Identifikation in Sozialen Netzwerken

Clemens H. Cap

October 2026

1 Hintergrund

Bei Inhalten in sozialen Netzen bestehen vielerlei einander widersprechende Ziele hinsichtlich der Identifizierung eines Autors und der Integrität der Inhalte. Ein Autor möchte namentlich als Autor genannt und erkennbar sein, zugleich will er sicherstellen, daß sein Artikel vom Systembetrieber nicht verändert werden kann. Ein anderer Autor möchte vielleicht namentlich nicht genannt werden und seine Meinung so unter einem Pseudonym veröffentlichen, daß seine spätere Identifikation als Autor ausgeschlossen ist. In einer Variante dieser Situation will er vielleicht von Dritten nicht als Autor identifiziert werden, später aber auf eigenen Wunsch nachweisen können, daß er tatsächlich Autor des Beitrags war. Ebenso kann zwischen einem namentlich und bürgerlich bekannten Nym (Hans Müller, geboren am 9. 9. 1999 in Ingolstadt) und einem Pseudonym (DonaldDuck23, Besitzer des privaten Schlüssels, der zum öffentlich bekannten Schlüssel 4711 paßt) unterschieden werden. Die Gesellschaft wiederum hat Interesse, daß bei kontroversen Themen der Verantwortliche identifiziert werden kann. In einem Beitrag genannte Personen wollen einen Ansprechpartner für inhaltliche Richtigstellung oder Entgegnung (was nur die grundsätzliche Kommunikationsmöglichkeit, nicht unbedingt die bürgerlich Identifizierung umfaßt); vielleicht aber wollen sie auch eine Person, die sie vor einem Gericht wegen Beleidigung verklagen können (was eine zivilgesellschaftliche Identifizierung erfordert, zumindest mittelbar über Zeit und Adresse des IP-Zugangs).

Bestehende soziale Netze und Systeme sind aber meist so gebaut, daß typischerweise nur eine dieser Interessen realisiert ist und dem Anwender die genaue Form nicht bekannt ist.

2 Aufgabenbeschreibung

Die Problemstellung umfaßt die nachfolgend genannten Aspekte.

1. **Klassifikation** der unterschiedlichen Anforderungen und Beschreibung in exemplarischen Use Cases. Dokumentation, wie sich diese Use Casese bereits in bestehenden sozialen Netzen (Sites sowie Software-Systemen dazu) realisiert finden.
2. **Herausarbeiten** widersprüchlicher Anforderungen (etwa: Übernahme inhaltlicher Verantwortung und Wunsch nach anonymer oder pseudonymer Veröffentlichung). Aufzeigen von Lösungsmöglichkeiten bei Widersprüchen.
3. **Abbildung** der einzelnen Use Cases auf informatische Verfahren und Algorithmen. (etwa: Nachweisbare Autorenschaft auf unterschiedliche Formen digitaler Signaturen und Zeitstempel). Analyse der Angriffsvektoren auf diese Verfahren.

Für die beschriebene Aufgabenstellung gibt es sehr viel einschlägige Prior Art, allerdings verteilt über mehrere Forschungsgebiete. Insbesondere die Kombination aus nachweisbarer Integrität, pseudonymer oder anonymer Autorenschaft, optionaler späterer Offenlegung der Identität und Manipulationsschutz gegenüber dem Plattformbetreiber ist bereits seit den 1980er/1990er Jahren Gegenstand kryptographischer Forschung.

Eine mögliche Taxaonomie kann daher beispielsweise längs folgender Dimensionen erfolgen:

1. Integrity: Ist eine nachträgliche Änderung nachweisbar?
2. Linkability: Sind mehrere Beiträge desselben Autors miteinander verknüpfbar?
3. Public author identification: Kennt die Öffentlichkeit die Identität?
4. Opening: Existiert eine Instanz, die die Identität offenlegen kann?
5. Author-controlled disclosure: Kann nur der Autor sich später selbst identifizieren?
6. Timestamp/provenance: Ist Publikationszeit/Historie nachweisbar?
7. Real-world identity binding: Ist der Schlüssel an eine bürgerliche Identität gebunden?

Vorkenntnisse: Für die Übernahme der Arbeit Voraussetzung sind gute bis sehr gute Kenntnisse kryptographischer Verfahren und präzise Sprachbeherrschung (C1 aufwärts oder Muttersprache in englisch oder deutsch) für die Beschreibung der Use Cases.