Improved Single-Key Attacks on 8-round AES

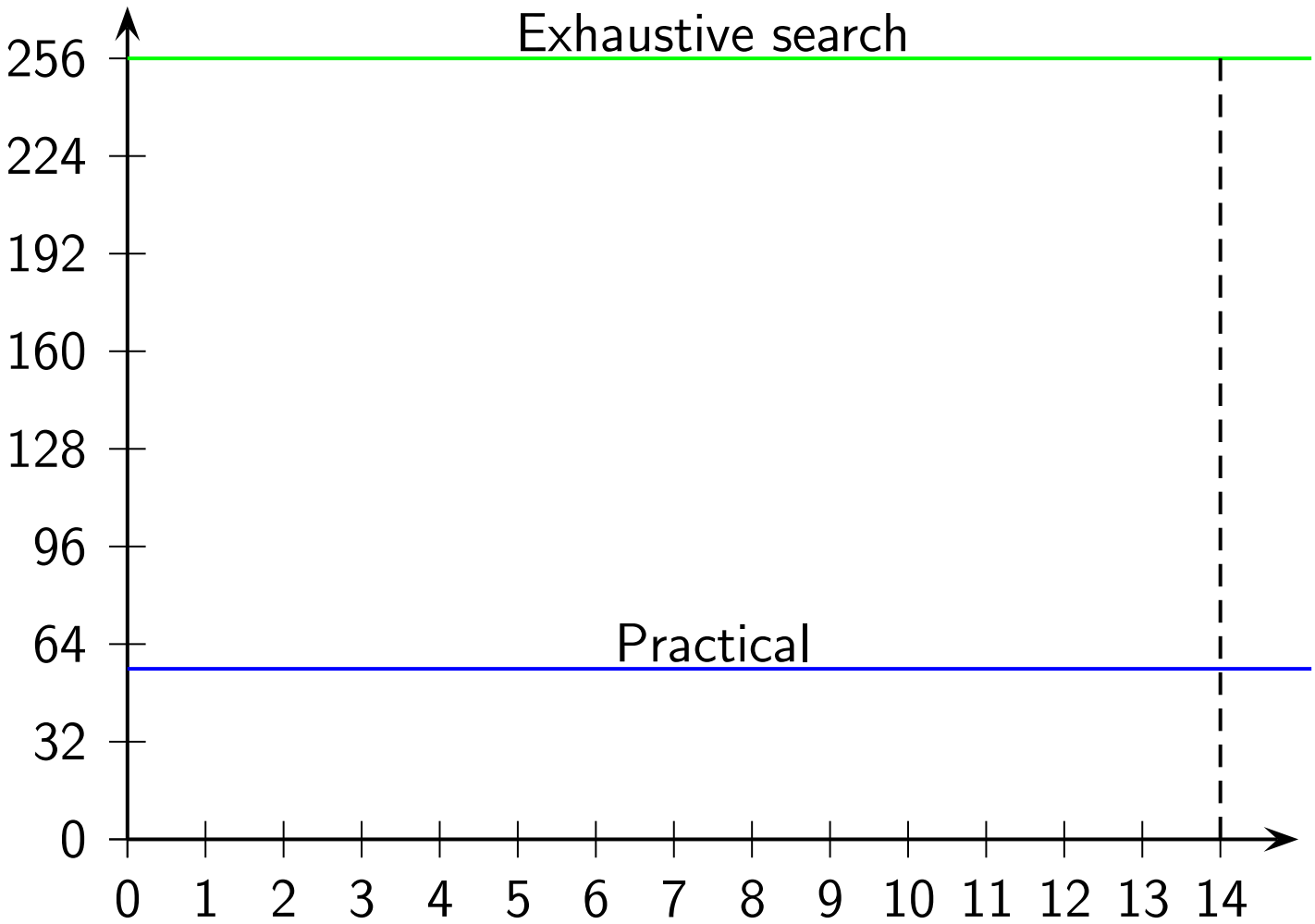
Orr Dunkelman, Nathan Keller, Adi Shamir

Faculty of Mathematics and Computer Science
Weizmann Institute of Science

June 1st, 2010

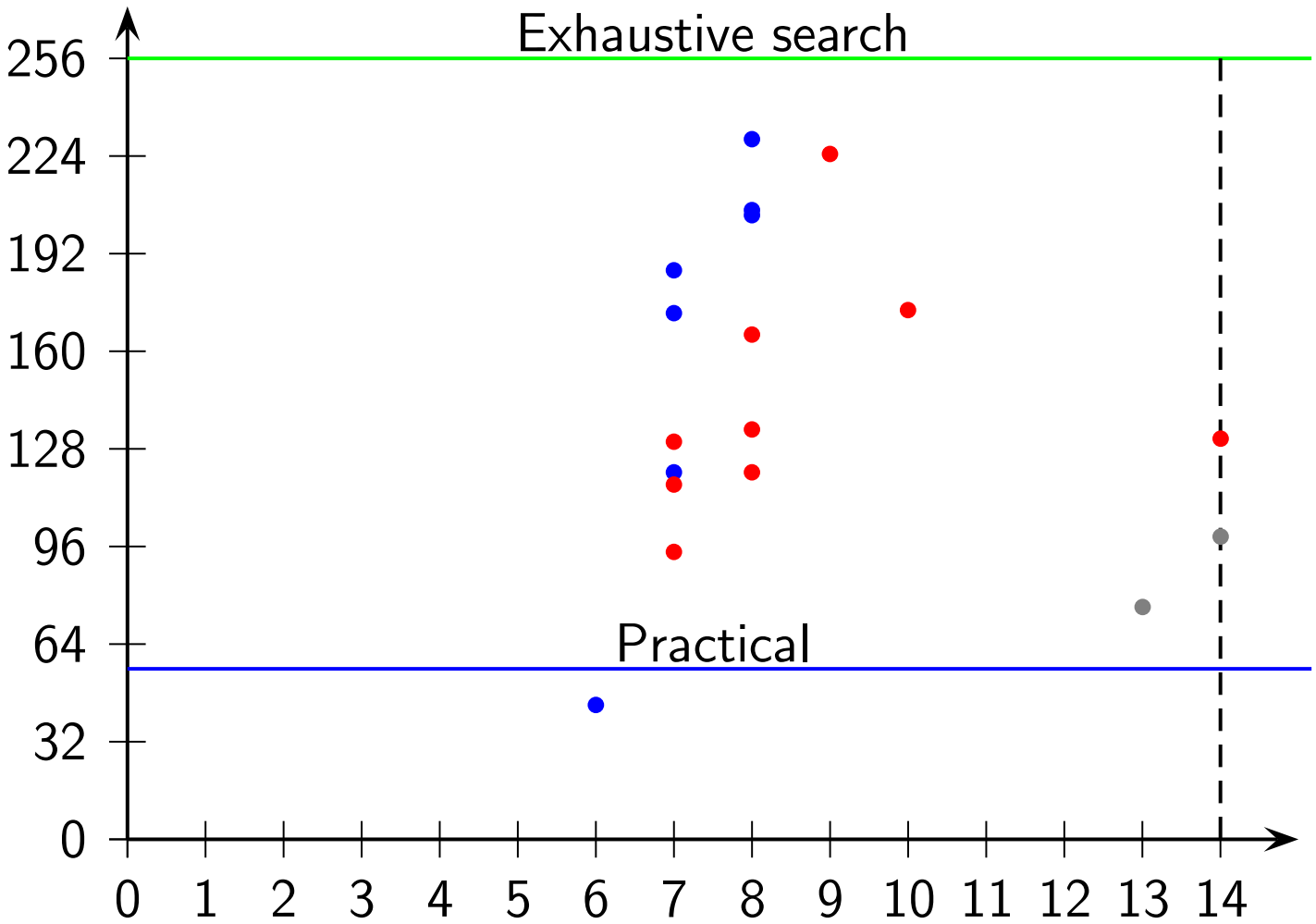
מכון ויצמן למדע
WEIZMANN INSTITUTE OF SCIENCE

Attacks on AES-256



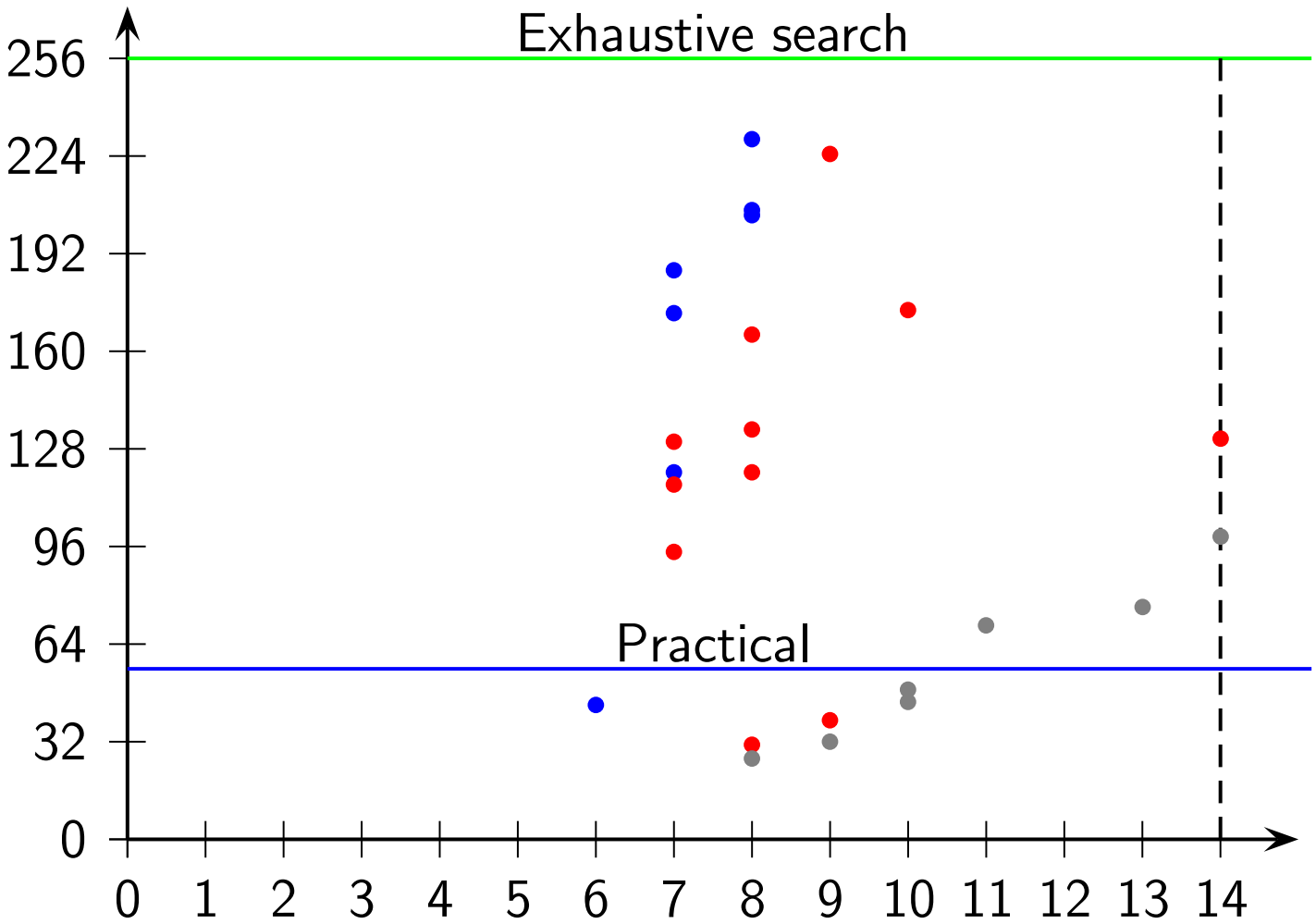
Blue — single key, Red — related-key, Gray — related-subkey

Attacks on AES-256



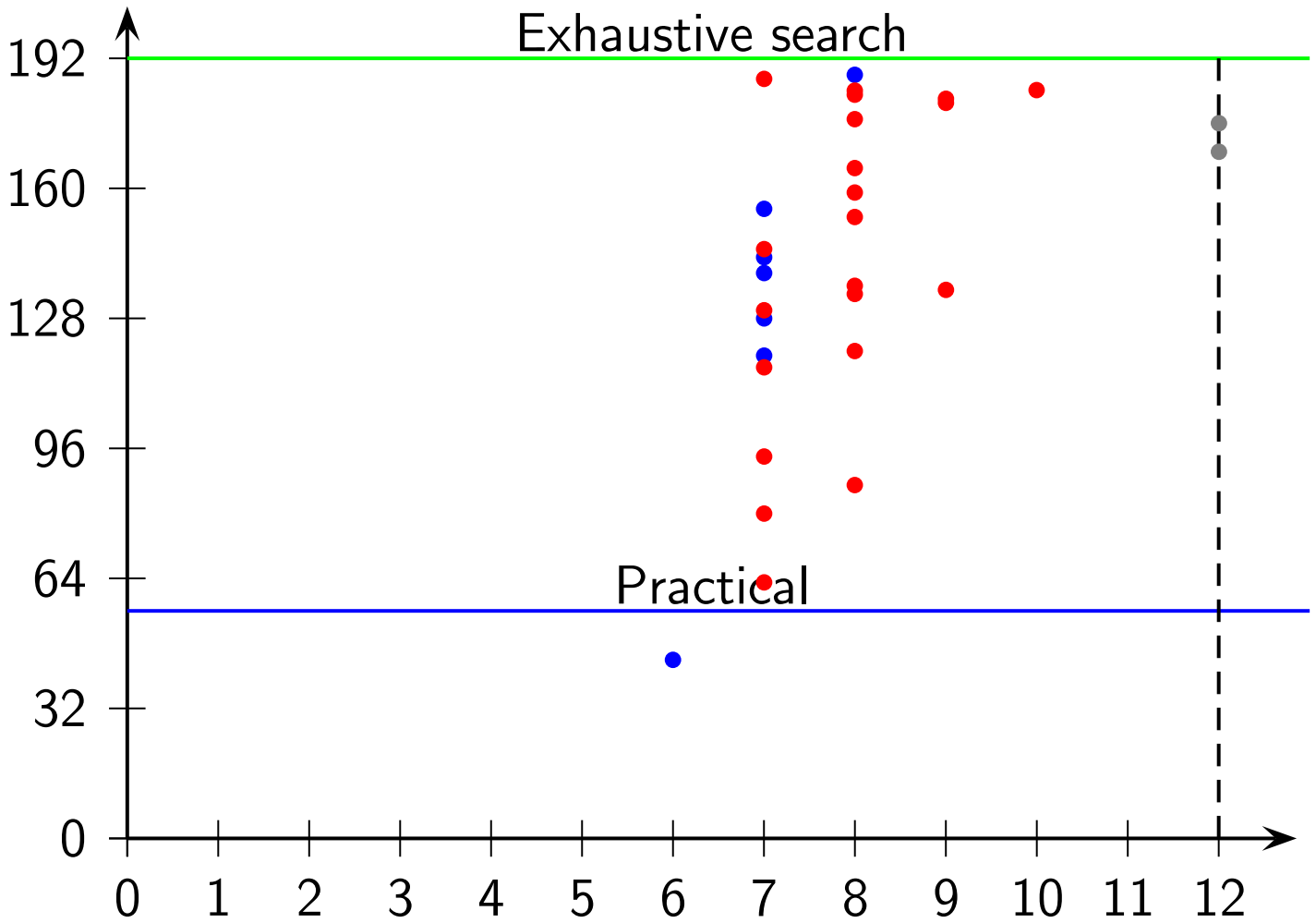
Blue — single key, Red — related-key, Gray — related-subkey

Attacks on AES-256



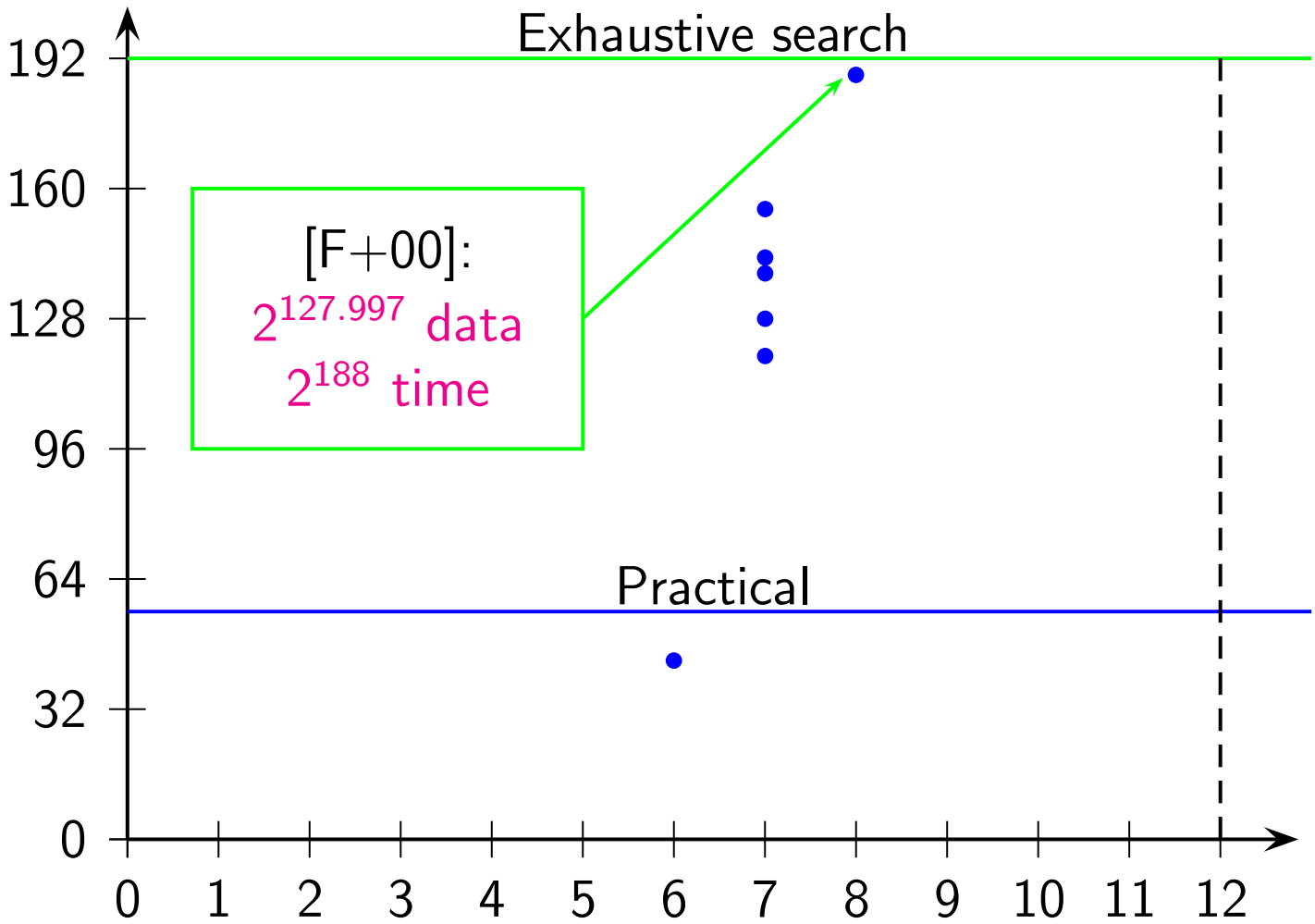
Blue — single key, Red — related-key, Gray — related-subkey

Attacks on AES-192



Blue — single key, Red — related-key, Gray — related-subkey

Attacks on AES-192



Blue — single key, Red — related-key, Gray — related-subkey

The Belgian Defense

- The attacks are in the *Related-Subkey* model.
- The attacks have no meaning when dealing with encryption.
- The most successful attacks are in the adaptive chosen plaintext and ciphertext model.
- The practical attacks are not on the full cipher.

Back to the Basics

- Consider single key attacks.
- Best (in term of rounds) attacks:

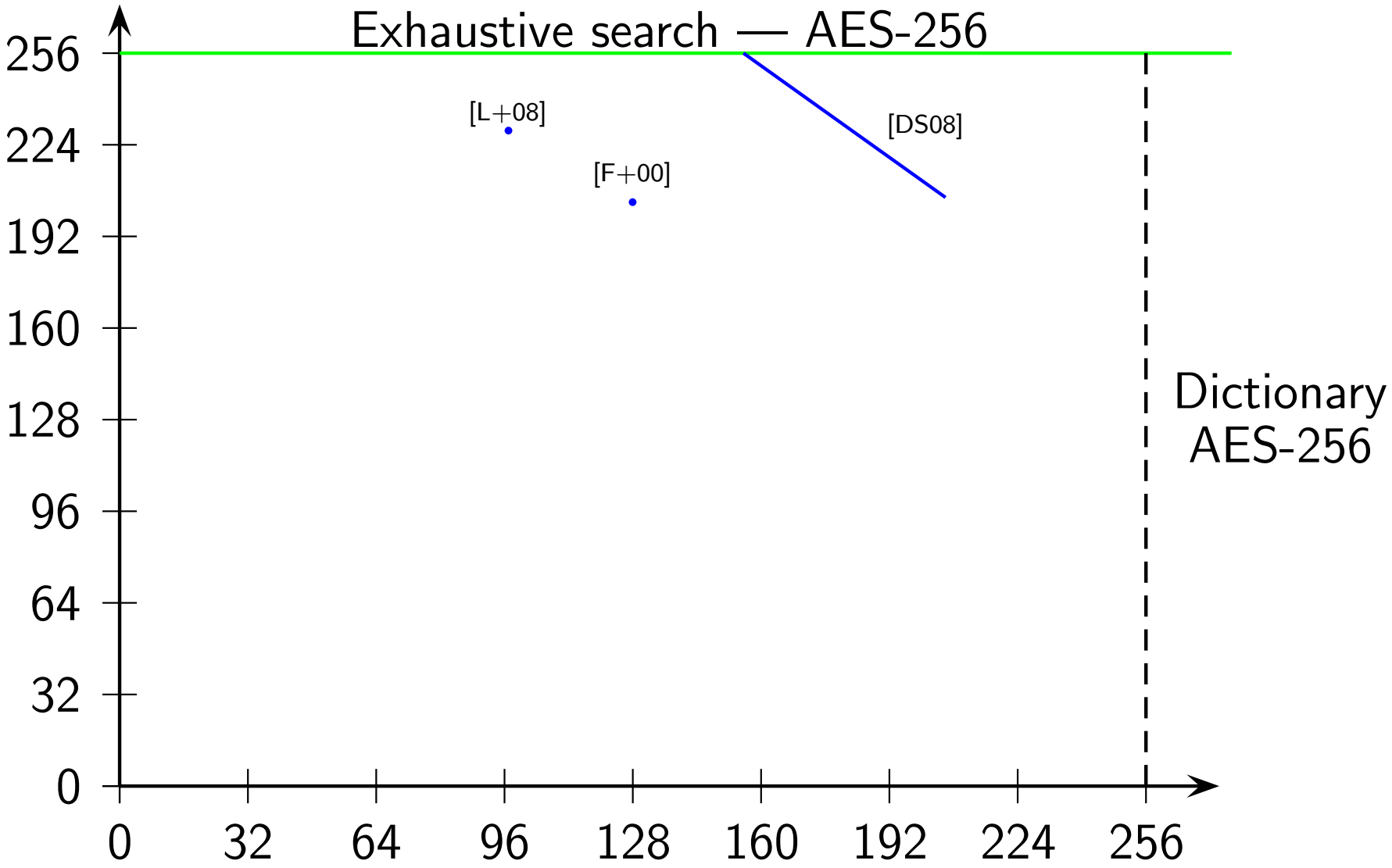
Version	Rounds	Data	Time	Memory	Ref.
AES-128	7	$2^{112.2}$	$2^{117.2}$	$2^{112.2}$	[L+08]
AES-192	8	$2^{127.997}$	2^{188}	2^{128}	[F+00]
AES-256	8	$2^{127.997}$	2^{204}	2^{128}	[F+00]

An Interesting Flavour of Attacks on AES

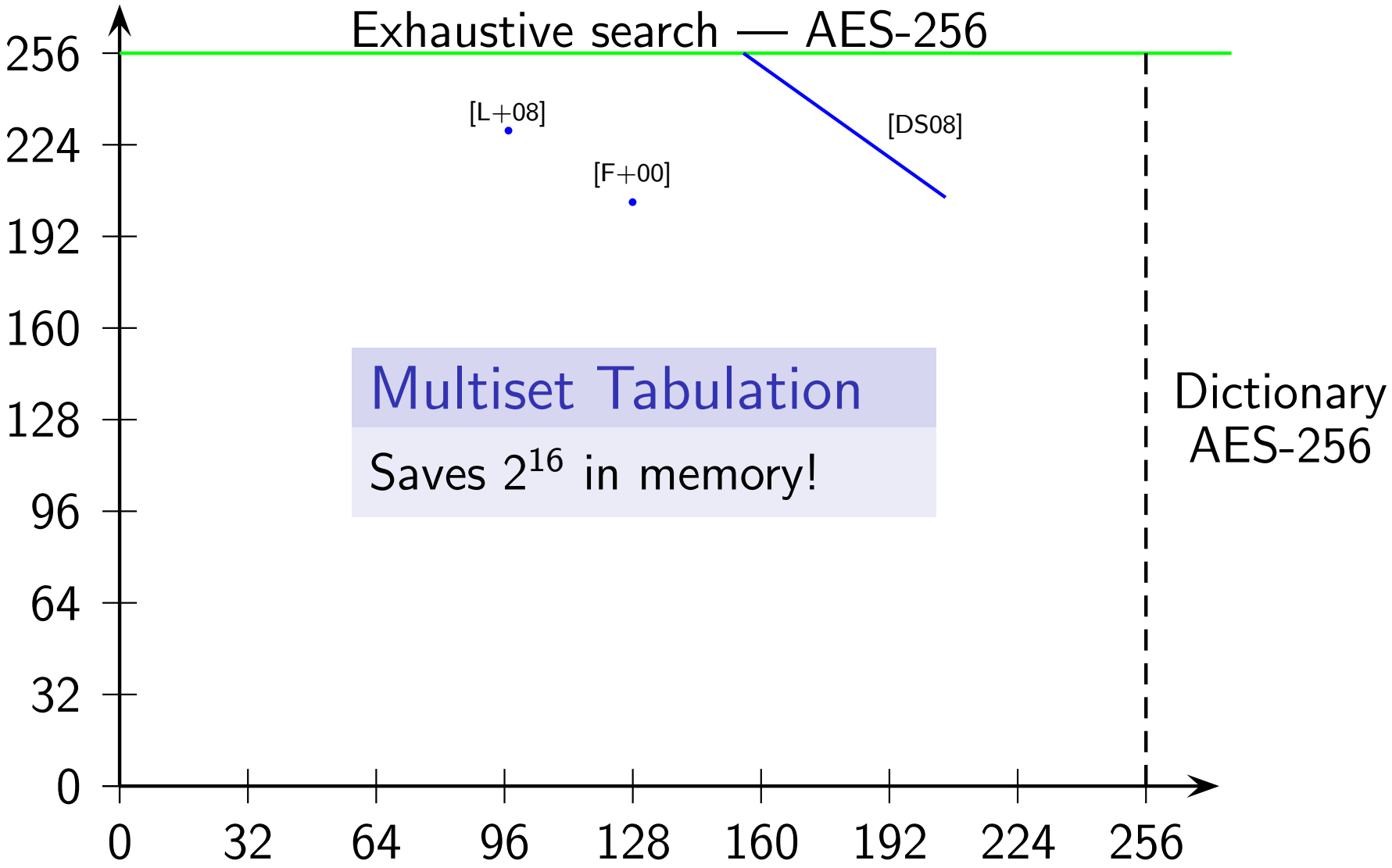
- Take Demirci-Selçuk's attack from FSE'08 (which in itself is based on Gilbert-Minier's attack from AES3)

Rounds	Data	Memory (Pre)	Time	MinMax	Ref.
7	2^{34+n}	2^{204-n}	2^{82+n}	2^{143}	[DS08]
8	2^{34+n}	2^{206-n}	$2^{205.6+n}$	$2^{205.8}$	[DS08]
8	$2^{34+\max(n-24,0)}$	2^{208-n}	2^{206+n} MA	2^{208}	[D+09]

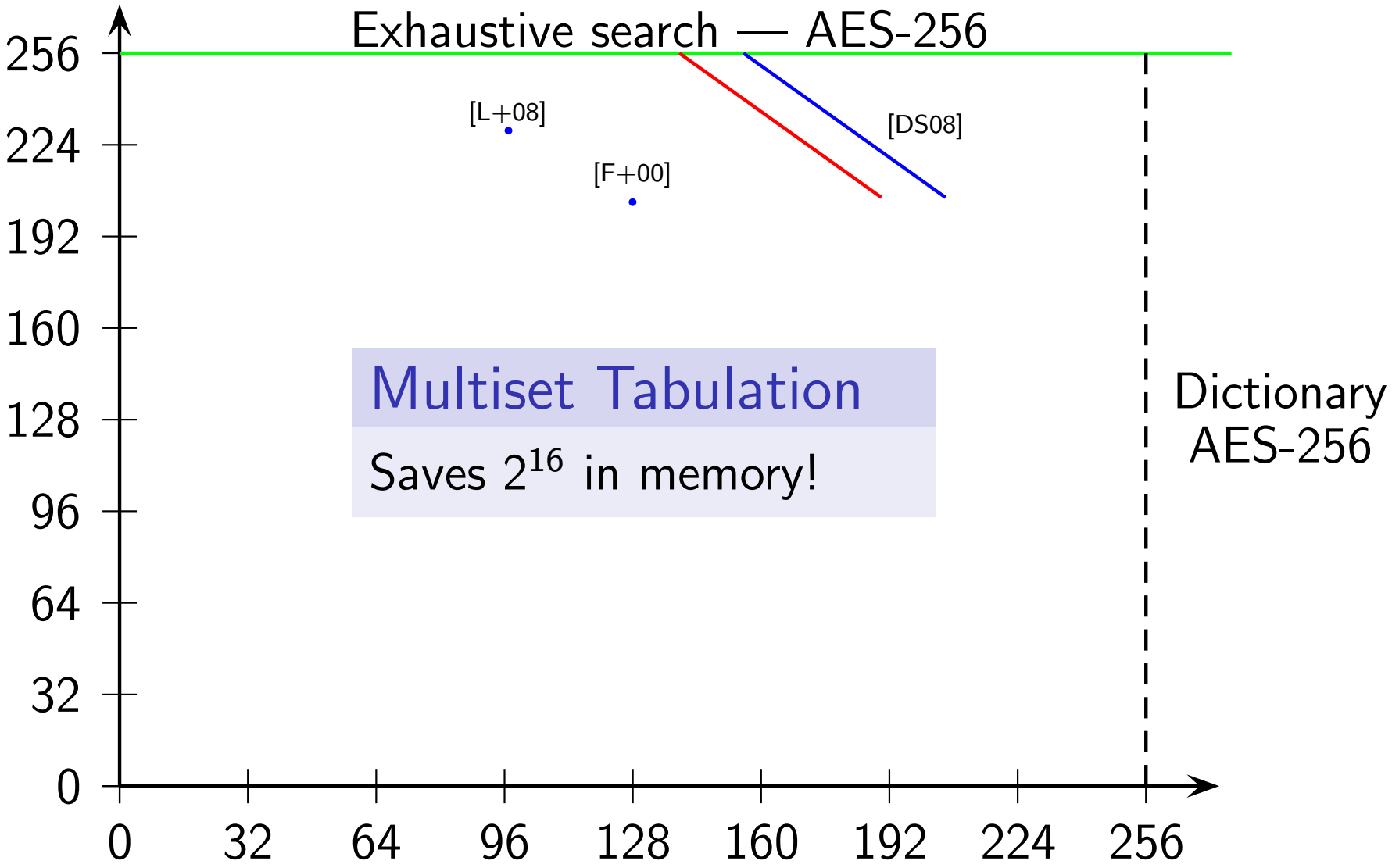
8-Round Single-Key Attacks on AES



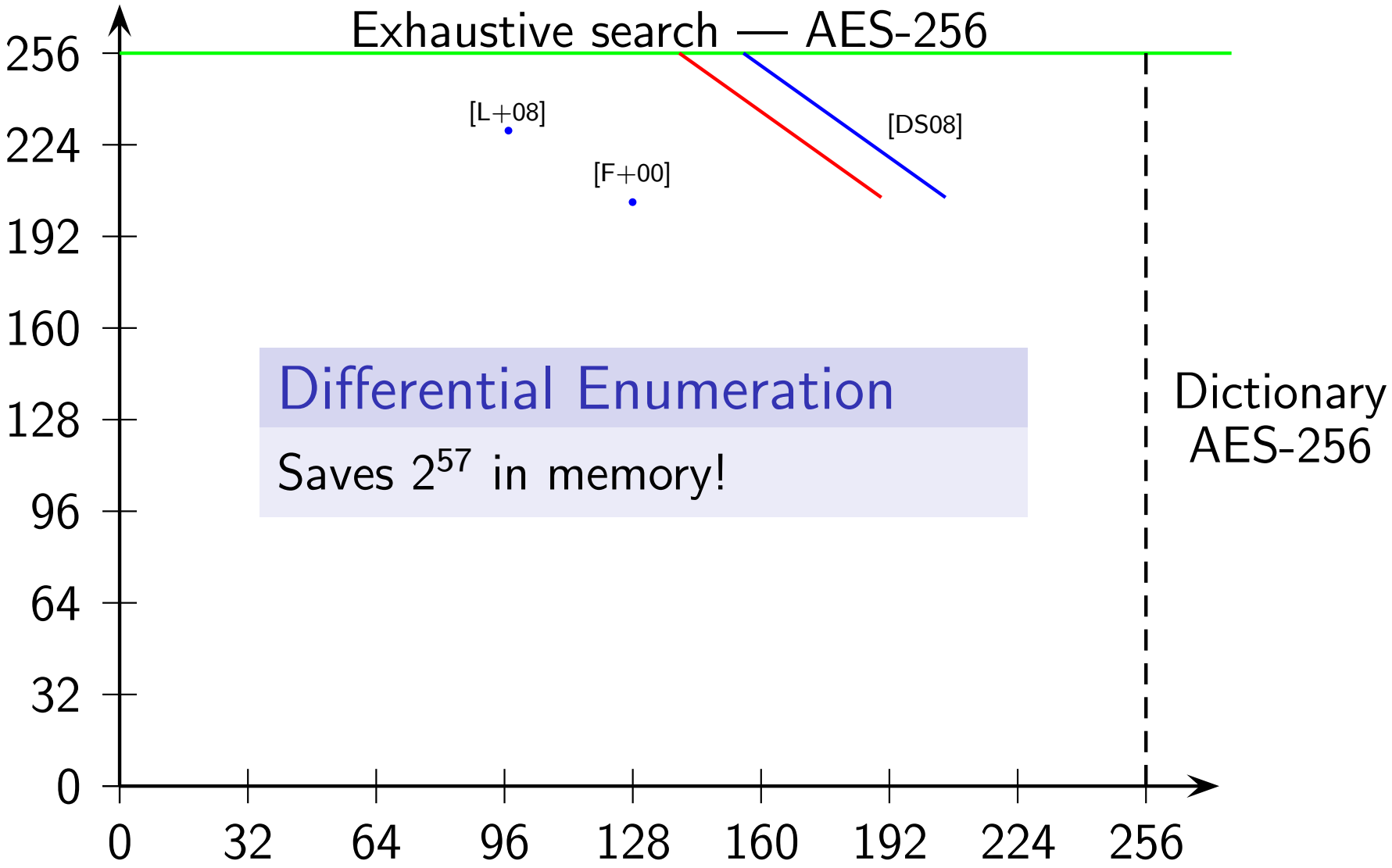
8-Round Single-Key Attacks on AES



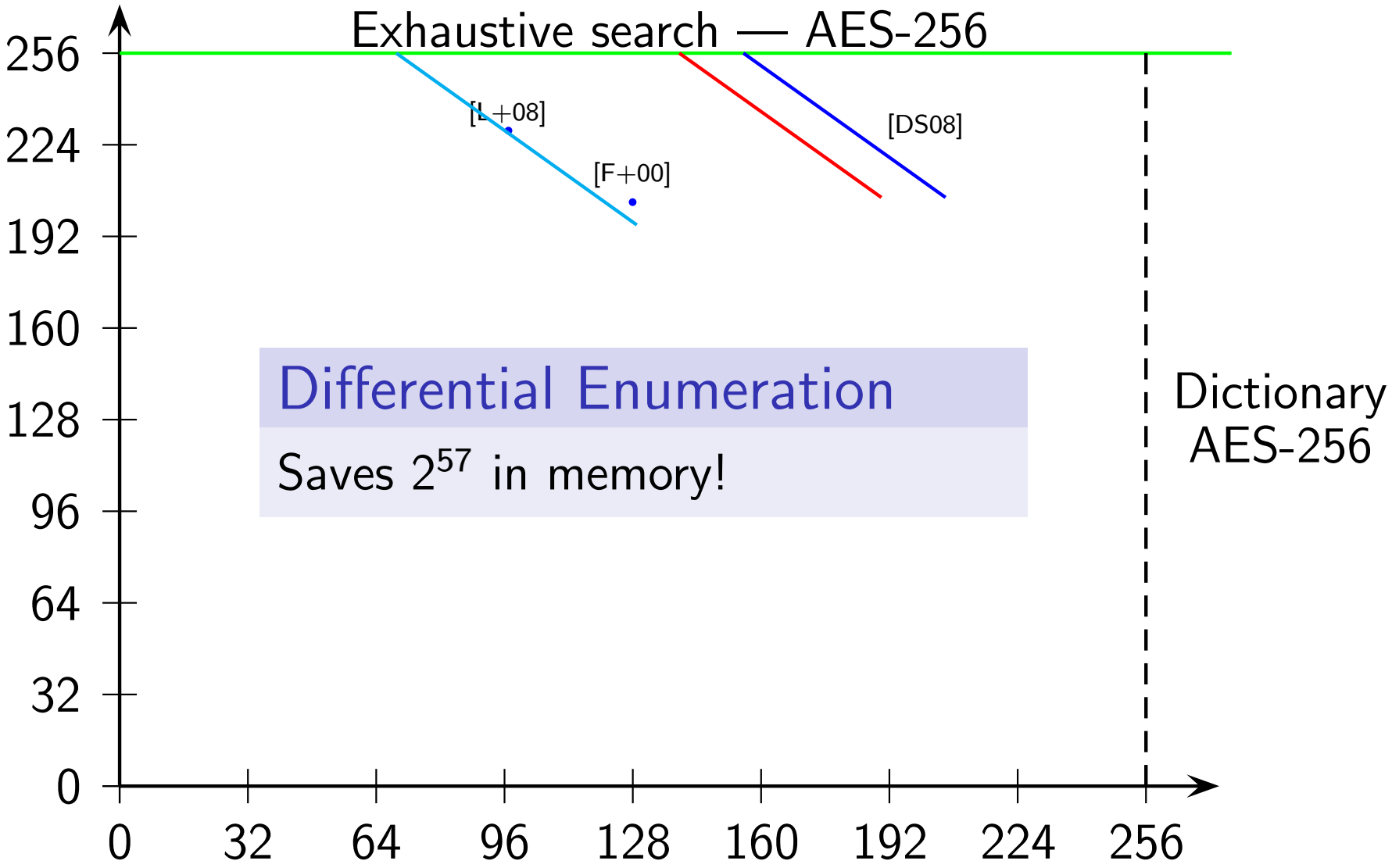
8-Round Single-Key Attacks on AES



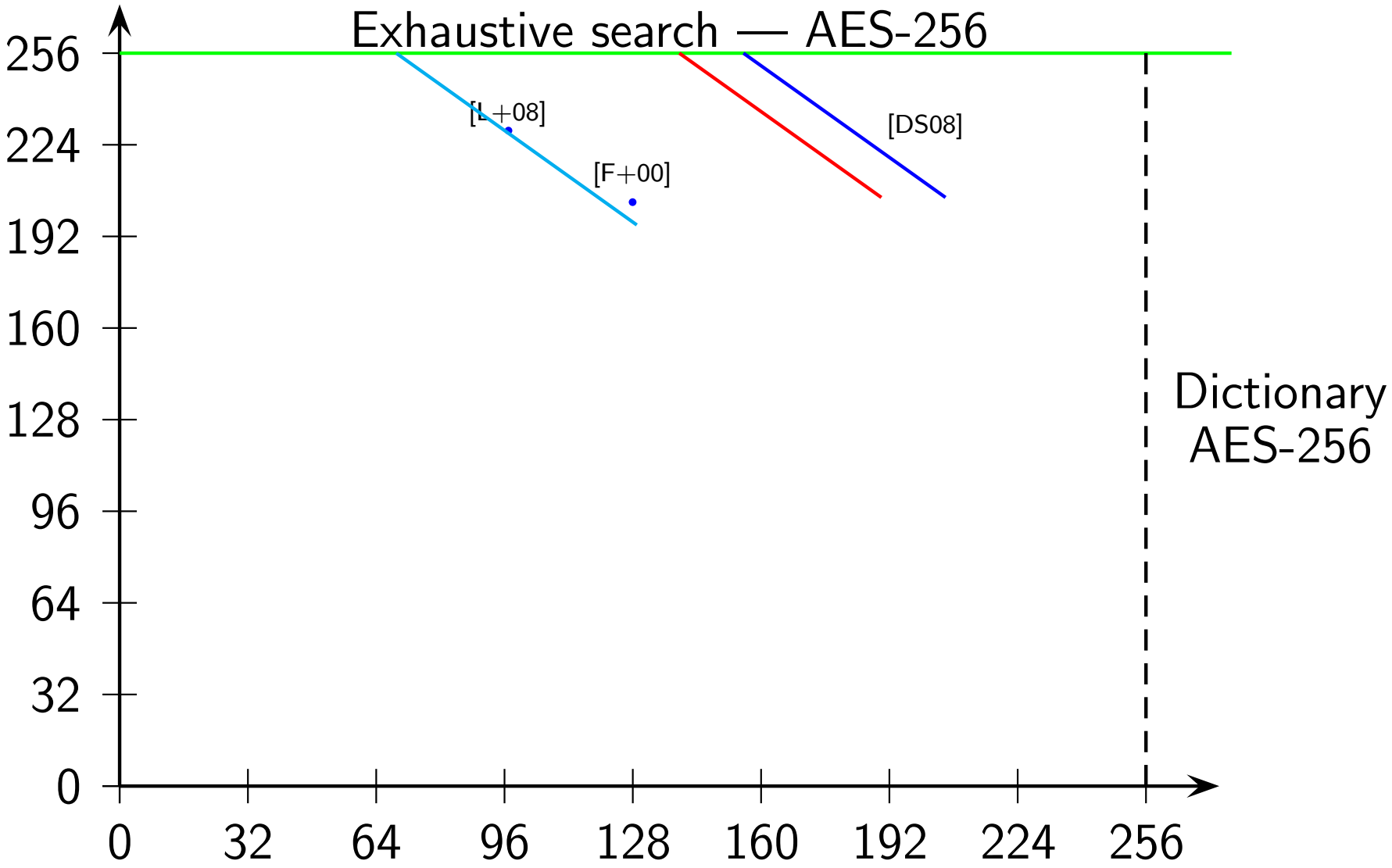
8-Round Single-Key Attacks on AES



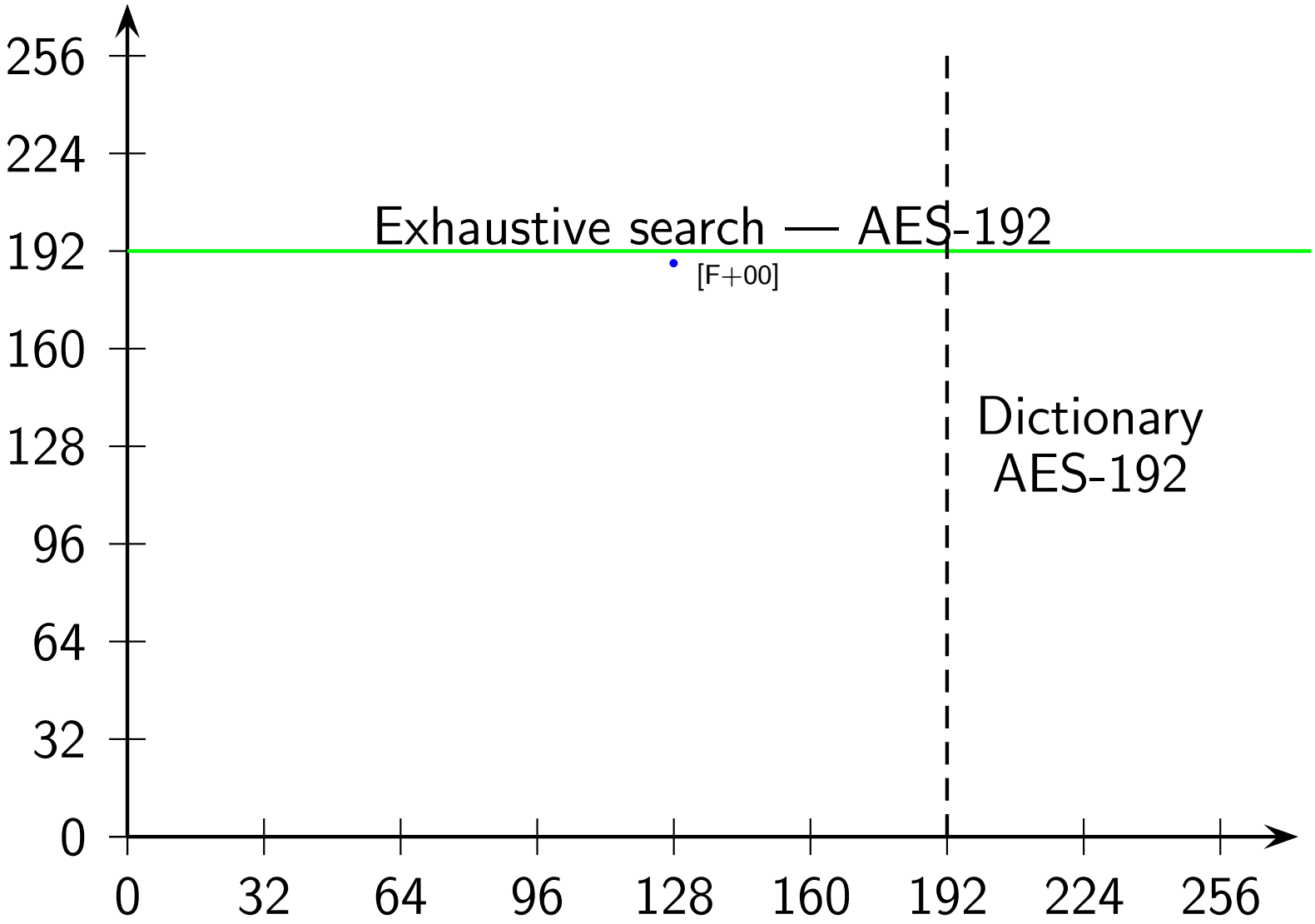
8-Round Single-Key Attacks on AES



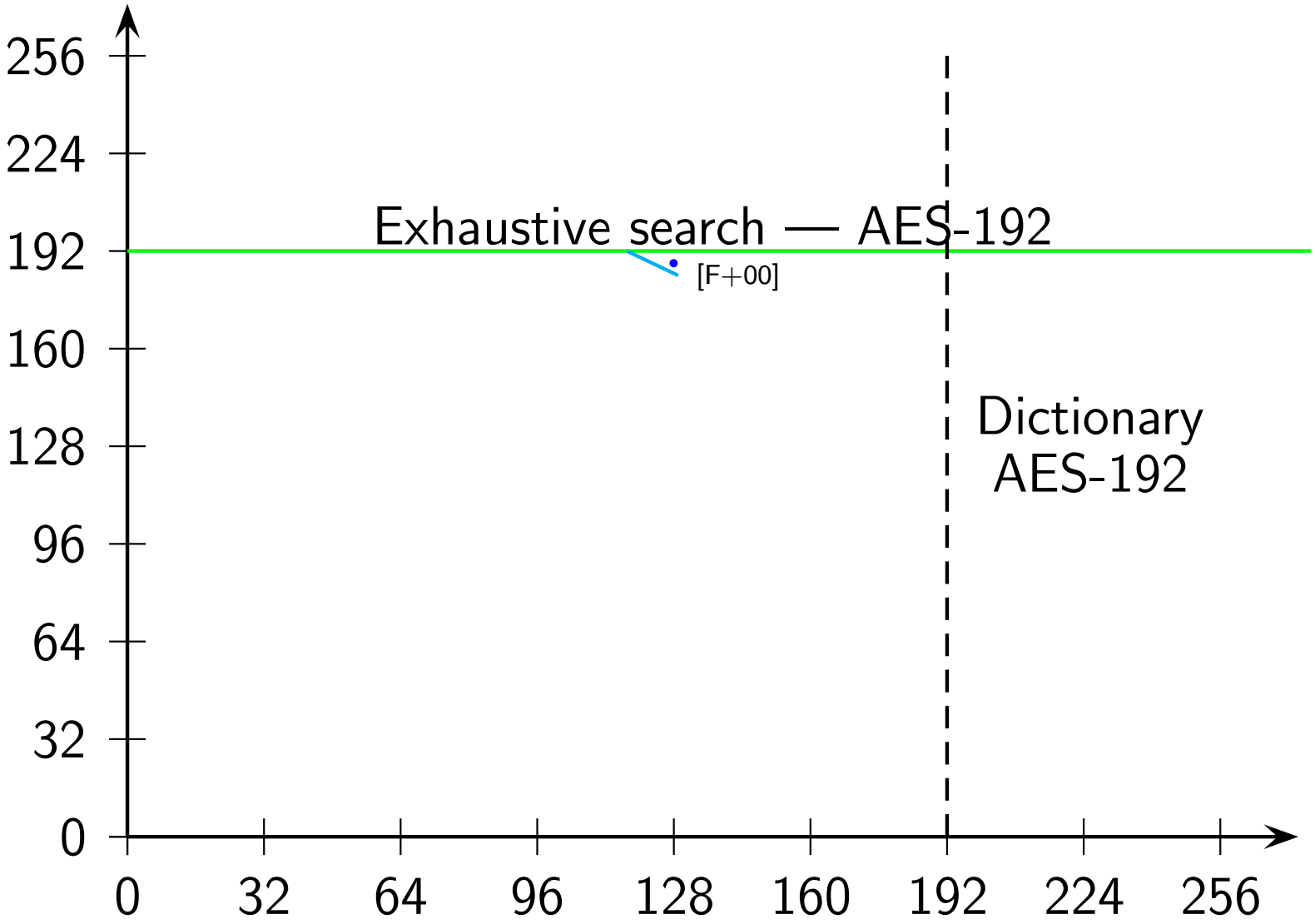
8-Round Single-Key Attacks on AES



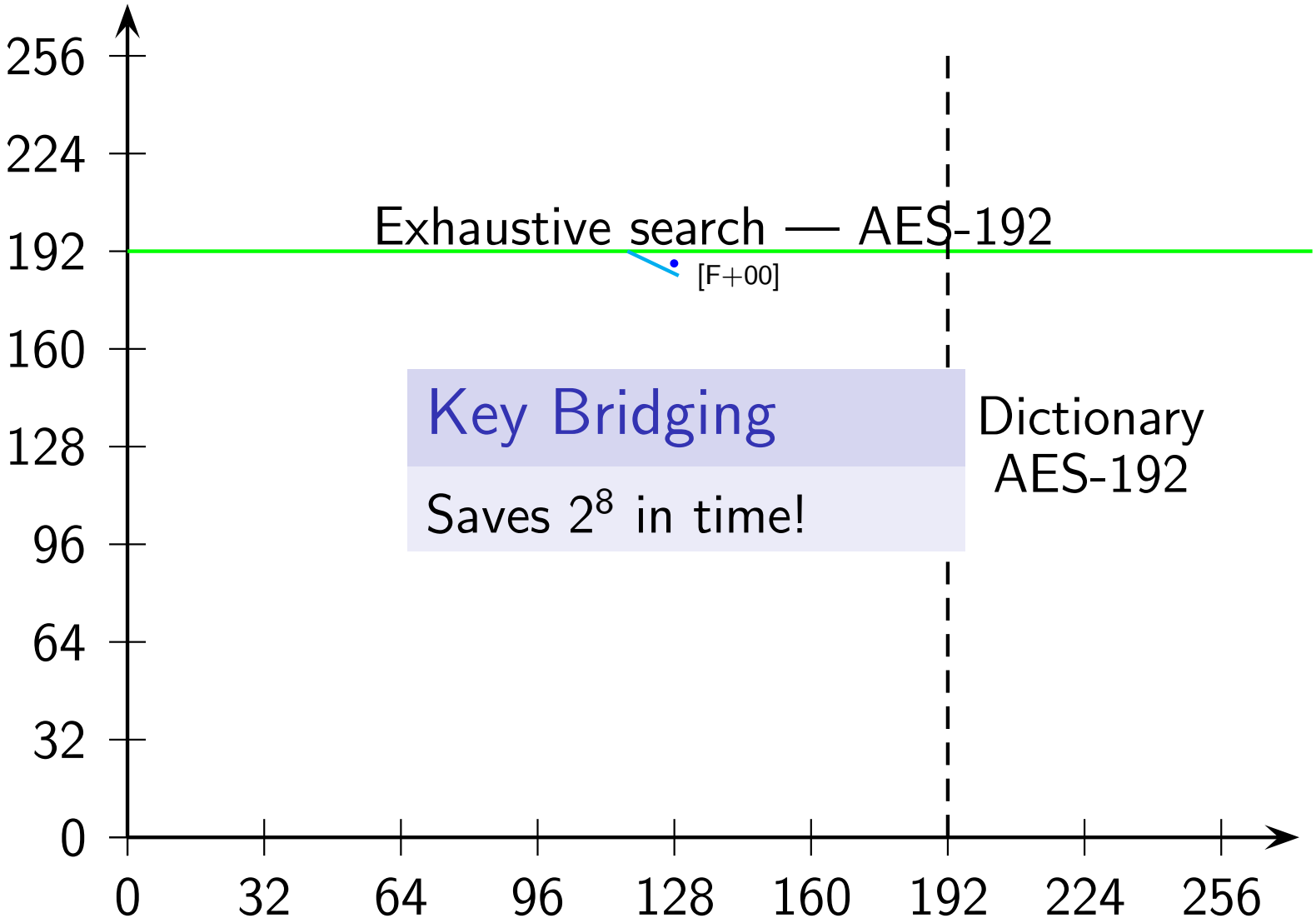
8-Round Single-Key Attacks on AES



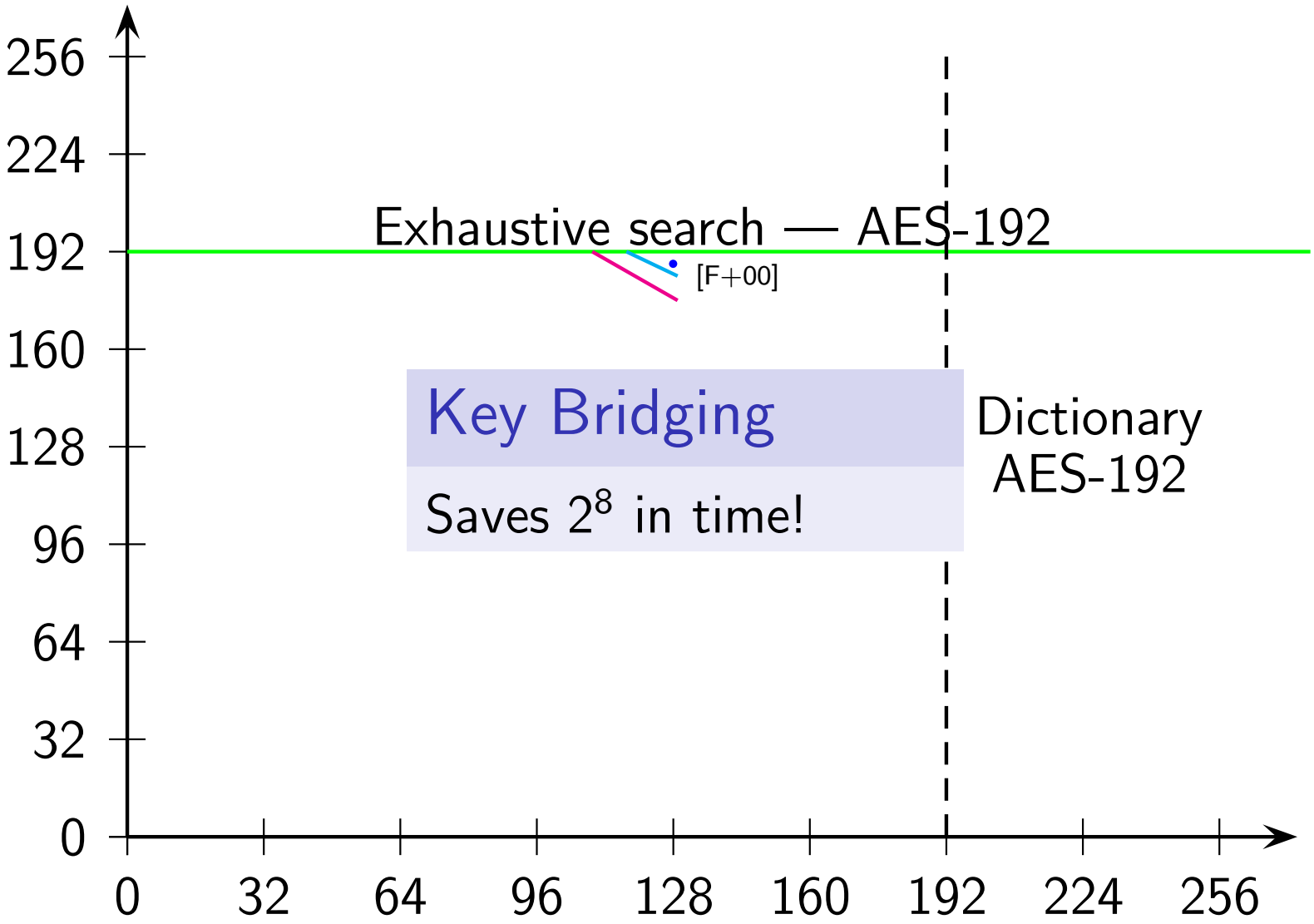
8-Round Single-Key Attacks on AES



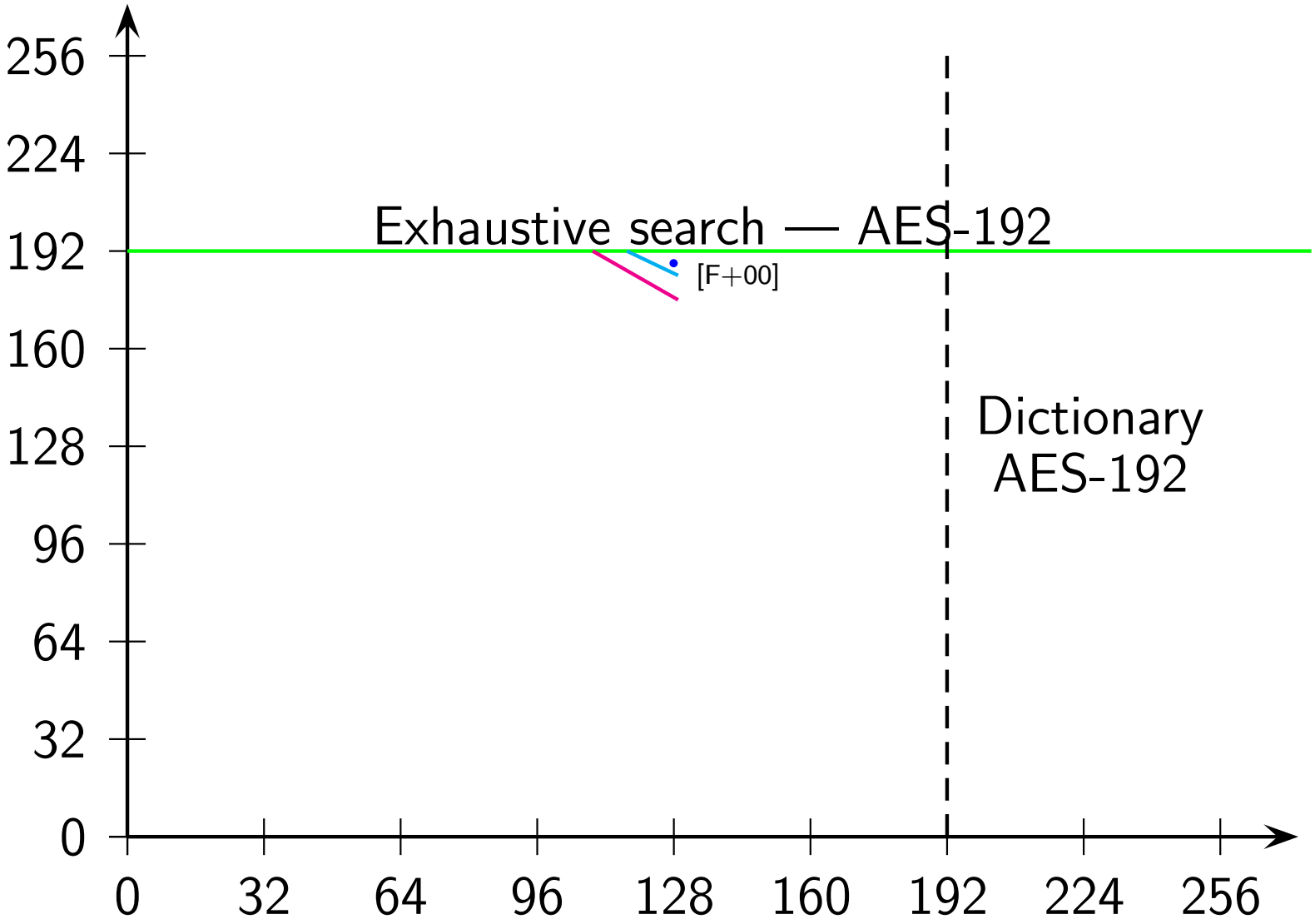
8-Round Single-Key Attacks on AES



8-Round Single-Key Attacks on AES



8-Round Single-Key Attacks on AES



Outcome?

- First **non-marginal** attack on 8-round AES-192, even if precomputation time is counted.
- Best known result on 8-round AES-256 (single key!).
- Improved other attacks with the key bridging.

Version	Rounds	Data	Memory (Pre)	Time	MinMax
All	7	$\mathbf{2}^{103+n}$	$\mathbf{2}^{129-n}$	$\mathbf{2}^{103+n}$	2^{116}
AES-192	8	$\mathbf{2}^{113+n}$	$\mathbf{2}^{129-n}$	$\mathbf{2}^{172+n}$	$\mathbf{2}^{172}$
AES-256	8	$\mathbf{2}^{113+n}$	$\mathbf{2}^{129-n}$	$\mathbf{2}^{196+n}$	$\mathbf{2}^{196}$

Questions?

Thank you for your attention.

http://eprint.iacr.org/2010/322