Rump Session 2016

Test of Time Awards at Major Crypto Conferences?

Marcel Keller

University of Bristol

Proposal: Test of Time Awards After Exactly 20 Years

- Why test of time awards?
  $\Rightarrow$ TCC, CCS, USENIX have it. Why not Crypto, EC, AC?
- Why 20 years?
  $\Rightarrow$ RSA 1977, PGP 1991, SSL 1994, TLS 1999
- Why exactly 20 years?
  $\Rightarrow$ Nobel prize delay

Eurocrypt 1996

1. *The Exact Security of Digital Signatures — How to Sign with RSA and Rabin*
   Mihir Bellare, Phillip Rogaway
   (979 citations)
2. *Security Proofs for Signature Schemes*
   David Pointcheval, Jacques Stern
   (939 citations)
3. *Designated Verifier Proofs and Their Applications*
   Markus Jakobsson, Kazue Sako, Russell Impagliazzo
   (859 citations)

Source: Google Scholar

NB: Not advocating a purely number-based award.