mgr inż. Wojciech Powiertowski
mgr inż. Jan Szuster
mgr inż. Maciej Kaczkowski
Transbit sp. z o.o.

Moduł kryptograficzny w zastosowaniach w telefonie AC-16SCIP oraz urządzeniu IPSec

Na potrzeby systemów SCIP oraz IPSec firma Transbit przy współpracy z WAT i prof. Jerzym Gawineckim zaprojektowała moduł sprzętowy (MKT) pozwalający na bezpieczne oraz odseparowane od warstwy oprogramowania wykonywanie zadań kryptograficznych. Moduł MKT pozwala na wydajne przeprowadzanie operacji matematycznych niezbędnych dla realizacji różnych zadań kryptograficznych, takich jak np. generacja danych losowych bazujących na szumie fizycznym, generacja liczb pierwszych dla algorytmu RSA, wykonywanie operacji potęgowania modularnego wykorzystując arytmetykę Montgomery'ego, oraz obliczanie krotności punktu na krzywych eliptycznych w celu zastosowania algorytmu ECDH.

Do tej pory moduł MKT został wykorzystany w telefonie AC-16SCIP, który jest wysiłkiem projektu badawczo-rozwojowego OR00006907 realizowanego wspólnie z WAT pod kierownictwem prof. Gawineckiego. Protokół SCIP (Secure Communication Interoperability Protocol) jest koalicyjnym (NATO) protokołem bezpiecznej komunikacji w relacji „end-to-end". Technologia ta może być wykorzystana w sieciach telefonii komórkowej, ISDN, PSTN, VoIP oraz radiostacjach, ponadto może służyć do ochrony zarówno połączeń głosowych jak i transmisji danych.

Moduł MKT w innej konfiguracji jest również wykorzystywany w projektowanym urządzeniu IPSec, realizującym bezpieczny transfer danych w sieciach IP. W urządzeniu IPSec moduł odpowiedzialny jest między innymi za realizację szyfrowania symetrycznego (szyfrowanie i deszyfrowanie AES oraz uwierzytelnianie SHA-2) oraz asymetrycznego (wsparcie dla operacji RSA). Dzięki swojej konstrukcji moduł MKT pozwala na osiągnięcie wydajności pracy trudnej do realizacji przez rozwiązania programowe.

Moduł MKT oparty został o matrycę FPGA i pozwala na osiąganie wysokich wydajności wszystkich funkcji kryptograficznych, przy jednoczesnym zapewnieniu wysokiego poziomu bezpieczeństwa, w tym ochrony danych wrażliwych przed nieuprawnionym dostępem czy ochroną układu przed penetracją. Szczelna konstrukcja modułu MKT zapewnia również ochronę elektromagnetyczną oraz środowiskową spełniając wojskowe normy klimatyczne i mechaniczne.