Cycle counts for authenticated encryption

D. J. Bernstein

`http://cr.yp.to`
`/streamciphers`
`/timings.html`

Standard construction:
encrypt with stream cipher;
authenticate the ciphertext
by appending encrypted hash.

How to hash the ciphertext?
AES(AES(c_1) $+ c_2$) $+ c_3$;
MD5 with a secret IV;
Poly1305, provable, fast;
UMAC, faster given SSE2;
VMAC, faster given AMD64;
Badger; MAC1071; etc.

How to encrypt the hash?
The same stream cipher;
MD5, secret IV; AES; etc.

Cost of standard construction
is cost of stream cipher
plus cost of encrypted hash
plus various overheads: e.g.
cache misses (non-orthogonal).

Alternative constructions?
eSTREAM solicited schemes.
Responses: NLS, Phelix, etc.

Is an authenticating cipher,
such as Phelix, faster than
the standard construction?

Previous eSTREAM timings
didn't include hash costs.

Maybe the fastest AE scheme depends on the situation.

Decrypting legitimate packets?
Rejecting forged packets?

Small packets? Large packets?
More packet-size effects?

Many keys active at once?
Only one key?

Pentium III? Pentium 4?
Athlon? UltraSPARC III?
PowerPC G5? Athlon 64 X2?
Core 2 Duo?

Let's measure everything!