New Crypto Algorithms (and Protocols) for Sensor Networks

Ricardo Dahab

IC - UNICAMP

(joint work with Leonardo Oliveira et al.)

Outline

- Introduction
- Security
- Goals
- Proposal
- Results
- Conclusion

Wireless Sensor Networks

NETWORKWORLD

New frontier for wirele
Sensor networks

Smart Sensors to Network the World

PC
PCMAG.COM

Meet NASA's Sensor Web

Security sensor market tops $420 million annually

SRI Consulting Business Intelligence

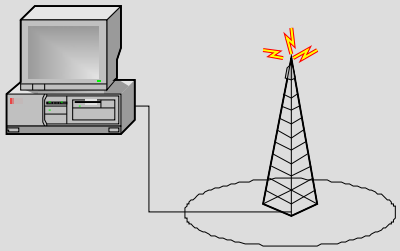
Meshed Sensor Networks

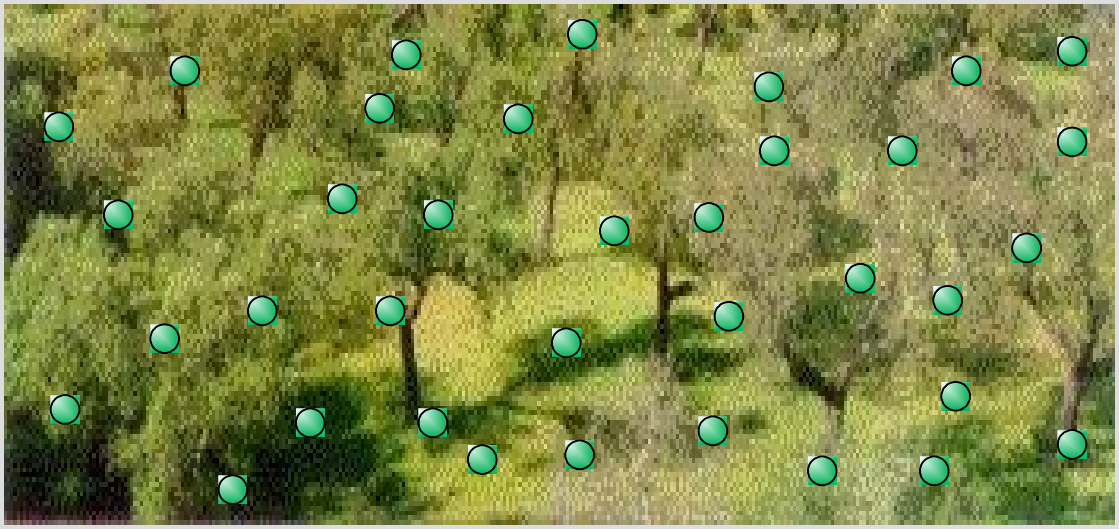
Deployment

- Tens of thousands of nodes are deployed in an *area of interest*

Setup

- Collected data is sent to the Base Station node.





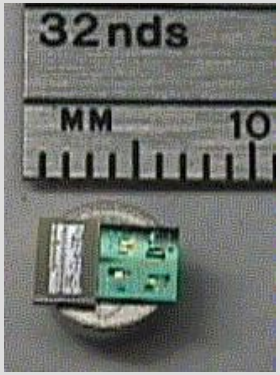
Sensor Node

Non-reusable ➡ low cost ➡ low resource

- E.g. MICAz Motes
  - 8-bit/7.38MHz CPU
  - 4KB SRAM, 128KB *flash*

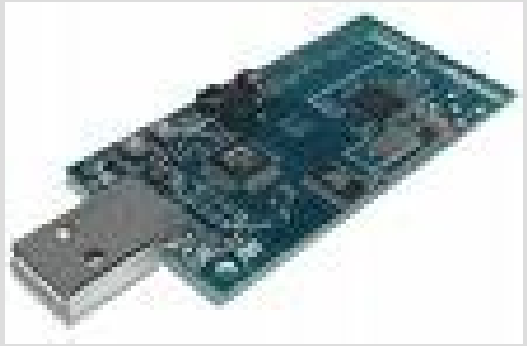
Popular Nodes

I(ntel)Mote (XScale/ARM)



Smart Dust

MICA Motes



TelosB (16-bit/8-MHz)

Sensor web

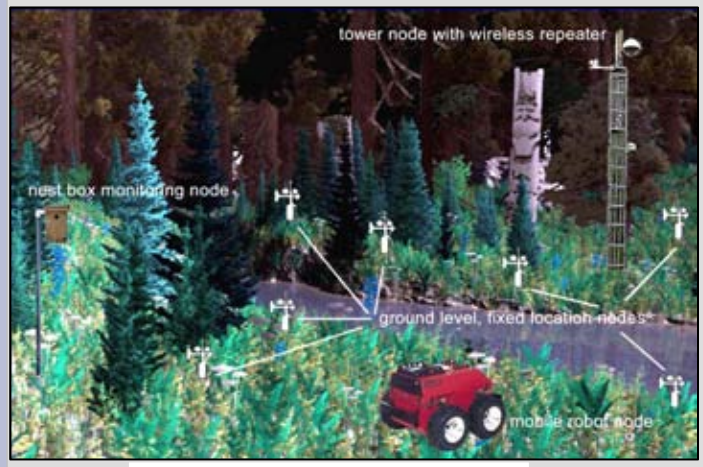
Applications

ANA
AGÊNCIA NACIONAL DE ÁGUAS
Declaração Anual de Uso de Recursos Hídricos

River monitoring

Interplanetary

Health Care



Ecosystem

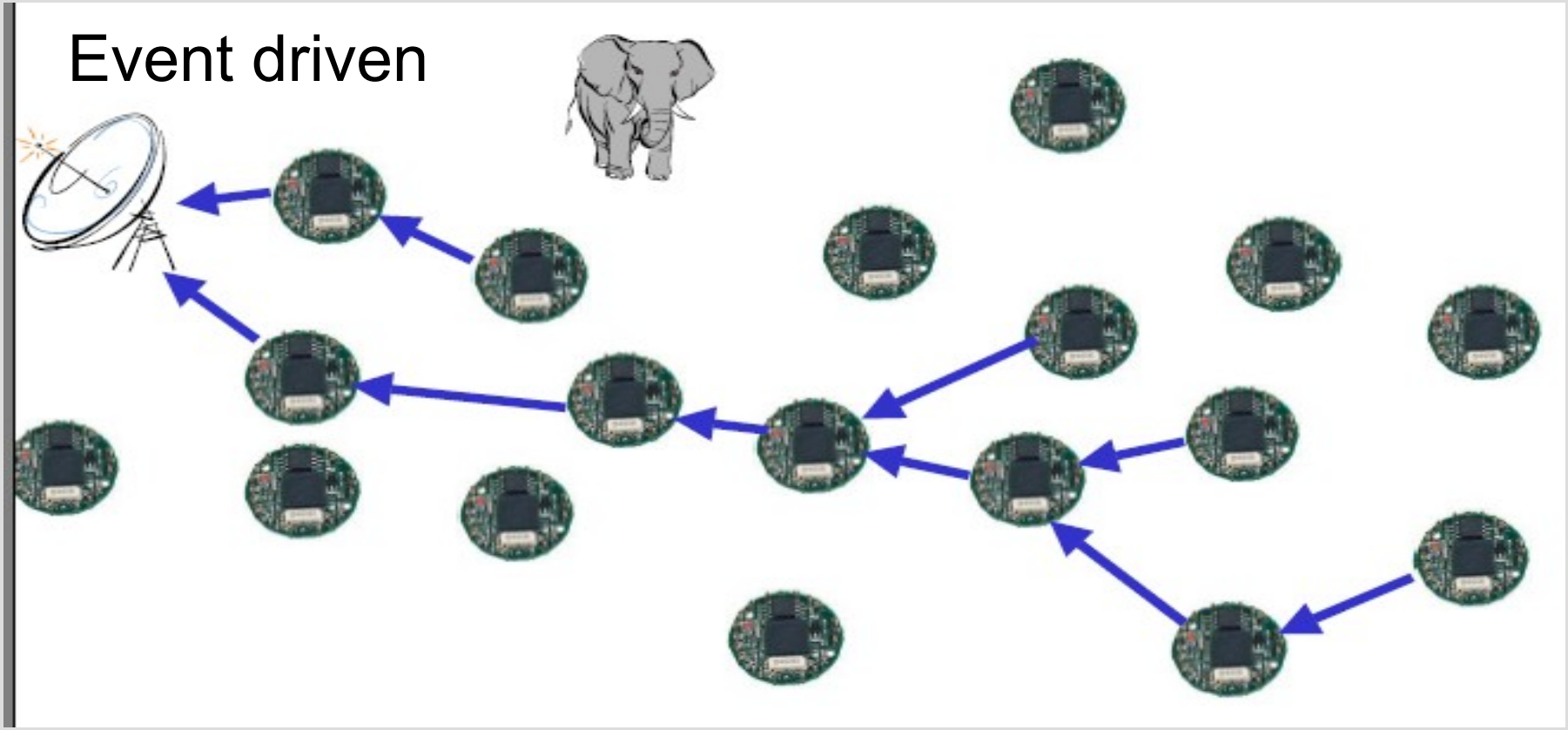
Great Duck Island

Air monitoring

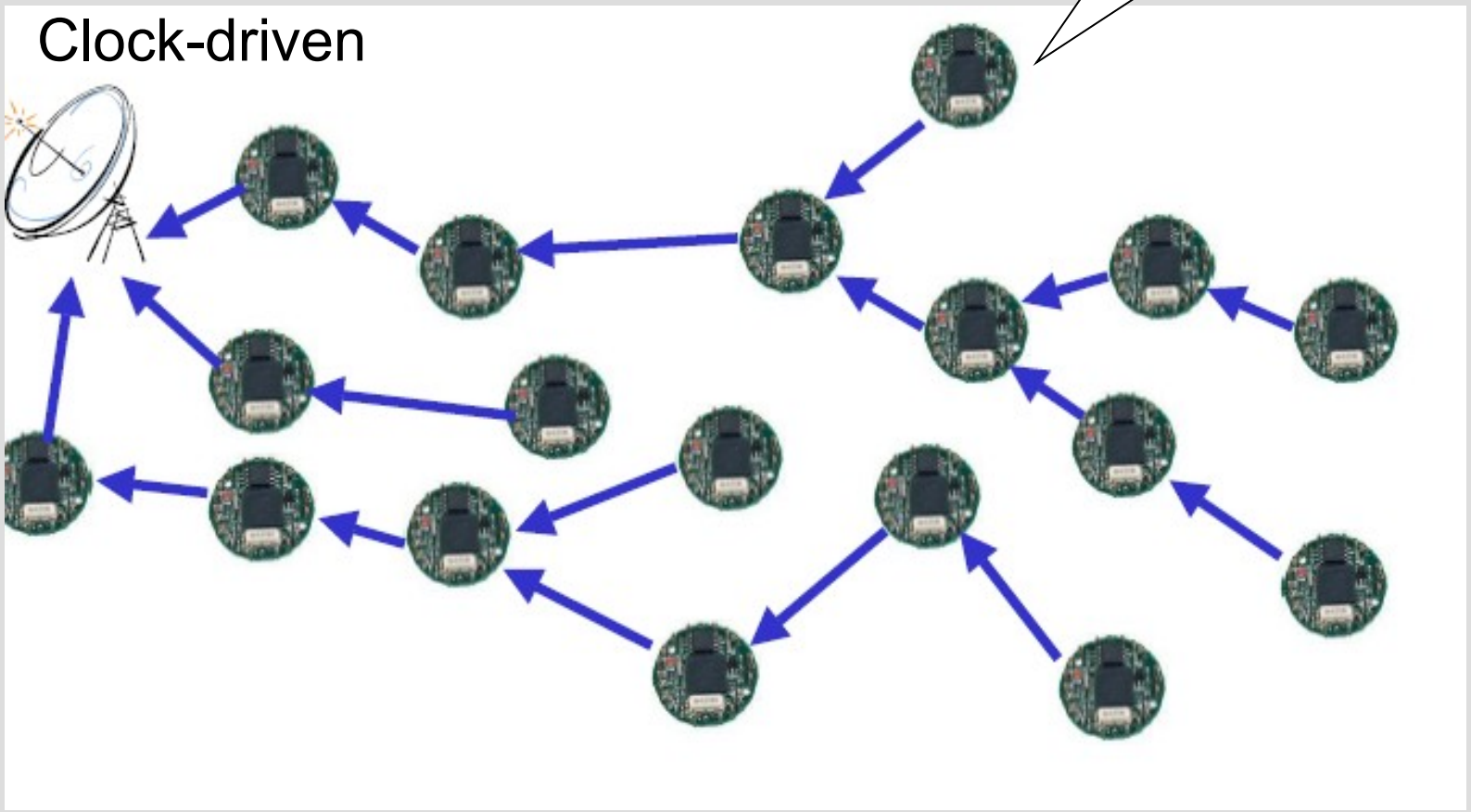
WSN vs MANETs

- Subclass of MANETs
- Nodes are quite static
- Do not possess PDA-level resources
- Communication is asymmetric
  - Mainly from nodes to Base Station
- Short lifetime
  - No battery recharge/replacement

Operation



Operation



Organization

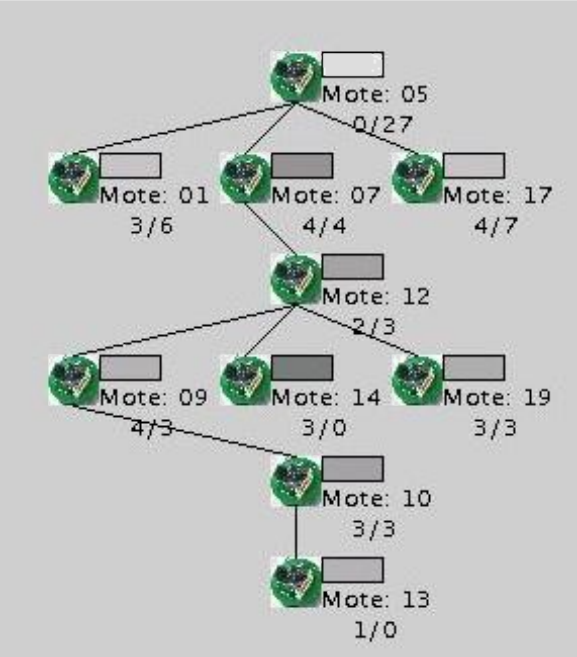
- Flat networks
  - Nodes play identical roles
- Hierarchical networks
  - Organized into clusters
  - Ordinary nodes and cluster-heads play different roles

Organization

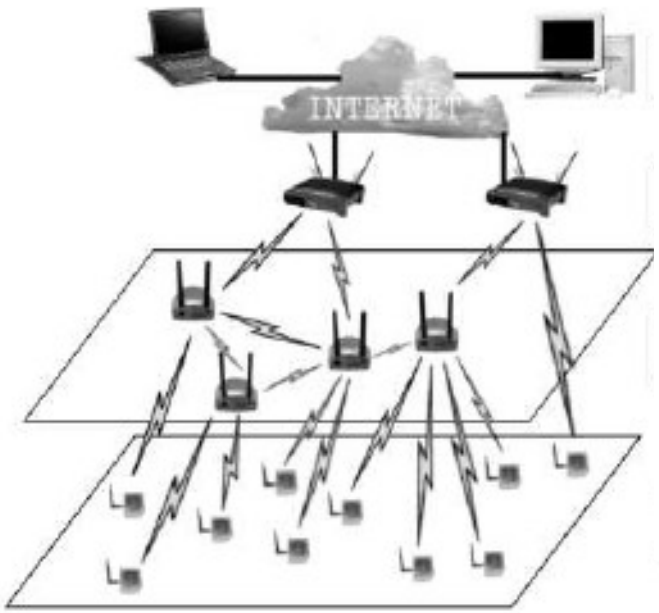
- Homogeneous networks
  - Nodes are endowed w/ equivalent hardware
- Heterogeneous networks
  - Nodes are endowed w/ different hardware

Organization

Flat and homogeneous



Hierarchical and heterogeneous



Challenge

Wireless communication, scarcity of resources, hostile environments

Broken Paradigm

The need for new approaches on

- E.g. communication, localization, security, data management, and fault management, etc.

Outline

- Introduction
- Security
- Goals
- Proposal
- Results
- Conclusion

Security in WSNs

Security problems in WSNs

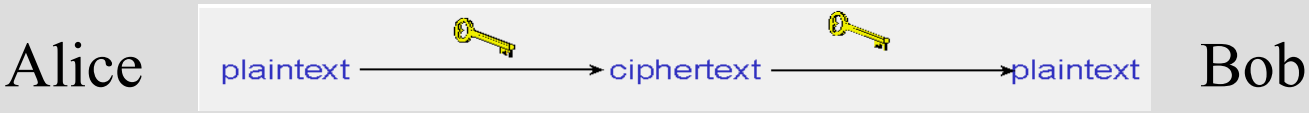
- Security solutions are bootstrapped through key distribution schemes
- Problem: traditional methods of key distribution
  - Symmetric cryptosystems
  - Public key cryptosystems (PKC)

  are inadequate for WSNs

Why conventional symmetric cryptosystems are inadequate

Symmetric Cryptosystems

- Nodes use shared secret keys to communicate
  - The same key is used to encrypt and decrypt data



- Is attractive to WSNs because of its energy efficiency

Problem

How to setup secret keys between communicating nodes?

Group Key

- All msgs would be encrypted using the same key
- Simple, known, and low cost solution (symmetric algorithm)

Group Key

- All msgs would be encrypted using the same key
- Simple, known, and low cost solution (symmetric algorithm)
- Problem
  - That's not robust

Group Key

- All msgs would be encrypted using the same key
- Simple, known, and low cost solution (symmetric algorithm)
- Problem
  - That's not robust

Once a node is compromised,
the whole network is compromised as well

Pairwise Secret Key

- Assigns a key for each pair of nodes
- Solves the problem of robustness
- Problem
  - Scalability
    - Nodes share a key w/ every other network node

Proposals for WSNs

- Use key predistribution schemes
  - Keys are loaded into nodes prior deployment
- Ideal when neighborhood is known a priori

Proposals for WSNs

- Use key predistribution schemes
  - Keys are loaded into nodes prior deployment
- Ideal when neighborhood is known a priori

Exception, not a rule

Why conventional public key cryptosystems are inadequate

Public Key Cryptosystems

- Each node carries only a pair of keys
  - A public and a private key
- Public keys are used to encrypt and private keys to decrypt data

Public Key Cryptosystems

- Each node carries only a pair of keys
  - A public and a private key
- Public keys are used to encrypt and private keys to decrypt data

Problem

- Conventional PKC has prohibitive costs!

Proposals for WSNs

- Adequate conventional algorithms to sensor nodes
- Employ more efficient techniques
  - E.g. elliptic curve cryptography

Problem

- Public key authentication is still required

Expensive!

Public Key Authentication

- Procedure of assuring that the pub. key of B held by A does in fact belong to B
  - Does this key really belong to Bob?
- Achieved through certificate exchange
  - E.g. PKI and Auth. Diffie-Hellman

High overhead

Certificates

- Certificate exchange
  - Communication overhead
- Certificate storage
  - Memory overhead
- Certificate authentication
  - Computation overhead

Outline

- Introduction
- Security
- Goals
- Proposal
- Results
- Conclusion

Goals

- Give a better quality solution to the key distribution problem in WSNs
- Show how IBE can solve the key distribution problem in WSNs
- Show that IBE is indeed feasible in resource constrained nodes
  - E.g. MICAz mote

Outline

- Introduction
- Security
- Goal
- Our proposal: apply IBC in WSNs
- Results
- Conclusion

Identity-Based Cryptography

- Does not require key authentication
  - Pub. keys are derived from pub. information
  - Keys are self-authenticated
- One scenario
  - Public keys are email addresses
    - It would be known that Leo's public key would be: `leob@ic.unicamp.br`

Identity-Based Cryptography

- Does not require key authentication
  - Pub. keys are derived from pub. information
  - Keys are self-authenticated
- Scenario
  - Public keys are email addresses
    - It would be known that Leo's public key would be: leob@ic.unicamp.br

Nodes would employ IDs as self-authenticated pub keys

However, IBC...

Requires a trusted entity

Requires that private keys to be delivered over a secure channel

IBC & WSNs: Synergy

- IBC is compatible with WSNS
  - Nodes employ nodes' IDs to protect the exchange of secret keys
- And vice-versa
  - IBC requires an unconditionally trusted entity
  - But WSNs fulfill this requirement
    - The BS is (unconditionally) trusted

Can nodes afford to run IBC primitives?

Feasibility

- Evaluation of pairings is the time consuming part in IBC

Feasibility

- Evaluation of pairings is the time consuming part in IBC
- Challenge
  - Parameters are twice as big as conventional elliptic curve cryptography parameters
- We estimated the costs of evaluating pairings in a resource-constrained node
  - MICAz node

Bilinear pairings

- A map of two cyclic groups into one

$$\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$$

  that satisfies bilinearity.
- This allows for new, elegant solutions for
  - Identity-based signatures
  - Tripartite Diffie-Hellman
  - many other crypto protocols

Feasibility

- Evaluation of pairings is the time consuming part in IBC
- Challenge

  Parameters much bigger than usual parameters

TinyTate

- Tate pairing
- Prime fields
- RSA-512 security level
  - Short network lifetime
- Underlying library
  - TinyECC (Liu, Kampanakis, and Ning 2005)

MICAz mote

- 8-bit, 7.3828-MHz ATmega 128L processor
- 4 KB of primary memory (SRAM)
- 128 KB of program space (ROM)

Outline

- Introduction
- Security
- Goal
- Our proposal: IBC for sensor networks
- Results
- Conclusion

Results

Tate Pairing		
Time (seconds)	RAM (bytes)	ROM (bytes)
30.21	1,831	18,384

- 46% of RAM, 14% of ROM
- In most applications nodes will need to compute pairings only once
- *Handbook of Wireless Mesh and Sensor Networking. McGraw-Hill International, NY. (Book Chapter: accepted)*

Updated Results

- NanoECC
  - Based on MIRACL and Eta_T pairing.
- RSA-1024 security level
- 10.96s

NanoECC: *Testing the Limits of Elliptic Curve Cryptography in Sensor Networks*, European conference on Wireless Sensor Networks (EWSN'08). To appear.

Even Faster Results

About 5s and coming down

- RSA-1024 security level
- New algorithms
- Work in Progress

Outline

- Introduction
- Security
- Goals
- Proposal
- Results
- Conclusion

Conclusion

- Current key distribution solutions for WNS are not completely adequate
- IBC can be used to solve the key distribution problem in WSNs
- Results indicate that IBC is indeed feasible in resource constrained nodes

Reference

- TinyPBC: Pairings for Authenticated Identity-Based Non-Interactive Key Distribution in Sensor Networks
- Leonardo B. Oliveira and Michael Scott and Julio López and Ricardo Dahab
- Cryptology Eprint Archive, report 2007/482, avalilable at **http://eprint.iacr.org/2007/482**

Et al.

P. Szczechowiak, J. Lopez, M. Scott, M. Collier, D. Aranha, F. Daguano, E. Morais, A. Loureiro

Ongoing and future work

- Improve timings and performance in general of pairing computations
- Implement complete IBC-based key distribution protocols in sensor nodes
- Work in progress
- Code and papers available at http://www.ic.unicamp.br/~leob

Thank you!