Oponentní posudek disertační práce

Autor: Ing. Lukáš Malina

Název: Privacy Preserving Cryptographic Protocol for Secure Heterogeneous Networks

Vydavatel: Fakulta informačních technologií, Vysoké učení technické v Brně

Zpracovatel posudku: doc. Ing. Jaroslav Dočkal, CSc., Vysoká škola Karla Engliše, a.s.

Námět disertační práce plně odpovídá oboru disertace. Oponovaná disertační práce je zcela aktuální z hlediska současného stavu vědy. Zpracovaná je v angličtině, evidentně proto, že se opírá o články publikované v zahraničních odborných časopisech. Téma práce je velice náročné, protože jde o novou a přitom velmi perspektivní oblast vědního výzkumu, v České republice se jí prakticky kromě autora disertační práce a jeho kolegů nikdo jiný hlouběji nezabývá. Výzkum v této oblasti je proto mimořádně náročný na potřebu mezinárodní spolupráce. Další složitosti musí přinášet vysoká dynamika rozvoje dané oblasti kryptografie.

Práce vykazuje zřetelné a nezpochybnitelné původní přínosné části. Ing. Lukáš Malina v ní navrhl dva původní protokoly, kriticky zhodnotil jejich výhody i nevýhody a diskutuje chování systému v případě předpokládaného útoku. Přitom nezapomněl na hodnocení efektivnosti navržených protokolů v jednotlivých fázích a snažil se o jejich optimalizaci jak při podepisování, tak při verifikaci podpisu. Správně pro účel praktické realizace volil použití knihovny jPBC. Do třetice navrhl rovněž možný kryptografický rámec pro zajištění privátnosti v rámci geosociálních služeb provozovaných na heterogenních sítích.

Osou práce jsou již publikované články a příspěvky na konferencích, jemuž je předřazena poměrně rozsáhlá úvodní část obsahující přehled základních pojmů a východisek v dané oblasti výzkumu. Pasáže popisující vývoj schémat skupinových podpisů ústí do tabulky 5.1 obsahující přehled parametrů těchto podpisů. Mám-li být upřímný, jiné přehledy mi připadají čtivější, viz např. Ratna Dutta a kol.: Pairing-Based Cryptography Protocols: A Survey, Subhra Mishra a Tilak Rajan Sahoo: A survey on Group Signature Schemes.

Co se mi na práci zvláště líbí, je důraz autora na výkonnostní analýzu (viz kapitola 6). Tento přístup mu poskytuje možnost jeho protokol srovnávat s jinými řešeními. Grafy a tabulky jsou správně, možná že u disertační práce by se hodilo dát do příloh navíc sejmuté obrazovky s výsledky časových testů, které by činily výsledky ještě více průkaznými (činí tak např. již zmínění autoři A survey on Group Signature Schemes).

Autor na dvou místech (s. 28 a s. 145) píše, že „hlavní cíl disertace je výzkum…“, já se domnívám, že samotný výzkum je spíše prostředek k získání nových poznatků – má připomínka je ale ryze formulační a netýká se obsahu práce.

Práce je mimořádně pečlivě zpracována, bez chyb a překlepů. Pro čtenáře, který v kryptografii není příliš doma, by možná bylo lépe, kdyby byl rozsah popisných pasáží menší, ale text nebyl tak letmý. Např. u definice CDHP na str. 36 je třeba stále uvádět, že jde o body na eliptické křivce, protože pod CDHP můžeme také chápat něco jako „jsou dána g, g^a a g^b, hledáme g^{ab}“.

Metody anonymní autentizace využívající skupinové podpisy mají své atraktivní uplatnění v cloudových technologiích. Ing. Malina se daným tématem zabýval mj. v příspěvku na konferenci TSP 2013, zajímalo by mě, proč se o tomto tématu nezmínil ve své práci (ne že by její rozsah nebyl dostatečný, to spíše naopak).

Práce obsahuje seznam použitých zkratek a 181 použitých zdrojů, a to podle mne převážně z let, kdy doktorand hledal, kudy své výzkumné úsilí zaměřit. Z roku 2013 (pokud nepočítám tituly vlastní) již je zdrojů cca deset (což by svědčilo o zúžení oblasti odborného zájmu) a z roku 2014 žádný – práce je signována 18.6. t.r., neboli ty úvodní přehledové pasáže bylo možné aktualizovat.

Co mi ale v této obsáhlé práci se značným množstvím citací zvláště chybí, je rejstřík.

Ing. Malina je publikačně mimořádně aktivní a to i v širokém spektru souvisejícím s disertací. U všech 23 prací uvedených v příloze je uveden jako spoluautor, u řady z nich je evidentní, že zpracoval rozhodující část článku resp. příspěvku, přesto by stálo za to odhadnout autorský podíl, doporučuji u obhajoby uvést ty články a publikace, u kterých šlo o podíl rozhodující.

Všechny v příloze uvedené publikace vyšly v angličtině, což je u těch zahraničních pochopitelné, méně u těch tří publikovaných v Elektrorevui. Je třeba uznat, že Ing. Lukáš Malina důstojně reprezentuje svoji školu a českou vědu v zahraničí, chybí mi však příspěvek k české odborné terminologii. Dobrým krokem v tomto směru by možná byla nabídka vhodného článku např. do Cryptoworldu.

Ing. Lukáš Malina prokázal ve své disertační práci schopnost samostatné i týmové vědeckovýzkumné práce. Kromě publikační činnosti je třeba ocenit kvalitu jeho vedení diplomantů. Během obhajoby by mohl uvést, jakým způsobem chce na výsledky dosažené v rámci disertační práce navázat ve své další výzkumné činnosti.

Závěrem je třeba uvést, že **disertační práce plně odpovídá obecně uznávaným požadavkům k udělení akademicko-vědeckého titulu doktora v oboru Teleinformatika.**

J. Dostálek

V Brně 7. srpna 2014