Streszczenie

Kryptograficzna funkcja haszująca jest odwzorowaniem z przestrzeni łańcuchów binarnych dowolnej długości w zbiór łańcuchów binarnych określonej długości. Spełnia ona dodatkowe założenia bezpieczeństwa gwarantujące, że nie spowoduje osłabienia algorytmu kryptograficznego, w którym zostanie użyta. Przykładowymi zastosowaniami kryptograficznych funkcji haszujących są podpisy cyfrowe oraz kody uwierzytelniania wiadomości. W rozprawie analizowane są kryptograficzne funkcje haszujące oraz omówione są główne zasady tworzenia bezpiecznych kryptograficznych funkcji haszujących.

Badamy zagadnienie konstruowania funkcji haszujących przy pomocy szyfrów blokowych oraz własności innych konstrukcji używanych do budowania funkcji kompresji. Pokazujemy jak zbudować rozróżniacze różnicowe z kluczem jawnym dla mCrypton, Hierocrypt-3, SAFER++ oraz Square. Nasz atak na SAFER++ jest pierwszym przykładem ataku „rebound" ze standardowymi różnicami. Pokazujemy ograniczenie dolne na złożoność wyszukiwania pary różnicowej dla ścieżki skróconych różnic w permutacji losowej, co pokazuje efektywność zaproponowanych rozróżniaczy. Wyniki naszej analizy świadczą o tym, że szyfry blokowe używane do budowy funkcji haszujących, powinny być również analizowane pod kątem kryptoanalizy z kluczem jawnym, w celu utrudnienia wyszukiwania kolizji.

Analizujemy funkcje haszujące oparte na szyfrze `IDEA` w kilku trybach. Demonstrujemy praktyczne algorytmy wyszukiwania kolizji i słabych kolizji wykorzystując słabe klucze `IDEA` oraz nową własność tego szyfru. Pokazujemy, że użycie szyfru, uważanego za bezpieczny w modelu z niejawnym kluczem, powinno być dokładnie przeanalizowane w przypadku rozmaitych trybów konstrukcji funkcji haszujących.

Streszczenie

Rozwijamy badania wykorzystujące analizę rotacyjną. Pokazujemy w jaki sposób rozszerzyć jej zastosowanie w przypadku najczęściej wykorzystywanych operacji takich jak: odejmowanie, przesunięcia, funkcje Boolowskie na łańcuchach bitów, wielokrotne dodawania i odejmowania. W szczególności podajemy wzory na prawdopodobieństwo zachowania własności rotacyjnej w przypadku wielokrotnych dodawań i odejmowań. Rozpatrujemy S-funkcje oraz ich zastosowania w kontekście analizy rotacyjnej. Nasze wyniki stosujemy do analizy BMW i SIMD. Proponujemy również nową analizę przesunięć i stosujemy ją do Shabal.

Wprowadzamy łańcuchy dodawań w kontekście analizy rotacyjnej. Pokazujemy, że założenia obowiązujące dla szyfrów Markowa nie zawsze mogą być używane i przypadku analizy rotacyjnej prawdopodobieństwo zachowania rotacji zależy nie tylko od ilości dodawań ale również od ich położenia w konstrukcji ARX. Podajemy dokładne wzory dla tych prawdopodobieństw, które stosujemy w analizie `BLAKE2`, `Skein` i SIMD.