

NSF Workshop on Wireless Security

Atlanta, GA, April 2008

# Physical-Layer Security: What next?

**João Barros**

Instituto de Telecomunicações  
Department of Computer Science  
Universidade do Porto  
and LIDS/MIT



INSTITUIÇÕES ASSOCIADAS:



INSTITUTO  
SUPERIOR  
TÉCNICO



Faculdade de Ciências  
e Tecnologia da  
Universidade de Coimbra



universidade  
de aveiro



Inovação

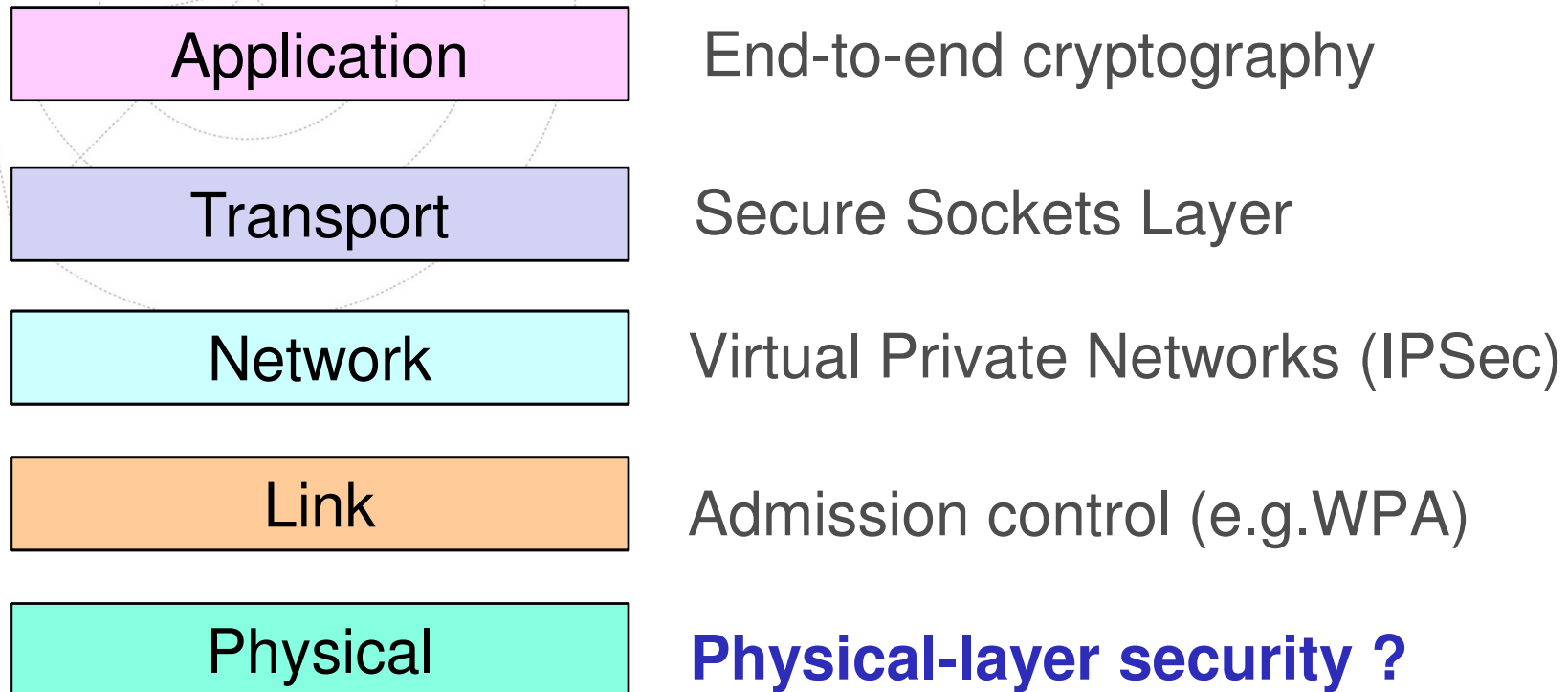


instituto de  
telecomunicações

*creating and sharing knowledge for telecommunications*

© 2005, Instituto de Telecomunicações. Todos os direitos reservados.

## Network Security: a patchwork of add-ons...

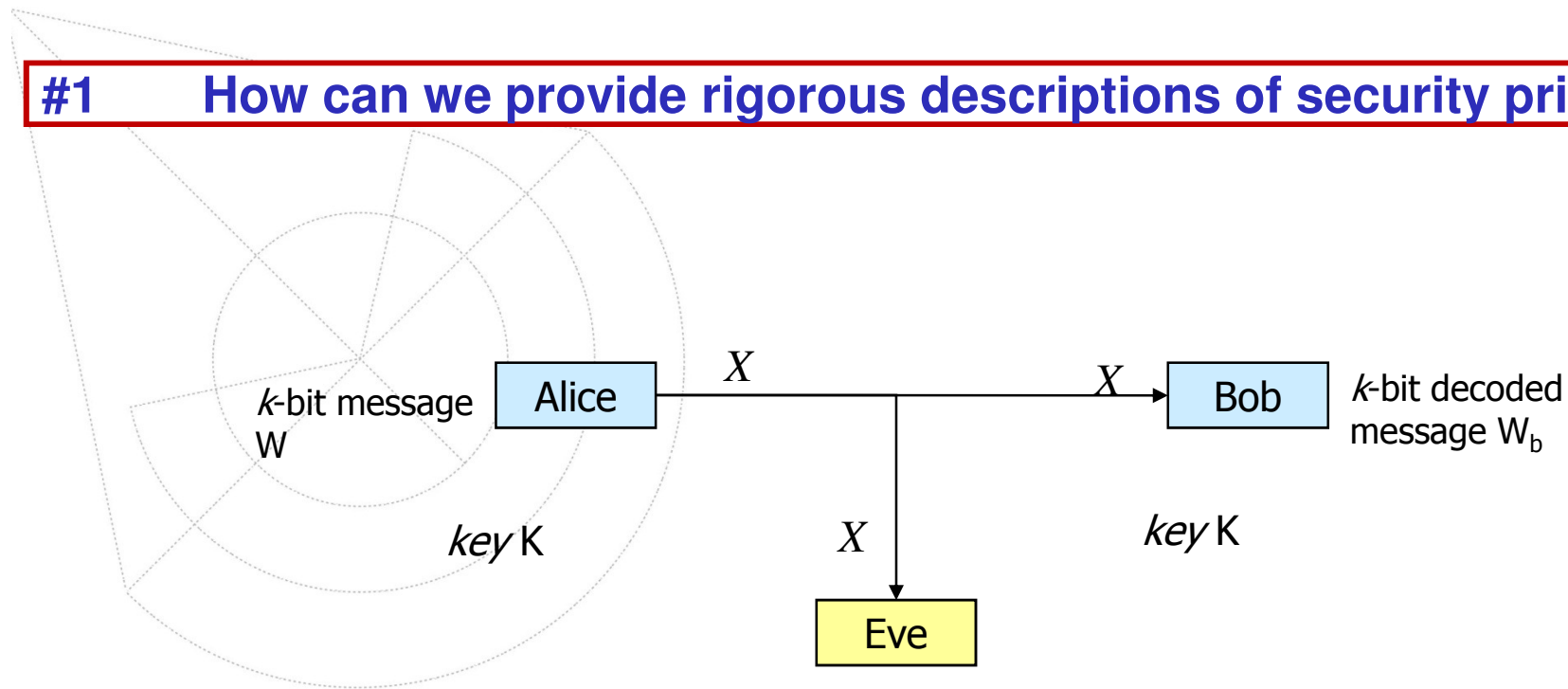




# Wireless Physical-Layer Security:

## 10 Open Issues

# #1 How can we provide rigorous descriptions of security primitives?



## Computational Security

Security schemes are based on (unproven) assumptions of intractability of certain functions;

Typically done at upper layers of the protocol stack

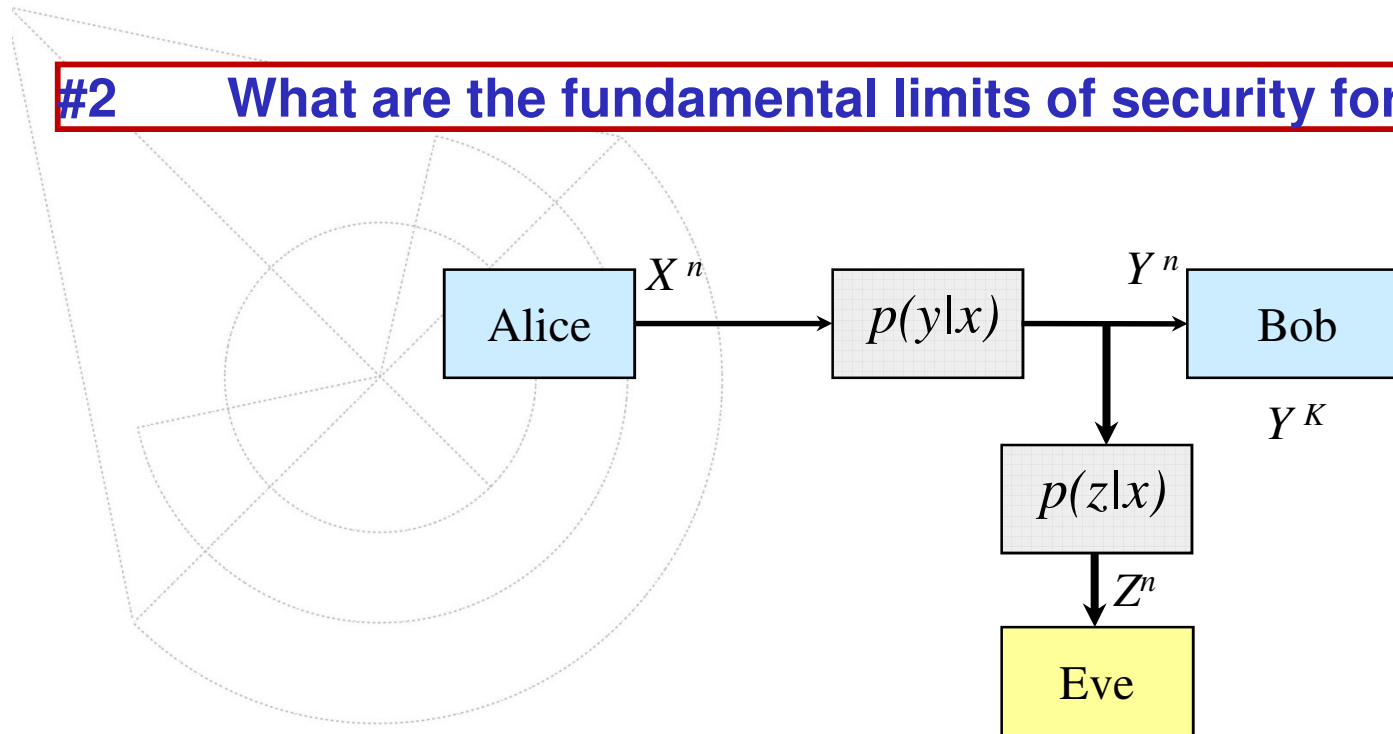
## Information-Theoretic (Perfect or unconditional) Security

strictest notion of security, **no computability assumption**

$$H(M|X)=H(M) \text{ or } I(X;M)=0$$

Implementable at the physical layer

## #2 What are the fundamental limits of security for *strong secrecy*?



- Theoretical results from the seventies (Wyner, Csiszár and Koerner)
- **Caveat:** eavesdropper must have a worse channel.
- Renaissance of information-theoretic security in the last 2 years.
- Most results are based on **weak secrecy conditions** (equivocation rate)
- **Strong secrecy** is possible (requires CS techniques)

NFC Forum : About NFC - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.nfc-forum.org/aboutnfc/

Getting Started Latest Headlines Adobe Flash Player Do... Fulbright Comission Joao Barros

Member Login

NFC FORUM

ABOUT THE FORUM MEMBERS JOIN

ABOUT NFC NEWS ROOM EVENTS RESOURCES SPECIFICATIONS

▶ About NFC

Near Field Communication (NFC) is a new, short-range wireless connectivity technology that evolved from a combination of existing contactless identification and interconnection technologies. Products with built-in NFC will dramatically simplify the way consumer devices interact with one another, helping people speed connections, receive and share information and even make fast and secure payments.

Operating at 13.56 MHz and transferring data at up to 424 Kbits/second, NFC provides intuitive, simple, and safe communication between electronic devices. NFC is both a "read" and "write" technology. Communication between two NFC-compatible devices occurs when they are brought within four centimeters of one another: a simple wave or touch can establish an NFC connection, which is then compatible with other known wireless technologies such as Bluetooth or Wi-Fi. The

NFC for Enterprises

Enterprises

Resources for press and analysts  
News Room

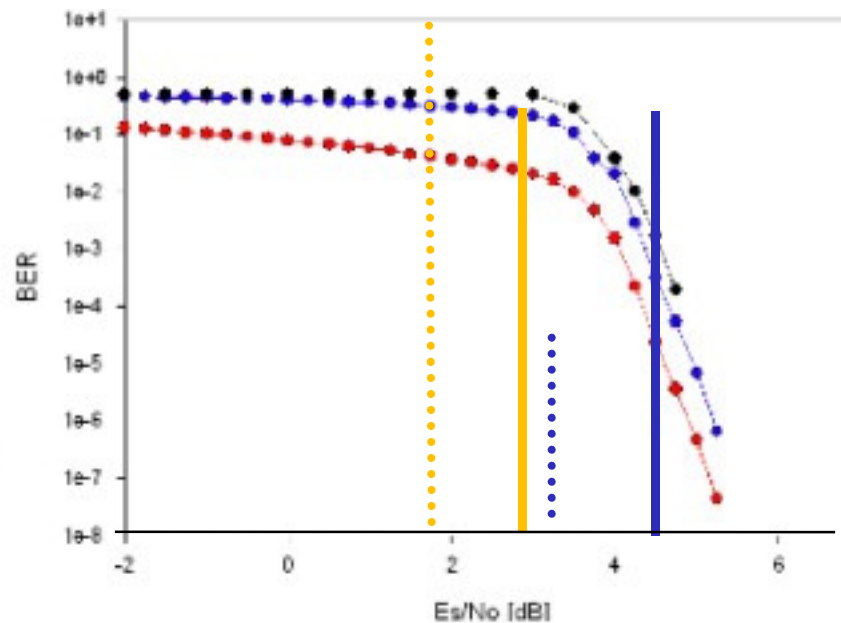
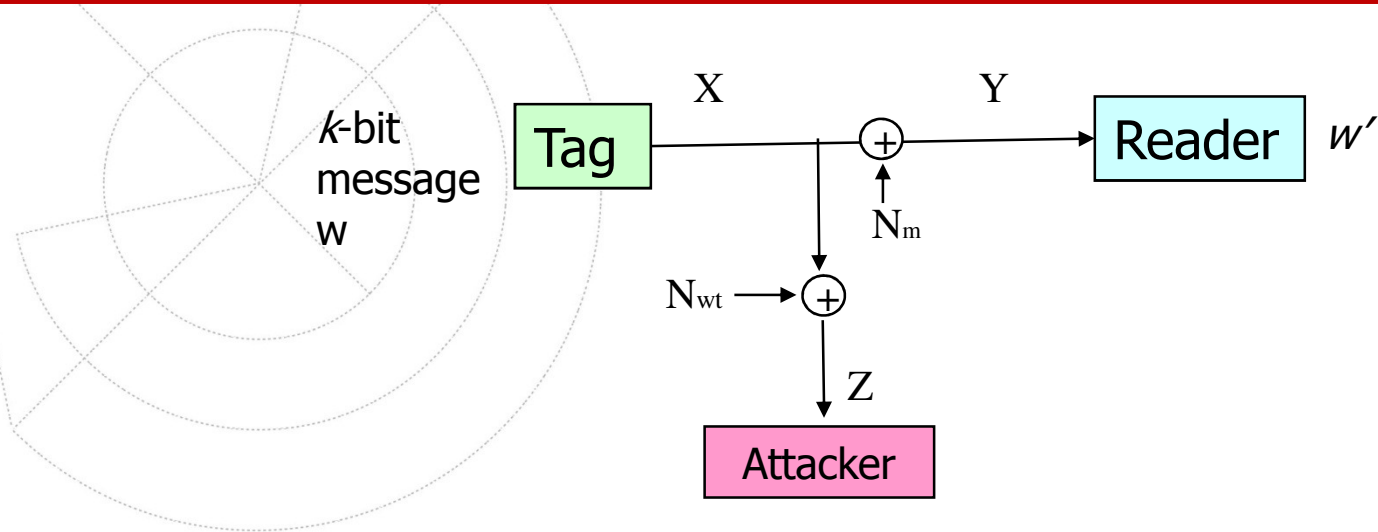
©2007 NFC FORUM ALL RIGHTS RESERVED.  
Site Map | Feedback | Privacy Policy

MasterCard Panasonic SONY Microsoft NXP NEC RENESAS VISA NOKIA SAMSUNG hp WTT Do Co Mo

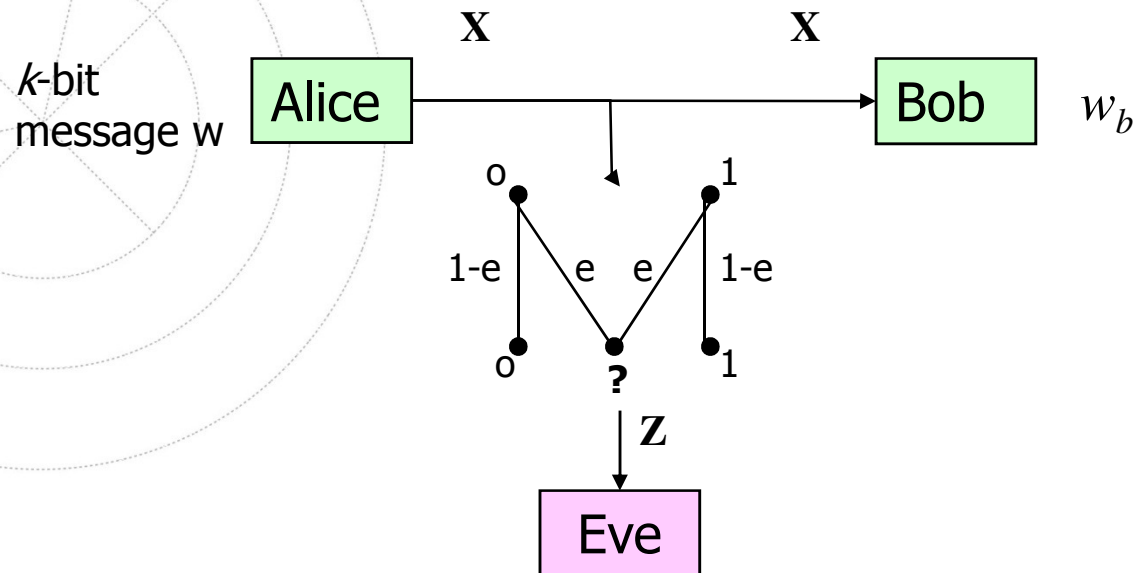
Because the transmission range is so short, NFC-enabled transactions are inherently secure. Also, physical proximity of the device to the reader gives users the reassurance of being in control of the process.



### #3 How can we leverage state-of-the-art channel coding to enhance security at the physical layer?



## #4 How do we construct secrecy achieving codes for wireless channels?



Main channel is noiseless; wire-tapper's channel is a BEC with erasure probability  $e$

Eve receives a subset of the transmitted bits (or packets)

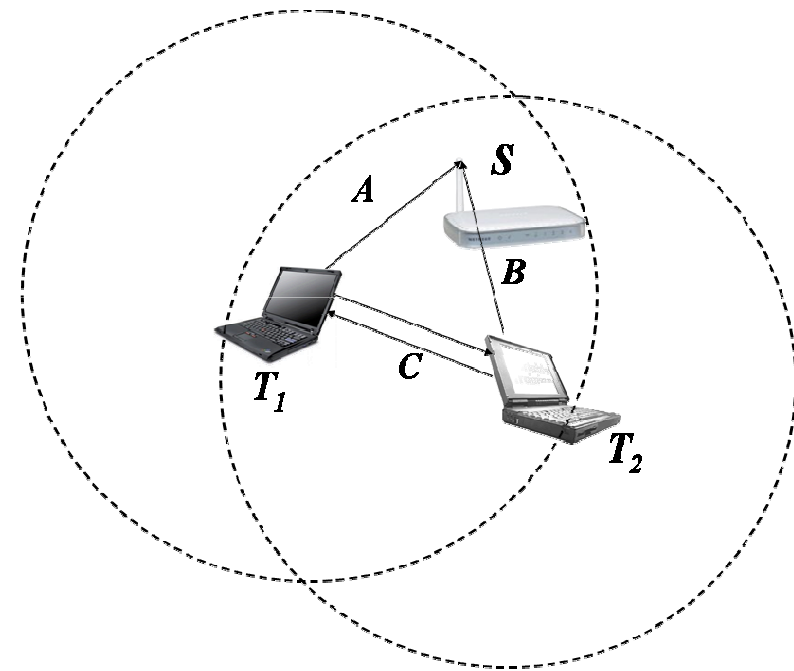
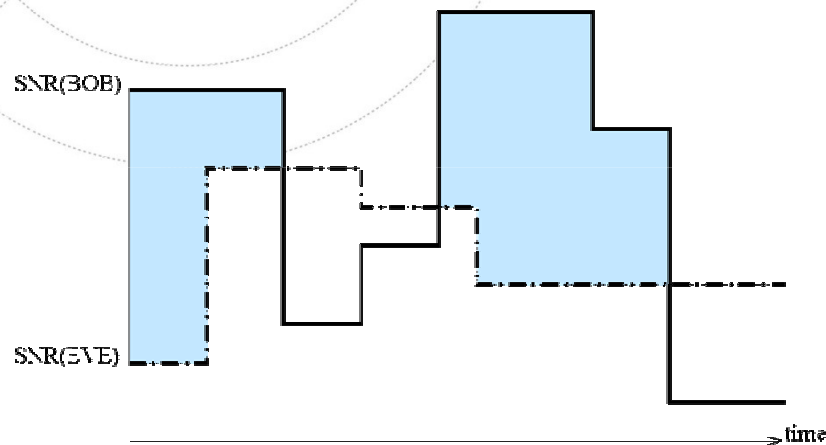
For this instance (only), we have secrecy capacity achieving codes.

## #5 How can we borrow from quantum cryptography?

- **Common Randomness:** Alice and Bob share correlated random sequences.
- **Reconciliation:** Alice sends Bob enough side information for Bob to reconstruct Alice's sequence.
- **Privacy Amplification:** Alice and Bob use hash functions to maximize Eve's equivocation.

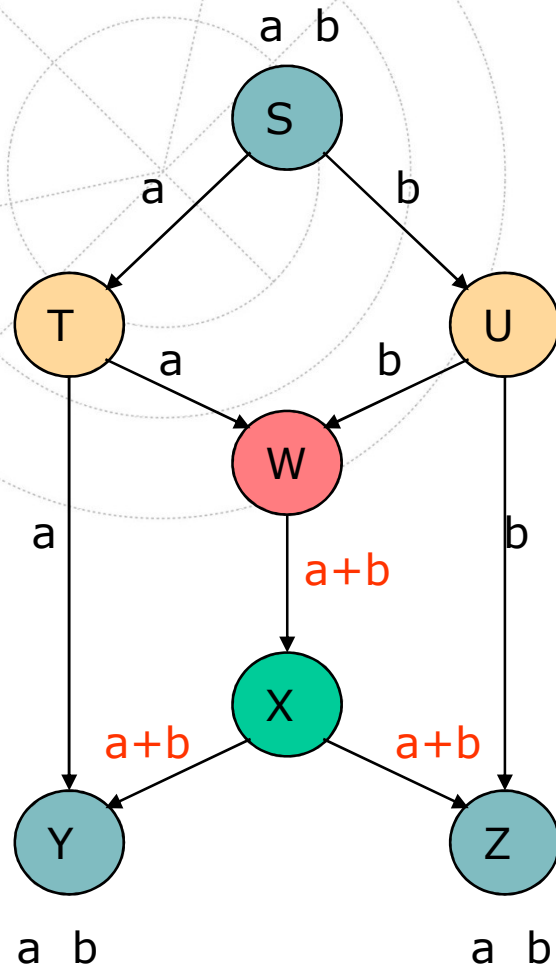
## #6 How can we leverage fading?

### Wireless Network with Potential Eavesdropping



- Goal: Exploit **channel variability** to secure information at the **physical-layer**.

## #7 How can we provide security for network coding?



- Intermediate nodes have different levels of confidentiality;
- Nodes T and U have **partial** information about the data;
- Node W has **full** access to the data;
- Node X cannot decode **any useful** data – a free cypher?
- **Active attacks** can easily compromise the information flow.



# Network Coding for Robust Architectures in Volatile Environments

European Project (Future Internet Call)

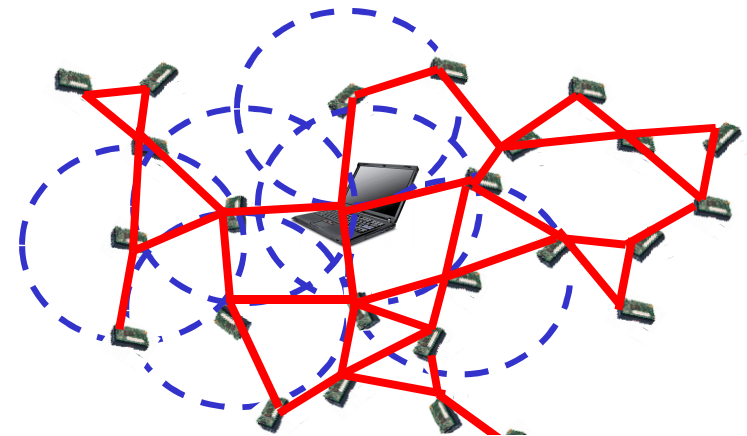
Partners:      **CERTH**            (Greece)  
                  **EPFL**             (Switzerland)  
                  **IT/FCUP**          (Portugal)  
                  **TELEFONICA** (Spain)  
                  **THOMSON**       (France)  
                  **TU Munich**      (Germany)  
                  **CUHK**             (Hong Kong)

Budget:        \$5.5M over 3 years

## #8 How can we use coding ideas to distribute secret keys?

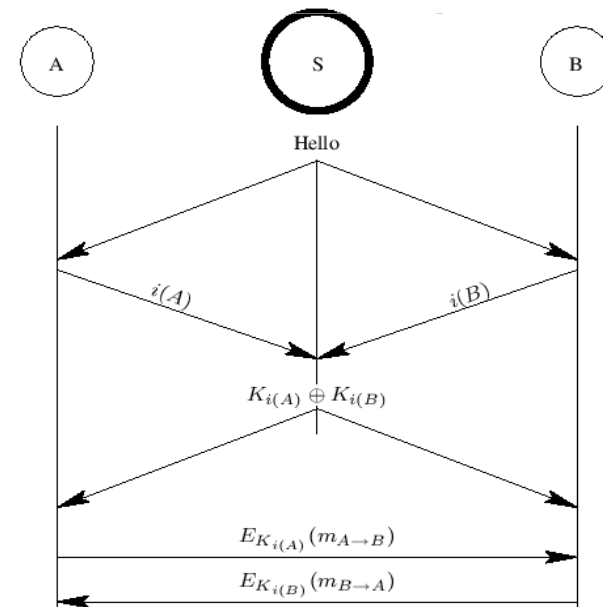
### ○ Problem:

- How can each pair of sensor nodes agree on a secret key?



### ○ Our approach:

- Key pre-distribution scheme;
- Uses **a mobile node** to complete the key distribution process *blindly using network coding*;
- Reduced memory requirements;



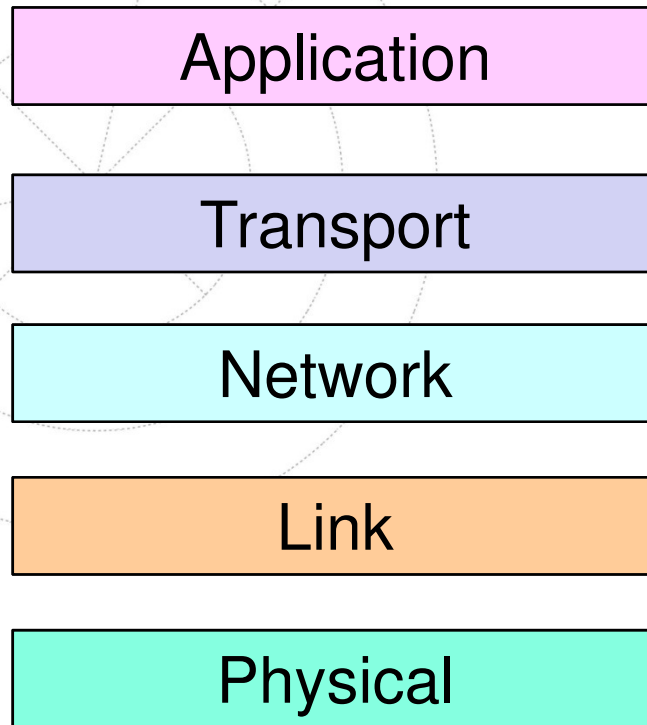
## #9 How can we use physical-layer techniques to go beyond secure communication?

- Cryptography is not only concerned with communicating securely.
- Based on noisy channels and state-of-the-art error correction codes we can implement **bit commitment and oblivious transfer**, which are the building stones of secure multi-party computation.
- **Authentication is a vital issue** and could potentially be carried out over noisy channels possibly without initial shared secret.

[Wolf and Maurer'98], [Trappe et al' ]

- **How about anonymity?**
- **How about non-repudiation?**

**#10 It may well be worth rethinking our security architecture.**



**Bottom-up Security?**

- How can we combine physical-layer security and cryptographic protocols?