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

Wspomaganie obliczeń dla systemów klucza publicznego opartych o teorię krzywych hipereliptycznych

W referacie przedstawiona będzie koncepcja wspomagania układowego obliczeń niezbędnych dla realizacji systemów klucza publicznego opartych o teorię krzywych hiperelitycznych.

Obecnie w wielu zastosowaniach informatyki, elektroniki i telekomunikacji wykorzystywane są systemy kryptograficzne asymetryczne. Opierają się one o problemy trudne obliczeniowo, takie jak faktoryzacja dużych liczb, logarytm dyskretny w grupie multiplikatywnej ciała skończonego, logarytm dyskretny w grupie punktów krzywej eliptycznej czy też jakobian krzywej hipereliptycznej. Zainteresowanie krzywymi eliptycznymi i hipereliptycznymi wynika z faktu, że oparte o nie kryptosystemy są w stanie zagwarantować podobny poziom bezpieczeństwa jak np. systemy oparte o problem faktoryzacji przy znacznie krótszych kluczach. Istotną sprawą w kontekście praktycznych zastosowań jest efektywna implementacja kryptosystemu, zarówno programowa jak i sprzętowa. Celem autorów było przedstawienie koprocesora wspomagającego sprzętową realizację operacji dodawania dywizorów w jakobianie krzywej hipereliptycznej genusu g nad ciałem $GF(2^n)$ danej równaniem:

$$C \ : \ y^2 + h(x)y = f(x),$$

gdzie $h(x) \in GF(2^n)$ jest wielomianem stopnia co najwyżej g, a $f(x) \in GF(2^n)$ jest monicznym wielomianem stopnia $2g + 1$. Dodatkowo nie istnieją rozwiązania spełniające jednocześnie równanie krzywej C i równania

$$2v + h(u) = 0, \quad h'(u)v - f'(u) = 0.$$

Koprocesor zbudowano w oparciu o układ mnożący operujący na elementach przedstawionych w bazach normalnych. Obliczenia inwersji elementu wykonano w oparciu o algorytm Tsui-Itoh, natomiast samo mnożenie zrealizowano na bazie rozwiązania Masseya-Omury. Obliczenia realizowane są na elementach z ciała $GF(2^{155})$. Wybrano tę wielkość wykładnika, gdyż umożliwia ona zbadanie możliwości przyspieszenia realizacji operacji mnożenia ze 155 podstawowych taktów w rozwiązaniu odniesienia do 31 lub 5 taktów. Co prawda pociąga to za sobą wzrost złożoności rozwiązania układowego, jednak nie tak znaczny, jak przyśpieszenia realizacji obliczeń.