CRYPTIC COMMONS
An online research workshop on
human/society/cryptography interfaces
May 20-21, 2021

# Cryptic Commons:

## Transdisciplinary Probes of the Ideal and Real World in Actual Cyber-Physical Systems

*Aalborg University / ONLINE. May 20-21, 2021.*

Cryptographers often refer to notions of the ideal world and the real world in the development and implementation of cryptographic primitives and protocols. This framing allows them to evaluate the trustworthiness of cryptographic tools, by comparing them against an ideal standard, in which there are no security breaches, total honesty and zero corruption. But how useful is this utopian framing of the "ideal" for tools that are meant to function in the cryptographic "real" world and significantly, in cyber-physical and social "actual" worlds? The workshop "Cryptic Commons" seeks to probe these questions with a series of keynote speakers from different disciplines, short examples from ongoing research and moderated, transdisciplinary debates.

'Cryptic commons' refers to the common language and understandings across disciplinary boundaries that are necessary to secure the development of future cryptographic tools that are socially, culturally and ethically sound. Researchers and developers from engineering, data science and cryptography often work in disciplinary silos where specialized developments can be pursued, and expertise honed. These are valuable fora for cutting-edge research. But this sometimes comes at the cost of insight from other disciplines. If data represents citizens, and data analytics is used to make fundamental decisions about citizens, then securing this data and how it is interpreted is a deeply social endeavor. Engineers, data scientists and cryptographers are however not trained to grasp social insights that are not quantifiable. At the same time, social science and humanities researchers often work far from the sites at which data tools and analytics are developed, and so they lack an understanding of the technical logics and methods within which their colleagues work.

This workshop brings together noted researchers interested in the development of cryptography and cyber-physical systems, and their social impacts. We invite scholars from a broad range of disciplines: cryptography, computer science, engineering and the social and human sciences to explore pathways for the collaborations and developments that are necessary for the making of cryptic commons.

During the workshop, we will probe what it means to be "stuck in the gap" and how to create "cryptic commons".

## Keynote speakers and roundtable participants

- Ross Anderson, Professor of Security Engineering, University of Cambridge and University of Edinburgh.
- Harold Vincent Poor, Professor of Electrical and Computer Engineering, Princeton University.
- Helen Nissenbaum, Professor at Cornell Tech and in the Information Science Department, Cornell.
- Susan Landau, Professor of Cyber Security and Policy, The Fletcher School and the School of Engineering, Tufts University.
- Michael J. Fischer, Professor of Anthropology and Science and Technology Studies, MIT.
- Rafael Wisniewski, Professor, Department of Electronic Systems, Aalborg University.
- Mads Græsbøll Christensen, Professor, Department of Architecture, Design and Media Technology.

# Workshop Program:

## Day 1: May 20th

| | |
|---|---|
| 13.30 – 14.00 (CET) | |
| Welcome & opening | Prof. Rafael Wisniewski, Principal Investigator SECURE |
| Workshop Concepts | Assoc. Prof. Astrid O. Andersen & Asst. Prof. Adrienne Mannov |
| Practical Directions | Signe Helbo Gregers Sørensen & Kîsta Bianco Kjær |
| 14:00-16.30:<br>**Plenary 1** | Historical layer: Versions of Crypto Dreams Across Time<br>Chair: Adrienne Mannov |
| 14.00 – 15.00<br>**Keynote 1** | Ross Anderson, Professor of Security Engineering, University of Cambridge and University of Edinburgh:<br>"Utopia Redux: Forty years of crypto dreams" |
| 15.00 – 15.15 | BREAK |
| 15.15 – 16.00 | Short presentations by Invited Researchers: |
| 15:15 – 15:30 | Sarah Scheffler, PhD student, Boston University: "A cryptographic view of "foregone conclusions" in compelled self-incrimination" |
| 15:30 – 15:45 | Diego Aranha, Aarhus University: "Quick update on the Brazilian Crypto Wars" |
| 15:45 – 16:00 | Rodrigo Ochigame, PhD candidate, MIT: "Parasemiotic Synthesis" |
| 16.00 – 16.30 | Panel Discussion: Dialogue with Keynote and Presenters<br>Discussant: Michael Fischer, Professor of Anthropology and Science and Technology Studies, MIT.<br>Panelists: Ross Anderson, Sarah Scheffler, Diego Aranha, Rodrigo Ochigame |
| Break | *Grab a snack and check out Science TV!* |
| 17.00-19.30:<br>**Plenary 2** | Mathematical Layer: Computing at the Edges of Math and Society<br>Chair: Jonas Falzarano Jessen |
| 17.00 – 18.00:<br>**Keynote 2** | H. Vincent Poor, Professor of Electrical and Computer Engineering, Princeton University: "Machine Learning at the Wireless Edge" |
| 18:00 – 18.15 | BREAK |
| 18.15 – 19:00 | Short presentations by invited researchers: |
| 18:15 – 18:30 | Manuel Sabin, UC Berkeley: "Power and Participatory Hurdles: Some Preemptive Points of Caution for Participatory Approaches to Machine Learning" |
| 18:30 – 18:45 | Jaron Gundersen (Postdoctoral researcher, Aalborg University (SECURE project): "Security with an incomplete communication graph" |
| 18:45 – 19:00 | Adrienne Mannov (Aarhus University) & Astrid Oberborbeck Andersen (Aalborg University – SECURE project): "From Trust to Care: A Speculative Ethics of the Actual in Cryptographic Worlds" |
| 19.00 – 19.30 | Panel Discussion: Computing at the Edges of Math and Society<br>Discussant: Michael Fischer, Professor of Anthropology and Science and Technology Studies, MIT, with SECURE researcher<br>Panelists: Mads Græsbøll Christensen. Manuel Sabin, Jaron Gundersen and Astrienne |
| 19.30 | *Thanks for today! See you tomorrow!* |

## Day 2: May 21st

| | |
|---|---|
| Welcome back! | Asst. Prof. **Adrienne Mannov** |

| | |
|---|---|
| 15.30-18.15:<br>**Plenary 3** | Social Layer: Iterations of the Social Along the Data Food Chain<br>Chair: Astrid Oberborbeck Andersen |
| 15.30 – 16.30:<br>**Keynote 3** | "Contextual Integrity Up and Down the Data Food Chain"<br>**Helen Nissenbaum**, Professor at Cornell Tech and in the Information Science Department, Cornell University. |
| 16:30 – 16.45 | BREAK |
| 16.45 – 17.30 | Short Presentations by Invited Researchers: |
| 16:45 – 17:00 | Nina Klimburg-Witjes, Dep. of Science and Technology Studies, University of Vienna: **"Hacking Humans? Social engineering and the construction of the 'deficient user' in cyber security discourses"** |
| 17:00 – 17:15 | Andreas Nautsch, Postdoctoral research fellow, EURECOM: **"How to ask without speech? On quantifying zero-evidence speech"** |
| 17:15 – 17:30 | Liina Kamm, Cybernetica (Estonia): **"Secondary use of registry data for research and decision-making"** |
| 17.30-18.00 | Panel Discussion<br>**Discussant: Michael Fischer**, Professor of Anthropology and Science and Technology Studies, MIT.<br>**Panelists: Prof. Helen Nisenbaum, Nina Klimburg-Witjes, Andreas Nautsch and Liina Kamm** |
| 18:00 - 18.15 | BREAK |
| 18.15 – 19.15 | Roundtable: Towards an agenda for the Cryptic Commons<br>With **Susan Landau**, Professor of Cyber Security and Policy, The Fletcher School and the School of Engineering, Tufts University, **Helen Nissenbaum, Ross Anderson, Rafael Wisniewski, Mads Græsbøll Christensen and Astrid Oberborbeck Andersen**<br>Discussion led by: **Prof. Michael Fischer** |
| 19.15-19.30 | Closing words and end of workshop: Mads Græsbøll Christensen, Professor, Aalborg University |

CRYPTIC COMMONS

An online research workshop on
human/society/cryptography interfaces

May 20-21, 2021

# Abstracts:

## Session 1: Historical layer: Versions of Crypto Dreams Across Time

## Keynote: Ross Anderson: "Utopia Redux: Forty years of crypto dreams"

*Presentations:*

### Sarah Scheffler, PhD candidate, Boston University: "A cryptographic view of "foregone conclusions" in compelled self-incrimination"

*Abstract*: The information security community has devoted substantial effort to the design, development, and universal deployment of strong encryption schemes that withstand search and seizure by computationally-powerful nation-state adversaries. In response, governments are increasingly turning to a different tactic: issuing subpoenas that compel people to decrypt devices themselves, under the penalty of contempt of court if they do not comply. Compelled decryption subpoenas sidestep questions around government search powers that have dominated the Crypto Wars and instead touch upon a different (and still unsettled) area of the law: how encryption relates to a person's right to silence and against self-incrimination.

In this work, we provide a rigorous, composable definition of a critical piece of the law that determines whether cryptosystems are vulnerable to government compelled disclosure in the United States. We justify our definition by showing that it is consistent with prior court cases. Under our definition, decryption is generally not compellable. However, we show that many techniques that bolster security overall can leave one more vulnerable to compelled disclosure. We hope this work will influence the design of future cryptographic primitives and contribute toward the legal debates over the constitutionality of compelled decryption.

### Diego Aranha, Aarhus University: "Quick update on the Brazilian Crypto Wars"

*Abstract:* In this presentation, the history of the crypto wars in Brazil is recapped, from Snowden to the nationwide blocking of WhatsApp that formally started it all.
Then I will briefly describe how the matter escalated to the Supreme Court and summarize two of the votes already cast by judges in favor of strong cryptography.

### Rodrigo Ochigame, PhD candidate, MIT: "Parasemiotic Synthesis"

*Abstract:* *A draft on 4 pages has been sent, which he asks to not circulate*

## Session 2: Mathematical Layer: Computing the mathematical and the Social Edges

### Keynote: H. Vincent Poor, Princeton University: “Machine Learning at the Wireless Edge”

*Abstract:* Wireless networks can be used as platforms for machine learning, taking advantage of the fact that data is often collected at the edges of the network, and also mitigating the latency and privacy concerns that backhauling data to the cloud would entail. This talk will present an overview of some results on distributed learning at the edges of wireless networks, in which machine learning algorithms interact with the physical limitations of the wireless medium. A particular focus of the talk will be on federated learning, in which end-user devices interact with edge devices such as access points to implement joint learning algorithms, and for which spectrum scheduling is a key issue. Despite the fact that data is maintained at the network edge, privacy is still of concern in such settings, and some recent approaches to privacy protection in this setting will also be discussed. Other aspects of distributed learning will also be discussed, as time permits.

*Bio:* H. Vincent Poor is the Michael Henry Strater University Professor at Princeton University, where his interests include information theory, machine learning and network science, and their applications in wireless networks, energy systems, and related areas. He is a member of U.S. National Academy of Engineering and U.S. National Academy of Sciences, and also a foreign member of the Chinese Academy of Sciences, the Royal Society and other national and international academies. Recent recognition of his work includes the 2017 IEEE Alexander Graham Bell Medal, and honorary doctorates and professorships from a number of universities in Asia, Europe and North America, including a D.Tech. honoris causa from Aalborg University.

*Presentations:*

### Manuel Sabin, UC Berkeley: “Power and Participatory Hurdles: Some Preemptive Points of Caution for Participatory Approaches to Machine Learning”

*Abstract:* In this position paper we consider some preemptive points of caution to consider as the field of Machine Learning (ML) looks to incorporate participatory approaches. While moving to incorporate the voices of communities that are most affected by the ML being developed and centering conversations on how ML redistributes power in society is crucial, we aim to take a closer look at how we might define “participation” and “power” and the consequences of different definitions.

Arguing dangerous consequences for possible definitions, we believe that acknowledging and incorporating these concerns into this nascent effort is crucial to avoiding inadvertently further entrenching systems of discrimination and oppression.

### Jaron Gundersen, Aalborg University: “Security with an incomplete communication graph”

Abstract: In multiparty computation, protocols are often proven secure using the real/ideal world paradigm. The idea in these proofs is that we compare what an adversary can do in an ideal world with what harm an adversary can do in the real world. If an adversary cannot do any more harm in the real world than in the ideal world, we say that the protocol is secure. We have some difficulties using this proof technique in a setup where the communication graph is not fully connected, meaning that we do not have a direct communication channel between every pair of parties. In this talk I will give some examples and illustrate some of the challenges we have when we try to prove protocols secure in this setup. From these examples I hope to challenge the definition of what the ideal world should be in a situation where we do not have a fully connected graph.

### Adrienne Mannov & Astrid Oberborbeck Andersen: From Trust to Care: A Speculative Ethics of the Actual in Cryptographic Worlds

*Abstract*: As ethnographers pursuing the social production of cryptographic logics and tools, we were presented with the notion of cryptographic trust early on. It took us some time to understand that when the cryptographers and co-researchers with whom we were working referred to trust, what they were actually referring to, was mathematical proof. If a cryptographic protocol could be shown to be either perfectly secure or computationally secure [need to check these terms], then it was a protocol that could be trusted. But in the social sciences, the humanities and philosophy, trust is a quite a different animal. The central paradigm for investigating trust, whether this refers to trust in individuals, groups, institutions, governments, science, and oneself, is that it is fundamentally an interpersonal phenomenon[1]. Ethnographers Broch-Due and Ystanes define trust as ‘a disposition, a powerful affect, a stance towards the world expressed in a confident reaching out to others. It is a social orientation towards the future nurtured by the gradual accumulation of positive experience and sometimes revealed in a leap of faith’ (2016: 1). A leap of faith is radically different from mathematical proof, so how do we connect the two? And should we? In this presentation, we take a critical stance to trust as the gold standard of cryptographic security and privacy. We argue that trust requires the vulnerable to make a “leap of faith”, rather than require the powerful to provide care. Pursuing the design relationship between the cryptographic ideal, the cryptographic real and the ethnographic actual, we posit a speculative ethics of the actual that connects the three. An ideal standard is useful and a real model may serve to test hypotheses, but they must be tethered to the actual of specific lived experiences to embed an ethics of care in cryptographic protocols.

## Session 3: Social Layer: iterations of the Social Along the Data Food Chain

## Keynote: Helen Nissenbaum: “Contextual Integrity Up and Down the Data Food Chain”

*Presentations:*

### Nina Klimburg-Witjes, Dep. of Science and Technology Studies, University of Vienna: “Hacking Humans? Social engineering and the construction of the “deficient user” in cyber security discourses”

*Abstract:* Social engineering (SE) in cyber security refers to the art of manipulating people to reveal sensitive information like passwords or personal data that can be used to gain unauthorized access to a computer system for any kind of cybercrime. More than two-thirds of all hacking attacks use SE, which leaves cyber security professionals in both companies and government organizations struggling to develop effective counter-measures. One of the reasons why hackers increasingly attend to the social layer of cyberspace is that formerly mainly technical hacks have led to even more elaborated security measures, thus co-producing new forms of hacking practices and knowledge. As a response, SE exploits what is understood as the user’s vulnerabilities, that is, curiosity, greed, or ignorance as a gateway into the technical infrastructures.

The paper explores how SE professionals – hackers, social engineering experts, and cyber security companies – construct a deficient user, who is often referred to as the weakest link in IT security systems. From a combined perspective of science and technology studies and critical security studies, it examines SE as a discourse arena in which experts co-produce sociotechnical deficits with their proposed solutions. Drawing on expert interviews and conference ethnography at two cyber security conferences (DEFCON and Black Hat), the analysis deals with the interplay between users in organizations, IT departments, and the larger SE expert discourse. As will be shown, digitalization has eroded the boundaries between the work-sphere and personal life as part of a neoliberal work regime. This leads to novel ways in which individual responsibility and deficiency is constructed vis-à-vis collective security, as firms and policy makers have addressed the increasing uncertainties by pathologizing the employee rather than calling for a larger socio-political response.

### Andreas Nautsch, Postdoctoral research fellow, EURECOM: “How to ask without speech? On quantifying zero-evidence speech”

*Abstract:* Speech is means to human communication, interchange, and development of each individual. Information is sensitive for there is speech and language; privacy is intimately linked to speech and contexts. Speech technology offers a host of applications from recognition of what was said (speech-to-text) to who spoke (voice biometrics). An essential to privacy preservation is to prohibit (or extensively limit) function creeps, such as the use of voice biometrics for speech data captured in speech-to-text applications when undesired. To modify acoustic speech data accordingly is the goal of the 2020 VoicePrivacy challenge. Within the VoicePrivacy setting, a quantification method for Zero-Evidence Biometric Recognition Assessment (ZEBRA) is proposed and presented in this talk. The approach is motivated from Shannon's perfect secrecy and the European Network of Forensic Science's (ENFSI) guideline for evaluative reporting in forensic sciences.

Liina Kamm, Cybernetica (Estonia): “Secondary use of registry data for research and decision making”

*Abstract:* In recent years, the idea of using machine learning to facilitate decision making and automate processes has excited both researchers and policymakers. For example, in Estonia there is a ML model that processes satellite photos to help government officials make sure that certain ecologically important areas are kept in the required state. The officials get an ordered list of where they should be looking and avoid having to drive to all those areas to check them out in person.

Now imagine, if we could use registry data and fire incident data to predict or prevent housefires.  In the last year, we have been working towards this in Estonia. However, we have hit an expected barrier between research and actual decision making: while the laws allow us to use registry data for research purposes (to find trends, train our model), the secondary use of these data is not allowed for decision making as this would constitute mass profiling, which is restricted by the General Data Protection Regulation (GDPR). We could use the model if we had an approval from the individuals, however the individuals, whom this would most benefit, are unlikely to find this issue and give the approval. The talk will focus on our key learnings from this project, including how privacy-preserving technologies cannot provide a complete solution to every data privacy problem.