Energy-Architecture Tuning for ECC-based RFID tags

Deepak Mane Patrick Schaumont

Bradley Department of Electrical and Computer Engineering
Virginia Tech
Blacksburg, VA

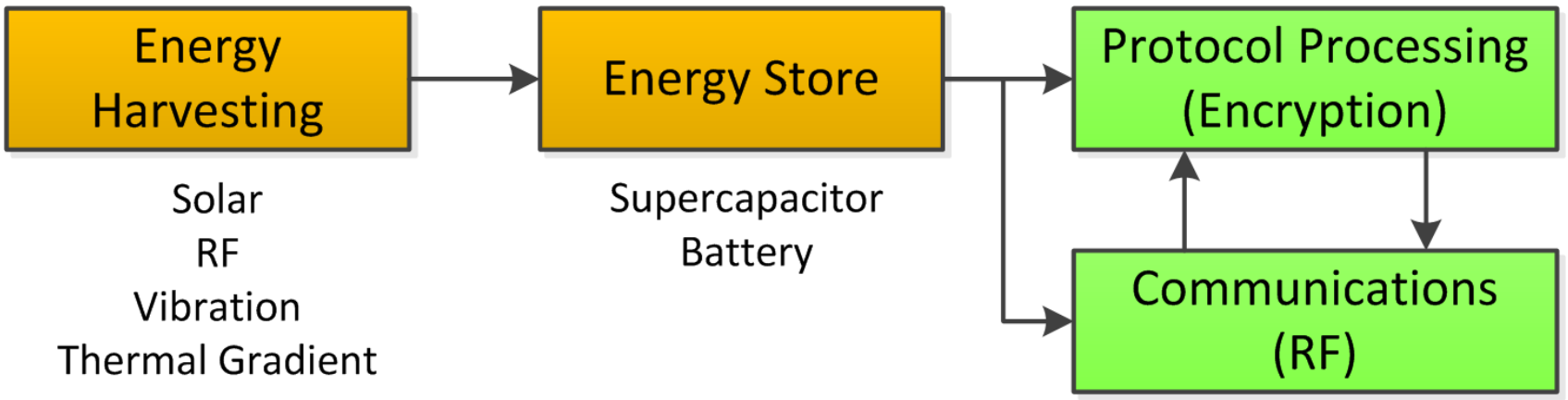
11 July 2013

1. Objectives
2. Energy Consumption in CMOS
3. Energy Measurement Methodology
4. Results and Analysis
5. Conclusions

Objectives of this research

- Challenges of ECC on RFID
  - Algorithmic complexity in layers
  - Complex algorithm-architecture interaction
  - Constraints in energy budget and execution time
- Objectives of this research
  - *Measure* how much encryption you get for 1 Joule?
  - Quantify the impact of security level (on energy)
  - Quantify the impact of architecture features (on energy)

Why care about *energy*?



- Traditional backscatter RFID is power constrained; but many alternatives possible
- RF is just one form of energy harvesting (besides solar, vibration, thermal, ..)
- Challenge: System-level dimensioning of energy harvester, energy store, algorithm

Example: is this stragegy optimal ?

Algorithm 1. Montgomery powering ladder scalar multiplication

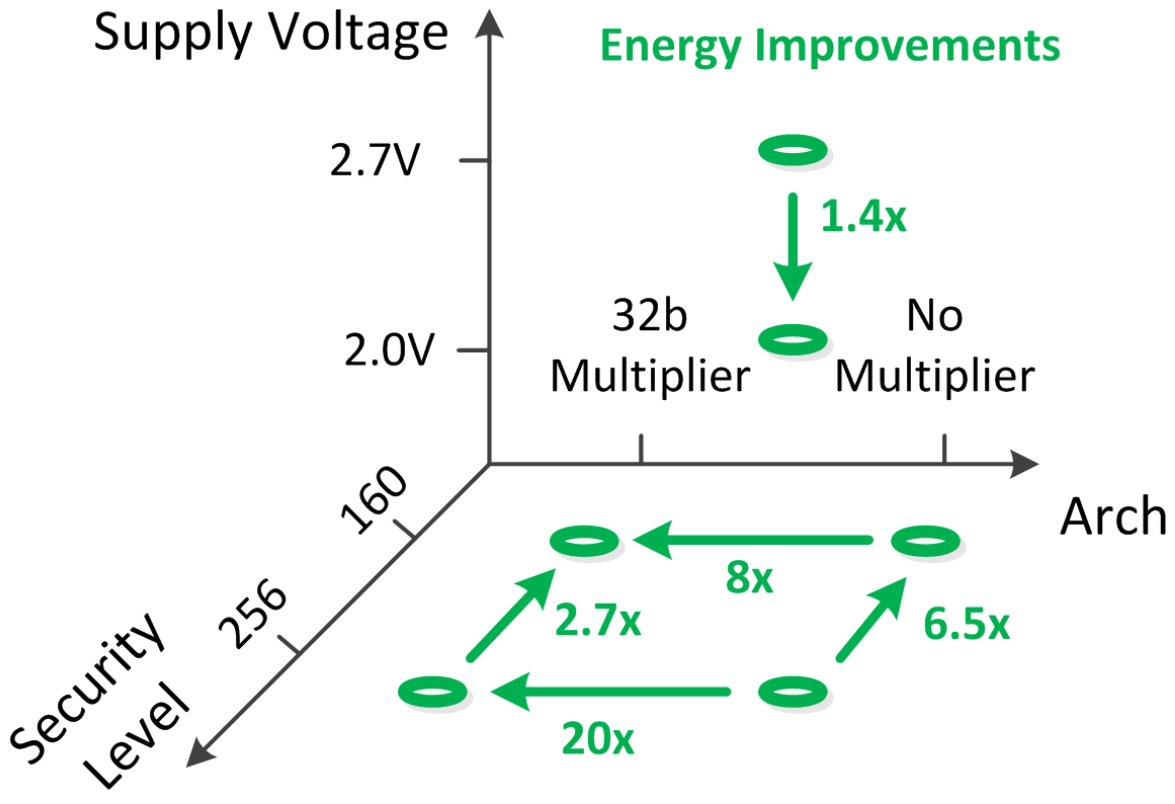
Input: $\boldsymbol{P} \in E(\mathbb{F}_q)$ and $k = (k_{n-1}, \ldots, k_0)_2 \in \mathbb{N}$, with $k_{n-1} \neq 0$
Output: $\boldsymbol{Q} = k\boldsymbol{P}$

1: $(X_0, Z_0) \leftarrow \boldsymbol{P}$; $(X_1, Z_1) \leftarrow 2\boldsymbol{P}$
2: $X_0 \leftarrow X_0 \times Z_1$; $X_1 \leftarrow X_1 \times Z_0$; $Z \leftarrow Z_0 \times Z_1$;
3: **for** $i = n - 2$ downto 0 **do**
4: $R_2 \leftarrow Z^2$, $R_3 \leftarrow R_2 + R_2$, $R_3 \leftarrow R_3 + R_2$, $R_1 \leftarrow Z \times R_2$, $R_2 \leftarrow 4b \times R_1$,
5: $R_1 \leftarrow {X_{1-k_i}}^2$, $R_5 \leftarrow R_1 + R_3$, $R_4 \leftarrow {R_5}^2$, $R_1 \leftarrow R_1 - R_3$, $R_5 \leftarrow X_{1-k_i} \times R_1$,
6: $R_5 \leftarrow R_5 + R_5$, $R_5 \leftarrow R_5 + R_5$, $R_5 \leftarrow R_5 + R_2$, $R_1 \leftarrow R_1 - R_3$, $R_3 \leftarrow {X_{k_i}}^2$,
7: $R_1 \leftarrow R_1 + R_3$, $X_{k_i} \leftarrow X_{k_i} - X_{1-k_i}$, $X_{1-k_i} \leftarrow X_{1-k_i} + X_{1-k_i}$, $R_3 \leftarrow X_{1-k_i} \times R_2$,
8: $R_4 \leftarrow R_4 - R_3$, $R_3 \leftarrow {X_{k_i}}^2$, $R_1 \leftarrow R_1 - R_3$, $X_{k_i} \leftarrow X_{k_i} + X_{1-k_i}$,
9: $X_{1-k_i} \leftarrow X_{k_i} \times R_1$, $X_{1-k_i} \leftarrow X_{1-k_i} + R_2$, $R_2 \leftarrow Z \times R_3$, $Z \leftarrow x_{\boldsymbol{P}} \times R_2$,
10: $X_{1-k_i} \leftarrow X_{1-k_i} - Z$, $X_{k_i} \leftarrow R_5 \times X_{1-k_i}$, $X_{1-k_i} \leftarrow R_3 \times R_4$, $Z \leftarrow R_2 \times R_5$.
11: *test_power_supply*().
12: **end for**
13: **return** $\boldsymbol{Q} = (X_0, Z)$.

[Pendl et al, RFIDSec 2011]

Main conclusions

Energy Profile for ECDSA `secp160r1` and `nistp256` on TI MSP430F5438A



1 Objectives

2 Energy Consumption in CMOS

3 Energy Measurement Methodology

4 Results and Analysis

5 Conclusions

Energy Consumption in CMOS

Energy consumed in CMOS

$$E_{algorithm} = n.[\alpha.C.V^2 + K.V.T_{clk}]$$

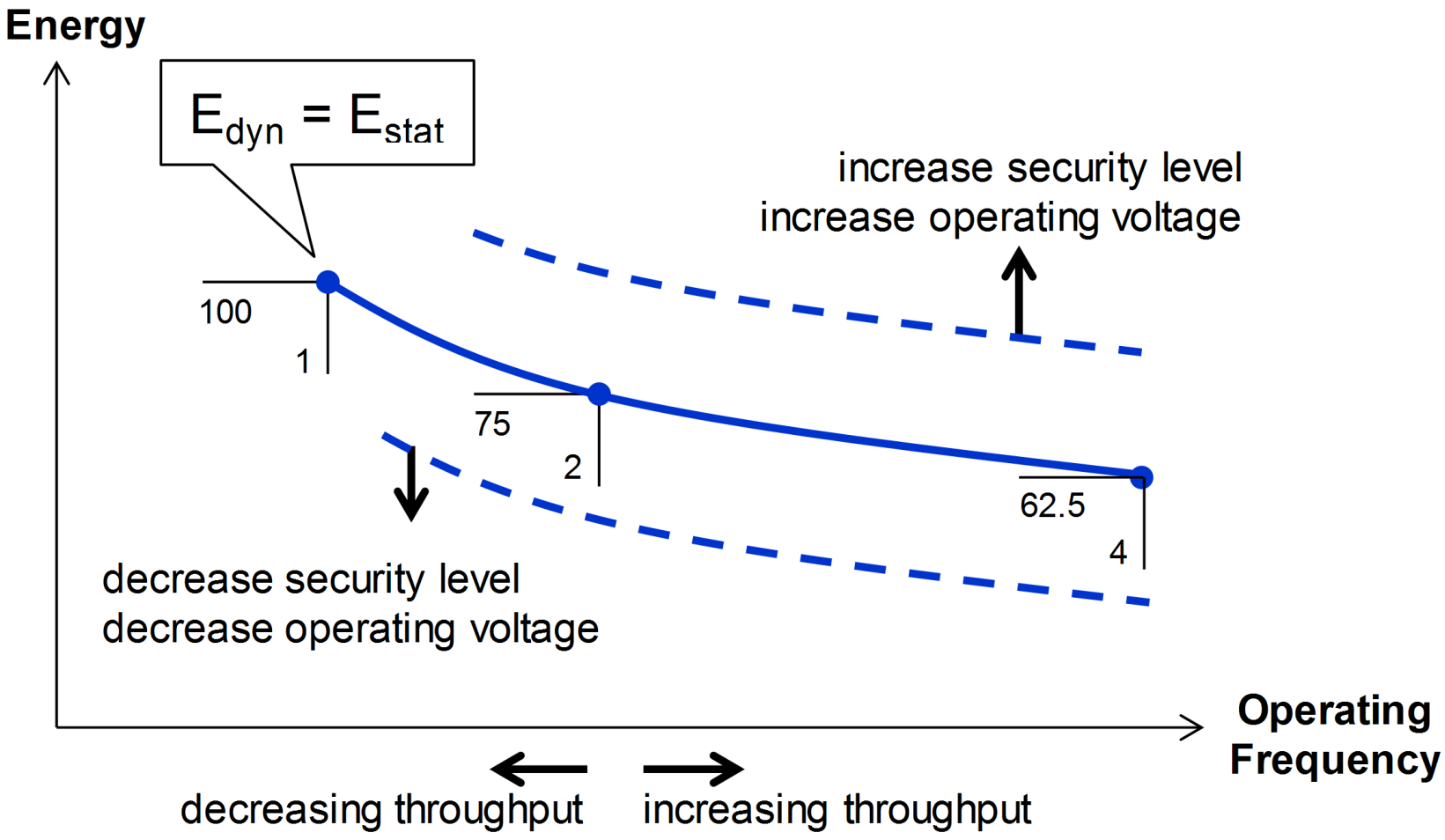
with

n	Cycle budget of algorithm
V	Voltage Supply
T_{clk}	Clock Period
C and K	Technology Constants

Observation

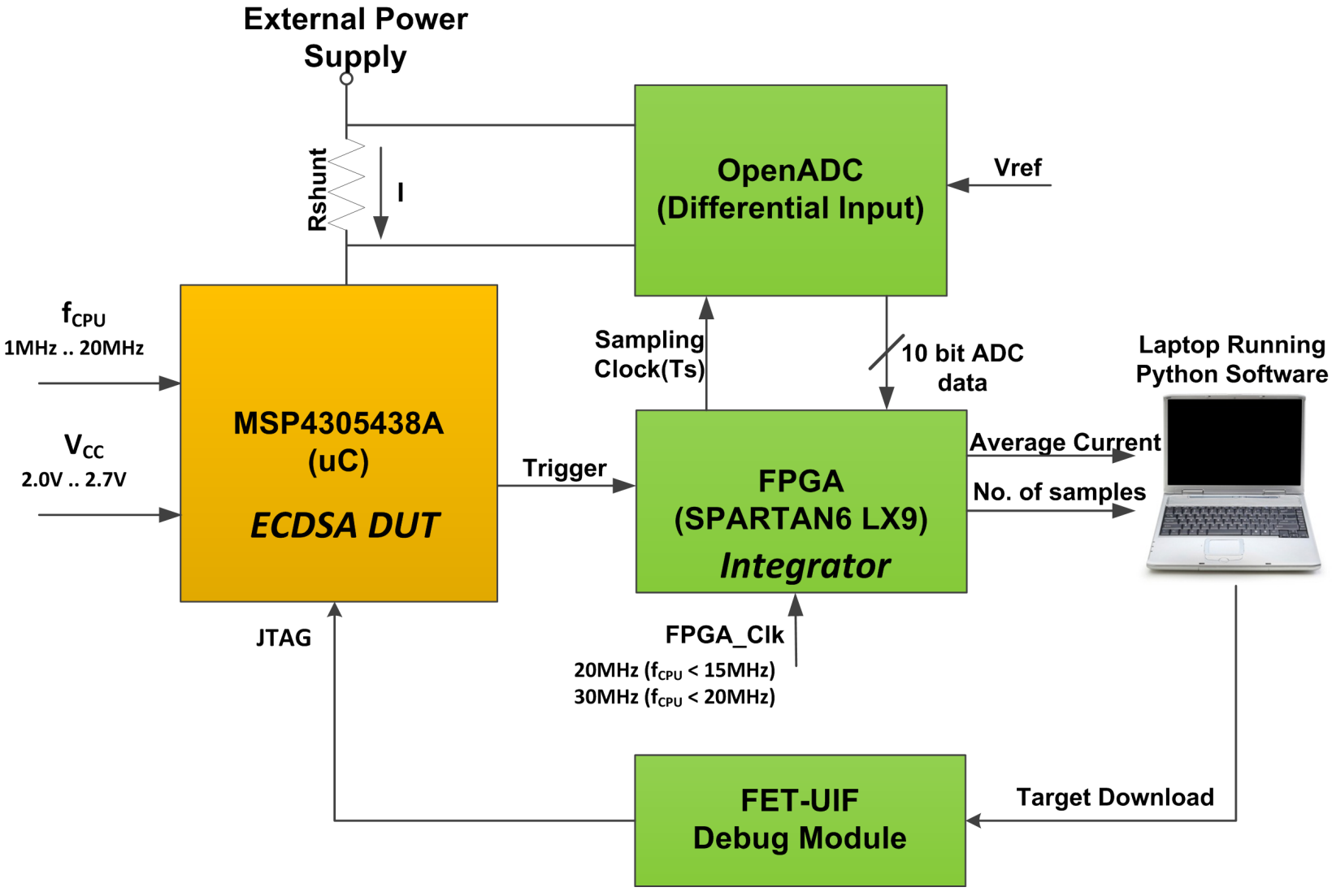
- Energy has a dynamic and a static component
- Static Energy decreases when T_{clk} decreases
  Dynamic Energy is independent of T_{clk}
- Static Power is independent of T_{clk}
  Dynamic Power increases when T_{clk} decreases

Energy Consumption in CMOS

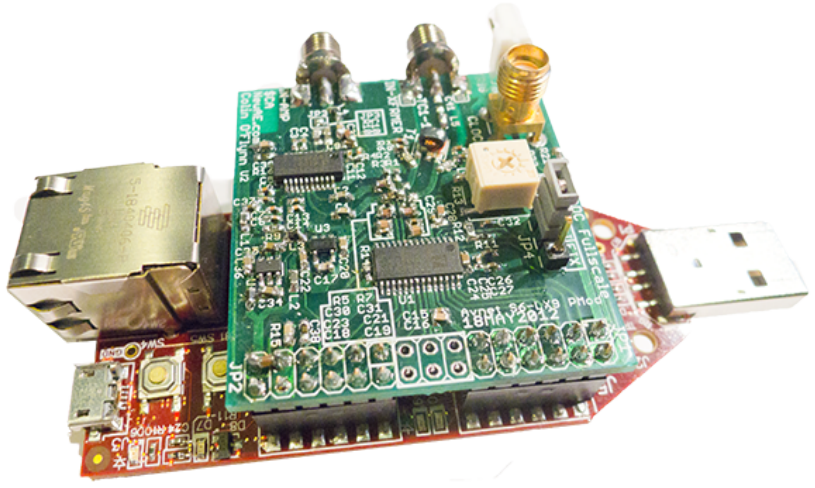


1. Objectives
2. Energy Consumption in CMOS
3. Energy Measurement Methodology
4. Results and Analysis
5. Conclusions

Infrastructure

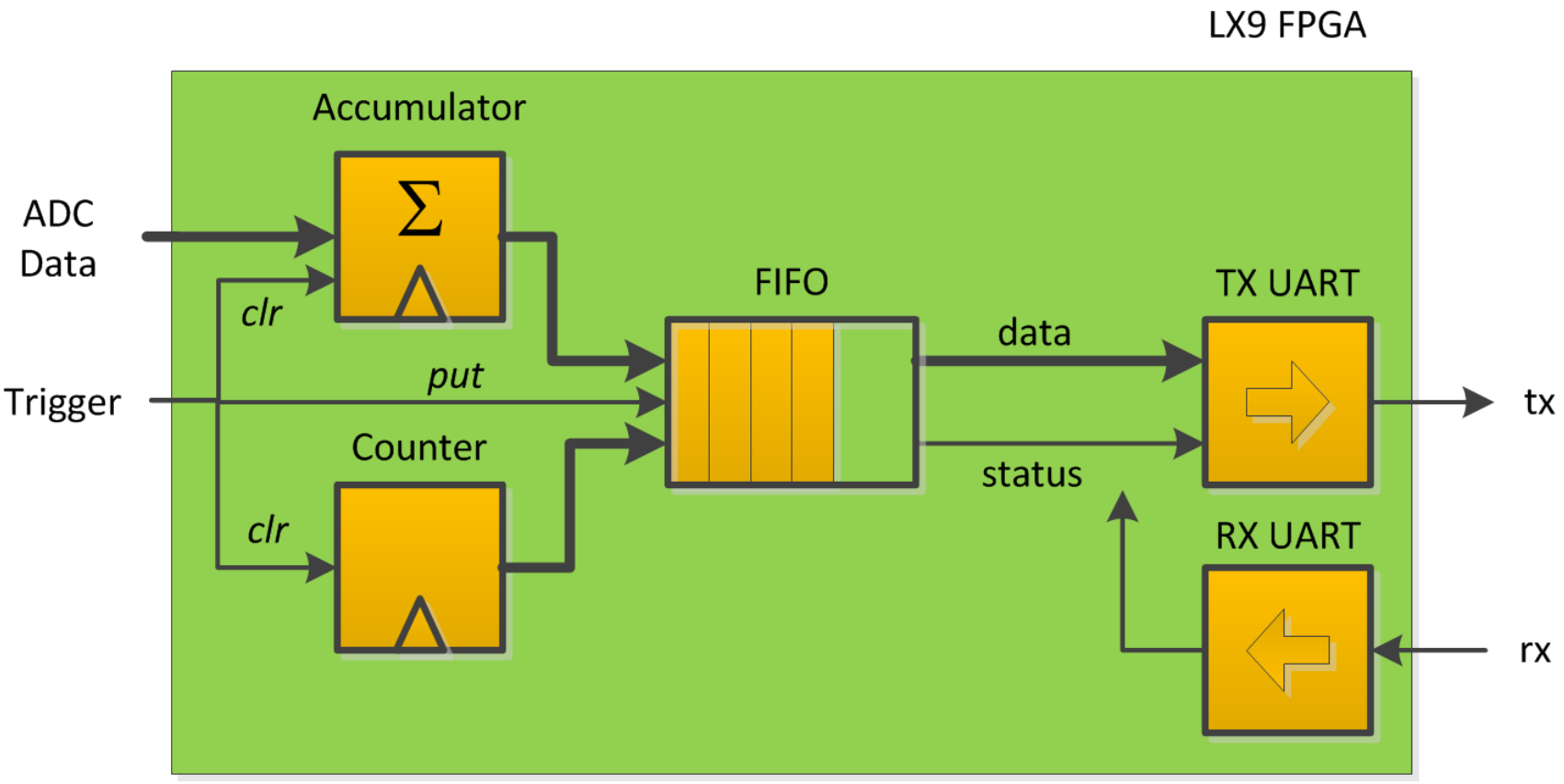


OpenADC

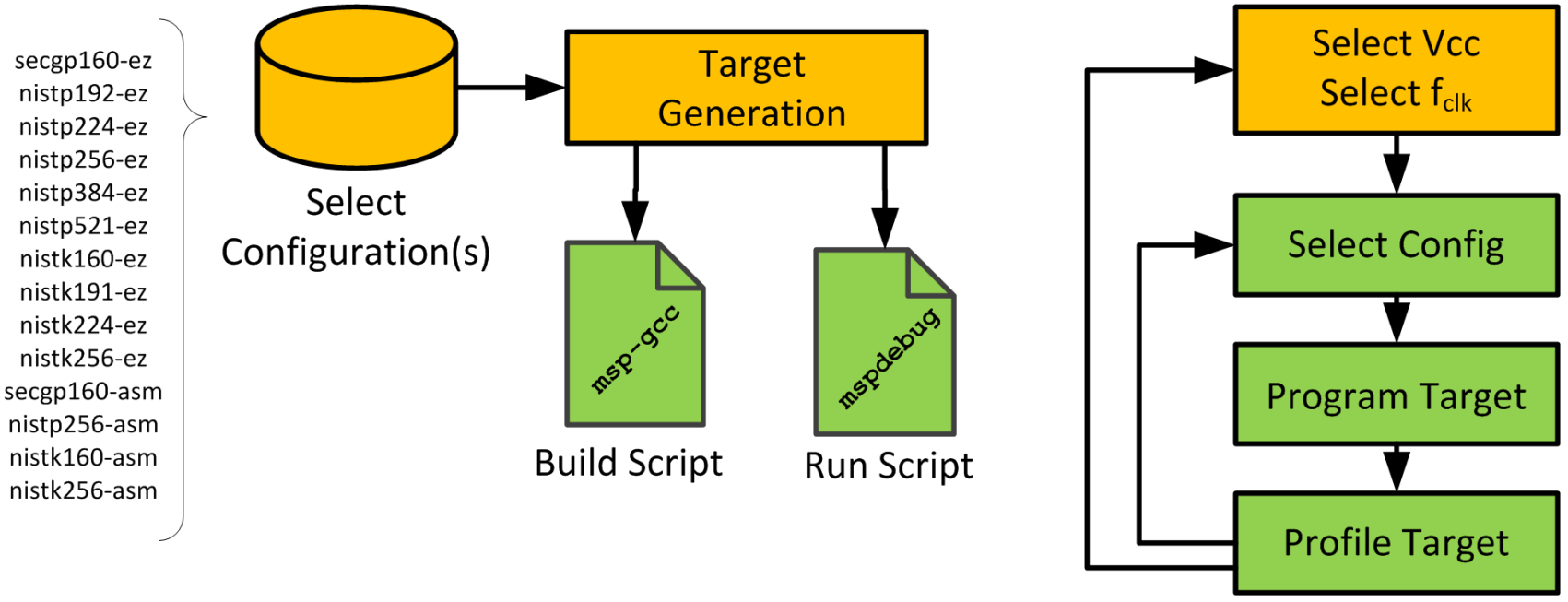


- C. Flynn, `http://www.newae.com/tiki-index.php?page=OpenADC`
- Low-cost 105MHz 10-bit ADC ($140 USD); attaches to FPGA board ($90 USD)
- Python postprocessing on laptop computes energy, handles data formatting
- We added trigger-controlled, real-time integration in FPGA

FPGA Integrator



Test Software Generation



- Using RELIC 0.3.3 with `easy` and `msp-asm` backend
- `msp-gcc 4.6.3`

1 Objectives

2 Energy Consumption in CMOS

3 Energy Measurement Methodology

4 Results and Analysis

5 Conclusions

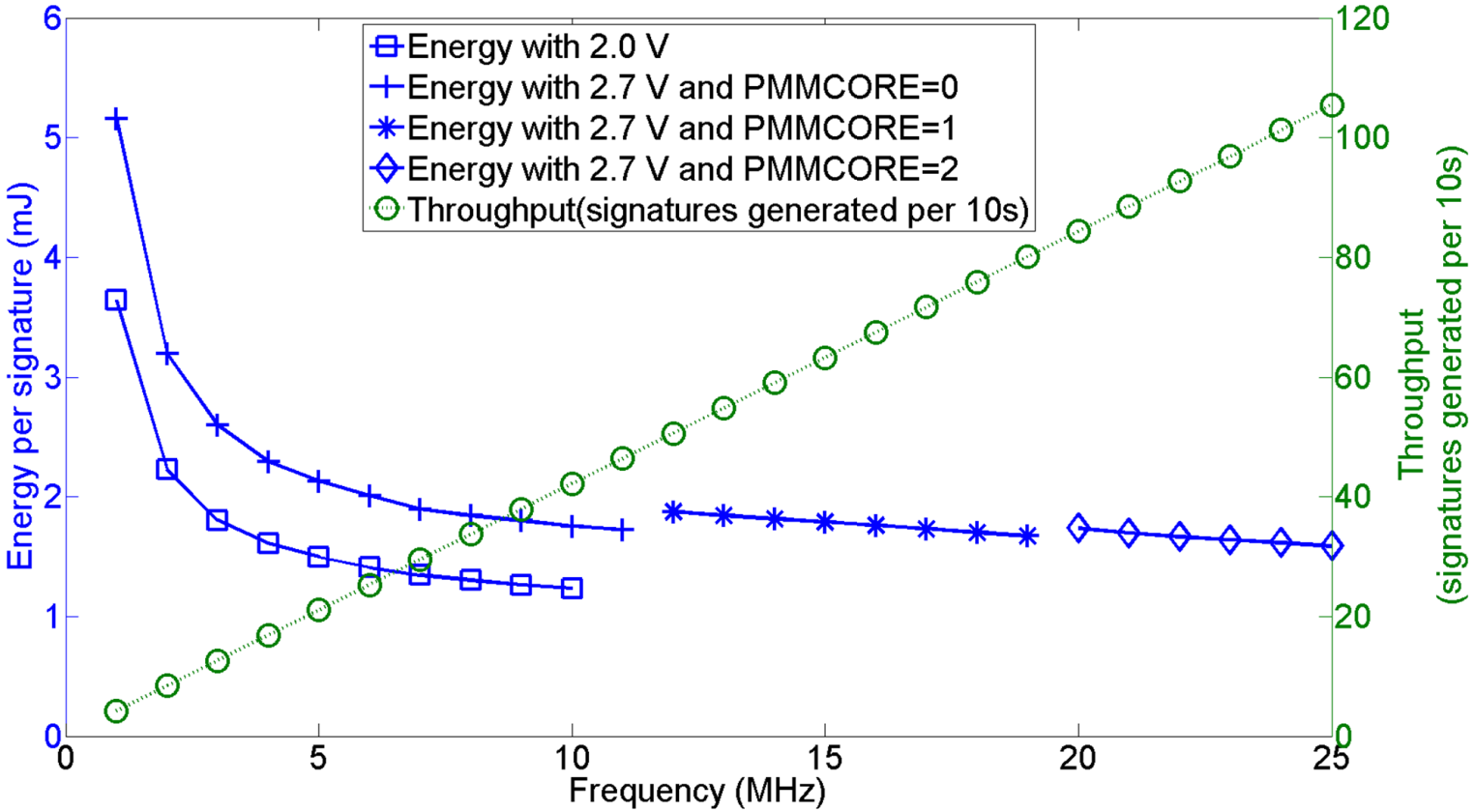
Performance

Operation	secp160r1	
	w/o hardware multiplier	with hardware multiplier
KeyGen	19,343,970	1,796,499
Sign	19,141,737	2,372,103
Verify	57,621,281	5,748,345
Related Efforts		
secp160 C [Wenger 11]	16,985,654	
secp160 ASM [Wenger 11]	8,779,931	
secp160 dsPIC [Wenger 11]		1,239,281
secp160 C [Gouvea 12]	2,520,000	
secp160 HWM [Gouvea 12]		1,744,000
P192 HWM [Hutter 12]		10,289,883

Footprint

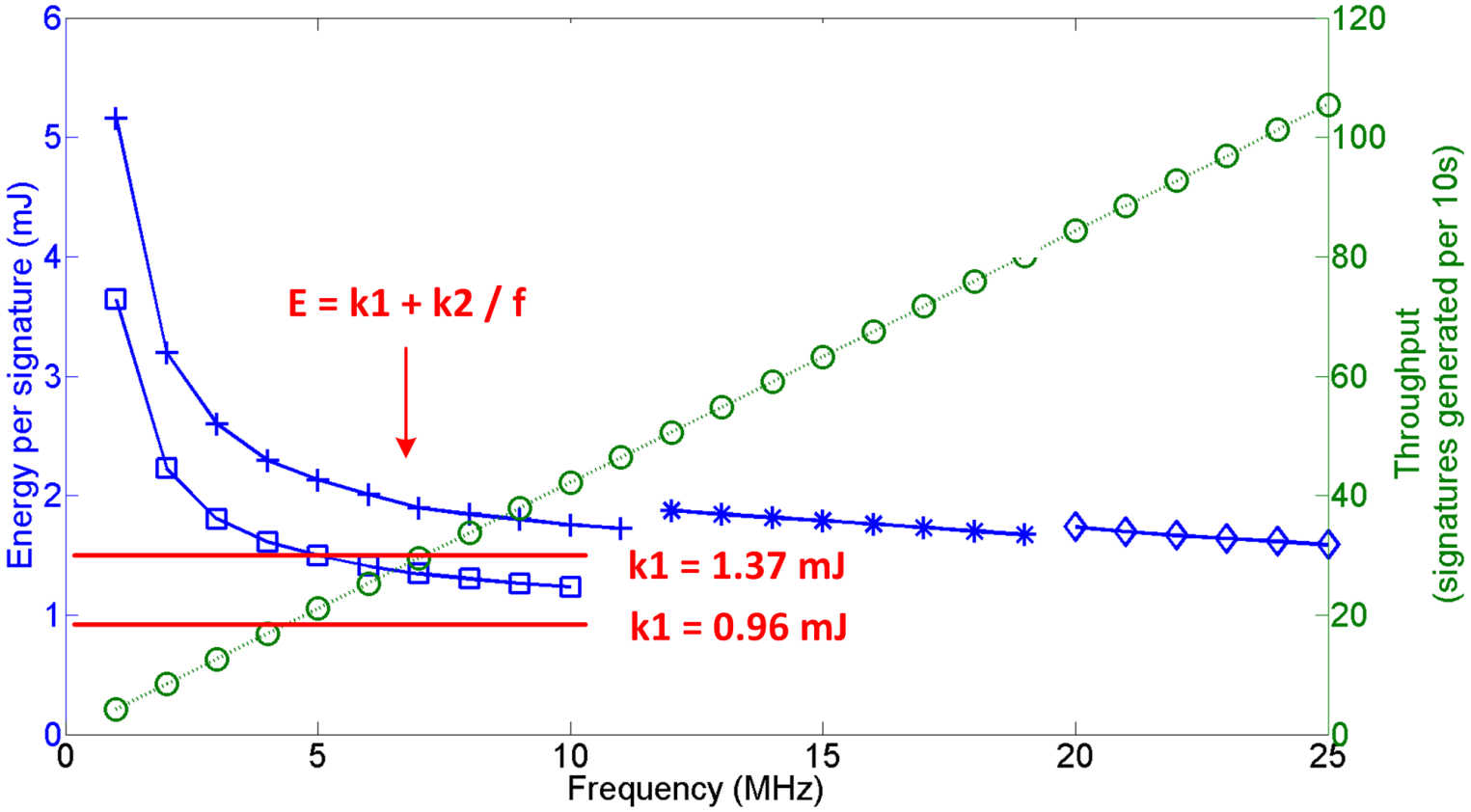
	secp160r1	
	w/o hardware multiplier	with hardware multiplier
Flash Bytes	27,134	28,168
RAM Bytes	1,074	1,074

secp160r1 ECDSA signing, using hardware multiplier

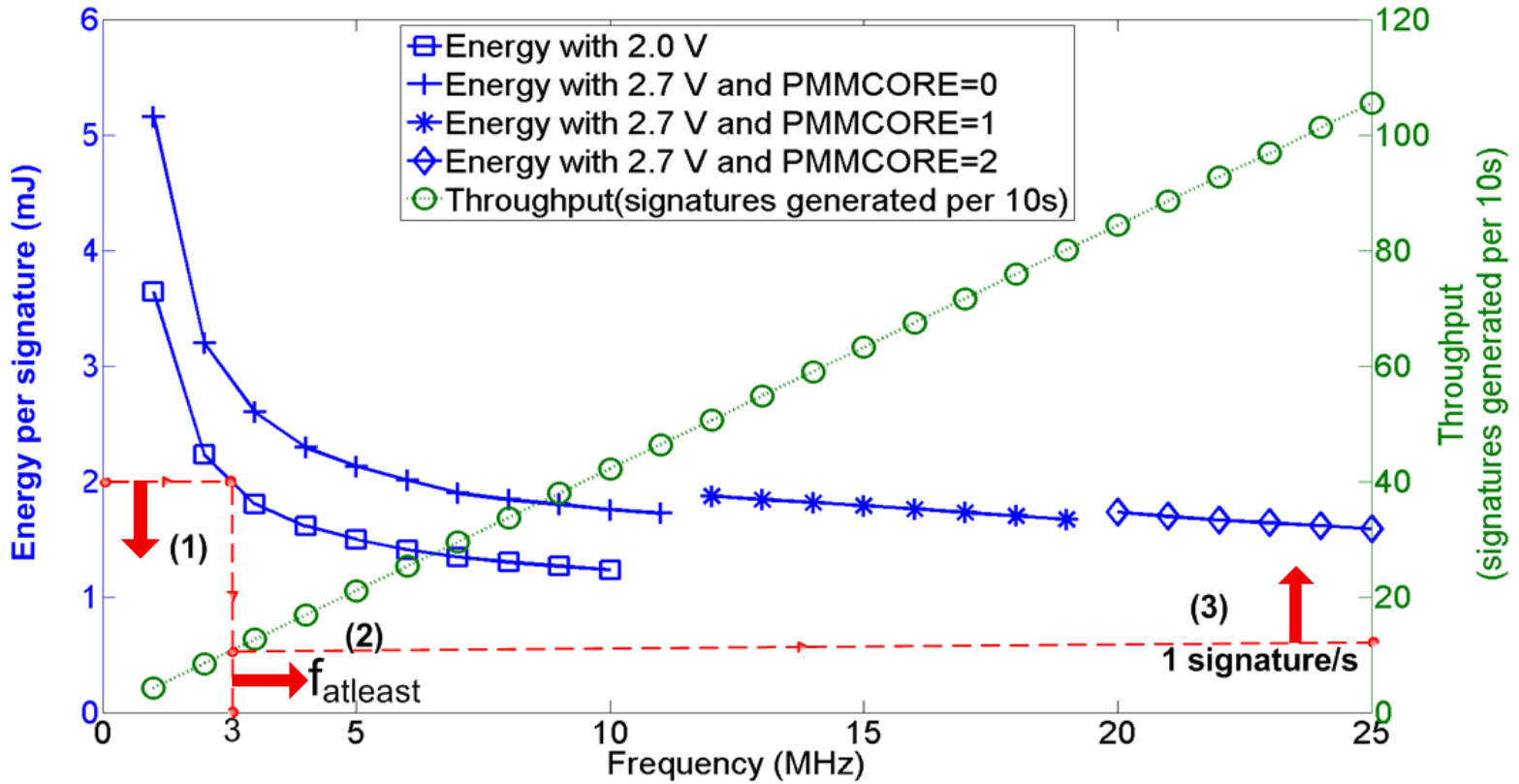


secp160r1 ECDSA signing, using hardware multiplier

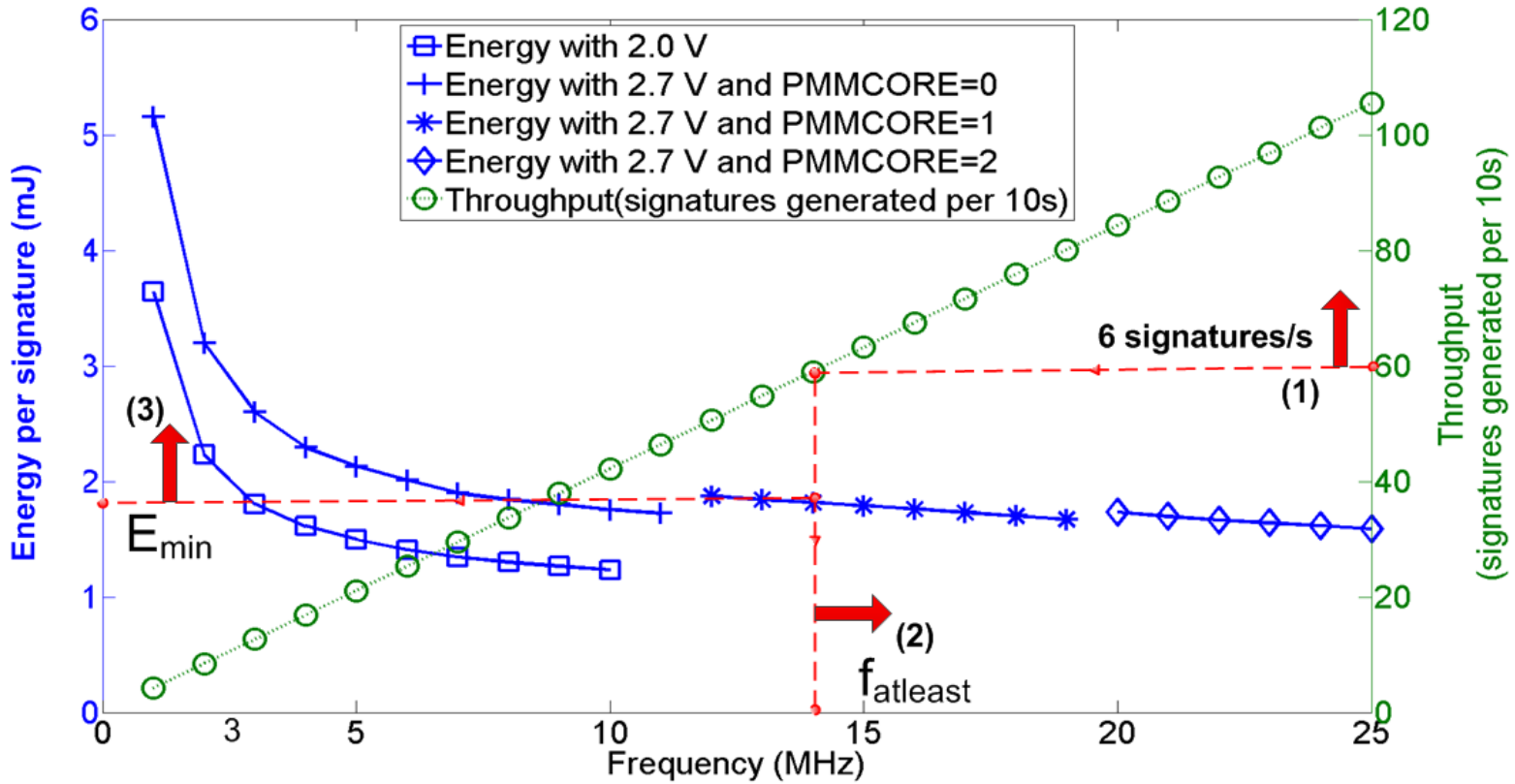
Dynamic Energy Consumption



Arch Tuning for Energy-constrained System

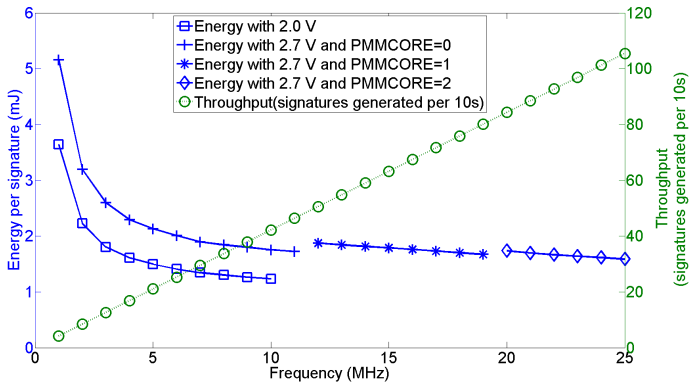


Arch Tuning for Throughput-constrained System

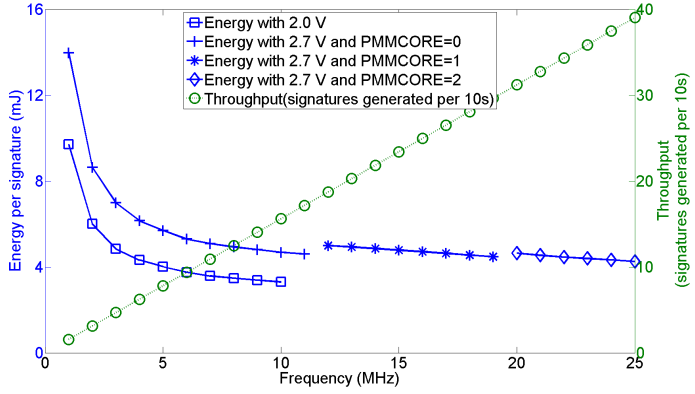


secp160r1 and nistp256 ECDSA signing

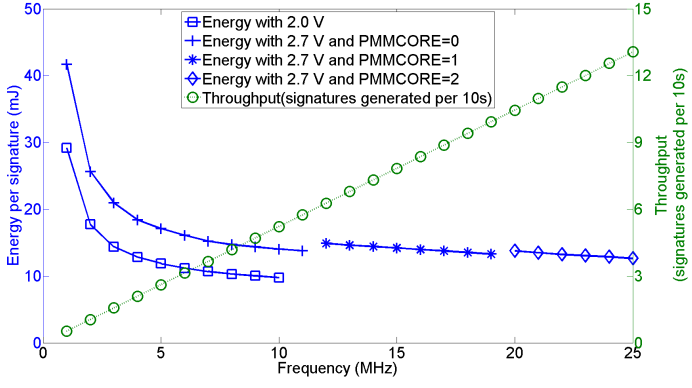
secp160r1, HWM



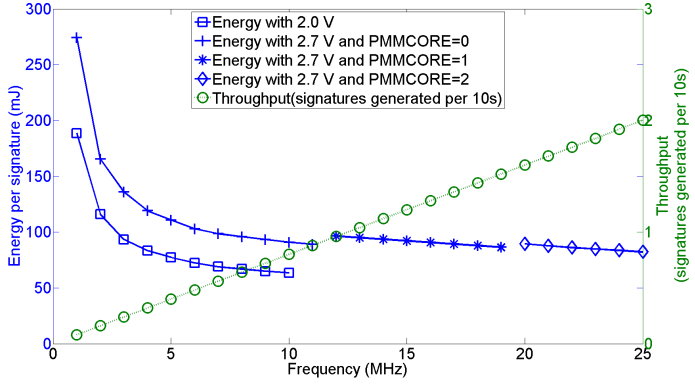
nistp256, HWM



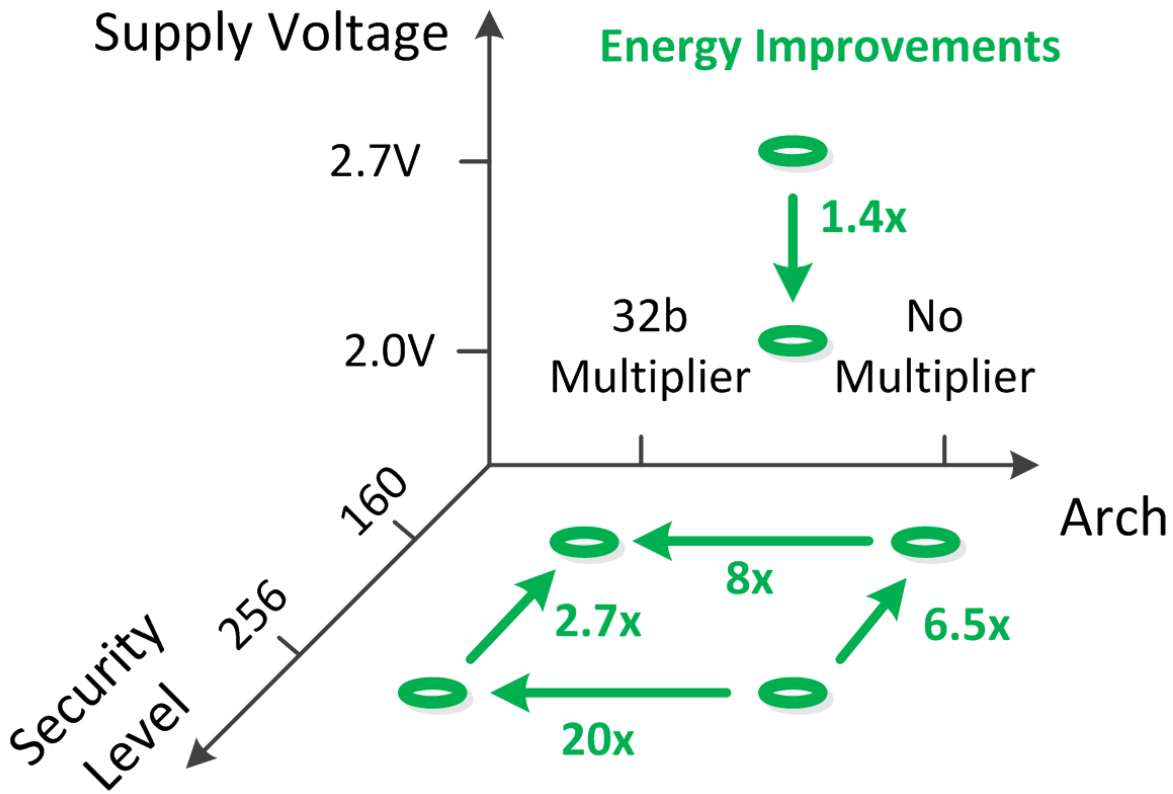
secp160r1, no HWM



nistp256, no HWM



`secp160r1` and `nistp256` ECDSA signing



Conclusions

- Ignoring overhead, faster & uninterrupted ECC execution is better
- Most significant impact comes from architecture specialization
- For untethered systems design, energy analysis is vital
- Future work, unsolved issues
  - Better architecture exploration, microcontroller power-modes
  - Need to include (RF) communication overhead