

Panel Discussion on Publications



Allison Bishop
Gregor Leander

Anne Canteaut (moderator)
Gaëtan Leurent

Cas Cremers
Kevin McCurley

iacr.org/publish

The Current IACR Landscape

Publication venues

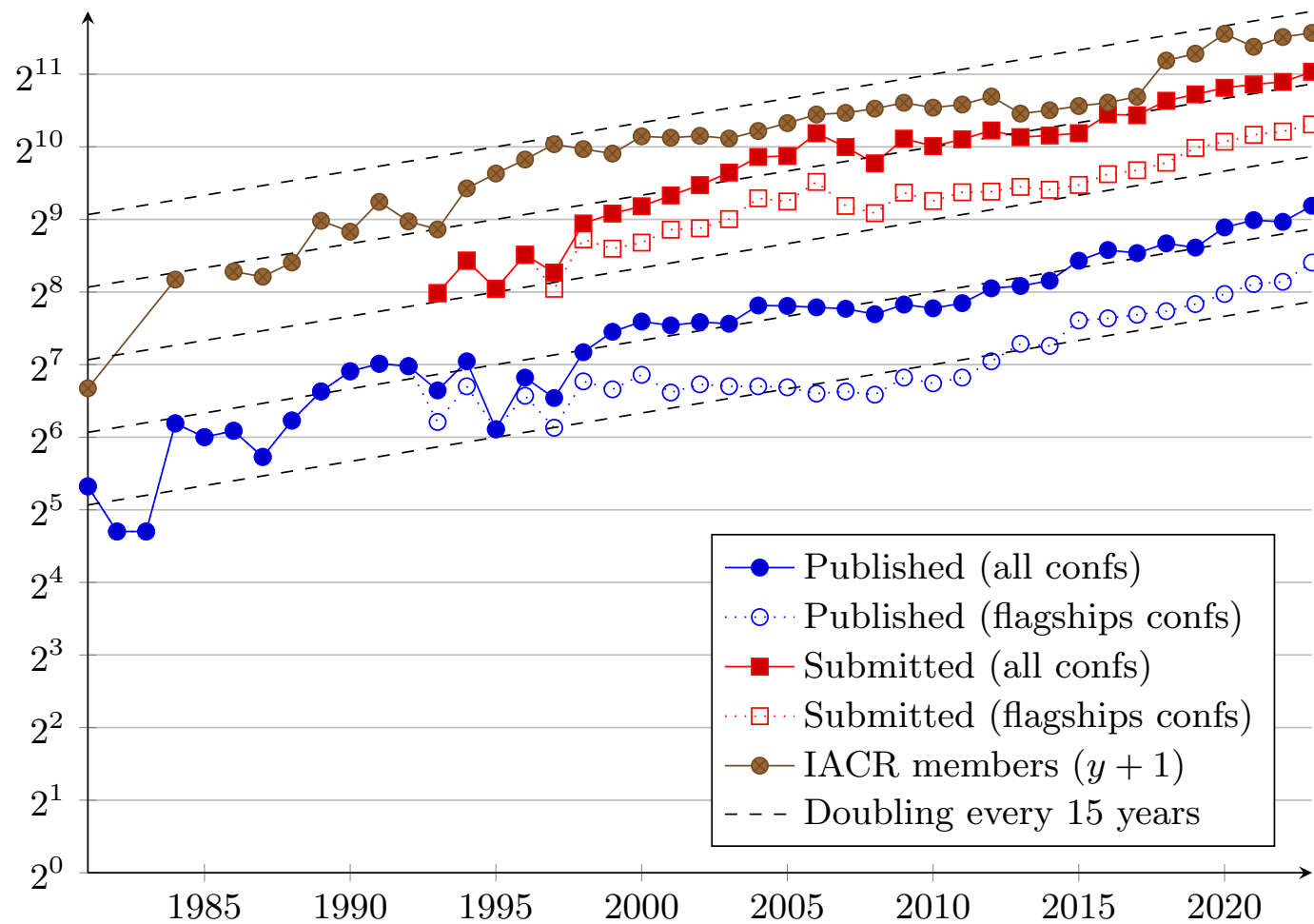
- Proceedings of Asiacrypt, Crypto, Eurocrypt, as Springer LNCS
- Proceedings of PKC, of TCC, as Springer LNCS
- IACR Transactions ToSC and TCHES, as RUB/OJS journals
- Journal of Cryptology, published by Springer
- IACR Communications in Cryptology Journal, published by IACR, new publishing platform
- Cryptology ePrint archive (not refereed)

Conferences and Symposia

- Asiacrypt, Crypto, Eurocrypt (multi-track)
- PKC, TCC
- FSE, CHES
- RWC (no publications but good talks)

Most reviewing is done with a version of HotCRP

A Regular Growth



Discussion Topics and Biggest Perceived Problem Areas

1. Business and funding models:

open access, cost of publishing, commercial vs. academic publisher...

2. Controlling and improving quality of publications:

How to improve the reviewing process?

- How to handle reviewing load?
- How to make reviews more useful to authors?

Would a journal publication be more appropriate?

3. Conferences:

- What are the main roles of conferences?
- Do we want to have presentation for each accepted paper?
- Scalability: Shorter talks? Posters?
- Should we take into account people who cannot or don't want to travel?

Open access and cost of publishing

An increasing number of funding agencies are demanding open access for the research they sponsor.

Open access is available in all venues, under **wildly varying costs**.

- Springer charges \$3090 / €2490 / £2190 per paper for Journal of Cryptology.
- Springer charges \$2890 / €2290 / £1970 per paper for LNCS
- ACM will charge \$1300/\$1800 in 2025 (member/non-member per paper)
- ToSC, TCHES, and CiC will continue to charge \$0.
- We estimate **actual cost for CiC is < \$5/paper** (except for copy editing)

Reviewer overload: the resubmission problem

- 157 papers that were rejected from Eurocrypt'24 (43% of rejected papers) were resubmitted to Crypto.
- 45 of these 157 resubmissions (29%) have been accepted at Crypto'24.
- 18 papers rejected from Eurocrypt'23 have been rejected from Crypto'2024.
- Some of those papers will be improved and eventually accepted
- Some papers will just never be accepted.
- Editorial reviews are done by volunteers. We need to use that wisely.

Purpose and scalability of conferences

If we keep having 20-minute talks for every paper, then

- We end up with many parallel tracks, or more days (\rightarrow more expensive), or
- The acceptance rate will decrease.

What is the purpose of a conference?

Do we want to decouple publications and conferences?

Does each paper have to be presented?

- If yes, do we want to increase the number of tracks, or to decrease the length of each talk?
- If not, do we prefer posters or no presentation at all?