Why Your Crypto Paper Got Rejected

» A Formal Analysis Attempt

The Honest Cryptographer

Asiacrypt Rump Session '25

Methodology: Why Beamer?

- **Alignment Principle:** We are conducting a *Formal Analysis* of the review process.

Formal attempts require formal presentation tools.

- **Contextual Fit:** Beamer is the natural habitat of the Rump Session.
  - → It compiles to PDF (as strictly required by the CfP).
  - → It proves we spent more time on **typesetting** than on the **research**.

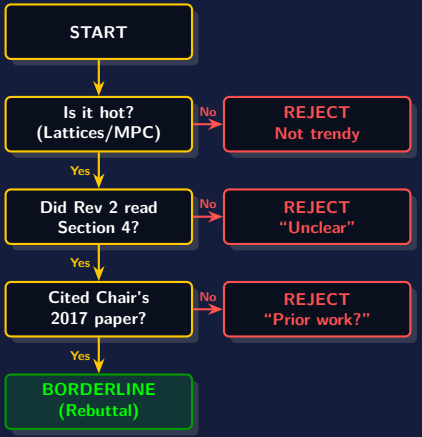
The “Idealized” Review Model

$$\texttt{Author} \rightarrow \texttt{Submit} \rightarrow \texttt{Eval} \rightarrow \texttt{Decide}$$

- **Assumption 1:** Reviewers actually read the paper.
- **Assumption 2:** They agree on what “novelty” and “important” means.
- **Assumption 3:** Decisions are consistent across venues.

IS IT TRUE THOUGH?

The Actual Decision Process



Adversarial Model: The "Reviewer 2" Paradigm

Definition 1: The Strong Adversary ($\mathcal{R}_2$)

Let $\mathcal{R}_2$ be a probabilistic polynomial-time adversary with access to the submission server.

Adversarial Capabilities:

- **Oracle Access:** Can query "Google Scholar" to find 1990s papers you missed.
- **Distinguishing Attack:** Can distinguish between English (US) and English (UK) spelling with advantage $\epsilon = 1$.
- **Denial of Service:** Capable of submitting the review 1 minute *after* the deadline, preventing rebuttal construction.

Sample “Consistent” Reviews

Review 1

“Technically interesting, but motivation unclear.”

Score: 3

Review 2

“Motivation great, but technical part unclear.”

Score: 3

Review 3

“Both clear, but I am just not excited.”

Score: 3

Final Decision: Weak Reject.

PC Comment: “Please carefully address all three mutually incompatible comments.”

Theorem 1: Impossibility of Consistency

Theorem (Indistinguishability)

Let $\mathcal{A}$ be the acceptance function. The output of $\mathcal{A}$ is computationally indistinguishable from a random oracle.

$$|\Pr[\mathcal{A}(P) = 1] - 0.5| < \epsilon$$

Proof via Existential Counter-Example:

- **Assumption:** The system is deterministic (i.e., fair).
- **Requirement:** Determinism holds if and only if all participants are rational ($\forall r : r \in \text{Honest}$).
- **Attack:** By Definition 1 (Slide 5), we proved that $\exists \mathcal{R}_2$ (The Adversary).
- **Conclusion:** The mere existence of the adversary breaks the security assumption. □

Corollary: Rump Session Completeness

Corollary 1

Any result not accepted by the main program eventually appears at a Rump Session with probability $1 - \epsilon$.

- **Lemma:** The Rump Session is the universal fallback channel.

Conclusion: Your paper is fine.

(The system is just random.)

Towards a Better Protocol

The "Utility" Axiom

Impossibility results are strictly forbidden without matching upper bounds.

↪ *Rationale:* Lower bounds are just "bad news." To have a "full paper," you must provide the solution.

Our Constructive Upper Bound (The Protocol):

- **Consensus Mechanism:** Rejection requires a **2-out-of-3** agreement from the PC.
- **Fail-Safe Mode:** If disagreement persists across 3 consecutive conferences:

$\rightarrow$ **Automatic Rump Session Invited Talk.**

Your paper was not rejected.

It was just load-balanced. . .

to the rump session.

Questions? Ask Reviewer 2.