Michał Misztal
Wojskowa Akademia Techniczna, Wydział Cybernetyki
Instytut Matematyki i Kryptologii
E-mail: mmisztal@wat.edu.pl

Kryptoanaliza różnicowa szyfru PP-1

W artykule zaprezentowano atak różnicowy na szyfr blokowy PP-1 zaprojektowany na Politechnice Poznańskiej. Złożoność tego ataku jest mniejsza od złożoności ataku brutalnego dla szyfru o dowolnej długości bloku. Atak opiera się na fakcie, że w projekcie szyfru wybrano S-blok niezależnie od permutacji. Zastosowana permutacja operuje na pojedynczych bitach, a w tablicy rozkładu różnic S-bloku (XOR profilu) możliwe są przejścia jeden bit na jeden bit. Umożliwia to skonstruowanie prostej jednorundowej charakterystyki prawie iteracyjnej z prawdopodobieństwem $1.5 \cdot 2^{-6}$. 9-krotne powtórzenie tej charakterystyki i jej „rozluźnienie" w ostatniej rundzie daje 10-rundową charakterystykę z prawdopodobieństwem $2^{-48.7}$. Zastosowanie tej charakterystyki w ataku 1R umożliwia atak różnicowy na wszystkie 11 rund szyfru o złożoności mniejszej od ataku brutalnego. Odpowiednie wykorzystanie podobnych charakterystyk umożliwia analogiczny atak na szyfr w wersjach z większą liczbą rund.

Słowa kluczowe: kryptoanaliza różnicowa, szyfr blokowy PP-1.