dr inż. Piotr Bora
mgr inż. Tomasz Kijko
Wojskowa Akademia Techniczna, Wydział Cybernetyki
Instytut Matematyki i Kryptologii

Implementacja sprzętowa koprocesora systemu klucza publicznego opartego na krzywych eliptycznych

W referacie przedstawione będą zagadnienia dotyczące implementacji sprzętowej (w układach logicznych) przykładowego algorytmu wyznaczania krotności punktu na krzywej eliptycznej jako operacji głównej koprocesora. Całość obliczeń realizowana będzie w ciele $GF(2^n)$, przy czym wskazane zostaną przykładowe wartości n, dla których tego typu rozwiązania są najekonomiczniejsze. Aby wykonać operację liczenia krotności punktu, należy rozważyć możliwość szybkiej i ekonomicznej implementacji układu mnożącego w ciele oraz szybkiego algorytmu inwersji. Pokazane zostaną rozwiązania przykładowe, ze wskazaniem możliwości zabezpieczenia przed atakami kryptoanalitycznymi na implementacje układowe. Podstawowe rozwiązania niezabezpieczone przed nimi umożliwiają, przy atakującym wyposażonym w odpowiedni sprzęt, odtworzenie tajnej wartości krotności już przy pojedynczym jej liczeniu, co stanowi wielkie zagrożenie.

W referacie przedstawione zostaną również wyniki zarówno zajętości układowej, jak i szybkości realizacji wyznaczania krotności, a co za tym idzie, wyznaczania klucza tajnego sesji. Należy tu zaznaczyć, że podstawowy i najprostszy protokół negocjacji klucza sesji MQV wymaga implementacji również układu mnożącego w ciele $GF(p)$, jednak można go tak zmodyfikować, żeby nie było to potrzebne i dla celów realizacji praktycznych takie rozwiązanie zostało wykonane.

Przedstawiane w referacie przykładowe implementacje zostały praktycznie przetestowane i zweryfikowane w oparciu o platformę ML507 firmy XILINX oraz w nowoprojektowanym w konsorcjum z firmą WASKO urządzeniu szyfrującym.

Praca naukowa finansowana ze środków na naukę w latach 2008–2010 jako projekt rozwojowy Nr R00 0031 06.