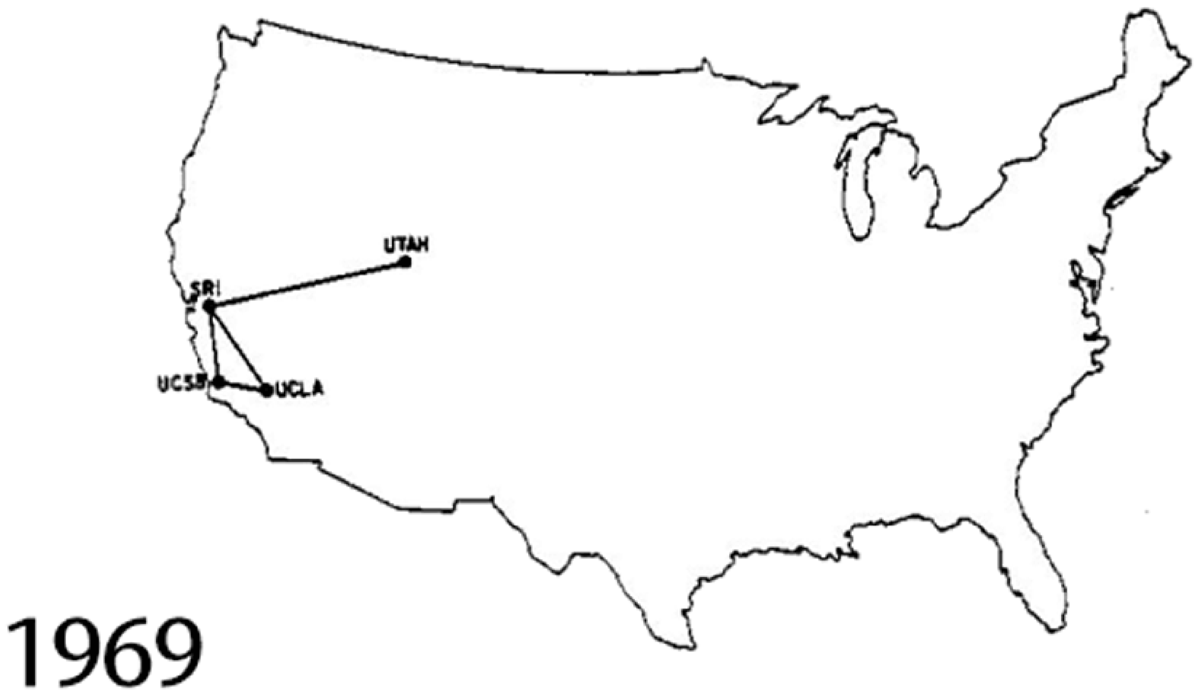
Security and Privacy for the Internet of Things

Biplab Sikdar
Department of Electrical and Computer Engineering
National University of Singapore, Singapore

The Internet in 1969

- Four computers
- University of California, Los Angeles
- SRI (Stanford Research Institute)
- University of California, Santa Barbara
- University of Utah
- 29/10/1969: First packets sent. Charlie Kline attempted to remote login from UCLA to SRI. The system crashed on receiving “g”.

The Internet in 1969



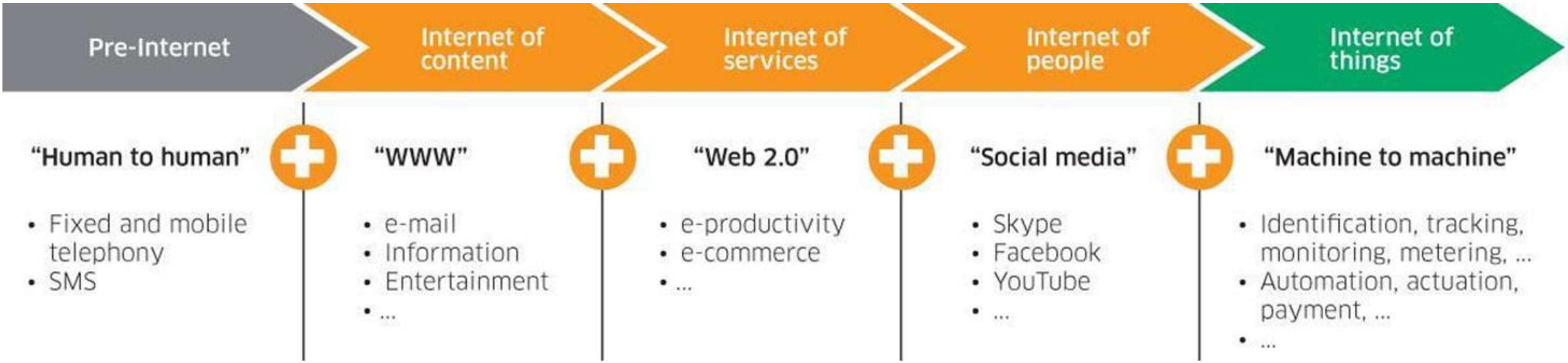
Common Applications Back Then

- Telnet: Remote login
- Electronic mail (1971): 75% of network traffic in 1973
- File transfer protocol (1973)
- Network voice protocol (1977)
- Mailing lists (LISTSERVs): virtual discussion groups (one of the first was SF-LOVERS, dedicated to science fiction fans)

The Application that Changed it All

- Hyper Text Transfer Protocol (HTTP): world wide web
- Led to the popularity of the "Internet"
- Internet commerce
- Social media
- Sharing economy

The Internet-of-Things: Evolution



Source: Marc Jadoul, Nokia, "The IoT: The next step in internet evolution", 2015

IoT Application Domains

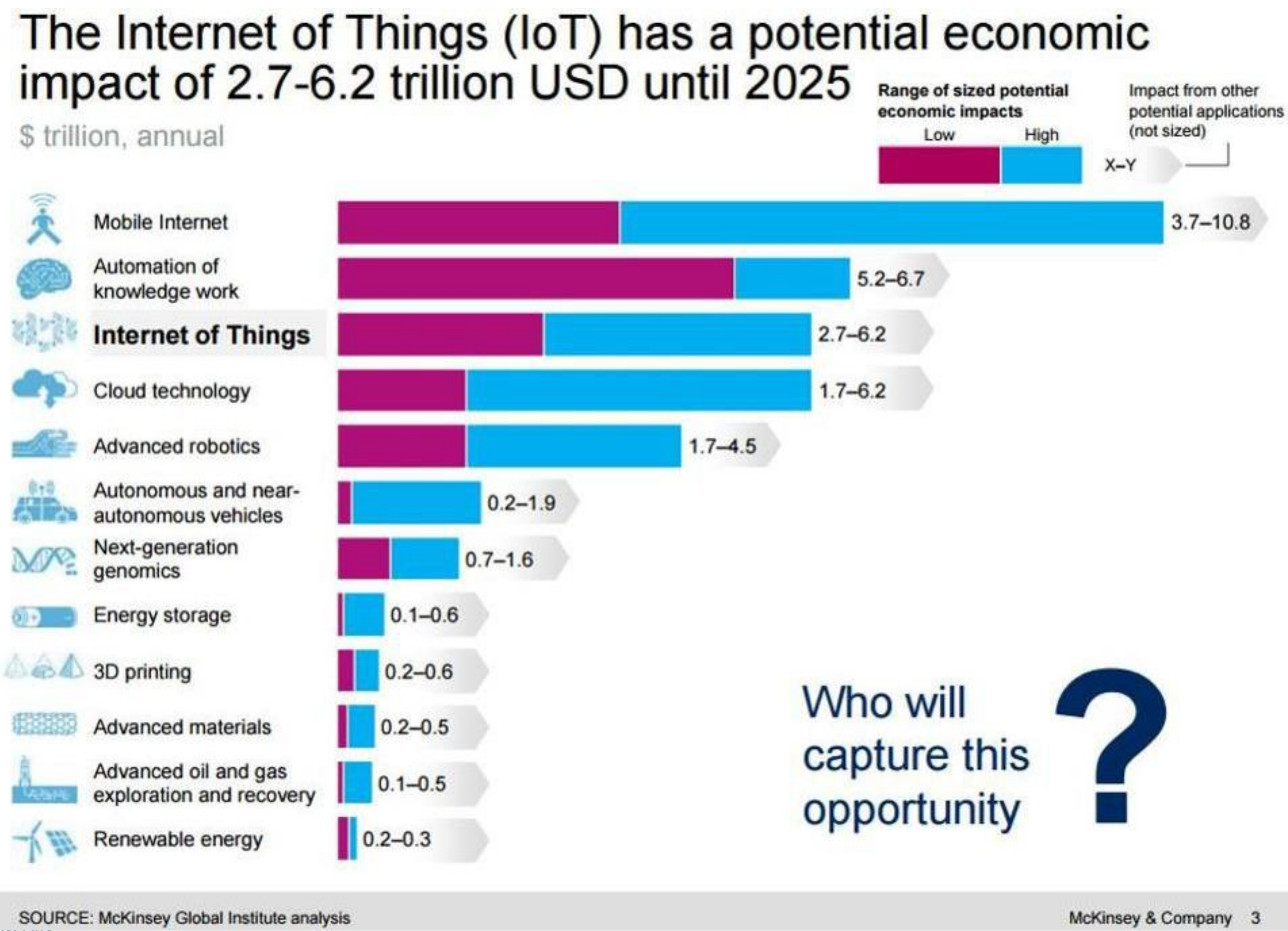
IOT ANALYTICS

2018

Insights that empower you to understand IoT markets

#	IoT Segment	Global share of IoT projects[1]	Americas	Europe	APAC	Trend[2]
1	Smart City	23%	34%	45%	18%	
2	Connected Industry	17%	45%	31%	20%	
3	Connected Building	12%	53%	33%	13%	
4	Connected Car	11%	54%	30%	12%	
5	Smart Energy	10%	42%	35%	19%	
6	Other	8%	50%	34%	11%	
7	Connected Health	6%	55%	29%	15%	
8	Smart Supply Chain	5%	49%	36%	12%	
9	Smart Agriculture	4%	39%	26%	31%	
10	Smart Retail	4%	53%	35%	9%	

The Internet-of-Things



National University of Singapore

Security Concerns

Stuxnet: Iran

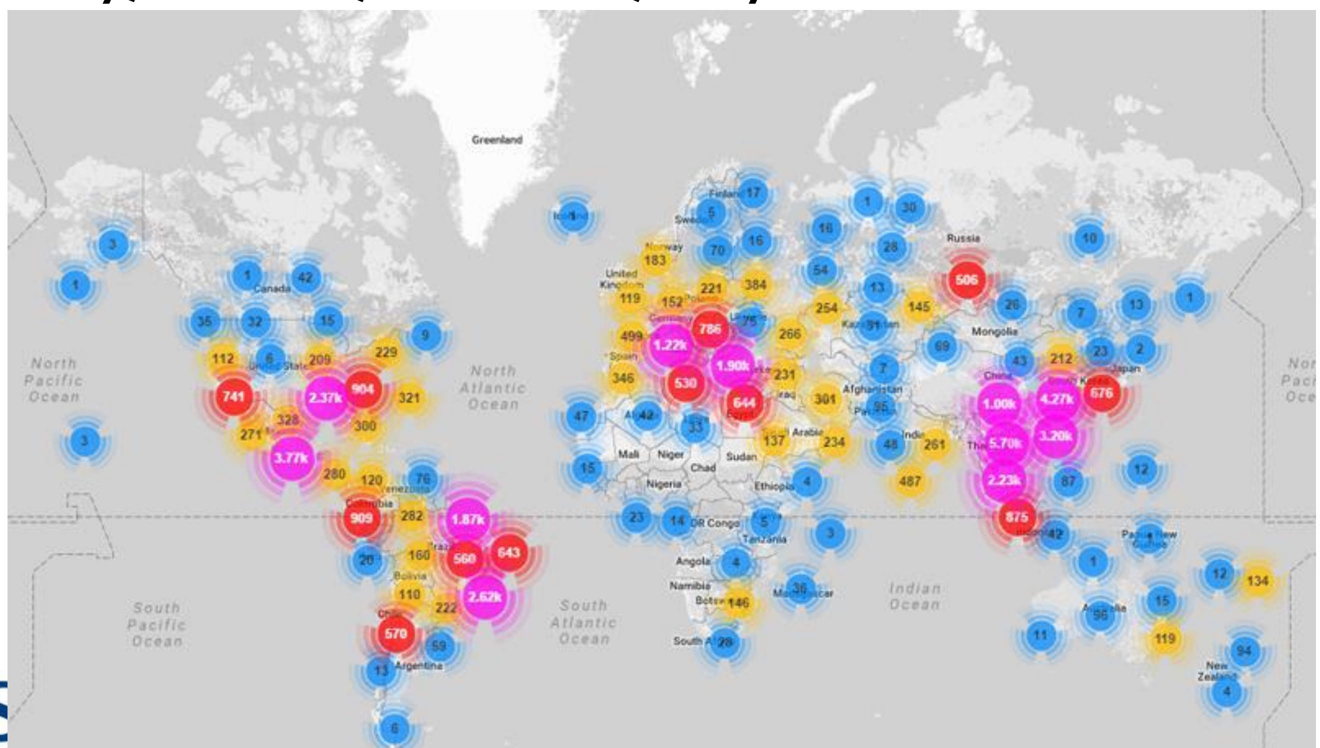
Ukraine Power Outage

Lansing BWL Ransomware

Saudi Aramco Cyberattack

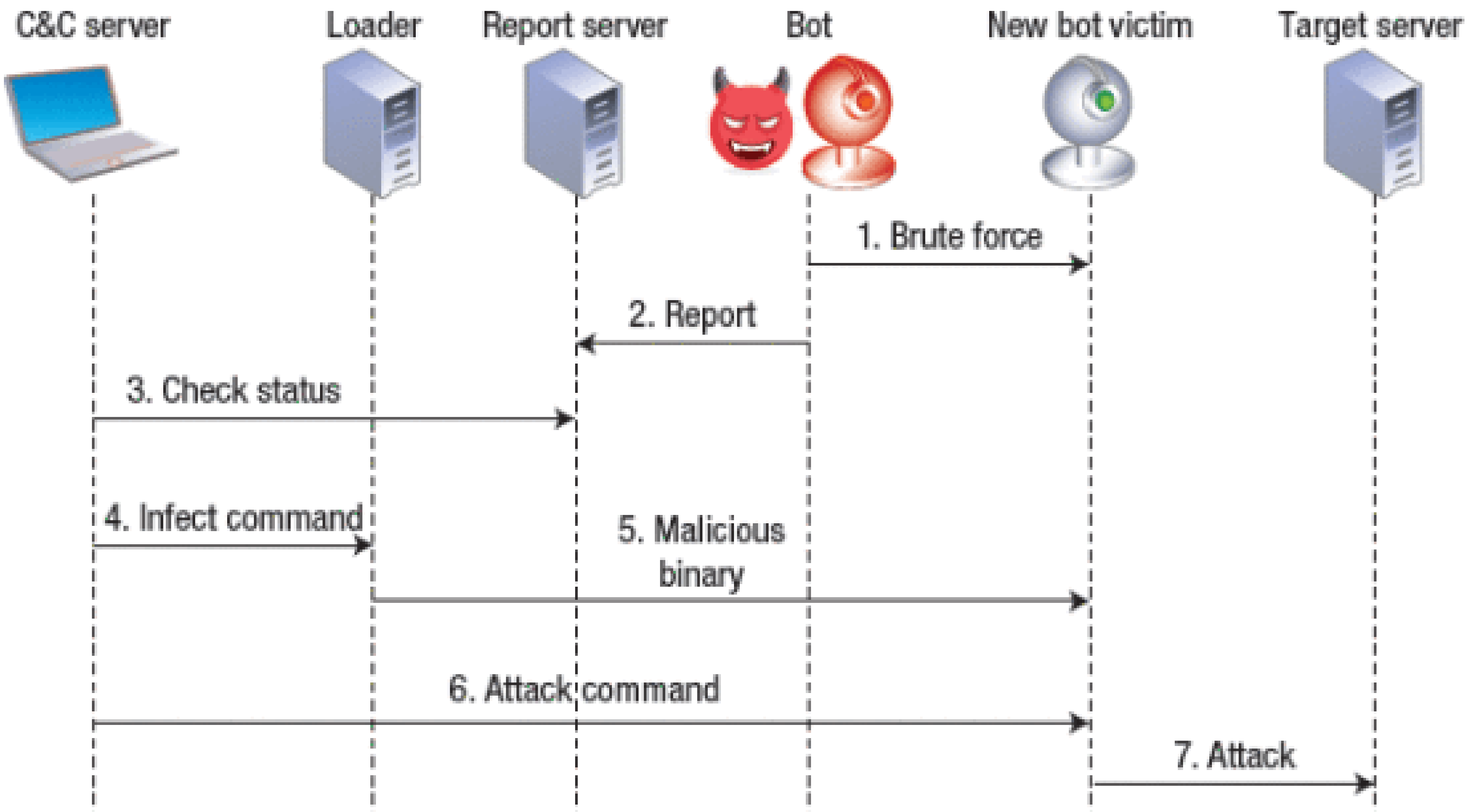
Mirai Botnet Attack

- DDoS attack on Dyn
- Dyn provides DNS services for Twitter, SoundCloud, Spotify, Reddit, Amazon, PayPal and other sites



NUS National University of Singapore

Mirai Botnet Overview

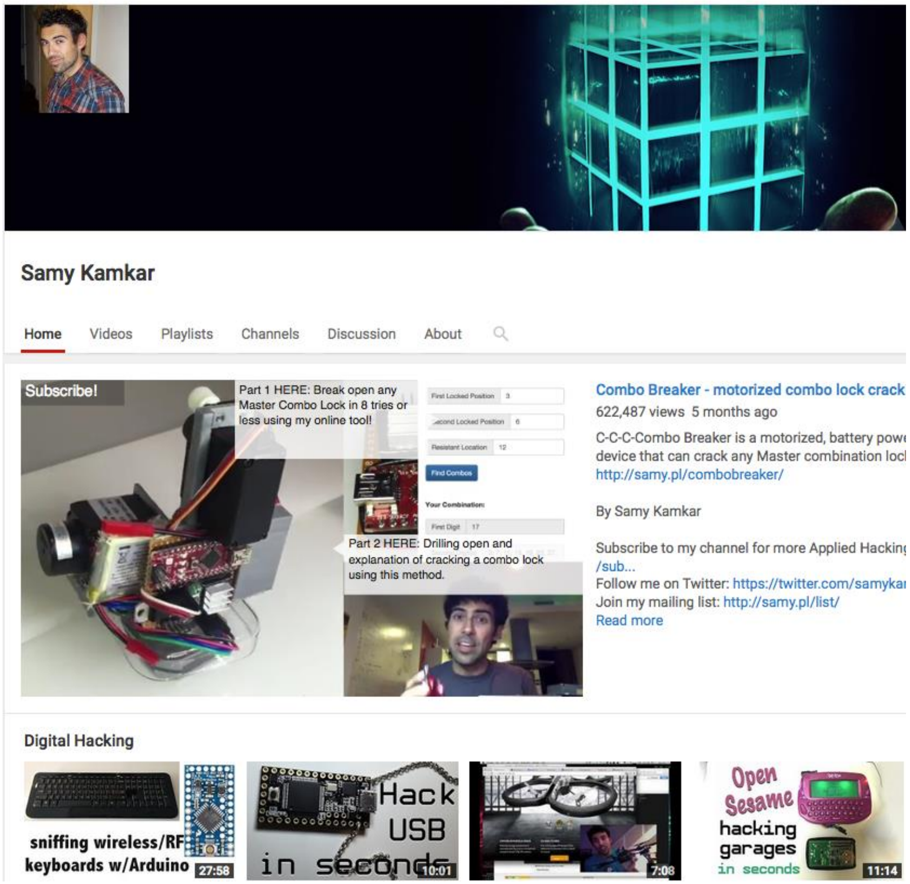


Mirai Botnet Attack

- Took over a number of IoT Devices such as CCTV cameras, DVRs, routers
  - White-labeled DVR and IP cameras
  - username: root and password: xc3511
  - password hardcoded into device firmware

Other Attacks involving IoT Devices

Hardware hacking



"Junk hacking"

"Stunt hacking"

Security for the IoT

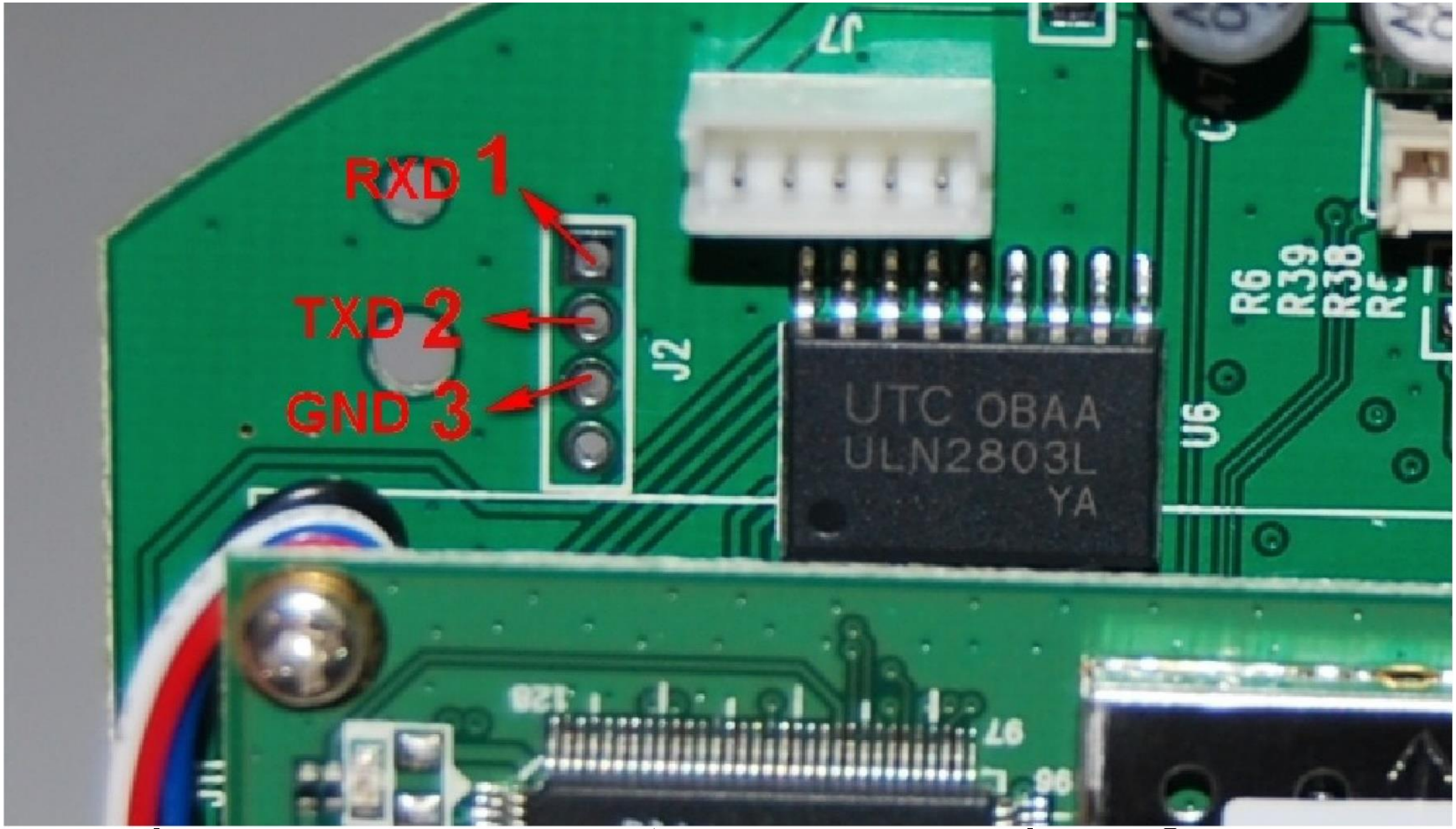
- Authentication, Integrity, Confidentiality: application specific requirements
- Lightweight security protocols for constrained environments
- Privacy preserving service
- Trust and ownership issues
- Physical Security

Image: www.wordstream.com

Why are IoT Devices Targeted?

- Always on – IoT devices are rarely turned off
- Many manufacturers shy away from security in favor of usability
- IoT devices aren't checked on by users – "setup and forget"
- There are millions of them – this allows for a significant amount of DDoS traffic from these devices
- Users don't interact with their devices actively – less likely to notice a hijacker

Top IoT Vulnerabilities



Security Challenges in IoT

- Shared data with monetary value
- Attacks on end point devices can propagate quickly
- Large number of identical devices (homogeneity)
- No user Interface
- Applications may not tolerate errors, control critical equipment or processes
- Limited computing and battery power
- Limited visibility into or control over internal workings

Securing an IoT System

- Secure data handling framework: control over data and the sources and the consumers of data
- Establishment and trust management
- Access control and account management (for devices without UI)
- Use of secure protocols for data transmission
- Firewall management and antivirus updates
- Remote updates and patching for IoT devices

Securing an IoT System

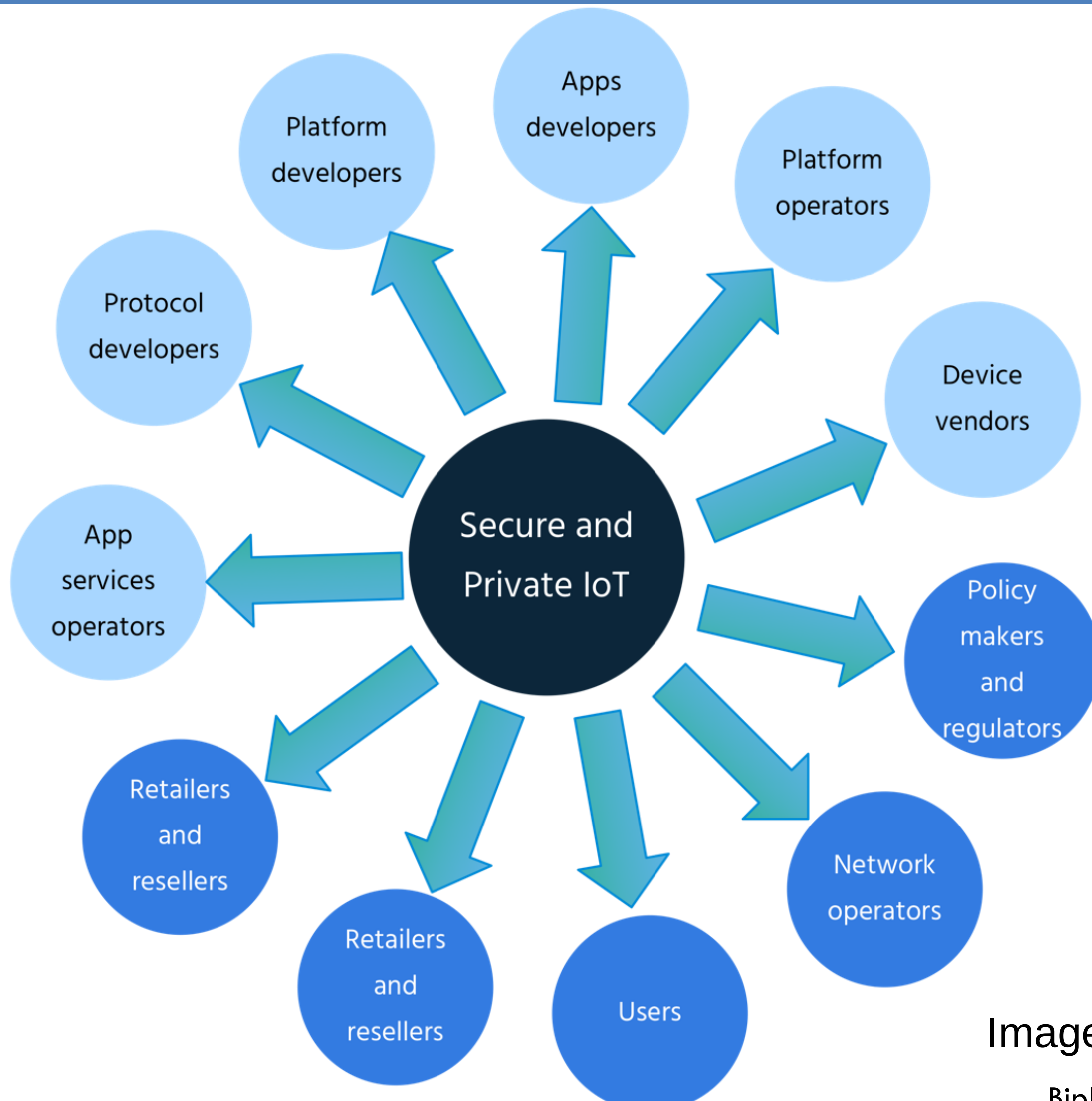


Image: Karen O'Donoghue

Physical Security for the IoT

- Conventional approach: embed secure secrets in IC
  - Non-volatile memory (ROM, Fuse, Flash or EEPROM)
  - Battery-backed RAM
- Many IoT devices deployed in remote or unattended locations
- Small size of IoT devices: easy to conceal if stolen
- Attacks on a physically accessible device:
  - Opening the device to gain access to its component parts
  - Connecting a lead to access a physical port on the device
  - Contactless technology to detect device activity: electromagnetic radiation, high/low frequency sounds, power supply fluctuations

Solution: Hardware Security Primitives

- Components that make up IoT devices include semiconductor based devices (ICs), passive components, sensors, batteries etc
- The manufacturing process of these components can provide them with unique characteristics
- Use these unique characteristics as security primitives or fingerprints

Physical Unclonable Functions

- [Suh07] "A Physical Unclonable Function (PUF) is a function that maps a set of challenges to a set of responses based on an intractably complex physical system"
- Exploit process variations during IC fabrication
  - Variation is inherent in fabrication process
  - The variations are unique for each physical instance
  - The variations are hard to eliminate or predict
  - Relative variation tends to increase as the fabrication process moves to smaller sized components

Physical Unclonable Functions

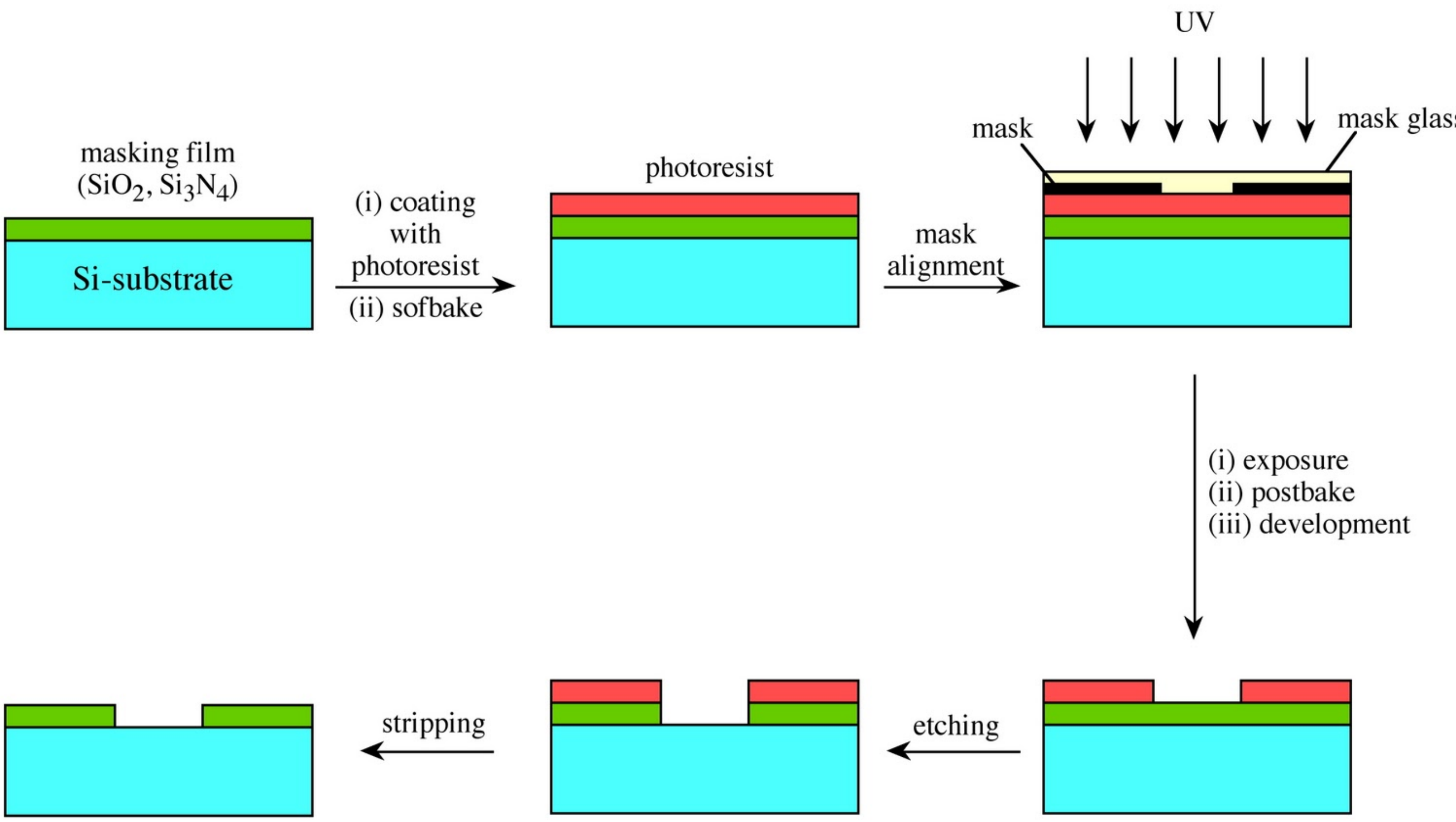
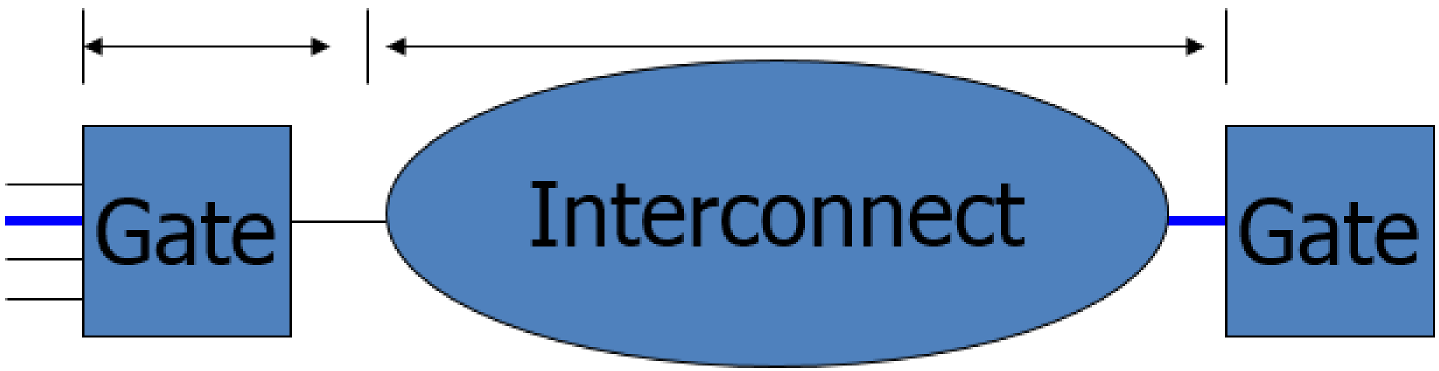


Image: Andrew Barron

Physical Unclonable Functions

- Circuit delay = Interconnect delay + Gate delay



Circuit Delay

Physical Unclonable Functions

- Designed versus fabricated features

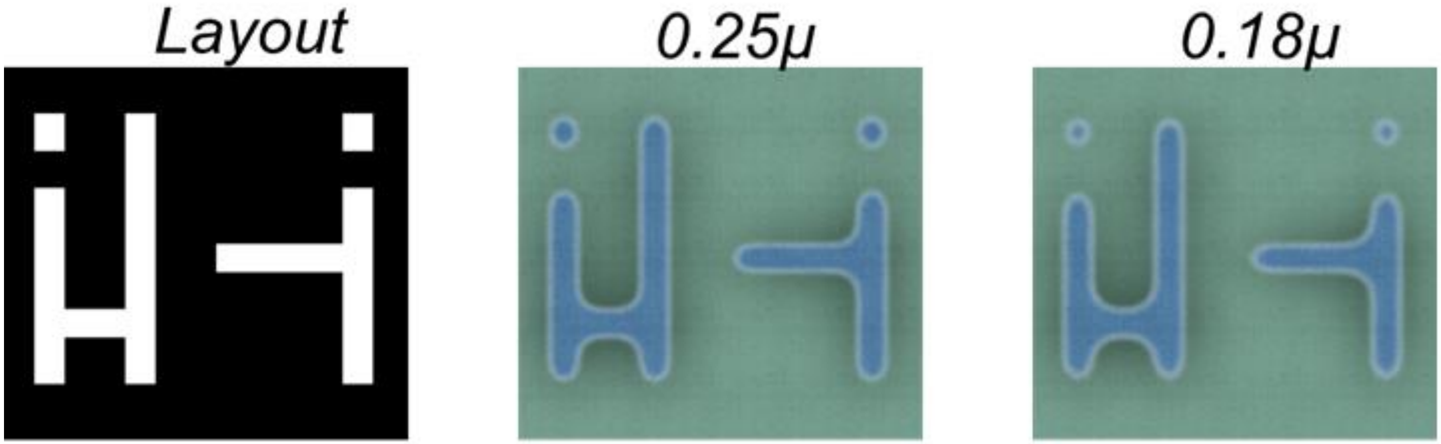


Image: Liu and Hu

Physical Unclonable Functions

- Chip design cannot be reliably fabricated
  - Gap
    - Lithography technology: 193nm wavelength
    - VLSI technology: 45nm features

Technology node	130nm	90nm	65nm	45nm
Gate length (nm) Tolerable variation (nm)	90 5.3	53 3.75	35 2.5	28 2
Wavelength (nm)	248	193	193	193

Source: Liu and Hu

Physical Unclonable Functions

- Chip
  - G

length

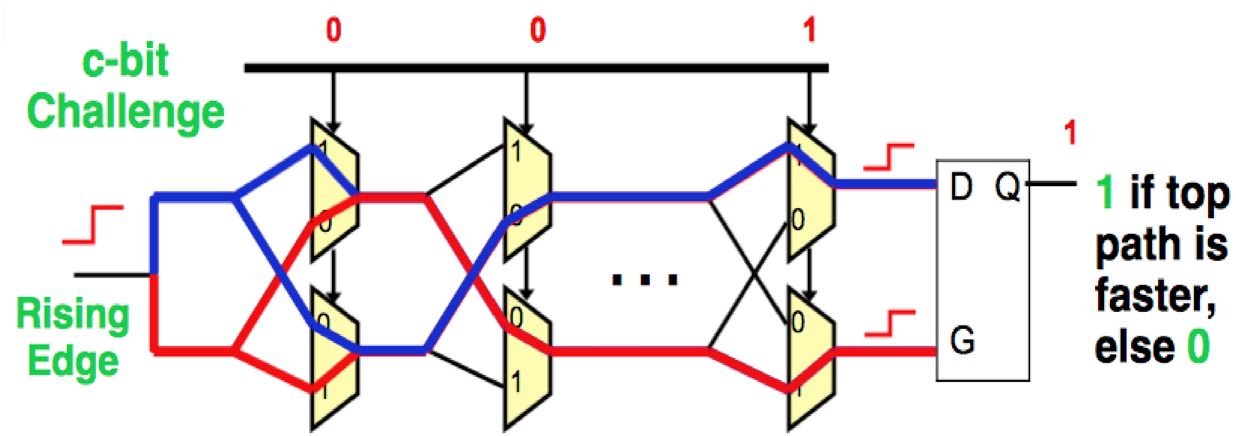
Large wavelength will degrade the printing quality, and thus there are significant variations on feature sizes (wire widths or channel wire).
After printing, circuit delay can be significantly different from what it is designed.

Technology node	130nm	90nm	65nm	45nm
Gate length (nm) Tolerable variation (nm)	90 5.3	53 3.75	35 2.5	28 2
Wavelength (nm)	248	193	193	193

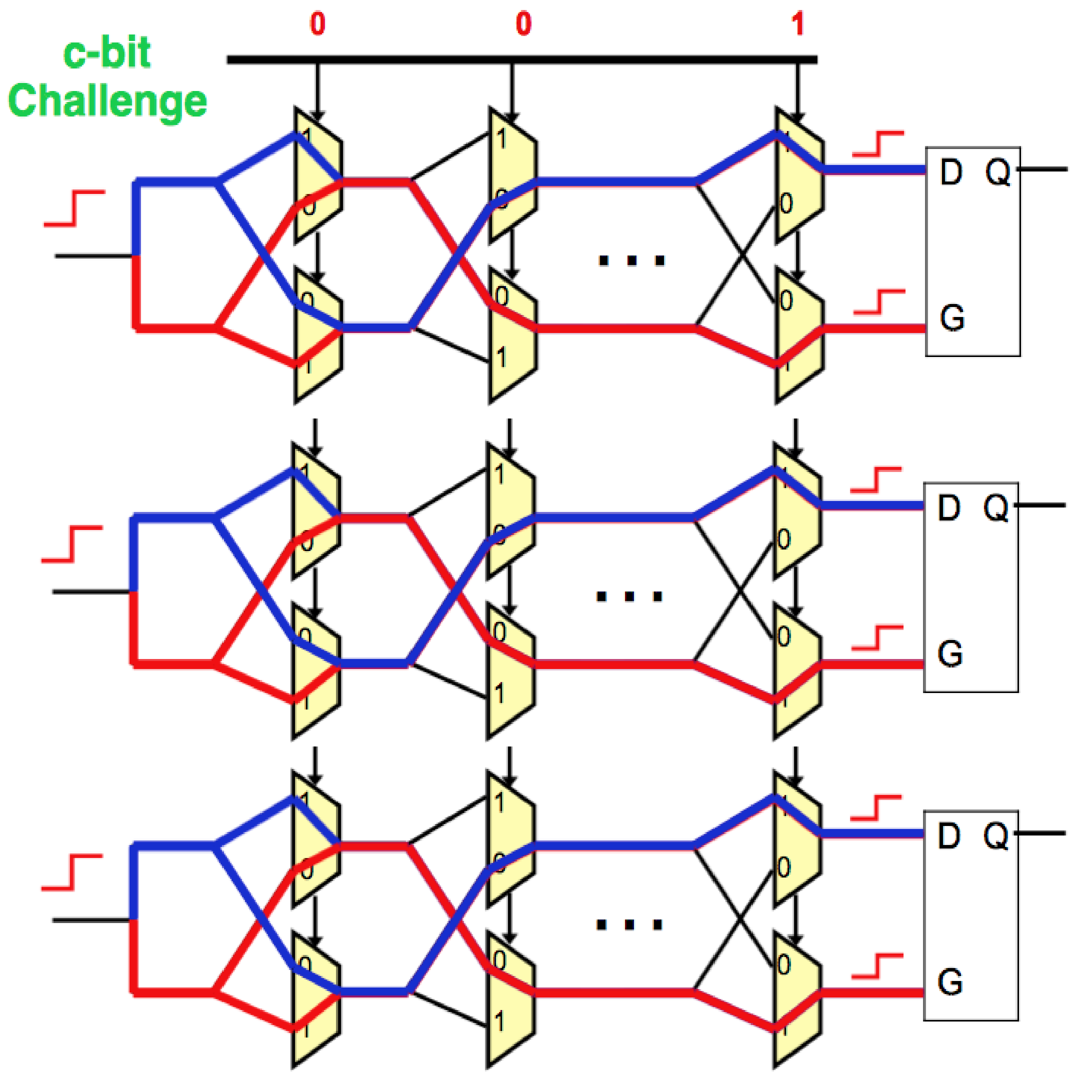
Source: Liu and Hu

Example: Arbiter PUF

- A c-bit challenge is given to the PUF
- Each challenge creates two paths through the circuit that are excited simultaneously
- The digital response is based on a (timing) comparison of the path delays



Example: Arbiter PUF



Physical Unclonable Functions

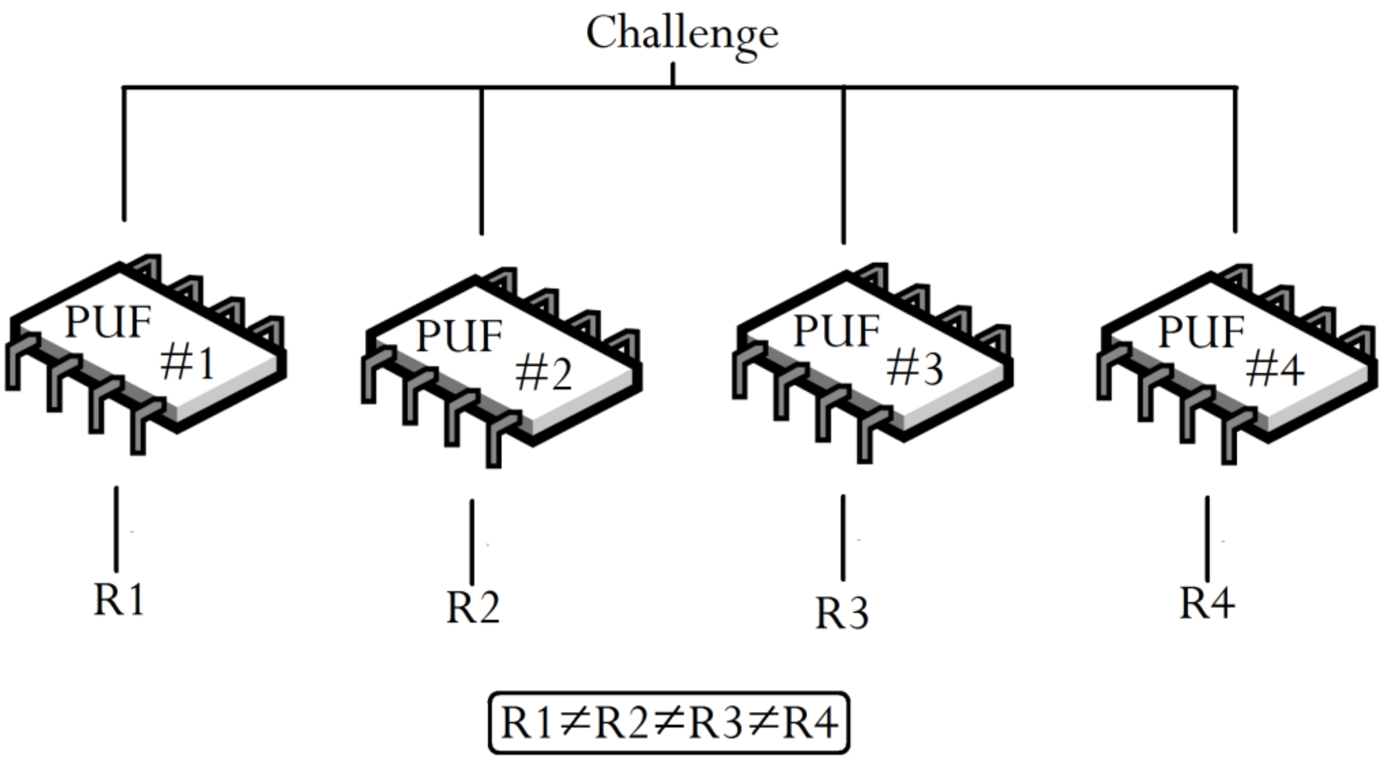


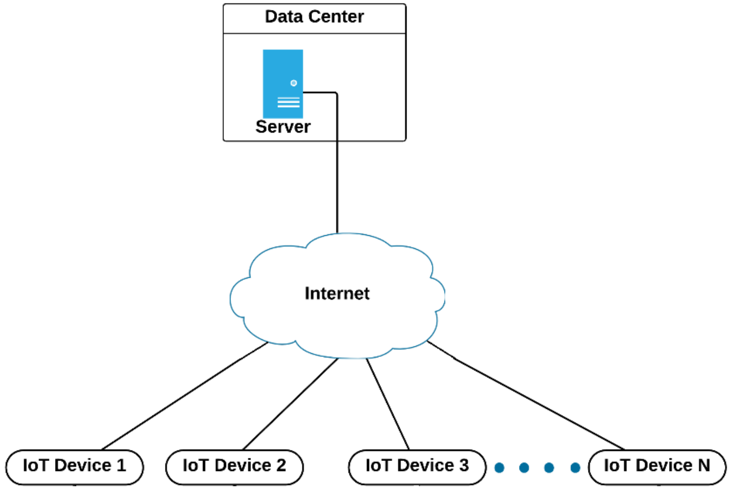
Image: Pedro Sosa

PUF Advantages

- Higher physical security: secrets hidden in complex micro-structure of ICs and not non-volatile memory
- Side channel attacks:
  - Timing attacks: PUFs use CRPs instead of secret keys and accurately measuring the timing delays of a circuit in an IC is significantly more difficult.
  - Power monitoring attacks: designing the PUF such that the number of zeros and ones in the latches is constant
  - Electromagnetic attacks: reduce fluctuations in current
  - Differential fault analysis: physical data corruption inside cryptographic implementations to reveal internal state.

PUF Based Mutual Authentication

- Network model



- PUF Assumptions
  - Not possible to accurately model PUF
  - Pair-wise PUF output-collision probability is zero
  - Physical tampering will modify PUF

PUF Based Mutual Authentication

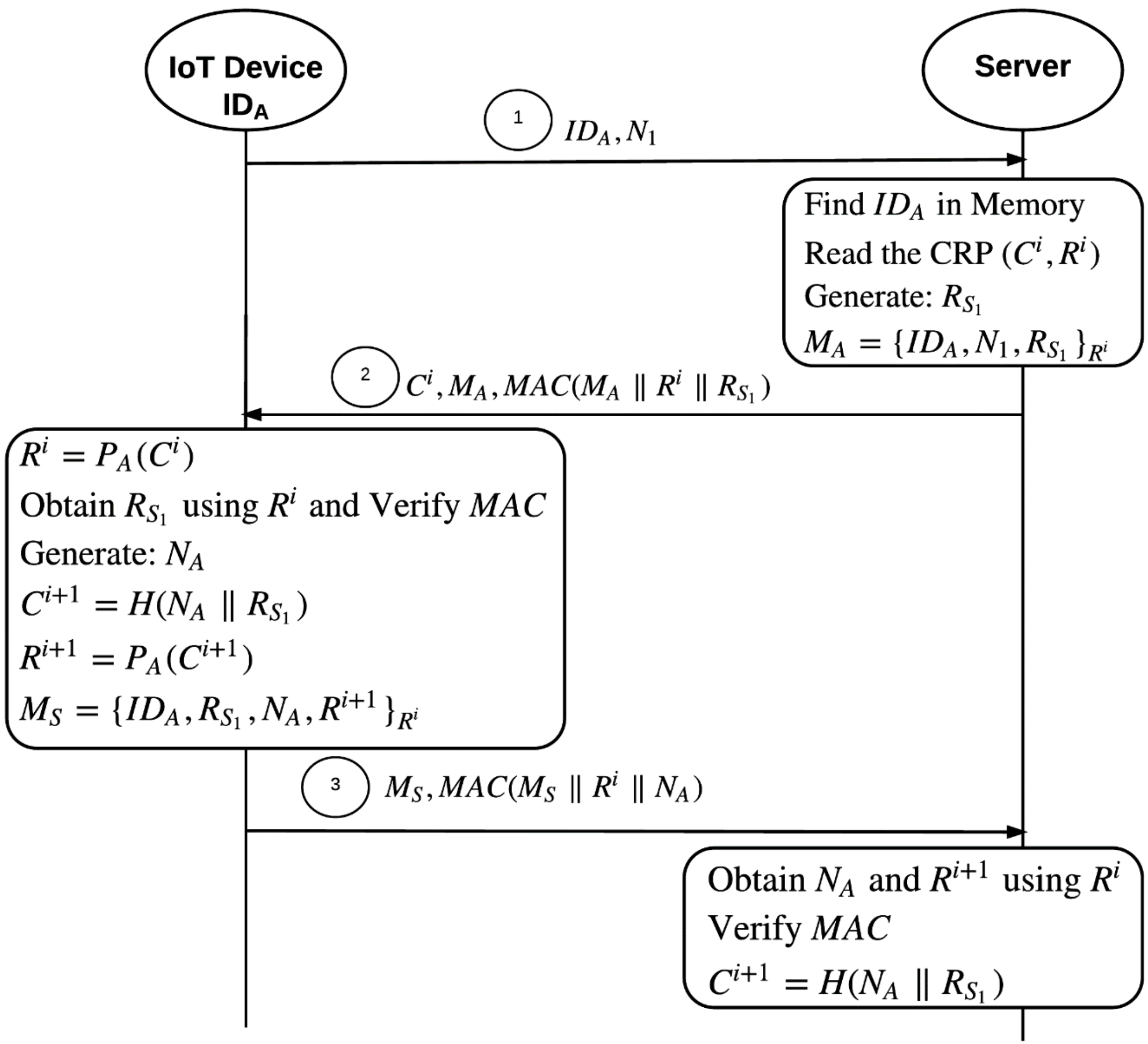
- Assumptions:
  - The PUF and the device's microcontroller are considered to be on the same chip and inseparable.
  - It is not possible to remove the PUF or tamper with the communication between the microcontroller and PUF.
  - IoT devices are constrained by their resources, while the servers in the data center have no such limitation.
  - IoT devices are physically unprotected and accessible by an adversary.
  - An adversary can eavesdrop, modify, inject, and replay messages.

Notation

Notation	Description
ID_i	ID of the IoT device
$\ominus$	XOR operation
$H(X)$	Hash of X
$\|\|$	Concatenation operator
$[Ex]_{Rec}$	Expression Ex is evaluated using the values from the received message
C^i	Challenge for the i'th round
R^i	Response of the respective PUF for C^i

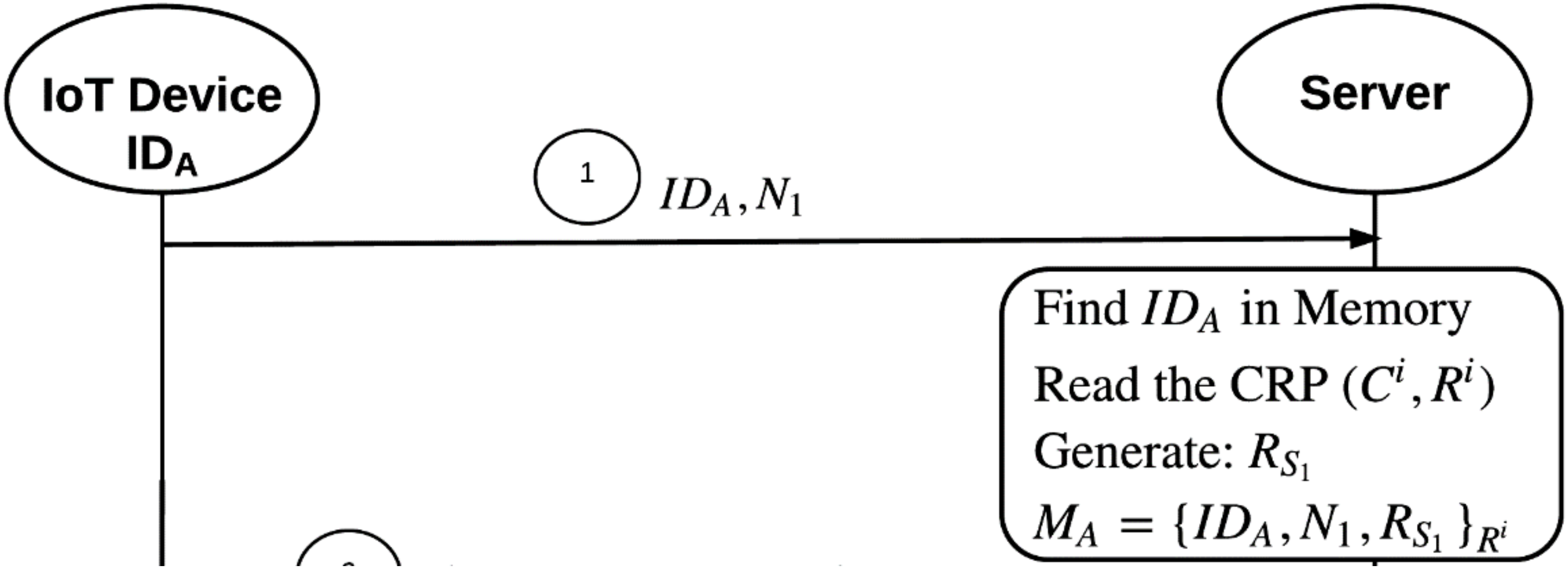
NUS National University of Singapore

Authentication Protocol

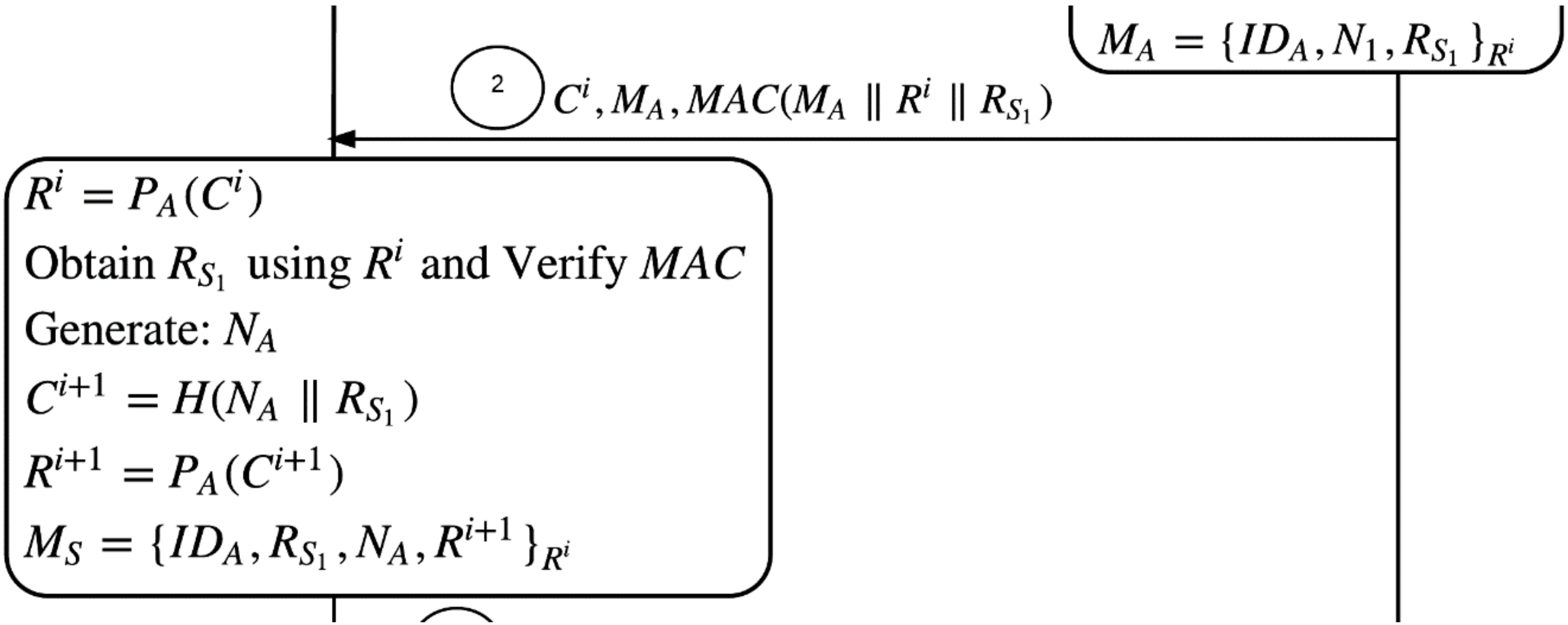


NUS National University of Singapore

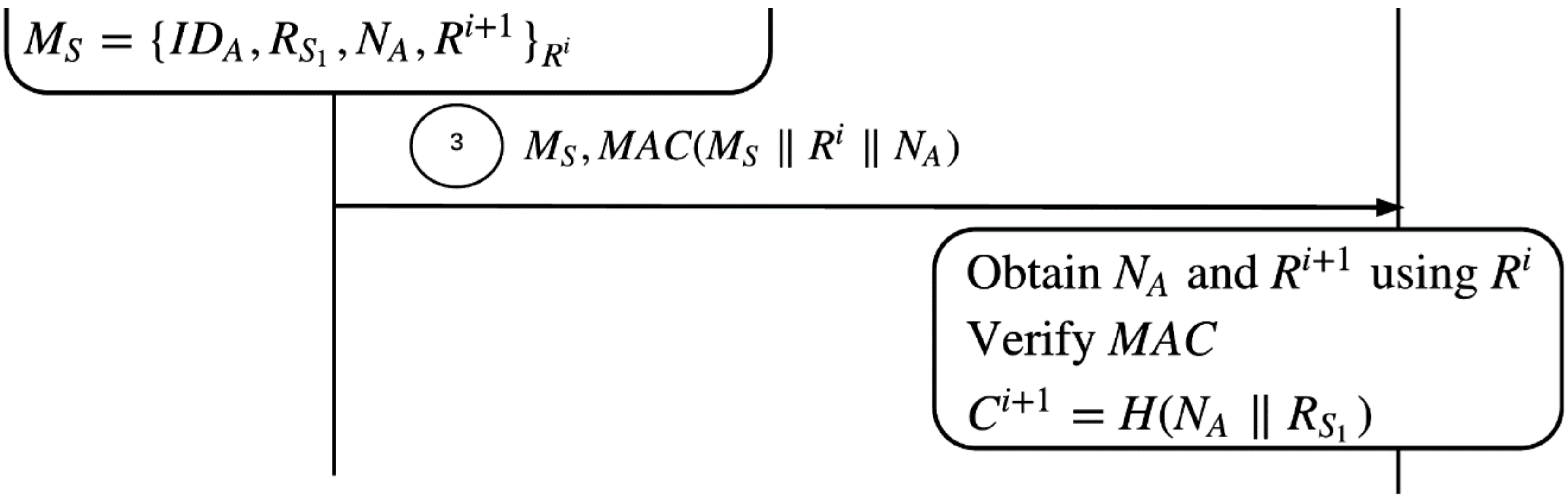
Authentication Protocol: Step 1



Authentication Protocol



Authentication Protocol

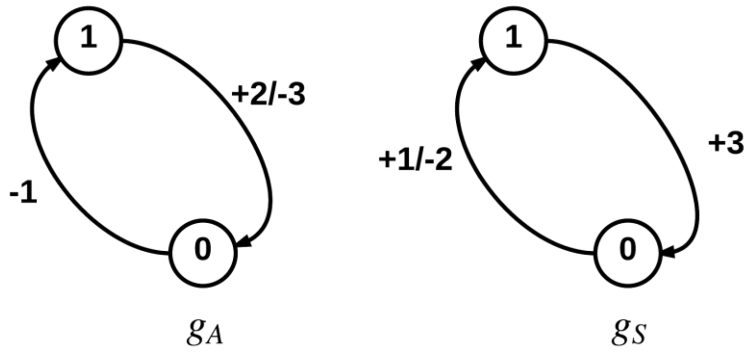


Proof of Correctness

- To prove correctness we need to show that the proposed protocols possess the following properties
  - Completeness: Protocol is able to accept all valid inputs
  - Deadlock Freeness: The protocol does not enter a state such that it stays in that state indefinitely.
  - Livelock or Tempo-blocking freeness: The protocol does not enter into an infinite loop.
  - Termination: When starting from the initial state, the protocol is always able to reach a well-defined final state.
  - No non-executable interactions: The protocol only contains transmission, reception, and interaction paths that are realized under normal operating conditions.

Proof of Correctness

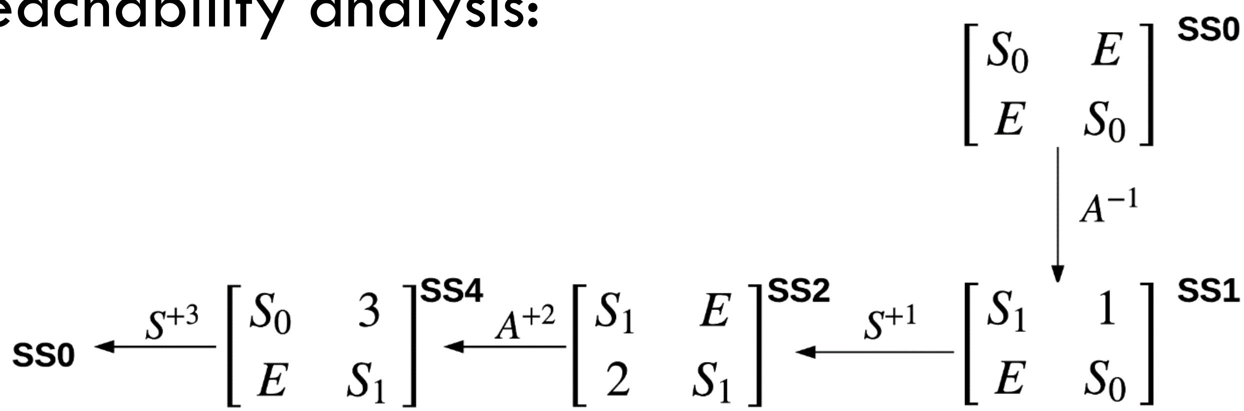
- Finite state machine for protocol entities



- -m (respectively, +m) on the directed arcs represent a transmission (reception) of message m
- +m/-n represents the reception of message m followed by the transmission of message n

Proof of Correctness

- Reachability analysis:



- Potential deadlock state: not an initial or final state and does not have any messages in the channel
- The protocol does not have any potential deadlock states, implying deadlock freeness.

Verification

- The logic has a set of inference rules
- Example: $$\frac{P| \equiv Q \overset{k}{\leftrightarrow} P \wedge P \triangleleft \{X\}_k}{P|\equiv Q|\sim X}$$
  - message-meaning rule (if P believes P and Q share a key, then P ought to believe anything that it receives encrypted with the key comes from Q)

$$\frac{\dfrac{\dfrac{\dfrac{A|\equiv \#(N_1) \wedge \dfrac{A|\equiv A \overset{R^i}{\leftrightarrow} S \wedge A \overset{R^i}{\triangleleft} N_1}{A|\equiv S \overset{R^i}{|\sim} N_1}}{A|\equiv S|\equiv A \overset{R^i}{\leftrightarrow} S} \wedge A|\equiv S|\equiv \{S\}^c \triangleleft|| R_{S_1} \wedge \dfrac{A|\equiv A \overset{R^i}{\leftrightarrow} S \wedge A \overset{R^i}{\triangleleft} R_{S_1}}{A|\equiv S \overset{R^i}{|\sim} R_{S_1}}}{A|\equiv S|\equiv \{A,S\}^c \triangleleft|| R_{S_1}} \wedge A|\equiv sup(S)}{A|\equiv \{A,S\}^c \triangleleft|| R_{S_1}} \wedge A|\equiv sup(S) \wedge \dfrac{A|\equiv \#(N_1) \wedge \dfrac{A \overset{R^i}{\triangleleft} N_1 \ \mathbf{R}\ R_{S_1}}{A \triangleleft N_1 \ \mathbf{R}\ R_{S_1}}}{A|\equiv \#(R_{S_1})}}{A|\equiv A \overset{R_{S_1}}{\leftrightarrow} S}$$

Proof of “A believes ~~R_{S1}~~ (N_A) is a good shared key of A and S”.

Verification

$$\frac{\dfrac{S \mid\equiv A \overset{R^i}{\leftrightarrow} S \wedge S \mid\equiv S^c \lhd\| R_{S_1} \wedge S \overset{R^i}{\mid\sim} R_{S_1}}{S \mid\equiv \{A, S\}^c \lhd\| R_{S_1}} \wedge A \mid\equiv \#(R_{S_1})}{S \mid\equiv A \overset{R_{S1}}{\leftrightarrow} S}$$

Proof of “S believes R_{S1} is a good shared key of A and S”.

$$\frac{\dfrac{A \mid\equiv A \overset{R^i}{\leftrightarrow} S \wedge A \mid\equiv S^c \lhd\| N_A \wedge A \overset{R^i}{\mid\sim} N_A}{A \mid\equiv \{A, S\}^c \lhd\| N_A} \wedge A \mid\equiv \#(N_A)}{A \mid\equiv A \overset{N_A}{\leftrightarrow} S}$$

Proof of “A believes ~~N_A~~ N_B is a good shared key of A and S”.

Verification

$$\dfrac{\dfrac{S \models \#(R_{S_1}) \wedge \dfrac{S \models A \overset{R^i}{\leftrightarrow} S \wedge S \overset{R^i}{\triangleleft} R_{S_1}}{S \models A \overset{R^i}{\mid\!\sim} R_{S_1}}}{S \models A \models A \overset{R^i}{\leftrightarrow} S} \wedge S \models A \models \{S\}^c \triangleleft\| N_A \wedge \dfrac{S \models A \overset{R^i}{\leftrightarrow} S \wedge S \overset{R^i}{\triangleleft} N_A}{S \models A \overset{R^i}{\mid\!\sim} N_A}}{S \models \{A,S\}^c \triangleleft\| N_A} \wedge \dfrac{S \models \#(R_{S_1}) \wedge \dfrac{A \overset{R^i}{\triangleleft} R_{S_1} \ \mathbf{R}\ N_A}{S \triangleleft R_{S_1} \ \mathbf{R}\ N_A}}{S \models \#(N_A)}$$

$$\overline{\qquad S \models A \overset{N_A}{\leftrightarrow} S \qquad}$$

Proof of “S believes N_A is a good shared key of A and S”.

$$\dfrac{\dfrac{A \models A \overset{R^i}{\leftrightarrow} S \wedge A \models S^c \triangleleft\| R^{i+1} \wedge A \overset{R^i}{\mid\!\sim} R^{i+1}}{A \models \{A,S\}^c \triangleleft\| R^{i+1}} \wedge A \models \#(R^{i+1})}{A \models A \overset{R^{i+1}}{\leftrightarrow} S}$$

Proof of “A believes R_{i+1} is a good shared key of A and S”

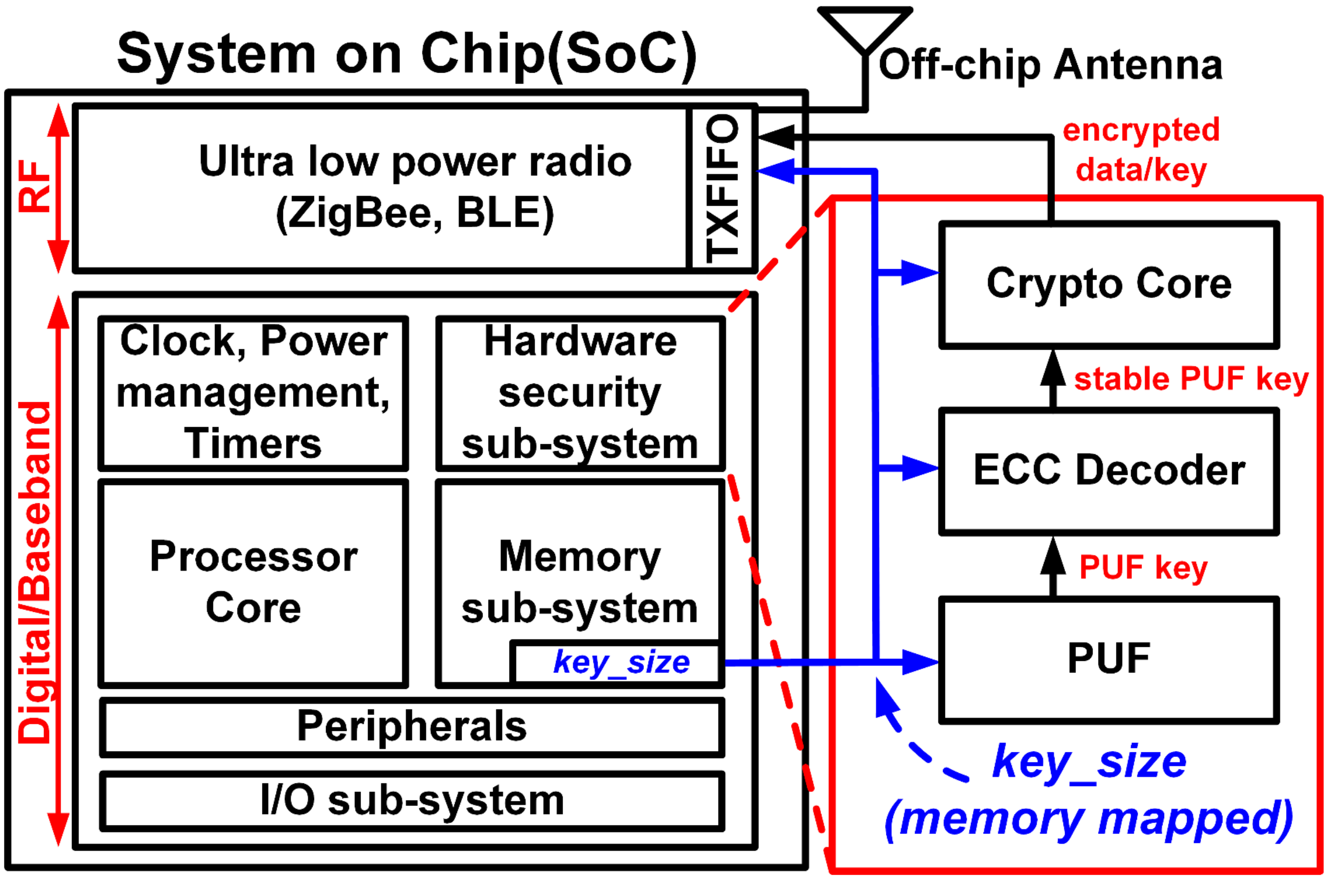
NUS National University of Singapore

Verification

$$
\cfrac{
\cfrac{
\cfrac{
S \mid\equiv \#(R_{S_1}) \wedge \cfrac{S \mid\equiv A \overset{R^i}{\leftrightarrow} S \wedge S \overset{R^i}{\triangleleft} R_{S_1}}{S \mid\equiv A \overset{R^i}{\mid\sim} R_{S_1}}
}{
S \mid\equiv A \mid\equiv A \overset{R^i}{\leftrightarrow} S
}
\wedge S \mid\equiv A \mid\equiv \{S\}^c \triangleleft\| R^{i+1} \wedge
\cfrac{S \mid\equiv A \overset{R^i}{\leftrightarrow} S \wedge S \overset{R^i}{\triangleleft} R^{i+1}}{S \mid\equiv A \overset{R^i}{\mid\sim} R^{i+1}}
}{
S \mid\equiv \{A, S\}^c \triangleleft\| R^{i+1}
}
\wedge
\cfrac{
S \mid\equiv \#(R_{S_1}) \wedge \cfrac{A \overset{R^i}{\triangleleft} R_{S_1} \ \mathbf{R}\ R^{i+1}}{S \triangleleft R_{S_1} \ \mathbf{R}\ R^{i+1}}
}{
S \mid\equiv \#(R^{i+1})
}
}{
S \mid\equiv A \overset{R^{i+1}}{\leftrightarrow} S
}
$$

Proof of “S believes R_{i+1} is a good shared key of A and S”

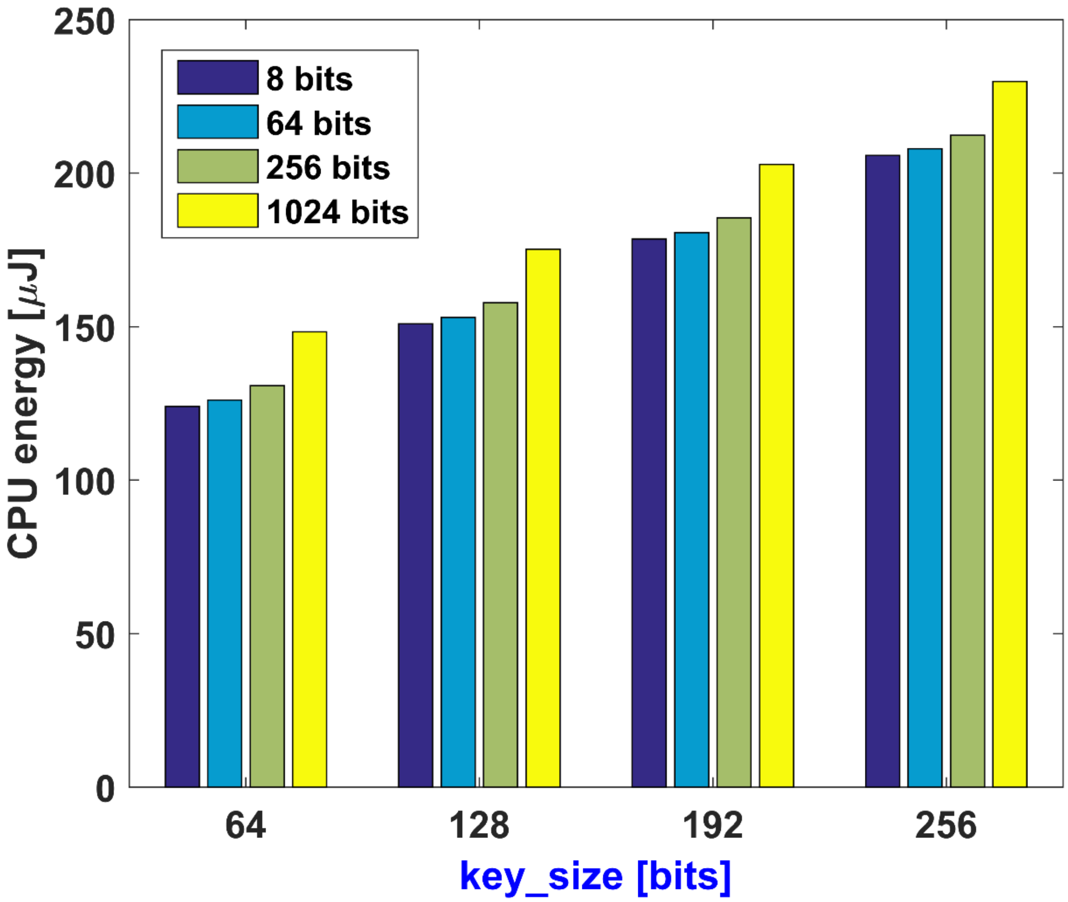
Implementation



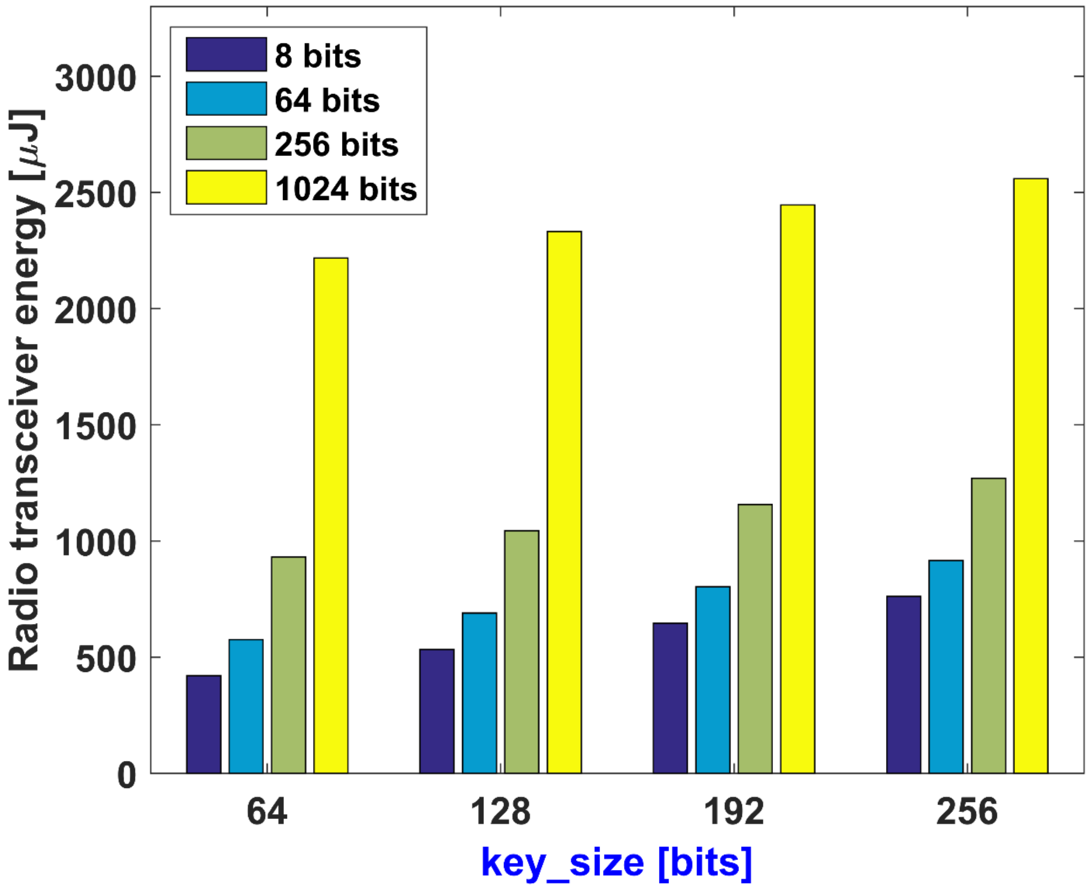
Energy Cost of Building Blocks

Sub-component	Domain	Energy	Example
PUF	Baseband (digital)	10 - 200 fJ/bit	PUF [14], [15]
ECC	Baseband (digital)	20 - 60 pJ/bit	BCH [27], [28]
Crypto	Baseband (digital)	1 - 30 pJ/bit	AES [24] - [26]
Wireless	Radio Frequency (RF)	2-10 nJ/bit	BLE [1]

Energy Consumption

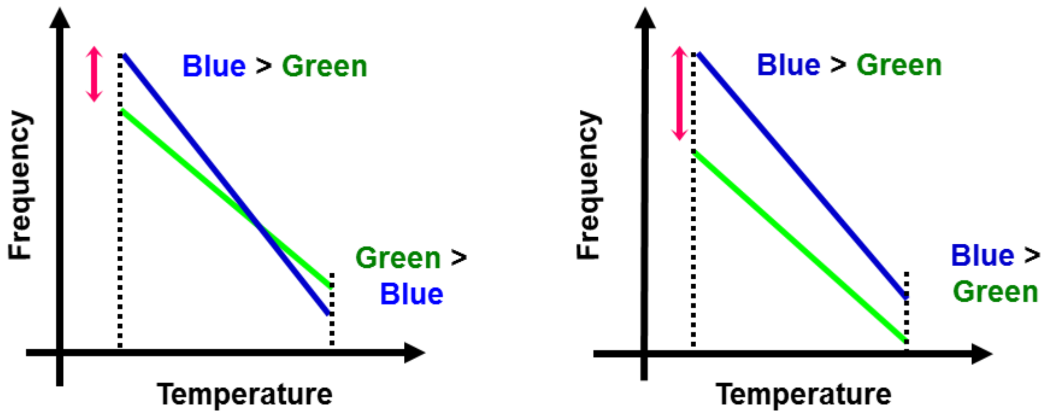


Energy Consumption



PUF Issues

- PUF output bit may "flip" when environmental conditions change (e.g. ring oscillator PUF [Tri07])



- Machine learning attacks on PUFs

Conclusions

- IoT presents a number of security challenges
- Coordinated efforts are required at all layers and by all stakeholders
- There are many promising solutions: PUFs

Thank You