Piotr Szczechowiak

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

Efficient Implementation of ECC and PBC on Wireless Sensor Networks

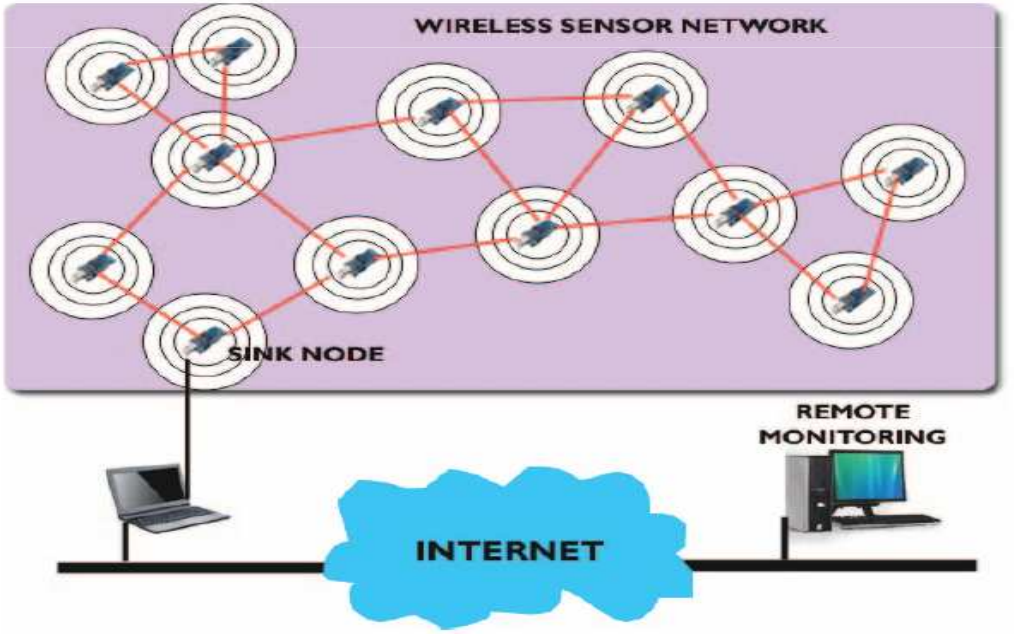
Overview

- Introduction
- Security in WSN
- WSN applications
- WSN motes
- Implementing ECC
- Pairing based protocols on motes
- Conclusions

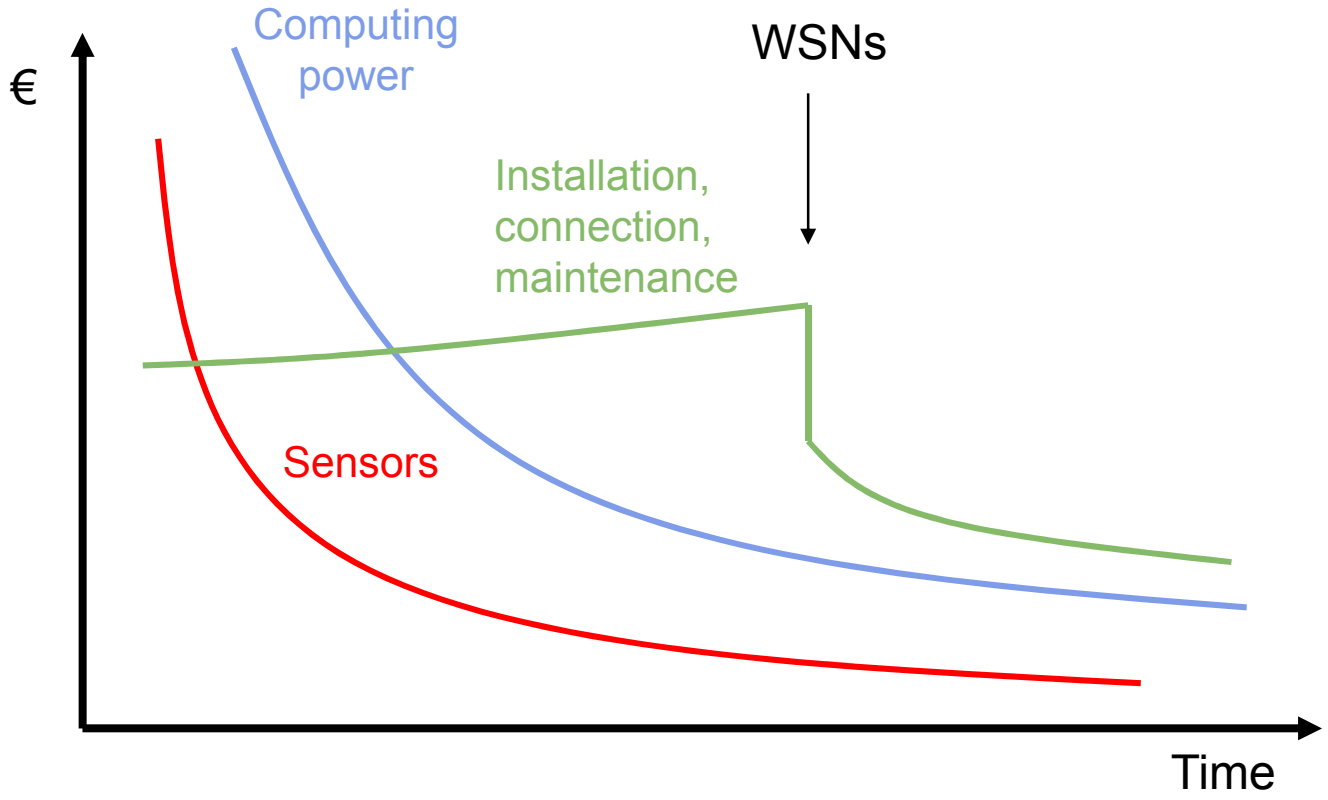
DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

WSN

- WSN is a wireless network of spatially distributed autonomous devices that uses sensors to cooperatively monitor physical/environmental conditions (temp, sound humidity, vibration, motion, etc.) at different locations



Why wireless sensors?

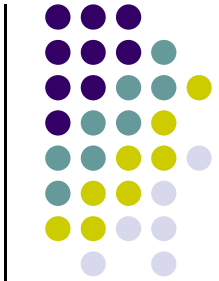


DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

Barriers for WSN widespread

1) Reliability (RF nature, software, security)
2) Standards (IEEE 802.15.4, Zigbee, Wireless HEART, ISA SP100)
3) Ease of use
4) Power consumption
5) Development cycle
6) Node size

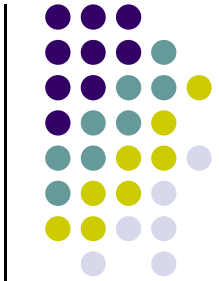
Motivation



- Security is one of the major problems in WSNs
- Future WSN applications ("internet of things") will need new lightweight and reliable security mechanisms
- Broad range of hardware platforms makes it difficult to design a universal security architecture
- Various applications require different security techniques and security levels

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

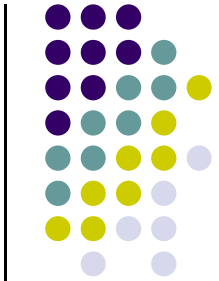
Present WSN security



- Security solutions in already deployed networks are insufficient (only symmetric cryptography solutions)
- Most of deployed networks uses 128-bit AES symmetric key encryption for end-to-end data confidentiality
- One common key for the whole network
- Network is compromised when the secret key of any of the nodes is revealed
- Limited security comparing to PKC

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

PKC for WSNs



- PKI can solve the problems of symmetric cryptography solutions
- No practical PKI scheme was developed for WSNs so far
- Traditional Public-key systems are too expensive and too complex for WSNs
- PKC based on ECC and pairings may become a security solution for the more demanding WSN applications

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

WSN application classes

Building automation

- Sensors plus inteligent control
- HVAC, security, lightning control, access control, building energy usage reduction

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

BUILDING AUTOMATION

Health care

- Security and privacy biggest problem
- Patient monitoring, fitness monitoring, diseases detection in open air

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

PERSONAL HEALTH CARE

Industrial monitoring

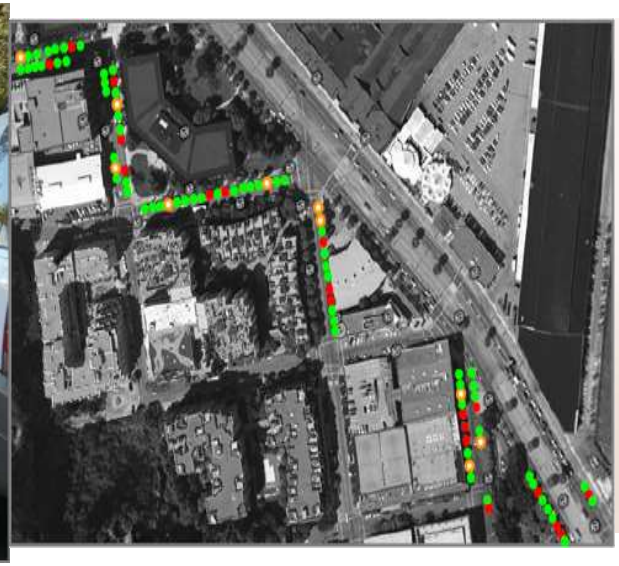
- Asset & energy management, process control
- Oil & gas refineries, remote measuring systems, assembly lines, infrastructures monitoring

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

INDUSTRIAL/ INFRASTRUCTURE MONITORING

Residential/commercial control

- Home lighting and security control, AMR
- Parking monitoring, energy management in supermarkets, traffic monitoring and control



DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

RESIDENTIAL/
COMMERCIAL
LIGHT/SECURITY
CONTROL

Military

- Security has the highest priority
- Intruder detection, perimeter security, national security, equipment monitoring

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

MILITARY

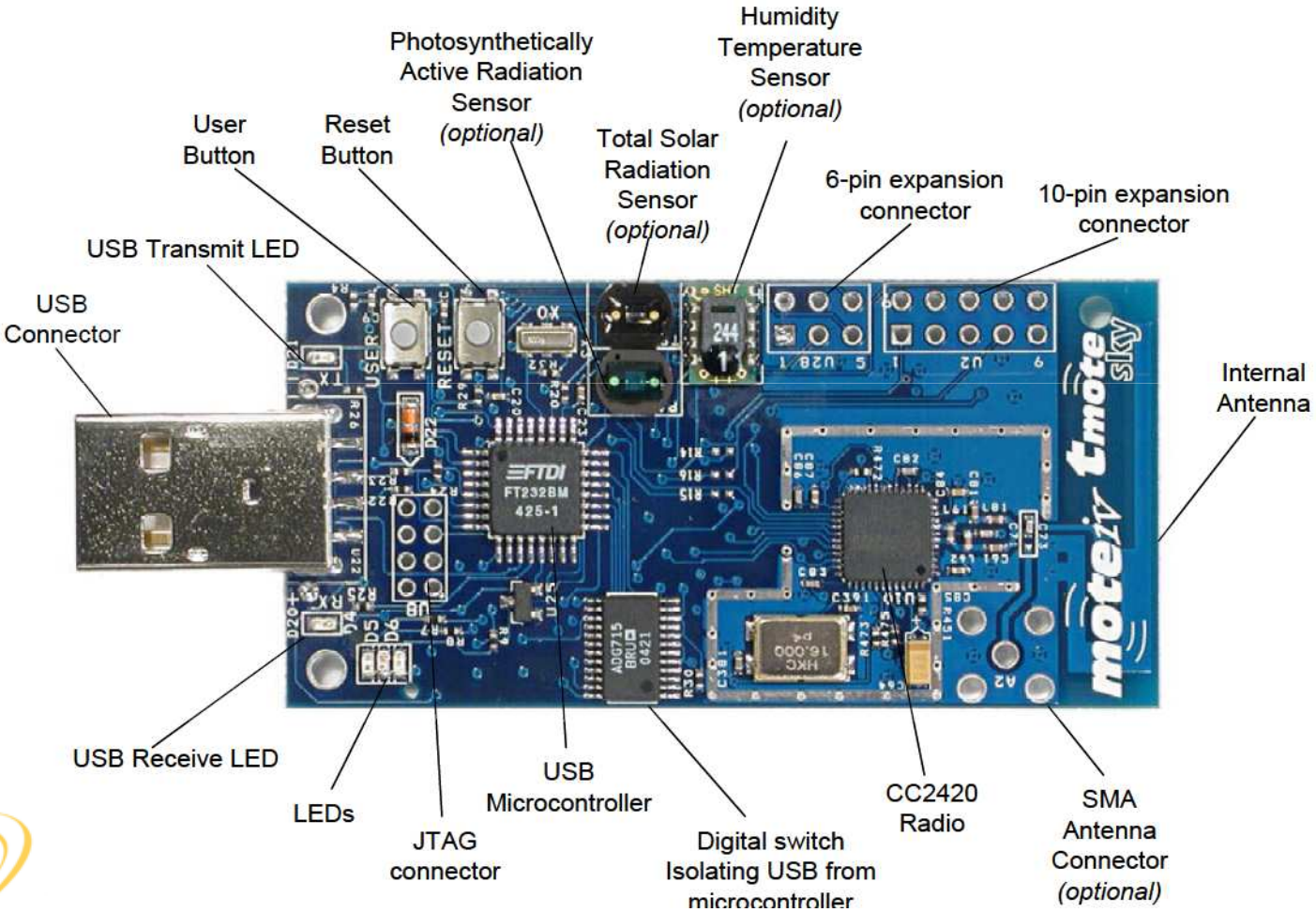
Enivronmental monitoring

- Deployments in open areas
- Wildfire detection, habitat monitoring, precision agriculture, µclimate monitoring

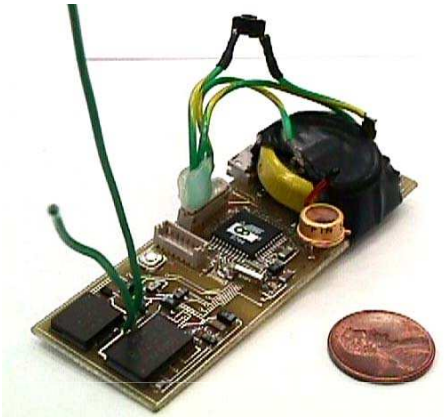
DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

ENVIRONMENTAL MONITORING

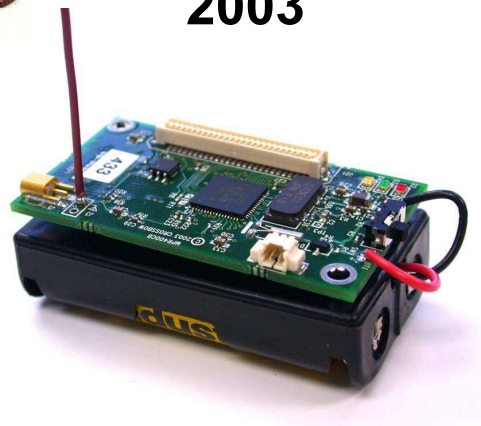
WSN motes



Motes 2000-2009



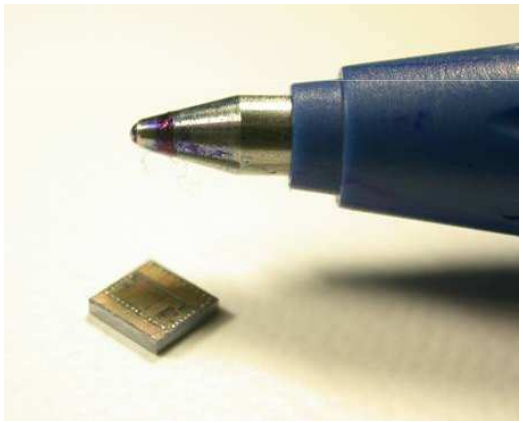
2000



2003

2009

Future



DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

WSN motes

- 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

WSN motes

- 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

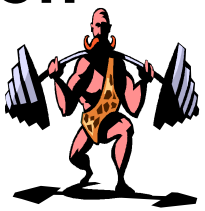
WSN motes

- Imote2: high spec WSN module
- Key features:
  - 250kbps, 2.4Ghz Wireless Transceiver
  - 32bit, 13-416MHz, Intel PXA271 CPU
  - 256kB SRAM, 32MB SDRAM, 32MB flash
  - DSP coprocessor for multimedia data
  - Moderate current consumption

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

Programming WSNs

- TinyOs operating system and nesC language
- No IDEs available, make-file programming
- Debugging difficult (JTAG, LEDs)
- Tendency to move to JAVA programming
- Limited memory – stack overflows
- Simulating environments for processors exist and allow cycle accurate simulation



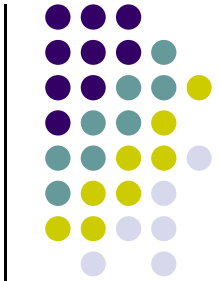
DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

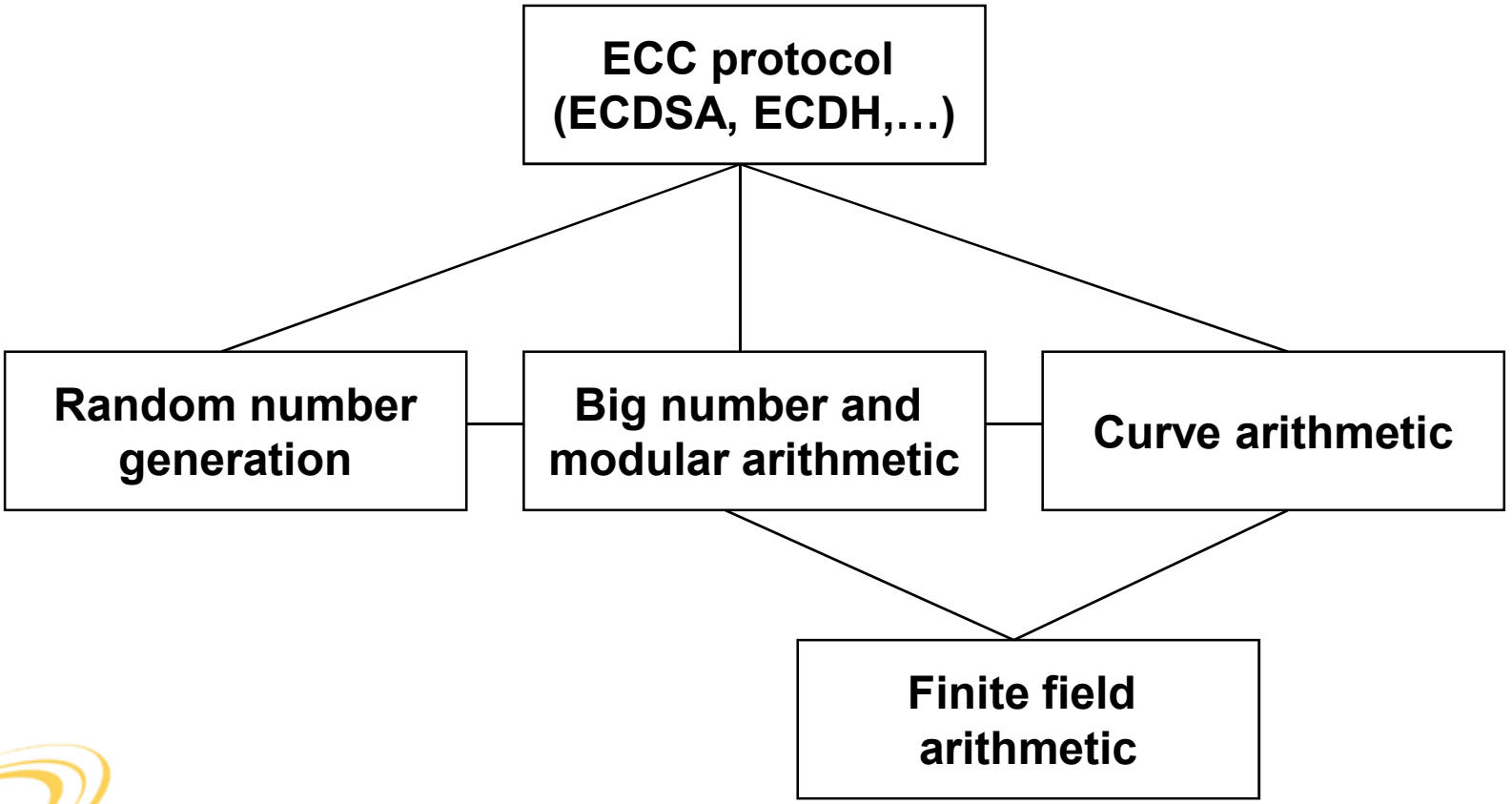
Implementation challenges

- 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

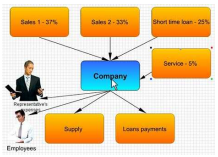
DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

Implementing ECC

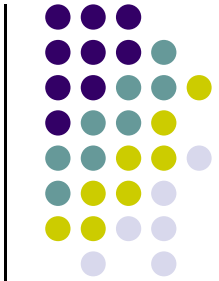




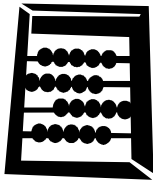
DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath



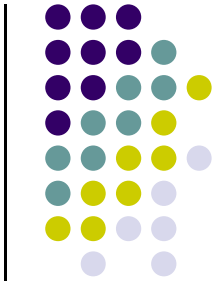
Finite field arithmetic



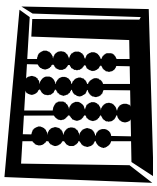
- Arithmetics over *GF(p)* and *GF(2^m)*
- For *GF(p)* multiplication, reduction, squaring, addition and subtraction implemented in assembly language
- Assembly routines generated automatically from user defined macros (MIRACL utility program)
- Memory allocation for big numbers exclusively from the stack



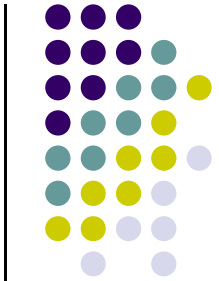
Hybrid multiplication



- Standard methods have redundant memory reads/writes for calculation of partial products
- Combines row-wise and column-wise multiplication methods
- Takes advantage of additional registers to store the temporary result
- Unnecessary memory operations are avoided
- Efficiency rises with no. of registers used



Finite field arithmetic



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

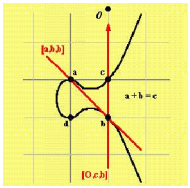
	ATmega	MSP430
hybrid multiplication	2654 (d=4)	1746 (d=2)
squaring	2193 (d=4)	1373 (d=2)
modular reduction	1228	990
modular addition	340-470	105-235
modular subtraction	340-470	105-235

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

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

Elliptic curve operations

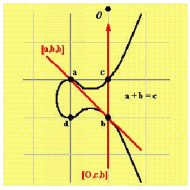
- Point representation - coordinates systems
- Point addition and doubling
- Scalar point multiplication *s*P
- This is the time critical operation that requires optimization
- If P is fixed we can use precomputation to speed up the calculations



DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

ECC implementations

- NIST k-163 Koblitz curve over $GF(2^{163})$ - no expensive point doublings required for point mul.
- $y^2=x^3-3x+157$, $p=2^{160}-2^{112}+2^{64}+1$ Solinas prime
- -3 coefficient set to reduce the number of operations in point doubling routine
- NAFs and projective coordinates
- Precomputation with window width 4



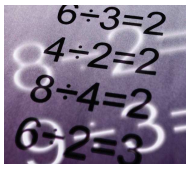
DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

Point multiplication results

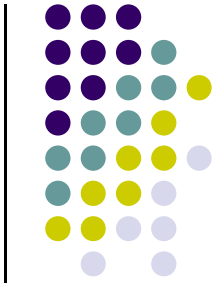
Performance of point multiplication using 160bit curve over the prime field and 163bit curve over the binary field

	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

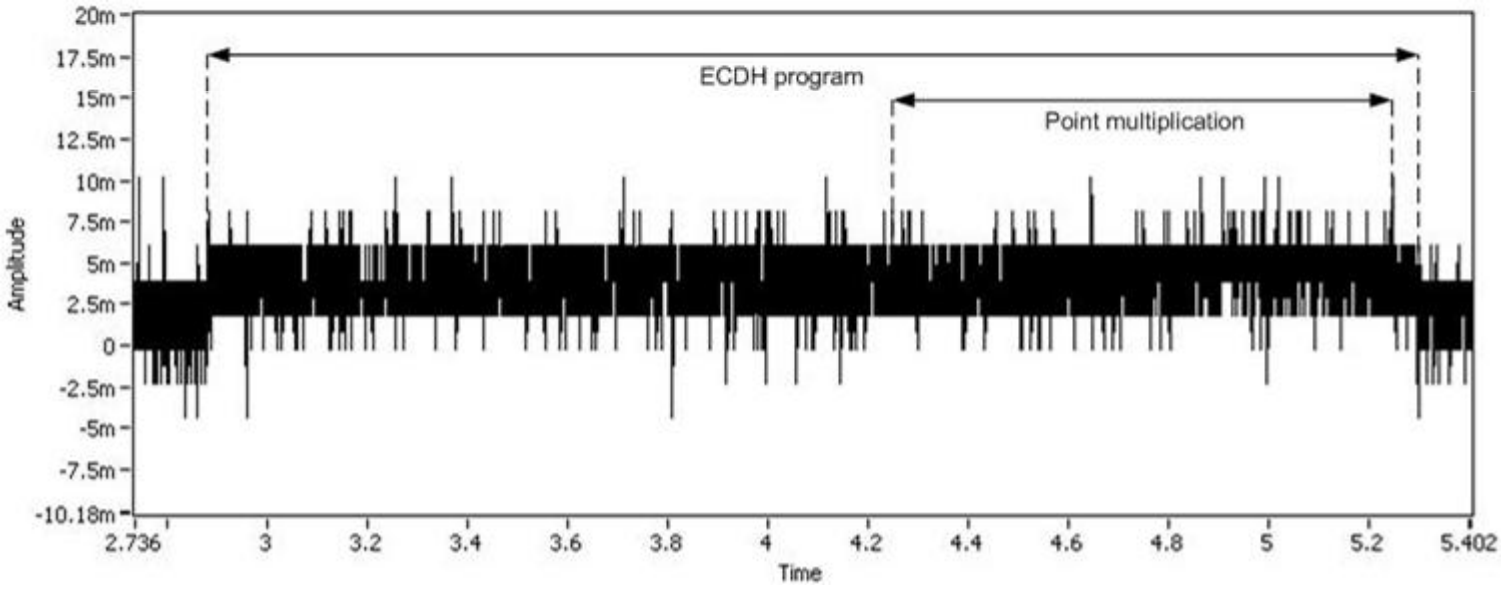
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath



Energy consumption



Current levels on Tmote Sky during example ECDH program execution



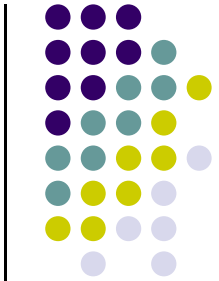
DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

Pairing-based crypto

- A new idea in Public Key Cryptography
- Traditional Public-key systems like RSA are too expensive for WSNs
- Pairing-based crypto is more flexible than methods based on integer factorisation and discrete logarithm
- Pairings facilitates creation of novel protocols (IBE)
- To calculate pairings we need efficient algorithms and suitable elliptic curves

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

Pairing-based crypto



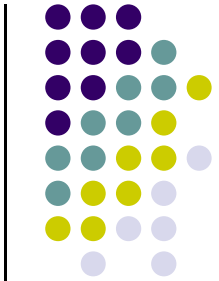
- Pairing is denoted as $\hat{e}(P,Q)$ where P and Q are points on an elliptic curve
- It has the property of bilinearity

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

- 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

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

Application to WSN security



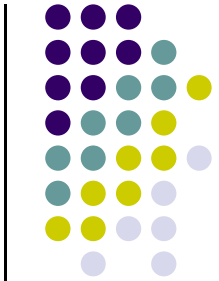
- Simple protocol (Sakai-Oghishi-Kasahara)
- Original network deployer has a secret *s* and issues node A with *sA*, where A is node's ID hashed to a curve point
- Node B is issued with secret key *sB*
- Both nodes share a common key now:

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

- No interaction required!

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

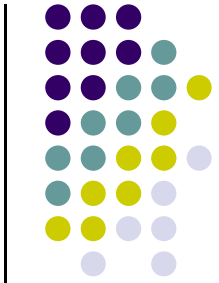
Advantages



- Nodes communication limited to minimum – energy savings on expensive radio transmission
- Simplified key infrastructure
- Scalability to large numbers of nodes in the network
- Simple addition of new nodes
- Resistance against physical node capture
- High complexity – implementation challenge, performance issues

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

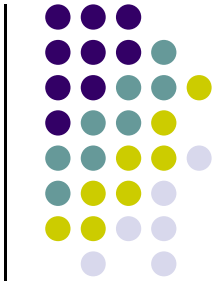
Pairings implementation



- In the binary field η_T is one of the fastest known pairings (trunkated Miller's loop)
- In our implementation, $y^2+y=x^3+x$ supersingular curve over GF(2^{271}), k=4
- In the prime field we implemented the Tate pairing over a non-supersingular MNT curve $y^2=x^3-3x+B$, k=4, GF(p), p - 160 bit prime
- Type 3 pairing – application in more demanding WSNs

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

Pairings implementation



- Implementation based on the MIRACL library
- Large integers and binary polynomials multiplication – the most time-critical arithmetic routines
- The efficiency of these operations has a crucial influence on the overall pairing performance
- Multiplication implementation in assembly language gives 50%-70% decrease in pairing execution time

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

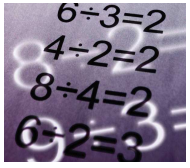
Pairing results

Results for pairing implementation over prime and binary fields on MICA2 Tmote Sky and Imote2 platforms

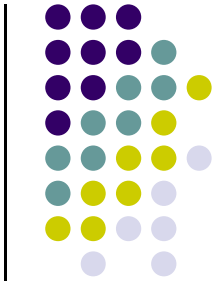
	MICA2		Tmote Sky		Imote2 (13MHz)		Imote2 (104MHz)	
	$\eta_T(P,Q)$	$e(P,Q)$	$\eta_T(P,Q)$	$e(P,Q)$	$\eta_T(P,Q)$	$e(P,Q)$	$\eta_T(P,Q)$	$e(P,Q)$
Timing	2.66s	7.43s	1.71s	4.61s	0.46s	0.62s	0.06s	0.08s
ROM	47.41KB	60.91KB	23.66KB	34.88KB	29.55KB	44.40KB	29.55KB	44.40KB
STACK	3.17KB	3.39KB	4.17KB	3.39KB	4.12KB	3.75KB	4.12KB	3.75KB
Current draw	7.86mA	7.88mA	3.45mA	3.68mA	31mA*	31mA*	66mA*	66mA*
Energy usage	62.73mJ	175.65mJ	17.70mJ	50.89mJ	12.12mJ	16.34mJ	3.76mJ	5.02mJ

* - manufacturer data

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath



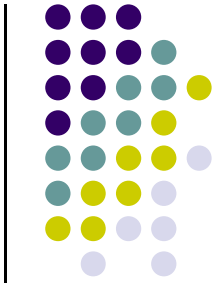
Conclusions



- In WSNs CPU capabilities, memory and energy resources are very limited (lightweight cryptosystem needed)
- Most of the WSN applications require high level of security – existing solutions are insufficient
- With pairings now viable on mote platforms new cryptographic schemes are possible
- Security parameters should be set just beyond current published broken records to achieve a secure system

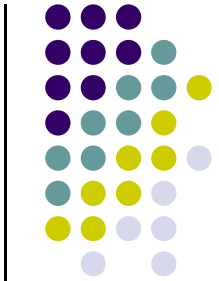
DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath

Conclusions



- ECC and PBC can help provide appropriate security levels in sensor networks
- We have tested the viability of software implementation of basic ECC and PBC primitives on different 8, 16 and 32 bit platforms
- Pairings can be calculated in as fast as 2.66s on a tiny 8-bit WSN mote (time comperable with point mul.)
- For commercial large scale deployments pairings implementation in hardware would by more beneficial

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath



Thank you for your attention

DCU
Dublin City University
Ollscoil Chathair Bhaile Átha Cliath