STRESZCZENIE ROZPRAWY DOKTORSKIEJ

Metody zautomatyzowanego poszukiwania charakterystyk różnicowych w odniesieniu do kryptoanalizy szyfrów blokowych

mgr inż. Władysław Dudzic

W rozprawie doktorskiej skupiono się przede wszystkim na kryptoanalizie różnicowej i automatyzacji procesu mającego na celu określenie podatności algorytmu na ataki z tej grupy. W pracy zaproponowano zautomatyzowaną metodę poszukiwania optymalnych charakterystyk różnicowych (pod kątem minimalnej liczby aktywnych skrzynek podstawieniowych lub maksymalnej wartości prawdopodobieństwa) oraz zautomatyzowaną metodę poszukiwania charakterystyk różnicowych obciętych przydatnych z punktu widzenia adwersarza. Zaproponowane metody do reprezentacji modelu opisującego propagację odpowiednio charakterystyki różnicowej lub charakterystyki różnicowej obciętej wykorzystują grafy `AIG`. Sam model generowany jest na podstawie implementacji funkcji wyznaczającej prawdopodobieństwo zadanej charakterystyki różnicowej (na potrzeby badań wykonywanej w języku funkcyjnym `Cryptol`). Graf `AIG` reprezentujący to przekształcenie poddawany jest redukcji funkcjonalnej, a następnie na potrzeby wyznaczenia konkretnej postaci charakterystyki, konwertowany do problemu `SAT`, w którym zmienne reprezentujące charakterystykę różnicową traktowane są jako zbiór niewiadomych.

Podczas przeprowadzonych badań wykazano, że dzięki zaproponowanemu podejściu można efektywnie poszukiwać charakterystyk różnicowych. Wykazano, że wydajność wykonanego w ramach rozprawy oprogramowania jest zdecydowanie wyższa niż w przypadku ogólnodostępnego narzędzia `CryptoSMT`. Testy wykonywano na szyfrach blokowych: `AES`, `KLEIN`, `MIDORI`, `PRESENT`, `SPECK`, `SIMON`, `PYJAMASK` oraz `SATURNIN`. Ponadto scharakteryzowano własności modeli `SAT` (reprezentowanych jako zbiór klauzul w postaci `CNF`), które według oceny autora mają wpływ na czas rozwiązania problemu. W pracy wskazano również szereg nieznanych dotąd w literaturze charakterystyk różnicowych, wyznaczonych za pomocą zaproponowanej metody (m.in. optymalną pod względem maksymalnej wartości prawdopodobieństwa charakterystykę różnicową na 5 rund szyfru blokowego `AES` oraz na 10 rund szyfru blokowego `SPECK` ze 128 bitowym blokiem danych, optymalną pod względem minimalnej liczby aktywnych skrzynek podstawieniowych charakterystykę różnicową na 14 rund szyfru blokowego `AES`). W podsumowaniu przeprowadzonych badań wskazano także wybrane przez autora perspektywiczne kierunki dalszego rozwoju opracowanych metod.

Słowa kluczowe: kryptoanaliza różnicowa, charakterystyka różnicowa, charakterystyka różnicowa obcięta, szyfry blokowe, grafy `AIG`, `SAT` solvers.