Curriculum Vitae **Christian Grothoff** November 11, 2024

Contents

1 General Information

1.1 Contact

Bern University of Applied Sciences
Room N.474
Höheweg 80
CH-2502 Biel-Bienne

christian@grothoff.org
http://grothoff.org/christian/
Phone (priv): +41-786926894
Phone (work): +41-323216488

Born February 28, 1977 in Germany. Citizen of Germany.

1.2 Brief Biography

Christian Grothoff is a professor for computer network security at the Bern University of Applied Sciences, researching future Internet architectures. His research interests include compilers, programming languages, software engineering, networking, security and privacy.

Previously, he was on the faculty of the Technische Universität München leading an Emmy-Noether research group in the area of computer networks. He earned his PhD in computer science from UCLA, an M.S. in computer science from Purdue University, and both a Diplom II in mathematics and the first Staatsexamen in chemistry from the Bergische Universität Gesamthochschule (BUGH) Wuppertal.

1.3 Education and Employment History

1996–2000	Diplom II (≈ M.S) in mathematics at BUGH Wuppertal
1996–2001	1. Staatsexamen (≈ B.S.) in chemistry at BUGH Wuppertal
2000–2003	M.S. in CS at Purdue University, West Lafayette, IN
2000–2005	PhD student in CS at Purdue University, West Lafayette, IN
2005–2006	PhD student in CS at UCLA, CA
2006–2009	Assistant Professor in CS at the University of Denver, CO
2009–2014	Emmy Noether research group leader at TU München
2014	Independent Journalist for Heise, The Intercept, Der Spiegel
2015	Independent Journalist for Heise, Le Monde
2014–2017	DÉCENTRALISÉ Research Team leader at Inria Rennes
2016–	Founder at Taler Systems S.A.
2017	Habilitation (HDR) at Université de Rennes 1, FR
2017–	Professor for Computer Network Security at BFH
2020–	Founder at Anastasis SARL

1.4 Honors and Awards

1998–2000	Kurt-Hansen Fellowship
2000	DAAD Fellowship
2000–2001	Barmenia Award for best graduates in mathematics
2002	Upsilon Pi Epsilon Honor Society (Purdue)
2009–2014	DFG Emmy Noether Award
2015	Most Influential OOPSLA Paper Award (for 2005)
2016–	Ashoka Fellow
2017–	GNU Advisory Board Member

1.5 Professional Associations

Christian Grothoff an associate member of the Free Software Foundation, and maintainer of five GNU packages.

2 Research

2.1 Publications

h-index: 27 (according to Google Scholar, based on 64 publications).

References

Refereed Journal Articles

[1] Christian Grothoff. "An Excess-Based Economic Model for Resource Allocation in Peer-to-Peer Networks". *Wirtschaftsinformatik*, 3-2003, pages 285–292, June 2003 (30% accepted).

[2] Krzysztof Palacz, Jason Baker, Chapman Flack, Christian Grothoff, Hiroshi Yamauchi, Jan Vitek "Engineering a Customizable Intermediate Representation". *Science of Computer Programming*, Volume 57 Issue 3, pages 357–378. Elsevier 2005
(supercedes "Engineering a Customizable Intermediate Representation" in the *Proceedings of the ACM SIGPLAN Workshop on Interpreters, Virtual Machines and Emulators, (IVME'03)*, pages 1–12. ACM SIGPLAN, 2003 (19% accepted)).

[3] Christian Grothoff, Jens Palsberg, and Jan Vitek. "Encapsulating objects with confined types". *ACM Transactions on Programming Languages and Systems*, Volume 29 Issue 6. ACM Press, 2007
(supercedes "Encapsulating objects with confined types" in the *Proceedings of the 16th ACM SIGPLAN conference on Object-oriented programing, systems, languages, and applications (OOPSLA 2001)*, pages 241–253. ACM SIGPLAN, 2001 (19% accepted)).

[4] Christian Grothoff. "The Runabout". In *Software Practice and Experience*, Volume 38, pages 1531–1560. Wiley InterScience, 2008
(supercedes "Walkabout revisited: The runabout". in *Proceedings of the European Conference on Object-oriented Programming (ECOOP 2003)*, pages 103–125. Springer-Verlag (LNCS 2743), 2003 (20% accepted)).

[5] Christian Grothoff, Krista Grothoff, Ludmila Alkhutova, Ryan Stutsman, and Mikhail Atallah. "Lost In Translation". In *Journal of Computer Security*, Volume 17 Issue 3, pages 269–304, IOS Press, 2009 (9% accepted)
(supercedes "Translation-based steganography" in *Proceedings of the Information Hiding Workshop (IH 2005)*, pages 219–233. Springer-Verlag, 2005 (31% accepted) and "Lost in Just the Translation" in *Proceedings of the 2006 ACM Symposium on Applied Computing*, pages 338–345, ACM, 2006 (19% accepted)).

[6] Kai Christian Bader, Christian Grothoff, and Harald Meier "Comprehensive and relaxed search for oligonucleotide signatures in hierarchically-clustered sequence datasets". In *Bioinformatics*, pages 1546–1554, Oxford University Press, 2011 27(11).

[7] Kai Christian Bader, Mikhail J. Atallah, and Christian Grothoff "Efficient Relaxed Search in Hierarchically-Clustered Sequence Datasets". In *ACM Journal of Experimental Algorithmics*, Vol. 17, No. 1, Article 1.4, June 2012.

[8] Florian Dold and Christian Grothoff. "Byzantine Set-Union Consensus using Efficient Set Reconciliation". In *EURASIP Journal on Information Security*, Vol. 2017, No. 1, July 2017
(supercedes "Byzantine Set-Union Consensus using Efficient Set Reconciliation" in *11th International Conference on Availability, Reliability and Security (ARES 2016)*, 2016 (24% accepted)).

[9] Christian Grothoff, Matthias Wachs, Monika Ermert and Jacob Appelbaum. "Towards Secure Name Resolution on the Internet". In *Computers & Security*, Volume 77, August 2018, Pages 694–708.

[10] Florian Dold and Christian Grothoff. "The 'payto' URI Scheme for Payments" In *Internet Requests for Comments*, RFC 8905, October 2020.

[11] David Chaum, Christian Grothoff and Thomas Moser. "How to Issue a Central Bank Digital Currency" In *SNB Working Papers*, Swiss National Bank, March 2021.

[12] David Chaum, Christian Grothoff and Thomas Moser. "Comment émettre une monnaie numérique de banque centrale" In *SNB Working Papers*, Swiss National Bank, March 2021.

[13] David Chaum, Christian Grothoff and Thomas Moser. "Cómo Emitir una Moneda Digital del Banco Central" In *SNB Working Papers*, Swiss National Bank, March 2021.

[14] Martin Schanzenbach, Christian Grothoff and Bernd Fix. "The GNU Name System" In *Internet Requests for Comments*, RFC 9498, November 2023.

Refereed Conference Papers

The following papers are *not* preliminary versions of the journal articles listed above.

[15] Krista Bennett, Christian Grothoff, Tzvetan Horozov, and Ioana Patrascu. "Efficient Sharing of Encrypted Data". In *Proceedings of the 7th Australasian Conference on Information Security and Privacy (ACISP 2002)*, pages 107–120. Springer-Verlag (LNCS 2384), 2002 (38% accepted).

[16] Krista Bennett and Christian Grothoff. "gap — Practical Anonymous Networking". In *Designing Privacy Enhancing Technologies (PET 2003)*, pages 141–160. Springer-Verlag (LNCS 2760), 2003 (27% accepted).

[17] Ronaldo A. Ferreira and Christian Grothoff and Paul Ruth. "A Transport Layer Abstraction for Peer-to-Peer Networks". In *Proceedings of the 3rd International Symposium on Cluster Computing and the Grid (GRID 2003)*, pages 398–403. IEEE Computer Society, 2003 (48% accepted).

[18] Neil Glew, Jens Palsberg, and Christian Grothoff. "Type-safe optimisation of plugin architectures". In *Proceedings of the Static Analysis Symposium (SAS'05)*, pages 135–154. Springer Verlag (LNCS 3672), 2005 (34% accepted).

[19] Philippe Charles, Christopher Donawa, Kemal Ebcioglu, Christian Grothoff, Allan Kielstra, Vivek Sarkar, and Christoph Von Praun. "X10: An object-oriented approach to non-uniform cluster computing". In *Proceedings of the 20th ACM SIGPLAN conference on Object-oriented programing, systems, languages, and applications (OOPSLA 2005)*. ACM SIGPLAN, pages 519–538, 2005 (18% accepted). **Most Influential Paper Award (in 2015)**.

[20] Mangala Gowri, Christian Grothoff, and Satish Chandra. "Deriving object typestates in the presence of inter-object references". In *Proceedings of the 20th ACM SIGPLAN conference on Object-oriented programing, systems, languages, and applications (OOPSLA 2005)*. ACM SIGPLAN, pages 77–96, 2005 (18% accepted).

[21] Rajkishore Barik, Christian Grothoff, Rahul Gupta and Vinayaka Pandit. "Optimal Bitwise Register Allocation using Integer Linear Programming". In *Languages and Compilers for High Performance Computing, 19th International Workshop, LCPC 2006*. Springer Verlag, pages 267–282, 2006.

[22] Nathan S. Evans, Chris GauthierDickey and Christian Grothoff. "Routing in the Dark: Pitch Black". In *23rd Annual Computer Security Applications Conference (ACSAC 2007)*. IEEE Computer Society, pages 305–314, 2007 (22% accepted).

[23] Chris GauthierDickey and Christian Grothoff. "Bootstrapping of Peer-to-Peer Networks". In *International Workshop on Dependable and Sustainable Peer-to-Peer Systems (DAS-P2P 2008)*. IEEE Computer Society, pages 205–208, 2008 (47% accepted).

[24] Nathaniel Nystrom, Vijay Saraswat, Jens Palsberg and Christian Grothoff. "Constrained Types for Object-Oriented Languages". In *Proceedings of the 23rd ACM SIGPLAN conference on Object-oriented programing, systems, languages, and applications (OOPSLA 2008)*. ACM SIGPLAN, 2008 (28% accepted).

[25] Nathan S. Evans, Roger Dingledine and Christian Grothoff. "A Practical Congestion Attack on Tor Using Long Paths". In *Proceedings of the 18th USENIX Security Symposium (USENIX Security '09)*. USENIX Association, pages 33–50, 2009 (15% accepted).

[26] Nathan S. Evans, Chris GauthierDickey, Christian Grothoff, Krista Grothoff, Jeff Keene and Matthew J. Rutherford. "Simplifying Parallel and Distributed Simulation with the DUP System". In *Proceedings 43rd Annual Simulation Symposium (ANSS-43 2010)*. Society for Modeling & Simulation International, pages 208–215, 2010.

[27] Kai Christian Bader, Tilo Eißler, Nathan Evans, Chris GauthierDickey, Christian Grothoff, Krista Grothoff, Jeff Keene, Harald Meier, Craig Ritzdorf and Matthew J. Rutherford. "DUP: A Distributed Stream Processing Language". In *IFIP International Conference on Network and Parallel Computing (NPC 2010)*, pages 232–246, 2010 (26% accepted).

[28] Andreas Müller, Nathan Evans, Christian Grothoff and Samy Kamkar. "Autonomous NAT Traversal". In *10th IEEE International Conference on Peer-to-Peer Computing (IEEE P2P 2010)*, pages 61–64, 2010 (23% accepted).

[29] Christian Grothoff. "The Free Secure Network Systems Group: Secure Peer-to-Peer Networking and Beyond". In *Proceedings of the First SysSec Workshop (SysSec 2011)*, pages 55–56, 2011 (69% accepted).

[30] Michael Herrmann and Christian Grothoff. "Privacy-Implications of Performance-Based Peer Selection by Onion-Routers: A Real-World Case Study using I2P". In *Privacy Enhancing Technologies Symposium (PETS 2011)*, pages 155–174, 2011 (24% accepted).

[31] Nathan Evans and Christian Grothoff. "Beyond Simulation: Large-Scale Distributed Emulation of P2P Protocols". In *4th Workshop on Cyber Security Experimentation and Test (CSET '11)*, http://www.usenix.org/events/cset11/tech/final_files/Evans.pdf, 2011 (40% accepted).

[32] Nathan Evans and Christian Grothoff. "R^5N: Randomized Recursive Routing for Restricted-Route Networks". In *5th International Conference on Network and System Security (NSS 2011)*, pages 316–321, 2011 (42% accepted).

[33] Nathan Evans, Bart Polot and Christian Grothoff. "Efficient and Secure Decentralized Network Size Estimation". In *IFIP International Conference on Networking (Networking 2012)*, pages 304–317, 2012 (28% accepted).

[34] Matthias Wachs, Christian Grothoff and Ramakrishna Thurimella. "Partitioning the Internet". In *7th International Conference on Risks and Security of Internet and Systems (CRISIS 2012)*, pages 1–8, 2012 (35% accepted).

[35] Matthias Wachs, Martin Schanzenbach and Christian Grothoff. "On the Feasibility of a Censorship Resistant Decentralized Name System". In *6th International Symposium on Foundations & Practice of Security (FPS 2013)*, 2013.

[36] Christian Grothoff, Bart Polot and Carlo von Loesch. "The Internet is Broken: Idealistic Ideas for Building a ~~NEW~~GNU Network". In *W3C/IAB Workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT)*, 2014.

[37] Bart Polot and Christian Grothoff. "CADET: Confidential Ad-hoc Decentralized End-to-End Transport". In *13th IEEE IFIP Annual Mediterranean Ad Hoc Networking Workshop (MedHocNet)*, 2014.

[38] Alejandra Morales Ruiz, Wilfried Daniels, Danny Hughes and Christian Grothoff. "Cryogenic: Enalbing Power-Aware Applications on Linux". In *2nd International Conference on ICT for Sustainability (ICT4S)*, 2014 (49% accepted).

[39] Matthias Wachs, Fabian Oelmann and Christian Grothoff. "Automatic Selection and Resource Allocation for Resilient Communication in Decentralized Networks". In *IEEE International Conference on Peer-to-Peer Computing (P2P)*, 2014.

[40] Matthias Wachs, Martin Schanzenbach and Christian Grothoff. "A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System". In *13th International Conference on Cryptology and Network Security (CANS)*, pages 127–142. Springer Verlag (LNCS 8813), 2014 (29% accepted).

[41] Álvaro García-Recuero, Jeffrey Burdges and Christian Grothoff. "Privacy-Preserving Abuse Detection in Future Decentralised Online Social Networks". In *Data Privacy Management (DPM)*, pages 78–93, 2016 (37% accepted).

[42] Neal Walfield, John Linwood Griffin and Christian Grothoff. "A Quantitative Analysis of Cell Tower Trace Data for Understanding Human Mobility and Mobile Networks". In *6th International Workshop on Mobile Entity Localization, Tracking and Analysis (MELT)*, accepted, 2016.

[43] Jeffrey Burdges, Florian Dold, Christian Grothoff and Marcello Stanisci. "Enabling Secure Web Payments with GNU Taler" In *Hot Topics in Privacy Enhancing Technologies*, HotPETs 2016.

[44] Christian Grothoff, Matthias Wachs, Monika Ermert and Jacob Appelbaum. "Towards Secure Name Resolution on the Internet". In *NDSS 2017 DNS Privacy Workshop (DPRIV17)*, 2017.

[45] Martin Schanzenbach, Christian Grothoff, Hansjürg Wenger and Maximilian Kaul. "Decentralized Identities for Self-sovereign End-users (DISSENS)". In *Open Identity Summit*, 2021.

[46] Antoine d'Aligny, Emmanuel Benoist and Christian Grothoff. "Project Depolymerization: Tokenization of Blockchains". In *4th Conference on Blockchain Research & Applications for Innovative Networks and Services*, 2022.

[47] Özgür Kesim, Christian Grothoff, Florian Dold and Martin Schanzenbach. "Zero-Knowledge Age Restriction for GNU Taler". In *27th European Symposium on Research in Computer Security (ESORICS)*, 2022.

[48] Özgür Kesim and Christian Grothoff. "Lost and Found in the Fog of Trust". In *JENSFEST'24*. ACM, 2024.

Non Peer-Reviewed Publications

[49] Christian Grothoff. "Turbo Vision: Bug in Outline". *DOS International* 7'95, page 169. DMV Daten- und Medien-Verlag Poing, July 1995.

[50] Christian Grothoff. "Ein Stethoskop für die CPU". *DOS International* 11'96, pages 272–273. DMV Daten- und Medien-Verlag Feldkirchen, November 1996.

[51] Christian Grothoff. "Schwerpunkt: Ökologische Steuerreform". In *Hochschul Umwelt Info (HUI) 2'96*, pages 18-28. Bundeskoordination Studentischer Ökologiearbeit (BSÖ), 1996.

[52] Dr. Martin Rocholl et al. "Ökologische Steuerreform, Positionspapier des deutschen Naturschutzrings (DNR)". *Koordinationsstelle DNR-Projekt Ökologische Finanzreform*, June 1997.

[53] Christian Grothoff. "Ein Kombinatorisches Standortproblem". *Diplomarbeit, Fachbereich Mathematik, BUGH Wuppertal*, 2000.

[54] Christian Grothoff. "Recycling Garbage Theory". *Purdue University, CSD TR#04-012*, 2004.

[55] Christian Grothoff. "Reading File Metadata with extract and libextractor". In *LinuxJournal* 6'2005, pages 86–88. SSC Publishing, 2005.

[56] Christian Grothoff. "Expressive Type Systems for Object-Oriented Languages". *PhD Thesis, University of California, Los Angeles*, 2006.

[57] Andrew Hunt and Christian Grothoff. "Multiple Vulnerabilities in Pidgin" CRISP Security Advisory 2007-1.

[58] Nils Durner, Nathan Evans and Christian Grothoff. "Vielleicht anonym? Die Enttarnung von StealthNet-Nutzern." In *c't magazin für computer technik* 31'2007, pages 218–221. Heise Zeitschriften Verlag, 2007.

[59] Nils Durner and Christian Grothoff. "Vulnerability in Subversion" CRISP Security Advisory 2007-2.

[60] Nils Durner, Nathan Evans and Christian Grothoff. "Anonymisierende Peer-to-Peer-Netze im Überblick" In *iX magazin für professionelle informationstechnik* 9'2008, pages 88–94. Heise Zeitschriften Verlag, 2008.

[61] Christian Grothoff. "URIs do not refer to unique files in Allmydata Tahoe" CRISP Security Advisory 2008-1.

[62] Nils Durner, Nathan Evans and Christian Grothoff. "Unerkannt im Internet" In *iX special: Sicher im Netz* 10'2008, pages 42–49. Heise Zeitschriften Verlag, 2008.

[63] Christian Grothoff. "Decentralized Open Network Services for a Resilient Economy and Free Society" In *FP8 Expert Group: Services in the future Internet*, European Commission, 2011 (invited).

[64] Bart Polot and Christian Grothoff. "Performance Regression Monitoring with Gauger". In *LinuxJournal* 9'2011, pages 68–75. SSC Publishing, 2011.

[65] Christian Grothoff "A Benchmark for HTTP 2.0 Header Compression." presented at *HTTPBIS WG (IETF 87)*, 2013.

[66] Christian Grothoff, Matthias Wachs, Hellekin Wolf and Jacob Appelbaum. "Special-Use Domain Name of Peer-to-Peer Name Systems" submitted as draft-grothoff-iesg-special-use-p2p-names-00 to IETF.

[67] Julian Kirsch, Christian Grothoff, Monika Ermert, Jacob Appelbaum, Laura Poitras and Henrik Moltke. "NSA/GCHQ: Das HACIENDA-Programm zur Kolonisierung des Internet" In *Heise Online* 8'2014. Heise Zeitschriften Verlag, 2014.

[68] Julian Kirsch, Christian Grothoff, Monika Ermert, Jacob Appelbaum, Laura Poitras and Henrik Moltke. "NSA/GCHQ: The HACIENDA-Programm for Internet Colonization" In *Heise Online* 8'2014. Heise Zeitschriften Verlag, 2014.

[69] Julian Kirsch, Christian Grothoff, Monika Ermert, Jacob Appelbaum, Laura Poitras and Henrik Moltke. "Das Five-Eyes-Botnetz" In *c't magazin für computer technik* 22/2014, pages 166-169. Heise Zeitschriften Verlag, 2014.

[70] Julian Kirsch, Christian Grothoff, Monika Ermert, Jacob Appelbaum, Laura Poitras and Henrik Moltke. "TCP Stealth vs. Five Eyes" In *c't magazin für computer technik* 22/2014, pages 170-173. Heise Zeitschriften Verlag, 2014.

[71] Julian Kirsch and Christian Grothoff. "Gut verschlossen: Unsichtbare Server mit TCP Stealth" In *iX magazin für professionelle Informationstechnik* 10'2014, pages 136-138. Heise Zeitschriften Verlag, 2014.

[72] Julian Kirsch, Christian Grothoff, Jacob Appelbaum and Holger Kenn. "TCP Stealth" submitted as draft-kirsch-iesg-tcp-stealth-00 to IETF.

[73] Laura Poitras, Marcel Rosenbach, Michael Sontheimer, Holger Stark, Andy Müller-Maguhn and Christian Grothoff. "Map of the Stars: The NSA and GCHQ Campaign Against German Satellite Companies" In *The Intercept*. 14.9.2014, First Look Media, 2014.

[74] Andy Müller-Maguhn, Laura Poitras, Marcel Rosenbach, Michael Sontheimer and Christian Grothoff. "Treasure Map: The NSA Breach of Telekom and Other German Firms" In *Spiegel Online International*. 14.9.2014, Spiegel-Verlag, 2014.

[75] Judith Horchert, Christian Grothoff and Christian Stöcker. "NSA-System Treasuremap: "Jedes Gerät, überall, jederzeit" In *Spiegel Online Netzwelt*. 17.9.2014, Spiegel-Verlag, 2014.

[76] Jacob Appelbaum, Aaron Gibson, Christian Grothoff, Andy Müller-Maguhn, Laura Poitras, Michael Sontheimer, Marcel Rosenbach and Christian Stöcker. "Prying Eyes: Inside the NSA's War on Internet Security" In *Spiegel Online International*. 29.12.2014, Spiegel-Verlag, 2014.

[77] Jacob Appelbaum, Aaron Gibson, Christian Grothoff, Andy Müller-Maguhn, Laura Poitras, Michael Sontheimer, Marcel Rosenbach and Christian Stöcker. "Fliegendes Schwein: Was die NSA knacken kann - und was nicht" In *Der Spiegel*, issue 1'2015, pages 30–32, Spiegel-Verlag, 2015.

[78] Yves Eudes, Christian Grothoff, Jacob Appelbaum, Monika Ermert, Laura Poitras and Matthias Wachs. "MoreCowBells: Nouvelles révélations sur les pratiques de la NSA" In *Le Monde*, 24.1.2015.

[79] Christian Grothoff and Monika Ermert. "Über Umwege ans Ziel" In *c't magazin für computer technik* 19'2015, pages 66-67. Heise Zeitschriften Verlag, 2015.

[80] Yves Eudes, Christian Grothoff. "Comment fonctionne Skynet, le programme ultra-secret de la NSA créé pour tuer." In *Le Monde*, 20.10.2015.

[81] Hellekin Wolf, Jaromil, Radium and Christian Grothoff. "Free Software Economics" In *Cost of Freedom: A Collective Inquiry*, pages 131-136. BookSprints, 2015.

[82] Christian Grothoff. "Design Requirements for Civil Internetworking". Protecting online privacy by enhancing IT security and strengthening EU IT capabilities. European Parliament, 2015.

[83] Monika Ermert and Christian Grothoff. "Data Mining für den Drohnenkrieg" In *c't magazin für computer technik* 3'2016, pages 82-85. Heise Zeitschriften Verlag, 2016.

[84] Christian Grothoff and Jens Porup. "The NSA's SKYNET program may be killing thousands of innocent people" In *ars technica uk*, 16.2.2016.

[85] Florian Dold and Christian Grothoff "GNU Taler: Ethical Online Payments for the Internet Age" In *ERCIM News*, No. 106, 2016.

[86] Jeffrey Burdges, Florian Dold, Christian Grothoff and Marcello Stanisci. "Enabling Secure Web Payments with GNU Taler" In *6th International Conference on Security, Privacy and Applied Cryptographic Engineering* (SPACE 2016), Springer, LNCS 10076, pages 251–270, 2016 (invited).

[87] Christian Grothoff. "The GNUnet System" *Thése d'habilitation à diriger des recherches, Université de Rennes 1, France*, 2017.

[88] Christian Grothoff. "Vertrauen im Nebel" In *spirit biel/bienne*, 1/2018, BFH, pages 16–17, 2018.

[89] Christian Grothoff. "Faire confiance dans le brouillard" In *spirit biel/bienne*, 1/2018, BFH, pages 16–17, 2018.

[90] Christian Grothoff, Martin Schanzenbach, Annett Laube, Emmanuel Benoist and Pascal Mainini. "Decentralized Authentication for Self-Sovereign Identities using Name Systems" https://gnunet.org/dasein, 2018.

[91] Christian Grothoff. "Was brauchen wir als Zivilgesellschaft eigentlich für eine Art von Netzwerk und was für eine Technik hätten wir den gerne? Verschriftlichung des Vortrags von Christian Grothoff an der FiFF Konferenz 2018. In *FIfF-Kommunikation* 1/19, pages 36–39, 2019.

[92] Christian Grothoff and Alex Pentland. "Digital cash and privacy: What are the alternatives to Libra?", https://medium.com/\spacefactor\@m{}medialab/digital-cash-and-privacy-what-are-the-alternatives-to-libra-dfa86380b511. MIT Media Lab on Medium, 19.07.2019.

[93] Christian Grothoff and Alex Pentland. "Kampf der Kryptowährungen - das sind die Alternativen zu Libra", SonntagsZeitung, Sonderbeilage Zukunft Banking, Seite 22, 1.12.2019.

[94] Christian Grothoff and Alex Pentland. "Digitales Geld und Datenschutz: Welche Alternativen es zu Libra gibt", Netzwoche, 4.10.2019.

[95] Christian Grothoff. "Free software payment system launches at Swiss university" In *Free Software Foundation Bulletin*, 37/2020.

[96] Christian Grothoff and Andreas Habegger. "GNU Taler – weit mehr als eine Spielerei" In *spirit biel/bienne*, 3/2020, BFH, 2020.

[97] Christian Grothoff and Andreas Habegger. "GNU Taler: bien plus qu'un simple gadget" In *spirit biel/bienne*, 3/2020, BFH, 2020.

[98] Christian Grothoff and Thomas Moser. "How to issue a privacy-preserving central bank digital currency" In *SUERF Policy Notes*, 114/2021, Société Universitaire Européenne de Recherches Financières (SUERF), 2021.

[99] Antoine d'Aligny, Emmanuel Benoist, Florian Dold, Christian Grothoff, Özgür Kesim and Martin Schanzenbach. "Who comes after us? The correct mindset for designing a Central Bank Digital Currency" In *SUERF Policy Notes*, 279/2022, Société Universitaire Européenne de Recherches Financières (SUERF), 2022.

[100] Priscilla Huang, Emmanuel Benoist, Christian Grothoff and Sebastian Javier Marchano. "Practical Offline Payments Using One-Time Passcodes" In *SUERF Policy Notes*, 622/2023, Société Universitaire Européenne de Recherches Financières (SUERF), 2023.

2.2 Software Systems

Christian Grothoff is a primary author of each of the applications and tools listed below. The systems are available from their respective Web pages which are all linked from http://grothoff.org/christian/.

The DUP System

DUP is a mini-language for writing distributed and parallel streaming applications using multi-stream pipelines. The DUP system includes the DUP runtime and a collection of supporting multi-stream stages or filters. It has been used in several research projects in groups from Technische Universität München, University of Denver and UCLA.

GNU Anastasis

GNU Anastasis is a key backup and recovery tool that allows users to distribute key shares to an open set of providers and to reconstruct the keys after passing authorization. Users can freely choose their providers and the authorization checks needed to recover the key material.

GNUnet

GNUnet is a framework for secure peer-to-peer networking that does not use any centralized or otherwise trusted services. The codebase consists of about 750,000 lines of C code, developed with contributions from over 50 developers worldwide.

GNU libextractor

GNU libextractor is a library used to extract meta-data from files of arbitrary type. It is designed to use plugins that perform the actual extraction. The goal is to provide developers of file-sharing networks and search tools with a universal library to obtain metadata and keywords to match against queries. *libextractor* consists of more than 35,000 lines of C and C++ code with bindings to Java, Perl, Python and PHP.

GNU libmicrohttpd

GNU libmicrohttpd is a library providing a simple, high-level abstraction for implementing HTTP servers. The focus of the project is to provide a compact, secure, reentrant, HTTP 1.1 compliant and easy to use implementation. In September 2012, GNU libmicrohttpd ranked in the top five out of over 500 "HTTP Server"-related projects in terms of popularity in the `http://freecode.com` database.

GNU Taler

GNU Taler is an electronic payment system based on blind-signatures. Taler enables the customer to remain anonymous, while those receiving payments are identifiable and auditable, and thus effectively subjected to the law and in particular taxation. Taler provides an open standard for a micropayment platform suitable for Web payments.

Runabout

The Runabout is an extension of the Java libraries that adds two-argument multi-dispatch to Java without changing the language or the VM. Like the Walkabout, the Runabout uses reflection to find visit methods. But instead of invoking the visit methods with reflection, the Runabout uses dynamic code generation to create code at runtime that will invoke the appropriate visit method. This puts the Runabout closer to MultiJava, a Java source compiler that compiles Java with multi-methods to ordinary Java bytecode. Unlike MultiJava, the Runabout runs when the application is executed, and not at compile time. Writing code with the Runabout is very similar to writing visitors or multi methods with MultiJava.

The dispatch in the Runabout is only about a factor of 3 slower than ordinary uni- or double dispatch (on Sun's JDK 1.4.1 for 10 million invocations) while saving huge amounts of trivial code and adding extensibility to the dispatch that could not be achieved otherwise. The original proposal has since spawned various successor projects by other researchers, including the Sprintabout and Poly/J.

2.3 Talks and Panels

2002 DefCon 10, on "GNUnet"

2002 Midwest Society for Programming Languages and Systems, on "The Runabout"

2004 Privacy Enhancing Technologies (PET) Workshop, on "Mix Cascades vs. Peer-to-Peer: Is One Concept Superior?" (Panel)

2005 Linux User Group (LUG) Camp, on "libextractor and GNUnet"

2005 DefCon 13, on "Lost in Translation"

2005 Southern California Workshop on Programming Languages and Systems, on "A Type System for Distributed Arrays"

2006 Front Range Information Security Conference (FRISC), on "Lost in Translation"

2006 International Conference on Object Oriented Programming, Systems Languages and Applications (OOPSLA), on "Young Guns/OO: The Next Generation" (Panel)

2007 DefCon 14, on "Routing in the Dark: Pitch Black"

2008 Rocky Mountain IPv6 Summit, on "Migrating Code to IPv6"

2008 University of Helsinki, on "Secure File-Sharing in the GNUnet Peer-to-Peer Framework"

2008 DefCon 15, on "De-Tor-iorate Anonymity"

2008 University of Dortmund, on "Secure File-Sharing in the GNUnet Peer-to-Peer Framework"

2008 University of Darmstadt, on "Secure File-Sharing in the GNUnet Peer-to-Peer Framework"

2008 Information Technology Study Group (ITSG) Fall Workshop, on "Anonymity" (Panel)

2008 University of California Los Angeles (UCLA), on "The DUP System"

2009 University of Mainz, on
"Towards Productive Parallel Programming"

2009 Front Range Architecture Compilers Tools And Languages (FRACTAL) Workshop, on
"Productive Parallel Programming for the Masses"

2009 Fórum Internacional do Software Livre, on
"Free Software for Privacy" (Keynote)

2009 Fórum Internacional do Software Livre, on
"The GNUnet Peer-to-Peer Framework"

2009 Fórum Internacional do Software Livre, on
"Tor and GNUnet: The Future of Internet Privacy" (Panel)

2010 GI-Beirat der Universitätsprofessoren, on
"Fast Primer Search with DUP"

2010 Linux User Group (LUG) Camp, on
"Spass mit paralleler und verteilter Programmierung"

2010 Linux User Group (LUG) Camp, on "ARM statt INIT"

2010 University of Wuppertal, on
"Distributed Stream Processing with the DUP System"

2010 GNU Hacker Meeting (GHM), on
"The GNUnet Peer-to-Peer framework"

2012 Linux User Group (LUG) Camp, on "tlsdate"

2012 GNU Hacker Meeting (GHM), on "A Quick Introduction to GNU libmicrohttpd"

2013 Linux User Group (LUG) Camp, on "GNU libmicrohttpd"

2013 Gulasch Programmier Nacht (GPN), on "GNU libmicrohttpd"

2013 University of Amsterdam, on "PRISM and an Agenda for European Network Security Research"

2013 IETF 87, on "A Benchmark for HTTP 2.0 Header Compression"

2013 Piratenpartei Berlin, on "Tools for Breaking out of PRISM"

2013 GNU Hacker Meeting (GHM), on "The GNU Name System and the Future of Social Networking with GNUnet"

2013 IRILL Paris, on "PRISM and an Agenda for European Network Security Research"

2013 IRISA Rennes, on "Components for Building Secure Decentralized Networks"

2013 30c3, on "The GNU Name System"

2013 30c3 YBTI Assembly, on "Secure Name Systems" (Panel)

2014 DAAD Alumni Meeting, on "A Public Key Infrastructure for Social Movements in the Age of Universal Surveillance"

2014 MPI SWS, on "Components for Building Secure Decentralized Networks"

2014 Council of Europe, on "After Snowden: using law and technology to counter snooping" (Panel)

2014 University of Oxford, on "A Public Key Infrastructure for Social Movements in the Age of Universal Surveillance"

2014 GNU Hacker Meeting (GHM), on "The GNU Name System (updated)"

2014 Daghstuhl (Privacy and Security in an Age of Surveillance), on "We fix the Net!"

2014 Free Open Source Software for Academia (fOSSa 2014), on "Taler: Taxable Anonymous Libre Electronic Reserves"

2014 Inria/DGA Formal methods and security seminar, on "Décentralisé NOW!"

2014 WeFixTheNet Workshop (2014), on "Taler: Taxable Anonymous Libre Electronic Reserves"

2015 ACTUX Meeting, on "Résistance des GNUs"

2015 Security in Times of Surveillance (TU Eindhoven), on "Knocking down the HACIENDA with TCP Stealth"

2015 Linux User Group (LUG) Camp, on "Résistance des GNUs"

2015 IETF 93, on "Special Use Domain Names of P2P Systems"

2015 IETF 93, on "Knocking down the HACIENDA with TCP Stealth"

2015 Studentenforum im Tönissteiner Kreis e.V., on "State Surveillance: Benefits and Risks"

2015 19th Workshop on Elliptic Curve Cryptography, on "Cryptography in GNUnet: Protocols for a Future Internet for Libre Societies"

2015 Invest in Cyber Convention, on
"La protection de la vie privée et sécurité des objets connectés" (Panel)

2015 Post Snowden Cryptography, on "The GNUnet: 45 Subsystems in 45 Minutes"

2016 Saarland University, on "A glimpse of the emerging GNUnet: GNU Taler"

2016 CubaConf, on "GNU Taler: A privacy-preserving online payment system for libre society"

2016 Journée du Conseil scientifique de l'Afnic, on "The GNU Name System: A clean-slate solution to the DNS security and privacy nightmare"

2016 Free Software Foundation Europe Fellowship Meeting (Düsseldorf), on "GNU Taler"

2016 Johns Hopkins University, on "The GNU Name System: A Public Key Infrastructure for Social Movements in the Age of Universal Surveillance"

2016 NPO Kongress, on "Netzwerksicherheit: Probleme und Lösungsansätze"

2016 MAPPING Second General Assembly, on "Anonymous Payment Systems"

2016 MAPPING Second General Assembly, on "Innovation, Complexity, Risk and Trust" (Panel)

2016 EIT Digital International Security Symposium, on "Enabling secure Web payments with Taler"

2016 iX Payment 2016, on "GNU Taler: Ein neues elektronisches Bezahlsystem"

2016 50p, Bangalore, 2016, on "GNU Taler: A Technological Option to Save our Democracy and Economy from 'Cashless' Totalitarianism"

2016 Sixth International Conference on Security, Privacy and Applied Cryptographic Engineering (SPACE 2016), on "Enabling Secure Web Payments with GNU Taler" (invited)

2017 Bern University of Applied Sciences, on "Social Networks versus Security and Privacy"

2017 TU Munich, on "Big Data, Little Data, No More Data"

2017 University of Luxemburg, on "Decentralizing Privacy-Preserving Network Applications"

2017 University of Luxemburg, on "GNU Taler"

2017 Chaos Singularity, on "GNU Taler"

2017 Rencontre Mondial du Logiciel Libre, on "GNU Taler: Payments for the Common Good"

2017 Still Hacking Anyway (SHA 2017), on "GNU Taler"

2018 First Values of Internet Technologies Workshop (VIT 2018), on "Escaping the Ossification Trap with GNUnet"

2018 20th European Financial Institutes – Information Sharing Analysis Center (FI-ISAC), on "GNU Taler"

2018 Politikforum Bern im Käfigturm, on "The Internet: We deserve a GNU one!"

2018 Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FiFFKon 2018), on "Netzwerkdienste für sozial-liberale Gesellschaften"

2019 Internet Research Task Force (IETF 104), on "GNU Name System: 2019 Edition"

2019 Bankademia, on "Surviving Private Key Compromise in Electronic Payment Systems"

2019 Network of Networks (Internet Society, University of Zurich), on "Privacy at the Edge"

2020 About and Beyond PKI, on "Use-Cases for Private Information Retrieval and Secure Multiparty Computation in Modern Network Architecture"

2020 NGI projects' contribution to technological developments of DNS and naming systems, on "The GNU Name System & NGI"

2022 Netzpolitischer Abend der Digitalen Gesellschaft in Zürich, on "Datenschutzfreundliches digitales Bezahlen"

2022 IPEN Webinar on "Central Bank Digital Currency" (Panel)

2023 MozTW Lab, on "Introduction to GNU Taler"

2023 Academica Sineca, on "The GNU Name System"

2024 Swiss Cyber Security Days, on "Bezahlbestätigungen für Offline-Händler"

2024 Datenspuren, on "GNU Taler für Events"

2024 FIND Academia + Innosuisse workshop, on "The GNU Taler payment system"

2.4 Funding

- NSF 0416969 "Curriculum Development Initiative in Cyber Trust at the University of Denver" (co-PI, $296,831). The primary goal of this grant was to establish a computer security center at the University of Denver. As part of his work on the grant, Christian Grothoff helped establish the Colorado Research Institute for Security and Privacy and obtain an NSA designation as a Center for Excellence in Information Assurance for the University of Denver. He also organized several regional conferences and workshops in the area of computer security. The award duration was from September 2004 to August 2009; I became a co-PI on this grant in August 2007.

- WIRED "Innovative Partnership for Job Creation and Employment" (co-PI, $405,000). The goal of the computer science part of the grant was to establish a new course and certificate program in mainframe administration at the University of Denver and to provide scholarships for underemployed IT administrators and programmers to help them obtain a certification as mainframe administrators. Christian Grothoff was responsible for the computer science portion, which is also supported by IBM with software and equipment valued at approximately $5,000,000. The program started July 2008 and ended December 2009. In January 2010 IBM announced that one of the scholarship recipients who participated in Grothoff's Mainframe course won IBM's Master of the Mainframe Contest (1st out of over 3,000 contestants).

- nlnet "Fast and Resillient Routing for GNUnet" (PI, $33,901). The goal of the proposed work was to design and implement a secure P2P routing protocol that will achieve availability and scalability without infringing on the openness of the network. The design targets fully-decentralized, restricted-route networks with malicious participants. The project started January 2009 and ended December 2009 culminating in the GNUnet 0.8.1 release which contains a prototype of such an algorithm.

- United States Department of Defense (DoD) Information Assurance Scholarship Program (IASP) Grant (PI, $2,280 plus option for up to $354,352). Under this grant, the DoD will fund up to 10 graduate students from the National Defense University to study information

security at the University of Denver. The program started July 2009 and ends June 2010. Funding started after Grothoff left the US for Technische Universität München; the project was handed over to a co-PI.

- NSF "Collaborative-Research: A Partnership for Developing the IA Workforce". The goal of this grant is to help the University of the District of Columbia build a quality program in information assurance (co-PI, $299,978). Funding started after Grothoff left the US for Technische Universität München; the project was handed over to another co-PI.

- Deutsche Forschungsgesellschaft "Secure Randomized Peer-to-Peer Routing Protocols" (PI, €1,305,200). This project is about the design, analysis and implementation of new secure and efficient routing protocols for open heterogeneous networks. Funded from September 2009 until August 2014.

- Cloudmark Inc. ($5,000). Unrestricted gift to lab in appreciation of our work on GNU libmicrohttpd (2010).

- FP7 "OpenLab-Eclectic" (PI, €123,334). This project was about improving tools for resource allocation, execution and observation of experiments in network testbeds (2013-2014, 9 months).

- The Renewable Freedom Foundation "GNUnet" (PI, €300,000). The goal of the proposed research and development effort was to use cryptography, network protocol design and secure software engineering to build the GNUnet, a fully decentralized secure global network that respects user freedoms, providing users with a free networking platform that protects their privacy in both economic and social contexts and provides them with a neutral, censorship-resistant news distribution mechanism to facilitate informed democratic decision-making processes. Various subsystems of GNUnet were developed or improved, and GNU Taler was formally launched as a sub-project and startup (2014-2017).

- Brittany Region (ARED 9174) for three years to develop GNU Taler (PI, €52,000).

- The Renewable Freedom Foundation "GNU Taler for Saleor" (PI, €10,000). The goal of this project was to develop a payment plugin to pay using GNU Taler for Saleor (2018).

- NLnet NGI DISCOVERY: "Standardizing the GNU Name System" (PI, €50,000). The goal of this project is to create a second implementation of the GNU Name System as well as an IETF draft doc-

umenting the protocol. Furthermore, we will package the resulting software for various distributions (2019-2020).

- NLnet NGI ZERO: "GNU Taler" (co-PI, €50,000). The goal of this project is to perform an independent security audit of the Taler exchange codebase, address discovered vulnerabilities, and to establish the knowledge foundation to operate an independent Taler auditor. (2020-2021).

- NGI TRUST: "Decentralized Identities for Self-Sovereign End-Users" (co-PI, €134,000). The goal of this project is to integrate the self-sovereign Reclaim:ID identity management and GNU Taler payments into a holistic, privacy-preserving one-click checkout user experience and to evaluate its usability (2020-2021).

- NGI LEDGER: "Anastasis" (PI, €125,000). The goal of this project was the implementation of the Anastasis key backup and recovery solution and the creation of a startup to drive the further adoption and operation of the service.

- NGI Fed4Fire+: "Taler Scalability" (PI, €10,000). The goal of this project is to demonstrate the scalability of the GNU Taler payment system in the Grid5000 (2021).

- NGI POINTER: "AP^3: Advanced privacy-preserving protocol extensions for the GNU Taler system" (€200,000). The goal of this project is to extend the core Taler payment protocol with privacy-preserving age restrictions, peer-to-peer payments and privacy-preserving auctions (2021-2022).

- NLnet NGI ZERO ENTRUST: "KYC for GNU Taler" (PI, €31,525). The goal of this project is to implement Know-Your-Customer support in GNU Taler, including integration of proprietary KYC providers as well as KYC providers supporting the OAuth2 standard and the implementation of a simple attestation service based on OAuth2 (2023-2024).

- NGI TALER (co-PI, €4,508,355). The goal of this project is to deploy GNU Taler across Europe and ensure its adoption across various verticals (2023-2026).

3 Teaching

3.1 Teaching at the University of Denver

- Instructor for "Compilers" (graduate level)

- Instructor for "Computer Security" (graduate level, 2x)
- Instructor for "Computer Security from a Free Software Perspective" (freshmen seminar, non-majors)
- Instructor for "Distributed Stream Processing" (graduate level)
- Instructor for "Introduction to Systems Programming" (undergraduate level)
- Instructor for "Mainframe Administration" (undergraduate, graduate and non-traditional students)
- Instructor for "Programming Languages" (both undergraduate and graduate students, 3x)
- Instructor for "UNIX tools" (undergraduate level)

3.2 Teaching at Technische Universität München

- Co-Instructor for "Masterkurs Rechnernetze" (graduate level)
- Instructor for "Peer-to-Peer Systems and Security" (graduate level)

3.3 Teaching at BFH

- Instructor for "Grundlagen der Informatik" (undergraduate)
- Instructor for "CS Basics" (undergraduate)
- Co-Instructor for "Secure IT Infrastructure" (undergraduate)
- Co-Instructor for "Management of Mobile Applications and Systems (undergraduate)
- Instructor for "Telematik" (undergraduate)
- Instructor for "Network Design and Services" (undergraduate)
- Instructor for "Networking" (undergraduate)
- Co-Instructor for "Seminar" (undergraduate)

3.4 Theses supervision

I was the primary advisor for the following theses:

- Nathan Evans: "Routing in the Dark: Pitch Black" (MS, 2009)

- Michael Herrmann: "Privacy-Implications of Performance-Based Peer Selection by Onion-Routers:A Real-World Case Study using I2P" (MS, 2011)
- Nathan Evans: "Methods for Secure Decentralized Routing in Open Networks" (PhD, 2011)
- Safey A. Halim: "Monkey: Automated debugging of deployed distributed systems" (MS, 2012)
- Martin Schanzenbach: "Design and Implementation of a Censorship Resistant and Fully Decentralized Naming System" (MS, 2012)
- Maximilian Szengel: "Distributed Evaluation of Policies for Group Management in Mesh Networks" (MS, 2012)
- Kai C. Bader: "High-performance approaches to the comprehensive computation and evaluation of signatures in bacterial sequence datasets" (PhD, 2013)
- Markus Teich: "Monkey - Generating Useful Bug Reports Automatically" (BS, 2013)
- Gabor X. Toth: "Design of a Social Messaging System Using Stateful Multicast" (MS, 2013)
- Andrey Uzunov: "Speeding up Tor with SPDY" (MS, 2013)
- Alejandra Morales Ruiz: "Cryogenic: Enabling Power-Aware Applications on Linux" (MS, 2014)
- Julian Kirsch: "Improved Kernel-Based Port-Knocking in Linux" (MS, 2014)
- Florian Dold: "Cryptographically Secure, Distributed Electronic Voting" (BS, 2014)
- Supriti Singh: "Comparison of Byzantine fault-tolerant Distributed Hash Tables" (MS, 2014)
- Nicolas Benes: "An Approach for Home Routers to Securely Delete Sensitive Data" (BS, 2014)
- Matthias Wachs: "A Secure Communication Infrastructure for Decentralized Networking Applications" (PhD, 2015)
- Florian Dold: "Byzantine Fault Tolerant Set Consensus with Efficient Set Reconciliation" (MS, 2015)

- Neal Walfield: "Location Prediction for Context-aware Applications" (PhD, 2016)
- Markus Teich: "Implementing Privacy Preserving Auction Protocols" (MS, 2017)
- Florian Dold: "The GNU Taler System" (PhD, 2019)
- Patrick Gerber: "Packaging Ascension for Debian: Automatic migration from DNS to GNS" (BS, 2019)
- Dennis Neufeld, Dominik Meister: "Anastasis: Password-less key recovery via multi-factor multi-party authentication" (BS, 2020)
- Amin Schaller, Antonio Musardo: "Comparison of PLT optimized HTTP/2 vs. HTTP/3 setups" (BS, 2021)
- Elias Summermatter: "Byzantine Fault Tolerant Set Reconciliation" (BS, 2021)
- Marco Boss: "GNU Taler Scalability" (BS, 2022)
- Joel Urech: "Frosix: FROST Multiparty Signatures on the Network" (BS, 2023)
- Kevin Schrag: "Fog of Trust" (BS, 2023)