The Role of Energy in the Lightweight Cryptographic Profile

Patrick Schaumont, Conor Patrick

Secure Embedded Systems
Virginia Tech
### Current view on Profile

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

*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
Suppose a system that uses:
- 1 Ahr battery
- AES consuming 1 mA of current.

How long does it last?
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
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
Under acceptable duty cycle of operation, energy-harvester systems have a **perpetual** lifetime.

'acceptable' means $E_{\text{harvested}} > E_{\text{consumed}}$
The energy balance

Table 1
- *Energy Store B* (J)
- *and/or Energy Influx b* (J/s)

Table 2, 3
- *Energy Quanta q* (J)
- *Duty cycle d* (1/s)
Energy Harvester Based Design

Harvester → Store → Compute → Comms/Storage

- Radio
- Bluetooth LE, WirelessHART
- EEPROM
- FRAM

nJ/byte

10^5
10^4
10^3
10^2
10^1
10^0
10^{-1}
10^{-2}
Energy Harvester Based Design

Harvester → Store → Compute → Comms/Storage

- **Harvester**
- **Store**
- **Compute**
- **Comms/Storage**

Software
- 8 bit processor

Hardware Block ciphers
- Chaskey
- Simon/Speck

**Hashing**
- AES

**Radio**
- Bluetooth LE, WirelessHART
- EEPROM
- FRAM

Energy Consumption (nJ/byte)

- 10^-2
- 10^-1
- 10^0
- 10^1
- 10^2
- 10^3
- 10^4
- 10^5
Energy Harvester Based Design

Harvester -> Store -> Compute -> Comms/Storage

- **Harvester**
  - Optical
  - Thermal
  - Mechanical (Piezo, Electro)
  - RF

- **Store**
  - $\mu W/cm^{2,3}$
    - $10^5$
    - $10^4$
    - $10^3$
    - $10^2$
    - $10^1$
    - $10^0$
    - $10^{-1}$
    - $10^{-2}$

- **Compute**
  - Hashing
    - Chaskey
    - Simon/Speck
  - AES

- **Comms/Storage**
  - Radio
    - Bluetooth LE, WirelessHART
  - Hardware
    - Block ciphers
  - Memory
    - FRAM
    - EEPROM

- **Costs**
  - nJ/byte
    - $10^5$
    - $10^4$
    - $10^3$
    - $10^2$
    - $10^1$
    - $10^0$
    - $10^{-1}$
    - $10^{-2}$
Energy Harvester Based Design

Harvester → Store → Compute → Comms/Storage

- **J**
  - Battery
  - Super Capacitor

- **nJ/byte**
  - Hashing
  - AES
  - Bluetooth LE, WirelessHART
  - EEPROM
  - FRAM

- **Hardware Block ciphers**
  - Chaskey
  - Simon/Speck
Energy Harvester Based Design

Harvester → Store → Compute + Comms

- Optical
- Thermal
- Mechanical (Piezo, Electro)
- RF

Energy Density

- $\mu W/cm^2$
  - $10^5$
  - $10^4$
  - $10^3$
  - $10^2$
  - $10^1$
  - $10^0$
  - $10^{-1}$
  - $10^{-2}$

1 block = 20 uJ

= 1 $\mu W$ x 20 sec

Energy Consumption

- $nJ/byte$
  - $10^5$
  - $10^4$
  - $10^3$
  - $10^2$
  - $10^1$
  - $10^0$
  - $10^{-1}$
  - $10^{-2}$

Based on data from TI, Penella-Lopez, Mitcheson
Energy Harvester Based Design

Harvester → Store → Compute + Comms

- Optical
- Thermal
- Mechanical (Piezo, Electro)
- RF

μW/cm²

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

nJ/byte

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

1 block = 20 uJ

= 4320 blocks / day

- Hashing
- AES
- Chaskey, Simon/Speck
- Hardware Block ciphers

Based on data from TI, Penella-Lopez, Mitcheson
Energy Harvester Based Design

Traditional design - atomic algorithm execution

\[ E_{\text{store}} \]

\( \text{store capacity} \)

\( \text{wasted energy} \)

\( \text{quanta requested} \)

\( \text{wait} \quad \text{proceed} \)
Improved design - precomputed execution

\[ E_{\text{store}} = E_{\text{store capacity}} \]

\[ \text{store capacity} = \text{wasted energy} \]

\[ \text{quanta requested} = \text{precomputed completion} \]

\[ \text{and } E(\text{green}) < E(\text{blue}) \]

\[ \text{and } t(\text{green}) < t(\text{blue}) \]
Assume 1 cm^2 of EH transducer.

Harvester → Store → Compute → Comms/Storage

- HARVESTER: Hardware Block cipher
- STORE: Super capacitor, FRAM
- COMPUTE: Hashing, 8 bit processor
- COMMS/STORAGE: Battery, Solar harvesting

Potential of 1.5 MB per day

Magnitude: 10^5, 10^4, 10^3, 10^2, 10^1, 10, 10^{-1}, 10^{-2}, 10^{-3}

Thank you for your attention.
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:
  - $\text{Energy} = K \times (\text{Power} \times \text{throughput} / \text{block-size})$

- $K = \text{technology constant, units: } CV^{2/2} \text{ J/gate)$

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

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

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