mgr inż. Arkadiusz Gąsecki
Wojskowa Akademia Techniczna
Instytut Matematyki i Kryptologii

Zastosowanie elementów kryptoanalizy liniowej w ataku algebraicznym na zredukowany szyfr DES

Idea połączenia dwóch znanych metod ataków na szyfr pojawiała się niejednokrotnie, niemniej dotychczas nie cieszyła się popularnością. Celem referatu jest prezentacja możliwości, jakie niesie wykorzystanie dwóch znanych technik kryptoanalizy, mianowicie kryptoanalizy liniowej oraz ataku algebraicznego. Szyfrem, jaki został wykorzystany do badań, jest algorytm DES, zredukowany do czterech rund. Dotychczas obie metody kryptoanalityczne były stosowane niezależnie, natomiast przedstawione podejście zakłada ich połączenie. Atak polegał na poszerzeniu równań opisujących algebraiczną strukturę szyfru o równanie wynikające z charakterystyki liniowej. Następnie, równania te zostały przekonwertowane do postaci, możliwej do rozwiązania za pomocą SAT-solvera. W tym przypadku użyto programu MiniSAT. Oczekiwanym rezultatem było przyspieszenie rozwiązywania układu równań, a co za tym idzie, znalezienie klucza użytego do zaszyfrowania tekstu jawnego. Tak przeprowadzony atak jest atakiem ze znanym tekstem jawnym, gdyż nie wiadomo a priori, czy dana para tekst jawny–szyfrogram spełnia równanie opisane poprzez charakterystykę liniową. Prawdopodobieństwo istnienia rozwiązania układu równań jest równe prawdopodobieństwu spełnienia ww. równania.

Drugim sposobem zwiększenia skuteczności kryptoanalizy jest połączenie układów opisujących więcej niż jedną parę w postaci: tekst jawny–szyfrogram. Z uwagi na fakt, iż każdy z tych układów zawiera opisane te same zmienne klucza, to tak rozszerzony układ będzie posiadał odpowiednio więcej równań, ale już mniej zmiennych do odszukania. Stąd oczekiwanie, iż taki rozszerzony układ będzie można rozwiązać łatwiej, niż każdy z układów osobno. Dodanie równań wynikających z charakterystyki liniowej ma wówczas jeszcze bardziej przyspieszyć rozwiązywanie układu, za cenę zmniejszenia prawdopodobieństwa jego znalezienia. Celem odczytu jest przedstawienie nie tylko metody odszukiwania klucza, wykorzystywanego do zaszyfrowania danych, ale również zależności pomiędzy liczbą znanych tekstów jawnych, czasem potrzebnym do rozwiązania układu a prawdopodobieństwem istnienia jego rozwiązania.