No MTI Crypto without Public Review

- Goal: Keeping "bad" crypto out of IETF standards
- Problem: IETF not competent (or timely) to review all crypto mechanisms
- Proposed solution: Rough consensus on how we (IETF) can address the goal
- Logistics: draft-rsalz-dbrg-speck-wap-wep submitted.
- Current home https://github.com/richsalz/draft-rsalz-dbrg-speck-wap-wep
- Next home?

What's "good enough"

- "I know it when I see it" *isn't**
- "Nobody cracked my cipher and claimed the reward" *isn't*.
- CFRG review
- Global competition: AES, SHA3, CAESAR, etc.
- Multiple papers in RWC, Crypto, Usenix, etc.

*Perhaps unless you're djb (kidding) (maybe)