CESEL: Flexible Crypto Accelerator for IoT

Kevin Kiningham
Dan Boneh, Mark Horowitz, Phil Levis
Background

- Cryptography is critical for IoT security
  - Code signing, data privacy, user authentication, …
  - TLS, WiFi, BLE, Thread, …
- However, cryptography can use a lot of energy
- Existing Solution: Fixed function hardware accelerators
  - Implement crypto algorithm directly in silicon
  - Huge energy savings, but inflexible
The Problem

• Security requirements change over time
  • Market requirements change
  • Crypto gets broken

• Long deployments mean change is more likely

• Current accelerators can’t adapt to new crypto
  • New cipher requires physical replacement of device
Flexible Acceleration

- We need **flexible** acceleration
  - Works for wide range of crypto
  - Gives “good enough” power reduction
Crypto Commonalities

- Investigated 38 crypto algorithms
  - Drawn from major protocols/libraries/competitions

- Symmetric ciphers/Hash functions
  - Bit/Byte permutations
  - Internally parallel
  - Operation width <= 64 bits

- Asymmetric ciphers
  - Long-word arithmetic operations (>128 bits)
CESEL Overview

- In order SIMD architecture with 256-bit data path
- Designed to execute as co-processor
- Split into Frontend (fetch/decode) and Backend (execute/writeback)
- Number of lanes and lane width is flexible
CESEL Frontend

- No data dependent control flow
  - Not needed in vast majority of crypto code
  - Simplifies implementation

- Loops use hardware “Loop Stack”
  - Hardware keeps track of loop iteration + boundary
  - Fetch stage can always predict next instruction

- 16-bit instructions
  - Minimizes energy cost of instruction fetches (significant in practice)
CESEL Backend

- SIMD lane width is flexible
  - 32x8 bits up to 1x256 bits
  - Set by special instruction during execution

- Internally, each operation mapped onto 16-bit execution units

- Fast byte permutation + bitslice
  - Useful in many cipher implementations
  - Turns bitwise operations into bytewise
Results

- Implemented CESEL in 180nm TSMC
- Measured total energy for multiple ciphers
- RISC-V CPU as baseline
  - 3.8-60x improvement
- ~20x more energy than dedicated ASIC

<table>
<thead>
<tr>
<th></th>
<th>ASIC</th>
<th>CESEL</th>
<th>RISC-V</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bitsliced AES</strong></td>
<td>7.07</td>
<td>147.5</td>
<td>9,036</td>
</tr>
<tr>
<td></td>
<td>(0.05x)</td>
<td>(1x)</td>
<td>(60x)</td>
</tr>
<tr>
<td><strong>SHA2</strong></td>
<td>-</td>
<td>3,279</td>
<td>12,360</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(1x)</td>
<td>(3.8x)</td>
</tr>
<tr>
<td><strong>ChaCha</strong></td>
<td>15.3</td>
<td>302.4</td>
<td>2,021</td>
</tr>
<tr>
<td></td>
<td>(0.05x)</td>
<td>(1x)</td>
<td>(6.7x)</td>
</tr>
<tr>
<td><strong>Curve 25519</strong></td>
<td>-</td>
<td>8,163</td>
<td>40,454</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(1x)</td>
<td>(5.0x)</td>
</tr>
<tr>
<td><strong>RSA</strong></td>
<td>-</td>
<td>16,840</td>
<td>87,401</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(1x)</td>
<td>(5.2x)</td>
</tr>
<tr>
<td><strong>R-LWE</strong></td>
<td>-</td>
<td>19,822</td>
<td>109,502</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(1x)</td>
<td>(5.5x)</td>
</tr>
</tbody>
</table>

Total estimated energy in nJ
Results

• Does this improvement matter?

• Estimated energy savings in real IoT application
  • Sensor collecting/transmitting ~1KB over BLE
  • Curve25519 key exchange once per week

<table>
<thead>
<tr>
<th></th>
<th>No Crypto</th>
<th>With CESEL</th>
<th>RISC-V Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>3100</td>
<td>3100</td>
<td>3100</td>
</tr>
<tr>
<td>Crypto</td>
<td>0</td>
<td>460</td>
<td>2300</td>
</tr>
<tr>
<td>Total</td>
<td>3100 (0.89x)</td>
<td>3560 (1x)</td>
<td>5400 (1.51x)</td>
</tr>
</tbody>
</table>

Total estimated energy in nJ
Recap

• IoT needs crypto acceleration + flexibility

• Our solution: CESEL
  • Wide SIMD + long word support
  • Special instructions (permute, bitslice)
  • No data-dependent control flow

• Significant energy savings compared to software
  • \( \sim 5x \) for most ciphers
  • \( 1.5x \) longer deployment time
• IoT needs crypto acceleration + flexibility

• Our solution: CESEL
  • Wide SIMD + long word support
  • Special instructions (permute, bitslice)
  • No data-dependent control flow

• Significant energy savings compared to software
  • \( \sim 5x \) for most ciphers
  • \( 1.5x \) longer deployment time

CESEL