Code-based Cryptography – Selected publications

[1] D. Augot, M. Finiasz, Ph. Gaborit, S. Manuel, and N. Sendrier. SHA-3 proposal: FSB. Submission to the SHA-3 NIST competition, 2008.

[2] D. Augot, M. Finiasz, and N. Sendrier. A family of fast syndrome based cryptographic hash function. In E. Dawson and S. Vaudenay, editors, *Progress in Cryptology - Mycrypt 2005*, number 3715 in LNCS, pages 64–83. Springer-Verlag, 2005.

[3] T. Berger, P.-L. Cayrel, P. Gaborit, and A. Otmani. Reducing key length of the mceliece cryptosystem. In B. Preneel, editor, *Progress in Cryptology – AFRICACRYPT 2009*, number 5580 in LNCS, pages 77–97. Springer-Verlag, 2009.

[4] D. Bernstein, T. Lange, and C. Peters. Attacking and defending the McEliece cryptosystem. In J. Buchmann and J. Ding, editors, *Post-Quantum Cryptography*, number 5299 in LNCS, pages 31–46. Springer-Verlag, 2008.

[5] D. J. Bernstein, T. Lange, C. Peters, and H. van Tilborg. Explicit bounds for generic decoding algorithms for code-based cryptography. In *Pre-proceedings of WCC 2009*, pages 168–180, 2009.

[6] T. Berson. Failure of the McEliece public-key cryptosystem under message-resend and related-message attack. In B. Kalisky, editor, *CRYPTO'97*, number 1294 in LNCS, pages 213–220. Springer-Verlag, 1997.

[7] B. Biswas and N. Sendrier. Mceliece cryptosystem in real life: theory and practice. In J. Buchmann and J. Ding, editors, *PQCrypto*, number 5299 in LNCS, pages 47–62. Springer-Verlag, 2008.

[8] A. Canteaut and F. Chabaud. A new algorithm for finding minimum-weight words in a linear code: Application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511. *IEEE Transactions on Information Theory*, 44(1):367–378, January 1998.

[9] A. Canteaut and N. Sendrier. Cryptanalysis of the original McEliece cryptosystem. In *Advances in Cryptology - ASIACRYPT'98*, number 1514 in LNCS, pages 187–199. Springer-Verlag, 1998.

[10] P.-L. Cayrel, P. Gaborit, and M. Girault. Identity-based identification and signature schemes using correcting codes. In *WCC 2007*, 2007.

[11] N. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based digital signature scheme. In C. Boyd, editor, *Asiacrypt 2001*, number 2248 in LNCS, pages 157–174. Springer-Verlag, 2001.

[12] M. Finiasz and N. Sendrier. Security bounds for the design of code-based cryptosystems. In Mitsuru Matsui, editor, *Advances in Cryptology - ASIACRYPT 2009*, number 5912 in LNCS, pages 88–105. Springer, 2009.

[13] Matthieu Finiasz. *Nouvelles constructions utilisant des codes correcteurs d'erreurs en cryptographie clef publique*. Thèse de doctorat, École Polytechnique, October 2004.

[14] J.-B. Fischer and J. Stern. An efficient pseudo-random generator provably as secure as syndrome decoding. In Ueli Maurer, editor, *Advances in Cryptology - EUROCRYPT'96*, number 1070 in LNCS, pages 245–255. Springer-Verlag, 1996.

[15] P. Gaborit. Shorter keys for code based cryptography. In *Proceedings of WCC 2005*, pages 81–90, 2005.

[16] P. Gaborit and M. Girault. Lightweight code-based identification and signature. In *IEEE Conference, ISIT'07*, pages 191–195, Nice, France, July 2007. IEEE.

[17] P. Gaborit, C. Laudaroux, and N. Sendrier. Synd: a very fast code-based cipher stream with a security reduction. In *IEEE Conference, ISIT'07*, pages 186–190, Nice, France, July 2007. IEEE.

[18] J. K. Gibson. Equivalent Goppa codes and trapdoors to McEliece's public key cryptosystem. In D. W. Davies, editor, *Advances in Cryptology - EUROCRYPT'91*, number 547 in LNCS, pages 517–521. Springer-Verlag, 1991.

[19] HyMES. Hybrid McEliece Encryption Scheme. `http://www-roc.inria.fr/secret/CBCrypto/index.php?pg=hymes`. Open source software.

[20] H. Janwa and O. Moreno. McEliece public key cryptosystems using algebraic-geometric codes. *Design, Codes and Cryptography*, 8:293–307, 1996.

[21] K. Kobara and H. Imai. Semantically secure McEliece public-key cryptosystems -Conversions for McEliece PKC-. In K. Kim, editor, *PKC'2001*, number 1992 in LNCS, pages 19–35. Springer-Verlag, 2001.

[22] P. J. Lee and E. F. Brickell. An observation on the security of McEliece's public-key cryptosystem. In C. G. Günther, editor, *Advances in Cryptology - EUROCRYPT'88*, number 330 in LNCS, pages 275–280. Springer-Verlag, 1988.

[23] J. S. Leon. A probabilistic algorithm for computing minimum weights of large error-correcting codes. *IEEE Transactions on Information Theory*, 34(5):1354–1359, September 1988.

[24] P. Loidreau and N. Sendrier. Weak keys in McEliece public-key cryptosystem. *IEEE Transactions on Information Theory*, 47(3):1207–1212, April 2001.

[25] 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. Jet Prop. Lab., California Inst. Technol., Pasadena, CA.

[26] C. Aguilar Melchor, P.-L. Cayrel, and P. Gaborit. A new efficient threshold ring signature scheme based on coding theory. In J. Buchmann and J. Ding, editors, *PQCrypto*, number 5299 in LNCS, pages 1–16. Springer-Verlag, 2008.

[27] L. Minder and A. Shokrollahi. Cryptanalysis of the Sidelnikov cryptosystem. In M. Naor, editor, *Advances in Cryptology - EUROCRYPT 2007*, number 4515 in LNCS, pages 347–360. Springer, 2007.

[28] R. Misoczki and P. Barreto. Compact McEliece keys from Goppa codes. In M. J. Jacobson Jr., V. Rijmen, and R. Safavi-Naini, editors, *Selected Areas in Cryptography*, number 5867 in LNCS, pages 276–392. Springer, 2009.

[29] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Prob. Contr. Inform. Theory*, 15(2):157–166, 1986.

[30] R. Overbeck and N. Sendrier. Code-based cryptography. In D. Bernstein, J. Buchmann, and E. Dahmen, editors, *Post-Quantum Cryptography*, pages 95–145. Springer, 2009.

[31] J. P. M. Schalkwijk. An algorithm for source coding. *IEEE Transactions on Information Theory*, 18(3):395–399, May 1972.

[32] N. Sendrier. On the concatenated structure of a linear code. *AAECC*, 9(3):221–242, 1998.

[33] N. Sendrier. Finding the permutation between equivalent codes: the support splitting algorithm. *IEEE Transactions on Information Theory*, 46(4):1193–1203, July 2000.

[34] N. Sendrier. On the security of the McEliece public-key cryptosystem. In M. Blaum, P.G. Farrell, and H. van Tilborg, editors, *Information, Coding and Mathematics*, pages 141–163. Kluwer, 2002. Proceedings of Workshop honoring Prof. Bob McEliece on his 60th birthday.

[35] N. Sendrier. Encoding information into constant weight words. In *IEEE Conference, ISIT'2005*, pages 435–438, Adelaide, Australia, September 2005.

[36] V. M. Sidel'nikov. A public-key cryptosystem based on Reed-Muller codes. *Discrete Mathematics and Applications*, 4(3):191–207, 1994.

[37] V. M. Sidel'nikov and S. O. Shestakov. On cryptosystem based on generalized Reed-Solomon codes. *Discrete mathematics (in russian)*, 4(3):57–63, 1992.

[38] J. Stern. A method for finding codewords of small weight. In G. Cohen and J. Wolfmann, editors, *Coding theory and applications*, number 388 in LNCS, pages 106–113. Springer-Verlag, 1989.

[39] J. Stern. A new identification scheme based on syndrome decoding. In D. R. Stinson, editor, *Advances in Cryptology - CRYPTO'93*, number 773 in LNCS, pages 13–21. Springer-Verlag, 1993.

[40] P. Véron. A fast identification scheme. In *IEEE Conference, ISIT'95*, page 359, Whistler, BC, Canada, September 1995.