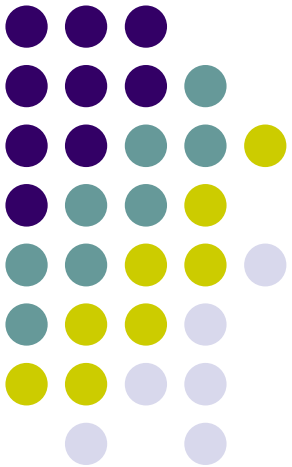
5th European conference on Wireless Sensor Networks
EWSN 2008

Piotr Szczechowiak

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor Networks



30.01.2008 – 01.02.2008 Bologna, Italy

Acknowledgements

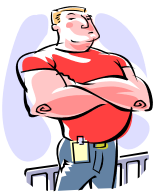
- Michael Scott
- Leonardo B. Oliveira
- Martin Collier
- Ricardo Dahab

Overview

- Introduction
- Elliptic Curve Cryptography
- Pairings
- WSN scenario
- Implementation and challenges
- Results and future work

WSN security requirements

- New and present WSN applications require reliable security mechanisms
- We need:
  - Information privacy
  - Entity authentication
  - Data integrity
  - Access control



Asymmetric cryptography

- Symmetric vs asymmetric crypto
- Asymmetric crypto too heavyweight?
- Constraints for PKC in WSN
- Benefits of using PKC
- RSA implementation for WSN's

Levels of security

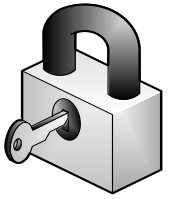
Key size comparison between symmetric, RSA and Elliptic Curve systems for equivalent level of security

Security level (bits)	80	112	128	192	256
Block cipher	SKIPJACK	3-DES	AES-Small	AES-Medium	AES-Large
EC parameter p	160	224	256	384	512
RSA modulus n	1024	2048	3072	8192	15360

***source: D. Hankerson, A. Menezes, S. Vanstone „Guide to elliptic curve Cryptography"**

Elliptic Curve Cryptography

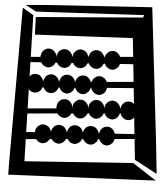
- Proposed by N. Koblitz and V. Miller in 1985
- Security based on ECDLP
- No subexponentional algorithms to solve ECDLP
- Smaller key sizes
- More complex than standard systems



DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

Finite field arithmetic

- Arithmetics over *GF(p)* and *GF(2^m)*
- For *GF(p)* multiplication, reduction, squaring, addition and subtraction were implemented in assembly language on Atmega128 and MSP430



Finite field arithmetic

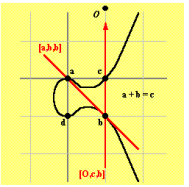
Timings in instruction cycles for basic arithmetic operations using 160-bit integers

	ATmega	MSP430
hybrid multiplication	2654 (d=4)	1746 (d=2)
squaring	2193 (d=4)	1373 (d=2)
modular reduction	1228	990
modular addition	340-470	105-235
modular subtraction	340-470	105-235

***modular reduction algorithm takes advantage of special form of the modulus**

Elliptic curve operations

- Point representation - coordinates systems
- Point addition and doubling
- Scalar point multiplication *s*P
- This is the time critical operation that requires optimization
- If P is fixed we can use precomputation to speed up the calculations



Pairings

- A new idea in cryptography
- To calculate pairings we need efficient algorithms and suitable elliptic curves
- Pairing is denoted as $\hat{e}(P,Q)$ where P and Q are points on an elliptic curve
- It has the property of bilinearity

$$\hat{e}(aP,bQ) = \hat{e}(bP,aQ) = \hat{e}(P,Q)^{ab}$$

Hard problems

- Given aP and P it is hard to find a
- Given $\hat{e}(P,Q)^a$ and $\hat{e}(P,Q)$ it is hard to find a
- Pairing based crypto is more flexible than methods based on integer factorisation and discrete logarithm
- Identity Base Encryption and other interesting schemes are now possible

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

How can we use pairings?

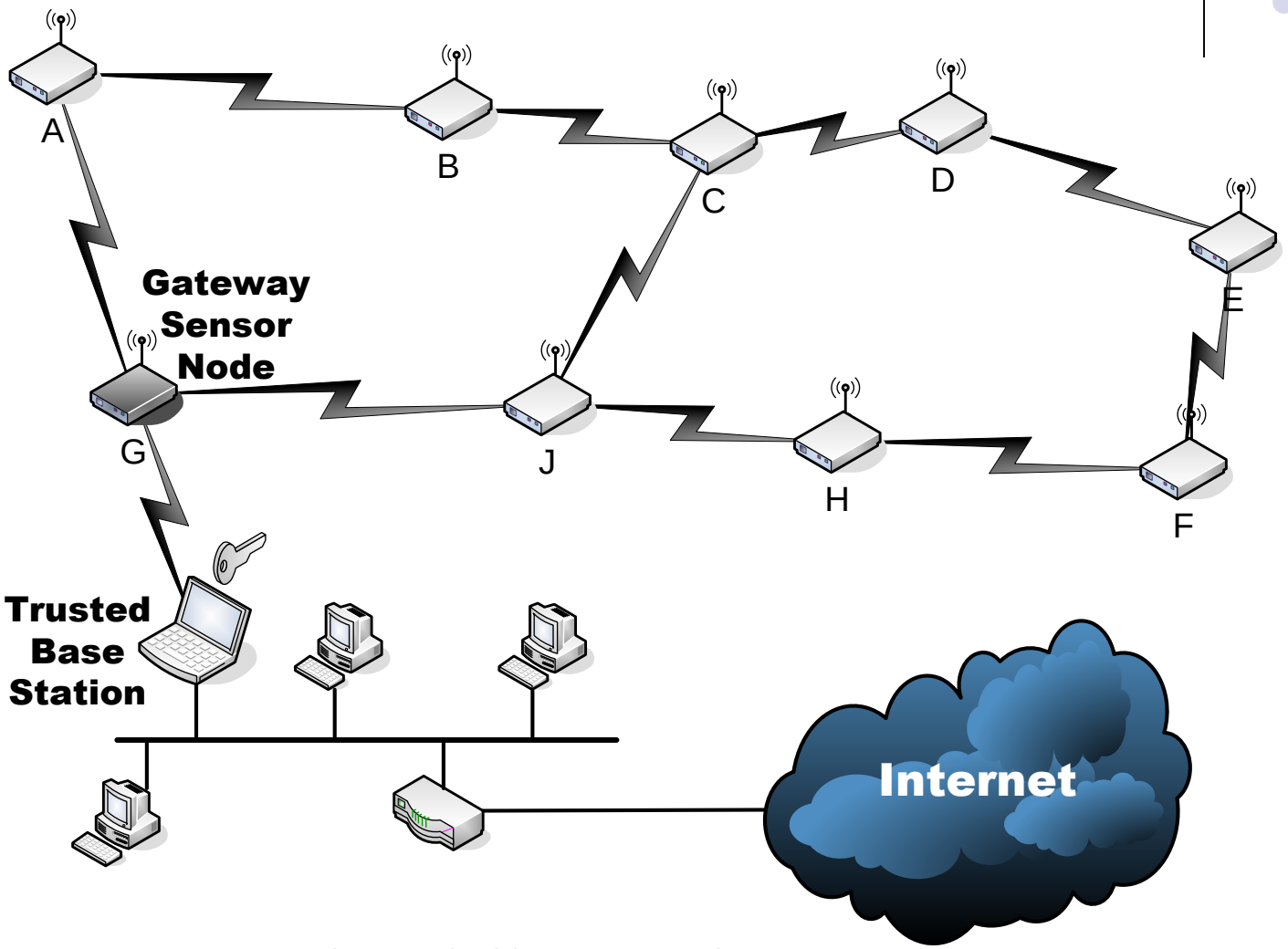
- Simple protocol (Sakai-Oghishi-Kasahara)
- trusted authority with secret *s* give Alice *s*A, where A is her ID hashed to a curve point
- The trusted authority gives Bob *s*B
- Alice and Bob share a common key now:

$$\hat{e}(A,sB)=\hat{e}(B,sA)$$

- No interaction required!

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

WSN Scenario



Implementation

- Tmote sky: IEEE 802.15.4 module
- Key features:
  - 250kbps, 2.4Ghz Wireless Transceiver
  - 16bit, 8Mhz, TI MSP430 microcontroller
  - 10kB RAM, 48kB ROM, 1MB external
  - Ultra low current consumption
  - Hardware multiplier unit on MSP430

Implementation

- MICA2: most popular research platform in Wireless Sensor Networks
- Key features:
  - 38.4kbps, 868/916 MHz radio
  - 8bit, 7.38Mhz, ATMEL ATmega128L
  - 4kB RAM, 128kB ROM, 512kB external
  - Low current consumption

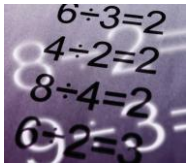
Challenges

- Efficient implementation of complex cryptographic functions
- Very small amount of memory ROM/RAM
- Portability for various WSN platforms
- Limited CPU capabilities
- Low battery capacity: 1 Month – 1 Year
- Computation time should be as short as possible

Results

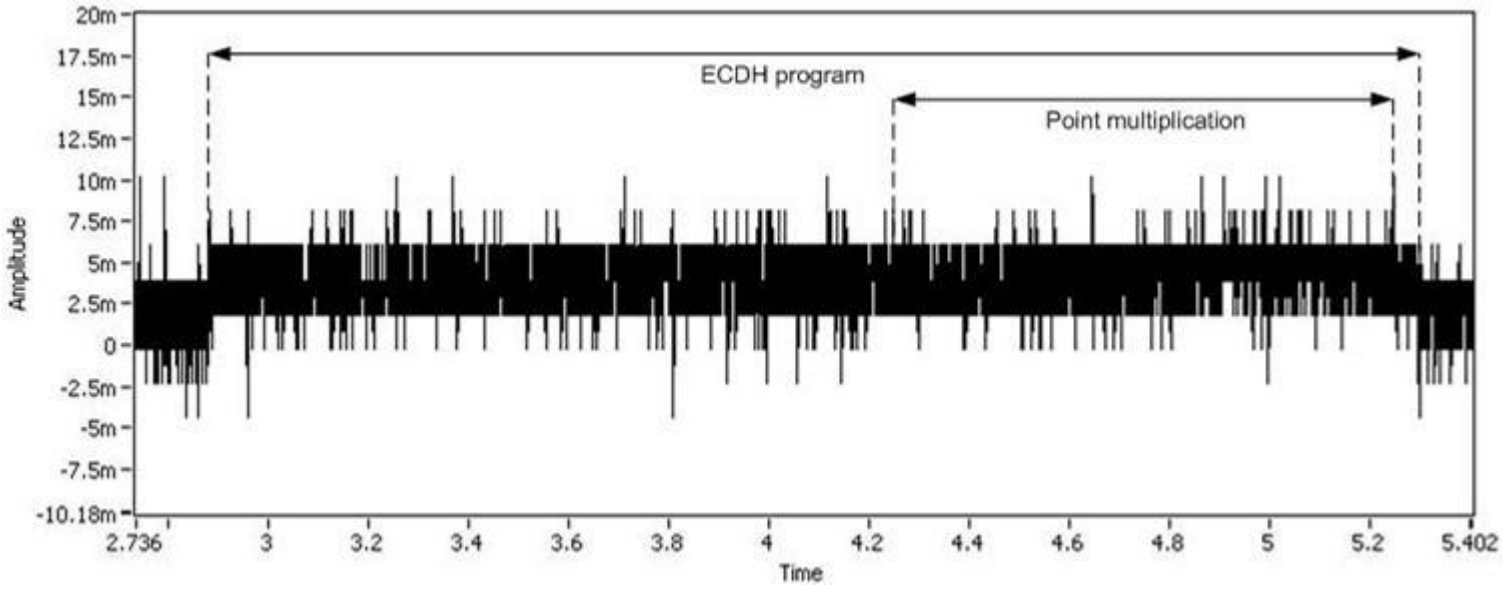
Performance of point multiplication using 160bit curve over the prime field and 163bit curve over the binary field

	MICA2		Tmote Sky	
	Binary field	Prime field	Binary field	Prime field
Computation time	2.16s	1.27s	1.04s	0.72s
Current draw	7.86mA	7.88mA	3.45mA	3.68mA
Energy consumption	50.93mJ	30.02mJ	10.76mJ	7.95mJ
ROM	32.4KB	46.1KB	32.1KB	31.3KB
RAM	1.7KB	1.8KB	2.8KB	2.9KB



Energy consumption

Current levels on Tmote Sky during example ECDH program execution



Pairings implementation

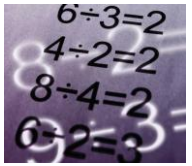
- In binary field: η_T one of the fastest known pairings k=4, GF(2^{271})
- On Tmote Sky: k=4 Tate pairing with p 256-bit prime, no precomputation
- On MICA2: k=4 Ate pairing over a non-supersingular curve with 256-bit prime 28KB of precomputation data

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

Results

Results for pairing implementation over prime and binary fields on both MICA2 and Tmote Sky paltforms

	MICA2		Tmote Sky	
	Binary field	Prime field	Binary field	Prime field
Computation time	10.96s	17.93s	5.25s	11.82s
Current draw	7.86mA	7.88mA	3.45mA	3.68mA
Energy consumption	258.44mA	423.87mJ	54.34mJ	130.49mA
ROM	53.5KB	71.9KB	30.3KB	47.0KB
RAM	2.8KB	2.5KB	3.7KB	3.0KB



Summary

- WSN's need lightweight cryptosystem
- ECC can help achieve this goal
- We have implemented all basic ECC primitives on 8 and 16bit platforms
- Pairings can be calculated in as fast as 5s
- With pairings new cryptographic schemes are possible

Research possibilities

- Further primitive optimization in terms of speed and memory usage
- Full implementation of a pairings based security protocol
- More powerful motes open new possibilities
- Crosslayer optimisation of security protocols

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

Thank you for your attention