Key Recovery Attacks of Practical Complexity on AES Variants

Alex Biryukov, Orr Dunkelman, Nathan Keller,
Dmitry Khovratovich, Adi Shamir

Département d'Informatique
École Normale Supérieure

France Telecom Chaire

18 August 2009

Current State of Affairs in Cryptanalysis

Time complexity of a related-key attack:

"Thus, the total time complexity of Step 2(b) is about $2^{256} \cdot 2^{167.0} = 2^{423.0}$ SHACAL-1 encryptions."

- Most cryptanalytic papers discuss certificational attacks.

Current State of Affairs in Cryptanalysis

Time complexity of a related-key attack:

"Thus, the total time complexity of Step 2(b) is about $2^{256} \cdot 2^{167.0} = 2^{423.0}$ SHACAL-1 encryptions."

- Most cryptanalytic papers discuss certificational attacks.
- These attacks are of great importance, but they do not help answering questions by users:
  1. Does this attack affect my system?
  2. Should I still use AES-256 for encryption?
  3. MD5 is still OK for certificates, right?

What a Break is?

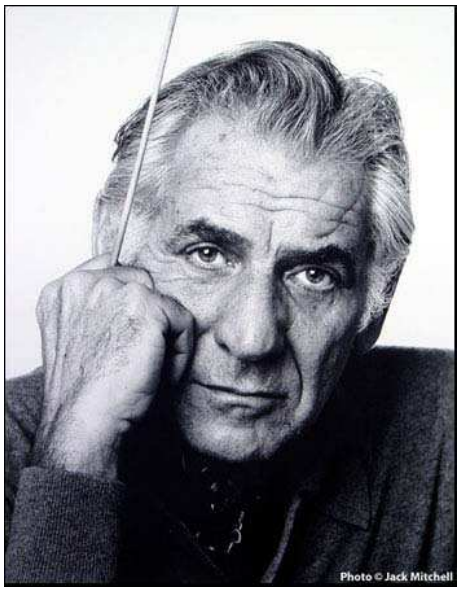
- There are several approaches towards what constitutes a certificational break.
- One approach: max(Time, Data, Memory) less than Exhaustive search' time.
- Another approach: (Time, Data, Memory) better then generic attacks.

A New Metric

- Time $\times$ Memory $<$ Exhaustive search.

A New Metric

- Time $\times$ Memory $<$ Exhaustive search.



Leonard Bernstein

A New Metric

- Time $\times$ Memory $<$ Exhaustive search.

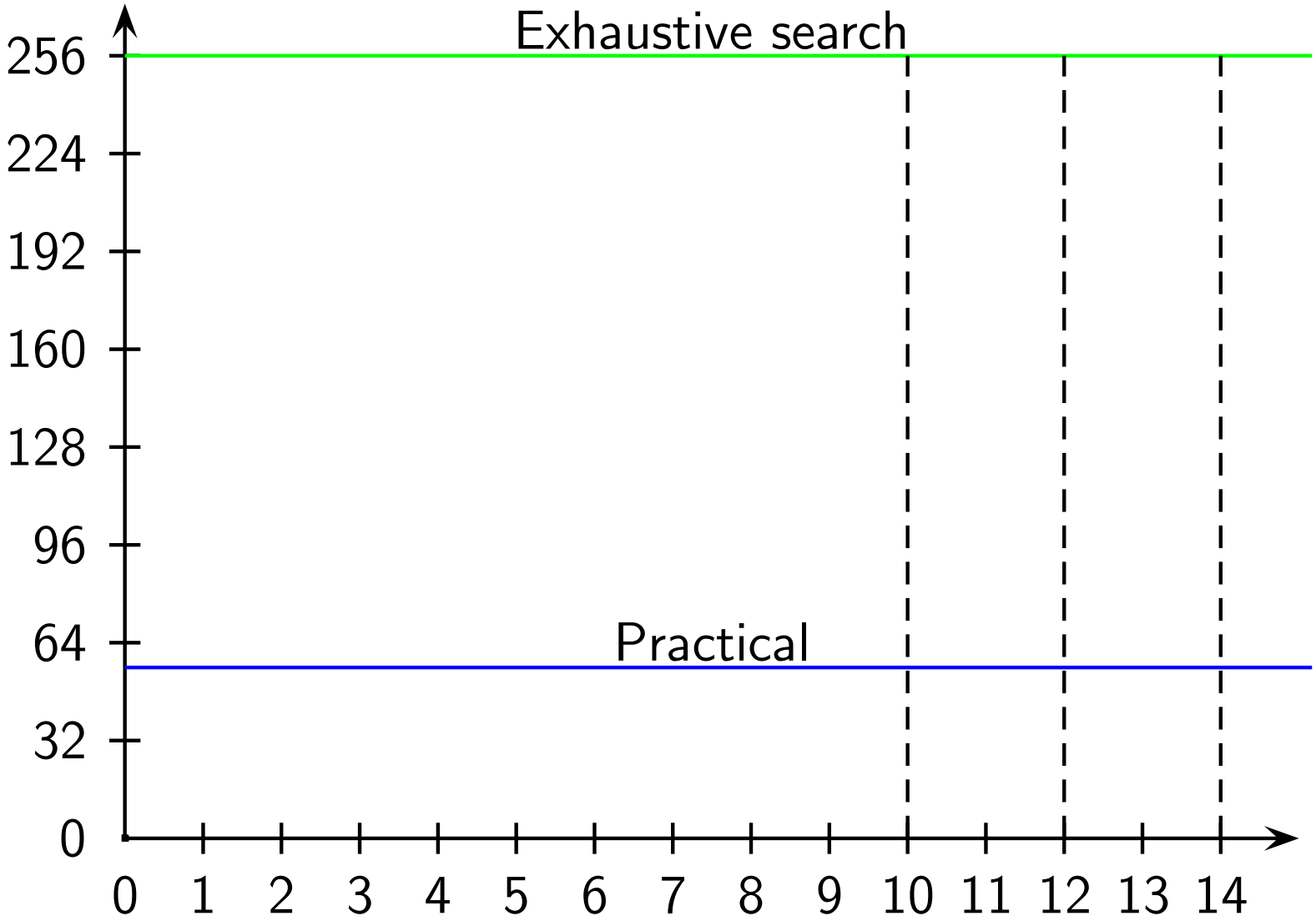
Lev Davidovich Bronstein
(Leon Trotsky)

A New Metric

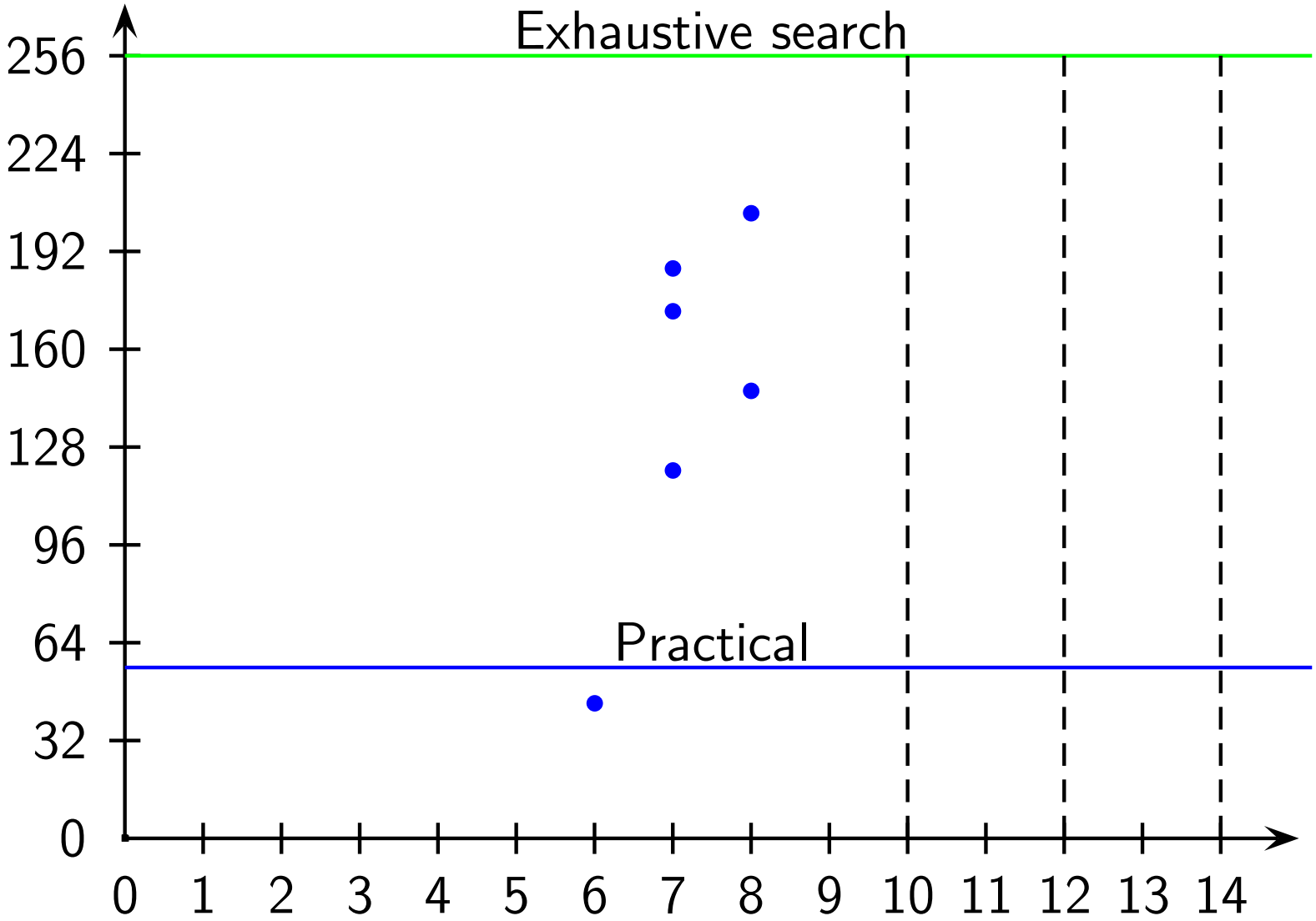
- Time $\times$ Memory $<$ Exhaustive search.

Daniel J. Bernstein

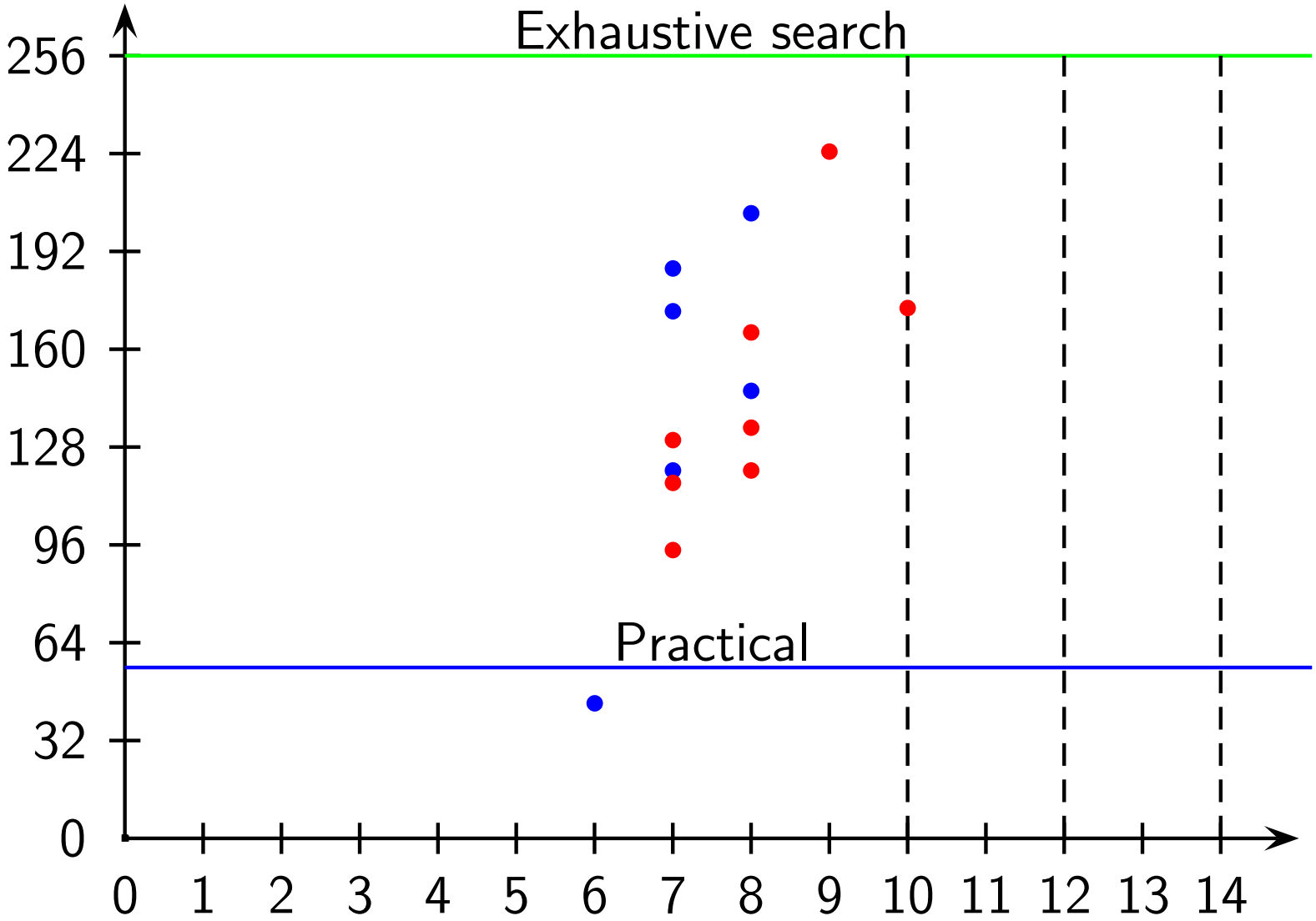
Time Complexity of Attacks on AES-256



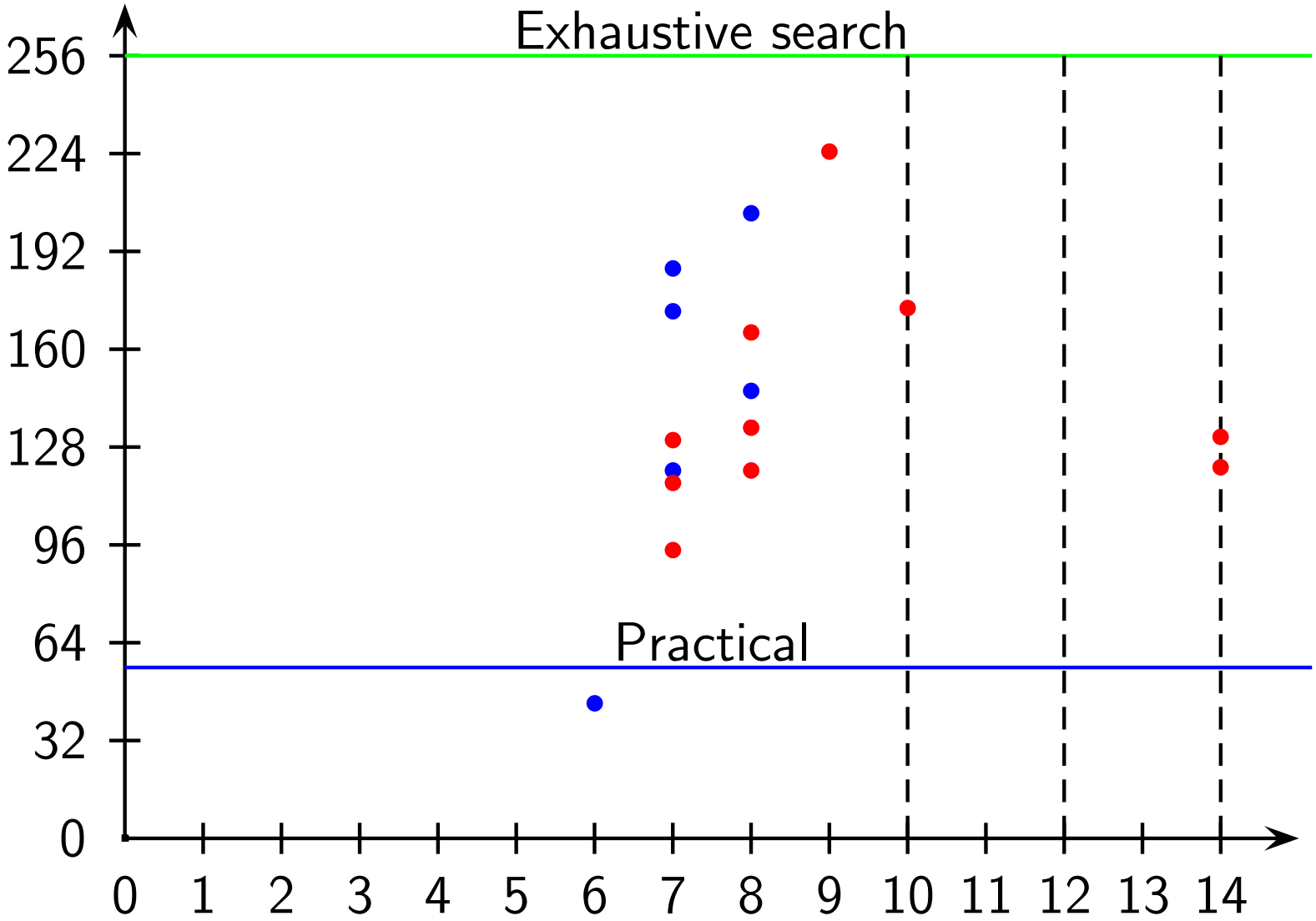
Time Complexity of Attacks on AES-256



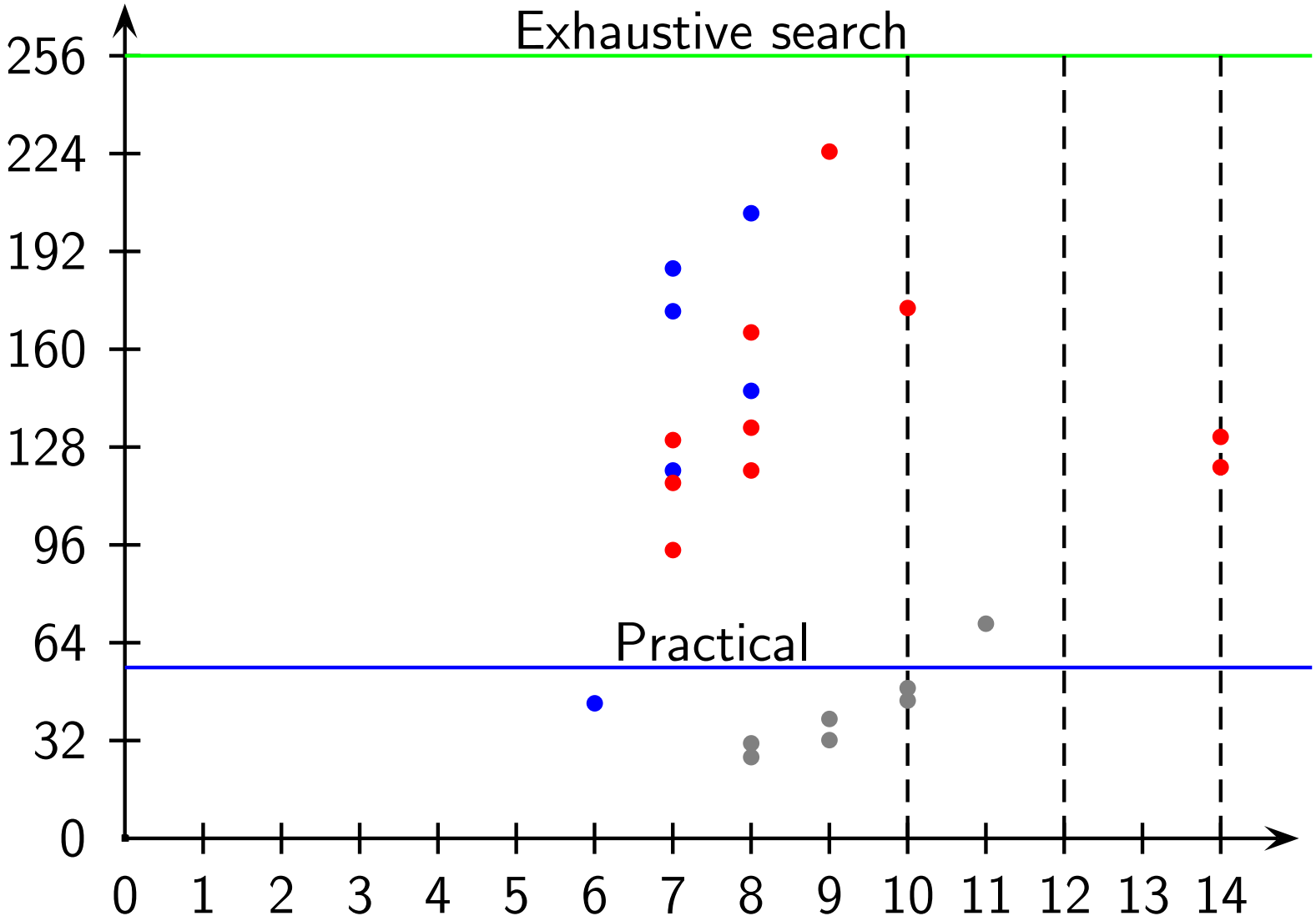
Time Complexity of Attacks on AES-256



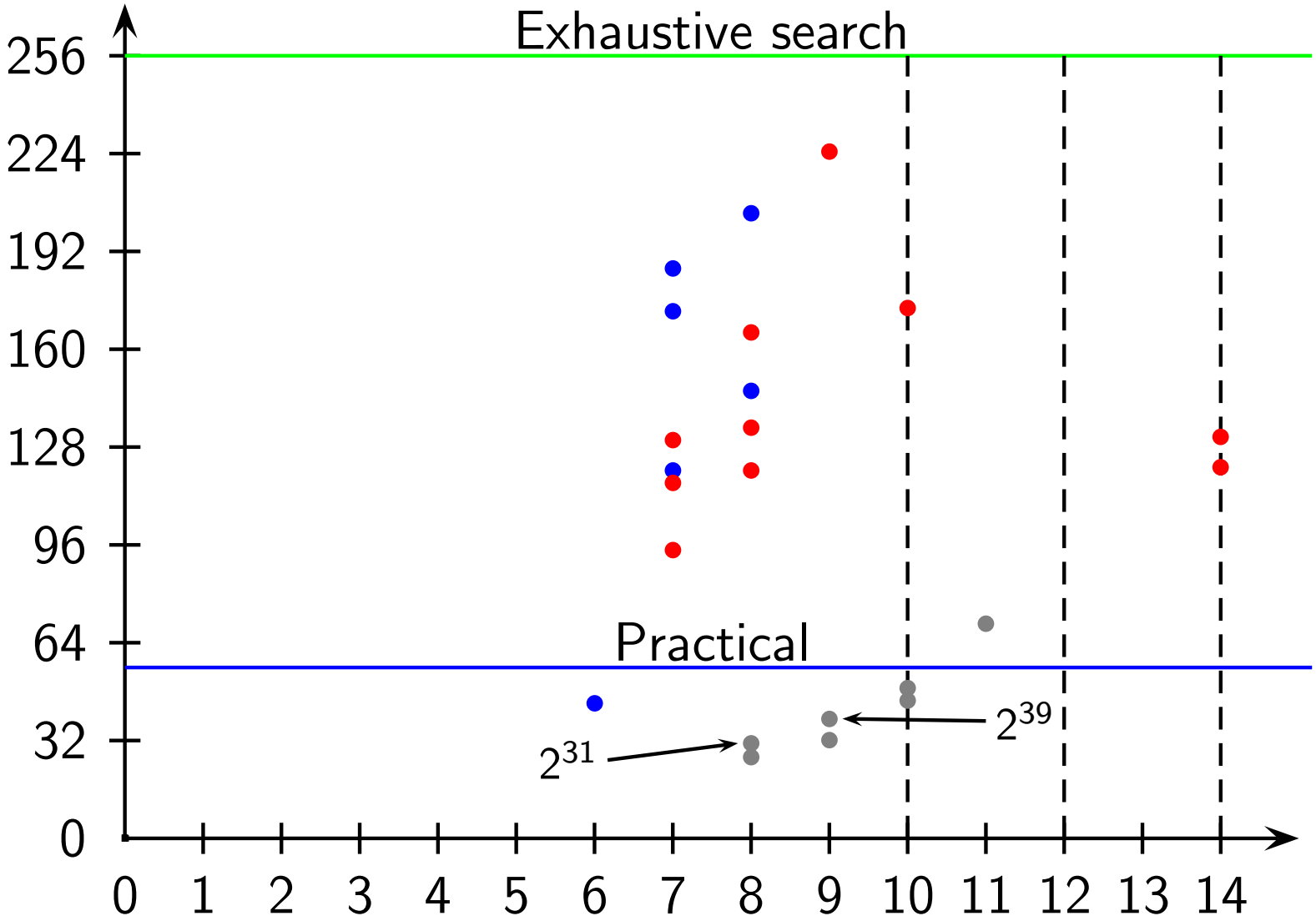
Time Complexity of Attacks on AES-256



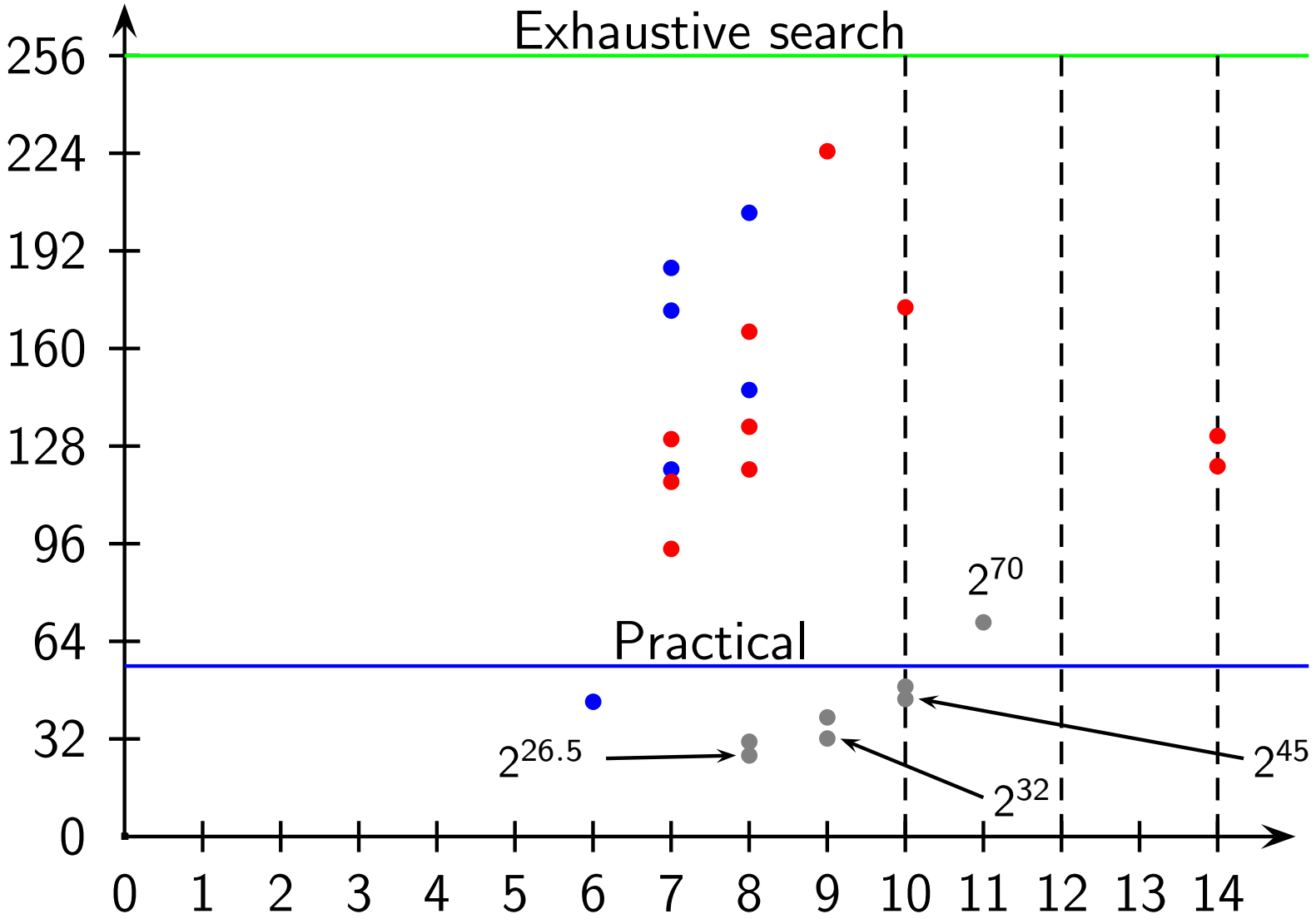
Time Complexity of Attacks on AES-256



Time Complexity of Attacks on AES-256

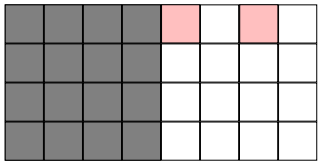


Time Complexity of Attacks on AES-256

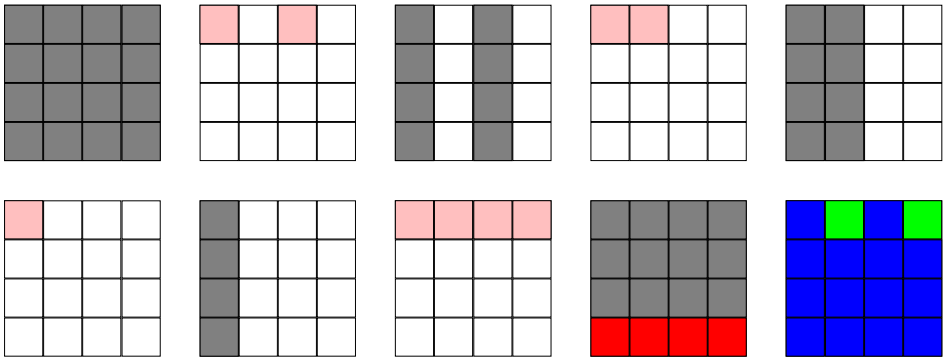


Key Schedule Algorithm of AES-256

Our results are based on the fact that key difference



leads to the 10 subkey differences



With probability 1!

Attacks

Rounds	Scenario	Time	Data	Memory	Result
8	Key Diff. – CP	2^{31}	2^{31}	2	Distinguisher
8	Subkey Diff. – CC	$2^{26.5}$	$2^{26.5}$	$2^{26.5}$	35 subkey bits
9	Key Diff. – CP	2^{39}	2^{38}	2^{32}	Full key
9	Subkey Diff. – CC	2^{32}	2^{32}	2^{32}	56 key bits
10	Subkey Diff. – CP	2^{49}	2^{48}	2^{33}	Distinguisher
10	Subkey Diff. – CC	2^{45}	2^{44}	2^{33}	35 subkey bits

Security Implications

- Extending AES-128 key to 256 bits actually reduces security!
- The security margins are smaller than expected.

Security Implications

- Extending AES-128 key to 256 bits actually reduces security!
- The security margins are smaller than expected.
- This is a good time to check that Serpent-support...

Conclusions

- Did we break the full AES with practical complexity?

Conclusions

- Did we break the full AES with practical complexity?

Conclusions

- Did we break the full AES with practical complexity?
- Should users be worried?

Conclusions

- Did we break the full AES with practical complexity?
- Should users be worried?

Questions?

Thank you for your attention!

The paper is available on eprint (2009/374)