Bachelor and Master Thesis Topics: Privacy, Security, and Digital Forensics

Chair of Parallelism & VLSI

May 27, 2025

1 Introduction

This document presents thesis topics in the areas of privacy-preserving technologies, anonymity networks, and digital forensics. These topics address current challenges and offer students opportunities to contribute to cutting-edge research in these fields. This document is part of the open thesis topic for the summer semester 2025 and structured in multiple parts. The first Section 2 details the thesis process and application requirements. Please read these carefully. Especially, the latter is helpful for a successful thesis topic applciation.

Following, several thesis topics are offered. The first topics in Section 3 fall into the cryptocurrency domain and cover Bitcoin mixing to santion mechanisms. Section 4 offers forensic topics focused on the hardened operation systems QubesOS and Whonix which are especially suitable for candidates with a digital forensics background. Section 5 covers the public perception of privacy enhancing technologies by collecting and analysing publicy available data. Section 6 specifically discusses the possibility of adding a content blocker into the Tor Browser. As the Tor browser is used by millions of active users that may face severe consequences in case of deanonymization, this might be an interesting topic for privacy fans. The last topic in section 7 investigates the possibility to use large language models in a more privacy-friendly way while not assuming large resources to run advanced LLMs locally.

2 Thesis Procedure and Timeline

2.1 Application and Topic Assignment Process

Application and Topic Allocation All submitted applications will be reviewed and evaluated. Successful applicants will be offered specific thesis topics based on their qualifications, interests, and supervisor capacity. Students then need to confirm their topic selection.

Introduction Meeting All students who have been assigned topics from this document will attend a mandatory introduction meeting. This session will cover the general expectations and guidelines for thesis work.

Abstract Following topic assignment, students enter the abstract development phase with a maximum duration of 3 months for master students and 2 months for bachelor students. During this phase, students must:

1. **Literature Review:** Conduct research into related work and current state of the field
2. **Gap Analysis:** Identify relevant research gaps in accordance with the chosen thesis topic
3. **Research Questions:** Formulate specific research questions that address identified gaps
4. **Methodology Development:** Design appropriate methods and approaches to answer the research questions

Throughout the abstract development and following thesis working phase, students can regularly ask questions and discuss with their supervisor. Especially during the initial timing, q1uestions and discussions are encouraged to refine the research approach.

Abstract Review Upon submission, the developed abstract will undergo a quality check to ensure feasible, well-defined research questions, an appropriate methodology and a realistic scope for the thesis timeline. If improvements are necessary, students will have the opportunity to refine and resubmit their abstract.

Official Registration Once the abstract is approved, the thesis will be officially registered with the university. The final submission deadline will be set according to university regulations and students receive confirmation of their registration and timeline.

A dedicated Moodle forum will serve as the central communication platform and provides additional resources and materials assisting you.

Students have flexibility in language choice:

- **Thesis Language:** English or German
- **Supervision Language:** English or German
- **Kolloquium Language:** English or German (independent of thesis language)

2.2 Application Requirements

To ensure the best match between students and thesis topics, please provide the following information in your application. This will help us assess your preparedness and align your interests with the most suitable research direction.

2.2.1 Required Application Components

Relevant Experience Describe relevant work experience, internships, research projects, or personal projects that could help with your chosen thesis topic. If you have no directly relevant experience, please explain any transferable skills or related activities.

Academic Background List university courses you have completed that provide helpful knowledge for your chosen topic.

Research Interest Statement In 2-5 sentences, explain what aspects of your chosen thesis topic you find most interesting and why. Consider addressing what specific challenges or problems within the topic motivate you and what unique perspective or approach you might bring to the topic.

Research Proposal Outline Provide a short text (approximately 200-400 words) that outlines

- From the provided list or based on your own interests, identify 2-3 specific research questions you would like to explore for your selected topic. Explain why these questions are important and how they contribute to the field.
- Describe your initial thoughts on how you would approach investigating these research questions. This should include general methods you plan to use for investigating the topic. How you plan to validate your findings or measure success? Do you have preliminary ideas for overcoming potential challenges?

Note: This is not a binding commitment but demonstrates your understanding of the research process.

Publication and Open Access Research results from these thesis topics may be of general interest to the privacy and digital forensics communities. We may seek to publish outstanding

work through academic papers, technical reports, or open-source releases to make findings publicly accessible. This could be done in a form of openly published theses, open-source tools or academic papers. For academic papers, students remain the first autor unless the work is combined with more comprehensive results from the supervisor. Please indicate if you are interested in a potential publication of the research results.

2.2.2 Application Format

Please structure your application as follows:

1. **Header:** Include your name, student ID, degree program (Bachelor/Master), and preferred thesis topic(s)
2. **Relevant Experience:** (maximum 300 words)
3. **Academic Background:** (Maximum 100 words)
4. **Research Interest Statement:** (2-5 sentences)
5. **Research Proposal Outline:** (200-400 words)
6. **Publication and Open Access:** (1-3 sentences)

Yopur application should contain only plain text for the requirements listed in 2.2. You can additionally attach documents (only in PDF format).

3 Cryptocurrency Sanctions and Privacy

In recent years, financial sanctions have emerged as a prominent policy instrument in the digital asset space (cryptocurrencies). Regulatory bodies, notably the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), have demonstrated an increasing willingness to target cryptocurrency entities, individuals, and critical infrastructure components perceived to facilitate illicit finance or sanctions evasion. The academic community is actively working to understand the effectiveness of these crypto-specific sanctions. Early empirical studies, such as the work by Zola, Medina, and Orduna [1] present a nuanced picture, indicating mixed results: while some sanctioned entities appear to be deterred, a significant portion continues their operations, often adapting their tactics to circumvent restrictions. These findings suggest that sanctions are not a simple "off switch" for illicit crypto activities. Effective sanctions must be more complex than blacklisting bitcoin addresses.

BIT1: How effective are newer or cost-optimized ZKP-based mixing services (e.g., those inspired by Wang et al.'s Merkle Pyramid Builder (MPB) approach [2]) or novel DeFi-based obfuscation strategies (e.g., complex sequences of swaps, liquidity provision, and withdrawals across multiple protocols) in providing robust unlinkability for Bitcoin-derived funds against simulated state-level tracing capabilities?

BIT2: Can novel heuristics reliably detect the use of specific advanced PETs when applied to Bitcoin transactions or Bitcoin-derived assets on other chains? This includes identifying subtle on-chain signatures of i.e. ZKP constructions, or characteristic interaction patterns with DeFi protocols that are indicative of layering or obfuscation. For instance, could behavioral or on-chain metadata heuristics be devised for Bitcoin transactions that interact with cross-chain bridges or exhibit patterns consistent with known state-sponsored APT laundering methodologies? A starting source could be [3].

BIT3: How resilient are different layers and components of the Bitcoin ecosystem (e.g., the P2P transaction propagation network, mining pool behavior regarding transaction inclusion, the Lightning Network, or federated sidechains) to attempts at censorship or transaction filtering that might be prompted by sanctions against interacting protocols or services? Starting literatur could be [4, 5].

BIT4: This research direction involves the design, implementation (as a Proof-of-Concept, PoC), and forensic analysis of a Bitcoin mixer. The goal is to explore critical design decisions that mixer developers face and to evaluate how these decisions impact the mixer's privacy guarantees and its susceptibility to various forensic analysis techniques. This constructive approach allows for a deep, practical understanding of mixer vulnerabilities and strengths from both a user's and an investigator's perspective.

4 Forensic Analysis of Security-Focused Operating Systems

In an era of escalating cyber threats and pervasive surveillance, users are increasingly turning to operating systems designed with security and privacy as paramount principles. Systems like QubesOS and Whonix offer robust architectures to protect against malware, isolate activities, and anonymize network traffic. QubesOS achieves security through compartmentalization, leveraging the Xen hypervisor to run applications and system components in isolated virtual machines (VMs). Whonix, often used in conjunction with QubesOS or other virtualization platforms, provides anonymity by routing all network connections through the Tor network via a two-VM design (Gateway and Workstation). The growing adoption of these platforms by security-conscious individuals, journalists, activists, and even enterprises necessitates a deeper understanding of their forensic implications. Traditional forensic methodologies, often designed for monolithic operating systems, may prove inadequate. The features chancing security (strong isolation, virtualization, traffic anonymization, potential amnesic properties) can obscure or complicate the recovery of digital evidence. For instance, inter-VM communication in QubesOS is tightly controlled, and artifacts may be distributed across multiple VMs, making correlation difficult. Whonix's Tor-based architecture inherently masks the origin and destination of network traffic, posing significant hurdles for network forensics. Furthermore, the potential use of Disposable VMs in QubesOS or live modes in Whonix can severely limit data persistence, challenging conventional disk-based forensic approaches

FOR1: The goal is to analyse forensic properties of one target system and develop procedure to conduct forensic investigations. This can include applying and potentially modifying exisiting approaches with server forensics seeming like a suitable venue but also creating new guidelines and tools. Concrelty, the following points provide some examples for interesting investigative angles:

- Artifact Location and Analysis in QubesOS dom0 and AppVMs. What specific forensic artifacts are generated in QubesOS dom0 and within individual AppVMs under various usage scenarios and how can they be reliably extracted?
- Forensic Analysis of Inter-VM Communication in QubesOS. How can inter-VM communication mediated by qrexec (e.g., copy/paste, file transfers, service calls) be forensically reconstructed in QubesOS? What logs or artifacts document these interactions, and where are they stored
- Memory Forensics of QubesOS and Whonix VMs. What are effective techniques for acquiring and analyzing memory dumps from QubesOS AppVMs, ServiceVMs (including sys-net, sys-firewall, sys-whonix), and Whonix-Gateway/Workstation VMs?
- Evaluating the Effectiveness of Anti-Forensic Features. How effective are the anti-forensic features or operational security practices associated with QubesOS (e.g., DisposableVMs, LVM discards) and Whonix (e.g., host live mode, disabling swap, Tor's anonymization) in preventing data recovery or obscuring user activity and which residual artifacts remain?
- Forensic Analysis of QubesOS DisposableVMs. What (if any) persistent or volatile artifacts are left behind by QubesOS DisposableVMs after they are closed? Can any in-

formation about the activities performed within a DispVM be recovered from dom0, the underlying TemplateVM, or system RAM?

This topic requires a powerful machine capable to run QubesOS since virtualizing it was not successful for us during experiments. Forensic experience helps when working on this topic.

FOR2: If you already have working experience in the digital forensics fields, it might be possible to generate an individualized topic together. This can range from mobile phone forensics to network forensics with a strong research focus. Previous work from the DFRWS conference[1] assist in getting an impression of suitable topics. The research topic must address new questions or unexplored/underexplored aspects of existing problems and must fill identified gaps in current knowledge.

5 Investigating Public Perception of Privacy-Enhancing Technologies (PETs) through Online Discourse

The continued growth of digital technologies has led to an unprecedented collection and use of personal data, making privacy a paramount concern for individuals and organizations. Privacy Enhancing Technologies (PETs) have emerged as crucial tools designed to safeguard this data during its storage, processing, and transmission. These technologies encompass a range of solutions, from encryption and anonymization techniques to more complex systems like Zero-Knowledge Proofs (ZKPs) and federated learning. While PETs offer significant potential to protect user privacy and enable secure data sharing, their widespread adoption and effective utilization are often hindered by a lack of public understanding, trust, and awareness. Misinformation and varying perceptions surrounding these technologies can create substantial barriers to their acceptance and, consequently, their ability to deliver on their privacy-protective promises. One of the core challenges for PETs lies in the perceivance by the general public. This perception, often shaped by incomplete or inaccurate information, directly influences user adoption and the overall effectiveness of these technologies. Therefore, understanding the nuances of public perception is critical for designing PETs that are not only robust but also user-friendly and trustworthy. This research aims to investigate the public perception of PETs by analyzing discussions and information presented on widely accessible online platforms.

Concretely, this topic must address (some) of the following key questions:

- What are the dominant themes and sentiments expressed in online discussions (e.g., on platforms like Reddit and YouTube) concerning various PETs, including VPNs, Tor, and Zero-Knowledge Proofs?
- How is information, and potentially misinformation, about PETs constructed, debated, and modified within collaborative knowledge platforms such as Wikipedia?
- What are the prevalent misunderstandings or knowledge gaps regarding PETs among online users?
- How do users' experiences with and perceptions of the usability of PETs influence their overall attitudes towards these technologies?

The analysis of data will likely require a grounded theory approach. This method allows themes and theories to emerge directly from the data, rather than being imposed by pre-existing hypotheses. In multiple phases, a codebook is constructed to structure the collected data and capture a wide range of information regarding the users' understanding, experiences, and concerns. An example for this method can be found in [6]. Alternatively, it might be possible

[1] https://dfrws.org/presentation/

with larger datasets to conduct quantitative analysis. This could include frequency counts of keywords related to specific PETs or concerns, and sentiment analysis to gauge the overall tone of discussions.

PETS1: The topic description lays the foundational methodology for this work. Still, the platform choice and analysis require customization. Examples for potentially interesting avenues for platforms are:

- *Wikipedia.* A qualitative content analysis could be performed on the edit summaries and the actual changes made to the articles. This could help identify points of contention, debates over definitions, perceived benefits and risks of PETs, and instances where misinformation or biased editing may have occurred. This involves examining how descriptions, explanations, and discussions about PETs have changed, and correlating these changes with significant external events, technological advancements, or shifts in public discourse.
- *Youtube.* Comments sections of videos from popular tech channels that discuss privacy, security, and specific PETs (e.g., Mental Outlaw, Techlore) will be analyzed. These channels often influence public understanding and generate significant user interaction.Online Forum and Social Media Analysis. Comments sections of videos from popular tech channels that discuss privacy, security, and specific PETs (e.g., Mental Outlaw, Techlore) will be analyzed. These channels often influence public understanding and generate significant user interaction
- *Subreddits* such as r/privacy, r/technology, and specific PET-focused communities like r/VPN, r/TOR, and r/zec (for Zcash and Zero-Knowledge Proofs) could be primary sources. These platforms are known for active discussions on technology and privacy.

6 Evaluating the Impact of uBlock Origin Integration on Tor Browser's Anonymity

The Tor network offers anonymity by routing internet traffic through a series of volunteer-operated relays, obfuscating the user's origin. The Tor Browser is specifically designed to increase this anonymity by standardizing browser fingerprints, aiming to make all users appear identical, therefore enlarging the anonymity set. Browser fingerprinting involves collecting a wide array of data points about a user's browser and device configuration (user-agent string, installed fonts, screen resolution, operating system, and browser plugins) to create a unique identifier. Even seemingly innocuous differences can distinguish a user, shrinking their anonymity set and increasing re-identification risk. Despite these efforts, users frequently request additional features, particularly privacy-enhancing extensions like content blockers. A prominent example is the long-standing request to integrate uBlock Origin, a popular open-source content blocker, into the Tor Browser [7]. Proponents argue that content blockers enhance usability by removing intrusive ads, improve security by blocking malvertising, and save bandwidth, which is particularly beneficial on the Tor network. This creates a fundamental tension: while such extensions offer benefits, any modification to the browser, including the addition of an extension and its specific configuration, can introduce new fingerprinting vectors and potentially undermine Tor's core anonymity promise. This topic aims to investigate the impact of integrating a standardized version of uBlock Origin into Tor Browser on its users' anonymity.

Arguments for integration often highlight that if all users were to use a standardized, non-customizable version of uBlock Origin, they would theoretically share the same fingerprint and therefore preserving the anonymity set. Additional benefits include significant bandwidth savings, which would lessen the load on the Tor network and improve page responsiveness, and enhanced usability and security against malvertising and intrusive trackers. The fact that Mull-

vad Browser (a collaboration between Mullvad VPN and the Tor Project) and Tails (an operating system that bundles Tor Browser) already ship with uBlock Origin is often presented as evidence of feasibility and existing precedent. However, significant concerns persist that primarly center on the risk of increased browser fingerprintability. Historically, the Tor Project has strongly advised against installing any add-ons, as they can compromise privacy and security by creating unique fingerprints. The main issue regarding uBlock Origin is that users might modify its settings, particularly the filter lists, thereby creating distinguishable configurations that would fragment the anonymity set.

Managing filter lists presents a substantial challenge: decisions about which lists to include by default, how to cache them, and how to update them without creating fingerprintable differences (e.g., users having slightly different list versions between Tor Browser updates) or requiring network requests that could de-anonymize users are critical hurdles. Any integrated solution would necessitate that filter lists are locked and updated synchronously with Tor Browser releases. Furthermore, potential conflicts and complexities could arise from the interaction between uBlock Origin's JavaScript control mechanisms and NoScript's existing global and site-specific JavaScript blocking, especially concerning Tor Browser's different security levels (Standard, Safer, Safest). While existing research [8, 9] provides a strong foundation, specific investiations into standardized and locked-down uBlock Origin configurations in the Tor browser remain a critical gap.

TOR1: The goal of this topic to evaluate the integration of uBlock Origin into the Tor browser. This likely includes determining different implementation strategies and alternatives. Each strategy should be evaluated regarding fingerprinting risks, anonymity set impact, security and other implications.

7 Advancing Privacy in Cloud-Based LLM Interactions

The proliferation of powerful Large Language Models (LLMs), often accessed via cloud-based APIs, presents significant opportunities across various domains. However, this paradigm introduces substantial privacy risks, particularly when user prompts contain Personally Identifiable Information (PII). The transmission of sensitive data to third-party servers raises concerns about potential misuse, unauthorized access, and compliance with increasingly stringent data protection regulations. A promising approach to mitigate these risks involves a hybrid or dual-LLM architecture, wherein a locally deployed LLM acts as a privacy-preserving intermediary. The fundamental concept underpinning this research is a system architecture featuring a local LLM, potentially lightweight and optimized for on-device execution, functioning as a "privacy guardian." This local LLM intercepts user prompts intended for a more powerful cloud-based LLM. Its primary responsibilities include identifying PII within the prompt, applying a sanitization technique to remove or transform this PII, and then forwarding the modified, privacy-enhanced prompt to the cloud LLM for primary processing. Upon receiving a response from the cloud LLM (which is based on the sanitized prompt), the local LLM undertakes the crucial task of restoring the original PII into the response in a coherent and contextually appropriate manner before it is presented to the user. This approach seeks to harness the advanced capabilities of cloud LLMs while significantly reducing the exposure of raw PII to external entities.

LLM1 The goal of this topic is to design, implement (as PoC) and evaluate parts of the entire system. This could include:

- The effectiveness of the local LLM in accurately identifying, sanitizing, and subsequently restoring PII without loss of critical information or introduction of errors is foundational to the entire architecture. What are the optimal PII sanitization techniques (e.g., masking, pseudonymization, Format-Preserving Encryption (FPE), generative replacement by

lightweight LLMs) for a local LLM in terms of balancing PII removal efficacy, computational efficiency (for on-device deployment), and reliable reversibility for accurate restoration?

- How accurately can a local LLM restore PII into a cloud LLM's response, maintaining contextual coherence and semantic integrity, especially when the response structure is complex (e.g., tables, code, lists) or the role of PII within the response is nuanced?
- How does the choice of local PII detection method (e.g., regular expressions, traditional statistical NER, advanced LLM-based NER) impact the overall efficacy and robustness of the sanitization-restoration cycle?
- How do different PII sanitization strategies (e.g., the type of placeholder used, the level of abstraction in pseudonyms or contextual masks, the use of FPE-generated strings versus natural language pseudonyms) affect the cloud LLM's ability to understand the prompt's underlying intent and accurately perform various downstream tasks (e.g., text summarization, question answering, code generation, creative writing, logical reasoning)?
- What is the cumulative impact of PII sanitization (by the local LLM), subsequent processing by the cloud LLM (on altered input), and final PII restoration (by the local LLM) on the overall quality in terms of fluency, coherence, factual correctness, and relevance of the final user-facing response?
- To what extent can PII be inferred by the cloud LLM from sanitized prompts, even if explicit identifiers are removed? This includes risks of semantic PII leakage or re-identification through the analysis of quasi-identifiers and contextual information remaining in the sanitized prompt.
- What are the vulnerabilities of the PII restoration process itself? Can an attacker, by manipulating the cloud LLM's response content or structure, trick the local LLM into incorrectly restoring PII, or worse, into leaking the PII mapping table or information about the sanitization keys?
- What are the performance implications (i.e., latency, throughput, and local computational/memory impact) of implementing different local PII sanitization and restoration techniques, particularly when relying on lightweight LLMs for these tasks?

Note: Since we don't have comprehensive (GPU-)computing power, it is favourable if applicants have GPUs capable of running smaller LLMs (i.e., RTX 3070, RTX 4060).

References

[1] Francesco Zola, Jon Ander Medina, and Raul Orduna. *Assessing the Impact of Sanctions in the Crypto Ecosystem: Effective Measures or Ineffective Deterrents?* 2024. arXiv: 2409.10031 [cs.CR].

[2] Zhipeng Wang et al. *Pay Less for Your Privacy: Towards Cost-Effective On-Chain Mixers.* Cryptology ePrint Archive, Paper 2023/1222. 2023. URL: https://eprint.iacr.org/2023/1222.

[3] Jan Zavřel et al. "Tumbling down the stairs: Exploiting a tumbler's attempt to hide with ordinary-looking transactions using wallet fingerprinting". In: *Forensic Science International: Digital Investigation* 52 (2025). DFRWS EU 2025 - Selected Papers from the 12th Annual Digital Forensics Research Conference Europe, p. 301869. ISSN: 2666-2817. DOI: https://doi.org/10.1016/j.fsidi.2025.301869.

[4] Federal Reserve Bank of New York. *Staff Report No. 1112*. Tech. rep. Accessed: 2025-05-27. Federal Reserve Bank of New York, 2024. URL: https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr1112.pdf.

[5] Zhipeng Wang, Xihan Xiong, and William J. Knottenbelt. *Blockchain Transaction Censorship: (In)secure and (In)efficient?* Cryptology ePrint Archive, Paper 2023/786. 2023. URL: https://eprint.iacr.org/2023/786.

[6] Pascal Tippe and Adrian Tippe. "Onion Services in the Wild: A Study of Deanonymization Attacks". In: *Proc. Priv. Enhancing Technol.* 2024.4 (2024), pp. 291–310. DOI: 10.56553/POPETS-2024-0117.

[7] Tor Project. *Add uBlock Origin to the Tor Browser*. GitLab Issue #17569. Accessed: 2025-05-27. 2023. URL: https://gitlab.torproject.org/tpo/applications/tor-browser/-/issues/17569.

[8] Saiid El Hajj Chehade, Ben Stock, and Carmela Troncoso. "Double-Edged Shield: On the Fingerprintability of Customized Ad Blockers". In: *Proceedings of the 34th USENIX Security Symposium*. To appear. USENIX Association, 2025. URL: https://www.usenix.org/system/files/conference/usenixsecurity25/sec25cycle1-prepub-432-el-hajj-chehade.pdf.

[9] Konstantinos Solomos et al. "The Dangers of Human Touch: Fingerprinting Browser Extensions through User Actions". In: *31st USENIX Security Symposium (USENIX Security 22)*. Boston, MA: USENIX Association, Aug. 2022, pp. 717–733. ISBN: 978-1-939133-31-1. URL: https://www.usenix.org/conference/usenixsecurity22/presentation/solomos.