Autoreferat

Janusz Szmidt

8 kwietnia 2019

Posiadane dyplomy i stopnie naukowe

- **Doktorat z matematyki:** rozprawa doktowska: *"The duality theorems. Cyclic representations. Langlands conjectures"* napisana pod kierunkiem profesora Krzysztofa Maurina, obroniona w Instytucie Matematyki Polskiej Akademii Nauk w 1976 roku.
- **Magisterium z fizyki:** praca: *"Twierdzenie o wzajemności Frobeniusa dla reprezentacji indukowanych w iloczynach tensorowych modułów Hilberta"* napisana pod kierunkiem dr hab. Antoniego Wawrzyńczyka i obroniona na Wydziale Fizyki Uniwersytetu Warszawskiego w 1972 roku.

Przebieg kariery naukowej

1972 - 1976 asystent i studia doktoranckie w Instytucie Matematycznym Polskiej Akademii Nauk.
1976 - 1992 starszy wykładowca, Instytut Kształcenia Nauczycieli, Warszawa.
I-VI 1979 stypendium, Instytut Matematyki, Uniwersytet Bonn.
1986 - 1988 stypendium im. Alexandra Humboldta, Instytut Matematyki Uniwersytetu w Getyndze.
1992 - 2012 adiunkt i starszy wykładowca, Wojskowa Akademia Techniczna.
1992 - 2012 starszy wykładowca, Wyższa Szkoła Informatyki Stosowanej i Zarządzania, Warszawa.
2008 - adiunkt, Wojskowy Instytut Łączności, Zegrze Południowe.

Spis treści

1. Wskazane osiągnięcia habilitacyjne

2. Lista prac zawierających wskazane osiągnięcia
   2.1. Nieliniowe rejestry przesuwne i ciągi de Bruijna
   2.2. Kryptoanaliza funkcji skrótu
   2.3. Atak kostek i nieliniowość

3. Inne wyniki naukowe i publikacyjne uzyskane po doktoracie
   3.1. Książki
   3.2. Materiały konferencyjne i prace
   3.2.1. Nieliniowe rejestry przesuwne
   3.2.2. Atak kostek
   3.2.3. Krzywe eliptyczne
   3.2.4. Wcześniejsze prace i referaty
   3.3. Teoria liczb
   3.4. Doktorat

4. Omówienie zagadnienia

5. Szczegóły osiągnięć
   5.1. Nieliniowe rejestry przesuwne i ciągi de Bruijna
   5.2. Kryptoanaliza funkcji skrótu
   5.2.1. Kryptoanaliza funkcji GOST
   5.2.2. Kryptonaliza funkcji FSR-255
   5.3. Atak kostek i nieliniowość
   5.3.1. Kryptoanaliza szyfru Trivium
   5.3.2. Kryptoanaliza szyfru TGR

6. Wykonane recenzje

7. Działalność dydaktyczna, udział w konferencjach i seminariach

8. Udział w projektach badawczo-rozwojowych w Wojskowym Instytucie Łączności
   8.1. Krzywe eliptyczne
   8.2. Kryptografia post-kwantowa

9. Cytowania prac w Web of Sciences

10. Cytoweania w Google Scholar
    Literatura

1 Wskazane osiagnięcie habilitacyjne

Wskazanym osiągnięciem jest cykl 8 prac zatytułowany:

Wybrane zastosowania funkcji Boolowskich do generacji ciągów de Bruijna oraz kryptoanalizy algorytmów symetrycznych

2 Lista prac zawierających wskazane osiągnięcie habitacyjne

2.1 Nieliniowe rejestry przesuwne i ciągi de Bruijna

MS J. Mykkeltveit, J. Szmidt
On cross joining de Bruijn sequences.
Conference: 11th International Conference on Finite Fields and their Applications. Location: Magdeburg, GERMANY Date: JUL 22-26, 2013.
Book Series: Contemporary Mathematics, Volume: 632, pages: 335-346, 2015.
(praca cytowana w Web of Science)

DLRS P. Dąbrowski, G. Łabuzek, T. Rachwalik, J. Szmidt
Searching for Nonlinear Feedback Shift Registers with Parallel Computing.
Information Processing Letters, Volume: 114, Issue: 5, pages: 268-272, 2014.
IF: 0.748 (2016), 0.788 (5 year).
(praca cytowan w Web of Science, Scopus, Lista A, 15 ptk.)

SD J. Szmidt, P. Dąbrowski
The construction of Nonlinear Feedback Shift Registers of Small Orders.
Conference: International Conference on Military Communications and Information Systems (ICMCIS). Location: Cracow, POLAND Date: MAY 18-19, 2015.
(praca cytowana w Web of Science, Scopus)

2.2 Kryptoanaliza funkcji skrótu

MPRKS F. Mendel, N. Pramstaller, Ch. Rechberger, M. Kontak, J. Szmidt
Cryptanalysis of the Gost Hash Function. Advances in Cryptology - CRYPTO 2008, Proceedings. Book Series: Lecture Notes in Cryptology, Volume: 5157, pages: 162-178, 2008. (praca cytowana w Web of Science, Scopus, Lista A (2010), 13 pkt.)

KS1 M. Kontak, J. Szmidt
Cryptanalysis of the FSR-255 Hash Function. Control and Cybernetics, Volume: 43, Issue: 2, pages: 365-374, 2014. (praca cytowana w Scopus, Lista B, 10 pkt.)

KS2 M. Kontak, J. Szmidt
The FSR-255 Hash Function is not Second-Preimage Resistant. Conference: Military Communications and Information Systems Conference (MCC). Location: Saint Malo, FRANCE Date: OCT 07-09, 2013. (praca cytowana w Web of Science, Scopus)

2.3 Atak kostek i nieliniowość

McS P. Mroczkowski, J. Szmidt
The Cube Attack on Stream Cipher Trivium and Quadraticity Tests.
Fundamenta Informaticae, Volume: 114, Issue: 3-4, pages: 309-318, 2012.
IF: 0.687 (2016), 0.773 (5 year).
(praca cytowana w Web of Science, Scopus, Lista A, 20 ptk.)

KS3 M. Kontak, J. Szmidt
Nonlinearity of the Round Function.
Control and Cybernetics, Volume: 36, Issue: 4, pages: 1037-1044, 2007.
IF: 0.3 (2010), 0.773 (5 year).
(praca cytowana w Web of Sciences, Scopus, Lista A, 20 pkt.)

3 Inne wyniki naukowe i publikacyjne uzyskane po doktoracie

3.1 Książki

1. J. Gawinecki, J. Szmidt
Zastosowanie Ciał Skończonych i Krzywych Eliptycznych w Kryptografii.
Wojskowa Akademia Techniczna, 307 stron, Warszawa, 2002.

2. J. Szmidt, M. Misztal
Wstęp do kryptologii.
Wyższa Szkoła Informatyki Stosowanej i Zarządzania, 248 stron, Warszawa, 2002.

3.2 Materialy konferencyjne i prace

3.2.1 Nieliniowe rejestry przesuwne

1. Z. Chang, M. F. Ezerman, A. A. Fahreza, S. Ling, J. Szmidt, H. Wang
Binary de Bruijn Sequences via Zech's Logarithms
Preprint 2018, Nanyang Technological University of Singapore.

2. M. F. Ezerman, A. A. Fahreza, J. Szmidt
On Cross-Join Method for de Bruijn Sequences and Zech's Logarithms.
The 3rd International Workshop on Boolean Functions and their Applications (BFA 2018). Loen, Norway, June 17-22, 2018.

3. M. F. Ezerman, A. A. Fahreza, J. Szmidt
   Perturbations of Binary de Bruijn Sequences.
   The 3rd International Workshop on Boolean Functions and their Applications (BFA 2018). Loen, Norway, June 17-22, 2018.

4. J. Szmidt
   Nonlinear Feedback Shift Registers and Zech Logarithms.
   Preprint arXiv 1710.09556v2, 2 Nov 2017.

5. J. Mykkeltveit, J. Szmidt
   Nieliniowe rejestry przesuwne i łączenie skrzyżowanych par stanów.
   Studia Bezpieczeństwa Narodowego. Kryptologia i Cyberbezpieczeństwo.
   Rok 4, Nr 6, str. 271-281, Warszawa 2014.

6. T. Rachwalik, J. Szmidt, R. Wicik, J. Zabłocki
   Generation of Nonlinear Feedback Shift Registers with Special-Purpose Hardware. Communications and Information Systems Conference (MCC), 2012. ISBN 978-83-62954-31-5, s. 455-463 (MK-321, MK-322, MK-323).

3.2.2 Atak kostek

1. J. Szmidt
   The Cube Attack on Courtois Toy Cipher.
   Number-Theoretical Methods in Cryptology. First International Conference, NuTMiC 2017. Warsaw, Poland, 11-13, 2017. Lecture Notes in Computer Sciences, (Eds), Jerzy Kaczorowski, Josef Piprzyk, Jacek Pomykała. Volume 10737, pages 241-253, 2017.
   (praca cytowana w Web of Science, Scopus).

2. P. Mroczkowski, J. Szmidt
   The cube attack in the algebraic cryptanalysis of CTC2.
   MCC 2010: Military Communications and Information Systems Conference,
   Wrocław, 27-28.09.2010. ISBN 978-83-61486-70-1, str.339-352, 2010.

3. P. Mroczkowski, J. Szmidt
   The Algebraic Cryptanalysis of the Block Cipher Katan32 Usong Modified Cube Attack. MCC 2011: Military Communications and Information Systems Conference, Amsterdam, 17-18.10.2011. ISBN 978-83-62954-20-9, str. 346-353, 2011.

3.2.3 Krzywe eliptyczne

1. P. Dąbrowski, R. Gliwa, J. Szmidt, R. Wicik
   Generation and Implementation of Cryptographically Strong Elliptic Curves.
   Number-Theoretical Methods in Cryptology. First International Conference, NuTMiC 2017. Warsaw, Poland, 11-13, 2017. Lecture Notes in Computer Sciences, (Eds), Jerzy Kaczorowski, Josef Piprzyk, Jacek Pomykała. Volume 10737, pages 25-36. 2017.
   (praca cytowana w Web of Science, Scopus).

2. R. Gliwa, J. Szmidt, R. Wicik
   Searching for cryptographically secure elliptic curves over prime fields.
   Science and Military, 2016, nr 1, volume 11, pages 10-13, ISSN 1336-8885 (print),
   ISSN 2453-7632 (on-line).

3. P. Dąbrowski, R. Gliwa, J. Szmidt, R. Wicik
   Generacja i implementacja kryptograficznie silnych krzywych eliptycznych.
   Przegląd Telekomunikacyjny - Wiadomości Telekomunikacyjne, 2016, nr 8-9 + CD,
   str. 827-833. ISSN 1230-3496, e-ISSN 2449-7487.
   część B według wykazu MNiSW - 9 pkt.

3.2.4 Wcześniejsze prace i referaty

1. J. Szmidt, M. Misztal
   Zastosowanie szyfrów blokowych i strumieniowych do generowania bitowych ciągów
   pseudolosowych. Biuletyn WAT, Numer 3, str. 91-112, 1998.

2. J. Szmidt, J. Nowakowski
   Pseudolosowe generatory bitowe i metody badania ich losowości.
   Biuletyn WAT, Numer 3, 1998, str. 65-90.

3. M. Misztal, J. Szmidt
   Propozycje nowych algorytmów blokowych w ramach konkursu AES.
   III Krajowa Konferencja Zastosowań Kryptografii ENIGMA'99, Warszawa 13.05.1999,
   Materiały Konferencyjne, Tutorial IV, str. 49-68.

4. M. Misztal, J. Szmidt
   Kryptosystemy oparte na krzywych eliptycznych.
   III Krajowa Konferencja Zastosowań Kryptografii ENIGMA'99, Warszawa 13.05.1999,
   Materiały Konferencyjne, Tutorial IV, str. 69-76.

5. J. Szmidt
   Krzywe eliptyczne jako alternatywa dla kryptosystemu RSA.
   IV Krajowa Konferencja Zastosowań Kryptografii ENIGMA'2000, Warszawa 25.05.2000,
   Materiały Konferencyjne, Tutorial III, str. 35-49.

6. J. Szmidt
   Kryptograficzne własności funkcji Boolowskich.
   V Krajowa Konferencja Zastosowań Kryptografii ENIGMA'2001, Warszawa 15.05.2001,
   Materiały Konferencyjne, Tutorial I, str. 33-50.

7. M. Misztal, J. Szmidt
   Numerical investigation of cyclicity statistics for elliptic curves over finite fields.
   Biuletyn WAT, Volume 51, No. 4, 2002, str. 93-108.

8. M. Kontak, J. Szmidt
   Nieliniowość funkcji rundy i jej zastosowanie do kryptoanalizy liniowej funcji skrótu
   Tiger w trybie szyfrowania.

X Krajowa Konferencja Zastosowań Kryptografii ENIGMA 2006, str. 105-121, ISBN 83-918247-8-0.

9. M. Grądzki, J. Szmidt
   Atak na certyfikaty stron WWW. Wyższa Szkoła Menażerska, materiały konferencyjne, 11 stron, Warszawa, 2007.

3.3 Teoria liczb

1. J. Szmidt
   The Selberg Trace Formula for the Picard Group SL(2,Z[i]).
   Acta Arithmetica. Volume: 42, Issue: 4, pages: 391-424, 1983.
   IF: 0.522 (5 year).

2. H. Iwaniec, J. Szmidt
   Density Theorems for Exceptional Eigenvalues of the Laplacian for Congruence Groups.
   In: Elementary and Analytic Theory of Numbers. Banach Center Publications, Volume 17, 1985.

3. J. Szmidt, J. Urbanowicz, D. Zagier
   Congruences among Generalized Bernoulli Numbers.
   Acta Arithmetica, Volume: 71, Issue: 3, pages: 273-278, 1995.
   IF: 0.522 (5 year).

4. J. Szmidt.
   The Selberg Trace Formula for the Modular Group over the Ring of Integers of an Imaginary Quadratic Number Field.
   Mathematica Gettingensis, preprint 52, 1987.

5. J. Szmidt, J. Urbanowicz
   Some new Congruences for Grneralized Bernoulli Numbers of Higher Order.
   The Fields Institute for Research in Mathematical Sciences, preprint FI94-LF05, 1994.

6. J. Szmidt
   The Summation Formula for Dirichlet Series with Cubic Gauss Sums.
   Biuletym Wojskowej Akademii Technicznej, Volume 42, 1993.

7. J. Pomykała, J. Szmidt
   On the Order of Vanishing of n-th Derivatives of L-functions for Elliptic Curves.
   Biuletym Wojskowej Akademii Technicznej, Volume 42, 1993.

8. J. Szmidt
   Zastosowanie Teorii Liczb w Kryptografii.
   Biuletym Wojskowej Akademii Technicznej, Volume 45, 1995.

3.4 Doktorat

1. J. Szmidt
   The Duality Theorems. Cyclic Representations. Langlands Conjectures.
   Dissertationes Mathematicae (Rozprawy Matematyczne), Volume 168, Warszawa, 1980.

2. J. Szmidt.
   Duality Theorem for Integrable Representations and Langlands Conjecture.
   BULLETIN DE L ACADEMIE POLONAISE DES SCIENCES-SERIE DES SCIENCES MATHEMATIQUES ASTRONOMIQUES ET PHYSIQUES.
   Volume: 25, Issue: 12, pages: 1215-1219, 1977.

3. J. Szmidt
   Invariant Kernels on Locally Compact Groups and Cyclic Representations.
   BULLETIN DE L ACADEMIE POLONAISE DES SCIENCES-SERIE DES SCIENCES MATHEMATIQUES ASTRONOMIQUES ET PHYSIQUES.
   Volume: 23, Issue: 10, pages: 1073-1078, 1975.

4. J. Szmidt, A. Wawrzyńczyk
   C^{∞}-vectors and Intertwining Operators for Banach Space Representations of Lie Groups.
   BULLETIN DE L ACADEMIE POLONAISE DES SCIENCES-SERIE DES SCIENCES MATHEMATIQUES ASTRONOMIQUES ET PHYSIQUES.
   Volume: 22, Issue: 5, pages: 513-520, 1974.

5. J. Szmidt
   Frobenius Reciprocity Theorem for Representations Induced in Hilbert Module Tensor Products.
   BULLETIN DE L ACADEMIE POLONAISE DES SCIENCES-SERIE DES SCIENCES MATHEMATIQUES ASTRONOMIQUES ET PHYSIQUES.
   Volume: 21, Issue: 1, Pages: 35-39, 1972.

4 Omówienie zagadnienia

Rejestry przesuwne ze sprzężeniem zwrotnym (*FSR - Feedback Shift Registers*) służą do generacji pseudolosowych ciągów binarnych o określonym okresie. Rejestry przesuwne są elementami składowymi szyfrów strumieniowych, szyfrów blokowych i jednokierunkowych funkcji skrótu oraz mogą być zastosowane do generacji kluczy kryptograficznych. Ze względu na zastosowaną funkcję sprzężenia zwrotnego rejestry przesuwne dzielimy na liniowe (*LFSR - Linear Feedback Shift Register*) i nieliniowe (*NLFSR - Nonlinear Feedback Shift Register*). Teoria *LFSR* jest dobrze ugruntowana matematycznie [16, 17, 26]. Ciągi generowane przez *LFSR* mają dobre własności statystyczne, ale są *słabe* kryptograficznie, ponieważ dla *LFSR* rzędu n znajomość $2n$ bitów generowanych przez ten rejestr pozwala odtworzyć, stosując algorytm Berlekampa-Masseya [27], cały ciąg (znaleźć wielomian charakterystyczny rejestru). *LFSR* znalazły szerokie zastosowanie w konstrukcji szyfrów strumieniowych, ale należy je łączyć z nieliniowymi funkcjami Boolowskimi. Mimo tego opracowano szereg ataków (korelacyjne, algebraiczne) na te konstrukcje.

Teoria nieliniowych rejestrów przesuwnych jest daleka od kompletności. Ciągi generowane przez *NLFSR* rzędu n (zwane ciągami de Bruijna, jeśli są o maksymalnym okresie 2^n) mają dobre własności statystyczne, ale mają również *mocne* własności kryptograficzne (dużą złożoność liniową). Ciągi de Bruijna znalazły wiele zastosowań: w telekomunikacji, w robotyce, w genetyce, w zapamiętywaniu sekwencji słów i oparto na nich także wiele sztuczek karcianych. W zastosowaniach kryptograficznych poszukujemy *NLFSR*, które generują zmodyfikowane ciągi de Bruijna (nie zawierają stanu zerowego) o dużym okresie ($> 2^{100}$) i które reprezentowane są przez nieliniową funkcję sprzężenia zwrotnego o niskim stopniu algebraicznym (np. kwadratową).

W przeciwieństwie do teorii *LFSR* podstawowe problemy *NLFSR* nie są rozwiązane. Należą do nich podanie warunków koniecznych i dostatecznych na funkcję sprzężenia zwrotnego, aby rejestr generował ciąg o maksymalnym okresie oraz konstrukcja nieliniowych funkcji sprzężenia o podanych wyżej własnościach. Znane są jedynie pewne szczególne konstrukcje i dotyczą one generowanych ciągów o maksymalnym okresie 2^{32}. Konstrukcje dla większych okresów mają bardzo skomplikowane funkcje sprzężenia zwrotnego. Poniżej przedstawimy podstawowe fakty z teorii rejestrów przesuwnych i omówimy uzyskane wyniki w ramach wskazanych osiągnięć z rozdziału 2.

W podrozdziale 5.2 przedstawiono wyniki z kryptoanalizy funkcji skrótu. W pracy [MPRKS] przeprowadzomo teoretyczny atak na funkcję skrótu *GOST*, która jest rosyjskim standardem. Był to pierwszy publikowany atak, a praca ta była prezentowana na konferencji *CRYPTO* w Santa Barbara. Prace [KS1, KS2] dotyczą praktycznej kryptoanalizy funkcji skrótu *FSR-255* zaprojektowanej przez polskich autorów.

Podrozdział 5.3 dotyczy metod kryptoanalizy algebraicznej i kryptoanalizy liniowej algorytmów kryptografii symetrycznej. Przeprowadzono atak kostek (podrozdział 2.3, McS) na szyfr strumieniowy *Trivium*, gdzie zastosowano po raz pierwszy testy kwadratowości do znajdowania równań kwadratowych na bity klucza. Praca [KS3] dotyczy kryptoanalizy liniowej szyfru blokowego zbudowanego z funkcji skrótu *Tiger*.

5 Szczegóły osiągnięć

5.1 Nieliniowe rejestry przesuwne i ciągi de Bruijna

Niech $\mathbb{F}_2 = \{0, 1\}$ będzie ciałem binarnym, zaś $\mathbb{F}_2^n$ n-wymiarową przestrzenią wektorową nad tym ciałem. Elementami przestrzeni $\mathbb{F}_2^n$ są wektory $(a_0, \ldots, a_{n-1})$ o długości n.

Definicja 1. Ciągiem de Bruijna rzędu n nazywamy cykliczny ciąg binarny o długości 2^n, w którym każdy podciąg kolejnych elementów o długości n występuje dokładnie jeden raz.

W pracach [13, 4] wykazano, że liczba cyklicznie nierównoważnych ciągów de Bruijna rzędu n jest równa

$$B_n = 2^{2^{n-1}-n}. \tag{1}$$

Definicja 2. Zmodyfikowanym ciągiem de Bruijna rzędu n nazywamy cykliczny ciąg binarny o długości $2^n - 1$ powstały z ciągu de Bruijna rzędu n przez usunięcie jednego zera w podciągu kolejnych n zer.

Istnieje wzajemnie jednoznaczna odpowiedniość między ciągami de Bruijna rzędu n a zmodyfikowanymi ciągami de Bruijna tego samego rzędu. W kryptografii stosujemy przeważnie zmodyfikowane ciągi de Bruijna, w celu uniknięcia zerowego wektora inicjującego.

Definicja 3. Funkcją Boolowską od n zmiennych nazywamy odwzorowanie

$$f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2,$$

gdzie argumenty funkcji będziemy indeksowali $x_0, \ldots, x_{n-1}$.

Funkcje Boolowskie reprezentuje się zwykle w postaci tzw. tablicy prawdy (*truth tabke*), która jest jednowymiarową tablicą o długości 2^n uporządkowanych wartości funkcji $[f(X_0), \ldots, f(X_{2^n-1})]$, gdzie liczby X_i przebiegają kolejno przedział całkowitoliczbowy $[0, \ldots, 2^n-1]$ i brane są w reprezezentacji binarnej. Wykazuje się, że równoważną reprezentacją funkcji Boolowskiej jest tzw. *Algebraiczna Postać Normalna* (*ANF - Algebraic Normal Form*), gdzie funkcja f przedstawiona jest w postaci wielomianu od n-zmiennych Boolowskich:

$$f(x_0, x_1, \ldots, x_{n-1}) = \sum a_{i_1,\ldots,i_t} x_{i_1} \cdots x_{i_t}, \quad a_{i_1,\ldots,i_t} \in \mathbb{F}_2, \tag{2}$$

gdzie suma jest po wszystkich t-podzbiorach $\{i_1, \ldots, i_t\} \subset \{0, 1, \ldots, n-1\}$. W sumie (2) utożsamiamy potęgi $x_i^k = x_i$. Jeśli $\mathbb{F}_2[x_0, \ldots, x_{n-1}]$ jest pierścieniem wielomianów od n zmiennych Boolowskich, zaś ideał $\mathcal{I} = \{x_i^k = x_i, i = 0, \ldots, n-1,\ k \in \mathbb{N}\}$ to funkcje Boolowskie w Algebraicznej Postaci Normalnej są elementami pierścienia ilorazowego $\mathbb{F}_2[x_0, \ldots, x_{n-1}]/\mathcal{I}$.

Definicja 4. Rejestrem przesuwnym ze sprzężeniem zwrotnym rzędu n nazywamy odwzorowanie $\mathfrak{F} : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ postaci

$$\mathfrak{F} : (x_0, x_1, \ldots, x_{n-1}) \longmapsto (x_1, x_2, \ldots, x_{n-1}, f(x_0, x_1, \ldots, x_{n-1})), \tag{3}$$

gdzie funkcja sprzężenia zwrotnego f jest funkcją Boolowską od n zmiennych.

Rejestr *FSR* jest zwany *nieosobliwym*, jeśli odwzorowanie $\mathfrak{F}$ jest bijekcją przestrzeni $\mathbb{F}_2^n$. Zostało wykazane w [35, 16], że warunkiem koniecznym i dostatecznycm nieosobliwości jest następująca postać funkcji sprzężenia zwrotnego

$$f(x_0, x_1, \ldots, x_{n-1}) = x_0 + F(x_1, \ldots, x_{n-1}), \tag{4}$$

gdzie F jest funkcją Boolowską od $n-1$ zmiennych.

Konsekwencją nieosobliwości rejestru jest fakt, że odwzorowanie $\mathfrak{F}$ rozkłada przestrzeń $\mathbb{F}_2^n$ na rozłączne cykle. W przypadku, gdy mamy tylko jeden cykl, to rejestr generuje ciąg de Bruijna.

Twierdzenie 1. [16]. Niech (s_t) będzie ciągiem de Bruijna rzędu n. Istnieje wtedy funkcja Boolowska $F(x_1, \ldots, x_{n-1})$ taka, że

$$s_{t+n} = s_t + F(s_{t+1}, \ldots, s_{t+n-1}), \quad t = 0, 1, \ldots, 2^n - n - 1. \tag{5}$$

Znaczy to, że ciągi de Bruijna generowane są przez pewne rekurencje. Liczba wszystkich możliwych funkcji Boolowskich od $n-1$ zmiennych w równaniu (5) równa jest $2^{2^{n-1}}$. Porównując ze wzorem (1) na liczbę wszystkich ciągów de Bruijna rzędu n otrzymujemy, że prawdopodobieństwo losowego trafienia na funkcję Boolowską postaci (4) generującą ciąg de Bruijna jest równe 2^{-n}. Ze względu na Algebraiczną Postać Normalną funkcje Boolowskie sprzężenia zwrotnego rejestrów mogą być liniowe

$$f(x_0, x_1, \ldots, x_{n-1}) = x_0 + c_1 x_1 + \cdots + c_{n-1} x_{n-1}, \tag{6}$$

gdzie $c_1, \ldots, c_{n-1} \in \mathbb{F}_2$, lub nieliniowe, które zawierają jednomiany wyższych algebraicznych stopni.

Teoria rekurencji liniowych jest matematycznie kompletna [16, 17, 26], w szczególności wiadomo, kiedy funkcje Boolowskie (6) generują ciągi o maksymalnym okresie $2^n - 1$.

Twierdzenie 2. Rekurencja liniowa (6) generuje ciąg binarny o maksymalnym okresie wtedy i tylko wtedy gdy wielomian

$$p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + 1 \tag{7}$$

jest wielomianem pierwotnym; tzn jego pierwiastki są generatorami grupy multiplikatywnej $GF(2^n)^*$ ciała skończonego $GF(2^n)$ zbudowanego z wielomianu (7).

Oznaczmy stan nieosobliwego rejestru (3) rzędu n przez $u = (x_0, x_1, \ldots, x_{n-1})$. Stan $\widehat{u} = (\overline{x_0}, x_1, \ldots, x_{n-1})$, gdzie $\overline{x_0} = x_0 + 1$, nazywamy stanem sprzężonym do stanu u. Załóżmy, że rozpatrywane stany rejestru leżą na jednym cyklu.

Definicja 5. Dwie pary stanów sprzężonych $(u, \widehat{u}), (v, \widehat{v})$ nazywamy *skrzyżowaą parą stanów*, jeśli poszczególne stany występują w kolejności $u, v, \widehat{u}, \widehat{v}$.

W pracy [19] wykazazno, że dla ciągów generowanych prze pierwotne *LFSR* (tzw. m-ciągów) istnieją skrzyżowane pary stanów i dla rejestru rzędu n liczba takich par jest równa

$$\frac{(2^{n-1} - 1)(2^{n-1} - 2)}{6}. \tag{8}$$

Mając dany m-ciąg generowany przez kongruencję liniową f postaci (6) i skrzyżowaną parę stanów dla tego ciągu daną przez stany $u = (a_0, a_1, \ldots, a_{n-1}),\ v = (b_0, b_1, \ldots, b_{n-1})$ budujemy nieliniową funkcję sprzężenia zwrotnego

$$f_1(x_0, x_1, \ldots, x_{n-1}) = f(x_0, x_1, \ldots, x_{n-1}) +$$
$$(x_1 + a_1 + 1) \cdots (x_1 + a_{n-1} + 1) + (x_1 + b_1 + 1) \cdots (x_1 + b_{n-1} + 1),$$

która generuje zmodyfikowany ciąg de Bruijna rzędu n. Powyższą konstrukcję nazywamy operacją (lub metodą) łączenia skrzyżowanych par stanów. Operację tę można zastosować również do ciągów de Bruijna. Budowanie funkcji sprzężenia zwrotnego dla rejestrów o maksymalnym okresie poprzez operację skrzyżowanych par stanów, która jest połączeniem dwóch operacji rozłączania cykli i łączenia w jeden cykl różny od cyklu wejściowego, jest podstawową metodą budowy nowych nieliniowych rejestrów przesuwnych. Opisana jest w monografii Golomba [16] z 1967 roku oraz w pracy [19].

Możemy teraz przejść do przedstawienia własnych rezultatów. Na pierwszym miejscu umieszczę twierdzenie udowodnione w pracy (podrozdz. 2.1, MS) z J. Mykkeltveitem.

Twierdzenie 3. Niech $(u_t),\ (v_t)$ będą różnymi ciągami de Brujna rzędu n. Wtedy ciąg (v_t) może być otrzymany z ciągu (u_t) przez wielokrotne zastosowanie operacji łączenia skrzyżowanych par stanów.

Twierdzenie to prawdziwe jest również dla zmodyfikowanych ciągów de Bruijna. Bezpośrednim wnioskiem jest fakt, że wychodząc z pojedynczego ciągu (lub funkcji sprzężenia zwrotnego dla rejestru o maksymalnym okresie), możemy wygenerować wszystkie ciągi de Bruijna określonego rzędu. Twiedzenie to było zaskoczeniem wśród specjalistów. Solomon Golomb wyraził wcześniej opinię, że raczej nie ma efektywnego algorytmu, który by generował wszystkie ciągi de Bruijna danego rzędu n, ponieważ liczba tych ciągów rośnie podwójnie wykładniczo

wraz ze wzrostem n. Twierdzenie 3 dostarcza taki algorytm, ale jest on nieefektywny. Dowód Twierdzenia 3 jest dowodem *nie wprost* i na tym etapie możemy jedynie zaimplementować algorytm, który na wejściu ma m-ciąg (lub rekurencję liniową definiującą ten ciąg), znaleźć skrzyżowane pary stanów dla tego ciągu i skonstruować odpowiadające im nieliniowe ciągi de Bruijna. Następnie postępujemy podobnie ze znalezionymi nowymi ciągami. Proces ten powtarzamy, aż wygenerujemy wszystkie ciągi de Bruijna danego rzędu. Proces ten przeprowadzamy, przekształcając funkcje Boolowskie sprzężenia zwrotnego, ale można go także zrealizować, operując jedynie ciągami de Bruijna.

W dalszych badaniach (nieopublikowanych, ale prezentowanych na konferencji *Boolean Functions and their Applications 2018, Loen, Norway*) (podrozdział 3.2, $[1 \div 4]$) uzyskałem bardziej szczegółową wersję algorytmu generowania wszystkich ciągów de Bruijna określonego rzędu. Punktem wyjścia są wyniki z pracy D. Coppersmith *et al.*, [9], gdzie wyprowadzono wzór na funkcję generującą liczby ciągów de Bruijna otrzymanych w wyniku zmian w tablicy prawdy funkcji Boolowskiej sprzężenia zwrotnego dla dowolnego *LFSR*.

Niech $S(n)$ będzie zbiorem funkcji Boolowskich $\mathbb{F}_2^{n-1} \to \mathbb{F}_2$, które generują ciągi de Bruijna rzędu n. Dla funkcji $F : \mathbb{F}_2^{n-1} \to \mathbb{F}_2$ definiujemy zbiór $S(F;k)$ funkcji $g \in S(n)$ takich, że waga (liczba jedynek) tablicy prawdy funkcji $F+g$ równa jest k. Znaczy to, że liczba wejść, dla których funkcje F i g są różne równa jest k. Wprowadzamy oznaczenie $N(F;k) = |S(F;k)|$ i definiujemy funkcję generującą

$$G(F;y) = \sum_k N(F;k) y^k. \tag{9}$$

Niech funkcja liniowa $l : \mathbb{F}_2^{n-1} \to \mathbb{F}_2$ generuje m-ciąg o okresie $2^n - 1$. W pracy [9] wyprowadzono wzór

$$G(\ell;y) = \frac{1}{2^n}\left((1+y)^{2^{n-1}} - (1-y)^{2^{n-1}}\right), \tag{10}$$

z którego możemy obliczyć dokładne wartości współczynników w rozwinięciu funkcji (9), mianowicie dla nieparzystych $1 \le k \le 2^{n-1}-1$ współczynniki $N(\ell,k)$ wyrażają się wzorem

$$N(\ell,k) = \frac{1}{2^{n-1}}\binom{2^{n-1}}{k} \quad \text{dla} \quad n \ge 2, \tag{11}$$

który jest klasycznym ciągiem kombinatorycznym cytowanym na stronie `https://oeis.org/A281123`. Dla $k=3$ otrzymujemy wzór (8) na liczbę skrzyżowanych par stanów w m-ciągu rzędu n (wzór Helleseth-Kløve [19]) oraz uogólnienia tego wzoru dla nieparzystych k:

$$N(\ell; k = 2j+1 \ge 5) = \frac{1}{k!}\prod_{i=1}^{k-1}(2^{n-1} - i).$$

Stosując wzór (11), otrzymujemy liczbę wszystkich cyklicznie nierównoważnych ciągów de Bruijna rzędu n:

$$G(\ell,1) = \sum_{k=1}^{2^{n-1}-1} N(\ell,k) = \frac{1}{2^{n-1}} \underbrace{\sum_{k=1}^{2^{n-1}-1}\binom{2^{n-1}}{k}}_{:=\alpha} = 2^{2^{n-1}-n}, \tag{12}$$

gdzie $\alpha = 2^{2^{n-1}-1}$ jest sumą nieparzystych elementów w 2^{n-1} wierszu trójkąta Pascala.

W szczególnych przypadkach dla rzędu $n = 4$ wzór (12) ma postać

$$\sum_{k=1}^{7} N(\ell, k) = 1 + 7 + 7 + 1 = 2^4.$$

zaś dla rzędu $n = 5$ mamy

$$\sum_{k=1}^{15} N(\ell, k) = 1 + 35 + 273 + 715 + 715 + 273 + 35 + 1 = 2^{11}. \tag{13}$$

Powyższe rozważania są potwierdzeniem Twiedzenia 3 i pozwalają szczegółowo sformułować algorytm generacji wszystkich ciągów de Bruijna (podrozdział 3.2 [1 ÷ 4]).

Przystąpię teraz do omówienia wcześniejszych prac o nieliniowych rejestrach przesuwnych wskazanych w ramach osiągnięć. W pracy [DLRS] zajmowaliśmy się poszukiwaniem i badaniem *NLFSR*, których funkcje sprzężenia zwrotnego są kwadratowe, tzn. w Algebraicznej Postaci Normalnej występują tylko jednomiany pierwszego i drugiego stopnia. Rejestry takie rozpatrywane były w pracy [5], gdzie podano znalezione eksperymentalnie przykłady rejestrów, których funkcja sprzężenia zawiera tylko jeden składnik kwadratowy i generują pełny okres o długości $2^n - 1$ dla rzędu $n \leqslant 12$. Autorzy [5] rozpatrywali funkcje sprzężenia postaci

$$G(x_0, x_1 \ldots, x_{n-1}) = f(x_0, x_1 \ldots, x_{n-1}) + x_i + x_i x_j, \tag{14}$$

gdzie f jest funkcją liniową postaci (6) z wielomianem pierwotnym (7), zaś składnik $x_i + x_i x_j$ dla $i \neq j,\ 1 \leqslant i, j \leqslant n-1$, jest zakłóceniem (perturbacją) funkcji liniowej f. W przypadku gdy funkcje postaci (14) generują ciągi o maksymalnym okresie $2^n - 1$, autorzy [5] zaproponowali dla tych ciągów nazwę *kwadratowe m-ciągi*.

Mamy następującą interpretację procesu generowania ciągu przez funkcję sprzężenia postaci (14). Funkcja f generuje ciąg stanów rejestru o maksymalnym okresie, wyrazy postaci $x_i + x_i x_j$ są równe 1 dla stanów $(x_0, \ldots, x_i, \ldots, x_j, \ldots, x_{n-1})$, w których $x_i = 1$ i $x_j = 0$, a wtedy mamy negację elementu w tablicy prawdy funkcji G i rozłączenie pełnego cyklu na dwa podcykle. Następna negacja w tej tablicy prawdy spowoduje połączenie tych dwóch cykli lub dalsze rozłączenie na mniejsze cykle. Zatem aby otrzymać rejestr postaci (14) o maksymalnym okresie to rozłączanie i łączenie cykli musi się tak ułożyć, aby przy ostatniej negacji w tablicy prawdy otrzymać tylko jeden cykl. Możemy to zinterpretować jako istnienie odpowiedniego ciągu skrzyżowanych par stanów dla rejestru z funkcją G. Pewne warunki zostały podane w pracy [MS]. Ponadto badania eksperymentalne (podrozdz. 3.2, [1 ÷ 4]) wskazują, gdzie poszukiwać takich rejestrów w trakcie generowania wszystkich ciągów de Bruijna. Weźmy przykład rejestrów rzędu 5. Wtedy należy wykonać trzy etapy algorytmu z pracy (podrozdz. 3.2, [4]), aby otrzymać kwadratowe m-ciągi. Dla większych rzędów należy wykonać więcej etapów, aby otrzymać takie ciągi. Związane jest to z tym, że wychodząc z liniowego m-ciągu, należy dodać do jego funkcji sprzężenia odpowiednią liczbę jednomianów pochodzących od skrzyżowanych par stanów, aby była szansa redukcji składników wyższych stopni algebraicznych. Konkluzja jest taka, że wiemy, gdzie mogą być funkcje sprzężenia kwadratowych m-ciągów, ale są one głęboko ukryte i dotarcie do nich może być obliczeniowo trudne dla rejestrów wyższego rzędu.

W pracy [DLRS] przeprowadzono systematyczne poszukiwanie rejestrów z funkcjami sprzężenia postaci (14) i maksymalnym okresie z wykorzystaniem zaawansowanych technik programistycznych. Otrzymaliśmy pełną listę funkcji sprzężenia dla kwadratowych m-ciągów dla

rzędów $n \leqslant 21$ i znaleźliśmy przykłady takich rejestrów dla rzędów $22 \leqslant n \leqslant 29$, które są obecnie nieliniowymi kwadratowymi rejestrami największego rzędu znanymi w literaturze. Eksperymentalne poszukiwanie nieliniowych rejestrów o maksymalnym okresie opiera się na prostej procedurze:

Algorytm 1

1. Bierzemy funkcję sprzężenia rejestru odpowiedniej postaci.
2. Initializujemy rejestr niezerowym stanem począdkowym, np. $(1, \ldots, 1)$.
3. Generujemy kolejne stany rejestru i sprawdzamy, kiedy pojawi się stan początkowy.
4. Wtedy decydujemy, czy mamy rejestr o pełnym okresie, czy też cykl zamknął się wcześniej.

Powyższy algorytm został zaimplementowany w pracy [DLRS] dla funkcji sprzężenia postaci (14). Wtedy należy wykonać:

Algorytm 2

1. Wygenerować wszystkie wielomiany pierwotne stopnia n.
2. Dla danego wielomianu tworzymy odpowiadającą rekurencję liniową i dodajemy do niej składniki $x_i + x_i x_j$ dla $i \neq j,\ 1 \leqslant i, j \leqslant n-1$.
3. Sprawdzamy według **Algorytmu 1**, czy powyższe rekurencje kwadratowe generują ciągi o maksymalnym okresie $2^n - 1$.

Algorytmy zostały zaimplementowane w języku C. Akgorytm 2 realizowany był jako obliczenia równoległe z wykorzystaniem programu *klient-serwer*. Zbiór wielomianów pierwotnych określonego stopnia n i wagi k (liczba niezerowych współczynników wielomianu) dzielony jest na określoną liczbę podzbiorów zależną od liczby wątków w dostępnych procesorach serwera. Wtedy dla ustalonego wielomianu Algorytm 1 realizowany jest na jednym wątku. W obliczeniach wykorzystano trzy serwery o łącznej liczbie 54 wątków. Znalezienie podanego w pracy [DLRS] przykładu *NLFSR* rzędu $n = 29$ trwało około dwóch tygodni.

Podstawowym atutem w zastosowaniach kryptograficznych *NLFSR* jest ich duża złożoność liniowa. Znalezione przykłady *NLFSR* mają maksymalną złożoność liniową równą $2^n - 2$ lub zbliżoną do niej. Obliczemie złożoności liniowej wymagało zaimplementowania uogólnionego algorytmu Euklidesa dla wielomanów. Dla rzędu $n = 26$ pomiar złożoności liniowej trwał 7 dni. W pracy tej podane są jeszcze przykłady *NLFSR* z funkcjami sprzężenia o bardziej złożonej Algebraicznej Postaci Normalnej dla rzędów $n \leqslant 31$, które zostały znalezione z wykorzystaniem implementacji Algorytmu 1 w układach *FPGA* (*Field Programmable Gate Arrays*).

Implementacja Algorytmu 1 w układach *hardwarowych* została zrealizowana we wcześniejszej pracy (podrozdz. 3.2.1, [6]). W układach *FPGA* generowanie pełnego cyklu przez rejestr odbywa się w jednym takcie procesora, ale częstotliwość taktowania zegara w procesorach *FPGA* jest znacznie niższa (np. 50 MHz) niż częstotliwość taktowania w procesorach *CPU* ($2 \div 4$ GHz). W pracy (podrozdz. 3.2.1, [6]) wykorzystano urządzenia ze wcześniejszych projektów Wojskowego Instytutu Łączności wyposażone w układy *FPGA* typu *Altera EP3C80*.

Znaleziono *NLFSR* o prostej *ANF* do rzędu $n = 27$ włącznie, co wymagało pracy urządzeń przez 21 godzin dla przykładu rejestru rzędu $n = 27$.

W ostatnich latach ukazało się szereg prac [7, 8, 12, 22, 23, 24, 25], w których zajmowano się generowaniem ciągów de Bruijna, wychodząc z pewnych rekurencji liniowych określonych przez wielomiany charakterystyczne i stosując metodę łączenia cykli. Prace te są zaawansowane technicznie. W wyniku zastosowania tych metod otrzymuje się pewną proporcję ciągów de Bruijna wśród wszystkich takich ciągów określonego rzędu. Powstaje pytanie, czy rekurencje liniowe mogą wygenerować wszystkie ciągi de Bruijna danego rzędu, stosując tylko metodę łączenia cykli. Na pytanie to nie znamy odpowiedzi na drodze teoretycznej.

W pracy (podrozdz. 2.1, [SD] zajmowaliśmy się eksperymentalnym zbadaniem, czy zbiór rekurencji liniowych jest wystarczający do wygenerowania wszystkich ciągów de Bruijna określonego rzędu. Dla danej rekurencji liniowej budujemy graf przystawań (*adjacency graph*), który opisuje strukturę cykliczną ciągów generowanych przez tą rekurencję wraz z położeniem sprzężonych par stanów na poszczególnych cyklach. Drzewa rozpinające tego grafu odpowiadają funkcjom sprzężenia zwrotnego rejestrów generujących ciągi de Bruijna skonstruowane z wyjściowej rekurencji liniowej przy pomocy metody łączenia cykli. Konstrukcję tą zaimplementowano dla rzędu $n = 4$, gdzie potwierdzono, że rekurencje liniowe generują wszysztkie 16 ciągów de Bruijna. Natomiast dla rzędu $n = 5$ rekurencje liniowe nie są wystarczające do wygenerowania wszystkich $2^{11} = 2048$ możliwych nierównoważnych cyklicznie ciągów de Bruijna. Wyniki ilościowe cytowanych wyżej prac wskazują, że dla większych wartości rzędów rekurencje liniowe i metoda łączenia cykli pozwalają jedynie na skonstruowanie małej proporcji wszystkich ciągów de Bruijna danego rzędu.

W pracy (podrozdz. 3.2.1, [4]) skonstruowano *NLFSR* wysokiego rzędu (o dużym okresie) zbudowane na trójmianach pierwotnych i wykorzystując logarytmy Zecha w ciałach skończonych do znajdowania skrzyżowanych par stanów. Funkcje sprzężenia tych rejestrów mają wysoki stopień algebraiczny i nie są praktyczne w implementacji.

Dyskutowane powyżej podejście do konstruowaia ciągów de Bruijna przy pomocy *NLFSR* związane jest z zastosowaniem *NLFSR* w kryptografii jako generatorów pseudolosowych, które mogą być łatwo implementowane w softwerze i hardwerze. Zgodne to jest z podejściem przedstawionym w monografiach [16, 17]. Rozwijane są również metody kombinatoryczne generowania ciągów de Bruijna. Przegląd różnych algorytmów konstrukcji *NLFSR* i ciągów de Bruijna znajdziemy w artykule [14]. Ostatnio ukazały się prace [21, 36, 6] o zastosowaniu algorytmów *zachłannych* do generacji ciągów de Bruijna. Matody te mają ograniczone zastosowanie w kryptografii.

5.2 Kryptoanaliza funkcji skrótu

5.2.1 Kryptoanaliza funkcji GOST

Funkcja skrótu *GOST* jest szeroko stosowana w Federacji Rosyjskiej, jej specyfikacja zawarta jest w rosyjskim standardzie [40]. Jest to jedyna funkcja skrótu, która może być użyta w rosyjskim algorytmie podpisu cyfrowego [39]. Dlatego też zawarta jest w kilku *RFC* (*Request for Comments*) i zaimplementowana w różnych aplikacjach kryptograficznych (np. *openSSL*). *GOST* jest iterowaną funkcją skrótu produkującą skróty 256-bitowe. Funkcja *GOST* definiuje, poza tradycyjną strukturą iteracyjną, sumę kontrolną obliczaną po wszystkich wejściowych blokach wiadomości. Suma kontrolna jest wtedy częścią końcowego obliczania wartości skrótu.

Szyfr blokowy *GOST* [38] jest głównym elementem składowym omawianej funkcji skrótu. W dalszej części opisu będziemy stosowali nazwę *GOST* w odniesieniu do funkcji skrótu.

Przed naszą pracą (podrozdz. 2.2, [MPRKS]) należy wymienić dwa wyniki [18, 29] dotyczące kryptoanalizy *GOST*. Było to badanie drugich przeciwobrazów dla długich wiadomości i konstrukcja pseudo przeciwobrazów dla funkcji kompresji *GOST*. Praca (podrozdz. 2.2, [MPRKS]) jest pierwszym atakiem kryptoanalitycznym na kolizje funkcji *GOST*. Było moim pomysłem zajęcie się tą funkcją i wykorzystanie punktów stałych szyfru blokowego *GOST* dla specjalnych wiadomości jawnych do konstrukcji kolizji dla funkcji skrótu. Wpierw skonstruowano kolizje dla funkcji kompresji *GOST* o złożoności 2^{96} wykonań tej funkcji i wymaganej pamięci 2^{70} bajtów. Następnie korzystając z multikolizji, zbudowano kolizje dla funkcji skrótu *GOST* o tej samej złożoności czasowej i pamięciowej. Posłużyło to do skonstruowania kolizji dla sensownych wiadomości, zachowując wymagania czasowe i pamięciowe. Przypomnijmy, że złożoność znajdowania kolizji dla funkcji o 256-bitowym skrócie wynikająca z paradoksu dnia urodzin (*birthday attack*) wynosi 2^{128} wykonań funkcji skrótu. Zatem dokonano *teoretycznego złamania* funkcji *GOST*.

Dalsza część pracy zawiera atak na przeciwobraz dla funkcji *GOST*. Dla danej wartości skrótu h funkcji H, celem tego ataku jest znalezienie takiej wiadomości M, że $H(M) = h$. Dla funkcji o 256-bitowym skrócie złożoność ataku z pełnym przeszukiwaniem (ataku *brutalnego*) wynosi 2^{256} wykonań funkcji skrótu. W pracy skonstruowano atak na przeciwobraz dla funkcji *GOST* o złożoności 2^{192} wykonań funkcji kompresji i 2^{70} bajtów wymaganej panięci. Zasoby pamięci potrzebne są przy znajdowaniu punktów stałych dla szyfru blokowego *GOST*. W pracy przeprowadzono także atak na drugi przeciwobraz dla funkcji skrótu *GOST*. W ataku tym dla danej wiadomości M i jej skrótu $H(M) = h$ szukamy drugiej wiadomości $M' \neq M$ takiej, że $H(M') = h$. Złożoność ataku *brutalnego* dla funkcji *GOST* wynosi tu 2^{256} wykonań funkcji skrótu. W pracy skonstruowano atak o złożoności 2^{192} wykonań funkcji kompresji i zasobach pamięci 2^{70} bajtów.

Przedstawione trzy ataki na funkcję skrótu *GOST* mają charakter teoretyczny, ale w literaturze uważane są jako *złamanie* tej funkcji. Praca była prezentowana na prestiżonej konferencji kryptograficznej *CRYPTO* na Uniwersytecie Santa Barbara w Kalifornii w 2008 roku.

5.2.2 Kryptoanaliza funkcji FSR-255

FSR-255 jest dedykowaną funkcją skrótu o zmiennej długości skrótu, która została zaprojektowana przez T. Gajewskiego, I. Janicką-Lipską i J. Stokłosę [15, 20]. Funkcja FSR-255 w swojej budowie wykorzystuje ogólny model iteracyjnej funkcji skrótu [30]. Pomysłem autorów było zastosowanie w funkcji kompresji siedemnastu 15-bitowych nieliniowych rejestrów przesuwnych w celu uzyskania nieliniowości całej funkcji FSR-255. Z tego powodu funkcja kompresji jest odwracalna, co było podstawą przeprowadzenia ataku na przeciwobraz i na drugi przeciwobraz. W pracach (podrozdz. 2.2, [KS1, KS2]) przedstawiono ataki na funkcję skrótu FSR-255. Atak na przeciwobraz ma złożoność 2^{11} wykonań funkcji kompresji, natomiast atak na drugi przeciw-obraz ma złożoność jednego wykonania funkcji kompresji. Wynika stąd, że FSR-255 nie jest odporna na znajdowanie kolizji. Ataki te zostały zrealizowane praktycznie.

5.3 Atak kostek i nieliniowość

Atak kostek (*cube attack*) jest jedną z metod kryptoanalizy algebraicznej, w której znajdowanie tajnego klucza sprowadzamy do problemu rozwiązania pewnego układu równań algebraicznych (liniowych lub nieliniowych). Atak ten został wprowadzony przez M. Vielhabera [34], a następnie w stosowanej aktualnie postaci przez I. Dinura i A. Shamira [11]. W ataku kostek na algorytmy symetryczne (szyfry strumieniowe, szyfry blokowe lub funkcje skrótu) dany algorytm opisany jest przez uklad równań, w którym mamy zmienne jawne (tekst jawny) oraz zmienne tajne (klucz kryptograficzny). W fazie wstępnej ataku (*pre-processing*) atakujący ma dostęp do zmiennych jawnych i tajnych algorytmu, którego dokładnej budowy nie musi znać, ale ma implementację algorytmu. Wykonuje sumowanie po wybranych kostkach tekstu jawnego i otrzymane wyniki interpretuje jako funkcje Boolowskie zależne od zmiennych tajnych. Funkcji tych nie oblicza dokładnie, ale przeprowadza testy, czy są to funkcje liniowe lub nieliniowe. Metoda ta opiera się na ogólnej zasadzie, że jeśli w jakimś dużym zbiorze funkcji Boolowskich mała frakcja funkcji z tego zbioru posiada określoną własność, to z dużym prawdopodobieństwem wszystkie funkcje z tego zbioru mają tą własność. Przyjęcie specjalnych wartości dla zmiennych tajnych pozwala na obliczenie wartości współczynników w znalezionych funkcjach liniowych lub kwadratowych.

W drugiej fazie ataku (*on line*) atakujący ma dostęp do tekstu jawnego, ale klucz jest tajny i jest on celem ataku. Atakujący korzysta z postaci funkcji Boolowskich znalezionych w pierwszej fazie odpowiadających określonym kostkom. Oblicza wartości tych funkcji sumując teksty jawne po odpowiadających kostkach. W ten sposób atakujący otrzymuje układ równań na nieznane bity klucza. Rozwiązując układ znajduje pewną liczbę bitów klucza. Pozostałe bity klucza znajduje metodą przeszukiwania. W pracach [34, 11] autorzy przeprowadzili atak kostek na szyfr strumieniowy Trivium o zredukowanej liczbie rund. W pracy Vielhabera [34] atak ten miał nazwę *AIDA* (Algebraic IV Differential Attack). Dinur i Shamir nadali mu nazwę *cube attack*, co odpowiada sumowaniu po kostkach tekstu jawnego.

5.3.1 Kryptoanaliza szyfru Trivium

W pracy (podrozdz. 2.3, [McS]) przeprowadziliśmy atak kostek na szyfr strumieniowy Trivium zredukowany do 709 rund (Trivium ma 1152 rundy). Po raz pierwszy zastosowano testy kwadratowości do badania funkcji Boolowskich wynikających z sumowania po kostkach tekstu jawnego. W fazie pierwszej ataku znaleziono 41 funkcji liniowych i 22 funkcje kwadratowe. W fazie drugiej ataku przeprowadzono eksperyment, gdzie zadano 80-bitowy klucz (*tajny*) algorytmu Trivium, następnie, po obliczeniu wartości funkcji z fazy pierwszej, otrzymano układ równań liniowych i kwadratowych na bity klucza. Układ równań rozwiązano w sposób elementarny, stosując odpowiednio dobrane podstawienia zmiennych. Wynikiem było znalezienie wszystkich bitów tajnego klucza, bez potrzeby użycia metody przeszukiwania.

5.3.2 Kryptoanaliza szyfru TGR

W pracy (podrozdział 2.3, [KS3]) badano odporność na metody kryptoanalizy liniowej [28] szyfru blokowego *TGR*, który jest funkcją skrótu *Tiger* [3] rozpatrywaną w trybie szyfrowania. Głównym osiągnięciem pracy jest obliczenie *nieliniowości* (*nonlinearity*) przekształcenia Boolowskiego o 32 wejściach i 32 wyjściach. Było to wyzwaniem eksperymentalnym, ponieważ standardowe metody obliczania nieliniowości nie obejmują takich wymiarów. Do obliczeń

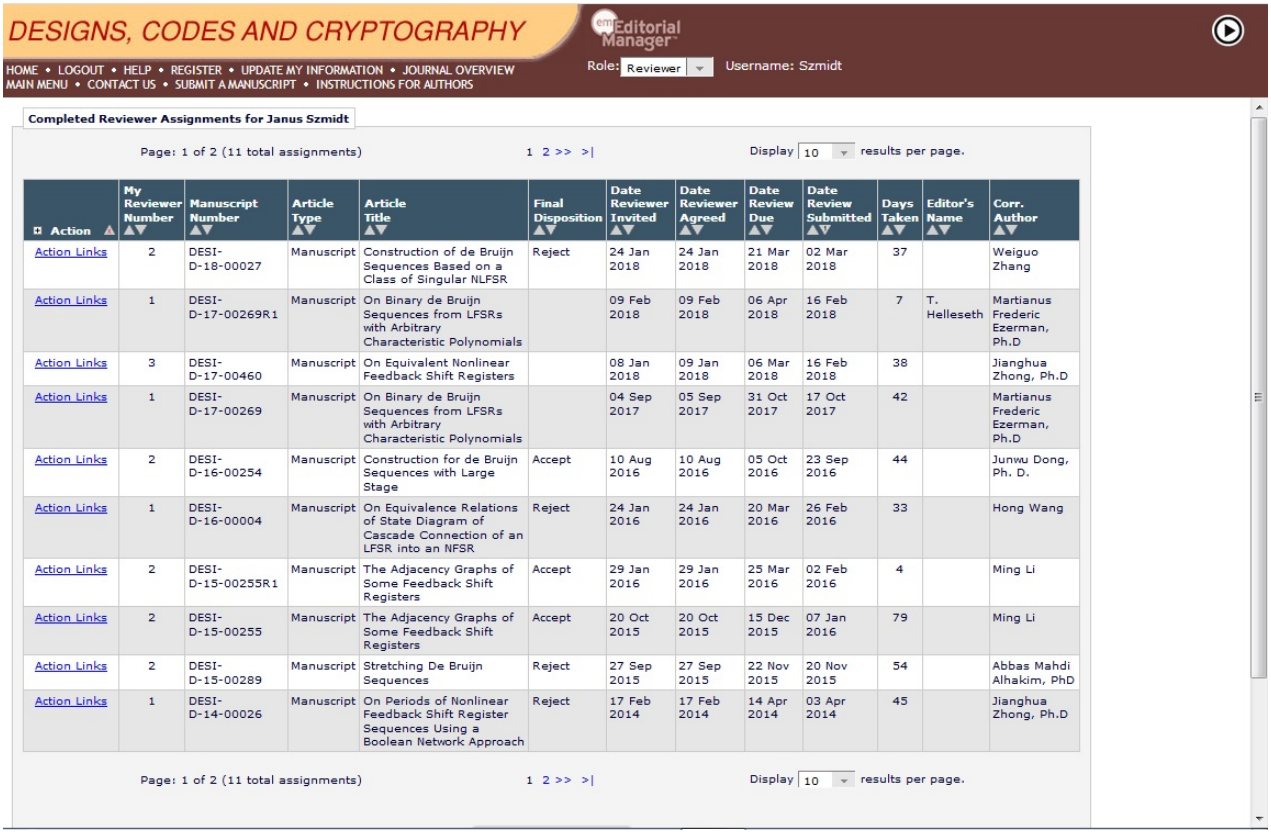
wykorzystano szczególną postać rozpatrywanych przekształceń Boolowskich i zastosowano metody transformacji ortogonalnych przedstawione w książce [1]. Przez nieliniowość funkcji Boolowskiej rozumie się jej odległość Hamminga do zbioru funkcji afinicznych. Nieliniowością przekształcenia Boolowskiego jest minimum nieliniowości funkcji Boolowskich otrzymanych jako kombinacje liniowe wszystkich wyjść tego przekształcenia.

Wielkość nieliniowości skrzynek podstawieniowych (*S-box*) odgrywa podstawową rolę w ocenie odporności szyfru blokowego, który je zawiera, na metody kryptoanalizy liniowej. W pracy (podrozdz. 2.3, [KS3]) wykazano odporność szyfru *TGR* zredukowanego do 16 rund na atak metodą kryptoanalizy liniowej wraz z ilościową oceną liczby tekstów jawnych potrzebnych do przeprowadzenia ataku.

6 Wykonane recenzje

Lista czasopism:

- Design, Codes and Cryptography - 11 recenzji
- IEEE Transations on Informatio Theory - 6 recenzji
- Cryptography and Communication - 3 recenzje
- Lecture Notes in Computer Sciences (konferencja Number-Theoretic Methods in Cryptology, Warsaw 2017)- 2 recenzje
- National coferece on Communication (India 2018) - 1 recenzja
- Przegląd Telekomunikacyjny - 1 recenzja
- Fundamenta Informaticae - 1 recenzja
- The Computer Journal (Oxford University Press) - 1 recenzja
- Transactions on Computers - 1 recenzja
- recenzja pracy doktorskiej Manish Garg : Some results of lower bounds of higher-order nonlinearities of Boolean functions, (Indian Institute of Technology, Roorkee)



DESIGNS, CODES AND CRYPTOGRAPHY

Editorial Manager

HOME • LOGOUT • HELP • REGISTER • UPDATE MY INFORMATION • JOURNAL OVERVIEW
MAIN MENU • CONTACT US • SUBMIT A MANUSCRIPT • INSTRUCTIONS FOR AUTHORS

Role: Reviewer Username: Szmidt

Completed Reviewer Assignments for Janus Szmidt

Page: 1 of 2 (11 total assignments) 1 2 >> >| Display 10 results per page.

Action	My Reviewer Number	Manuscript Number	Article Type	Article Title	Final Disposition	Date Reviewer Invited	Date Reviewer Agreed	Date Review Due	Date Review Submitted	Days Taken	Editor's Name	Corr. Author
Action Links	2	DESI-D-18-00027	Manuscript	Construction of de Bruijn Sequences Based on a Class of Singular NLFSR	Reject	24 Jan 2018	24 Jan 2018	21 Mar 2018	02 Mar 2018	37		Weiguo Zhang
Action Links	1	DESI-D-17-00269R1	Manuscript	On Binary de Bruijn Sequences from LFSRs with Arbitrary Characteristic Polynomials		09 Feb 2018	09 Feb 2018	06 Apr 2018	16 Feb 2018	7	T. Helleseth	Martianus Frederic Ezerman, Ph.D
Action Links	3	DESI-D-17-00460	Manuscript	On Equivalent Nonlinear Feedback Shift Registers		08 Jan 2018	09 Jan 2018	06 Mar 2018	16 Feb 2018	38		Jianghua Zhong, Ph.D
Action Links	1	DESI-D-17-00269	Manuscript	On Binary de Bruijn Sequences from LFSRs with Arbitrary Characteristic Polynomials		04 Sep 2017	05 Sep 2017	31 Oct 2017	17 Oct 2017	42		Martianus Frederic Ezerman, Ph.D
Action Links	2	DESI-D-16-00254	Manuscript	Construction for de Bruijn Sequences with Large Stage	Accept	10 Aug 2016	10 Aug 2016	05 Oct 2016	23 Sep 2016	44		Junwu Dong, Ph. D.
Action Links	1	DESI-D-16-00004	Manuscript	On Equivalence Relations of State Diagram of Cascade Connection of an LFSR into an NFSR	Reject	24 Jan 2016	24 Jan 2016	20 Mar 2016	26 Feb 2016	33		Hong Wang
Action Links	2	DESI-D-15-00255R1	Manuscript	The Adjacency Graphs of Some Feedback Shift Registers	Accept	29 Jan 2016	29 Jan 2016	25 Mar 2016	02 Feb 2016	4		Ming Li
Action Links	2	DESI-D-15-00255	Manuscript	The Adjacency Graphs of Some Feedback Shift Registers	Accept	20 Oct 2015	20 Oct 2015	15 Dec 2015	07 Jan 2016	79		Ming Li
Action Links	2	DESI-D-15-00289	Manuscript	Stretching De Bruijn Sequences	Reject	27 Sep 2015	27 Sep 2015	22 Nov 2015	20 Nov 2015	54		Abbas Mahdi Alhakim, PhD
Action Links	1	DESI-D-14-00026	Manuscript	On Periods of Nonlinear Feedback Shift Register Sequences Using a Boolean Network Approach	Reject	17 Feb 2014	17 Feb 2014	14 Apr 2014	03 Apr 2014	45		Jianghua Zhong, Ph.D

Page: 1 of 2 (11 total assignments) 1 2 >> >| Display 10 results per page.

Scores Returned

ACTION	COMPLETED	ID/TITLE	STATUS
Select...	17-Aug-2018	IT-18-0413 On the Number of Non-singular Feedback Shift Registers with the Certain Number of Circles	EIC: Barg, Alexander Reject (13-Oct-2018) Assignments: AE: Mesnager, Sihem ADM: Jess, Lisa
Select...	24-Feb-2017	IT-15-0728.R2 On the Affine Sub-Families of Quadratic NFSRs *Files archived*	EIC: Narayan, Prakash Accept (14-May-2017) *Archiving completed on 21-Dec-2018* Assignments: AE: Tang, Xiaohu ADM: Jess, Lisa
Select...	13-Dec-2016	IT-15-0728.R1 On the affine sub-families of Grain-128: General methods for quadratic characteristic functions *Files archived*	EIC: Kschischang, Frank Revision Required (04-Jan-2017) a revision has been submitted *Archiving completed on 21-Dec-2018* Assignments: AE: Tang, Xiaohu ADM: Jess, Lisa
Select...	19-Aug-2016	IT-16-0175.R1 The Adjacency Graphs of Linear Feedback Shift Registers with Primitive-like Characteristic Polynomials *Files archived*	EIC: Kschischang, Frank Accept (24-Oct-2016) *Archiving completed on 02-Jun-2018* Assignments: AE: Tang, Xiaohu ADM: Jess, Lisa
Select...	03-Jun-2016	IT-16-0175 The Adjacency Graphs of Linear Feedback Shift Registers with Primitive-like Characteristic Polynomials *Files archived*	EIC: Kschischang, Frank Revision Required (21-Jun-2016) a revision has been submitted *Archiving completed on 02-Jun-2018* Assignments: AE: Tang, Xiaohu ADM: Jess, Lisa
Select...	26-Jun-2014	IT-14-0473 On Periods of Nonlinear Feedback Shift Register Sequences Using a Boolean Network Approach *Files archived*	EIC: Kschischang, Frank Reject (23-Sep-2014) *Archiving completed on 30-Jan-2018* Assignments: AE: Helleseth (GE), Tor ADM: Jess, Lisa

Reviewer View Manuscripts
0 Review and Score
6 **Scores Returned**
Invitations
Legacy Instructions

7 Działaność dydaktyczna, udział w konferencjach i seminariach

W czasie pracy w latach 1992 - 2012 w Instytucie Matematyki i Kryptologii Wojskowej Akademii Technicznej byłem współtwórcą powołania specjalizacji *Kryptologia* na Wydziale Cybernetyki WAT-u. Prowadziłem szereg wykładów z różnych działów kryptologii i metod matematycznych stosowanych w tej dziedzinie. Prowadziłem także wykłady z matematyki dla I roku studiów. Kierowałem około 70 pracami dyplomowymi (prace inżynierskie, magisterskie i podyplomowe) z zakresu kryptologii i ochrony danych. Brałem udział w projektach badawczych prowadzonych w Instytucie Matematyki i Kryptologii WAT-u. W tych latach byłem także zatrudniony w Wyższej Szkole Informatyki Stosowanej i Zarządzania pod auspicjami PAN w Warszawie, gdzie prowadziłem wykłady z kryptologii i kierowałem około 30 pracami dyplomowymi. Wynikiem działaności dydaktycznej i udziału w projektach badawczych w tych latach są dwie książki (podrozdz. 3.1). Aktualnie jestem promotorem pomocniczym dwóch prac doktorskich (mgr. inż. Marcina Kontaka i mgr. inż. Przemysława Dąbrowskiego).

W czasie pracy w Wojskowej Akademii Technicznej i w Wojskowym Instytucie Łączności brałem udział w wielu konferencjach krajowych i zagranicznych z kryptologii i matematyki (ciała skończone, ciągi i ich zastosowania, funkcje Boolowskie). Wygłaszałem referaty na seminariach w tych instytucjach oraz w Instytucie Matematyki i Instytucie Podstaw Informatyki PAN, na Politechnice Warszawskiej, Politechnice Poznańskiej i Politechnice Lubelskiej, na Uniwersytecie Warszawskim, Uniwersytecie Śląskim i Uniwersytecie Poznańskim oraz w Narodowym Centrum Kryptologii. Odbyłem tygodniowe wizyty na Uniwersytetach w Magdeburgu, Bergen, Grazu, Bratysławie i Singapurze, gdzie wygłosiłem referaty. Prezentowałem swoje prace na konferencjach w Magdeburgu, Grazu i Loen (Norwegia). Byłem w komitecie programowym konferencji Number-Theoretic Methods in Cryptology (NuTMiC 2017) w Warszawie i będę w tym komitecie na konferencji NuTMiC 2019 w Paryżu. Współpracuję z Uniwersytetem w Singapurze, gdzie przygotowujemy publikację (podrozdz. 3.2.1, [1]).

8 Udział w projektach badawczo-rozwojowych w Wojskowym Instytucie Łączności

1. J. Szmidt (kierownik projektu i główny wykonawca)
   Badanie nieliniowych rejestrów przesuwnych.
   Projekt nr. 831: Badania Statutowe, Ministerstwo Obrony Narodowej, 2018.

2. J. Szmidt
   Projekt wstępny algorytmów i protokołów kryptograficznych MKp opartych o krzywe eliptyczne. Opracowanie w ramach projektu NCBiR *Guarana*, radiostacja przenośna, 21 stron, 2018. (patrz: Materiały konferencyjne i prace).

3. J. Szmidt
   Aktualny stan oceny bezpieczeństwa kryptosystemów opartych na krzywych eliptycznych z perspektywy zastosowania komputerów kwantych. Opracowanie w ramach projektu NCBiR *Guarana*, radiostacja przenośna, 32 strony, 2017.

4. J. Szmidt
   Projekt wstępny mechanizmu autoryzacji z użyciem NDK. Opracowanie niejawne w ramach projektu NCBiR *Guarana*, radiostacja przenośna, 27 stron, 2017.

5. J. Szmidt
   Postkwantowy algorytm podpisu cyfrowego oparty na algorytmach symetrycznych. Opracowanie w ramach projektu NCBiR *Guarana*, radiostacja przenośna, 34 strony, 2017.

6. J. Szmidt
   Realizacja bezpicznych operacji arytmetycznych na krzywych eliptycznych. Opracowanie w ramach projektu NCBiR *Guarana*, radiostacja przenośna, 24 strony, 2016.

7. J. Szmidt
   Projekt wstępny silnego uwierzytelnienia nośnika danych kryptograficznych z wykorzystaniem algorytmów kryptografii symetrycznej. Opracowanie niejawne w ramach projektu NCBiR *Guarana*, radiostacja przenośna, 30 stron, 2015.

8. J. Szmidt
   Analiza bezpieczeństwa krzywych eliptycznych wybranych zgodnie za standardami NATO, NIST FIPS i ANSI X.63. Opracowanie niejawne w ramach projektu NCBiR *Guarana*, radiostacja przenośna, 31 stron, 2015.

9. J. Szmidt
   Opracowanie algorytmu poszukiwania krzywych eliptycznych zgodnych ze standardami NATO. Opracowanie niejawne w ramach projektu NCBiR *Guarana*, radiostacja przenośna, 28 stro, 2015.

10. J. Szmidt
    Analiza standardowych krzywych eliptycznych stosowanych w NATO pod kątem ich efektywnej implementacji. Opracowanie niejawne w ramach projektu NCBiR *Guarana*, radiostacja przenośna; 23 strony, 2014.

8.1 Krzywe eliptyczne

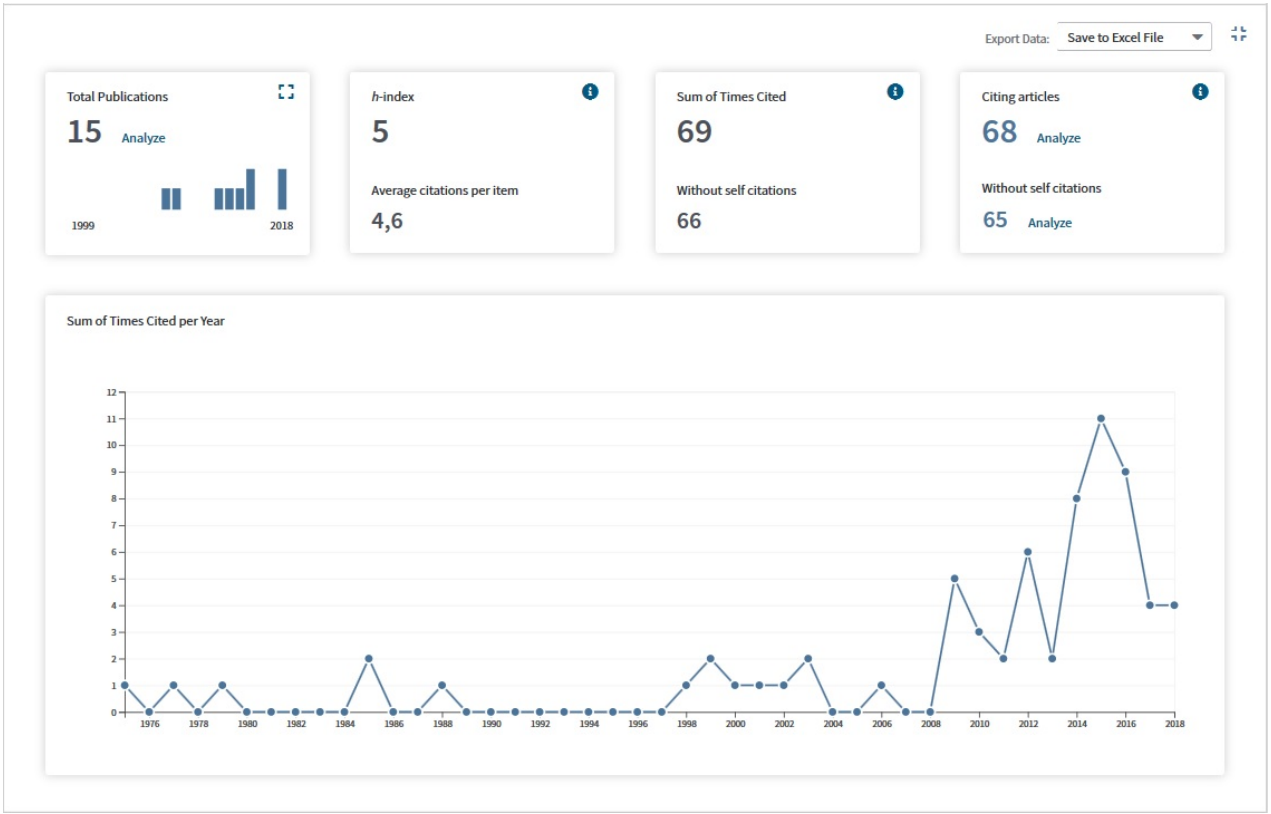
W czasie pracy w Instytucie Matematyki i Kryptologii Wojskowej Akademii Technicznej oraz w Wojskowym Instytycie Łączności zajmowałem się zastosowniem krzywych eliptycznych w kryptografii. Wynikiem są prace cytowane w (podrozdz. 3.2.3) oraz udział w projektach badawczych (rozdz. 8, projekty 2, 3, 6, 8, 9, 10). Celem tych projektów było generowanie krzywych eliptycznych nad ciałami skończonymi, które spełniają określone warunki kryptograficzne, a następnie implementacja protokołów kryptograficznych na tych krzyrych. Ostatnio wygenerowano losowe krzywe eliptyczne nad ciałem skończonym $\mathbb{F}_p$, gdzie $p = 2^{521} - 1$ jest liczbą pierwszą Mersenna, które są odporne na ataki na problem logarytmu dyskretnego na tych krzywych (projekt 2, patrz: Materiały konferencyjne i prace). Opracowane metody generacji krzywych znajdą praktyczne zastosowanie w projektowanych systemach i urządzeniach.

8.2 Kryptografia post-kwantowa

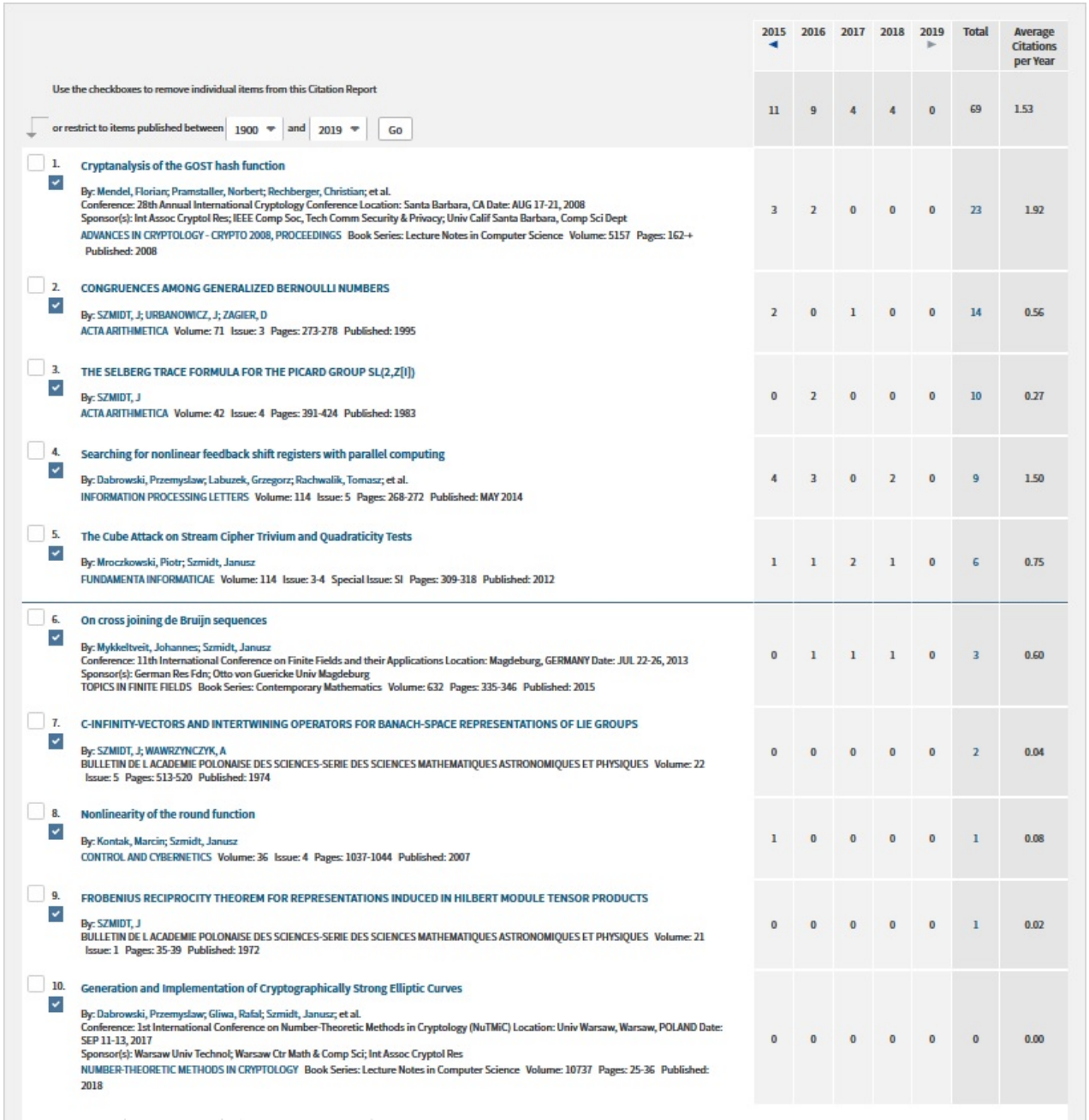
W ostatnuch latach prowadzone są intensywne prace nad budową komputerów kwantowych. W roku 1997 Peter Shor opublikował pracę [32], w której przedstawił algorytm na komputer kwantowy, który faktoryzuje liczby naturalne lub oblicza logarytmy dyskretne w ciałach skończomych i na krzywych eliptycznych ze złożonością wielomianową. W tym celu wymagane są komputery kwantowe o wielkiej skali (kilka tysięcy q-bitów, aktualnie budowane są komputery kwantowe o liczbie q-bitów mniejszej niż 100). Jeśli w przyszłości będą zbudowane komputery o wielkiej skali, to będzie to zagrożenie dla współcześnie stosowanych algorytmów klucza publicznego opartych na problemie faktoryzacji lub na problemie logarytmu dyskretnego.

Z tego względu opracowywane są aktualnie algorytmy klucza publicznego oparte na innych problemach trudnych obliczeniowo, które odporne są na ataki przyszłymi komputerami kwantowymi. Należą do nich problemy w kratach, rozwiązywanie układów równań kwadratowych w ciałach skończonych, problemy z teorii kodów korekcyjnych i inne. W Wojskowym Instytucie Łączności podjęliśmy wstępne prace nad algorytmami postkwantowymi, tzn. opartymi na problemach trudnych obliczeniowych, które odporne są na kryptoanalizę z zastosowaniem komputerów kwantowych. Prowadzę wykład dla pracowników instytutu, gdzie przedstawiane są projekty zgłoszone na konkurs NIST-u (amerykański National Institut of Standards and Technology) na kryptografię postkwantową.

9 Cytowania prac w Web of Science



h-index = 5, IF = 2,779 (pozycje 2, 3, 4, 5, 6) z listy Web of Science).
Liczba cytowań prac z osiągnięcia habilitacyjnego w Web of Science: 42).



		2015 ◄	2016	2017	2018	2019 ►	Total	Average Citations per Year
Use the checkboxes to remove individual items from this Citation Report or restrict to items published between 1900 and 2019 Go		11	9	4	4	0	69	1.53
1.	**Cryptanalysis of the GOST hash function** By: Mendel, Florian; Pramstaller, Norbert; Rechberger, Christian; et al. Conference: 28th Annual International Cryptology Conference Location: Santa Barbara, CA Date: AUG 17-21, 2008 Sponsor(s): Int Assoc Cryptol Res; IEEE Comp Soc, Tech Comm Security & Privacy; Univ Calif Santa Barbara, Comp Sci Dept ADVANCES IN CRYPTOLOGY - CRYPTO 2008, PROCEEDINGS Book Series: Lecture Notes in Computer Science Volume: 5157 Pages: 162-+ Published: 2008	3	2	0	0	0	23	1.92
2.	**CONGRUENCES AMONG GENERALIZED BERNOULLI NUMBERS** By: SZMIDT, J; URBANOWICZ, J; ZAGIER, D ACTA ARITHMETICA Volume: 71 Issue: 3 Pages: 273-278 Published: 1995	2	0	1	0	0	14	0.56
3.	**THE SELBERG TRACE FORMULA FOR THE PICARD GROUP SL(2,Z[I])** By: SZMIDT, J ACTA ARITHMETICA Volume: 42 Issue: 4 Pages: 391-424 Published: 1983	0	2	0	0	0	10	0.27
4.	**Searching for nonlinear feedback shift registers with parallel computing** By: Dabrowski, Przemyslaw; Labuzek, Grzegorz; Rachwalik, Tomasz; et al. INFORMATION PROCESSING LETTERS Volume: 114 Issue: 5 Pages: 268-272 Published: MAY 2014	4	3	0	2	0	9	1.50
5.	**The Cube Attack on Stream Cipher Trivium and Quadraticity Tests** By: Mroczkowski, Piotr; Szmidt, Janusz FUNDAMENTA INFORMATICAE Volume: 114 Issue: 3-4 Special Issue: SI Pages: 309-318 Published: 2012	1	1	2	1	0	6	0.75
6.	**On cross joining de Bruijn sequences** By: Mykkeltveit, Johannes; Szmidt, Janusz Conference: 11th International Conference on Finite Fields and their Applications Location: Magdeburg, GERMANY Date: JUL 22-26, 2013 Sponsor(s): German Res Fdn; Otto von Guericke Univ Magdeburg TOPICS IN FINITE FIELDS Book Series: Contemporary Mathematics Volume: 632 Pages: 335-346 Published: 2015	0	1	1	1	0	3	0.60
7.	**C-INFINITY-VECTORS AND INTERTWINING OPERATORS FOR BANACH-SPACE REPRESENTATIONS OF LIE GROUPS** By: SZMIDT, J; WAWRZYNCZYK, A BULLETIN DE L ACADEMIE POLONAISE DES SCIENCES-SERIE DES SCIENCES MATHEMATIQUES ASTRONOMIQUES ET PHYSIQUES Volume: 22 Issue: 5 Pages: 513-520 Published: 1974	0	0	0	0	0	2	0.04
8.	**Nonlinearity of the round function** By: Kontak, Marcin; Szmidt, Janusz CONTROL AND CYBERNETICS Volume: 36 Issue: 4 Pages: 1037-1044 Published: 2007	1	0	0	0	0	1	0.08
9.	**FROBENIUS RECIPROCITY THEOREM FOR REPRESENTATIONS INDUCED IN HILBERT MODULE TENSOR PRODUCTS** By: SZMIDT, J BULLETIN DE L ACADEMIE POLONAISE DES SCIENCES-SERIE DES SCIENCES MATHEMATIQUES ASTRONOMIQUES ET PHYSIQUES Volume: 21 Issue: 1 Pages: 35-39 Published: 1972	0	0	0	0	0	1	0.02
10.	**Generation and Implementation of Cryptographically Strong Elliptic Curves** By: Dabrowski, Przemyslaw; Gliwa, Rafal; Szmidt, Janusz; et al. Conference: 1st International Conference on Number-Theoretic Methods in Cryptology (NuTMiC) Location: Univ Warsaw, Warsaw, POLAND Date: SEP 11-13, 2017 Sponsor(s): Warsaw Univ Technol; Warsaw Ctr Math & Comp Sci; Int Assoc Cryptol Res NUMBER-THEORETIC METHODS IN CRYPTOLOGY Book Series: Lecture Notes in Computer Science Volume: 10737 Pages: 25-36 Published: 2018	0	0	0	0	0	0	0.00

11. **The Cube Attack on Courtois Toy Cipher** By: Szmidt, Janusz Conference: 1st International Conference on Number-Theoretic Methods in Cryptology (NuTMiC) Location: Univ Warsaw, Warsaw, POLAND Date: SEP 11-13, 2017 Sponsor(s): Warsaw Univ Technol; Warsaw Ctr Math & Comp Sci; Int Assoc Cryptol Res NUMBER-THEORETIC METHODS IN CRYPTOLOGY Book Series: Lecture Notes in Computer Science Volume: 10737 Pages: 241-253 Published: 2018	0	0	0	0	0	0	0.00
12. **The Construction of Nonlinear Feedback Shift Registers of Small Orders** By: Szmidt, Janusz; Dabrowski, Przemyslaw Conference: International Conference on Military Communications and Information Systems (ICMCIS) Location: Cracow, POLAND Date: MAY 18-19, 2015 2015 INTERNATIONAL CONFERENCE ON MILITARY COMMUNICATIONS AND INFORMATION SYSTEMS (ICMCIS) Published: 2015	0	0	0	0	0	0	0.00
13. **The FSR-255 Hash Function Is Not Second-Preimage Resistant** By: Kontak, Marcin; Szmidt, Janusz Conference: Military Communications and Information Systems Conference (MCC) Location: Saint Malo, FRANCE Date: OCT 07-09, 2013 2013 MILITARY COMMUNICATIONS AND INFORMATION SYSTEMS CONFERENCE (MCC) Published: 2013	0	0	0	0	0	0	0.00
14. **DUALITY THEOREM FOR INTEGRABLE REPRESENTATIONS AND LANGLAND CONJECTURES** By: SZMIDT, J BULLETIN DE L ACADEMIE POLONAISE DES SCIENCES-SERIE DES SCIENCES MATHEMATIQUES ASTRONOMIQUES ET PHYSIQUES Volume: 25 Issue: 12 Pages: 1215-1219 Published: 1977	0	0	0	0	0	0	0.00
15. **INVARIANT KERNELS ON LOCALLY COMPACT GROUPS AND CYCLIC REPRESENTATIONS** By: SZMIDT, J BULLETIN DE L ACADEMIE POLONAISE DES SCIENCES-SERIE DES SCIENCES MATHEMATIQUES ASTRONOMIQUES ET PHYSIQUES Volume: 23 Issue: 10 Pages: 1073-1078 Published: 1975	0	0	0	0	0	0	0.00

10 Cytowania w Google Scholar

h-index = 9. Liczba cytowań prac z osiągnięcia habilitacyjnego w Google Scholar : 100.

1. The Selberg trace formula for the Picard group SL (2, Z [i]) J Szmidt - Acta Arithmetica, 1983 - infona.pl Cytowane przez 26 Powiązane artykuły Wszystkie wersje 6 Web of Science: 10

2. Cryptanalysis of the Gost Hash Function
. . . , C Rechberger, M Kontak, J Szmidt - Annual International . . . , 2008 - Springer. Cytowane przez 56 Powiązane artykuły Wszystkie wersje 29

3. Zastosowanie ciał skończonych i krzywych eliptycznych w kryptografii J A Gawinecki, J Szmidt - 2002 - Wojskowa Akademia Techniczna . . . Cytowane przez 7

4. Zastosowanie ciał skończonych i krzywych eliptycznych w kryptografii G Jerzy, S Janusz - Wojskowa Akademia Tech-niczna, 1999 Cytowane przez 2

5. Congruences among generalized Bernoulli numbers J Szmidt, J Urbanowicz, D Zagier - Acta Arithmetica, 1995. Cytowane przez 26 Powiązane artykuły Wszystkie wersje 11 Web of Science: 14

6. Generation of Nonlinear Feedback Shift Registers with special-purpose hardware T Rachwalik, J Szmidt, R Wicik. . . - . . . and Information Systems . . . , 2012 - ieeexplore.ieee.org Cytowane przez 23 Powiązane artykuły Wszystkie wersje 9

7. Cube Attack on Courtois Toy Cipher. P Mroczkowski, J Szmidt - IACR Cryptology ePrint Archive, 2009 - pdfs.semanticscholar.org Cytowane przez 17 Powiązane artykuły Wszystkie wersje 7

8. The cube attack on stream cipher Trivium and quadraticity tests P Mroczkowski, J Szmidt - Fundamenta Informaticae, 2012 - content.iospress.com Cytowane przez 18 Powiązane artykuły Wszystkie wersje 11 Web of Science: 6

9. On cross joining de Bruijn sequences J Mykkeltveit, J Szmidt - Topics in Finite Fields, 2015 - books.google.com Cytowane przez 19 Powiązane artykuły Wszystkie wersje 5

10. Searching for nonlinear feedback shift registers with parallel computing . . . , G Łabuzek, T Rachwalik, J Szmidt - Information Processing . . . , 2014 - Elsevier Cytowane przez 13 Powiązane artykuły Wszystkie wersje 7 Web of Science: 9

11. The construction of nonlinear shift registers of small orders.
J Szmidt, P Dąbrowski - 2015 International Conference on . . . , 2015 - ieeexplore.ieee.org Cytowane przez 2 Powiązane artykuły Wszystkie wersje 5

12. The FSR-255 is not second-preimage resistant.
M Kontak, J Szmidt - 2013 Military Communications and . . . , 2013 - ieeexplore.ieee.org. . . Cytowane przez 1. Wszystkie wersje 2

13. Nonlinearity of the Round Function.
M Kontak, J Szmidt - Control and Cybernetics, 2007 - Citeseer Cytowane przez 1 Wszystkie wersje 13

Literatura

[1] N. Ahmed and K. R. Rao. *Orthogonal Transforms for Digital Processing*. Springer-Verlag, 1975.

[2] A. Alhakim, *Connectedness of the cross-join graph of de Bruijn sequences*. arXiv: 1805.12059v1, 30 May 2018.

[3] R. Anderson and E. Biham. *Tiger: New Hash Function*. Third International Workshop, Fast Software Encryption. LNCS 1039. Springer-Verlag, pp. 89-97, 1996.

[4] N. G. de Bruijn. *A combinatorial problem.* Indag. Math., 8(1946), pp. 461-467.

[5] A. H. Chan, R. A. Games, J. J. Rushanan. *On the Quadratic m-Sequences*. Proceedings of Fast Software Encryption, LNCS vol. 809, 1994, pp. 166-173.

[6] Z. Chang, M. F. Ezerman, A. A. Fahreza. *On Greedy Algorithms for Binary de Bruijn Sequences*. arXiv: 1902.08744v1, 23 Feb. 2019.

[7] Z. Chang, M. F. Ezerman, A. A. Fahreza, S. Ling, H. Wang. *Large Order Binary de Bruijn Sequences via Zech's Logarithms*. arXiv: 1705.03150v1 [cs.IT] 9 May 2017.

[8] Z. Chang, M. F. Ezerman, S. Ling, H. Wang. *On binary de Bruijn sequences from LFSRs with arbitrary characteristic polynomials*. Des. Codes Cryptogr. (2018). DOI. 10.1007/s10623-018-0509-y.

[9] D. Coppersmith, R. C. Rhoades, J. M. Vanderkam. *Counting de Bruijn Sequences as Perturbation of Linear Recursions.* arXiv: 1705.07835v [math.CO] 22 May 2017.

[10] N. Courtois. *How Fast can be Algebraic Attacks on Block Ciphers ?*. IACR Cryptology ePrint Archive, 2006/168.

[11] I. Dinur and A. Shamir. *Cubic Attacks on Tweakable Black Box Polynomials.* EUROCRYPT 2009. A. Joux, editor. LNCS, vol 5479, pp. 278-299. Springer 2009.

[12] J. Dong, D. Pei. *Construction for de Bruijn sequences with large stage.* Design, Codes and Cryptography, published online 1 December, 2016.

[13] C. Flye Sainte-Marie. *Solution to question nr. 48.* L'Intermédiaire des Mathématiciens, 1(1894). pp. 107-110.

[14] H. Fredricksen. *A survey of full length nonlinear shift register cycle algorithms.* SIAM Review, 24(2):195–221, 1982.

[15] T, Gajewski, I. Janicka-Lipska, J. Stokłosa. *The FSR-255 family of hash functions with a variable length of hash result.* In: J. Sołdek, L. Drobiazgiewicz, eds., Artificial Intelligence and Security in Computing Systems. Kluwer Academic Publishers, Boston, 239-248, 2003.

[16] S. W. Golomb. *Feedback Shift Registers.* San Francisco, Holden-Day, 1967, revised edition, Laguna Hills, CA, Aegean Park Press, 1982.

[17] S. Golomb, G. Gong. *Signal Design for Good Correlation. For Wirelles Communication, Cryptography, and Radar.* Cambridge University Press, 2005.

[18] P. Gauravaram and J. Kelsey. *Linear-XOR and Additive Checksums Don't Protect Damg°ard-Merkle Hashes from Generic Attacks.* In Tal Malkin, editor, CT-RSA, volume 4964 of LNCS, pages 36–51. Springer, 2008.

[19] T. Helleseth, T. Kløve. *The number of cross-join pairs in maximum length linear sequences.* IEEE Trans. on Inform. Theory, 31(1991), pp. 1731-1733.

[20] I. Janicka-Lipska, J. Stokłosa. *FSR-255 cryptographic hash function.* In: W. Burakowski, A. Wieczorek, eds. NATO Regional Conference on Military Communications and Information Systems, Zegrze 2001, vol. I, 321-324.

[21] D. E. Knuth. *The Art of Computer Programming*, Volume 4A, Combinatorial Algorithms. Addison-Wesley Professional, 2011.

[22] M. Li, Y. Jiang, D. Lin. *The adjacency graphs of some feedback shift registers.* Design, Codes and Cryptography, 82(3), 2017, pp. 695-713.

[23] C.Y. Li, X.Y. Zeng, T. Helleseth, C.L. Li and L. Hu. *The properties of a class of linear FSRs and their applications to the construction of nonlinear FSRs.* IEEE Trans. Inf. Theory, 60, no. 5, 2014, pp. 3052-3061.

[24] C.Y. Li, X.Y. Zeng, C.L. Li and T. Helleseth. A class of de Bruijn sequences. IEEE Trans. Inf. Theory, vol. 60, no. 12, 2014, pp. 7955-7969.

[25] C.Y. Li, X.Y. Zeng, C.L. Li, T. Helleseth and M. Li. *Construction of de Bruijn sequences from LFSRs with reducible characteristic polynomial.* IEEE Trans. Inf. Theory, vol. 62, no. 1, 2016, pp. 610-624.

[26] R. Lidl, H. Niederreiter. *Finite Fields.* Encyclopedia of Mathematics and its Applications 20. Cambridge Unuversity Press 1997.

[27] J.L. Massey. *Shift register synthesis and BCH decodung.* IEEE Trans. of Inf. Theory. IT-15(1), (1969), pp. 122-127.

[28] M. Matsui. *Linear Cryptanalysis Method for DES Cipher.* In: T. Helleseth, ed., Advances in Cryptology. Proceedings of Eurocrypt'93. LNCS 765. Springer-Verlag, pp. 386-397, 1994.

[29] F. Mendel, N. Pramstaller, and Ch. Rechberger. *A (Second)Preimage Attack on the GOST Hash Function.* In Kaisa Nyberg, editor, FSE, volume 5086 of LNCS, pages 224–234. Springer, 2008.

[30] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, Boca Raton, FL., 1996.

[31] J. Mykkeltveit, J. Szmidt. *On cross joining de Bruijn sequences.* Contemporary Mathematics, 2015, vol.63, pp.335-346.

[32] P. W. Shor. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J. Comput., 26(5), pp. 1484–1509, 1997.

[33] J. Szmidt, P. Dąbrowski. *The Construction of Nonlinear Feedback Shift Registers of Small Orders.* International Conference on Military Communications and Informational Systems, May 2015.

[34] M. Vielhaber. *Breaking ONE.TRIVIUM by AIDA an Algebraic IV Differential Attack.* IACR Cryptology ePrint Archive, 2007/413.

[35] E.A. Walker. *Non-linear Recurring Sequences.* Canadian J. Math., (1959) II, pp. 370-378.

[36] X. Wang, D. Wong, and W. Zhang. *A simple greedy de Bruijn sequence construction.* In SEquences and Their Applications (SETA), Hong Kong, 2018.

[37] *Workshop on Boolean Functions and their Applications*, BFA 2018, Loen, Norway.

[38] *GOST 28147-89, Systems of the Information Treatment.* Cryptographic Security. Algorithms of the Cryptographic Transformation, 1989. (In Russian).

[39] *GOST 34.10-94, Information Technology Cryptographic Data Security Produce and Check Procedures of Electronic Digital Signature Based on Asymmetric Cryptographic Algorithm*, 1994. (In Russian).

[40] *GOST 34.11-94, Information Technology Cryptographic Data Security Hashing Function*, 1994. (In Russian).

J. Szmidt