References

[1] M. Ahmadian-Attari and P.G. Farrell. Multi-dimensional ring tcm codes for fading channels. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 158–168. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[2] Alexei Ashikhmin and Alexander Barg. Minimal supports in linear codes. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 13–13. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[3] Victor Buttigieg and Patrick G. Farrell. Constructions for variable-length error-correcting codes. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 282–291. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[4] P. Caballero-Gil and A. Fúster-Sabater. Linear span analysis of a set of periodic sequence generators. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 22–33. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[5] Christian Cachin. On-line secret sharing. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 190–198. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[6] Anne Canteaut. A new algorithm for finding minimum-weight words in large linear codes. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom,*

December 18-20, 1995), volume 1025 of *LNCS*, pages 205–212. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[7] P.Z. Fan and M. Darnell. The synthesis of perfect sequences. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 63–73. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[8] Willi Geiselmann. A note on the hash function of tillich and zémor. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 257–263. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[9] Yongfei Han, Dieter Gollmann, and Chris Mitchell. Minimal weight k-sr representations. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 34–43. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[10] J.W.P. Hirschfeld. The main conjecture for mds codes. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 44–52. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[11] H.P. Ho and P. Sweeney. Soft decision decoding of reed solomon codes using the dorsch algorithm. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 94–99. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[12] Valeri Korjik, Michael Ivkov, Yuri Merinovich, Alexander Barg, and Henk C.A. van Tilborg. A broadcast key distribution scheme based on

block designs. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 2–12. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[13] Stefan Lucks. How traveling salespersons prove their identity. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 142–149. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[14] David J.C. MacKay and Radford M. Neal. Good codes based on very sparse matrices. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 100–111. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[15] C.J. Mitchell. A storage complexity based analogue of maurer key establishment using public channels. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 84–93. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[16] Graham Norton. Some decoding applications of minimal realization. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 53–62. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[17] Vladimir A. Oleshchuk. Church-rosser codes. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 199–204. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[18] W.T. Penzhorn and G.J. Kühn. Computation of low-weight parity checks for correlation attacks on stream ciphers. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 74–83. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[19] Simon J.D. Phoenix and Paul D. Townsend. Quantum cryptography: Protecting our future networks with quantum mechanics. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 112–131. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[20] Richard G.E. Pinch. Distribution of recurrent sequences modulo prime powers. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 188–189. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[21] T.M. Quirke and M. Darnell. Analysis of sequence segment keying as a method of cdma transmission. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 270–281. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[22] Cristian Radu, René Govaerts, and Joos Vandewalle. Prepaid electronic cheques using public-key certificates. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 132–141. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[23] Nicolas Sendrier. Efficient generation of binary words of given weight. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 184–187. Springer-

Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[24] Sooyoung Kim Shin and Peter Sweeney. Sequential decoding for a subcode of reed solomon codes. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 14–21. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[25] Andrew Smith and Colin Boyd. An elliptic curve analogue of mccurley's key agreement scheme. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 150–157. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[26] E.V. Stansfield and M. Walker. Coding and cryptography for speech and vision. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 213–236. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[27] Paul C. van Oorschot. Design choices and security implications in implementing diffie-hellman key agreement. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 1–1. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[28] Henk C.A. van Tilborg. Authentication codes: An area where coding and cryptology meet. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 169–183. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[29] Pascal Véron. Cryptanalysis of harari's identification scheme. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography*

and Coding, (Cirencester, United Kingdom, December 18-20, 1995), volume 1025 of *LNCS*, pages 264–269. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.

[30] Victor Zyablov, Sergo Shavgulidze, and Jorn Justesen. Some constructions of generalised concatenated codes based on unit memory codes. In Colin Boyd, editor, *Proceedings of the 5th IMA Conference on Cryptography and Coding, (Cirencester, United Kingdom, December 18-20, 1995)*, volume 1025 of *LNCS*, pages 237–256. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.