

{tag} International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

[Volume 156](#)

-
[Number 1](#)

Year of Publication: 2016

Authors:

Frimpong Twum, J. B. Hayfron-Acquah, W. W. Oblitey, R. K. Boadi

10.5120/ijca2016912342

{bibtex}2016912342.bib{/bibtex}

Abstract

The ability to detect and correct data loss is of crucial importance to securing and recovering data stored on any storage facility (most importantly, the cloud). Reed-Solomon (RS) codeword is the most used for achieving this purpose. RS codeword is widely used for detecting and recovering data transmission errors as well as data loss in storage. This paper illustrates how the coefficients of the encoding polynomial needed for the generation of the RS codeword are generated. An efficient algorithm for generating the encoding polynomial coefficient is proposed. The algorithm is implemented in JAVA for Galois Field [GF(256)] with 32 parity shards – RS[255,223]8,32 to obtain an array of 32 coefficients as follows: {232, 29,189, 50, 142, 246, 232, 15, 43, 82, 164, 238, 1, 158, 13, 119, 158, 224, 134, 227, 210, 163, 50, 107, 40, 27, 104, 253, 24, 239, 216,45}

References

1. Plank, J. S. (2013). Erasure Codes for Storage Systems. Available at: https://www.usenix.org/system/files/login/articles/10_plank-online.pdf
2. REDTITAN, (2011). Error detection and correction. Available at: <http://www.pclviewer.com/rs2/galois.html>
3. cs.cmu.edu (1998). Reed-Solomon Codes. An introduction to Reed-Solomon codes: principles, architecture and implementation. Available at: https://www.cs.cmu.edu/~guyb/realworld/reedsolomon/reed_solomon_codes.html
4. Cox, R. (2012). Finite Field Arithmetic and Reed-Solomon Coding. Available at: <http://research.swtch.com/field>
5. Trench W. F., (2003). Introduction to Real Analysis. Library of Congress Cataloging-in-Publication Data. Available at: http://ramanujan.math.trinity.edu/wtrench/texts/TRENCH_REAL_ANALYSIS.PDF
6. Wang, J. (2009). Computer Network Security Theory and Practice. Springer
7. Benvenuto, C. J. (2012). Galois Field in Cryptography. Available at: https://www.math.washington.edu/~morrow/336_12/papers/juan.pdf
8. Lynson, B. Tutorial on Reed-Solomon Error Correction Coding. NASA Tech Brief MSC-21834. Available at: <http://jeffareid.net/misc/msc-21834.pdf>
9. Hill, T. (2013). Reed Solomon Codes Explained. Available at: <https://www.tony-hill.info/app/download/.../Reed+Solomon+Explained+V1-0.pdf>
10. Plank, J. S. (1997). A Tutorial on Reed-Solomon Coding for Fault-Tolerance in RAID-like Systems. Software-Practice and Experience. Vol.27, No.9, 995–1012. Available at: <http://cgi.di.uoa.gr/~ad/M155/Papers/RS-Tutorial.pdf>
11. Mathematics Stack Exchange, (2011). Addition and Multiplication in a Galois Field Available at: <http://math.stackexchange.com/questions/89805/addition-and-multiplication-in-a-galois-field>

Index Terms

Computer Science

Algorithms

Keywords

Reed Solomon Codes, Galois Field, Encoding Polynomial, Error detection and Correction