New Directions in Rate Limiting

Watson Ladd, IETF 123

Where we were

- BBS schemes: well-understood implementation, limitations
- Information theoretic unlinkability inapplicable to rate limiting
- Circuit based could do more, but computational rate limiting
- Both are f=PRF(k, site) but the PRF is more secure in PQ world for circuit

Where we are

- Recent eprint (2025/1030) shows information theoretic rate limiting
- Google released age verification tech based on circuits
- Circuit security got scarier in PQ setting with Fiat-Shamir attacks

A bit of the solution

- T1[i1(x)]+T2[i2(x)]+p(x)
- Draw graph linking T1 T2 if both queried
- If no cycles bigger than degree(p), win
- Parameters not great: limited number of shows (which we can turn into one credential per table entry), polynomials big
- Have thought about hypergraph, promising results (better realistic parameters)

Large solution space to all your problems

- Circuits vs. BBS
- Credential issuing formats
- Multissuer possible
- Rate limiting
- Bottom line: what makes sense for the Internet, what can we deploy?