# Hodnocení vedoucího diplomové práce

Autor/autorka práce: **Bc. Petr Podávka**

Název práce: **Energeticky efektivní ověřování v bezdrátových sítích**

Student pracoval na řešení zadaného úkolu samostatně. Prvá část diplomové práce je věnována popisu používaných kryptografických algoritmů. Další část se zabývá popisem použitého vývojového prostředí i popisem použitého hardware (modul s procesorem CC3200). Poslední část je věnována popisu a realizaci vlastních algoritmů včetně publikování výsledků měření.

Diplomant nastudoval vedoucím doporučené metody distribuce klíčů (maticová a polynomiální) a implementoval je. Navíc přidal metodu ověřování pomocí ECC, kterou implementoval (ale v jiném prostředí) v rámci semestrální práce. Pro srovnání také připravil jednoduchou aplikaci používající protokol TLS (s hardwareovou podporou CC3200).

Vývoj probíhal na modulu s procesorem CC3200, který je určen pro aplikace s protokolem WiFi. Celá aplikace je napsána pod operačním systémem TI-RTOS, určeným pro mikroprocesorové aplikace. Měl sice k dispozici firemní knihovny, ale narážel na ne příliš detailní popis knihoven a ladících prostředků, dodávaných firmou Texas Instruments.

Při měření odběru, které bylo součástí zadání, narazil na problém dostupnosti zařízení, schopného dostatečně přesně zobrazovat časový průběh odběru. Nakonec byl použit osciloskop měřící úbytek napětí na odporu 0,5 ohmu, zapojeného do napájecí větve. Výsledné úbytky napětí byly v řádech mV, silně zašuměné. Domnívám se ale, že pro porovnání jednotlivých algoritmů jsou důležitá a dostačující měření časová, která byla také provedena.

Za kladný výsledek diplomantovy práce považuji i to, že musel vyřešit optimalizaci počítání se 128 bitovými čísly, protože měl k dispozici pouze 16 bitovou aritmetiku danou použitým procesorem.

Dosažené výsledky jsou použitelné pro realizaci bezdrátových senzorických sítí s požadavkem na zajištění bezpečné vzájemné komunikace, konkrétně např. implementaci zabezpečení protokolu WHART.

Práce je psána čtivě a s přehledem. Některé části popisu algoritmů jsou podle mě psány příliš stručně. V práci jsem našel minimální počet překlepů. Práce má pěknou grafickou úpravu.

Diplomant splnil zadání. Přesto mám na diplomanta následující otázku:

Na str. 43 se zabýváte vzájemným ověřováním uzlů a tvrdíte, že je možné vytvořit algoritmus vzájemného ověření pomocí tří zpráv. Mohl byste to dokázat?

Navrhuji hodnocení známkou **výborně** a práci doporučuji k obhajobě.

V Plzni 6. června 2017

Ing. Jiří Ledvina, CSc.

SOUHLASÍ
S ORIGINÁLEM

Západočeská univerzita v Plzni
Fakulta aplikovaných věd
katedra informatiky a výpočetní techniky