How to Publish

TECHNISCHE UNIVERSITÄT DARMSTADT

Cryptoplexity

Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

November 2020

Marc Fischlin

Publication Venues

Four Types of Venues

Journals	Conferences (with peer-reviews/ proceedings)	"accountable"
Workshops / Conferences (without peer reviews/proceedings)	Electronic Archives	"non-accountable"

Four Types of Venues

Journals	Conferences (with peer-reviews/ proceedings)
Workshops / Conferences (without peer reviews/proceedings)	Electronic Archives

"accountable"

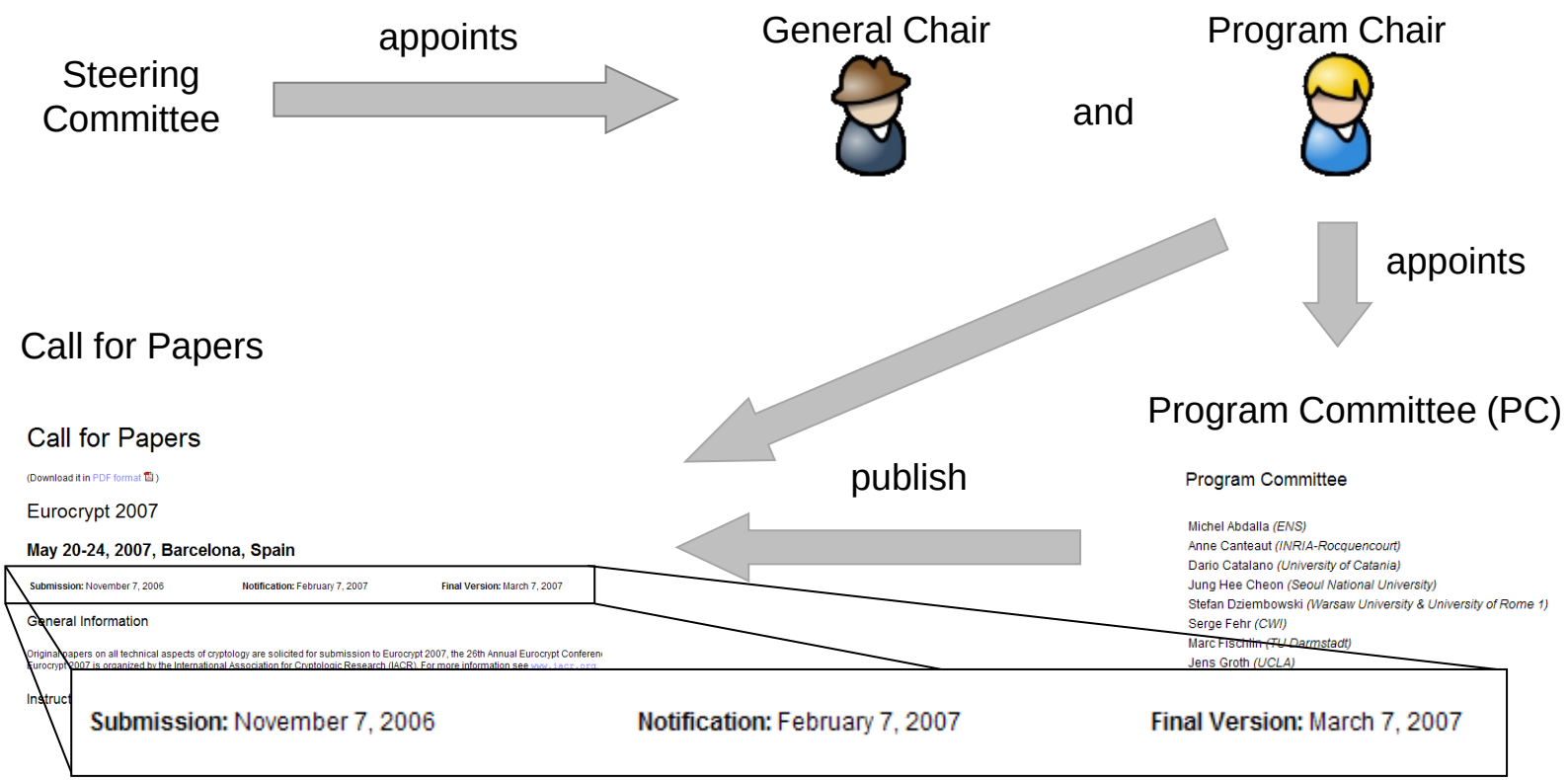
"non-accountable"

Conferences

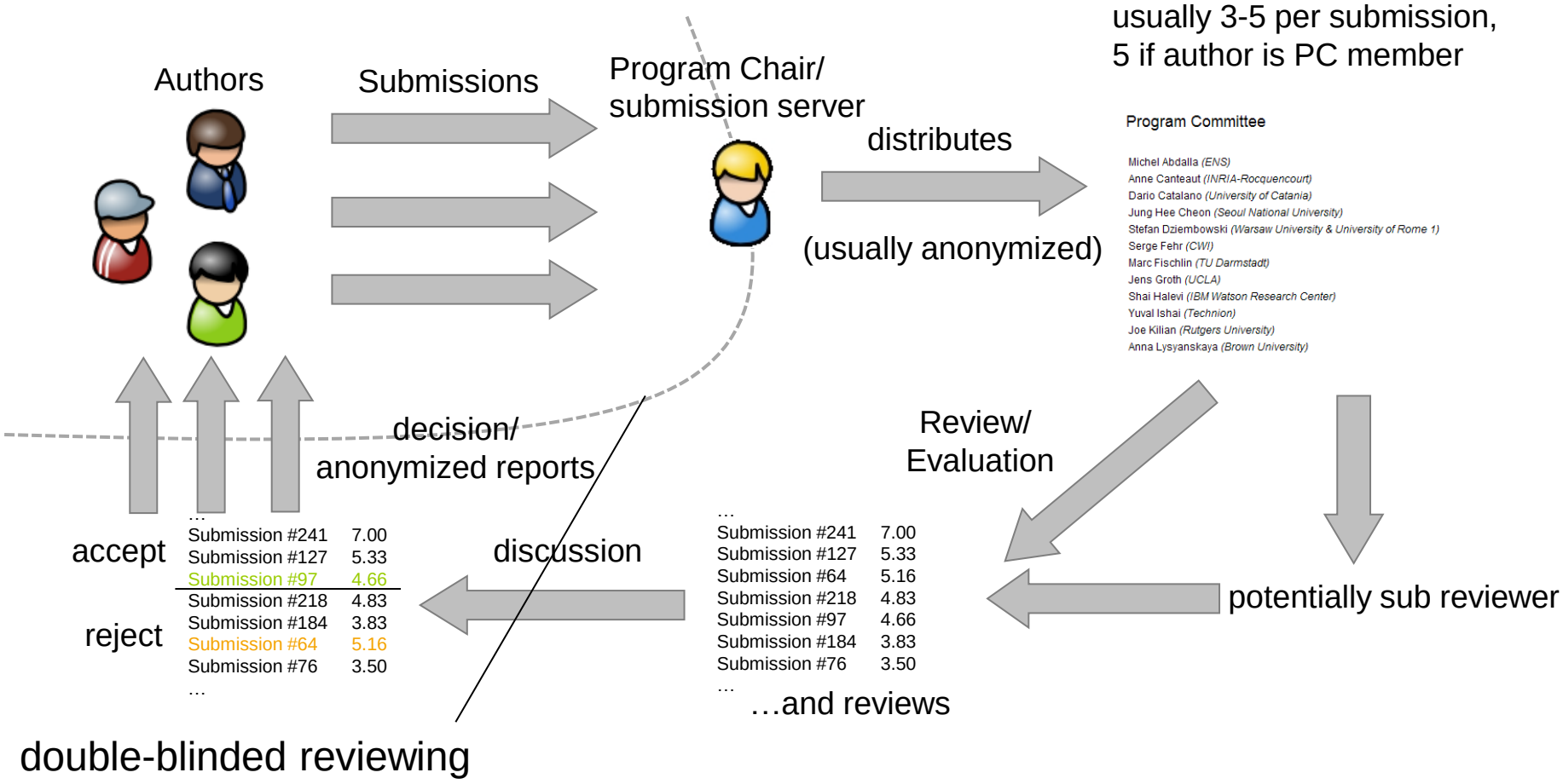
- in Journals
  - classical way to publish (still is in some disciplines)
  - very long delay from submission to publication (years!)
  - comprehensive presentation and thorough reviewing

- Conferences with Proceedings
  - delay can be shorter, if accepted (ca. 3 – 6 months)
  - typically, limited number of pages (ca. 10-20 pages)
  - publications checked less thoroughly (?)

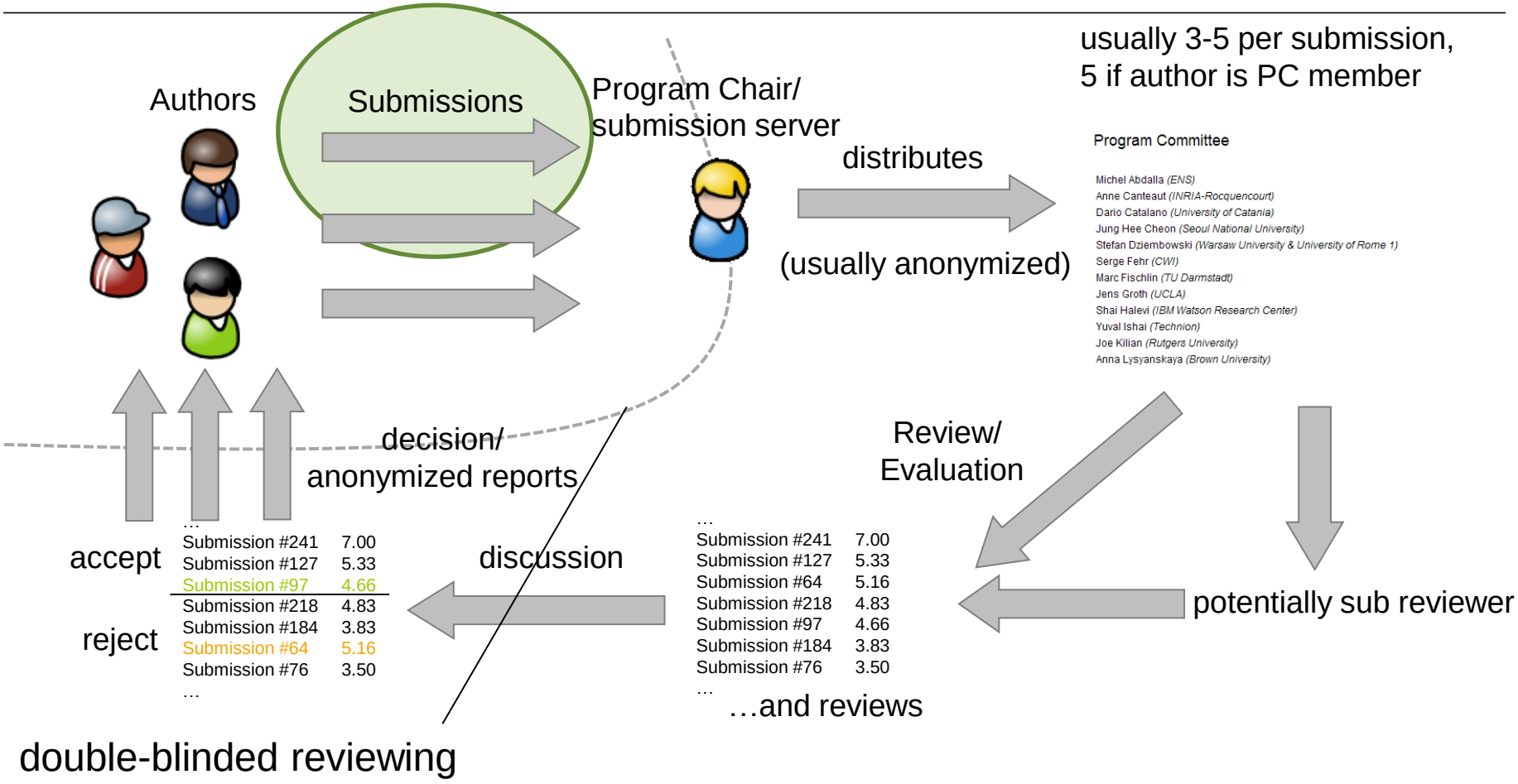
Setting up a Conference



Conference Process



Conference Process



How to Find Conferences?

- for main conferences every year around same time
- more and more conference moving to year-round submission cycles (eg, one every quater)
- for „our“ community:
  International Association of Cryptological Research (IACR):

  www.iacr.org/events/

see also: ATHENE Conference Radar

How to pick the right conference?

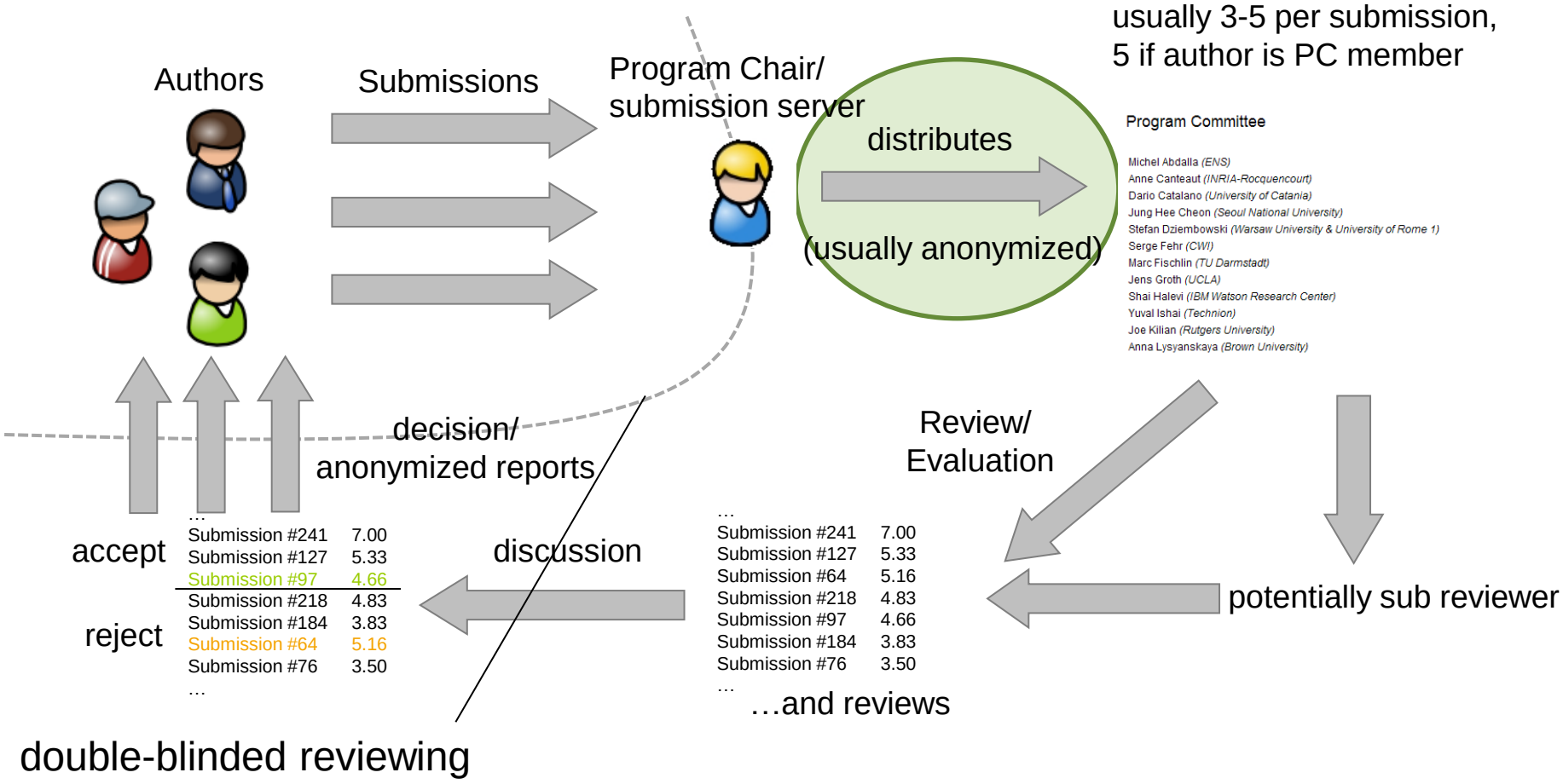
- one of the toughest questions in research…
- rule of thumb:
  cited papers appear at conferences of similar quality
  (but quality of results must also be good, of course)
- another good indicator: present at workshop and observe reaction (but subtract politeness)
- and then there is the story of the GMR ZK paper…

Conference Ranking

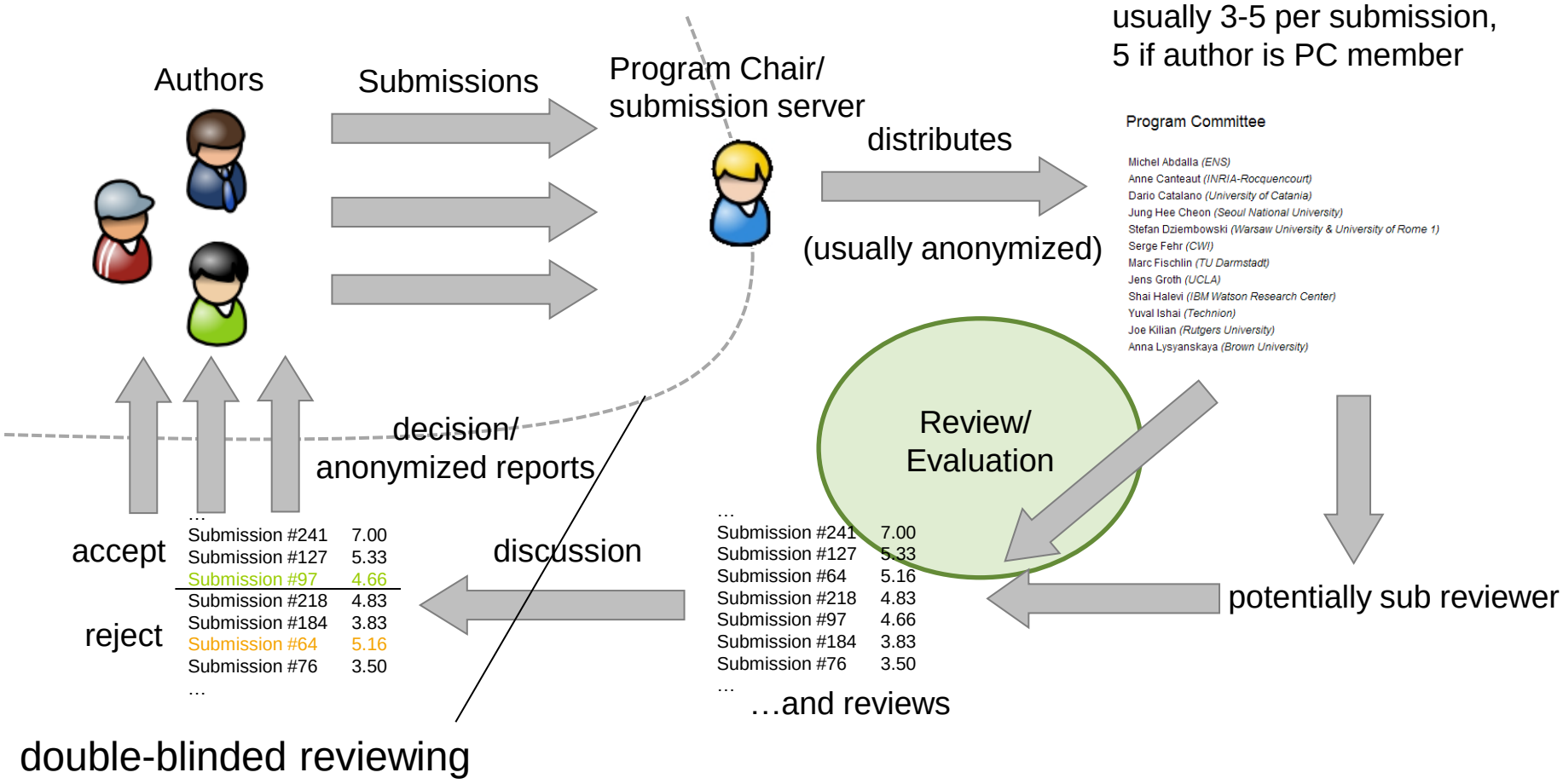
good general source:
Core Ranking

Crypto	Security	Theory	
• Crypto, Eurocrypt	• CCS, S&P • Usenix, NDSS	• STOC, FOCS • PODC	first tier / A*
• Asiacrypt, • TCC, CHES	• ESORICS, CSFW	• ICALP, STACS, CCC	second tier / A
• PKC, FSE, CT-RSA, ACNS	• AsiaCCS, ARES		third tier / B

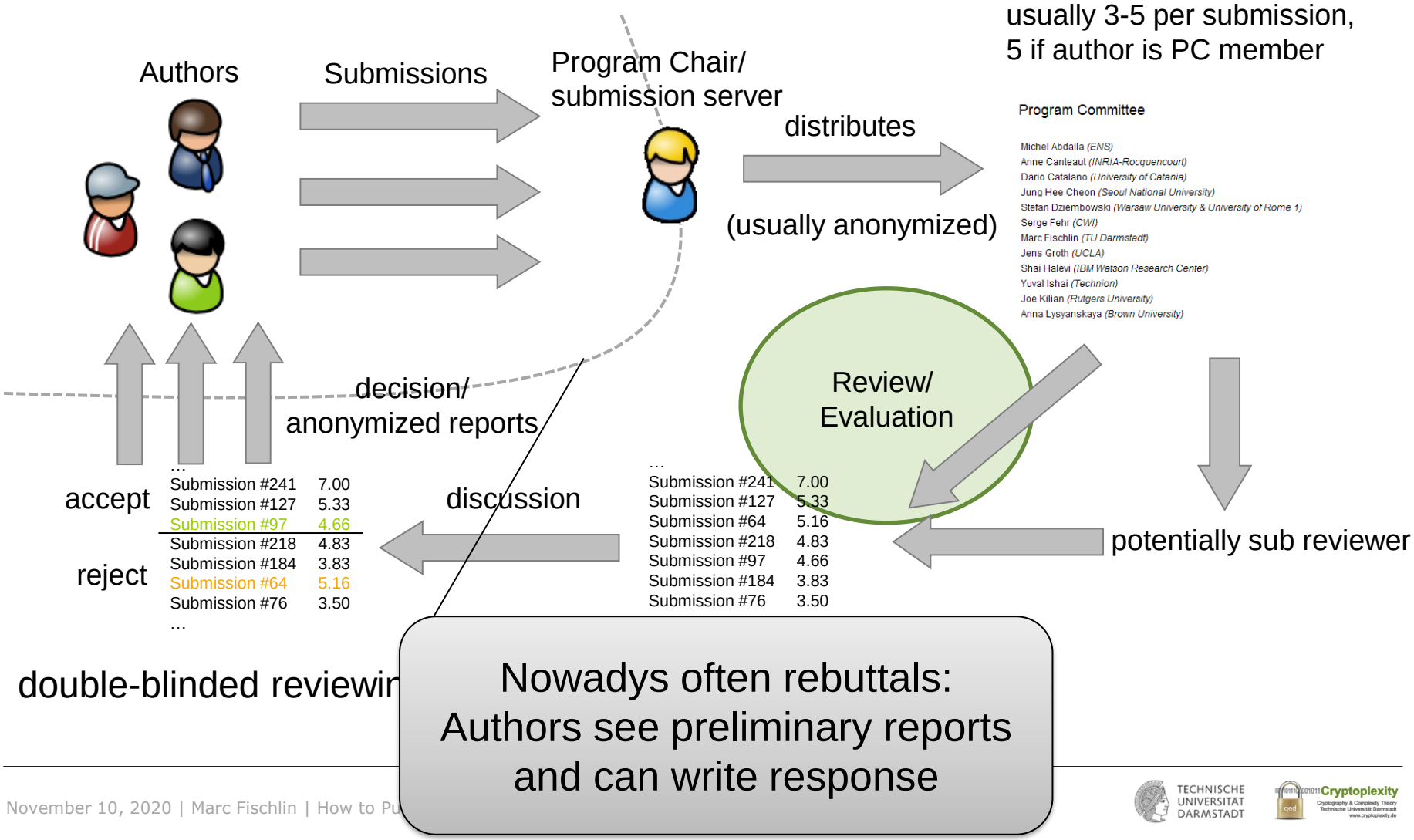
Conference Process



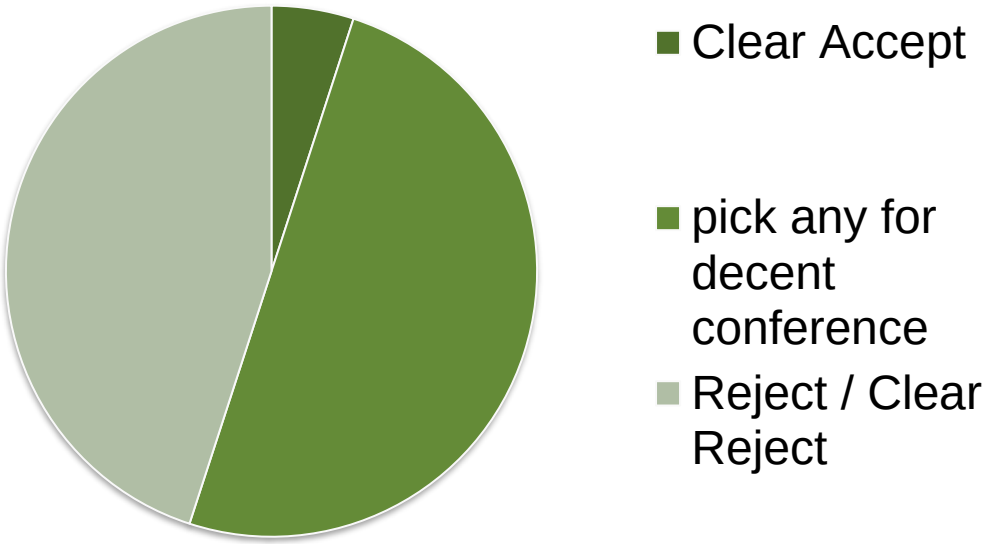
Conference Process



Conference Process: Rebuttal

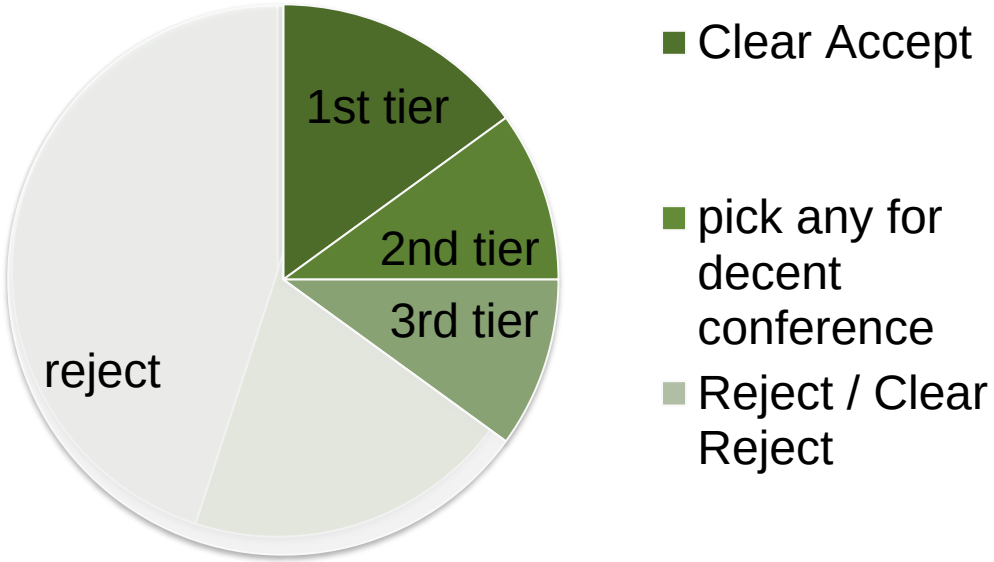


Quality Distribution of Submissions



- (not so serious) Hypothesis:
  At every major crypto conference the „clear-accept number“ is a constant, equal to 8.

Acceptance Rates (approximately)



- 1st tier conferences: 10% - 20%
- 2nd tier conferences: 20% - 30%
- 3rd tier conferences: 30% - 40%

What‘s Wrong with the Reviewing Process today?

- Time Constraints
  - reviewers have too little time (or don‘t want to spend much time)
- Empirical Constraints
  - reviewers know that > ¾ of their assigned papers won‘t make it
- Expectations
  - reviewers expect to learn something useful, non-trivial
- Subconscious Bias
  - my area is important, holds especially for more junior reviewers

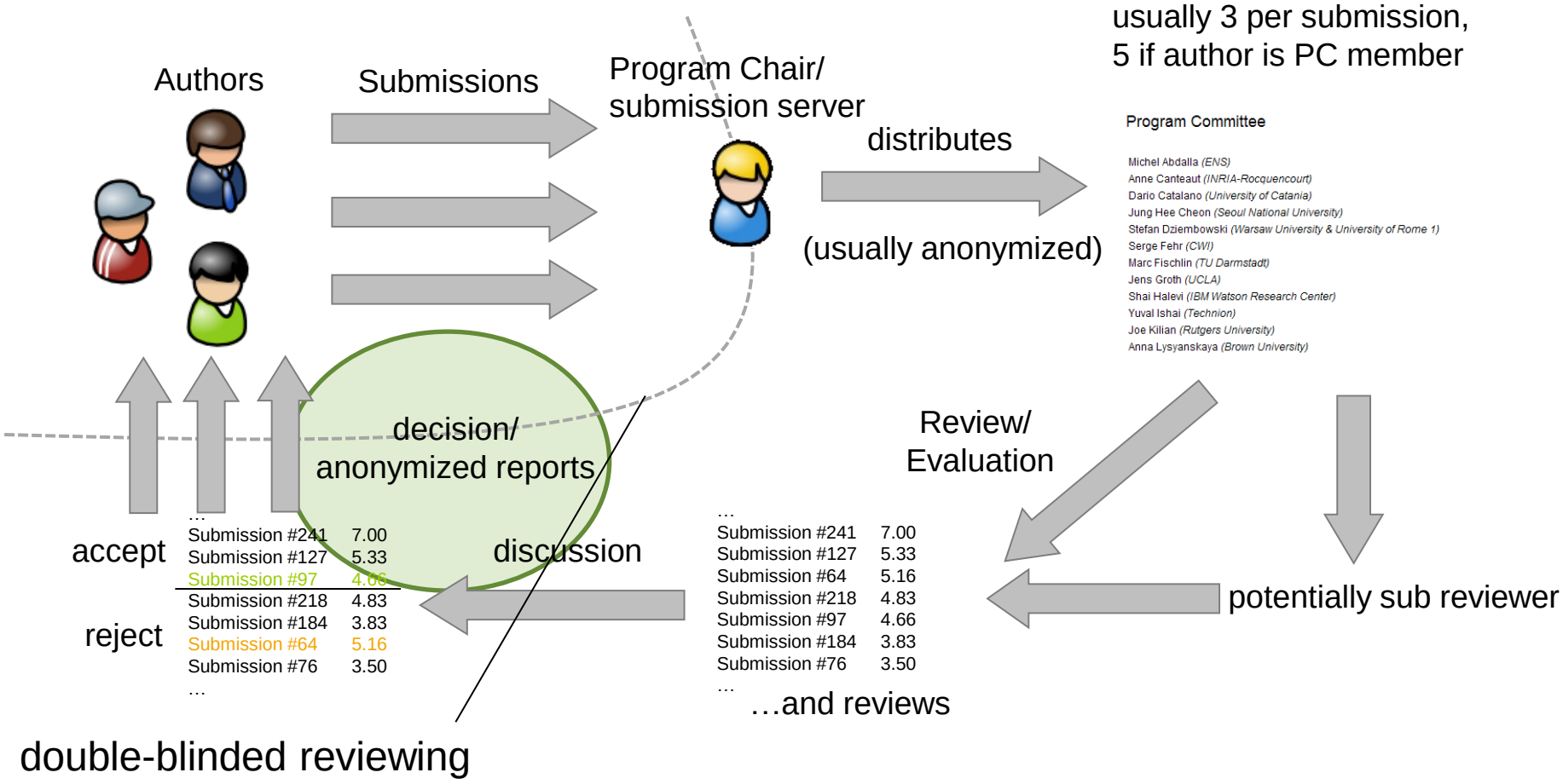
Implications of Conditions

- reviewers often check local soundness
  but ignore question of importance of contribution and alternative solutions
- reviewers are happy if they find flaw, and stop immediately
- reviewers are impressed by technically involved results (if they at least get the main points)

How a Review should be

- be constructive
  - describe how authors can improve paper instead of dislikes
  - If there‘s a flaw, can one fix it *easily*? Else, is this part important?
- importance / concept over technical hardness
  - Does this paper advance the field? Or is it just complicated?
  - But: Technique can also be important (eg, hybrid method)
- be polite and fair

Conference Process



If the Paper gets Accepted

- take reviewers comments into account,
  but authors take responsbility for final version!
- when merge is demanded, comply
- when shepherding is enforced, obey to requests
- can sometimes ask for extra pages for final version

Four Types of Venues

Journals

Conferences (with Proceedings)

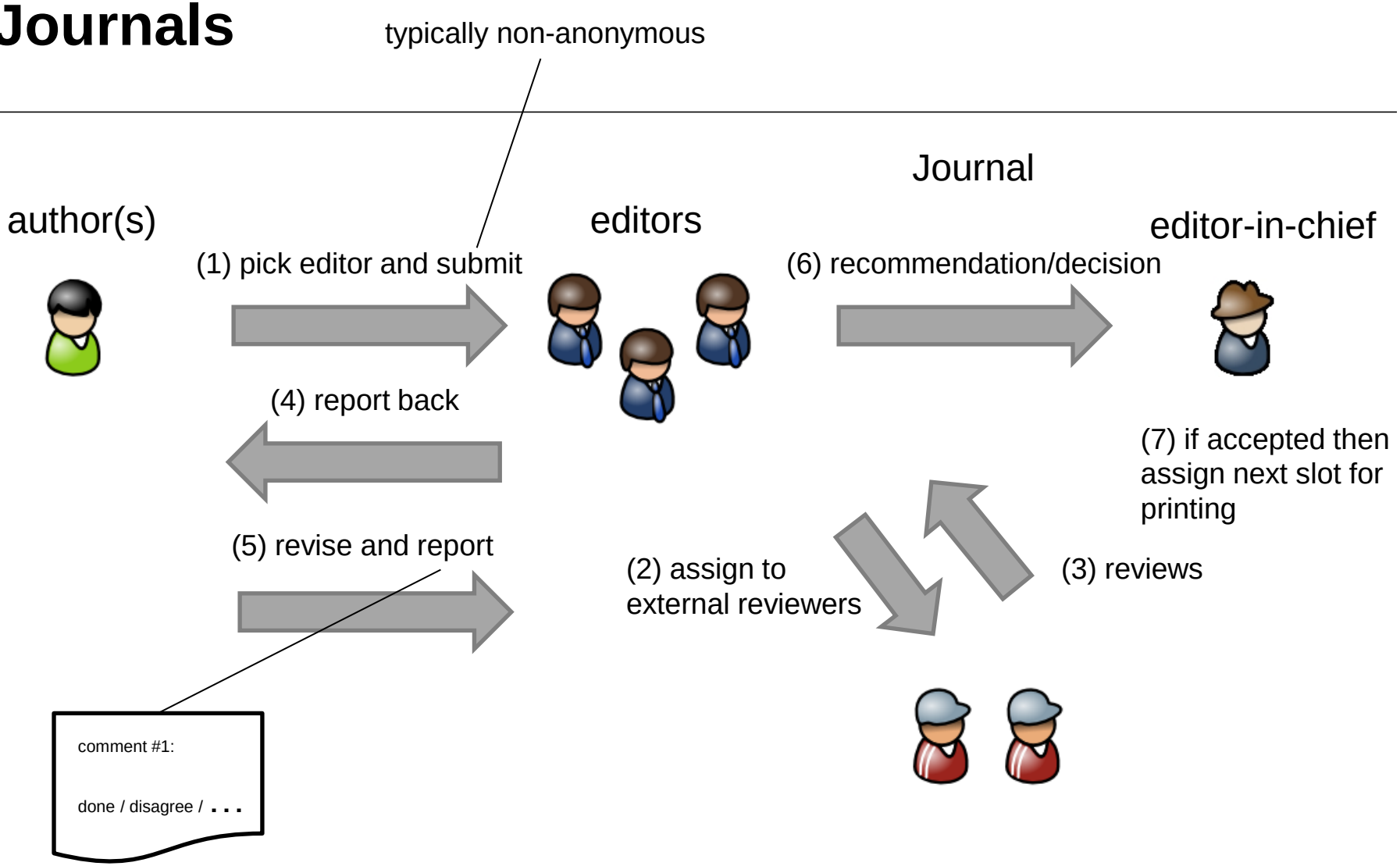
Workshops / Conferences without Proceedings)

Electronic Archives

"accountable"

"non-accountable"

Journals



Journal Ranking

Microsoft Academic Research
not comprehensive

Crypto / Security

- Journal of Cryptology, TISSEC
- Journal of Mathematical Cryptology; Designs, Codes and Cryptography; IJACT

General

- JACM, CACM
- SIAMCOMP, JCSS
- TCS

many more journals

only few crypto journals
(cf. number of conferences)

Four Types of Venues

Journals	Conferences (with peer reviews/ proceedings)	"accountable"
Workshops / Conferences (without peer-reviews/proceedings)	Electronic Archives	"non-accountable"

Workshops

- usually no paper, just presentation
- can usually still publish at conferences and journals
- regular workshops in our community at:
  - Dagstuhl
  - Bertinoro
  - Leiden
  - ….

Electronic Archives

- typically no reviewing (just format)
- can still publish elsewhere, but time‘s ticking!
- known archives in our community:
  - „the“ crypto archive: eprint.iacr.org
  - other crypto-related archives: arXiv.org
  - …