Michał Glet
Wojskowa Akademia Techniczna
Instytut Matematyki i Kryptologii

Analiza metod projektowania funkcji skrótu oraz możliwości zastosowania w projekcie przekształceń trójkątnych

Przekształcenia trójkątne przedstawiają nowe metody znajdowania i analizowania pewnych szczególnych przekształceń matematycznych, posiadających niezwykle istotne cechy z punktu widzenia kryptologa. Przykładem może być przekształcenie o własności pojedynczego cyklu, multipermutacja czy też kwadrat łaciński. W związku z tym przekształcenia trójkątne z powodzeniem mogą stanowić alternatywę dla obecnie używanych prymitywów kryptograficznych, takich jak LFSR'y. Można je również wykorzystać do konstrukcji funkcji kompresji w funkcjach skrótu.

Referat przedstawia i analizuje możliwości zastosowania przekształceń trójkątnych do budowy nowych funkcji skrótu i prezentuje przykładową, autorską konstrukcję bazującą na schemacie MD i multipermutacjach. Przedstawiona konstrukcja, prócz teoretycznego bezpieczeństwa, zapewnia duże możliwości równoległego przetwarzania obliczeń.