Codes and Lattices in Cryptography
Mini-Course
FCT-UNL

Instructor: João Ribeiro

Spring 2023

Where to look for research in cryptography

The target audience of this mini-course may be interested in searching for cutting-edge theoretical cryptography research on their own (yay if this is you!). One should keep in mind that theoretical cryptography is a subfield of theoretical computer science and follows its norms. Some of these, such as alphabetical ordering of authors, are similar to those used in other fields of mathematics. However, the main (read more prestigious and selective) venues for cryptography (and theoretical computer science in general) are *conferences*. Sometimes, extended versions of conference papers appear in journals. Some common choices are the Journal of the ACM (JACM) and the SIAM Journal on Computing (SICOMP) (for the absolute best papers), and the Journal of Cryptology and the IEEE Transactions on Information Theory (good, but below JACM and SICOMP). However, not everyone does this (I believe that it should be done more often).

Almost all cryptography papers are freely available online. The main repository for cryptography preprints is the Cryptology ePrint Archive (https://eprint.iacr.org/), but some cryptography preprints also appear on the arXiv, usually under the cs.CR, cs.CC, and math.IT tags. What follows is my (João) personal and non-exhaustive ranking of various conferences. Other people may have different opinions. Keep in mind also that, as with all publication venues, the review process can be somewhat noisy at times.

- CRYPTO and Eurocrypt are the most prestigious cryptography conferences. Great cryptography papers sometimes also appear in the ACM Symposium on Theory of Computing (STOC) and the IEEE Symposium on the Foundations of Computer Science (FOCS), which are generalist theoretical computer science conferences and widely considered to be the most prestigious venues in all of theoretical computer science. These four venues should be the first places to look at for current research in cryptography.

- The Theory of Cryptography Conference (TCC) and Asiacrypt also feature great cryptography research, a tier below CRYPTO and Eurocrypt. In particular, TCC is the flagship conference of the theoretical cryptography community. Another theoretical computer science conferences of the same tier that features good cryptography research is the Innovations in Theoretical Computer Science Conference (ITCS). This conference values conceptual contributions.

- The Information-Theoretic Cryptography Conference (ITC) and the Conference on Public-Key Cryptography (PKC) are a tier below TCC and Asiacrypt and publish good research too.

- Quantum cryptography work also appears in the venues above. Other great conferences to look out for in this topic are QIP (the top conference), TQC, and QCRYPT. QIP and QCRYPT are talk or poster only, and it is not uncommon to see authors give a talk about a work at QIP and publish it at CRYPTO/Eurocrypt/STOC/FOCS.

- More applied cryptography research sometimes also appears at CRYPTO and Eurocrypt, and other times it appears at security conferences. Top conferences for security research are (in no particular order) CCS, S&P, USENIX, NDSS, and PETS.