A Recent “Attack” on RSA Public Keys

The Story

- Preprint posted to IACR ePrint on 02-15-2012
- Popular media coverage includes sensational headlines such as
  - “Researchers crack online encryption system” (Infoworld)
  - “Flaw Found in an Online Encryption Method” (New YorkTimes)

RSA Refresher

- Modulus n = pq (p,q prime)
- Choose $1 < e < \varphi(n) = (p-1)(q-1)$
- Calculate $d = e^{-1} \bmod \varphi(n)$
  - Mult. Inverse of e mod $\varphi(n)$
- Public Key: (n,e); Secret Key: (n,d)
- To encrypt message m: $c = m^e \pmod{n}$
- To decrypt ciphertext c: $m = c^d \pmod{n}$

The Attack

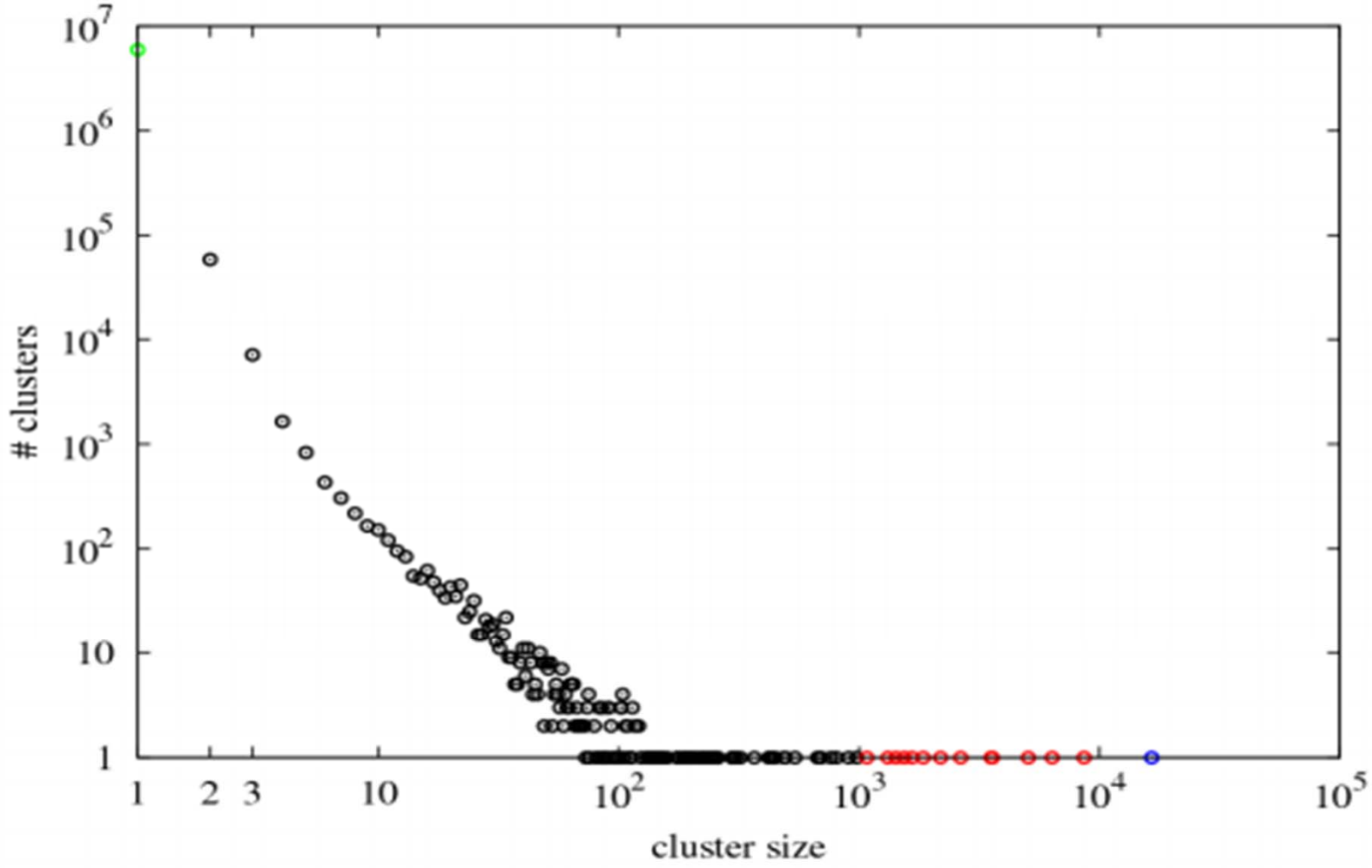


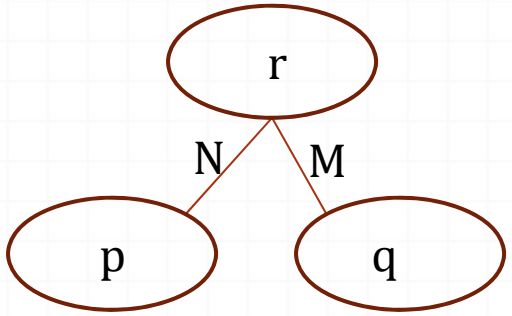
Fig. 2. Number of certificate clusters as a function of the cluster-size.

Why this is Bad

- If all keys use distinct primes, then graph of c distinct moduli should be c connected components
  - Each component a single edge connecting two unknown primes
- With the dataset ($c \approx 6$ million), found 1995 connected components with at least two edges. (RSA keys that share primes)
  - Footnote in paper: "We chose not to describe the details of our calculation"

Why this is Bad (cont'd)

- If a connected component is a depth-one tree, two moduli associated to edges in tree can be factored!
  - In this case, RSA secret key is computed.



- Once we factor a tree like this, we can start moving outward in the graph, dividing by primes we know.

The Calculation (Euclid's Algorithm)

- Example: $N_1 = 15$ $N_2 = 12$; $\gcd(N_1, N_2) = ?$
  - $15 / 12 = 1$
  - $15 - 12 * 1 = \mathbf{3}$
  - $12 / 3 = 4$
  - $12 - 4 * 3 = \mathbf{0}$
- If we know two RSA moduli share a prime, we can factor them this way.

It's less bad than it sounds

- .2% of RSA keys in the dataset fully factored.
- Most of these keys generated by embedded devices (routers, VPN endpoints, etc.)
  - These devices tend to generate keys on first boot
  - Not enough entropy to select primes that are "random enough"
- Device manufacturers contacted in order to start working on fixes.
- RSA not insecure, but bad randomness makes crypto insecure!

Bibliography

- A. Lenstra, J. Hughes, M. Augier, J. Bos, T. Kleinjung, C. Wachter. Ron was wrong, Whit is right. Cryptology ePrint Archive, Report 2012/064, 2012 http://eprint.iacr.org/2012/064.pdf
- New research: There's no need to panic over factorable keys-just mind your Ps and Qs: http://goo.gl/zOXJi
- Flaw Found in an Online Encryption Method: http://goo.gl/HYGCo
- Researchers crack online encryption system: http://goo.gl/KQKEH
- Researchers: Two in 1,000 RSA public keys are insecure: http://goo.gl/1hMml