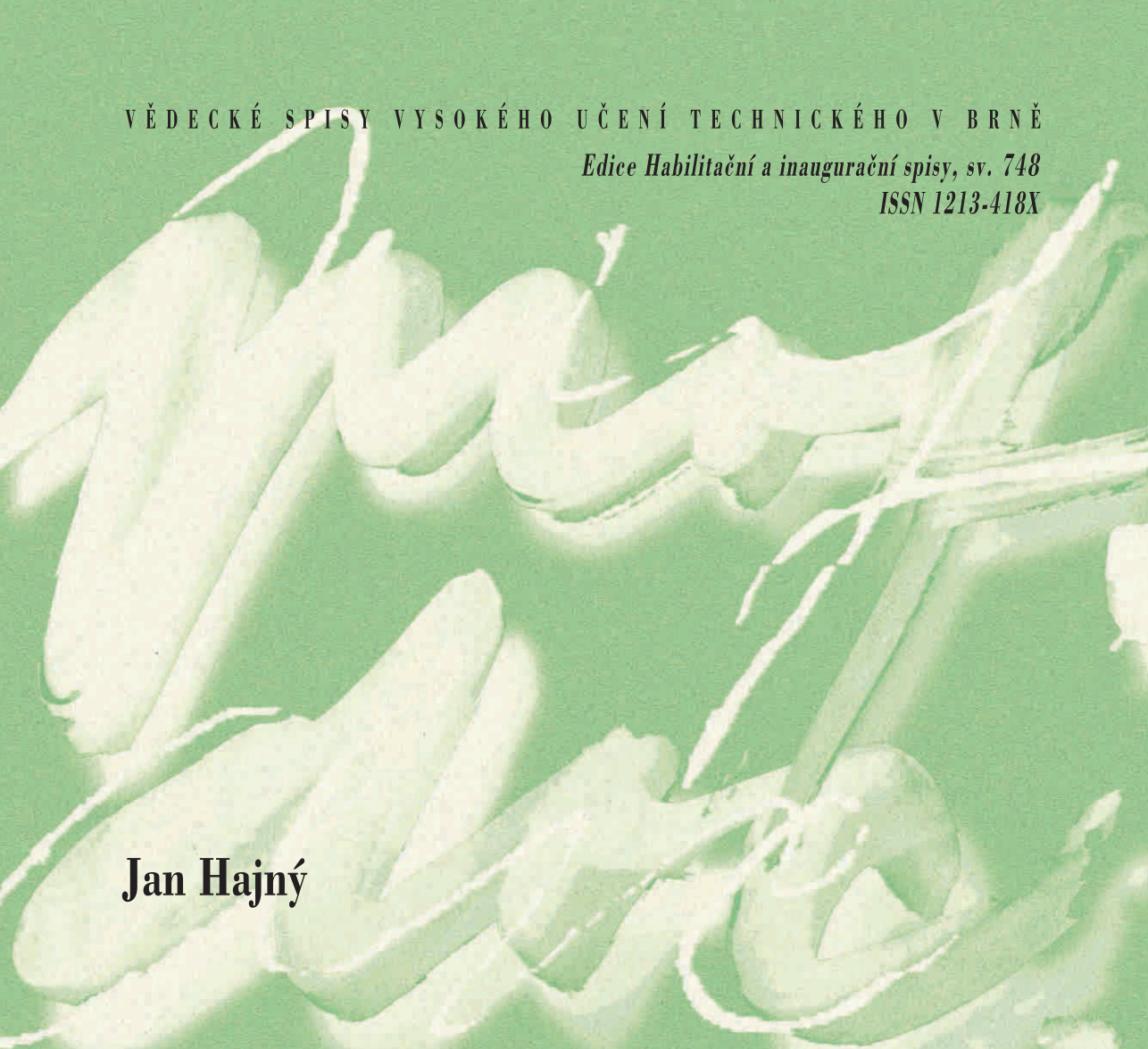
VĚDECKÉ SPISY VYSOKÉHO UČENÍ TECHNICKÉHO V BRNĚ
Edice Habilitační a inaugurační spisy, sv. 748
ISSN 1213-418X



Jan Hajný

VYBRANÉ TRENDY MODERNÍ KRYPTOGRAFIE

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
Ústav telekomunikací

doc. Ing. Jan Hajný, Ph.D.

VYBRANÉ TRENDY MODERNÍ KRYPTOGRAFIE

SELECTED TRENDS IN MODERN CRYPTOGRAPHY

TEZE PŘEDNÁŠKY K PROFESORSKÉMU JMENOVACÍMU ŘÍZENÍ
V OBORU TELEINFORMATIKA

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
NAKLADATELSTVÍ VUTIUM

BRNO 2023

KLÍČOVÁ SLOVA

Kryptografie, autentizace, soukromí, osobní atributy, revokace, kryptografické protokoly.

KEYWORDS

Cryptography, authentication, privacy, personal attributes, revocation, cryptographic protocols.

ISBN 978-80-214-6136-9
ISSN 1213-418X

OBSAH

Curriculum Vitae

Jan Hajný

Zaměstnavatel:	Fakulta elektrotechniky a komunikačních technologií (FEKT) Vysoké učení technické v Brně (VUT), Česká republika
Členství:	International Association for Cryptologic Research (IACR)
Web:	`https://www.vut.cz/lide/jan-hajny-89784`

PROFESNÍ ZKUŠENOSTI

2022 - Nyní	Člen panelu ERC Consolidator Grant
2021 - Nyní	Hodnotitel Evropské komise (DG CNECT) v programu Horizon Europe
2019 - Nyní	Vedoucí skupiny Brno Applied Cryptography & Security Engineering (AXE)
2019 - Nyní	Předseda rady a garant magisterského programu "Informační bezpečnost"
2018 - Nyní	Člen Vědecké rady FEKT, VUT
2018 - Nyní	Předseda rady a garant bakalářského programu "Informační bezpečnost"
2016 - Nyní	Docent na FEKT, VUT
2020 - 2022	Člen pracovní skupiny European Union Agency for Cybersecurity (ENISA): European Cybersecurity Skills Framework
2014 - 2020	Hodnotitel Evropské komise (REA) v programu Horizon 2020
2012 - 2019	Vedoucí skupiny Advanced Cybersecurity ve výzkumném centru SIX, VUT
2008 - 2015	Akademický pracovník na FEKT, VUT

KVALIFIKACE

2015, 2016	Výzkumné stáže v IBM Research, Curych, Švýcarsko (Dr. Jan Camenisch)
2016	Habilitace na FEKT, VUT Habilitační práce: "Cryptographic Proofs of Knowledge and Their Usage in Systems Protecting Digital Identity"
2008 - 2012	Doktorský program na FEKT, VUT Doktorská práce: "Autentizační protokoly a ochrana soukromí" Vedoucí práce: doc. Ing. Karel Burda, CSc.
2010 - 2011	Fulbrightovo stipendium na Dpt. of Mathematics, Dpt. of Computer Science (prof. N. Hopper), University of Minnesota, USA
2008	Studijní stáž na Department of Computer Science (prof. I. Damgård) University of Arhus, Dánsko
2003 - 2008	Bakalářské a magisterské studium na FEKT, VUT

VYBRANÉ VÝZKUMNÉ PROJEKTY

2023 - 2026	Horizon Europe #101087529: CHESS, (hlavní řešitel na VUT)
2023 - 2026	Digital Europe #101091684: CZQCI (HŘ na VUT)
2022 - 2025	MVČR VJ02010010: Nástroje pro verifikaci bezpečnosti kryptografických zařízení s využitím AI (HŘ)

2021 - 2025	VJ01010008: Kybernetická bezpečnost sítí v postkvantové éře (HŘ)
2019 - 2022	VJ01030001: Mezinárodní partnerství pro trénink dovedností kybernetické bezpečnosti (HŘ)
2019 - 2022	VJ01030002: Mezinárodní partnerství pro výzkum kryptografie a kyberbezpečnosti (HŘ)
2019 - 2022	Horizon 2020 #830892: SPARTA (HŘ na VUT)
2018 - 2020	TAČR TL02000398: Právní a technické prostředky pro ochranu soukromí v kyberprostoru (HŘ)
2017 - 2020	MPO FV20354: Automatizovaná správa a monitoring ochranného vybavení
2016 - 2018	MVČR VI1VS/185: Bezpečné řízení přístupu pro kritické infrastruktury
2016 - 2018	MVČR VI1VS/059: Kryptografické zabezpečení pro 100 GbE sítě
2015 - 2016	Horizon 2020 #664353: ADWICE: Advanced Cybersecurity (vedoucí skupiny)
2014 - 2016	TAČR TA04010476: Bezpečné systémy pro ověření uživatelů el. služeb (HŘ)
2014 - 2016	GAČR 14-25298P: Výzkum kryptografických primitiv pro bezpečnou autentizaci a ochranu digitální identity (HŘ)
2012 - 2014	TAČR TA02011260: Systém pro kryptografickou ochranu elektronické identity

VÝUKA

2020 - Nyní	Seminář informační bezpečnosti (Garant, vyučující)
2018 - Nyní	Cryptologic Protocol Theory (Garant, vyučující)
2013 - Nyní	Základy kryptografie (Garant, vyučující)
2016 - 2019	Foundations of Cryptography (Garant, vyučující)
2014 - 2019	Bezpečnost ICT 1 (Garant, vyučující)
2013 - 2015	Počítače a programování
2008, 2009, 2011	Bezpečnost informačních systémů
2009, 2010	Návrh, správa a bezpečnost počítačových sítí

VEDENÍ STUDENTSKÝCH PRACÍ

2008 - Nyní	Bakaláři: 30, Magistři: 26, Doktorandi: 7, z čehož 2 již obhájeny

ORGANIZACE AKCÍ

2022	IEEE Euro Security&Privacy, EuroCSEP Co-Chair
2021, 2022	ARES ETACS (Education, Training and Awareness in Cybersecurity) General Chair
2021, 2022	ARES SP2I (Security and Privacy in Intelligent Infrastructures) Programový výbor
2019 - 2022	CECC (Central European Conference on Cryptography) Programový výbor
2016 - 2022	Santa's Crypt Programový výbor

PUBLIKACE V ČÍSLECH (1/2023)

Časopisy	18/15 publikací (Scopus/WoS)
Konference	75/58 publikací (Scopus/WoS)
Vše	125/93/73 publikací (Scholar/Scopus/WoS)
h-index	18/14/9 (Scholar/Scopus/WoS)

1 ÚVOD

Tématem této teze jsou aktuální trendy v oblasti moderní kryptografie, zejména ty zaměřené na oblast autentizace osob a řízení přístupu k elektronickým službám. Motivace zacílení práce na kryptografii je dána zejména jejím aktuálním dynamickým rozvojem a její nezastupitelnou rolí v současných i budoucích informačních a komunikačních technologiích (ICT). Významná část bezpečnostních mechanismů těchto systémů je totiž v současnosti implementována právě pomocí kryptografických protokolů a algoritmů. Zajištění kybernetické bezpečnosti ICT systémů bez moderní kryptografie je nereálné a stále větší počet služeb a systémů na kryptografické mechanismy kriticky spoléhá. Na rozdíl od relativně nedávné minulosti okolo roku 2010, kdy byla kybernetická bezpečnost opomíjené téma, se nyní tato oblast objevuje stále častěji jako priorita jak pro akademickou, tak aplikovanou sféru. Doložit to lze zvyšujícím se počtem různých výzev výzkumných programů [56, 55] i zvyšujícím se objemem zakázek v průmyslu [58]. Aktuální národní i evropská legislativa [69, 61] navíc přímo určuje vybraným subjektům zavádět mechanismy kybernetické ochrany, lze tedy předpokládat, že rozvoj této oblasti je stále na počátku.

Aktuální rozvoj kryptografie sebou přináší i určitou roztříštěnost a značnou tematickou šíři současných trendů. Za poslední dekádu kryptologická komunita objevila řadu témat a oblastí, ve kterých došlo k zásadnímu posunu ve vědění i praktické aplikovatelnosti. Namátkou můžeme jmenovat technologie jako blockchain a kryptoměny [65], homomorfní šifrování [59], postkvantové systémy [67], technologie na ochranu soukromí [68], výpočty více stran či pokroky v kryptoanalýze, např. pomocí postranních kanálů. Nově se výzkum zaměřil i na netechnické aspekty kryptografických mechanismů, zejména jejich použitelnost v praxi a přijetí uživateli.

Není v možnostech daných rozsahem této teze věnovat se všem aktuálním trendům v moderní kryptografii. Z tohoto důvodu byly zvoleny vybrané trendy, které jsou v oblasti zájmu autora a ve kterých byl tým VUT v Brně nějakým způsobem aktivní a přispěl k posunutí hranic vědění či přinesl nové praktické technologie. Zaměřením této práce je tedy oblast autentizace a ověřování vlastností osob využívajících elektronické systémy.

Teze je členěna celkem na pět kapitol, přičemž po *Kapitole 1: Úvod* jsou v *Kapitole 2: Moderní autentizace* představeny základní principy kryptografických protokolů pro autentizaci osob, dále v *Kapitole 3: Kryptografická atributová pověření* jsou představeny systémy s ochranou soukromí a současný stav v této oblasti. Jsou zde také definovány základní problémy v této oblasti a uvedena řešení, ke kterým přispěl autor teze. V *Kapitole 4: Další trendy v moderní kryptografii* jsou popsány oblasti, které představují v současnosti hlavní výzvy, a směry, kterými se moderní kryptografie ubírá. Závěrečné shrnutí je obsaženo v *Kapitole 5: Závěr*.

2 MODERNÍ AUTENTIZACE

Proces autentizace je v širším pohledu chápán jako proces ověření deklarované identity uživatele či jiné entity (např. zařízení, softwarové komponenty či procesu). Obvykle se autentizace využívá při řízení přístupu, ať už fyzického či k elektronickým aktivům. Společně s *autentizací* se obvykle při řízení přístupu implementují i mechanismy pro *autorizaci*, tj. přiřazení a kontrolu oprávnění uživatelů, a *účtování*, tj. záznam časových a dalších logovacích údajů o přístupech. Vznikají tak tzv. AAA protokoly, z anglického Authentication, Authorisation a Accounting. Příklady takových protokolů jsou Kerberos [60], RADIUS [74] či TACACS [57].

Byť jsou výše uvedené autentizační protokoly ve své specifikaci velmi odlišné, principy pro ověření identity uživatelů se u nich výrazněji neliší. Pro ověření identity uživatele používají tzv. dokazovací faktor, který může patřit do jedné z následujících skupin:

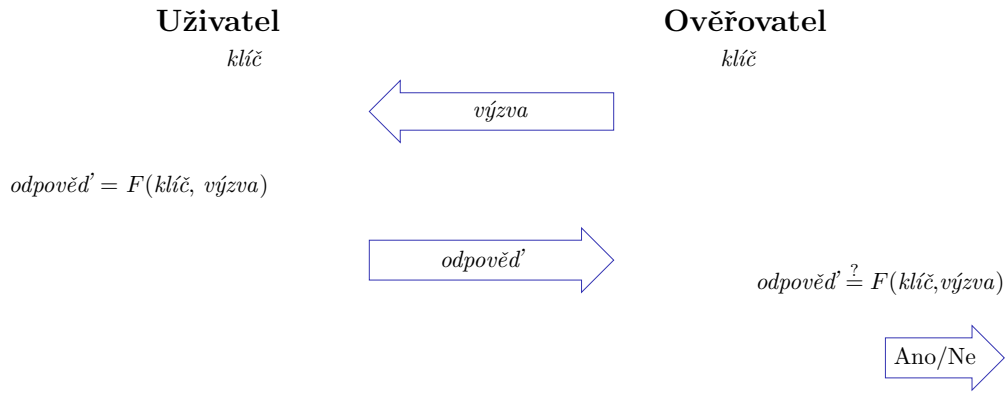
- znalost: ověření je provedeno na základě znalosti tajné informace, typicky hesla či klíče,
- vlastnictví: ověření je provedeno na základě vlastnictví uživatelova zařízení, typicky tokenu či čipové karty,
- behaviorální faktor: ověření je provedeno na základě specifického chování uživatele, například způsobu psaní na klávesnici,
- biometrický faktor: ověření je provedeno na základě tělesného rysu uživatele, například otisku prstu.

Přestože je zejména biometrický faktor v praxi často používán (např. u čteček prstů či ve skenerech obličejů u mobilních telefonů či letištních bran), z pohledu kryptografie je nejzajímavější a nejpoužívanější autentizace pomocí znalosti. Je to dáno tím, že ostatní faktory se na autentizaci pomocí znalosti dají často převést. Autentizační protokol umožňující ověření uživatele pomocí znalosti může být přeměněn na protokol založený na vlastnictví (znalost je uložena v zařízení) či biometrii (znalost je uložena ve formě markantů). Protože tématem této teze je moderní kryptografie, budeme se nadále věnovat autentizaci pomocí znalosti.

Současné autentizační protokoly využívající znalost jako dokazovací faktor obvykle fungují na principu prokazování znalosti uživatelského hesla, tajného klíče (symetrické systémy) či soukromého klíče (asymetrické systémy). Způsob prokázání můžeme rozdělit na tyto nejčastěji používané skupiny:

- přenos šifrované znalosti: uživatel znalost zašifruje klíčem ověřovatele a pošle přes nezabezpečenou síť. Ověřovatel dešifruje, porovná se svým záznamem a rozhodne o přijetí či odmítnutí uživatele.
- Mechanismus výzva-odpověď: uživatel obdrží od ověřovatele výzvu, která je unikátní. Na tuto výzvu musí odpovědět odpovědí sestavenou na základě hodnot znalosti (např. kryptografického klíče) a unikátní výzvy. Pokud je odpověď správná, ověřovatel uživatele přijme, v opačném případě je uživatel odmítnut. Základní princip je uveden na Obrázku 2.

Zatímco přenos šifrovaného hesla byl populární v autentizačních protokolech z 80. a 90. let (např. RADIUS, Kerberos), v moderních kryptografických systémech, jakým je např. proto-

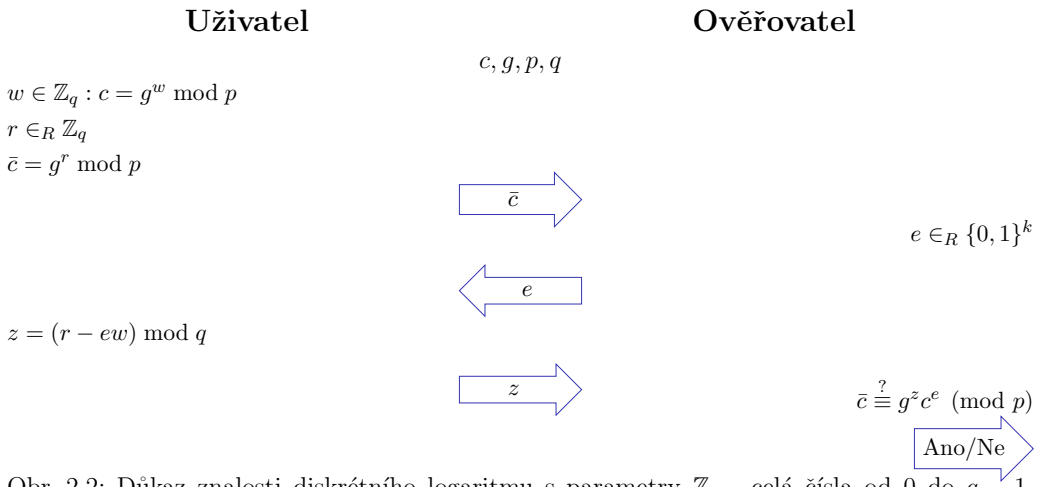


Obr. 2.1: Mechanismus výzva-odpověď.

kol TLS, již používán není. Důvodem jsou jeho bezpečnostní slabiny, zejména náchylnost na útoky opakováním a hrubou silou. Naopak mechanismy výzva-odpověď tvoří základ většiny moderních řešení. Ta se liší zejména ve volbě funkce F, pomocí které uživatel počítá odpověď z výzvy a své znalosti. Tato funkce může být implementována pomocí symetrických primitiv (hashovací funkce, bloková šifra) či asymetricky (digitální podpis, asymetrické šifrování). Hlavním požadavkem je jednocestnost funkce, tj. z odpovědi nesmí být možné vypočítat vstupy, zejména uživatelskou znalost.

Mechanismus výzva-odpověď je v dnešní době základem většiny v praxi používaných protokolů, kterou označujeme jako Generaci 1, tj. protokoly vzniklé obvykle před rokem 2000, při praktickém použití bezpečné, avšak bez moderních vlastností, jakými jsou např. formální důkazy bezpečnosti či funkce pro ochranu soukromí uživatelů. Příklady jsou např. protokoly TLS 1.3 [73], Kerberos [60] či EAP [41].

Počátkem 90. let se však začaly objevovat návrhy nových autentizačních protokolů, které přinesly z pohledu bezpečnosti zásadní zlepšení. Na rozdíl od protokolů popsaných výše totiž umožňovaly sestavení formálního důkazu bezpečnosti na základě jednoznačně definovaného modelu a definice vlastností. Příkladem takových protokolů jsou zejména tzv. protokoly s nulovou znalostí (angl. zero-knowledge protocols). Ty definují interakci mezi uživatelem a ověřovatelem pomocí matematického modelu založeném na interaktivním páru Turingových strojů, který musí splňovat požadavky úplnosti (completeness), spolehlivosti (soundness) a nulové znalosti (zero-knowledge). Požadavky i model jsou definovány např. v pracích autora zde [9] či zde [6]. Přestože je teoreticky možné sestavit protokoly s nulovou znalostí pro důkazy k jakémukoliv tvrzení založeném na NP problému, v praxi se nejčastěji používají protokoly, kde se prokazuje znalost hodnot diskrétního logaritmu. Příkladem takového protokolu je Schnorrův protokol na Obrázku 2, který je standardizován dle ISO/IEC 9798-5 a v praxi často využíván. Je také základem pro složitější protokoly, např. atributová pověření popsaná v následující kapitole. Schnorrův protokol splňuje požadavky na úplnost (tedy zaručuje přijetí čestných uživatelů), spolehlivost (tedy zaručuje odmítnutí nečestných uživatelů) a nulovou



Obr. 2.2: Důkaz znalosti diskrétního logaritmu s parametry $\mathbb{Z}_q$ - celá čísla od 0 do $q - 1$, (c, g, p, q) - parametry kryptosystému typu DLP.

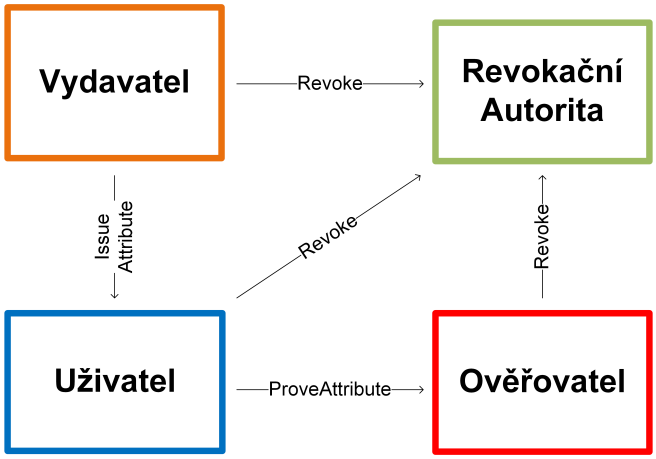
znalost (tedy garantuje, že neunikne žádná informace o uživatelském tajemství). Více o interaktivních důkazech znalosti založených na diskrétních logaritmech je možné nalézt např. v práci autora [9].

Protokoly, jakým je i Schnorrův protokol popsaný výše, můžeme zařadit do tzv. Generace 2, která umožňuje bezpečné ověření znalosti uživatele, na rozdíl od Generace 1 však za použití formálního modelu, jednoznačné definice vlastností a především rigorózního důkazu bezpečnosti. Tyto protokoly vznikaly především na přelomu století, nyní jsou již dobře známé a aplikovatelné do praktických systémů.

Výzkum v oblasti moderní kryptografie pro autentizaci pokračoval po Generaci 2 zejména snahou o zavedení nových funkcí pro ochranu soukromí. Hlavní myšlenkou byl předpoklad, že ne ve všech systémech je nutné pro řízení přístupu znát identitu uživatele, v některých systémech je možné anonymně ověřit pouze některé atributy uživatele, jako např. jeho věk, platnost registrace či národnost. Vznikly tak nové autentizační systémy, které v rámci této práce řadíme do Generace 3, tj. protokoly s ochranou soukromí. Jelikož jsou tyto protokoly hlavním motivem této teze, je jim věnována samostatná následující kapitola.

3 KRYPTOGRAFICKÁ ATRIBUTOVÁ POVĚŘENÍ

U kryptografických atributových pověření (angl. cryptographic attribute-based credentials) je proces autentizace chápán odlišně od protokolů popsaných v dřívějších kapitolách. Autentizace zde není ověřením identity uživatele, ale jeho osobních atributů. Ty mohou představovat jakoukoliv osobní charakteristiku, např. věk, národnost, pohlaví či držení nějakého oprávnění.



Obr. 3.1: Entity a protokoly systému atributových pověření.

Samotný proces se zásadně nemění - stále je nutné ověřit uživatelovo držení daného atributu, nejčastěji pomocí specifické znalosti s atributem svázané.

Role jednotlivých entit se ale u atributových pověření liší. K uživateli a ověřovateli se navíc přidává vydavatel osobních atributů a revokační autorita, která je schopna atributy i uživatele ze systému odebírat. Schéma atributového pověření je zobrazeno na Obrázku 3.1.

Atributová pověření obvykle definují následující protokoly:

- vydávání atributu (angl. issue): protokol sloužící k vydání kryptografické konstrukce a relevantních klíčů reprezentujících vlastnictví osobního atributu.
- Prokázání atributu (angl. prove): protokol sloužící k ověření vlastnictví osobních atributů na základě ověření znalosti relevantních klíčů.
- Revokace atributu (angl. revoke): protokol sloužící k odebrání osobních atributů uživatele prostřednictvím zneplatnění relevantních klíčů.

Aby bylo atributové schéma skutečně anonymní a chránilo soukromí uživatelů, je nutné, aby splňovalo alespoň následující požadavky:

- anonymita (angl. anonymity): protokol prokázání osobních atributů nezveřejní informace o identitě uživatele.
- Selektivní odhalení (angl. selective disclosure): uživatel si může vybrat, které atributy během ověřovací relace ověřovateli odhalí a které zůstanou skryty.
- Nespojitelnost relací (angl. unlinkability): ověřovací relace jednoho uživatele jsou vzájemně nespojitelné.
- Nesledovatelnost (angl. untraceability): anonymita a nespojitelnost relací platí i pro vydavatele atributů, kteří nesmí být schopni uživatele identifikovat či sledovat na základě přepisů autentizačních relací.

Zatímco výzkum v oblasti klasických autentizačních protokolů (tzv. Generace 1) a protokolů

s prokazatelnou bezpečností (tzv. Generace 2) již dosáhl svých cílů a jsou nám známy efektivní algoritmy, které požadované funkce realizují, u atributových pověření patřících do Generace 3 stále existuje řada překážek a výzev, které jsou tématem aktuálního výzkumu v oblasti moderní kryptografie.

3.1 Analýza současného stavu

První konstrukce atributových pověření splňující alespoň část požadavků popsaných výše se začaly objevovat v literatuře okolo roku 2000. Jedná se zejména o schémata Idemix [51] a U-Prove [72], která jsou založena na digitálních podpisech se specifickými vlastnosti. U Idemix tomu byla schopnost měnit digitální podpis i po jeho vydání, bez vlivu na jeho platnost. Uživatel si tak mohl změnit digitální podpis na osobních atributech tak, aby jej vydavatel nepoznal a dosáhl tak anonymity i nespojitelnosti relací. U U-Prove tomu byl podpis, jehož hodnotu vydavatel neznal, přestože se podílel na jeho vytvoření. U obou schémat byla v počátcích zásadním problémem chybějící revokace. Ta byla postupně dodávána až v následujících verzích, zejména u systému Idemix. Objevila se celá řada variant [47, 48, 49, 77, 53], žádná však není zcela praktická pro reálné nasazení. Přehled různých přístupů k revokaci uvádíme ve výčtu níže:

- Zneplatnění identifikátorů pověření [72]: každá autentizační relace obsahuje konstantní anonymní identifikátor (pseudonym), podle kterého lze uživatele revokovat. Tento způsob přímo brání nespojitelnosti relací.
- Zneplatnění atributových klíčů [43, 46, 79]: každá autentizační relace obsahuje ve skryté formě kryptografického závazku atributové klíče. Pokud jsou tyto klíče známy ověřovateli, může je v relaci identifikovat a autentizaci odmítnout. Atributové klíče však v tomto případě musí znát i ověřovatel, nejen uživatel, což je zásadní bezpečnostní riziko.
- Epochy životnosti [47]: každý atribut platí pouze pro omezenou dobu, po jejíž uplynutí musí uživatel o atribut znovu požádat. Tento přístup není použitelný v případech, kde jsou pověření uložena na offline zařízení, např. čipové kartě. Navíc revokace v tomto případě není okamžitá, ale nastane až po změně epochy.
- Kryptografické akumulátory [49, 62, 66, 63]: přístup umožňuje zjistit, zda atributový klíč nebyl zneplatněn pomocí tzv. akumulátoru. Přístup bohužel opět vyžaduje pravidelné aktualizace uživatelských pověření, vždy po odstranění něčích atributů.
- Ověřitelné šifrování [71, 70]: mechanismus umožňuje dešifrovat uživatelský identifikátor či pseudonym v případě porušení pravidel. Přístup je problematický z pohledu možného zneužití a zabránění schopnosti sledovat uživatele prostřednictvím dešifrování na straně ověřovatele.
- Kombinace výše uvedených [64, 80]: některá schémata se snaží kombinovat více přístupů dohromady, bohužel eliminovat jednotlivé slabiny není zcela možné.

K uvedeným schématům přidal tým VUT v Brně vedený autorem této teze i vlastní návrh [11]. Jeho hlavní výhodou byla rychlá a praktická revokace, nevýhodou poměrně velká

náročnost na přenášená data a bezpečnost postrádající formální důkaz. Po roce 2015 byl v kryptografické komunitě udržován zejména systém Idemix, z důvodu nemožnosti zajištění nespojitelnosti u U-Prove a spojení týmů VUT v Brně a IBM Research Lab Zurich za účelem publikace společného řešení. Vznikly tak konstrukce uvedené v sekcích níže. Tyto konstrukce navrhují řešení k aktuálním problémů identifikovaným výše, zejména efektivní konstrukci, revokaci a implementovatelnosti na dostupných zařízeních. Řešení navržená autorem této teze ve spolupráci se spoluautory jsou podrobněji popsána v publikacích [3, 2, 10].

3.2 Problém konstrukce s nízkou výpočetní složitostí

Tato kapitola popisuje první problém spojený s návrhem kryptografických atributových pověření, kterým je příliš vysoká výpočetní složitost existujících systémů. Ty jsou založeny buď na neefektivních algebraických strukturách (např. tzv. RSA grupě využívající modulus o velikosti 3072 bitů a více), jedná se o např. Idemix [51], nebo vyžadují aritmetické operace, které jsou výpočetně velmi náročné a na výkonově omezených zařízeních nerealizovatelné v akceptovatelném čase. Jedná se zejména o operace bilineárního párování, které se často oběvují u nástupců systému Idemix [51]. V kapitole níže, která shrnuje výsledky autora a vědeckého týmu, jsou uvedeny základní principy řešení tohoto problémy pomocí využití tzv. algebraického MACu (Message Authentication Code). Ten umožňuje použití efektivních algebraických struktur s parametry o velikosti řádově stovek bitů, například eliptických křivek, bez nutnosti využít výpočetně náročné operace, jakými je bilineární párování na straně výpočetně omezeného uživatele. Řešení je podrobně popsáno v publikaci [2].

3.2.1 Řešení: protokoly založené na algebraickém MACu

V kryptografii je MAC (Message Authentication Code) obvykle funkcí, která pro (téměř) libovolně dlouhou zprávu vytvoří krátký autentizační tag, který nelze bez znalosti klíče podvrhnout. MAC se obvykle využívá jako jednoduší a rychlejší varianta digitálního podpisu, avšak postrádá nepopiratelnost. Typickým znakem klasického MACu je, že z jeho znalosti nelze odvodit již žádné informace o obsahu zprávy, z níž byl vypočítán. Je to dáno použitím hashovacích funkcí, které jsou z definice funkce jednocestné, tedy jakoukoliv strukturu zprávy a informace o ní ve výstupu "zničí". Toto však neplatí pro tzv. algebraický MAC, který není založen na využití hashovacích funkcí, ale na jednocestných operacích, které se používají v kryptografii, typicky modulárním mocnění. Při zachování stejného účelu, tedy výpočtu autentizačního tagu ze zprávy a klíče, tak algebraické MACy dovolují ještě zachovat informace o konstrukci zprávy a lze tedy výstupy použít v důkazech s nulovou znalostí. Lze tedy například prokázat nejen autentičnost a integritu nějaké zprávy, ale také její znalost, a to bez odhalení zprávy samotné. Této funkce se využívá právě při konstrukci efektivních atributových pověření.

Pro účely využití v atributových pověření jsme v práci [2] definovali vlastní algebraický MAC složený z algoritmů Setup, KeyGen, MAC a Verify. Ty jsou definovány takto:

$\mathsf{Setup}(1^\kappa)$: zvolíme parametry prvočíselné grupy s generátorem g a řádem q jako $par = (\mathbb{G}, g, q)$.

$\mathsf{KeyGen}(par)$: náhodně zvolíme $x_i \leftarrow_r \mathbb{Z}_q^*$ pro $i = (0, \ldots, n)$, kde n je počet zpráv, které chceme vložit do MACu. Vytvoříme tajný klíč $sk = (x_0, \ldots, x_n)$ a veřejné parametry $ipar \leftarrow (X_0, \ldots, X_n)$, kde $X_i = g^{x_i}$.

$\mathsf{MAC}(sk, \vec{m})$: pro tajný klíč $sk = (x_0, \ldots, x_n)$ a množinu zpráv $\vec{m} = (m_1, \ldots, m_n)$ vytvoříme algebraický MAC jako $\sigma = g^{\frac{1}{x_0 + \sum_{i=1}^{n} m_i x_i}}$ a pomocné hodnoty $\sigma_{x_i} \leftarrow \sigma^{x_i}$ for $i = (1, \ldots, n)$[1].

$\mathsf{Verify}(sk, \vec{m}, \sigma)$: s tajným klíčem a zprávami $sk = (x_0, \ldots, x_n)$, $\vec{m} = (m_1, \ldots, m_n)$ můžeme MAC ověřit pomocí rovnice $g \stackrel{?}{=} \sigma^{x_0 + \sum_{i=1}^{n} m_i x_i}$.

Protože v atributových pověřeních není možné využívat opakovaně konstantní hodnotu MAC (vedlo by to ke spojitelnosti relací), je možné MAC tzv. randomizovat, tedy měnit jeho hodnotu, ale zachovat platnost. K tomu je použit algoritmus `Randomize`.

`Randomize`(par, σ): Náhodně zvolíme $r \leftarrow_r \mathbb{Z}_q$ a spočteme nový generátor $h = g^r$ a MAC $\hat{\sigma} = \sigma^r$.

Z popisu výše uvedených algoritmů je patrné, že nevyžadují složité operace bilineárního párování a zároveň udržují strukturu MACu takovou, že vložené zprávy jsou v exponentu, tedy je možné prokázat jejich znalost pomocí protokolů umožňující důkazy znalosti o diskrétních logaritmech. Konkrétně lze prokázat znalost zpráv v MACu, které neleží v množině zveřejněných D, pomocí protokolu popsaného v Camenisch-Stadler [50] notaci jako:

$$PK_{MAC} = PK\{(\langle m_i \rangle_{i \notin D}, r) : \hat{\sigma}_{x_0} \prod_{i \in D} \hat{\sigma}_{x_i}^{m_i} = g^r \prod_{i \notin D} \hat{\sigma}_{x_i}^{-m_i}\}. \tag{3.1}$$

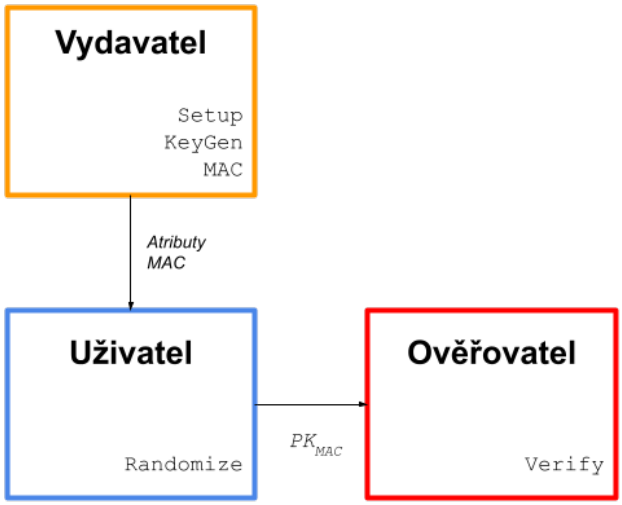
Podrobnosti o protokolech sloužících k důkazům znalosti a způsob jejich konstrukce jsou podrobně popsány v práci autora zde [9].

Pro algebraický MAC uvedený výše byl sestaven formální důkaz bezpečnosti založený na platnosti předpokladu složitosti problému SCDHI (n-Strong Computational Diffie-Hellman Inversion Problem), podrobnosti vč. důkazu jsou uvedeny v plném článku [1].

Výše uvedená konstrukce je pak přímo použitelná při návrhu atributových pověření. V jejich případě Vydavatel spouští algoritmy Setup a KeyGen pro získání základních parametrů a klíčů. Následně vydává Uživateli osobní atributy, které potvrdí právě algebraickým MACem pomocí algoritmu MAC. Uživatel pro přijetí atributů s autentizačním tagem hodnoty MACu randomizuje pomocí algoritmu `Randomize`. Při komunikaci s ověřovatelem pak zasílá pouze pozměněný MAC (tedy Ověřovatel ho není schopen sledovat ani spojovat relace) a prokazuje znalost osobních atributů pomocí protokolu PK_{MAC}. Tento systém je zobrazen na Obrázku 3.2.

Efektivnost systému popsaného výše spočívá zejména ve využití symetrické funkce MAC, která umožňuje ponechat většinu výpočtů na ověřovateli, což je v praxi většinou terminál či výpočetní server. Oproti uživatelskému zařízení, často reprezentovanému čipovou kartou,

[1]Pomocné hodnoty nejsou nutné pro ověření MACu, ale velmi urychlují důkazy znalosti zpráv pomocí protokolů pro důkazy diskrétního logaritmu.



Obr. 3.2: Entity a protokoly systému atributových pověření založeného na algebraickém MACu.

je ověřovatel nesrovnatelně výkonnější, což má velmi pozitivní vliv na běh celého protokolu. Návrh systému byl optimalizován právě pro použití programovatelných karet na uživatelově straně, které nemají podporu složitějších operací, jakou je např. bilineární párování, a mají nízký výpočetní výkon. Srovnání našeho návrhu s ostatními algoritmy je z pohledu výpočetní složitosti uvedeno v Tabulce 3.1. Tabulka udává počet nejnáročnějších operací modulárního mocnění v prvočíselné grupě (Exp. prime), v RSA grupě (Exp. RSA) v závislosti na počtu skrytých atributů (proměnná u). Mimo výkonové parametry udává tabulka i podporu nespojitelnosti, zda systém využívá MAC a jaký má bezpečnostní model. Z tabulky je patrné, že v době vydání publikace byl náš návrh s $(u + 2)$ mocněními v prvočíselné grupě nejrychlejším schématem s podporou nespojitelnosti relací. Výsledky měření z reálné implementace jsou uvedeny dále v Kapitole 3.4.1.

3.3 Problém efektivní revokace

Přestože konstrukce algebraického MACu popsaná výše umožňuje efektivní vydávání a ověřování uživatelských atributů se zachováním funkcí na ochranu soukromí, stále chybí funkcionalita, která by umožňovala uživatelské atributy zneplatnit, neboli revokovat. Jedná se o velmi podstatnou funkci zejména z pohledu vydavatelů a ověřovatelů atributů. Právě pro ně je systém téměř nepoužitelný, pokud nejsou schopni zneplatnit uživatele, kteří porušují pravidla či kterým vypršela doba platnosti jejich atributů.

Způsobů, jak zajistit revokaci uživatelů a jejich osobních atributů, je celá řada. Základní

Tab. 3.1: Srovnání výpočetní složitosti prezentace atributů u různých schémat atributových pověření.

	Exp. prime	**Exp. RSA**	**Nespojitelnost**	**MAC**	**Model**
U-Prove [72]	$u+1$	0	✗	✗	-
Idemix [51]	0	$u+3$	✓	✗	sRSA [76]
Ringers et al. [75]	$n+u+9$	0	✓	✗	whLRSW [81]
MACDDH [52]	$6u+12$	0	✓	✓	DDH [44]
MACGGM [52]	$5u+4$	0	✓	✓	GGM [78]
MACBB [42]	$u+12$	0	✓	✓	q-sDH [45]
NIKVAC [54]	$2u+3$	0	✓	✓	GGM+IND-CPA
Naše schéma	$u+2$	0	✓	✓	n-SCDHI [2]

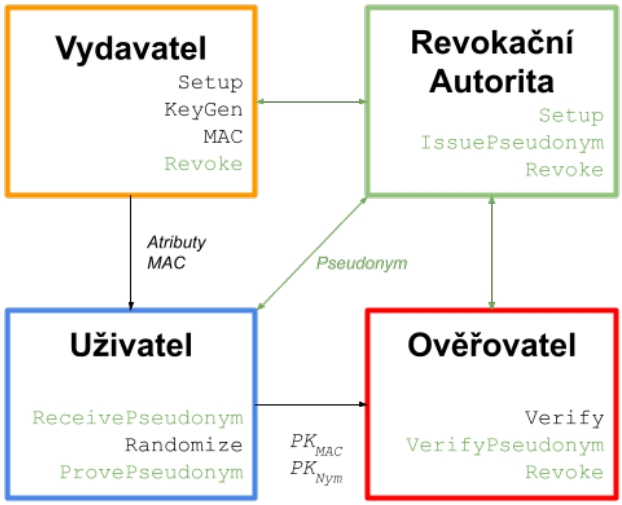
přístupy jsou identifikovány již v Kapitole 3.1 výše, podrobný popis je uveden např. v práci autora [3]. V této kapitole představíme přístup založený na konstrukci algebraického MACu popsaného v předchozí kapitole a kombinujícího přístupy omezení počtů randomizace a epoch platnosti. Výsledky uvedené v této části vycházejí zejména ze článku [3], v němž je možné nalézt podrobnější popis, formální důkazy i další odkazy na literaturu.

3.3.1 Řešení: kombinace epoch platnosti a omezené randomizace

Systém atributových pověření, tak jak byl popsán v Kapitole 3.2.1 a zobrazen na Obrázku 3.1, poskytuje úplnou ochranu soukromí, tedy anonymitu, nespojitelnost relací a nesledovatelnost uživatele ostatními entitami. Abychom byli schopni zavést mechanismy na revokaci uživatelů, je nutné základní schéma rozšířit o novou entitu Revokační Autority a algoritmy zajišťující schopnost identifikace a sledování uživatele v oprávněných případech. Aktualizované blokové schéma uvádíme na Obrázku 3.3, nově přidané komponenty značíme zeleně. Dodané algoritmy pro revokaci jsou následující:

- $(spar, pk_{RA}, sk_{RA}) \leftarrow$`Setup`$(1^{\mathcal{K}}, n)$: algoritmus má na vstupu bezpečnostní parametr $1^{\mathcal{K}}$ a proměnnou n označující maximální počet autentizačních relací, které je schopen uživatel vygenerovat. Výstupem algoritmu jsou systémové parametry $spar$, veřejný klíč pk_{RA} a soukromý klíč Revokační Autority sk_{RA}.
- $(rh') \leftarrow$ `IssuePseudonym`$(spar, sk_{RA}, rh) \leftrightarrow$ `ReceivePseudonym`$(spar, pk_{RA}) \rightarrow (w)$: do algoritmu vstupují na straně RA systémové parametry $spar$, soukromý klíč revokační autority sk_{RA} a seznam tzv. revokačních pojítek rh, na straně uživatele pouze veřejné parametry $spar, pk_{RA}$. Výstupem RA je aktualizovaný seznam revokačních pojítek rh'. Výstupem uživatele je jeho vlastní revokační pojítko w[2].
- $(C, \pi, c) \leftarrow$`ProvePseudonym`$(spar, w, epoch, ctr)$: algoritmus má na vstupu systémové parametry $spar$, revokační pojítko w, aktuální čas $epoch$ a čítač ctr. Výstupem algoritmu je pseudonym C, kryptografický závazek k revokačnímu pojítku c a důkaz znalosti o

[2]Jedná se o unikátní hodnotu, které propojuje uživatelovo pověření a pseudonym a které je v případě potřeby použito k zneplatnění pověření.



Obr. 3.3: Entity a protokoly systému atributových pověření s revokací.

správné konstrukci těchto hodnot π.

- $(0/1) \leftarrow$ `VerifyPseudonym` $(spar, pk_{RA}, C, \pi, c, epoch, RL_{epoch})$: vstupem algoritmu jsou systémové parametry $spar$, veřejný klíč pk_{RA}, pseudonym C s odpovídajícím důkazem π a závazek c s odpovídajícím revokačním seznamem RL_{epoch}. Výstupem je 1 pokud pseudonym a důkaz jeho konstrukce je správný, v opačném případě algoritmus vrátí 0.
- $(RL_{epoch}, rd', revoked') \leftarrow$ `Revoke`$(spar, rh, rd, \{C_R, epoch_R\}, epoch, revoked)$: vstupem algoritmu jsou systémové parametry $spar$, seznam revokačních pojítek rh, revokační databáze rd, pseudonym uživatele, který má být revokován C_R a identifikátor relevantní epochy $epoch_R$ a seznam revokovaných pojítek $revoked$. Výstupem je aktualizovaný revokační seznam pro další epochu RL_{epoch} aktualizovaná revokační databáze rd' a aktualizovaný seznam revokačních pojítek $revoked'$.

Základní myšlenkou kryptografického systému popsaného výše je vydat uživateli unikátní identifikátor, tzv. pseudonym C, který bude nespojitelný s jeho identitou a který bude moci uživatel maximálně $n$krát změnit bez vlivu na jeho platnost. Pro každou autentizační relaci tedy bude schopen nejen prokázat své osobní atributy, ale bude nucen prezentovat i tento pseudonym a jeho autentičnost, tj. že byl skutečně vydán Revokační Autoritou. Po n autentizačních relacích bude nucen požádat o pseudonym nový, jinak začnou být jeho relace spojitelné. Zároveň je pseudonym použitelný pouze v určitém časovém okně, tzv. epoše $epoch$, například týdnu. V případě, že dojde k porušení pravidel, či uživatel sám zažádá o odstranění ze systému, seznam jeho pseudonymů pro danou epochu RA zveřejní na veřejném seznamu, tzv. blacklistu RL_{epoch}. Všechny uživatelovy relace tedy budou ověřovatelem odmítnuty, jelikož ten během ověřovací relace kontroluje, zda není pseudonym na blacklistu.

Tab. 3.2: Výpočetní složitost algoritmů revokačního schématu.

	Uživatel	**RA**	**Ověřovatel**
`IssuePseudonym`	0P, 0E, 0L	0P, 0E, 0L	-
`ProvePseudonym`	$(5j + 3)$E	-	-
`VerifyPseudonym`	-	-	$2j$P $(4 + 3j)$E $\log(k^j\|U_R\|)$L
`Revoke`	-	$k^j\|U\|$E $\log(k^j\|U\|)$L	-

$|U_R|$: celkový počet revokovaných uživatelů.

$|U|$: celkový počet uživatelů.

P: operace bilineárního párování.

E: operace skalárního násobení bodu na eliptické křivce.

L: Look-ups: počet vyhledávání v setříděné tabulce.

Abychom svázali pseudonym a atributové pověření, využíváme tzv. revokační pojítko w, které je vloženo jak do pseudonymu, tak do pověření jako specifický osobní atribut. Uživatel pak během kryptografického důkazu vlastnictví atributů také prokazuje, že pseudonym je založen na stejném pojítku, jaké je vloženo také do pověření. Uživatel je tak se svými pseudonymy svázán a není možné použít cizí pseudonym k prokázání svých atributů. Pro důkazy znalostí atributů, pojítka a jejich vztahů se opět používají kryptografické protokoly pro důkazy o diskrétních logaritmech ve strukturách eliptických křivek.

Konkrétní specifikace kryptografických protokolů obecně popsaných výše je uvedena ve článku [3], kde je uveden také formální důkaz bezpečnosti revokačního systému. Protože je jeho primárním účelem použití na výkonově omezených zařízeních, uvádíme zde také analýzu složitosti jednotlivých algoritmů, ze které vyplývá, že systém je vhodný i po implementaci na výkonově omezených zařízeních, jakými jsou čipové karty. Analýza je uvedena v Tabulce 3.2.

3.4 Problém reálné implementace na embedded zařízeních

V Kapitole 3.2.1 byl popsán teoretický návrh systému kryptografických atributových pověření. Hlavní motivací tohoto návrhu bylo vytvořit technologii, která bude splňovat všechny bezpečnostní požadavky, bude podporovat všechny potřebné funkce na ochranu soukromí a na rozdíl od v té době existujících systémů bude implementovatelná v praxi na reálných zařízeních. Obdobný cíl byl stanoven i během návrhu systému pro efektivní revokaci, který byl popsán v Kapitole 3.3.1. Nízká výpočetní a paměťová složitost a schopnost běhu na výkonově velmi omezených zařízeních byla hlavním přínosem těchto návrhů a odlišovala je od ostatních existujících kryptosystémů. V následující kapitole uvádíme výkonovou analýzu a výsledky z implementace

navržených algoritmů. Tyto výsledky jsou podobněji popsány ve článcích [10, 4].

3.4.1 Řešení: systém Privacy-ABC pro čipové karty

Systém atributových pověření s efektivní revokací, tak jak byl obecně popsán v textu výše a podrobně specifikován v publikacích [3, 2], byl experimentálně implementován v prostředí, kde Uživatelovy algoritmy běží na programovatelné čipové kartě a ověřovací terminál realizovaný embedded systémem spouští algoritmy Ověřovatele. Ostatní entity byly reprezentovány standardními počítači. Toto nastavení reflektuje reálný případ použití atributových pověření např. při řízení přístupu do budov či použití v hromadné dopravě, kde v budoucnu předpokládáme např. použití elektronických dokladů jako dokazovacích faktorů. Konkrétní protokol pro ověření uživatele byl implementován dle specifikace na Obrázku 3.4, který uvádíme pouze pro ilustraci a seznámení čtenáře s počtem a typem operací, které musí čipová karta vykonat. Pro konkrétní popis algoritmů, definici proměnných a bližší detaily odkazujeme čtenáře na publikaci [10]. Proměnné a operace schématu atributového pověření je znázorněno černě, revokační schéma červeně.

Výsledky měření času nutného pro výpočet všech kryptografických hodnot na straně čipové karty a jejich ověření na straně terminálu jsou uvedeny na Obrázku 3.5. Je prezentován průměr z 10 měření pro různé počty uložených osobních atributů a různé počty atributů uložených na kartě. Konkrétní parametry kryptografického systému, hardwaru a softwaru byly během měření následující:

- algebraická struktura: eliptická křivka Barreto-Naehrig o velikosti 254b podporující bilineární párování (BN-254),
- hardware Uživatele: čipová karta MCU SC23Z018, 1.75 kB RAM, 252 kB ROM, 18 kB EEPROM, OS MultOSv4.3.1,
- hardware Ověřovatele: Raspberry Pi 4 Model B, ARM Cortex-A72, 4 GB RAM, Raspberry Pi OS 4.19 – 32b.

Z grafů uvedených na Obrázku 3.5 vyplývá, že systém bez revokace potřebuje zhruba 600 ms - 1100 ms pro prokázání vlastnictví osobních atributů, a to včetně režie způsobené přenosem dat mezi kartou a terminálem pomocí RFID rozhraní. Tato hodnota je akceptovatelná pro reálné nasazení například v systémech řízení přístupu do budov. Při aktivní revokaci vyžaduje implementace systému zhruba 2 s - 2,6 s pro ověření uživatele. To je akceptovatelné např. pro řízení přístupu k elektronickým službám, nikoliv pro řízení fyzického přístupu, kde je nutná další optimalizace. Za zmínku stojí poměrně velká režie způsobená komunikací v případě aktivní revokace, která přidává až 50% času. Nejsnazší způsob optimalizace doby běhu algoritmů tedy vidíme ve volbě výkonnějších čipových karet a případně optimalizaci přenosových protokolů. Naměřené hodnoty však prokazují praktickou implementovatelnost navrženého kryptografického systému na reálných zařízeních, které jsou již řadu let na trhu.

Uživatel $\mathcal{U}$ **Ověřovatel $\mathcal{V}$**

$$params_{\mathrm{I}} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_{\mathrm{T}}, g_1, g_2, \mathbf{e})$$
$$params_{\mathrm{RA}} = (k, j, (h_1, \ldots, h_j), (\alpha_1, \ldots, \alpha_j))$$
$$pk_{\mathrm{RA}}, RL$$

$Attributes : (m_1, \ldots, m_{n-1}, m_{\mathrm{r}})$
$\sigma, (\sigma_{x_1}, \ldots, \sigma_{x_{n-1}}, \sigma_{x_{\mathrm{r}}})$ $\qquad sk_{\mathrm{V}} = (x_0, \ldots, x_{n-1}, x_{\mathrm{r}})$

$\xleftarrow{nonce,\ epoch}$

$Randomizers : \{(e_1, \sigma_{e_1}), \ldots, (e_k, \sigma_{e_k})\}$
$e_I, e_{II} \xleftarrow{\$} (e_1, \ldots, e_k)$
$\sigma_{e_I}, \sigma_{e_{II}} \xleftarrow{\$} (\sigma_{e_1}, \ldots, \sigma_{e_k})$
$i \leftarrow \alpha_1 e_I + \alpha_2 e_{II}$
$C \leftarrow g_1^{\frac{1}{i - m_{\mathrm{r}} + \mathcal{H}(epoch)}}$
$\rho, \rho_v, \rho_i, \rho_{m_{\mathrm{r}}}, \rho_{m_{z \notin D}}, \rho_{e_I}, \rho_{e_{II}} \xleftarrow{\$} \mathbb{Z}_q$
$\hat{\sigma} \leftarrow \sigma^{\rho}$
$\hat{\sigma}_{e_I} \leftarrow \sigma_{e_I}^{\rho}, \hat{\sigma}_{e_{II}} \leftarrow \sigma_{e_{II}}^{\rho}$
$\bar{\sigma}_{e_I} \leftarrow \hat{\sigma}_{e_I}^{-e_I} g_1^{\rho}, \bar{\sigma}_{e_{II}} \leftarrow \hat{\sigma}_{e_{II}}^{-e_{II}} g_1^{\rho}$

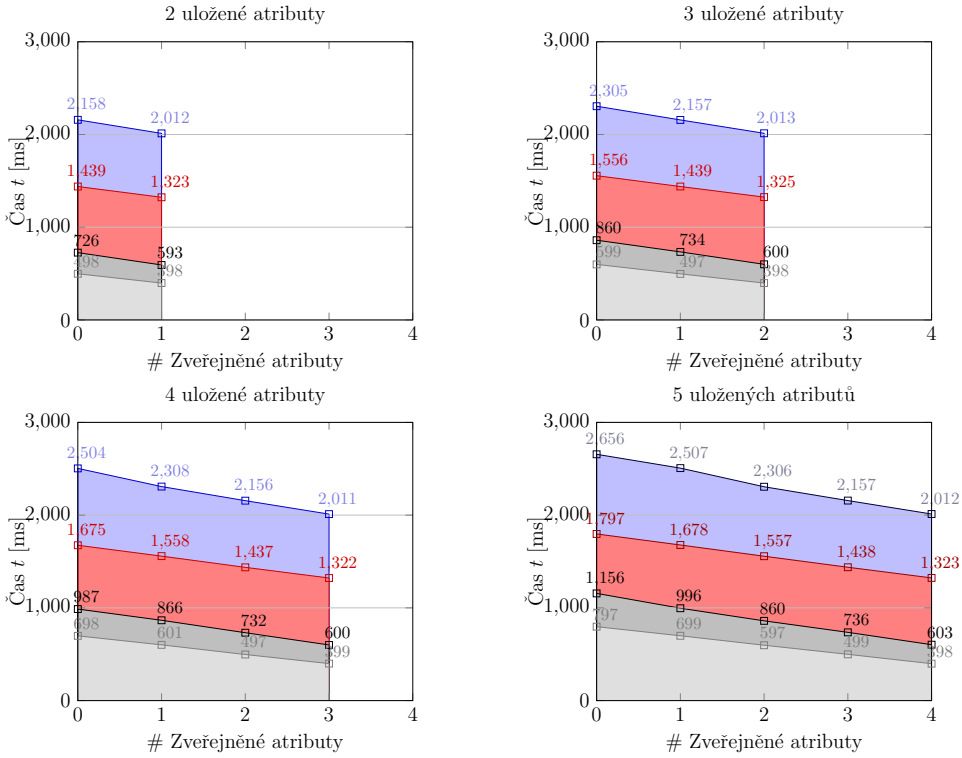
$t_{\mathrm{verify}} \leftarrow g_1^{\rho_v} \sigma_{x_{\mathrm{r}}}^{\rho_{m_{\mathrm{r}}} \rho} \prod_{z \notin D} \sigma_{x_z}^{\rho_{m_z} \rho}$
$t_{\mathrm{revoke}} \leftarrow C^{\rho_{m_{\mathrm{r}}}} C^{\rho_i}$
$t_{\mathrm{sig}} \leftarrow g_1^{\rho_i} h_1^{\rho_{e_I}} h_2^{\rho_{e_{II}}}, t_{\mathrm{sigI}} \leftarrow g_1^{\rho_v} \hat{\sigma}_{e_I}^{\rho_{e_I}}, t_{\mathrm{sigII}} \leftarrow g_1^{\rho_v} \hat{\sigma}_{e_{II}}^{\rho_{e_{II}}}$
$e \leftarrow \mathcal{H}(t_{\mathrm{verify}}, t_{\mathrm{revoke}}, t_{\mathrm{sig}}, t_{\mathrm{sigI}}, t_{\mathrm{sigII}}, \hat{\sigma}, \hat{\sigma}_{e_I}, \bar{\sigma}_{e_I}, \hat{\sigma}_{e_{II}}, \bar{\sigma}_{e_{II}}, C, nonce)$

$\langle s_{m_z} \leftarrow \rho_{m_z} - e m_z \rangle_{z \notin D}$
$s_v \leftarrow \rho_v + e\rho$
$s_{m_{\mathrm{r}}} \leftarrow \rho_{m_{\mathrm{r}}} - e m_{\mathrm{r}}$
$s_i \leftarrow \rho_i + ei$
$s_{e_I} \leftarrow \rho_{e_I} - e e_I, s_{e_{II}} \leftarrow \rho_{e_{II}} - e e_{II}$
$\pi \leftarrow (e, s_{m_{z \notin D}}, s_v, s_{m_{\mathrm{r}}}, s_i, s_{e_I}, s_{e_{II}})$

$\xrightarrow{m_{z \in D}, \pi, C, \hat{\sigma}, \hat{\sigma}_{e_I}, \bar{\sigma}_{e_I}, \hat{\sigma}_{e_{II}}, \bar{\sigma}_{e_{II}}}$

$t_{\mathrm{verify}} \leftarrow \hat{\sigma}^{-e x_0} g_1^{s_v} \hat{\sigma}^{x_{\mathrm{r}} s_{m_{\mathrm{r}}}} \prod_{z \notin D} \hat{\sigma}^{x_z s_{m_z}} \prod_{z \in D} \hat{\sigma}^{-e x_z m_z}$
$t_{\mathrm{revoke}} \leftarrow (g_1 C^{-\mathcal{H}(epoch)})^{-e} C^{s_{m_{\mathrm{r}}}} C^{s_i}$
$t_{\mathrm{sig}} \leftarrow g_1^{s_i} h_1^{s_{e_I}} h_2^{s_{e_{II}}}, t_{\mathrm{sigI}} \leftarrow g_1^{s_v} \hat{\sigma}_{e_I}^{s_{e_I}} \bar{\sigma}_{e_I}^{-e}, t_{\mathrm{sigII}} \leftarrow g_1^{s_v} \hat{\sigma}_{e_{II}}^{s_{e_{II}}} \bar{\sigma}_{e_{II}}^{-e}$
$e \stackrel{?}{=} \mathcal{H}(t_{\mathrm{verify}}, t_{\mathrm{revoke}}, t_{\mathrm{sig}}, t_{\mathrm{sigI}}, t_{\mathrm{sigII}}, \hat{\sigma}, \hat{\sigma}_{e_I}, \bar{\sigma}_{e_I}, \hat{\sigma}_{e_{II}}, \bar{\sigma}_{e_{II}}, C, nonce)$
$\mathbf{e}(\bar{\sigma}_{e_I}, g_2) \stackrel{?}{=} \mathbf{e}(\hat{\sigma}_{e_I}, pk_{\mathrm{RA}})$
$\mathbf{e}(\bar{\sigma}_{e_{II}}, g_2) \stackrel{?}{=} \mathbf{e}(\hat{\sigma}_{e_{II}}, pk_{\mathrm{RA}})$
$C \notin RL$

Obr. 3.4: Specifikace algoritmů `Show` a `Verify` použitá pro implementaci na čipové kartě a terminálu. Definice proměnných a podrobný technický popis je uveden v [10].



Obr. 3.5: Čas nutný k ověření uživatele: červeně - čas ověření atributů včetně revokace, modře - celkový čas s komunikací, světle šedě - čas ověření atributů bez revokace a tmavě šedě - celkový čas bez revokace s komunikací.

4 DALŠÍ TRENDY V MODERNÍ KRYPTOGRAFII

V této práci jsme se věnovali primárně kryptografickým systémům pro ochranu soukromí (angl. Privacy Enhancing Technologies, zkratka PETs). Důvodem pro toto zaměření jsou předešlé zkušenosti a výsledky autora a jeho týmu v této oblasti. Je třeba však připomenout, že moderní kryptografie je velmi široká oblast, ve které popsané technologie zastupují jen malou část. Principy, které byly v této práci představeny, však najdou silné využití i mimo technologie na ochranu soukromí. Zejména interaktivní důkazové systémy založené na protokolech s nulovou znalostí a jejich efektivní varianty, tzv. Σ-protokoly, bývají velmi často využívány i v klasických autentizačních systémech, komunikačních systémech pro výkonově omezená zařízení, systémech s autentizovaným šifrováním či různých protokolech pro decentralizované systémy. Inspirace algoritmy představenými v této práci je patrná například u systémů pro sběr dat ze senzorů [30, 35, 34], systémů pro řízení přístupu na základě silné autentizace [13] či například komunikačních systémů pro dopravní prostředky, tzv. VANETs[1] [19].

Rozsah této práce neumožnil bližší popis dalších oblastí moderní kryptografie, které jsou neméně důležité a ve kterých je výzkumný tým VUT v Brně v současnosti aktivní. Jedná se například o oblasti kvantové a postkvantové kryptografie [28, 25], optimalizace kryptografických systémů pro hardwarově akcelerované implementace [32, 24, 40, 33], či návrhy kryptografických systémů pro výkonově omezená zařízení [34]. Bližší informace je tak možné nalézt na stránkách výzkumné skupiny AXE[2].

V neposlední řadě považujeme za důležité zmínit důležitost zastoupení kryptografie a obecněji kybernetické bezpečnosti ve vzdělávání. Při současném dynamickém rozvoji informačních a komunikačních systémů a v nich používaných kryptografických mechanismů je podstatnou součástí rozvoje této oblasti i její začlenění do výukových programů a studijních plánů. Zejména kyberbezpečnost se však svojí interdisciplinaritou vymyká klasickému pojetí výuky v rámci separátních předmětů a vyžaduje hlubší způsob integrace do studijních plánů. I v této oblasti je VUT v Brně v rámci skupiny AXE aktivní a tvoří celou řadu výsledků se svými partnery [22, 21, 23].

5 ZÁVĚR

Cílem této teze bylo představit vybrané trendy v oblasti moderní kryptografie, zejména návrhu autentizačních protokolů a protokolů na ochranu soukromí. Z důvodu omezeného rozsahu jsme se soustředili na poměrně úzkou oblast tzv. kryptografických atributových pověření, které tvořily jeden z pilířů výzkumných aktivit skupiny AXE VUT v Brně. V tezi jsme popsali hlavní principy kryptografického návrhu samotných atributových pověření a dále tzv. revokačních schémat, které se používají pro identifikaci útočníků a zneplatnění uživatelských pověření. Právě efektivní revokační schémata představují nejvýznamnější přínos autora vědecké komu-

[1] VANET: Vehicular Ad-Hoc Network
[2] https://axe.vut.cz

nitě, zejména z důvodu chybějící existence efektivních algoritmů před publikací autorových prací. V rámci této teze jsme představili celou cestu uvedení atributových pověření s efektivní revokací do praxe, od základního teoretického návrhu algoritmů, přes formální důkaz bezpečnosti, integraci jednotlivých komponent až po implementaci a měření na reálných zařízeních. Využitelnost uvedených výsledků výzkumu a vývoje je podpořena využitím návrhů v praktických produktech komerčních partnerů a úspěšnými projekty VaV, které byly díky výzkumu popsanému v této tezi zdárně dokončeny.

Přestože byly v rámci této teze prezentovány ucelené výsledky kryptografického návrhu, bezpečnostní analýzy i implementace, stále ještě existuje řada výzev pro další výzkum. Zde představené protokoly jsou prokazatelně bezpečné a v praxi implementovatelné, avšak stále mají své slabiny. Mezi nejvýznamnější patří například zranitelnost vůči útokům kvantovými počítači (což je problém naprosté většiny asymetrických systémů používaných v praxi) či poměrně vysoká výpočetní náročnost na straně revokační autority a nutnost sdílení symetrického klíče mezi vydavatelem atributů a ověřovatelem. Řešením může být využití nových algebraických struktur, například mřížek, které jsou hojně využívány v současných návrzích jednodušších postkvantových systémů.

REFERENCE

Vybrané publikace autora

[1] Camenisch, Jan, Drijvers, Manu, Dzurenda, Petr, and Hajny, Jan. *Fast Keyed-Verification Anonymous Credentials on Standard Smart Cards*. Cryptology ePrint Archive, Paper 2019/460, 2019. doi:10.1007/978-3-030-22312-0. `https://eprint.iacr.org/2019/460`.
URL `https://eprint.iacr.org/2019/460`

[2] Camenisch, Jan, Drijvers, Manu, Dzurenda, Petr, and Hajny, Jan. *Fast Keyed-Verification Anonymous Credentials on Standard Smart Cards*. In Gurpreet Dhillon, Fredrik Karlsson, Karin Hedström, and André Zúquete, editors, ICT Systems Security and Privacy Protection, pp. 286–298. Cham: Springer International Publishing, 2019. ISBN 978-3-030-22312-0.

[3] Camenisch, Jan, Drijvers, Manu, and Hajny, Jan. *Scalable Revocation Scheme for Anonymous Credentials Based on N-Times Unlinkable Proofs*. In Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society, WPES'16, pp. 123–133. New York, NY, USA: Association for Computing Machinery, 2016. ISBN 9781450345699. doi:10.1145/2994620.2994625.
URL `https://doi.org/10.1145/2994620.2994625`

[4] Casanova-Marqués, Raúl, Dzurenda, Petr, and Hajny, Jan. *Implementation of Revocable Keyed-Verification Anonymous Credentials on Java Card*. In Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES '22. New York, NY, USA: Association for Computing Machinery, 2022. ISBN 9781450396707. doi:10.1145/3538969.3543798.
URL `https://doi.org/10.1145/3538969.3543798`

[5] Dzurenda, Petr, Casanova-Marqués, Raúl, Malina, Lukas, and Hajny, Jan. *Real-World Deployment of Privacy-Enhancing Authentication System Using Attribute-Based Credentials*. In Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES '22. New York, NY, USA: Association for Computing Machinery, 2022. ISBN 9781450396707. doi:10.1145/3538969.3543803.
URL `https://doi.org/10.1145/3538969.3543803`

[6] Hajny, J. *Úvod do Zero-Knowledge protokolů*. "`http://www.elektrorevue.cz/cz/clanky/komunikacni-technologie/230/uvod-do-zero-knowledge-protokolu/`", 2008.

[7] Hajny, J., Malina, L., and Zeman, V. *Practical anonymous authentication - Designing anonymous authentication for everyday use*. In Proceedings of the 8th International

Conference on Security and Cryptography (SECRYPT 2011), pp. 405–408. 2011. ISBN 978-989-8425-18- 8.

[8] Hajny, Jan. Authentication Protocols and Privacy Protection. Ph.D. thesis, Brno University of Technology, 2012.

[9] Hajný, Jan. *Cryptographic Proofs of Knowledge and Their Usage in Systems Protecting Digital Identity.* Print, 2016.

[10] Hajny, Jan, Dzurenda, Petr, Casanova-Marques, Raul, and Malina, Lukas. *Privacy ABCs: Now Ready for Your Wallets!* In 2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), pp. 686–691. 2021. doi:10.1109/PerComWorkshops51409.2021.9431139.

[11] Hajny, Jan, Dzurenda, Petr, and Malina, Lukas. *Privacy-PAC: Privacy-Enhanced Physical Access Control.* In Proceedings of the 13th Workshop on Privacy in the Electronic Society, pp. 93–96. New York, NY, USA: ACM, 2014. ISBN 978-1-4503-3148-7. doi: 10.1145/2665943.2665969.
URL http://doi.acm.org/10.1145/2665943.2665969

[12] Hajny, Jan, Dzurenda, Petr, and Malina, Lukas. *Attribute-based credentials with cryptographic collusion prevention.* Security and Communication Networks, 8(18):3836–3846, 2015. doi:https://doi.org/10.1002/sec.1304.
URL https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1304

[13] Hajny, Jan, Dzurenda, Petr, and Malina, Lukas. *Secure Physical Access Control with Strong Cryptographic Protection.* In Proceedings of the 12th International Conference on Security and Cryptography (SECRYPT 2015), pp. 220–227. 2015. ISBN 978-989-758-117-5. doi:10.5220/0005524202200227.

[14] Hajny, Jan, Dzurenda, Petr, Malina, Lukas, and Zeman, Vaclav. *Cryptography for Privacy- Preserving Electronic Services.* In 37th International Conference on Telecommunications and Signal Processing (TSP). 2014. ISBN 978-80-214-4983-1.

[15] Hajny, Jan and Malina, Lukas. *Practical Revocable Anonymous Credentials.* In Bart De Decker and DavidW. Chadwick, editors, Communications and Multimedia Security, vol. 7394 of *Lecture Notes in Computer Science*, pp. 211–213. Springer Berlin Heidelberg, 2012. ISBN 978-3-642-32804-6. doi:10.1007/978-3-642-32805-3_22.
URL http://dx.doi.org/10.1007/978-3-642-32805-3_22

[16] Hajny, Jan and Malina, Lukas. *Unlinkable Attribute-Based Credentials with Practical Revocation on Smart-Cards.* In Stefan Mangard, editor, Smart Card Research and Advanced Applications, vol. 7771 of *Lecture Notes in Computer Science*, pp. 62–76. Springer Berlin Heidelberg, 2013. ISBN 978-3-642-37287-2. doi:10.1007/978-3-642-37288-9_5.
URL http://dx.doi.org/10.1007/978-3-642-37288-9_5

[17] Hajny, Jan, Malina, Lukas, and Dzurenda, Petr. *Practical Privacy-Enhancing Technologies*. In 38th International Conference on Telecommunications and Signal Processing (TSP). 2015. ISBN 978-1-4799-8498-5.

[18] Hajny, Jan, Malina, Lukas, Martinasek, Zdenek, and Tethal, Ondrej. *Performance Evaluation of Primitives for Privacy-Enhancing Cryptography on Current Smart-Cards and Smart-Phones*. In Joaquin Garcia-Alfaro, Georgios Lioudakis, Nora Cuppens-Boulahia, Simon Foley, and William M. Fitzgerald, editors, Data Privacy Management and Autonomous Spontaneous Security, vol. 8247 of *Lecture Notes in Computer Science*, pp. 17–33. Springer Berlin Heidelberg, 2014. ISBN 978-3-642-54567-2. doi: 10.1007/978-3-642-54568-9_2.
URL http://dx.doi.org/10.1007/978-3-642-54568-9_2

[19] Hajny, Jan, Malina, Lukas, Martinasek, Zdenek, and Zeman, Vaclav. *Privacy-preserving SVANETs - Privacy-preserving Simple Vehicular Ad-hoc Networks*. In SECRYPT 2013 - Proceedings of the 10th International Conference on Security and Cryptography, Reykjavík, Iceland, 29-31 July, 2013, pp. 267–274. 2013. ISBN 978-989-8565-73-0.

[20] Hajny, Jan, Malina, Lukas, and Tethal, Ondrej. *Privacy-Friendly Access Control Based on Personal Attributes*. In Maki Yoshida and Koichi Mouri, editors, Advances in Information and Computer Security, vol. 8639 of *Lecture Notes in Computer Science*, pp. 1–16. Springer International Publishing, 2014. ISBN 978-3-319-09842-5.

[21] Hajny, Jan, Ricci, Sara, Piesarskas, Edmundas, Levillain, Olivier, Galletta, Letterio, and De Nicola, Rocco. *Framework, Tools and Good Practices for Cybersecurity Curricula*. IEEE Access, 9:94723–94747, 2021. doi:10.1109/ACCESS.2021.3093952.

[22] Hajny, Jan, Ricci, Sara, Piesarskas, Edmundas, and Sikora, Marek. *Cybersecurity Curricula Designer*. In Proceedings of the 16th International Conference on Availability, Reliability and Security, ARES 21. New York, NY, USA: Association for Computing Machinery, 2021. ISBN 9781450390514. doi:10.1145/3465481.3469183.
URL https://doi.org/10.1145/3465481.3469183

[23] Hajny, Jan, Sikora, Marek, Grammatopoulos, Athanasios Vasileios, and Di Franco, Fabio. *Adding European Cybersecurity Skills Framework into Curricula Designer*. In Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES '22. New York, NY, USA: Association for Computing Machinery, 2022. ISBN 9781450396707. doi:10.1145/3538969.3543799.
URL https://doi.org/10.1145/3538969.3543799

[24] Jedlicka, Petr, Malina, Lukas, Socha, Petr, Gerlich, Tomas, Martinasek, Zdenek, and Hajny, Jan. *On Secure and Side-Channel Resistant Hardware Implementations of Post-Quantum Cryptography*. In Proceedings of the 17th International Conference on

Availability, Reliability and Security, ARES '22. New York, NY, USA: Association for Computing Machinery, 2022. ISBN 9781450396707. doi:10.1145/3538969.3544423. URL https://doi.org/10.1145/3538969.3544423

[25] Klicnik, Ondrej, Munster, Petr, Horvath, Tomas, Hajny, Jan, and Malina, Lukas. *Quantum Key Distribution Polygon.* In 2021 13th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), pp. 263–266. 2021. doi:10.1109/ICUMT54235.2021.9631732.

[26] Klicnik, Ondrej, Tomasov, Adrian, Munster, Petr, Horvath, Tomas, and Hajny, Jan. *Long-term Parameters Monitoring of the IDQ Clavis 3 QKD System.* In 2022 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp. 1–4. 2022. doi:10.23919/SoftCOM55329.2022.9911354.

[27] Malina, Lukas, Castellà-Roca, Jordi, Vives-Guasch, Arnau, and Hajny, Jan. *Short-Term Linkable Group Signatures with Categorized Batch Verification.* In Joaquin Garcia-Alfaro, Frédéric Cuppens, Nora Cuppens-Boulahia, Ali Miri, and Nadia Tawbi, editors, Foundations and Practice of Security, vol. 7743 of *Lecture Notes in Computer Science*, pp. 244–260. Springer Berlin Heidelberg, 2013. ISBN 978-3-642-37118-9. doi:10.1007/978-3-642-37119-6_16.

[28] Malina, Lukas, Dzurenda, Petr, Ricci, Sara, Hajny, Jan, Srivastava, Gautam, Matulevičius, Raimundas, Affia, Abasi-Amefon O., Laurent, Maryline, Sultan, Nazatul Haque, and Tang, Qiang. *Post-Quantum Era Privacy Protection for Intelligent Infrastructures.* IEEE Access, 9:36038–36077, 2021. doi:10.1109/ACCESS.2021.3062201.

[29] Malina, Lukas and Hajny, Jan. *Privacy-preserving framework for geosocial applications.* Security and Communication Networks, 7(11):1764–1779, 2014. ISSN 1939-0122.

[30] Malina, Lukas, Hajny, Jan, Fujdiak, Radek, and Hosek, Jiri. *On Perspective of Security and Privacy-Preserving Solutions in the Internet of Things.* Comput. Netw., 102(C):83–95, 2016. ISSN 1389-1286. doi:10.1016/j.comnet.2016.03.011. URL https://doi.org/10.1016/j.comnet.2016.03.011

[31] Malina, Lukas, Hajny, Jan, and Martinasek, Zdenek. *Efficient Group Signatures with Verifier-local Revocation Employing a Natural Expiration.* In SECRYPT, pp. 555–560. 2013. ISBN 978-989-8565-73-0.

[32] Malina, Lukas, Ricci, Sara, Dobias, Patrik, Jedlicka, Petr, Hajny, Jan, and Choo, Kim-Kwang. *On the Efficiency and Security of Quantum-resistant Key Establishment Mechanisms on FPGA Platforms.* In Proceedings of the 19th International Conference on Security and Cryptography - Volume 1: SECRYPT,, pp. 605–613. INSTICC, SciTePress, 2022. ISBN 978-989-758-590-6. doi:10.5220/0011294200003283.

[33] Malina, Lukas, Ricci, Sara, Dzurenda, Petr, Smekal, David, Hajny, Jan, and Gerlich, Tomas. *Towards Practical Deployment of Post-quantum Cryptography on Constrained Platforms and Hardware-Accelerated Platforms.* In Emil Simion and Rémi Géraud-Stewart, editors, Innovative Security Solutions for Information Technology and Communications, pp. 109–124. Cham: Springer International Publishing, 2020. ISBN 978-3-030-41025-4.

[34] Malina, Lukas, Srivastava, Gautam, Dzurenda, Petr, Hajny, Jan, and Fujdiak, Radek. *A Secure Publish/Subscribe Protocol for Internet of Things.* In Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES '19. New York, NY, USA: Association for Computing Machinery, 2019. ISBN 9781450371643. doi:10.1145/3339252.3340503.
URL `https://doi.org/10.1145/3339252.3340503`

[35] Malina, Lukas, Srivastava, Gautam, Dzurenda, Petr, Hajny, Jan, and Ricci, Sara. *A Privacy-Enhancing Framework for Internet of Things Services.* In Network and System Security: 13th International Conference, NSS 2019, Sapporo, Japan, December 15–18, 2019, Proceedings, pp. 77–97. Berlin, Heidelberg: Springer-Verlag, 2019. ISBN 978-3-030-36937-8. doi:10.1007/978-3-030-36938-5_5.
URL `https://doi.org/10.1007/978-3-030-36938-5_5`

[36] Martinasek, Zdenek, Hajny, Jan, Smekal, David, Malina, Lukas, Matousek, Denis, Kekely, Michal, and Mentens, Nele. *200 Gbps Hardware Accelerated Encryption System for FPGA Network Cards.* In Proceedings of the 2018 Workshop on Attacks and Solutions in Hardware Security, ASHES '18, pp. 11–17. New York, NY, USA: Association for Computing Machinery, 2018. ISBN 9781450359962. doi:10.1145/3266444.3266446.
URL `https://doi.org/10.1145/3266444.3266446`

[37] Ometov, Aleksandr, Masek, Pavel, Malina, Lukas, Florea, Roman, Hosek, Jiri, Andreev, Sergey, Hajny, Jan, Niutanen, Jussi, and Koucheryavy, Yevgeni. *Feasibility characterization of cryptographic primitives for constrained (wearable) IoT devices.* In 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), pp. 1–6. 2016. doi:10.1109/PERCOMW.2016.7457161.

[38] Ricci, Sara, Dzurenda, Petr, Hajny, Jan, and Malina, Lukas. *Privacy-Enhancing Group Signcryption Scheme.* IEEE Access, 9:136529–136551, 2021. doi:10.1109/ACCESS.2021.3117452.

[39] Ricci, Sara, Jedlicka, Petr, Cibik, Peter, Dzurenda, Petr, Malina, Lukas, and Hajny, Jan. *Towards CRYSTALS-Kyber VHDL Implementation.* In Proceedings of the 18th International Conference on Security and Cryptography - Volume 1: SECRYPT,, pp. 760–765. INSTICC, SciTePress, 2021. ISBN 978-989-758-524-1. doi:10.5220/0010580407600765.

[40] Ricci, Sara, Malina, Lukas, Jedlicka, Petr, Smékal, David, Hajny, Jan, Cibik, Peter, Dzurenda, Petr, and Dobias, Patrik. *Implementing CRYSTALS-Dilithium Signature Scheme on FPGAs.* In Proceedings of the 16th International Conference on Availability, Reliability and Security, ARES 21. New York, NY, USA: Association for Computing Machinery, 2021. ISBN 9781450390514. doi:10.1145/3465481.3465756.
URL https://doi.org/10.1145/3465481.3465756

Další publikace

[41] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and Levkowetz, H. *Extensible Authentication Protocol (EAP).* RFC 3748 (Proposed Standard), 2004. Updated by RFC 5247.
URL `http://www.ietf.org/rfc/rfc3748.txt`

[42] Barki, Amira, Brunet, Sollen, Desmoulins, Nicolas, and Traoré, Jacques. *Improved Algebraic MACs and Practical Keyed-Verification Anonymous Credentials.* In SAC'16 Proceedings. 2016.

[43] Bichsel, Patrik, Camenisch, Jan, Gross, Thomas, and Shoup, Victor. *Anonymous credentials on a standard java card.* In Proceedings of the 16th ACM conference on Computer and communications security, CCS '09, pp. 600–610. New York, NY, USA: ACM, 2009. ISBN 978-1-60558-894-0.

[44] Boneh, Dan. *The Decision Diffie-Hellman Problem.* In Proceedings of the Third International Symposium on Algorithmic Number Theory, ANTS-III, pp. 48–63. London, UK, UK: Springer-Verlag, 1998. ISBN 3-540-64657-4.
URL `http://dl.acm.org/citation.cfm?id=648184.749735`

[45] Boneh, Dan and Boyen, Xavier. *Short Signatures Without Random Oracles.* In EUROCRYPT'04, pp. 56–73. Springer Berlin Heidelberg, 2004. ISBN 978-3-540-24676-3.

[46] Brickell, Ernie, Camenisch, Jan, and Chen, Liqun. *Direct Anonymous Attestation.* In Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS '04, pp. 132–145. New York, NY, USA: ACM, 2004. ISBN 1-58113-961-6. doi: 10.1145/1030083.1030103.
URL `http://doi.acm.org/10.1145/1030083.1030103`

[47] Camenisch, Jan, Kohlweiss, Markulf, and Soriente, Claudio. *Solving revocation with efficient update of anonymous credentials.* In Proceedings of the 7th international conference on Security and cryptography for networks, SCN'10, pp. 454–471. Berlin, Heidelberg: Springer-Verlag, 2010. ISBN 3-642-15316-X, 978-3-642-15316-7.

[48] Camenisch, Jan and Lysyanskaya, Anna. *An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation.* In Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology, EUROCRYPT '01, pp. 93–118. London, UK: Springer-Verlag, 2001. ISBN 3-540-42070-3.

[49] Camenisch, Jan and Lysyanskaya, Anna. *Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials.* In Proceedings of the 22nd Annual

International Cryptology Conference on Advances in Cryptology, CRYPTO '02, pp. 61–76. London, UK, UK: Springer-Verlag, 2002. ISBN 3-540-44050-X.
URL http://dl.acm.org/citation.cfm?id=646767.704437

[50] Camenisch, Jan and Stadler, Markus. *Proof Systems for General Statements about Discrete Logarithms*. Tech. rep., IBM, 1997.

[51] Camenisch, Jan and Van Herreweghen, Els. *Design and implementation of the idemix anonymous credential system*. In Proceedings of the 9th ACM conference on Computer and communications security, CCS '02, pp. 21–30. New York, NY, USA: ACM, 2002. ISBN 1-58113-612-9.

[52] Chase, Melissa, Meiklejohn, Sarah, and Zaverucha, Greg. *Algebraic MACs and Keyed-Verification Anonymous Credentials*. In ACM SIGSAC'14 Proceedings, pp. 1205–1216. 2014. ISBN 978-1-4503-2957-6.

[53] Chu, Cheng-Kang, Liu, Joseph K, Huang, Xinyi, and Zhou, Jianying. *Verifier-local revocation group signatures with time-bound keys*. In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, pp. 26–27. ACM, 2012.

[54] Couteau, Geoffroy and Reichle, Michael. *Non-Interactive Keyed-Verification Anonymous Credentials*. Cryptology ePrint Archive, Report 2019/117, 2019. https://eprint.iacr.org/2019/117.

[55] EU. *Digital Europe Programme*. "https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/digital-europe-programme_en", 2023.

[56] EU. *Horizon Europe*. "https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en", 2023.

[57] Finseth, C. *An Access Control Protocol, Sometimes Called TACACS*. RFC 1492 (Informational), 1993.
URL http://www.ietf.org/rfc/rfc1492.txt

[58] Gartner. *Cybersecurity Research and Insights for Digital Business*. "https://www.gartner.com/en/information-technology/insights/cybersecurity", 2023.

[59] Gentry, Craig. A fully homomorphic encryption scheme. Stanford university, 2009.

[60] Kohl, J. and Neuman, C. The Kerberos Network Authentication Service (V5). **IETF!**, 1993. RFC 1510.

[61] komise, Evropská. *Směrnice o bezpečnosti sítí a informací*. "https://digital-strategy.ec.europa.eu/cs/policies/nis-directive", 2023.

[62] Lapon, Jorn, Kohlweiss, Markulf, De Decker, Bart, and Naessens, Vincent. *Performance Analysis of Accumulator-Based Revocation Mechanisms.* In Kai Rannenberg, Vijay Varadharajan, and Christian Weber, editors, Security and Privacy - Silver Linings in the Cloud, vol. 330 of *IFIP Advances in Information and Communication Technology*, pp. 289–301. Springer Berlin Heidelberg, 2010. ISBN 978-3-642-15256-6. doi: 10.1007/978-3-642-15257-3_26.

[63] Lin, Zi and Hopper, Nicholas. *Jack: scalable accumulator-based nymble system.* In Proceedings of the 2010 ACM Workshop on Privacy in the Electronic Society, WPES 2010, Chicago, Illinois, USA, October 4, 2010, pp. 53–62. 2010. doi:10.1145/1866919.1866927.
URL `http://doi.acm.org/10.1145/1866919.1866927`

[64] Lueks, Wouter, Alpár, Gergely, Hoepman, Jaap-Henk, and Vullers, Pim. *Fast Revocation of Attribute-Based Credentials for Both Users and Verifiers.* In ICT Systems Security and Privacy Protection - 30th IFIP TC 11 International Conference, SEC 2015, Hamburg, Germany, May 26-28, 2015, Proceedings, pp. 463–478. 2015. doi: 10.1007/978-3-319-18467-8_31.
URL `http://dx.doi.org/10.1007/978-3-319-18467-8_31`

[65] Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. Accessed: 2015-07-01.
URL `https://bitcoin.org/bitcoin.pdf`

[66] Nguyen, Lan. *Accumulators from Bilinear Pairings and Applications.* In Alfred Menezes, editor, Topics in Cryptology CT-RSA 2005, vol. 3376 of *Lecture Notes in Computer Science*, pp. 275–292. Springer Berlin / Heidelberg, 2005. ISBN 978-3-540-24399-1.

[67] NIST. *Post-Quantum Cryptography.* "`https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022`", 2023.

[68] NIST. *Privacy-Enhancing Cryptography.* "`https://csrc.nist.gov/projects/pec`", 2023.

[69] NUKIB. *Legislativa kybernetické bezpečnosti.* "`https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/`", 2023.

[70] Okamoto, Tatsuaki and Uchiyama, Shigenori. *A new public-key cryptosystem as secure as factoring.* In Kaisa Nyberg, editor, Advances in Cryptology - EUROCRYPT 98, vol. 1403 of *Lecture Notes in Computer Science*, pp. 308–318. Springer Berlin / Heidelberg, 1998. ISBN 3-540-64518-7.

[71] Paillier, Pascal. Advances in Cryptology — EUROCRYPT '99: International Conference on the Theory and Application of Cryptographic Techniques Prague, Czech Republic, May 2–6, 1999 Proceedings, chap. Public-Key Cryptosystems Based on Composite

Degree Residuosity Classes, pp. 223–238. Springer Berlin Heidelberg, 1999. ISBN 978-3-540-48910-8. doi:10.1007/3-540-48910-X_16.
URL http://dx.doi.org/10.1007/3-540-48910-X_16

[72] Paquin, Christian. *U-Prove Cryptographic Specification V1.1.* Tech. rep., Microsoft Corporation, 2011.

[73] Rescorla, Eric. *The Transport Layer Security (TLS) Protocol Version 1.3.* RFC, 8446:1–160, 2018.
URL http://dblp.uni-trier.de/db/journals/rfc/rfc8400-8499.html

[74] Rigney, Carl, Willens, Steve, Rubens, Allan C., and Simpson, William Allen. *Remote Authentication Dial In User Service (RADIUS).* RFC, 2865:1–76, 2000.
URL http://dblp.uni-trier.de/db/journals/rfc/rfc2800-2899.html

[75] Ringers, Sietse, Verheul, Eric R., and Hoepman, Jaap-Henk. *An Efficient Self-blindable Attribute-Based Credential Scheme.* In FC'17 Proceedings, pp. 3–20. 2017.

[76] Rivest, Ronald L. and Kaliski, Burt. RSA Problem, pp. 532–536. Springer US, 2005. ISBN 978-0-387-23483-0.

[77] Schaffer, Martin and Schartner, Peter. *Anonymous authentication with optional shared anonymity revocation and linkability.* In Proceedings of the 7th IFIP WG 8.8/11.2 international conference on Smart Card Research and Advanced Applications, CARDIS'06, pp. 206–221. Berlin, Heidelberg: Springer-Verlag, 2006. ISBN 3-540-33311-8, 978-3-540-33311-1.

[78] Shoup, Victor. Lower Bounds for Discrete Logarithms and Related Problems, pp. 256–266. 1997. ISBN 978-3-540-69053-5.

[79] Tsang, Patrick P., Au, Man Ho, Kapadia, Apu, and Smith, Sean W. *Blacklistable Anonymous Credentials: Blocking Misbehaving Users Without Ttps.* In Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS '07, pp. 72–81. New York, NY, USA: ACM, 2007. ISBN 978-1-59593-703-2. doi:10.1145/1315245.1315256.
URL http://doi.acm.org/10.1145/1315245.1315256

[80] Verheul, Eric R. *Practical backward unlinkable revocation in FIDO, German e-ID, Idemix and U-Prove.* IACR Cryptology ePrint Archive, 2016:217, 2016.
URL http://eprint.iacr.org/2016/217

[81] Wei, Victor K. and Yuen, Tsz Hon. *More short signatures without random oracles*, 2005. https://eprint.iacr.org/2005/463.

POUŽITÉ ZKRATKY

Akronym	**Význam**
AAA	Authentication, Authorisation, Accounting
AXE	Applied Cryptography and Security Engineering Group
ABC	Attribute-Based Credentials
AES	Advanced Encryption Standard
CS	Camenisch Stadler
DL	Discrete Logarithm
DLP	Discrete Logarithm Problem
EAP	Extensible Authentication Protocol
ICT	Information and Communication Technologies
MAC	Message Authentication Code
NIST	National Institute for Standards and Technology
NP	Non-Polynomial
PETs	Privacy-Enhancing Technologies
PK	Proof of Knowledge
RA	Revocation Authority
RFID	Radio Frequency Identification
RL	Revocation List
RSA	Rivest Shamir Adleman
TLS	Transport Layer Security
VANETs	Vehicular Ad-Hoc Network
ZK	Zero Knowledge

ABSTRACT

This thesis is focused on the area of modern cryptography, particularly on the design of cryptographic protocols for user authentication and electronic system access control. The document summarizes current trends in authentication protocols and focuses specifically on systems with advanced privacy protection. The basic principles of attribute-based credentials, i.e., the cryptosystems allowing access control based on personal attributes instead of personal identity, are described. In the introduction of Section 3.1, a short overview of the current state of the art in attribute-based credentials is presented. Next, the main challenges and respective solutions designed by the author are introduced. The solutions are further detailed in Section 3.2.1 and Section 3.3.1. Namely, the cryptographic protocols with low computational complexity and efficient revocation are presented. The theoretical constructions are supported by results from an experimental implementation using smart cards. Finally, Section 4 briefly introduces applications for attribute-based credentials and mentions other areas of modern cryptography and future challenges.