

Laurence Lerch

Ethik der Kryptographie



Nomos

Ethik | Ethics

herausgegeben von | edited by

Prof. Dr. Peter G. Kirchschräger

Prof. Dr. Christine Abbt

Prof. Dr. Georges Enderle

Band | Volume 3

Laurence Lerch

Ethik der Kryptographie



Nomos

Gefördert durch die Hanns-Seidel-Stiftung aus Mitteln des deutschen Bundesministeriums für Bildung und Forschung. Publiziert mit Unterstützung des Schweizerischen Nationalfonds zur Förderung der wissenschaftlichen Forschung.

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

1. Auflage 2025

© Der Autor

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

Zugl.: Luzern, Universität, Diss., 2024

ISBN (Print): 978-3-7560-3158-0
ISBN (ePDF): 978-3-7489-5500-9

DOI: <https://doi.org/10.5771/9783748955009>



Onlineversion
Nomos eLibrary



Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung 4.0 International Lizenz.

Danksagung

Die Universität Luzern hat die vorliegende Arbeit im Frühjahrssemester 2024 als Dissertation angenommen. Literatur und Forschung ist dementsprechend bis April 2024 berücksichtigt. Die vorangegangenen drei Jahre des unermüdlichen Forschens behalte ich als lehrreiche, aber auch entbehrungsreiche Zeit in Erinnerung, in der ich viel auf die Unterstützung meines akademischen und persönlichen Umfelds angewiesen war. Zunächst danke ich meinem Betreuer Prof. Dr. Peter G. Kirchschräger und dem Institut für Sozialethik an der Universität Luzern. Dort habe ich einen Platz gefunden, wo ich eigenständig denken, arbeiten und lernen durfte. Auch meinem Zweitgutachter Prof. Dr. Christian Preidel gebührt ein solcher Dank.

Inhaltlich möchte ich mich zudem bei all jenen Menschen bedanken, die sich seit Jahren unermüdlich für die Weiterentwicklung und die Verbreitung von Kryptographie einsetzen – sei es in der Wissenschaft, der Gesellschaft, der Politik oder den Medien. Ich denke hier zum einen an all jene, die sich als Cypherpunks identifizieren, zum anderen aber auch an die unzähligen Organisationen weltweit, die sich für Privatsphäre, Datenschutz und freie Meinungsäußerung engagieren. Ihr seid es, die mich zu diesem Forschungsthema gebracht haben.

Für dieses Unterfangen unerlässlich war aber auch die Fürsorge meiner Familie und Freunde. Dies nicht nur in den Jahren des intensiven Forschens, sondern vielmehr in all den vorherigen Kinder- und Jugendjahren, in denen sie mir stets den Raum zum Lernen und zur eigenen Entfaltung gegeben haben. Meinen beiden Eltern, meinen Großeltern aus Greding und Donauwörth, meiner Patentante sowie meinen sechs Geschwistern gilt dieser Dank ebenso wie Anke, die mich immer auf diesem Weg begleitet und die Arbeit in unzähligen Stunden Korrektur gelesen hat.

Inhaltsverzeichnis

Danksagung	5
Einführung	9

Teil I Kryptographie & Technologie

1	Klassische Kryptographie	19
1.1	Die Anfänge von Kryptographie und Kryptoanalyse	20
1.2	Die Mechanisierung der Kryptographie	32
2	Moderne Kryptographie	37
2.1	Ein neues Paradigma durch die Mathematik	38
2.2	Der Data Encryption Standard (DES)	44
2.3	Diffie-Hellman und RSA	50
2.4	Kryptographie und Informationssicherheit	56
2.5	Quantum Computing und Verschlüsselung	66

Teil II Kryptographie & Gesellschaft

3	Aktivismus und Kryptographie	79
3.1	Pretty Good Privacy (PGP)	80
3.2	Cryptoaktivismus	87
3.3	Cyberpunks und Crypto-Anarchie	95
4	Internet, Kryptographie und Regulierung	109
4.1	Internet und Kryptographie	110
4.2	Warum das Internet <i>doch</i> regulierbar ist	116
4.3	Und warum auch Kryptographie regulierbar ist	125

Teil III Kryptographie & Ethik

5	Ethische Zugänge zur Kryptographie	147
5.1	Konsequentialistische und pflichtethische Ansätze	148
5.2	Menschenrechte und Kryptographie	164
5.3	Werte, Normen und <i>latent ambiguities</i>	178
6	Zielkonflikte und (Schein-)Dichotomien	187
6.1	Kryptographie und Dual Use	188
6.2	Privacy vs. Sicherheit	196
6.3	Überwachung vs. Kryptographie	204
7	Transparenz, Gleichheit und Identität	221
7.1	Transparenz und Verschlüsselung	221
7.2	Egalitäre Kryptographie	235
7.3	Identifikation mithilfe von Kryptographie	244
8	Synthese und Anwendung	253
8.1	Client-Side-Scanning (CSS)	254
8.2	Regulierung über Intermediäre	269
8.3	Zukunft (einer Ethik) der Kryptographie	276
	Schluss und Ausblick	285
	Literatur	293