

ESCAPADE: Enhancing communication security by cross-layer physical and data-link (PDX) techniques



Application scenario 1

- ▶ Secure wireless networks without pre-shared **secret keys**



Application scenario 1

- ▶ Secure wireless networks without pre-shared **secret keys**

open network



Application scenario 1

- ▶ Secure wireless networks without pre-shared **secret keys**



open network



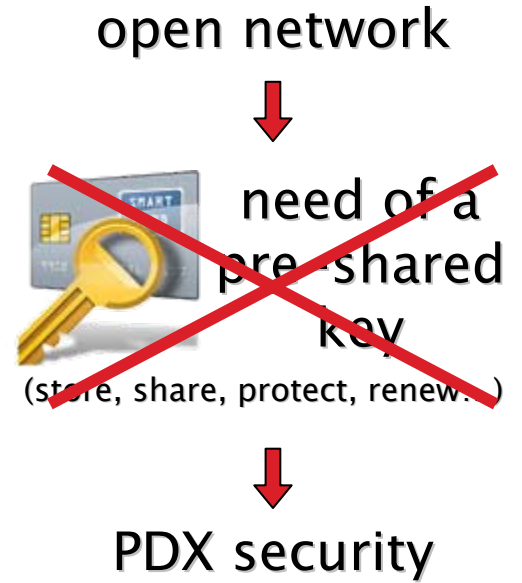
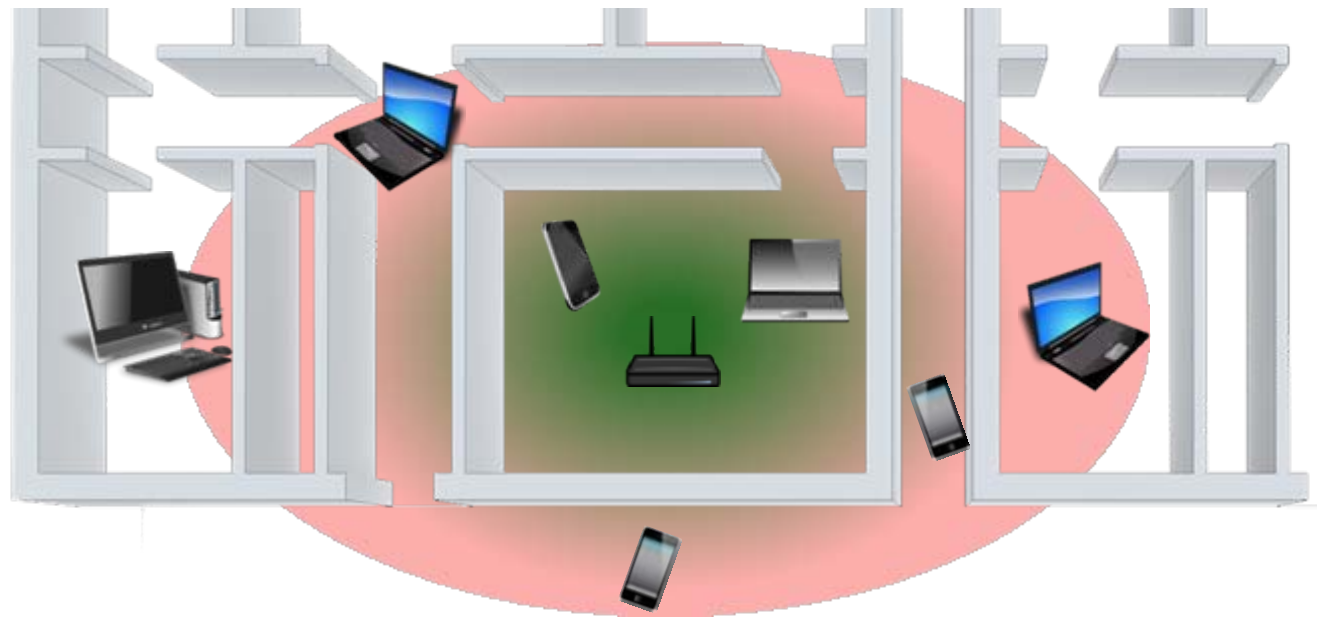
need of a
pre-shared
key



(store, share, protect, renew...)

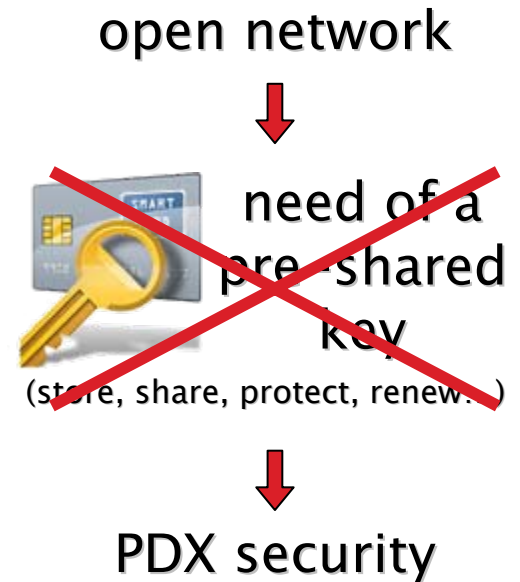
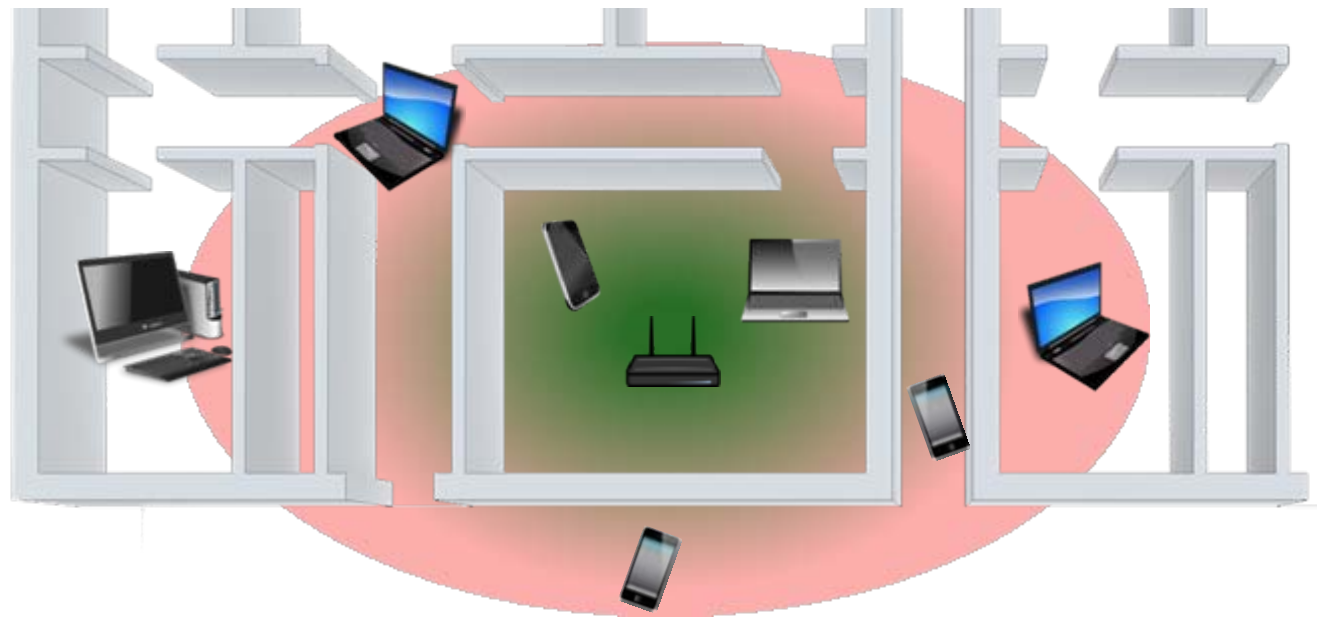
Application scenario 1

- Secure wireless networks without pre-shared **secret keys**



Application scenario 1

- Secure wireless networks without pre-shared **secret keys**



- Can be implemented in existing **IEEE 802.11b/g/n** networks
- Existing (free) **network card drivers** can be adapted
- Minimal hardware costs, mostly **software** development costs

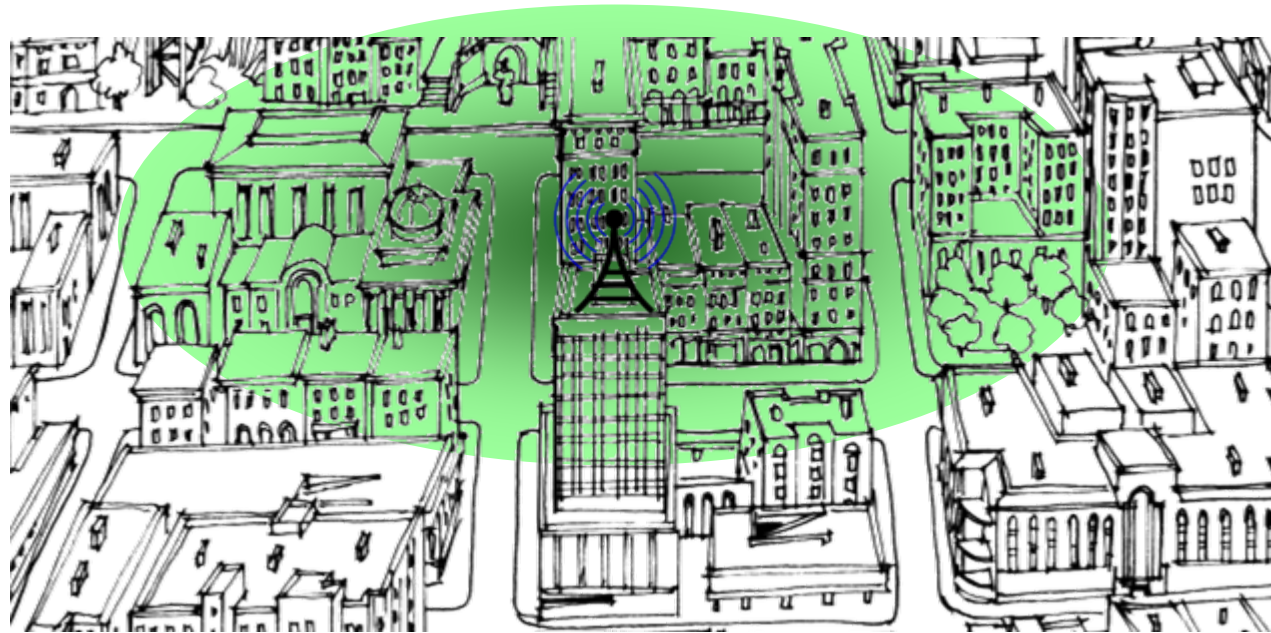
Application scenario 2

- ▶ Broadcast transmission with **confidential messages**



Application scenario 2

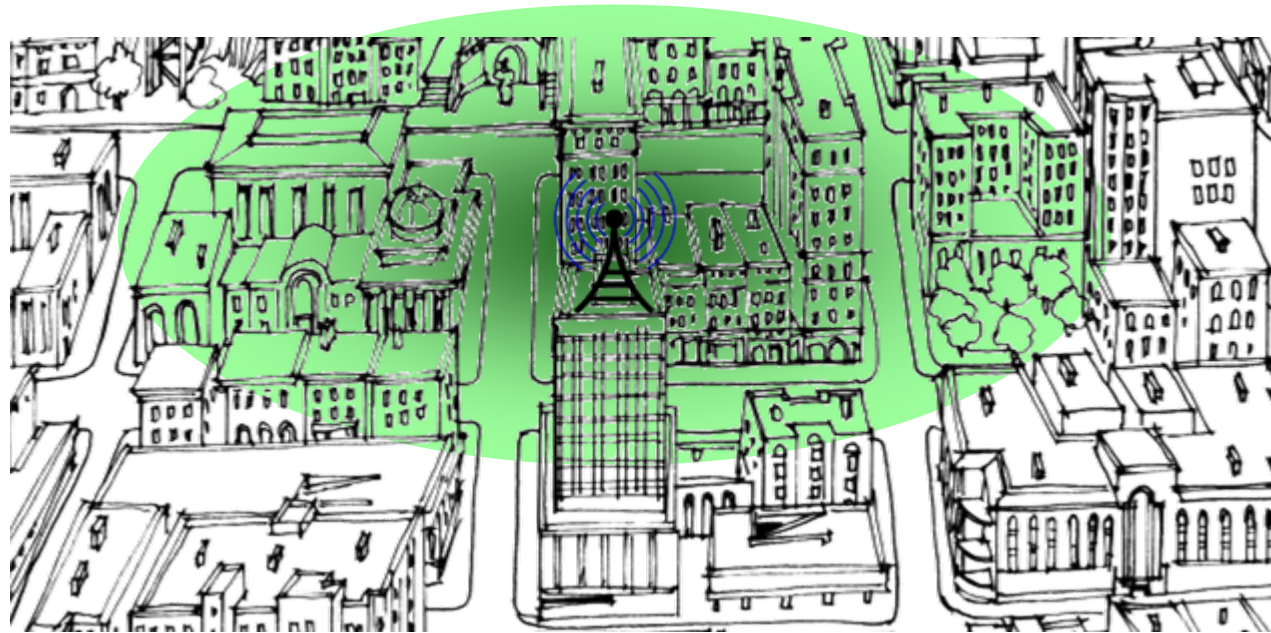
- ▶ Broadcast transmission with **confidential messages**



only free-to-air

Application scenario 2

- ▶ Broadcast transmission with **confidential messages**



only free-to-air

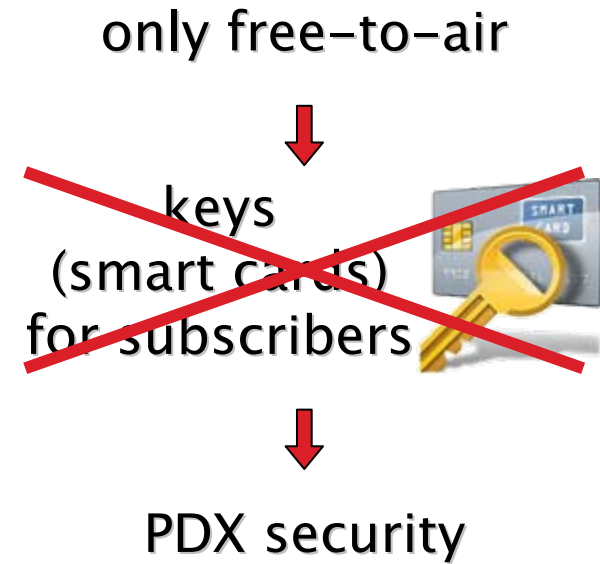
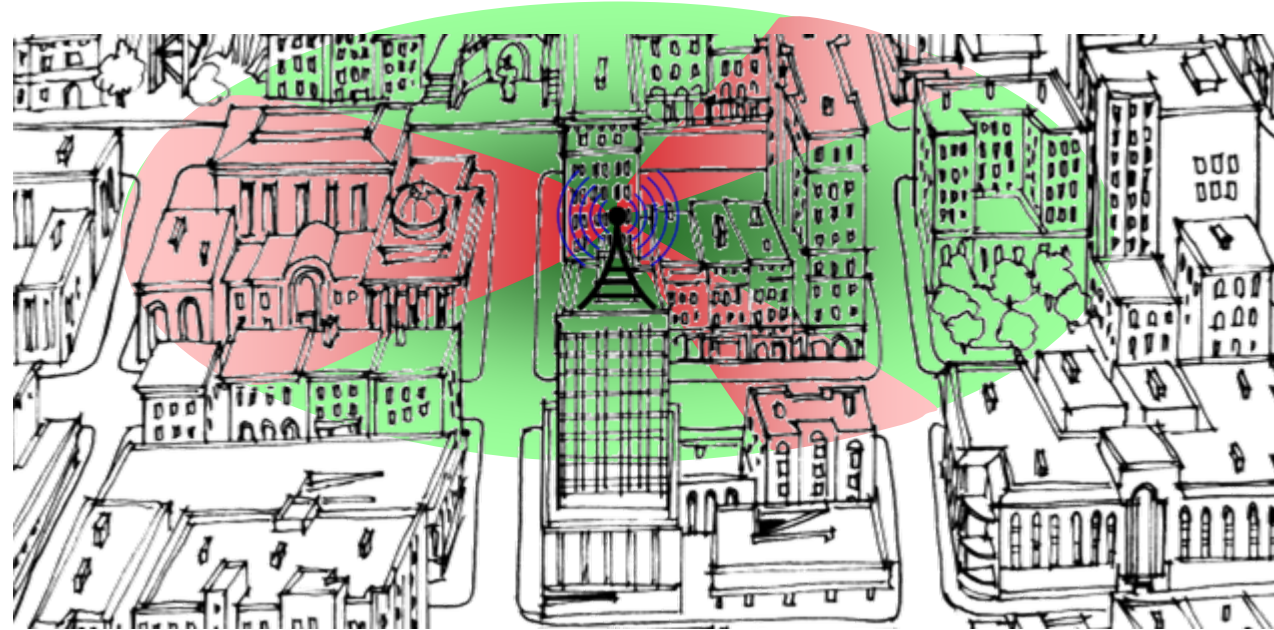


keys
(smart cards)
for subscribers



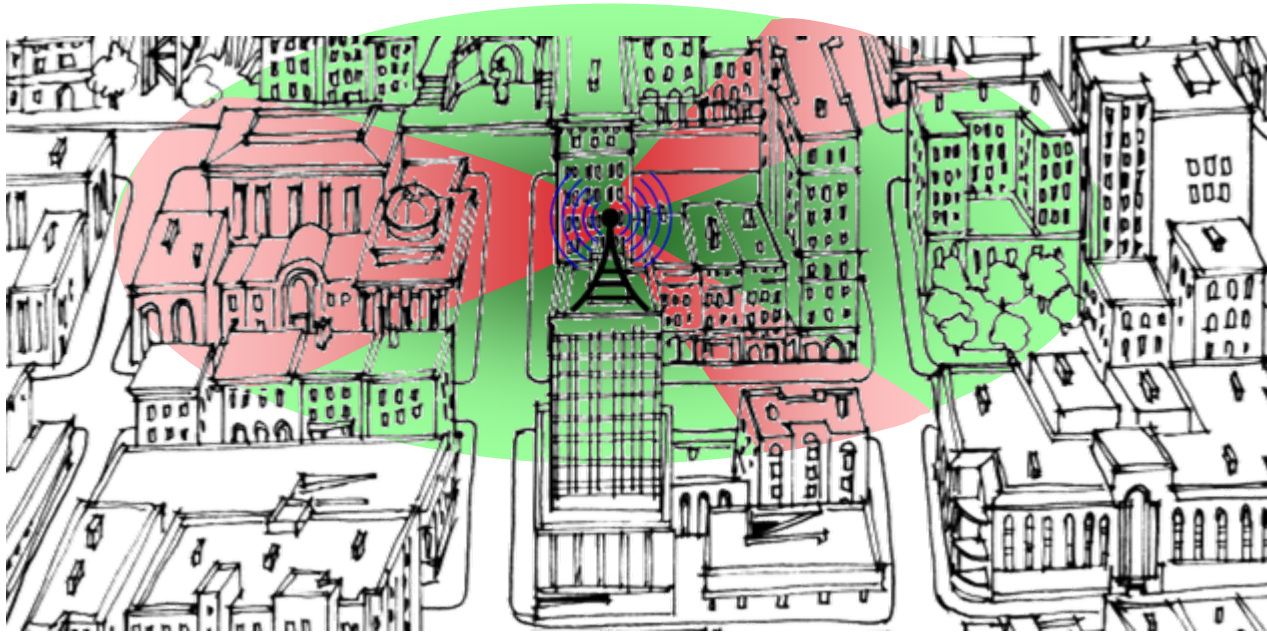
Application scenario 2

- ▶ Broadcast transmission with **confidential messages**



Application scenario 2

- ▶ Broadcast transmission with **confidential messages**

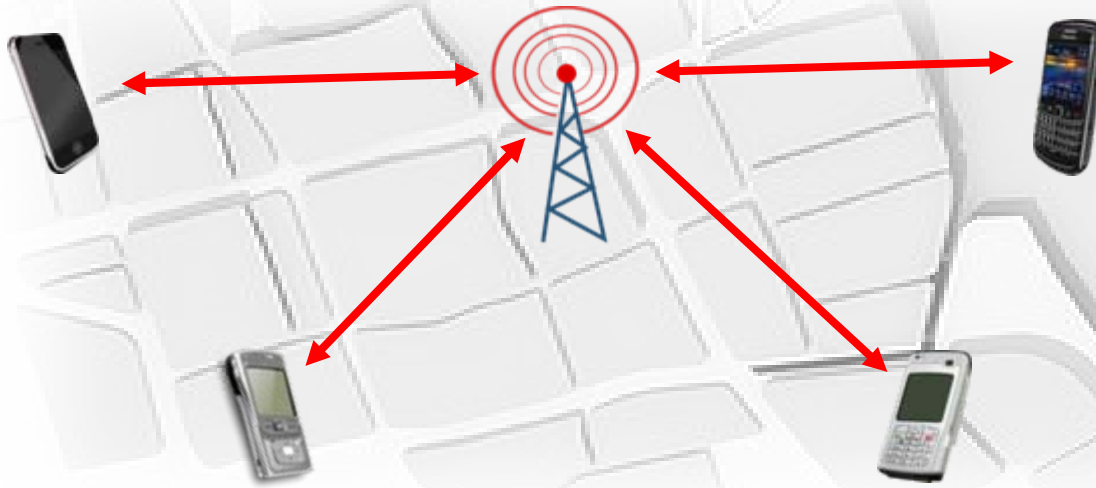


- ▶ Possible applications:

- Digital television broadcasting (DVB-T2/S2/NGH/T2mobile)
- Data broadcasting services with conditional access

Application scenario 3

- ▶ Secure Cooperative Multiple Access Channels



Application scenario 3

- ▶ Secure Cooperative Multiple Access Channels



- ▶ 3G and beyond cellular systems with intermediate nodes (**relays** and **femtocells**)

Application scenario 3

- ▶ Secure Cooperative Multiple Access Channels



- ▶ 3G and beyond cellular systems with intermediate nodes (**relays** and **femtocells**)
- ▶ Intermediate nodes are not controlled directly by the operator: possibly **untrustworthy**

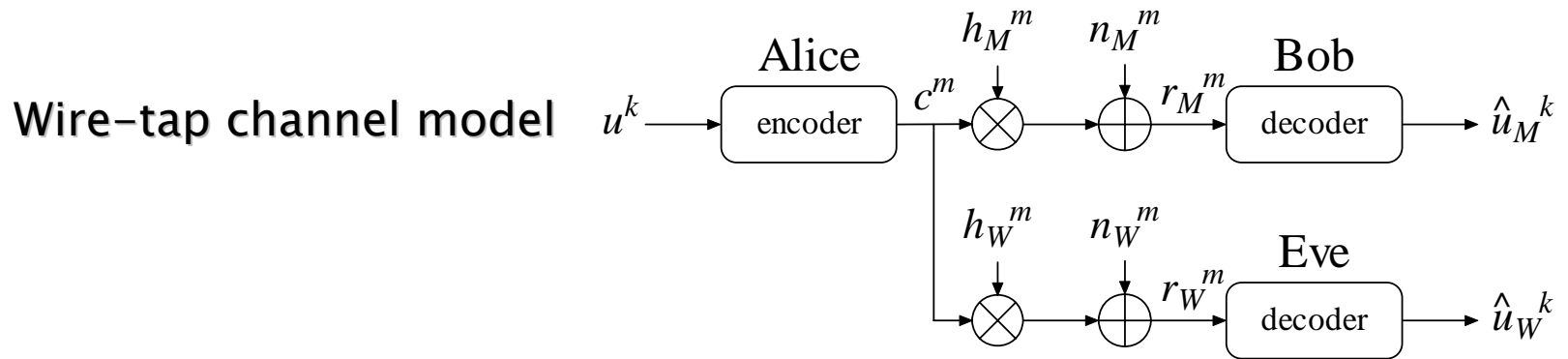
Application scenario 3

- ▶ Secure Cooperative Multiple Access Channels



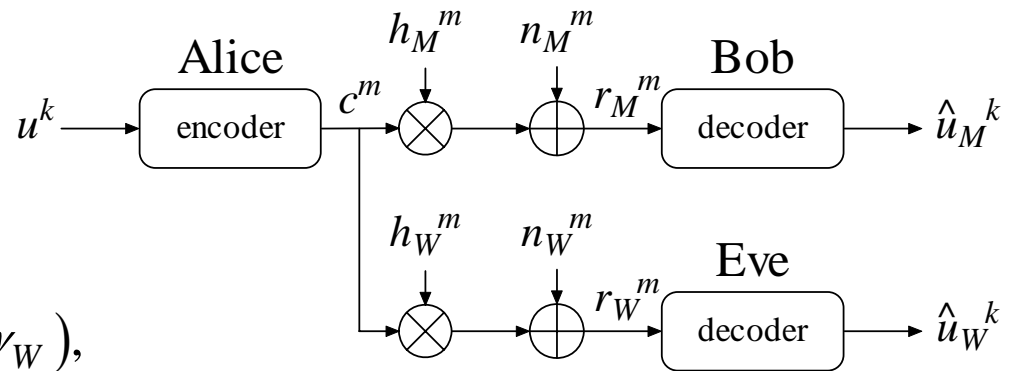
- ▶ 3G and beyond cellular systems with intermediate nodes (**relays** and **femtocells**)
- ▶ Intermediate nodes are not controlled directly by the operator: possibly **untrustworthy**

Physical Layer Security model



Physical Layer Security model

Wire-tap channel model



Secrecy Capacity

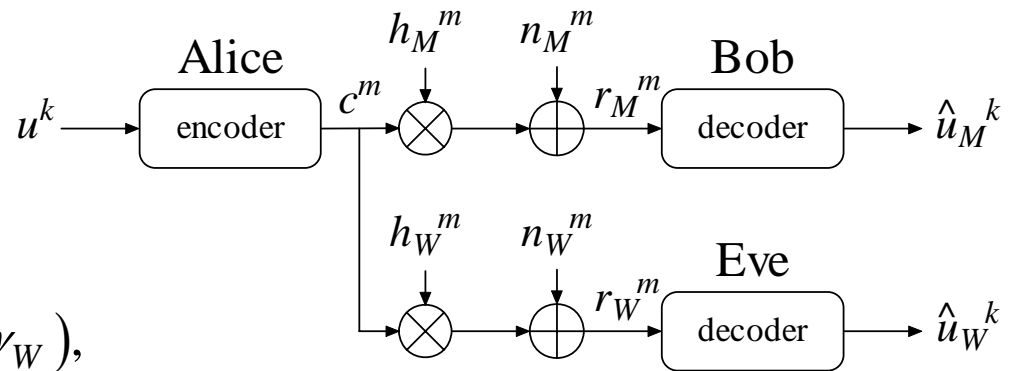
$$C_s = \sum_{\gamma_M > \gamma_W} \log(1 + \gamma_M) - \log(1 + \gamma_W),$$

$$\gamma_M = |h_M^n|^2 \frac{P}{N_M}, \quad \gamma_W = |h_W^n|^2 \frac{P}{N_W}.$$



Physical Layer Security model

Wire-tap channel model

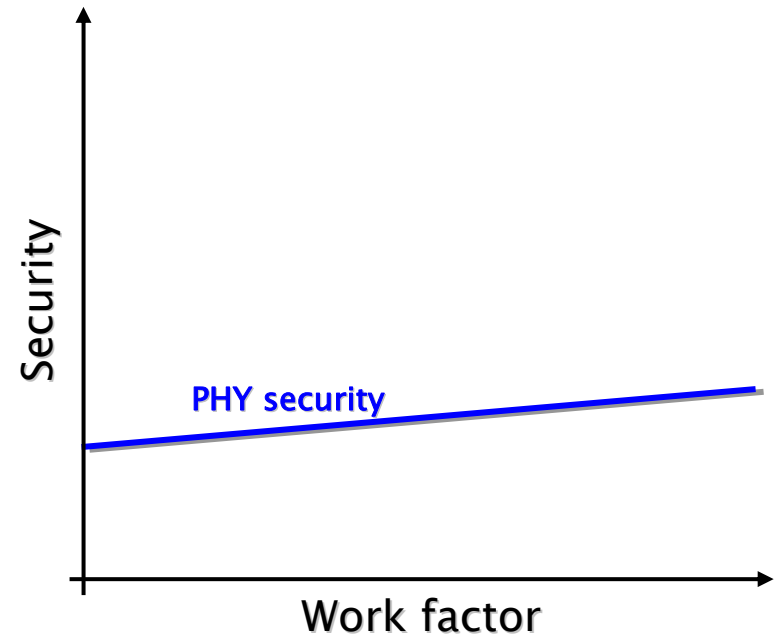


Secrecy Capacity

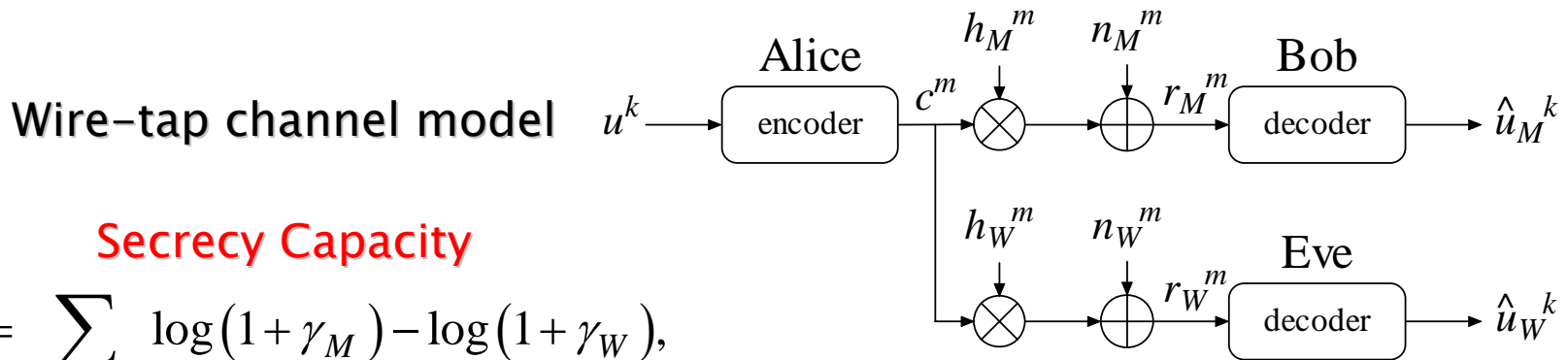
$$C_s = \sum_{\gamma_M > \gamma_W} \log(1 + \gamma_M) - \log(1 + \gamma_W),$$

$$\gamma_M = |h_M^n|^2 \frac{P}{N_M}, \quad \gamma_W = |h_W^n|^2 \frac{P}{N_W}.$$

- ▶ **Inherent** wireless security exists



Physical Layer Security model

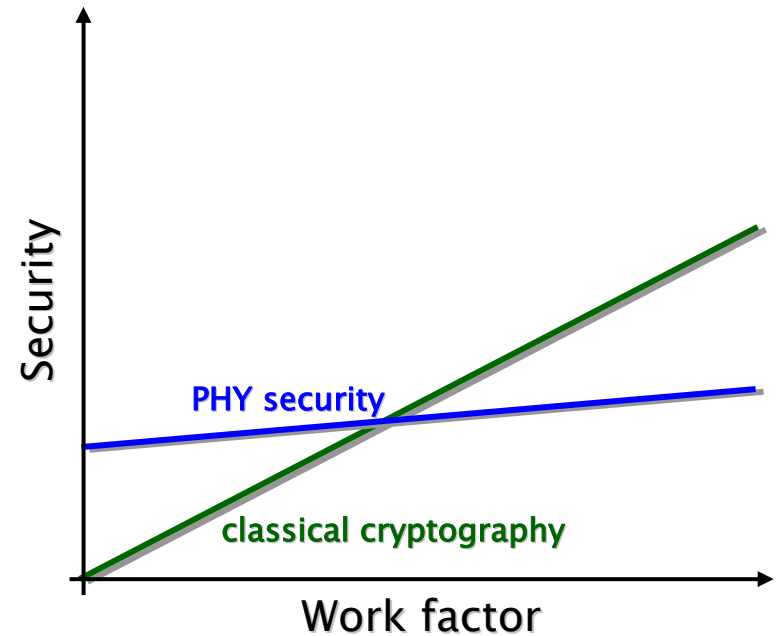


Secrecy Capacity

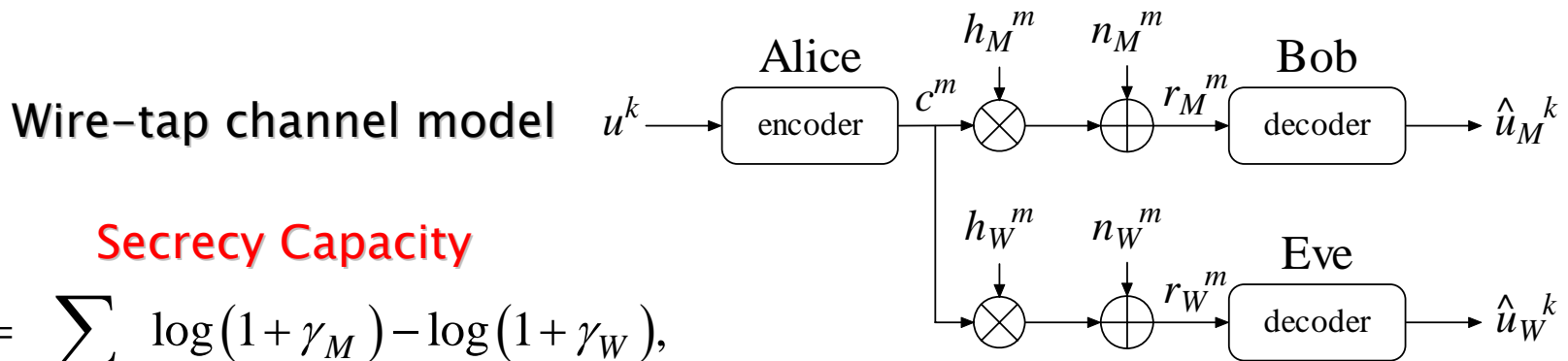
$$C_s = \sum_{\gamma_M > \gamma_W} \log(1 + \gamma_M) - \log(1 + \gamma_W),$$

$$\gamma_M = |h_M^n|^2 \frac{P}{N_M}, \quad \gamma_W = |h_W^n|^2 \frac{P}{N_W}.$$

- ▶ **Inherent** wireless security exists
- ▶ Classical cryptography is only based on **computational assumptions**



Physical Layer Security model

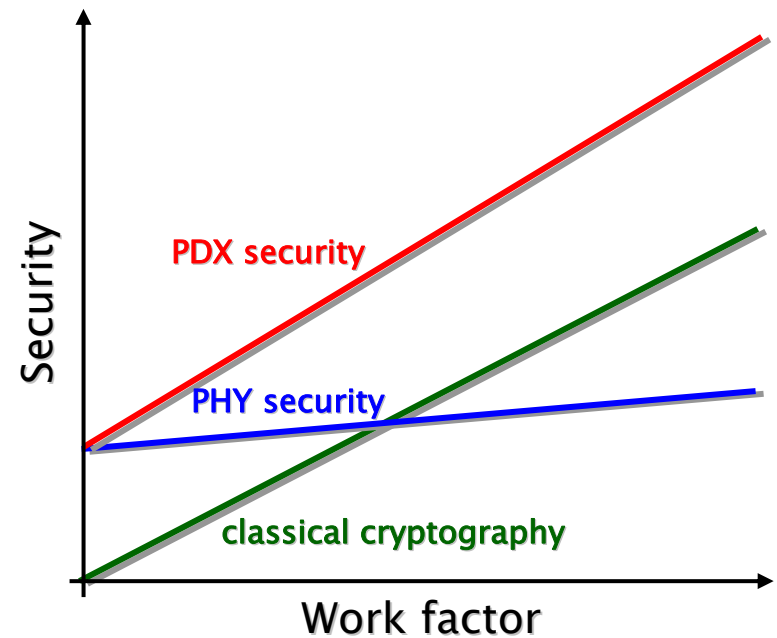


Secrecy Capacity

$$C_s = \sum_{\gamma_M > \gamma_W} \log(1 + \gamma_M) - \log(1 + \gamma_W),$$

$$\gamma_M = |h_M^n|^2 \frac{P}{N_M}, \quad \gamma_W = |h_W^n|^2 \frac{P}{N_W}.$$

- ▶ **Inherent** wireless security exists
- ▶ Classical cryptography is only based on **computational assumptions**
- ▶ Exploiting the physical layer can **enhance** communication security

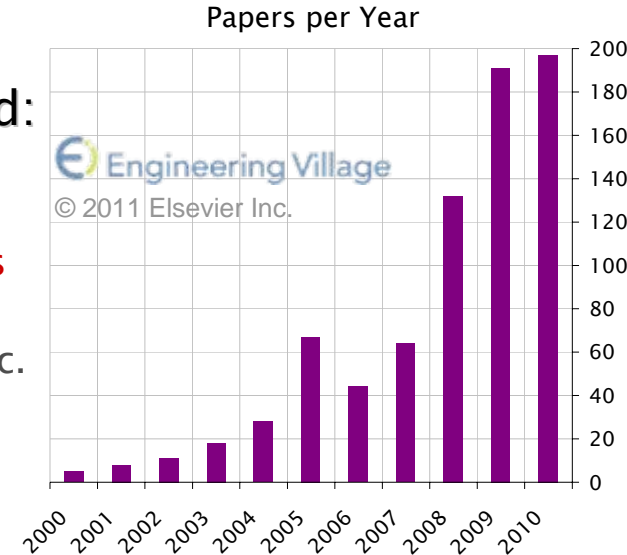


Physical Layer Security importance

- ▶ **Physical layer security** is a breakthrough in communication security paradigms:
 - **Unconditional** security (no computational assumptions)
 - Reinforcement of **higher layer** security protocols
 - No more need of pre-shared **secret keys**
 - Crucial for securing **cooperative communications** (future cellular networks)

- ▶ Locates within the topic of **homeland security**, strategic for the national economy (D.D. 27/09/2010 no. 584/ric)

- ▶ Well established and **continuously growing** field:
 - Dedicated workshops at **top conferences**
 - Specific **books** and **special issues of international journals**
 - 2011 IEEE Communications Soc. & Information Theory Soc. Joint Paper **Award** (M. Bloch, J. Barros, M. R. D. Rodrigues, S. W. McLaughlin)



State of the art

- ▶ The randomness of wireless channels can be exploited to provide information security at the **physical layer** (PHY)
- ▶ **Theoretical limits** of PHY security have been widely investigated
- ▶ Some **practical schemes** available only for toy channel models
- ▶ Emerging trend: **PHY** and **Data Link** cross-layer (**PDX**) schemes for integrated security
- ▶ Dominant techniques eligible for PDX security:
 - Channel coding (especially **LDPC** coding)
 - Orthogonal Frequency-Division Multiplexing (**OFDM**)
 - Cross-layer solutions with Automatic Repeat-reQuest (**ARQ**)



State of the art

- ▶ The randomness of wireless channels can be exploited to provide information security at the **physical layer** (PHY)
- ▶ **Theoretical limits** of PHY security have been widely investigated
- ▶ Some **practical schemes** available only for toy channel models
- ▶ Emerging trend: **PHY** and **Data Link** cross-layer (**PDX**) schemes for integrated security
- ▶ Dominant techniques eligible for PDX security:
 - Channel coding (especially **LDPC** coding)
 - Orthogonal Frequency-Division Multiplexing (**OFDM**)
 - Cross-layer solutions with Automatic Repeat-reQuest (**ARQ**)

Open Issues

- ▶ No efficient **practical solutions** for PDX security in **most scenarios**
- ▶ No publicly available **tools** for **implementing** and **assessing** PDX security schemes in **wireless networks**



Project goals

for the Scientific/Technical community

- ▶ New **practical error protection** and **secrecy achieving codes** tailored for wireless transmissions
- ▶ New **protocols** and **optimization tools** for PDX secure wireless transmission
- ▶ New **network codes** for PDX secrecy in **cooperative systems** and new **detection tools** against rogue nodes

papers,
workshops,
seminars,
simulators,
website



Project goals

for the Scientific/Technical community

- ▶ New **practical error protection** and **secrecy achieving codes** tailored for wireless transmissions
- ▶ New **protocols** and **optimization tools** for PDX secure wireless transmission
- ▶ New **network codes** for PDX secrecy in **cooperative systems** and new **detection tools** against rogue nodes

papers,
workshops,
seminars,
simulators,
website

for Companies/Manufacturers

- ▶ **Practical PDX security solutions** ready for **existing** and **future** wireless networks
- ▶ **Software tools** for implementing and assessing PDX security techniques

tech. reports,
patents,
software,
testbeds



Project goals

for the Scientific/Technical community

- ▶ New **practical error protection** and **secrecy achieving codes** tailored for wireless transmissions
- ▶ New **protocols** and **optimization tools** for PDX secure wireless transmission
- ▶ New **network codes** for PDX secrecy in **cooperative systems** and new **detection tools** against rogue nodes

papers,
workshops,
seminars,
simulators,
website

for Companies/Manufacturers

- ▶ **Practical PDX security solutions** ready for **existing** and **future** wireless networks
- ▶ **Software tools** for implementing and assessing PDX security techniques

tech. reports,
patents,
software,
testbeds

for Customers/Everyday life

- ▶ Wireless **devices** (based on commercial hardware) that implement PDX security
- ▶ Easier deployment of **secure wireless networks** (without pre-shared keys)

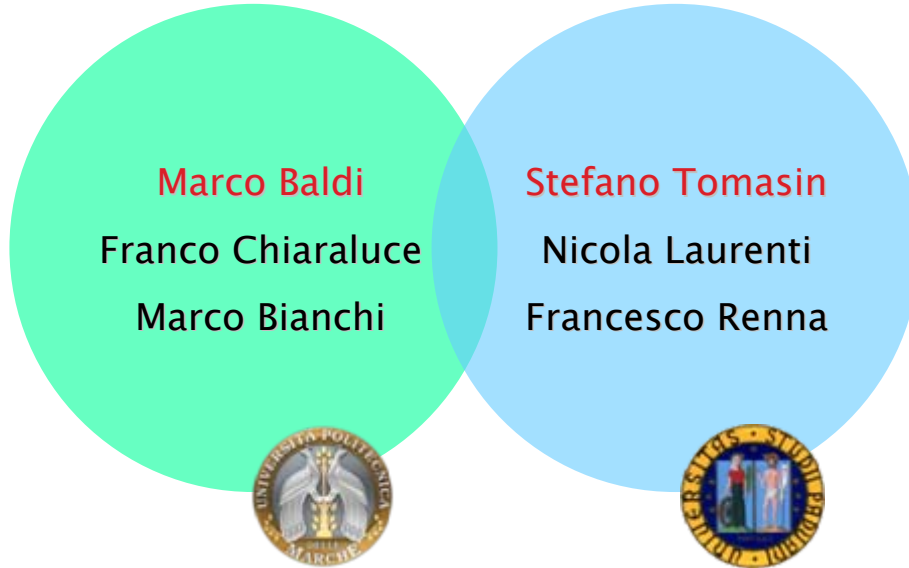
card drivers,
website



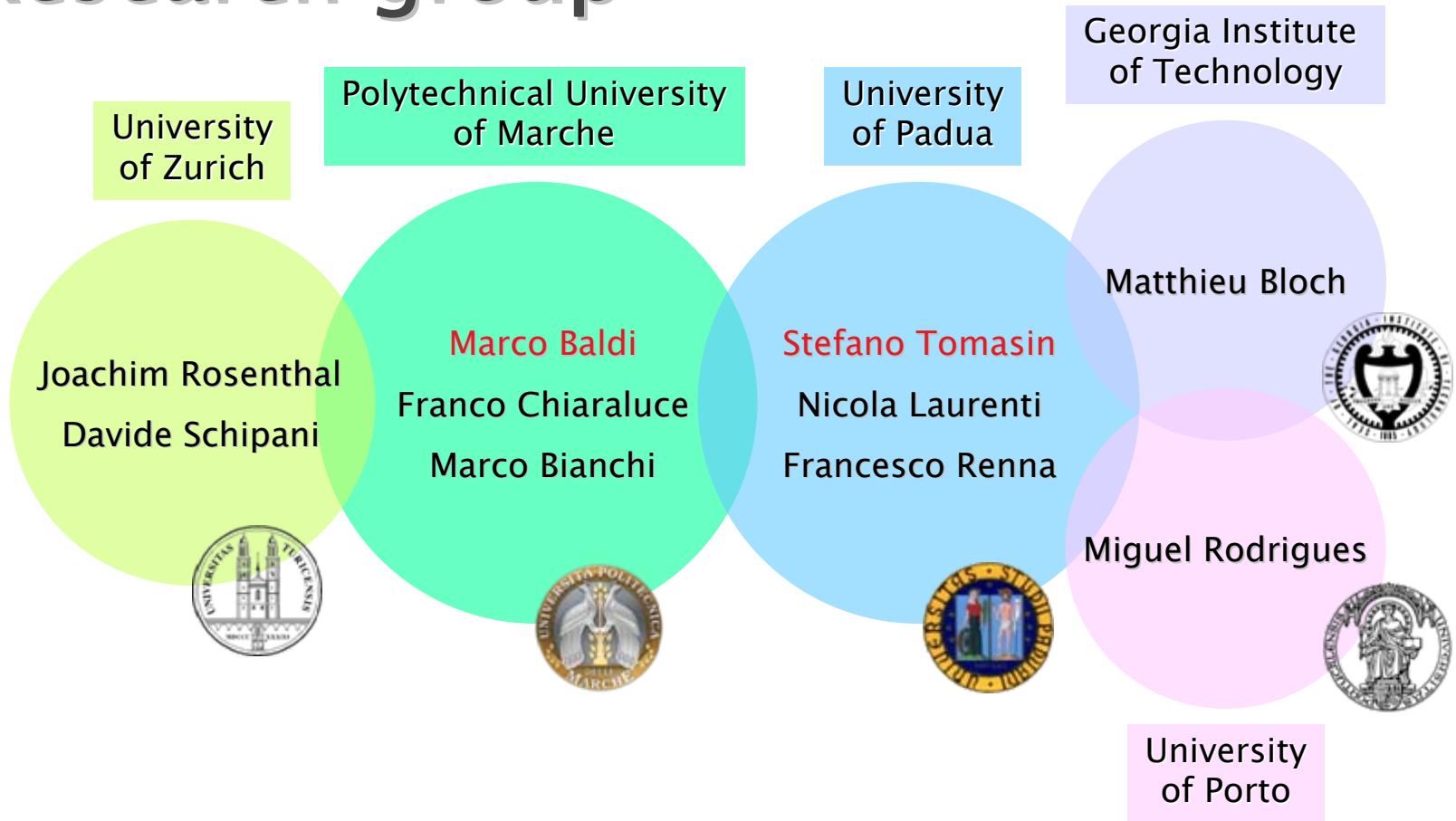
Research group

Polytechnical University
of Marche

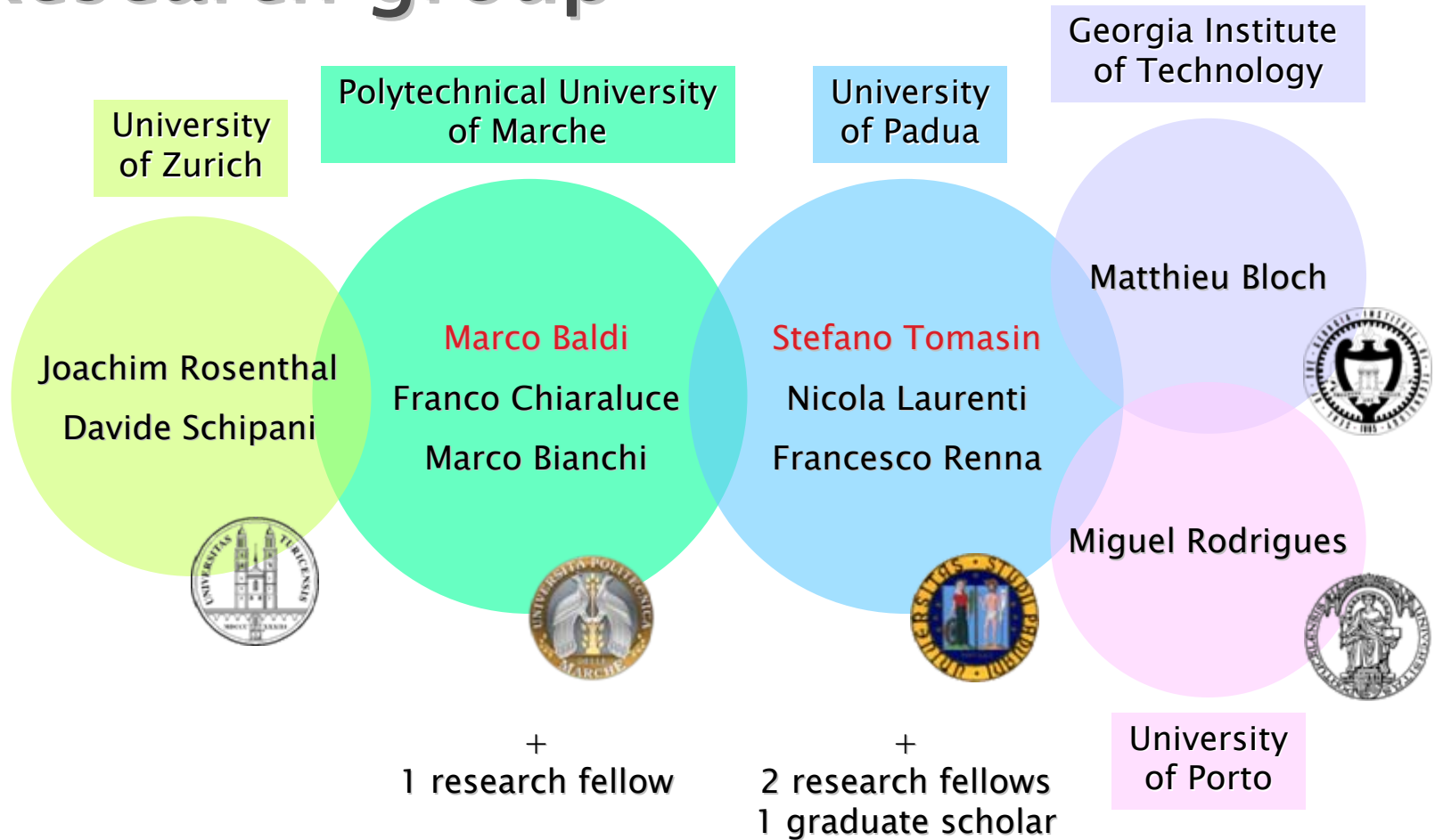
University
of Padua



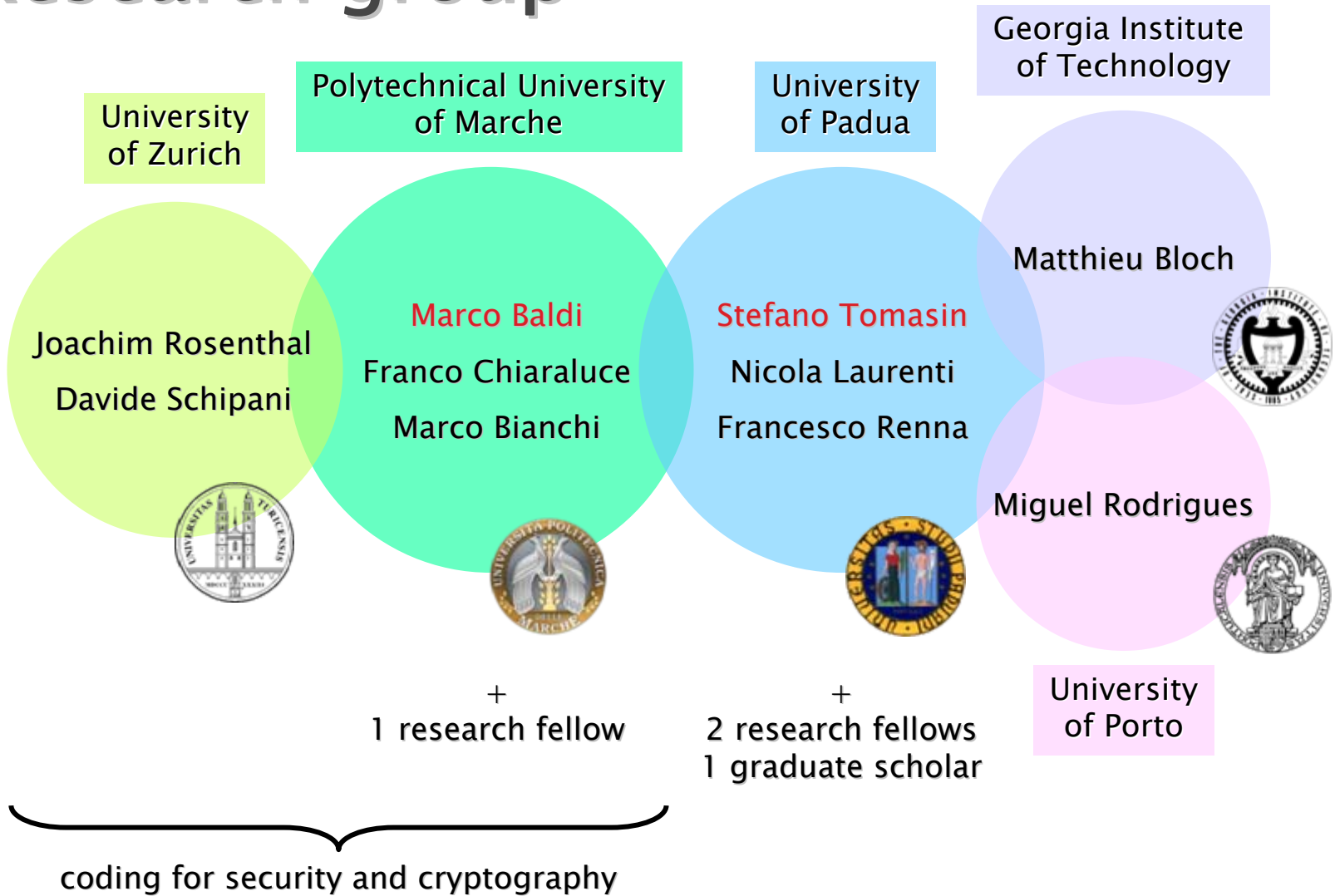
Research group



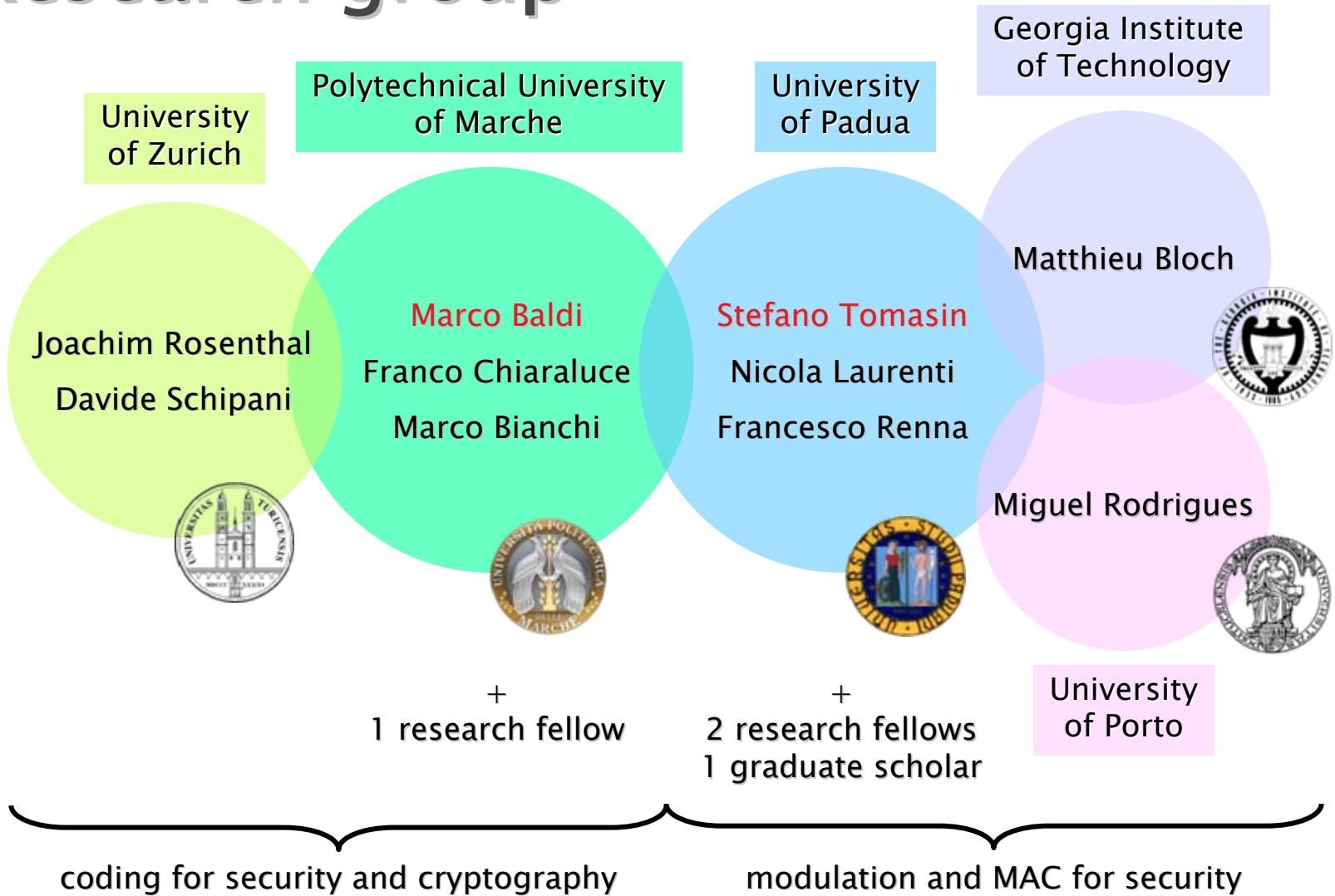
Research group



Research group



Research group



Some recent results

▶ Related scientific papers:

- **M. Baldi**, F. Bambozzi, **F. Chiaraluce**, “On a family of circulant matrices for quasi-cyclic low-density generator matrix codes”, *IEEE Trans. Inf. Theory*, Sep. 2011.
- **M. Baldi**, **M. Bianchi**, **F. Chiaraluce**, **J. Rosenthal**, **D. Schipani**, “A variant of the McEliece cryptosystem with increased public key security”, *Proc. WCC 2011*.
- **M. Baldi**, **M. Bianchi**, **F. Chiaraluce**, “Increasing physical layer security through scrambled codes and ARQ”, *Proc. IEEE ICC 2011*.
- **M. Baldi**, **M. Bianchi**, **F. Chiaraluce**, “Non-systematic codes for physical layer security”, *Proc. IEEE ITW 2010*.
- S. Dehnie, **S. Tomasin**, “Detection of selfish nodes in networks using CoopMAC protocol with ARQ”, *IEEE Trans. Wireless Commun.*, Jul. 2010.
- **S. Tomasin**, M. Levorato, M. Zorzi, “Steady state analysis of coded cooperative networks with HARQ protocol”, *IEEE Trans. Commun.*, Aug. 2009.
- **F. Renna**, **M. Bloch**, **N. Laurenti**, “Semi-blind key-agreement over MIMO fading channels”, *Proc. IEEE ICC 2011*.
- **F. Renna**, **N. Laurenti**, H.V. Poor, “Physical layer secrecy for OFDM systems”, *Proc. EW 2010*.
- **F. Renna**, **N. Laurenti**, H.V. Poor, “High SNR secrecy rates with OFDM signaling over fading channels”, *Proc. PIMRC 2010*.

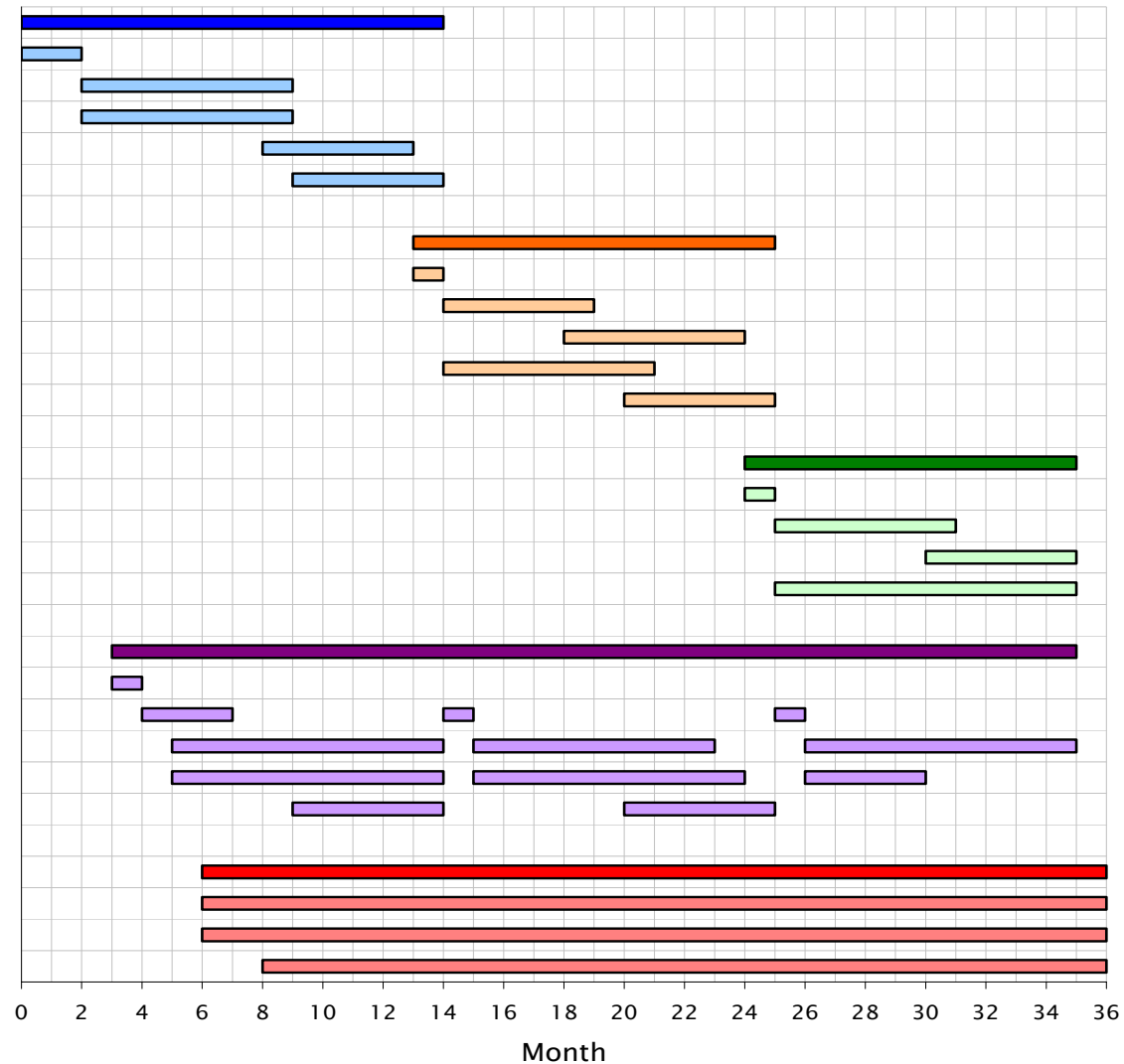
▶ Related patents:

- **M. Baldi**, **M. Bianchi**, **F. Chiaraluce**, **J. Rosenthal**, **D. Schipani**, “Method and apparatus for public-key cryptography based on error correcting codes”, *Swiss Patent Application*, Ref. P160183, July 2011.
- A. Morello, **S. Tomasin**, P. Baracca, L. Vangelista and N. Benvenuto, “Method and apparatus for receiving numerical signals modulated by frequency division multiplexing”, *WIPO Patent Application*, WO 2011/024118(A2), March 2011.
- M. Butussi and **S. Tomasin**, “Interpolated channel estimation for mobile OFDM systems”, *WIPO Patent Application*, WO 2010/081896, July 2010.



Project organization

11/12



ESCAPADE

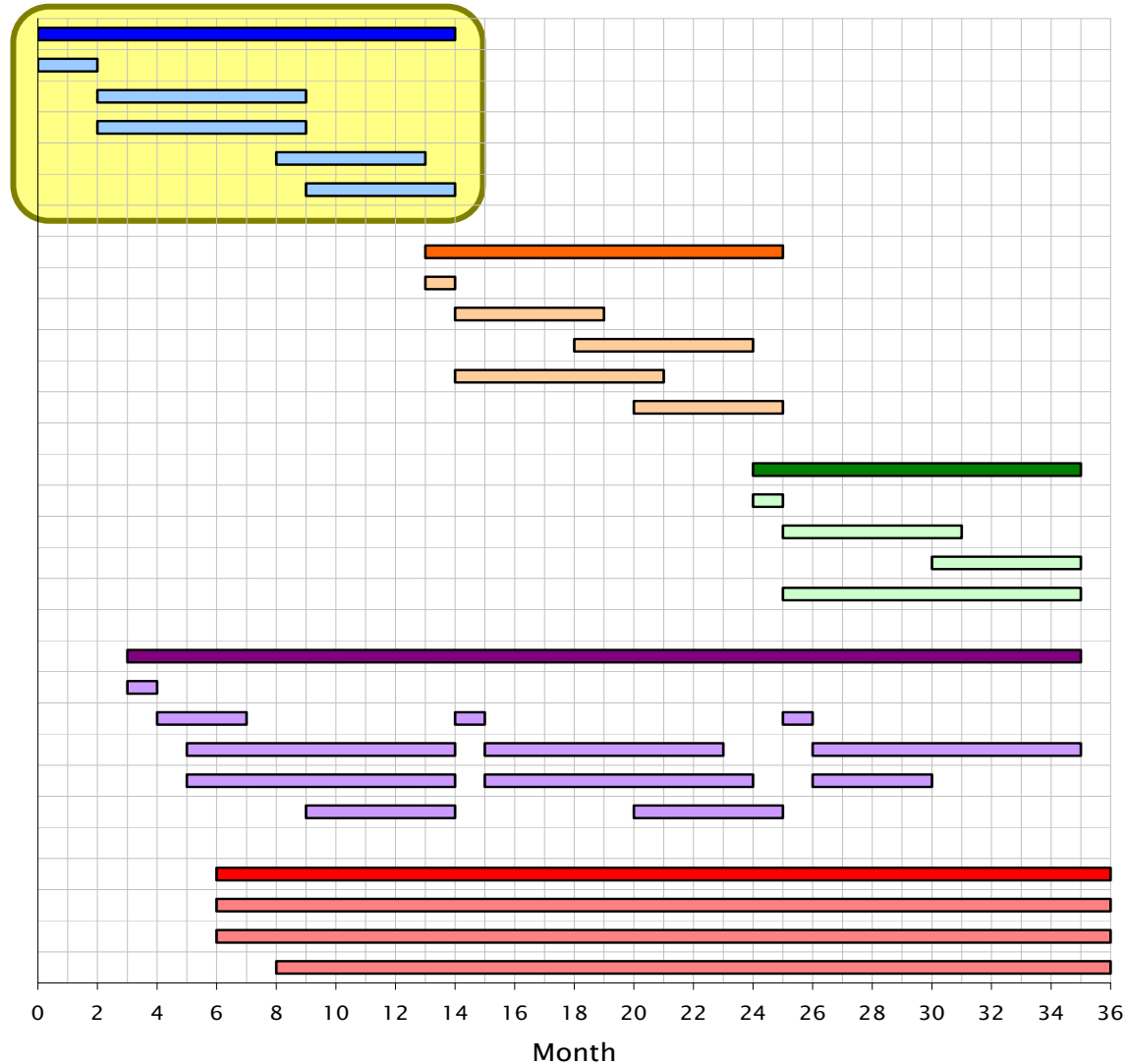
FUTURO
IN RICERCA

Project organization

11/12

WP1: PDX security for point to point transmissions

- M1.1: Definition of the system model and parameters
- M1.2: Physical layer security through OFDM techniques
- M1.3: Physical layer security through coding techniques
- M1.4: Physical layer security through HARQ techniques
- M1.5: Joint usage of OFDM, coding and HARQ



Project organization

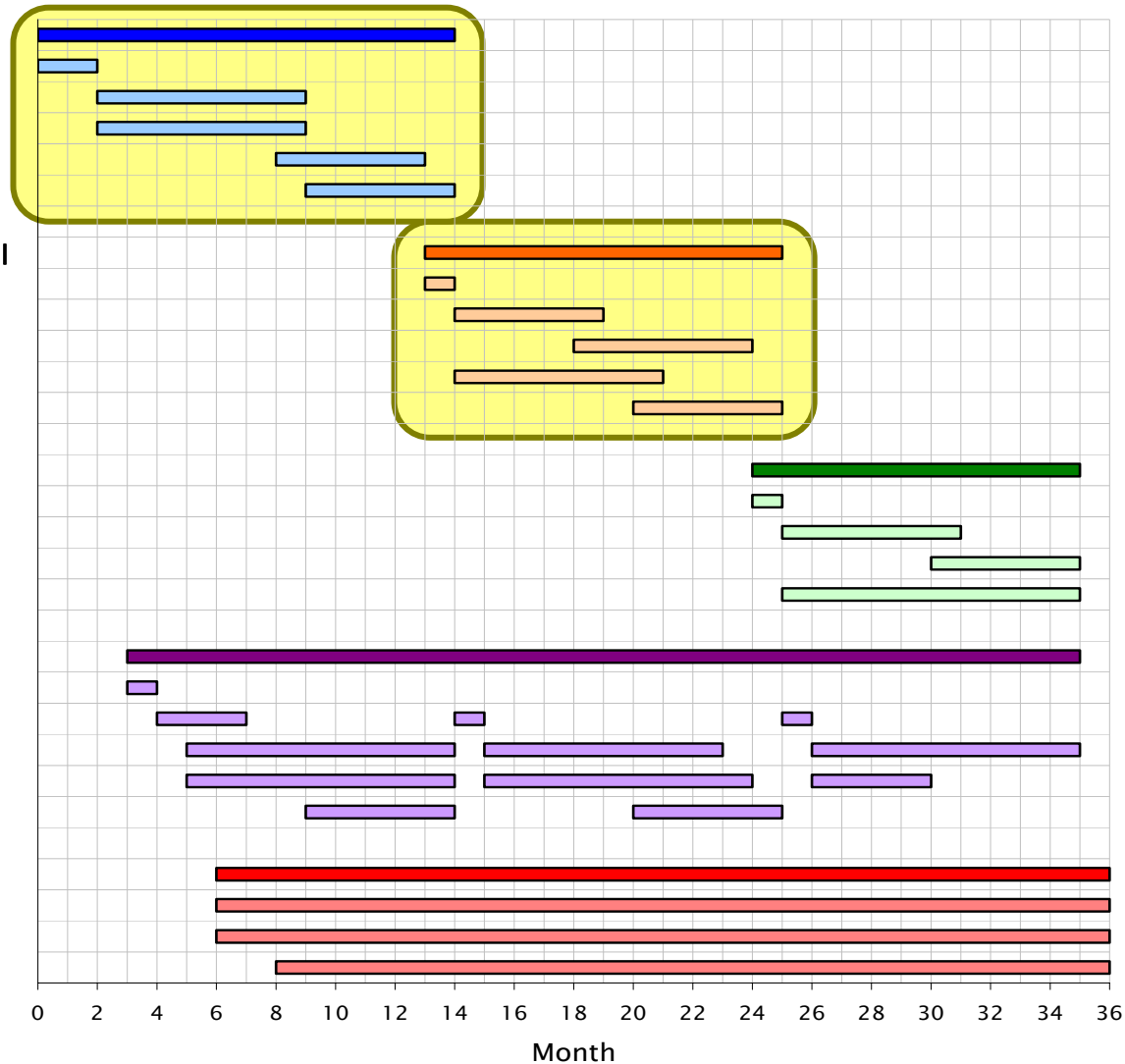
11/12

WP1: PDX security for point to point transmissions

- M1.1: Definition of the system model and parameters
- M1.2: Physical layer security through OFDM techniques
- M1.3: Physical layer security through coding techniques
- M1.4: Physical layer security through HARQ techniques
- M1.5: Joint usage of OFDM, coding and HARQ

WP2: PDX security for the confidential broadcast channel

- M2.1: Definition of the broadcast channel model
- M2.2: Algorithms for OFDM power and channels allocation
- M2.3: Design of modulation and beamforming techniques
- M2.4: Design of selective coding techniques
- M2.5: Design and optimization of HARQ strategies



ESCAPADE

FUTURO
IN RICERCA

Project organization

11/12

WP1: PDX security for point to point transmissions

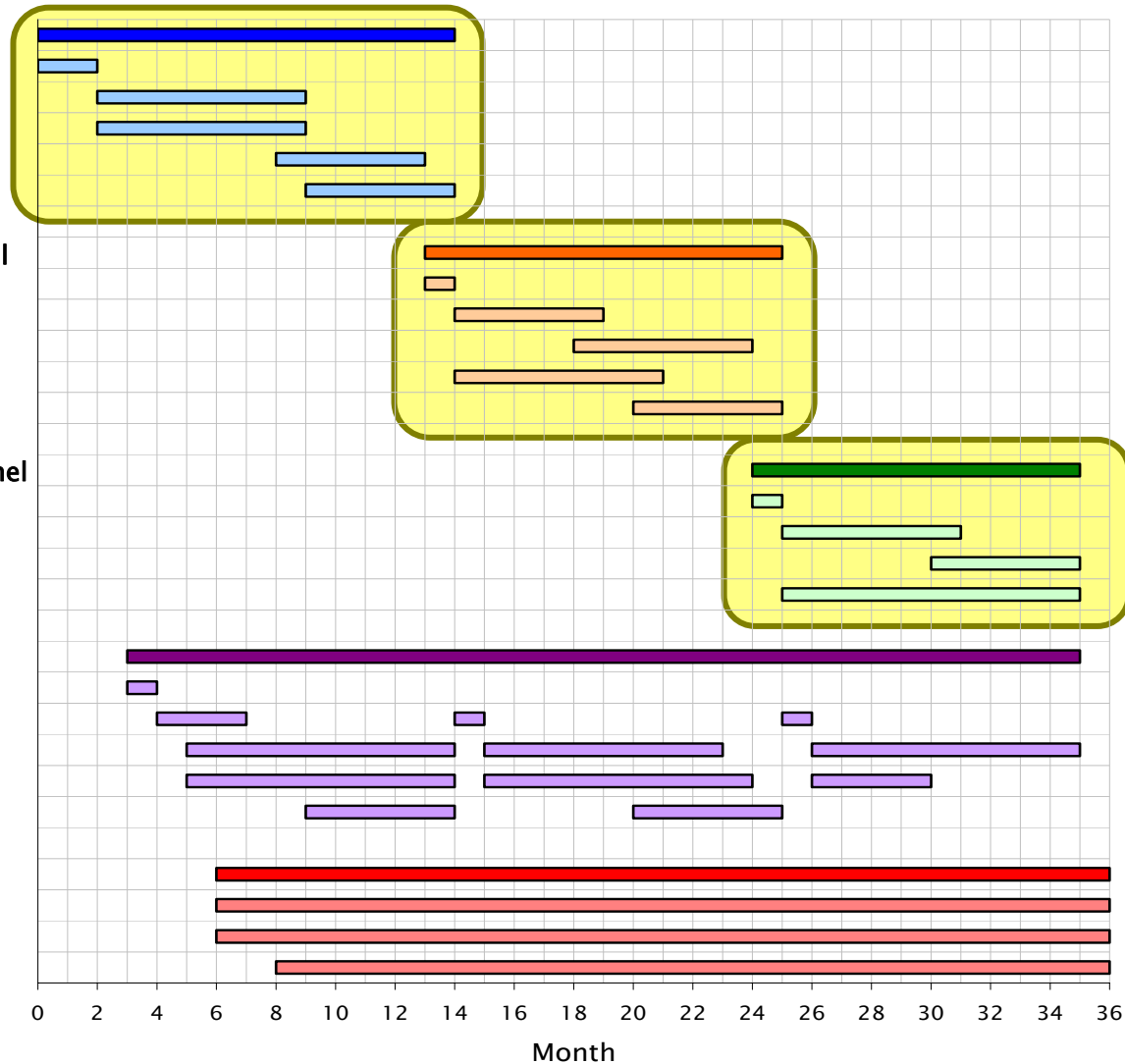
- M1.1: Definition of the system model and parameters
- M1.2: Physical layer security through OFDM techniques
- M1.3: Physical layer security through coding techniques
- M1.4: Physical layer security through HARQ techniques
- M1.5: Joint usage of OFDM, coding and HARQ

WP2: PDX security for the confidential broadcast channel

- M2.1: Definition of the broadcast channel model
- M2.2: Algorithms for OFDM power and channels allocation
- M2.3: Design of modulation and beamforming techniques
- M2.4: Design of selective coding techniques
- M2.5: Design and optimization of HARQ strategies

WP3: PDX security for cooperative multiple access channel

- M3.1: Definition of the channel model
- M3.2: Design of cooperative coding techniques
- M3.3: Design of network coding techniques
- M3.4: Design of a reputation management system



ESCAPADE

FUTURO
IN RICERCA

Project organization

11/12

WP1: PDX security for point to point transmissions

- M1.1: Definition of the system model and parameters
- M1.2: Physical layer security through OFDM techniques
- M1.3: Physical layer security through coding techniques
- M1.4: Physical layer security through HARQ techniques
- M1.5: Joint usage of OFDM, coding and HARQ

WP2: PDX security for the confidential broadcast channel

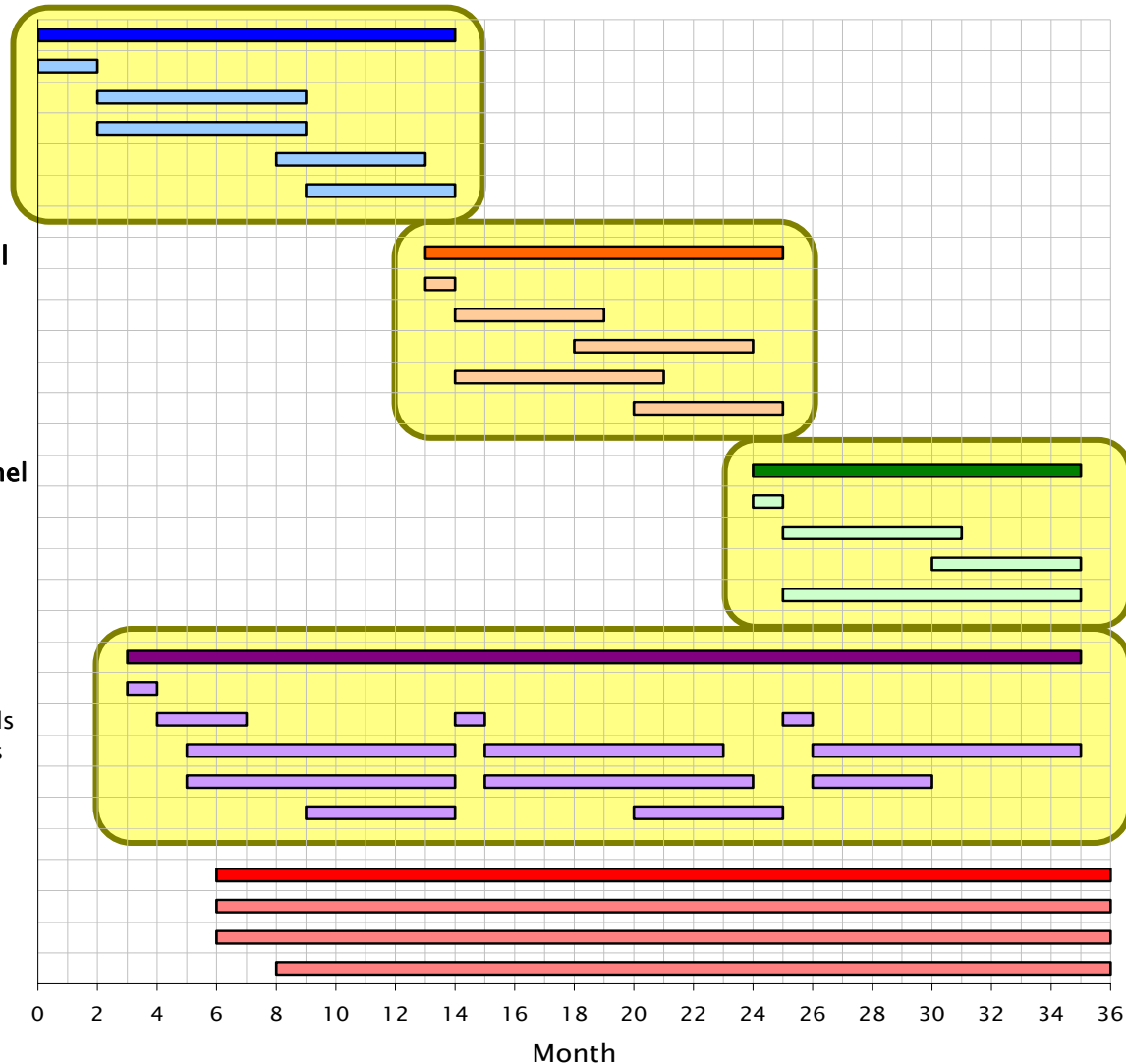
- M2.1: Definition of the broadcast channel model
- M2.2: Algorithms for OFDM power and channels allocation
- M2.3: Design of modulation and beamforming techniques
- M2.4: Design of selective coding techniques
- M2.5: Design and optimization of HARQ strategies

WP3: PDX security for cooperative multiple access channel

- M3.1: Definition of the channel model
- M3.2: Design of cooperative coding techniques
- M3.3: Design of network coding techniques
- M3.4: Design of a reputation management system

WP4: Evaluation tools for PDX security

- M4.1: Definition of software model and conventions
- M4.2: Implementation of sources/sinks and channel models
- M4.3: Implementation of the coding and decoding routines
- M4.4: Implementation of the OFDM simulation routines
- M4.5: Implementation of the HARQ simulation routines



Project organization

11/12

WP1: PDX security for point to point transmissions

- M1.1: Definition of the system model and parameters
- M1.2: Physical layer security through OFDM techniques
- M1.3: Physical layer security through coding techniques
- M1.4: Physical layer security through HARQ techniques
- M1.5: Joint usage of OFDM, coding and HARQ

WP2: PDX security for the confidential broadcast channel

- M2.1: Definition of the broadcast channel model
- M2.2: Algorithms for OFDM power and channels allocation
- M2.3: Design of modulation and beamforming techniques
- M2.4: Design of selective coding techniques
- M2.5: Design and optimization of HARQ strategies

WP3: PDX security for cooperative multiple access channel

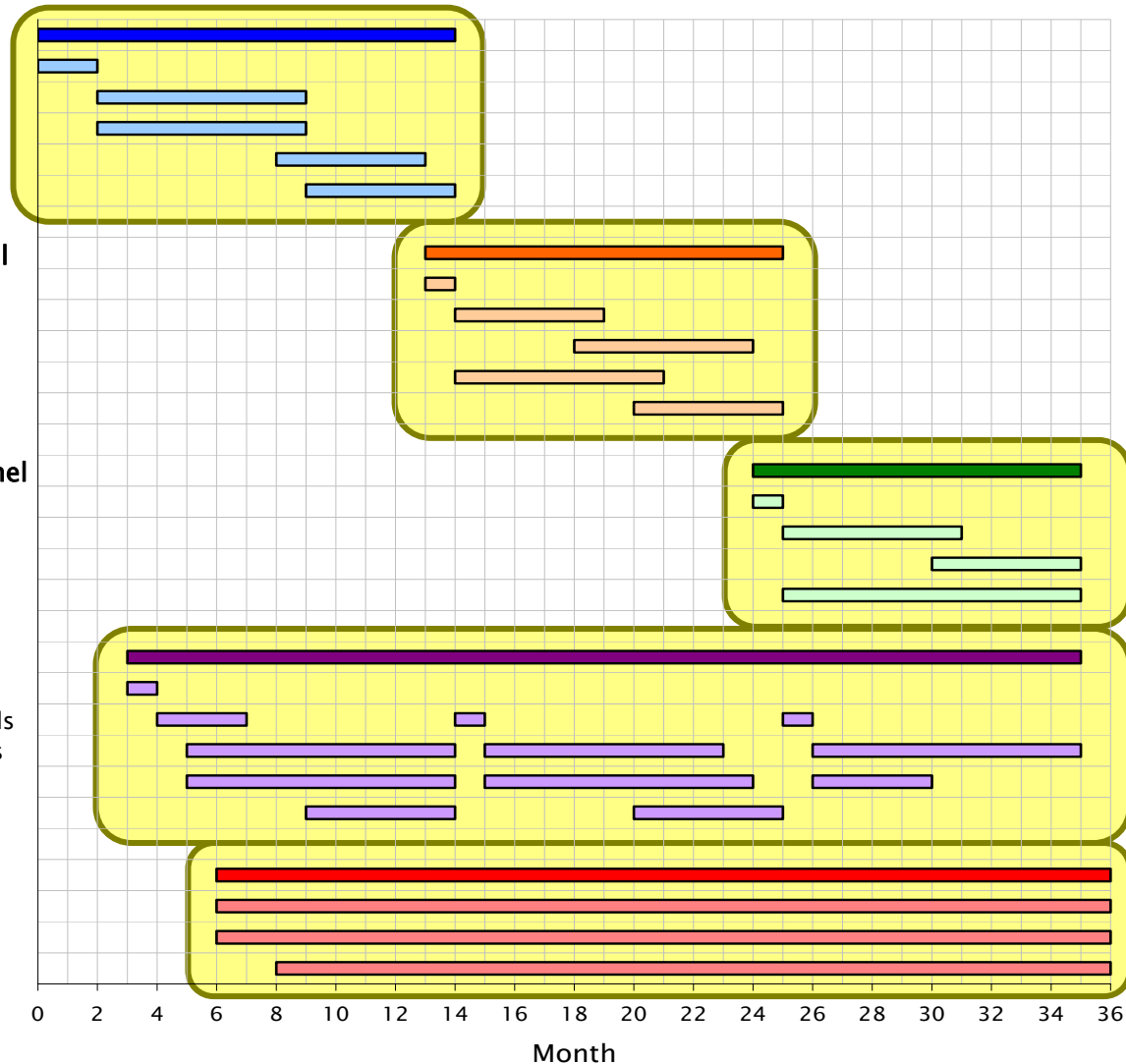
- M3.1: Definition of the channel model
- M3.2: Design of cooperative coding techniques
- M3.3: Design of network coding techniques
- M3.4: Design of a reputation management system

WP4: Evaluation tools for PDX security

- M4.1: Definition of software model and conventions
- M4.2: Implementation of sources/sinks and channel models
- M4.3: Implementation of the coding and decoding routines
- M4.4: Implementation of the OFDM simulation routines
- M4.5: Implementation of the HARQ simulation routines

WP5: Results dissemination and scientific networking

- M5.1: Preparation and submission of scientific papers
- M5.2: Development and publication of the project website
- M5.3: Scientific exchange with other research institutions



ESCAPADE

FUTURO
IN RICERCA

Outcomes per WP

- ▶ WP1 (PDX security for point to point transmissions)
 - Definition, study and simulation of new PDX techniques for wireless networks
 - Choice of coding techniques, OFDM and modulation schemes
 - Design of HARQ techniques for increased security

- ▶ WP2 (PDX security for confidential and common transmissions over the broadcast channel)
 - Design of selective coding techniques for different levels of PDX security
 - Design and optimization of algorithms for resources allocation in OFDM
 - Design of HARQ techniques for the broadcast channel

- ▶ WP3 (PDX security for cooperative multiple access channel)
 - Study of cooperative coding under the PDX security viewpoint
 - Design of network coding techniques to be integrated in the system
 - Definition of a reputation management system to improve cooperation

- ▶ WP4 (Evaluation tools for PDX security)
 - Development of a software simulator of the whole system (in C++ or Matlab/Octave)
 - Development of modified drivers for existing network cards

- ▶ WP5 (Results dissemination and scientific networking)
 - Preparation of scientific papers and submission to international journals and conferences
 - Application for international patents on security techniques and principles
 - Implementation of the project website for disseminating the results and the software tools
 - Organization of seminars, workshops and scientific visits



Outcomes per WP

- ▶ **WP1 (PDX security for point to point transmissions)**
 - Definition, study and simulation of new PDX techniques for wireless networks
 - Choice of coding techniques, OFDM and modulation schemes
 - Design of HARQ techniques for increased security
- ▶ **WP2 (PDX security for confidential and common transmissions over the broadcast channel)**
 - Design of selective coding techniques for different levels of PDX security
 - Design and optimization of algorithms for resources allocation in OFDM
 - Design of HARQ techniques for the broadcast channel
- ▶ **WP3 (PDX security for cooperative multiple access channel)**
 - Study of cooperative coding under the PDX security viewpoint
 - Design of network coding techniques to be integrated in the system
 - Definition of a reputation management system to improve cooperation
- ▶ **WP4 (Evaluation tools for PDX security)**
 - Development of a software simulator of the whole system (in C++ or Matlab/Octave)
 - Development of modified drivers for existing network cards
- ▶ **WP5 (Results dissemination and scientific networking)**
 - Preparation of scientific papers and submission to international journals and conferences
 - Application for international patents on security techniques and principles
 - Implementation of the project website for disseminating the results and the software tools
 - Organization of seminars, workshops and scientific visits

Year 1



Outcomes per WP

- ▶ **WP1 (PDX security for point to point transmissions)**
 - Definition, study and simulation of new PDX techniques for wireless networks
 - Choice of coding techniques, OFDM and modulation schemes
 - Design of HARQ techniques for increased security
- ▶ **WP2 (PDX security for confidential and common transmissions over the broadcast channel)**
 - Design of selective coding techniques for different levels of PDX security
 - Design and optimization of algorithms for resources allocation in OFDM
 - Design of HARQ techniques for the broadcast channel
- ▶ **WP3 (PDX security for cooperative multiple access channel)**
 - Study of cooperative coding under the PDX security viewpoint
 - Design of network coding techniques to be integrated in the system
 - Definition of a reputation management system to improve cooperation
- ▶ **WP4 (Evaluation tools for PDX security)**
 - Development of a software simulator of the whole system (in C++ or Matlab/Octave)
 - Development of modified drivers for existing network cards
- ▶ **WP5 (Results dissemination and scientific networking)**
 - Preparation of scientific papers and submission to international journals and conferences
 - Application for international patents on security techniques and principles
 - Implementation of the project website for disseminating the results and the software tools
 - Organization of seminars, workshops and scientific visits

Year 1

Year 2



Outcomes per WP

- ▶ **WP1 (PDX security for point to point transmissions)**
 - Definition, study and simulation of new PDX techniques for wireless networks
 - Choice of coding techniques, OFDM and modulation schemes
 - Design of HARQ techniques for increased security
- ▶ **WP2 (PDX security for confidential and common transmissions over the broadcast channel)**
 - Design of selective coding techniques for different levels of PDX security
 - Design and optimization of algorithms for resources allocation in OFDM
 - Design of HARQ techniques for the broadcast channel
- ▶ **WP3 (PDX security for cooperative multiple access channel)**
 - Study of cooperative coding under the PDX security viewpoint
 - Design of network coding techniques to be integrated in the system
 - Definition of a reputation management system to improve cooperation
- ▶ **WP4 (Evaluation tools for PDX security)**
 - Development of a software simulator of the whole system (in C++ or Matlab/Octave)
 - Development of modified drivers for existing network cards
- ▶ **WP5 (Results dissemination and scientific networking)**
 - Preparation of scientific papers and submission to international journals and conferences
 - Application for international patents on security techniques and principles
 - Implementation of the project website for disseminating the results and the software tools
 - Organization of seminars, workshops and scientific visits

Year 1**Year 2****Year 3**

Outcomes per WP

- ▶ **WP1 (PDX security for point to point transmissions)**
 - Definition, study and simulation of new PDX techniques for wireless networks
 - Choice of coding techniques, OFDM and modulation schemes
 - Design of HARQ techniques for increased security
- ▶ **WP2 (PDX security for confidential and common transmissions over the broadcast channel)**
 - Design of selective coding techniques for different levels of PDX security
 - Design and optimization of algorithms for resources allocation in OFDM
 - Design of HARQ techniques for the broadcast channel
- ▶ **WP3 (PDX security for cooperative multiple access channel)**
 - Study of cooperative coding under the PDX security viewpoint
 - Design of network coding techniques to be integrated in the system
 - Definition of a reputation management system to improve cooperation
- ▶ **WP4 (Evaluation tools for PDX security)**
 - Development of a software simulator of the whole system (in C++ or Matlab/Octave)
 - Development of modified drivers for existing network cards
- ▶ **WP5 (Results dissemination and scientific networking)**
 - Preparation of scientific papers and submission to international journals and conferences
 - Application for international patents on security techniques and principles
 - Implementation of the project website for disseminating the results and the software tools
 - Organization of seminars, workshops and scientific visits

Year 1

Year 2

Year 3

Years 1+2+3



Outcomes per WP

- ▶ **WP1 (PDX security for point to point transmissions)**
 - Definition, study and simulation of new PDX techniques for wireless networks
 - Choice of coding techniques, OFDM and modulation schemes
 - Design of HARQ techniques for increased security
- ▶ **WP2 (PDX security for confidential and common transmissions over the broadcast channel)**
 - Design of selective coding techniques for different levels of PDX security
 - Design and optimization of algorithms for resources allocation in OFDM
 - Design of HARQ techniques for the broadcast channel
- ▶ **WP3 (PDX security for cooperative multiple access channel)**
 - Study of cooperative coding under the PDX security viewpoint
 - Design of network coding techniques to be integrated in the system
 - Definition of a reputation management system to improve cooperation
- ▶ **WP4 (Evaluation tools for PDX security)**
 - Development of a software simulator of the whole system (in C++ or Matlab/Octave)
 - Development of modified drivers for existing network cards
- ▶ **WP5 (Results dissemination and scientific networking)**
 - Preparation of scientific papers and submission to international journals and conferences
 - Application for international patents on security techniques and principles
 - Implementation of the project website for disseminating the results and the software tools
 - Organization of seminars, workshops and scientific visits

Year 1

Year 2

Year 3

Years 1+2+3

Years 1+2+3



Thank you

