Discussion: Remote Timing Attacks are Practical

600.624

2/11/05

Outline

- Why are timing attacks important?
- Clarifications
  - Zero-One Gap / Neighborhood Size etc.
- Problems
- Questions
- Extensions
- Contribution
- Discussion

How fast can we factor?

- Seny: RSAP. How do you go after crypto?
- RSA Challenge
  - RSA-576
    - 576 bits (174 digits)
    - Factored in 2 years (2001-2003) used "Lattice Sieving"
- http://www.rsasecurity.com/rsalabs/

How fast can we factor? (2)

- Number Field Sieves
  - "Fast Algorithms"
- Complexity:

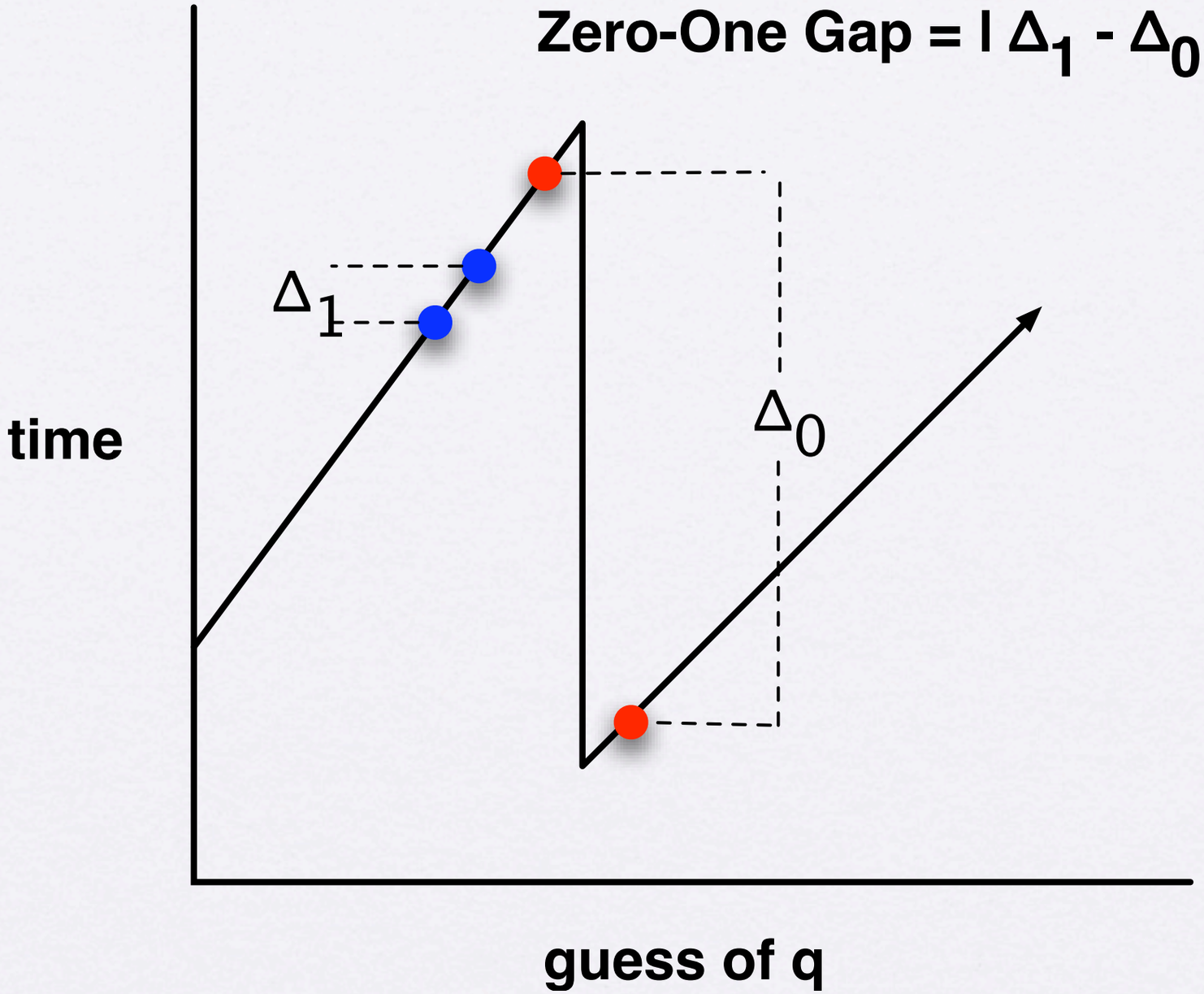
$$O(e^{c(\log n)^{1/3}(\log\log n)^{2/3}})$$

Dangers of Timing Attacks

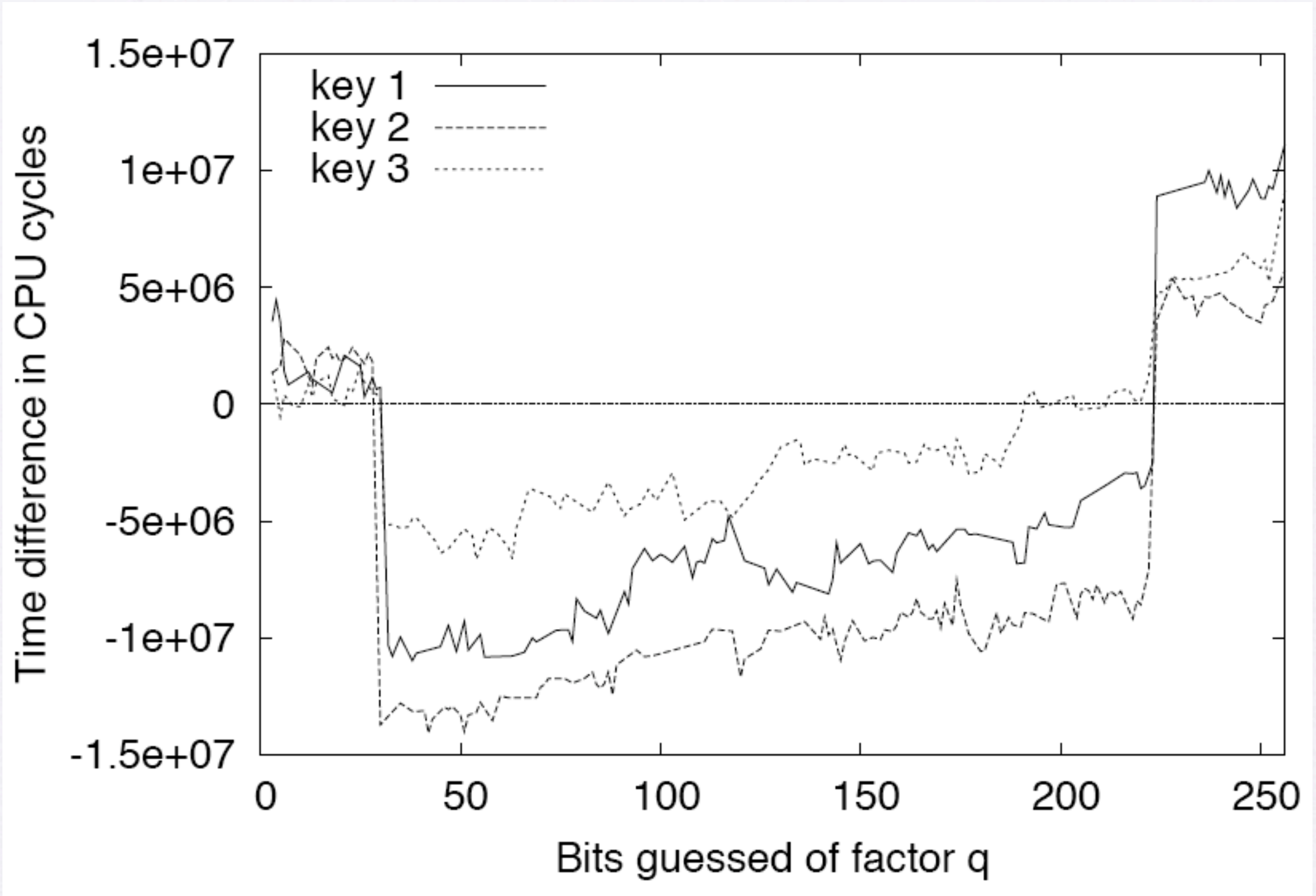
- Probably not going to crack RSA (or El Gamal) any time soon
- Dangers: Poor passwords (keys, entropy), timing attacks

Clarifications

What is the Zero-One Gap?



Zero-One Gap


1.5e+07
1e+07
5e+06
0
-5e+06
-1e+07
-1.5e+07
Time difference in CPU cycles
key 1
key 2
key 3
0
50
100
150
200
250
Bits guessed of factor q

What is the "neighborhood size"?

- Need to get better estimates at number of reductions (more on that later...)

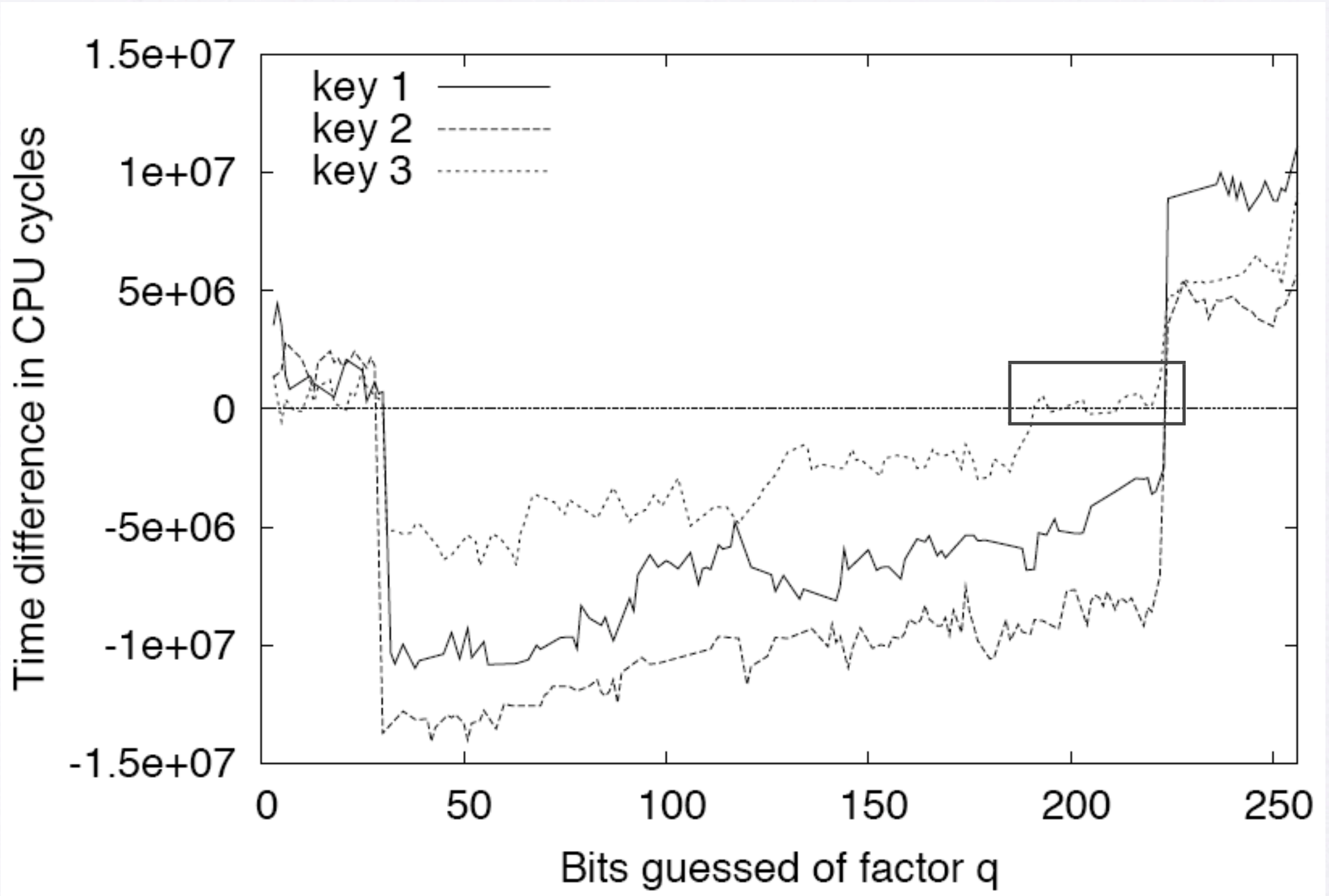
$$T_g = \sum_{1=0}^{n} \texttt{DecryptTime}(g + i)$$

$$T_{g_{hi}} = \sum_{1=0}^{n} \texttt{DecryptTime}(g_{hi} + i)$$

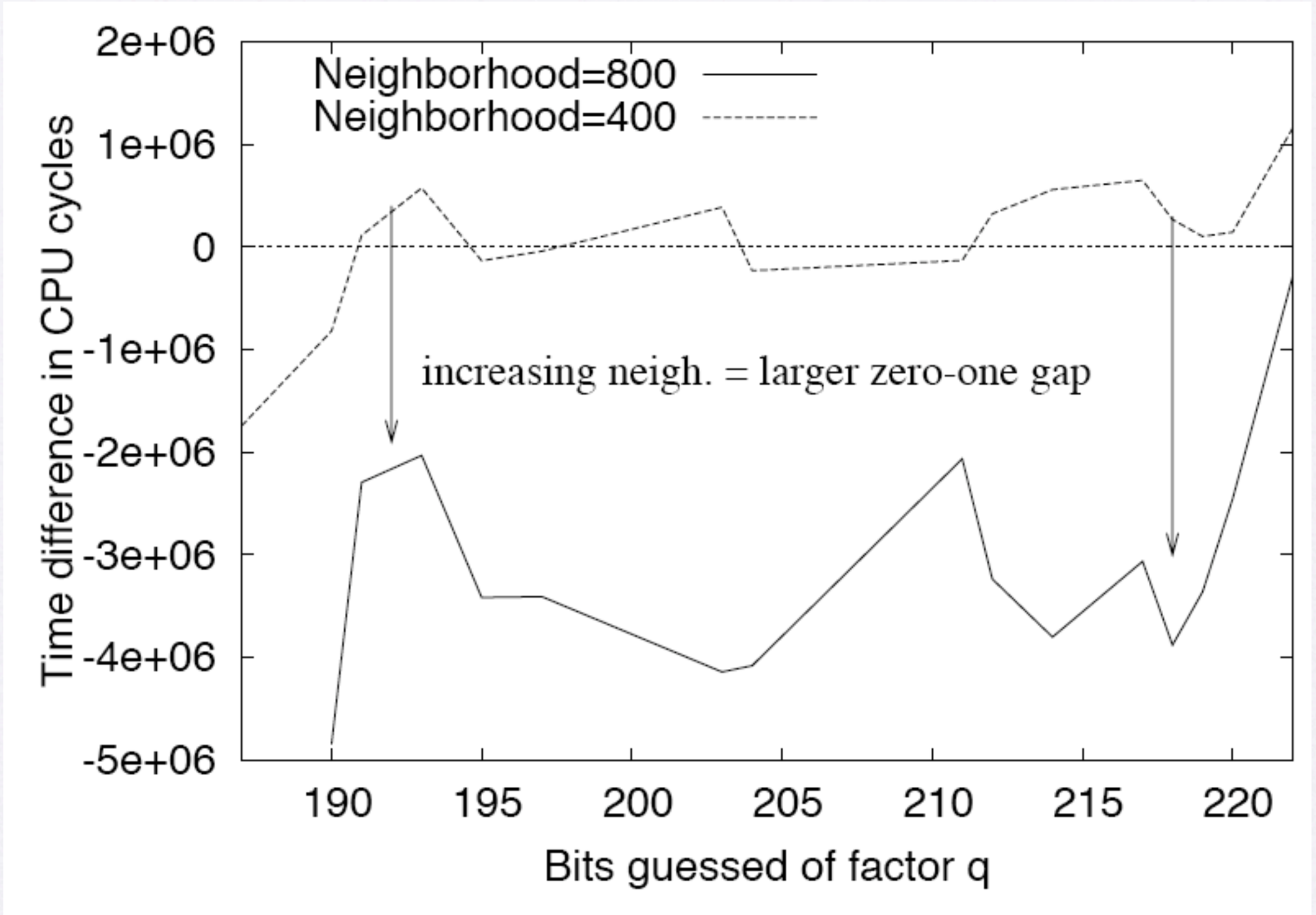
$$\Delta = |T_g - T_{g_{hi}}|$$

- Why increment *i*? (Multiplication??)

Neighborhood



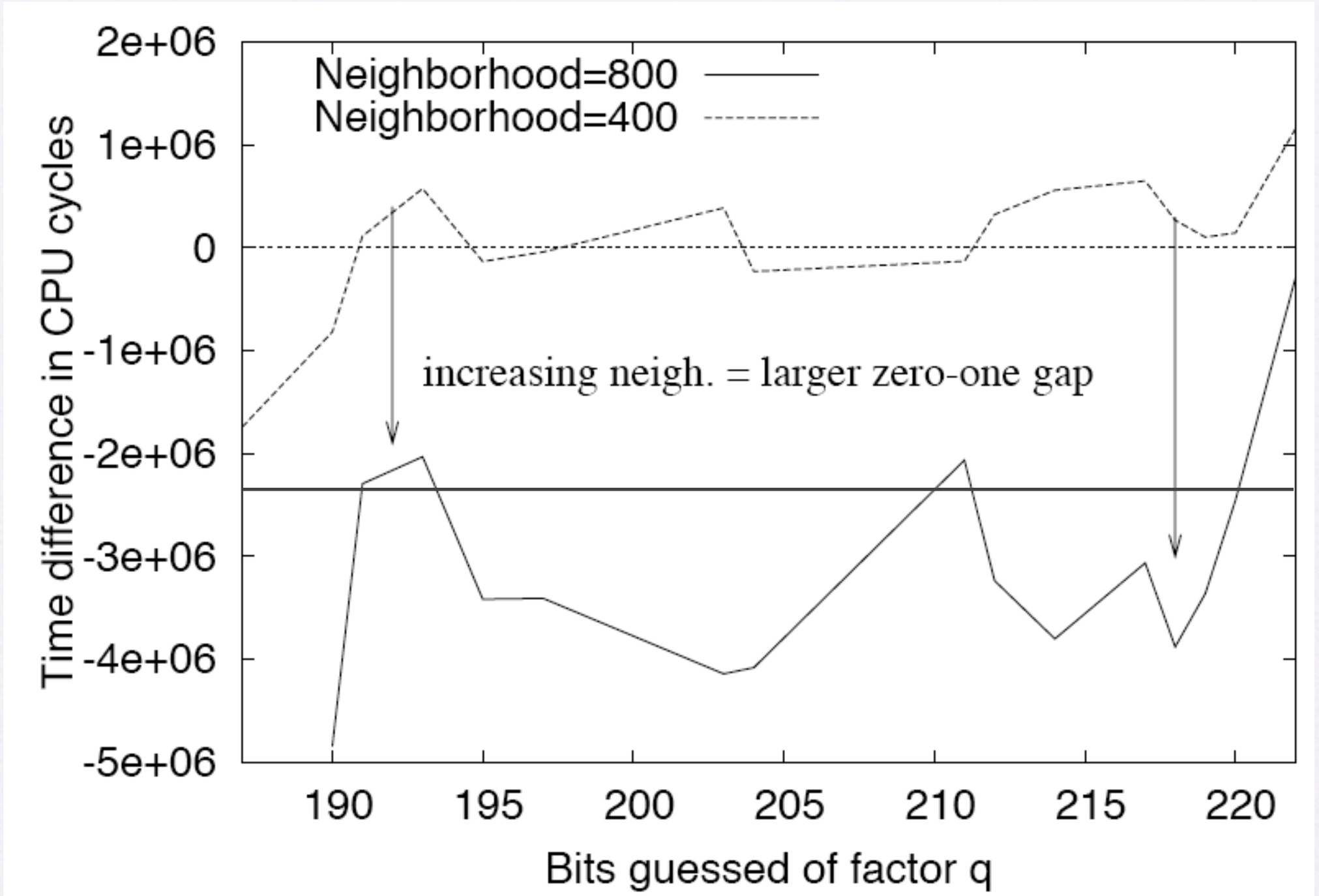
Neighborhood



1 ms?

- State that 1 ms of Zero-One Gap is sufficient for attack.
- Where did this number come from?

1 ms (2)



Can we really tolerate 1 ms network variance?

Problems

Great Paper! (?)

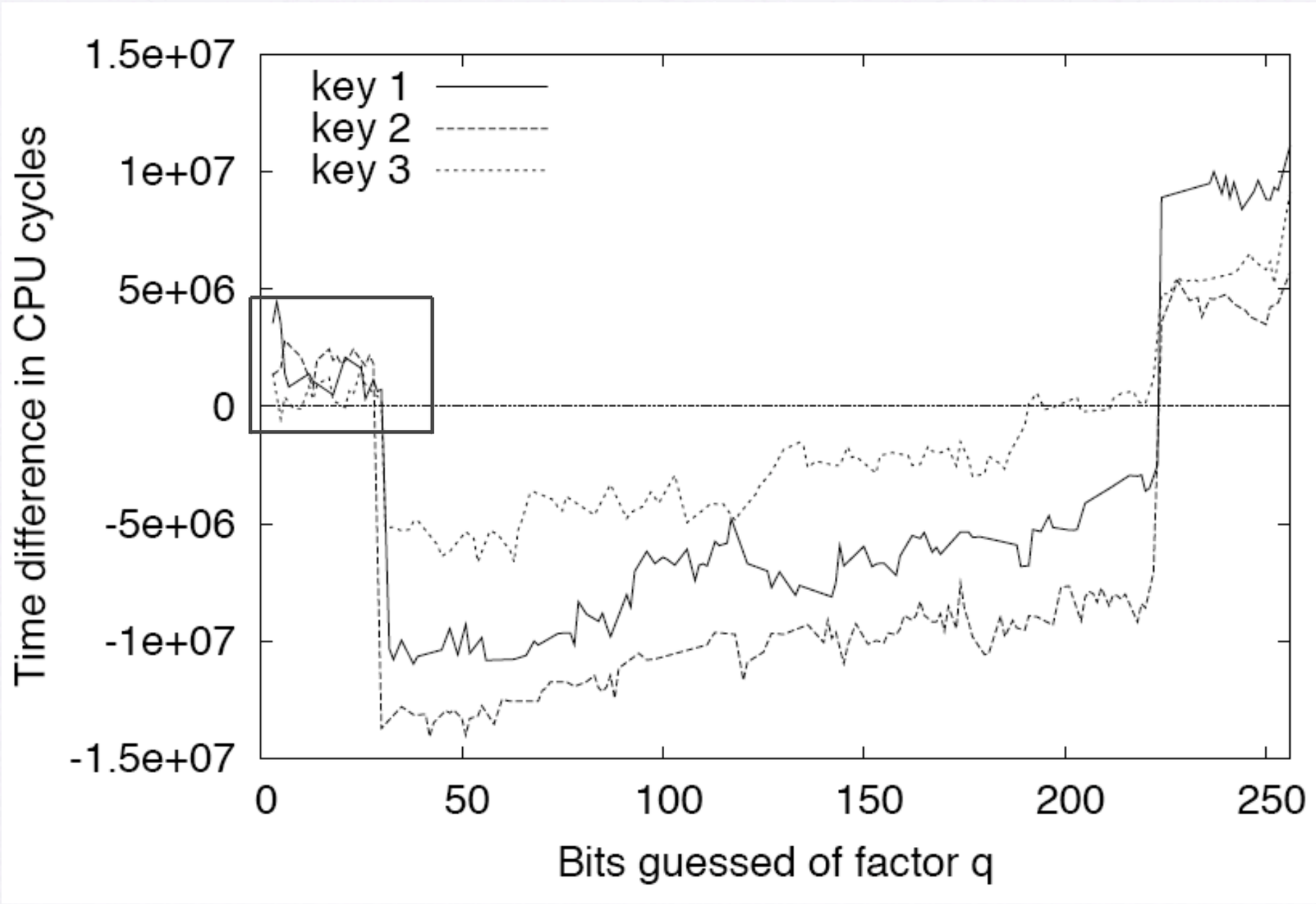
- Were the mathematics adequately explained?
- Did they provide empirical evidence that this attack is feasible?

“remote timing attacks are **PRACTICAL**”

- Setup:
  - 3 Hop Network
  - Load on the server
- Experiments:
  - broke 2.5/3 keys
  - sample size (?!?)
    - What does this mean for failure rate?

Questions

- What about the first bits?



Questions (2)

- Would using OAEP prevent the attack?
  - Quick Answer: no.
- What about RSA Signatures?
  - hashing?

Questions (3)

- Why include the VM Model?
  - Some people liked it...
- What is the failure rate?
  - Come back to this...

Questions (4)

- How are they averaging their timing samples?
- What does this imply about distribution?
- What does this mean about their error rate?

Defenses (″Hacks″)

- Queueing Algorithms
- Add a delay on decryption failure
- Application layer Firewall
- What about RSA batching?

Better Defenses (?)

- Blinding
  - “Are we wrong to rely on blinding considering it isn’t provably secure?”
- Quantizing

Extensions

- What is the smallest neighborhood/sample size parameters such that the attack will work?

Extensions (2)

- Are there p/q or e/d pairs for which Multiplication and Reductions offset? (See key 3.) If so, what percent of the key space is vulnerable? (HARD??)

Contribution

- We all accepted this paper... discuss why.

Discussion

- Anything you would like to bring up?