Code-based Cryptography – Selected publications

[1] Carlos Aguilar, Philippe Gaborit, and Julien Schrek. A new zero-knowledge code based identification scheme with reduced communication. In *ITW 2011*, pages 648–652, Paraty, Brazil, October 2011. IEEE.

[2] Michael Alekhnovich. More on average case vs approximation complexity. In *FOCS 2003*, pages 298–307. IEEE, 2003.

[3] Michael Alekhnovich. More on average case vs approximation complexity. *Computational Complexity*, 20(4):755–786, 2011.

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

[5] 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*, volume 3715 of *LNCS*, pages 64–83. Springer, 2005.

[6] Magali Bardet, Julia Chaulet, Vlad Dragoi, Ayoub Otmani, and Jean-Pierre Tillich. Cryptanalysis of the McEliece public key cryptosystem based on polar codes. In Tsuyoshi Takagi, editor, *PQCrypto 2016*, volume 9606 of *LNCS*, pages 118–143. Springer, 2016.

[7] Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer. Decoding random binary linear codes in $2^{n/20}$: How 1+1=0 improves information set decoding. In D. Pointcheval and T. Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 520–536. Springer, 2012.

[8] 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*, volume 5580 of *LNCS*, pages 77–97. Springer, 2009.

[9] Daniel J. Bernstein, Tung Chou, and Peter Schwabe. Mcbits: Fast constant-time code-based cryptography. In Guido Bertoni and Jean-Sébastien Coron, editors, *CHES 2013*, volume 8086 of *LNCS*, pages 250–272. Springer, 2013.

[10] D.J. Bernstein. Grover vs. mceliece. In N. Sendrier, editor, *PQCrypto*, volume 6061 of *LNCS*, pages 73–80. Springer, 2010.

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

[12] D.J. Bernstein, T. Lange, and C. Peters. Smaller decoding exponents: Ball-collision decoding. In P. Rogaway, editor, *Advances in Cryptology - CRYPTO 2011*, volume 6841 of *LNCS*, pages 743–760. Springer, 2011.

[13] D.J. Bernstein, T. Lange, and C. Peters. Wild mceliece incognito. In B.-Y. Yang, editor, *PQCrypto 2011*, volume 7071 of *LNCS*, pages 244–254. Springer, 2011.

[14] D.J. Bernstein, T. Lange, C. Peters, and P. Schwabe. Faster 2-regular information-set decoding. In Y.M. Chee, Z. Guo, S. Ling, F. Shao, Y. Tang, H. Wang, and C. Xing, editors, *IWCC 201*, volume 6639 of *LNCS*, pages 81–98. Springer, 2011.

[15] D.J. Bernstein, T. Lange, C. Peters, and P. Schwabe. Really fast syndrome-based hashing. In A. Nitaj and D. Pointcheval, editors, *Progress in Cryptology - AFRICACRYPT 2011*, volume 6737 of *LNCS*, pages 134–152. Springer, 2011.

[16] 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.

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

[18] B. Biswas and N. Sendrier. McEliece cryptosystem implementation: Theory and practice. In J. Buchmann and J. Ding, editors, *PQCrypto*, volume 5299 of *LNCS*, pages 47–62. Springer, 2008.

[19] 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.

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

[21] P.-L. Cayrel, P. Gaborit, and M. Girault. Identity-based identification and signature schemes using correcting codes. In *WCC 2007*, pages 69–78, 2007.

[22] Julia Chaulet and Nicolas Sendrier. Worst case QC-MDPC decoder for mceliece cryptosystem. In *IEEE Conference, ISIT 2016*, pages 1366–1370. IEEE Press, 2016.

[23] Tung Chou. Qcbits: Constant-time small-key code-based cryptography. In Benedikt Gierlichs and Axel Y. Poschmann, editors, *CHES 2016*, volume 9813 of *LNCS*, pages 280–300. Springer, 2016.

[24] N. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based digital signature scheme. In C. Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 157–174. Springer, 2001.

[25] Alain Couvreur, Irene Marquez Corbella, and Ruud Pellikaan. A polynomial time attack against algebraic geometry code based public key cryptosystems. In *IEEE Conference, ISIT 2014*, pages 1446–1450, Honolulu, HI, USA, July 2014. IEEE.

[26] Alain Couvreur, Ayoub Otmani, and Jean-Pierre Tillich. Polynomial time attack on wild mceliece over quadratic extensions. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 17–39. Springer, 2014.

[27] Hang Dinh, Cristopher Moore, and Alexander Russell. The mceliece cryptosystem resists quantum fourier sampling attacks. *CoRR*, abs/1008.2390, 2010.

[28] J.-C. Faugère, V. Gauthier, A. Otmani, L. Perret, and J.-P. Tillich. A distinguisher for high rate McEliece cryptosystems. In *ITW 2011*, pages 282–286, Paraty, Brazil, October 2011.

[29] J.-C. Faugère, A. Otmani, L. Perret, and J.-P. Tillich. Algebraic cryptanalysis of McEliece variants with compact keys. In H. Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 279–298. Springer, 2010.

[30] Jean-Charles Faugère, Ludovic Perret, and Frdéric de Portzamparc. Algebraic attack against variants of mceliece with goppa polynomial of a special form. In *Advances in Cryptology - ASIACRYPT 2014*, LNCS. Springer, 2014. to appear.

[31] M. Finiasz. Parallel-CFS: Strengthening the CFS McEliece-based signature scheme. In A. Biryukov, G. Gong, and D.R. Stinson, editors, *Selected Areas in Cryptography*, volume 6544 of *LNCS*, pages 159–170. Springer, 2010.

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

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

[34] 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*, volume 1070 of *LNCS*, pages 245–255. Springer, 1996.

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

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

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

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

[39] Qian Guo, Thomas Johansson, and Paul Stankovski. A key recovery attack on MDPC with CCA security using decoding errors. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016*, volume 10031 of *LNCS*, pages 789–818. Springer, December 2016.

[40] Stefan Heyse, Ingo von Maurich, and Tim Güneysu. Smaller keys for code-based cryptography: QC-MDPC McEliece implementations on embedded devices. In Guido Bertoni and Jean-Sébastien Coron, editors, *CHES*, volume 8086 of *LNCS*, pages 273–292. Springer, 2013.

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

[42] K. Kobara and H. Imai. Semantically secure McEliece public-key cryptosystems -Conversions for McEliece PKC-. In K. Kim, editor, *PKC 2001*, volume 1992 of *LNCS*, pages 19–35. Springer, 2001.

[43] G. Landais and N. Sendrier. Implementing cfs. In S. Galbraith and M. Nandi, editors, *Indocrypt 2012*, volume 7668 of *LNCS*, pages 474–488. Springer, December 2012.

[44] 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*, volume 330 of *LNCS*, pages 275–280. Springer, 1988.

[45] 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.

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

[47] C. Löndahl and T. Johansson. A new version of mceliece pkc based on convolutional codes. In Tat Wing Chim and Tsz Hon Yuen, editors, *ICICS*, volume 7618 of *LNCS*, pages 461–470. Springer, 2012.

[48] I. Marquez-Corbella, E. Martinez-Moro, and R. Pellikaan. Evaluation of public-key cryptosystems based on algebraic geometry codes. In J. Borges and M. Villanueva, editors, *Proceedings of the Third International Castle Meeting on Coding Theory and Applications*, pages 199–204, Cardona Castle, Barcelona, September 2011.

[49] A. May, A. Meurer, and E. Thomae. Decoding random linear codes in $\tilde{O}(2^{0.054n})$. In D.H. Lee and X. Wang, editors, *Advances in Cryptology - ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 107–124. Springer, 2011.

[50] Alexander May and Ilya Ozerov. On computing nearest neighbors with applications to decoding of binary linear codes. In Elisabeth Oswald and Marc Fischlin, editors,

Advances in Cryptology – EUROCRYPT 2015, Part I, volume 9056 of *LNCS*, pages 203–228. Springer, 2015.

[51] 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.

[52] 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*, volume 5299 of *LNCS*, pages 1–16. Springer, 2008.

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

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

[55] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo S. L. M. Barreto. MDPC-McEliece: New McEliece variants from moderate density parity-check codes. In *IEEE Conference, ISIT 2013*, pages 2069–2073, Instanbul, Turkey, July 2013.

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

[57] R. Nojima, H. Imai, K. Kobara, and K. Morozov. Semantic security for the mceliece cryptosystem without random oracles. *Designs, Codes and Cryptography*, 49(1-3):289–305, 2008.

[58] A. Otmani, J.-P. Tillich, and L. Dallot. Cryptanalysis of two mceliece cryptosystems based on quasi-cyclic codes. *Mathematics in Computer Science*, 3(2):129–140, April 2010.

[59] Ayoub Otmani and Jean-Pierre Tillich. An efficient attack on all concrete kks proposals. In B.-Y. Yang, editor, *PQCrypto 2011*, volume 7071 of *LNCS*, pages 98–116. Springer, 2011.

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

[61] Ray A. Perlner. Optimizing information set decoding algorithms to attack cyclosymmetric MDPC codes. In *PQCrypto 2014*, volume 8772 of *LNCS*, pages 220–228. Springer, 2014.

[62] C. Peters. *Curves, Codes, and Cryptography*. PhD thesis, Technische Universiteit Eindhoven, 2011.

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

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

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

[66] 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.

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

[68] N. Sendrier. Decoding one out of many. In B.-Y. Yang, editor, *PQCrypto 2011*, volume 7071 of *LNCS*, pages 51–67. Springer, 2011.

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

[70] 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.

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

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

[73] Rodolfo Canto Torres and Nicolas Sendrier. Analysis of information set decoding for a sub-linear error weight. In Tsuyoshi Takagi, editor, *PQCrypto 2016*, volume 9606 of *LNCS*, pages 144–161. Springer, 2016.

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

[75] C. Wieschebrink. Cryptanalysis of the niederreiter public key scheme based on grs subcodes. In N. Sendrier, editor, *PQCrypto 2010*, volume 6061 of *LNCS*, pages 61–72. Springer, 2010.