BIBLIOGRAPHY

Afzal, M. & Masood, A. 2008. "Algebraic cryptanalysis of a nlfsr based stream cipher". *International Conference on Information & Communication Technologies: from Theory to Applications, ICTTA'08. IEEE.*

Afzal, M. & Masood, A. 2008. "Resistance of Stream Ciphers to Algebraic Recovery of Internal Secret States". *Third International Conference on Convergence and Hybrid Information Technology, ICCIT*, Vol. 2. pp. 625-630.

Agren, M., Hell, M., Johansson, T., & Meier, W. 2011. "A New Version of Grain-128 with Authentication". *Presented at SKEW 2011, skew2011.mat.dtu.dk/proceedings/.*

Andrasiu, M., Popescu, A. & Simion, G. "Statistical Evaluation of Cryptographic Algorithm" 2010. *8th International Conference on IEEE.* pp. 473 – 476

Berbain, B., Gilbert, H., & Joux, A. 2009. "Algebraic and correlation attacks against linearly filtered non linear feedback shift registers". *Selected Areas in Cryptography-SAC.* Lecture Notes in Computer Science, R. Avanzi, L. Keliher, and F. Sica, Eds., Vol. 5381. Springer- Verlag. pp. 184-198.

Berzati, A., Canovas, C., Castagnos, G., Debraize, B., Goubin, L., Gouget, A., Paillier, P., & Salgado, S. 2009. "Fault Analysis of Grain-128". *Hardware Oriented Security and trust, IEEE International Workshop.* pp. 7-14.

Bucerzan, D., Craciun, M. & Chis, V. "Stream Ciphers Analysis Method" 2010. *Int. J. of Computers, Communications & Control, ISSN 1841 - 9844.*

De Cannière, C., Kiiciik, O. and Preneel, B. 2008. "Analysis of Grain's initialization algorithm". *Progress in Cryptology – AFRICACRYPT 2008, Lecture Notes in Computer Science, Springer-Verlag,* Vol. 5023. pp. 276–289.

Dinur, I., Güneysu, T., Paar, C., Shamir, A., & Zimmermann, R. 2011. "An Experimentally Verified Attack on Full Grain-128 using Dedicated Reconfigurable Hardware". Cryptology ePrint Archive, Report 2011/282. 22 Dec 2011 <http://eprint.iacr.org/2011/282>

Dinur, I., & Shamir, A. "Breaking Grain-128 with dynamic cube attacks". 2011. *Fast Software Encryption 2011, ser. To be published in Lecture Notes in Computer Science, A. Joux, Ed. Springer-Verlag.*

Dinur, I., & Shamir, A. 2011. "Breaking Grain-128 with Dynamic Cube Attacks". *Proceedings of FSE 2011*, LNCS 6733, Springer. pp. 167-187.

Dubrova, E. A Method for Generating Full Cycles by a Composition of NLFSRs. 2012. *Cryptology ePrint Archive, Report 2012/492.* <http://eprint.iacr.org/2012/492>

Hell, M., Johansson, T., Maximov, A., & Meier, W. 2006. "A stream cipher proposal: Grain – 128". *Information Theory, IEEE International Symposium.* pp. 1614-1618.

Hell, M., Johansson, T., Maximov, A., & Meier, W. 2008. "The Grain family of stream ciphers". *New Stream Cipher Designs: The eSTREAM Finalist, LNCS 4986.* pp. 179-190.

Karmakar, S. & Roy Chowdhury, D. "Fault Analysis of Grain – 128 by Targeting NFSR". *AFRICACRYPT 2011, LNCS 6737.* pp. 298 – 315

Knellwolf, S., Meier, W., & Naya-Plasencia, M. 2010. "Conditional Differential Cryptanalysis of NLFSR Based Cryptosystems". *International Association for Cryptology Research.* pp. 130 – 145.

Lee, Y., Jeong, K., Sung, J., & Hong, S. 2008. "Related-Key Chosen IV Attacks on Grain-v1 and Grain-128". *Y. Mu, W. Susilo, and J. Seberry (Eds.), ACISP 2008, LNCS 5107*, pp. 321-335.

Li, L. "Testing Several Types of Random Number Generators" 2012.

Maximov A. 2006. "Cryptanalysis of the "Grain" family of stream ciphers".*ACM Symposium on Information, Computer and Communications Security (ASIACCS'06).* pp. 283-288.

n.a. 12 September 1997. "Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard". *Federal Register, The Daily Journal of the United States Government.* < https://www.federalregister.gov/articles/1997/09/12/97-24214/announcing-request-for-candidate-algorithm-nominations-for-the-advanced-encryption-standard>

n.a. 25 February 2013. "Plaintext". *WIKIPEDIA, The Free Encyclopedia.* < http://en.wikipedia.org/wiki/Plaintext>

n.a. 13 March 2013. "Ciphertext". *WIKIPEDIA, The Free Encyclopedia.* < http://en.wikipedia.org/wiki/Ciphertext>

n.a. 14 April 2013. "Stream Cipher". *WIKIPEDIA, The Free Encyclopedia.* < http://en.wikipedia.org/wiki/Stream_cipher>

Rotz, W., Falk, E., Wood, D. & Mulrow, J. "A Comparison of Random Number Generators Used in Business" 2001. *Proceedings of the Annual Meeting of the American Statistical Association.*

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J. & Vo, S. 2010. "A Statistical Test Suite

for Random and Pseudorandom Number Generators for Cryptographic Applications," NIST Special Publication 800-22.

Soto, J. & Bassham, L. 2000. "Randomness Testing of the Advanced Encryption Standard Finalist Candidates," <http://csrc.nist.gov/publications/nistir/ir6483.pdf>

Soto, J., "Randomness Testing of the AES Candidate Algorithms," <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.39.231>

Soto, J. "Statistical Testing of Random Number Generators" 1999, Proceedings of the 22nd National Information Systems Security Conference, Crystal City, Virginia. <http://csrc.nist.gov/groups/ST/toolkit/rng/documents/nissc-paper.pdf>

Zhang, H. & Wang, X. 2009. "Cryptanalysis of stream cipher Grain family". Cryptology ePrint Archive, Report 2009/109. 22 Dec 2011. <http://eprint.iacr.org/>

Zhao, B., Liu, Q. & Liu, X. 2011. "Evaluation of Encrypted Data Identification Methods Based on Randomness Test". *IEEE/ACM International Conference on Green Computing and Communications.*

PUBLICATIONS

1. Norul Hidayah Lot @ Ahmad Zawawi, Kamaruzzaman Seman, Nurzi Juana Mohd Zaizi. 2014. "A New Proposed Design of a Stream Cipher Algorithm: Modified Grain-128". International Journal of Computer and Information Technology. Vol. 03. September. pp. 902-908.
2. Norul Hidayah Lot @ Ahmad Zawawi, Kamaruzzaman Seman, Nurzi Juana Mohd Zaizi. 2013. "Randomness analysis on grain-128 stream cipher". (Paper). *International Conference on Mathematical Sciences and Statistics 2013 (ICMSS2013).* University Putra Malaysia (UPM). 5th - 7th February.