Il Laboratorio UnivPM di Cyber Security

Marco Baldi
Università Politecnica delle Marche
Dipartimento di Ingegneria dell'Informazione
`m.baldi@univpm.it`
`cybsec.univpm.it`

UNIVERSITÀ POLITECNICA DELLE MARCHE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

cini Cyber Security National Lab

Attività del Lab UnivPM

- **Ricerca/Innovazione**
  - Pubblicazioni scientifiche
  - Progetti di ricerca scientifica
  - Partecipazione a reti nazionali e internazionali
- **Didattica/Formazione**
  - Corsi Laurea Triennale e Magistrale
  - Seminari/Master
- **Terza missione**
  - Brevetti
  - Collaborazioni con aziende
  - Progetti di ricerca applicata

Sicurezza a tutti i livelli

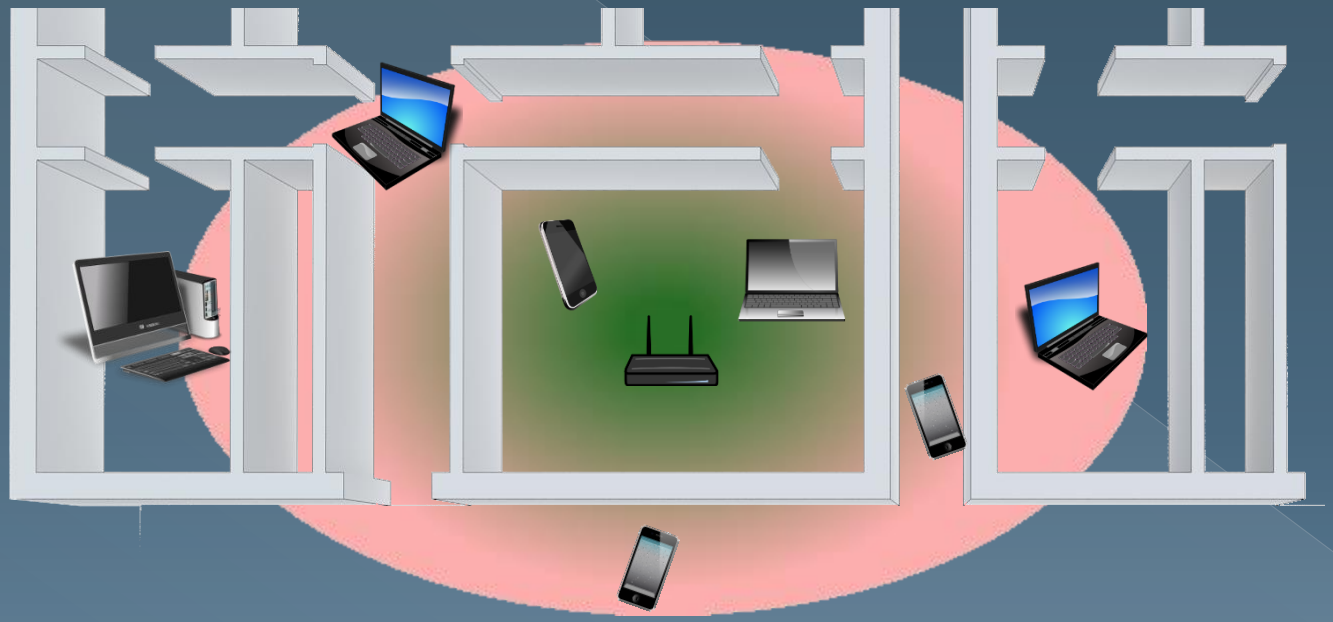
Data	**Application** Network Process to Application
Data	**Presentation** Data Representation and Encryption
Data	**Session** Interhost Communication
Segments	**Transport** End-to-End Connections and Reliability
Packets	**Network** Path Determination and IP (Logical Addressing)
Frames	**Data Link** MAC and LLC (Physical Addressing)
Bits	**Physical** Media, Signal, and Binary Transmission

Competenze Lab Univpm

	AT DESIGN TIME	RUN-TIME			POST-MORTEM
		OBFUSCATION	*MONITORING*	*ISOLATION*	
PHYSICAL		physical layer security		physical layer security	forensics
NETWORK & COMPUTER	formal verification	encryption	intrusion detection		forensics
APPLICATION	formal verification + privacy by design	encryption + privacy by design	intrusion detection		forensics

Sicurezza a livello fisico?

Sicurezza a livello fisico



rete aperta

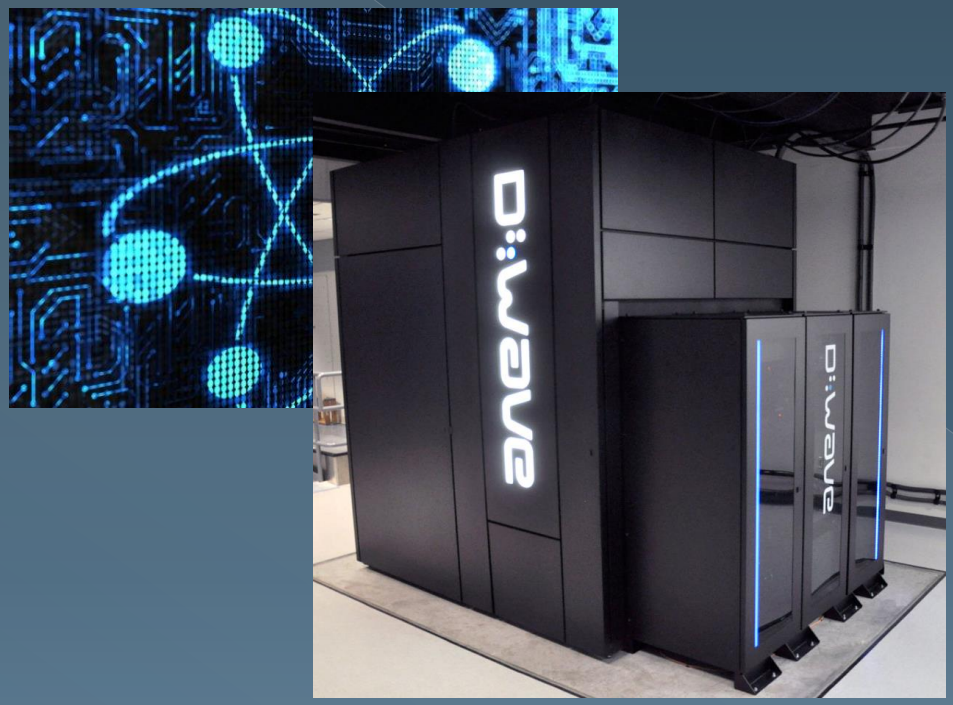
chiave precondivisa

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

PHY security

Reti wireless sicure senza bisogno di **chiavi segrete**

Crittografia Post-Quantica



*The effort to build "a **cryptologically useful** quantum computer" is part of a **$79.7 million** NSA research program titled "**Penetrating Hard Targets**."*

NISTIR 8105
DRAFT

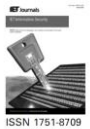
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Report on Post-Quantum Cryptography

Crittografia Post-Quantica

www.ietdl.org

Published in IET Information Security
Received on 25th February 2011
Revised on 30th December 2012
Accepted on 28th January 2013
doi: 10.1049/iet-ifs.2012.0127



ISSN 1751-8709

Security and complexity of the McEliece cryptosystem based on quasi-cyclic low-density parity-check codes

Marco Baldi, Marco Bianchi, Franco Chiaraluce
Dipartimento di Ingegneria dell'Informazione, Università Politecnica delle Marche, Ancona, Italy
E-mail: m.baldi@univpm.it

Abstract: In the context of public key cryptography, the McEliece cryptosystem represents a very smart solution based on the hardness of the decoding problem, which is believed to be able to resist the advent of quantum computers. Despite this, the original McEliece cryptosystem based on Goppa codes, has encountered limited interest in practical applications, partly because of some constraints imposed by this very special class of codes. The authors have recently introduced a variant of the McEliece cryptosystem including low-density parity-check codes, that are state-of-the-art codes, now used in many telecommunication standards and applications. In this study, the authors discuss the possible use of a bit-flipping decoder in this context, which gives a significant advantage in terms of complexity. The authors also provide theoretical arguments and practical tools for estimating the trade-off between security and complexity, in such a way to give a simple procedure for the system design.

J Criptol
DOI: 10.1007/s00145-014-9187-8

Journal of CRYPTOLOGY

Enhanced Public Key Security for the McEliece Cryptosystem*

Marco Baldi · Marco Bianchi · Franco Chiaraluce
Università Politecnica delle Marche, Ancona, Italy
m.baldi@univpm.it; m.bianchi@univpm.it; f.chiaraluce@univpm.it

Joachim Rosenthal · Davide Schipani
University of Zurich, Zurich, Switzerland
rosenthal@math.uzh.ch; davide.schipani@math.uzh.ch

Communicated by Tatsuaki Okamoto

US 20140105403A1

(19) **United States**
(12) **Patent Application Publication**
Baldi et al.
(10) **Pub. No.: US 2014/0105403 A1**
(43) **Pub. Date: Apr. 17, 2014**

(54) **METHOD AND APPARATUS FOR PUBLIC-KEY CRYPTOGRAPHY BASED ON ERROR CORRECTING CODES**

(75) Inventors: **Marco Baldi**, Macerata (MC) (IT); **Marco Bianchi**, Fano (PU) (IT); **Franco Chiaraluce**, Osimo (AN) (IT); **Joachim Jakob Rosenthal**, Zollikon (CH); **Davide Mose' Schipani**, Zurich (CH)

Assignee: **UNIVERSITAT ZURICH**, Zurich (CH)

Appl. No.: **14/110,448**
PCT Filed: **Apr. 2, 2012**
PCT No.: **PCT/EP12/56005**
§ 371 (c)(1),
(2), (4) Date: **Dec. 9, 2013**

Foreign Application Priority Data

Apr. 9, 2011 (CH) 0635/11
Jul. 7, 2011 (CH) 1140/11

Publication Classification

(52) **U.S. Cl.**
CPC *H04L 9/0819* (2013.01)
USPC **380/282**

(57) **ABSTRACT**

Methods and apparatus for generating a private-public key pair, for encrypting a message for transmission through an unsecure communication medium (**30**), and for decrypting the message are disclosed. The methods are based on the well-known McEliece cryptosystem or on its Niederreiter variant. More general transformation matrices Q are used in place of permutation matrices, possibly together with an appropriate selection of the intentional error vectors. The transformation matrices Q are non-singular non matrices having the form Q=R+T, where the matrix R is a rank-z matrix and the matrix T is some other matrix rendering Q non-singular. The new Q matrices, though at least potentially being dense, have a limited propagation effect on the intentional error vectors for the authorized receiver. The use of this kind of matrices allows to better disguise the private key into the public one, without yielding any further error propagation effect. Based on this family of Q matrices, the presently proposed cryptosystem enables the use of different families

University of Zurich[UZH]

2007 IEEE International Symposium on Information Theory

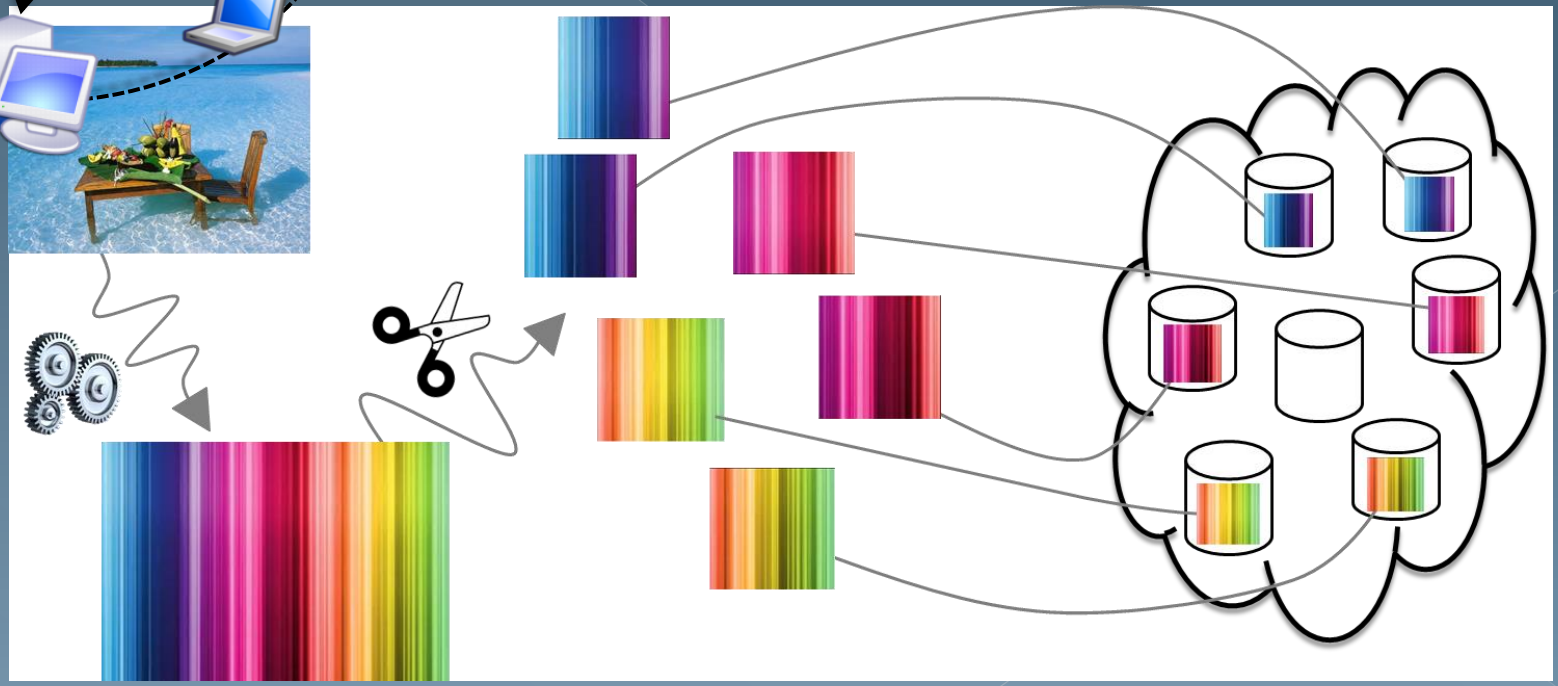
24th – 29th June 2007 • Acropolis Congress and Exhibition Center • Nice, France

ISIT 2016 BARCELONA

2016 IEEE International Symposium on Information Theory

Barcelona, Spain | July 10-15, 2016

Dispersed Cloud Storage



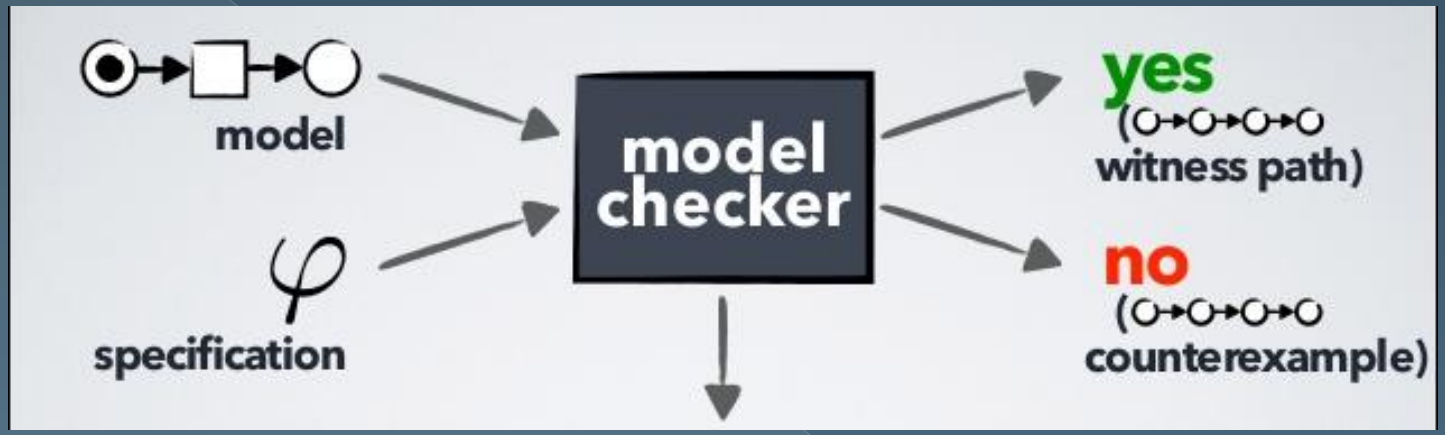
Privacy by Design & IoT Security

P_bD

GfK

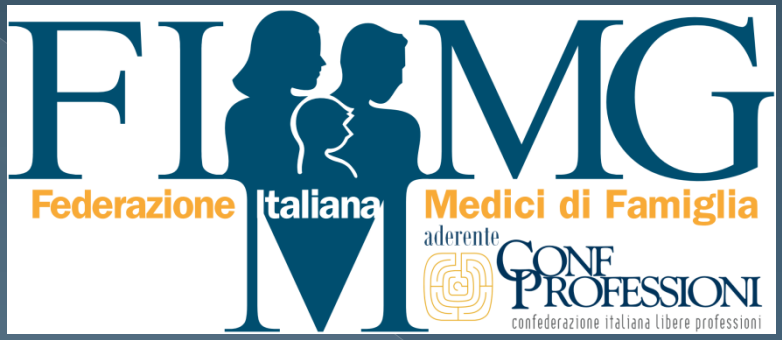
Grottinilab
Communicating with the future

Verifica Formale di Sicurezza

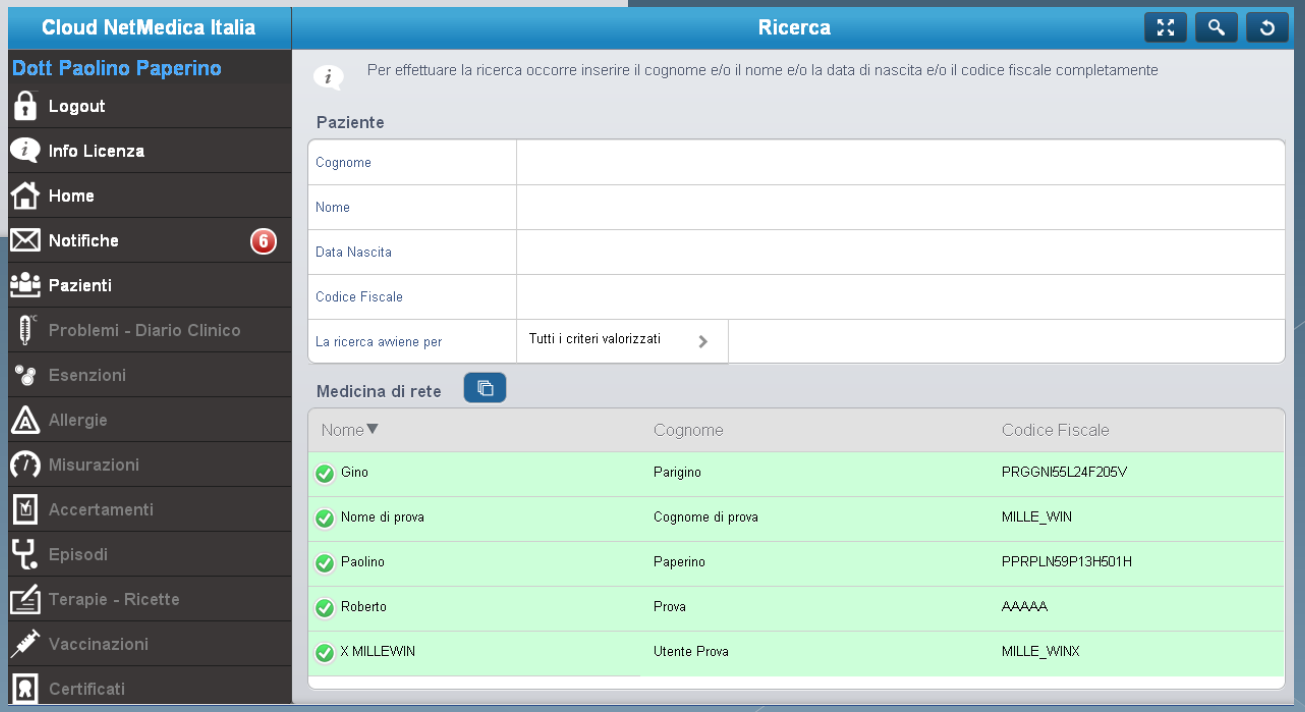


- Verificata la sicurezza di
  - SET
  - iKP
  - Dispersed Cloud Storage
- Individuate falle in:
  - SAML 2.0
  - Kerberos

Sicurezza Dati Sanitari



Nuvola Sanitaria



Consulting

- Digital Forensics
- Security Information & Incident Response

Attività Scientifica e Ricerca

- Progetto di Ricerca MIUR «**ESCAPADE**» (tot. budget 426'500 €)

Presidenza del Consiglio dei Ministri
Ministero dell'Istruzione dell'Università e della Ricerca

FUTURO IN RICERCA

- Organizzazione di conferenze/workshop

Workshop on Communication Security
September 11-12, 2014, Ancona, Italy

11th International Workshop on Security and High Performance Computing Systems (SHPCS 2016)

- Partecipazione a comitati tecnici ed editoriali

Journal of Computer Security

IEEE GlobalSIP

IEEE COMMUNICATIONS LETTERS

Future Generation Computer Systems

- Convenzioni con aziende ed enti

esa

FIMMG Federazione Italiana Medici di Famiglia aderente CONFPROFESSIONI

polizia delle comunicazioni

VIDEX
Top quality videointercoms and access control systems

Nodo del Laboratorio Nazionale di Cyber Security

- 240 Faculties
  - 68 Full Prof
  - 57 Ass. Prof
  - 100 Researchers
- 178 PhD students
- 76 postdocs
- 51 Experts

cini
Cyber Security National Lab

Gruppo Cyber Security UnivPM

- Marco Baldi
- Franco Chiaraluce
- Emanuele Frontoni
- Christian Fusciello
- Luca Spalazzi
- Primo Zingaretti
- Nicola Maturo
- Francesco Spegni
- Massimo Battaglioni
- Annalisa Cenci
- Marina Paolanti
- Giacomo Ricciutelli
- Linda Senigagliesi
- Mirco Sturari