Oponentský posudek dizertační práce

Název práce: **Kryptoanalýza postranními kanály**

Autor: **Ing. Zdeněk Martinásek**

Oponent: **Ing. Tomáš VANĚK, Ph.D.**
České Vysoké učení technické v Praze, Česká republika
Fakulta elektrotechnická
Katedra telekomunikační techniky

Aktuálnost dizertační práce

Problematika kryptoanalýzy pomocí postranních kanálů představuje moderní a velmi efektivní způsob útoků na kryptografické systémy, kdy se útočník nesoustředí na hledání slabin ve vlastním kryptografickém algoritmu, ale na chyby v jeho praktické implementaci. Jak se ukazuje v praxi, tento přístup je mnohdy výrazně jednodušší a efektivnější. Cílem předložené dizertační práce je návrh, optimalizace a experimentální ověření nového útoku postranními kanály, který by měl být efektivnější než existující útoky. Téma dizertační práce je tak velmi aktuální a zajímavé.

Orientace dizertanta v problematice, studium literatury

Problematika útoků postranními kanály je poměrně obsáhlá a složitá, dizertant se musel na jedné straně podrobně seznámit s různými možnostmi, jak provádět přesnou analýzu spotřeby mikroprocesorů, na druhé straně s problematikou optimalizace úloh pomocí neuronových sítí, což jsou naprosto odlišné oblasti. Toto propojení elektrotechniky a informatiky tak činí jeho práci ještě více zajímavou a moderní. Dizertant uvádí celkem 113 cizích zdrojů použité literatury a 11 zdrojů vlastních publikačních aktivit vztahujících se k tématu. Všechny cizí zdroje uvedené v seznamu literatury jsou v práci řádně citovány.

Formulace cílů práce a splnění cílů práce

Cíle specifikované v zadání práce byly jasně určené a měly předpoklad úspěšného splnění. Cíle dizertační práce považuji je za splněné.

Vlastní přínos dizertační práce

Hlavním přínosem předložené dizertační práce je návrh a optimalizace kryptoanalytických postupů a technik s cílem získat klíč šifrovacího algoritmu z mikroprocesoru na základě analýzy jeho spotřeby. Výsledkem řešení je nový postup kombinující výhody stávajících řešení, kterými jsou jednoduchá proudová analýza a diferenciální proudová analýzy. Zcela původní a nová je myšlenka využít ke klasifikaci a interpretaci naměřených neznámých hodnot neuronových sítí.

Rozsah a interpretace výsledků, publikace

Dizertant provedl důkladnou analýzu výsledků vlastní verze útoku postranním kanálem kombinující klasické analýzu spotřeby s následnou aplikací neuronové sítě, která ve svém důsledku umožňuje velmi výrazným způsobem snížit množství měření proudových cyklů na zkoumaném mikroprocesoru. Výsledná metoda vykazuje na zkoumaném procesoru více než 95% úspěšnost odhadu klíče. Hlavní myšlenky dizertační práce byly publikovány, jak na odborných konferencích, tak i v impaktovaných časopisech.

Přehlednost a struktura dizertační práce

Dizertační práce je členěna do pěti kapitol a má přehlednou a logickou strukturu. Autor nejdřív popisuje základní principy útoků postranními kanálu a stávající stav poznání v této oblasti. Na

tomto základě předkládá popis vlastního způsobu analýzy, která vykazuje lepší výsledky než stávající metody.

Formální, jazyková a stylistická úroveň práce

Práce je psaná v českém jazyce a jak po jazykové, tak i stylistické stránce má úroveň odpovídající tomuto typu prací. Práce obsahuje minimální množství překlepů či gramatických chyb. Jednou z mále je např. chybějící jednotka napětí U_c na str. 55. Grafická úroveň práce je dobrá, autor se dodržuje ustálené typografické konvence. V text jsou uváděny odkazy na použitou literaturu.

Celkové hodnocení dizertační práce

Předložená dizertační práci Ing. Zdeňka Martináska je dobře zpracovaná a jak po obsahové, tak i formální stránce odpovídá všeobecným požadavkům kladeným na dizertační práce. Dizertační práci doporučuji k obhajobě.

Otázky pro dizertanta

1) Proč je práce zaměřena na analýzu operací AddRounfKey a SubBytes, když operace SubBytes nepracuje s klíčem tj. z hlediska základního cíle analýzy, kterým je snaha získat klíč není důležitá?

2) Popis implementace AES na straně 53 neodpovídá tomu, jak je definován AES ve standardu FIPS-197. Podle standardu (viz [1], strana 15, Fig.5) jsou operace v rundě (mimo poslední) prováděny v pořadí SubBytes, ShiftRow, MixColumns a AddRoundKey. Dizertant uvádí jiné pořadí operací. Prosím o vysvětlení. Nebylo by nejjednodušší provádět analýzu nikoliv na vlastních rundách AES, ale na operaci AddRoundKey aplikovanou ještě před první rundou? Tato operace není součástí první rundy, ale jedná se o tzv. „key whitening“, který zvyšuje odolnost blokových šifer.

3) Str. 53 – proč je pro operace SubBytes a ShiftRow uveden souhrnný čas, zatímco u ostatních operací jsou uváděny individuální časy?

4) Kapitola 4.2 - Jaká byla chyba měření (vliv použité metodiky, přesnost měřicích přístrojů, náhodné chyby) při analýzách vlivu napájecího napětí, odporu bočníku či frekvence hodinového signálu vzhledem k naměřeným hodnotám? Byla měření prováděna opakovaně?

V Praze, 4.6.2013

.....

Ing. Tomáš Vaněk, Ph.D.