

My background

- M.Sc. «IT-Systems Engineering»
 - Hasso Plattner Institute, Potsdam
 - 2021
- PhD studies in Quantum Computing
 - 2021 – 2022
- Master's studies «Informasjonssikkerhet»
 - IFI, UiO
 - 2023 (– ongoing)





I'm working here right now

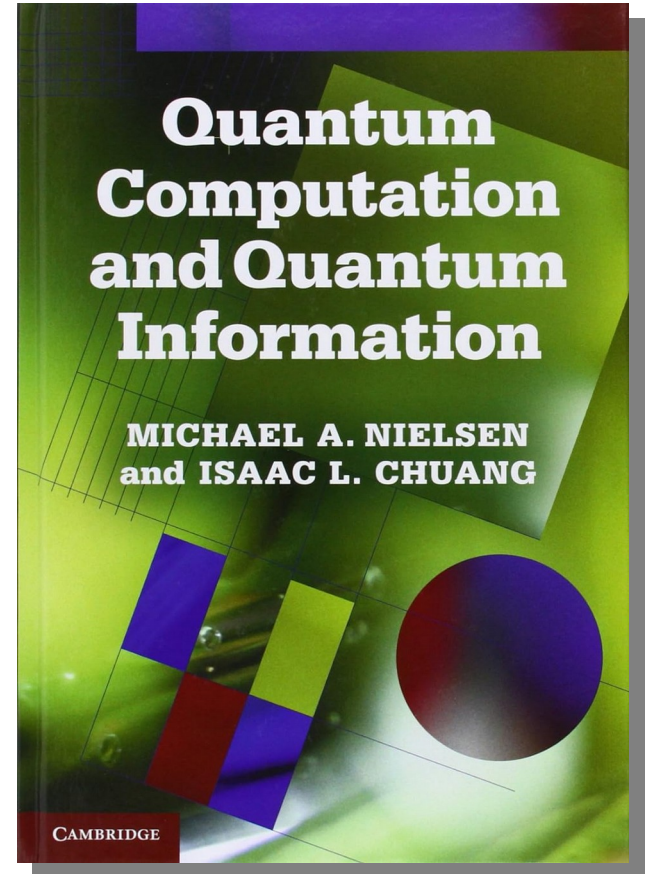
DATA@UIO



UNIVERSITETET
I OSLO

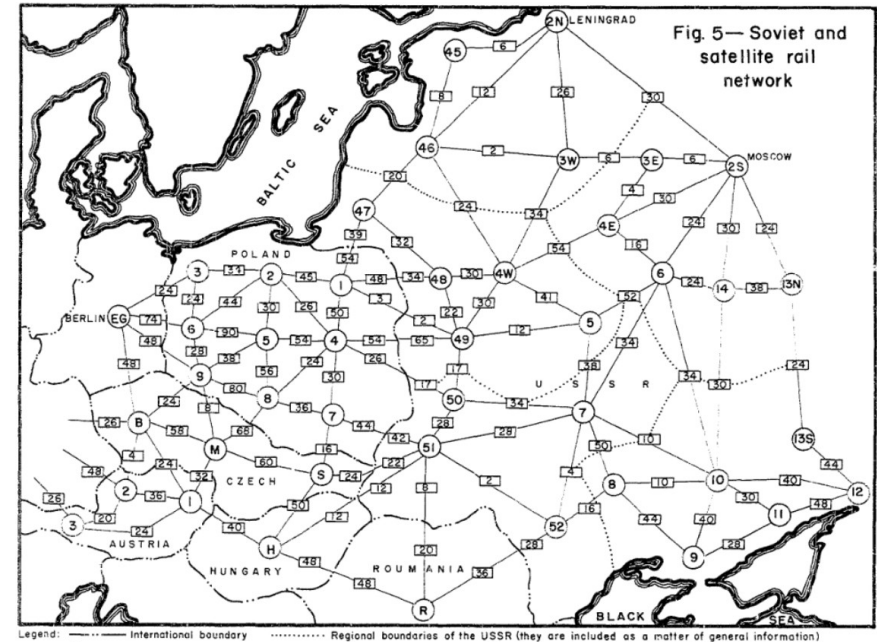
A subset of my research interests

- Algorithmic Game Theory
- Quantum Computing
- GDPR and digital politics
- Cryptography
- ...



Master's Thesis: «Flow Based Network Creation Games», 2020

- Max-flow / Min-cut
- Uncoordinated Network Creation
- «Algorithmic» Game Theory
 - Comp. Complexity of finding equilibria
 - Convergence and stability
 - Quality of equilibria
- <https://doi.org/10.24963/ijcai.2020/20>



Recent publication about research data from a Norwegian Corona-app

- Alternative title candidates:
 - «Data anonymisation: How to mess it up»
 - «TIL that SHA256 is not an anonymization method»
- Norsk Informasjonssikkerhetskonferanse (NISK) 2022
- <https://ojs.bibsys.no/index.php/NIK/article/view/1022>

Attack vectors to re-identify individuals from the anonymised Smittestopp dataset

Hagen Echzell

Independent Researcher
Oslo, Norway
hagen.pub@echzell.org

Abstract. The first version of “Smittestopp”, the Norwegian Institute of Public Health’s (NIPH) contact tracing application, centrally stored data about the population’s contact patterns with reference to a static personal identifier, a decision that has been widely discussed and criticised. After the Norwegian Data Protection Authority had temporarily forbidden further data collection and processing in June 2020, NIPH announced to discontinue the app and stated that all data related to the application would be deleted. Nevertheless, in October 2021, researchers from an institution involved in the development of the app published a paper called “Nationwide rollout reveals efficacy of epidemic control through digital contact tracing” [3]. In their paper, they analysed a derived dataset based on the Smittestopp data that was announced to be deleted. The authors claim that this derived dataset was anonymised and therefore does not include any personal data. We challenge this assumption by explaining how different external sets of personal data can be matched with the dataset, which potentially leads to a re-identification of persons and a disclosure of their private contacts. We conceptually show how some of these methods can be applied on an example case using publicly available information on Erna Solberg, Norway’s former prime minister. We conclude that it appears reasonably likely that individuals can be re-identified and that the dataset should not be considered anonymised.

Keywords: Anonymisation · Contact Tracing · GDPR · Privacy · Smittestopp

I'll be writing another Master's Thesis, soon!

Looking for:

- Ideas
- Research or industrial partners
- Funding
- Potential PhD opportunities afterwards

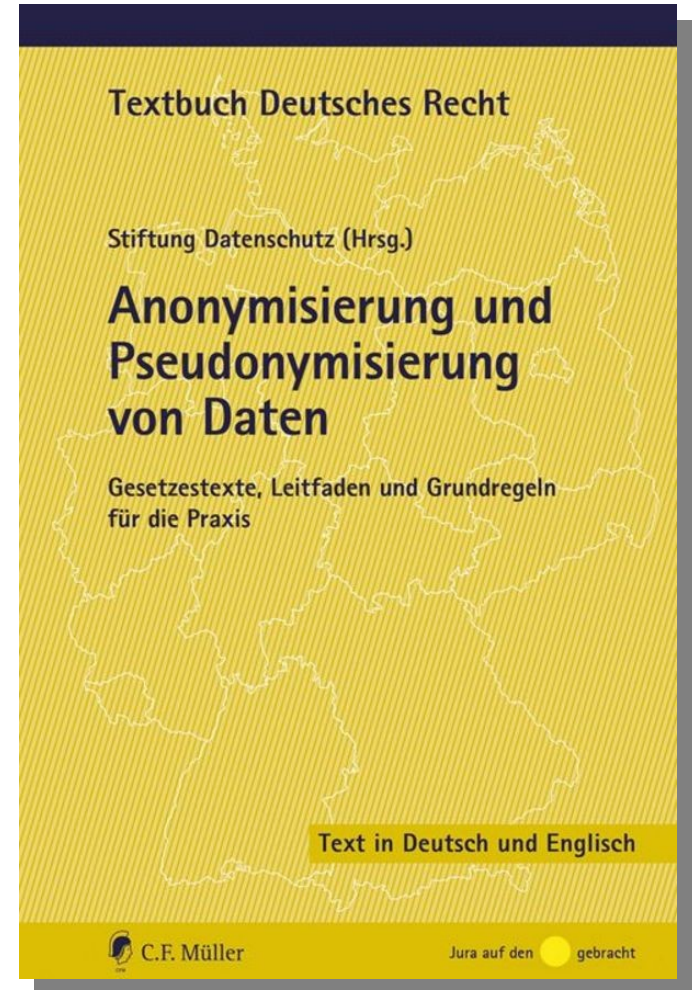
Digital central bank money

- Norges Bank hires Web3-folks to work on blockchain-stuff
- I'd like to explore alternatives
 - GNU Taler (<https://taler.net/en/>)
 - Blind signatures
- Currency or payment system?
- Potential for interdisciplinary research



Data Anonymisation

- There are some formal approaches (*k-anonymity*, *l-diversity*, ...)
- Properly applying them is still more art than science
- No universal, formal concept of anonymous data
 - Apply ideas from Information Theory or homomorphic encryption?
- Also some open legal questions



Secure, decentralized communication

- New regulation for communication services
 - Digital Markes Act (Art. 7)
 - Interoperability obligations
- Decentral E2EE?
- Public Key infrastructure?
- New IETF Standards:
 - Message Layer Security (MLS)
 - More IM Interoperability (MIMI)



Business, Economy, Euro

Digital Markets Act (DMA)



Let's have a chat or send me an email

- <mailto:hagen.pub@echzell.org>
- <https://cv.derhagen.eu/> (slightly outdated)



Utlendinger kan få sikkerhetsklarering

For å være en aktuell kandidat til stillingen, **må du være norsk statsborger**, og du må kunne sikkerhetsklareres og autoriseres for nivå HEMMELIG og NATO SECRET med særinstrukser fra Nasjonal Sikkerhetsmyndighet.

Jeg er utenlandsk statsborger, kan jeg få sikkerhetsklarering? ^

En utenlandsk statsborger kan gis sikkerhetsklarering etter en konkret individuell helhetsvurdering dersom det ikke er rimelig grunn til å tvile på at personen er sikkerhetsmessig skikket. I tillegg til vurderingskriteriene i [sikkerhetsloven § 8-4](#) skal det i vurderingen legges vekt på hjemlandets sikkerhetsmessige betydning, personens tilknytning til hjemlandet og Norge, jf. [sikkerhetsloven § 8-7](#).



NSM