzmacniaczy. W celu weryfikacji pasma sygnału na wyjściu detektorów skonstruowałem układ pobudzający detektory HgCdTe skokiem jednostkowym źródła optycznego. W tym celu zbudowałem impulsowy układ sterujący laserem na zakres tzw. średniej podczerwieni (MWIR) oraz układ przedwzmacniacza transimpedancyjnego współpracujący z badanymi detektorami. Na rys. 16 zamieściłem fotografię zrealizowanego systemu składającego się z układu pobudzającego impulsem laserowym i układu przedwzmacniacza z detektorem MWIR. Prace te zaowocowały m.in publikacją [B13], kilkoma raportami badawczymi, a ich rozwój był przedmiotem jednej z prac magisterskich wykonanych pod moim kierownictwem.

Dodatkowymi działaniami związanymi z pracą naukową były publikacje [B14] i [B16]. Pierwsza z nich dotyczyła badań nad wykorzystaniem systemu Linux w systemie wbudowanym czasu rzeczywistego na potrzeby zastosowań w awionice. W pracy [B14] przeprowadzono analizę opóźnień związanych z obsługą zdarzeń w systemie Linux. Zagadnienie to było istotne ze względu na wykorzystanie systemu czasu rzeczywistego do kontroli tzw. sztucznego horyzontu w statku powietrznym. Głównym autorem rozwiązania sztucznego horyzontu do zastosowań awionicznych był mój ówczesny magistrant, Pan dr inż. Radosław Rybaniec. Publikacja [B16] dotyczyła z kolei modelowania deterministycznego zachowania zatrzasków typu D. W pracy, razem z prof. Leszkiem Opalskim zaproponowałem dokładniejsze, niż funkcjonujące w literaturze, modele opisu czasu odpowiedzi układów przerzutnikowych.

5.2 Pozostałe publikacje przed doktoratem

B19. Burd Aleksander, Wieczorek Piotr Z.: Low-cost fast ramp circuit for sampling oscilloscope, w: Proceedings of SPIE: Photonics Applications in Astronomy, Communications, Research and High Energy Physics Experiments, vol. 6159, 2006, 61592S-1-61592S-5
swój wkład w tę publikację oceniam na 20%

B20. Wieczorek Piotr Z.: Measurement system for thermal drift of propagation time in fast pulse circuits, w: Proceedings of SPIE: Photonics Applications in Astronomy, Communications, Research and High Energy Physics Experiments, vol. 6347, 2006, 63472F-1-63472F-7

B21. Wieczorek Piotr Z., Burd Aleksander: Precise low-current source for sub-nanosecond pulse measurements, w: Proceedings of SPIE: Photonics Applications in Astronomy, Communications, Research and High Energy Physics Experiments, vol. 6159, 2006, 61592V-1-61592V-7
swój wkład w tę publikację oceniam na 80%

B22. Wieczorek Piotr Z.: D-latch quasi-static macromodel in metastability optimization, w: Elektronika – konstrukcje, technologie, zastosowania, 2011, Vol. 52, nr 9, ss. 178-181

B23. Wieczorek Piotr Z., Opalski Leszek J.: Non-linear Modelling of Resolve Time in D-latch Circuits, w: MIXDES 2011 18th International Conference Mixed Design of Integrated Circuits and Systems, 2011, ISBN 978-83-932075-0-3, ss. 456-459
swój wkład w tę publikację oceniam na 70%

B24. Wieczorek Piotr Z.: Wpływ wybranych parametrów konstrukcyjnych przerzutników na kształt odpowiedzi czasowej, w: Elektronika – konstrukcje, technologie, zastosowania, vol. 8, 2009, ss. 114-119

B25. Filipkowski Andrzej, Ogrodzki Jan, Opalski Leszek J. [i in.]: Data acquisition system for ion-selective potentiometric sensors, w: Proc. SPIE. vol. 7502, 2009, SPIE, ss. 750226-1-750226-10, DOI:10.1117/12.838257
swój wkład w tę publikację oceniam na 20%

B26. Wieczorek Piotr Z., Opalski Leszek J.: An empirical of transient responses of potentiometric ion sensors, w: Proc. SPIE. vol. 7124, 2008, 71240V-1-71240V-9
swój wkład w tę publikację oceniam na 80%

B27. Wieczorek Piotr Z., Opalski Leszek J., Ogrodzki Jan: Electrical properties of potentiometric sensors: an empirical study, w: Proc. SPIE. vol. 6937, 2008, 69372K(1-8), DOI:10.1117/12.784766
swój wkład w tę publikację oceniam na 50%

B28. Wieczorek Piotr Z., Opalski Leszek J.: Statistical method of evaluation of flip-flop dynamical parameters, w: Proc. SPIE. vol. 6937, 2008, ss. 693714-1-693714-9, DOI:10.1117/12.784669
swój wkład w tę publikację oceniam na 70%

Przed rozpoczęciem studiów doktoranckich aktywnie uczestniczyłem w pracach badawczych zespołu naukowego mojego ówczesnego promotora pracy magisterskiej Pana dr inż. Aleksandra Burda. W tym czasie zajmowałem się konstrukcją szybkich analogowych układów impulsowych. W wyniku realizowanych prac powstały trzy publikacje (których jestem współautorem) związane z zagadnieniami kształtowania impulsów elektrycznych na potrzeby techniki oscyloskopowej [B19], [B21], oraz jedna dotycząca dryfu termicznego tych układów [B20]. Moje zainteresowanie układami analogowymi rozwijałem podczas studiów doktoranckich, w trakcie których, zajmowałem się modelowaniem i optymalizacją układów przerzutnikowych pod kątem niezawodności i szybkości (metastabilności). W tym czasie ukazała się seria publikacji [B22]-[B24] dotyczących tych zagadnień. W publikacji [B28] wspólnie z moim promotorem dr hab. inż. Leszkiem Opalskim, prof. PW zaproponowałem statystyczną metodę analizy parametrów układów przerzutnikowych.

W trakcie studiów doktoranckich aktywnie uczestniczyłem w grancie europejskim FP6 pt. „Water Risk Management in Europe" (WARMER). W grancie typ byłem odpowiedzialny za weryfikację parametrów elektrycznych czujników jonoselektywnych oraz konstrukcję aparatury pomiarowej. Wyniki tych prac zostały opisane w publikacjach [B25]-[B27] i raportach badawczych grantu (tzw. 'deliverables').