I. KONCEPCJA POLSKIEJ POLITYKI W ZAKRESIE KRYPTOLOGII I CYBERBEZPIECZEŃSTWA

NOWE WYZWANIA DLA POLSKIEJ KRYPTOLOGII DRUGIEJ DEKADY XXI WIEKU

Krzysztof Bondaryk[*], **Jacek Pomykała**[**]

[*] Narodowe Centrum Kryptologii, MON
[**] Uniwersytet Warszawski

Streszczenie. W artykule analizujemy wyzwania dla polskiej kryptologii XXI wieku ze szczególnym uwzględnieniem potrzeb narodowej kryptologii i roli, jaką spełniają w niej wybrane dziedziny matematyki, takie jak teoria liczb i geometria algebraiczna. W szczególności pokreślono rolę i bezpieczeństwo kryptosystemów bazujących na iloczynach dwuliniowych, a także problemy złożoności obliczeniowej ważnych dla kryptologii algorytmów deterministycznych. Wskazano na znaczenie funkcji typu L we współczesnej kryptografii i kryptoanalizie.

Słowa kluczowe: polska polityka kryptologiczna, bezpieczeństwo informacji, wydajność obliczeniowa i funkcjonalność kryptosystemu, kryptoanaliza i trudne problemy obliczeniowe, derandomizacja, L-funkcje, Krzywe eliptyczne, CM metoda, Liczby B-wyjątkowe, ekwipartycja mod 1, funkcje jednokierunkowe, kryptosystemy oparte na politykach dostępu, geometria algebraiczna, teoria liczb.

Nowe wyzwania dla polityki kryptologicznej w Polsce są determinowane szeregiem procesów i wydarzeń ostatnich lat, a szczególnie minionego roku. Ujawniona skala programu globalnej inwigilacji prowadzonej ostatniego roku przez służby specjalne USA, konflikt rosyjsko-ukraiński czy stale rosnąca liczba incydentów teleinformatycznych w domenie GOV.PL[1], wymuszają konieczność podjęcia przez państwo energicznych działań dla zapewnienia ochrony informacji i danych jego instytucji i obywateli. W nurt ten wpisują się intensywne działania Narodowego Centrum Kryptologii (NCK) określające potrzebę stworzenia długofalowej polityki kryptologicznej Polski (por. [1], [2]). Ponadto Polska jako członek Unii Europejskiej

[1] Jak wynika z raportu Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL, w 2013 r. odnotowano 5670 incydentów teleinformatycznych.

będzie zobowiązana do implementacji nowej dyrektywy Network & Information Security przyjętej przez Parlament Europejski w marcu 2014r. Poszerzyła ona znacząco kompetencje Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA). W rezultacie ENISA stanie się główną organizacją zwalczającą cyberprzestępczość w UE, konsolidującą wysiłki organów ścigania i jednostek działających na rzecz ochrony prywatności w państwach członkowskich. Będzie również wspierać Komisję Europejską w rozwoju współpracy między członkami UE w kwestiach bezpieczeństwa cyberprzestrzeni oraz promować standardy zarządzania i zabezpieczania informacji i danych.

Z powyższych powodów Polska stanęła przed wyzwaniem określenia fundamentów polityki kryptologicznej w zgodzie z rozwiązaniami unijnymi, przy jednoczesnym zabezpieczeniu interesów narodowych. Prace takie prowadzone są również w innych państwach unijnych. Warto przy tym zauważyć, że większość państw wysoko rozwiniętych spełnia następujące kryteria [3]:

— posiada własną politykę kryptologiczną;
— ustanowiło państwowe standardy i normy kryptograficzne;
— wymaga implementacji własnych rozwiązań kryptograficznych dla sfery cywilnej i wojskowej;
— posiada potencjał do samodzielnego zapewnienia interoperacyjności kryptologicznej w NATO i UE;
— rozwija własne zdolności kryptoanalityczne;
— posiada centrum kompetencji kryptologicznych.

Wynika z tego konieczność oparcia fundamentów polskiej polityki kryptologicznej na następującej triadzie pojęciowej (KUW):

— konsolidacji narodowych potencjałów naukowego i przemysłowego,
— unifikacji rozwiązań kryptologicznych dla sektorów strategicznych, w tym zasad certyfikacji i akredytacji;
— wymagań dotyczących zdefiniowanych norm i rozwiązań narodowych, a także przymusu "polonizacji" rozwiązań zagranicznych.

Uzyskanie pozytywnych efektów działań po zaakceptowaniu założeń KUW będzie zależało od wielu czynników, w tym: woli politycznej władz państwowych do kształtowania rynku oraz formułowania zamówień rządowych, a także konsolidacji pod auspicjami NCK, potencjału badawczego ośrodków naukowych kraju w dziedzinie kryptologii.

W dniach 5–6 czerwca 2014 roku odbyła się na Wydziale Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego konferencja naukowa nt. *Kryptografia i bezpieczeństwo informacji*[2], pod patronatem honorowym

[2] kbi2014.mimuw.edu.pl

Uniwersytetu Warszawskiego, Narodowego Centrum Kryptologii oraz Narodowego Centrum Badań i Rozwoju. Stanowiła ona okazję do spotkania i wymiany poglądów przedstawicieli środowisk naukowo-badawczych, administracji publicznej i przemysłu w zakresie bezpieczeństwa teleinformatycznego. Konferencja dotyczyła współczesnych badań naukowych w dziedzinie kryptologii prowadzonych przez różne ośrodki badawcze w kraju, szeroko rozumianego problemu bezpieczeństwa informacji oraz rozwiązań praktycznych w dziedzinie walki z cyberprzestępczością [4], [5]. Tak szerokie postrzeganie znaczenia kryptologii w dziedzinie bezpieczeństwa cyberprzestrzeni i ochrony informacji staje się obecnie normą na świecie. Z tego względu, stopień zabezpieczenia państwowej infrastruktury teleinformatycznej przed atakami cybernetycznymi powinien być istotnym, ale nie jedynym czynnikiem związanym z rozwojem polskiej kryptologii w najbliższych latach. Jej rozwój powinien służyć zarówno siłom zbrojnym, służbom specjalnym, policji i strukturom antyterrorystycznym, jak i sektorom gospodarki o znaczeniu strategicznym, administracji publicznej oraz polskim obywatelom.

Konsensus osiągnięty podczas konferencji wobec takiego wielostronnego rozumienia kryptologii wydaje się stanowić zaledwie pierwszy krok uczyniony w kierunku rzeczywistej konsolidacji polskich środowisk naukowych, przemysłowych i administracji publicznej w celu rozbudowy realnych środków bezpieczeństwa informacji i danych w państwie.

Kolejnym, być może drobnym ale potrzebnym krokiem, mogłoby się stać stworzenie, funkcjonującej pod auspicjami NCK, platformy dyskusyjnej o narodowej kryptologii, która umożliwiałaby wymianę poglądów przedstawicieli polskiej nauki, przemysłu oraz rządu i administracji. Takie przedsięwzięcie miałoby przede wszystkim na celu ułatwienie współpracy pomiędzy władzami a ośrodkami badawczymi i przedsiębiorstwami oraz konsolidację i ukierunkowywanie wspólnych wysiłków na rzecz budowy polskiej kryptologii. Problemem polskiej kryptologii pozostaje bowiem to, że ze względu na długotrwały brak zainteresowania państwa budową narodowych rozwiązań kryptologicznych, badania w tej dziedzinie przyjęły charakter prac ściśle teoretycznych. Spowodowało to również rozluźnienie więzów między ośrodkami badawczymi a krajowym przemysłem związanym z kryptografią, zmagającym się z problemem braku zamówień rządowych na swoje produkty. Z kolei administracja publiczna, nie mając często wiedzy o rozwiązaniach krajowych, preferuje pozyskiwanie gotowych produktów zagranicznych, nie dbając przy tym zwykle o zabezpieczenie interesów narodowych poprzez uzyskanie praw do ich modyfikacji, „polonizacji" i in.

Ważnym przedsięwzięciem wspierającym przedstawioną powyżej inicjatywę jest powstanie czasopisma naukowego poświęconego kryptologii, prezentującego poglądy i prace naukowo-badawcze oraz produkty polskiego przemysłu.

Warto przy tej okazji zadać pytanie o kompetencje środowisk naukowych w Polsce w zakresie kryptologii i bezpieczeństwa informacji. Wiele krajowych uczelni zarówno cywilnych jak i wojskowych posiada w swych programach nauczania odpowiednie przedmioty (wykłady, seminaria, laboratoria)
z dziedziny kryptologii i bezpieczeństwa cybernetycznego. Problematyka kryptologiczna jest również dyskutowana podczas licznych, regularnie przeprowadzanych konferencjach naukowych, zarówno krajowych, jak i międzynarodowych[3].

Materiały z jednej z takich konferencji, zorganizowanej przez Wydział Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego i objętej patronatem przez NCK, stanowią treść niniejszego numeru czasopisma. Ich lektura pozwala udzielić na zadane powyżej pytanie ostrożnie optymistycznej odpowiedzi. Jest bowiem tak, że przynajmniej w obszarze badań podstawowych w matematyce polskie ośrodki naukowe mają osiągnięcia, które zarówno ze względu na ich poziom jak i zakres, pozwalają z nadzieją patrzeć na przyszłość polskiej kryptologii.

Dbając o kontynuację i rozwój tego kierunku badań podstawowych, stanowiących przecież fundament dla nowoczesnych rozwiązań z zakresu kryptografii oraz kryptoanalizy, trzeba jednak upomnieć się również o zacieśnienie więzów między ośrodkami naukowymi, krajowym przemysłem oraz administracją publiczną, a także zadbać o harmonijny rozwój badań kryptologicznych o charakterze technicznym, stosowanym, które zaowocowałyby równie wartościowymi pracami jak te, o których przeczytać można w niniejszym numerze czasopisma.

Istotnym rezultatem przeprowadzonej konferencji jest podkreślenie wiodącej roli matematyki w zapewnianiu bezpieczeństwa informacji. Matematyka daje możliwości ścisłego zdefiniowania paradygmatów bezpieczeństwa informacji przy użyciu języka algorytmiki i pojęć modelowania matematycznego. Ponadto podstawą bezpieczeństwa wielu systemów kryptograficznych są głębokie problemy badawcze takich dziedzin matematyki jak teoria liczb czy geometria algebraiczna. Prowadzone w tych obszarach badania podstawowe na ogół wyprzedzają

[3] Między innymi Central European Conference on Cryptology, ENIGMA, Cryptography and Security Systems Conference, Advanced Computer Systems, Międzynarodowa Konferencja Naukowa z tytułu rocznicy złamania Enigmy, Cyberprzestępczość i Ochrona Informacji i KBI2014.

o wiele lat ich zastosowania praktyczne. W celu skrócenia tego dystansu niezbędna jest ścisła współpraca matematyków i informatyków.

Znaczenie metod teorii liczb i geometrii algebraicznej w kryptologii

Ostatnie lata pokazują coraz to donioślejszą rolę teorii liczb i geometrii algebraicznej w dziedzinie kryptologii. Choć metody teorii krzywych eliptycznych nad ciałami skończonymi są przedmiotem badań kryptologicznych już od lat osiemdziesiątych ubiegłego stulecia, pojawiają się coraz to nowe problemy teoretyczne i obliczeniowe z nimi związane. Kryptosystemy eliptyczne i hipereliptyczne są niezwykle interesujące przynajmniej z dwu zasadniczych powodów. Po pierwsze ich złożoność obliczeniowa jest lepsza od analogicznych kryptosystemów opartych na tradycyjnej arytmetyce modularnej. To pozwala na taką implementację systemu, w której podobny poziom bezpieczeństwa jest zagwarantowany przez stosowanie znacznie krótszych kluczy kryptograficznych. Po drugie arytmetyka na krzywej eliptycznej pozwala na wykorzystanie (dzięki efektywnej konstrukcji iloczynów dwuliniowych) odpowiedniej struktury do uzyskania dodatkowych funkcjonalności systemów kryptograficznych. Przykładem jest wykorzystanie iloczynu dwuliniowego do ustanowienia klucza tajnego dzielonego przez trzy podmioty [6], (por. [7]) lub do stworzenia systemu szyfrowania asymetrycznego opartego na tożsamości [8]. Warto dodać, że te innowacyjne idee przyczyniły się do projektowania i upowszechnienia nie tylko kryptosystemów bazujących na tożsamości [9], lecz także kryptosystemów bezcertyfikatowych (patrz np. [10], [11]). Ten nurt znalazł w szczególności szerokie zastosowanie w kryptografii grupowej opartej na protokołach współdzielenia sekretu [12], [13], kryptosystemach bazujących na politykach dostępu [14], [15], a także systemach wzmacniania prywatności [16], [17], i bezpieczeństwa informacji klasyfikowanej bazujących na modelu ORCON [18].

Z drugiej strony warto podkreślić nową ideę kryptografii opartej na torusie [19] (ang. torus based cyptography). Przypomnijmy, że torus algebraiczny jest rozmaitością algebraiczną, która nad pewnym rozszerzeniem ciała podstawowego F_p jest produktem kartezjańskim określonej liczby kopii multyplikatywnej grupy modularnej G_m. Jest to więc uogólnienie grupy modularnej z działaniem zadanym przez funkcje wymierne, co pozwala w wielu przypadkach zmniejszyć złożoność działania mnożenia w grupie F_q^*, gdzie q jest potęgą liczby pierwszej p. Inaczej mówiąc można zredukо-

wać działanie mnożenia w grupie F_q^* do działania mnożenia w F_p^* osiągając przy tym istotną korzyść obliczeniową.

W tym kontekście szczególnego znaczenia nabierają badania dotyczące wydajności obliczeniowej generowania i funkcjonowania odpowiednich systemów kryptograficznych (por. [20], [21]). Rozwiązania derandomizacji ważnych algorytmów kryptograficznych zostały zaproponowane w [22], [23], [48]. Inny problem polega na zaprojektowaniu bezpiecznych i możliwie wydajnych obliczeniowo algorytmów i protokołów kryptograficznych. Takie protokoły mają na ogół naturę algebraiczną i są związane z trudnymi problemami obliczeniowej teorii liczb. Zwykle generowanie parametrów takich systemów sprowadza się do wyznaczenia pary liczb pierwszych (p, q) związanych z charakterystyką rozważanego ciała oraz rzędem i generatorem odpowiedniej podgrupy multyplikatywnej, w której problem logarytmu dyskretnego jest obliczeniowo trudny.

W przypadku klasycznego protokołu ElGamala [24] jest to para odpowiednio dużych liczb pierwszych (p, q) spełniających warunek podzielności $q|p-1$ oraz element g rzędu q w grupie Z_p^*. W przypadku protokołów wykorzystujących krzywe eliptyczne nad ciałem skończonym szukamy krzywej eliptycznej parametryzowanej liczbami (a, b) zadanej równaniem Weierstrassa $E: y^2 = x^3 + ax + b$. W celu znalezienia odpowiedniej krzywej, tradycyjnie wykorzystuje się teorię mnożenia zespolonego (ang. CM method) otrzymując nieoczekiwanie dobrą złożoność heurystyczną odpowiednich algorytmów [25], [26]. Dalsze ciekawe wnioski wypływają z uogólnienia metody Cocksa-Pincha dla p-f (ang. pairing friendly) krzywych supereliptycznych mających genus równy 4 [27].

Zauważmy, że w przypadku systemów bazujących na arytmetyce krzywych eliptycznych metoda mnożenia zespolonego redukuje problem do znalezienia odpowiedniej krzywej E zadanej równaniem Weierstrassa w klasie krzywych o wyróżniku $\Delta < 0$ przy założeniu, że istnieje odpowiednia para liczb pierwszych (p, q) spełniających warunki:

$$q|p + 1 - t \tag{1}$$

$$4p - t^2 = -\Delta f^2 \tag{2}$$

gdzie t jest śladem poszukiwanej krzywej E.

Co więcej rozważając odpowiednią krzywą nad ciałem $l = p^n$-elementowym można wykorzystać wzór Weila w celu wyznaczenia liczby punktów wymiernych krzywej E nad tym ciałem. Z drugiej strony w badaniu kryptosystemów z iloczynem dwuliniowym, kluczowym pojęciem jest stopnień zanurzenia k krzywej E/F_p (nad ciałem F_p) względem q, gdzie q

jest liczbą pierwszą dzielącą rząd E/F_p, będący z definicji rzędem p modulo q tj. minimalnym k spełniającym spełniającym podzielność:

$$q|p^k - 1 \tag{3}$$

Jeśli $q > k$ to to powyższy warunek jest równoważny podzielności (patrz np. Lemat 2.4 pracy [28]):

$$q|\phi_k(p) \tag{4}$$

gdzie $\phi_k(x)$ jest k-tym wielomianem cyklotomicznym. Krzywe eliptyczne, które posiadają podgrupy dużego rzędu będącego liczbą pierwszą z odpowiednio małym stopniem zanurzenia są zwane powszechnie p-f krzywymi i odgrywają kluczowa rolę w kryptografii opartej na tożsamości i kryptosystemach bazujących na polityce dostępu. Dlatego celowe są badania dotyczące efektywnego znajdowania liczb pierwszych p i q spełniających warunki typu (3) lub (4) [29]. Jednym ze stosowanych w praktyce podejść jest ustalenie najpierw odpowiednio wielkiej liczby pierwszej q a następnie poszukiwanie p jako rozwiązania kongruencji $\phi_k(x) = 0(\mathrm{mod}\, q)$. Liczbę pierwszą p leżącą w odpowiedniej klasie reszt znajdujemy wtedy deterministycznie i efektywnie obliczeniowo o ile najmniejsza liczba pierwsza w zadanym postępie $\mathrm{mod}\, q$ jest relatywnie mała. Tu z pomocą przychodzi analityczna teoria liczb i w szczególności metoda wielkiego sita, która odgrywa istotną rolę w badaniu rozmieszczenia zer odpowiednich L-funkcji Dirichleta w pobliżu prostej $\mathrm{Re}\, s = 1$ [30], [31].

Wracając do kryptosystemów eliptycznych, z twierdzenia Hassego wynika, że wyróżnik Δ krzywej E, spełniający równanie $\Delta f^2 = t^2 - 4p$ jest ujemny wtedy i tylko wtedy gdy $\Delta f^2 = (N + 1 - p)^2 - 4N < 0$ (gdzie N jest rzędem krzywej E/F_p). Zatem mamy tu do czynienia z problemem przedstawialności liczby m postaci $m = 4p$ lub $m = 4N$ przez formę kwadratową $x^2 + \Delta y^2$, gdzie ($-\Delta$ jest wyróżnikiem krzywej E). Co więcej y jest tu zmienną regularną podczas gdy regularność (nieregularność) zmiennej x odpowiada nieregularności (regularności) parametru m. Rozmieszczenie rozwiązań odpowiedniej kongruencji $x^2 + \Delta y^2 = 0 \mod m$ z nieregularną zmienną x prowadzi do badania sum trygonometrycznych typu Kloostermana (por. [32]). Do ich szacowania wykorzystuje się teorię form modularnych i stowarzyszonych z nimi L-funkcji. Warto zauważyć, że sumy trygonometryczne w sposób naturalny pojawiają się przy badaniu ekwipartycji ($\mathrm{mod}\, 1$) w sensie Weyla (por. [33]) ale także przy badaniu ekstraktorów losowości [34], [35], [36]. Teoria funkcji typu L stanowi jednak bezpośrednie wyzwanie dla współczesnej kryptografii na co wskazała

już praca [37], w której zaproponowano nowy typ funkcji jednokierunkowej zadanej przez ciąg wartości symbolu Kroneckera dla modułu d (charakteru rzeczywistego modulo $4d$). Kontynuując tę ideę zaproponowano w [33] jej uogólnienie dla szerokiej klasy Selberga funkcji typu L. Szczególnie interesujące z obliczeniowego punktu widzenia są funkcje L wymiernych krzywych eliptycznych, których współczynniki $a_E(n)$ mogą być obliczone za pomocą wielomianowego algorytmu Schoofa. To ma ważną konsekwencję, a mianowicie jeśli $E\colon y^2 = x^3 + ax + b$ i (a, b) potraktować jako ziarno to ciąg binarny $(a_E(p_1) \bmod 2, a_E(p_2) \bmod 2, \ldots)$ zadaje eliptyczny generator pseudolosowy o dobrych własnościach kryptograficznych (patrz [33]) dla ciągu kolejnych liczb pierwszych $p_1 < p_2 < p_3 < \ldots$. Z drugiej strony zachowanie L-funkcji krzywych eliptycznych w punkcie symetrii równania funkcyjnego dla zadanej ich rodziny jest ze względu na głęboką hipotezę Bircha i Swinnertona-Dyera [38] związane z ich średnią jej rangą. W tym kierunku stosowne badania dla szerokiej klasy funkcji typu L przeprowadzono w pracach [39], [40].

Klasyczne L-funkcje Dirichleta pojawiają się także w kryptologii w związku z wydajnością obliczeniową kryptosystemów asymetrycznych, a także redukcją problemu faktoryzacji do problemu logarytmu dyskretnego w grupie Z_n^*. Kluczowe znaczenie odgrywa tu pojęcie B-wykładnika (tj. wykładnika podgrupy Z_n^* generowanej przez liczby nie przekraczające B). Dla liczb pierwszych n problem znajdowania małego generatora Z_n^* (por. [41]), jest do dziś przedmiotem intensywnych badań dotyczących gęstości liczb pierwszych o zadanym najmniejszym pierwiastku pierwotnym (patrz [42]). Liczby naturalne n, których redukcje modulo liczby pierwsze p, $(p|n)$ mają B-wykładniki odległe od $p-1$ (w sensie multyplikatywnym) o co najmniej d nazywamy (B, d)-wyjątkowymi. W pracy [31] udowodniono ich górne ograniczenie jako funkcji B i d wykorzystując najlepsze znane twierdzenia gęstościowe dla zer odpowiednich L-funkcji Dirichleta. Liczby te okazują się też mieć kluczowe znaczenie dla badania deterministycznej redukcji problemu faktoryzacji do obliczania wartości funkcji Eulera $\varphi(n)$ (por. [43]). Z drugiej strony liczby (B, d)-wyjątkowe są tymi, które powodują, że redukcja faktoryzacji n do obliczania logarytmu dyskretnego w Z_n^* nie jest wielomianowa (por. [44], [45], [49]).

Reasumując, badania w dziedzinie teorii liczb i geometrii algebraicznej stanowią obecnie matematyczny fundament i tym samym kluczowe wyzwanie dla współczesnej kryptografii asymetrycznej. Duży potencjał badawczy polskich środowisk naukowych w tych dziedzinach stanowi silną przesłankę do budowania na nim polskiej kryptologii w oparciu o doświadczenia implementacyjne polskich uczelni technicznych (patrz np. [46], [47]).

Od wielu lat istnieje współpraca naukowa w ramach wspólnego seminarium badawczego z kryptologii przedstawicieli Instytutu Matematyki Wydziału MIMUW i Zakładu Podstaw Telekomunikacji, Wydziału Telekomunikacji i Technik Informacyjnych Politechniki Warszawskiej, a od roku także z przedstawicielami Instytutu Matematyki PAN w Warszawie. Obecna rozszerzona formuła współpracy polega między innymi na organizowaniu cyklu otwartych seminariów nt. zastosowań matematyki w kryptologii, która obejmuje trzy główne tematy: matematyczne aspekty kryptografii, teoretyczne i praktyczne problemy obliczeniowe w kryptologii oraz bezpieczeństwo informacji. Poza zaproszeniami kierowanymi do prelegentów z różnych ośrodków badawczych kraju seminarium jest okazją do wspólnych konsultacji przedstawicieli nauki, przemysłu i administracji publicznej pod auspicjami Narodowego Centrum Kryptologii.

Konferencja KBI2014 pokazała potrzebę dalszego rozwijania i rozszerzenia tej współpracy do regularnych spotkań kryptologicznych i konferencji naukowych z udziałem przedstawicieli jednostek badawczych, przedsiębiorców oraz administracji publicznej, pod patronatem Narodowego Centrum Kryptologii. Tak szeroka konsultacja społeczna stwarza nowy impuls do realizacji długofalowej polityki kryptologicznej w Polsce na najbliższe lata oraz rozwoju potencjału naukowego na rzecz budowy systemu bezpieczeństwa informacji [50].

Literatura

[1] http://www.bbn.gov.pl/pl/wydarzenia/5536,Doktryna-cyberbezpieczenstwa-dobre-praktyki-i-wspolpraca-publiczno-prywatna.html.

[2] http://wyborcza.biz/biznes/1,101558,15673560,Cyberszable_i_cyberczolg_czyli_jak_na_ataki_hakerow.html

[3] K. Bondaryk, *Potrzeba polityki kryptologicznej w Polsce*, referat zaproszony konferencji kryptografia i bezpieczeństwo informacji, Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego.

[4] B. Hołyst, *Wiktymologiczne aspekty cyberprzestępczości*, referat zaproszony konferencji pt. „Kryptografia i bezpieczeństwo informacji", Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego.

[5] J. Gawinecki, *Zagrożenia cyberprzestępczości a kryptografia narodowa*, referat zaproszony konferencji pt. „Kryptografia i bezpieczeństwo informacji", Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego.

[6] A. Joux, *A one round protocol for tripartite Diffie-Hellman*, Journal of Cryptology 17 (4): 263–276 (2004).
[7] W. Diffie, M. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory 22 (6): 644–654. (1976).
[8] D. Boneh, M. Franklin, *Identity-Based Encryption From the Weil Pairing*, SIAM Journal on Computing, 2003, t. 32, nr. 3, p. 586–611.
[9] J. Pomykała, *ID-based digital signatures with security enhanced approach*, J. Telecommunications and Information Technology 4, s. 146–153, 2009.
[10] M. Girault, *Self-certied public keys*, Advances in Cryptology: Eurocrypt'91, p. 490–497, Springer, 1991.
[11] J. Pejaś, *Schematy podpisu cyfrowego z jawnymi I niejawnymi certyfikatami w infrastrukturze z wieloma urzedami zaufania*, rozprawa habilitacyjna, Szczecin 2013 IEEE Standard for Identity-Based Cryptographic Techniques using Pairings, Std 1363$^{\text{TM}}$-2013.
[12] M. Kula, *Matroidy I dzielenie sekretów*, referat zaproszony konferencji pt. „Kryptografia i bezpieczeństwo informacji", Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego.
[13] J. Derbisz, *Wielowymiarowe rozszerzenia schematów podziału sekretu*, referat na konferencji pt. „Kryptografia i bezpieczeństwo informacji", Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego.
[14] W. Bagga, S. Crosta, R. Molva, *Policy-based Encryption Schemes from Bilinear Pairing*, Proc. of the 2006 ACM Symposium on information, computer and communication security, ACM Press, pp. 368–368, New York 2006.
[15] A. Pragacz, *Ogólne struktury dostępu z hierarchią*, referat na konferencji pt. „Kryptografia i bezpieczeństwo informacji", Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego.
[16] B. Hołyst, J. Pomykała, P. Potejko (red.), *Nowe techniki badań kryminalistycznych a bezpieczeństwo informacji*, Wyd. PWN, Warszawa 2014.
[17] K. Durnoga, J. Pomykała, *Racjonalne generowanie systemów kryptograficznych*, to appear.
[18] B. Hołyst, J. Pejaś, J. Pomykała (red.), *Cyberprzestępczość i bezpieczne systemy zarządzania informacją klasyfikowaną*, wyd. WSM, Warszawa 2013.
[19] K. Rubin, A. Silverberg, *Torus-Based Cryptography*, CRYPTO 2003: 349–365.

[20] M. Grześkowiak, *Metody generowania liczb pierwszych w kryptosystemach z kluczem publicznym*, referat zaproszony konferencji pt. „Kryptografia i bezpieczeństwo informacji", Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego.

[21] J. Pomykała, *Teoria liczb w kryptologii*, referat na konferencji pt. „Kryptografia i bezpieczeństwo informacji", Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego.

[22] M. Skałba, *Derandomizacja wybranych algorytmów kryptograficznych*, referat na konferencji pt. „Kryptografia i bezpieczeństwo informacji", Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego.

[23] B. Źrałek, *Rozszerzony algorytm Pohliga-Hellmana i jego zastosowanie do faktoryzacji*, referat na konferencji pt. „Kryptografia i bezpieczeństwo informacji", Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego.

[24] T. A. Elgamal , *A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*, IEEE Transactions on Information Theory 1985, t. IT-31, nr. 4, s. 469–472 or CRYPTO 84, s. 10–18, Springer-Verlag.

[25] Z. Jelonek, *Krzywe eliptyczne z zadanym pierścieniem endomorfizmów i podgrupą ustalonego rzędu*, referat na konferencji pt. „Kryptografia i bezpieczeństwo informacji", Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego.

[26] R. Dryło, *Konstruowanie krzywych hipereliptycznych genusu 2 z małym stopniem zanurzeniowym*, referat na konferencji pt. „Kryptografia i bezpieczeństwo informacji", Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego.

[27] A. Dąbrowski, *Metoda Cocksa-Pincha dla pewnych klas krzywych algebraicznych*, referat zaproszony konferencji pt. „Kryptografia i bezpieczeństwo informacji", Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego.

[28] A. K. Lenstra, *Using cyclotomic polynomials to construct efficient discrete logarithm cryptosystems over finite fields*, ACISP' 97 Springer-Verlag 1997.

[29] M. Grześkowiak, *Algorithms for relatively cyclotomic primes*, Fundamenta Informaticae 125 (2013), pp. 161–181.

[30] J. Pomykała, J. A. Pomykała, *Systemy informacyjne, modelowanie i wybrane techniki kryptograficzne*, MIKOM, Warszawa 1999.

[31] J. Pomykała, *On q-orders in primitive modular groups*, Acta Arithmetica, 166 4 (2014) p. 397–404.

[32] J. Pomykała, *On the greatest prime divisor of quadratic sequences*, Sém. Théor. Nombres Bordeaux 3(2), p. 361–375, 1991.

[33] J. Kaczorowski, *Zastosowanie funkcji L w kryptologii*, referat zaproszony konferencji pt. „Kryptografia i bezpieczeństwo informacji", Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskieg.

[34] Y. Dodis, X. Li, T. D. Wooley, D. Zuckerman, *Privacy amplification and non-malleable extractors via character sums*, In: Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS '11, pages 668–677,IEEE Computer Society.

[35] K. Durnoga, *Niekowalne ekstraktory losowości*, referat na konferencji pt. „Kryptografia i bezpieczeństwo informacji", Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego.

[36] K. Durnoga, B. Źrałek, *On randomness extractors and computing discrete logarithms in bulk*, submitted.

[37] M. Anshel, D. Goldfeld, *Zeta functions, one-way functions, and pseudorandom number generators*, Duke Math. J. 88(1997), 371–390.

[38] B. J. Birch, H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. Reine Angew. Math. 218 (1965), p. 79–108.

[39] A. Dąbrowski, J. Pomykała, *Nonvanishing of motivic L-functions*, Math. Proc. Cambridge Philos. Soc., 130(2), pp. 221–235, 2001.

[40] A. Perelli, J. Pomykała, *Averages of twisted elliptic L-functions*, Acta Arith, 80, pp. 149–163, 1997.

[41] T. Adamski, *Średnia złożoność obliczeniowa probabilistycznego algorytmu wyszukiwania pierwiastków pierwotnych modulo n*, referat na konferencji pt. „Kryptografia i bezpieczeństwo informacji", Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego.

[42] A. Paszkiewicz, *Badania własności liczb pierwszych i wielomianów nieprzywiedlnych pod kątem zastosowania w telekomunikacji*, Rozprawa habilitacyjna, Politechnika Warszawska, Warszawa 2012.

[43] J. B. Conrey, *Problem 8 in: Future directions in algorithmic number theory*, The American Institute of Mathematics, 2003, http://www.aimath.org

[44] J. Pomykała, B. Źrałek, *On Reducing Factorization to the Discrete Logarithm Problem Modulo a Composite*, Computational Complexity, Volume 21, Number 3, p. 421–429, Springer-Verlag, 2012.

[45] J. Pomykała, (d, B)-*exceptional numbers with applications to cryptology*, PTM-DMV Mathematical Conference, Poznań 2014.

[46] J. Gawinecki, P. Bora, M. Jurkiewicz, T. Kijko, *Zastosowanie krzywych eliptycznych do konstrukcji bezpiecznych algorytmów i protokołów kryptograficznych*, referat na konferencji pt. „Kryptografia i bezpieczeństwo informacji", Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego.

[47] P. Bęza, J. Gocławski, P. Mral, D. Waszkiewicz, P. Sapiecha, *Akceleracja obliczeń kryptograficznych z wykorzystaniem procesorów GPU*, referat na konferencji pt. „Kryptografia i bezpieczeństwo informacji", Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego.

[48] J. Pomykała, B. Źrałek, *Dynamic group tnreshold signature based onderandomized Weil pairing computation*, Metody Informatyki Stosowanej, 4/2008 (t. 17) s. 183–194

[49] J. Pomykała, *On exponents of modular subgrous generated by small intervalls*, (submitted)

[50] L. Grabarczyk, *Rozwój potencjału naukowego na rzecz budowy systemu bezpieczeństwa informacji*, referat zaproszony konferencji pt. „Kryptografia i bezpieczeństwo informacji", Warszawa 5–6 czerwiec 2014, Wydział Matematyki Informatyki i Mechaniki Uniwersytetu Warszawskiego.

NEW CHALLENGES FOR POLISH CRYPTOLOGY IN SECOND DECADE OF XXI CENTURY

Abstract. In this paper we analyze the challenges for the twenty-first century Polish cryptology with special emphasis on the needs of the national cryptology and the role they perform in the selected areas of mathematics such as number theory and algebraic geometry. In particular, we stress the role and security of bilinear based cryptosystems, as well as the problems of computational complexity of deterministic algorithms important for cryptology. We pointed out the importance of L-functions in modern cryptography and cryptoanalysis.

Keywords: Polish Cryptology Policy, information security, efficiency and functionality of cryptosystem, cryptoanalysis and hard computational problems, derandomization, L-functions, elliptic curves, CM method, B-exceptional numbers, equiparition mod 1, one-way functions, policy based cryptosystems, algebraic geometry, number theory