FACULTY
OF INFORMATICS

Kontakt / Email:
doc. RNDr. Petr Švenda, Ph.D.
svenda@fi.muni.cz

Místo / Datum
Brno
23. července 2019

Posudek na disertační práci Ing. Petra Dzurendy s názvem "Cryptographic Protection of Digital Identity"

Předložená práce se věnuje oblasti kryptografických autentizačních schémat se zvýšenou mírou ochrany soukromí, s vymezením na schémata prokazatelně bezpečná a zároveň prakticky implementovatelná na zařízeních s omezenými prostředky typu kryptografická čipová karta. Jádrem práce je návrh a analýza čtyř základních schémat, doplněných dalšími podpůrnými publikacemi analyzujícími výkonnostní charakteristiky na konkrétních platformách. Celkově se jedná o více jak 10 konferenčních nebo časopiseckých publikací.

Práce je rozdělená do šesti nosných kapitol. Základní kryptografická primitiva potřebná pro konstrukci studentem navrhovaných schémat jsou popsána ve druhé kapitole. Třetí kapitola poskytuje přehled současného stavu výzkumu v oblasti skupinových podpisů (group signatures), autentizace prokazováním dílčích atributů (attribute-based credentials) a systematický přehled a srovnání vlastností různých platforem pro kryptografické čipové karty. Čtvrtá kapitola prezentuje návrh schématu pro autentizaci s využitím více dílčích zařízení spolu výkonnostním srovnáním na sadě různých zařízení včetně čipových karet a mobilních zařízení. Schéma pro anonymní sběr dat použitelných na zařízeních s omezenou výpočetní kapacitou je prezentován v kapitole pět včetně rychlostního srovnání na široké sadě různých zařízení. Šestá kapitola adaptuje existující schéma Hajný-Malina (HM12) pro anonymní prokázání vlastností pro eliptické křivky a opět vyhodnocuje rychlost pomocí praktické implementace na čipových kartách včetně srovnání s původní variantou. V sedmé kapitole je popsána poslední ze čtyř studentem nově navržených schémat zaměřující se na verifikaci anonymizovaných atributů pro scénář spojující certifikující a verifikující entitu, díky kterému lze obecně dosáhnout výkonnostně optimálnější schémata. Zároveň se opět zaměřuje na doménu čipových karet, které komplikují vlastní implementaci díky omezenému API rozhraní.

1) Odpovídá námět práce oboru disertace a je aktuální z hlediska současného stavu vědy?

Předložená práce se věnuje výzkumně relevantní oblasti se zaměřením na praktickou aplikovatelnost navržených schémat. Přestože je oblast skupinových podpisů a anonymizovaná autentizace založená na atributech zkoumána již relativně dlouhou dobu, v běžném použití ještě není, až na výjimky, příliš rozšířená. Kromě vyšších nároků na pochopení a implementaci

navržených schémat je důvodem i snížený výkon existujících schémat – aktuální problém, na jehož řešení se schémata navrhovaná v práci systematicky zaměřují. Po teoretické i praktické stránce se jedná o kvalitně provedený výzkum s odpovídající akademickou publikací formou kvalitních konferencí a časopisů.

V práci mohlo být jasněji specifikováno, které oblasti student v rámci výzkumného týmu primárně řešil – dle náplně textu předpokládám, že šlo především o část návrhu umožňující efektivní implementaci, samotnou implementaci a její vyhodnocení.

V rámci práce jsem také postrádal souhrn možných budoucích výzkumných oblastí hodných prostudování. V rámci obhajoby bych prosil o uvedení alespoň části z nich.

2) *Vykazuje práce původní přínosné části?*

Práce obsahuje celou řadu nových původních výsledků. Velmi kladně hodnotím provedené detailní výkonnostní srovnání navržených schémat na paletě různých hardwarových platforem. Za hlavní výsledek práce považuji demonstraci faktu, že nově navržená schémata jsou dostatečně výkonná i pro použití na omezených zařízeních bez nutnosti snižovat celkovou bezpečnostní úroveň.

3) *Bylo jádro disertační práce na potřebné úrovni publikováno? Vyplývá ze seznamu vědecké činnosti uchazeče, že se jedná o pracovníka s vědeckou erudicí?*

Všechna navržená schémata byla publikována na kvalitních akademických konferencích s převažujícím hodnocením CORE B, nebo v impaktovaných časopisech, které patří mezi kvalitní místa pro prezentaci vědeckého výzkumu. Vytvořený text je velmi dobře čitelný a dobře zasazený do aktuálního výzkumného kontextu s referencemi na relevantní vědecké práce.

4) *Dotazy k obhajobě*

- V obrázku 3.1 je uvedeno rychlostní srovnání skupinových podpisů na telefonu Nexus. Z jakého důvodu je implementace podepisování pro schéma DP pomalejší s předpočítáním než bez něj?
- Pokud by bylo možné rozšířit existující API karet, které generické operace by byly přínosné pro další zrychlení navržených i souvisejících schémat?
- Prezentovaná schémata jsou založena na ECC umožňující jejich efektivní implementaci na současných omezených systémech. Do jaké míry by bylo možné modifikovat schémata na využití post-kvantových schémat?
- Častým problémem u komplikovanějších kryptografických schémat je jejich bezpečná implementace. Jaké jsou potenciálně problematická místa u navržených schémat? Jsou provedené implementace veřejně dostupné?

5) Závěrečné shrnutí

Předložená disertační práce dle mého názoru odpovídá obecně uznávaným požadavkům k udělení akademického titulu a prokazuje schopnost uchazeče provádět kvalitní vědecký výzkum s následnou publikací na kvalitních konferencích a časopisech. Doporučuji práci uznat jako disertační.

S uctivým pozdravem,

[redacted]

doc. RNDr. Petr Švenda, Ph.D.