Gliwice, 27.09.2024 r.

Szymon Sarna

Tytuł rozprawy doktorskiej:
„System kryptograficzny implementowany w pSoC”

Streszczenie

Rozprawa doktorska pt. „System kryptograficzny implementowany w pSoC” przedstawia przebieg badań i rozwój systemu kryptograficznego firmy Digital Core Design. Poprzez analizę źródeł literaturowych i początkowej implementacji tytułowego systemu zidentyfikowano obszary, w których można podnieść jego bezpieczeństwo i efektywność. Za cel obrano m.in.: implementację układu mnożącego, generatora liczb prawdziwie losowych, zweryfikowanie odporności na ataki kanałem pobocznym oraz opracowanie protokołu z kluczami jednorazowymi.

Kluczowym elementem rozwijanego systemu kryptograficznego jest ko-procesor CryptOne, umożliwiający akcelerację obliczeń w algorytmach kryptografii asymetrycznej, takich jak RSA i ECC. Krytyczny wpływ na ich wydajność ma operacja mnożenia modulo, w związku z czym weryfikowano możliwość jej optymalizacji. W trakcie procesu badań i implementacji opracowano unikalne połączenie metod zaproponowanych w literaturze oraz oryginalnych rozwiązań, czego efektem jest podniesienie wydajności oraz ograniczenie zapotrzebowania na zasoby logiczne względem wersji referencyjnej. Opracowana architektura charakteryzuje się też bardzo dobrymi parametrami na tle innych rozwiązań opublikowanych w literaturze.

Obok układu mnożącego, na poziomie sprzętowym weryfikowano również możliwość wdrożenia generatora liczb prawdziwie losowych. Co do zasady, jest to fundamentalny komponent każdego systemu kryptograficznego, niemniej jego wiarygodna implementacja w układzie cyfrowym jest istotnym wyzwaniem ze względu na ograniczenia narzędzi projektowych oraz specyfikę mierzonych zjawisk fizycznych. Przeprowadzone badania i analizy pozwoliły na implementację generatora, którego źródłem losowości jest błąd fazy sygnału zegarowego. Zgodność z modelem stochastycznym oraz pozytywna weryfikacja przez zestaw testów statystycznych istotnie podnoszą wiarygodność opracowanej implementacji.

Obok generacji kluczy kryptograficznych generatory liczb losowych odgrywają istotną rolę w mechanizmach zabezpieczających przed atakami kanałem pobocznym. Jest to grupa ataków, które umożliwiają przełamywanie zabezpieczeń układów kryptograficznych, m.in. na podstawie obserwacji różnego rodzaju zjawisk fizycznych towarzyszących obliczeniom. Może to być np. czas, rozpraszana moc lub promieniowanie elektromagnetyczne. Ataki te stanowią poważne zagrożenie dla bezpieczeństwa nieomal każdej implementacji, dlatego postanowiono przygotować stanowisko pomiarowe i środowisko programowe, które umożliwią weryfikację podatności i skuteczności zastosowanych zabezpieczeń.

Badania obejmowały przeprowadzenie takich ataków jak prosta i różnicowa analiza rozpraszanej mocy. Opracowane metody, narzędzia i wnioski stanowią fundament do weryfikowania bezpieczeństwa rozwijanego systemu kryptograficznego w kontekście ataków kanałem pobocznym.

Systemy kryptograficzne, jak sama nazwa wskazuje, łączą w sobie różne funkcje i poziomy abstrakcji. W części sprzętowej implementowane są mechanizmy, które realizują operacje opisane przez instrukcje maszynowe, algorytmy i aplikacje. Świadomość zakresu tych zagadnień i możliwość podniesienia bezpieczeństwa na różnych poziomach były przyczynkiem do przeprowadzenia badań nad algorytmami z kluczami jednorazowymi. Wśród powszechnie używanych rozwiązań można spotkać algorytmy z akronimem OTP (ang. *One-Time-Password*), oznaczającym hasła jednorazowe, jednak pomimo unikalności kodów lub haseł często „wewnątrz" zaszyty jest stały klucz kryptograficzny. W związku z tym przygotowano koncepcję protokołu z kluczami jednorazowymi, który został następnie wdrożony i uruchomiany w oparciu o rozwijany system kryptograficzny. Protokół ten charakteryzuje się unikalnymi własnościami, które sprawiają, że może być on odpowiedzią na niektóre ze współczesnych wyzwań związanych z bezpieczeństwem tele-informatycznym.

Podsumowując, w ramach pracy doktorskiej osiągnięto postawione cele badawcze. Opracowane rozwiązania, również o oryginalnym charakterze, przełożyły się na poprawę parametrów i właściwości sytemu kryptograficznego w zakresie bezpieczeństwa, wydajności oraz zapotrzebowania na zasoby logiczne. Finalne efekty przeprowadzonych badań znalazły również zastosowanie i zostały wdrożone w produktach firmy Digital Core Design.