# Problem wyszukiwania kostek w kontekście kryptoanalizy szyfrów blokowych

Marcin Dawiec

**Promotor**

dr hab. inż. Andrzej Paszkiewicz, prof. WAT

**Promotor pomocniczy**

dr inż. Michał Misztal

W rozprawie przedstawiono propozycję rozwiązania problemu poszukiwania kostek, który jest istotny z punktu widzenia metod kryptoanalizy wykorzystujących kostki, takich jak:

- atak za pomocą kostek (ang. *cube attack*);
- testy za pomocą kostek (ang. *cube testers*);
- atak za pomocą dynamicznych kostek (ang. *dynamic cube attack*);
- atak za pomocą warunkowych kostek (ang. *conditional cube attack*);
- ataki typu *cube-like* (ang. *cube-like attack*).

Poszukiwanie kostek jest problemem wspólnym dla wszystkich wymienionych powyżej ataków oraz zwykle jest to najbardziej czasochłonny etap ich realizacji. W literaturze najbardziej rozpowszechnionym sposobem wyszukiwania kostek jest metoda oparta na idei błądzenia losowego. Jej zaletą jest możliwość aplikacji dla algorytmów o nieznanej budowie. Jednakże zgodnie z zasadą Kerckhoffsa bezpieczeństwa szyfru nie można opierać na nieznajomości jego specyfikacji. Stąd powstało pytanie, czy wiedza na temat konstrukcji atakowanego algorytmu może być przydatna w kontekście poszukiwania kostek.

W rozprawie przedstawiono propozycję sposobu poszukiwania kostek, w którym wykorzystując wiedzę o atakowanym algorytmie można budować zbiór $\mathscr{R}$ zawierający wszystkie kostki. Zbiór ten może zawierać elementy, które nie są kostkami, ale z pewnością będzie zawierał wszystkie kostki. Ograniczenie przestrzeni, w której poszukiwane są kostki powoduje, w porównaniu do metody błądzenia losowego, zwiększenie skuteczności znajdowania kostek. Tym samym prowadzi to do zmniejszenia złożoności obliczeniowej fazy wstępnej (w której

poszukiwane są kostki) ataków wykorzystujących kostki. Ograniczenie przestrzeni możliwych kostek osiąga się poprzez budowanie postaci ANF zredukowanych wielomianów głównych. W przypadku szyfrów blokowych są nimi funkcje boolowskie bitów bloku danych i bitów klucza. W rozprawie przedstawiono sposób budowania tych wielomianów dla szyfrów blokowych oraz metodę tworzenia zbioru $\mathscr{R}$.

Zaproponowaną w dysertacji metodę zastosowano do ataku na składający się z 5 rund algorytm blokowy CTC o 120-bitowym bloku danych i kluczu. Wcześniejszy najlepszy znany atak wykorzystujący kostki przeprowadzany był dla 4 rund szyfru. Na potrzeby ataku kostek poszukiwano za pomocą metody losowej i opartej na analizie zredukowanych wielomianów głównych. Zastosowanie metody losowej okazało się nieskuteczne — przy jej pomocy nie znaleziono żadnej kostki, natomiast druga metody pozwoliła na znalezienie 120 kostek — wystarczającej liczby do odkrycia klucza.