KRIPTOANALIZA SEKVENCIJALNIH KRIPTOGRAFSKIH ALGORITAMA ZASNOVANA NA UPOTREBI BINARNOG DIJAGRAMA ODLUČIVANJA

Slobodan Bojanić, *Universidad Politecnica de Madrid*, *slobodan@die.upm.es*
Srđan Đorđević, *Elektronski fakultet u Nišu, srdjan.djordjevic@elfak.ni.ac.rs*

Sadržaj – *U ovom radu dat je pregled postupaka kriptoanalize koji se zasnivaju na korišćenju različitih varijanti Binarnog Dijagrama Odlučivanja (BDD). Radi se o kriptoanalizi protočnih šifara koje koriste linearni pomerački registar sa povratnom spregom (LFSR), jedanog od najznačajnijih i najšire korišćenih blokova u generatorima niza ključeva. Pored opisa napada data je i procena njihove prostorne i vremenske kompleksnosti. Rad opisuje i moguće pravce daljeg usavršavanja prezentovanih kriptoanalitičkih napada.*

1. UVOD

Sekvencijalni kriptosistem spada u simetrične kriptosisteme kod kojih je ključ za šifrovanje i dešifrovanje isti. Odlika ovog kriptosistema je da se šifrovanje obavlja nad svakom jedinicom podatka otvorenog teksta pojedinačno.

Kod šifarskih sistema je potrebno uskladiti kriptografsku sigurnost sa hardverskim i softverskim performansama tako da su se novija istraživanja sekvencijalnih sistema fokusirala na šifrate koji nude bolje performanse za određene arhitekture (8, 16, 32 ili 64 bitna) uz zadovoljavajuće hardverske resurse u smislu broja gejtova, površine ili potrošnje.

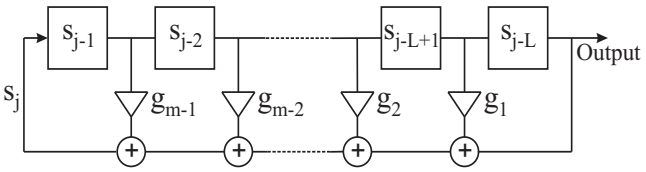
Koncept kriptografskog napada predložio je Kraus 2002 [1]. Ovaj pristup dao je dobre rezultate u napadima na kriptosisteme: A5/1, E_0 i kriptosistem sa "sažimajućim generatorom" (self-shrinking). Nešto kasnije su objavljene i verzije OBDD i ZBDD ovog metoda za kriptoanalizu Bluetooth kriptogeneratora [4, 5]. Vremenska složenost ovih kriptografskih metoda uslovljena je brojem čvorova u binarnim dijagrama odlučivanja koji se konstruišu tokom kriptografskog napada.

U nastavku rada, u drugom poglavlju je dat pregled LFSR kriptosistema. U trećem poglavlju predstavljen je binarni dijagram odlučivanja (Binary Decision Diagram, BDD) kao i njegove varijante koje se primenjuju u kriptoanalizi. Kratak pregled BDD kriptoanalize LFSR kriptosistema, poznatijeg kao Krausov metod, dat je u četvrtom poglavlju. Dve adaptirane i optimizovane verzije Krausovog metoda koje su prilagodjene specifičnostima E_0 kriptosistema, opisane su u poglavlju 5 i 6 respektivno. U poglavlju 7 je dat zaključak sa mogućim pravcima daljeg usavršavanja prezentovanih kriptoanalitičkih metoda.

2. LFSR KRIPTOSISTEMI

LFSR (Linear Feedback Shift Register) je veoma korišćen u sekvencijalnim kriptosistemima za generisanje pseudoslučanog niza kako zbog svojih kriptografskih odlika tako i pogodnosti u implementaciji. Naime izlazni niz ovog registra karakterišu veoma dugi period i uniformna raspodela kao i jednostavna hardverska i softverska implementacija.

Blok šema LFSR-a, prikazana je na slici 1. On predstavlja pomerački registar čiji je ulazni bit linearna kombinacija njegovog prethodnog stanja. Povratna vrednost dobija se izvodjenjem EXOR operacije nad sadržajem odabranih memorijskih ćelija. Zavisno od izbora bitova čija će vrednost biti korišćena za povratnu spregu množač, g_i dobija vrednost 0 ili 1.



Sl. 1. *Blok šema linearnog pomeračkog registra sa povratnom spregom (LFSR)*

Kako je LFRS linearni sistem čija izlazna sekvenca je potpuno linearna, to ga čini veoma osetljivim na kriptoanalitičke napade. Da bi se uklonila linearnost generisanog pseudoslučajnog niza, nekoliko pozicija registra ili izlazni nizovi više pomeračkih registara se kombinuju pomoću Bulove nelinearne funkcije. Pored ove tehnike za dobijanje zadovoljavajuće kriptografske sigurnosti koristi se i taktno okidanje jednog LFSR registra drugim LFSR registrom. Dodatni blok LFSR generatora kojim se postiže zadovoljavajuća kriptografska sigurnost sistema je nelinearna kompresiona funkcija, *C*.

Generisanje radnog ključa u LFSR kriptosistemima obavlja se u dve faze na sledeći način:

$$k_{cipher} = C(L(k)) \tag{1}$$

gde je: k tajni ključ; k_{cipher} radni ključ ili niz ključeva; $L(k)$ linearni niz bitova formiran iz jednog ili više paralelnih LFSR-a; C nelinearna kompresiona funkcija

Dijagram odlučivanja našao je primenu u poznatim LFSR protočnim kriptosistemima kao što su: E_0 koji se koristi u Bluetooth bežičnim tehnologijama, *A5/1* i *A5/2* koji se koriste u GSM mobilnoj telefoniji, kriptosistem zasnovan na "sažimajućem generatoru". Svi ovi kriptografski metodi su kao i većina poznatih kriptografskih napada bazirani na otkrivanju ključa (key recovery).

Algoritam šifrovanja toka podataka E_0 sastoji se iz tri dela. Prvi deo obavlja funkciju inicijalizacije i u njemu se generiše ključ za svaki paket podataka upotrebom četri registara različitih dužina (25, 31, 33, 39 bitova). Drugi deo generiše niz slučajnih bitova metodom koju su osmislili Massey i Ruppel. Nelinearna kombinaciona funkcija se uobičajeno predstavlja pomoću četvorobitnog konačnog automata. Suma četiri izlazna bita LFSR-a predstavlja ulaz u konačni automat čime se ažurira njegovo stanje. Sa svakim taktnim impulsom generiše se izlazni bit šifrata korišćenjem izlaza pomeračkih registara i dva interna stanja, od kojih je svako dužine 2 bita. Praktično, izlazi četiri LFSR registara se kombinuju XOR funkcijom sa izlaznim bitom nelinearne kombinacione logike.

U trećem delu kriptosistema obavlja se šifrovanje kao i u svakom drugom sekvencijalnom kriptosistemu korišćenjem XOR operacije na ulaznom i generisanom nizu.

3. BINARNI DIJAGRAM ODLUČIVANJA

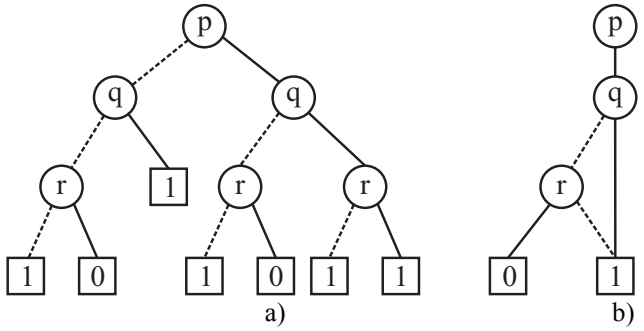
Binarni dijagram odlučivanja (BDD) [2] je direktan acikličan graf koji se koristi za predstavljanje diskretnih funkcija. Svaki neterminalni čvor ima tačno dva čvora potomka (stepen izlaznog granjanja 2) dok dva završna čvora predstavljaju konstantnu funkciju 1, odnosno konstantnu funkciju 0. Značajna osobina ovih grafova je kanoničnost, odnosno za dve Bulove funkcije možemo da tvrdimo da su jednake ukoliko su njihove BDD-reprezentacije jednake. Druga bitna osobina ove strukture podataka je da su rezultati obrade na raspolaganju za dalju upotrebu.

BDD se formira eliminacijom dva tipa redundantnosti. Transformacije kojima se eliminišu redundantnosti su:

(1) eliminacija čvorva dijagrama čije su obe izlazne ivice usmerene ka istom čvoru

(2) međusobno izomorfni podgrafovi se spajaju u jedan podgraf

Slika 2 prikazuje primer generisanja BDD iz binarnog stabla odlučivanja primenom gornjih transformacija.



Sl. 2. *a) Binarno stablo odlučivanja b) Binarni dijagram odlučivanja*

Varijante BDD koje su našle primenu u kriptografiji su Slobodni binarni dijagram odlučivanja (Free Binary Decision Diagram, FBDD), Uredjen binarni dijagram odlučivanja (Ordered Binary Decision Diagram, OBDD) kao i Binarni dijagram odlučivanja sa potisnutim nulama (Zero-suppressed Binary Decision Diagram, ZBDD).

FBDD je BDD u kojem se duž svakog puta promenjive pojavljuju najviše jedanput. OBDD je dijagram odlučivanja u kojem je pored uslova da se svaka promenjiva pojavljuje isključivo jedanput duž svakog puta i da je redosled promenjivih isti duž svakog puta.

Redukovani BDD (ROBDD) je OBDD koji je redukovan sa dva pravila redukcije: pravilo brisanja i pravilo spajanja. Ovim pravilima redukcije uklanjaju se redundantnosti iz OBDD dijagrama.

Binarni dijaram odlučivanja sa potisnutim nulama (ZBDD) [3] daje jedinstvenu i kompaktnu reprezentaciju skupova. Ovom strukturom podataka je manipulisanje skupovima mnogo jednostavnije i efikasnije u odnosu na originalan BDD.

Skup elemenata p može se predstaviti n-bitnim vekotrom ($x_1, x_2, \ldots, x_n$), gde je $x_i = 1$ ukoliko je element sa indeksom i sadržan u p. Skup S može se predstaviti karakterističnom funkcijom $X_s(p): \{0,1\}^n \rightarrow \{0,1\}$ gde je $X_s(p) = 1$ ukoliko je $p \in S$ ili 0 u suprotnom. Drugačije rečeno ZBDD je BDD sa sledećim pravilima redukcije:

1. Pravilo spajanja: spoj identičnih podstabala (dobijanje kanoničnosti);

2. Pravilo potiskivanja nula: eliminacija čvorova čije je 1-potomak nulti terminalni čvor i njegova zamena nultim terminalnim čvorom.

Primenom gornjih pravila postiže se visoko kompresovanje razređenih skupova koji su predstavljeni u formi bulove funkcije

4. FBDD KRIPTOANALIZA LFSR KRIPTOSISTEMA

Kriptoanaliza protočnih kriptosistema sastoji se u određivanju tajnog ključa k koji ispunjava uslov $k_{cipher}=E(k)$, za dati niz ključeva k_{cipher} i dati algoritam šifrovanja E. Prema algoritmu kriptoanalize koji je predložio Kraus [1] problem određivanja tajnog ključa se svodi na postupak generisanja minimalnog FBDD, P koji treba da donese odluku da li k ispunjava uslov $k_{cipher}=C(L(k))$. Značajne osobine FBDD grafova je da oni mogu efikasno da se minimizuju i da omogućavaju efikasno izlistavanje.

Algoritam se sastoji od tri koraka:

- Za svako $m \geq 1$ konstruiše se minimalni FBDD Q_m koji određuje da li kompresiona funkcija $C(Z)$ za zadati binarni niz Z, $z \in \{0,1\}^m$ daje prefiks radnog ključa k_{cipher}. Zavisno od toga da li interni niz binarnih simbola generiše prefiks poznatog radnog ključa on se prihvata ili odbacuje.

- Konstrukcija minimalnih FBDD R_m, na osnovu kojih se određuje da li zadati binarni niz Z može biti generisan od strane LFSR-a. Ovi dijagrami odlučivanja uzimaju početne vrednosti LFSR generatora i na osnovu njihovih polinoma povratne sprege odredjuju da li je m-ti bit u internom nizu bitova korektan ili ne.

- Konstrukcija trećeg skupa FBDD dijagrama P_m rezultat je preklapanja Q_m i R_m. Ovim grafom se donosi odluka da li šifarski algoritam primenjen nad ulaznoj sekvenci $z \in \{0,1\}^m$ daje prefiks radnog ključa k_{cipher}.

Krausov algoritam inkrementalno odredjuje FBDD za rastući broj bitova. Kriptoanalitički napad predložen od strane Krausa je veoma efikasan u odnosu na LFSR generatore niza ključeva. Slabosti LFSR generatora pseudloslučajnih brojeva su posledica male memorije kompresora koja je rezultat pririode kriptosistema.

Operacija sinteze dijagrama ograničava veličinu konstruisanog dijagrama na sledeći način:

$$|SYNTH(P,Q)| \leq |R| \cdot |Q| \qquad (2)$$

gde je $|Q|$ veličina FBDD koji predstavlja kompresor, $|R|$ je veličina FBDD koja odredjuje da li je sekvenca dobijne upotrebom LFSR-a

Autori algoritma su objavili na osnovu odredjenih procena da je za kriptoanalitički napad na E_0 kriptosistem vremenska složenost algoritma $O(2^{81})$, dok je prostorna složenost $O(2^{77})$.

5. OBDD KRIPTOANALIZA E0 KRIPTOSISTEMA

Jedna optimizacija FBDD kriptografskog napada za odredjene specifičnosti E_0 kriptosistema predložena je od strane Shaked i Wool [4]. Oni su umesto FBDD predložili OBDD strukturu podataka kao i novi način predstavljanja nelinearne funkcije.

OBDD kriptoanalitički metod koristi pravilnosti E_0 generatora ključa, koja se ogleda u činjenici da se u toku svakog taktnog intervala u sva četiri pomeračka registra sadržaj memorijskih ćelija pomera za jedno mesto i iz svakoga od njih po jedan izlazni bit puni kompresor. Redosled promenjivih internog niza binarnih simbola izražen je u funkciji od indeksa taktnog impulsa m $(0 \le m \le 127)$ kao i indeksa pomeračkih registara $(1 \le i \le 4)$, kao $j = 4 \cdot m + i - 1$. Ovakav način indeksiranja dovodi do četiri odvojene jednačine za linearne binarne sekvence pridružene svakom od četiri pomeračka registra pojedinačno. Različite dužine pomeračkih registara iziskuju odredjena prilagodjavanja u algoritmu.

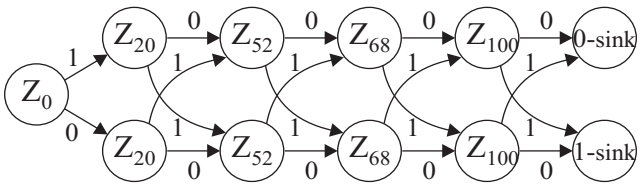
Svaki od internih bitova predstavlja izlaz jednog od LFSR registara koji je izražen u funkciji od četiri prethodna bita istog pomeračkog registra. Algoritmom se konstruiše BDD u skladu sa polinomom povratne sprege, prema kome se donosi odluka da li je interni bit z_k uskladjen sa prefiksom $\{z_j\}_{j=1}^{k-1}$. Tabela I daje pregled osnovnih jednačina konzistencije za dva načina indeksiranja pomeračkih registara. OBDD koji predstavlja relacije konzistetncije LFSR-a sadrži 5 promenjivih i 11 čvorova.

TABELA I

RELACIJE KONZISTENCIJE

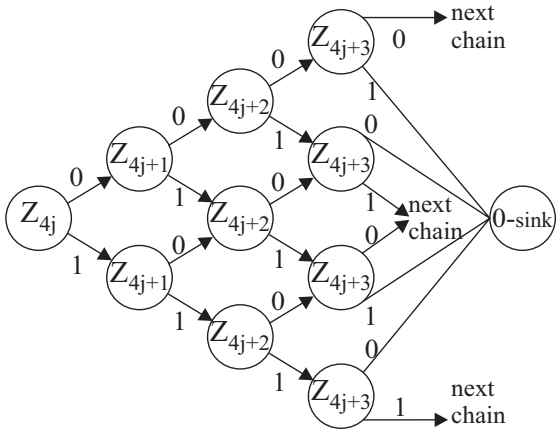
LFSR	Osnovne jednačine konzistencije
1	$z_i = z_{i-8} \oplus z_{i-12} \oplus z_{i-20} \oplus z_{i-25}$
2	$z_i = z_{i-12} \oplus z_{i-16} \oplus z_{i-24} \oplus z_{i-31}$
3	$z_i = z_{i-4} \oplus z_{i-24} \oplus z_{i-28} \oplus z_{i-33}$
4	$z_i = z_{i-4} \oplus z_{i-28} \oplus z_{i-36} \oplus z_{i-39}$
LFSR	Normalizovane jednačine konzistencije
1	$z_i = z_{i-32} \oplus z_{i-48} \oplus z_{i-80} \oplus z_{i-100}$
2	$z_i = z_{i-48} \oplus z_{i-64} \oplus z_{i-96} \oplus z_{i-124}$
3	$z_i = z_{i-16} \oplus z_{i-96} \oplus z_{i-112} \oplus z_{i-132}$
4	$z_i = z_{i-16} \oplus z_{i-112} \oplus z_{i-144} \oplus z_{i-156}$

Sledeći korak OBDD kriptografskog napada na E_0 kriptosistem je konstrukcija OBDD-a koji reprezentuje nelinearnu funkciju. Ovaj OBDD je konstruisan na osnovu prenosne funkcije kompresora i poznatog niza radnog ključa.



Sl. 3. *OBDD koji reprezentuje proveru konzistencije bita z_{100}*

Vrednost kompresorske jedinice se ažurira sumom izlaznih bitova četiri LFSR registara. Odgovarajuća BDD struktura koja predstavlja sumu četiri bita, pod nazivom osnovni lanac, ilustrovana je na slici 4. Nelinearna kompresiona funkcija predstavljena je sa 16 ovakvih identičnih podgrafova, za svako od mogućih stanja.



Sl. 4. *Dijagram "osnovnog lanca" koji reprezentuje sumu 4 bita*

Analiza složenosti algoritma sastoji se od procene veličine OBDD grafa. Veličina sintetizovanog OBDD, $|P|$ ograničena je sa dve relacije. Prvo ograničenje broja čvorova dijagrama je broj uspešnih dodela:

$$|P| \le m \cdot |One(P)| \tag{3}$$

gde je: $One(P)$ skup uspešnih dodela za BDD P, m je broj promenjivih koje su sadržane u BDD.

Drugo ograničenje je vezano za operaciju sinteze dijagrama odlučivanja:

$$|P| \le |Q(m)| \cdot 2^{m-n} \tag{4}$$

gde je: $|Q(m)|$ veličina OBDD reprezentacije nelinearne funkcije, m broji promenjivih, n veličina zadatog ključa. Ovo ograničenje pretpostavlja da je broj uvedenih OBDD čvorova tokom provere konzistentnosti LFSR dupliciran sa svakom novom promenjivom. Makismalan broj čvorova OBDD grafova konstruisanih tokom kriptografskog napada, odredjen kao presek dve granice, iznosi $|P| \approx 2^{86}$.

6. ZBDD KRIPTOANALIZA E0 KRIPTOSISTEMA

ZBDD kriptoanalitički napad na E_0 kriptosistem [5] zasnovan je na FBDD metodu, pri čemu je korišćena drugačija struktura podataka. ZBDD je varijanta BDD-a dobijena tako što je jedno od pravila redukcije dijagrama izmenjeno. Svaki put od korena grafa do završnog čvora 1 odgovara jednoj od kombinacija.

Motivacija za korišćenje ZBDD strukture podataka u kriptoanalizi se zasniva na njenoj pogodnost u predstavljanju i obradi skupova. Ova struktura podataka je posebno efikasna u manipulaciji sa skupom kombinacija, predstavljenim u formi binarnog vektora. Svaki bit u ovom vektoru označava prisustvo ili odsustvo odredjenog člana kombinacije. Skup kombinacija može se prikazati Bulovom fukcijom koja se naziva karakteristična funkcija.

Graf koji odlučuje da li niz binarnih simbola Z može da se generiše linearnim generatorom, označen sa R_m, konstruisan je korišćenjem ZBDD strukture podataka umesto do tada upotrebljavanih OBDD ili FBDD.

Struktura podataka koja predstavlja nelinearnu funkciju $C(Z)$ i odlučuje da li zadati binarni niz Z generiše prefiks radnog ključa označen je sa Q_m. Obzirom da konačni automat E_0 kriptosistema ima 16 stanja on je predstavljen četvorobtnom promenjivom q_i^n za $(1 \le i \le 3)$. Nakon učitavanja $m+1$ ulaznih simbola formira se sledeća funkcija za određivanje Q_m:

$$F\left(q_3^{m+1}, q_2^{m+1}, q_1^{m+1}, q_0^{m+1}, z_{4m+3}, z_{4m+2}, z_{4m+1}, \ldots, z_0\right)$$

Algoritam preslikava kriptoanalitčki postupak u problem manipulacije sa kombinacijama skupova. Određivanje Q_m se svodi na proveru svih mogućih kombinacija ulaznih bitova i stanja konačnog automata. Najveći broj operacija nad skupovima je definisan i implementiran ZBDD grafovima.

Broj promenjivih i broj ograničenja tokom nekih koraka algoritma je promenjiv i može se izraziti u funkciji dužine svakog pomeračkog registra, L_i for $0 \le i \le 3$. Tokom prvih $|L_0|$koraka algoritma uvode se 4 promenjive i jedno ograničenje tako da se broj uspešnih dodela umnožava sa 2^3 po taktnom intervalu. Narednih $|L_1|$ koraka izlaz prvog registra L_0 je poznat i predstavlja dodatno ograničenje tako da se u ovom slučaju broj dodela umnožava sa 2^2. Na isti način nakon sledećih $|L_2|$ koraka broj dodela se multiplicira za 2^1 po taktnom intervalu. Nakon narednih $|L_3|$ koraka broj ograničenja je jednak broju promenivih tako da broj uspešnih dodela konstantan. Ukupna vremenska kompleksnost algoritma iznosi 2^{82}, dok je prostorna kompleksnost 2^{23}.

7. ZAKLJUČAK

Rad daje sažet pregled BDD kriptografskih metoda koji su do sada publikovani. Dat je opis algoritama kao i analiza njihove složenosti.

Opisani kriptografski metodi se zasnivaju na metodu pretraživanja unazad (backtracking) [6], prema kome se formira binarno stablo pretraživanja na osnovu funkcija povratne sprege LFSR registara i nelinearne kompresione funkcije. Pokazalo se da BDD struktura podataka daje veoma dobre rezultate u kriptografskoj analizi.

Jedan od mogućih pravaca daljih istraživanja je modifikacija FDDD kriptografskog napada radi umanjenja zauzeća memorije, jer je to trenutno značajan nedostatak ovog metoda. Drugo otvoreno pitanje je kombinovanje FBDD kriptoanalitičkog napad sa drugim metodama kriptoanalize.

ZAHVALNOST

Rezultati prikazani u ovom radu ostvareni su u okviru projekta TR 11007. čiju realizaciju finansira Ministarstvo nauke Republike Srbije u periodu 2008-2010.

LITERATURA

[1] Krause, M., „*BDD-Based Cryptanalysis of Keystream Generators*“, In EUROCRYPT, Vol. 2332 of LNCS, 2002, pp. 222–237.

[2] Bryant, R. E., “*Graph-based algorithms for boolean function manipulation*“, IEEE Transactions on Computers, Vol. C-35, No. 8, Aug., 1986, pp. 677–691.

[3] Minato, S., “*Zero-suppressed BDDs and their applications*“, International Journal on Software Tools for Technology Transfer (STTT), Vol. 3, No. 2, 2001, pp. 156–170.

[4] Shaked, Y., Wool, A., “*Cryptanalysis of the Bluetooth E0 cipher using OBDD's*“, In Proceedings of 9th Information Security Conference, LNCS 4176, 2006, pp. 187–202.

[5] Ghasemzadeh, M., Meinel, Ch., Shirmohammadi, M., Shazamanian, M. H., “*ZDD-Based Cryptanalysis of E0 Keystream Generator*“, In Proceedings of 3th International Conference on Mathematical Sciences (ICM 2008), Mar., 2008.

[6] Zenner, E., Krause, M., Lucks, S.,“*Improved cryptanalysis of the self-shrinking generator*“ In V. Varadharajan and Y. Mu, editors, Australasian Conference on Information Security and Privacy ACISP'01, Lecture Notes in Computer Science, Vol. 2119, 2001, pp. 21-35.

Abstract – *This paper provides an overview of cryptanalysis methods based on the use of different variants of Binary Decision Diagram (BDD). It is cryptanalysis of stream cipher algorithms that use Linear Feedback Shift Register (LFSR), one of the most important and widely used building blocks for keystream generators. In addition to the description of the methods, the estimation of their space and time complexity is given. The paper also describes the possible directions of further development of the presented cryptanalysis attacks.*

CRYPTANALYSIS OF THE STREAM CIPHER ALGORITHMS USING BINARY DECISION DIAGRAM

Slobodan Bojanić, Srđan Đorđević