KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Bezpieczeństwo sprzętowe i kryptografia nowej generacji [S1MiKC2>BSiKNG]

Przedmiot

Kierunek studiów
Mikroelektronika i komunikacja cyfrowa

Rok/Semestr
3/6

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
30

Laboratorium
24

Inne
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

3,00

Koordynatorzy

dr inż. Łukasz Matuszewski
lukasz.matuszewski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać usystematyzowaną wiedzę z zakresu algebry, rachunku prawdopodobieństwa i teorii liczb. Powinien znać przynajmniej jeden język opisu sprzętu HDL, potrafić konfigurować układy konfigurowalne FPGA i znać ich strukturę oraz podstawowe właściwości. Powinien być zaznajomiony z podstawami sieci telekomunikacyjnych przewodowych i bezprzewodowych

Cel przedmiotu

Przekazanie studentom podstawowej wiedzy na temat kryptografii. Wytworzenie u studentów umiejętności oceny jakości zabezpieczeń kryptograficznych. Zapoznanie z nowoczesnymi metodami szyfrowania oraz algorytmami kryptograficznymi stosowanymi zarówno w oprogramowaniu, jak i sprzęcie. Poznanie niebezpieczeństw i sposobów zabezpieczenia sprzętowych realizacji układowych, w tym zabezpieczeń przed atakami fizycznymi, takimi jak ataki bocznokanałowe (side-channel attacks) czy ataki inwazyjne. Rozwinięcie umiejętności praktycznego wykorzystania narzędzi kryptograficznych oraz wdrażania rozwiązań bezpieczeństwa sprzętowego w rzeczywistych aplikacjach.

Przedmiotowe efekty uczenia się

Wiedza:

Posiada wiedzę na temat nowoczesnych technologii kryptograficznych. Zna podstawowe pojęcia i zasady kryptografii. Zna zasady zabezpieczeń sprzętowych i zagrożenia dla sprzętowych implementacji kryptografii. (K1_W14)

Umiejętności:
Potrafi integrować uzyskane informacje, dokonywać ich interpretacji, wyciągać wnioski i uzasadniać opinie. (K1_U02, K1_U16)

Kompetencje społeczne:
Zna ograniczenia własnej wiedzy i umiejętności, rozumie konieczność dalszego dokształcania się. Ma poczucie odpowiedzialności za zaprojektowane systemy elektroniczne i telekomunikacyjne i zdajesobie sprawę z potencjalnych niebezpieczeństw dla innych ludzi lub społeczeństwa ich nieodpowiedniego wykorzystania. (K1_K01, K1_K04)

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wykład:
Weryfikacja efektów kształcenia odbywa się poprzez test wielokrotnego wyboru. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania stanowią treść wykładu. Do uzyskania oceny 3.0 niezbędne jest zdobycie ponad połowy możliwych punktów.
Laboratorium:
1. Ocenianie ciągłe - każdorazowa weryfikacja wiedzy poprzez odpowiedzi ustne na pytania zadawane w trakcie wykonywania ćwiczeń laboratoryjnych.
2. Sprawozdania z wykonanych ćwiczeń, uwzględniające analizę poprawności uzyskiwanych rezultatów i identyfikację potencjalnych problemów.
3. Ocena uzyskana ze sprawdzianu podsumowującego ćwiczenia, sprawdzającego zarówno wiedzę teoretyczną, jak i praktyczne umiejętności.

Treści programowe

Wprowadzenie do kryptografii:
Przegląd podstawowych pojęć: szyfrowanie symetryczne i asymetryczne, podpis cyfrowy, funkcje skrótu. Algorytmy kryptograficzne: AES, RSA, ECC, SHA. Kryptografia postkwantowa - koncepcje i wyzwania.
Sprzętowe implementacje kryptografii:
Architektura sprzętowa a bezpieczeństwo - porównanie rozwiązań sprzętowych i programowych. Moduły kryptograficzne sprzętowe (HSM - Hardware Security Module, TPM - Trusted Platform Module). Układy FPGA i ASIC w kryptografii - projektowanie i implementacja. Sprzętowe generowanie liczb losowych (TRNG) i jego znaczenie dla kryptografii.
Zabezpieczenia sprzętowe:
Technologie zabezpieczające układy scalone: Zabezpieczenia fizyczne. Metody przeciwdziałania atakom inwazyjnym i nieinwazyjnym. PUF (Physical Unclonable Function) - unikalne identyfikatory sprzętowe. Mechanizmy ochrony przed klonowaniem układów scalonych.
Ataki na sprzęt kryptograficzny:
Ataki bocznokanałowe (Side-Channel Attacks): Analiza mocy pobieranej (Power Analysis). Ataki czasowe (Timing Attacks). Analiza emisji elektromagnetycznej (EM Analysis). Analiza dźwiękowa i drgań (Acoustic and Vibration Analysis). Ataki błędów (Fault Injection Attacks): Wstrzykiwanie błędów przy użyciu promieniowania laserowego, elektromagnetycznego i napięciowego. Efekty błędów na algorytmy kryptograficzne. Ataki inwazyjne: Dekapsulacja układów scalonych i analiza mikroskopowa. Probing - bezpośrednie sondowanie sygnałów wewnętrznych układu.
Praktyczne aspekty bezpieczeństwa sprzętowego:
Projektowanie bezpiecznych układów scalonych na przykładzie FPGA i ASIC. Wdrożenie protokołów kryptograficznych przy użyciu układów sprzętowych. Analiza przypadków rzeczywistych ataków na sprzęt kryptograficzny i wnioski z nich płynące.
Laboratoria i projekty:
Praktyczne ćwiczenia z wykorzystaniem modułów HSM i TPM. Symulacja ataków bocznokanałowych w kontrolowanych warunkach laboratoryjnych. Weryfikacja bezpieczeństwa sprzętowych realizacji układowych przy użyciu narzędzi diagnostycznych. Projektowanie i implementacja sprzętowych mechanizmów zabezpieczających.

Tematyka zajęć

Wykłady:
Wprowadzenie do kryptografii, Algorytmy kryptograficzne, Kryptografia postkwantowa, Architektura sprzętowa a bezpieczeństwo, Moduły kryptograficzne sprzętowe, Układy FPGA i ASIC w kryptografii, Sprzętowe generowanie liczb losowych (TRNG), Ataki bocznokanałowe (Side-Channel Attacks), Ataki błędów i ataki inwazyjne, Zabezpieczenia sprzętowe.
Laboratorium:
Implementacja algorytmów kryptograficznych w układach FPGA, Analiza bezpieczeństwa modułów sprzętowych HSM i TPM, Symulacja ataków bocznokanałowych, Weryfikacja sprzętowych generatorów liczb losowych (TRNG), Projektowanie sprzętowych zabezpieczeń przed atakami inwazyjnymi.

Metody dydaktyczne

Wykład: prezentacja multimedialna, ilustrowana przykładami podawanymi na tablicy.
Laboratorium problemowe: praca z komputerem i układami FPGA.

Literatura

Podstawowa:
A. J. Menezes, P. C. van Oorschot, S. A. Vanstone „Kryptografia stosowana”, WNT, Warszawa 2005.
B. Schneier „Kryptografia dla praktyków”, WNT, Warszawa, 2002.
W. Stallings „Kryptografia i bezpieczeństwo sieci komputerowych”, Wyd. V, Helion 2012.

Uzupełniająca:
. A. Buchmann „Wprowadzenie do kryptografii”, PWN, 2006.
N. Ferguson, B. Schneier „Kryptografia w praktyce”, Helion, 2004.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	84	3,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	54	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	30	1,00