STS Encounters

Accessibility statement

This is an accessibility statement for the journal: Encounters.

Conformance status

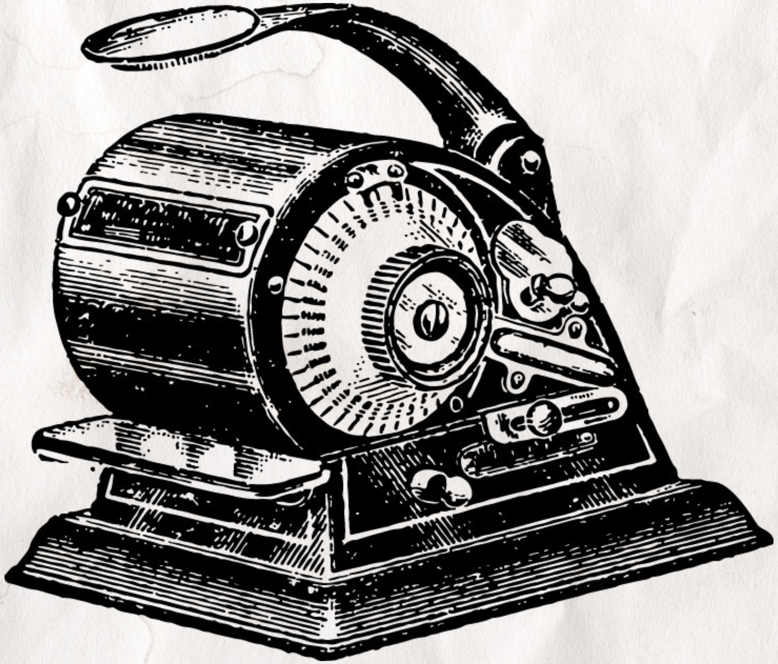
The Web Content Accessibility Guidelines (WCAG) defines requirements for designers and developers to improve accessibility for people with disabilities. It defines three levels of conformance: Level A, Level AA, and Level AAA. This statement is relevant for volume 10, number 5, 2018 through volume 12, number 1, 2021. Encounters is partially conformant with WCAG 2.1 level AA. Partially conformant means that some parts of the content do not fully conform to the accessibility standard. Despite our best efforts to ensure accessibility, footnotes and graphs may not be accessible for screen readers at this point in time.

Feedback

We welcome your feedback on the accessibility of the journal. Please let us know if you encounter accessibility barriers. You can reach us at:

E-mail: imvko@cc.au.dk
Address: STS Center, Helsingforsgade 14, 8200 Aarhus N

ENGAGING THE DATA MOMENT



Special issue
Volume 11• Number 1 • 2020

STS Encounters

SPECIAL ISSUE

Volume 11• Number 1 • 2020

Cryptic Commonalities
Working Athwart Cryptography, Mathematics and Anthropology

Adrienne Mannov
Department of Culture & Learning, Aalborg University, Denmark

Astrid Oberborbeck Andersen
Department of Culture & Learning, Aalborg University, Denmark

Maja Hojer Bruun
Danish School of Education (DPU), Aarhus University, Denmark

DASTS is the primary academic association for STS in Denmark. Its purpose is to develop the quality and breadth of STS research within Denmark, while generating and developing national and international collaboration.

Abstract

Based on ongoing interdisciplinary research about advances in a cryptographic technique called Secure Multiparty Computation (MPC), this article explores how research commonalities are carved out among mathematicians, engineers and anthropologists. STS scholars and anthropologists are increasingly engaged in research about and with data scientists and engineers, particularly as this relates to discrimination, surveillance and rights. Cryptography––a sub-genre of mathematics and often-invisible infrastructure enabling secure digital communication––has received less attention. The article argues that the ubiquity of digital computing in our lives necessitates the creation of socio-mathematical vocabularies. Such vocabularies have the potential to lead to new situated data security practices based on local perceptions of rights and protection. STS scholars and anthropologists are uniquely situated to do this work. The article follows three anthropologists in their endeavors to find "cryptic commonalities" by "tacking back and forth" (Cf. Helmreich 2009) between mathematicians', engineers' and their own scientific vocabularies. Despite these attempts, however, the parties often "talk past each other". Instead of shying away from the awkwardness that such moments produce, the authors embrace "epistemic disconcertment" (Cf. Verran 2013a), carving out a space in which they can communicate productively with each other. This space does not turn mathematicians into anthropologists or STS scholars into engineers, but it does make space for a shared scientific "pidgin" that enables collaboration (Cf. Galison 2010). With this pidgin, the authors walk the reader through the logics of MPC, and specifically, a cryptographic technique called "Shamir Secret Sharing" (Shamir 1979). In doing so, we join emerging voices in the crypto-community in an effort to develop cryptographic techniques for social good. This requires not just an understanding of the math, but also the social worlds impacted by these techniques.

Keywords: interdisciplinarity, cryptography, socio-mathematical vocabulary, data security, data rights

> Nobody really understood what the [mathematical] function was anyway. The panel discussion afterwards (…) really ended up being about citizens' data security and not about cryptography anyway. Leif[1] said afterwards that this always happens: "People don't get it, and so they talk about what they do get."

This field note excerpt is one of the author's reflections on a research presentation and panel discussion at the People's Political Festival – called Folkemødet in Danish – in June 2018. The authors of this paper are part of a three-year research project funded by a Danish university for the explicit purpose of fostering research relationships across disciplines. The university had chosen to send our research project on cryptography to the festival, showcasing it as a cutting-edge, interdisciplinary project at the festival's "Tech Tent".

The research team consists of engineers, mathematicians, and anthropologists. Together, we are working on the further development of a cryptographic technique called "Secure Multiparty Computation" (MPC). MPC securely computes some function of secret information in a decentralized network with multiple actors. More specifically, our team was working with a scheme called "Shamir's Secret Sharing", which does not cover or hide data, as is the case with traditional cryptography. Instead, it fragments data in such a way that it is nearly impossible to infer the mathematical relation between the fragment and its original data. Our presentation and panel discussion at Folkemødet, noted above, were structured around an app that the team developed to demonstrate how secret sharing works.

As we began the project in 2018, we were regularly told that the mathematics of MPC were somehow inaccessible for those outside high-level mathematics, because, as Leif, a mathematician, noted, "people don't get it." Although Leif's comment referred to our panel discussion at Folkemødet, our experiences in the research group made

[1] All informants' names are pseudonyms, and identifying settings and characteristics have been blurred to protect their identities.

clear that it was also relevant to our collaboration. Put simply, could the authors of this paper "get" cryptography enough to work meaningfully with our colleagues? And did they need to "get" us in order to generate something together? What might "getting it" mean in practice? This article is about our research team's attempts to carve out a new and shared conceptual and practice-able space in which to understand the socio-technical relationship between the mathematical and social work that MPC can do.

In this article, we describe and analyze two kinds of knowledge work, both of which tap into the question of "getting" cryptography, technically and socially. First is the kind of labor that goes into interdisciplinary collaborations: the construction of a common problem where collaboration across anthropology, mathematics and engineering can take place. Second is the work of generating a presentation of MPC for a lay audience at a specific event: Folkemødet. We draw on Stefan Helmreich's (2009) notion of working athwart theory to describe and conceptualize the crafting of a common problem and the construction of a shared itinerary towards 'cryptic commonalities': spaces in which collaboration can happen. The team's researchers belong to different academic communities and disciplines – broadly described as mathematics, engineering and anthropology – and each researcher "tacks back and forth" (ibid 2009:24) between their own discipline and the common project. We show how these athwart movements, which are simultaneously methodological, epistemological and ontological, contribute to the construction of a socio-mathematical vocabulary. This enables commonalities and disconnects between the team's disciplines––centered around MPC––to stand out, rendering them legible, relevant and generative for the research group (and potentially broader publics). We argue that such socio-mathematical vocabularies are necessary in order to enable new data security practices to emerge, situated in specific social settings and based on local perceptions of rights and protection. STS and anthropology have much to offer in the construction of such vocabularies. The article is thus a call for scholars within STS and anthropology to take the work of cryptographers seriously, as sites where social worlds are engaged and created. Specifically, in this historical "data moment", when secure digital communication rests on an invisible cryptographic infrastructure, it is crucial that we (STS and anthropology scholars) engage ourselves in the making of cryptic commonalities.

In what follows, we situate the field of cryptography in relation to other STS and anthropological engagements with data science, and point towards the productive openings that exist for collaborations with colleagues from mathematics and engineering. Thereafter, we address in more detail the epistemological investments involved in establishing a common vocabulary across different forms of knowing (Verran 2013a; 2013b; 2014). Armed with these perspectives, we offer a kind of itinerary of understanding that has evolved over two years of (ongoing) research. We invite the reader to move athwart with us, beginning with the story of MPC and our struggle to "burrow" (Verran 2013a:156) a path to a common language with our research colleagues. With this, we begin to imagine shared research outcomes by working to identify what one of our co-researchers calls the "ontology of the damn problems". After this, we tack back to Folkemødet, and to three examples of how we and our co-researchers moved athwart towards a shared language (Cf. Galison 2010) through the creation of a Secret Sharing app and various modes of explanation (supported by images of an e-mail, a screenshot, and a piece of explanatory code). Old questions about math and ontology remain, but despite this tension, we close with a call to join forces through a shared language that is both possible and necessary. In our pursuit of cryptic commonalities, it becomes possible for us ––STS scholars, anthropologists and cryptographers–– to imagine how local perceptions of rights and protection in specific social settings may be included for the purpose of promoting equitable computational worlds in this data moment.

Where Cryptography Fits In

STS and anthropological engagement with mathematics and mathematicians is not a large field. In addition to Verran's work (to which we turn shortly), we note Maurer's work on statistics and finance (2002), Miyazaki's scholarship on arbitrage and arbitrageurs (2013), and Engelke's links between Christianity, Number and the work of philosopher Alain Badiou (2010). These contributions situate an interest in mathematics as socially relevant for practices of calculation, financialization and faith. Our study of cryptography adds to this interest in mathematics as socially relevant for practices of security and privacy, particularly since the Internet revolution (Bruun et al. 2020). There are also important critical histories of the use of mathematics in modernity, such as Deringer (2018), that reference the role mathematics has played in notions of quantitative certainty, prediction, risk mitigation and industrialization.

Probability, prediction, statistics, optimization and other mathematical tools are key to the booming field of data science and the growing ubiquity of AI technologies and machine learning methods (Dourish & Bell 2011; Mackenzie 2017). These technologies have caught the attention of venture capitalists, technologists and social scientists alike because they represent a watershed moment of change, both in business models and products, but also in social impact and scale. Here, scale refers to the process of datafication and the enormous amounts of digital data that are generated and required for fine-grained machine learning predictions and advanced analytical algorithms (Alpaydin 2016; Zuboff 2019). The way personal data is being linked to unprecedented numbers of people poses new questions about ethics (Zuboff 2015), law (Richards & Hartzog 2019) and rights (Irani et al., 2016; Taylor, 2017), amongst other things.

The central role that algorithms are now playing in automated decision-making, and the issues of bias and discrimination, in particular, to which they have given rise, have inspired interest among STS scholars and anthropologists in the critical study of algorithms: work examining the everyday life and sociality of the algorithmic present (boyd & Crawford (2012), Dourish (2016), Fisch (2013), Lowrie (2018), Mackenzie (2015), and Seaver (2018)). As Poul Dourish writes, "an awareness has developed that algorithms, somehow mysterious and inevitable, are contributing to the shape of our lives in ways both big and small" (2016:1). The ways these technologies "shape our lives" have inspired a steady stream of erudite STS and anthropological analyses of AI and discrimination, including Barocas & boyd (2017), Barabas (2019), Dourish & Bell (2011), Gray & Suri (2019), Irani et al. (2016), Ochigame (2019), and Selbst et al. (2019), to name just a few.

Cryptographers develop technical tools that have the potential to protect data privacy and offset some of the negative ways in which datafication can lead to mass surveillance. New cryptographic techniques can prevent abuse of data and enable data analysis without revealing that data's content to anyone. Thus, cryptography has always *also* been deeply political, and particualr historical events, such as the breaking of the German Enigma code during World War II and the Cypherpunk movement in the 1980s and 1990s, have played out this political significance. STS scholars and anthropologists have yet to wade into this territory[2], but some cryptographers have. At a key conference in 2015 for the International Association for Cryptologic Research, Phil Rogaway gave a groundbreaking talk[3] entitled "The moral character of cryptographic work" (2015). Normally, each year's distinguished fellow gives a technical talk, but Rogaway had something else on his mind. His abstract reads:

> Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently political tool, and it confers on the field an intrinsically *moral* dimension. The Snowden revelations motivate

[2] Dalsgaard and Gad (2018) address questions of cryptographic techniques in their ethnographic research on e-voting; not as the main object of study but as part of the socio-technical constellation of the digitalization of elections.

[3] The IACR is the flagship organization for cryptographers.

> a reassessment of the political and moral positioning of cryptography. They lead one to ask if our inability to effectively address mass surveillance constitutes a failure of our field. I believe that it does. I call for a community-wide effort to develop more effective means to resist mass surveillance. I plead for a reinvention of our disciplinary culture to attend not only to puzzles and math, but, also, to the societal implications of our work.

From this perspective, cryptography is not "just" math, but a culture that can attend to "moral" work. Rogaway's talk made big waves in the "crypto-community" and although others have not made such prominent pronouncements, they have addressed the ways in which cryptographic work can tackle issues of privacy, data security, surveillance (e.g. Diffie & Landau 2007; Narayanan 2013) and discrimination (e.g. Nissenbaum 2010; Schlesinger et al. 2018). This work signals an opening towards addressing social, political and moral issues connected to cryptography. As we have argued elsewhere (Bruun et al. 2020), cryptography can have a powerful impact on the socio-technical fields in which it is produced, imagined and deployed. As scholars at the intersection of anthropology and STS, we join this critical dialogue around cryptography as a socio-technical constellation, to further develop cryptography for social good. We turn now to the concrete collaboration in which our dialogue with cryptography, and its social interweaving, began.

Moving Athwart Forms of Knowing

Our cryptographic itinerary began in 2017, when we were approached by Jason, a mathematician and control and systems engineer who was drafting a proposal for a research project on Secure Multiparty Computation. In order to qualify for the solicited grant, the team needed to be interdisciplinary and consist of researchers from different faculties: technical sciences, natural sciences and––preferably also––human and social sciences. Jason explained that as engineers, they were experts in developing new systems and technologies that function efficiently in themselves, but the humans that use the systems somehow never behave according to the design. How, he asked, could humans be convinced to accept new smart technologies? And how could the technologies be designed in such a way that humans would not compromise their functionality?

At the outset, Jason did not know how anthropologists work; how we pose questions to methodologically and conceptually engage with the world. We, in turn, knew nothing about Secure Multiparty Computation, cryptography or data-security in cyber-physical systems, the focus of the project. We began by formulating research questions, work packages and tasks that we all could foresee as meaningful to the common project and realistic to accomplish. One of the methodological challenges that attracted us was the fact that the technologies developed by the team – MPC and cyber-physical systems––had only been applied in social worlds outside of university math labs to a very limited extent[4.]. Thus, our empirical fieldwork would take place among developers (cryptographers) and in settings where such technologies could be implemented in the future. The lack of an empirical and concrete site (field) in which to study the technology in *practice*––called "use-case" in engineering (Barros-Justo et al. 2019)––turned out to be a challenge to establishing a common problem. It meant that we had to create these settings through various experimental formats, such as the Secret Sharing app that we describe below. It also meant that much of our ethnographic material is generated in interaction with and about mathematical theory[5].

[4] Two exceptions are: "Secure Multiparty Computation Goes Live" (Bogetoft et al., 2008), a technical paper on a sugar beet auction and "Accessible Privacy-Preserving Web-Based Data Analysis" (Lapets et al., 2018), a technical paper on the gender pay gap in Boston.

[5] We are quick to add that although "interaction with and about mathematical theory" did not lead us to sites in which we could study MPC in everyday life, it did generate fruitful paths for exploration, including the development of both the Secret Sharing app we describe in this article and a VR prototype, and interacting with researchers at workshops and conferences. These paths deserve to be unpacked in detail, but are beyond the scope of this article.

Cryptography is a highly specialized discipline, and so it is quite difficult for those *not* trained in this field to understand and use the mathematical operations that cryptographically secure data. Echoing Kuhn's paradigms, cryptography could be portrayed by social scientists as "a world apart" (Latour and Woolgar 1986:17), with "news of another world" (Traweek 1992:2) couched in very different knowledge traditions and logics (Verran, 2013a). Even after two years of collaboration, our search for commonalities remain cryptic and are under continuous construction, through concrete encounters that take place across disparate and incommensurable forms of knowing (Verran 2013a), shaped by differing notions of scientific validity, proof, disciplinary belonging and specialization of labor (Galison 2010).

First, we have found it helpful to consider what kind of intellectual space our collaboration occupies. Philosopher of science Peter Galison theorizes interdisciplinary collaboration as a "trading zone" in which scientists from different disciplines can find each other in "common––but restricted––interlanguages" (ibid 2010:51) of "out-talk scientific pidgin". Pidgin (a linguistic term) is stripped of the nuances and depth of the original language, but it is by no means a "lesser" version of it (ibid 2010:47–48); it generates agreement in a delimited space, "where coordination is good enough" (ibid 2010:37). Noting that "science is forever in flux", Galison's examples range from collaborative work between theoretical physicists and radio engineers during WWII to the stabilization of interlanguages into new disciplines, such as nanoscience (2010:33–34).

Secondly, whereas Galison helps us conceptualize interdisciplinarity, STS scholar Helen Verran offers insights into how to qualify the practices and concrete encounters in which different knowledge systems meet. The knowledge encounters that Verran describes and theorizes are postcolonial, situated between modern science and indigenous knowledge traditions: looking at traditional forms of land management through fires in Australia (2013a), or the ontological status of numbers in Nigeria (2014). Although the knowledge encounter we describe takes place at a Scandinavian university, we can learn from the sensitivities and attitudes that Verran develops. One suggestion is to embrace "epistemic disconcertment" (Verran, 2013a), a term that describes and qualifies the moment in which persons with divergent ways of knowing are confronted with a radically different knowledge claim. Crucial in "doing difference together in good faith" is to recognize the difference, and not try to explain it away or deny its truth value (2013b:144–45). In spite of this divide, Verran's perspectives have helped us to identify the quality of our interactions with our co-researchers.

And thirdly, Helmreich offers techniques for navigating in this epistemically disconcerting intellectual space. He explains that working athwart theory "asks for (...) an empirical itinerary of association and relations…", rather than direct representation of comparisons in kind (2009:24). We recognize that establishing cryptic commonalities will not turn mathematicians into anthropologists, or vice versa. But by tacking back and forth, spaces for new understandings are carved out in an ongoing, albeit productively "thin" (Galison 2010:44), and cumulative fashion.

The story of Secure Multiparty Computation – and our history with it

Formally, Secure Multiparty Computation (MPC) belongs to the field of cryptography. Standard cryptography "hides" data (called "plaintext") by masking it, or covering it with a kind of code (called "cyphertext") that can only be opened with a key. The whole "secret" is thus visible once the key is used. MPC is different. The particular MPC method that we used in the Folkemøde app is called "secret sharing". In 1979, cryptographer Adi Shamir presented the idea of fragmenting data into smaller pieces called "shares" and doing computations on them in a network of participants. This is called Shamir Secret Sharing

Shamir, 1979)[6]. This scheme does not cover or hide the whole secret. It fragments it mathematically so that it is nearly impossible to infer the mathematical relation between the fragment and secret. The whole secret is never submitted to any party (Lapets et al. 2016:5). The techniques informing MPC have existed for decades (Lapets et al. 2018:2), but they have only been deployed for practical use a handful of times since the early 2000s (see note 3). For example, if we wanted to know the average salary for researchers at our university department, we could compute it using MPC. This would give us an analysis that was useful––on average my colleagues earn more than me and I need to ask for a raise––but would protect information about an individual's salary. This is possible because MPC fragments information (i.e. an individual's salary) in such a way, that it is not possible to infer the whole (the salary) from the part because the relationship between whole and part is not obvious. For example, MPC uses techniques that enable a fragment to appear larger than the whole (see footnote 9).

"I think we're talking past each other"

In order to understand the story of MPC, the authors consulted scientific papers, textbooks, Wikipedia pages and countless YouTube videos[7]. In addition, informal interviews and conversations with and participant observation among cryptographers have provided invaluable insights that have found their way into the story we tell here. For example, in judging whether a particular cryptographic scheme is secure, cryptographers often talk about the relationship between what they call the "ideal world" and the "real world", a distinction that is central to the notion of a "trusted third party" (TTP). A TTP receives encrypted messages, decrypts them and generates an analysis. The TTP must retain trust by not disclosing or using the decrypted messages for its own purposes (Tilborg and Jajodia, 2011). But there is growing concern that TTPs may in fact not be trustworthy (See also Bruun et al. 2020). This was the topic of an informal, and initially confused conversation, while waiting for coffee at a cryptography conference (fieldwork for the authors of this paper) with cryptographer, Abe.

> Abe told us [co-author] that the TTP was an example of the "ideal world". She countered: Some actors are not necessarily happy with a TTP, because they're asking to use the data for their own internal analytics. This was not "ideal". Abe insisted that the TTP was part of the "ideal world", but admitted that the term was perhaps abused. On this point, Abe and our co-author agreed. Approaching the debate from another angle, our co-author offered an example: She has a message for Abe that she doesn't want the other café guests to hear. This is "real world", she concluded. Abe countered: This is "ideal world".

As they stood in line, our co-author remarked, "I think we're talking past each other". Abe was surprised, but making the miscommunication explicit made it possible to unpack the terms in greater detail. "Real" and "ideal" have specific meanings for cryptographers that did not match our co-author's understandings. We "ascribed utterly different significance" to the terms discussed (Collins et al. 2010:8). For the co-author, "real" was something that she could experience outside of mathematical theory, in the applied, social world. "Ideal" referred to a best-case scenario that could be imagined, but not experienced. The cryptographer's "ideal world", Abe explained, refers to the ideal mathematical trust and security that the *concept* of a TTP provides: the trusted third party is completely trustworthy, not corrupted (does not share secrets with others), cannot be attacked from the outside, and computes a function of the provided secrets accurately. Elaborating on this, Abe explained that the cryptographic understanding of "real world" had to do with measuring schemes against this "ideal" as a

[6] Another major influence in the development of MPC was "Yao's Garbled Circuits" (Yao, 1986).

[7] See for example "RSA encryption made easy": https://www.youtube.com/watch?v=t-5lACDDoQTk; retrieved 5/9/2020.

standard. But in cryptography, neither the “ideal world” nor the “real world” has any connection to what we (authors) might call “actual” practice. Rogaway explains, “Most academic cryptography isn’t really crypto-for-security *or* crypto-for-privacy: it is, one could say, *crypto-for-crypto*––meaning that it doesn’t ostensibly benefit commerce or privacy, and it’s quite speculative if it will ever evolve to do either” (2015:24). Abe’s definitions remained within the *crypto-for-crypto* logic, whereas our co-author was looking to explain these terms in the context of some practical benefit. Letting Abe know that we were not on the same epistemic page reminds us of Verran’s “burrowing device” that “digs” into epistemic disconcertment “by provoking it further” (2013a:156). It was awkward to name the miscommunication, because it felt like a provocation; but doing so bore fruit.

Part of the problem in communicating with cryptographers like Abe is that explanations are usually based in abstract, theoretical concepts. But references to “ideal” and “real” worlds are seductive because they are recognizable as everyday words used outside of mathematics and thereby suggest a conceptual link between the theoretical and the “actual” social world as it is experienced in everyday life. Cryptographers’ *theoretical* schemes exist, of course, in the actual world, in the form of papers, presentations and notes on a chalkboard, but the scenarios they imagine them to address do not. In a rare exchange that made these epistemic tensions explicit, one mathematician with whom we are working explained that “all these normative terms [are] being used that really don't map to the technical uses of them”. To take another example, cryptographic schemes are populated with “social actors” called “Alice, Bob, Eve, or Mallory”, and these actors have social characteristics. They can be malicious (Mallory); they can be curious (Eve, who eavesdrops); they can “cheat”, be “corrupted”, or be “motivated” to share secret information with outsiders. These figures, however, are purely theoretical in the sense that they are imagined by cryptographers in the form of abstract mathematical assumptions about generalized archetypal characters in the actual world. They have no empirical basis other than the mathematical proofs that show how well a given scheme functions. But following Abe’s taxonomy, these characters correspond to the “real” as they represent imagined threats, whereas in an ideal setting, they would not exist at all. Still, cryptographic tools were originally developed for state-centric and military purposes, and later, for civilians to protect what they see as the human right to freedom of opinion and expression (Hellegren, 2017). So, there is a (hi)story linking the mathematics of cryptography and its social relevance in actual practice. But the social practice of the development of cryptographic primitives (theoretical tools) in the academic worlds in which we move is usually driven by mathematical puzzles, not societal problems.

Making “talking past each other” explicit was one way of burrowing towards a shared understanding of the epistemological differences between crypto-for-crypto and crypto in the “actual” world. Another technique was to move closer to the epistemological and social practice of mathematical theory among our colleagues. We now turn to such moments.

Moving towards a common problem: where is the ontology?

Nate is an engineer with our project, and in our conversation with him about mathematics, he challenged the idea that mathematics is based on pure theory. He brought the researcher’s ideation process to the forefront:

> And that’s always the problem with mathematics; it’s taught in this deductive manner. And that’s basically never the way mathematics comes about. It starts with somebody in the shower who thinks he’s discovered the theory of everything. It really starts with having some very concrete ideas. You look at some instances that you don’t understand (...) and then you discover, “Hey, here

> are some related problems” (…) And then you realize, “Hey, wait a minute, that must mean” this, this and this. And then the general theory comes. But when it’s (…) presented, then it’s the general theory that’s there and the other stuff [is presented] as if it came from the general theory.

Nate explained that there is a tendency among his colleagues to accept new theoretical ideas as “intuition”, instead of tracing the ideation process in an explicit way: “The only way we can have a discussion about whether a model is right or wrong is to be explicit about our assumptions. It is typical for a lot of research in our field to be built on intuition, so the assumptions are not made explicit.” By challenging “intuition”, Nate seems to identify the *researcher’s* relationship to the generation of ideas. We recognize Nate’s insistence on tracing the ideation process, which we can relate to our own ethnographic thinking. Nate also looks for inspiration from other disciplines in our project:

> So, if you ask [a mathematician], he’ll say, “This is the problem I’m solving.” (...) This is his area, and this is the way the problem is defined. And the problem we’re looking at is a little bit different, right? But I think it’s interesting to try and transfer some of the things there and see if we can learn something from it (them), you know?

Nate addresses the questions of identifying the scientific “problem” and of how scientists from different disciplines identify and frame problems differently. In doing so, Nate practices what Verran calls “infracritique”, because he recognizes that his colleagues’ scientific knowledge is framed differently from his own (2014:530). By taking these differences seriously, he works athwart theory and looks to be inspired in new ways. According to Verran, recognizing these basic differences through “epistemic disconcertment” is the first step toward “doing difference generatively and in good faith” (Verran 2013a:144). Lest readers think our endeavors were frictionless, it must be said that finding common spaces and “doing difference in good faith” (Verran 2013a:144) were not always possible. Thankfully, Nate was not just curious about his mathematics colleagues, but also about how anthropologists work. He continued:

> So, I was sitting and discussing [this project] with a [friend who is a sociologist] and some colleagues, and [my friend] said, “Well, the first thing you have to do with this, is to establish” - what do you call it? - “an ontology”. And I thought, “Hell yes, that’s what we’re missing in this whole project. We don’t know what the damn problems are! We don’t have the words, we don’t have hierarchies of knowledge and how they relate to each other [and] what problems are relevant to solve.” (…) I have no idea if we’re actually trying to solve totally irrelevant problems. (...) So, I was hoping that was precisely what you guys could help us understand, [to] help us find use-cases.

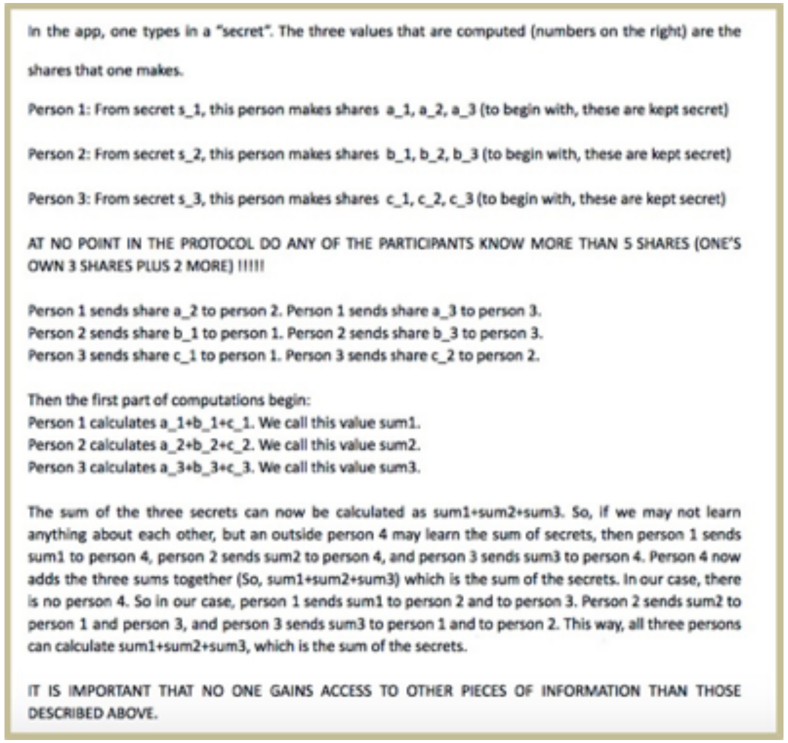
For Nate, identifying relevant problems included issues that were both external to mathematics and identifying “hierarchies of knowledge”, something he refers to as an “ontology”. As we saw in our conversation with Abe, this required continual tacking back and forth (Helmreich 2009:24) between researchers and their respective hierarchies of knowledge: What is ideal, real or actual?

Nate also makes a leap and links the project’s ontology to what he refers to as use-cases. In engineering, use-cases are meant “to elicit, to specify and to validate software requirements of a system in terms of the main actors (external elements that interact with the system) and their goals” (Barros-Justo et al. 2019:1). This echoes Jason’s initial interest in designing technologies in such a way that their functionality would not be compromised by humans. This was not how we imagined our contribution. We needed to find an “actual” social situation in which

MPC could be used to solve a relevant problem, one in which the main actors' problems and solutions were internal and defined relationally (See Salmond, 2017).

At this early point in the project, we knew very little about each other's disciplinary logics. We lacked both a common problem and a common language. As a mathematician, Abe needed neither a use-case nor a social situation in order to proceed. As an engineer, Nate needed a use-case for his science to be relevant. As anthropologists, a use-case can translate into a social world and actual situations, adjacent to mathematics. An opportunity to imagine a use-case together, as engineers and anthropologists, came with an invitation to present our work on MPC at Folkemødet in the summer of 2018. We return therefore to our Folkemøde app and our mathematics colleague, Leif.

Making MPC Legible to Ourselves and to Others



In the app, one types in a "secret". The three values that are computed (numbers on the right) are the shares that one makes.

Person 1: From secret s_1, this person makes shares a_1, a_2, a_3 (to begin with, these are kept secret)

Person 2: From secret s_2, this person makes shares b_1, b_2, b_3 (to begin with, these are kept secret)

Person 3: From secret s_3, this person makes shares c_1, c_2, c_3 (to begin with, these are kept secret)

AT NO POINT IN THE PROTOCOL DO ANY OF THE PARTICIPANTS KNOW MORE THAN 5 SHARES (ONE'S OWN 3 SHARES PLUS 2 MORE) !!!!!

Person 1 sends share a_2 to person 2. Person 1 sends share a_3 to person 3.
Person 2 sends share b_1 to person 1. Person 2 sends share b_3 to person 3.
Person 3 sends share c_1 to person 1. Person 3 sends share c_2 to person 2.

Then the first part of computations begin:
Person 1 calculates a_1+b_1+c_1. We call this value sum1.
Person 2 calculates a_2+b_2+c_2. We call this value sum2.
Person 3 calculates a_3+b_3+c_3. We call this value sum3.

The sum of the three secrets can now be calculated as sum1+sum2+sum3. So, if we may not learn anything about each other, but an outside person 4 may learn the sum of secrets, then person 1 sends sum1 to person 4, person 2 sends sum2 to person 4, and person 3 sends sum3 to person 4. Person 4 now adds the three sums together (So, sum1+sum2+sum3) which is the sum of the secrets. In our case, there is no person 4. So in our case, person 1 sends sum1 to person 2 and to person 3. Person 2 sends sum2 to person 1 and person 3, and person 3 sends sum3 to person 1 and to person 2. This way, all three persons can calculate sum1+sum2+sum3, which is the sum of the secrets.

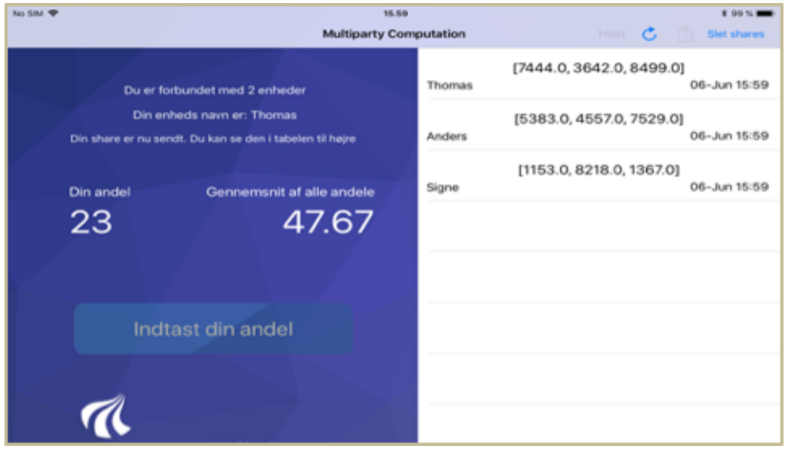
IT IS IMPORTANT THAT NO ONE GAINS ACCESS TO OTHER PIECES OF INFORMATION THAN THOSE DESCRIBED ABOVE.

Figure 1 Translation of the Folkemøde app's MPC function from algorithms to prose.

The Translation above (Figure 1) grew out of the shared idea to develop an app that would demonstrate how it was possible to analyze "secret" information without having access to or disclosing that information. We hoped that demonstrating MPC in an app at Folkemødet would foster an understanding about how it worked and spark public engagement. This required that we burrow deeper into the mathematics, tacking back and forth between modes of knowledge.

Leif, a mathematician with the project, sent us an email explaining (Figure 1) *in words* (and syntax) how MPC functioned in our app. Our interest in the mathematics of MPC was met by some project colleagues with surprise and occasional irritation. “You don’t need to know how the math works,” one would say when we asked for an explanation. Instead of sending us rows of algorithms and formulas, Leif “translated” his mathematical understanding of the MPC function in our app to written words that we all understood. When we refer to commonalities, we are not suggesting that mathematics and anthropological approaches to MPC are the same; there is no “isomorphism of direct representation” (Helmreich 2009:24). Instead, the commonalities work as a kind of “pidgin”. As in Galison’s example about collaborative work between theoretical physicists and radio engineers during WWII, Leif “held back” some details, while choosing to put others “on the table” in order to facilitate collaboration (2010:29). His explanation did not convey the full depth of his discipline, but it sketched an itinerary of understanding that connected us. In this instance, Leif reached out to us, so that working athwart theory became a multidimensional endeavor.

Performing Athwart



Du er forbundet med 2 enheder

Din enheds navn er: Thomas

Din share er nu sendt. Du kan se den i tabelen til højre

Din andel 23

Gennemsnit af alle andele 47.67

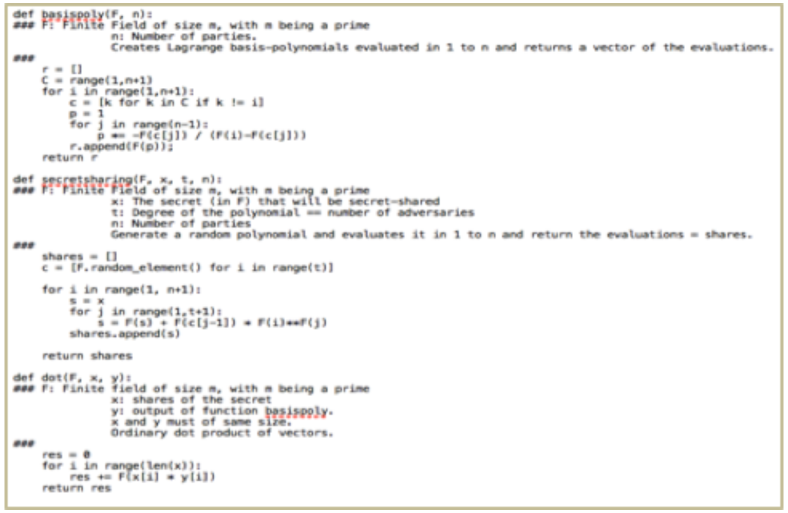
Thomas	[7444.0, 3642.0, 8499.0]	06-Jun 15:59
Anders	[5383.0, 4557.0, 7529.0]	06-Jun 15:59
Signe	[1153.0, 8218.0, 1367.0]	06-Jun 15:59

Figure 2 Screenshot from the Folkemøde app.

Our presentation at Folkemødet began with Leif’s explanation of how MPC could be used to secure citizens’ electricity consumption data in order to optimize the Smart Grid. Thereafter, he introduced our co-author, who presented the app. She explained that it was programmed for several iPads that “carry out secret and secure distributed computations together,” adding that the audience could follow along with the computations by viewing the screens in the tent (see Figure 2). We chose to use “real secrets”, namely the age when participants first fell in love. There was some playfulness involved in this choice. The team hoped that this light-heartedness would engage the audience and spark their interest in the mathematical functions and their integration into the app’s algorithms.

This app screenshot was another version of MPC “pidgin” (Cf. Galison 2010). It did not explain the protocol in prose, but illustrated the ways in which participants’ “secrets” were fragmented into “shares”. Again, it does not represent the full mathematical project. The upper right corner of the screenshot shows three participants in the network, and next to each name, the fragments of the other participants’ secrets. On the left, for the purpose of illustration, one participant’s secret is displayed (“your part, 23”), and next to this, the average (“47.67”). The average is the analysis that MPC provides in this protocol. Only the fragments are circulated in the network. The other participants’ secrets are not circulated or disclosed, nor do they exist in any back-end version of the app. They cannot be inferred by analyzing the fragments. We pursue how this is possible in the next section. The reason we are able to do this is that multiple athwart movements between mathematicians, engineers and anthropologists have created a trading zone that is “good enough” (Galison, 2010, p. 37) to enable a sufficient explanation.

The Insides of Secret Sharing



```
def basispoly(F, n):
### F: Finite Field of size m, with m being a prime
            n: Number of parties.
            Creates Lagrange basis-polynomials evaluated in 1 to n and returns a vector of the evaluations.
###
    r = []
    C = range(1,n+1)
    for i in range(1,n+1):
        c = [k for k in C if k != i]
        p = 1
        for j in range(n-1):
            p *= -F(c[j]) / (F(i)-F(c[j]))
        r.append(F(p));
    return r

def secretsharing(F, x, t, n):
### F: Finite Field of size m, with m being a prime
            x: The secret (in F) that will be secret-shared
            t: Degree of the polynomial == number of adversaries
            n: Number of parties
            Generate a random polynomial and evaluates it in 1 to n and return the evaluations = shares.
###
    shares = []
    c = [F.random_element() for i in range(t)]

    for i in range(1, n+1):
        s = x
        for j in range(1,t+1):
            s = F(s) + F(c[j-1]) * F(i)**F(j)
        shares.append(s)

    return shares

def dot(F, x, y):
### F: Finite field of size m, with m being a prime
            x: shares of the secret
            y: output of function basispoly.
            x and y must of same size.
            Ordinary dot product of vectors.
###
    res = 0
    for i in range(len(x)):
        res += F(x[i] * y[i])
    return res
```

Figure 3 MPC explanatory code written in SageMath, designed for the development of the Folkemøde app.

In the explanatory code displayed in Figure 3, the app's key functions are shown in another kind of pidgin. They are written in a language called SageMath (an open source version of Python). We call it pidgin here because the lines above, written by one of our mathematics colleagues, were meant to be simple enough for the app developer (who is not a mathematician) to understand, but detailed enough to stay true to the mathematical functions it should compute. The three key algorithms are: *basispoly (F, n)* which generates Lagrange polynomials[8] from the secrets in a finite field based on a prime number of potential participants in the network; *secretsharing (F, x, t, n)*, which generates "shares" through modular arithmetic and the polynomials in *basispoly (F, n); and dot (F, x, y)*, which reconstructs the secrets.

In what follows, we examine more closely the insides of the *secretsharing (F, x, t, n)* algorithm at the core of Adi Shamir's 1979 MPC scheme and our app. Taking the onto-epistemic underpinnings of this cryptographic scheme seriously is our own attempt to do difference in good faith (Verran 2013a:144), and, significantly, to work towards a shared "ontology of the damn problems," as Nate put it. In other words, we needed to understand how the algorithm works and so we have attempted to unpack it. Our explicit questions about the "insides" of *secretsharing (F, x, t, n)*, may have seemed to our colleagues like the "stutterings of an idiot" (Stengers in Verran 2013a:156). We asked them for feedback on an earlier version of this article, in order to be sure we had described the mathematical functions and relationships correctly. It was returned full of the red markings of a patient but not very impressed math teacher. But our clumsy attempts bore fruit. This is our rendering:

Shamir Secret Sharing (Shamir 1979) is represented in the second step––*secretsharing (F, x, t, n)*––of the explanatory code displayed in Figure 3. *Secretsharing (F, x, t, n)* distributes *only fragments* (or shares) of secrets within a network of at least three parties. In this sense, its distributive scheme is communal. The shares that *secretsharing (F, x, t, n)* generates are based on the participant's secret information, but the shares are *different each time*, even if the number of participants and their secrets are the same. Returning to Figure 2, if we had run the protocol again with the same secrets and number of participants, the shares would have been different, but the average would have been the same. It is significant to note that the shares are significantly *larger* than the original secret. This is the work that the polynomials from *basispoly (F, n)* and the modular arithmetic[9] in *secretsharing (F, x, t, n)* do in the code.

What might this mean socially? How might this rendering help us

[8] Lagrange polynomials lie beyond the scope of this article, but curious readers may consult: https://www.khanacademy.org/math/multivariable-calculus/applications-of-multivariable-derivatives/constrained-optimization/a/lagrange-multipliers-examples; accessed 7/7/2019

[9] Also referred to as "clock arithmetic": https://www.khanacademy.org/computing/computer- science/cryptography/modarithmetic/a/what-is-modular-arithmetic; accessed 7/7/19.

to “attend to the societal implications of our work” (Rogaway 2015)? For Verran, numbers may be understood as cultural practice (2010): they are *conceptual formations* (2013b:28) that need to be explored and “decomposed”. She explains that decomposing a concept such as “a number (…) involves everting to reveal the concept’s insides” (2018:24), also known as “foundationism” (2014:529). By trying to understand the “insides” of secretsharing, we suggest that the changing and counterintuitive share sizes and the scheme’s communal characteristics are informed by a certain kind of “foundationism” that lends itself not only to mathematical puzzle-solving, but also to an investment in using and protecting data that is both robust and communal. If a cryptographic scheme is socially communal, what might this mean in practice for data rights and social good? We do not know the answer to this question, but without unpacking the cryptographic scheme, we and our co-researchers have no common language with which to ask.

We hope that the reader has learned something about the mathematical logics informing MPC and that this might inspire a curiosity in the social implications of cryptographic schemes. In a sense, our pidgin explanation for a Public Engagement in Science extends to you. Perhaps you would like to join the conversation? Perhaps you remain on the outside, not knowing how to ask (Horst and Michael, 2011). But if we are to take seriously the work of “humanizing algorithmic systems,” then we must at the very least cultivate a curiosity about their inner workings, including those of cryptographic systems like MPC, on their own terms (Lowrie 2018:354).

Emergent Cryptic Commonalities

In this article, we have pursued an itinerary of understanding in which we seek cryptic commonalities with our co-researchers from mathematics and engineering. We began with the questions: Could the authors of this paper “get” cryptography enough to work meaningfully with our colleagues? And did those colleagues need to “get” us in order to generate something together? What might “getting it” mean in practice? We have suggested that “getting it” entailed moving athwart theory, ideally in multiple directions, between anthropology and STS to mathematics, but also between engineering and mathematics, tacking back and forth (Helmreich, 2009). We described how this move into foreign territory could be awkward, particularly when calling attention to miscommunication. But it could also be fruitful if, instead of avoiding epistemic disconcertment, we burrowed further (Verran 2013a:156) and found a shared trading zone. Our colleagues inspired us to consider together how to understand what problems were relevant, even when their ontology was (and is still) not quite determined. Finally, we ventured into ever-deeper layers of understanding, developing a kind of pidgin that enabled us to take MPCs mathematics, its functions and algorithms seriously on their own terms.

Questions remain, of course. We have taken for granted that commonalities may be found, and we have set about generating them, insisting that some form of pidgin translation can facilitate scientific trade across disciplines. For some mathematicians and philosophers, this is foolish. Mathematical physicist and Fellow of the Royal Society (UK) Sir Roger Penrose posited the “math-matter-mind triangle” (Penrose 2007:1029) in which “math arises from the mind, the mind arises out of matter, and that matter can be explained in terms of math” (Hut et al. 2006). The relationships that Penrose’s triangle sets up between math, mind and matter underpins why we think that pursuing cryptic commonalities is both a reasonable and possible endeavor for us to pursue. Nevertheless, some question these relationships; they suggest that math is the origin of everything, implying the “reduction of the world around us, including our minds, to mathematical laws of physics (ibid 2006:2). According to this logic, matter can be reduced to math, and, since the mind is also matter, it too can be reduced to math. This stance does not lend itself to translation (pidgin, or otherwise) trading zones, or burrowing devices that help bridge onto-epistemological confusion. According to anthropologist Matthew Engelke, philosopher Alain Badiou echoes this view: Math is. It resists mediation or representation. “mathematics is ontology” (Badiou in Engleke 2010:815). But cryptographers practiced cryptic commonalities long before we did, fashioning a field that is itself a kind of pidgin. But cryptographers practiced cryptic commonalities long before we did, fashioning a field that is itself a kind of pidgin: a serendipitous construction arising from mathematics, computer science, military strategy, business models, semiotics and much more (Cf. Galison 2010). We add STS and anthropology to this list.

"Cryptic commonalities" is of course a play on words. Our research is ongoing, and Jason has increasingly called upon the anthropologists on his team to explain to outsiders how MPC works. He recently reflected that he struggles to offer a helpful explanation to outsiders because he does not know how and where to begin the translation, in order to choose the appropriate level of information. This means that while he navigates expertly through the hierarchies of his own knowledge, his epistemic tools are somewhat less sharp when he needs to move athwart. In this way, our *common* problem is to further develop cryptography for social good by finding ways to translate these schemes in ways that are socially relevant. But the other way to understand the idea of "cryptic commonalities" is that what and how we are sharing remain *cryptic*.

What we do know is that in this historical moment – characterized by this special issue as a *data moment* – data has gained value in and of itself, leading to the exponential growth of surveillance technologies. For this reason, it is urgent that anthropology, STS, and the social sciences more broadly move in good faith closer to, into, and behind the math driving these technologies. Cryptographer Phil Rogaway called for "a community-wide effort to develop more effective means to resist mass surveillance" (2015). By building cryptic commonalities, we humbly include ourselves in this community. We believe that Rogaway's call requires voices that not only understand the math but also the specific computational social contexts in which it is embedded. Together, this will form a foundation upon which joint social engagement for equitable computational worlds must be built.

Acknowledgements

Many thanks to our co-researchers for their patience and support, to the cryptographers who continue to develop a socio-mathematical pidgin with us, and to the anonymous reviewers for their generous feedback on earlier versions of this article. Research for this article was funded by Aalborg University's strategic research funds.

References

Alpaydin, E. (2016) Machine learning: the new AI, MIT Press essential knowledge series. MIT Press, Cambridge, MA.

Barabas, C. (2019) Beyond Bias: Re-imagining the Terms of “Ethical AI” in Criminal Law. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3377921

Barocas, S., boyd, d. (2017). Engaging the ethics of data science in practice. Communications of the ACM 60, 23–25. https://doi.org/10.1145/3144172

Bogetoft, P., Christensen, D.L., Damgård, I., Geisler, M., Jakobsen, T., Krøigaard, M., Nielsen, J.D., Nielsen, J.B., Nielsen, K., Pagter, J., Schwartzback, M., Toft, T., 2008. Secure Multiparty Computation Goes Live. IACR.

boyd, d. , Crawford, K. (2012). Critical Questions For Big Data: Provocations for a cultural, technological, and scholarly phenomenon. Information, Communication & Society 15:5, 662–679. https://doi.org/10.1080/1369118X.2012.678878

Bruun, M.H., Andersen, A.O., Mannov, A. (2020) Infrastructures of Trust and Distrust. The Politics and Ethics of Emerging Cryptographic Technologies. Anthropology Today 36, 13–17. https://doi.org/10.1111/1467-8322.12562

Dalsgaard, S., Gad, C. (2018) Digital Unbounding of the Polling Booth: Ethnography in Small Places. Ethnos 83:4, 782–799. https://doi.org/10.1080/00141844.2017.1348379

Deringer, W. (2018) Calculated values: finance, politics, and the quantitative age. Harvard University Press, Cambridge, Massachusetts. London, England.

Diffie, W., Landau, S.E. (2007) Privacy on the line: the politics of wiretapping and encryption, Updated and expanded edition. MIT Press, Cambridge, Mass.

Dourish, P. (2016) Algorithms and their others: Algorithmic culture in context. Big Data & Society 3:2. https://doi.org/10.1177/2053951716665128

Dourish, P., Bell, G. (2011) Divining a digital future: mess and mythology in ubiquitous computing. MIT Press, Cambridge, Mass.

Engelke, M. (2010) Number and the Imagination of Global Christianity; or, Mediation and Immediacy in the Work of Alain Badiou. South Atlantic. Quarterly. 109(4), 811–829. https://doi.org/10.1215/00382876-2010-018

Fisch, M. (2013) Tokyo’s Commuter Train Suicides and the Society of Emergence. Cultural Anthropology. Vol. 28:(2), 320–343. https://doi.org/10.1111/cuan.12006

Galison, P. (2010) Trading with the Enemy, in: Gorman, M.E. (Ed.), Trading Zones and International Expertise: Creating New Kinds of Collaboration. The MIT Press, Cambridge, pp. 25–52.

Gray, M.L., Suri, S. (2019) Ghost work: how to stop Silicon Valley from building a new global underclass. Houghton Mifflin Harcourt, Boston.

Hellegren, Z.I. (2017) A history of crypto-discourse: encryption as a site of struggles to define internet freedom. Internet Histories. 1:4, 285–311. https://doi.org/10.1080/24701475.2017.1387466

Helmreich, S. (2009) Alien ocean: anthropological voyages in microbial seas. University of California Press, Berkeley.

Horst, M., Michael, M, (2011). On the Shoulders of Idiots: Re-thinking Science Communication as ‘Event.’ Science as Culture. 20:3, 283–306. https://doi.org/10.1080/09505431.2010.524199

Irani, L., Lustig, C., Pine, K., Nardi, B., Lee, M.K., Nafus, D., Sandvig, C. (2016) Algorithmic Authority: The Ethics, Politics, and Economics of Algorithms that Interpret, Decide, and Manage. CHI'16 Extended Abstracts, May 07-12, 2016, San Jose, CA, USA.

Lapets, A., Jansen, F., Albab, K.D., Issa, R., Qin, L., Varia, M., Bestavros, A. (2018). Accessible Privacy-Preserving Web-Based Data Analysis for Assessing and Addressing Economic Inequalities, in: Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS) - COMPASS ’18. Presented at the the 1st ACM SIGCAS Conference, ACM Press, Menlo Park and San Jose, CA, USA, pp. 1–5. https://doi.org/10.1145/3209811.3212701

Lapets, A., Volgushev, N., Bestavros, A., Jansen, F., Varia, M. (2016) Secure Multi-Party Computation for Analytics Deployed as a Lightweight Web Application. (Technical Report No. BU-CS-TR 2016-008). Computer Science Department, Boston University.

Latour, B., Woolgar, S. (1986) Laboratory life: the construction of scientific facts. Princeton University Press, Princeton, N.J.

Lowrie, I. (2018) Algorithms and Automation: An Introduction. Cultural. Anthropology. 33(3), 349–359. https://doi.org/10.14506/ca33.3.01

Mackenzie, A. (2017) Machine Learners. Archaeology of a Data Practice. The MIT Press, Cambridge, MA.

Mackenzie, A. (2015) The production of prediction: What does machine learning want? European Journal of Cultural Studies. 18(4-5), 429–445. https://doi.org/10.1177/1367549415577384

Maurer, B. (2002) Repressed futures: financial derivatives' theological unconscious. Economy and Society, 31:1, 15–36. https://doi.org/10.1080/03085140120109231

Miyazaki, H. (2013) Arbitraging Japan: dreams of capitalism at the end of finance. University of California Press, Berkeley, CA, USA.

Narayanan, A. (2013) What happened to the crypto dream? IEEE Security and Privacy Magazine. 11 (Part I), 75–76.

Nissenbaum, H.F. (2010) Privacy in context: technology, policy, and the integrity of social life. Stanford Law Books, Stanford, Calif.

Ochigame, R. (2019) The Invention of "Ethical AI" How Big Tech Manipulates Academia to Avoid Regulation. The Intercept. https://theintercept.com/2019/12/20/mit-ethical-ai-artificial-intelligence/

Penrose, R. (2007) The Road to Reality: A Complete Guide to the Laws of the Universe, Nachdr. ed. Vintage Books, London.

Richards, N., Hartzog, W. (2019) The Pathologies of Digital Consent. 96(6) Washington University Law Review. 1461 (2019).

Rogaway, P. (2015). The Moral Character of Cryptographic Work?

Salmond, A. (2017). Uncommon Things. Anthropologica Volume 59, 251–266.

Schlesinger, A., O'Hara, K.P., Taylor, A.S. (2018). Let's Talk About Race: Identity, Chatbots, and AI, in: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18. Presented at the the 2018 CHI Conference, ACM Press, Montreal QC, Canada, pp. 1–14. https://doi.org/10.1145/3173574.3173889

Seaver, N. (2018) What Should an Anthropology of Algorithms Do? Cult. Anthropol. 33, 375–385. https://doi.org/10.14506/ca33.3.04

Selbst, A.D., boyd, d., Friedler, S.A., Venkatasubramanian, S., Vertesi, J. (2019) Fairness and Abstraction in Sociotechnical Systems, in: Proceedings of the Conference on Fairness, Accountability, and Transparency - FAT* '19. Presented at the the Conference, ACM Press, Atlanta, GA, USA, pp. 59–68. https://doi.org/10.1145/3287560.3287598

Shamir, A.(1979) How to Share a Secret. Commun. ACM 22, 612–613.

Taylor, L. (2017) What is data justice? The case for connecting digital rights and freedoms globally. Big Data Soc. 4, 205395171773633. https://doi.org/10.1177/2053951717736335

Tilborg, H.C.A. van, Jajodia, S. (Eds.) (2011) Encyclopedia of cryptography and security, 2nd ed. ed, Springer reference. Springer, New York.

Traweek, S. (1992) Beamtimes and lifetimes: the world of high energy physicists, 1. ed. ed. Harvard Univ. Press, Cambridge, Mass.

Verran, H. (2018) Decomposing numbersRejoinder to Vilaça, Aparecida: "The devil and the hidden life of numbers: Translations and transformations in Amazonia. HAU J. Ethnogr. Theory 8, 23–26. https://doi.org/10.1086/698356

Verran, H. (2014) Working With Those Who Think Otherwise. Common Knowl. 20, 527–539. https://doi.org/10.1215/0961754X-2733075

Verran, H. (2013a) Engagements between disparate knowledge traditions: Toward doing difference generatively and in good faith., in: Green, L. (Ed.), Contested Ecologies: Dialogues in the South on Nature and Knowledge. HSRC Press, Cape Town, pp. 141–161.

Verran, H. (2013b) Numbers Performing Nature in Quantitative Valuing. NatureCulture 23–37.

Verran, H. (2010) Number as an inventive frontier in knowing and working Australia's water resources. Anthropological Theory 10(1-2), 171–178. https://doi.org/10.1177/1463499610365383

Yao, A.C.-C. (1986) "How to generate and exchange secrets" (extended abstract). 27th Annual Symposium on Foundations of Computer Science (sfcs 1986), Toronto, ON, Canada, 1986, pp. 162-167, doi: 10.1109/SFCS.1986.25.

Zuboff, Shoshana, and Karin Schwandt. 2019. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. London, England: Profile Books.

Zuboff, S. (2015) Big other: Surveillance Capitalism and the Prospects of an Information Civilization. Journal of Information Technology. 30(1), 75–89.

Author bios

Adrienne Mannov received her PhD in social anthropology from Copenhagen University, and in 2021, she will join the staff at Aarhus University as assistant professor. Her research interests focus on globalization and material, physical and existential security. Her most recent work addresses the links between civilian security and data encryption.

Astrid Oberborbeck Andersen is associate professor at the Department of Culture and Learning, Aalborg University. Her research centers on human-environment relations, focusing on the uses and management of natural resources and ecosystems, and on social life in cyber-physical systems. Based in anthropology, she specializes in work across disciplines, and experiments with formats for ethnographic knowledge production.

Maja Hojer Bruun is associate professor at the Department of Educational Anthropology of Aarhus University. Her research interests include science and technology, organisational and economic anthropology, and interventionist and experimental ethnographic methods. She is the co-editor of the Palgrave Handbook for the Anthropology of Technology that will be published in 2021.