Challenges and Opportunities for Energy-Harvested Security

Patrick Schaumont

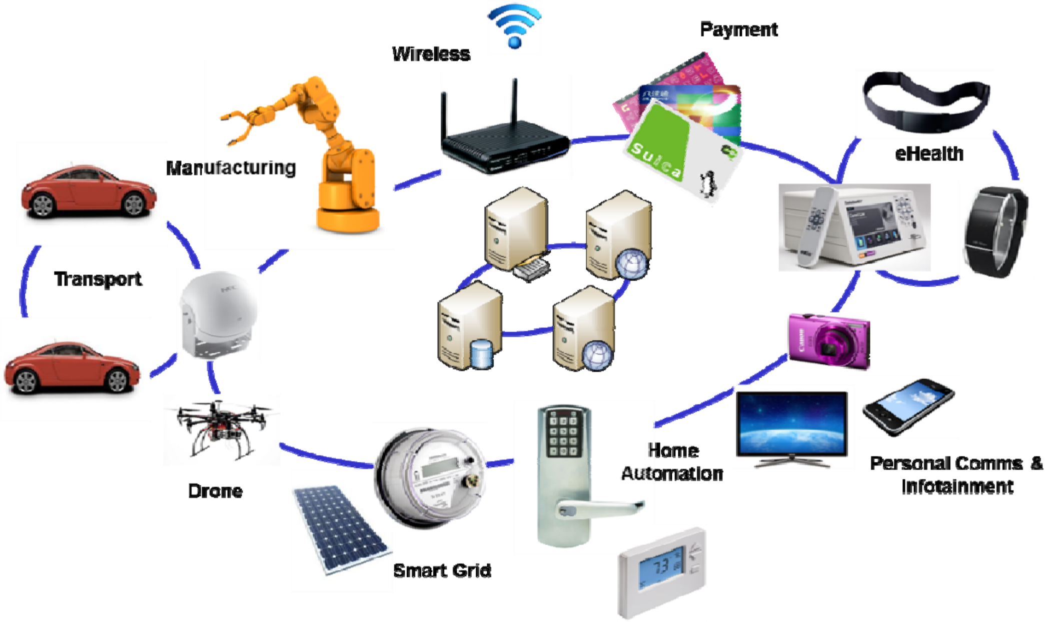
Associate Professor
Bradley Department of ECE
Virginia Tech

Acknowledgements
National Science Foundation
My Students: Aydin Aysu, Deepak Mane, Krishna Pabbuleti, Bilgiday Yuce

IoT, Energy Harvesting and Security?

The Internet of Things is a matter of

- **.. making it scalable**
- **.. making it low-maintenance**
- **.. event-driven iso human-driven computing**



2 hands
2 ears
2 eyes
1 head

IoT, Energy Harvesting and Security?

The Internet of Things is a matter of

- **.. making it scalable**
- **.. making it low-maintenance**
- **.. event-driven iso human-driven computing**

but security *still* has to come for ‘free’

IoT, Energy Harvesting and Security?

The Internet of Things is a matter of

- **.. making it scalable**
- **.. making it low-maintenance**
- **.. event-driven iso human-driven computing**

but security *still* has to come for ‘free’

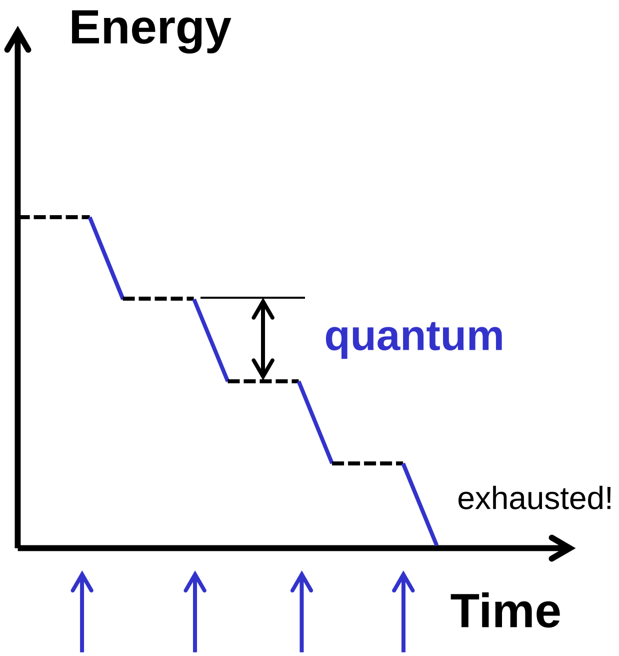
This talk:

Energy harvesting delivers free security (and not only because of the free Joules)

Battery-operated vs Energy-Harvested

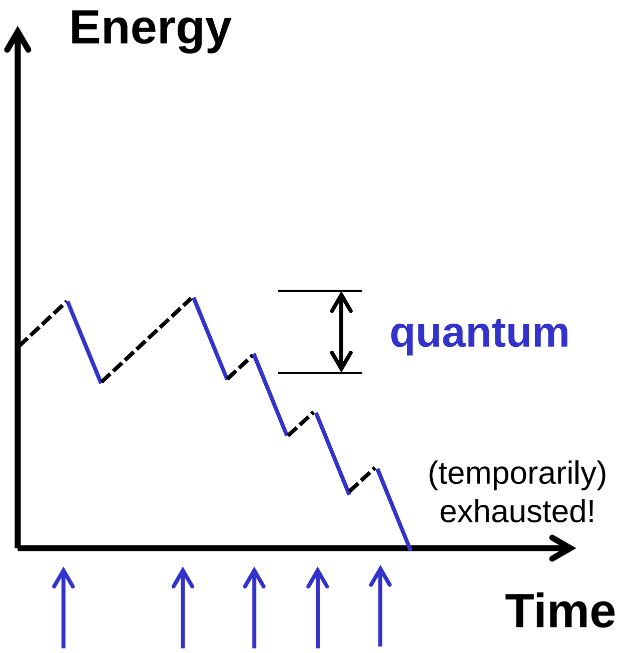
Battery Operation

limited by battery capacity

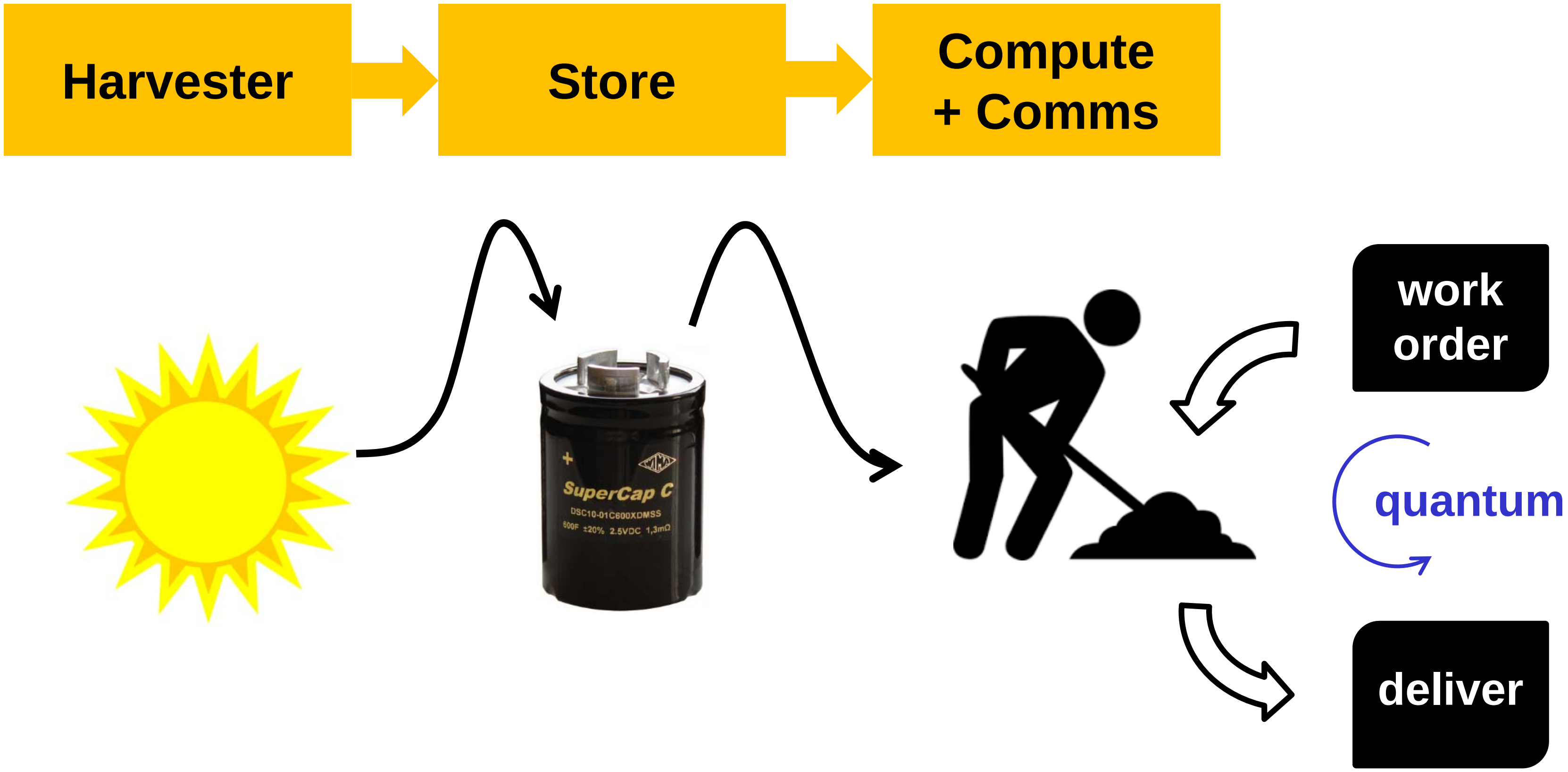


Energy Harvesting

unlimited energy
at a throughput limited
by harvesting process



Energy Harvester Based Design



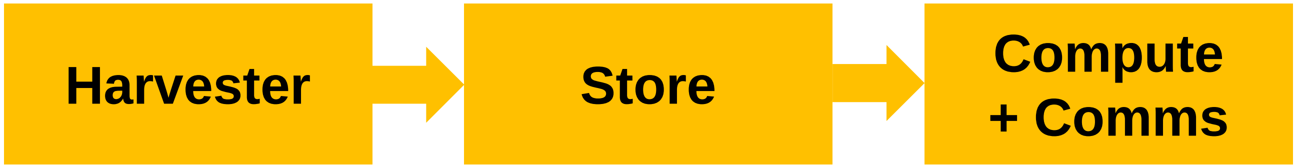
Harvester → Store → Compute + Comms

work order

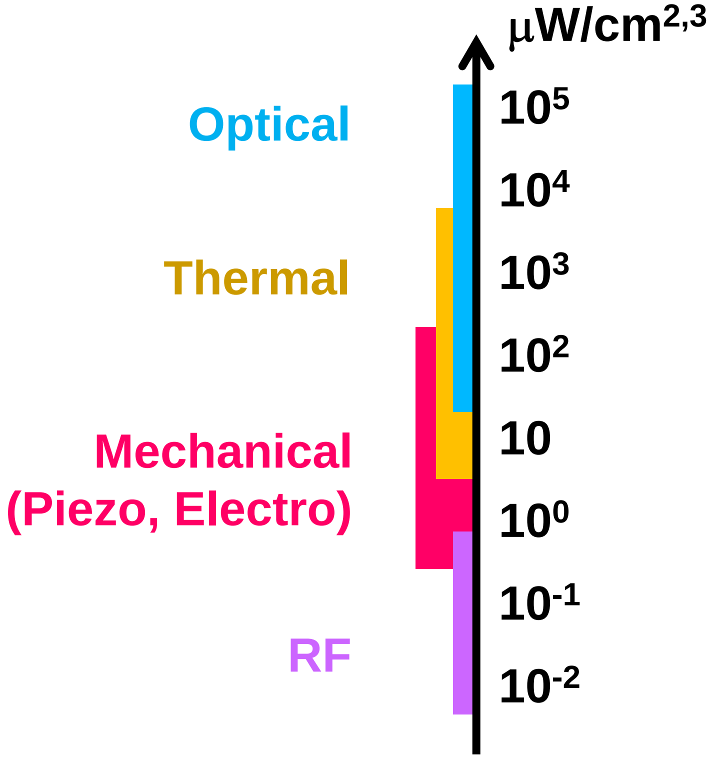
quantum

deliver

Energy Harvester Based Design

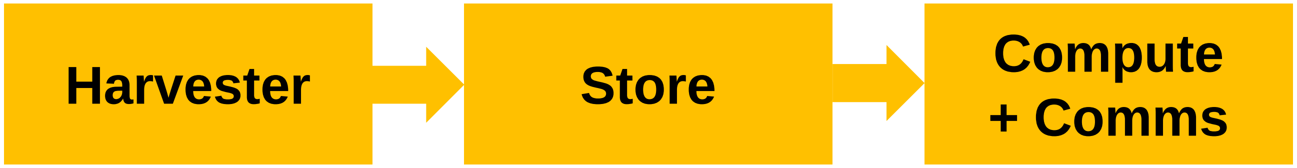


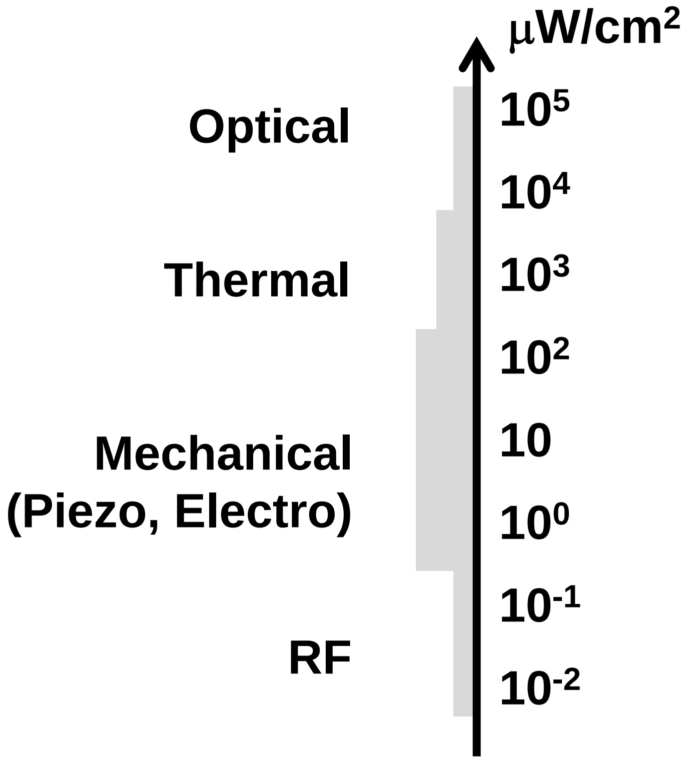
Harvester → Store → Compute + Comms



Based on data from TI, Penella-Lopez, Mitcheson

Energy Harvester Based Design



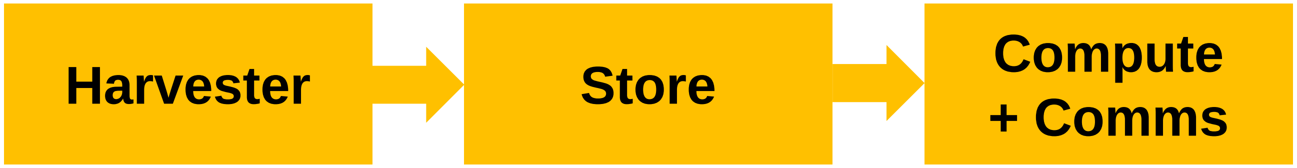


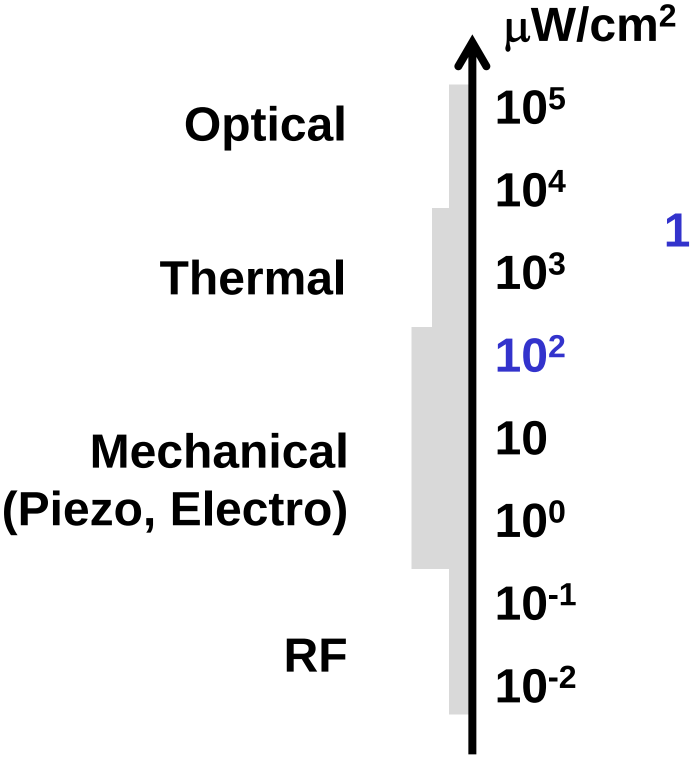
Based on data from TI, Penella-Lopez, Mitcheson

283 mJ	ECDSA + ECDH on MicaZ
89 mJ	ECMQV on WinS
20 mJ	ECDSA on MSP430 EZRF

Based on data from de Meulenaer, Mane, Grosschadl

Energy Harvester Based Design

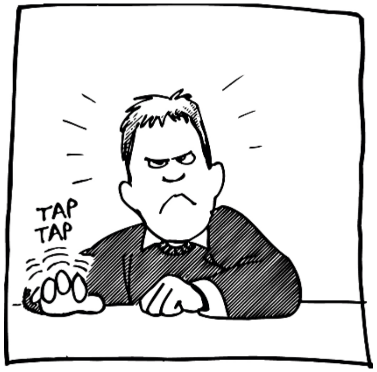




20 mJ

=

100 μW x 200 sec

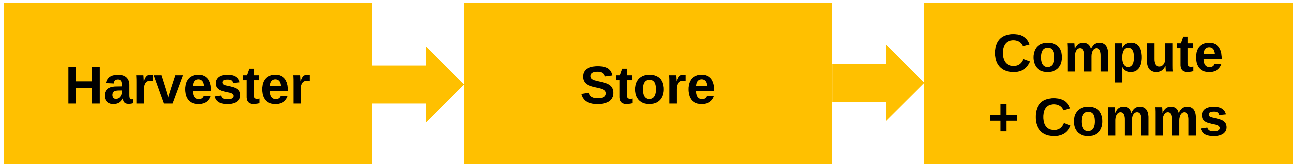


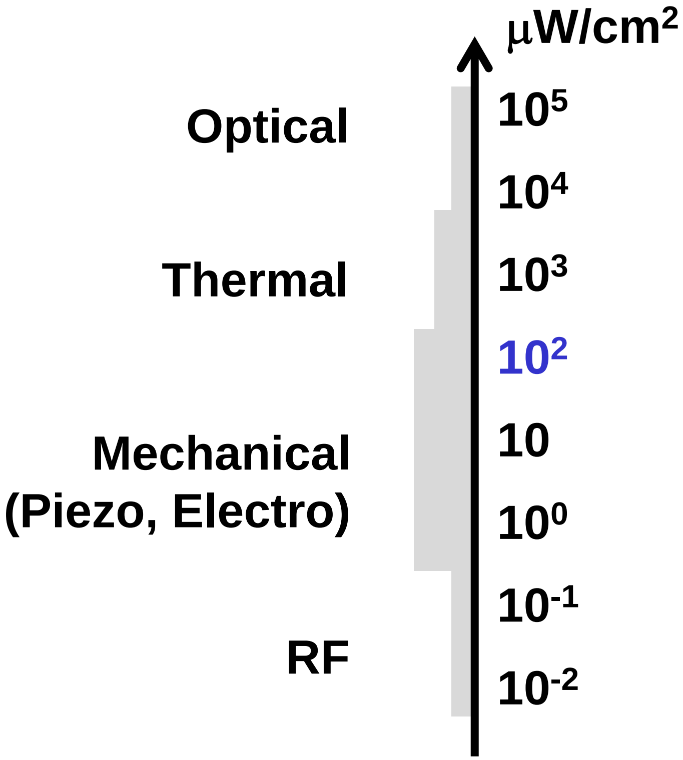
283 mJ	ECDSA + ECDH on MicaZ
89 mJ	ECMQV on WinS
20 mJ	ECDSA on MSP430 EZRF

Based on data from TI, Penella-Lopez, Mitcheson

Based on data from de Meulenaer, Mane, Grosschadl

Energy Harvester Based Design





100 μW x 1 day
=
432 ECDSA
@ 20 mJ

283 mJ	ECDSA + ECDH on MicaZ
89 mJ	ECMQV on WinS
20 mJ	ECDSA on MSP430 EZRF

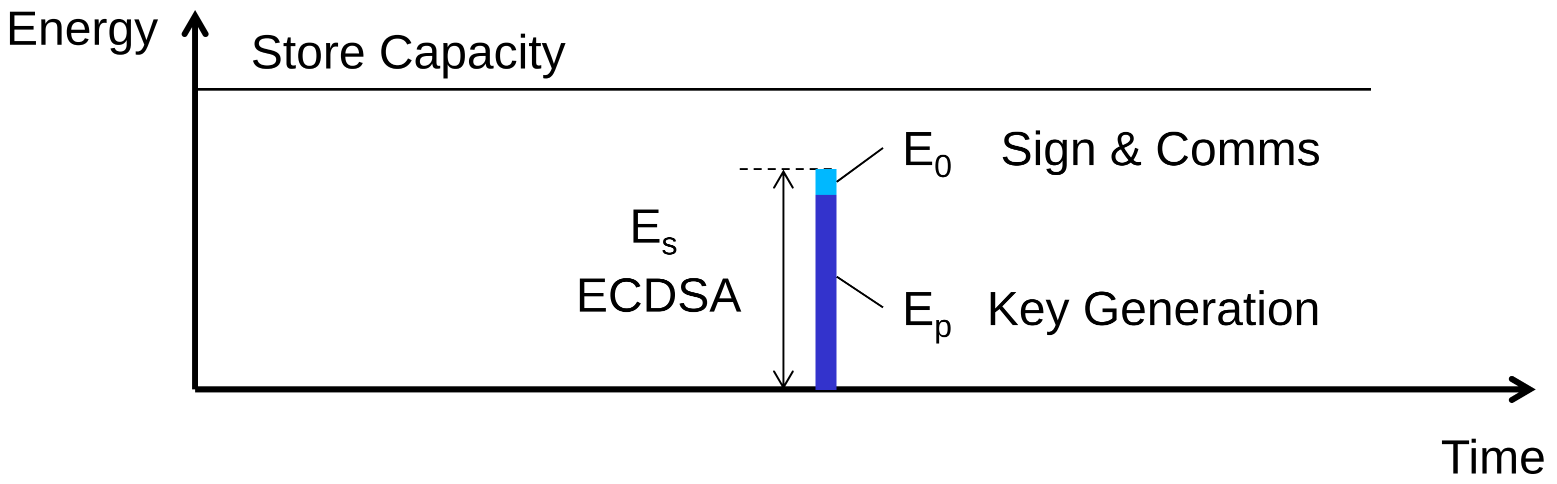
Based on data from TI, Penella-Lopez, Mitcheson

Based on data from de Meulenaer, Mane, Grosschadl

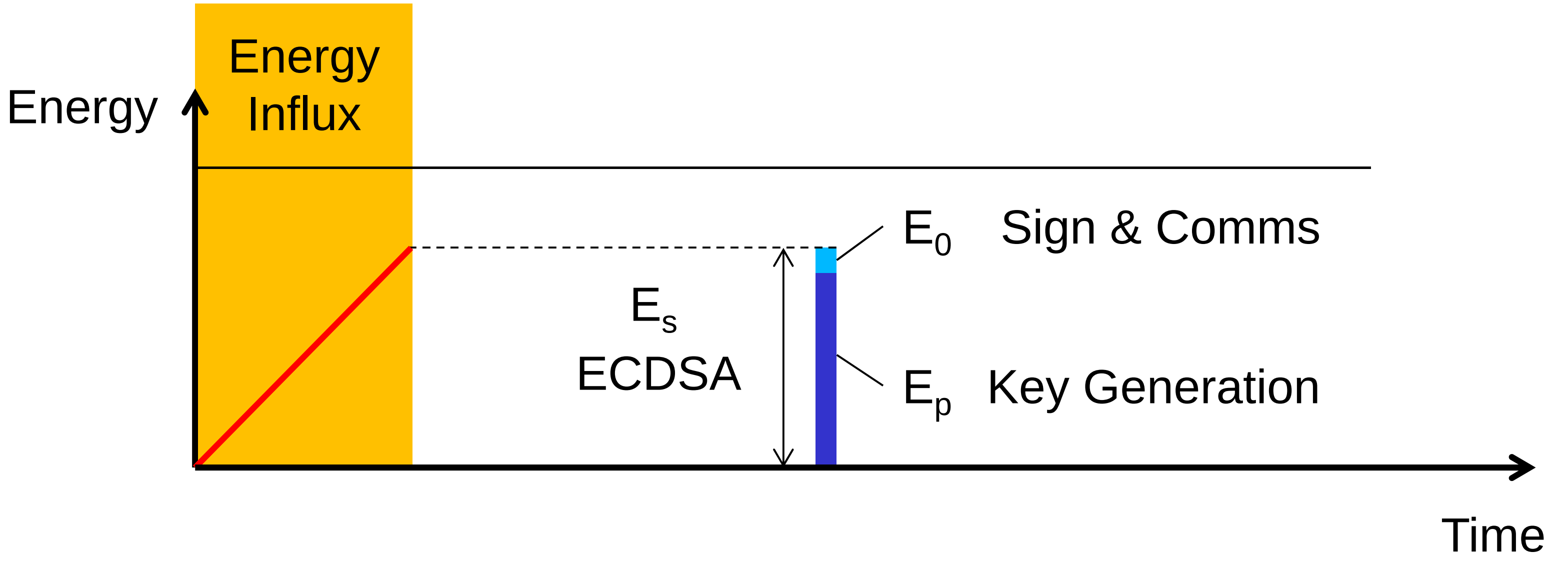
How to reach Enlightenment?

- **Almost every cryptographic algorithm extensively processes key material**
  - **Block Ciphers use Round Keys**
  - **Stream Ciphers create Key Streams**
  - **PK Ciphers generate Key pairs**
  - **(EC)DSA uses Per-message Keys**
  - **Hash-based Ciphers use Hash Chains**
  - **Lattice-based Signatures use a Verification Key**
  - **...**
- **Preparing processed key material does *not* depend on the real-time input**

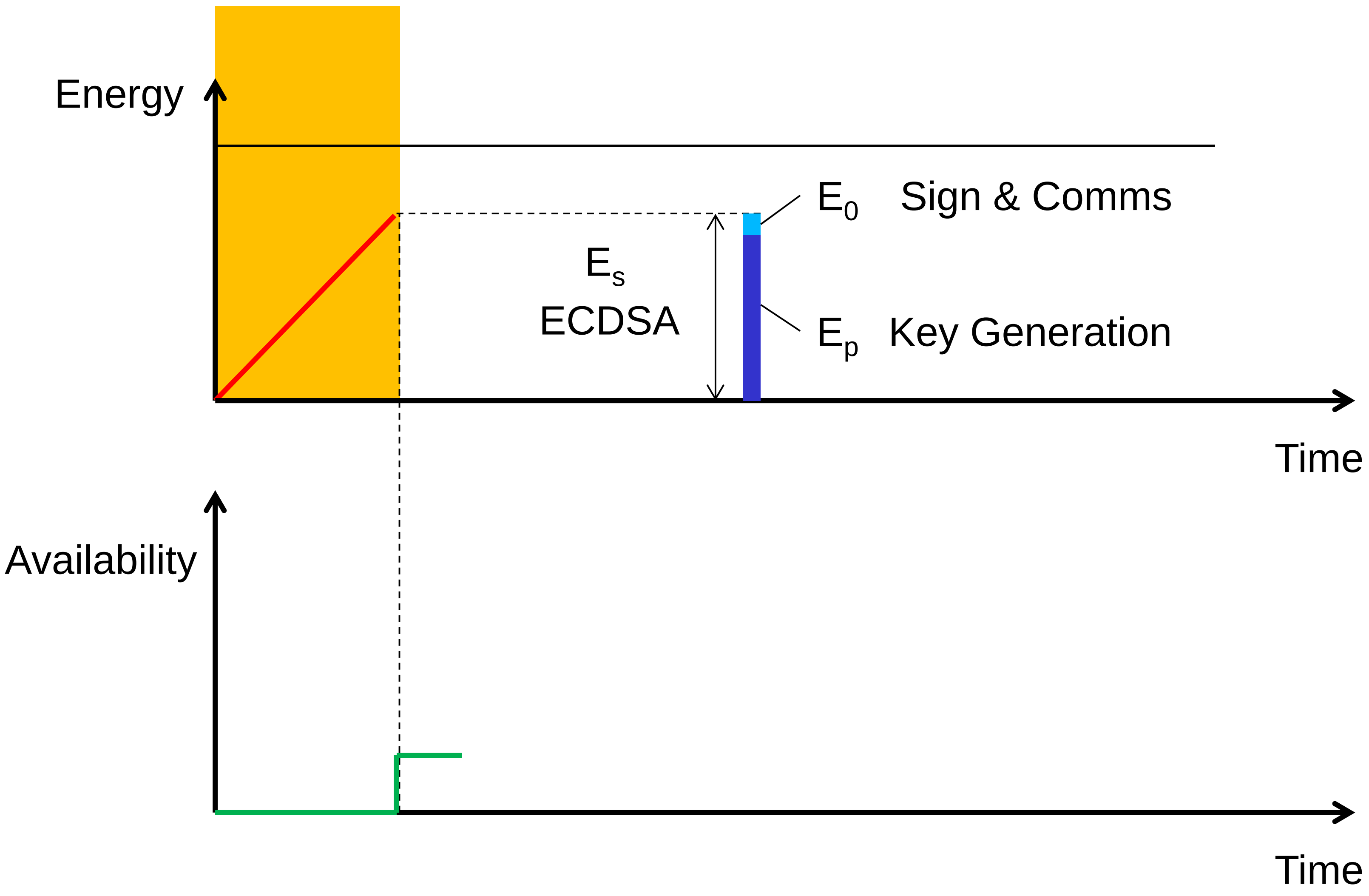
Precomputing Mechanism (1)



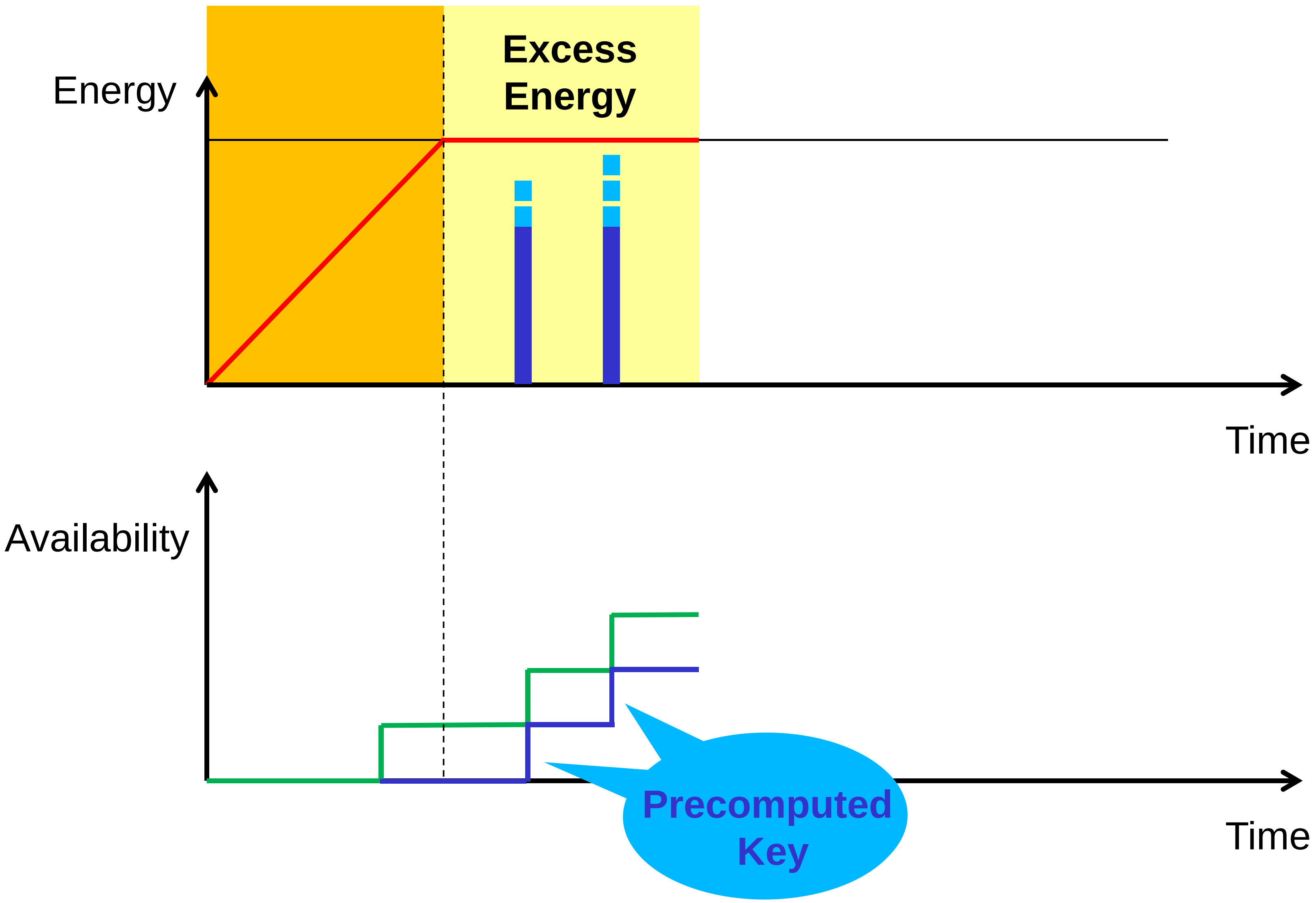
Precomputing Mechanism (2)



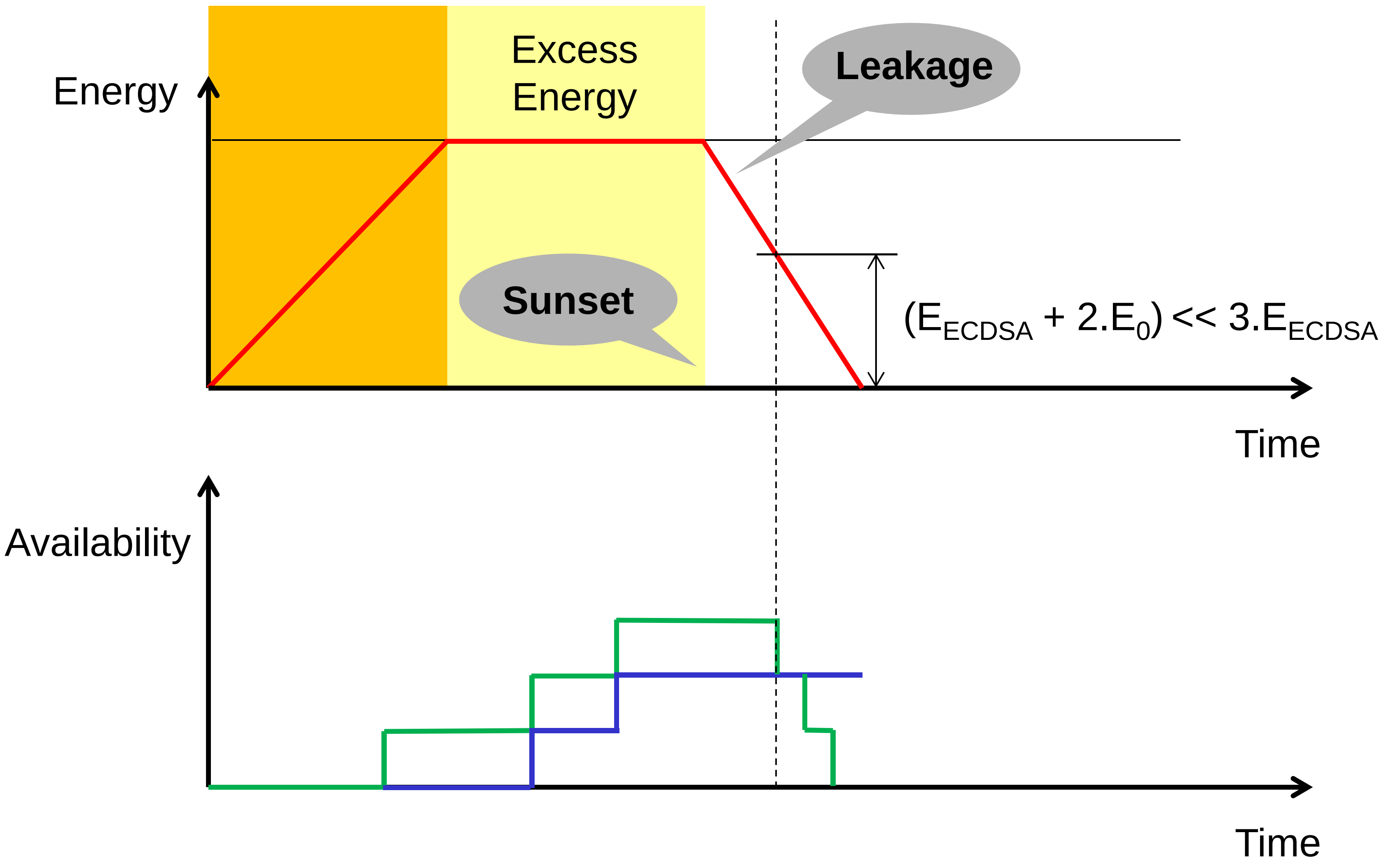
Precomputing Mechanism (3)



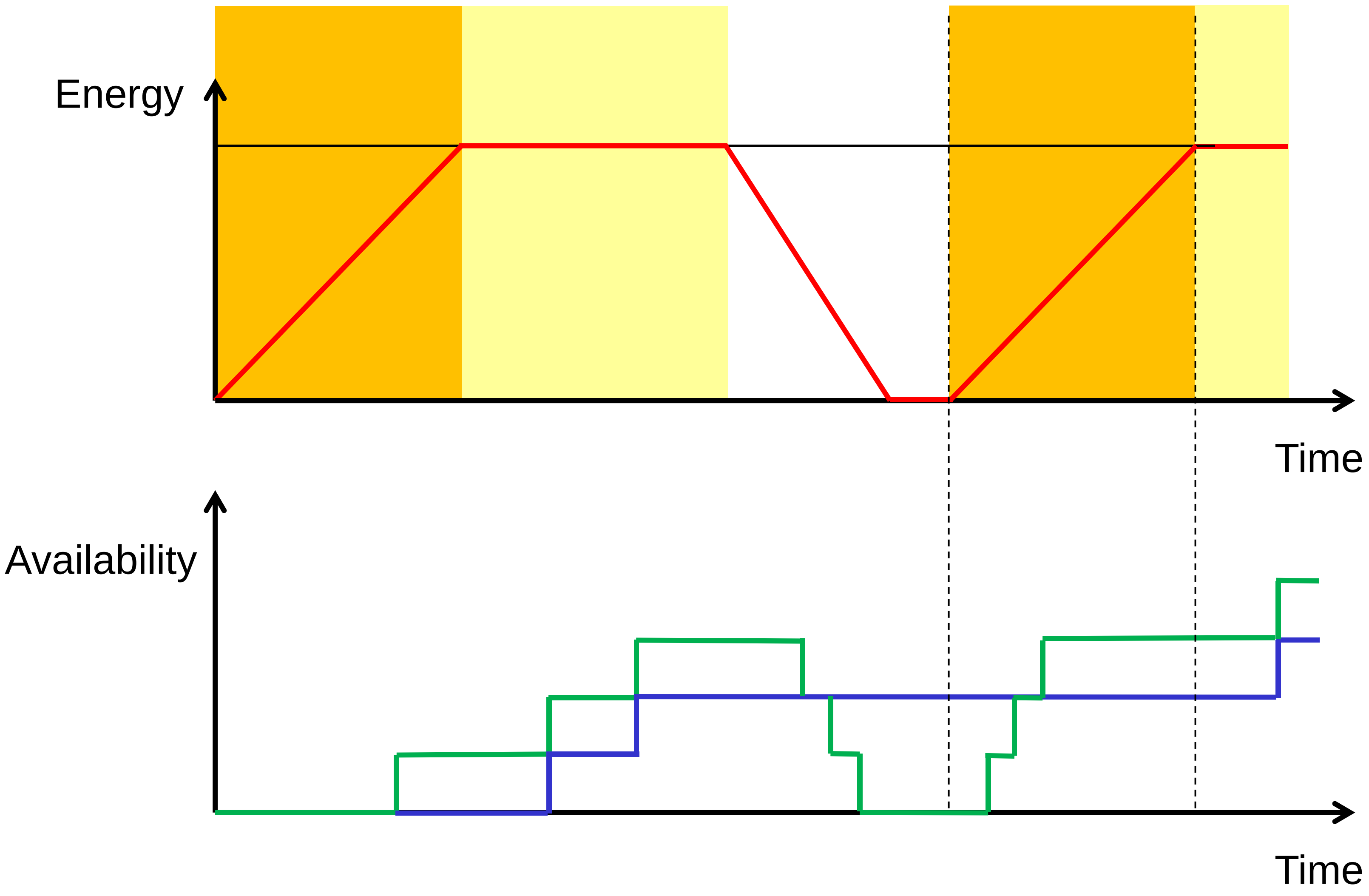
Precomputing Mechanism (4)



Precomputing Mechanism (5)



Precomputing Mechanism (6)



Key Principle

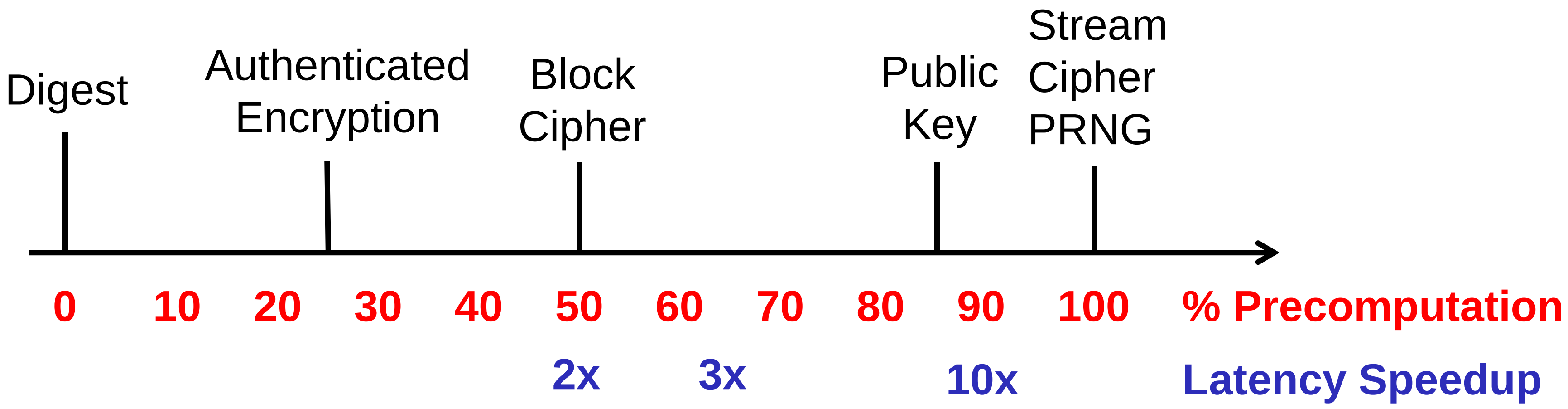
- **Never waste energy – compute keys!**
- **Advantages**
  - **Significantly decreased latency**
  - **Smaller energy store**
  - **More work done under limited Energy Influx**

	$(T_p+T_0)/T_0$	$(E_p+E_0)/E_0$
Hash-based (Winternitz l=256, 128 bit)	23.5	12
Lattice-based (GLV, 128 bit)	14.7	2.5

Based on data from Aysu (IACR ePrint 2015/288)

Challenges

- **Stored Key Material is Tamper Sensitive**
- **How to achieve Precomputed Integrity?**
  - **AE and Digests depend on input**



Digest

Authenticated Encryption

Block Cipher

Public Key

Stream Cipher PRNG

0 10 20 30 40 50 60 70 80 90 100 % Precomputation

2x 3x 10x Latency Speedup

Thanks

A Jug Fills Drop by Drop