

LOW-COST STANDARD SIGNATURES IN WIRELESS SENSOR NETWORKS

G. Ateniese, G. Bianchi, A. Capossele, and C. Petrioli
Sapienza - University of Rome

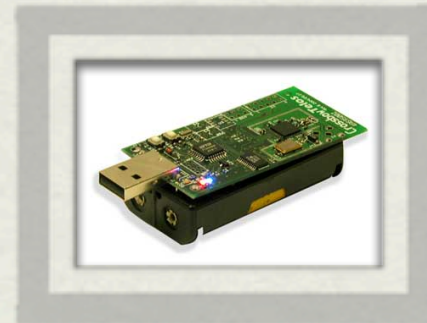
SECURITY ON WSN

- Military, Healthcare, and Industrial Control
- Different Requirements and Constraints

imote2



TelosB



Mica



MOTES

MICA2



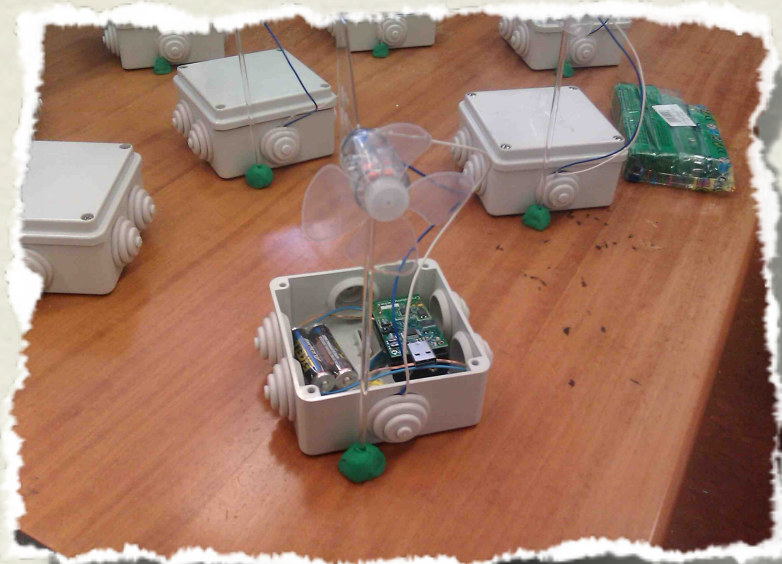
- 868/916MHz, 433 or 315MHz multi-channel transceiver
- 19.2 kbps data rate
- 512kB Flash memory
- 128kB Program memory
- 8 MHz Atmega 128L microcontroller with 4kB RAM

TelosB

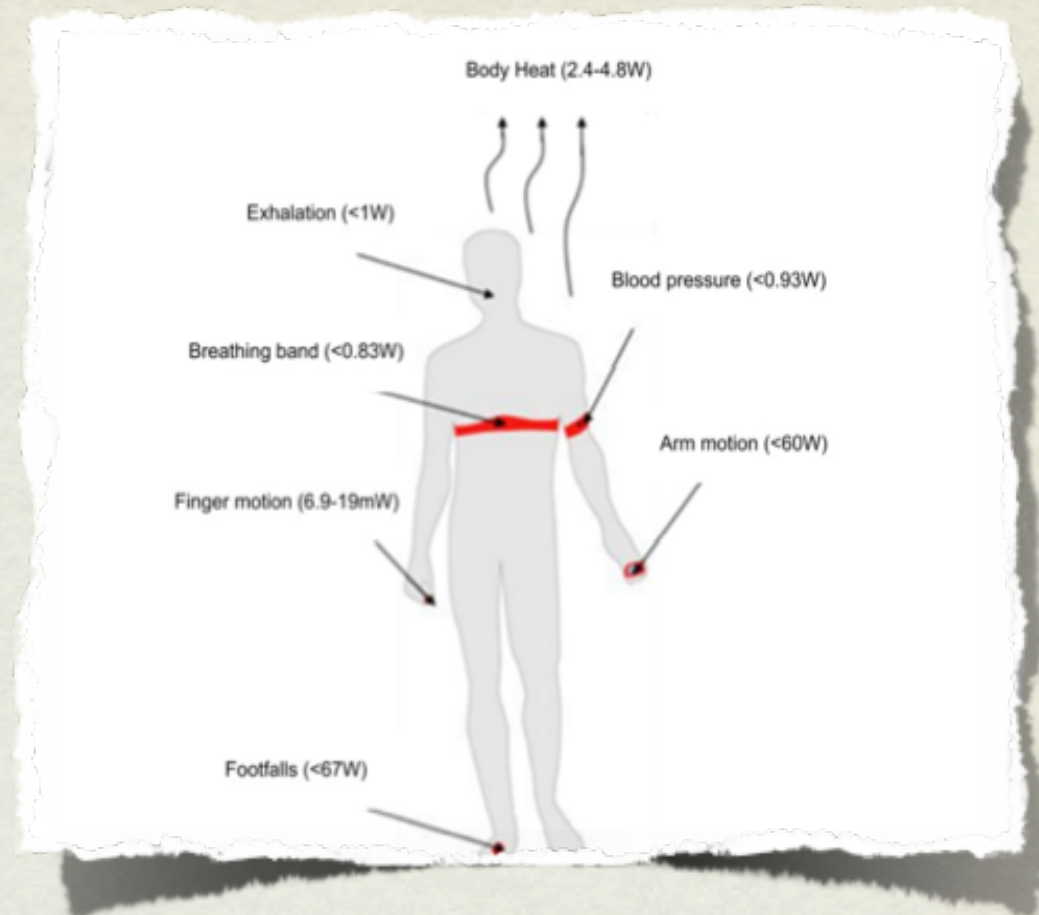


- IEEE 802.15.4/ZigBee compliant RF transceiver (2.4 GHz)
- 250 kbps data rate
- 1MB Flash memory
- 48kB Program memory
- 8 MHz TI MSP430 microcontroller with 10kB RAM

ENERGY SOURCES



Wind, Solar, etc.



Human Body

INTERESTING IDEA

- Modern sensors are equipped with flash memories which make memory consumption a less critical requirement
- Emerging energy harvesting technologies provide occasional energy peaks which could be exploited for anticipating otherwise costly computational tasks

Combine **pre-computation** techniques + **energy harvesting**

GENERATE DL PAIRS

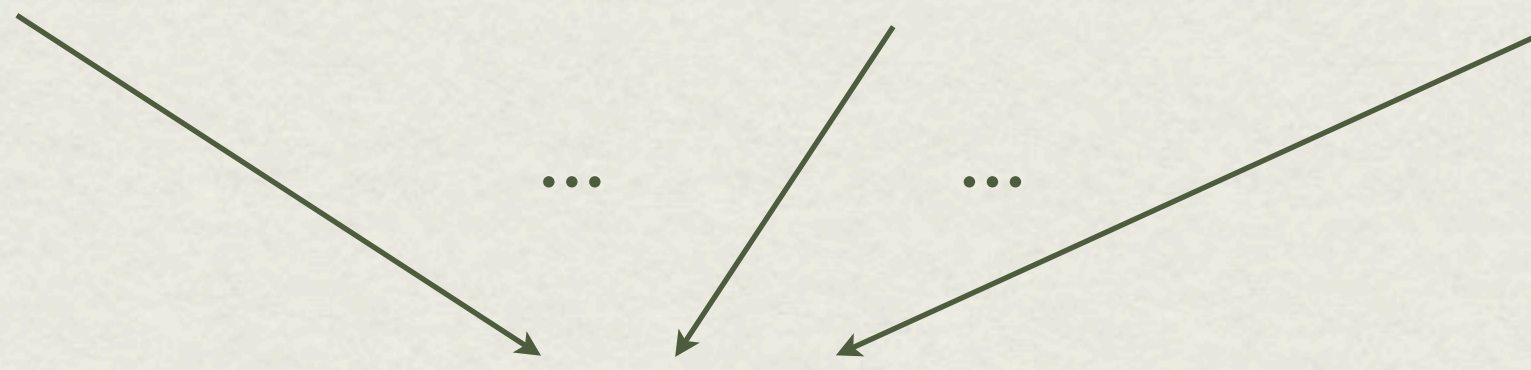
$$r, g^r$$

Boyko, Peinado and Venkatesan (BPV)

Our Improved version: I-BPV

PRE-COMPUTATION

$$(x_1, g^{x_1}) \mid (x_2, g^{x_2}) \mid \dots \mid (x_n, g^{x_n})$$


$$(r, g^r) = \left(\sum x_i, g^{\sum x_i} \right)$$

I-BPV GENERATOR

- Random walk on a Cayley graph expander
- Hidden Subset Sum problem (HSS)
- Affine HSS when used with ECDSA

Given integers $M, b_1, \dots, b_m \in \mathbb{Z}_M$,

find $\alpha_1, \dots, \alpha_n \in \mathbb{Z}_M$ such that

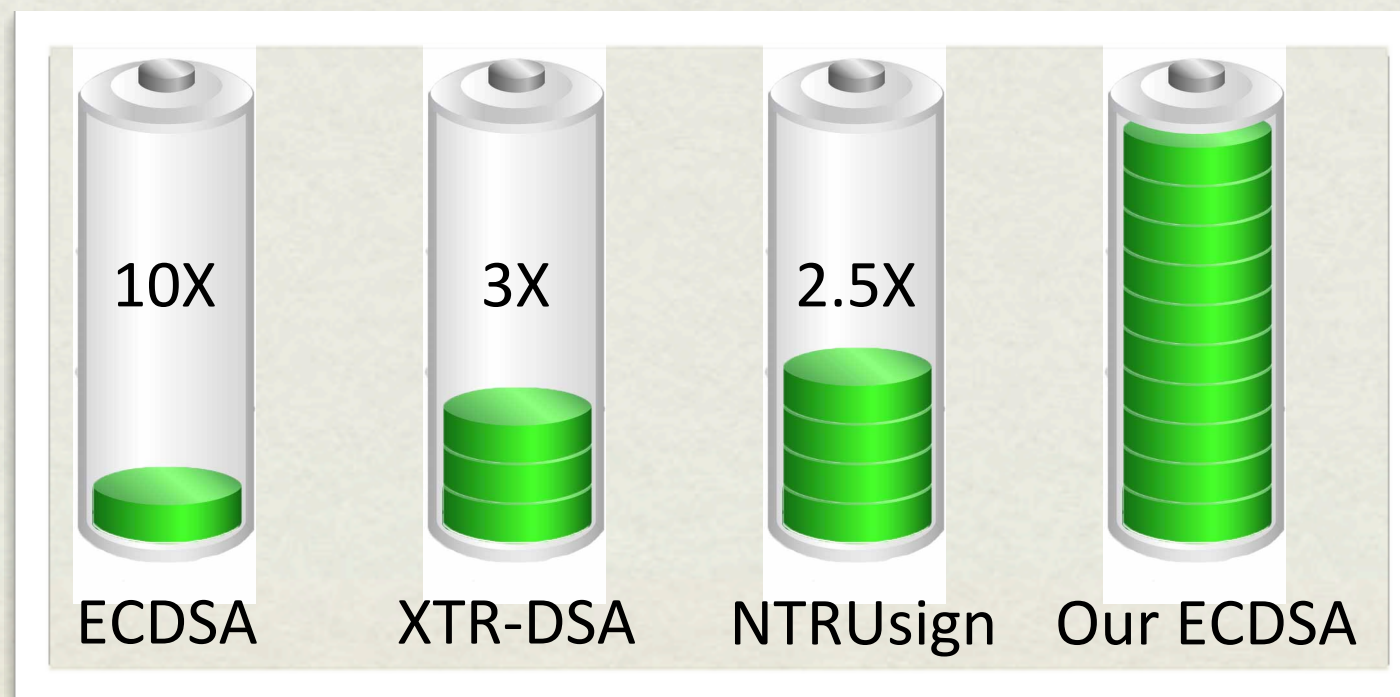
each b_i is some subset sum of $\alpha_1, \dots, \alpha_n$ modulo M .

CAYLEY GRAPHS ARE EXPANDERS

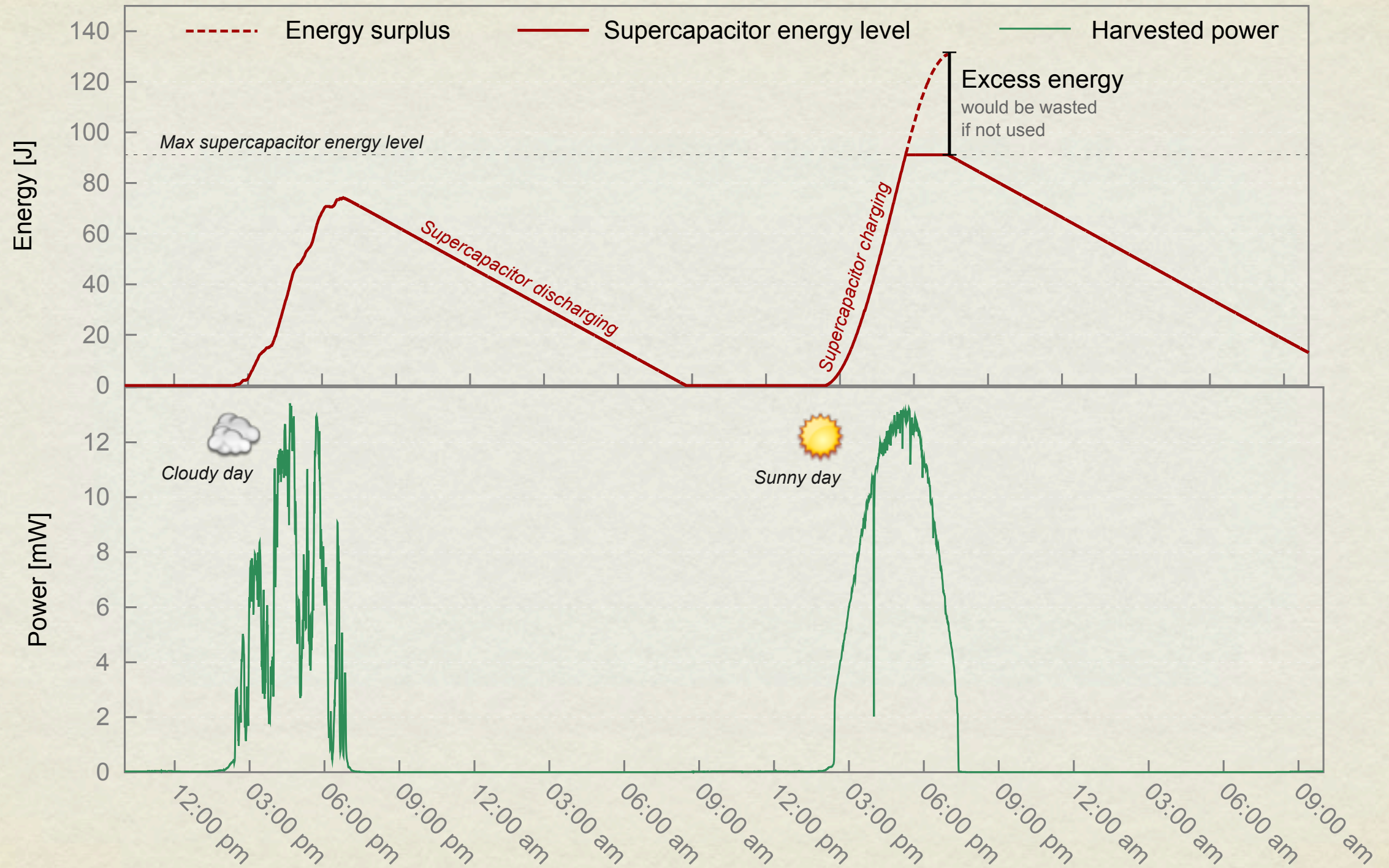
- I-BPV output essentially follows the uniform distribution
- Memory usage much smaller than before, fits current FLASH
- With proper parameters, security of I-BPV depends on its resistance to birthday attacks

COMPARISONS

Author(s)	Scheme	ROM	RAM	—Sig—	— k_{priv} —	— k_{pub} —	t_{sign}	$E_{CPU}(t_{sign})$
Gura et al.,	RSA	7.4kB	1.1kB	128B	128B	131B	10.99s	263.8mJ
Liu et al.,	ECDSA	19.3kB	1.5kB	40B	21B	40B	2.001s	14.8mJ
Driessen et al.,	NTRUSign	11.3kB	542kB	127B	383B	127B	0.619s	22.3mJ
	ECDSA	43.2kB	3.2kB	40B	21B	40B	0.918s	22.0mJ
	XTR-DSA	24.3kB	1.6kB	40B	20B	176B	0.965s	23.2mJ
This work	ECDSA	18.2kB	1.2kB	40B	21B	40B	0.346s	8.1mJ

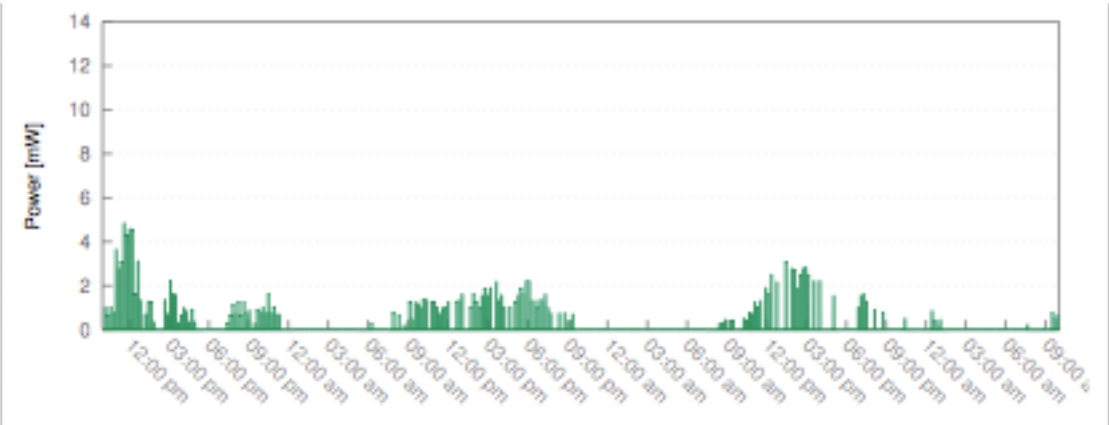
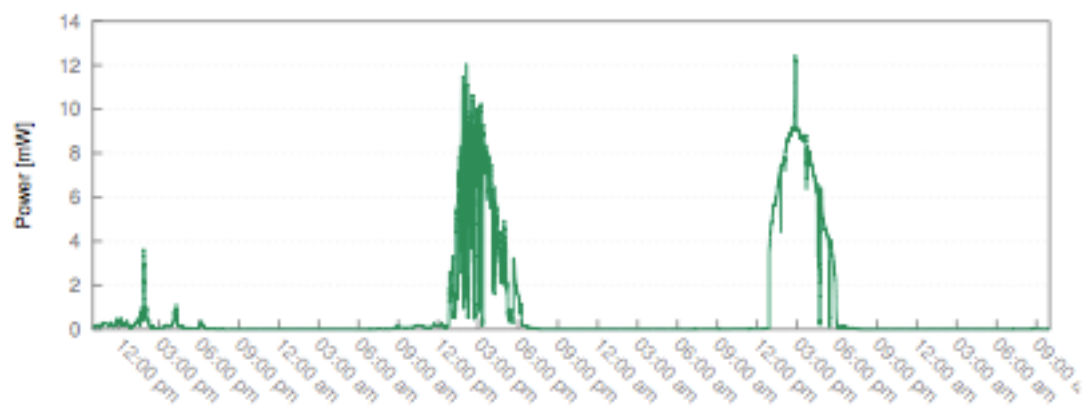


ENERGY HARVESTING



WHY NOT FULL-EXP?

	Naive			BPV		
	Precomputations	Signatures	FLASH	Precomputations	Signatures	FLASH
Day 1	6823	6823	0	19428	12726	6702
Day 2	77	77	0	0	597	6105
Day 3	3778	3778	0	6354	12459	0
Day 4	5302	5302	0	16038	13506	2532
Day 5	4758	4758	0	12936	15454	14
Day 6	5351	5351	0	17528	10783	6759
Day 7	5468	5468	0	15276	16664	5371
Average	4310	4310	0	11758	11532	2525



CONCLUSIONS

- Standard Signature (ECDSA) on mote platforms
- Significantly reduced energy cost and improved performance (better than NTRUsign) at the cost of 12kB
- ECDSA-signature generation time below 350 ms over MICA2 motes, with an energy consumption below 10 mJ
- Exploitation of harvested energy for security protocols