MobiCom 18
New Delhi, India

Body-Guided Communications: A Low-Power, Highly Confined Primitive to Track and Secure Every Touch

Viet Nguyen[1], Mohamed Ibrahim[1], Hoang Truong[2], Phuc Nguyen[2],
Marco Gruteser[1], Richard Howard[1], Tam Vu[2]

[1] WINLAB/Rutgers University
[2] University of Colorado at Boulder

Motivation: User identification/authentication

Increasing number of devices
Decreasing interaction time

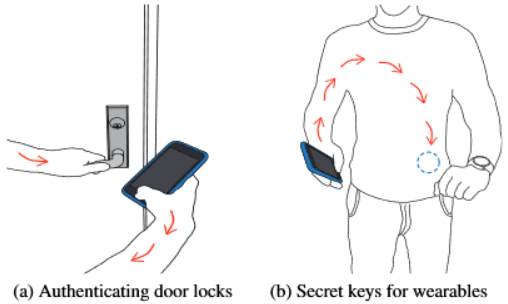
Overhead for authentication

Multiple users working on the same device

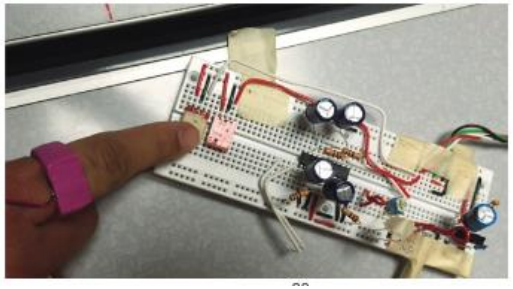
A convenient yet secure user identification/authentication is desirable

Existing user identification/authentication techniques

- Vulnerable to man-in-the-middle attack
  - Radio tokens
  - NFC
- Low data rate
  - SignetRing [1]
  - Hessar et al. [2]
- High power consumption
  - Vibratory communication [3]



(a) Authenticating door locks (b) Secret keys for wearables



[1] Vu et al. “Distinguishing Users with Capacitive Touch Communication”
[2] Hessar et al. “Enabling On-body Transmissions with Commodity Devices”
[3] Roy et al. “Ripple II: Faster Communication through Physical Vibration”

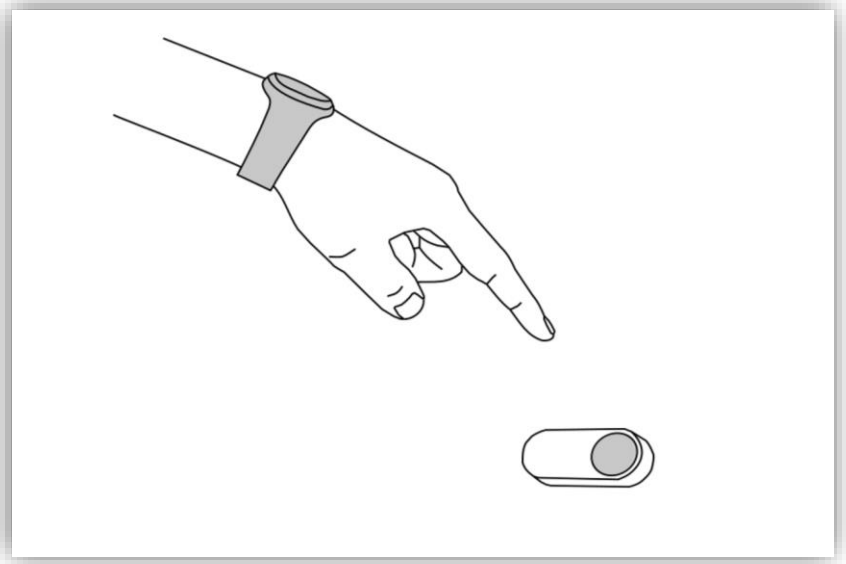
Key idea

Increasing use of wearable devices

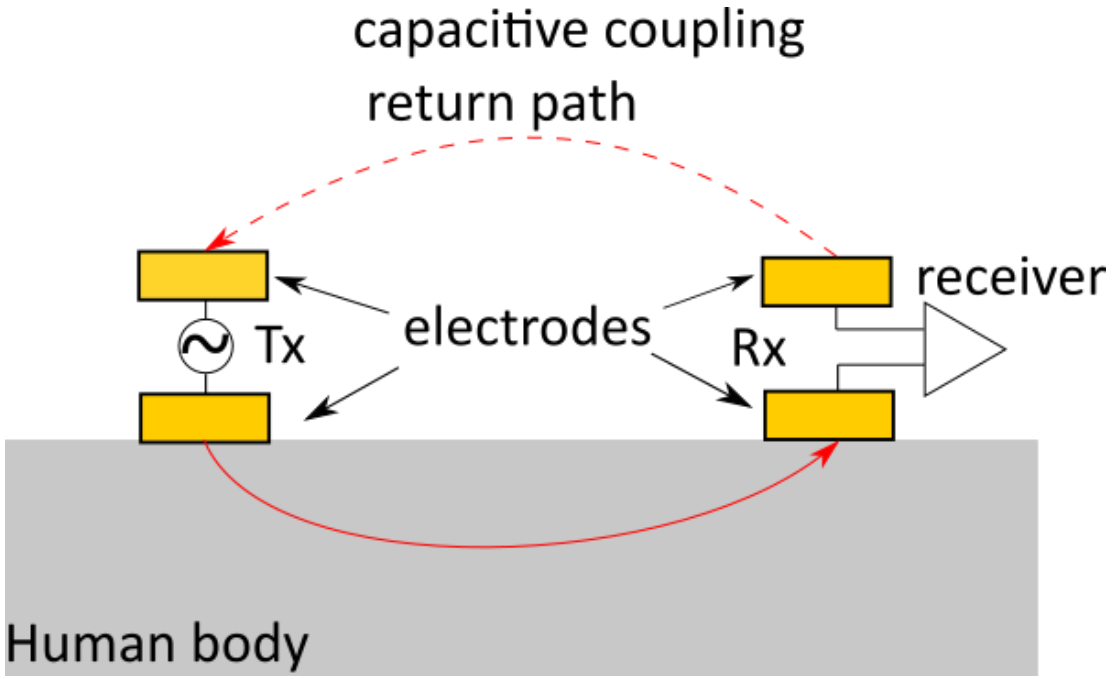
Most interactions are through touch

A body-guided communication system that

- Confines signal to a few cm around the hand
- Achieves high data rate to transmit a complete authentication code on every touch
- Achieves low power consumption

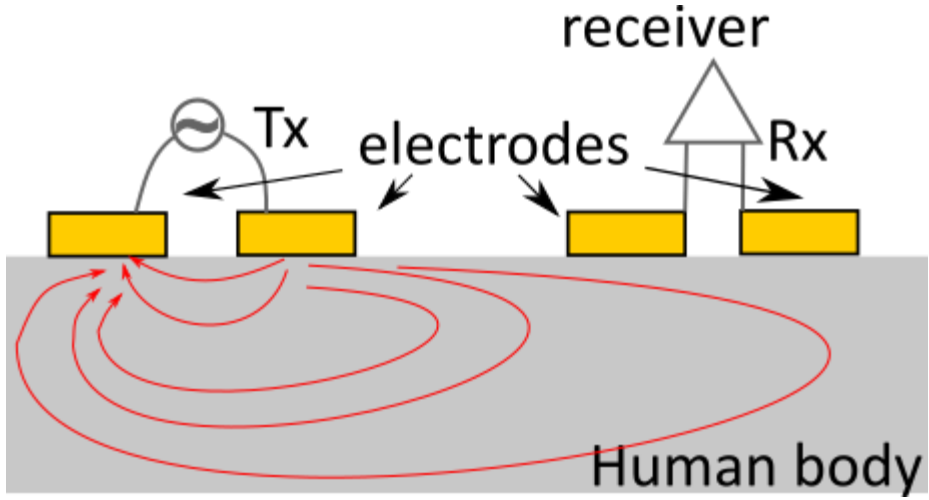


On-body communication



Capacitive Coupling

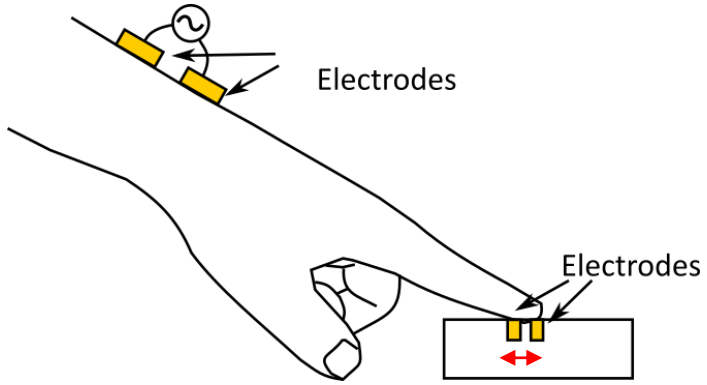
- Path loss is much more dependent on the surrounding environments



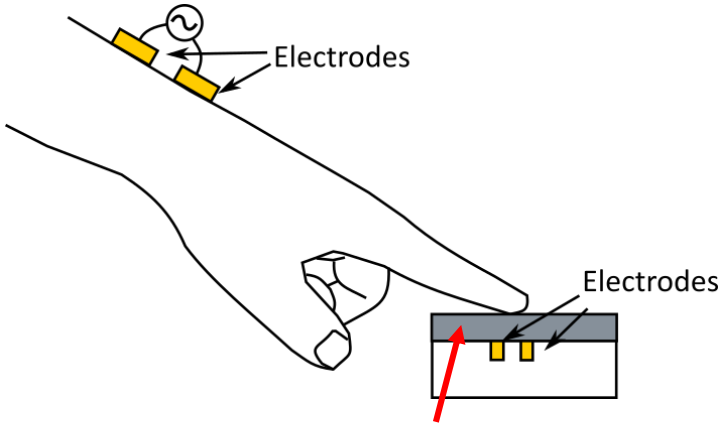
Resistive Coupling

- The received signal decreases with Tx-Rx distance
- The received signal is higher when interelectrode spacing is longer

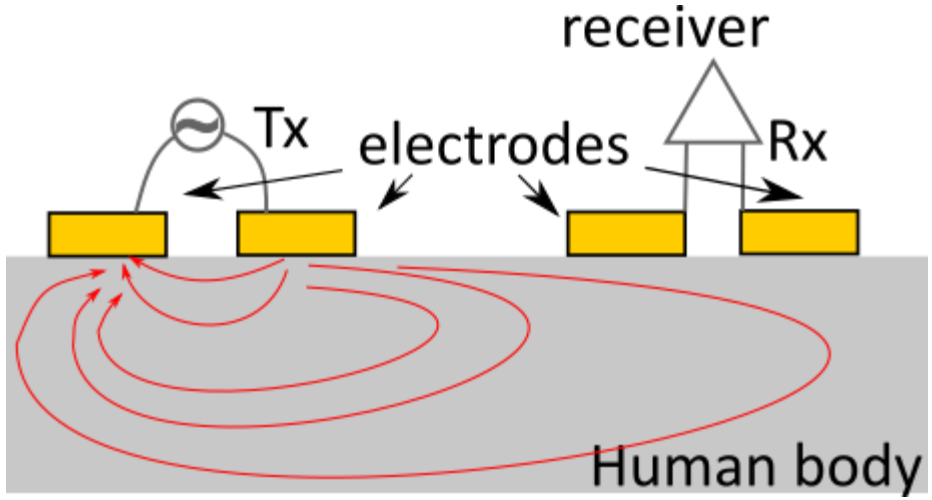
Challenges



RX: inter-electrode distance too small



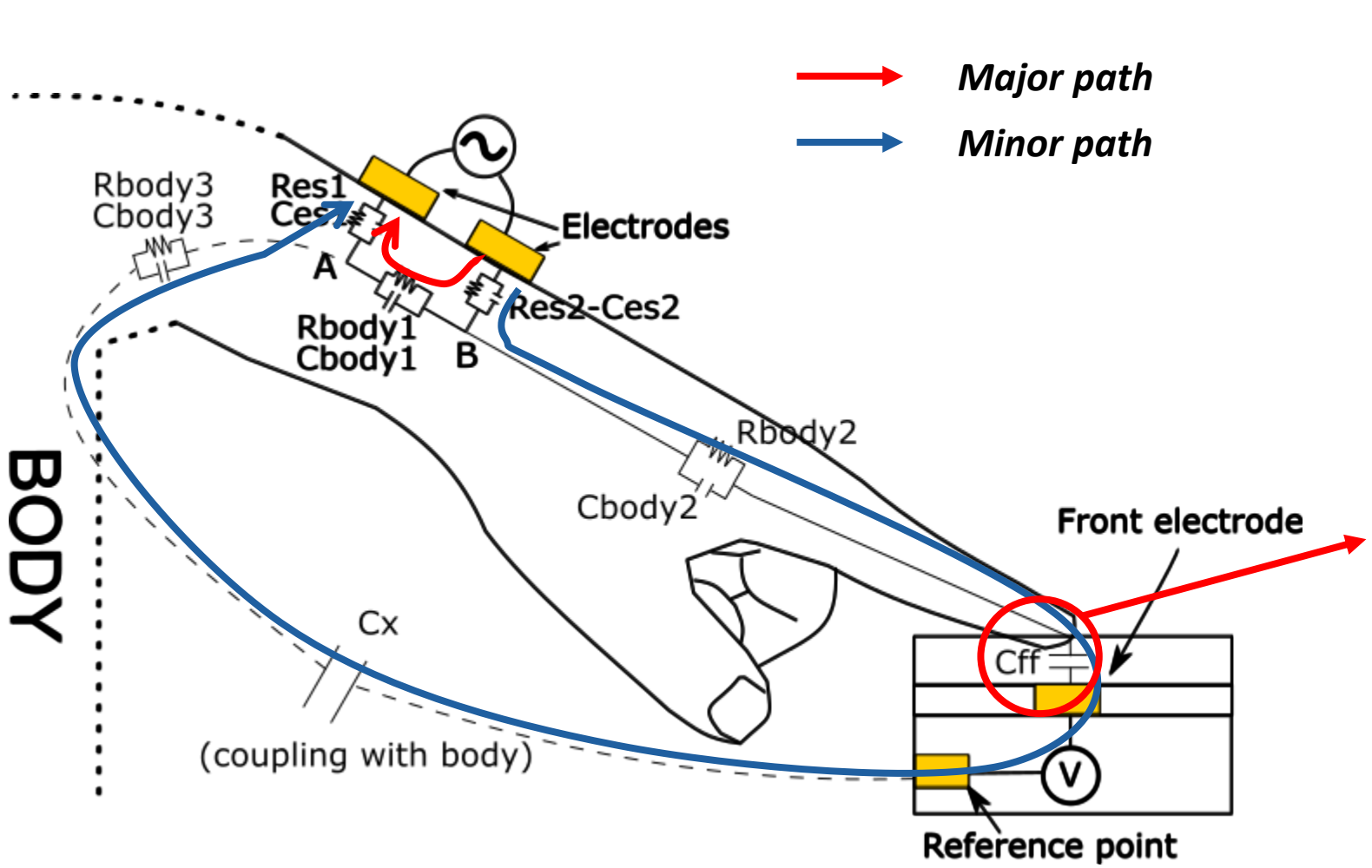
RX: electrodes hidden behind non-conductive layers

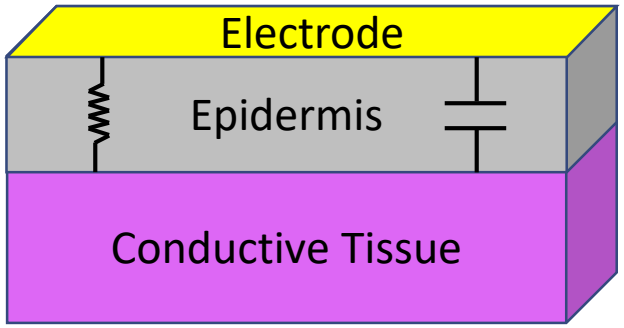


Resistive Coupling

- The received signal decreases with Tx-Rx distance
- The received signal is higher when interelectrode spacing is longer

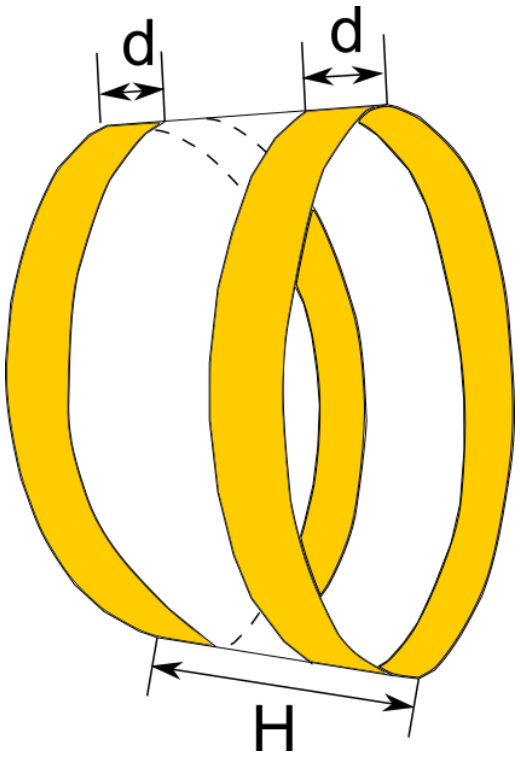
Body-guided Communication

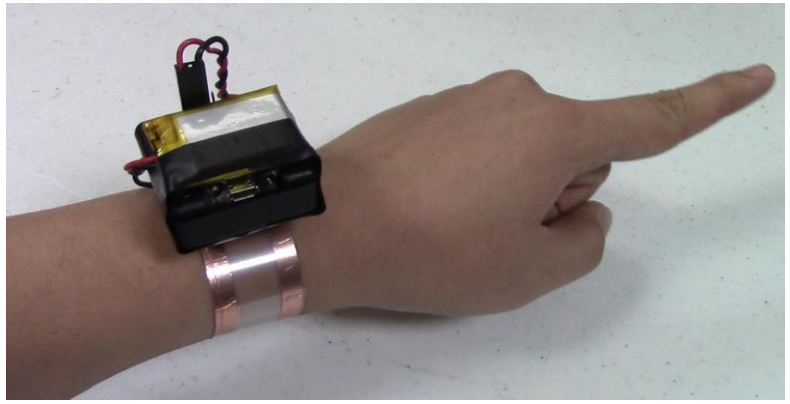




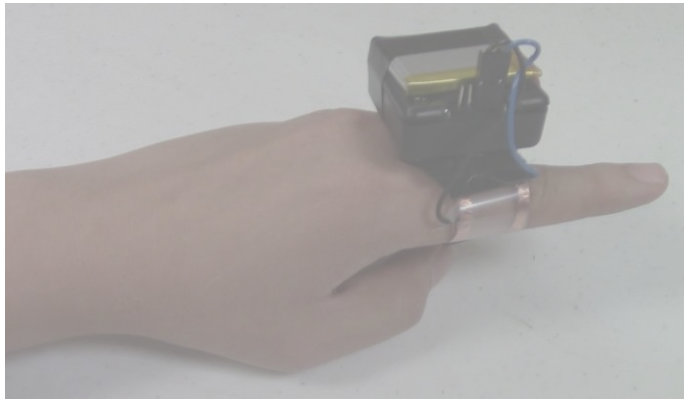
Cff: the limiting factor when the finger moves away from the touch surface
→ **Touch association** for per-touch authentication

Wearable prototype design





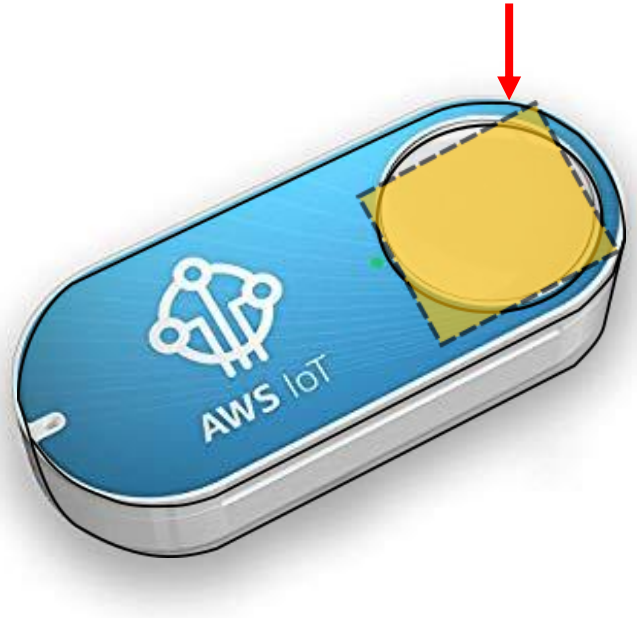
H = 2.4cm
d = 0.6cm



H = 2cm
d = 0.3cm

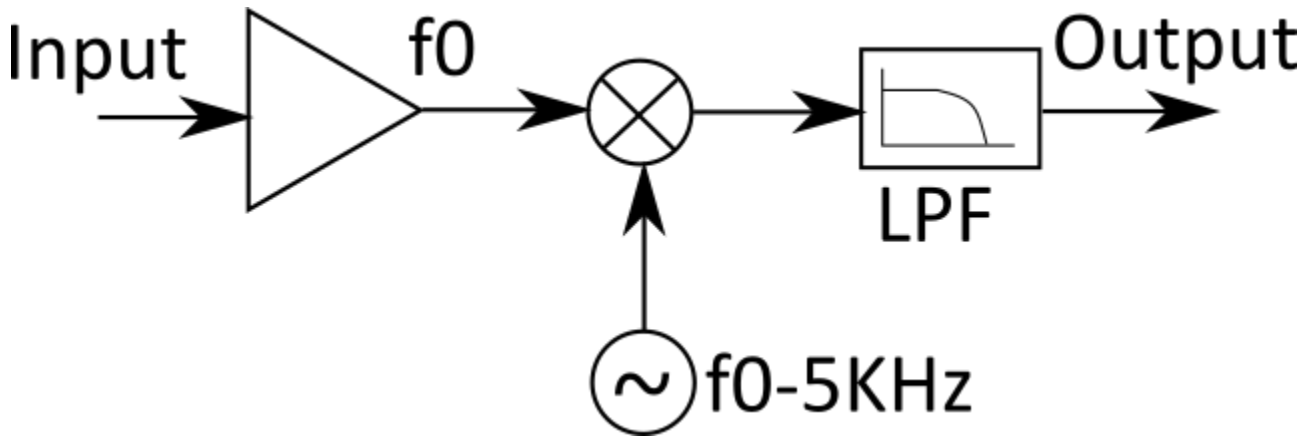
Design of electrode on touched devices

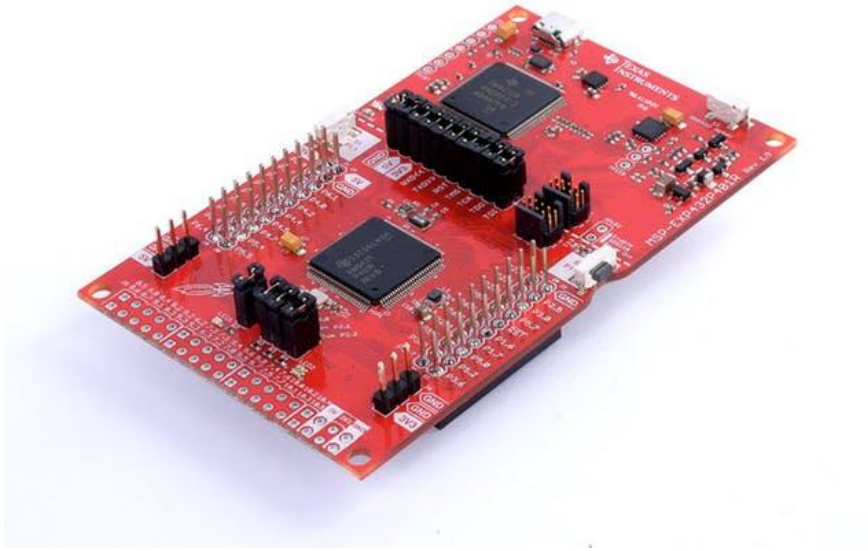
Electrode size: 1cm^2
Under the front-facing case (1mm thick)



Electrode size: 13x6cm^2
On the back of the phone (phone thickness = 1cm)

Receiver design

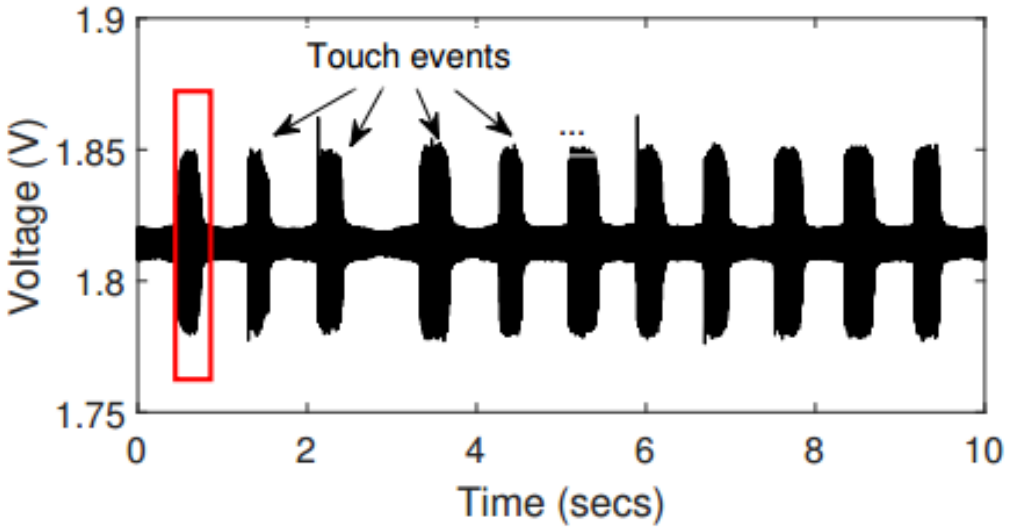


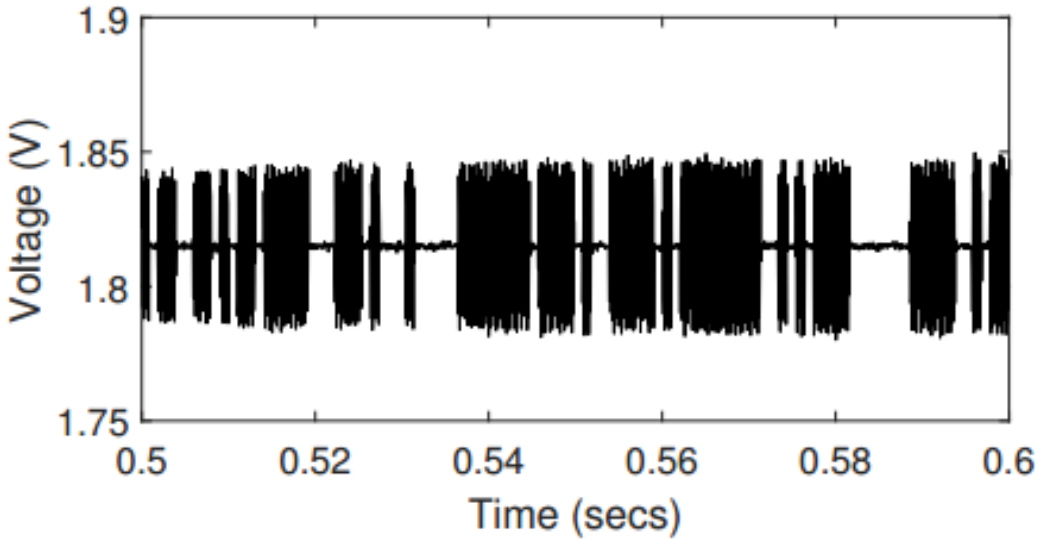


- ❖ Dual-buffered memory
- ❖ Ping-pong DMA
- → real-time decoding

Received signal

Transmitter modulates a 128-bit ID using OOK
Carrier frequency = 150KHz
Signal after mixing at the receiver = 5KHz





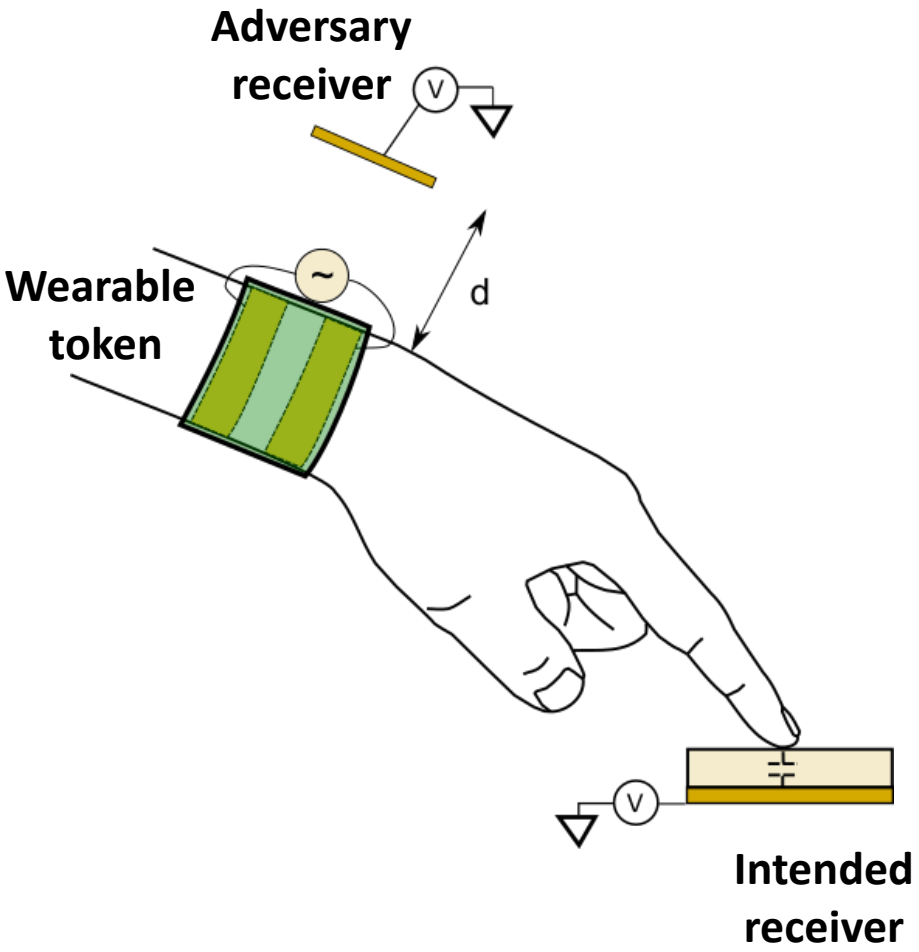
Zoomed-in from red area on the left

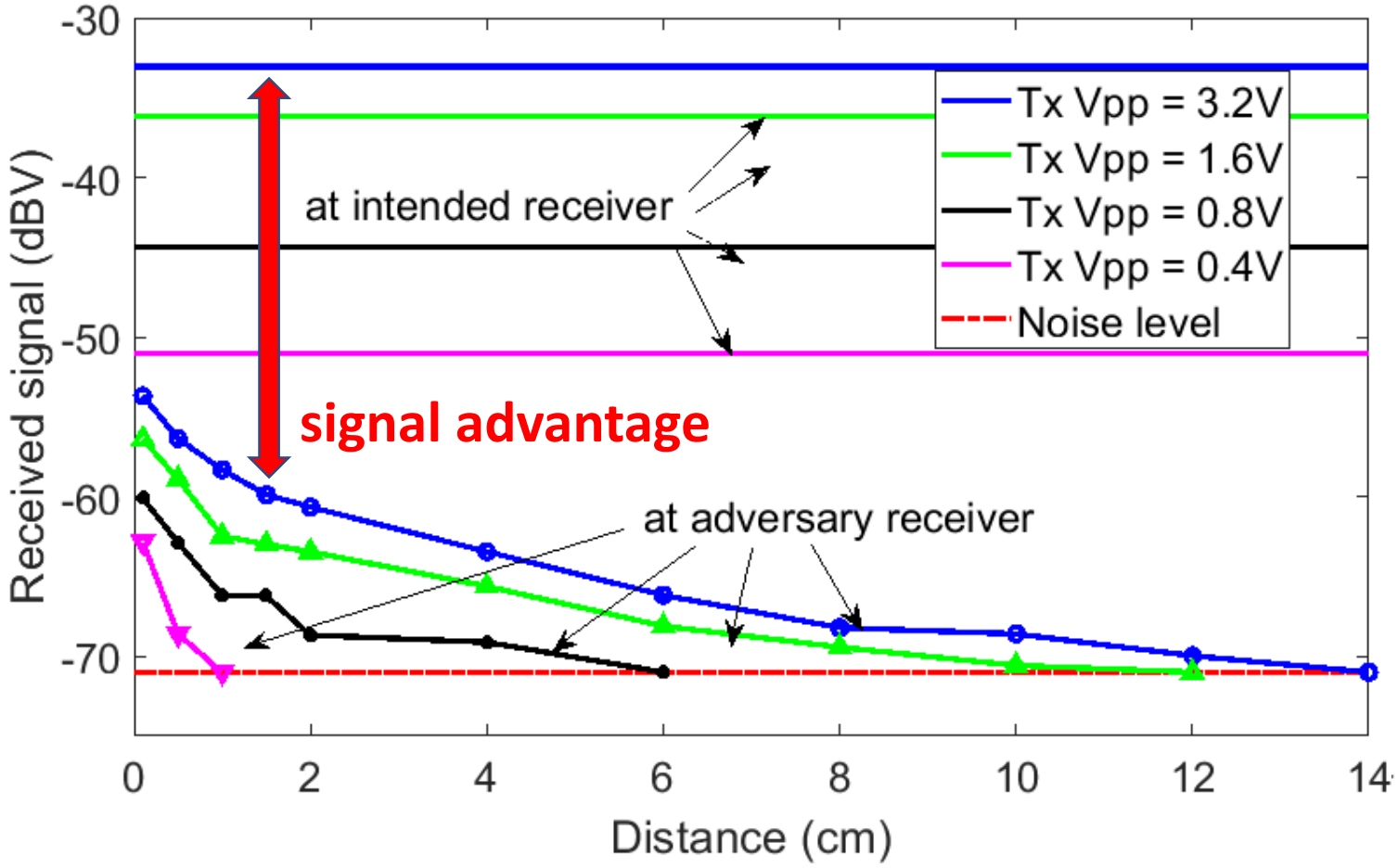
Protection against remote monitoring

Highly-confined signal

Per-touch authentication

Low-power



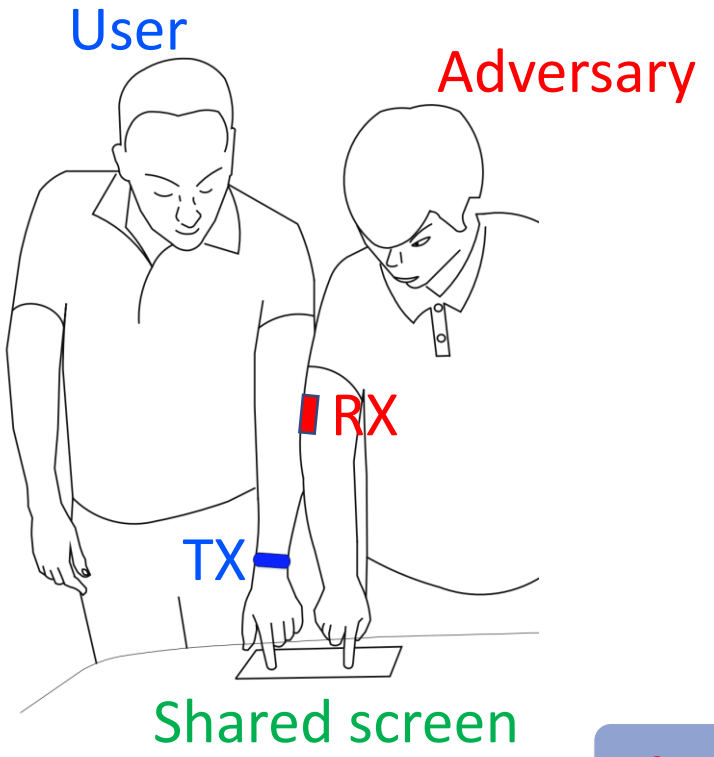


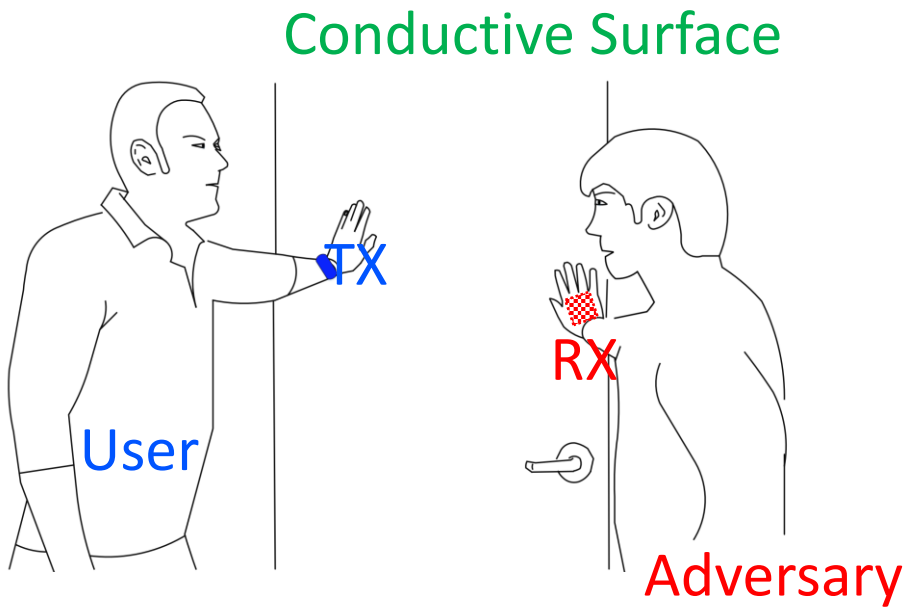
Protection against contacts

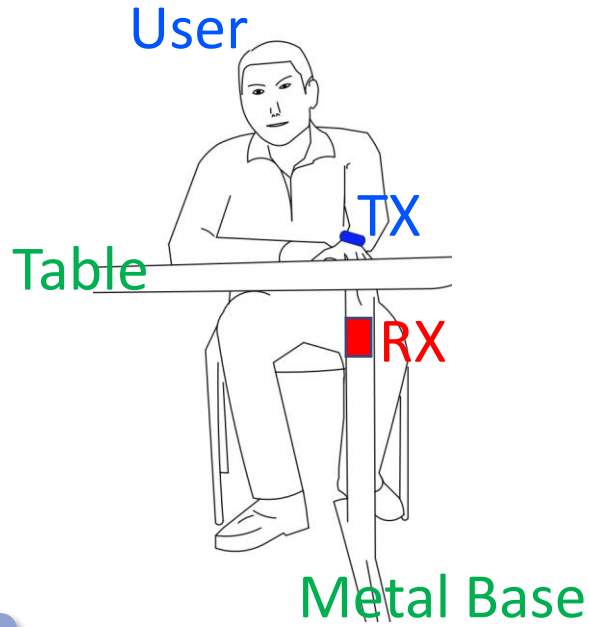
Highly-confined signal

Per-touch authentication

Low-power







Signal advantage is always greater than 10dB

No positive signal advantage possible for RF, NFC, etc.

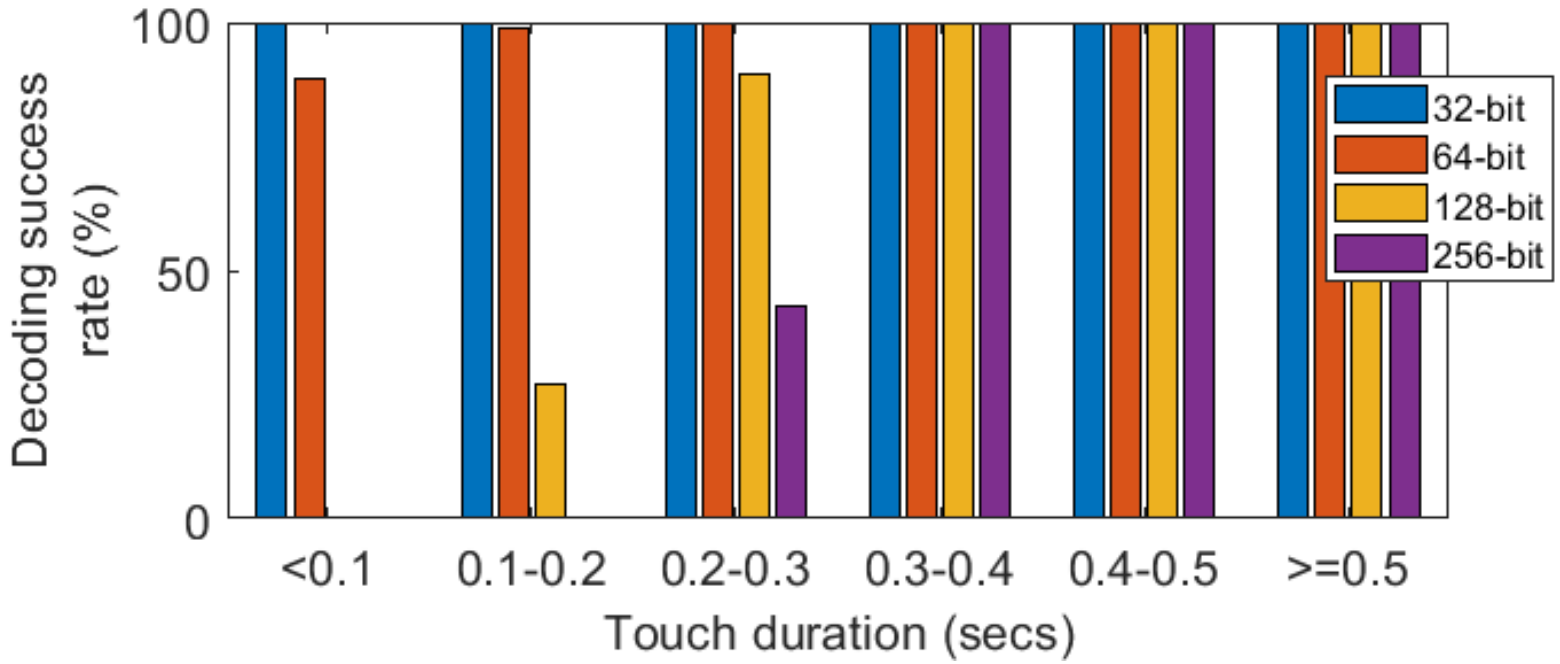
Per-touch authentication/identification

Highly-confined signal

Per-touch authentication

Low-power

- 2170 touches over 5 days
- Touch duration: 50.7ms - 1.78s
- 32, 64, 128, and 256-bit code
- Data rate: 1kbps



For 128-bit code: 89.5% accuracy for 200-300ms touch duration

100% for above 300ms touch duration

Power consumption

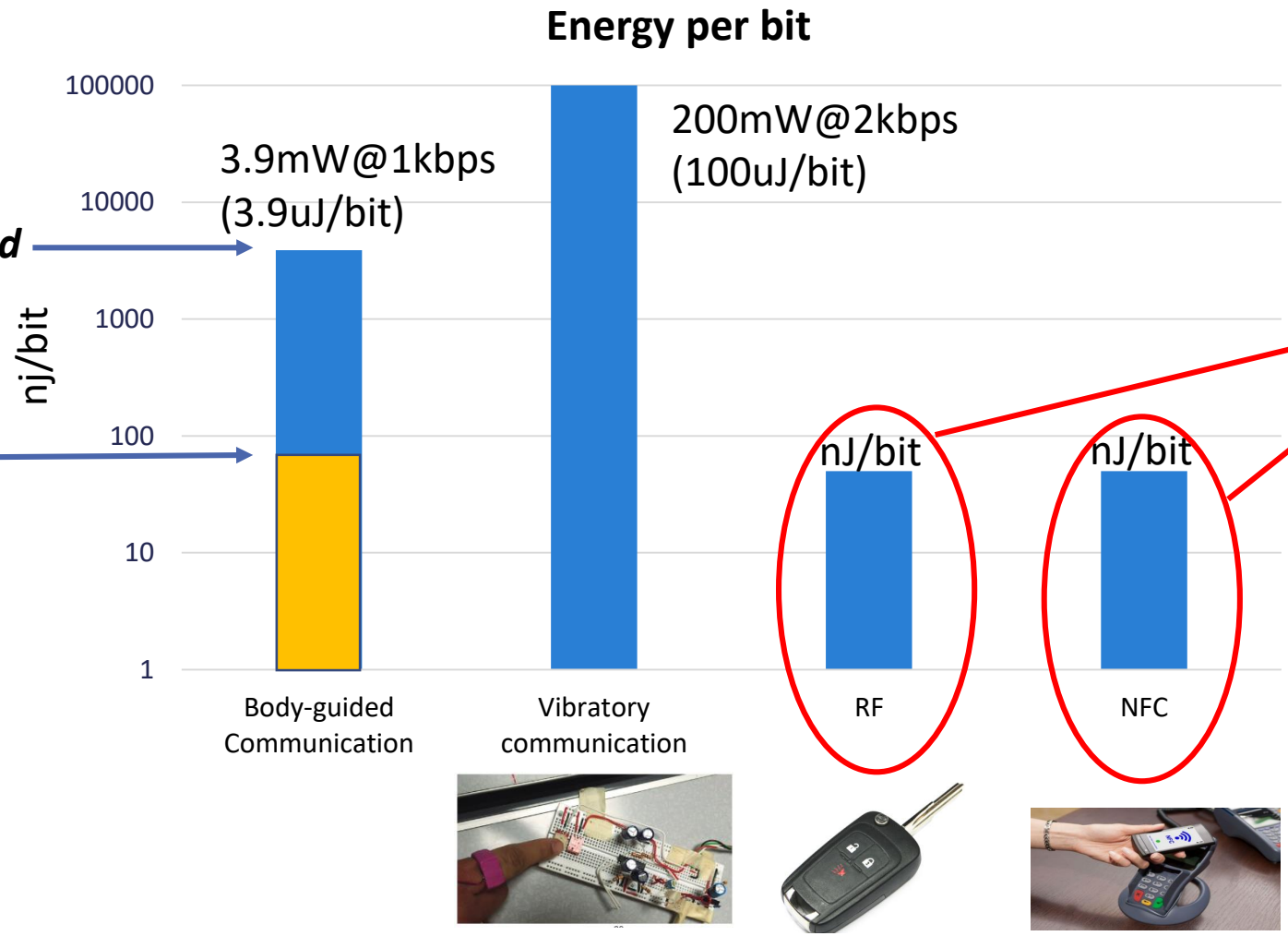
Highly-confined signal

Per-touch authentication

Low-power

Current MSP430-based prototype

Theoretical limit
90nJ/bit



Susceptible to eavesdropping
No touch association

Conclusion

- Proposed a body-guided communication method for securing every touch interaction from users with a variety of devices
- More secure against eavesdropping than other wireless methods
  - The signal received at the intended receiver is at least 20dB higher than that at an adversary's receiver in proximity
- Low power consumption
  - Token consumes 3.9uJ/bit, much lower than vibratory communication (per-touch communication)
- Robust per-touch authentication
  - Reliably deliver a 128-bit ID code on every touch longer than 300ms

Thank you!