Biuletyn WAT
Vol. LX, Nr 3, 2011

Zastosowanie technik algebraicznych w kryptoanalizie różnicowej na przykładzie szyfru blokowego DES

ARKADIUSZ GĄSECKI, MICHAŁ MISZTAL

Wojskowa Akademia Techniczna, Wydział Cybernetyki,
Instytut Matematyki i Kryptologii, 00-908 Warszawa, ul. S. Kaliskiego 2
email: agasecki@wat.edu.pl; mmisztal@wat.edu.pl

Streszczenie. Artykuł omawia nowy sposób ataku na szyfr blokowy DES. Zaprezentowany pomysł polega na połączeniu dwóch znanych metod kryptoanalizy, tj. kryptoanalizy różnicowej oraz ataku algebraicznego. W artykule scharakteryzowano budowę algorytmu, elementy wykorzystanych ataków oraz sposób ich połączenia. Przedstawione zostały także otrzymane wyniki oraz omówiono efekty w porównaniu z zaprezentowanymi metodami kryptoanalizy stosowanymi oddzielnie.
Słowa kluczowe: kryptologia, kryptoanaliza, szyfr blokowy, kryptoanaliza różnicowa, atak algebraiczny, SAT solver

1. Wstęp

Idea połączenia dwóch znanych metod kryptoanalizy, a mianowicie kryptoanalizy różnicowej oraz ataków algebraicznych, została pokazana w pracy *Algebraic Techniques in Differential Cryptanalysis* [1]. Zaprezentowano w niej różne sugestie kombinacji tych dwóch ataków, a także rezultaty na przykładzie algorytmu PRESENT. W dokumencie tym omówiony zostanie jeden z przedstawionych tamże ataków dla szyfru blokowego DES. W sekcji drugiej scharakteryzowany zostanie pokrótce schemat tego algorytmu. W sekcji trzeciej pokazane zostaną wykorzystane do kryptoanalizy znane ataki różnicowe. W sekcji czwartej omówione będą rezultaty znanych ataków algebraicznych na szyfr DES. Sekcja piąta poświęcona będzie

przedstawieniu idei ataku połączonego. W sekcji szóstej będą zaprezentowane otrzymane wyniki. W sekcji siódmej dokonane zostanie podsumowanie rezultatów.

2. Budowa algorytmu DES

Algorytm DES był przez wiele lat standardem szyfrowania danych. Ma on strukturę tzw. sieci Feistela. Długość bloku wejściowego wynosi 64 bity. Efektywna długość klucza wynosi 56 bitów (standardowo długość klucza wynosi 64 bity, jednak co ósmy bit jest pomijany – pierwotnie miał on służyć kontroli parzystości). Liczba rund wynosi 16. Przebieg algorytmu jest następujący:

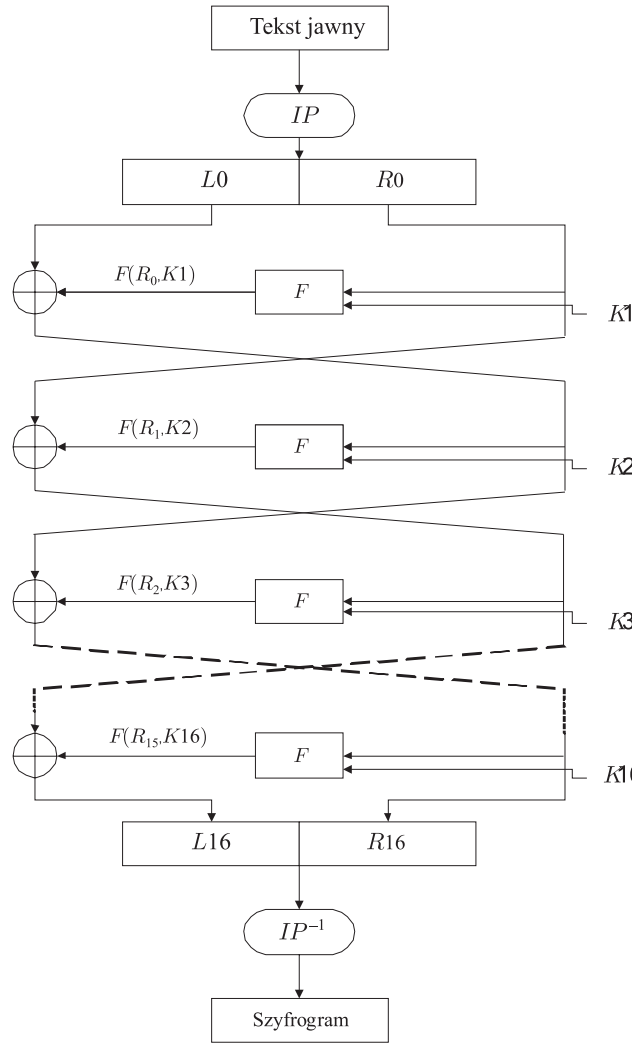
- najpierw dane poddawane są permutacji wejściowej (IP);
- następnie 16 razy powtarzana jest runda algorytmu, czyli:
  a) dane na wejściu rundy dzielone są na dwie 32-bitowe połowy – lewą L_i oraz prawą R_i;
  b) prawa połowa przechodzi przez funkcję rundy F – na tym etapie dodawany jest podklucz rundy;
  c) wynik funkcji rundy jest dodawany modulo 2 (XOR) z lewą połową;
  d) połowy są zamieniane stronami (z wyjątkiem ostatniej rundy);
- na końcu wykonywana jest odwrócona permutacja początkowa (IP^{-1}).

Deszyfrowanie jest analogiczne w stosunku do szyfrowania, z tą różnicą, że wygenerowane podklucze używane są w odwrotnej kolejności. Schemat blokowy algorytmu prezentuje rysunek 1.

Funkcja rundy algorytmu DES otrzymuje na wejściu 32 bity danych. Najpierw poddawane są one rozszerzeniu poprzez ich powielenie do 48 bitów (permutacja z rozszerzeniem). Następnie wyjście jest sumowane modulo 2 (XOR) z 48-bitowym podkluczem danej rundy.

Wynik poddawany jest operacji nieliniowej w następujący sposób:

- najpierw zostaje podzielony na 8 fragmentów 6-bitowych,
- każdy fragment jest argumentem odrębnej funkcji podstawieniowej – tzw. S-boxy,
- wyjście każdej funkcji jest czterobitowe,
- wyniki są łączone, dając w efekcie 32-bitowy rezultat,
- rezultat ten poddawany jest kolejnej permutacji.



Rys. 1. Schemat blokowy algorytmu DES

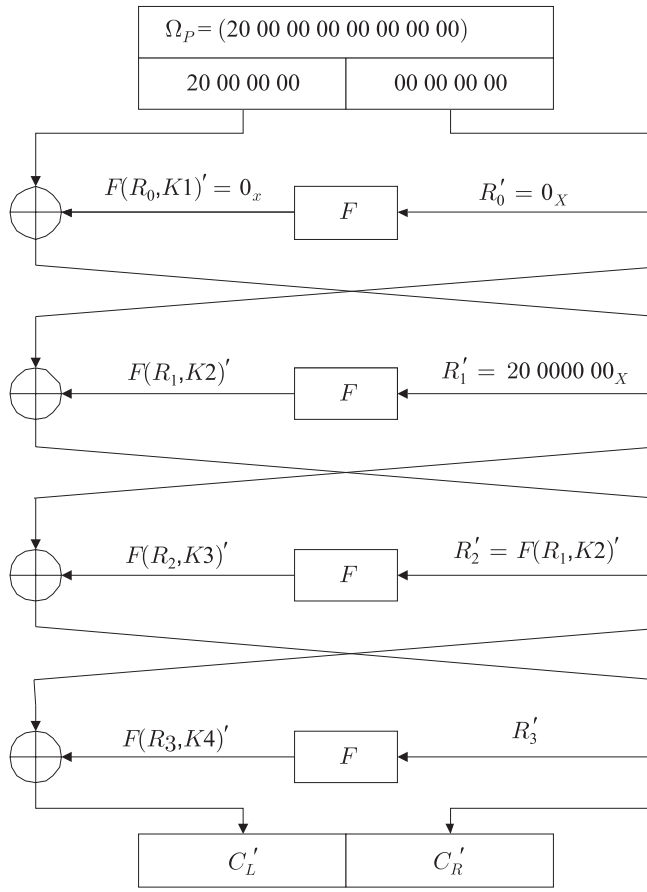
Istotą funkcji rundy są skrzynki podstawieniowe (S-boxy) – przyjmują one sześć bitów na wejściu, zaś na wyjściu rezultat jest czterobitowy.

3. Kryptoanaliza różnicowa DES

Mechanizm kryptoanalizy różnicowej algorytmu DES został po raz pierwszy opisany i upubliczniony przez E. Bihama i A. Shamira w [4].

Pokazali oni m.in. atak na DES zredukowany do czterech i sześciu rund.

Dla pierwszego przypadku wykorzystali jednorundową charakterystykę pewną, która prowadzi do przejścia różnicowego postaci zaprezentowanej na rysunku 2.



Rys. 2. Przejście różnicowe dla czterech rund DES

Na podstawie powyższego przejścia posiadamy następujące informacje:

- różnica wyjścia funkcji F z pierwszej rundy jest równa zero $R_0' = 0_X$,
- 28bitów różnicy wyjściowej z drugiej rundy $F(R_1, K2)'$ jest równe zero,
- odpowiednie bity wyjścia z rundy czwartej są równe odpowiadającym im bitom z lewej połowy różnicy szyfrogramów.

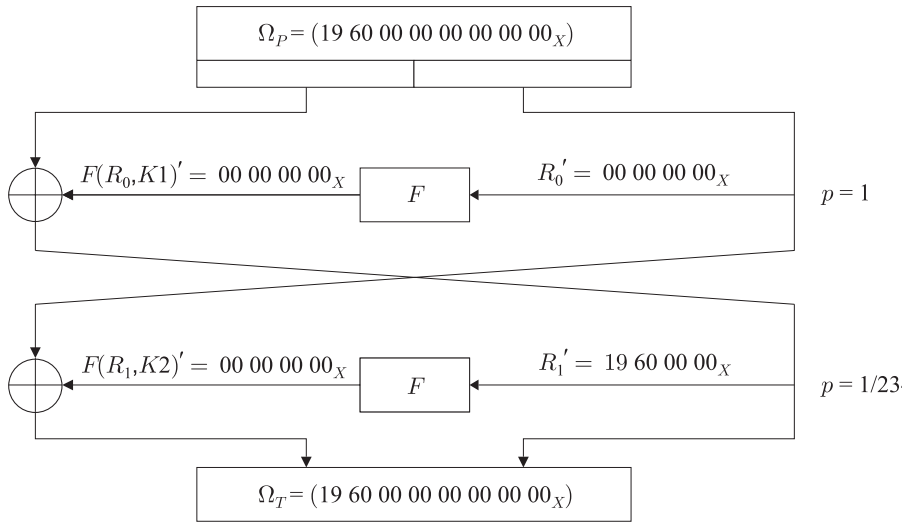
Mając taką informację, można wyznaczyć następujące wartości funkcji F w ostatniej rundzie:

– wyjście po permutacji rozszerzającej E dla obu tekstów: $S_E = E(C_R)$, $S_E^* = E(C_R^*)$
– różnicę wyjść dla siedmiu S-boxów: $S_0' = P^{-1}(F(R_3, K4)' = C_L'$,

P^{-1} oznacza odwrócenie permutacji P z funkcji rundy.

Wartości te pozwalają na wyznaczenie siedmiu części podklucza użytego w ostatniej rundzie o łącznej długości 42 bitów. Do odgadnięcia pozostanie czternaście bitów, które można wówczas znaleźć za pomocą pełnego przeszukiwania.

Alternatywą dla powyższego ataku jest atak z użyciem charakterystyki iteracyjnej, pokazanej w [4]. Jest ona zaprezentowana na rysunku 3.

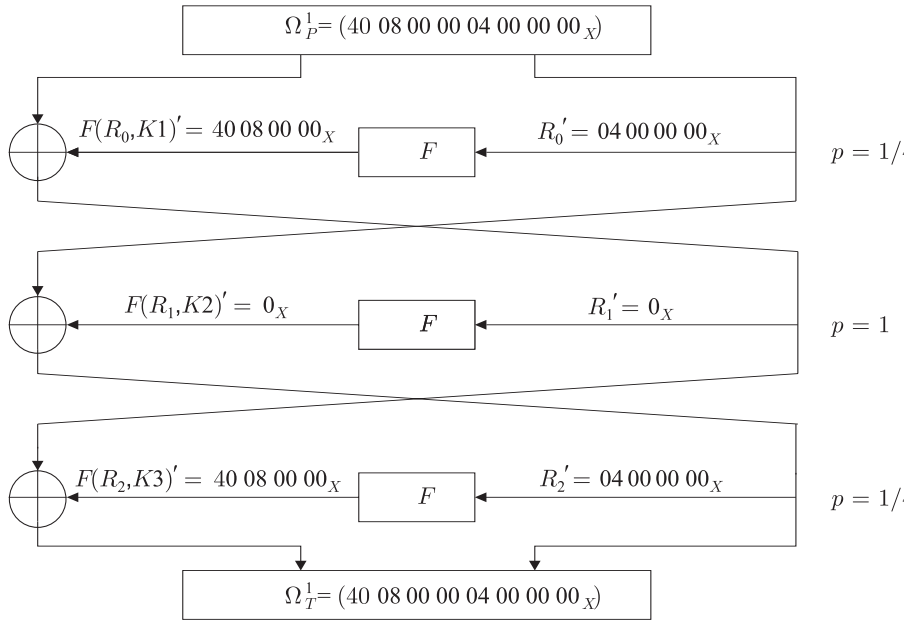


Rys. 3. Dwurundowa charakterystyka iteracyjna

Jeśli zostanie ona skonkatenowana raz ze sobą, wówczas możliwe będzie jej użycie, jednakże prawdopodobieństwo znalezienia par tekst jawny – szyfrogram, spełniających tą charakterystykę, wyniesie $(1/234)^2$.

W przypadku standardowego ataku różnicowego na sześć rund wykorzystywana jest charakterystyka pokazana na rysunku 4.

Znajduje ona zastosowanie w atakach typu 3R. Istnieje również druga, analogiczna trzyrundowa charakterystyka, o takim samym prawdopodobieństwie. Obie dają łącznie możliwość znalezienia 42 bitów klucza. W przypadku posiadania 120 prawidłowych par tekstów jawnych i szyfrogramów, szansa na znalezienie klucza wynosi 95%.



Rys. 4. Trzyrundowa charakterystyka różnicowa

4. Ataki algebraiczne na algorytm DES

Ataki algebraiczne na szyfr DES zostały przeprowadzone przez N. Courtois i G.V. Barda i opisane w [2]. Wykorzystali oni fakt równoważności wielomianowej dwóch NP-trudnych problemów. Pierwszy z nich to problem rozwiązywania układu równań wielu zmiennych, zawierających równania kwadratowe, nad ciałem $GF(2)$ (tzw. problem MQ). Drugi to problem spełnialności klauzul logicznych (SAT). Autorzy zauważyli, iż w przypadku, gdy układ równań jest rzadki i nadokreślony, wówczas techniki stosowane w SAT-solverach, programach próbujących znaleźć rozwiązania problemu SAT, pozwalają uzyskać wynik szybciej, aniżeli przy pełnym przeszukiwaniu przestrzeni rozwiązań.

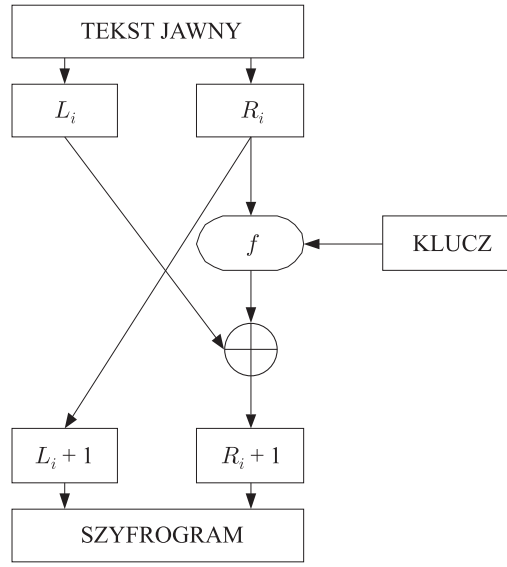
Układy równań, opisujące szyfr DES w zależności od ilości rund, dostępne są w [3]. Autorom udało się m.in. dokonać znalezienia klucza dla sześciu rund DES w ciągu 68 sekund, przy założeniu, iż znają oni 20 dowolnych bitów klucza.

5. Idea nowego ataku

Nowy rodzaj ataku na szyfry blokowe polega na połączeniu dwóch znanych już metod kryptoanalizy. Jedna z nich to przedstawiona przez

E. Bihama i A. Shamira w [4] kryptoanaliza różnicowa. Wykorzystuje ona schematy probabilistyczne – jej istota polega na przewidywaniu możliwych przejść poszczególnych bitów przez kolejne rundy algorytmu. Na tej podstawie atakujący próbuje znaleźć bity podkluczy dla określonych rund. Ta metoda wymaga znajomości dużej liczby par tekst jawny – szyfrogram. Druga metoda to atak algebraiczny. Jego zastosowanie opiera się o wykorzystanie algebraicznej struktury szyfrów. Krótko mówiąc, polega on na przedstawieniu algorytmu szyfrującego w postaci układu równań niskiego stopnia (często kwadratowych), a następnie rozwiązaniu go, by uzyskać bity klucza. Jednym z pomysłów zaprezentowanych w [1] było rozszerzenie tego ataku tak, by wykorzystać dwie pary tekst jawny – szyfrogram. Mając bowiem dwa układy równań F oraz F^* dla dwóch par (P, C) i (P^*, C^*) i tego samego klucza K, można je połączyć, otrzymując nowy układ $\bar{F} = F \cup F^*$. Do takiego układu można wprowadzić dodatkowe równania poprzez wykorzystanie zależności probabilistycznych wynikających z kryptoanalizy różnicowej. Te równania nie zwiększają ilości zmiennych w układzie, stąd oczekiwanie, iż będzie można rozwiązać go łatwiej, aniżeli układ $\bar{F}$.

W tym przypadku dokonywana jest kryptoanaliza szyfru w postaci sieci Feistela (rys. 5). Ponadto znane są dla tego szyfru charakterystyki różnicowe dla określonej liczby rund $\Omega = (\delta_0, \delta_1, \ldots, \delta_r)$, gdzie różnica w rundzie i-tej pojawi się z prawdopodobieństwem p_i. Dana charakterystyka Ω będzie więc zachodzić z prawdopodobieństwem $p = \prod p_i$.



Rys. 5. Jedna runda sieci Feistela

Każde jednorundowe przejście różnicowe wprowadza dodatkowe równania dla aktywnych S-box'ów. Poprzez $X_{i,j}$ oraz $X^*_{i,j}$ oznaczany jest j-ty bit wejścia do S-box'a w rundzie i-tej odpowiednio dla układów F oraz F^*. Analogicznie odpowiadające im bity wyjścia oznaczane są poprzez $Y_{i,j}$ oraz $Y^*_{i,j}$. Efektem są równania poniższej postaci:

$$X_{i,j} + X^*_{i,j} = X'_{i,j} \rightarrow Y'_{i,j} = Y_{i,j} + Y^*_{i,j}.$$

Wartości $X'_{i,j}$ oraz $Y'_{i,j}$ są znane na podstawie charakterystyki. Analogicznie dla nieaktywnych S-box'ów równania te przyjmą postać:

$$X_{i,j} + X^*_{i,j} = 0 = Y_{i,j} + Y^*_{i,j}.$$

Ponieważ szyfr jest w postaci sieci Feistela, więc dotyczą one tylko części bitów dla każdej rundy. Następnie należy wykorzystać równania z układu $F' = F \cup F^*$ i dodać do nich te wynikające z charakterystyki. Prowadzi to do nowego układu dającego rozwiązanie z prawdopodobieństwem $1/p$. Będzie ono z pewnością istniało, jeśli do konstrukcji równań wykorzystane zostały pary spełniające daną charakterystykę różnicową. Korzyść takiego rozwiązania jest taka, iż w przeciwieństwie do kryptoanalizy różnicowej wystarczy w tym przypadku tylko jeden dobry (tj. spełniający charakterystykę) zestaw dwóch par tekst jawny – szyfrogram. Nowo otrzymany układ powinien zaś być łatwiejszy do rozwiązania od układu F bądź F^*, gdyż wprowadzono do niego wiele nowych liniowych zależności bez dodawania żadnych nowych zmiennych.

Do przeprowadzenia ataku na algorytm DES zredukowany do czterech rund można w łatwy sposób wykorzystać dwie charakterystyki różnicowe:

- charakterystykę pewną,
- charakterystykę iteracyjną.

Obie pokazane zostały w sekcji drugiej.
W przypadku charakterystyki pewnej wystarczy znajomość dwóch par tekst jawny – szyfrogram takich, by różnica tekstów jawnych była zgodna z charakterystyką. W tym przypadku nieistotna jest różnica szyfrogramów. Użycie charakterystyki pewnej pozwala na wprowadzenie do układu dodatkowych 204 równań.

W przypadku charakterystyki iteracyjnej wymagana jest odpowiednia różnica zarówno tekstów jawnych jak i szyfrogramów. Dla czterech rund trzeba ją skonkatenować raz ze sobą, stąd zachodzi ona z prawdopodobieństwem $(1/234)^2$. Pozwala ona na dodanie 320 równań do układu.

W przypadku ataku na algorytm zredukowany do sześciu rund wykorzystuje się tą samą charakterystykę iteracyjną, co w przypadku ataku

na DES czterorundowy. W ten sposób do układu można wprowadzić dodatkowe 480 równań – na każdą rundę przypada bowiem 48 równań opisujących różnicę wejść i 32 opisujące różnicę wyjść. Prawdopodobieństwo tej charakterystyki w tym przypadku zmaleje do $(1/234)^3$, co powoduje, iż trudniej jest znaleźć parę ją spełniającą.

6. Przeprowadzenie ataku

Do rozwiązania układu równań wykorzystany został program MiniSAT, używany zasadniczo do rozwiązywania problemu spełnialności formuł logicznych. Ataki przeprowadzono na komputerze klasy PC, wyposażonym w dwurdzeniowy procesor taktowany zegarem 1.73 GHz oraz 1024 MB pamięci RAM.

Do przeprowadzenia ataku na cztery rundy użyto po cztery zestawy danych dla charakterystyki pewnej oraz charakterystyki iteracyjnej. Dla każdego zestawu danych dokonano ataku algebraicznego zwykłego oraz poszerzonego o równania wynikające z danej charakterystyki. Konwersję równań przeprowadzano dwiema metodami:

- konwersja dwumianowa, polegająca na tym, iż najpierw konwersji poddawane są wszystkie dwumiany z układu równań. Następnie konwertowane są poszczególne równania, przy czym wszelkie dwumiany w sumie zastępowane są przypisanymi wcześniej oznaczeniami.
- konwersja prosta, polegająca na sekwencyjnym konwertowaniu równań. W przypadku napotkania równania zawierającego dwumian, najpierw konwertowany jest ten dwumian, zaś następnie całe równanie.

Obie metody dają ten sam rezultat, różnica występuje tylko w kolejności zapisu klauzul logicznych. Z powodu zastosowania dwóch metod dla jednego zestawu danych dokonano łącznie czterech ataków.

Tabele 1 i 3 przedstawiają wyniki ataku z użyciem odpowiednio wybranej charakterystyki pewnej i iteracyjnej pod kątem złożoności czasowej.

Tabele 2 i 4 przedstawiają wykorzystanie pamięci przy tych atakach.

Podobnie jak w przypadku ataku na cztery rundy, do przeprowadzenia ataku na sześć rund użyto po cztery zestawy danych spełniających charakterystykę iteracyjną. Dane zostały wybrane w następujący sposób: szyfrowano dwa teksty jawne różniące się o wartość określoną przez charakterystykę, a następnie sprawdzano, czy różnica szyfrogramów także jest zgodna z charakterystyką.

Dla każdego zestawu danych dokonano próby ataku algebraicznego zwykłego oraz poszerzonego o równania wynikające z charakterystyki. Konwersję równań przeprowadzano dwiema metodami. Stąd dla jednego zestawu danych dokonano łącznie próby czterech ataków.

Tabela 1

Zestawienie czasowe ataków na cztery rundy DES – charakterystyka pewna

	Atak zwykły		Atak poszerzony	
Numer zestawu	Konwersja dwumianowa	Konwersja prosta	Konwersja dwumianowa	Konwersja prosta
1	59,45 s	4,50 s	0,43 s	0,58 s
2	157,93 s	33,60 s	1,15 s	4,43 s
3	6,12 s	8,03 s	0,35 s	0,24 s
4	5,17 s	22,21 s	0,42 s	0,40 s

Tabela 2

Wykorzystanie pamięci przy atakach na cztery rundy DES – charakterystyka pewna

	Atak zwykły		Atak poszerzony	
Numer zestawu	Konwersja dwumianowa	Konwersja prosta	Konwersja dwumianowa	Konwersja prosta
1	7,13 MB	5,37 MB	3,22 MB	3,20 MB
2	8,56 MB	6,82 MB	3,47 MB	5,04 MB
3	5,47 MB	5,50 MB	3,09 MB	3,09 MB
4	5,15 MB	6,30 MB	3,22 MB	3,23 MB

Tabela 3

Zestawienie czasowe ataków na cztery rundy DES – charakterystyka iteracyjna

	Atak zwykły		Atak poszerzony	
Numer zestawu	Konwersja dwumianowa	Konwersja prosta	Konwersja dwumianowa	Konwersja prosta
1	29,68 s	20,24 s	0,96 s	0,82 s
2	19,31 s	381,46 s	0,33 s	0,38 s
3	76,97 s	6,57 s	12,21 s	0,11 s
4	22,24 s	60,99 s	29,08 s	105,04 s

Tabela 4

Wykorzystanie pamięci przy atakach na cztery rundy DES – charakterystyka iteracyjna

	Atak zwykły		Atak poszerzony	
Numer zestawu	Konwersja dwumianowa	Konwersja prosta	Konwersja dwumianowa	Konwersja prosta
1	6,52 MB	6,11 MB	3,62 MB	3,48 MB
2	6,26 MB	11,02 MB	3,11 MB	3,22 MB
3	7,62 MB	5,32 MB	5,64 MB	2,94 MB
4	6,13 MB	7,32 MB	6,62 MB	7,75 MB

W przypadku ataku zwykłego próby znalezienia rozwiązania, niezależnie od zestawu danych i sposobu konwersji, przekraczały czas 1000 s. Dlatego też wyniki dla tej metody zostały pominięte. Rezultaty prezentuje tabela 5.

TABELA 5

Wyniki ataku na sześć rund DES

	Konwersja dwumianowa		Konwersja prosta	
Numer zestawu	Czas	Pamięć	Czas	Pamięć
1	387,35 s	13,98 MB	16,66 s	8,46 MB
2	–	–	–	–
3	219,59 s	12,53 MB	218,99 s	14,02 MB
4	638,35 s	16,06 MB	100,13 s	10,98 MB

Tabela 6 pokazuje wyniki poszerzonego ataku na sześć rund. Rozszerzenie polegało na użyciu do ataku nie dwóch, lecz czterech par. Zastosowane zostały te same zestawy danych, zagregowane w dwa nowe.

TABELA 6

Wyniki rozszerzonego ataku na sześć rund DES

	Konwersja dwumianowa		Konwersja prosta	
Numer zestawu	Czas	Pamięć	Czas	Pamięć
1+2	125,70 s	21,56 MB	99,21 s	17,51 MB
3+4	36,41 s	11,10 MB	46,54 s	13,41 MB

7. Podsumowanie

Zaprezentowany atak pokazał możliwość rozszerzenia zwykłego ataku algebraicznego. Jednakże bardziej istotny jest tu fakt, iż opiera się on o kryptoanalizę różnicową. Dodatkowe równania są tu bowiem wprowadzane na podstawie charakterystyk różnicowych. Przy porównaniu zwykłej kryptoanalizy różnicowej z zaprezentowanym atakiem widać, iż ma on w stosunku do niej jedną zaletę – wymagana ilość par spełniających charakterystykę. Dla czterech rund wystarczy jedna taka para, by znacznie przyspieszyć atak. Dla sześciu rund pokazano, iż wystarczające są dwie pary. Przy zestawieniu tego rezultatu z wymaganymi 160 parami dla kryptoanalizy różnicowej widać, iż przewaga jest znaczna.

Przy zestawieniu zaprezentowanego ataku z próbami zwykłego ataku algebraicznego widoczne są dwie różnice. Na niekorzyść dla zmodyfikowanej metody przemawia fakt, iż wymagane dane muszą spełniać określone własności. W zwykłym ataku algebraicznym wystarczy dowolny tekst jawny

i odpowiadający mu szyfrogram. Pod kątem złożoności czasowej lepiej prezentuje się jednakże nowy sposób. Widać to zwłaszcza na przykładzie ataku na sześć rund, gdzie zwykłe ataki algebraiczne musiały zostać pominięte ze względu na zbyt długi czas oczekiwania na rozwiązanie układu równań. Ciekawie pod tym względem zaprezentowały się również wyniki dla czterech rund z charakterystyką pewną, gdyż w tym przypadku czas potrzebny na znalezienie rozwiązania był w każdym przypadku zdecydowanie lepszy dla ataku poszerzonego. Jednocześnie wymagania na posiadane dane nie były zbyt skomplikowane – istotna była tylko różnica tekstów jawnych.

Podsumowując, przedstawione wyniki pokazują, iż „połączenie sił" kryptoanalizy różnicowej i ataków algebraicznych może przynieść korzyść w postaci efektywniejszej kryptoanalizy, zarówno pod względem złożoności czasowej jak i ilości wymaganych danych. Dają one także wstęp do rozwijania idei łączenia różnych metod ataków.

Praca naukowa finansowana ze środków na naukę w latach 2009-2011 jako projekt rozwojowy Nr O R00 0043 07.

Artykuł wpłynął do redakcji w dniu 07.02.2011 r. Zweryfikowaną wersję po recenzji otrzymano w maju 2011 r.

LITERATURA

[1] M. Albrecht, C. Cid, *Algebraic Techniques in Differential Cryptanalysis*, IACR Cryptology ePrint Archive, Report 2008/177.

[2] N.T. Courtois, G.V. Bard, *Algebraic Cryptanalysis of the Data Encryption Standard*, IACR Cryptology ePrint Archive, Report 2006/402.

[3] N.T. Courtois, *Examples of equations generated for experiments with algebraic cryptanalysis of DES*, http://www.cryptosystem.net/aes/toyciphers.html

[4] E. Biham, A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, Journal of Cryptology, IACR, 1991.

A. GĄSECKI, M. MISZTAL

Application of algebraic techniques in differential cryptanalysis against block cipher DES

Abstract. Article describes a new method of cryptanalysis of block cipher DES. Presented idea combines two, already known techniques, namely differential cryptanalysis and algebraic attacks. The article covers a description of the block cipher DES, used elements of attacks and the way of their combination. Then, comes the presentation of the results and comparison with already known techniques of cryptanalysis, but used separately.

Keywords: cryptology, cryptanalysis, block cipher, differential cryptanalysis, algebraic attack, SAT solver