Photo Credit: thinkgeek.com

TARDIS

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

Amir Rahmati[1], Mastooreh Salajegheh[1], Dan Holcomb[2], Jacob Sorber[3], Wayne Burleson[1], Kevin Fu[1]

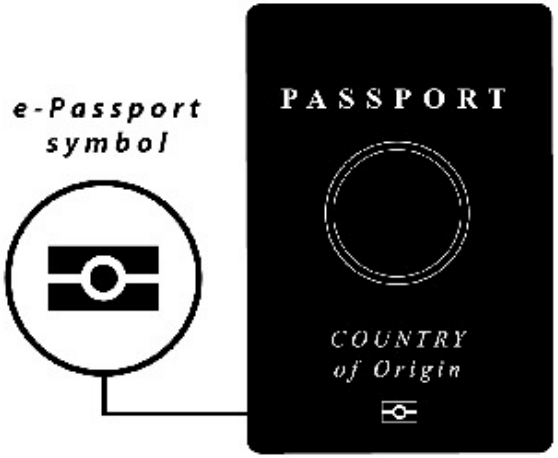
1 UMass Amherst 2 UC Berkeley, 3 Dartmouth College

This research is supported by NSF grants CNS-0831244, CNS-0845874, CNS-0923313, CNS-0964641, SRC task 1836.074, Gigascale Systems Research Center, and a Sloan Research Fellowship. Any opinions, findings, conclusions, and recommendations expressed in these materials are those of the authors and do not necessarily reflect the views of the sponsors. Portions of this work are patent pending.

Batteryless Devices

Transportation

Payment



Passports

Employee IDs

Photo Credit: digboston.com, mobileedgeblog.com, dhs.gov, vanntel.com

Batteryless Devices

Transportati

nt

Things in Common

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

Passports

Employee IDs

Photo Credit: digboston.com, mobileedgeblog.com, dhs.gov, vanntel.com

Security Vulnerabilities

Oyster card hack details revealed

By Peter Price
Click reporter

Details of how to hack one of the world's most popular smartcards have been published online.

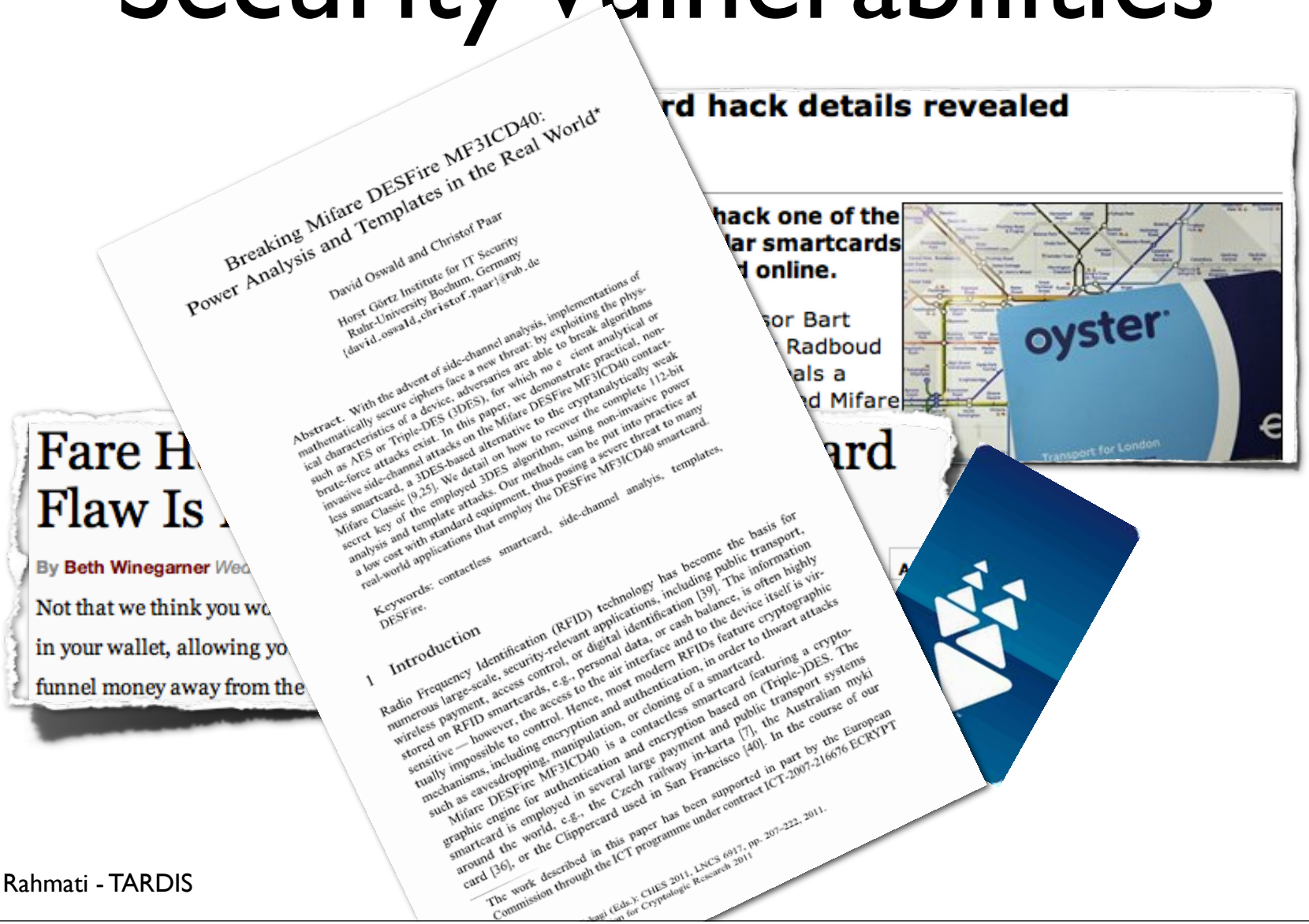
The research by Professor Bart Jacobs and colleagues at Radboud University in Holland reveals a weakness in the widely used Mifare

Fare Hack: Exploiting a Clipper Card Flaw Is Easy

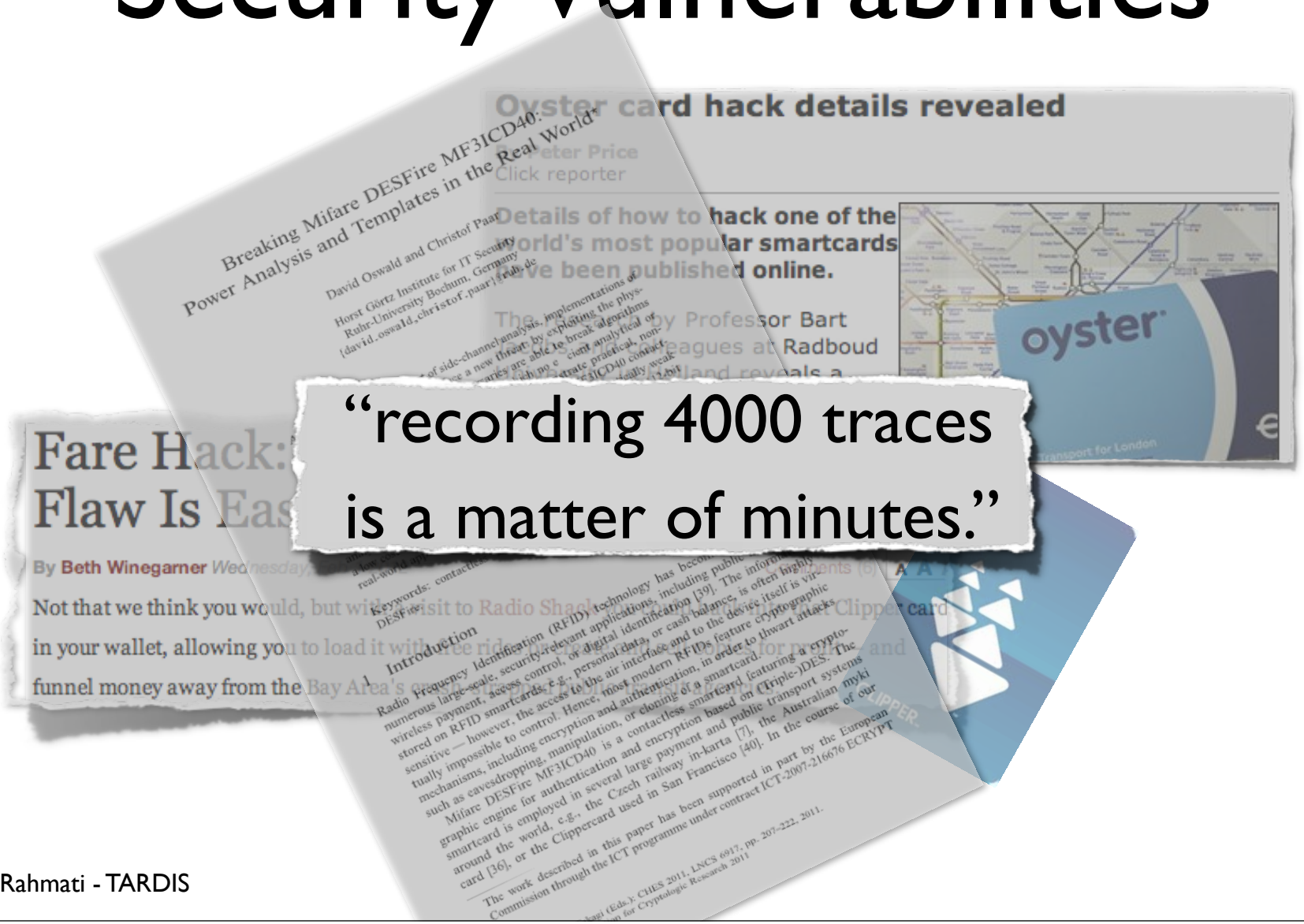
By Beth Winegarner *Wednesday, Feb 1 2012* Comments (6)

Not that we think you would, but with a visit to Radio Shack you could hack into that Clipp
in your wallet, allowing you to load it with free rides or create and sell copies for profit —
funnel money away from the Bay Area's crash-strapped public-transit agencies.

Security Vulnerabilities



Security Vulnerabilities



"recording 4000 traces is a matter of minutes."

Smart Card Threats

Power Analysis

Reverse Engineering

Brute Force

Photo Credit: landlsoft.com

Smart Card Threats

Power Analysis

Reverse Engineering

Brute Force

Photo Credit: landlsoft.com

Smart Card Threats

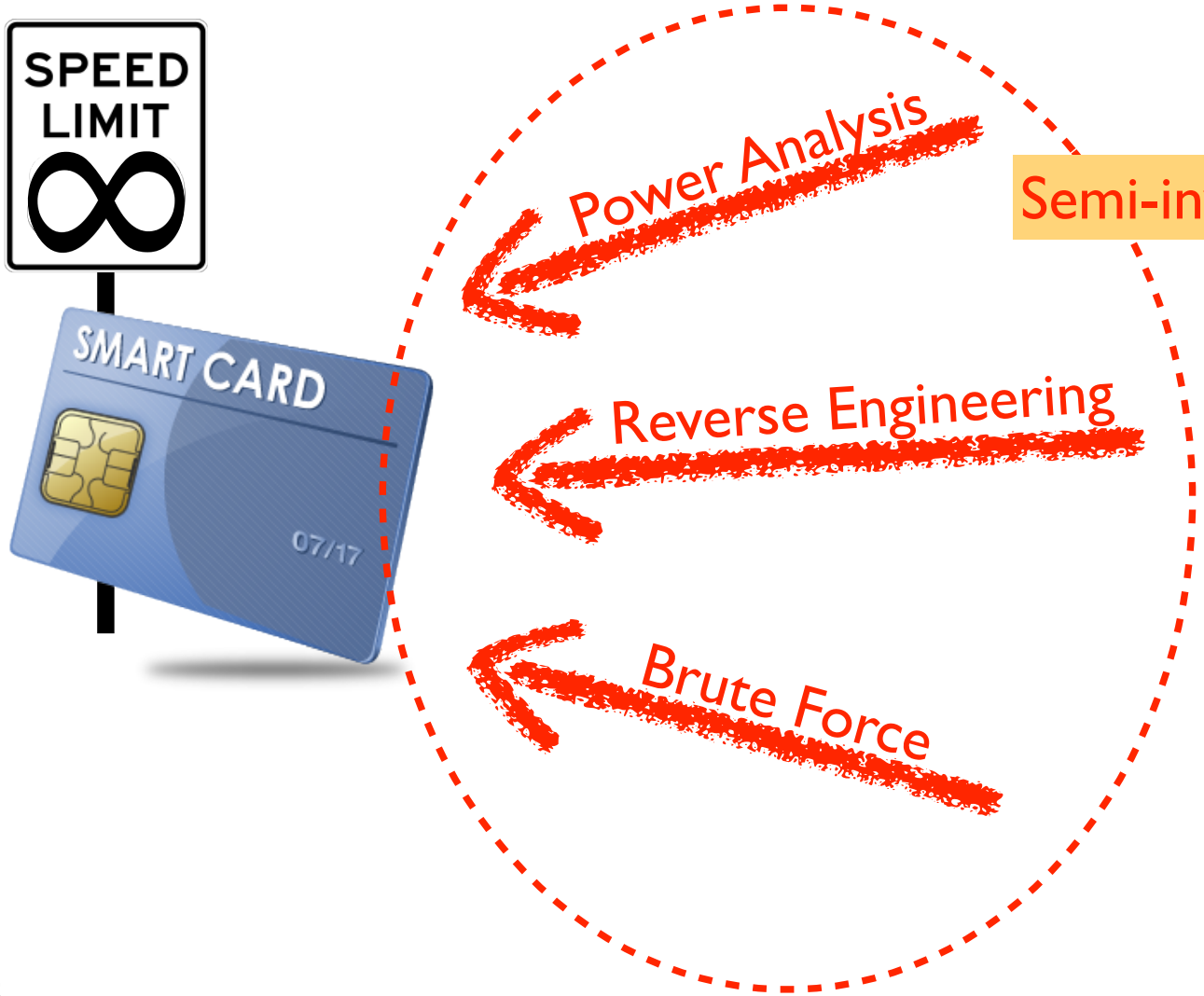


Photo Credit: landlsoft.com

Vulnerable to Brute Force Attacks

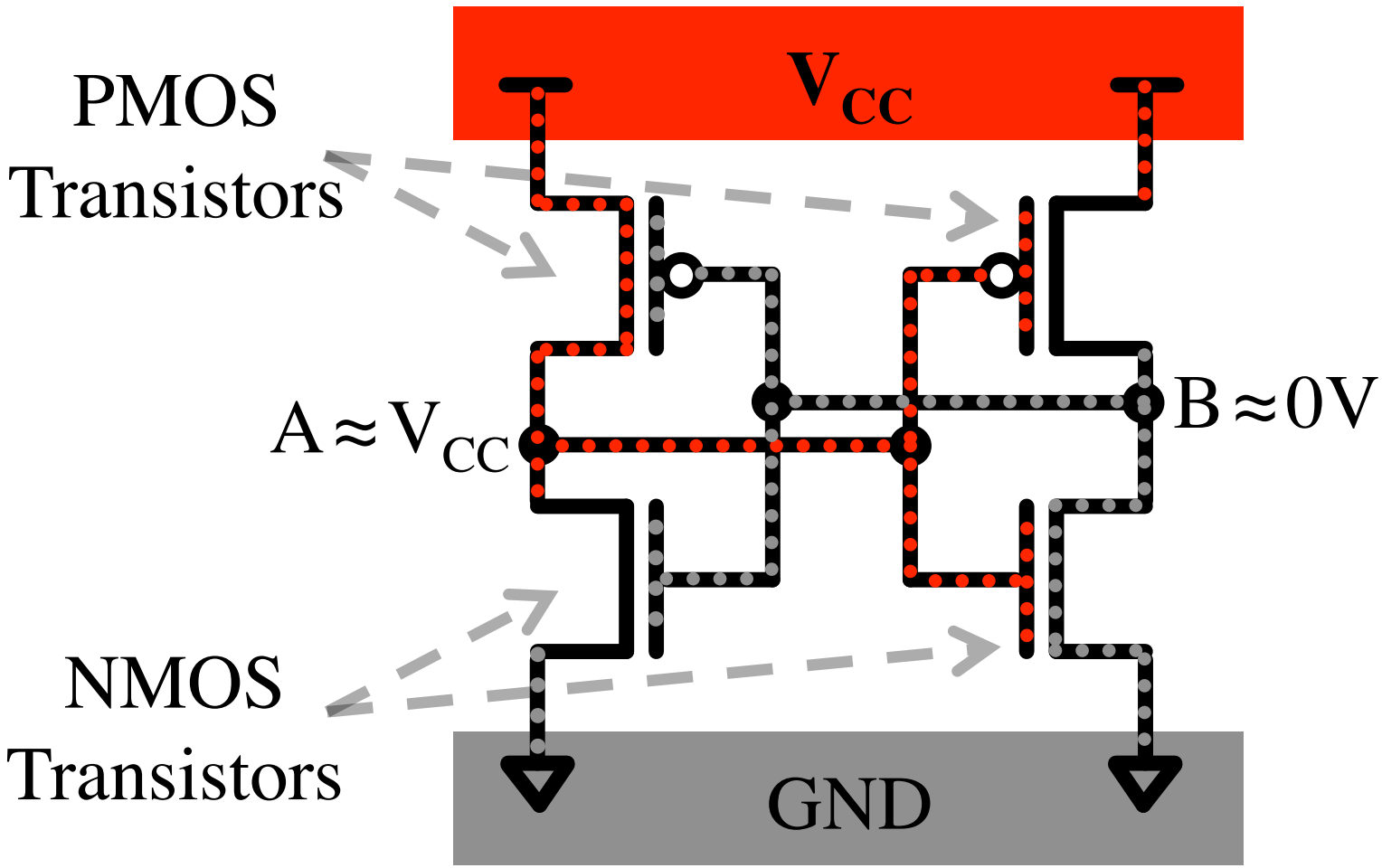
Device	#Queries	Time
UHF RFID Tags[Shamir'07]	200	2 Seconds
MIFARE Classic[Garcia'09]	1,500	16 Seconds
Digital Signal Transponder[Bono'05]	75,000	1 Hour
MIFARE DESFire[Paar'11]	250,000	7 Hours
GSM SIM Cards[Goldberg'99]	150,000	8 Hours

Photo Credit: thinkgeek.com

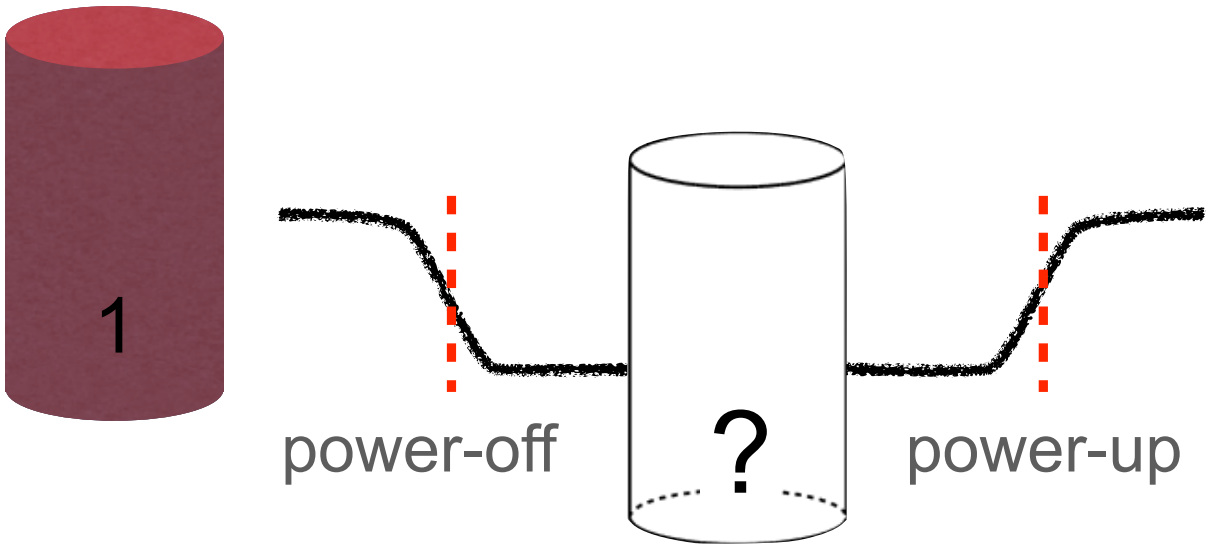
Our Contribution: TARDIS

A time-keeping technique based on SRAM decay

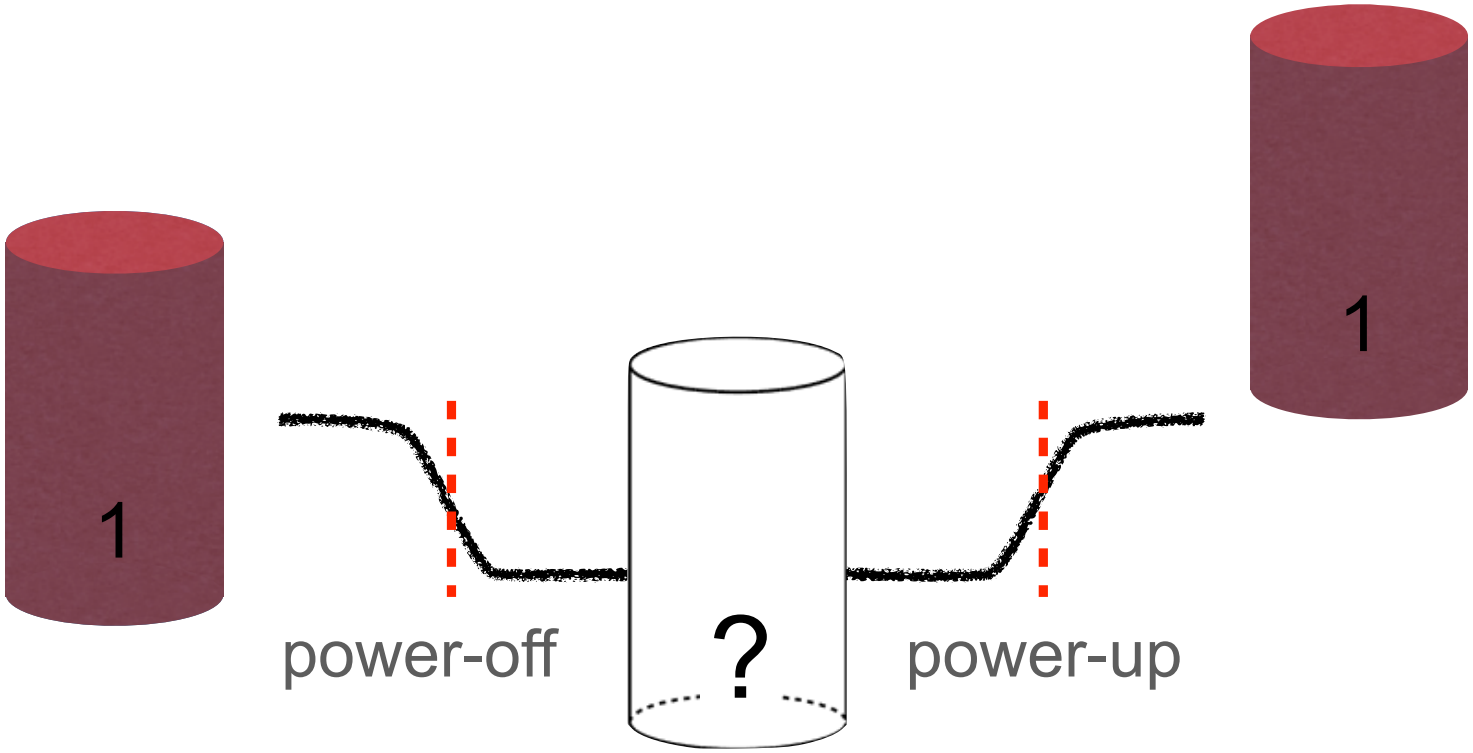
SRAM Remanence



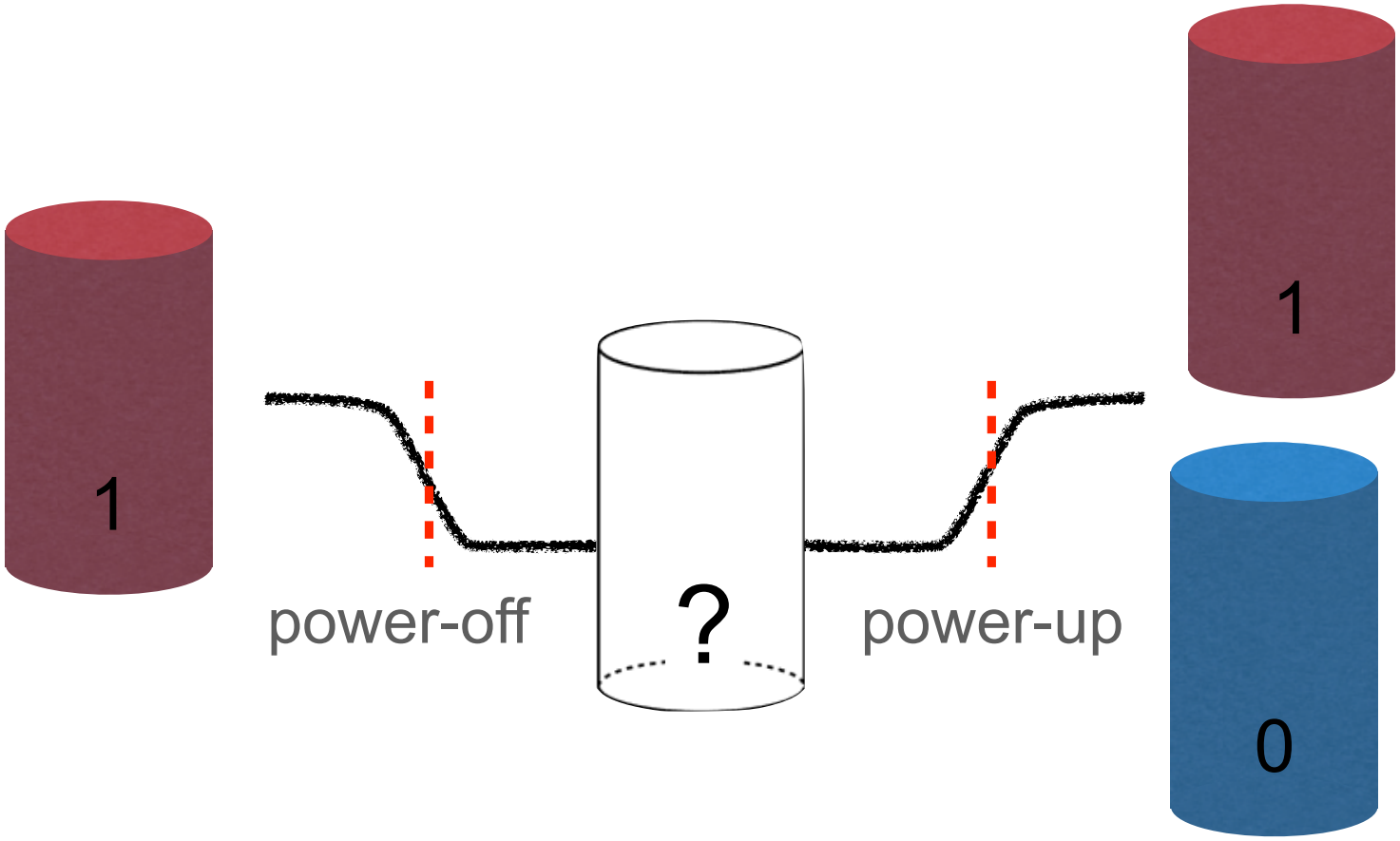
SRAM Remanence



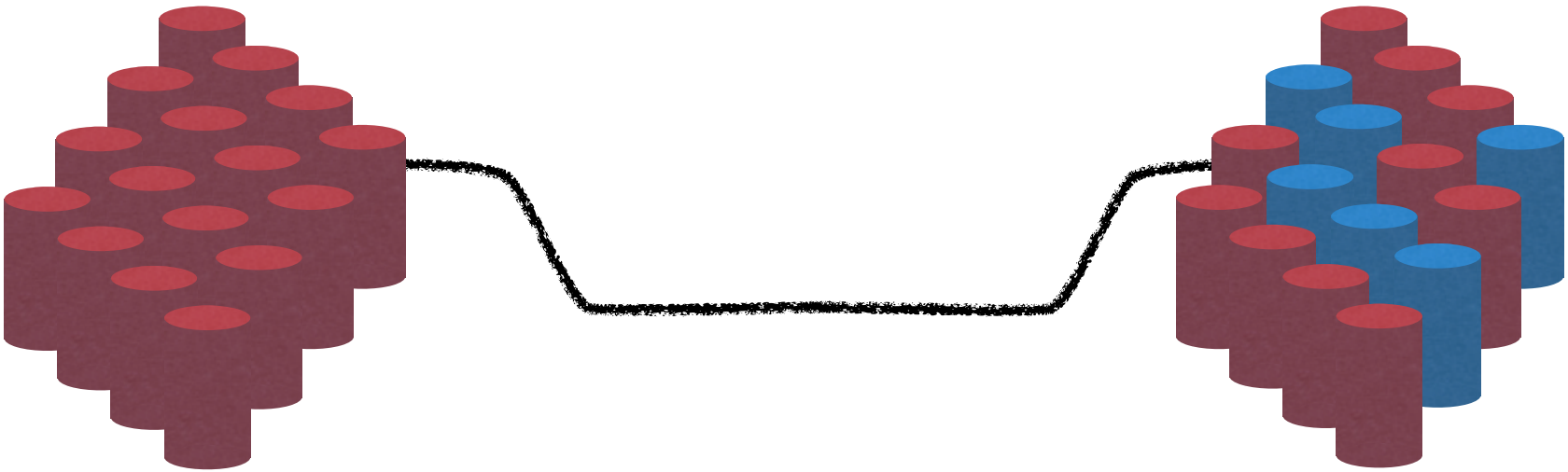
SRAM Remanence



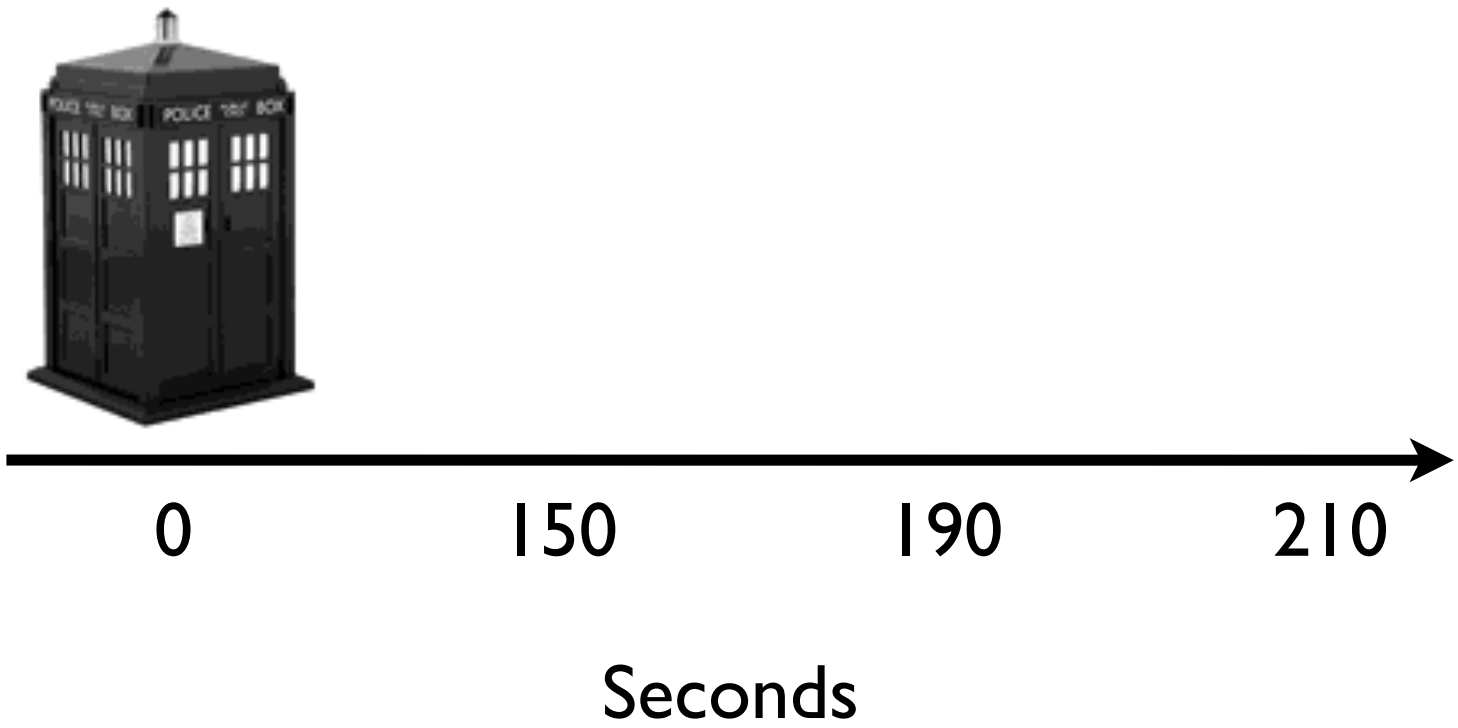
SRAM Remanence



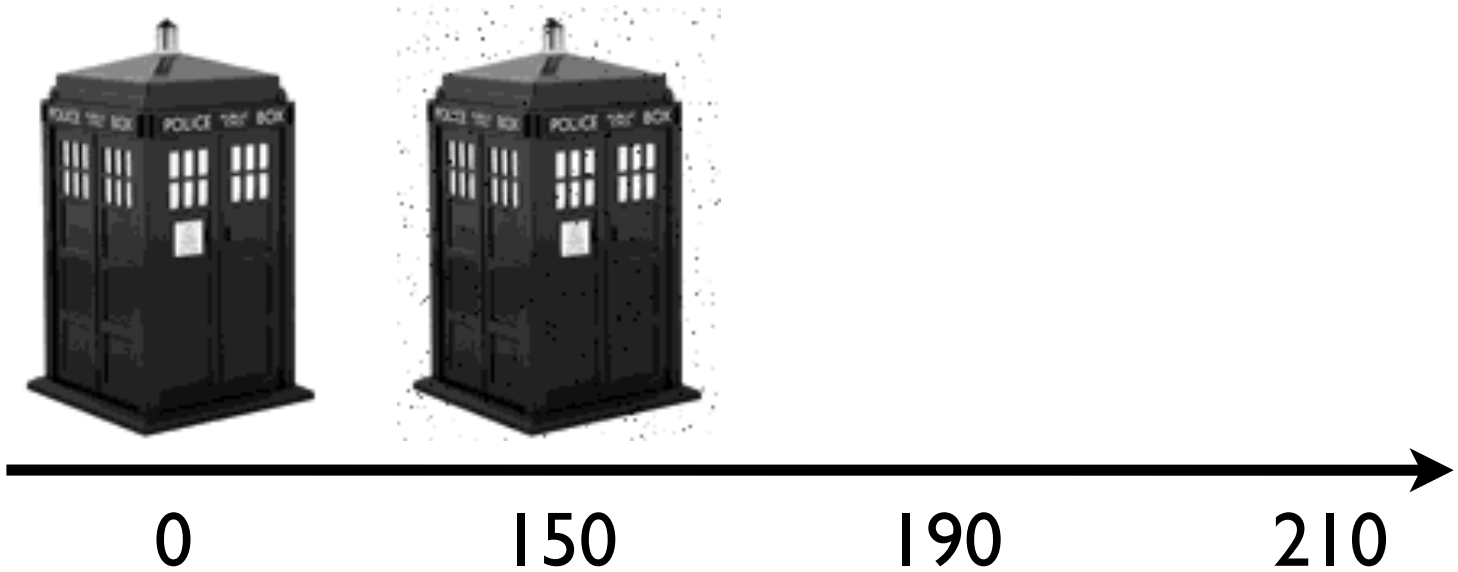
SRAM Remanence



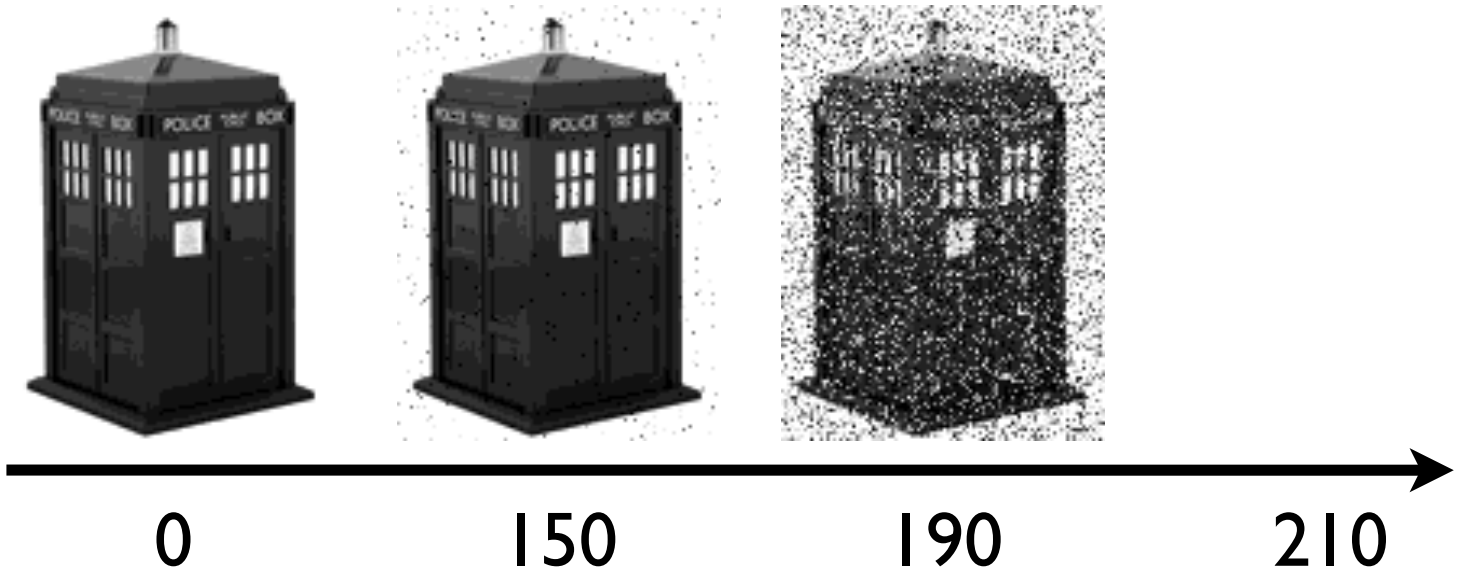
SRAM Remanence



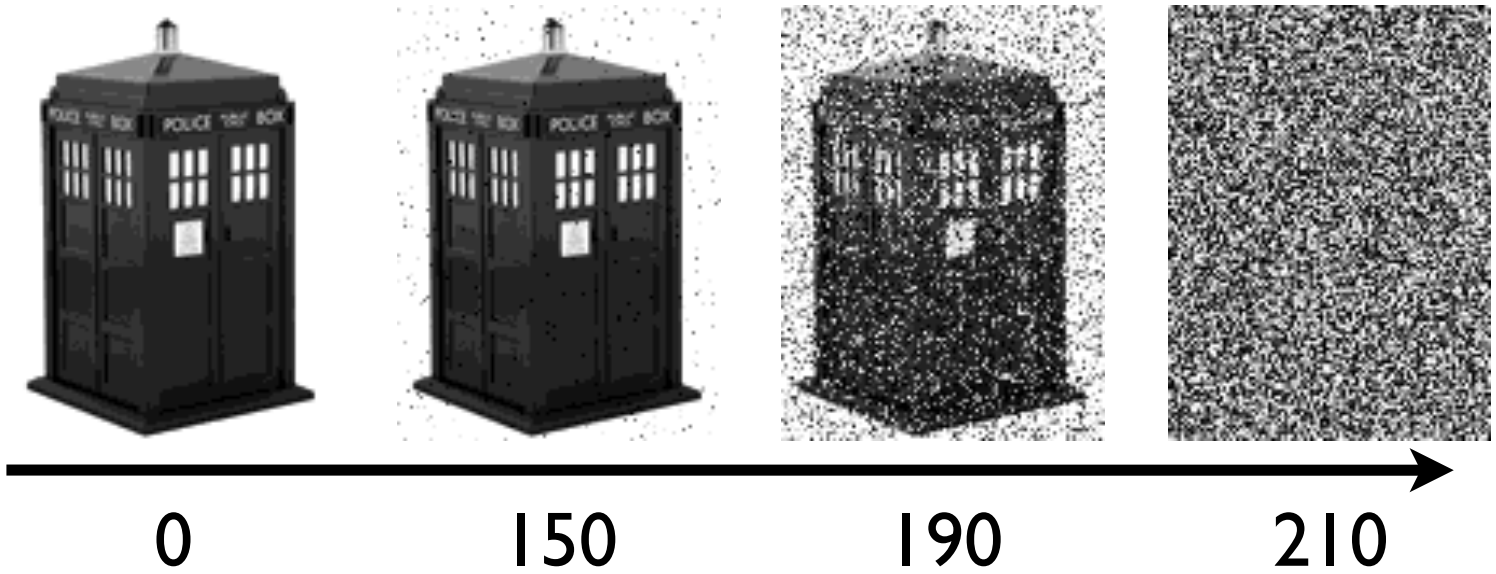
SRAM Remanence



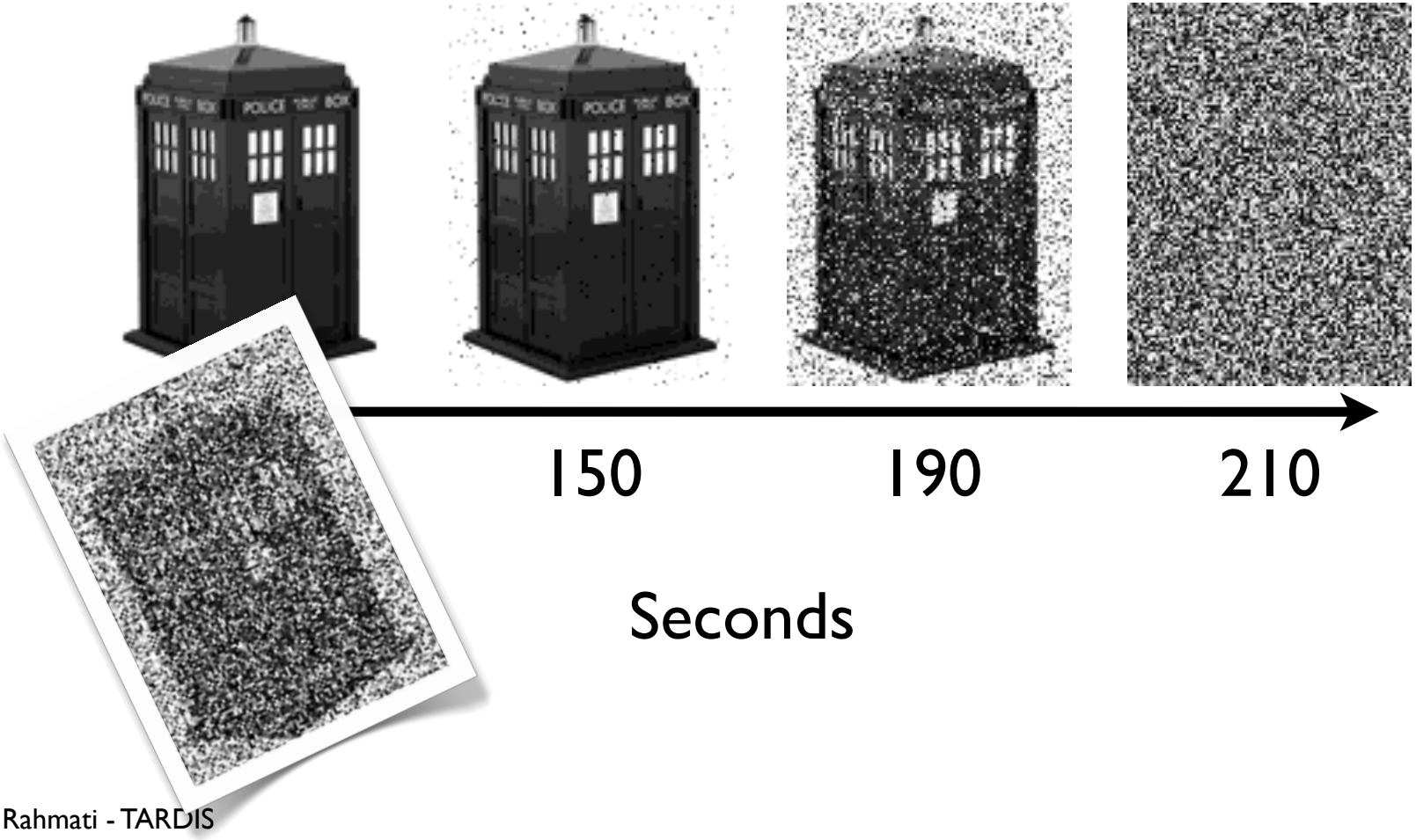
SRAM Remanence



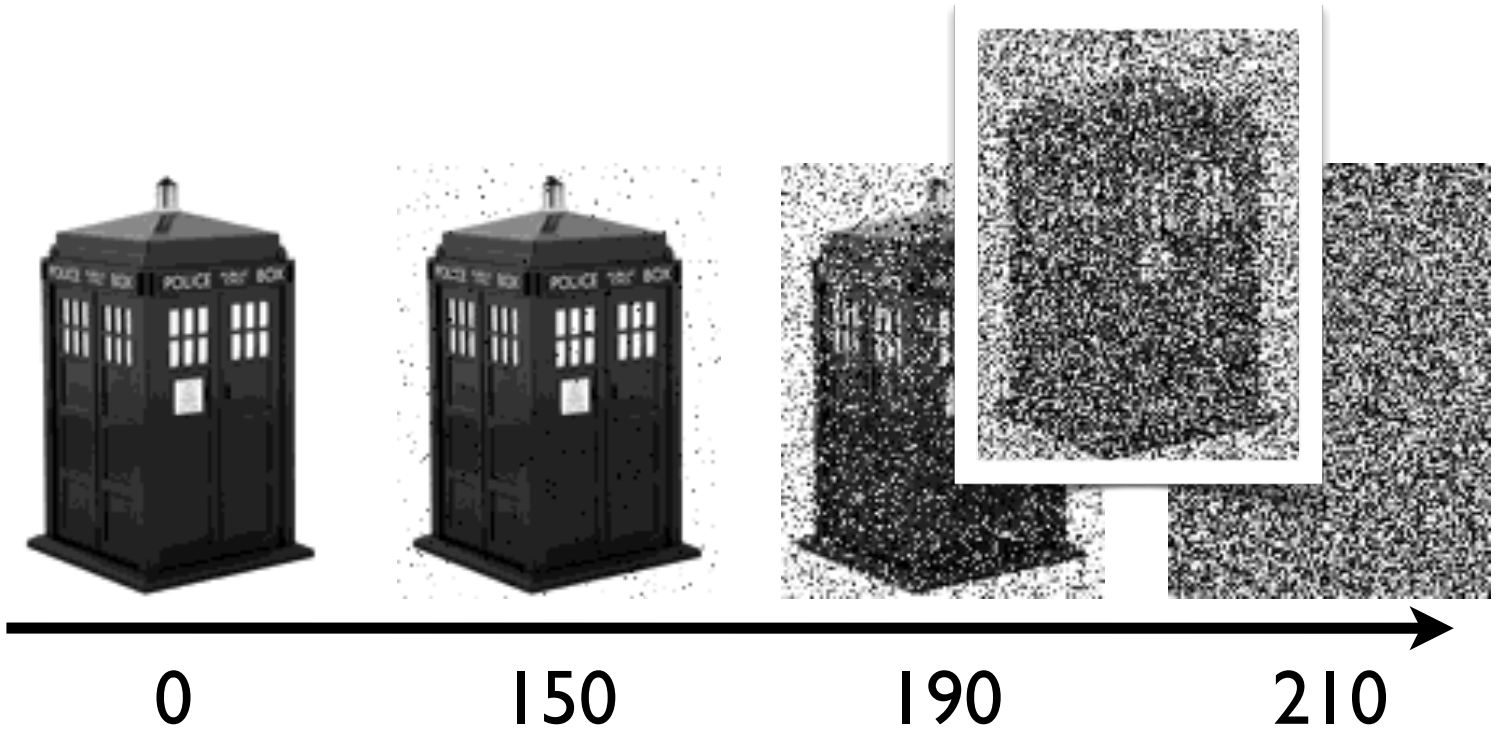
SRAM Remanence



SRAM Remanence

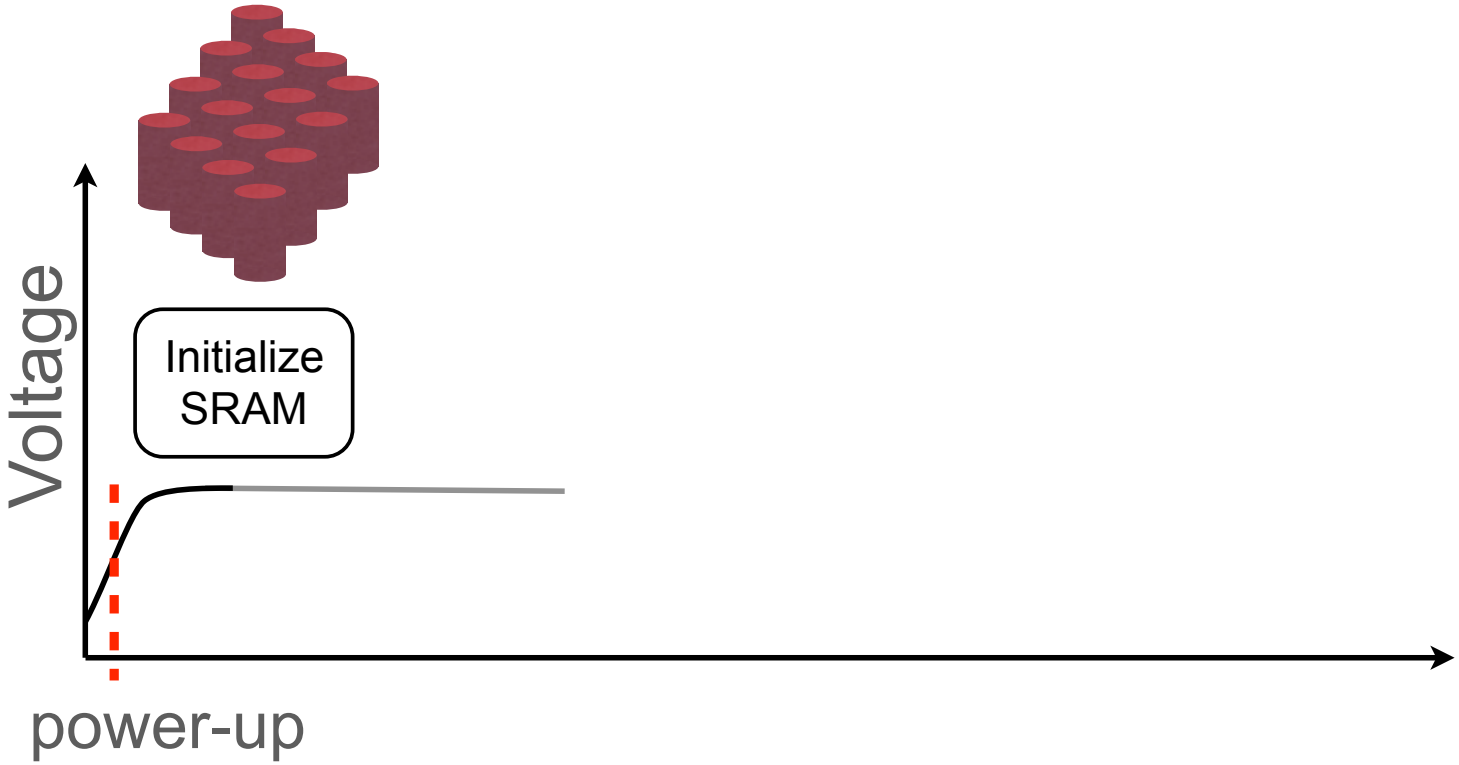


SRAM Remanence

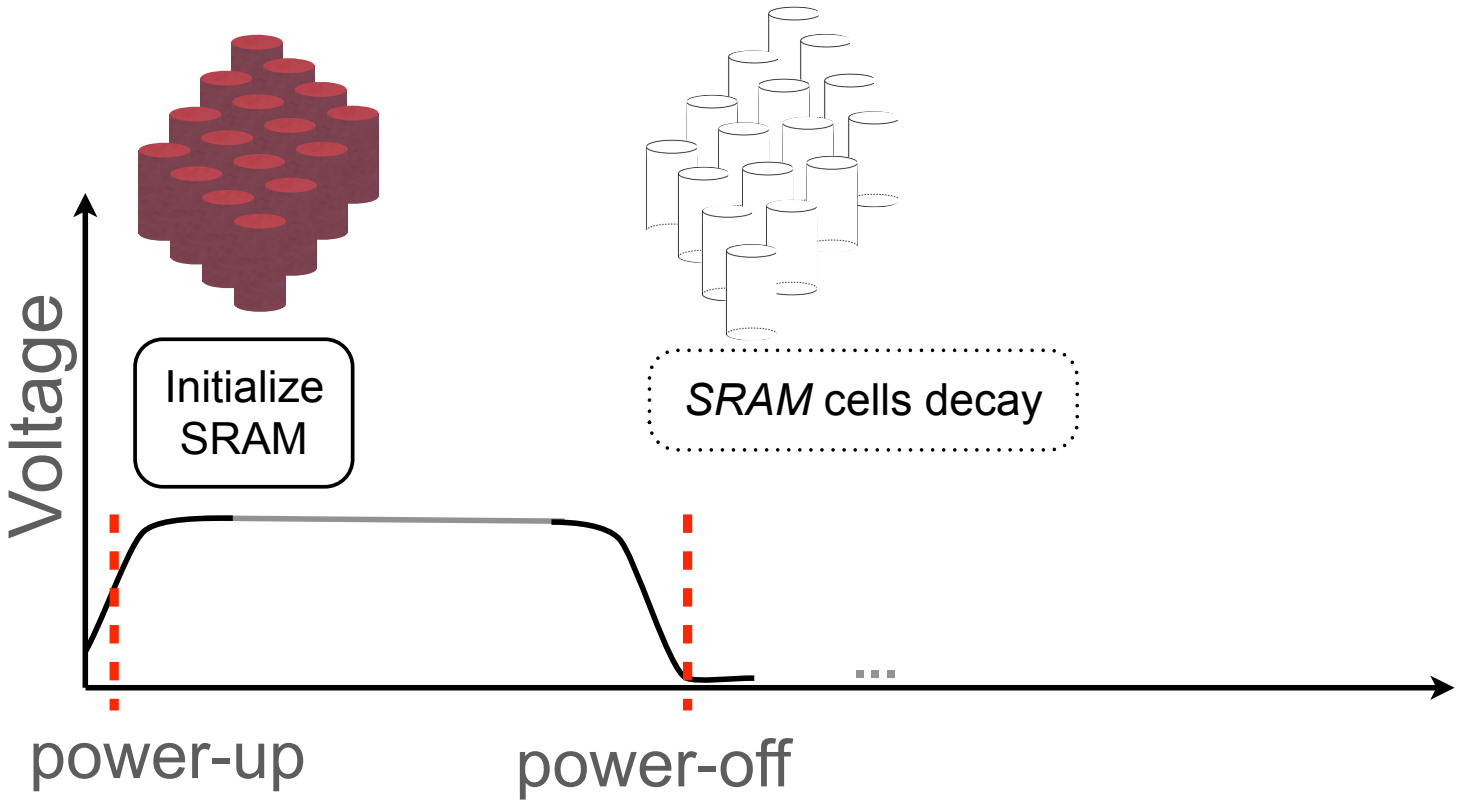


The TARDIS Algorithm

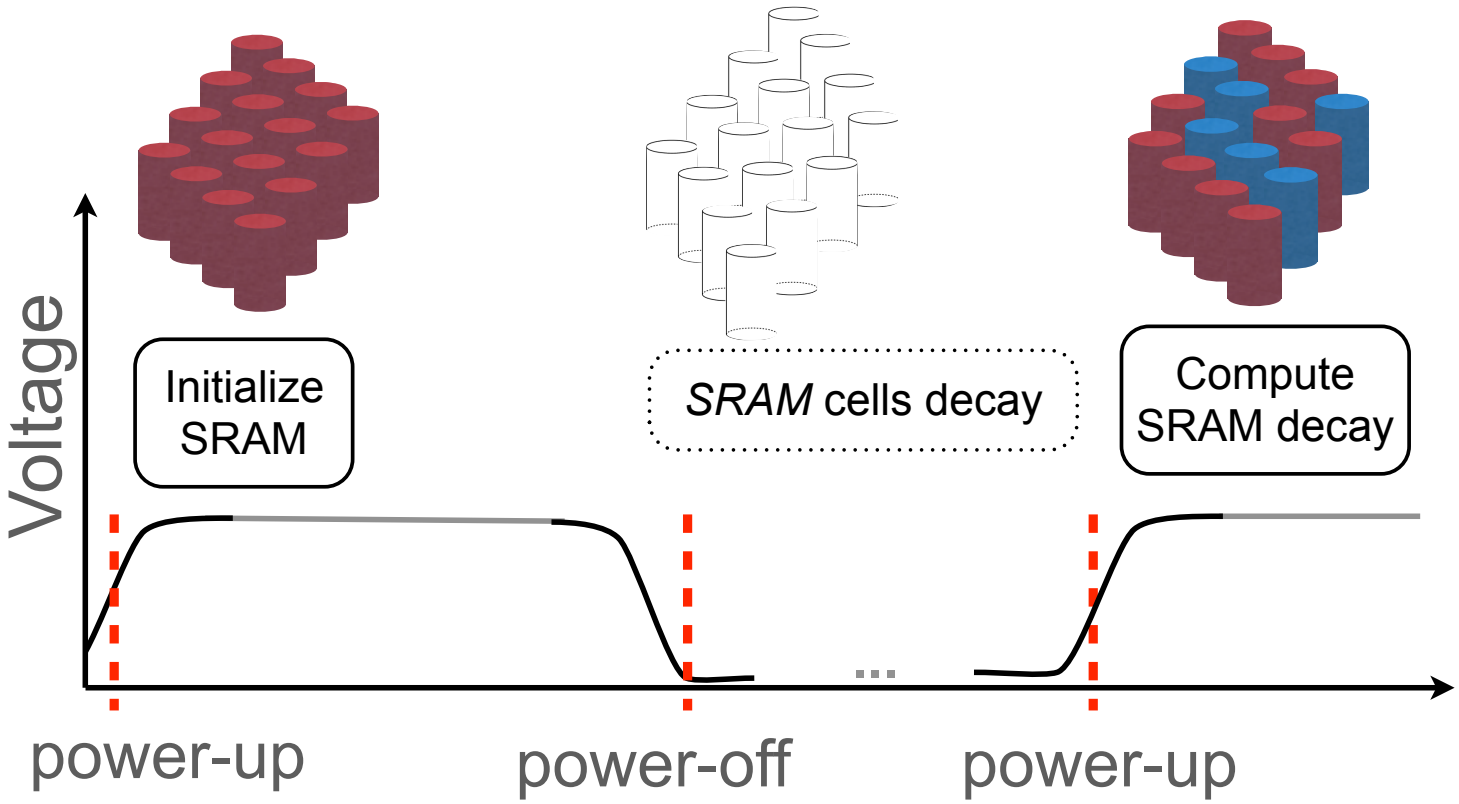
The TARDIS Algorithm



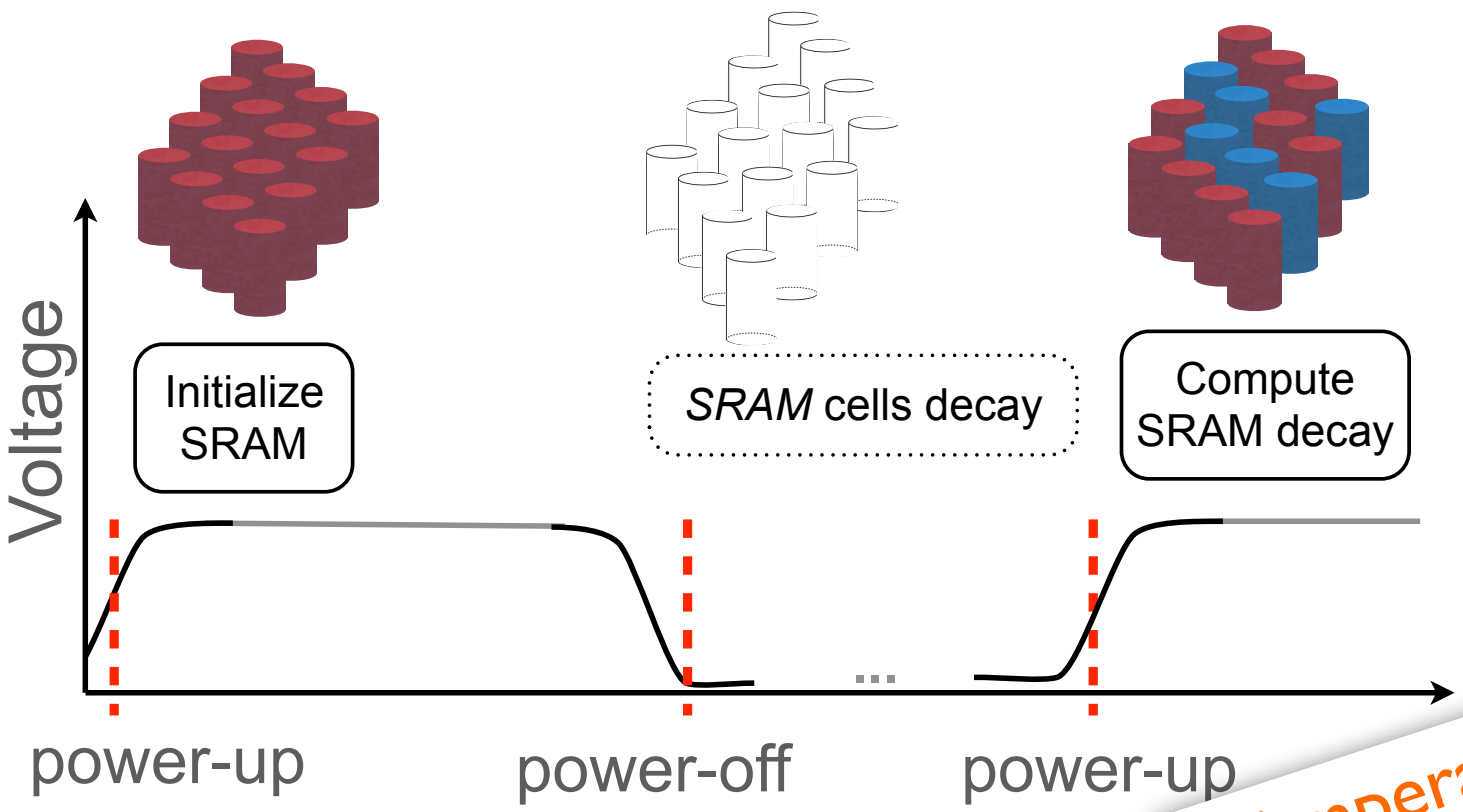
The TARDIS Algorithm



The TARDIS Algorithm



The TARDIS Algorithm

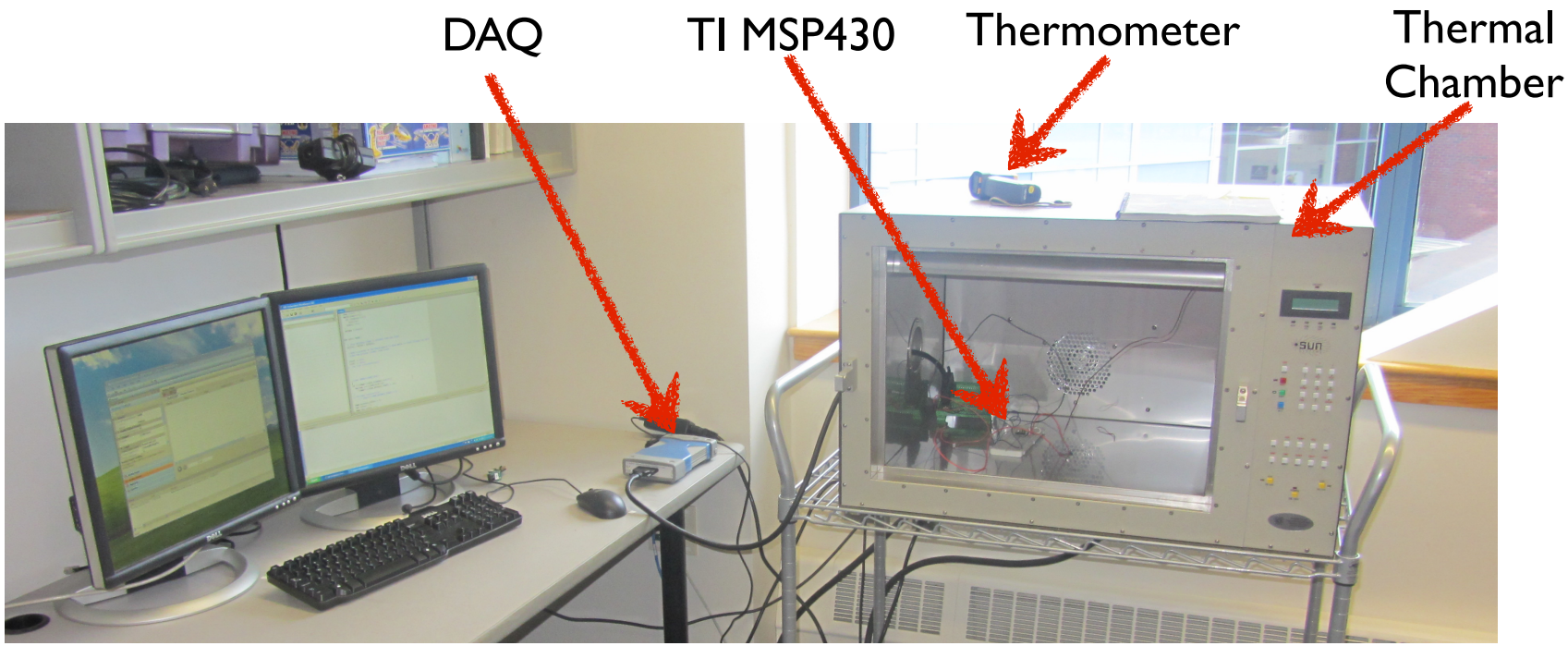


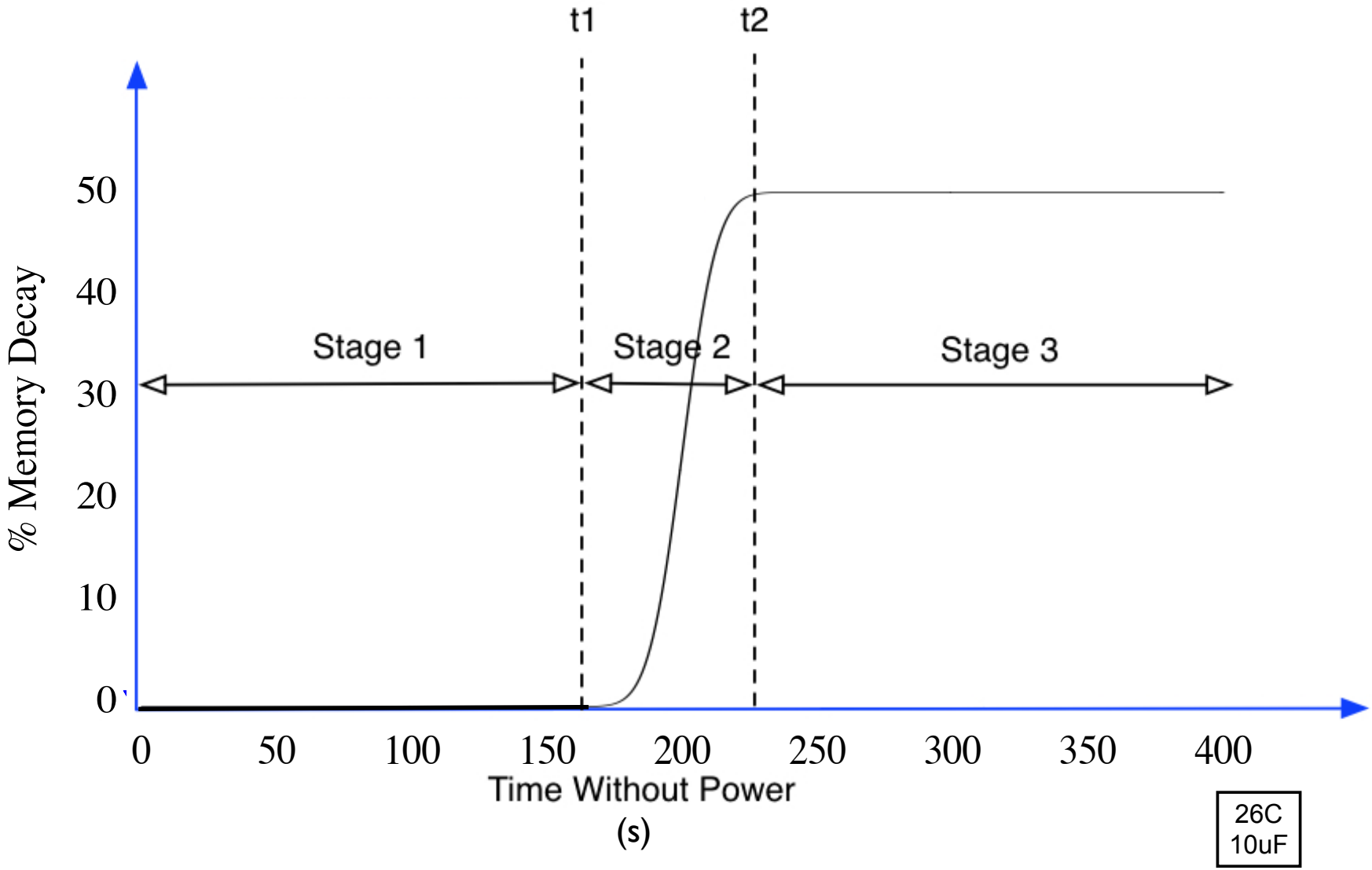
Temperature Later...

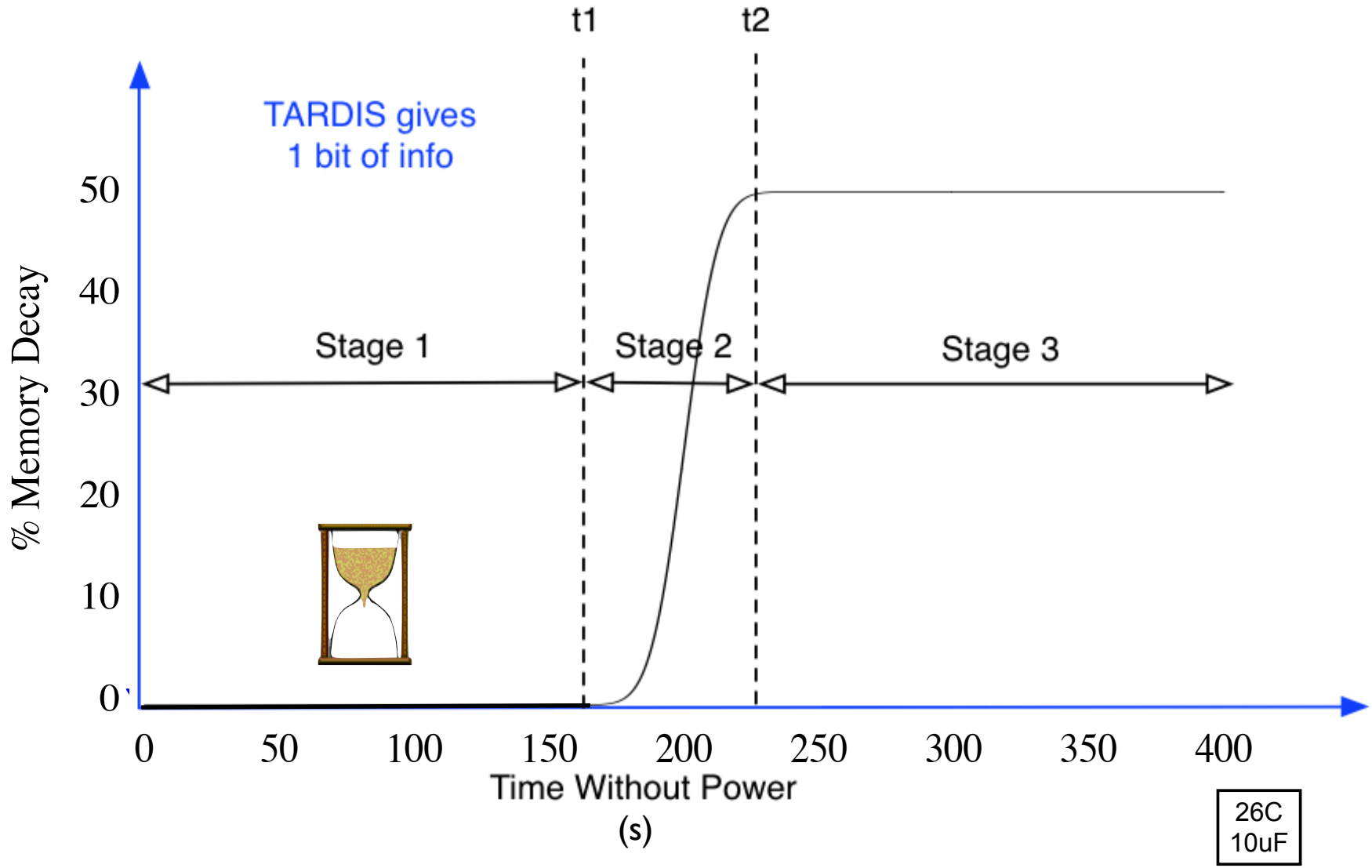
Factors Influencing SRAM Decay

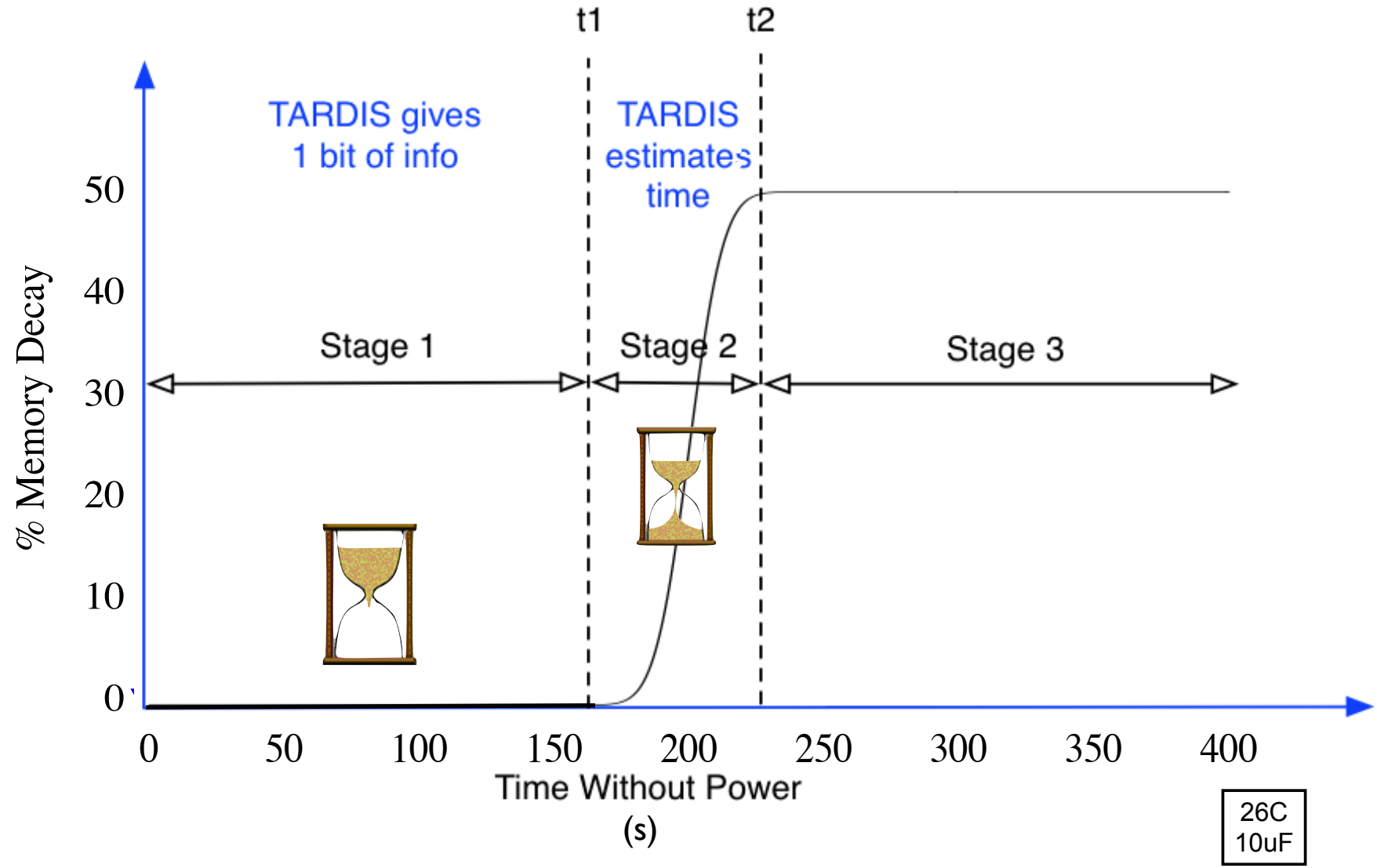
- ✓ SRAM Size
- ✓ Circuit Capacitance
- ✓ Temperature
- ✗ Chip Variation

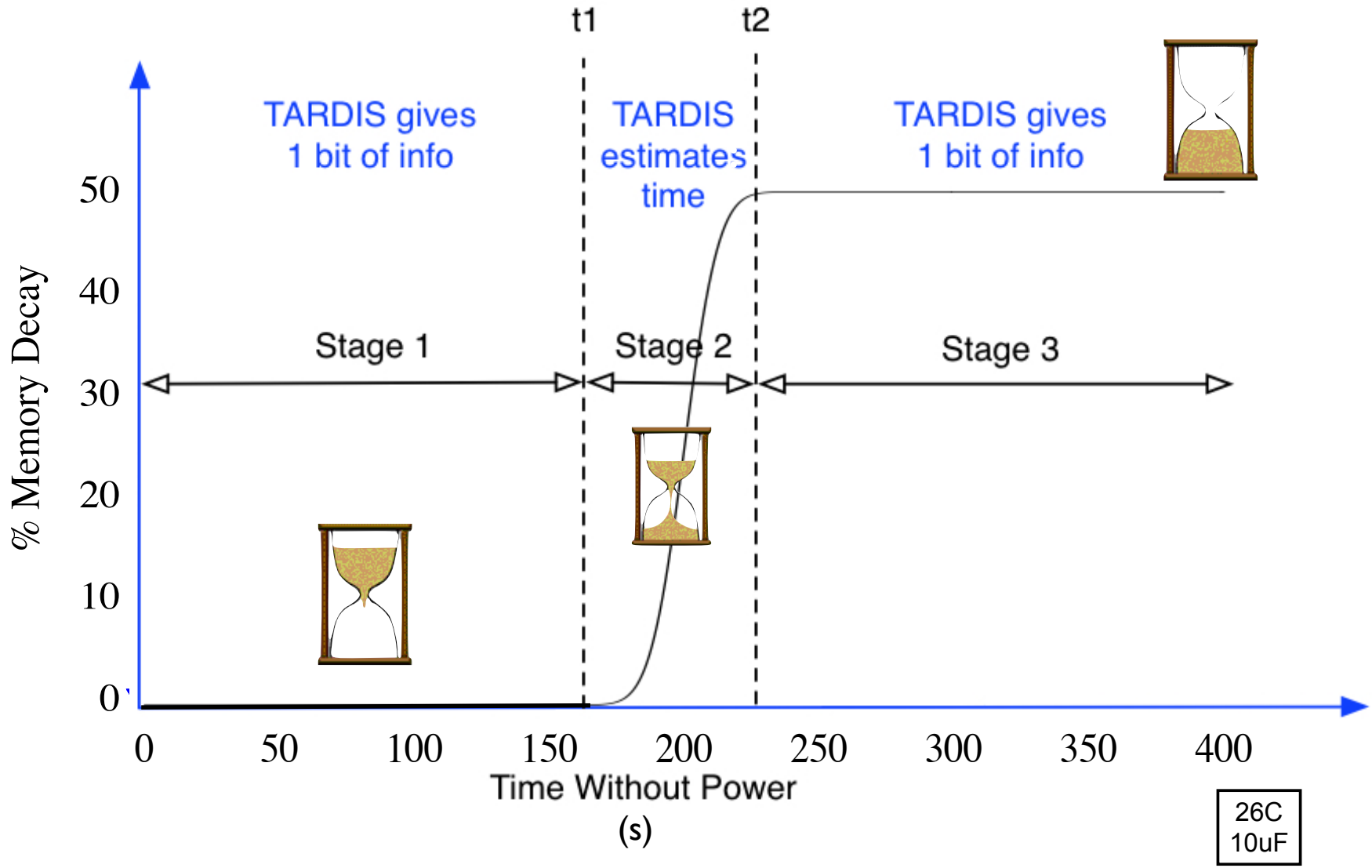
Experimental Setup



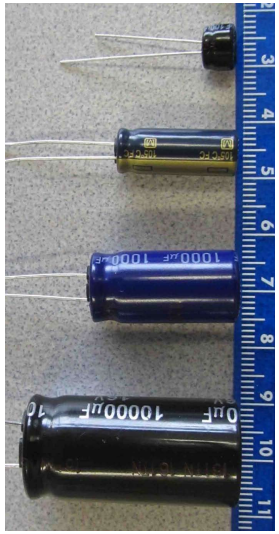

t1
t2
% Memory Decay
50
40
30
20
10
0
Stage 1
Stage 2
Stage 3
0
50
100
150
200
250
300
350
400
Time Without Power
(s)
26C
10uF


t1
t2
TARDIS gives
1 bit of info
% Memory Decay
50
40
30
20
10
0
Stage 1
Stage 2
Stage 3
0
50
100
150
200
250
300
350
400
Time Without Power
(s)
26C
10uF


t1
t2
TARDIS gives
1 bit of info
TARDIS
estimates
time
Stage 1
Stage 2
Stage 3
% Memory Decay
0
10
20
30
40
50
0
50
100
150
200
250
300
350
400
Time Without Power
(s)
26C
10uF

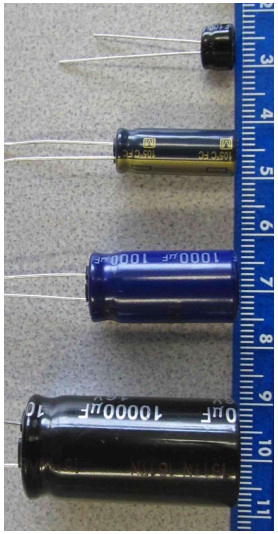

t1
t2
TARDIS gives
1 bit of info
TARDIS
estimates
time
TARDIS gives
1 bit of info
Stage 1
Stage 2
Stage 3
% Memory Decay
0
10
20
30
40
50
0
50
100
150
200
250
300
350
400
Time Without Power
(s)
26C
10uF

Circuit Capacitnce



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

Circuit Capacitnce

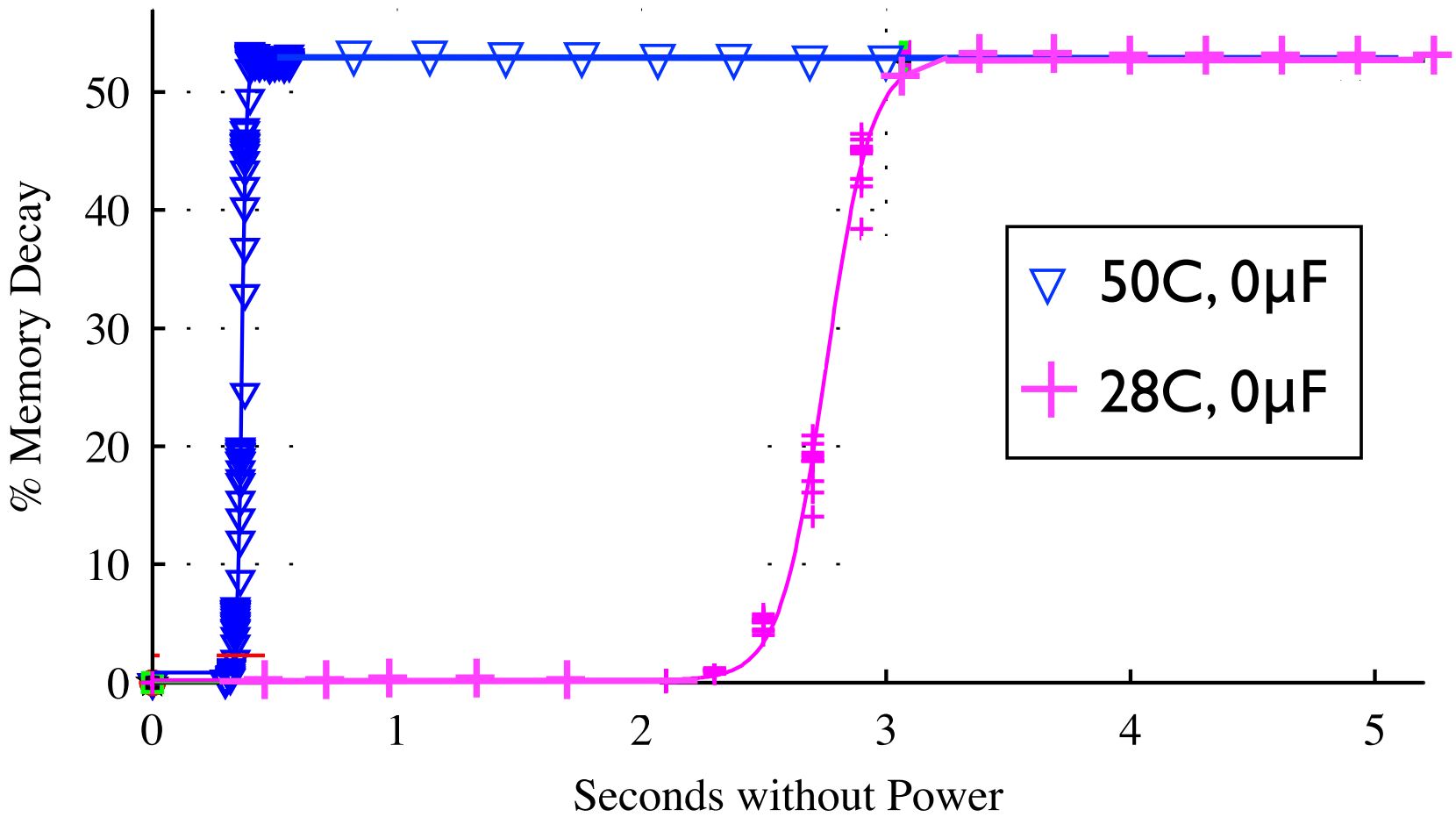


Capacitor Size	Expiration time	Scale
~0μF	2.1×10^{0}s	Seconds
10μF	2.25×10^{2}s	Minutes
100μF	1.98×10^{3}s	1/2 Hour
1000μF	2.12×10^{4}s	Hours
10000μF	$>1.96 \times 10^{5}$s	Days

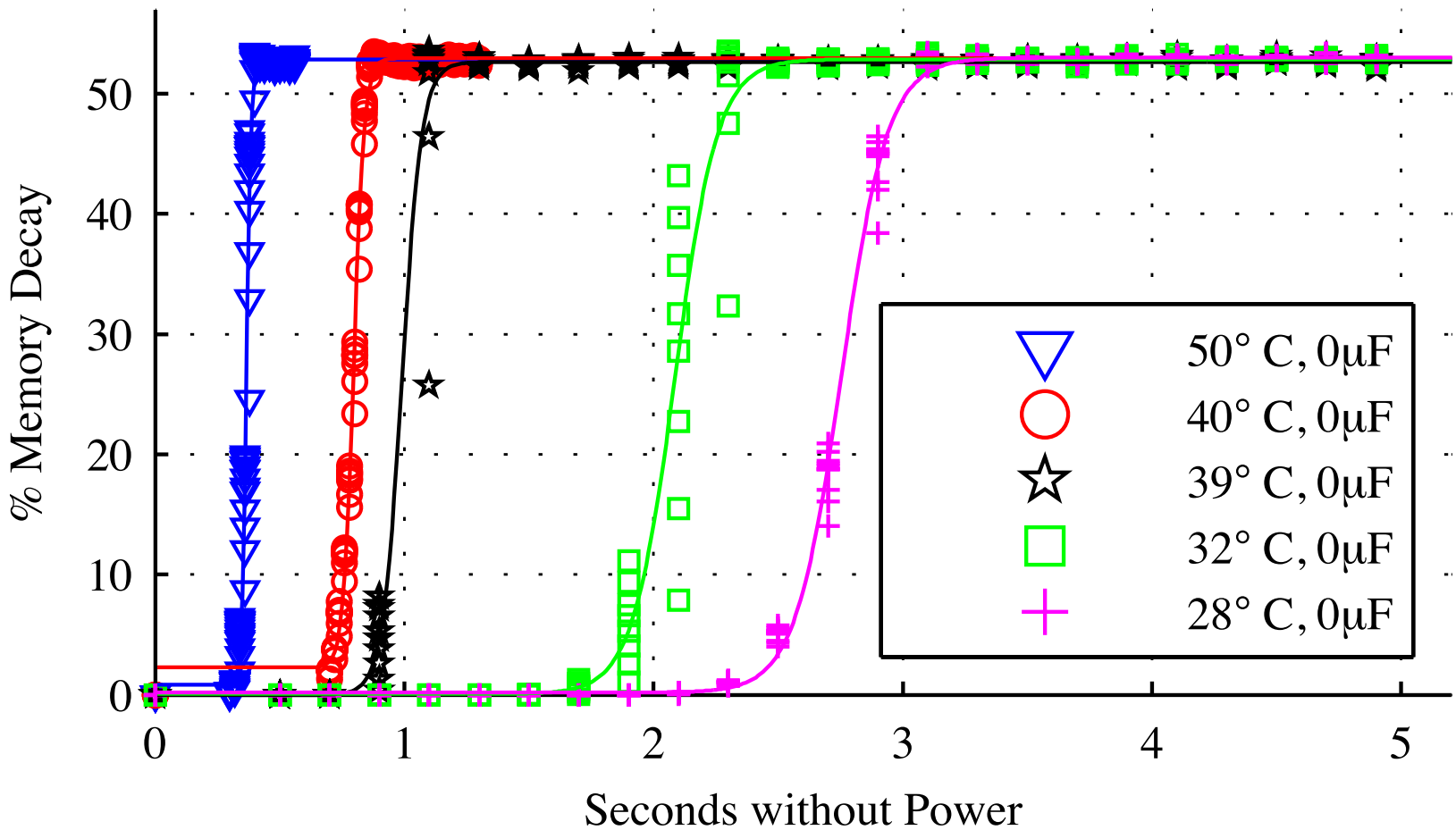
Smart Cards

Batteryless Sensor = 100,000μF

Temperature

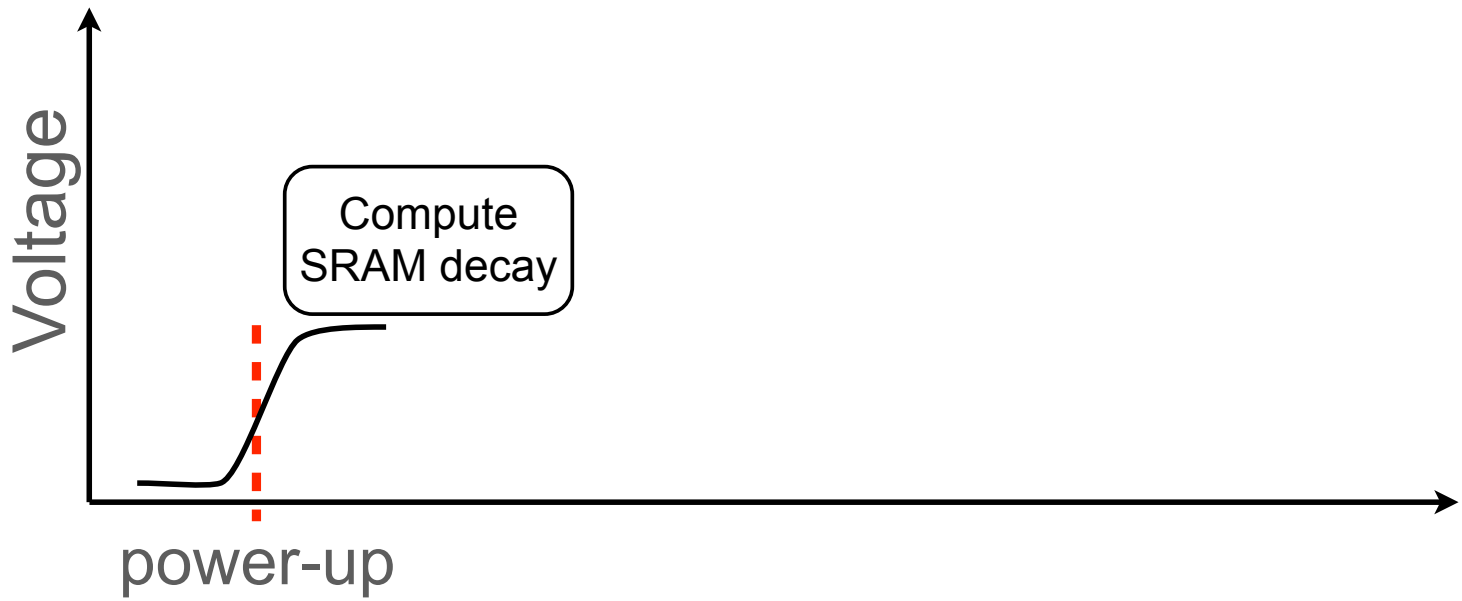


Temperature

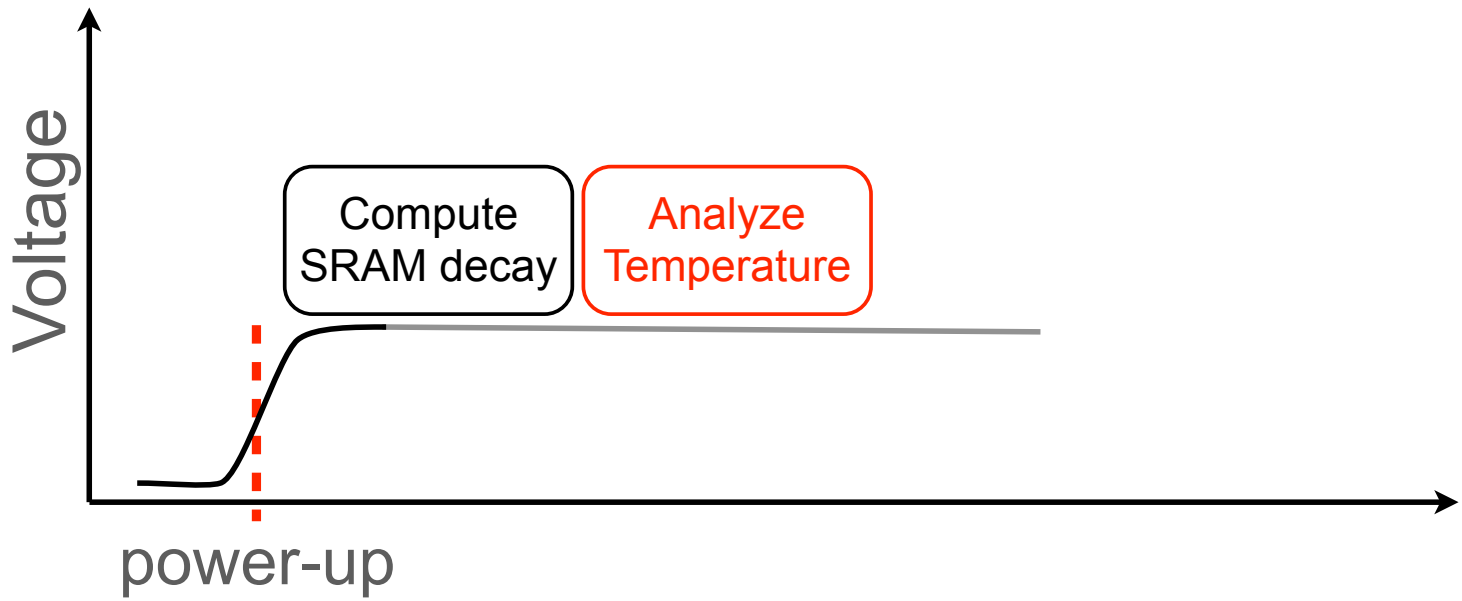


Compensate for Temperature

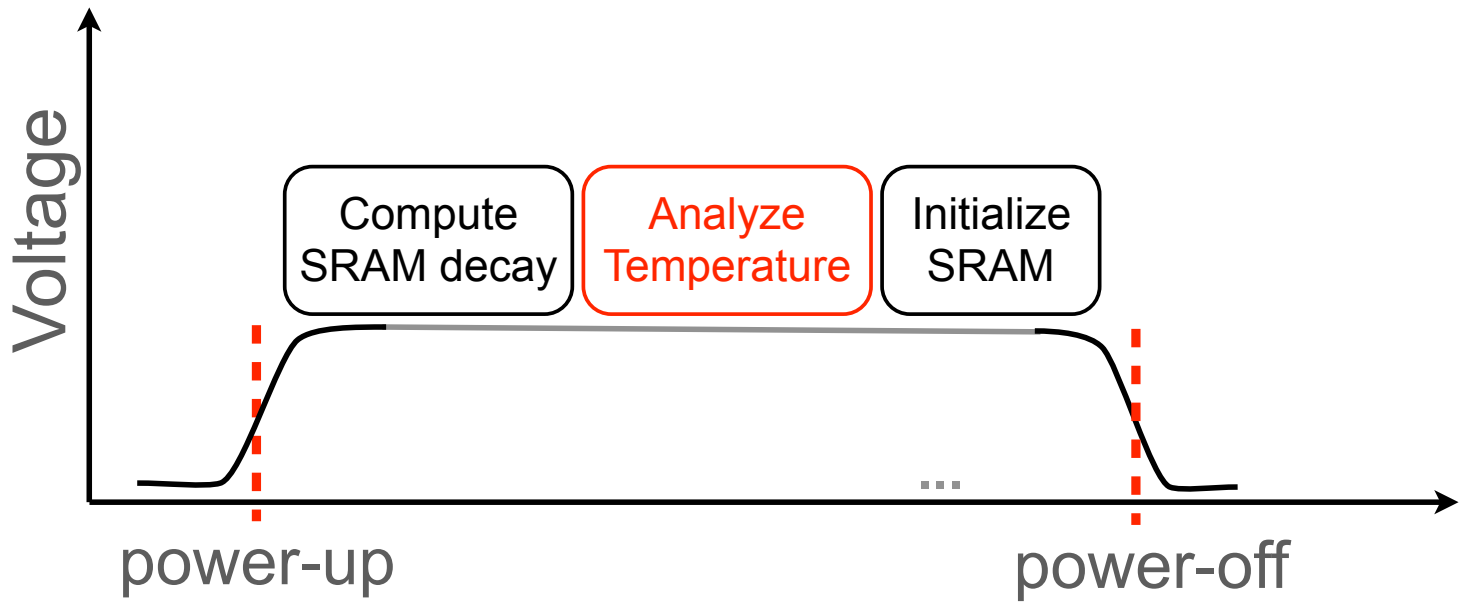
Compensate for Temperature



Compensate for Temperature



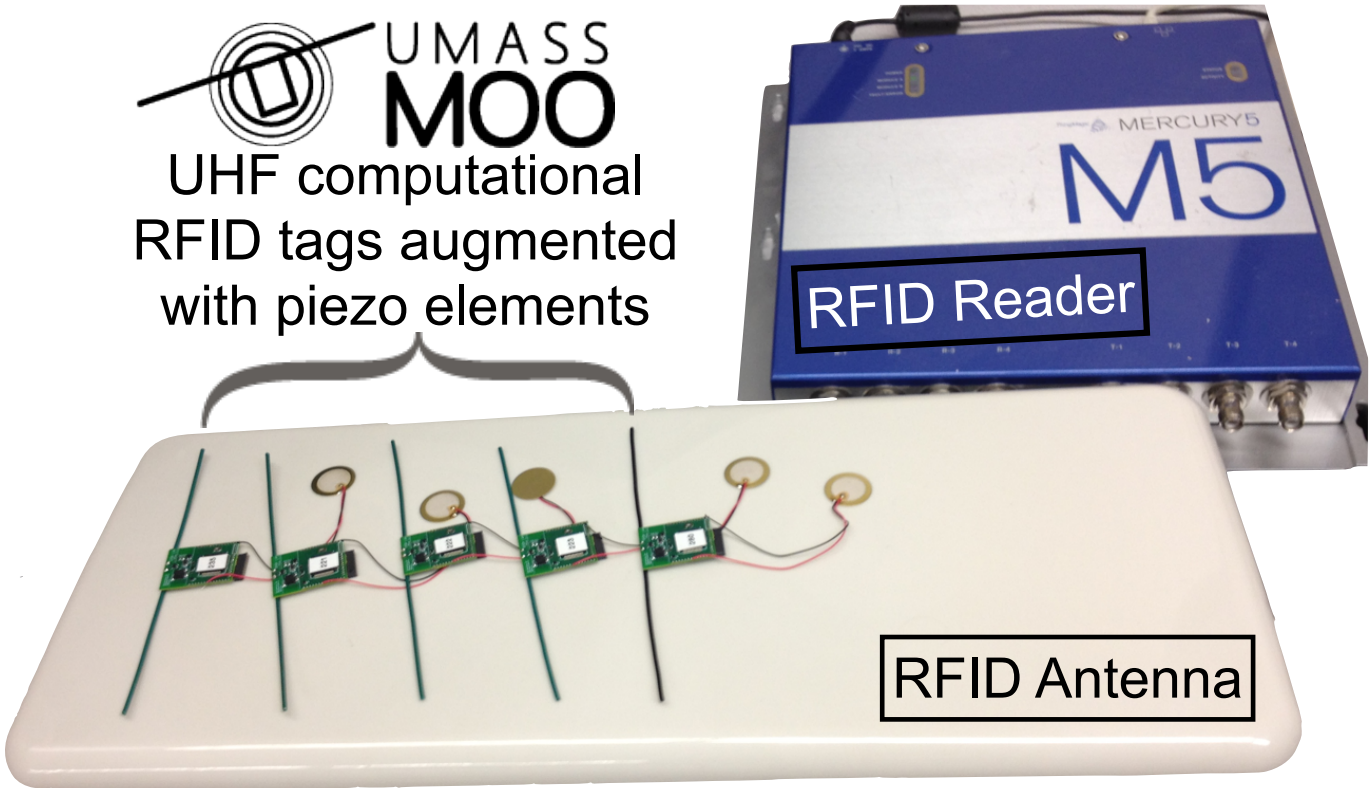
Compensate for Temperature



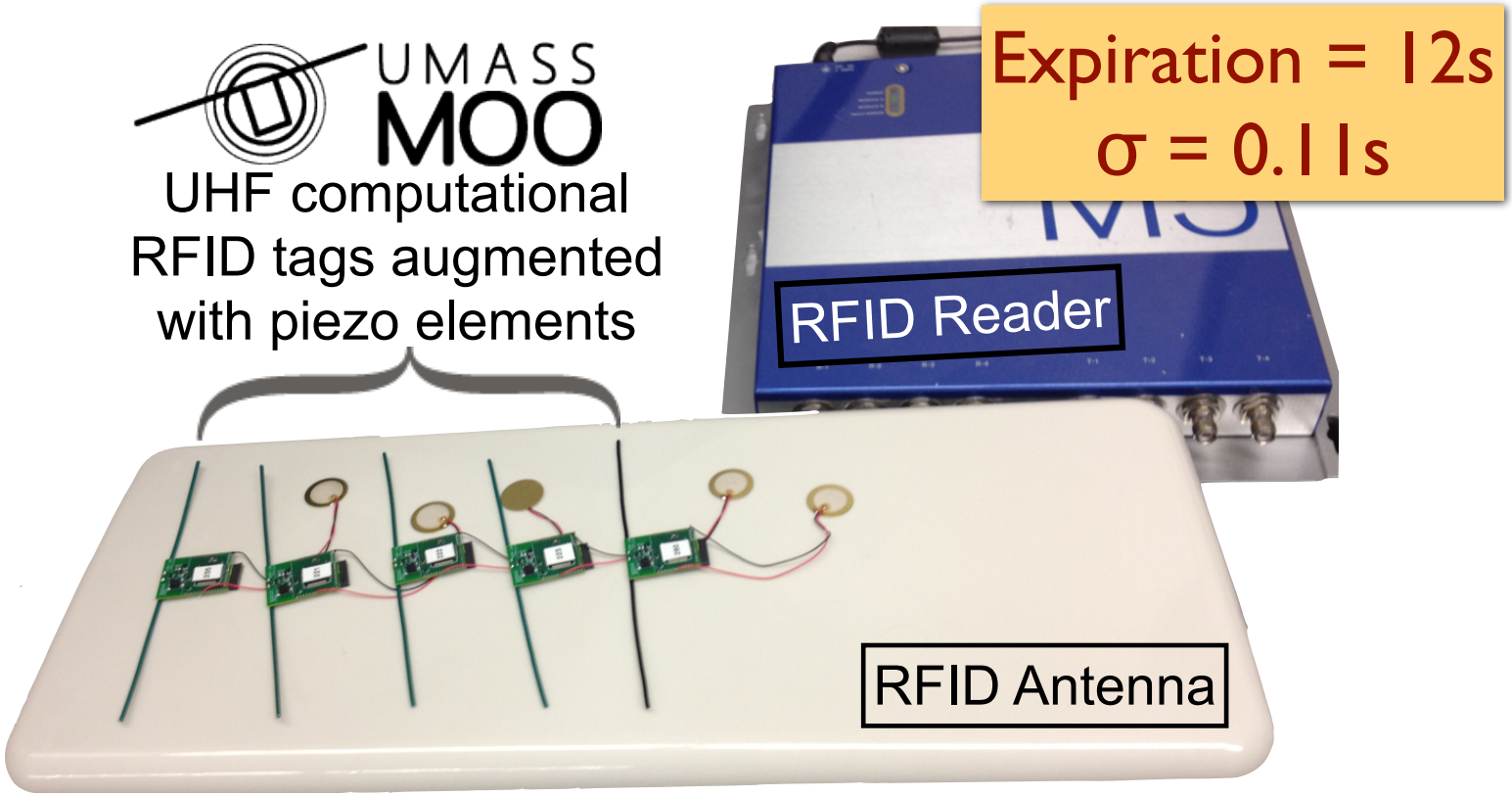
Implementation

UMASS MOO

UHF computational RFID tags augmented with piezo elements



Implementation



The Effect of TARDIS*

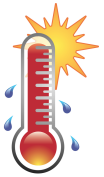
Device	#Queries	Time
UHF RFID Tags[Shamir'07]	200	2 Seconds
MIFARE Classic[Garcia'09]	1,500	16 Seconds
Digital Signal Transponder[Bono'05]	75,000	1 Hour
MIFARE DESFire[Paar'11]	250,000	7 Hours
GSM SIM Cards[Goldberg'99]	150,000	8 Hours

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

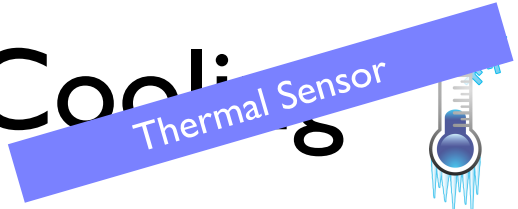
* Assuming a 12 seconds TARDIS

Attacking the TARDIS

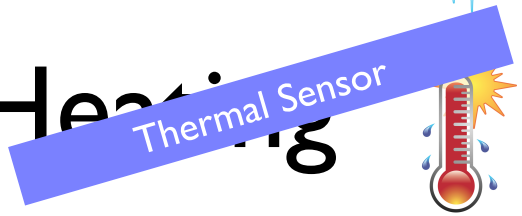
- Cooling 
- Heating 

Attacking the TARDIS

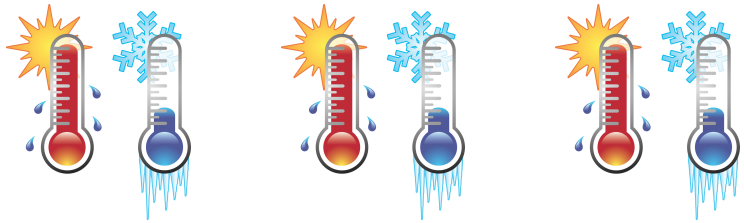
- Cooling



- Heating



Attacking the TARDIS

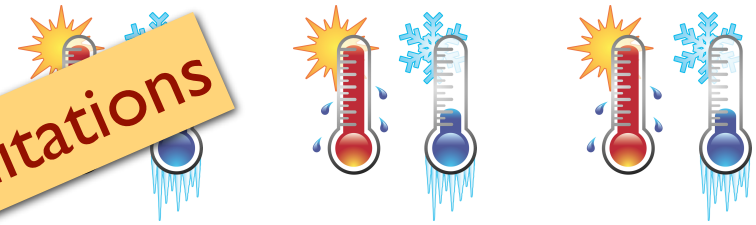
- ~~Cooling~~ Thermal Sensor 
- ~~Heating~~ Thermal Sensor 
- Pulse 

Attacking the TARDIS

- Cooling
- Heating
- Pulse

Thermal Sensor

Thermal Sensor



Physical Limitations

Attacking the TARDIS

- Cooling
- Heating
- Pulse

Thermal Sensor

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.

Photo Credit: thinkgeek.com

SPQR LABORATORY

https://spqr.cs.umass.edu/tardis/