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.
$r^r, g^r$

Boyko, Peinado and Venkatesan (BPV)

Our Improved version: I-BPV
\[
(x_1, g^{x_1}) \mid (x_2, g^{x_2}) \mid \ldots \mid (x_n, g^{x_n})
\]

\[
(r, g^r) = \left( \sum x_i, g^{\sum x_i} \right)
\]
Random walk on a Cayley graph expander

Hidden Subset Sum problem (HSS)

Affine HSS when used with ECDSA

Given integers $M, b_1, \ldots, b_m \in \mathbb{Z}_M$, find $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_M$ such that each $b_i$ is some subset sum of $\alpha_1, \ldots, \alpha_n$ 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

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

- **ECDSA**
- **XTR-DSA**
- **NTRUsign**
- **Our ECDSA**
ENERGY HARVESTING

[Diagram showing energy harvesting with time-of-day and weather conditions.]
WHY NOT FULL-EXP?

<table>
<thead>
<tr>
<th></th>
<th>Naive</th>
<th>BPV</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Precomputations</td>
<td>Signatures</td>
</tr>
<tr>
<td>Day 1</td>
<td>6823</td>
<td>6823</td>
</tr>
<tr>
<td>Day 2</td>
<td>77</td>
<td>77</td>
</tr>
<tr>
<td>Day 3</td>
<td>3778</td>
<td>3778</td>
</tr>
<tr>
<td>Day 4</td>
<td>5302</td>
<td>5302</td>
</tr>
<tr>
<td>Day 5</td>
<td>4758</td>
<td>4758</td>
</tr>
<tr>
<td>Day 6</td>
<td>5351</td>
<td>5351</td>
</tr>
<tr>
<td>Day 7</td>
<td>5468</td>
<td>5468</td>
</tr>
<tr>
<td>Average</td>
<td>4310</td>
<td>4310</td>
</tr>
</tbody>
</table>
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