ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 *2006. Nr. 1(65)*
ELEKTRONIKA IR ELEKTROTECHNIKA

T 180 *TELECOMMUNICATION ENGINEERING*
TELEKOMUNIKACIJŲ INŽINERIJA

Mažoritarinės funkcijos kriptografinių savybių tyrimas

P. Nefas, A. Vobolis
Telekomunikacijų katedra, Kauno technologijos universitetas,
Studentų g. 50, LT–51368 Kaunas, Lietuva, tel. +370 37 223459, el. p. petrasnefas@gmail.com

Įvadas

Svarbus kriptografinių sistemų analizės etapas – matematinio modelio sudarymas ir šifro mazgų aprašymas diskretinėmis, dažniausiai Bulio, funkcijomis. Atliekant kriptoanalizę, diskretinė funkcija yra naudingas matematinis modelis, kuriuo galima pavaizduoti informacijos keitimą srautiniuose šifruose. Šis modelis patogus tuo, kad srautinius šifrus galima analizuoti diskretinės matematikos pagrindu, prieš tai tinkamai įvertinus kriptografines Bulio funkcijos savybes. Bulio funkcija, susidedanti iš *n* kintamųjų, – tai *n*-matės vektorinės erdvės F_2^n atvaizdavimas vienmatėje erdvėje $F_2 = \{0,1\}$ [2]:

$$\Phi : F_2^n \to F_2 \,, n > 0 . \qquad (1)$$

Svarbus Bulio funkcijų analizės metodas – Walsho transformacija $W_f(u)$. Funkcijos f Walsho transformacija, esant vektoriui $u \in F_2^n$ vadinama skaitinė vertė [2]:

$$\begin{cases} W_f(u) = \sum_{x \in F_2^n} (-1)^{f(x)+\langle u,x \rangle}, \\ \langle u, x \rangle = \sum_{n=1}^{n} x_i u_i . \end{cases} \qquad (2)$$

Viena iš esminių kriptografinių savybių yra subalansavimas. Reikalavimai subalansavimui remiasi Golombo postulatais. Funkcija $f(x)$ vadinama subalansuota, jei

$$wt(f) = wt(f \oplus 1) = 2^{n-1}; \qquad (3)$$

čia $wt(f)$ yra funkcijos $f(x) \in F_2^n$ Hemingo svoris, t.y. skaičius x rinkmenų, tenkinančių lygybę $f(x) = 1$. Subalansuotos funkcijos Walsho transformacijos vertė, esant nuliniam vektoriui:

$$W_f(0) = \sum_{x \in F_2^n} (-1)^{f(x)} = 0 . \qquad (4)$$

Kita kriptografinė Bulio funkcijos savybė yra netiesiškumas. Funkcijos tiesiškumas suprantamas kaip matematinio uždavinio efektyvaus sprendinio buvimas. Todėl kriptografinių sistemų netiesiškumas yra fundamentali ir neatskiriama savybė. Konkretus netiesiškumo traktavimas ir jį aprašantys parametrai gali būti įvairūs.

Dažniausiai netiesiškumas apibrėžiamas funkcijos Hemingo atstumu iki afiniųjų funkcijų visumos. Pagal Mebuso transformacijos teorema kiekvieną Bulio funkciją galima vienareikšmiškai išreikšti ANF (algebrinės normalinės formos) polinomu [4]:

$$f(x) = \bigoplus_{I \subseteq \{1,\ldots,n\}} a_I \left(\prod_{i \in I} x_i \right). \qquad (5)$$

Polinomo laipsnis $\deg f$ – tai netiesiškumo laipsnis. Jei polinomo laipsnis $\deg f = 1$, tai tokia funkcija vadinama afiniąja funkcija[4]:

$$\begin{cases} f(x) = a_0 \oplus a_1 x_1 \oplus .... \oplus a_n x_n , \\ dist(f, A_n) = \min\limits_{l_{a,b} \in A_n} \{ dist(f, l_{a,b}) \,|\, l_{a,b} = \\ = \langle a, x \rangle \oplus b \in A_n, a \in F_2^n, b \in F_2 ; \end{cases} \qquad (6)$$

čia $\langle a, x \rangle = a_1 x_1 \oplus \ldots \oplus a_n x_n$ – skaliarinė sandauga.

Netiesiškumo parametras nusako galimybę analizuojamąją funkciją pakeisti afiniuoju analogu. Šis atstumas vadinamas funkcijos netiesiškumu ir žymimas taip:

$$N_f = \min_{l_{a,b} \in A_n} \{ dist(f, l_{a,b}) \,|\, l_{a,b} \in A_n \} . \qquad (7)$$

Funkcijos *f* Hemingo atstumas iki afiniųjų funkcijų $dist(f, A_n)$ [2] susijęs su Walsho transformacijos koeficientais tokia išraiška:

$$dist(f, A_n) = 2^{n-1} - \frac{1}{2} \max_{a \in F_2^n} \left| W_f(a) \right| . \qquad (8)$$

Remiantis tiesinės sandoros funkcijos apibrėžimu įvesta absoliučiai netiesinių funkcijų sąvoka. Absoliučiai netiesinė funkcija yra tada, kai $\hat{F}(w) = 2^{n/2}$. Ši savybė absoliučiai netiesines funkcijas sutapatina su kombinatorinėmis bent funkcijomis, todėl šios funkcijos kriptografijoje vadinamos bent funkcijomis.

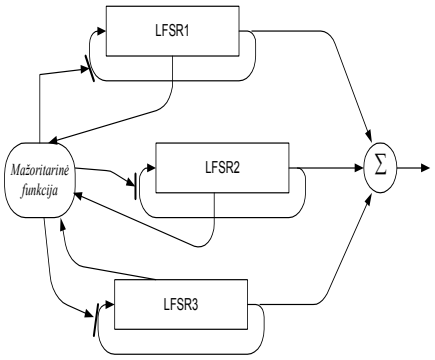
Bent funkcijos yra labai naudingos kriptografinės funkcijos, kadangi jos tuo pat metu turi maksimalų

$$dist(f, A_n) = 2^{n-1} - 2^{\frac{n}{2}-1} \qquad (9)$$

atstumą iki visų tiesinių funkcijų ir maksimalų 2^{n-2} atstumą iki visų funkcijų, turinčių tiesinę sandarą. Generatoriai, sukurti bent funkcijų pagrindu, yra atsparūs tiesinei sintezei. Kadangi Walsho transformacijos koeficientai yra sveikieji skaičiai, todėl maksimaliai netiesinės funkcijos egzistuoja tik esant lyginiam kintamųjų skaičiui.

Srautinio šifro modelio tyrimas

Dideliam kriptografiniam atsparumui pasiekti srautinių šifrų konstruktoriai naudoja mazgus postūmio registro judesio netolydumui didinti. Vienas tokių sprendimų yra R. Rueppelio pasiūlyta mažoritarinė LFSR pakopų sinchronizacija (1 pav.).

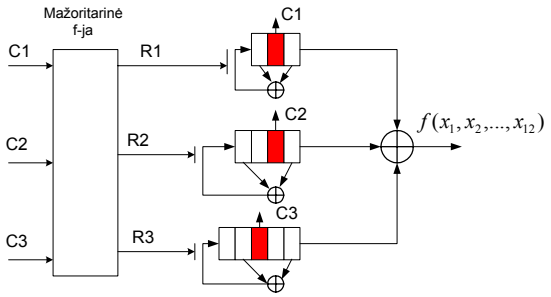


1 pav. LFSR pakopų sinchronizacija

Šis būdas įgyvendintas A5/1 šifre. A5/1 šifras yra išnagrinėtas ir jo kriptoanalizė atlikta, tačiau ji remiasi bendraisiais šifrų analizės metodais: gimimo dienos paradoksu, laiko ir atminties pakeitimo ataka, ypatingų padėčių ataka ir t.t., tai yra buvo pasinaudota konstrukciniais šifro trūkumais, bet nebuvo sudarytas šios schemos matematinis modelis, nenustatyta šifravimo gamos generuojančioji funkcija ir neįvertintos jos kriptografinės charakteristikos ir kriterijai.

Sukurkime šifrą, kurio LFSR pakopos būtų sinchronizuojamos mažoritarine funkcija , o šifro raktų erdvė pakankamai nedidelė, kad galėtume atlikti išsamią statistinę šio šifro analizę. Galimas tokios konstrukcijos pavyzdys pateiktas 2 pav.

Ši srautinio šifro schema turi trijų, keturių ir penkių skilčių ilgio LFSR. Registrų ilgiai ir jų atvadai parinkti taip, kad išėjimo gama, nesant mažoritarinės sinchronizacijos, turėtų didžiausią periodą. Pirmasis registras generuoja maksimalią ilgio seką, kurios periodas 7, antrasis atitinkamai – 15, trečiasis – 31 periodo seką. Tokio generatoriaus raktų ilgis 12 bitų, o visa raktų erdvė– 2^{12} , arba 4096, skirtingi raktų variantai.



2 pav. Analizuojamoji srautinio šifro schema

Perrinkime visas galimas raktų kombinacijas ir atlikime generuojamos gamos statistinę analizę: apskaičiuokime generuojamos sekos periodą ir tiesinį kompleksiškumą Berlekamp ir Massey algoritmu. Rezultatus surašome į lentelę.

Lentelė. Sekos periodas ir tiesinis kompleksiškumas

Sekų skaičius	54	127	255	511	511	3149
Sekos periodas	1	17	37	42	39	89
Generuojamos sekos tiesiškumas	1	7	8	9	9	89

Sudarydami matematinį modelį, remsimės tik paskutinės skilties rezultatais, o kitus paneigsime dėl šių priežasčių:

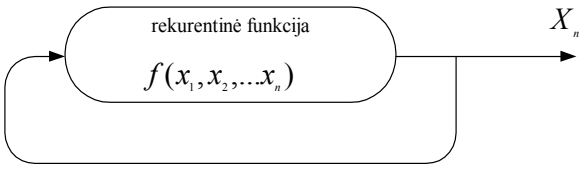
1. 89 bitų ilgio sekos nagrinėjamoje grupėje yra kriptografiniu požiūriu stipriausios;

2. Likusios sekos – tai ypatingi atvejai: pirmojoje skiltyje yra tos raktų kombinacijos, kurių bent du registrai užpildyti nuliais, antrojoje skiltyje – kai trečiojo registro visos skiltys užpildytos nuliais , trečiojoje – kai antrojo, ir ketvirtojoje – kai trečiojo. Ypatingų atvejų susidarymo dažnis priklauso nuo registrų ilgių. Tikimybė, kad trumpiausio registro visos skiltys yra nuliai, lygi $1/2^n$, tad realiomis sąlygomis, kai registro ilgis viršija 20, ypatingų atvejų skaičius bus palyginti nereikšmingas.

Šis generatorius 3149 atvejais generuoja periodinę 89 bitų ilgio seką, kuri konkrečiam raktui skiriasi faze:

$S_1, .., S_i = \{$00000111010110001110101011110111100111011011100111111100110001111100011101100101001 10000$\}$; čia *i=1,..,89.*

Norėdami rasti generuojančiąją sekos funkciją, tam tikslui analizuojamą schemą pakeiskime rekurentiniu generatoriumi, kuris generuotų tokią seką (3 pav.).



3 pav. Hipotetinis generatorius

Rekurentinės sekos, generuojančios funkcijos kintamųjų skaičių, apibrėžia ilgiausio pasikartojančio segmento ilgis generuojamoje sekoje. Randame ilgiausią pasikartojantį segmentą:{ 0001110101}. Jo ilgis yra 10 bitų, vadinasi, turi būti 11 inicialinių generuojančiosios sekos bitų.

Tokios sekos generuojančiosios funkcijos $f(x_1,...x_{11})$ didžiausias polinomo laipsnis būtų 11, o teisingumo lentelės verčių matrica turėtų 2^{11} elementų, iš jų: nulių matrica $\lfloor F^0 \rfloor$ – 38 elementus , vienetų matrica $\lfloor F^1 \rfloor$ – 51 elementą, neapibrėžtų reikšmių matrica $\lfloor F^d \rfloor$ turėtų likusius 1959 elementus. Tokios funkcijos analizė yra ypač sudėtinga ir pareikalautų labai didelių skaičiavimo ir laiko išteklių.

Kriptografiniu požiūriu prasminga rasti tokią generuojančiąją funkciją, kuri generuotų seką, artimą nagrinėjamai (santykinis Hemingo atstumas < 0,5), o polinomo laipsnis būtų kiek galima mažesnis. Akivaizdu, kad 89 bitų periodinę seką generuotų funkcija, kurios kintamųjų skaičius būtų bent 7 ($2^7 - 1 > 89$).

Transformuokime analizuojamąją seką, pakeisdami kai kuriuos sekos elementus taip, kad ilgiausias pasikartojantis fragmento ilgis neviršytų 7 bitų, o Hemingo atstumas tarp sekų būtų ne didesnis kaip 44. Galimas tokios sekos variantas:

$\hat{S}_1,..,\hat{S}_i$ = {00011111010110001110010011110111100111011011100110111100100001011100011011010101001110000}, čia *i=1,..,89*.

Šios sekos ilgiausio pasikartojančio fragmento ilgis yra septyni bitai, o Hemingo atstumas nuo pradinės sekos – 12 bitų. Tokią seką generuotų septynių kintamųjų Bulio funkcija $f(x_1,..x_7)$, maksimalus polinomo laipsnis yra 7.

Šios funkcijos teisingumo lentelė yra 8×2^7 matmenų. Bet kuri 8 bitų sekos $\hat{S}_1,..,\hat{S}_i$ atkarpa yra funkcijos teisingumo lentelės viena eilutė , kurios pirmieji septyni bitai – tai funkcijos argumentų vertės, o aštuntas bitas – funkcijos vertė.

Tokių atkarpų kartu su cikliniu postūmiu yra 89, o neapibrėžtų verčių matrica turi 39 elementus, vadinasi, yra 2^{39} skirtingų funkcijų, kurios generuoja tokią seką. Priskirkime visus neapibrėžtų verčių matricos elementus nulių matricai. Kaip žinome, kiekvieną visiškai apibrėžtą funkciją galime išreikšti unikaliu ANF polinomu:

$$f(x_1,...x_n) = \oplus_{u \in F_2^n} a_u x^u \ ; \qquad (10)$$

čia x^I – vienanaris, lygus

$$x^u = \prod_{i=1}^{n} x_i^{u_i}, \qquad (11)$$

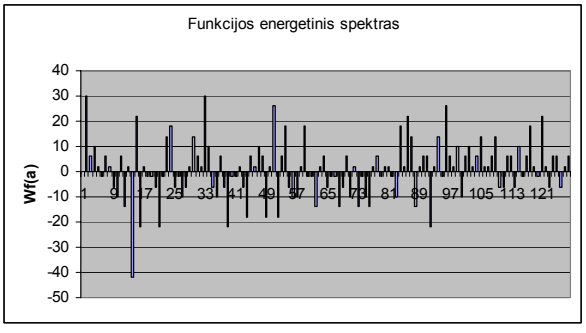
o $a_u \in F_2$ – tai teisingumo lentelės elementas. Sudarę rekurentinės sekos teisingumo lentelę, išvedame sekos ANF:

$$\begin{aligned} f(x_1,..x_7) &= x_1x_2x_3x_4x_5x_6 + \\ &+ x_1x_2x_3x_4x_5x_7 + x_1x_2x_3x_4x_5 + \\ &+ x_1x_2x_3x_4x_6x_7 + x_1x_2x_3x_4x_5x_7 + \\ &+ x_1x_2x_3x_5x_7 + x_1x_2x_3x_6 + \\ &+ x_1x_2x_4x_7 + x_1x_2x_5x_7 + \\ &+ x_2x_3x_4x_5x_6x_7 + x_2x_3x_4x_7 + \\ &+ x_2x_3x_6x_7 + x_2x_3 + +x_2x_4x_6 + \\ &+ x_2x_6 + x_3x_4x_5x_6x_7 + x_3x_5x_7 + \\ &+ x_4x_5x_7 + x_6x_7. \end{aligned} \qquad (12)$$

Įvertinkime funkcijos netiesiškumą Hemingo atstumu iki afiniųjų funkcijų. Išreikškime atstumą šios funkcijos Walsh ir Hadamard transformacijos koeficientais:

$$\begin{cases} dist(f, A_n) = 2^{n-1} - \frac{1}{2} \max\limits_{a \in F_2^n} \left|W_f(a)\right|, \\ W_f(a) = \sum_{x \in F_2^n} (-1)^{f(x)+\langle a,x \rangle}, \\ \langle a,x \rangle = \sum_{n=1}^{n} x_i a_i; \end{cases} \qquad (13)$$

čia a_i ir $f(x)$ – tai funkcijos teisingumo lentelės atitinkami elementai. 4 pav. pateikti funkcijos $f(x_1,..x_7)$ Walsh ir Hadamardo transformacijos rezultatai – funkcijos energinis spektras. Abscisių ašyje leksikografine tvarka atidėtos funkcijos argumentų vertės, ordinatėje – atitinkamas Walsho ir Hadamardo transformacijos koeficientas $W_f(a)$.



4 pav. Funkcijos energinis spektras

Matome, kad maksimali transformacijos $|W_f(a)|$ vertė lygi 42, kai $x_1,...,x_7 = \{0,0,0,1,1,0,1\}$.

Apskaičiuojame netiesiškumą:

$$dist(f, A_n) = 2^{7-1} - \frac{1}{2}42 = 40 \cdot \quad (14)$$

Dabar, žinodami funkcijos $f(x_1,...x_7)$ netiesiškumą, įvertinkime seką $S_1,..,S_i$ generuojančios funkcijos $f(x_1,...x_{11})$ netiesiškumą. Kadangi Hemingo atstumas tarp dviejų sekų $S_1,..,S_i$ ir $\hat{S}_1,..,\hat{S}_i$ yra 12 bitų, tai akivaizdu, kad $f(x_1,...x_{11})$ atstumas iki afiniųjų funkcijų

$$dist(f(x_1,...x_{11}), A_n) \le 40 + 12 = 52 . \quad (15)$$

Matome, kad $f(x_1,...x_{11})$ nėra bent funkcija, kadangi maksimalus netiesiškumas

$$dist(f, A_n) = 2^{n-1} - 2^{\frac{n}{2}-1} = 58 . \quad (16)$$

Išvados

Mažoritarinės funkcijos yra paprasto dizaino ir labai netiesiškos, todėl plačiai naudojamos srautiniams šiframs konstruoti. Atliktas tyrimas parodė kelis esminius tokių šifrų trūkumus. Generuojančioji funkcija yra nesubalansuota, t. y. gamoje yra „nuliukų“ ir „vienetukų“ disbalansas, todėl tokia seka yra jautri testinei analizei. Šifravimo gama yra ne maksimalaus 2^N-1, o tik $\sim 2^{\frac{2}{3}N}$ bitų periodo, kur N − rakto ilgis, todėl ją keblu taikyti didesniems failams šifruoti. Tokio šifro generuojančioji funkcija nepriklauso bent funkcijų klasei, jos taikymas srautinių šifrų registrams valdyti neužtikrina maksimalaus netiesiškumo, todėl galima tokio šifro šifravimo gamos tiesinė sintezė. Mažoritarinės funkcijos neapibrėžtumų matrica turi 1959 elementus, vadinasi, egzistuoja 2^{1959} funkcijų, kurios generuoja tokią seką, todėl tolesniam tyrimui svarbu turėti algoritmą mažiausio laipsnio funkcijos paieškai.

Literatūra

1. **Rueppel R.A.** Security Models and Notions for Stream Ciphers // Cryptography and Coding 11, C. Mitchell, ed.- Oxford: Clarendon Press, 1992. – P. 213 – 230.
2. **Zhang X.M, Zheng Y.** Normalized Measures for Cryptographic security // Journal of Universal Computer science. – 2002. – No. 1(5). – P. 316–333.
3. **Menezes, P. van Oorschot and S.Vanstone.** Handbook of Applied Cryptography // by A., CRC Press, 1996. – P. 169 – 190.
4. **Pommerening K.** Fourier Analysis of Boolean Maps. A Tutorial–Fachbereich Mathematik der Johannes-Gutenberg-Universitaet Saarstrasse 21 D-55099 Mainz.– 2003.– P. 3–41.
5. **Wegener, John** The Complexity of Boolean Functions // Wiley & Sons Ltd., and B.G. Teubner, Stuttgart July 1987. ISBN: 0471 -91555-6. –P. 243–249.

Pateikta spaudai 2005 04 29

P. Nefas, A.Vobolis. Mažoritarinės funkcijos kriptografinių savybių tyrimas // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2005. – Nr. 1(65). – P. 73–76.

Mažoritarinė funkcija – netiesinė Bulio funkcija, priklausanti slenkstinių funkcijų klasei. Ši funkcija dėl savo savybių – netiesiškumo, nesudėtingo dizaino – plačiai naudojama srautiniams šiframs konstruoti. Plačiausiai žinoma R. Rueppelio schema, realizuota A5/1 schemoje, tai yra LFSR judesių valdymas mažoritarine schema. Straipsnyje tirtos galimybės sukurti srautinio šifro su LFSR mažoritarine sinchronizacija matematinį modelį. Sukonstruotas 12 skilčių srautinis šifras, kurio trys registrai yra trijų, keturių ir penkių skilčių ilgio. Šio šifro statistinė analizė parodė, kad 76 % visų sekų – tai periodinė 89 bitų seka. Sudaryta rekursinė vienuolikos bitų sekos teisingumo lentelė. Sudaryta generuojančiosios funkcijos nulių bei vienetų matrica. Nustatyta, kad generuojančioji funkcija nepriklauso bent funkcijų klasei, taigi nėra maksimaliai netiesinė. Funkcijos neapibrėžtumų matrica turi 1959 elementus, vadinasi, yra 2^{1959} funkcijų, kurios tokią seką generuoja**.** Il.4, bibl.5 (lietuvių kalba; santraukos lietuvių, anglų, rusų k.).

P. Nefas, A.Vobolis. Majority Function Investigation of Cryptografical Features // Electronics and Electrical Engineering. – Kaunas: Technologija 2005. – No. 1(65). – P.73–76.

Majority function is nonlinear Boolean function, which belongs to threshold functions class. This function has features like nonlinearity, simple design which enables its using in constructing stream ciphers. Most known Ruppel`s scheme is used in A5/1 which enables LFSR control with majority scheme. In this article we investigate LFRS majority synchronization by using mathematical model. Constructed 12 segments stream cipher which registers are three, four and five segments length. Statistical analysis of this cipher showed that 76 % of all sequences are 89 bits sequence. Constructed recursive eleven bits sequence truth table. Constructed generating function matrix or ones and zeros. Determined that generating function doesn't belongs to Bent functions class so it is not nonlinear. Functions matrix has 1959 elements so exists 2^{1959} functions which generate that sequence. Il. 4, bibl. 5 (in Lithuanian; summaries in Lithuanian, English, Russian).

П. Нефас А. Воболис. Анализ криптографических свойств мажоритарной функции // Электроника и электротехника. – Каунас: Технология 2005. – № 1(65). – P. 73–76.

Мажоритарная функция это нелинейная булевая функция, принадлежащая к так называемому классу пороговых функций. Из-за своих свойств– нелинейности и несложного дизайна мажоритарная функция широко применяется в конструировании потоковых шифров. Наиболее широко известна схема Р. Руеппеля, применена в схеме A5/1,это мажоритарное управление движением линейных регистров сдвига. В статье анализируется возможность создания математической модели поточного шифра с мажоритарной синхронизацией. Статистический анализ сконструированного 12- разрядного поточного шифра показал, что 76 процентов всех генерированных гамм этого шифра имеет длину 89 битов. Составлена таблица истинности рекурсивной функции и матрица нолей и единиц генерирующей функции. Установлено, что функция не принадлежит к классу бент–функций ,следовательно не является максимально нелинейной. Ил.4, библ.5 (на литовском языке; рефераты на литовском, английском и русском яз.)