dr inż. Piotr Bora
mgr inż. Tomasz Kijko
Wojskowa Akademia Techniczna, Wydział Cybernetyki
Instytut Matematyki i Kryptologii
E-mail: {pbora,tkijko}@wat.edu.pl

System klucza publicznego oparty na krzywych eliptycznych

W referacie przedstawione zostanie przykładowe rozwiązanie systemu klucza publicznego zbudowanego w oparciu o krzywe eliptyczne nad ciałem $GF(2^n)$. Przykład obejmuje sposób wyznaczania krzywych eliptycznych spełniających warunki bezpieczeństwa oraz metody wykonywania szybkich obliczeń krotności punktów na krzywej. Jako platformę sprzętową wybrano strukturę FPGA firmy Altera z rodziny STRATIX II.