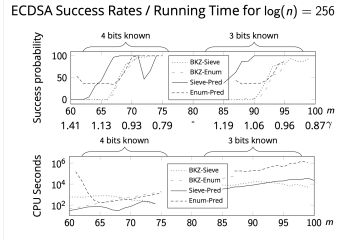
CAREER: Cryptographic Security at Internet Scale (2048563)

Challenge:

- Detect flawed cryptographic implementations from internet traffic.
- Scale up cryptanalytic computations.

Solution:

- Develop and deploy traffic flows analysis tools. (Up and running.)
- Design algorithms to detect vulnerabilities. (Ongoing.)
- Carry out new cryptanalytic records. (Done.)



Scientific impact:

- Improved understanding of hidden number problem and ECDSA cryptanalysis.
- RSA key exposure vulnerabilities much more widespread than realized.

Broader impact and broader participation:

- Disclosed and fixed cryptographic flaws affecting major vendors.
- Training PhD student: George Sullivan, UCSD.
- Undergraduate researchers: Jessica Lam, Annie Dai, Dustin Lin
- Popularization articles: IEEE S&P, Techniques de l'Ingénieur

Nadia Heninger UCSD