What is theoretical computer science? An ethnography of merit

Ola Michalec, Alex Kavvos, François Dupressoir

University of Bristol – School of Computer Science

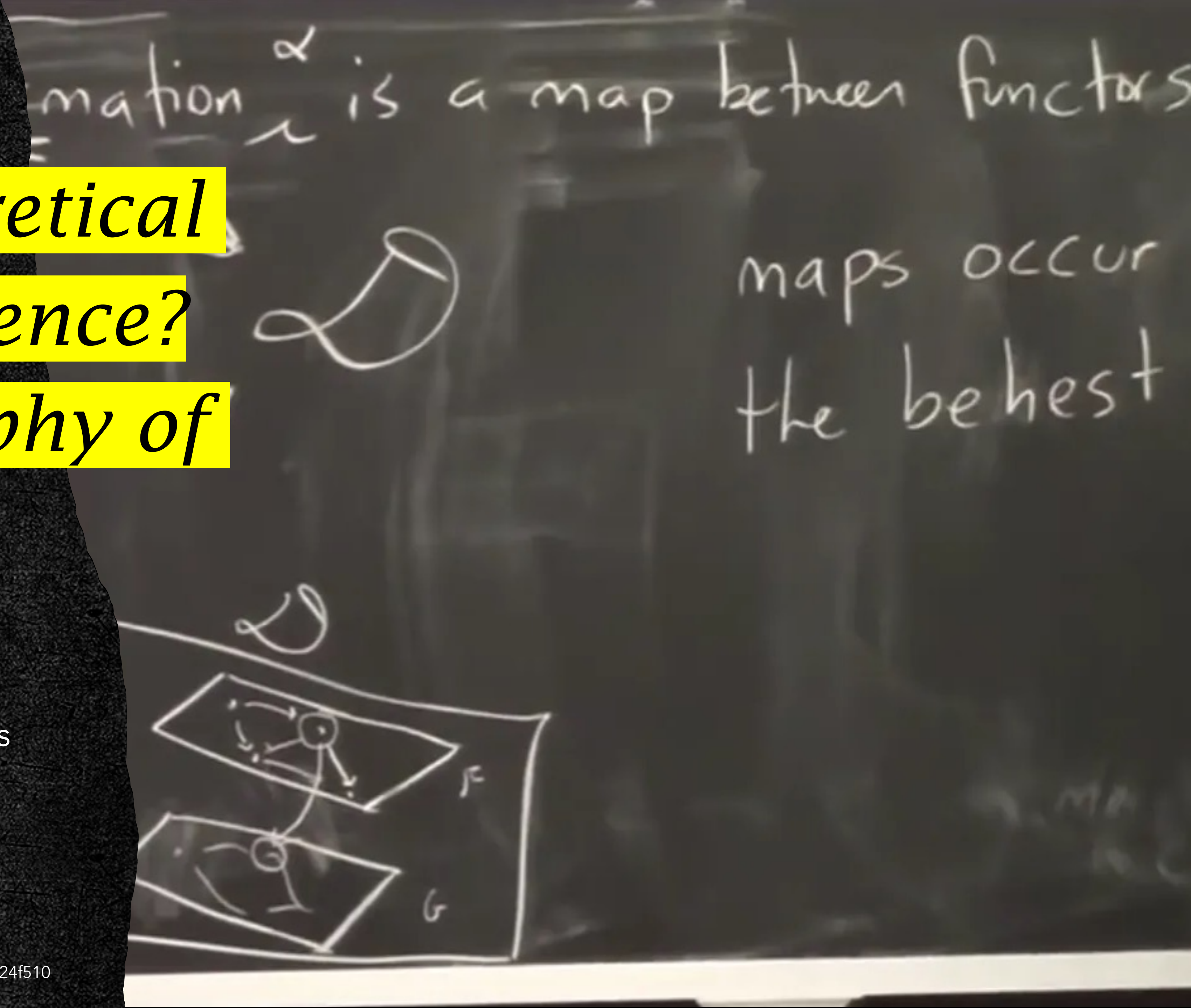


Image: https://medium.com/geekculture/category-theory-and-haskell-a6bd624f510

Research team

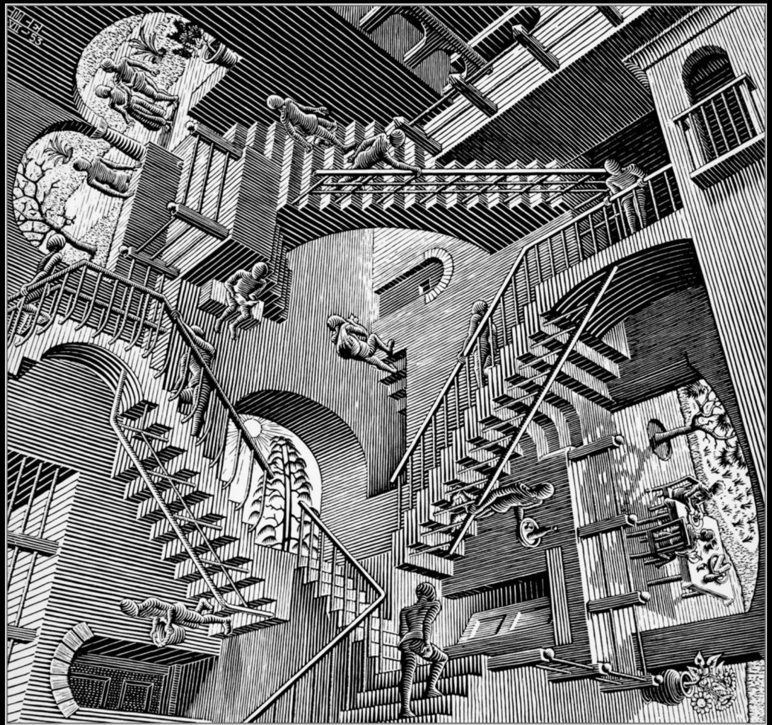
François - cryptography

Alex – Programming Languages

Ola – Science and Technology Studies

TCS Paradox

Fundamental for providing safety and security assurances, and advancing computing more generally…



…but funders and head of departments are cautious towards TCS due to its long timescales or previously unfulfilled promises.

Image: https://news.artnet.com/art-world-archives/mc-escher-copyrights-acquired-salvatore-iaquinta-federico-giudiceandrea-2400450

Research questions

How and why TCS is valued, by whom, and how its value changes over time?

Who decides what kind of TCS is done and which topics then become ‘undone’?

“We chat about these question in the conference corridors and I worry that no written record will survive” - Alex

Project framework

- Pilot workshop in 2024, funded by Research Institute for Sociotechnical Cyber Security (RISCS)
- Full bid submission in 2024
- We'd love to hear from you, receive feedback and collaborate!

RISCS Research Institute for Sociotechnical Cyber Security

Science ethnography

Bruno Latour

Researching "science in action"
– day to day practices, collaborations, tacit norms, cultures of research

Relevant studies: ethnographies of maths and CS

"How mathematicians represent their ideas to each other has implications for far more than the social status of those representations. (…) Mathematics and its representations prove inseparable and in many ways indistinguishable. Rather than work with stable incarnations of formal ideas, mathematicians must grapple with the always-fragmentary nature of their own understanding of their ongoing (and particularly nascent) projects, and their still more limited understandings of the work of their peers."

(Michael Barany)

Post-quantum encryption contender is taken out by single-core PC and 1 hour!

“It's true that the attack uses mathematics which was published in the 1990s and 2000s. In a sense, the attack doesn't require new mathematics; it could have been noticed at any time. (…) In general there is a lot of deep mathematics which has been published in the mathematical literature but which is not well understood by cryptographers. I lump myself into the category of those many researchers who work in cryptography but do not understand as much mathematics as we really should. “

(David Jao)

Relevant studies: research evaluation in mathematics

“Mathematicians acknowledge that peer review does not guarantee correctness, they still value it. For mathematicians, peer review ‘adds a bit of certainty’, especially in contrast to papers only submitted to preprint servers such as arXiv”. Most importantly, whether a finding is a proof, cannot be established by the peer review alone: Publishing an argument in a peer-reviewed journal is often only the first step in having a result accepted. Results get accepted if they stand the test of time and are used by other mathematicians” (Greiffenhagen, 2022)

"Starting from 1993 multiple groups of mathematicians studied my *erroneous* “Cohomological Theory” paper at seminars and used it in their work and none of them noticed the mistake. And it clearly was not an accident. **A technical argument by a trusted author, which is hard to check and looks similar to arguments known to be correct, is hardly ever checked in detail**” (Voevodsky, 2014)

Relevant studies: research evaluation in mathematics

Focused fields are higher status in mathematics. Focus here is defined as:
"1. Research structured around a limited number of important questions (or conjectures)
2. The active researchers in the field are aware of most of those questions
3.They agree that progress on one of those questions would be highly valuable for the field."
(Schlenker, 2020)

"There are big open questions, but it is a regular occurrence that one of them will get closed, which triggers a whole lot of very rapid progress (and consequently a lot of attention), then the question will get closed _in practice_ and become a problem for "applied cryptographers" to look at."
(François' comment)

Is TCS Undone Science?

- We argue that there are areas of TCS which are left systematically ignored, unfunded and incomplete
- We claim that Undone CS research should include both macro and micro perspectives (vis-à-vis Frickel)
- The stakeholders advocating for Undone CS are not necessary lay citizens or activists! Political struggles also happen *inside* the scientific community.

Methods

- Science ethnography as collaborative ethnography
- Bibliometrics: past 50 years of POPL and IACR
- Biography of artefacts to understand the narratives of merit

Empirical vignette: new journal in cryptology

- Rapid growth od the field since the realisation of Fully Homomorphic Encryption in 2009
- Many commercial applications and industry standards in 2017- “8 years from math to money!”
- Cryptography venues saturated and rejecting good papers – ‘default reject’ culture
- Creation of a new open access journal “the IACR Communications in Cryptology” – fast turnaround time, not limited by number of slots, all fields of crypto, positive review culture

Conclusions

Collaborate with us!

f.dupressoir@bristol.ac.uk

alex.kavvos@bristol.ac.uk

Ola.Michalec@Bristol.ac.uk

References

- Barany, M. J., & MacKenzie, D. (2014). Chalk: Materials and concepts in mathematics research. Representation in scientific practice revisited, 107.
- Barany, M. J. (2010). Mathematical research in context. MSc diss., University of Edinburgh
- Jane Calvert. 2013. Collaboration as a research method? navigating social scientific involvement in synthetic biology. In Early engagement and new technologies: Opening up the laboratory. Springer, 175–194.
- Eden, A. H. (2007). Three paradigms of computer science. Minds and machines, 17, 135-16
- Frickel, S., Gibbon, S., Howard, J., Kempner, J., Ottinger, G., & Hess, D. J. (2010). Undone science: charting social movement and civil society challenges to research agenda setting. Science, Technology, & Human Values, 35(4), 444-473
- Greiffenhagen, C. (2023). Checking correctness in mathematical peer review. Social Studies of Science, 0(0).
- Kuhn, T. (1962). The structure of scientific revolutions. Chicago: University of Chicago Press
- Latour, B. (1983) Give me a laboratory and I will raise the world. Science observed: Perspectives on the social study of science, 141–170
- Liveley et al (2022) Stories of Cyber Security (SOCS). RISCS report https://www.riscs.org.uk/wp-content/uploads/2022/04/SOCS-Combined-Report-V4.-Final.pdf
- O’Donovan, C., Michalec, A., & Moon, J. R. (2022). Capabilities for transdisciplinary research. Research Evaluation, 31(1), 145-158
- Pollock, N. and Robin Williams. 2010. E-infrastructures: how do we know and understand them? Strategic ethnography and the biography of artefacts. Computer Supported Cooperative Work (CSCW), 19, 521–556 .
- Robeyns, I. (2005). The capability approach: a theoretical survey. Journal of human development, 6(1), 93-117.
- Schiaffonati, V., & Verdicchio, M. (2014). Computing and experiments: a methodological view on the debate on the scientific nature of computing. Philosophy & Technology, 27, 359-376
- Schlenker, J.-M. (2020) The prestige and status of research fields within mathematics. https://arxiv.org/abs/2008.13244
- Stephens N, Lewis(J. (2017) Doing laboratory ethnography: reflections on method in scientific workplaces. Qual Res. Apr;17(2):202-216. doi: 10.1177/1468794116678040. Epub 2017 Apr 13. PMID: 28546784; PMCID: PMC5426556.