

Embedded Security

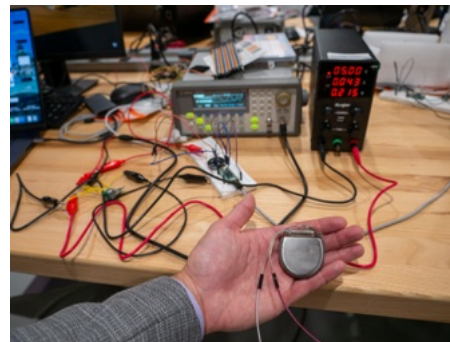
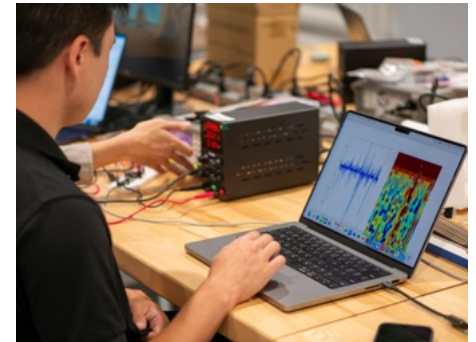
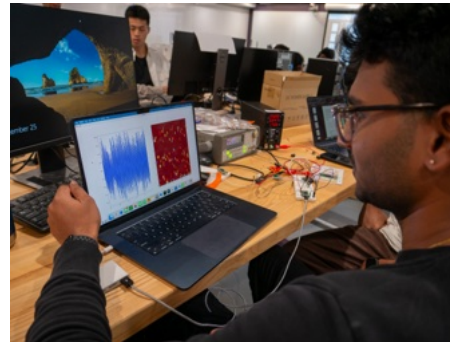
EECE 5698-08: Special Topics: Cyber-Physical Security of IoT Systems in the Age of AI

Lecture 9: Clocks, Time Travel, & Fuming Nitric Acid

Prof. Kevin Fu

November 6, 2025

<https://spqrlab1.github.io/emsec/>



Today's Learning Goals

- Learn how to synthesize timers for embedded security
 - Create a timer from SRAM decay
 - Can use to thwart brute force attacks on smartcards
- Dopant-level hardware trojans
- Using fuming nitric acid and microscopes to reverse engineer cryptographic hardware

TARDIS

Time and Remanence Decay in SRAM
to Implement Secure Protocols on
Embedded Devices without Clocks

Amir Rahmati¹, Mastooreh Salajegheh¹, Dan Holcomb²,
Jacob Sorber³, Wayne Burleson¹, Kevin Fu¹

¹ UMass Amherst ² UC Berkeley, ³ Dartmouth College

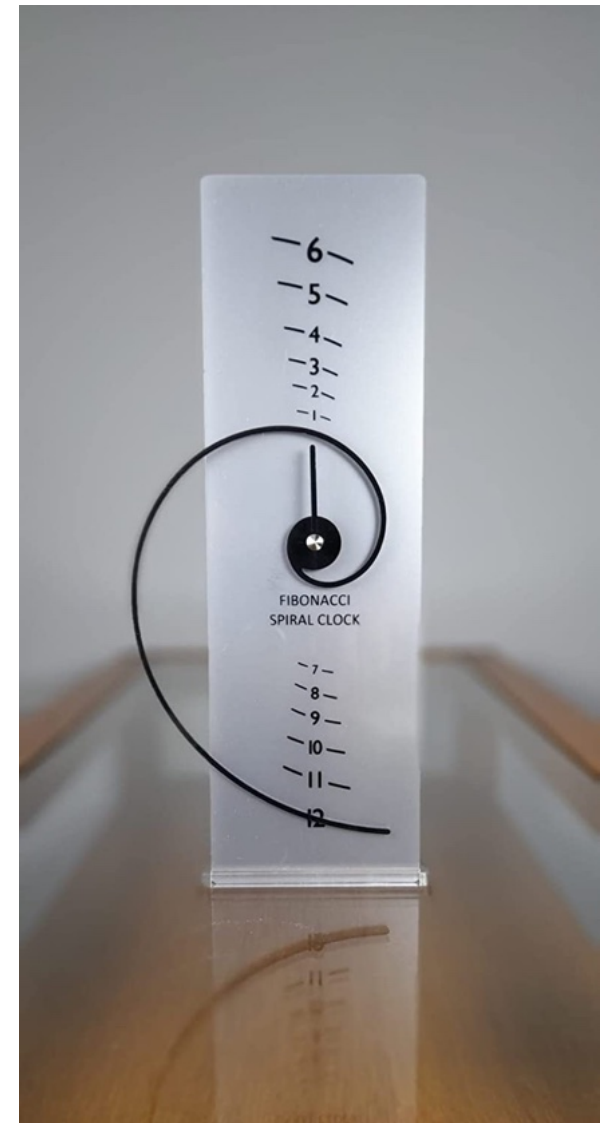


Water Clock

This large, bulky contrivance gives the time accurate to within half an hour per day since it was last set. It requires a source of water, and it must be kept still because it marks time by the regulated flow of droplets of water. It is primarily an amusement for the wealthy and a tool for the student of arcane lore. Most people have no way to tell exact time, and there's little point in knowing that it is 2:30 p.m. if nobody else does.

Price: 1,000 gp
Weight: 200 lb

Advertisements



<https://holiviantales.wordpress.com/the-marketplace/tools-and-skill-kits/water-clock/>

https://www.amazon.com/Fibonacci-Clocks-Spiral-Clock-Silver/dp/B09SJ4MIG5/ref=asc_df_B09SJ4MIG5/

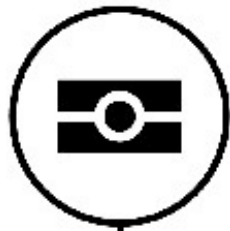
Batteryless Devices



Transportation



e-Passport
symbol



- No long running clocks
- Adversary controls power & time
- Hold secrets

Passports



Employee
IDs

Security Vulnerabilities

Breaking Mifare DESFire MF3ICD40:
Power Analysis and Templates in the Real World*

David Oswald and Christof Paar
Horst Görtz Institute for IT Security
Ruhr-University Bochum, Germany
(david.oswald, christof.paar)@rub.de

... of side-channel analysis, implementations of
... a new threat: by exploiting the phys-
... are able to break algorithms or
... which no efficient analytical, non-
... demonstrate practical, non-
... MF3ICD40 contact-
... 12-bit

rd hack details revealed

hack one of the
lar smartcards
d online.

for Bart
Radboud
als a



“recording 4000 traces
is a matter of minutes.”

Fare H
Flaw Is

By Beth Winegarner Wed

Not that we think you w
in your wallet, allowing yo
funnel money away from the

Keywords: contactless
DESFire.

1 Introduction

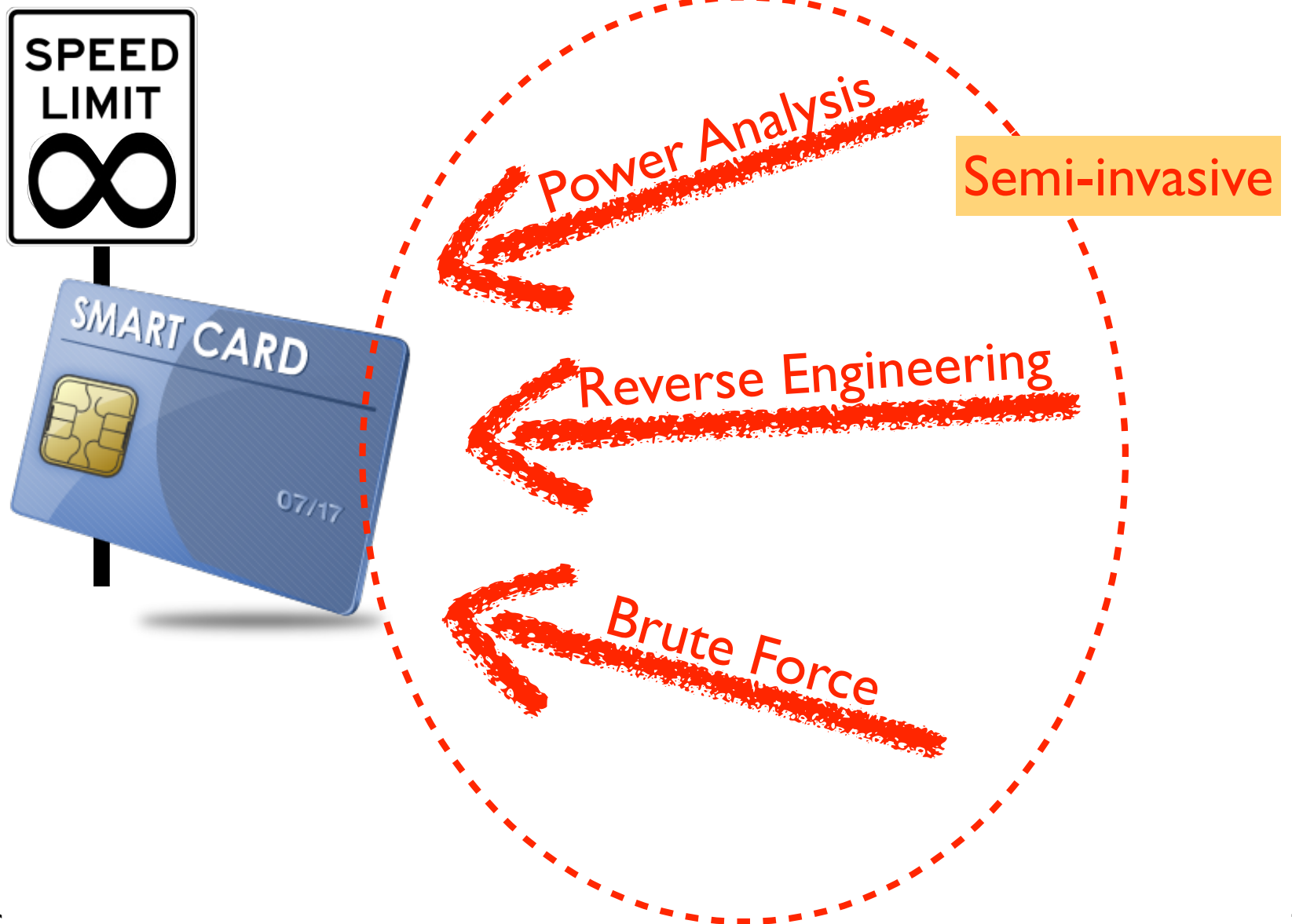
Radio Frequency Identification (RFID) technology has become numerous large-scale, security-relevant applications, including public wireless payment, access control, or digital identification [39]. The information stored on RFID smartcards, e.g., personal data, or cash balance, is often highly sensitive — however, the access to the air interface and to the device itself is virtually impossible to control. Hence, most modern RFIDs feature cryptographic mechanisms, including encryption and authentication, in order to thwart attacks such as eavesdropping, manipulation, or cloning of a smartcard.

Mifare DESFire MF3ICD40 is a contactless smartcard featuring a cryptographic engine for authentication and encryption based on (Triple-)DES. The smartcard is employed in several large payment and public transport systems around the world, e.g., the Czech railway in-karta [7], the Australian myki card [36], or the Clippercard used in San Francisco [40]. In the course of our

The work described in this paper has been supported in part by the European Commission through the ICT programme under contract ICT-2007-216676 ECRYPT

© 2011, LNCS 6917, pp. 207–222, 2011.
Commission for Cryptologic Research 2011

Smart Card Threats



Vulnerable to Brute Force Attacks

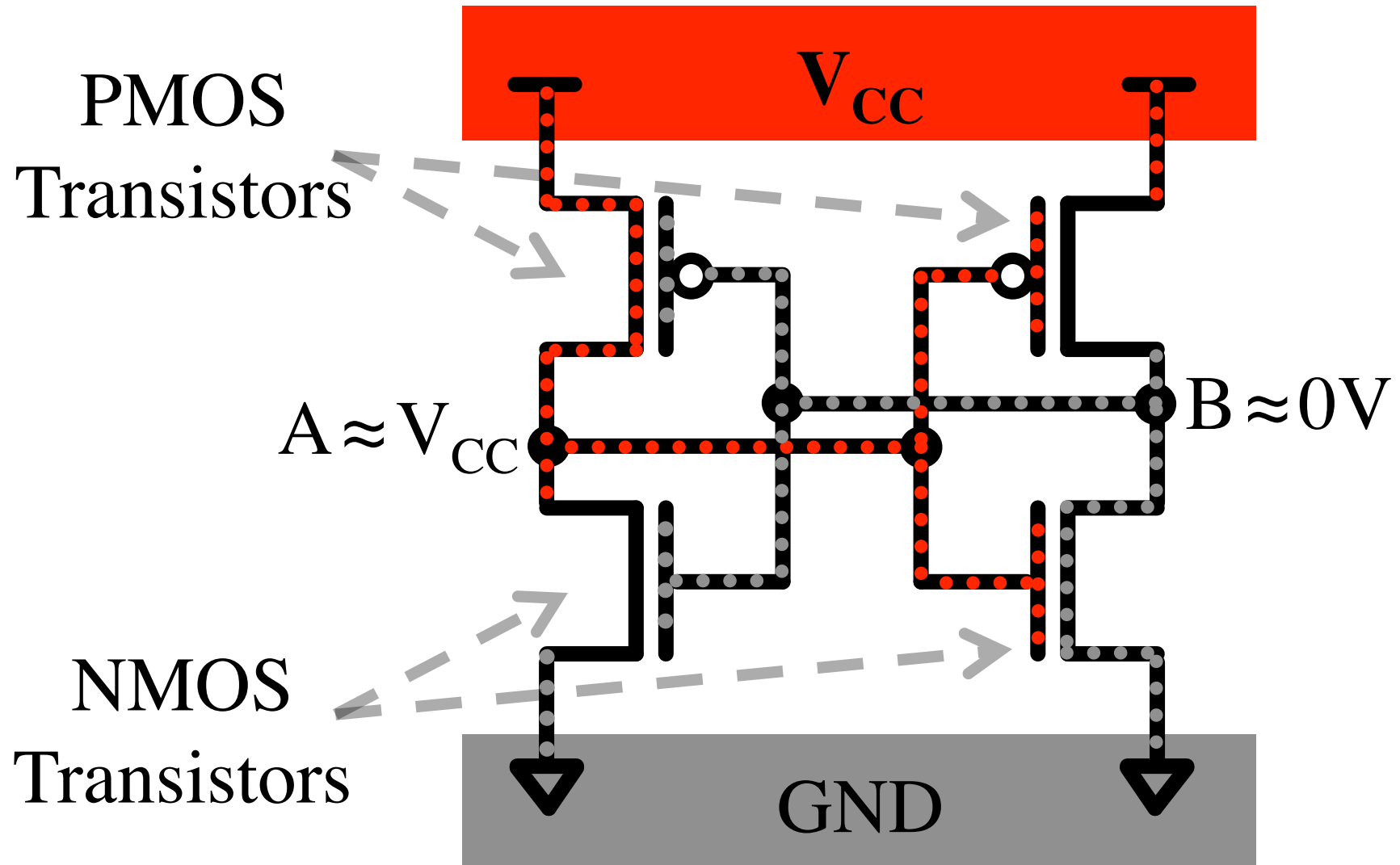
Device	#Queries	Time
UHF RFID Tags[Shamir'07]	200	2 Seconds
MIFARE Classic[Garcia'09]	1,500	16 Seconds
Digital Signal Transponder[Bono'05]	75,000	1 Hour
MIFARE DESFire[Paar'11]	250,000	7 Hours
GSM SIM Cards[Goldberg'99]	150,000	8 Hours



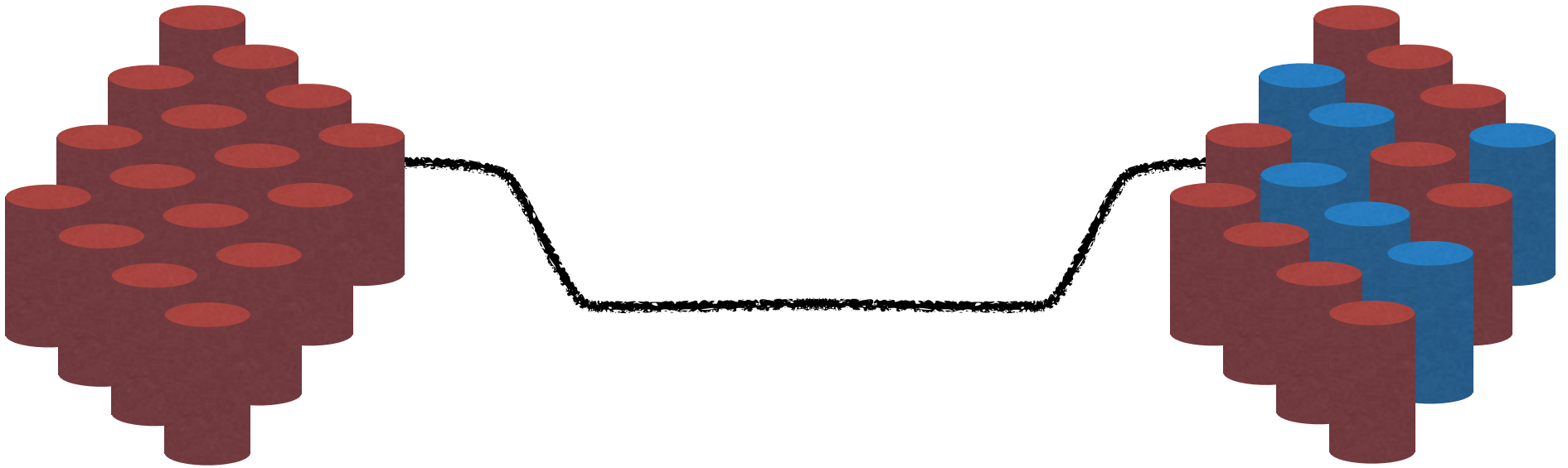
Our Contribution: TARDIS

A time-keeping technique based on SRAM decay

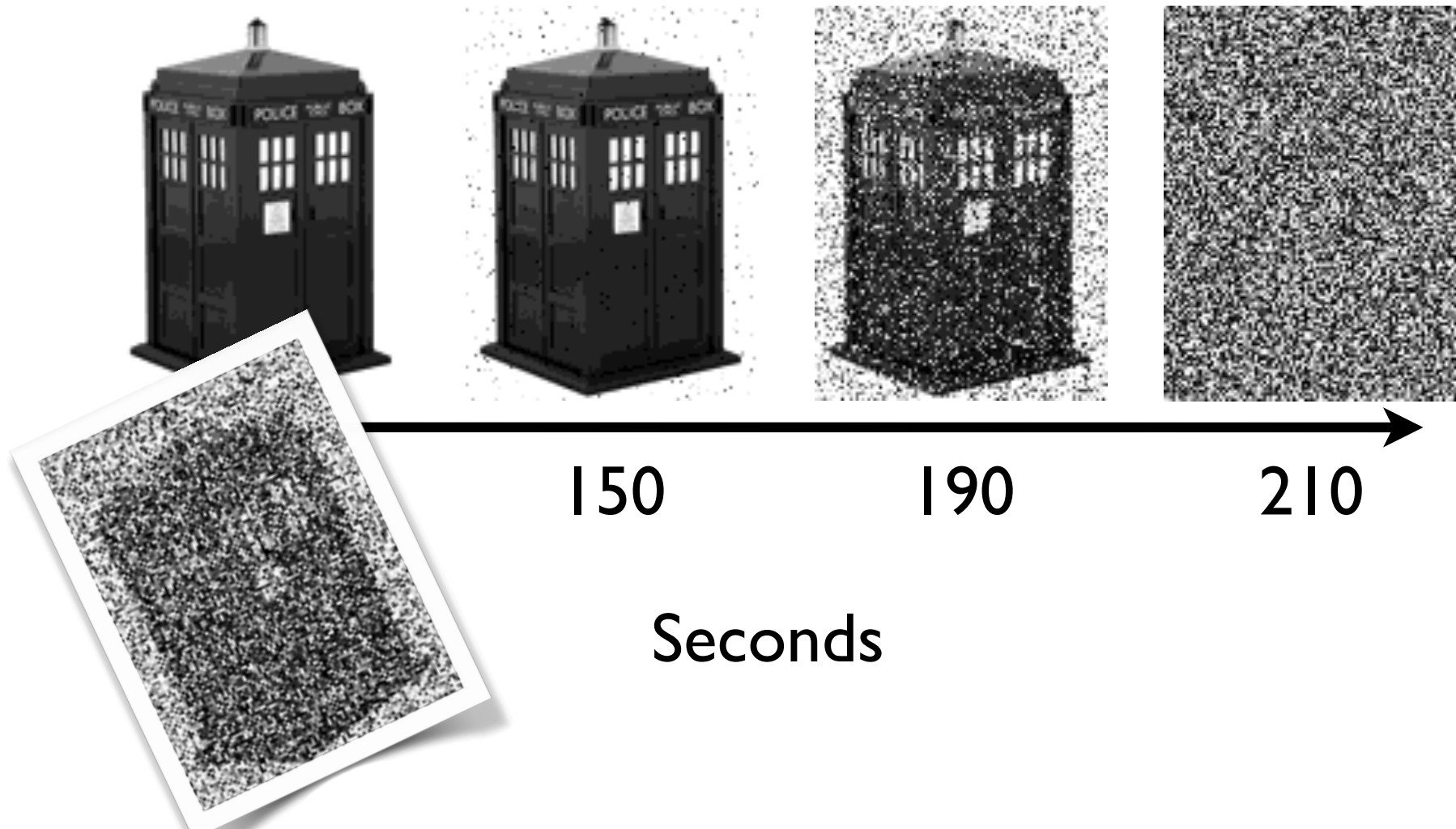
SRAM Remanence



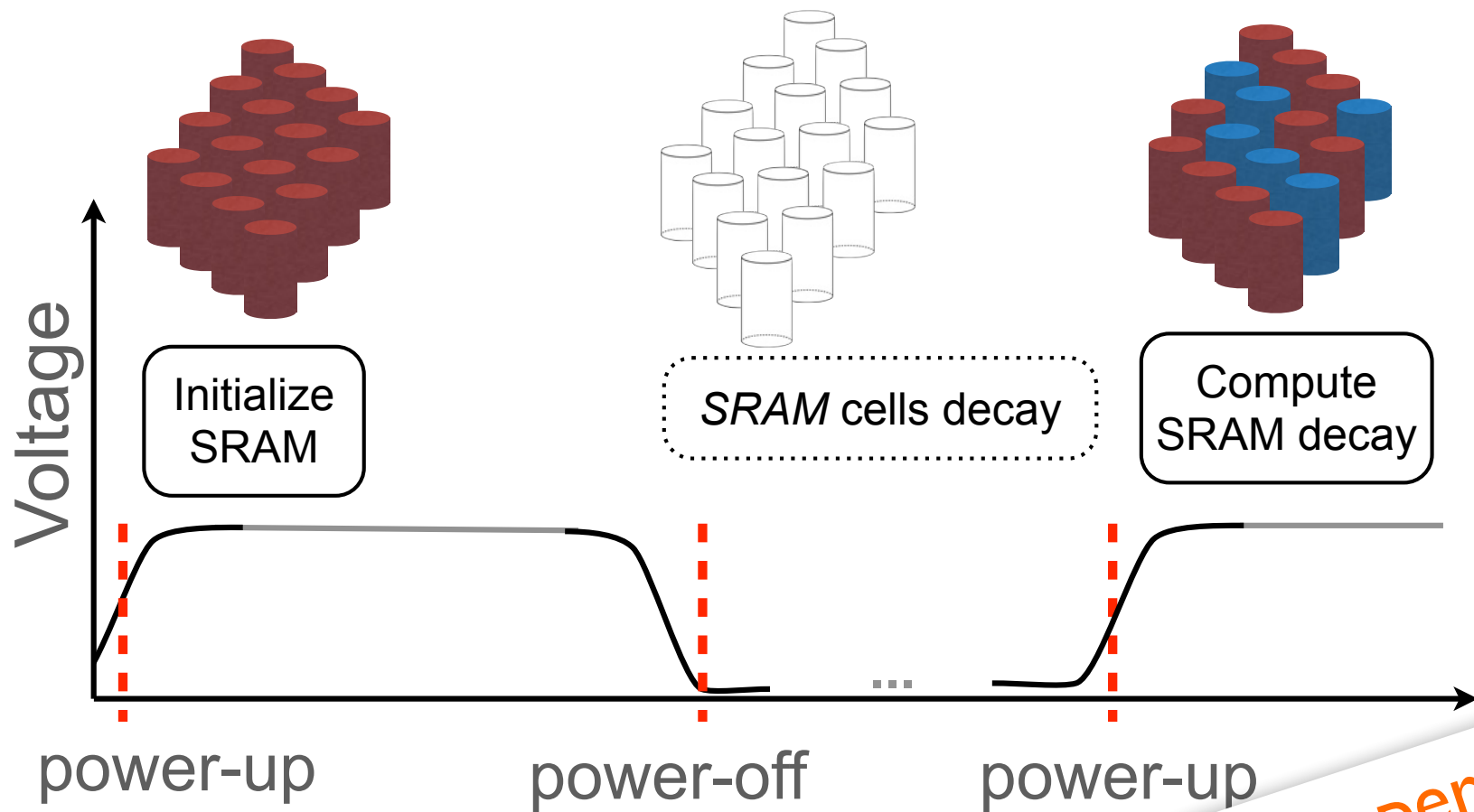
SRAM Remanence



SRAM Remanence



The TARDIS Algorithm

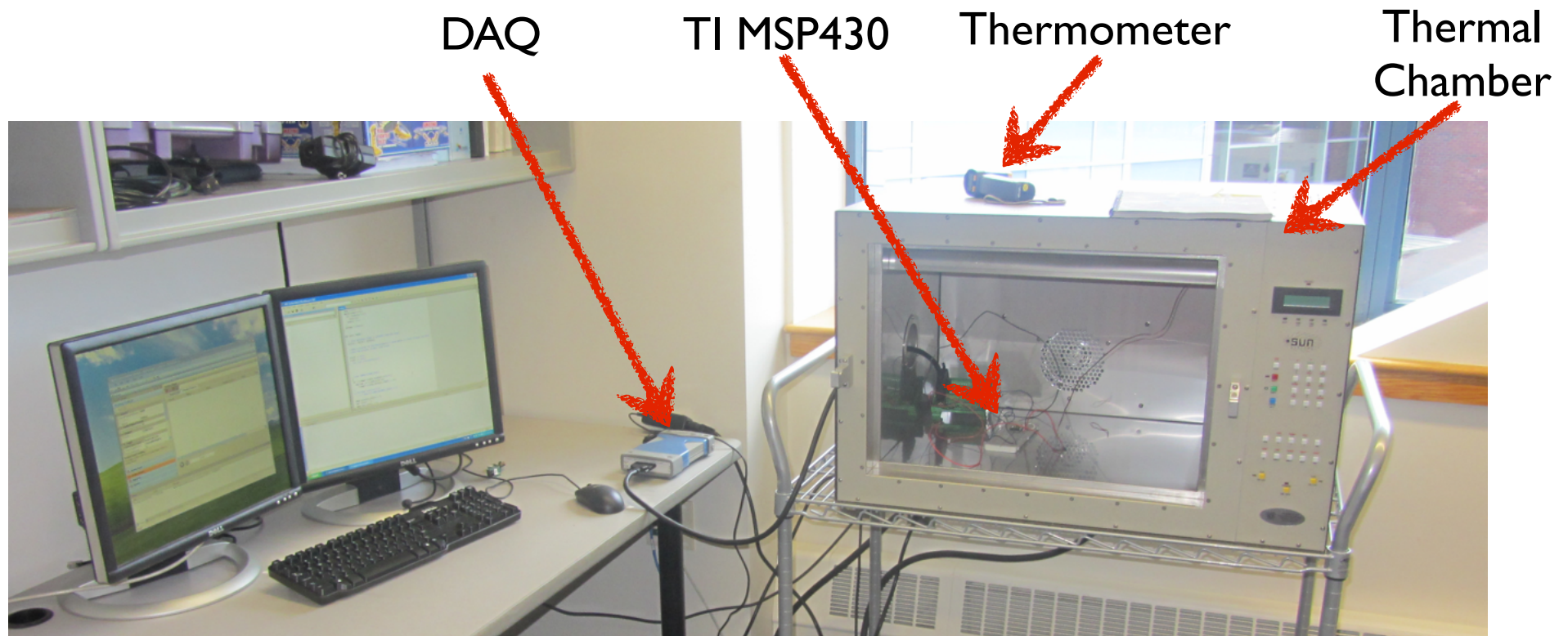


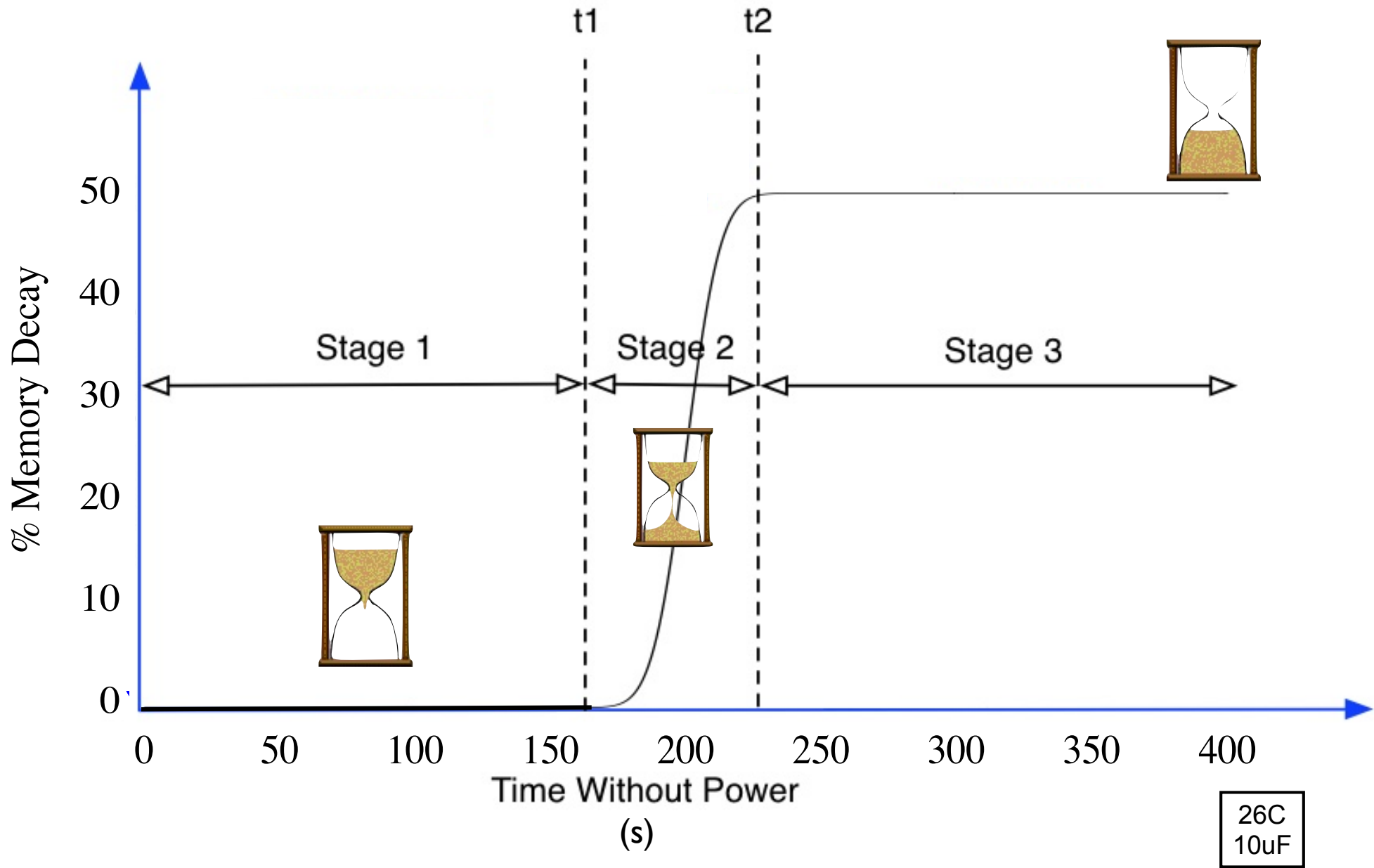
Temperature
Later...

Factors Influencing SRAM Decay

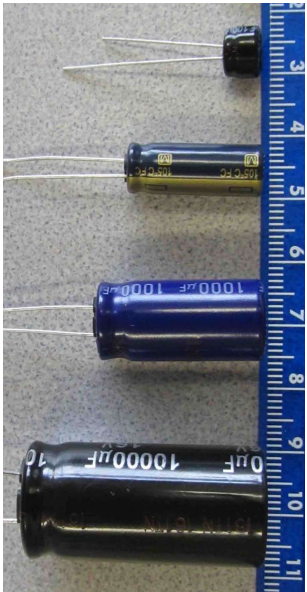
- ✓ SRAM Size
- ✓ Circuit Capacitance
- ✓ Temperature
- ✗ Chip Variation

Experimental Setup





Circuit Capacitance

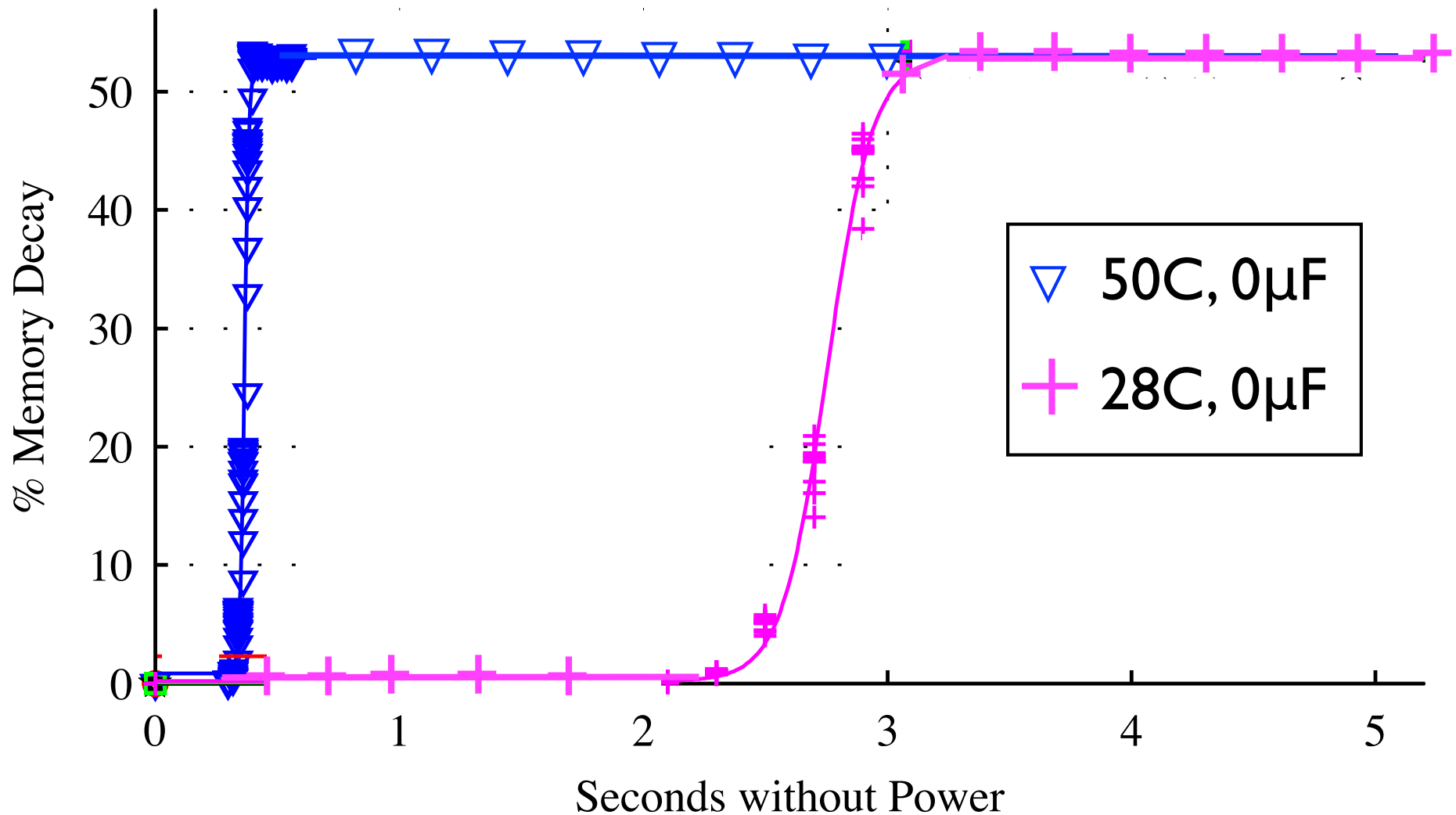


Capacitor Size	Expiration time	Scale
$\sim 0\mu\text{F}$	$2.1 \times 10^0 \text{s}$	Seconds
$10\mu\text{F}$	$2.25 \times 10^2 \text{s}$	Minutes
$100\mu\text{F}$	$1.98 \times 10^3 \text{s}$	1/2 Hour
$1000\mu\text{F}$	$2.12 \times 10^4 \text{s}$	Hours
$10000\mu\text{F}$	$> 1.96 \times 10^5 \text{s}$	Days

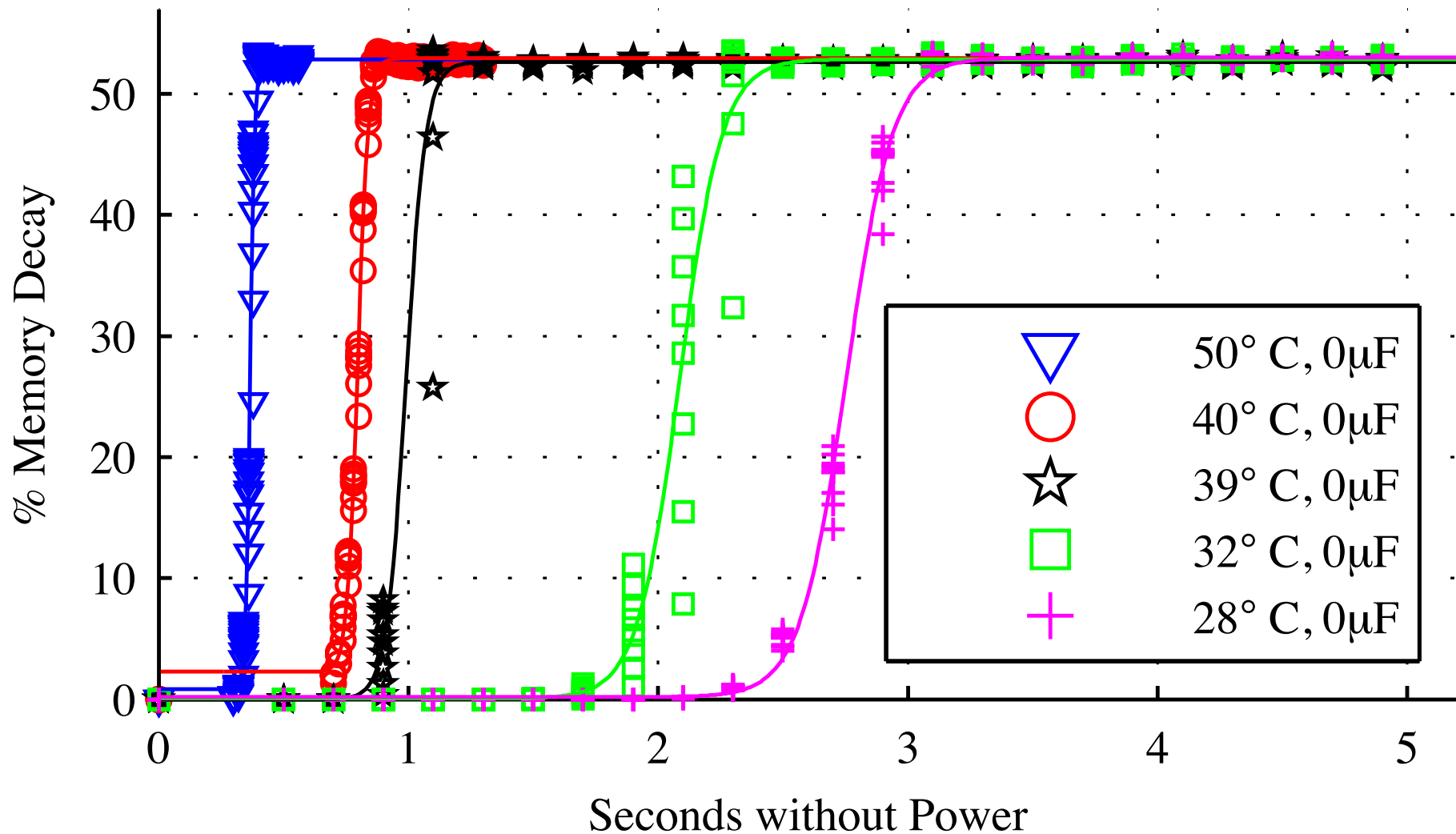
Smart Cards

Batteryless Sensor = 100,000 μF

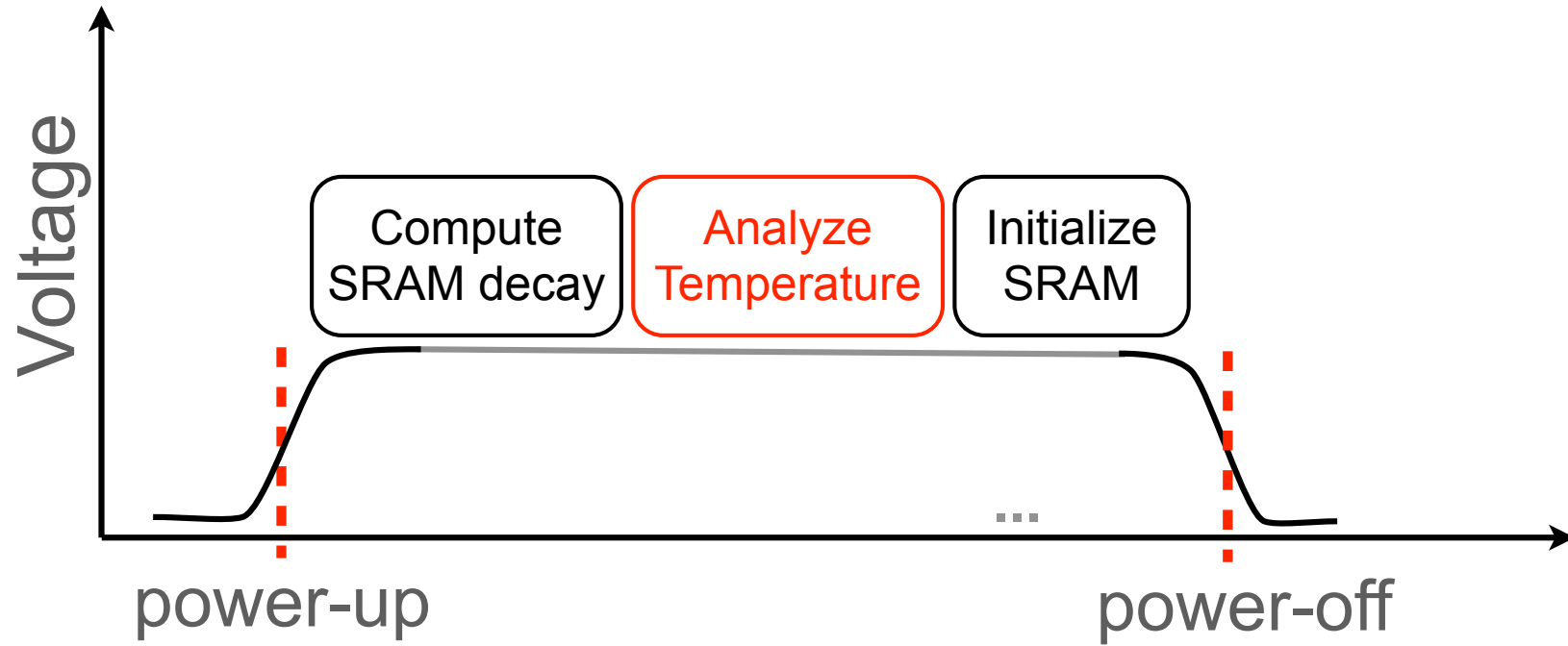
Temperature



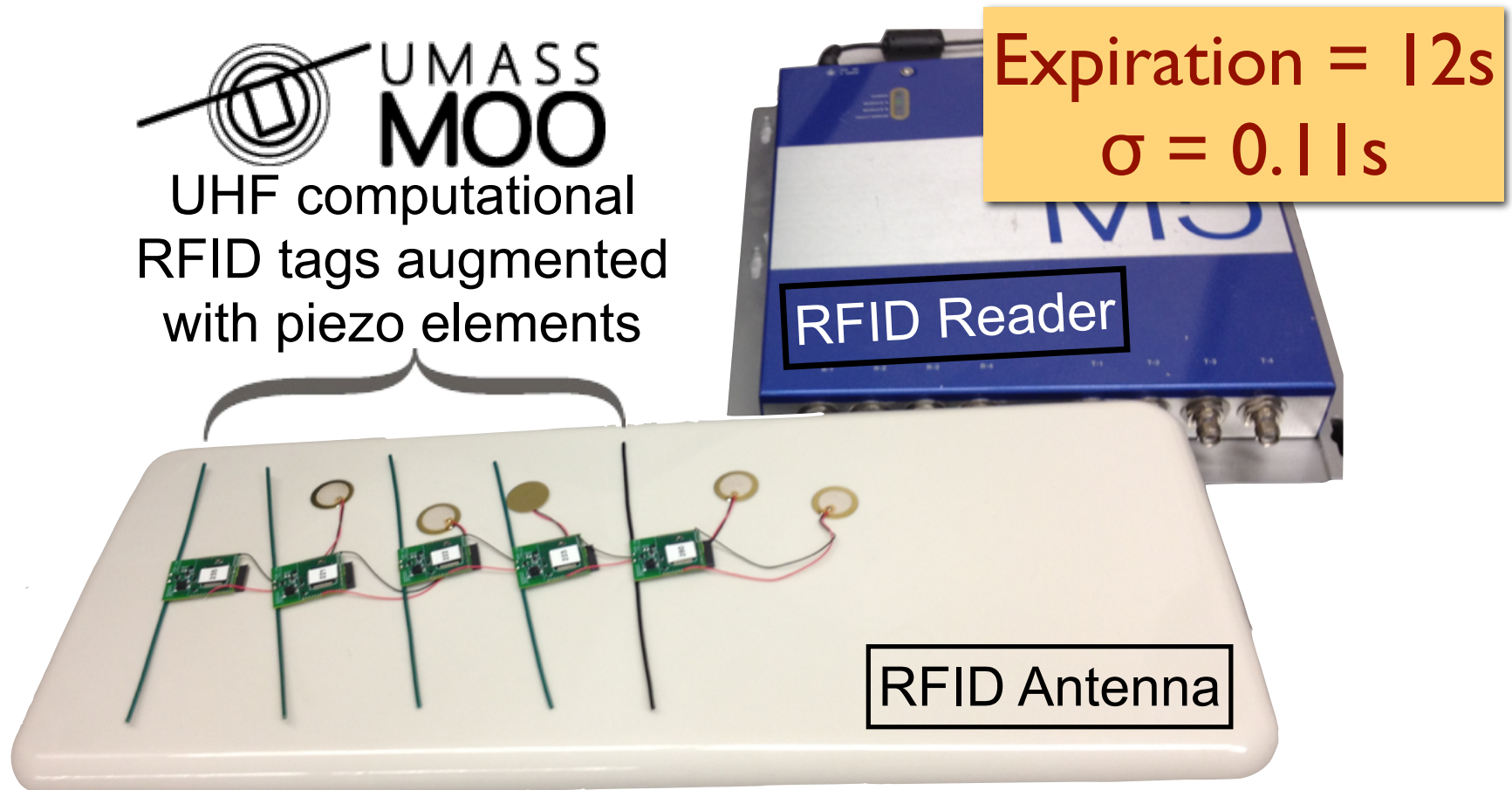
Temperature



Compensate for Temperature



Implementation



The Effect of TARDIS*

Device	#Queries	W/O TARDIS	W/ TARDIS
UHF RFID Tags	200	2 Seconds	40 Minutes
MIFARE Classic	1,500	16 Seconds	5 Hours
Digital Signal Transponder	75,000	1 Hour	10 Day
MIFARE DESFire	250,000	7 Hours	35 Days
GSM SIM Cards	150,000	8 Hours	21 Days

* Assuming a 12 seconds TARDIS

Attacking the TARDIS

- Cooling

Thermal Sensor

- Heating

Thermal Sensor



Physical Limitations

Thermal Fuse

Other Applications

- Time out in authentication protocols
- Temporary ownership (Resurrecting Duckling)
- RTC replacement in low-power sensors
- E-passports [Avoine'08]
- Time released cryptography [May'93,Rivest'96,May'01]

Related Work

Data Remanence in Volatile Memory

- Data retention in SRAM [Gutmann'01, Skorobogatov'02]
- FERNS [Holcomb'07]
- DRAM cold boot attack [Halderman'08]
- Background to data retention [Flautner'02]
- First proposed attacks [Anderson'96]
- SRAM attack [Taun'07]

Related Work

Reliable Time

- Lamport Clock [Lamport'78]
- Use Multiple Sources of Time [Rousseau'01]

Conclusion



uses memory decay to estimate time.



makes brute force attacks orders of magnitude harder.



is just software.



uses remanence decay for good.

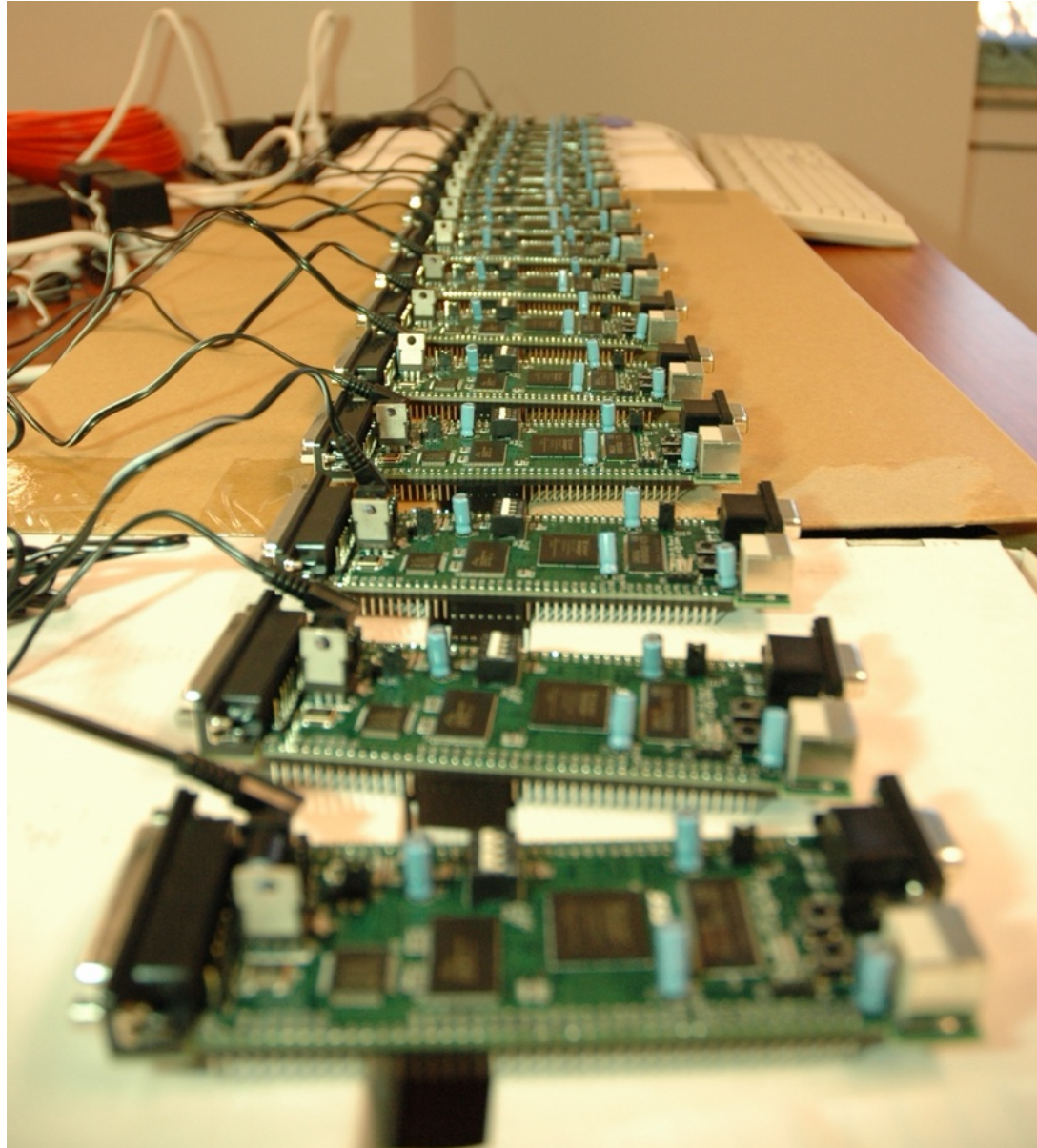
In-Class Exercise (5 minutes)

- Talk with neighbor
- Think about circuits or sensors in embedded systems that have inductance or capacitance
- How might you synthesize a timer or electronic water clock?
- Report back to class

2003-2005 JHU



2003-2005 JHU



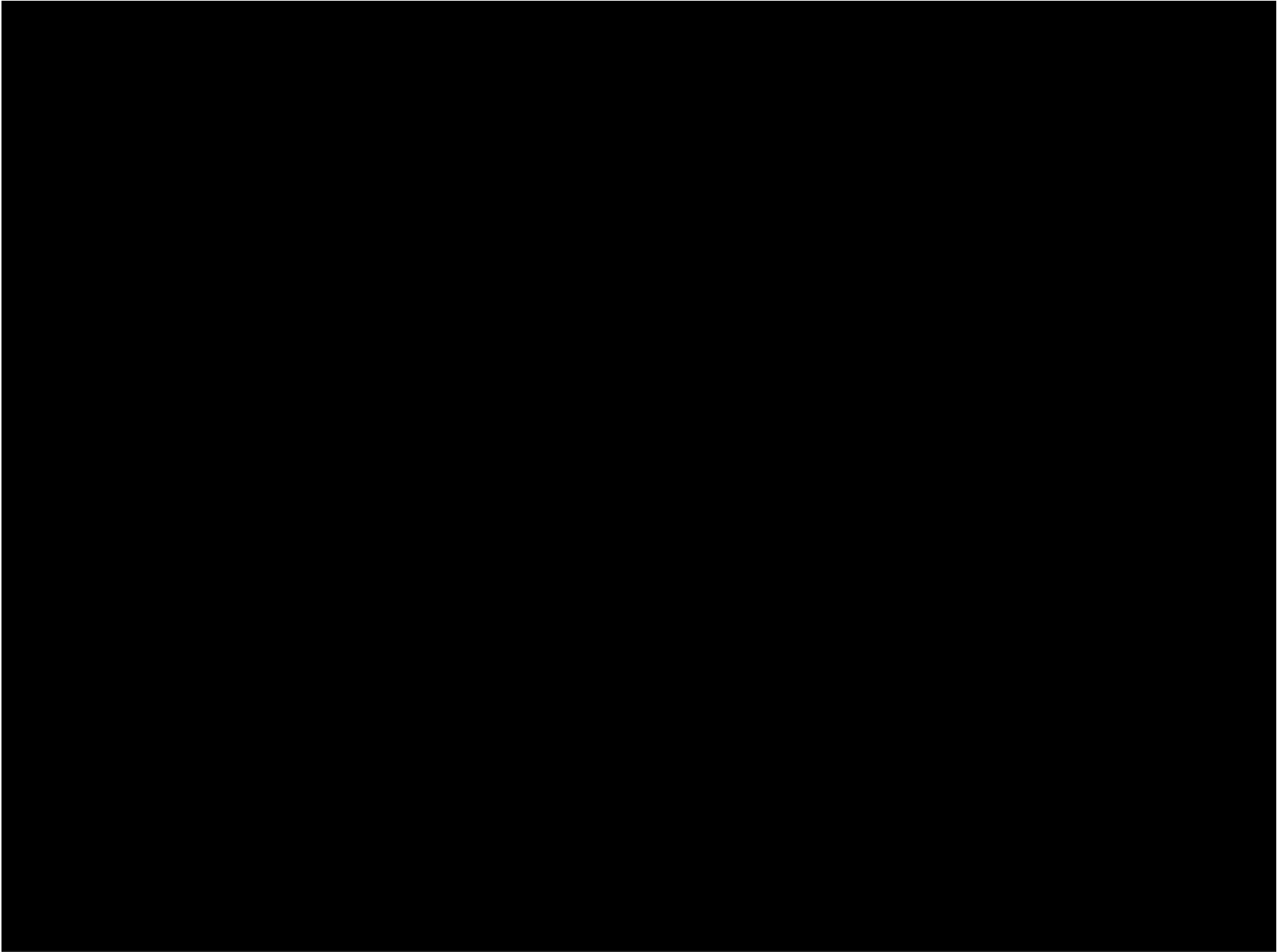
2003-2005 JHU



2006 UMass Amherst



2006 UMass Amherst



2006 UMass Amherst



Excerpts from a talk by Christian Paar

Hardware Trojans and Other Threats against Embedded Systems

RUB



[Janet Lackey](#) under CC license

ASIA-CCS

Abu Dhabi, April 3, 2017

Christof Paar

Ruhr Universität Bochum

hgi
Horst Görtz Institut
für IT-Sicherheit

Our Thoughts ca. 2012

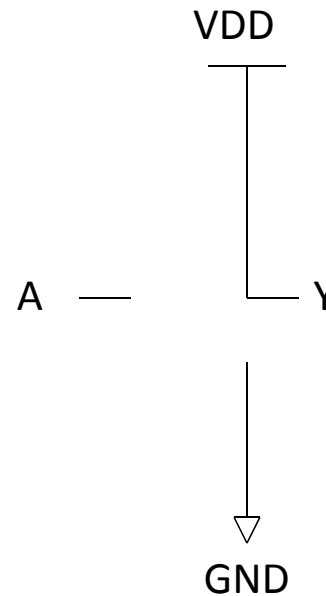
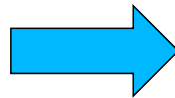
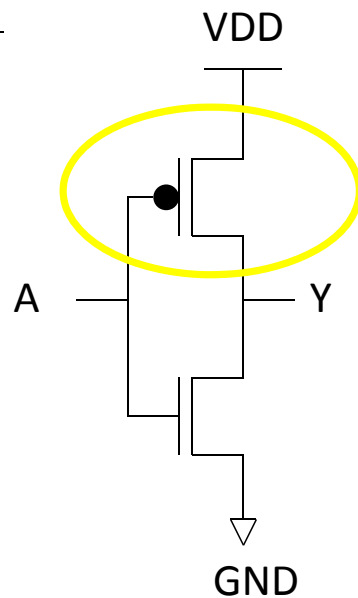
1. *Designing* Trojan could be fun too
2. Especially those that go *undetected*



Simple Example: Inverter Trojan

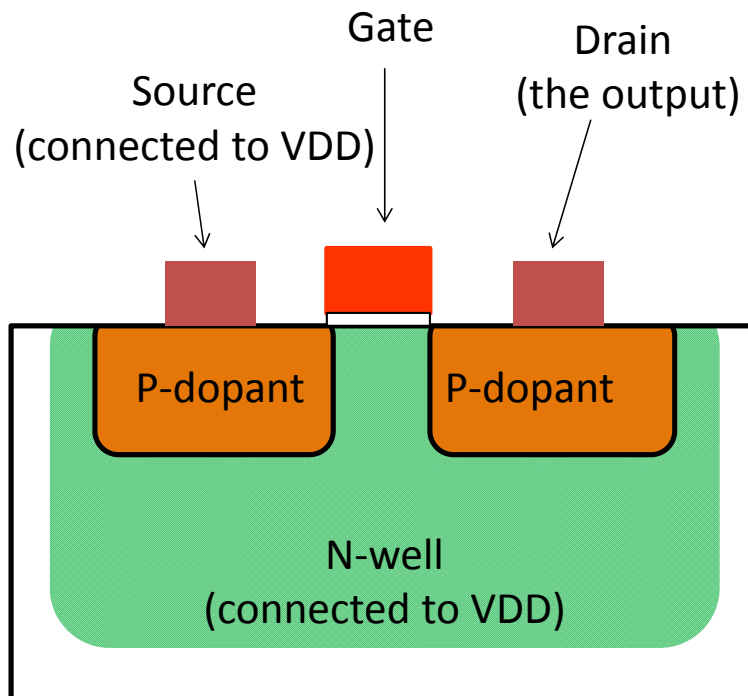
Let's modify an inverter so that it always outputs "1" (VDD) **without visible changes**.

A	Y
0	1
1	0

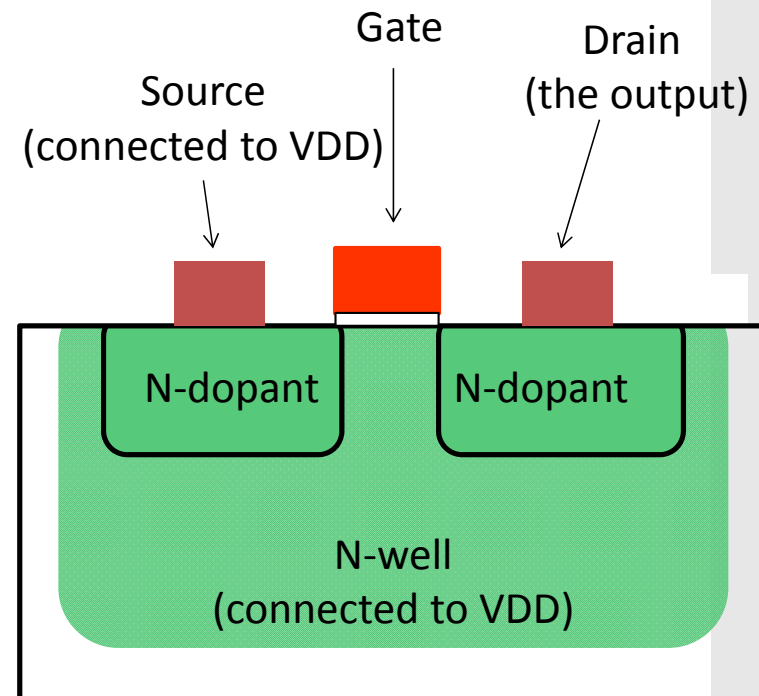


PMOS Transistor Trojan

RUB

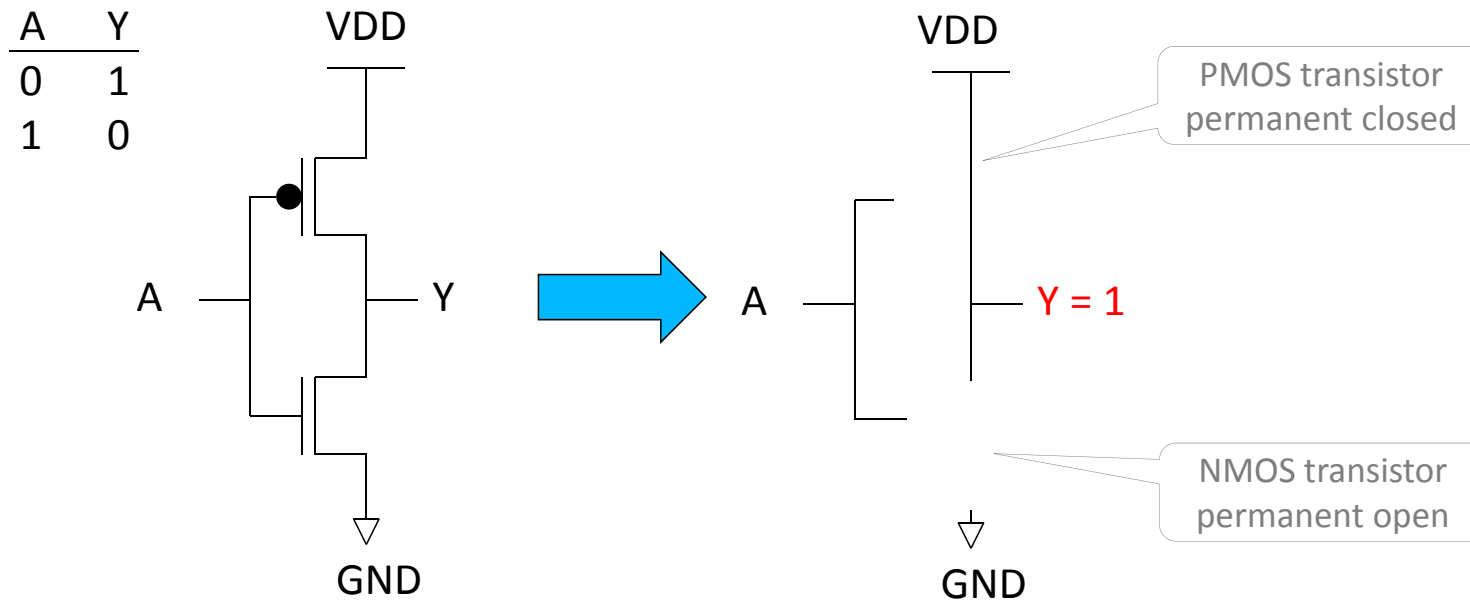


Unmodified PMOS transistor



Trojan trans. w/ constant VDD output

“Always One” Trojan Inverter



Q1: Can the manipulation be detected?

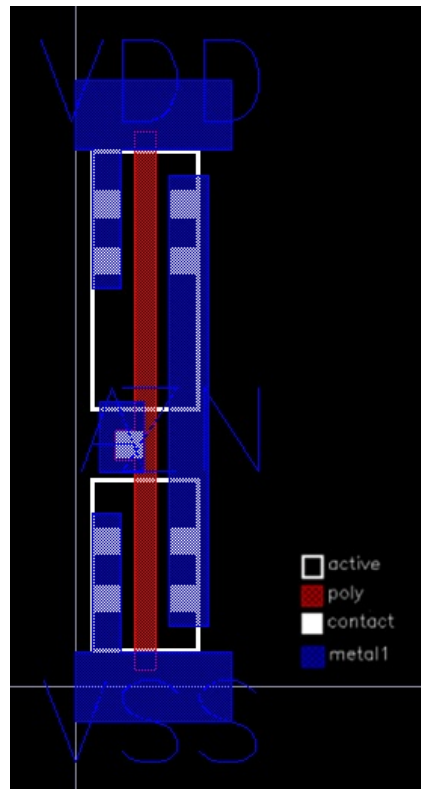
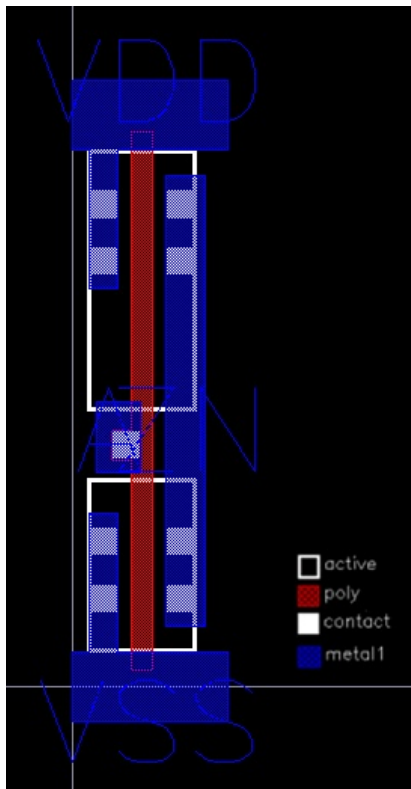
Q2: How to build a useful Trojan from here?

Detection: layout view of Trojan inverter

Which one has the Trojan?

Original Inverter

“Always One” Trojan



Unchanged:

- All metal layers
- Polysilicon layer
- Active area
- Wells

⇒ Dopant changes (very ?)
difficult to detect using
optical inspection!

Excerpts from a talk by Karsten Nohl

Meeting at BART

Karsten Nohl with Starbug, Henryk Plötz, and David Evans

MIFARE Classic Reverse-Engineering and Vulnerabilities

Our Project

Reverse-engineering of the Mifare crypto and evaluating its security

- ◆ Reconstruct circuit from photos of chip
- ◆ Sniff reader-tag communication



verify

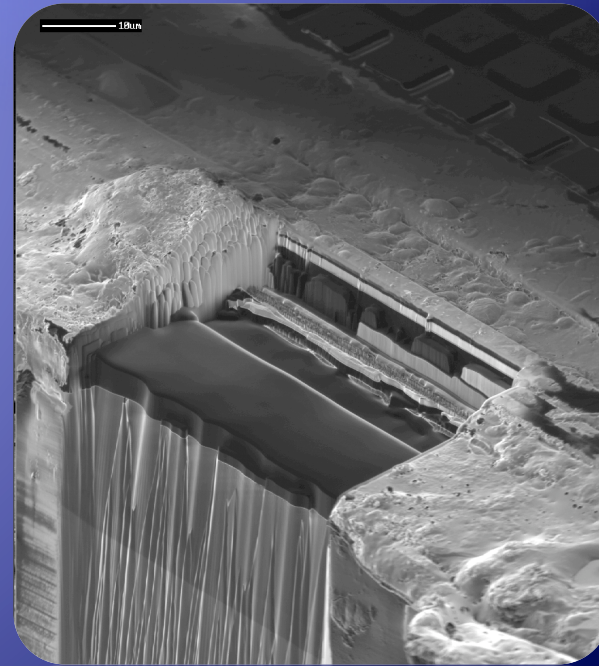
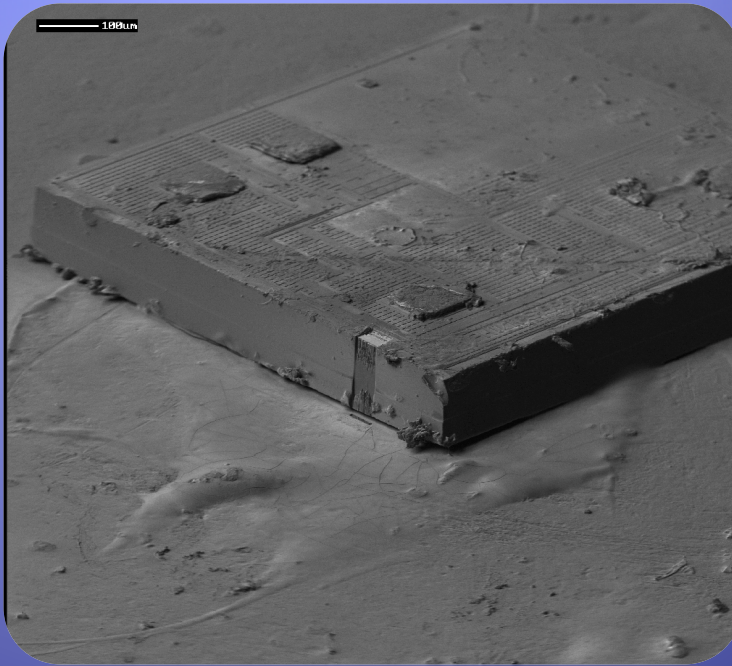
Reverse-Engineering

Obtaining Chips

- ◆ Chemically extracting chips:
 - ◆ acetone
 - ◆ fuming nitric acid
- ◆ Shortcut: buy blank chips!



Mifare Classic RFID tag

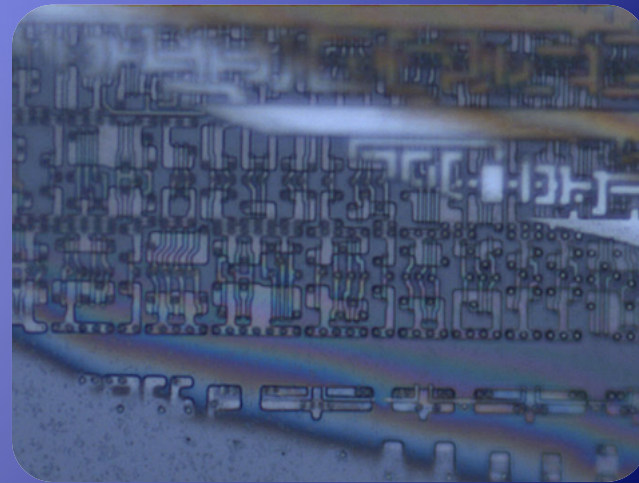


Getting Ready to Polish

- ◆ Embed chip in plastic
 - ◆ Downside: tilt

Alternative:

- ◆ Glue back of chip to plastic plate
 - ◆ Good results since backside is mostly plane

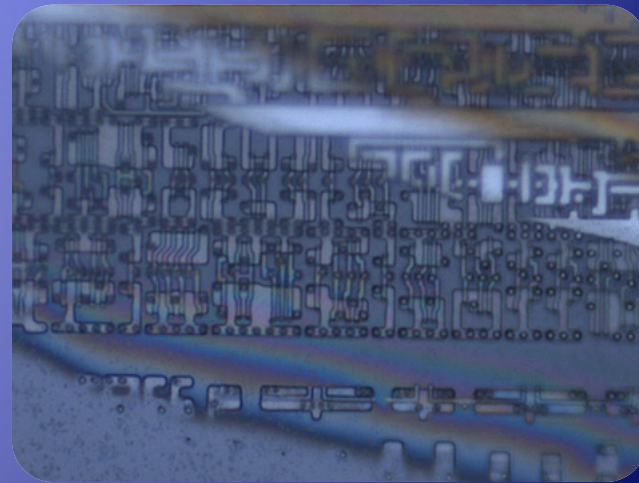


Getting Ready to Polish

- ◆ Embed chip in plastic
 - ◆ Downside: tilt

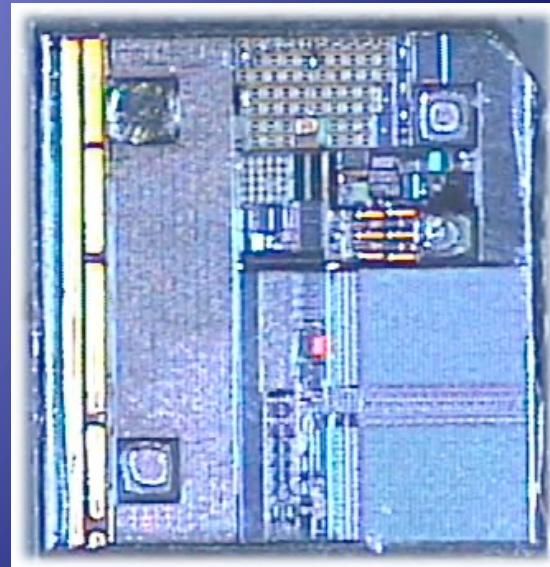
Alternative:

- ◆ Glue back of chip to plastic plate
 - ◆ Good results since backside is mostly plane



Polishing

- ♦ Manual or automatic
 - ♦ Polishing paper ($0.3\ \mu\text{m}$)
 - ♦ Polishing fluid ($0.04\ \mu\text{m}$)

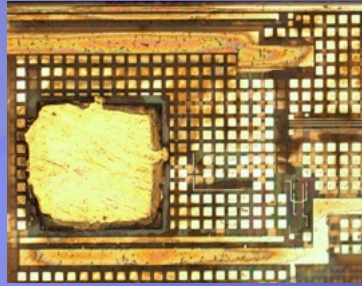


Imaging Chip

- ◆ Optical microscope (Zeiss)
 - ◆ 500x magnification
 - ◆ Camera 1 Mpixel
 - ◆ Black and white
- ◆ Stitching images
 - ◆ Panorama software (hugin)
 - ◆ Each image $\sim 100 \times 100 \mu\text{m}$
- ◆ Align different layers

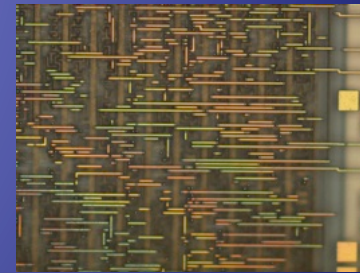
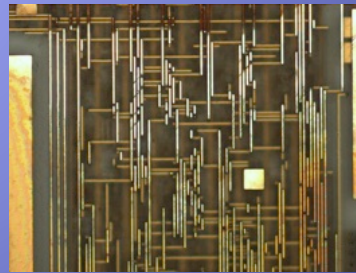
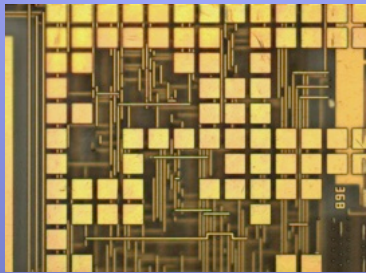


Chip Layer

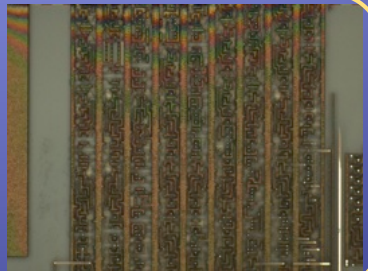


Cover layer

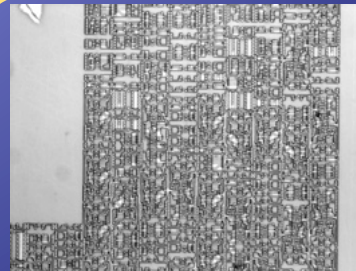
3 interconnection layer



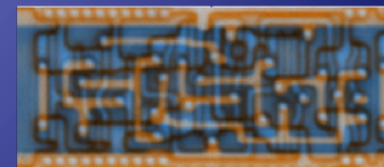
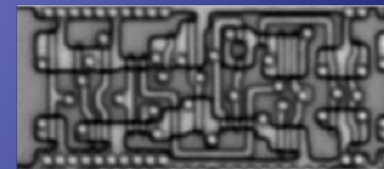
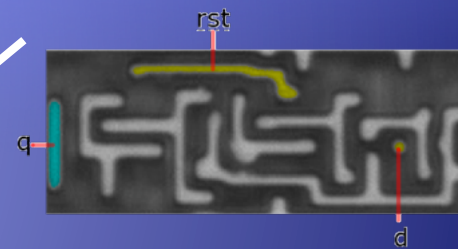
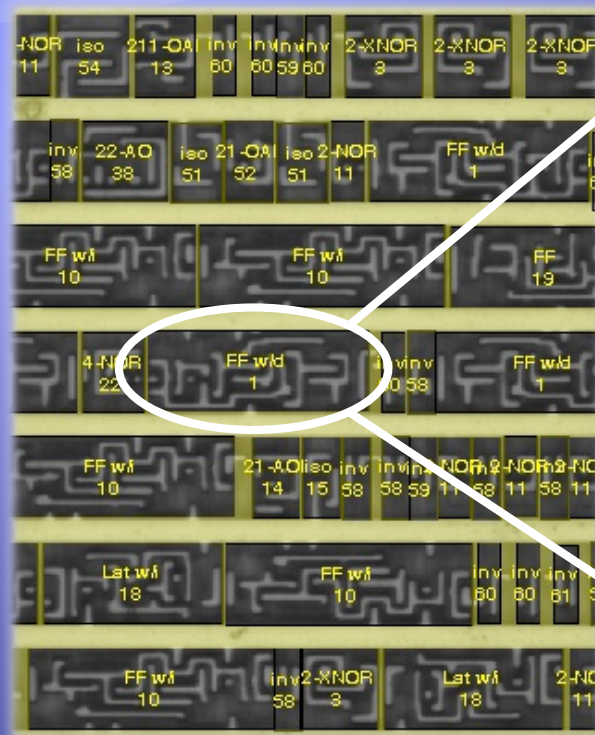
Logic
layer



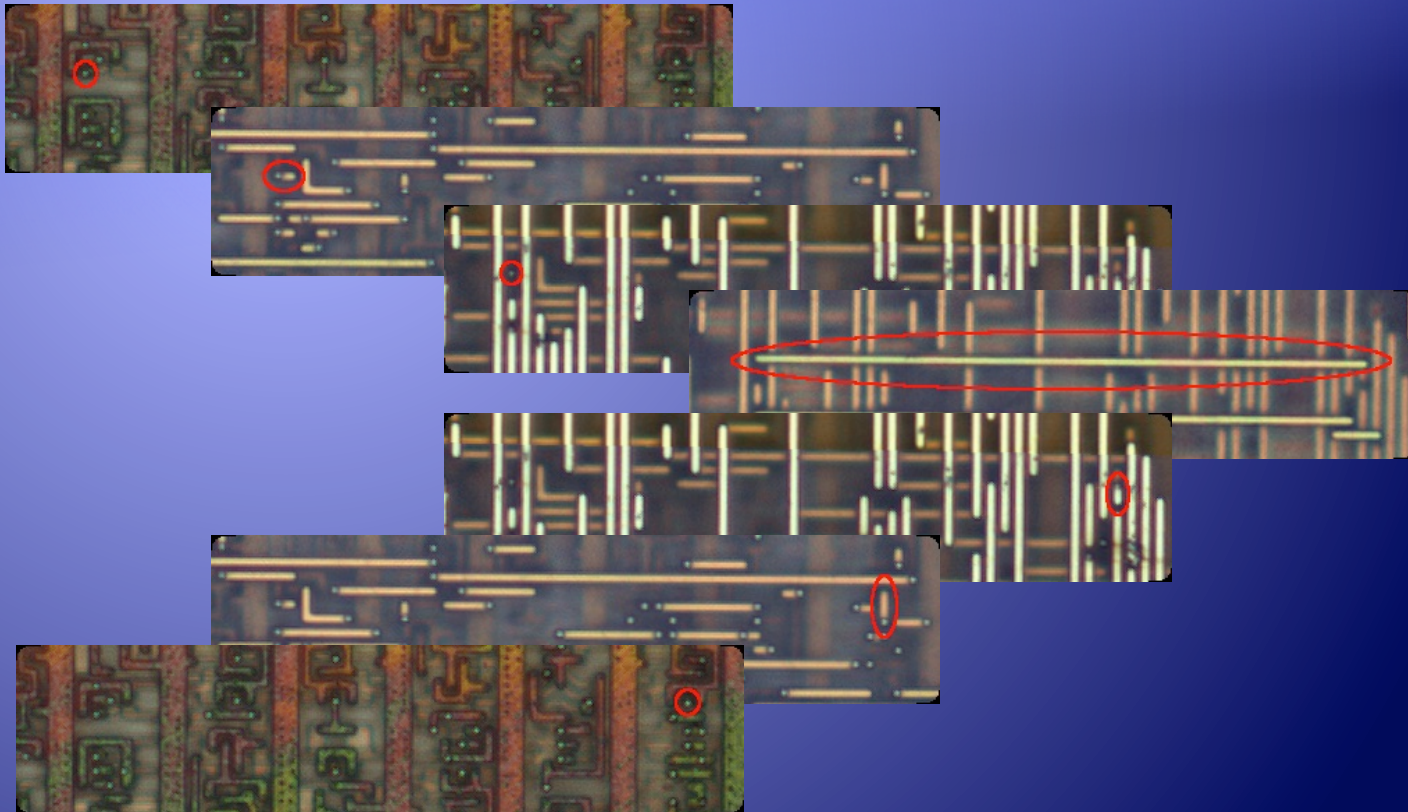
Transistor
layer



Logic Gates



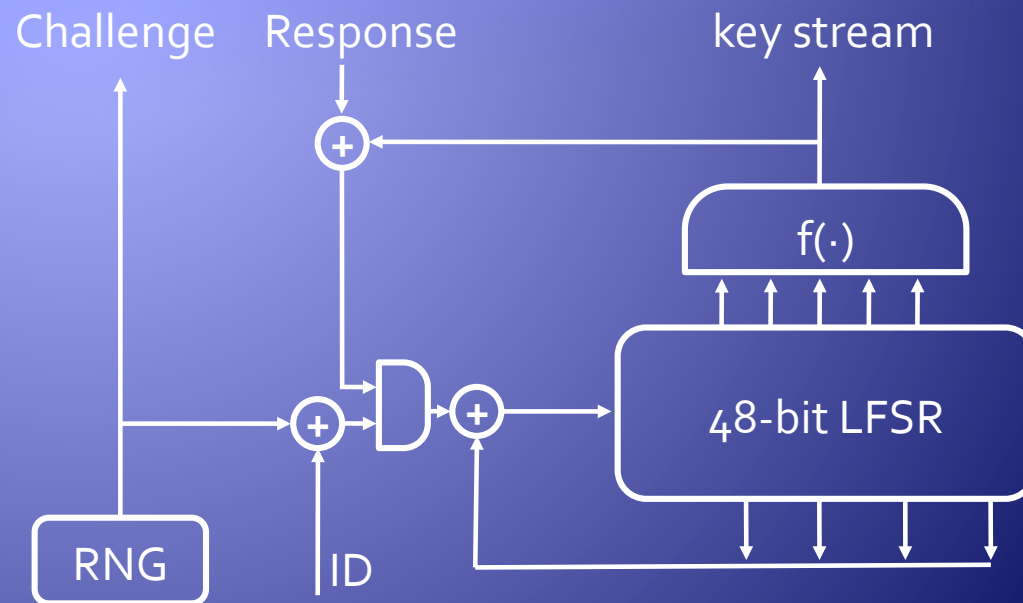
Tracing Connections



Encircle Crypto

- ◆ Even tiny RFID chip too large to analyze entirely
 - Crypto <10% of gates!
- ◆ Focus on interesting-looking parts:
 - Strings of flip-flops (registers)
 - XOR
 - Units around edges that sparsely connected to the rest of the chip

Mifare Crypto-1



Lessons Learned

- ◆ Obscurity and proprietary crypto add security only in the short-run
 - ◆ (but lack of peer-review hurts later)
- ◆ Constraints of RFIDs make good crypto extremely hard
 - ◆ Where are the best trade-offs?
 - ◆ How much security is needed?
 - ◆ Good news: Secure cards available for fair collection!

Final Stretch

- Coming up
 - ▶ Monday 11/10: Circuit-level security
 - ▶ Thursday 11/13: Lab 4 time
 - ▶ Monday 11/17: Provably Uncloneable Functions
 - ▶ Thursday 11/20: Team Project Milestone Presentations
 - ▶ Monday 11/24: Final project lab time & 11/24-11/28 Project Demos
 - ▶ Monday 12/1: Embedded Security of Computer Vision, Defense Documents due
 - ▶ Thursday 12/4: In-class tournament!
 - ▶ Monday 12/8: Final project report due