



UNIVERSITÀ  
POLITECNICA  
DELLE MARCHE

# Gruppo codici e crittografia

## Università Politecnica delle Marche

Marco Baldi – Paolo Santini

Università Politecnica delle Marche

Dipartimento di Ingegneria dell'Informazione

[m.baldi@univpm.it](mailto:m.baldi@univpm.it), [p.santini@pm.univpm.it](mailto:p.santini@pm.univpm.it)

# Componenti del gruppo

- Giovanni Cancellieri *PO* *coding*
- Franco Chiaraluce *PA* *coding, crypto, physec*
- Marco Baldi *RTDB* *coding, crypto, physec*
- Giacomo Ricciutelli *PostDoc* *coding, physec*
- Massimo Battaglioni *PhD* *coding*
- Linda Senigagliesi *PhD* *physec*
- Paolo Santini *PhD* *coding, crypto*

*SSD: ING-INF/03 – Telecomunicazioni*

# Attività didattica

- Sicurezza nelle reti di telecomunicazione
- Privacy and security of biomedical data
- Teoria dell'informazione e codici
- Telecomunicazioni
- Trasmissioni numeriche
- Comunicazioni ottiche
- Teoria dei segnali

# Attività di ricerca

- Progetto di codici correttori o rilevatori d'errore
- Codifica di canale per comunicazioni spaziali
- Crittografia post-quantica basata su codici
- Sicurezza delle comunicazioni a livello fisico
- Information-theoretic security
- Codifica per dispersed cloud security
- Private information retrieval
- Applicazioni della tecnologia blockchain

# Progetto di codici correttori o rilevatori

- Progetto, ottimizzazione e studio delle proprietà di codici LDPC, QC-LDPC, SC-LDPC su base:
  - Algebrica
  - Combinatoria
  - Pseudo-casuale
- Progetto di codici rilevatori d'errore per canali asimmetrici e memorie.
- Studio delle proprietà strutturali di codici polari concatenati.
- M. Battaglioni, A. Tasdighi, G. Cancellieri, F. Chiaraluce and M. Baldi, «Design and Analysis of Time-Invariant SC-LDPC Convolutional Codes with Small Constraint Length», IEEE Transactions on Communications, in press.
- M. Baldi, G. Cancellieri and F. Chiaraluce, «Array Convolutional Low-Density Parity-Check Codes», IEEE Communications Letters, vol. 18, no. 2, pp. 336-339, Feb. 2014.
- M. Baldi, M. Bianchi, G. Cancellieri and F. Chiaraluce, «Progressive Differences Convolutional Low-Density Parity-Check Codes», IEEE Communications Letters, vol. 16, no. 11, pp. 1848-1851, Nov. 2012.
- M. Baldi, G. Cancellieri and F. Chiaraluce, «Interleaved Product LDPC Codes», IEEE Transactions on Communications, vol. 60, no. 4, pp. 895-901, Apr. 2012.
- M. Baldi, M. Bianchi, F. Chiaraluce, T. Kløve, «A class of punctured simplex codes which are proper for error detection», IEEE Transactions on Information Theory, vol. 58, no. 6, pp. 3861-3880, Jun. 2012.
- M. Baldi, F. Bambozzi and F. Chiaraluce, «On a Family of Circulant Matrices for Quasi-Cyclic Low-Density Generator Matrix Codes», IEEE Transactions on Information Theory, vol. 57, no. 9, pp. 6052-6067, Sep. 2011.

# Codifica per comunicazioni spaziali

- Progetto ed analisi di tecniche di codifica per comunicazioni downlink (TM) e uplink (TC).
- Trasmissioni codificate e spread spectrum per ambienti ostili (jamming, scintillazione solare).
- Sviluppo di simulatori base-band / end-to-end.
- Progetti finanziati dall'Agenzia Spaziale Europea (RESCUe, NEXCODE, PROTOCOL-A.3, ...)
- M. Baldi et al., «State-of-the-art space mission telecommand receivers», IEEE Aerospace and Electronic Systems Magazine, vol. 32, no. 6, pp. 4-15, July 2017.
- M. Baldi, N. Maturo, E. Paolini, F. Chiaraluce, «On the use of ordered statistics decoders for low-density parity-check codes in space telecommand links», EURASIP Journ. on Wirel. Commun. and Networking, vol. 2016, no. 272, pp. 1-15, Nov. 2016.
- M. Baldi, F. Chiaraluce, R. Garelo, N. Maturo, I. Aguilar Sanchez, S. Cioni, «Analysis and performance evaluation of new coding options for space telecommand links - Part I/Part II», Int. J. Satell. Commun. and Network., vol. 33, no. 6, pp. 509-525/527-542, Sep. 2014.
- M. Baldi, F. Chiaraluce, N. Maturo, G. Liva, E. Paolini, «A Hybrid Decoding Scheme for Short Non-Binary LDPC Codes», IEEE Communications Letters, vol. 18, no. 12, pp. 2093-2096, Dec. 2014.

# Sicurezza a livello fisico

- Comunicazioni sicure su canali wiretap (no chiavi segrete, solo differenze di canale).
  - Progetto ed ottimizzazione di schemi di codifica per sicurezza a livello fisico.
  - Tecniche miste physec/crypto per sicurezza su canali wiretap (senza chiavi segrete) in condizioni pratiche.
- L. Senigagliesi, M. Baldi and F. Chiaraluce, «Semantic Security with Practical Transmission Schemes over Fading Wiretap Channels», *Entropy*, vol. 19, no. 9, Sep. 2017.
  - M. Baldi, F. Chiaraluce, N. Laurenti, S. Tomasin and F. Renna, «Secrecy Transmission on Parallel Channels: Theoretical Limits and Performance of Practical Codes», *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 11, pp. 1765-1779, Nov. 2014.
  - M. Baldi, M. Bianchi, N. Maturo and F. Chiaraluce, «A Physical Layer Secured Key Distribution Technique for IEEE 802.11g Wireless Networks», *IEEE Wireless Communications Letters*, vol. 2, no. 2, pp. 183-186, Apr. 2013.
  - M. Baldi, M. Bianchi and F. Chiaraluce, «Coding With Scrambling, Concatenation, and HARQ for the AWGN Wire-Tap Channel: A Security Gap Analysis», *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 883-894, June 2012.

# Sicurezza nei sistemi dispersed cloud

- Tecniche di cifratura, codifica e slicing per sicurezza ed affidabilità nei sistemi dispersed cloud.
- No chiavi segrete.
- Metriche di sicurezza di tipo information-theoretic.
- Verifica formale di sicurezza dei protocolli progettati.
- M. Baldi, E. Bartocci, F. Chiaraluce, A. Cucchiarelli, L. Senigagliesi, L. Spalazzi and F. Spegni, «A probabilistic small model theorem to assess confidentiality of dispersed cloud storage», Proc. 14th International Conference on Quantitative Evaluation of Systems, vol. 10503 of LNCS, pp. 123-139, Springer, 2017.
- M. Baldi, F. Chiaraluce, L. Senigagliesi, L. Spalazzi and F. Spegni, «Security in heterogeneous distributed storage systems: A practically achievable information-theoretic approach», Proc. IEEE Symposium on Computers and Communications (ISCC), Heraklion, Greece, pp. 1021-1028, 2017.
- M. Baldi, L. Senigagliesi and F. Chiaraluce, “Achieving semantic security without keys through coding and all-or-nothing transforms over wireless channels”, Proc. IEEE Global Conference on Signal and Information Processing (GlobalSIP), Washington, DC, pp. 964-969, 2016.



# Private information retrieval

- Proprietà di privacy delle informazioni recuperate da un sistema di storage distribuito (DSS) basato su una rete P2P.
  - In presenza di uno o più nodi spia, essi non possono distinguere quali file l'utente vuole leggere.
  - Metriche di sicurezza di tipo information-theoretic.
  - Estensione a scenari di comunicazione più complessi.
- S. Kumar, E. Rosnes, A. Graell i Amat, «Private Information Retrieval in Distributed Storage Systems Using an Arbitrary Linear Code», Proc. IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, Jun. 2017.



# Applicazioni tecnologia blockchain

- Attività progettuale e di ricerca su applicazioni innovative della tecnologia blockchain:
    - Sviluppato e brevettato sistema basato su blockchain per il rilascio e la revoca di certificati di chiave pubblica.
    - Applicazioni su dati medico/sanitari (in fase di sviluppo).
  - Collaborazione con Namirial S.p.A.
- 
- M. Baldi and F. Chiaraluce, “A trusted cryptocurrency scheme for secure and verifiable digital transactions”, First Monday, vol. 22 no. 11, 2017.
  - M. Baldi, F. Chiaraluce, E. Frontoni, G. Gottardi, D. Sciarroni and L. Spalazzi, «Certificate Validation Through Public Ledgers and Blockchains», Proc. ITASEC17, pp. 156-165, Venice, Italy, Jan. 2017.
  - M. Baldi, F. Chiaraluce, E. Frontoni, G. Gottardi, A. Lazzari, D. Sciarroni e L. Spalazzi, «Sistema e metodo per la gestione e validazione di certificati digitali», domanda di brevetto 102017000017721, Feb. 2017.

# Crittografia post-quantica



# Crittografia post-quantica

- È dimostrato che problemi come la fattorizzazione di grandi interi e il calcolo del logaritmo discreto possono essere risolti in tempo polinomiale con algoritmi quantistici.
- I sistemi di crittografia asimmetrica attualmente più diffusi (RSA, ElGamal, DSA, ECDSA, Diffie-Hellman, ...) non possono essere ritenuti sicuri.
- Call NIST per proposte di sistemi crittografici post-quantici.



- P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput., Vol. 26, No. 5, pp. 1484-1509, 1997.
- L. K. Grover, "A fast quantum mechanical algorithm for database search," Proc. 28th Annual ACM Symposium on the Theory of Computing, p. 212, 1996.
- NIST Post-quantum crypto project. <http://csrc.nist.gov/groups/ST/post-quantum-crypto/>

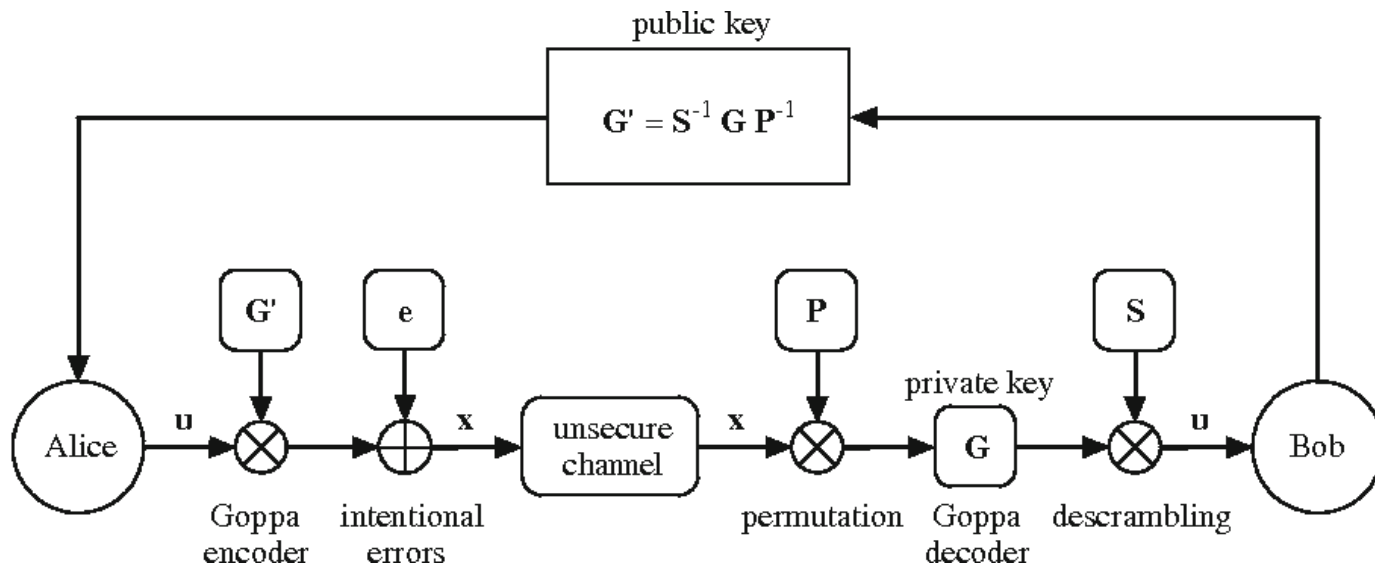
# Crittografia basata su codici

- I sistemi basati su codici sono ritenuti tra i candidati più promettenti per la crittografia post-quantica.
- *Syndrome Decoding Problem (SDP)*: un codice random non può essere decodificato in tempo polinomiale.
- Errori intenzionali vengono introdotti in cifratura; la conoscenza della chiave privata consente di decodificarli in modo efficiente.

- NIST Internal Report 8105, "Report on Post-Quantum Cryptography," Feb. 2016.

# Sistema di McEliece

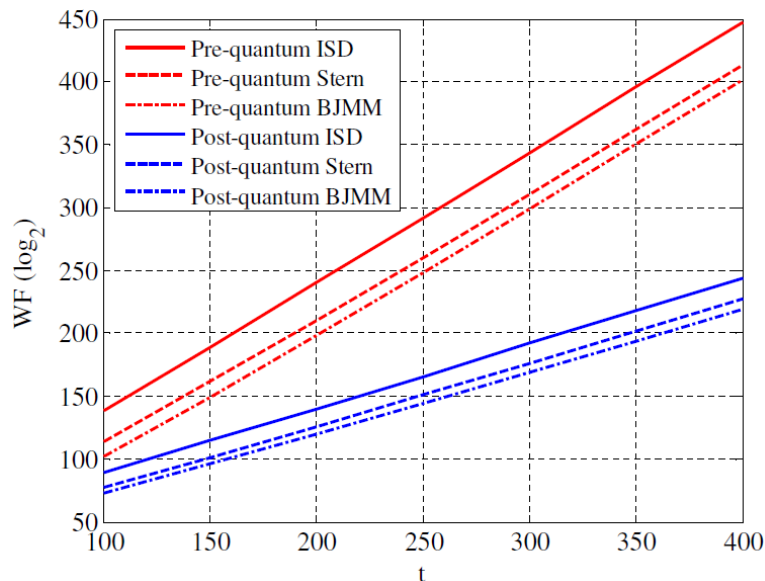
- Proposto nel 1978 da Robert McEliece.
- La struttura del codice privato è offuscata tramite permutazioni e scrambling, affinché la chiave pubblica sia indistinguibile dalla matrice generatrice di un codice random.



- R. McEliece, "Public-Key System Based on Algebraic Coding Theory," DSN Progress Report 44, pp. 114-116, 1978.

# Sistema di McEliece: sicurezza

- I migliori attacchi post-quantici hanno complessità  $WF \approx 2^{\alpha t}$ , con  $t = |e|$ .



- Chiavi pubbliche grandi: più di 100 *kB* per 80-bit security.
- Y. Hamdaoui, N. Sendrier, "A non asymptotic analysis of information set decoding," IACR Cryptology ePrint Archive, Report 2013/162.
- S.H.S. de Vries, "Achieving 128-bit Security against Quantum Attacks in OpenVPN," Master Thesis, University of Twente, 2016.

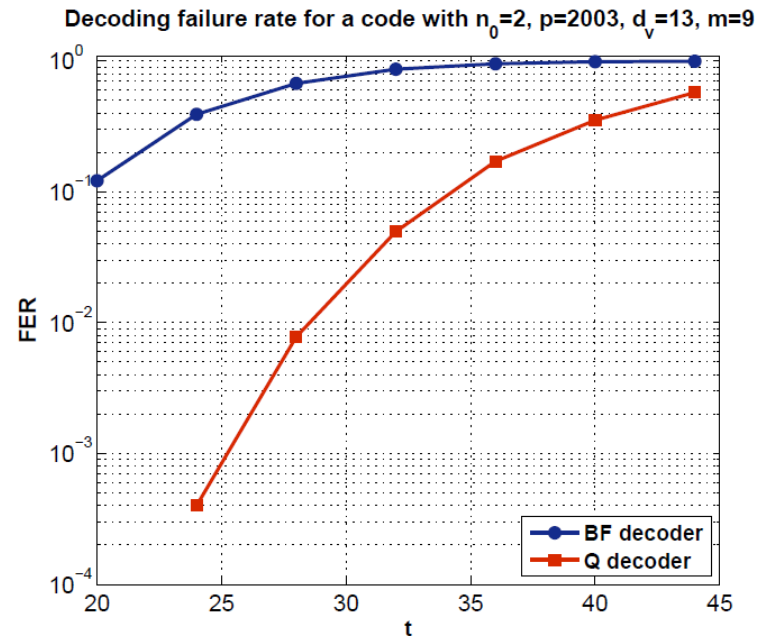
# Codici QC-LDPC in McEliece

- Sostituire codici Goppa con codici quasi-ciclici (QC) per comprimere la chiave; utilizzare codici *low-density parity-check* (LDPC) per decodificare in modo efficiente.
- Possibilità di utilizzare aritmetica polinomiale per velocizzare le operazioni matriciali.
- LEDAkem & LEDApkc: due candidati UnivPM-PoliMI basati su codici QC-LDPC al primo round della competizione NIST.
- M. Baldi, F. Chiaraluce, "Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes," Proc. IEEE ISIT 2007, Nice, France, Jun. 2007, pp. 2591-2595.
- M. Baldi, F. Chiaraluce, M. Bianchi, "Security and complexity of the McEliece cryptosystem based on quasi-cyclic low-density parity-check codes," IET Information Security, vol. 7, no. 3, pp. 212-220, 2013.
- M. Baldi, A. Barengi, F. Chiaraluce, G. Pelosi, P. Santini. "LEDAkem. first round submission to the NIST post-quantum cryptography call," Nov. 2017.
- M. Baldi, A. Barengi, F. Chiaraluce, G. Pelosi, P. Santini. "LEDApkc. first round submission to the NIST post-quantum cryptography call," Nov. 2017.



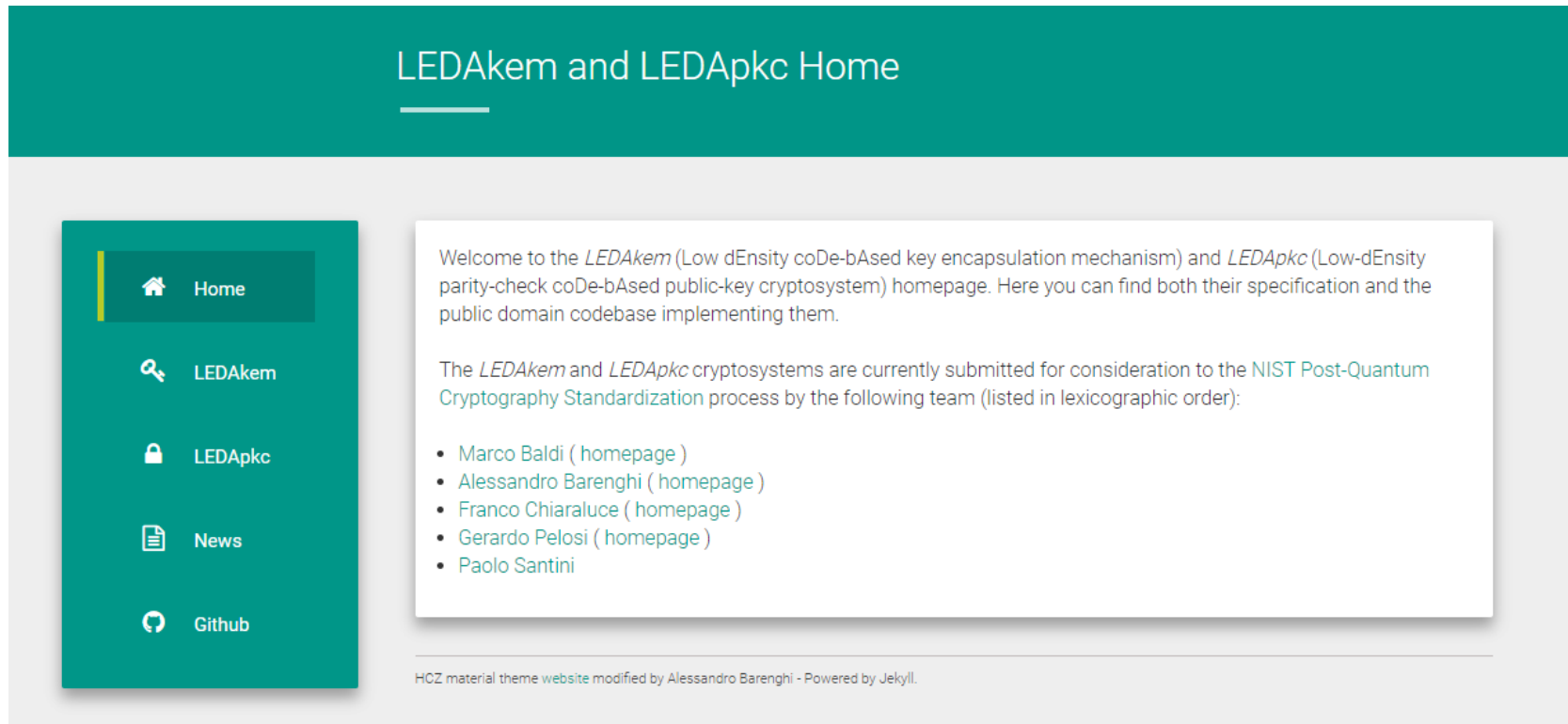
# LEDAkem & LEDApkc

- Q-decoder: nuovo algoritmo di decodifica.
- Dimensionamento post-quantico.
- Robustezza contro attacchi statistici:
  - chiavi effimere in LEDAkem;
  - stima del tempo di vita delle chiavi in LEDApkc.
- Implementazione ANSI C99 open source.



- T. Fabšic, V. Hromada, P. Stankovski, P. Zajac, Q. Guo, T. Johansson, "A reaction attack on the QC-LDPC McEliece cryptosystem," in Post-Quantum Cryptography: 8th International Workshop, PQCrypto 2017, T. Lange and T. Takagi, Eds. Utrecht, The Netherlands: Springer International Publishing, Jun. 2017, pp. 51–68.

# LEDAkem & LEDApkc



LEDAkem and LEDApkc Home

Welcome to the *LEDAkem* (Low dEnsity coDe-bAsed key encapsulation mechanism) and *LEDApkc* (Low-dEnsity parity-check coDe-bAsed public-key cryptosystem) homepage. Here you can find both their specification and the public domain codebase implementing them.

The *LEDAkem* and *LEDApkc* cryptosystems are currently submitted for consideration to the [NIST Post-Quantum Cryptography Standardization](#) process by the following team (listed in lexicographic order):

- [Marco Baldi \( homepage \)](#)
- [Alessandro Barengi \( homepage \)](#)
- [Franco Chiaraluce \( homepage \)](#)
- [Gerardo Pelosi \( homepage \)](#)
- [Paolo Santini](#)

HOZ material theme website modified by Alessandro Barengi - Powered by Jekyll.

[www.ledacrypt.org](http://www.ledacrypt.org)

# Firme digitali basate su codici QC-LDPC

- Schema proposto nel 2013: generazione efficiente delle chiavi e semplicità di decodifica.
- Generazione di firme con tempi dell'ordine del  $\mu s$ .
- Work in progress per resistere ad attacchi statistici.



- M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, D. Schipani, "Using LDGM codes and sparse syndromes to achieve digital signatures," in Post-Quantum Cryptography, ser. Lecture Notes in Computer Science, P. Gaborit, Ed. Springer Berlin Heidelberg, 2013, vol. 7932, pp. 1–15.
- A. Phezzo, J.-P. Tillich, "An Efficient Attack on a Code-Based Signature Scheme," Proc. PQCrypto 2016, vol. 9606 of LNCS, pp 86-103, 2016.
- M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani. "Method and apparatus for public-key cryptography based on error correcting codes". Pat. WO/2012/139919 – US/9191199. Oct. 2015.

# Soft McEliece

- Errori binari sostituiti da campioni gaussiani.
- Possibilità di utilizzare l'informazione soft in decodifica: chiavi compatte.
- Generando il vettore d'errore a partire da una sequenza di informazione, si aumenta l'efficienza di cifratura.
- Possibilità di attacchi basati sull'informazione soft.



- M. Baldi, P. Santini, F. Chiaraluce, "Soft McEliece: MDPC code-based McEliece cryptosystems with very compact keys through real-valued intentional errors," Proc. IEEE ISIT 2016, Barcelona, pp. 795-799, July 2016.
- Q. Guo, T. Johansson, E. Mårtensson, P. Stankovski, "Information set decoding with soft information and some cryptographic applications," Proc. IEEE ISIT 2017, Aachen, 2017, pp. 1793-1797.

# McEliece basato su codici GRS

- Utilizzo di codici Generalized Reed Solomon (GRS): massima efficienza (minime chiavi) tra i codici algebrici, ma rischio di recupero della struttura.
- Per nascondere la struttura del codice privato, la permutazione è sostituita da una matrice densa costruita come somma di una sparsa e di una densa di basso rango.
- Attacchi efficienti, ma solo per specifici set di parametri.
  - M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, D. Schipani, "Enhanced Public Key Security for the McEliece Cryptosystem," *Journal of Cryptology*, Vol. 29, No. 1, pp 1-27, 2016.
  - A. Couvreur, P. Gaborit, V. Gauthier-Umana, A. Otmani, J.-P. Tillich, "Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes," *Designs, Codes and Cryptography*, vol. 73, pp. 641-666, 2014.
  - A. Couvreur, A. Otmani, J.-P. Tillich, V. Gauthier-Umana, "A Polynomial-Time Attack on the BBCRS Scheme," *Public-Key Cryptography (PKC 2015)*, vol. 9020 of Springer LNCS, pp. 175-193, 2015.
  - M. Baldi, F. Chiaraluce, J. Rosenthal, P. Santini, D. Schipani, "On the Security of Generalized Reed-Solomon Code-Based Cryptosystems," *IET Information Security*, under review.
  - M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani. "Method and system for the digital signature". Pat. WO/2014/188336. May 2014.