The Role of Energy in the Lightweight Cryptographic Profile

Patrick Schaumont, Conor Patrick

Secure Embedded Systems
Virginia Tech

Current view on Profile

Physical characteristics	Performance characteristics	Security characteristics
Area (in GE)	Latency (in clock cycles)	Minimum security strength (bits)
Memory (RAM/ROM)	Throughput (cycles per byte)	Attack models
Implementation type (hardware, software, or both)	Power (μW)	Side channel resistance requirements

Reflects resource cost

Reflects performance and energy cost

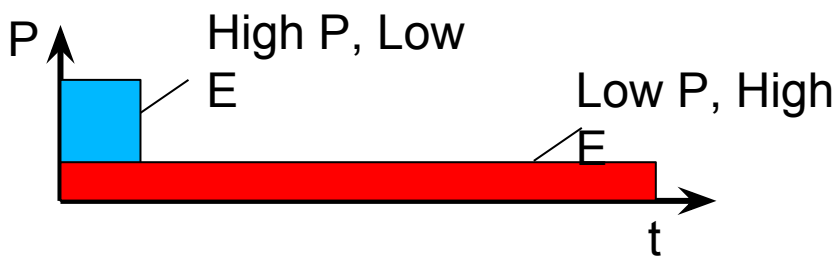
Reflects security

There is a characteristic for power, but what about *energy*?

Energy and Power

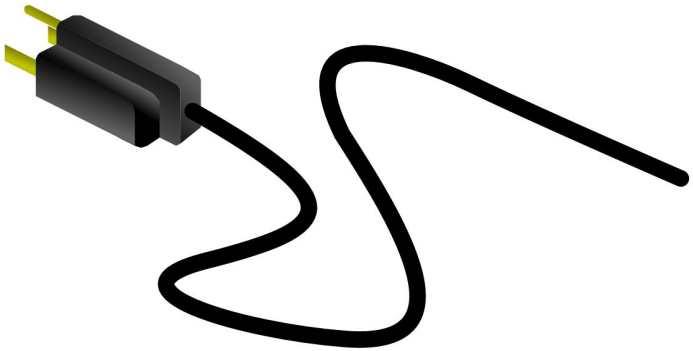
- **Energy equals work (J)**
  - **In crypto = the number of crypto operations**
- **Power equals work per unit of time (J/s)**
  - **In crypto = the number of crypto operations / second**

- **Low power is not the same as low energy**
  - **Energy = Power x Time**

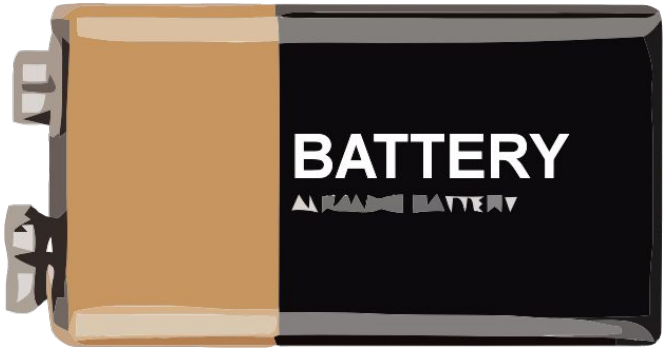


Transitioning to Lightweight

Typical Cryptosystems

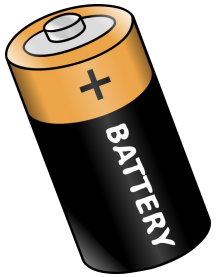


Lightweight Cryptosystems



Continuous Power vs. Limited Power

Design under the current scheme

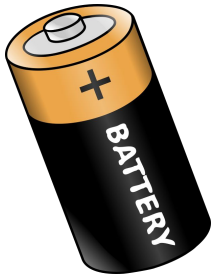


Suppose a system that uses:

- **1 Ahr battery**
- **AES consuming 1 mA of current.**

How long does it last?

Design under the current scheme



Suppose a system that uses:

- **1 Ahr battery**
- **AES consuming 1 mA of current.**

How long does it last?

1000 hours/42 days? Maybe.

Still need to know:

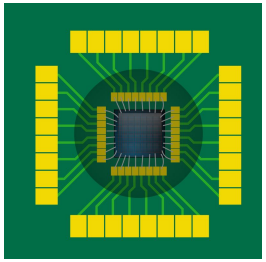
- **How much ciphertext do we process per Joule?**
- **How much ciphertext do we need per day?**

How to answer these questions

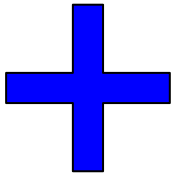
- **Joules per byte?**
- **Bytes per day?**

- Atomic energy cost of a operation
  - Example: Encrypting 1 block costs 12 nano-Joules
  - More precise
  - Energy is a resource

X bytes of memory



Y gates



Z Joules

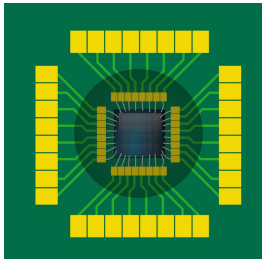
How to answer these questions

- **Joules per byte?**
- **Bytes per day?**

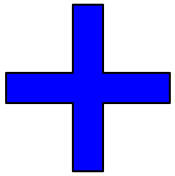
Power / Throughput -- only reflects average case

- Atomic energy cost of a operation
  - Example: Encrypting 1 block costs 12 nano-Joules
  - More precise
  - Energy is a resource

X bytes of memory



Y gates

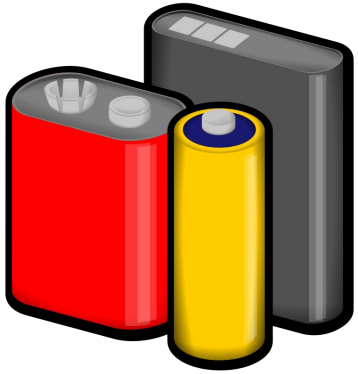


Z Joules

Energy harvesting consideration

Conventional battery

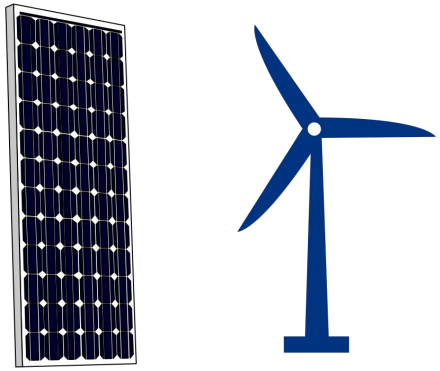
(finite **J**, large J/s)



Cheap
High density
Limited
Servicing cost

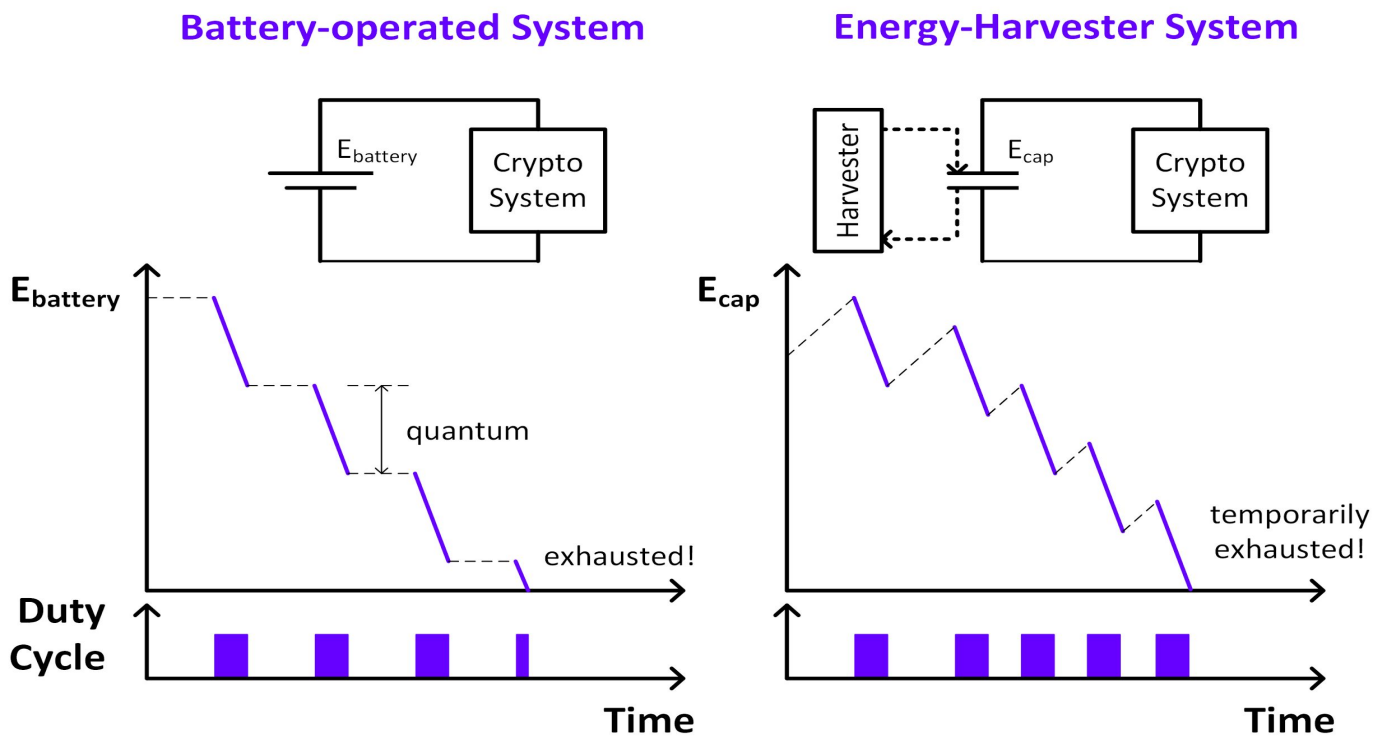
Energy Harvester

(infinite J, finite **J/s**)



Complex
Low supply
Unlimited
Infinite lifetime

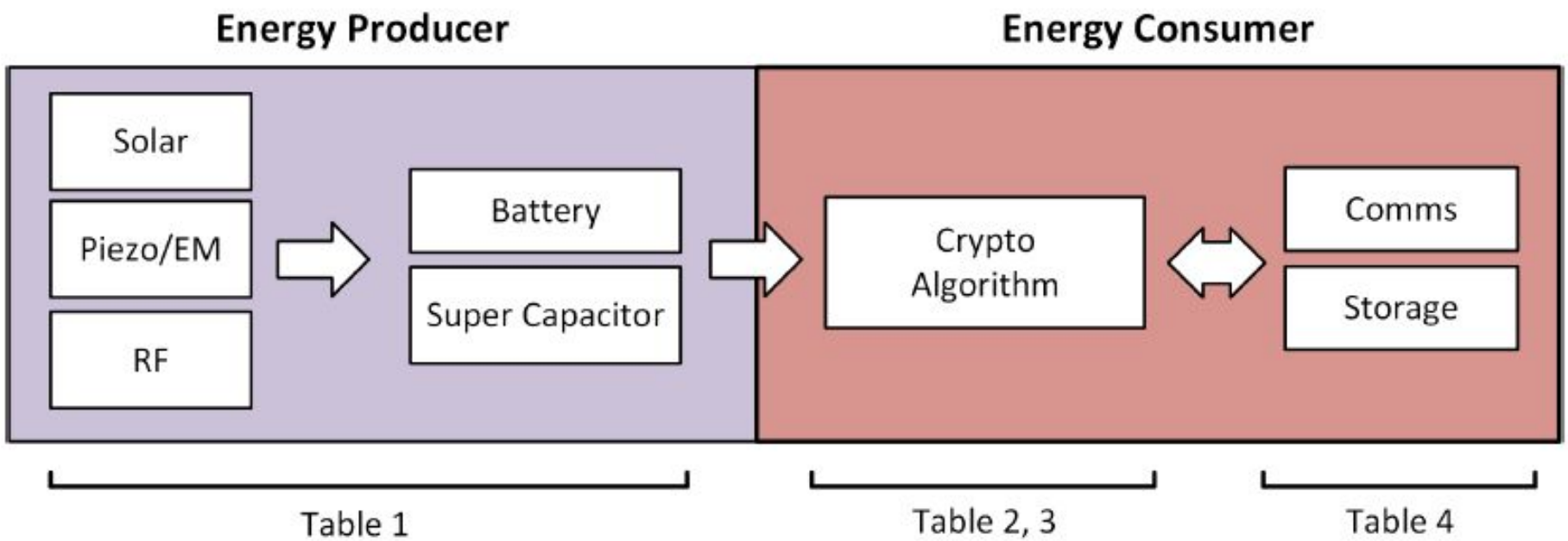
Energy Harvesting vs Battery Operation



- **Under acceptable duty cycle of operation, energy-harvester systems have a *perpetual* lifetime**

'acceptable' means $E_{harvested} > E_{consumed}$

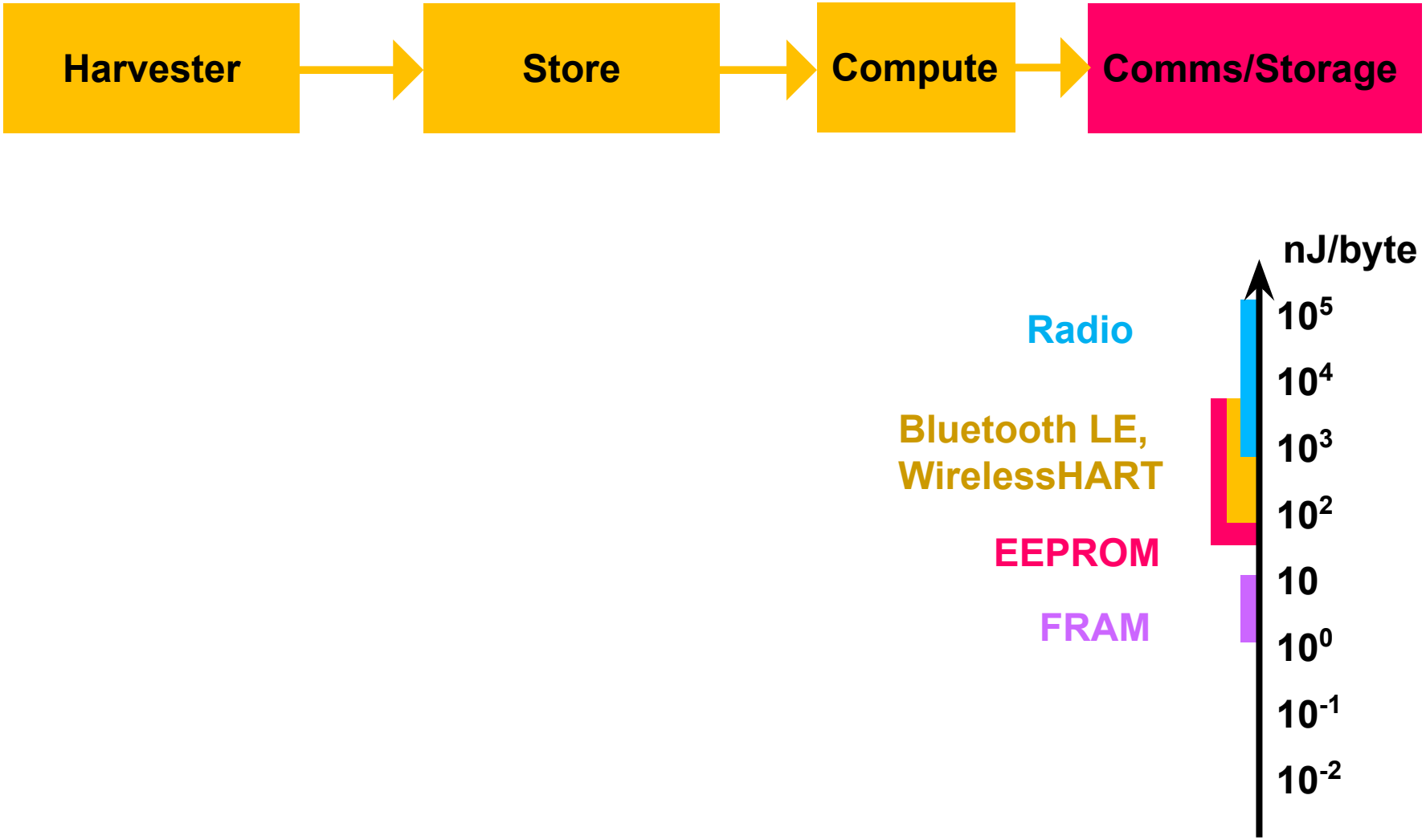
The energy balance



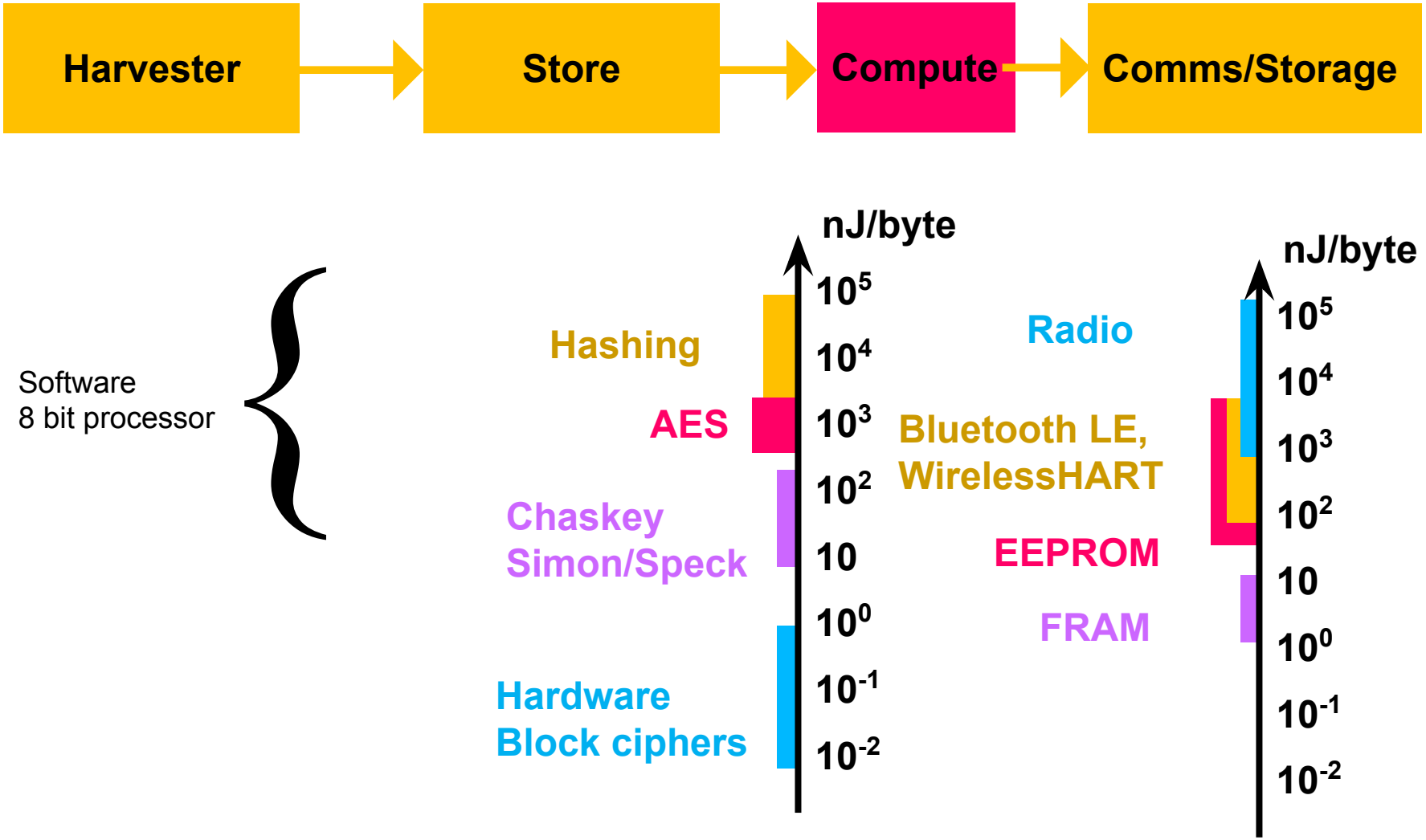
- *Energy Store B (J)*
- *and/ or Energy Influx b (J/s)*

- *Energy Quanta q (J)*
- *Duty cycle d (1/s)*

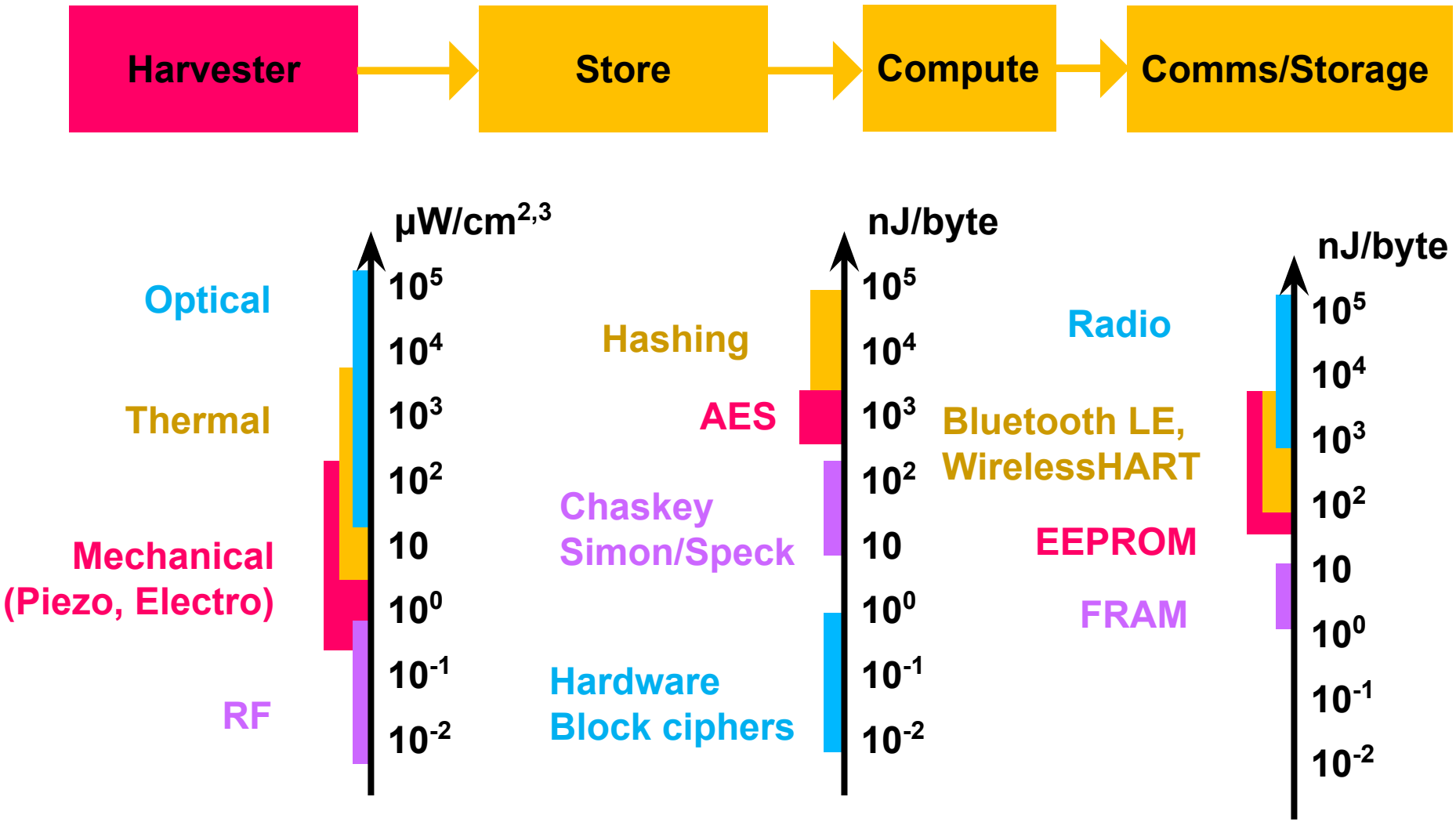
Energy Harvester Based Design



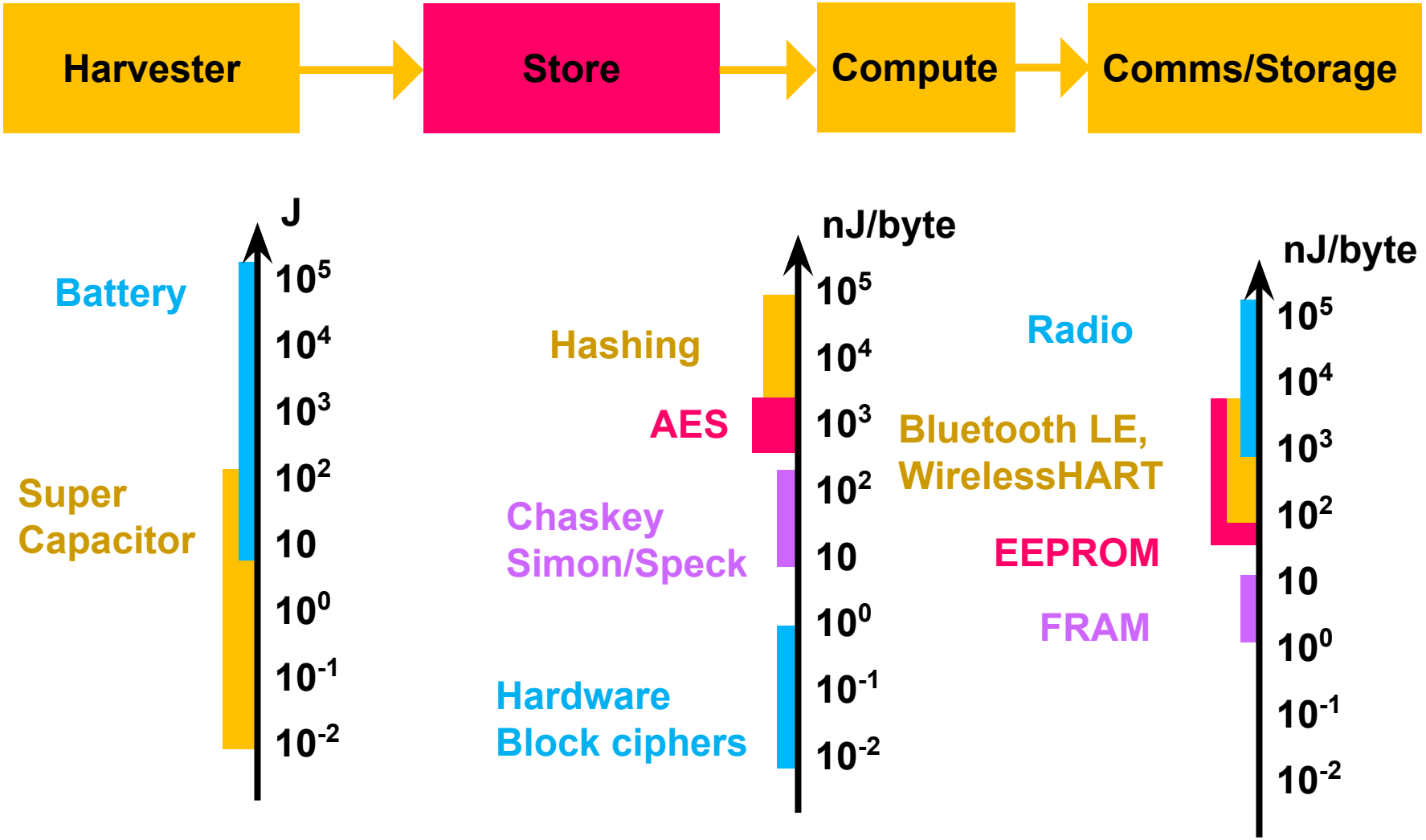
Energy Harvester Based Design



Energy Harvester Based Design



Energy Harvester Based Design



Energy Harvester Based Design

Harvester → Store → Compute + Comms

μW/cm²

Optical

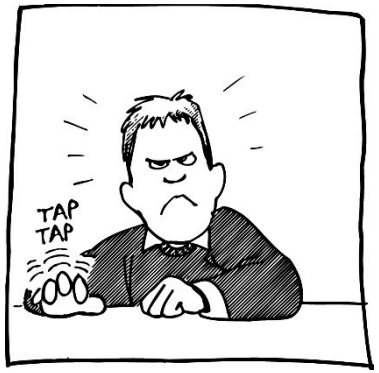
Thermal

Mechanical (Piezo, Electro)

RF

10^5
10^4
10^3
10^2
10
10^0
10^{-1}
10^{-2}

1 block = 20 uJ
=
1 μW x 20 sec



nJ/byte

Hashing

AES

Chaskey, Simon/Speck

Hardware Block ciphers

10^5
10^4
10^3
10^2
10
10^0
10^{-1}
10^{-2}

Based on data from TI, Penella-Lopez, Mitcheson

Energy Harvester Based Design

Harvester → **Store** → **Compute + Comms**

	$\mu W/cm^2$
Optical	10^5
	10^4
Thermal	10^3
	10^2
Mechanical (Piezo, Electro)	10
	10^0
	10^{-1}
RF	10^{-2}

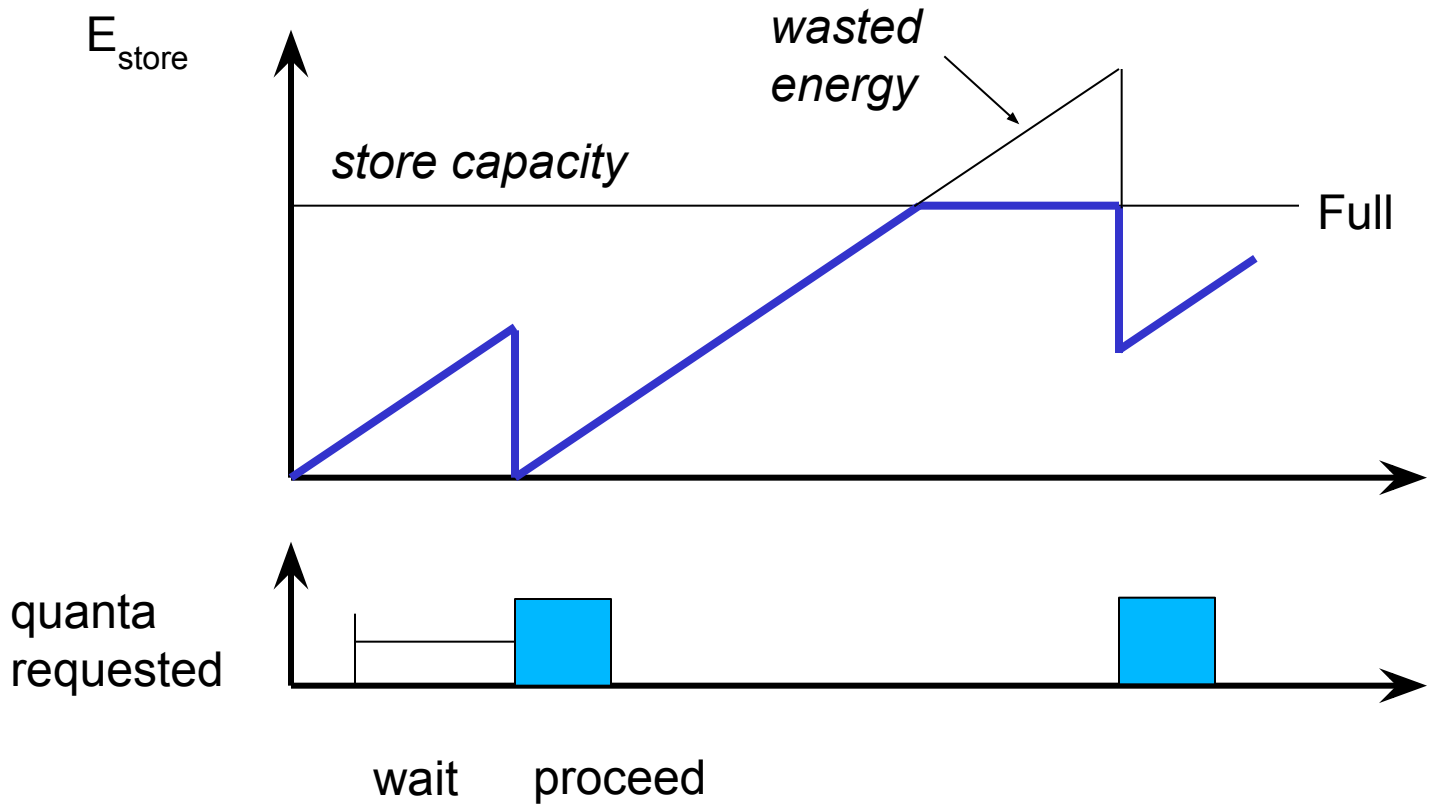
1 block = 20 uJ
=
4320 blocks / day

	nJ/byte
	10^5
Hashing	10^4
AES	10^3
	10^2
Chaskey, Simon/Speck	10
	10^0
Hardware Block ciphers	10^{-1}
	10^{-2}

Based on data from TI, Penella-Lopez, Mitcheson

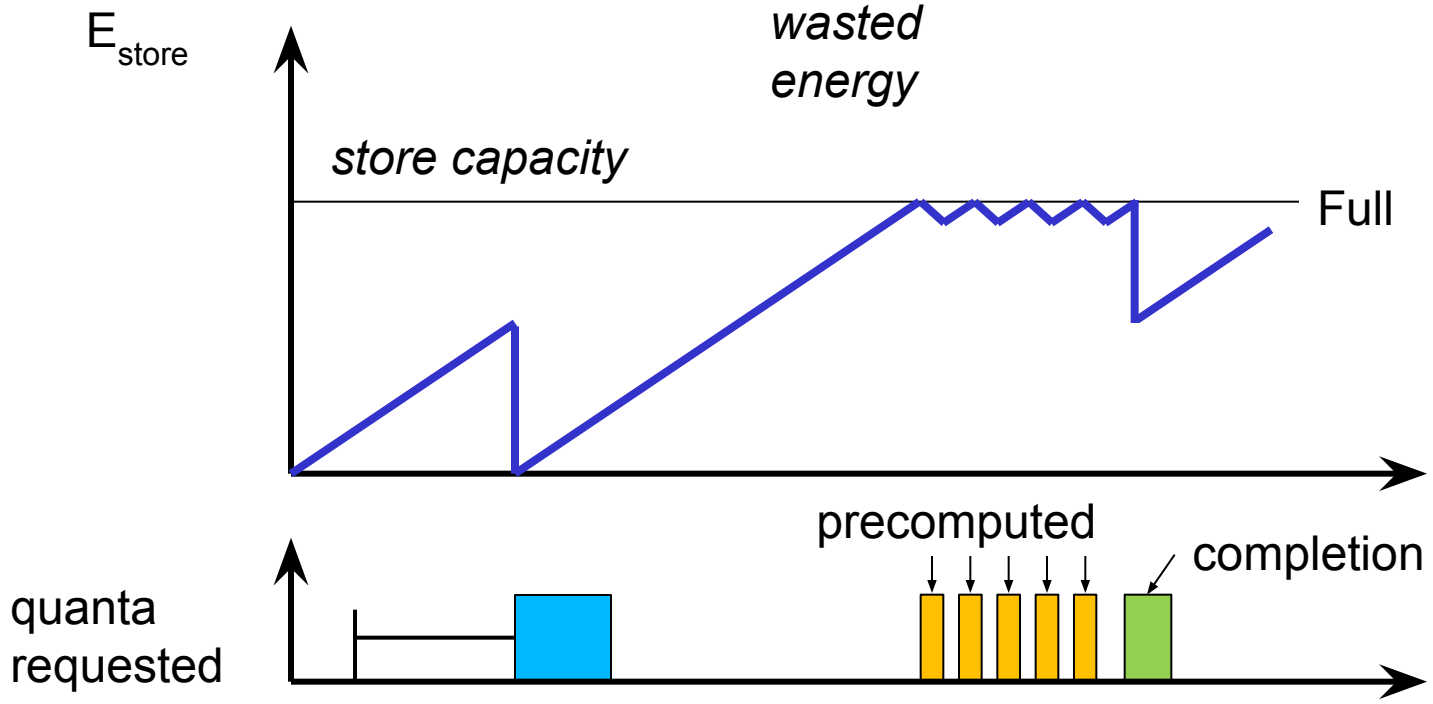
Energy Harvester Based Design

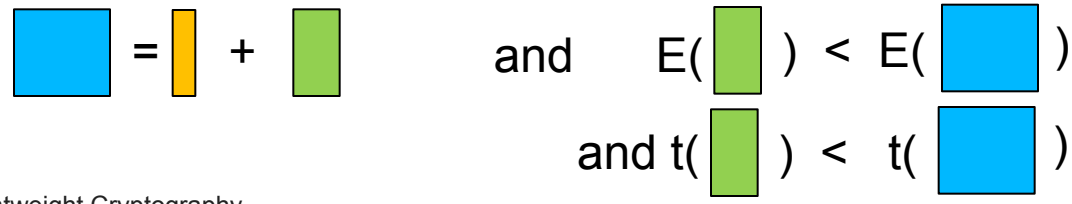
Traditional design - atomic algorithm execution



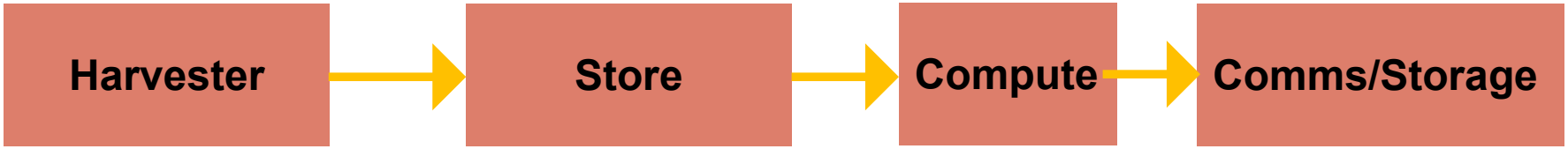
Energy Harvester Based Design

Improved design - precomputed execution

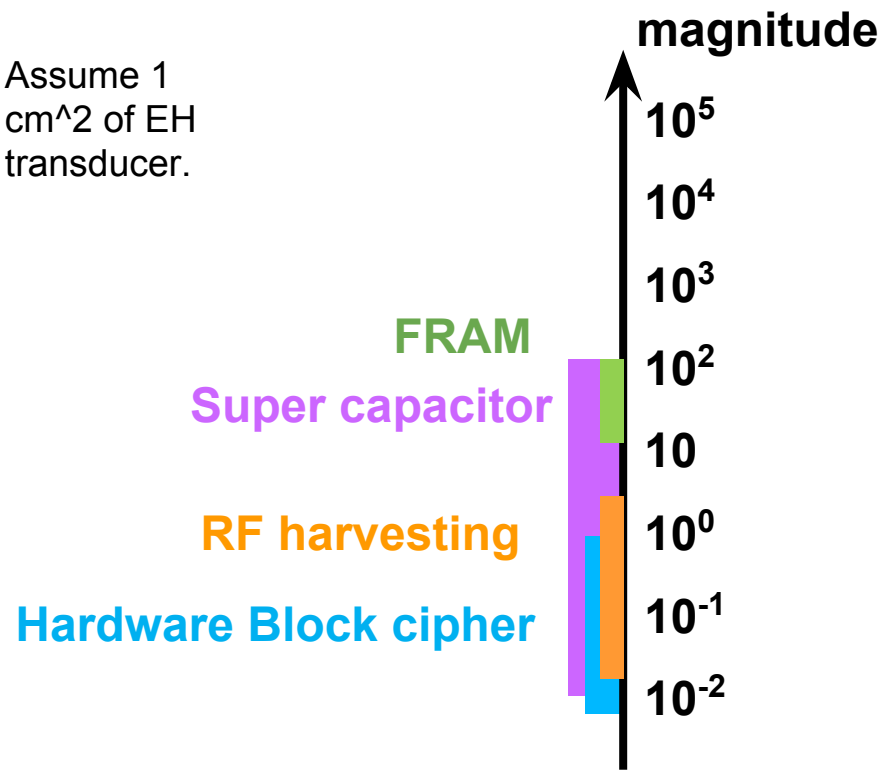




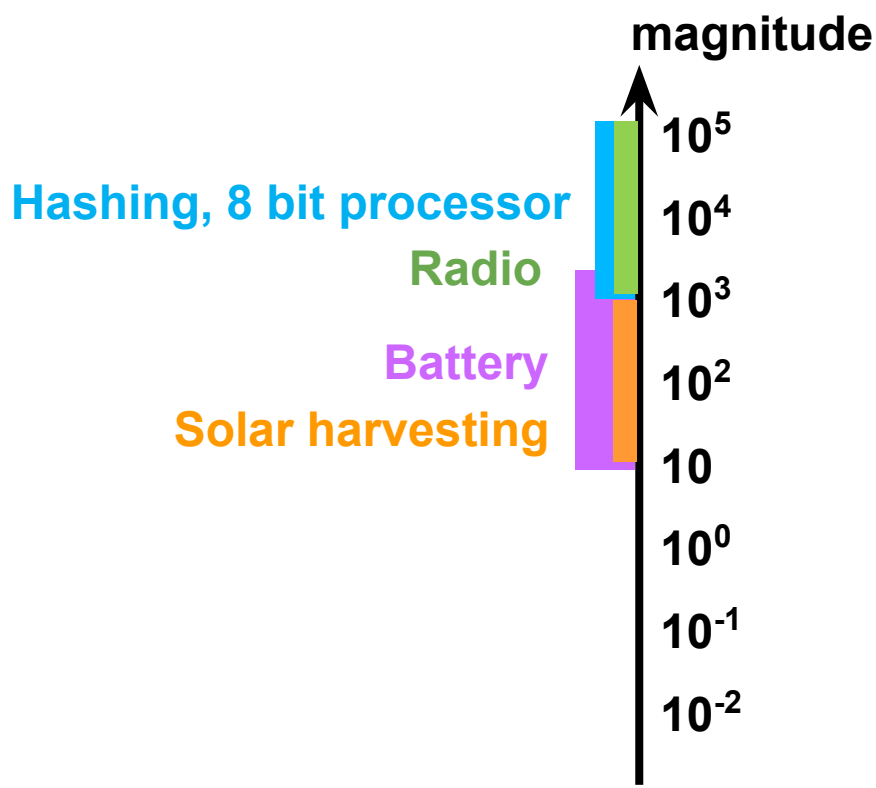
Putting it all together



Assume 1 cm^2 of EH transducer.



Potential of **1.5 MB** per day



Potential of **1.5 MB** per day

We need better energy metrics

- **Joules per byte (J/byte)**
- **Hard to compare HW implementations**
  - **Different hardware implements of same cipher will vary in magnitudes for J/byte.**

- **Relativeness of cipher J/byte seems to hold.**
- **It would be best for authors to report J/byte relative to another cipher on same platform.**

What we did

- **Approximate:**
  - **Energy = K * (Power * throughput / block-size)**

- **K = technology constant, units: CV^2/2 J/gate)**

- **Provides results not useful for design, but may work for comparison.**

Conclusion

Physical characteristics	Performance characteristics	Security characteristics
Area (in GE)	Latency (in clock cycles)	Minimum security strength (bits)
Memory (RAM/ROM)	Throughput (cycles per byte)	Attack models
Implementation type (hardware, software, or both) **Energy**	Power (μW)	Side channel resistance requirements

- **Energy harvesting -- new LWC paradigm.**
- **J/byte -- crucial metric for engineers and designers.**
- **Secure LW design involves a lot of balancing.**