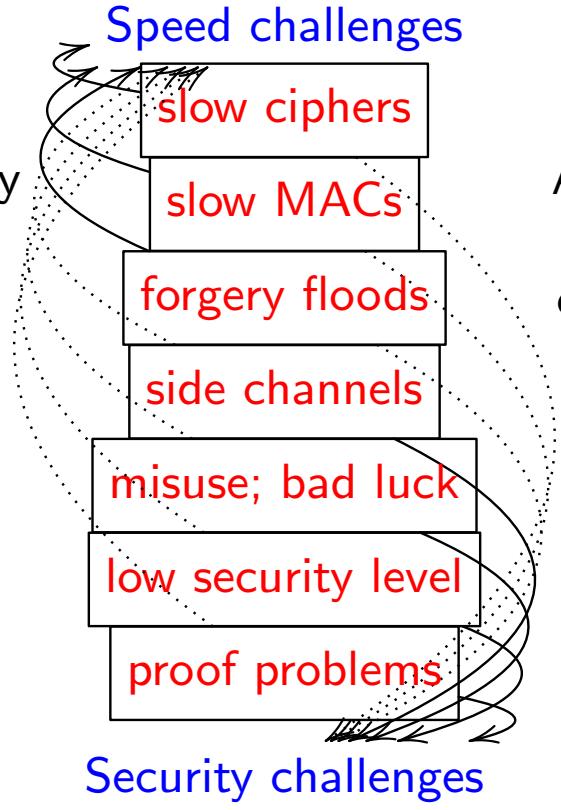
# Authenticated ciphers

The high-performance workhorse of cryptography:
encrypting and authenticating messages using a shared secret key.

**Challenge:**
Major recent failures of confidentiality and integrity in SSH, TLS, etc.
Performance pressure continues to hurt security: EAXprime, Simon, etc.

**Solution:**
Improve efficiency without compromising security.
Improve security without compromising efficiency.




**Scientific impact:**
Influential cipher designs: AEZ, HS1-SIV, ICEPOLE.
Security analysis/proofs: e.g., Dual EC and AMAC.
Universal hardware API.
Many new speed records.

**Broader impact:**
e.g., AEZ under consideration by Tor; AMAC security analysis bolstering confidence in widely deployed Ed25519; many ciphers already using universal hardware API; various PhD students.

| | | |
|---|---|---|
| 1314885 | UCDavis | Phillip Rogaway |
| 1314592 | CSUS | Ted Krovetz |
| 1314919 | UIC | Daniel J. Bernstein (coordinator) |
| 1314540 | GMU | Krzysztof Gaj, Jens-Peter Kaps |