Building a battlefield
for authenticated encryption

D. J. Bernstein

University of Illinois at Chicago
Krovetz–Rogaway, tomorrow:

Look at how slow AES-GCM is!

Cycles/byte for 4096-byte authenticated encryption:

- 3.73 on Core i5-650.
- 3.88 in 32-bit mode.
- 10.9 without AES insns.
- 39.3 on UltraSPARC III.
- 50.8 on ARM Cortex A8.
- 53.5 on PowerPC 970.
Krovetz–Rogaway, tomorrow:

Look at how slow AES-GCM is!

Cycles/byte for 4096-byte authenticated encryption:
  3.73 on Core i5-650.
  3.88 in 32-bit mode.
  10.9 without AES insns.
  39.3 on UltraSPARC III.
  50.8 on ARM Cortex A8.
  53.5 on PowerPC 970.

Paper advertises AES-OCB3, which is faster. *Quel surprise!*
Were these AES-GCM speeds the state of the art?

Not even close. Paper is ignoring

- better AES implementations (e.g., 2008 Bernstein–Schwabe);
Were these AES-GCM speeds the state of the art?

Not even close. Paper is ignoring

- better AES implementations (e.g., 2008 Bernstein–Schwabe);
- faster ciphers than AES-CTR (e.g., any eSTREAM finalist);
Were these AES-GCM speeds the state of the art?

Not even close. Paper is ignoring

- better AES implementations (e.g., 2008 Bernstein–Schwabe);
- faster ciphers than AES-CTR (e.g., any eSTREAM finalist);
- faster authenticators (e.g., Poly1305, HMAC-???)
Were these AES-GCM speeds the state of the art?

Not even close. Paper is ignoring

- better AES implementations (e.g., 2008 Bernstein–Schwabe);
- faster ciphers than AES-CTR (e.g., any eSTREAM finalist);
- faster authenticators (e.g., Poly1305, HMAC-???
- serious redesigns (e.g., Phelix, Grain-128a).
Were these AES-GCM speeds the state of the art?

Not even close. Paper is ignoring
- better AES implementations (e.g., 2008 Bernstein–Schwabe);
- faster ciphers than AES-CTR (e.g., any eSTREAM finalist);
- faster authenticators (e.g., Poly1305, HMAC-???);
- serious redesigns (e.g., Phelix, Grain-128a).

Paper is also sloppy with security. Big trouble near $2^{64}$ blocks, avoided by some older schemes.
What do we do after SHA-3?
What do we do after SHA-3? Let’s have a competition for authenticated encryption! Much more fun than, e.g., cycling back to block ciphers.
What do we do after SHA-3? Let’s have a competition for authenticated encryption! Much more fun than, e.g., cycling back to block ciphers.

Easy: Speed competition. ECRYPT benchmarking will soon cover authenticated encryption.
What do we do after SHA-3? Let’s have a competition for authenticated encryption! Much more fun than, e.g., cycling back to block ciphers.

Easy: Speed competition. ECRYPT benchmarking will soon cover authenticated encryption.

What do we do after SHA-3? Let’s have a competition for authenticated encryption! Much more fun than, e.g., cycling back to block ciphers.

Easy: Speed competition. ECRYPT benchmarking will soon cover authenticated encryption.


Potential timing problem: NIST needs to take a break. ECRYPT II ends in 2012. But does this really matter?
Competition already has a name, thanks to Greg Rose: eSAFE.
Competition already has a name, thanks to Greg Rose: eSAFE.
(Only 655000 Google hits.)
Competition already has a name, thanks to Greg Rose: eSAFE. (Only 655000 Google hits.)

What does eSAFE stand for? Not sure yet.
Competition already has a name, thanks to Greg Rose: eSAFE. (Only 655000 Google hits.)

What does eSAFE stand for?
Not sure yet.

ECRYPT
Secure
Authenticated
Fast
Encryption