

Anh V. Vu

GE-01, Department of Computer Science and Technology, William Gates Building, 15 JJ Thomson Ave, Cambridge, UK, CB3 0FD
☎ (+44) 746 351 1312 | ✉ anh.vu@trmlabs.com, anh.vu@cst.cam.ac.uk | 🏠 www.cst.cam.ac.uk/people/vv301 | 📺 anhvvcs

My research provides timely empirical measurements to explore cyberspace and its societal impact at scale, with a focus on the underground subcultures that foster online crime and harms. By integrating insights from both academia and industry, my work blends expertise in computer science and criminology to help better understand online threats and inform policy decisions for safety and security.

Education

University of Cambridge

Cambridge, UK

DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE

05 Jan 2022 – 05 Jan 2025

- Supervisor: Professor Alice Hutchings · Advisor: Professor Ross Anderson
- Thesis: Online Crime and Harms Following Externalities · Passed with no corrections
- Examiners: Professor Jon Crowcroft, Professor Nicolas Christin

Japan Advanced Institute of Science and Technology

Ishikawa, Japan

MASTER OF SCIENCE IN INFORMATION SCIENCE

01 Oct 2017 – 21 Dec 2018

- Supervisor: Professor Mizuhito Ogawa
- Thesis: Formal Semantics Extraction from Natural Language Specifications for ARM
- Examiners: Professor Mizuhito Ogawa, Professor Kazuhiro Ogata, Professor Keita Yokoyama, Professor Minh Le Nguyen

Vietnam National University

Hanoi, Vietnam

BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

05 Sep 2012 – 29 Jun 2016

- Supervisor: Professor Xuan Hieu Phan
- Thesis: User Behaviour Analysis and Personalisation in a Vietnamese Medical Information System
- Honours Programme · High Distinction (top 10/473) · GPA: 3.66/4.0

Work Experience

TRM Labs | Blockchain Intelligence

San Francisco, USA

RESEARCH SCIENTIST

28 Apr 2025 – Present

- **Managers:** Adam Brownell, Aymen Jaffry / **Topics:** Financial Cybercrime, Blockchain Intelligence, Crypto Mixing Services
- Working within the Traceability Team to develop new innovative methods for tracing obscured blockchain transactions by illicit actors.

University of Cambridge

Cambridge, UK

VISITING RESEARCHER

28 Apr 2025 – Present

- **Advisor:** Professor Alice Hutchings / **Topics:** Cybersecurity, Cybercrime, Online Harms
- Regularly visiting the Cambridge Cybercrime Centre and the Security Group to engage in continuous learning and research discussions.

University of Cambridge

Cambridge, UK

RESEARCH ASSISTANT

27 Oct 2019 – 27 Apr 2025

- **Advisors:** Dr Richard Clayton, Professor Alice Hutchings, Professor Ross Anderson / **Topics:** Cybersecurity, Cybercrime, Online Harms
- Collected large-scale cybercrime and extremist datasets, then analysed the longitudinal dynamics of their underground subcultures.
- Maintained a [data-sharing](#) platform, allowing over 400 researchers worldwide to access our cybercrime and extremist datasets.

Delft University of Technology

Delft, Netherlands

VISITING RESEARCH STUDENT

11 Jun 2024 – 11 Jul 2024

- **Advisor:** Professor Rolf van Wegberg / **Topics:** Financial Cybercrime, Crypto Mixing Services
- Collaborated on a research project co-funded by the Dutch Law Enforcement on the facilitators of financial cybercrime.
- Analysed on-chain transactions of crypto mixers to understand the dynamics of their ecosystem following law enforcement interventions.

National University of Singapore

Singapore, Singapore

RESEARCH INTERN

06 Jan 2019 – 25 Jul 2019

- **Advisor:** Professor Min Suk Kang / **Topics:** Blockchain Network Security, Bitcoin, Cryptocurrency
- Conducted experiments simulating adversarial scenarios on our newly discovered partitioning attack against the Bitcoin P2P network.

Vietnam National University

Hanoi, Vietnam

ASSISTANT LECTURER

01 Oct 2016 – 30 Sep 2017

- **Advisor:** Professor Dinh Hieu Vo / **Topics:** Software Engineering, Data Scraping
- Taught several undergraduate modules, including Fundamentals of Informatics (INT1003) and Object-Oriented Programming (INT2204).
- Collected large-scale datasets for a Vietnamese [bibliographic database](#) designed to measure and analyse scholarly literature.

- **Advisor:** Mr Ngoc Tuan Le / **Topics:** Android, Robotics
- Mentored the FPT S.M.A.C Challenge 2015 competition, which had around 100 participants from over 50 teams.
- Researched and developed a mobile platform enabling developers to interact with smart humanoid robots (NAO).

Publications

⚡ Peer-reviewed Conferences

Assessing the Aftermath: the Effects of a Global Takedown against DDoS-for-hire Services

CORE A* PDF 

ANH V. VU, BEN COLLIER, DANIEL R. THOMAS, JOHN KRISTOFF, RICHARD CLAYTON, ALICE HUTCHINGS

13–15 Aug 2025

- **SEC'25** – USENIX Security Symposium

Seattle, USA

No Easy Way Out: the Effectiveness of Deplatforming Forums to Suppress Hate and Harassment

CORE A* PDF 

ANH V. VU, ALICE HUTCHINGS, ROSS ANDERSON

20–23 May 2024

- **S&P'24** – IEEE Symposium on Security and Privacy · Acceptance Rate 17.8% · [Briefing](#) · [CyCon](#)

San Francisco, USA

- Press coverage: [The Register](#) · [LBT](#)

Getting Bored of Cyberwar: the Role of Low-level Cybercrime Actors in the Russia-Ukraine Conflict

CORE A* PDF 

ANH V. VU, DANIEL R. THOMAS, BEN COLLIER, ALICE HUTCHINGS, RICHARD CLAYTON, ROSS ANDERSON

13–17 May 2024

- **WWW'24** – ACM World Wide Web Conference · Acceptance Rate 20.2% · [CyCon](#)

Sentosa, Singapore

- Press coverage: [New Scientist](#) · [Associated Press](#) · [SC Magazine](#) · [The Record](#) · [LBT](#)

Turning Up the Dial: the Evolution of a Cybercrime Market Through Set-up, Stable, and Covid-19 Eras

CORE A PDF 

ANH V. VU, JACK HUGHES, ILDIKO PETE, BEN COLLIER, YI TING CHUA, ILIA SHUMAILOV, ALICE HUTCHINGS

27–29 Oct 2020

- **IMC'20** – ACM Internet Measurement Conference · Acceptance Rate 24.5%

Pittsburgh, USA

- Press coverage: [Hacker News](#) · [Cambridge Research](#) · [LBT](#)

A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network

CORE A* PDF 

MUOI TRAN, INHO CHOI, GI JUN MOON, ANH V. VU, MIN SUK KANG

18–20 May 2020

- **S&P'20** – IEEE Symposium on Security and Privacy · Acceptance Rate 12.4%

San Francisco, USA

- Press coverage: [CoinDesk](#)

Formal Semantics Extraction from Natural Language Specifications for ARM

CORE A PDF 

ANH V. VU, MIZUHITO OGAWA

07–11 Oct 2019

- **FM'19** – International Symposium on Formal Methods · Acceptance Rate 30.0%

Porto, Portugal

⚡ Peer-reviewed Workshops

Yet Another Diminishing Spark: Low-level Cyberattacks in the Israel-Gaza Conflict

PDF 

ANH V. VU, ALICE HUTCHINGS, ROSS ANDERSON

30 Jun – 04 Jul 2025

- **EuroS&PW'25** – IEEE European Symposium on Security and Privacy Workshops · [Briefing](#)

Venice, Italy

- Press coverage: [Computer Weekly](#) · [Fast Company](#) · [Infosecurity](#) · [LBT](#)

ExtremeBB: A Database for Large-Scale Research into Online Hate, Harassment, and Extremism

PDF 

ANH V. VU, LYDIA WILSON, YI TING CHUA, ILIA SHUMAILOV, ROSS ANDERSON

09–14 Jul 2023

- **WOAH@ACL'23** – ACL Workshop on Online Abuse and Harms · [Website](#)

Toronto, Canada

PostCog: A Tool for Interdisciplinary Research into Underground Forums at Scale

PDF 

ILDIKO PETE, JACK HUGHES, ANDREW CAINES, ANH V. VU, H. GUPTA, ALICE HUTCHINGS, ROSS ANDERSON, PAULA BUTTERY

06–10 Jun 2022

- **EuroS&PW'22** – IEEE European Symposium on Security and Privacy Workshops · [Website](#)

Genoa, Italy

⚡ Book Chapters

Identifying and Collecting Public Domain Data for Tracking Cybercrime and Online Extremism

PDF 

LYDIA WILSON, ANH V. VU, ILDIKO PETE, YI TING CHUA

01 Jun 2024

- Chapter in: Open Source Investigations in the Age of Google

World Scientific

- Press coverage: [Center for Strategic and International Studies \(CSIS\)](#)

Teaching & Supervision

Guest Lectures

- Malicious AI and Dark Side Security (FIT3183) – Monash University, Malaysia (24 Oct 2024), invited by Professor Raphael Phan. Guest lecture on “Beyond Whack-A-Mole: Disrupting Online Crime and Harms through Law Enforcement and Industry Efforts”.

Supervisions at Cambridge

Supervisions at Cambridge (tutorials at Oxford) are a defining feature of undergraduate education, involving small-group and personalised teaching. One to three students prepare essays, problem sets, or readings in advance, which are then discussed in depth with a subject specialist during the sessions. This interactive format encourages critical thinking and individual analysis, while also providing tailored feedback. I have been fortunate to supervise a range of subjects for many Cambridge undergraduates, who are among the brightest minds in the world.

- Algorithms
 - Sutton Trust Summer School 2023: 4 groups of 10 students, 4 hours in total
 - Sutton Trust Summer School 2022: 4 groups of 12 students, 4 hours in total
- Software and Security Engineering
 - Easter 2022-2023: 11 groups of 23 students for Clare (5), Emmanuel (2), Selwyn (3), Kings’ (9), and Fitzwilliam (4) College, 33 hours in total
 - Easter 2021-2022: 6 groups of 14 students for Kings’ (8) and Robinson (6) College, 18 hours in total
- Databases
 - Michaelmas 2022-2023: 7 groups of 15 students for Clare (5), Emmanuel (2), Selwyn (3), and Downing (5) College, 21 hours in total
- Object-Oriented Programming
 - Michaelmas 2022-2023: 8 groups of 18 students for Gonville & Caius (5), Trinity Hall (4), and Kings’ (9) College, 32 hours in total
 - Michaelmas 2021-2022: 5 groups of 10 students for Robinson (6) and Fitzwilliam (4) College, 20 hours in total

Final-year Undergraduate Projects at Cambridge

- 2023-2024: Andrei-Cosmin Moroca → Software Engineer @ Bloomberg

Teaching at Vietnam National University

- 2016-2017: Fundamental of Informatics (INT1003)
- 2016-2017: Object-Oriented Programming (INT2204)

Research Talks

- Assessing the Aftermath: the Effects of a Global Takedown against DDoS-for-hire Services
 - [Conference] · USENIX Security Symposium (SEC’25) Seattle, USA · in person · 13 Aug 2025
 - [Conference] · Cambridge Cybercrime Conference (CCC’25) Cambridge, UK · in person · 23 Jun 2025
 - [Workshop] · Workshop on Security and Human Behaviour (SHB’25) Cambridge, UK · in person · 10 Jun 2024
- Beyond Whack-A-Mole: Disrupting Online Crime and Harms through Law Enforcement and Industry Efforts
 - [Seminar] · University of Cambridge Cambridge, UK · in person · 03 Dec 2024
- Yet Another Diminishing Spark: Low-level Cyberattacks in the Israel-Gaza Conflict
 - [Workshop] · IEEE European Symposium on Security and Privacy Workshops (EuroS&PW’25) Venice, Italy · in person · 30 Jun 2025
 - [Conference] · Cambridge Cybercrime Conference (CCC’24) Cambridge, UK · in person · 10 Jun 2024
- Armed Conflicts and the Changing Behaviour of Low-level Cybercrime Actors
 - [Conference] · IEEE Symposium on Security and Privacy (S&P’24), short talk San Francisco, USA · in person · 20 May 2024
- No Easy Way Out: the Effectiveness of Deplatforming an Extremist Forum to Suppress Hate and Harassment
 - [Workshop] · Workshop on Security and Human Behaviour (SHB’24) Harvard University, USA · in person · 05 Jun 2024
 - [Conference] · IEEE Symposium on Security and Privacy (S&P’24) San Francisco, USA · in person · 20 May 2024
 - [Conference] · Cambridge Cybercrime Conference (CCC’23) Cambridge, UK · in person · 22 Jun 2023
- Getting Bored of Cyberwar: the Role of Low-level Cybercrime Actors in the Russia-Ukraine Conflict
 - [Invited Talk] · DSO National Laboratories Singapore · in person · 17 May 2024
 - [Conference] · ACM World Wide Web Conference (WWW’24) Sentosa, Singapore · in person · 15 May 2024
 - [Conference] · Cambridge Cybercrime Conference (CCC’22) Cambridge, UK · in person · 05 Sep 2022
- ExtremeBB: A Database for Research into Online Hate, Harassment, the Manosphere and Extremism
 - [Workshop] · ACL Workshop on Online Abuse and Harms (WOAH@ACL’23) Toronto, Canada · online · 13 Jul 2023
- PostCog: A ‘Search Engine’ Enabling Interdisciplinary Research into Underground Forums at Scale
 - [Workshop] · IEEE European Symposium on Security and Privacy Workshops (EuroS&PW’22) Genoa, Italy · in person · 06 Jun 2022
 - [Seminar] · University of Cambridge Cambridge, UK · online · 27 May 2022
- Turning Up the Dial: the Evolution of a Cybercrime Market Through Set-Up, Stable, and Covid-19 Eras
 - [Conference] · ACM Internet Measurement Conference (IMC’20) Pittsburgh, USA · online · 29 Oct 2020
- Formal Semantics Extraction from Natural Language Specifications for ARM
 - [Conference] · International Symposium on Formal Methods (FM’19) Porto, Portugal · in person · 11 Oct 2019

Podcasts

- Hacking Out: Defacement and Hate Online amid Global Conflicts, with Michael Joyce and Professor Alice Hutchings.

Professional Activities

Programme Committees

- The International Conference on Financial Cryptography and Data Security (FC): 2025
- The International Workshop on Cryptoasset Analytics (CAAW@FC): 2025
- The ACM World Wide Web Conference (WWW): 2024
- The ACM Internet Measurement Conference (IMC): 2022 (shadow)

Journal Reviewers

- Journal of Cybersecurity: 2024

External Reviewers

- The APWG Symposium on Electronic Crime Research (eCrime): 2024
- The USENIX Security Symposium (SEC): 2024, 2023
- The IEEE European Symposium on Security and Privacy Workshops (EuroS&PW): 2022

Honours & Awards

Selected as a Cambridge representative at the Global Young Scientists Summit	Singapore, Jan 2023
Awarded the Monbukagakusho Honours Scholarship in financial support for my master's study	Japan, 2017 – 2018
Awarded Outstanding Undergraduate Student at Vietnam National University	Vietnam, Jun 2016
Awarded the Shinnyo-en Japan Scholarship in financial support for my undergraduate study	Vietnam, 2012 – 2016

Professional Skills

Security · Cybercrime · Blockchain Intelligence · Threat Intelligence · Open-Source Intelligence · Statistics · Data Science · Data Analytics · Databases · Malware Analysis · Reverse Engineering · Applied Formal Methods · Machine Learning · Software Engineering | **Programming:** Python · Java · C/C++ · SQL | **Tools:** IDA Pro · Capstone | **Languages:** English (full professional proficiency) · Vietnamese (mother tongue)

References

Professor Alice Hutchings

PHD SUPERVISOR

- Computer Laboratory, University of Cambridge
- Email: alice.hutchings@cl.cam.ac.uk
- Office: (+44) 1223 763 660

Dr Richard Clayton

FORMER LINE MANAGER

- Former director, Cambridge Cybercrime Centre
- Email: richard.clayton@cl.cam.ac.uk
- Office: (+44) 1223 763 570

Professor Mizuhito Ogawa

MSC SUPERVISOR

- School of Information Science, JAIST
- Email: mizuhito@jaist.ac.jp
- Office: (+81) 761 511 247

Professor Min Suk Kang

INTERNSHIP ADVISOR

- School of Computing, KAIST
- Email: minsukk@kaist.ac.kr
- Office: N5-2322

Research Statement

My research provides timely empirical measurements to explore cyberspace and its societal impact at scale, with a focus on the underground subcultures that foster online crime and harms. By integrating insights from both academia and industry, my work blends expertise in computer science and criminology to help better understand online threats and inform policy decisions for safety and security. My primary approach is data-driven, with research questions addressed by rigorous quantitative and qualitative measurements of large-scale real-world evidence.

I. MEASURING SECURITY AND ONLINE WICKEDNESS

Externalities, such as Covid-19, may cause significant shifts and enduring changes in human behaviour, both offline and online. My recent work explores the effects of major incidents that *intensify* or *disrupt* online crime and harms.

► Intensifying Online Crimes: The Pandemic and Armed Conflicts

Turning Up the Dial @ IMC'20 [1] evidences the significant influence of Covid-19 on illicit trading activity on the largest underground hacking forum. This empirical observation can be attributed to the increasing time spent online by individuals during lockdowns. The paper reveals that various forum users overcame the 'cold-start problem' – where new traders face difficulty settling transactions due to a lack of reputation, yet they cannot gain reputation without trading – by engaging in low-value exchanges to build their trustworthiness before developing larger trading volumes.

Getting Bored of Cyberwar @ WWW'24 [2] explores the involvement of volunteer hackers and low-level cybercrime actors in the Russia-Ukraine conflict. Although they promptly participated in targeting digital assets of both countries after the invasion using DDoS and defacement attacks, this intensification was short-lived, with a clear loss of interest after a few weeks. Their activity may cause immediately noticeable effects, but the impact was mainly propaganda dissemination instead of contributing to the 'hard' digital frontline. While popular narratives tend to overhype and conflate these actors with persistent state-sponsored hackers, we believe they should be considered separately.

Yet Another Diminishing Spark @ EuroS&PW'25 [3] compares defacements seen in the Russia-Ukraine conflict to those in the Israel-Hamas war, discovering similar patterns peaking shortly after the war started. While attacks were two-sided in the case of Russia-Ukraine, they have been mostly one-sided in the Israel-Hamas war: most targeted Israel while no significant waves have hit Palestine, presumably as Palestine has far fewer sites, many of which are hosted overseas. The scale of attacks on Israel and Palestine has been much less than those on Russia or Ukraine.

► Disrupting Online Harms: Industry and Law Enforcement Interventions

No Easy Way Out @ S&P'24 [4] examines a concerted effort to dismantle Kiwi Farms, the largest forum for online hate and harassment. We show that solely relying on deplatforming, even by swift actions of several competent tech firms, can be insufficient. The forum traffic and activity were quickly disrupted, but gradually recovered after a few months. Many users temporarily decamped to Telegram, but returned when the forum was back and became even more connected. The industry often does better than government actions, but this extraordinary event suggests that shutting down a dispersed community is unlikely to be effective if the censor cannot incapacitate or deter the key operators.

Assessing the Aftermath @ SEC'25 [5] examines a global takedown of DDoS-for-hire services involving the FBI, NCA, and Dutch Police. In two waves (December 2022 and May 2023), over 60 domains were seized and redirected to police-deployed pages to collect access information. More than half of the first-wave seized domains and all second-wave seized domains quickly resurrected – albeit with significantly reduced traffic. We show that completely eliminating booters and DDoS attacks is hard; the market has demonstrated resilience, with the statistically significant drops in global DDoS attacks lasting only around six weeks. While such recurring efforts may not prevent determined actors from running and selling DDoS attacks in the long term, they contribute to making the market untenable to operate at scale, particularly during periods of heightened attack volumes, such as school holidays and Christmas.

► Data Licensing: Reproducibility and Extensibility

Reproducibility and extensibility are crucial to me. All data used in my work can be shared with researchers, enabling them to immediately pursue ideas to address real-world problems without spending months or years collecting data.

ExtremeBB @ ACL WOA'23 [6] is a dataset for large-scale research into online hate, harassment, and extremism. Outside of Cambridge, it has been licensed to 67 scholars in 27 groups across 21 institutions in 7 countries. I co-authored

[PostCog @ EuroS&PW'22](#) [7], an interactive ‘search engine’ enabling researchers, especial non-technical scientists, to analyse our data visually and straightforwardly. I contributed to a chapter outlining how we ethically collect and share cybercrime and extremist datasets, as part of the book [Open Source Investigations in the Age of Google](#) [8].

II. CYBER ATTACKS AND DEFENSES

I believe the best way to safeguard things is to figure out how to attack them. I am particularly fascinated by fundamental research uncovering novel practical attack vectors, and research that develops tools to counter such threats.

[EREBUS @ S&P'20](#) [9] is a novel attack capable of partitioning the Bitcoin P2P network in a stealthy manner, without the victims realising they are being isolated. It leverages the advantages of big Internet entities such as ASes and ISPs to intercept and monitor thousands of ‘shadow’ malicious Bitcoin nodes. These can subsequently establish connections with legitimate nodes, gradually populating a large number of IP addresses into the victims’ peering tables, and ultimately isolating them from the rest of the network. This vector also affects many other Bitcoin-based cryptocurrencies, such as Litecoin, Bitcoin Cash, and Dogecoin, necessitating a few protocol tweaks in the Bitcoin codebase.

[CORANA @ FM'19](#) [10] is a dynamic symbolic execution engine designed for multiple ARM Cortex variants. Complicated obfuscations such as packers, indirect jumps, and dead conditional branches (often referred to as opaque predicates) pose challenges to traditional approaches for malware analysis, including both static and dynamic methods. CORANA is capable of effectively tracing IoT malware in the presence of these obfuscations. It was partly generated from natural language specifications of ARM instructions, and our paper demonstrates that this method can be systematically generalised to other variants, opening a potential research direction in applying formal methods to malware analysis.

REFERENCES

- [1] A. V. Vu, J. Hughes, I. Pete, B. Collier, Y. T. Chua, I. Shumailov, and A. Hutchings, “Turning Up the Dial: the Evolution of a Cybercrime Market Through Set-up, Stable, and Covid-19 Eras,” in *Proceedings of the ACM Internet Measurement Conference (IMC)*, 2020.
- [2] A. V. Vu, D. R. Thomas, B. Collier, A. Hutchings, R. Clayton, and R. Anderson, “Getting Bored of Cyberwar: Exploring the Role of Low-level Cybercrime Actors in the Russia-Ukraine Conflict,” in *Proceedings of the ACM Web Conference (WWW)*, 2024.
- [3] A. V. Vu, A. Hutchings, and R. Anderson, “Yet Another Diminishing Spark: Low-level Cyberattacks in the Israel-Gaza Conflict,” in *Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2025.
- [4] A. V. Vu, A. Hutchings, and R. Anderson, “No Easy Way Out: the Effectiveness of Deplatforming an Extremist Forum to Suppress Online Hate and Harassment,” in *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2024.
- [5] A. V. Vu, B. Collier, D. R. Thomas, J. Kristoff, R. Clayton, and A. Hutchings, “Assessing the Aftermath: the Effects of a Global Takedown against DDoS-for-hire Services,” in *Proceedings of the USENIX Security Symposium (SEC)*, 2025.
- [6] A. V. Vu, L. Wilson, Y. T. Chua, I. Shumailov, and R. Anderson, “ExtremeBB: A Database for Large-Scale Research into Online Hate, Harassment, the Manosphere and Extremism,” in *ACL Workshop on Online Abuse and Harms (WOAH@ACL)*, 2023.
- [7] I. Pete, J. Hughes, A. Caines, A. V. Vu, H. Gupta, A. Hutchings, R. Anderson, and P. BATTERY, “PostCog: A Tool for Interdisciplinary Research into Underground Forums at Scale,” in *Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2022.
- [8] L. Wilson, A. V. Vu, I. Pete, and Y. T. Chua, “Identifying and Collecting Public Domain Data for Tracking Cybercrime and Online Extremism,” in *Open Source Verification in the Age of Google*, 2024.
- [9] M. Tran, I. Choi, G. J. Moon, A. V. Vu, and M. S. Kang, “A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network,” in *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2020.
- [10] A. V. Vu and M. Ogawa, “Formal Semantics Extraction from Natural Language Specifications for ARM,” in *Proceedings of the International Symposium on Formal Methods (FM)*, 2019.