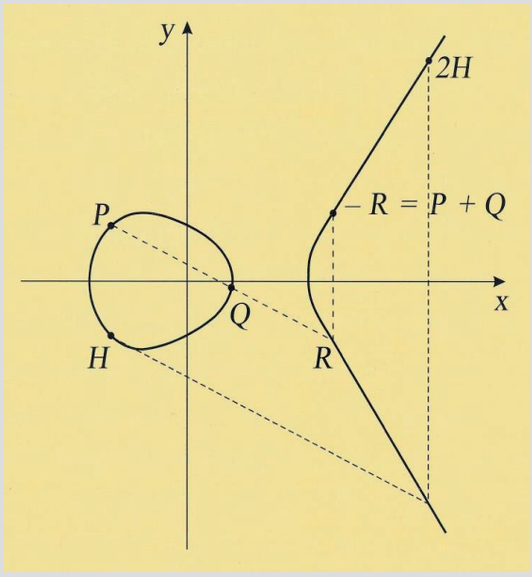
GENERATOR KOPROCESORA KRYPTOGRAFICZNEGO OPERUJĄCEGO NA ELEMENTACH Z CIAŁA GF(2N)

Urządzenie jest rezultatem projektu rozwojowego Nr O R00 0043 07 pt. „Demonstrator technologii generatora koprocesora kryptograficznego operującego na elementach z ciała GF(2n)" (29.06.2009 – 29.06.2011) zrealizowanego w ramach konsorcjum Nauki i Przemysłu Wojskowej Akademii Technicznej i firmy WASKO S.A. Generator stanowi unikalne narzędzie wspomagające projektanta systemów kryptograficznych z zakresu projektowania implementacji rozwiązań klucza publicznego na krzywych eliptycznych oraz do wytwarzania implementacji systemów kryptograficznych dla struktur FPGA i ASIC wykonujących obliczenia na krzywych eliptycznych projektowanych systemów. Generator ma strategiczne znaczenie dla przyśpieszania konstrukcji nowych rozwiązań klucza publicznego opartego na elementach z ciała charakterystyki 2. Aplikacja generatora jest unikalnym w skali światowej rozwiązaniem. Umożliwia generowanie kodu w języku opisu sprzętu VHDL oraz AHDL, definiującego strukturę jądra kryptograficznego. Innowacją jest to, że skonstruowane wzorcowe rozwiązanie oprócz tego, że jest najmniejsze, to umożliwia obliczenia dla dowolnego wielomianu pierwotnego danego stopnia bez zmiany koprocesora. Następną innowacją jest fakt, że wykazano możliwość dekompozycji układu mnożącego w sposób niespotykany dotychczas w literaturze światowej. Udowodniono również, że rozwiązanie jest zabezpieczone także przed atakiem poboru mocy.

Urządzenie zostało wyróżnione:

- Brązowym medalem na 111. Międzynarodowych Targach Wynalazczości „Concurs Lepine", Paryż 2012.
- Złotym Medalem na 61. Międzynarodowych Targach Wynalazczości Badań Naukowych i Nowych Technik BRUSSELS INNOVA, Bruksela 15-17.11.2012.
- Dyplomem Ministra Nauki i Szkolnictwa Wyższego na Giełdzie Wynalazków Nagrodzonych na Światowych Wystawach Wynalazczości w 2012 roku, Warszawa 5-7.02.2013.



Kierownik projektu: prof. dr hab. n. mat. inż. Jerzy August Gawinecki – dyrektor Instytutu Matematyki i Kryptologii, Wydział Cybernetyki WAT

Wydział Cybernetyki
Instytut Matematyki i Kryptologii
Piotr Kacprzyk
tel. +48 22 683 95 56
e-mail: pkacprzyk@wat.edu.pl