Mobile Token-Based Authentication

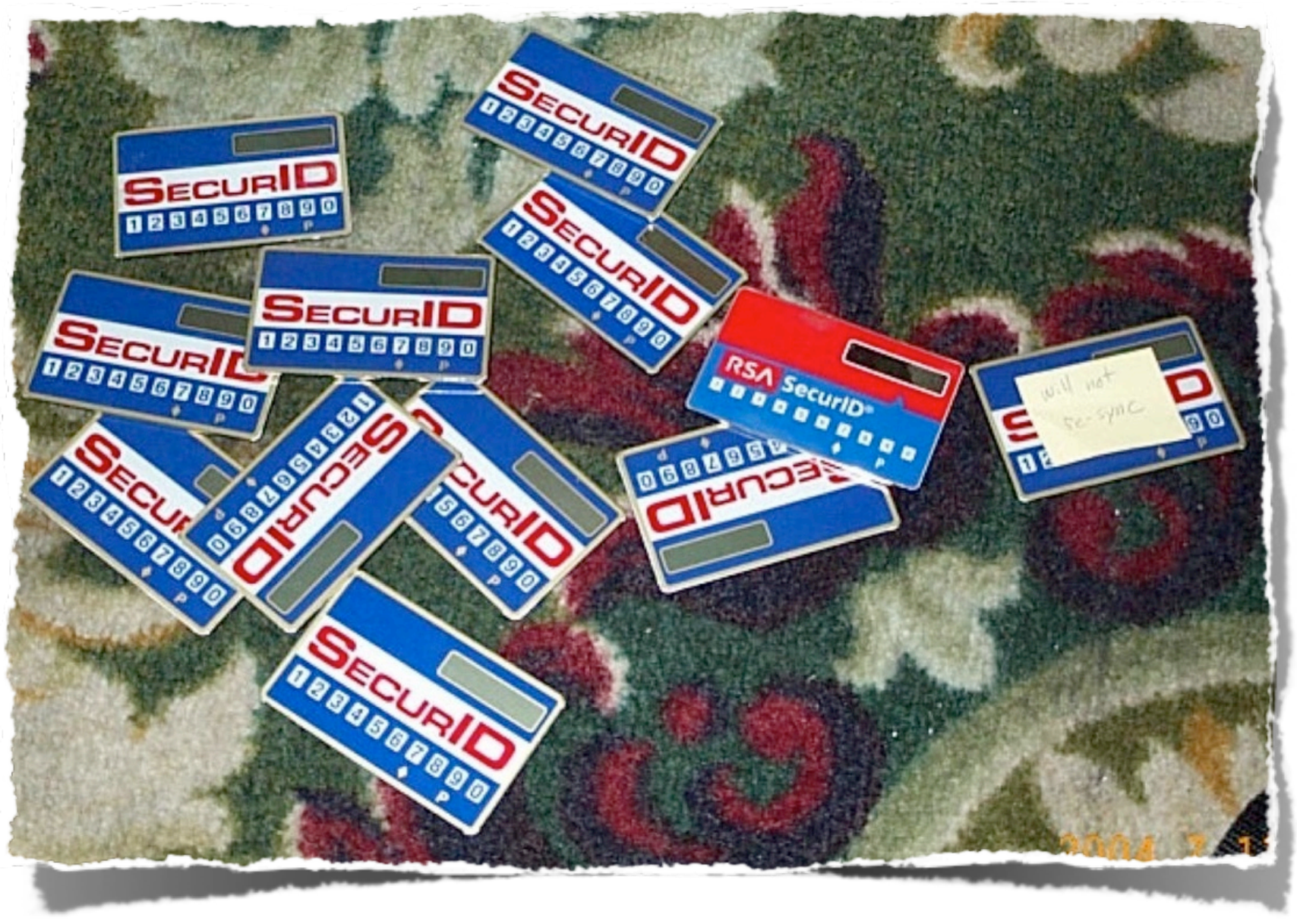
On a Budget

Hristo Bojinov Dan Boneh
Stanford Computer Security Lab

Stanford Computer Security Lab

The future of keys?

Motivation #1



Versatility of smartphones

Motivation #2

Smartphones vs. keys

$100

arbitrary apps

use all day

palm-size

fragile

Smartphones vs. keys

$100	$1
arbitrary apps	unlock doors
use all day	a few times daily
palm-size	tiny
fragile	tough

Talk overview

General theme: Unlocking smartphones

Talk overview

General theme: Unlocking smartphones

Part 1: About this work

- **Compass as a receiver**
- **Microphone as a receiver**
- **Cost and power**

Talk overview

General theme: Unlocking smartphones

Part 1: About this work

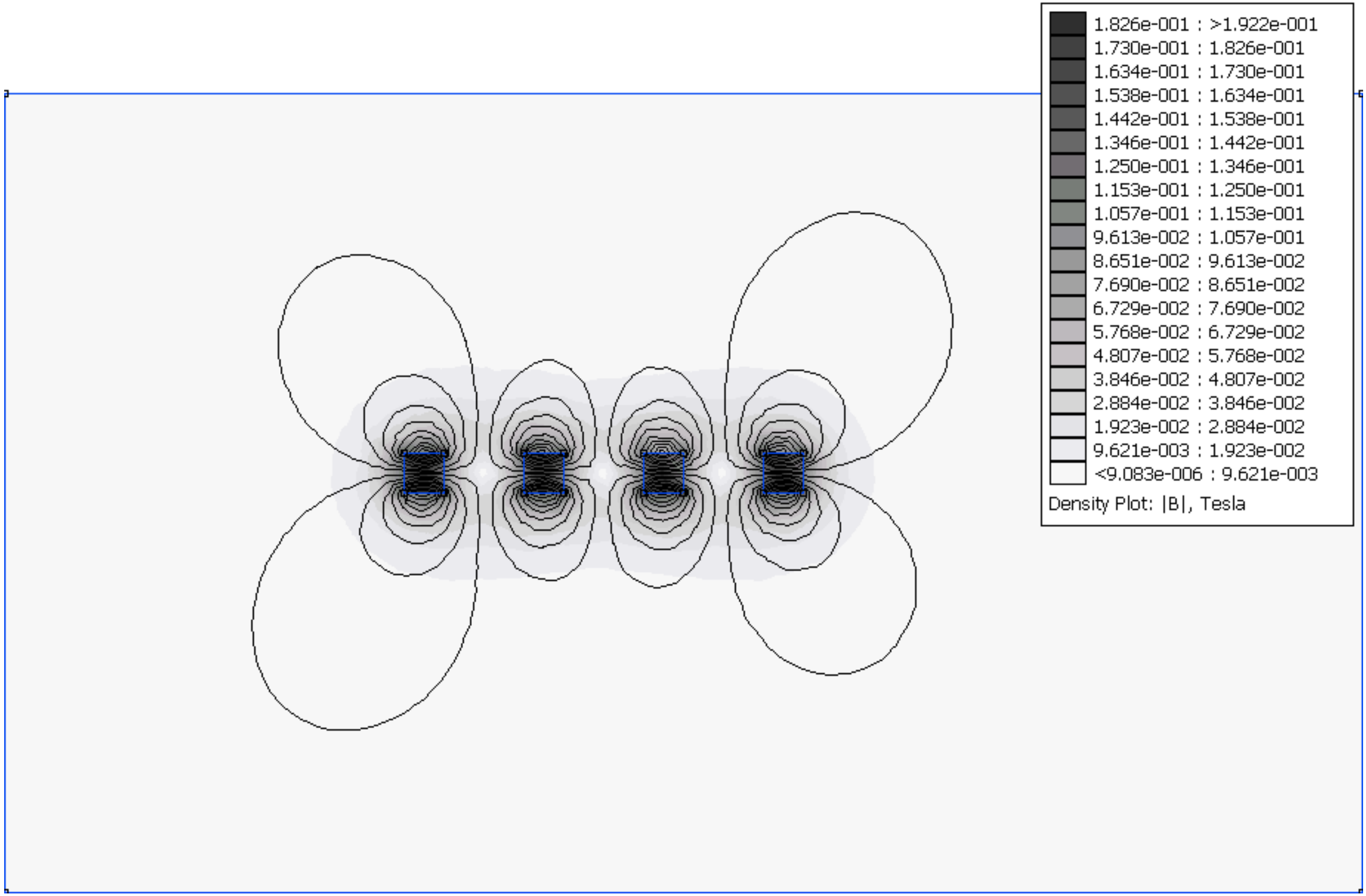
- **Compass as a receiver**
- **Microphone as a receiver**
- **Cost and power**

Part 2: On-going and future work

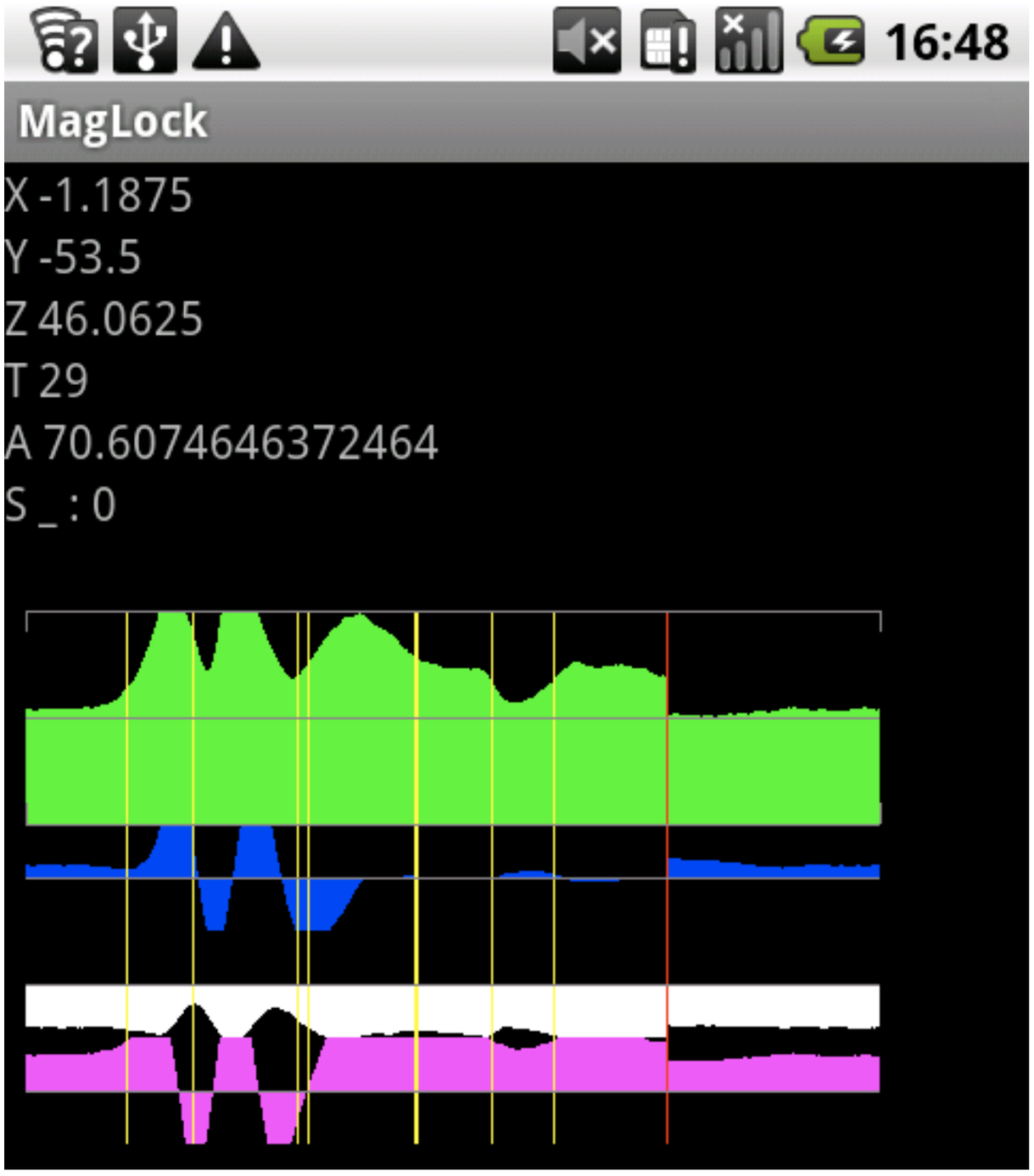
Compass

Stanford Computer Security Lab

Permanent magnets

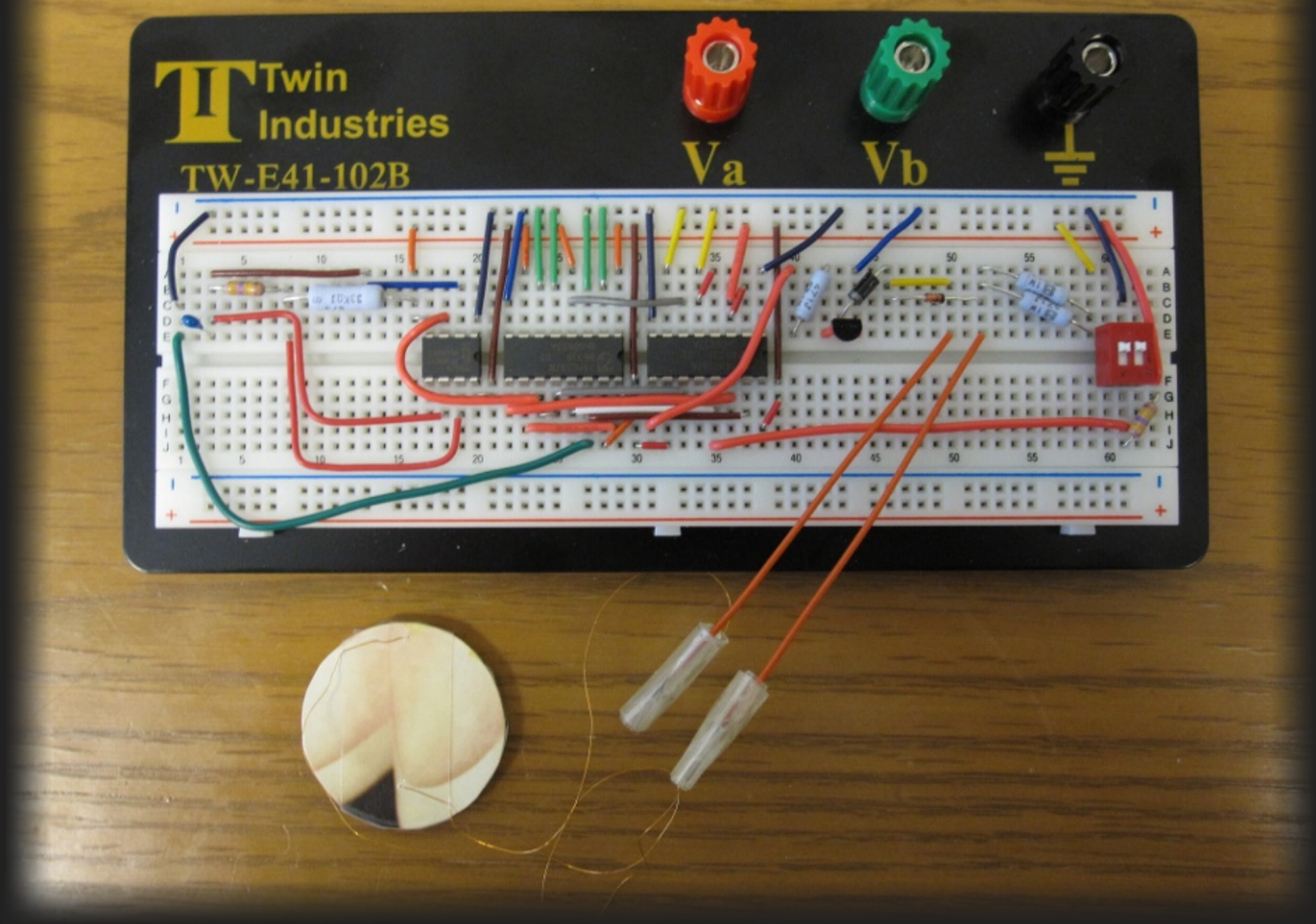


Permanent magnets *(continued)*

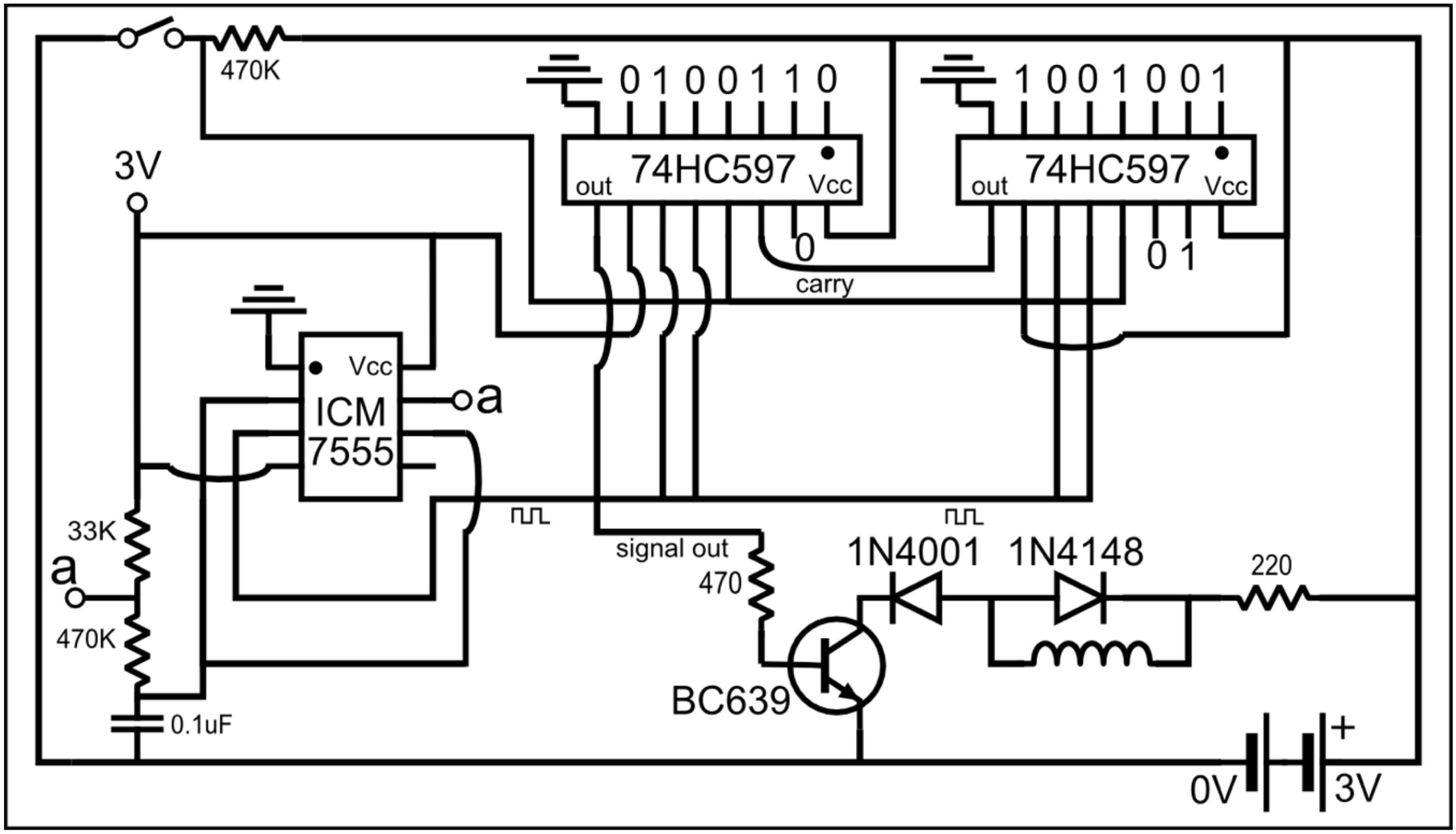


Poor resolution: distance to magnets is too great!

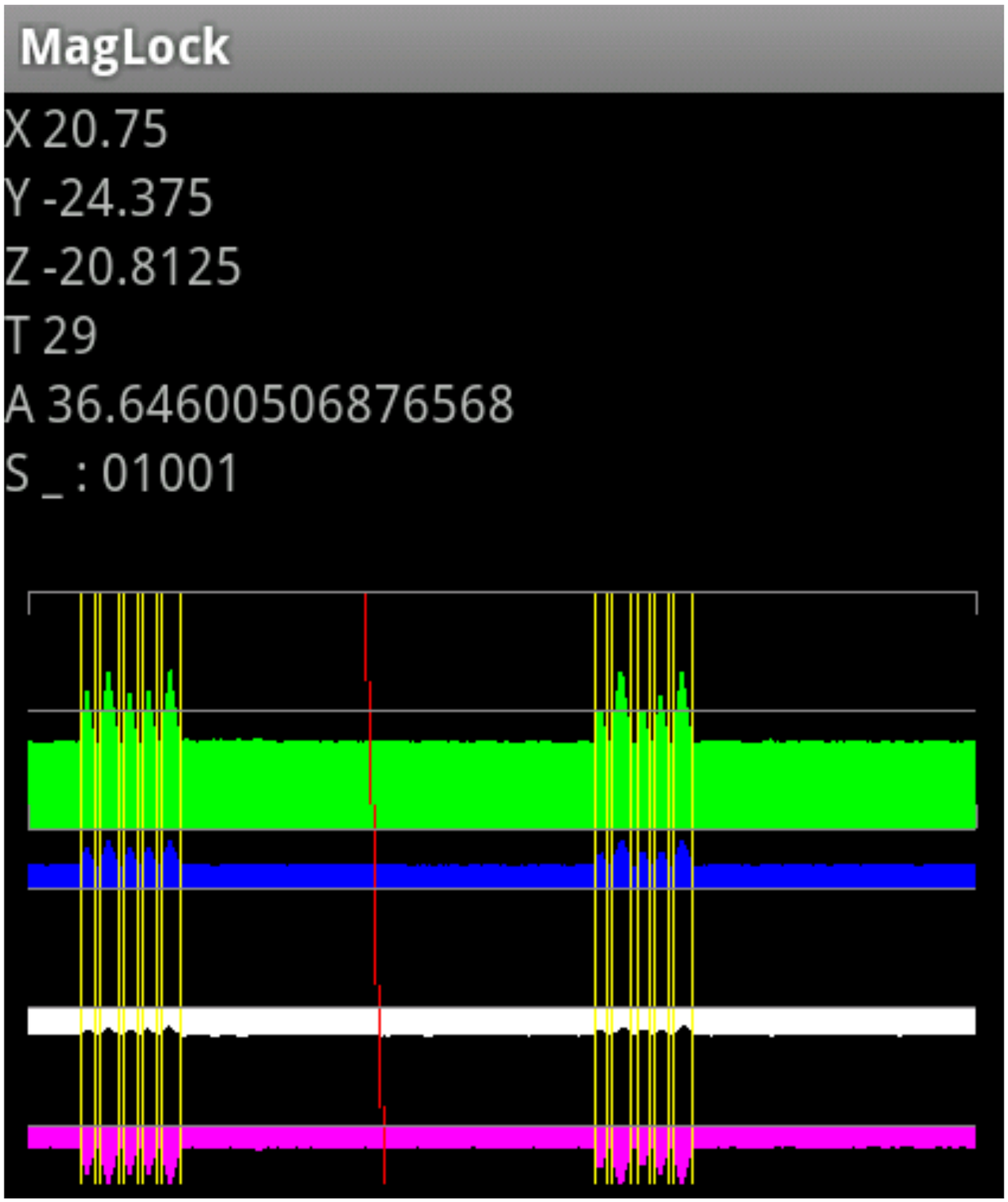
Magkey prototype



Magkey circuit

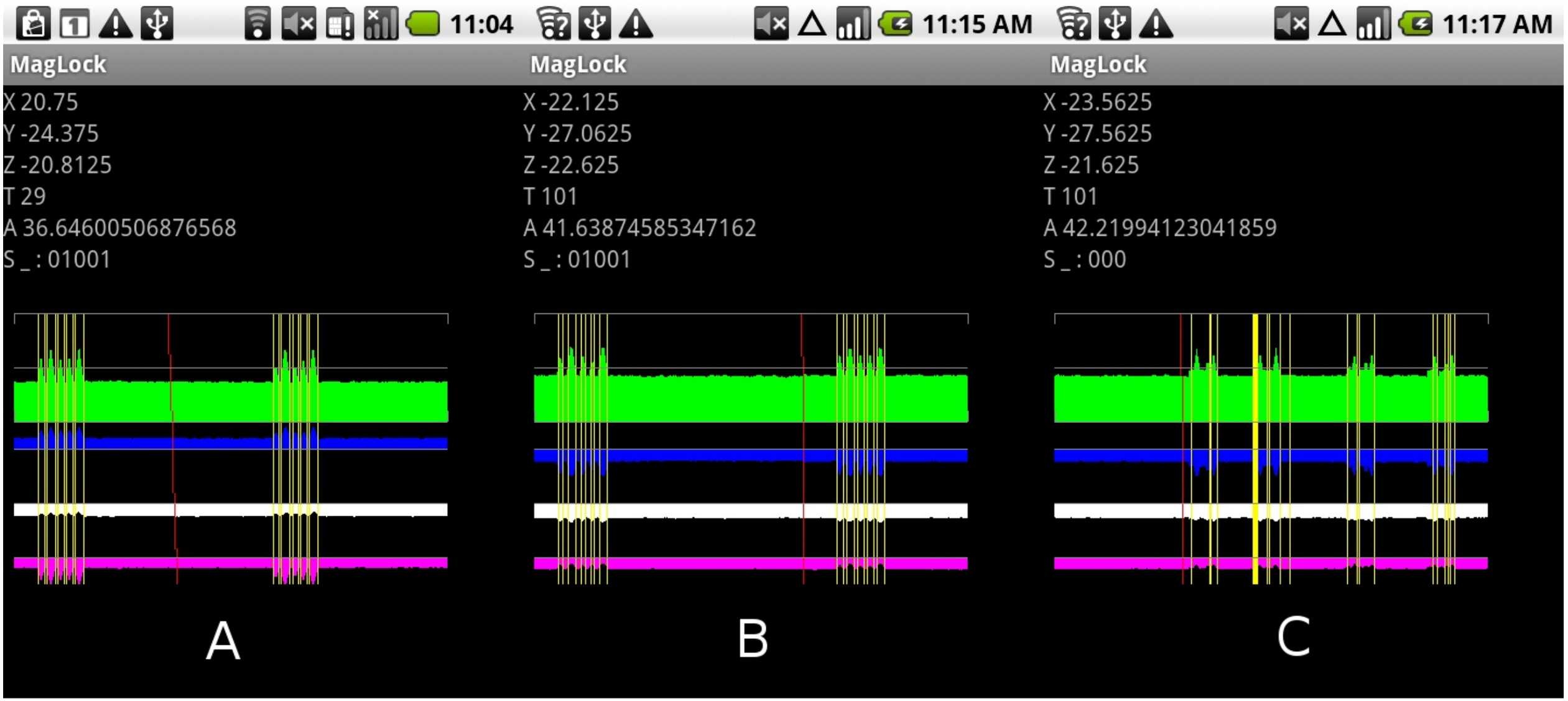


MagLock app



up to ~5 baud (N1)
about 1 inch range

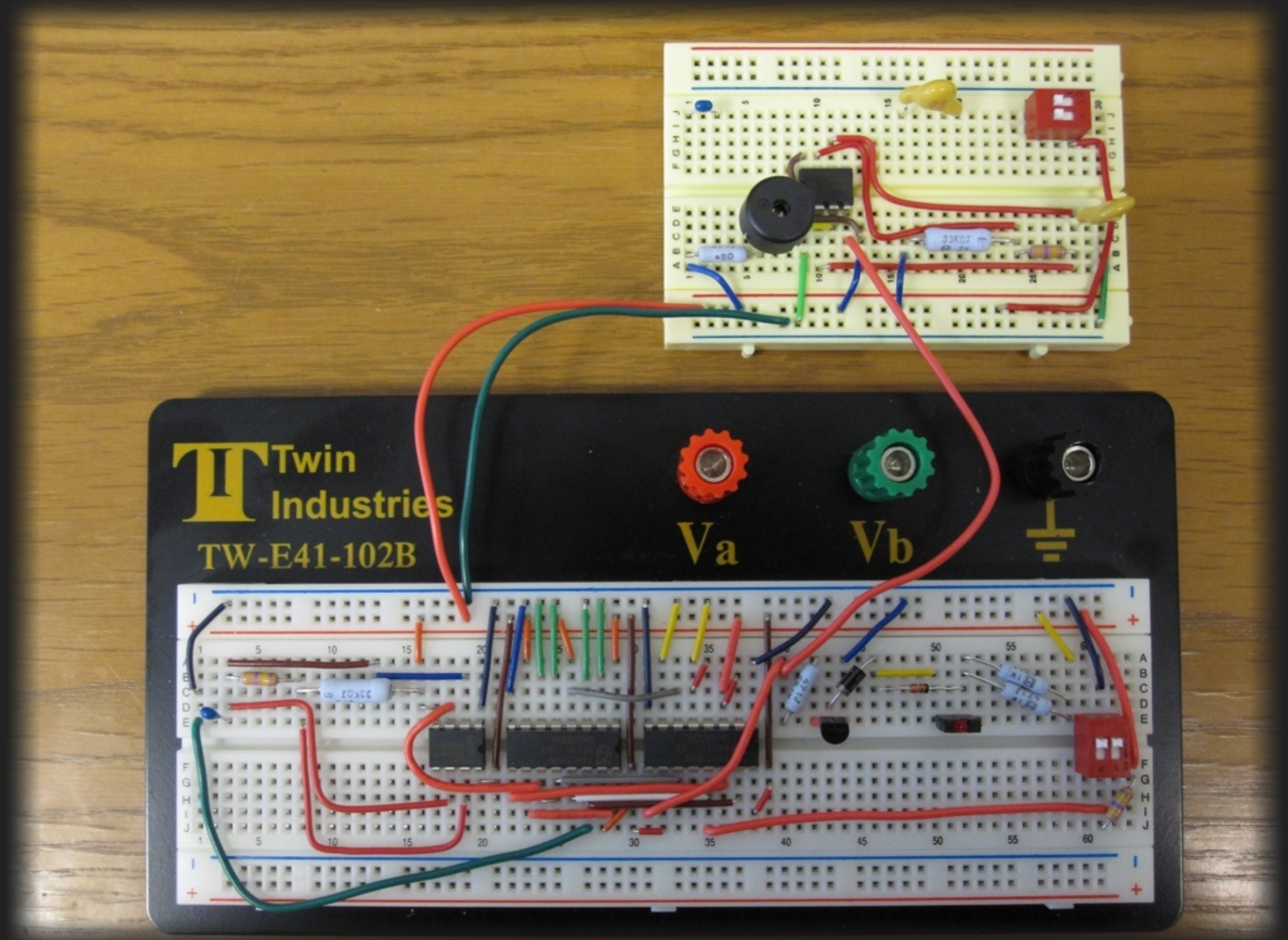
MagLock app


11:04
11:15 AM
11:17 AM
MagLock
X 20.75
Y -24.375
Z -20.8125
T 29
A 36.64600506876568
S _ : 01001
MagLock
X -22.125
Y -27.0625
Z -22.625
T 101
A 41.63874585347162
S _ : 01001
MagLock
X -23.5625
Y -27.5625
Z -21.625
T 101
A 42.21994123041859
S _ : 000
A
B
C

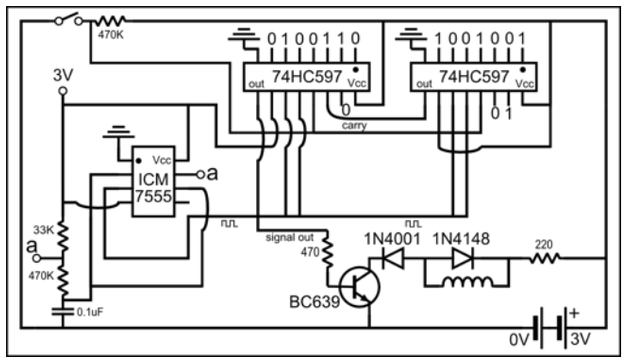
Microphone

Stanford Computer Security Lab

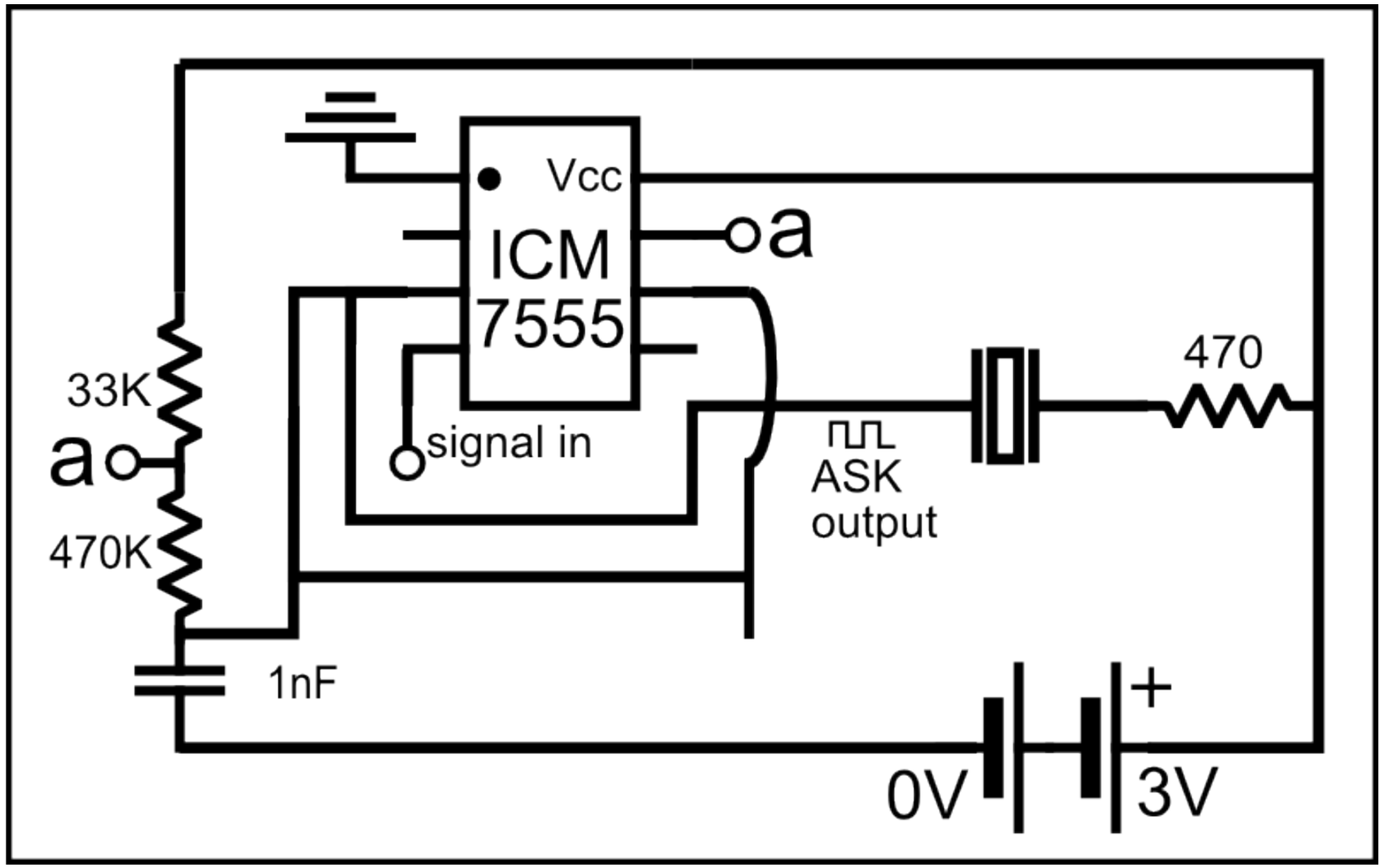
Mickey prototype



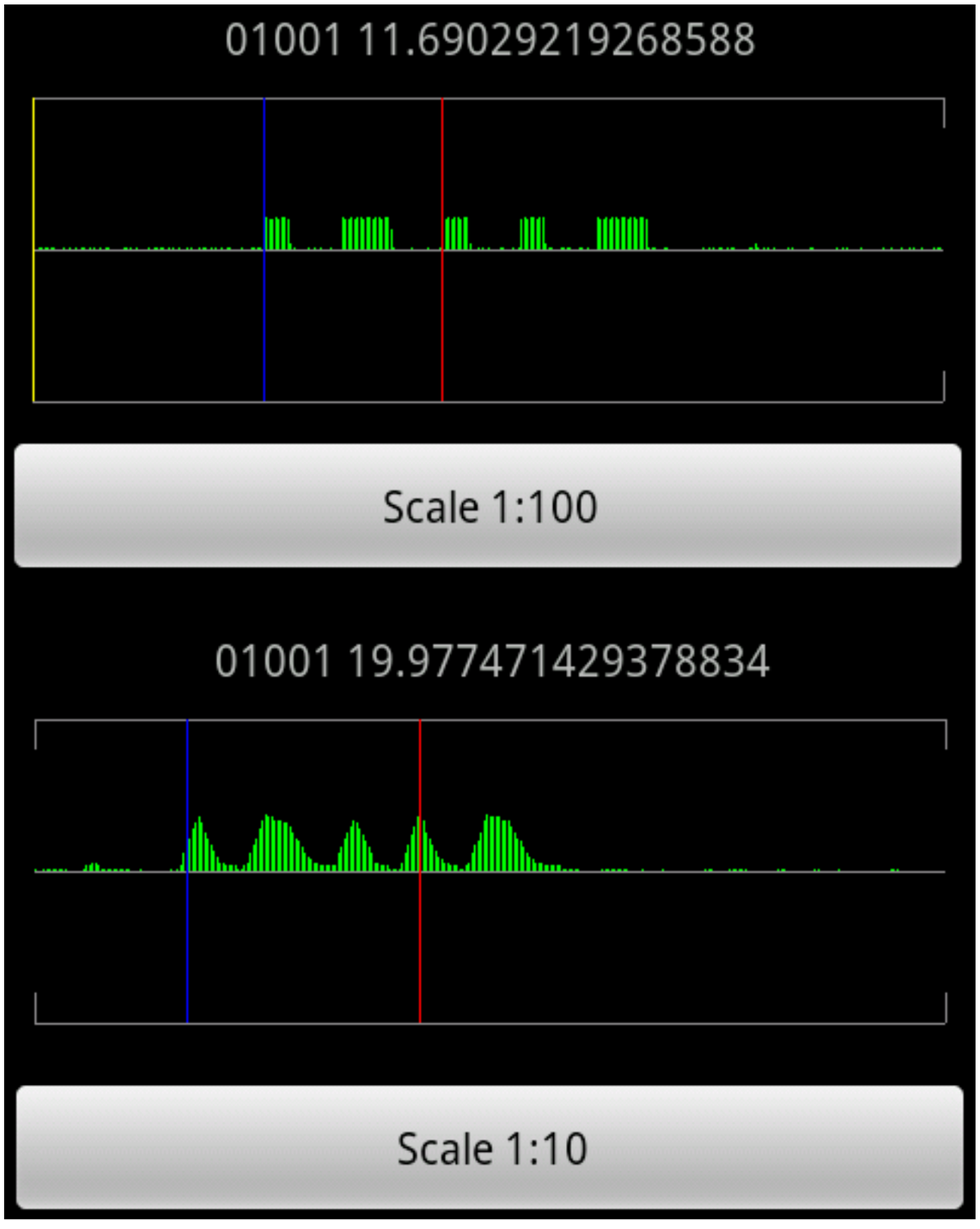
Mickey circuit



Magkey, minus the coil, plus:



MicLock app



up to ~100 baud (N1)
about 1 foot range

MicLock app


11:35
12:05
12:04
MicLock
MicLock
MicLock
Record
Record
Record
01001 11.69029219268588
01001 19.977471429378834
01001 19.977471429378834
Scale 1:100
Scale 1:100
Scale 1:10

Cost and Power

Stanford Computer Security Lab

Cost

Component	Unit cost	Magkey	Mickey
Timer IC	$0.20	$0.20	$0.40
Shift Register IC	$0.25	$0.50	$0.50
Discrete	*varies*	$0.37	$0.38
Total (Prototype)		$1.07	$1.28
PIC IC	*$0.38*	*$0.38*	*$0.38*
Total (PIC)		*$0.75*	*$0.76*

Current and longevity

Current Mode	Magkey	Mickey
Average	6.91mA	0.23mA
Peak	16.00mA	0.25mA
Continuous	210 hrs	6500 hrs
On-demand	>5 yrs	>10 yrs

What's Next?

Stanford Computer Security Lab

Low-power wireless

Contactless cards (e.g. NFC)

- No batteries required in token
- Off-the-shelf tokens: today
- Short practical range

Low-power wireless

Contactless cards (e.g. NFC)

- No batteries required in token
- Off-the-shelf tokens: today
- Short practical range

Bluetooth 4.0 (Low-energy)

- Might be more pervasive than NFC: laptops, PCs
- Designed for long-term, synchronous operation
- A decent alternative we might consider

So, what is next?

Prove token authentication viability (mobile devices)

- Analyze more [proprietary] technologies
- Influence NFC security agenda

So, what is next?

Prove token authentication viability (mobile devices)

- Analyze more [proprietary] technologies
- Influence NFC security agenda

Develop end-to-end token authentication theme

- Authentication on the web, multi-tenant tokens
- PC authentication... keychains, PAM, Windows?

Conclusion

Conclusion

Massive opportunity to redo user authentication:

- Phones are the most versatile computers to date
  - ★ *Rapid, on-going evolution, diverse inputs*
- Momentum to standardize light-weight wireless
- Threats are more abundant than ever before

Address local, mobile app, and web authentication.

Drive the security agenda into standards efforts.

Time for Q&A.

http://seclab.stanford.edu

Stanford Computer Security Lab