References

1. Abe M, Haralambiev K, Ohkubo M (2010) Signing on elements in bilinear groups for modular protocol design. IACR Cryptology ePrint Archive, 2010:133
2. Adida B, Rivest RL (2006) Scratch & vote: self-contained paper-based cryptographic voting. In: Proceedings of the 5th ACM workshop on privacy in electronic society. ACM, New York, pp 29–40
3. Agrawal S, Boneh D, Boyen X, Freeman DM (2010) Preventing pollution attacks in multi-source network coding. In: Public key cryptography–PKC 2010. Springer, Berlin, pp 161–176
4. Ahn JH, Boneh D, Camenisch J, Hohenberger S, Waters B et al (2012) Computing on authenticated data. In: Theory of cryptography. Springer, Berlin, pp 1–20
5. Attrapadung N, Libert B (2011) Homomorphic network coding signatures in the standard model. In: Public key cryptography–PKC 2011. Springer, Berlin, pp 17–34
6. Attrapadung N, Libert B, Peters T (2012) Computing on authenticated data: new privacy definitions and constructions. In: Advances in cryptology–ASIACRYPT 2012. Springer, Berlin, pp 367–385
7. Attrapadung N, Libert B, Peters T (2013) Efficient completely context-hiding quotable and linearly homomorphic signatures. In: Public-key cryptography–PKC 2013. Springer, Berlin, pp 386–404
8. Bernstein DJ, Buchmann J, Dahmen E (2009) Post-quantum cryptography. Springer, Berlin
9. Blake IF, Seroussi G, Smart N (1999) Elliptic curves in cryptography, vol 265. Cambridge University Press, Cambridge
10. Blumenthal D, Tavenner M (2010) The "meaningful use" regulation for electronic health records. N Engl J Med 363(6):501–504
11. Boneh D, Boyen X (2004) Short signatures without random oracles. In: Advances in cryptology–EUROCRYPT 2004. Springer, Berlin, pp 56–73
12. Boneh D, Boyen X (2008) Short signatures without random oracles and the SDH assumption in bilinear groups. J Cryptol 21(2):149–177
13. Boneh D, Boyen X (2011) Efficient selective identity-based encryption without random oracles. J Cryptol 24(4):659–693
14. Boneh D, Freeman DM (2011) Homomorphic signatures for polynomial functions. In: Advances in cryptology–EUROCRYPT 2011. Springer, Berlin, pp 149–168
15. Boneh D, Freeman DM (2011) Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures. In: Public key cryptography–PKC 2011. Springer, Berlin, pp 1–16
16. Boneh D, Boyen X, Shacham H (2004) Short group signatures. In: Advances in cryptology–CRYPTO 2004. Springer, Berlin, pp 41–55

G. Traverso et al., *Homomorphic Signature Schemes*, SpringerBriefs in Computer Science, DOI 10.1007/978-3-319-32115-8

17. Boneh D, Gentry C, Lynn B, Shacham H (2003) Aggregate and verifiably encrypted signatures from bilinear maps. In: Advances in cryptology–EUROCRYPT 2003. Springer, Berlin, pp 416–432
18. Boneh D, Freeman D, Katz J, Waters B (2009) Signing a linear subspace: signature schemes for network coding. In: Public key cryptography–PKC 2009. Springer, Berlin, pp 68–87
19. Boyen X, Fan X, Shi E (2014) Adaptively secure fully homomorphic signatures based on lattices. IACR Cryptol 2014:916. http://eprint.iacr.org/2014/916 [ePrint Archive]
20. Catalano D (2014) Homomorphic signatures and message authentication codes. In: Security and cryptography for networks. Springer, Berlin, pp 514–519
21. Catalano D, Fiore D, Warinschi B (2011) Adaptive pseudo-free groups and applications. In: Advances in cryptology–EUROCRYPT 2011. Springer, Berlin, pp 207–223
22. Catalano D, Fiore D, Warinschi B (2012) Efficient network coding signatures in the standard model. In: Public key cryptography–PKC 2012. Springer, Berlin, pp 680–696
23. Catalano D, Fiore D, Warinschi B (2014) Homomorphic signatures with efficient verification for polynomial functions. In: Advances in cryptology–CRYPTO 2014. Springer, Berlin, pp 371–389
24. Charles D, Jain K, Lauter K (2009) Signatures for network coding. Int J Inf Coding Theory 1(1):3–14
25. Chaum D, Essex A, Carback R, Clark J, Popoveniuc S, Sherman A, Vora P (2008) Scantegrity: end-to-end voter-verifiable optical-scan voting. IEEE Secur Priv 6(3):40–46
26. Cheng C, Jiang T, Liu Y, Zhang M (2015) Security analysis of a homomorphic signature scheme for network coding. Secur Commun Netw 8(18):4053–4060 (2015). doi:http://dx.doi.org/10.1002/sec.1321
27. Coron J-S, Lepoint T, Tibouchi M (2015) New multilinear maps over the integers. Technical report, Cryptology ePrint Archive, Report 2015/162. http://eprint.iacr.org
28. Cortier V, Fuchsbauer G, Galindo D (2015) Beleniosrf: a strongly receipt-free electronic voting scheme. IACR Cryptology ePrint Archive, 2015:629
29. Cramer R, Shoup V (2000) Signature schemes based on the strong RSA assumption. ACM Trans Inf Syst Secur 3(3):161–185
30. Czap L, Vajda I (2010) Signatures for multisource network coding. Technical report, ArXiv
31. Dong J, Curtmola R, Nita-Rotaru C (2011) Practical defenses against pollution attacks in wireless network coding. ACM Trans Inf Syst Secur 14(1):7
32. Dutta R, Barua R, Sarkar P (2004) Pairing-based cryptographic protocols: a survey. IACR Cryptology ePrint Archive, 2004:64
33. El Gamal T (1984) A public key cryptosystem and a signature scheme based on discrete logarithms. In: Advances in cryptology, proceedings of CRYPTO'84, Santa Barbara, CA, August 19–22, 1984, proceedings, pp 10–18
34. Freeman DM (2012) Improved security for linearly homomorphic signatures: a generic framework. In: Public key cryptography–PKC 2012. Springer, Berlin, pp 697–714
35. Gennaro R, Halevi S, Rabin T (1999) Secure hash-and-sign signatures without the random oracle. In: Advances in cryptology–EUROCRYPT 1999. Springer, Berlin, pp 123–139
36. Gennaro R, Katz J, Krawczyk H, Rabin T (2010) Secure network coding over the integers. In: Public key cryptography–PKC 2010. Springer, Berlin, pp 142–160
37. Gentry C (2009) Fully homomorphic encryption using ideal lattices. In: Proceedings of the 41st annual ACM symposium on theory of computing, STOC 2009, Bethesda, MD, May 31–June 2, 2009, pp 169–178
38. Gentry C, Peikert C, Vaikuntanathan V (2008) Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the fortieth annual ACM symposium on theory of computing. ACM, New York, pp 197–206
39. Gentry C, Sahai A, Waters B (2013) Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based. In: Advances in cryptology – CRYPTO 2013 – 33rd annual cryptology conference, Santa Barbara, CA, August 18–22, 2013. Proceedings, Part I, pp 75–92

40. Goldwasser S, Micali S, Rivest RL (1988) A digital signature scheme secure against adaptive chosen-message attacks. SIAM J Comput 17(2):281–308
41. Gorbunov S, Vaikuntanathan V, Wichs D (2015) Leveled fully homomorphic signatures from standard lattices. In: Proceedings of the forty-seventh annual ACM on symposium on theory of computing, STOC 2015, Portland, OR, June 14–17, 2015, pp 469–477
42. Guangjun L, Bin W (2013) Secure network coding against intra/inter-generation pollution attacks. Communications, China 10(8):100–110
43. Hiromasa R, Manabe Y, Okamoto T (2013) Homomorphic signatures for polynomial functions with shorter signatures. In: The 30th symposium on cryptography and information security, Kyoto
44. Hohenberger S, Waters B (2009) Short and stateless signatures from the RSA assumption. In: Advances in cryptology–CRYPTO 2009. Springer, Berlin, pp 654–670
45. Jing Z (2014) An efficient homomorphic aggregate signature scheme based on lattice. Math Probl Eng 2014:9 pp. Article ID 536527
46. Johnson R, Molnar D, Song DX, Wagner D (2002) Homomorphic signature schemes. In: Topics in cryptology - CT-RSA 2002, the cryptographer's track at the RSA conference, 2002, San Jose, CA, February 18–22, 2002, proceedings, pp 244–262
47. Kalra D, Ingram D (2006) Electronic health records. In: Information technology solutions for healthcare. Springer, Berlin, pp 135–181
48. Katz J (2010) Digital signatures. Springer, Berlin
49. Katz J, Waters B (2008) Compact signatures for network coding. http://www,cs.umd.edu/-jkatz/papers/NetworkC-dingSigs, pdf
50. Lee S-H, Gerla M, Krawczyk H, Lee K-W, Quaglia EA (2011) Performance evaluation of secure network coding using homomorphic signature. In: 2011 International symposium on network coding (NetCod). IEEE, New York, pp 1–6
51. Li F, Luo B (2012) Preserving data integrity for smart grid data aggregation. In: 2012 IEEE third international conference on smart grid communications (SmartGridComm). IEEE, New York, pp 366–371
52. Libert B, Peters T, Joye M, Yung M (2013) Linearly homomorphic structure-preserving signatures and their applications. In: Advances in cryptology–CRYPTO 2013. Springer, Berlin, pp 289–307
53. Libert B, Peters T, Joye M, Yung M (2015) Linearly homomorphic structure-preserving signatures and their applications. Des Codes Crypt 77(2–3):441–477
54. Makri E, Everts MH, de Hoogh S, Peter A, op den Akker H, Hartel PH, Jonker W (2013) Privacy-preserving verification of clinical research. In: Sicherheit 2014: Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 7. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 19–21 März 2014, Wien, Österreich, pp 481–500. http://subs.emis.de/LNI/Proceedings/Proceedings228/article4.html
55. Menezes AJ, Okamoto T, Vanstone S et al (1993) Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans Inf Theory 39(5):1639–1646
56. Menezes AJ, Van Oorschot PC, Vanstone SA (1996) Handbook of applied cryptography. CRC Press, Boca Raton, FL
57. Molnar D (2003) Homomorphic signature schemes. PhD thesis, Citeseer
58. Paillier P (1999) Public-key cryptosystems based on composite degree residuosity classes. In: Advances in cryptology - EUROCRYPT'99, international conference on the theory and application of cryptographic techniques, Prague, May 2–6, 1999, proceeding, pp 223–238
59. Park C, Itoh K, Kurosawa K (1993) Efficient anonymous channel and all/nothing election scheme. In: Advances in cryptology - EUROCRYPT'93, workshop on the theory and application of cryptographic techniques, Lofthus, May 23–27, 1993, proceedings, pp 248–259
60. Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 21(2):120–126

61. Robertson A, Cresswell K, Takian A, Petrakaki D, Crowe S, Cornford T, Barber N, Avery A, Fernando B, Jacklin A et al (2010) Implementation and adoption of nationwide electronic health records in secondary care in England: qualitative analysis of interim results from a prospective national evaluation. BMJ 341:c4564
62. Shao J, Zhang J, Ling Y, Ji M, Wei G, Ying B (2013) Multiple sources network coding signature in the standard model. In: Internet and distributed computing systems. Springer, Berlin, pp 195–208
63. Shor PW (1994) Algorithms for quantum computation: discrete logarithms and factoring. In: 35th annual symposium on foundations of computer science, 1994 proceedings. IEEE, New York, pp 124–134
64. Wang Y (2010) Insecure "provably secure network coding" and homomorphic authentication schemes for network coding. IACR Cryptology ePrint Archive, 2010:60
65. Wang F, Hu Y, Wang B (2013) Lattice-based linearly homomorphic signature scheme over binary field. Sci China Inf Sci 56(11):1–9
66. Wang F, Wang K, Li B, Gao Y (2015) Leveled strongly-unforgeable identity-based fully homomorphic signatures. In: Information security. Springer, Berlin, pp 42–60
67. Waters B (2005) Efficient identity-based encryption without random oracles. In: Advances in cryptology–EUROCRYPT 2005. Springer, Berlin, pp 114–127
68. Xia Z, Culnane C, Heather J, Jonker H, Ryan PY, Schneider S, Srinivasan S (2010) Versatile prêt à voter: handling multiple election methods with a unified interface. In: Progress in cryptology-INDOCRYPT 2010. Springer, Berlin, pp 98–114
69. Yan W, Yang M, Li L, Fang H (2012) Short signature scheme for multi-source network coding. Comput Commun 35(3):344–351
70. Yang L, Li F (2013) Detecting false data injection in smart grid in-network aggregation. In: 2013 IEEE international conference on smart grid communications (SmartGridComm). IEEE, New York, pp 408–413
71. Yu Z, Wei Y, Ramkumar B, Guan Y (2008) An efficient signature-based scheme for securing network coding against pollution attacks. In: INFOCOM 2008. The 27th conference on computer communications. IEEE. IEEE, New York
72. Yun A, Cheon JH, Kim Y (2010) On homomorphic signatures for network coding. IEEE Trans Comput (9):1295–1296
73. Zhang N (2010) Signatures for network coding
74. Zhang P, Yu J, Wang T (2012) A homomorphic aggregate signature scheme based on lattice. Chin J Electron 21(4):701–704
75. Zhang J, Shao J, Ling Y, Ji M, Wei G, Ying B (2015) Efficient multiple sources network coding signature in the standard model. Concurr Comput Pract Exp 27(10):2616–2636. doi:http://dx.doi.org/10.1002/cpe.3322
76. Zhao F, Kalker T, Médard M, Han KJ (2007) Signatures for content distribution with network coding. In: IEEE international symposium on information theory, 2007. ISIT 2007. IEEE, New York, pp 556–560