dr inż. Piotr Bora
Wojskowa Akademia Techniczna
Wydział Cybernetyki
Instytut Matematyki i Kryptologii

Możliwości implementacyjne wybranych algorytmów strumieniowych trzeciej fazy projektu ECRYPT

Dobre algorytmy szyfrowania danych powinny również spełniać kryteria wykonywalności praktycznej. Poważnym problemem jest, jeśli opracowany algorytm nie może uzyskać w danym rozwiązaniu programowym lub sprzętowym wymaganej przez nas szybkości przetwarzania.

W przedstawionym komunikacie pokazane zostanie zbiorcze podsumowanie szybkości przetwarzania algorytmów zakwalifikowanych do trzeciej fazy projektu ECRYPT. Algorytmy te zostały podzielone na dwie grupy: przeznaczone do realizacji programowych oraz przeznaczone do realizacji układowych. Jednak, jak to w życiu często bywa, rozbudowane systemy kryptograficzne wymagają użycia algorytmów, które są dobrze implementowane w postaci programu, jak i na bramkach i przerzutnikach.

Analizy obejmować będą wybrane algorytmy. Przedstawione podsumowanie obejmować będzie rozwiązania realizowane w oparciu o struktury programowalne FPGA. Są to struktury coraz powszechniej stosowane w urządzeniach zarówno szyfrujących, jak i przetwarzających duże ilości danych. Umożliwiają one uzyskanie dużej uniwersalności i reprogramowalności sprzętu, a także bezpieczeństwa własności intelektualnej.