DNSSEC NSEC5: Elliptic Curves

Jan Včelák
⟨jan.vcelak@nic.cz⟩

2016 April 7

Authenticated Denial of Existence in DNSSEC

1

example.com

www.example.com

mail.example.com

2

H(example.com) = e1654f27

H(www.example.com) = a029e8a9

H(mail.example.com) = 3c294eff

3

3c294eff

a029e8a9

e1654f27

4

NSEC: 3c294eff → a029e8a9

NSEC: a029e8a9 → e1654f27

NSEC: e1654f27 → 3c294eff

1. Take all names in the zone.
2. Compute hashes of the names.
3. Sort the hashes.
4. Build NSEC records from subsequent pairs.

Preventing zone content enumeration

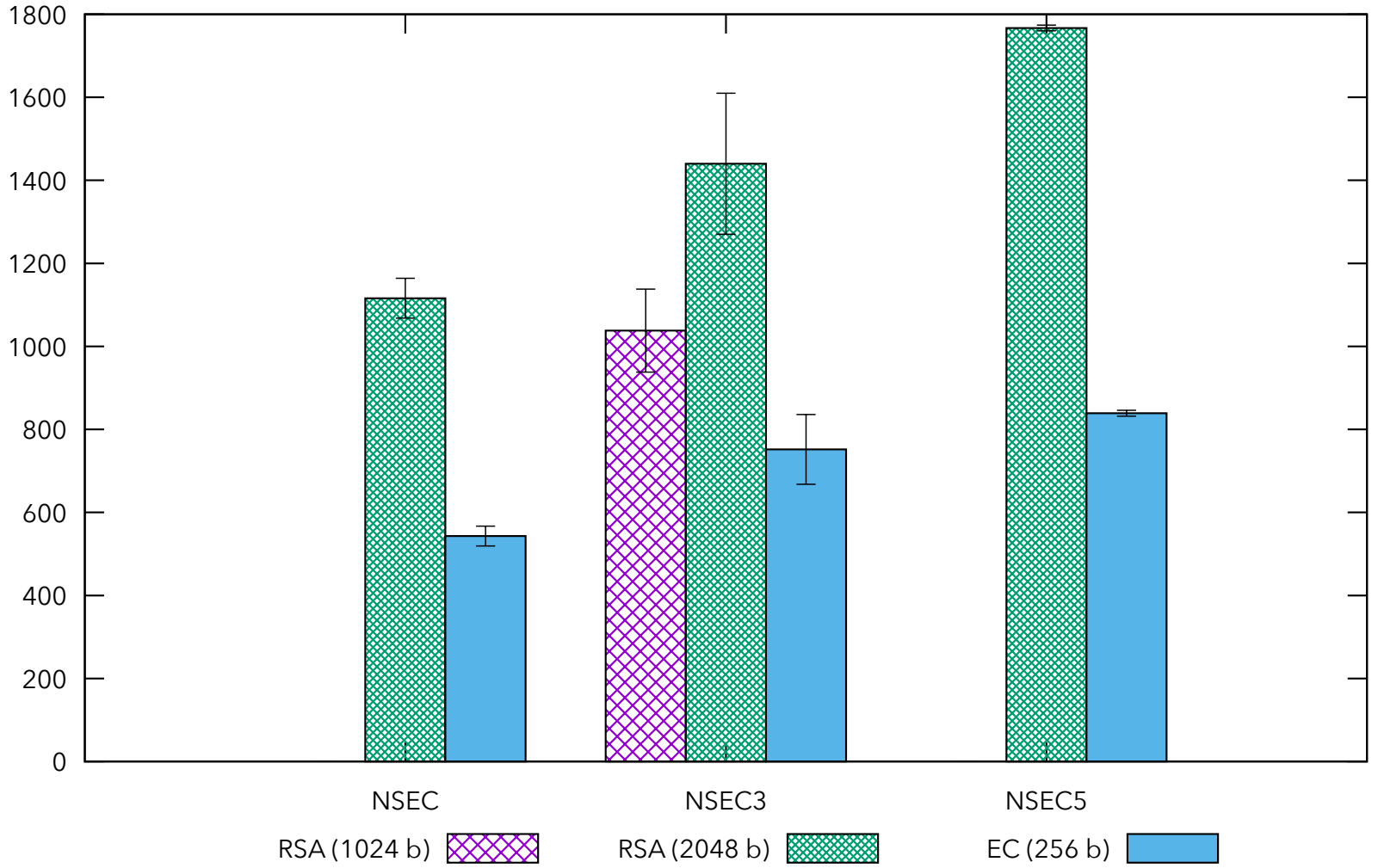
- NSEC (RFC 4034, March 2005)
  - No domain name hashing
  - Zone content enumeration is trivial
- NSEC3 (RFC 5155, March 2008)
  - Uses SHA-1 for domain name hashing
  - Zone content enumeration is still possible
- NSEC5 (**draft-vcelak-nsec5**)
  - Uses public-key hashing scheme
  - Zone content enumeration is impossible

NSEC5 public-key hashing scheme

- RSA based scheme (draft -00)
  - RSA FDH (Full Domain Hash)
  - NSEC5 proof is 256 bytes for 2048-bit key
- EC based scheme (draft -02)
  - Custom VRF (Verifiable Random Function) [1]
  - Uses secp256r1 or Ed25519
  - NSEC5 proof is 81 bytes

[1] Goldberg S., Naor M., Papadopoulos D., Reyzin L. *NSEC5 from Elliptic Curves* in ePrint Cryptology Archive 2016/083. January 2016.

NSEC response size measurements



RSA is RSASHA256 for DNSKEY, RSAFDH-SHA256-SHA256 for NSEC5
EC is ECDSAP256 for DNSKEY, EC-P256-SHA256 for NSEC5

NSEC5 Resources

- Current draft:

  https://tools.ietf.org/html/draft-vcelak-nsec5-02
- Working copy of the draft:

  https://gitlab.labs.nic.cz/knot/nsec5-rfc
- NSEC5 project page:

  https://www.cs.bu.edu/~goldbe/papers/nsec5.html
- Sample NSEC5 crypto implementation:

  https://gitlab.labs.nic.cz/knot/nsec5-crypto