

# Diversity in public key cryptography using coding theory and related problems

Nicolas Sendrier\*  
INRIA - Projet CODES - BP 105  
78153 Le Chesnay CEDEX - France  
Nicolas.Sendrier@inria.fr

**Cryptography and diversity** Most popular public key cryptographic schemes rely either on the factorisation problem (RSA, Rabin), or on the discrete logarithm problem (Diffie-Hellman, Elgamal, DSA). These systems have evolved and today instead of the classical groups  $(\mathbf{Z}/n\mathbf{Z})$  we may use groups on elliptic curves. They allow a shorter block and key size for the same level of security. An intensive effort of the research community has been and is still being conducted to investigate the main aspects of these systems: implementation, theoretical and practical security.

It must be noted that these systems all rely on algorithmic number theory. As they are used in most, if not all, applications of public key cryptography today (and it will probably remain so in the near future), cryptographic applications are vulnerable to a single breakthrough.

Diversity is the only way to dilute that risk, and the cryptographic research community should prepare and propose alternatives to the number theoretic based systems. Some propositions have been made in the last 25 years, in particular based on hard problems in algebraic coding theory. This is an interesting alternative, because these cryptosystems rely on other intractability assumptions, which keep them safe from breakthroughs in algorithmic number theory. Though they present some bad properties (a large public key for instance), these systems possess interesting features: probabilistic encryption, high throughput, easy generation of public keys (in contrast to elliptic curves generation).

**The class of McEliece like cryptosystems** The original McEliece cryptosystem [5] remains unbroken, if one is careful enough when choosing parameters. It is a trapdoor based probabilistic encryption scheme: the messages are encoded using a public code, and random noise is added to the transmitted codeword. The trapdoor is a decoding algorithm for the apparently random public code. This is implemented using Goppa codes whose support is permuted. Thus the security rely on two hard problems: either decoding a random code, either retrieving the trap-door permutation. It is well established that these problems are indeed intractable, and further work must be done to augment the area of applications of McEliece like cryptosystems. A first step in this direction has been accomplished by inventing a signature scheme with short signature [1], using a McEliece public key. The dual scheme is the Niederreiter scheme [7] which offers attractive particularities: small block size, ultra-fast encryption.

---

\*Joint work with Matthieu Finiasz (INRIA - Projet CODES), Pierre Loidreau (ENSTA) and Daniel Augot (INRIA - Projet CODES)

**Cryptosystems based on decoding the rank metric** This family of these cryptosystems is roughly based the same principle to that of McEliece cryptosystem, except that the metric in use is the rank metric [3]. This allows taking public-keys of a much smaller size than for McEliece cryptosystem, typically between ten and twenty times smaller. All the known attacks against the system have an exponential complexity in various parameters. However, Gibson showed by publishing two potential attacks that the parameters of the system had to be carefully chosen. Good parameters were proposed by Gabidulin and Ourivski. Recently Ammar, Gabidulin, Honary and Ourivski proposed the use of another family of codes which are derived from Gabidulin codes [2]. It is important to study their structure, the structure of the Gabidulin codes, and even further properties of the rank metric.

**Cryptographic hardness of Reed-Solomon decoding** While the decoding of Reed-Solomon codes has received a lot of attention from coding theorists from a positive point a view, a negative view has only been considered very recently, first by Naor and Pinkas [6] who introduced the Polynomial Reconstruction problem (PR), then more thoroughly by Kiayias and Yung [4] who established several robustness properties which are relevant to cryptography. We consider that the problem of decoding Reed-Solomon is important and quite universal, and that it may have more applications in coding theory. For instance, it is possible to design a public-key cryptosystem whose security relies on the difficulty of the PR problem. Furthermore the practical cost of solving the problem remains to be established.

## References

- [1] N. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based digital signature scheme. In *Asiacrypt 2001*, number 2248 in LNCS, pages 157–174. Springer-Verlag, 2001.
- [2] E. Gabidulin, A. Ourivski, B. Honary, and B. Ammar. A new family of rank codes and applications to cryptography. In *Proceedings IEEE ISIT 2002*, page 268, July 2002.
- [3] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. *LNCS*, 573, 1991.
- [4] A. Kiayias and M. Yung. Cryptographic hardness based on the decoding of Reed-Solomon codes with applications. In Springer-Verlag, editor, *ICALP 2002*, number 2380 in LNCS, pages 232–243, 2002.
- [5] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN Prog. Rep.*, Jet Prop. Lab., California Inst. Technol., Pasadena, CA, pages 114–116, January 1978.
- [6] M. Naor and B. Pinkas. Oblivious transfer and polynomial evaluation. In ACM, editor, *STOC 99*, pages 245–254, 1999.
- [7] H. Niederreiter. Knapsack-type crytosystems and algebraic coding theory. *Prob. Contr. Inform. Theory*, 15(2):157–166, 1986.