A Cryptographically Protected Phone System

Andres Erbsen Adam Yedidia

November 13, 2014

Why?

Why not?

- Some information is very sensitive
- Privacy is a basic right
- Users **assume** that phone calls are private

Eavesdropping is easy

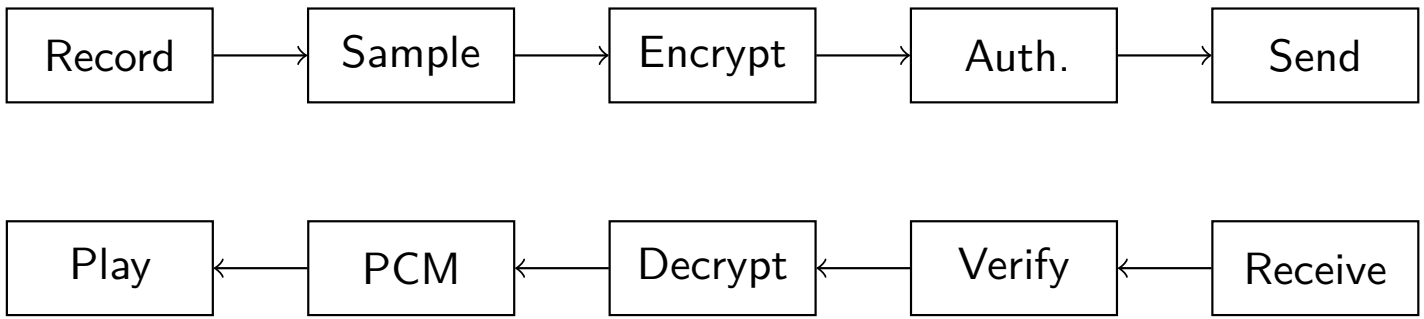
- *Intercepting GSM traffic* by Steve D. Hulton (2008)
- Software radio ($750) or maintenance-mode phone (??, was $5)
- 2TB of precomputatiuted A5/1 tables ($100)
- Udacity CS387: demo in class

How?

- Easier that it looks
- Standing on the shoulders of giants
  - Reuse proven components
- Giants standing on out shoulders
  - Companies lack incentives
  - Google RedPhone
- Rigor still required
- Usability matters

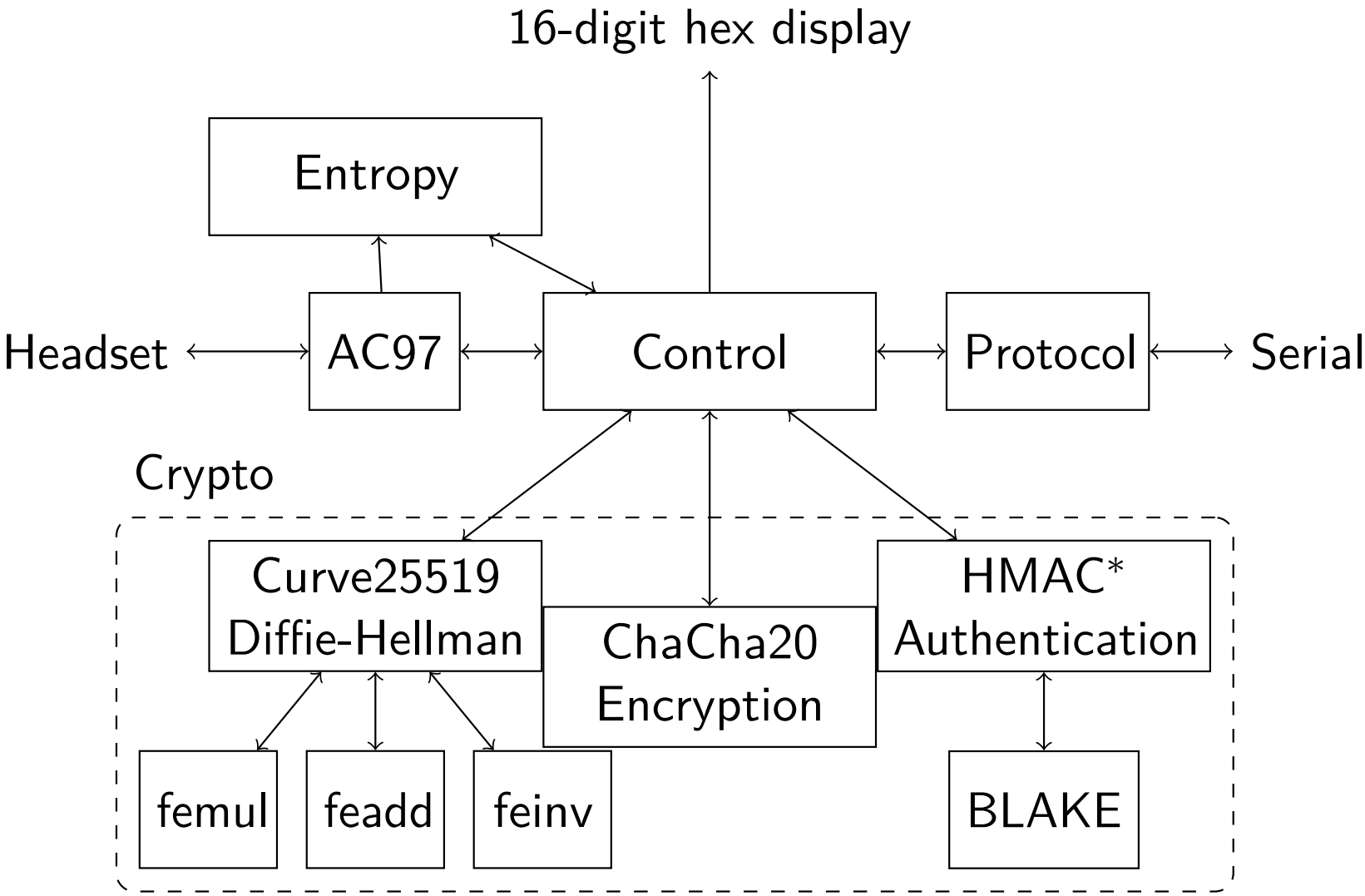
How? (continued)

1. Setup shared key (Diffie-Hellman)
2. Stretch the key

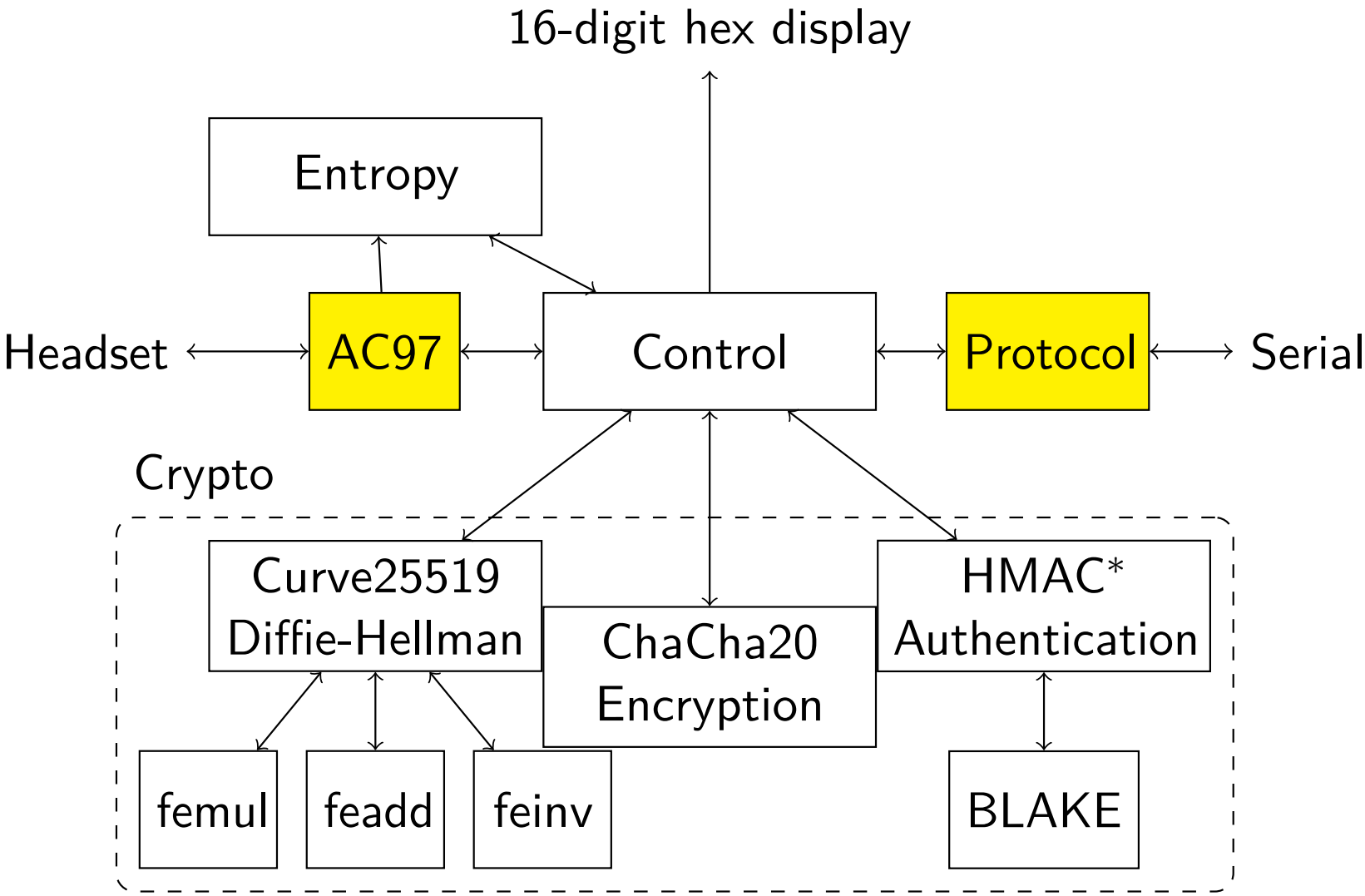


5. Check correspondence.

Design


16-digit hex display
Entropy
Headset
AC97
Control
Protocol
Serial
Crypto
Curve25519
Diffie-Hellman
ChaCha20
Encryption
HMAC*
Authentication
femul
feadd
feinv
BLAKE

Design


16-digit hex display
Entropy
Headset
AC97
Control
Protocol
Serial
Crypto
Curve25519
Diffie-Hellman
ChaCha20
Encryption
HMAC*
Authentication
femul
feadd
feinv
BLAKE

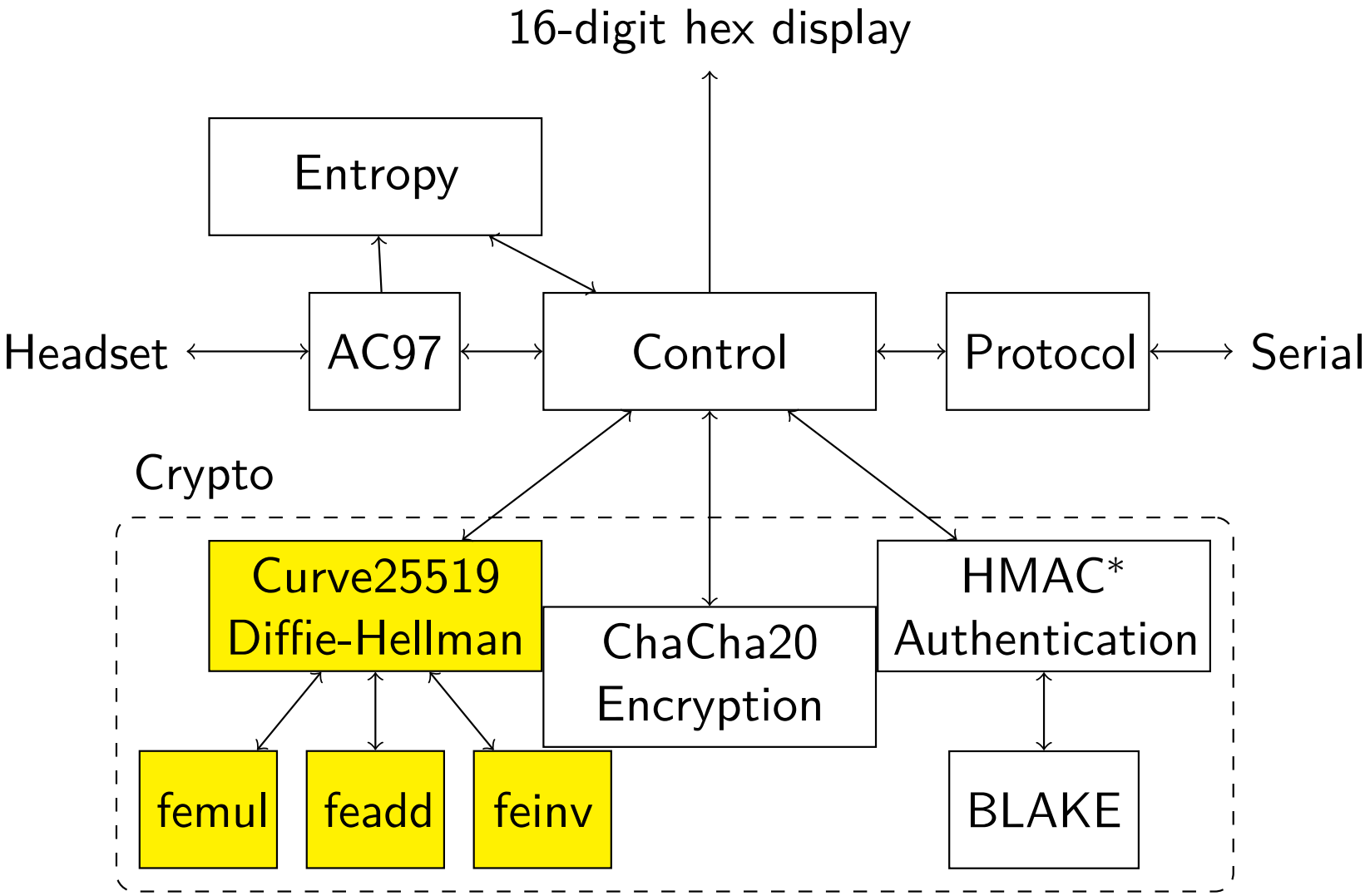
Serial communication

- Same as without crypto (almost)
- Unsynchronized clocks
- Between two labkits
  - Wire clock and data for each direction
  - Ground
- $<$ 1Mbit/s

Audio interface

- Similar to lab5a
- 18 bits 48000 times a second
- Keep 16 for simplicity
- Minimal buffering
  - For authentication

Design


16-digit hex display
Entropy
Headset
AC97
Control
Protocol
Serial
Crypto
Curve25519
Diffie-Hellman
ChaCha20
Encryption
HMAC*
Authentication
femul
feadd
feinv
BLAKE

Diffie-Hellman key exchange

- Whitfield Diffie, Martin Hellman, and Ralph Merkle (1976)
- Two people communicating in the presence of an eavesdropper can make their communications uncrackable, **even with no prior agreements and having never spoken before**.

$$(g^a)^b = g^{ab} = (g^b)^a$$

$$g^a \not\to a$$

$$g^a, g^b \not\to g^{ab}$$

Arithmetic mod public prime P (≈ 3000 bits)

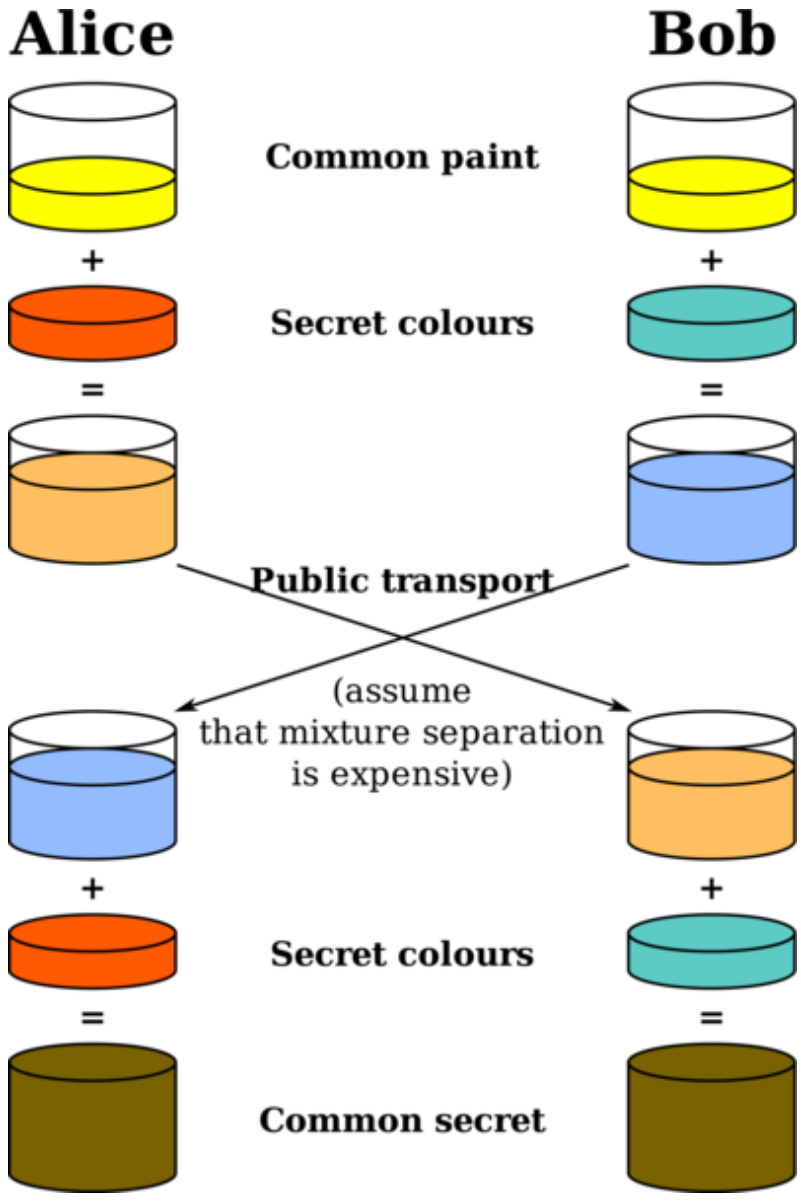


Figure 1: Diffie-Hellman with colors

Exponentiation

$$x^n = \begin{cases} x\,(x^2)^{\frac{n-1}{2}}, & \text{if } n \text{ is odd} \\ (x^2)^{\frac{n}{2}}, & \text{if } n \text{ is even.} \end{cases}$$

$$x^{23} = x^1 \cdot x^2 \cdot x^4 \cdot x^{16}$$

Elliptic Curve Variant by Daniel Bernstein

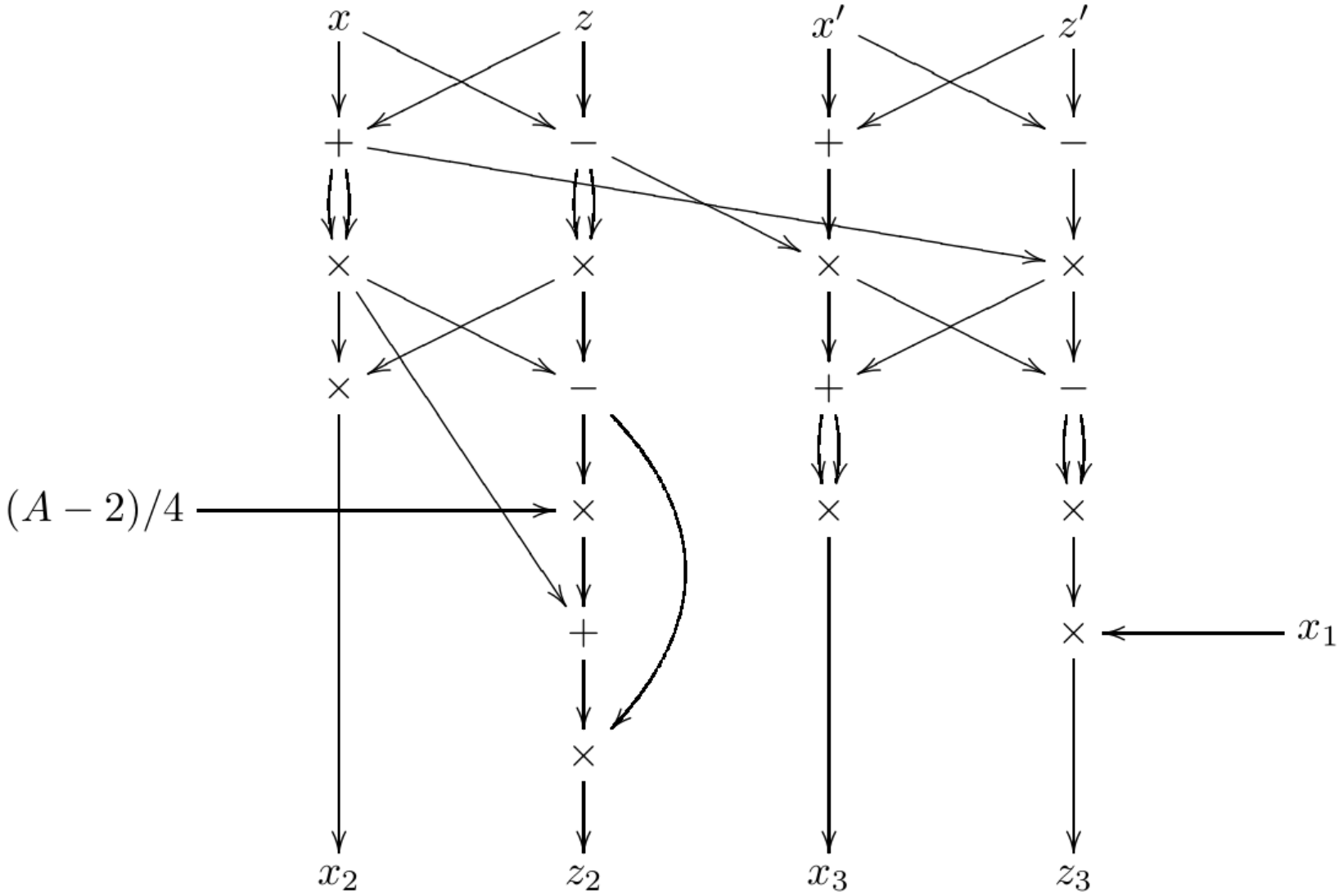
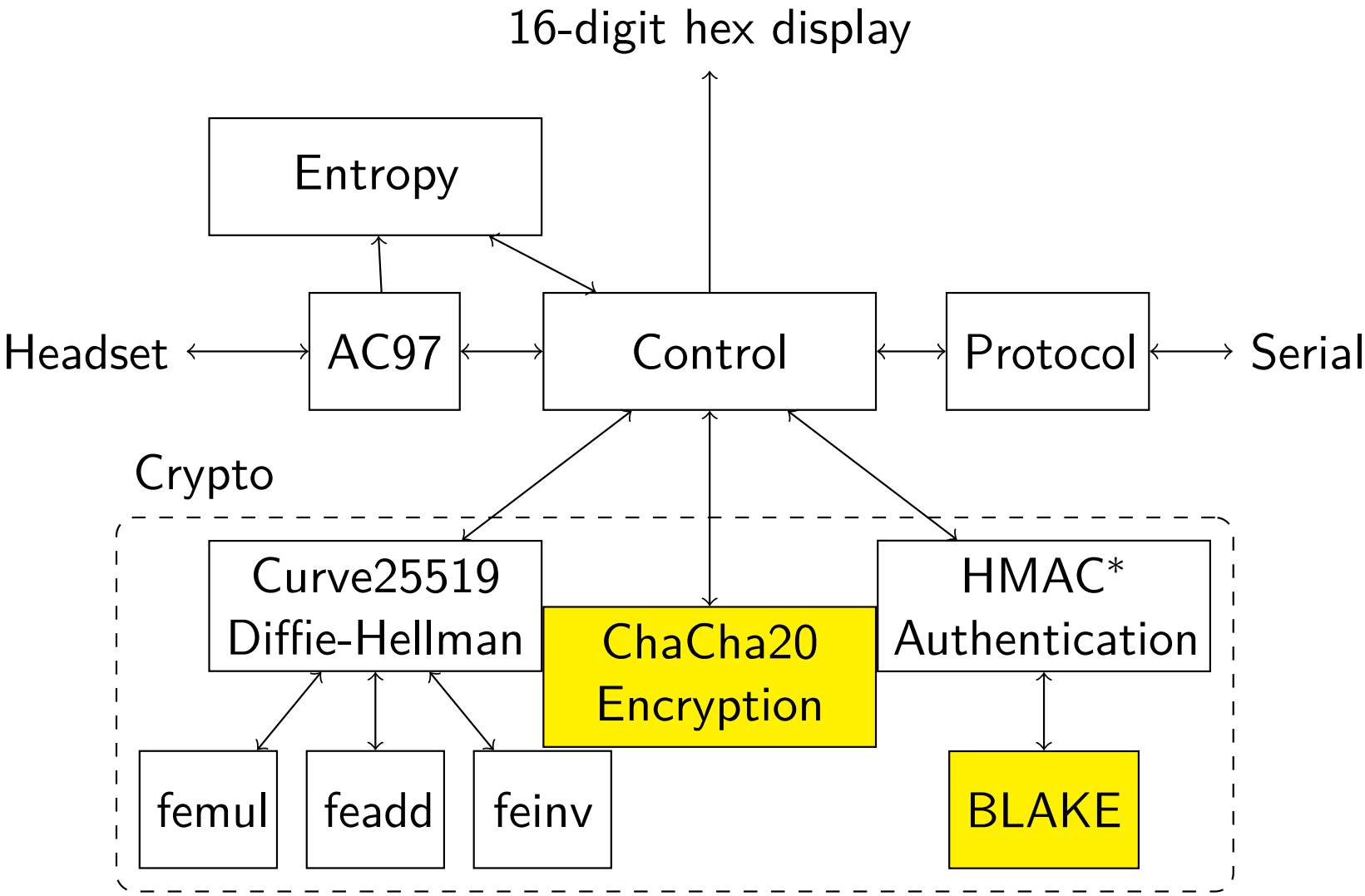


Figure 2: Exponentiation step using fractions mod $P = 2^{255} - 19$

Arithmetic modulo $P = 2^{255} - 19$

- Schoolbook multiplication with 15 digits
  - 15 17x17 multipliers ($15 \cdot 17 = 255$)
  - Wrap each row of partial products mod 2^{255}
  - Add $19 \times$ #overflow
- Schoolbook addition, subtraction
  - Compute both $a + b$ and $a + b - P$
  - Select using carry bits
- Inversion: $x^{P-2} \equiv x^{-1} \bmod P$
  - Another square-and-multiply

Design

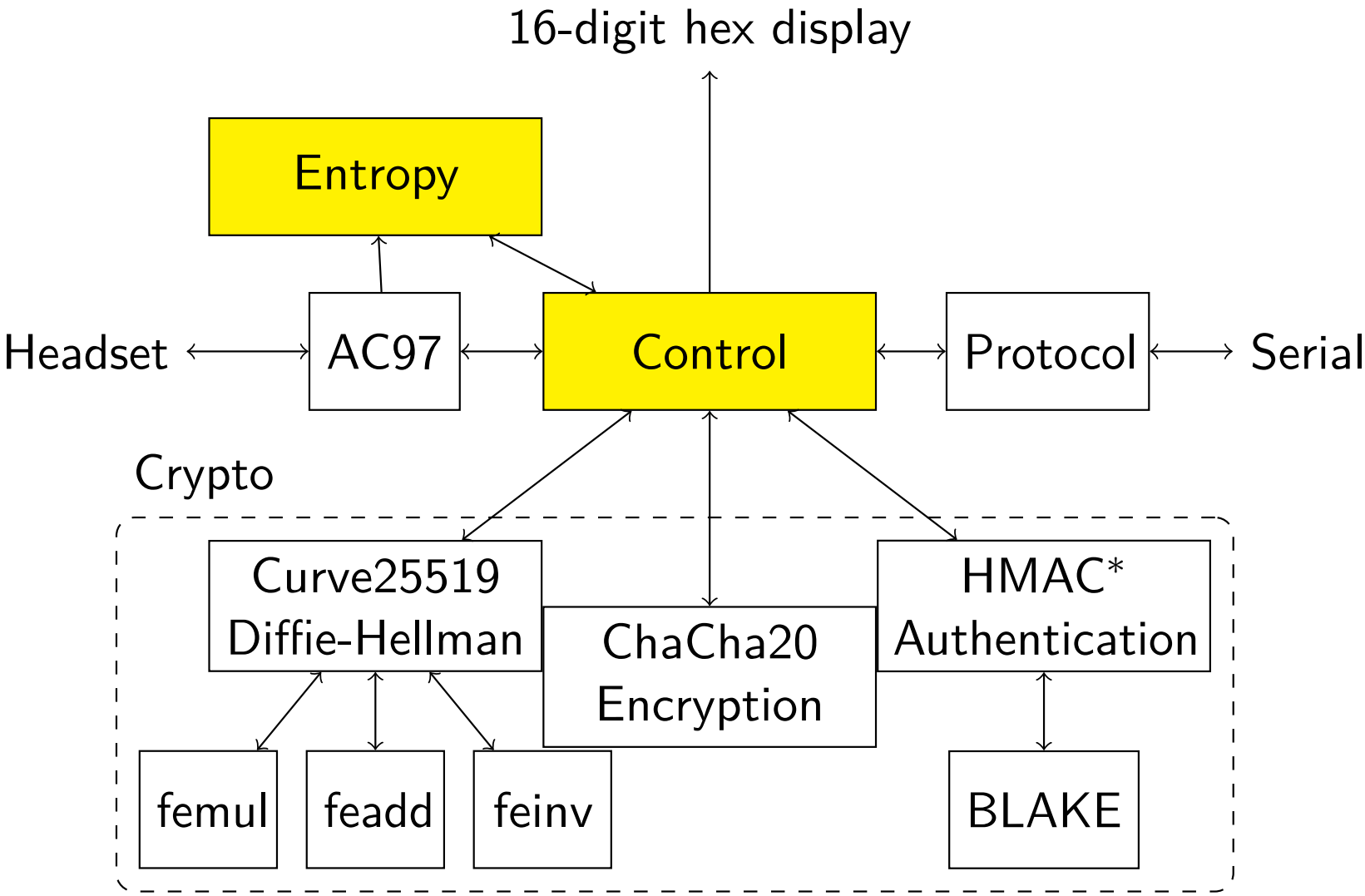

16-digit hex display
Entropy
Headset
AC97
Control
Protocol
Serial
Crypto
Curve25519
Diffie-Hellman
ChaCha20
Encryption
HMAC*
Authentication
femul
feadd
feinv
BLAKE

Key stretching and hashing

- ARX design
  - 32-bit addition
  - rotation
  - exclusive or
- ChaCha20
  - input: key, index into stream
  - 16x32 bits of state and output
  - 20 rounds of the following for different a, b, c, d:

```
a += b; d ^= a; d <<<= 16;
c += d; b ^= c; b <<<= 12;
a += b; d ^= a; d <<<= 8;
c += d; b ^= c; b <<<= 7;
```

Design


16-digit hex display
Entropy
Headset
AC97
Control
Protocol
Serial
Crypto
Curve25519
Diffie-Hellman
ChaCha20
Encryption
HMAC*
Authentication
femul
feadd
feinv
BLAKE

True randomness

- No fun if the attacker can guess our secrets
- Pseudo-randomness won't do
- Computation cannot create randomness
- Simple solution: noise from microphone
- State of art: metastability, diode breakthrough, photon phase

The user's responsibility

Is anybody laughing yet?

The user's responsibility

Is anybody laughing yet?

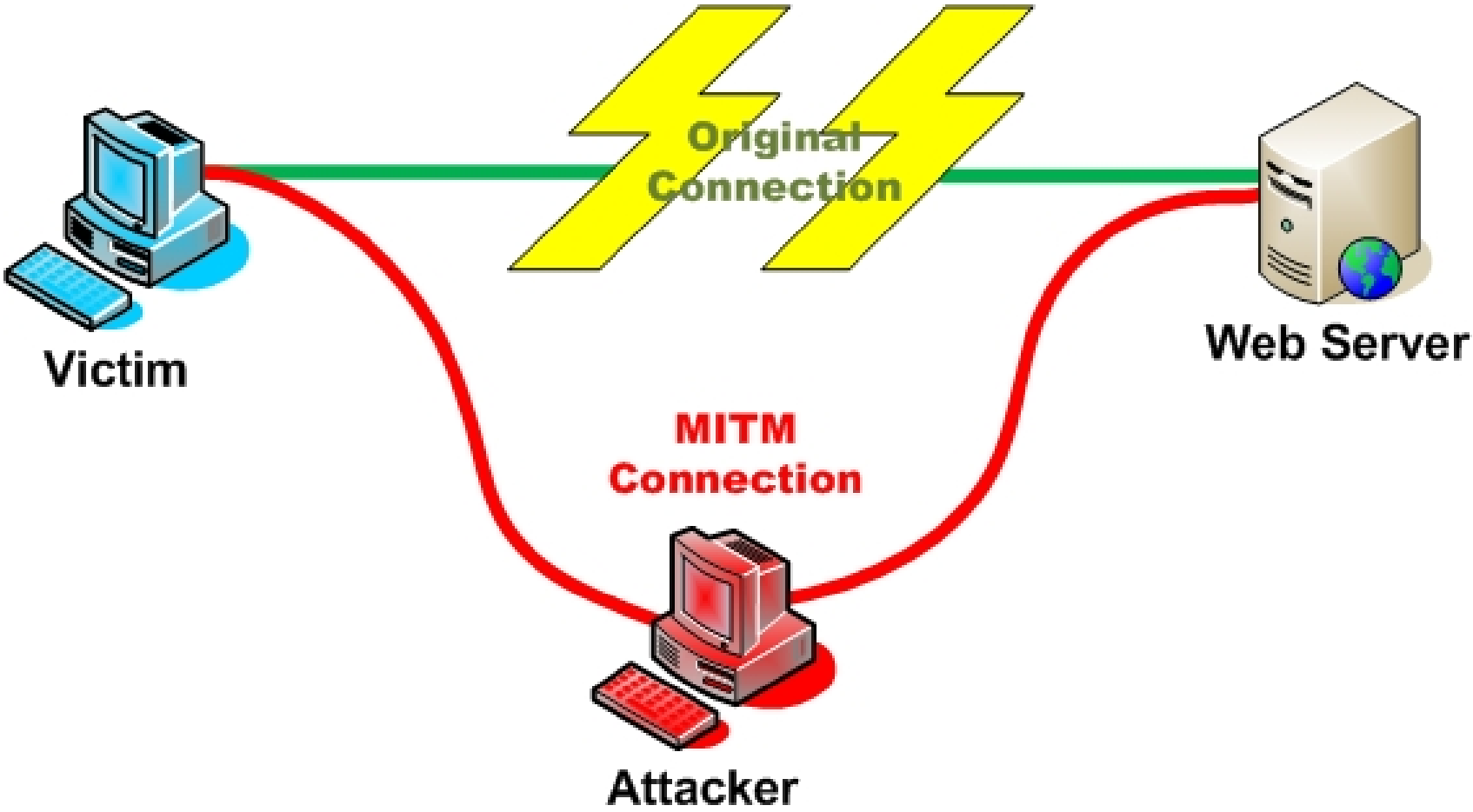


Figure 3: Man-In-The-Middle

The user's responsibility

- Labkit displays a value that determines g^a, g^b
- The conversing parties read the value they see
  - Same value $\Rightarrow$ good security
  - Different value $\Rightarrow$ caught red-handed
- Human voice is hard to imitate
- Detection deters attacks?

The underlying protocol

- Send hash of g^a
- Receive hash of g^b
- Send g^a
- Set display to the first 64 bits of the hash of g^a, g^b
- Continue as specified

Credits:

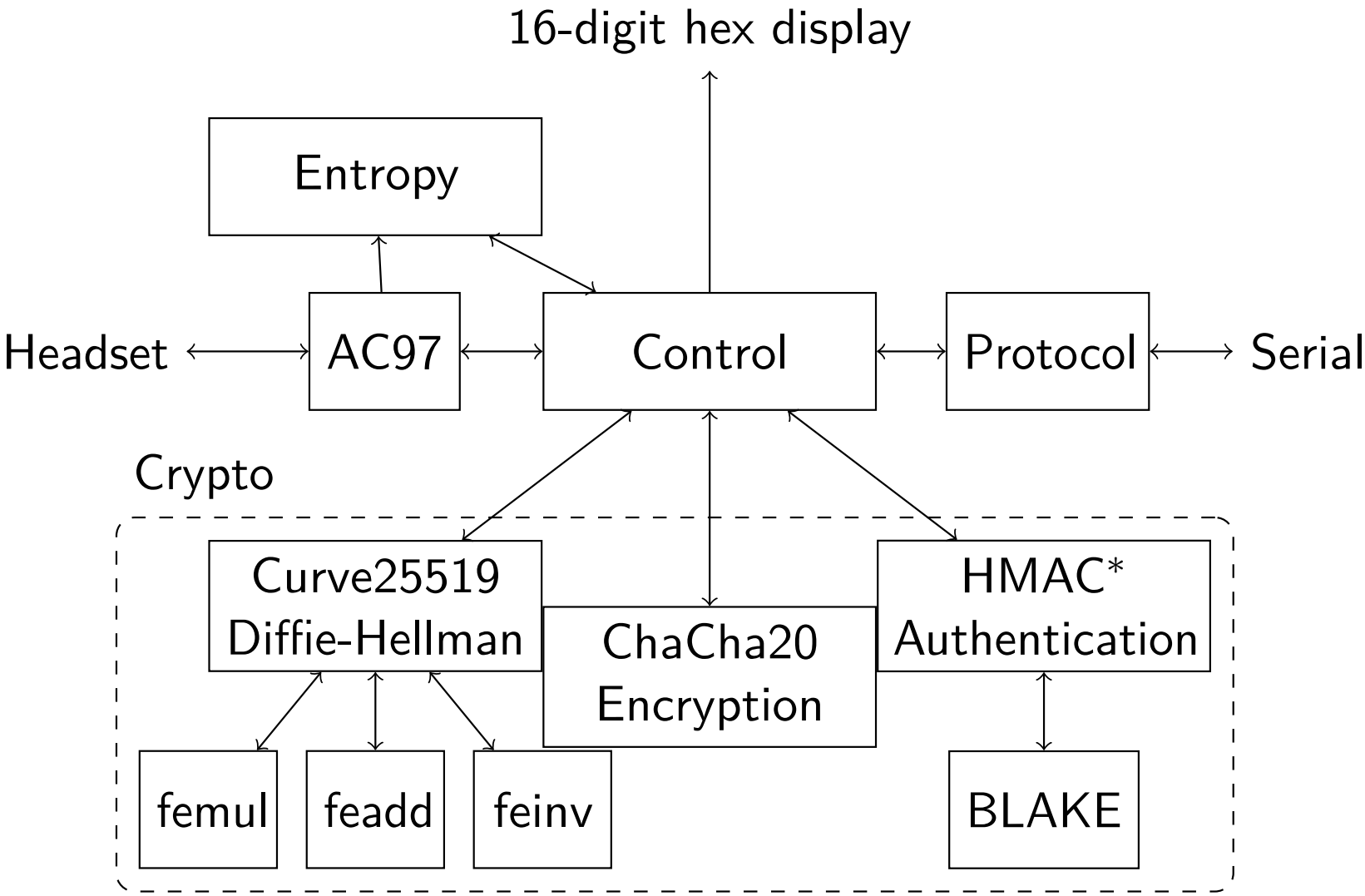
Diffie-Hellman with colors: A.J. Han Vinck, University of Duisburg-Essen https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange#mediaviewer/File:Diffie-Hellman_Key_Exchange.svg

Curve25519 Montgomery step: Daniel Bernstein http://cr.yp.to/ecdh/curve25519-20060209.pdf

ChaCha20 pseudocode: Daniel Bernstein http://cr.yp.to/chacha/chacha-20080128.pdf

Man-In-The-Middle figure: Open Web Application Security Project https://www.owasp.org/index.php/Man-in-the-middle_attack

Questions?


16-digit hex display
Entropy
Headset
AC97
Control
Protocol
Serial
Crypto
Curve25519
Diffie-Hellman
ChaCha20
Encryption
HMAC*
Authentication
femul
feadd
feinv
BLAKE