Pierre Loidreau,

né le 12 mars 1974
11, rue des pommiers 35520 Montreuil le Gast
Courriel : Pierre.Loidreau@m4x.org

Situation actuelle

Ingénieur Cryptologue au CELAR et chercheur associé à l'IRMAR, Université de Rennes 1

Diplômes et cursus

- 25 janvier 2007 : Diplôme d'habilitation à diriger les recherches de l'université Pierre et Marie Curie, Paris 6, spécialité Informatique. Sujet du document : *Métrique rang et cryptographie*
- 2001 Docteur en sciences de l'Ecole Polytechnique, spécialité *Algorithmique*, mention Très Honorable. Sujet de la thèse : *Etude et Optimisation de cryptosystèmes à clé publique fondés sur la théorie des codes correcteurs*, effectuée au Projet CODES de l'INRIA sous la direction de Pascale Charpin
- 1997 : DEA d'Algorithmique - Ecole Polytechnique et Paris 6
- 1996 : Diplôme d'*Ingénieur de l'Ecole Polytechnique*
- 1994-1995 : Licence et Maîtrise de mathématiques pures de l'université de Franche-Comté, option probabilités.

Encadrement de thèses

- Cédric Faure *Études de systèmes cryptographiques construits à l'aide de codes correcteurs d'erreurs* (soutenance le 17 mars 2009, co-encadrement avec N. Sendrier)
- Bassem Sakkour *Etude du décodage des codes de Reed-Muller et application à la cryptographie à clé secrète* (soutenue en avril 2007)

Liste des publications les plus significatives

1. R. Fourquet, P. Loidreau et C. Tavernier Finding good linear approximations of block ciphers and its application to cryptanalysis of reduced round DES In *Proceedings of 5th international Workshop on Coding and Cryptography, WCC 2009*, Mai 2009
2. L. Chaussade, P. Loidreau et F. Ulmer Skew codes of prescribed rank and distance In *Designs codes and cryptography*, 2008.
3. E. M. Gabidulin et P. Loidreau Properties of subspace subcodes of Gabidulin codes In *Advances in Mathematics of communication*, 2008.
4. P. Loidreau. A Welch-Berlekamp like algorithm for decoding Gabidulin codes. In *Proceedings of the 4th International Workshop on Coding and Cryptography, WCC 2005*, Mars 2005.
5. C. Faure et P. Loidreau. A new public-key cryptosystem based on the problem of reconstructing p-polynomials. In *Proceedings of the 4th International Workshop on Coding and Cryptography, WCC 2005*, Mars 2005.
6. T. P. Berger et P. Loidreau. Designing an efficient and secure public-key cryptosystem based on reducible rank codes. In *Proceedings of INDOCRYPT 2004*, Décembre 2004.
7. P. Loidreau. Sur la reconstruction des polynômes linéaires : un nouvel algorithme de décodage des codes de Gabidulin. *Comptes Rendus de l'Académie des Sciences : Série I*, 339(10) :745–750, 2004.
8. P. Loidreau. Codes derived from binary Goppa codes. *Problems of Information Transmission*, 37(2) :91-9, 2001.
9. P. Loidreau. Strengthening McEliece public-key cryptosystem. In T. Okamoto, editor, *Advances in Cryptology - ASIACRYPT 2000*, LNCS. IACR, Springer-Verlag, Décembre 2000.

10. P. Loidreau et N. Sendrier. Weak keys in McEliece public-key cryptosystem. *IEEE Transactions on Information Theory*, 47(3) :1207-1211, Mars 2001.

Activités liées à la recherche

Comités de programmes :

- Membre du comité de programme du congrès *5th International Workshop on Coding and Cryptography, WCC 2007*, avril 2007, INRIA Rocquencourt.

Responsabilité d'action :

- Responsable de l'action *Mathématiques discrètes appliquées au codage et à la protection de l'information* du programme ECO-NET du Ministère des Affaires Etrangères, consistant à développer les liens de recherches avec des pays de l'ancien bloc de l'Est. Durée : 2 ans, terminée fin décembre 2005.

Participation à des Actions :

- Membre de l'ACI OCAM (Opérateurs Cryptographiques et Arithmétique Matérielle) dontle but est d'étudier l'implantation matérielle de primitives cryptographiques utilisant la théorie algébrique des codes, septembre 2003 à août 2006.
- Membre de l'ACI ACCESS (Outils algébriques et combinatoires pour la construction et l'étude de systèmes à clé publique), 2001 à 2004.

Organisation d'événements et de séminaires :

- Membre du comité d'organisation de la conférence *Fast Software Encryption, FSE 2005*, 21–23 février 2005, ENSTA.
- Président du comité d'organisation du congrès *3rd International Workshop on Coding and Cryptography, WCC 2003*, 24–28 mars 2003, INRIA Rocquencourt.
- Membre du comité d'organisation du congrès *2nd International Workshop on Coding and Cryptography, WCC 2001*, 08–12 janvier 2001, Paris, Cercle Militaire.
- Organisateur du séminaire mensuel - 2002-2007, *Codage, Cryptographie et Algorithmique* à l'ENSTA.

Travail de rapporteur pour des revues :

- Journal of Symbolic Computation
- IEEE Transaction on Information Theory.
- Designs, Codes and Cryptography.
- Comptes Rendus de l'Académie des Sciences, série I.
- Journal of Cryptology.

Autres activité

- Membre du bureau de la SMF depuis juin 2007
- Membre du conseil d'administration de la *Société Mathématique de France* (SMF) depuis juin 2006.
- Membre de la commission enseignement de la SMF depuis juin 2003.