References

ANcode:

J. M. Diamond, "Checking codes for digital computers," Proc. IRE, vol. 43, pp. 487-488, Apr. 1955.

#第一位提出ANcode 概念

D. T. Brown, "Error detecting and error correcting binary codes for arithmetic operations," IRE Trans.

Electron. Comput., vol. EC-9, pp. 333-337, Mar. 1960

#提出An+B 編碼檢測AWE

H. L. Garner, "The Residue Number System," in IRE Transactions on Electronic Computers, vol. EC-8, no. 2, pp. 140-147, June 1959

#提出RNS

R. Chien, "On linear residue codes for burst-error correction," in IEEE Transactions on Information Theory, vol. 10, no. 2, pp. 127-133, April 1964

#延伸ANcode為Linear Residue Code

U. Schiffel, “Hardware error detection using AN-codes,” Ph.D. dissertation, Technische Universität Dresden, Fakultät Informatik, 2011.

#比較三種Arithmetic Codes，提出錯誤模型

G. G. Langdon and C. K. Tang, "Concurrent Error Detection for Group Look-ahead Binary Adders," in IBM Journal of Research and Development, vol. 14, no. 5, pp. 563-573, Sep. 1970

#提出MMR

Chao-Kai Liu and Tse Lin Wang, "Error-Correcting Codes in Binary-Coded-Decimal Arithmetic," in IEEE Transactions on Computers, vol. C-27, no. 11, pp. 977-984, Nov. 1978

H. -W. Fu, T. -Y. Chen, C. -D. Tsai, M. -W. Shen and T. -C. Huang, "AN-Coded Redundant Residue Number System for Reliable Neural Networks," 2021 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), Penghu, Taiwan, 2021, pp. 1-2

#在高可靠度神經網路第一個結合ANcode和RRNS

C. -D. Tsai, H. -W. Fu, T. -Y. Chen and T. -C. Huang, "TAIWAN Online: Test AI with AN Codes Online for Automotive Chips," 2021 IEEE International Test Conference in Asia (ITC-Asia), Shanghai, China, 2021

#有提到若Double-error correcting codes被提出後可靠度可以提高超過一萬倍

T. -C. Huang, "Self-Checking Residue Number System for Low-Power Reliable Neural Network," 2019 IEEE 28th Asian Test Symposium (ATS), Kolkata, India, 2019, pp. 37-375

#提出基於RNS的錯誤檢測與定位方法並降低功耗

L. -Y. Lin, J. Schroff, T. -P. Lin and T. -C. Huang, "Residue Number System Design Automation for Neural Network Acceleration," 2020 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan), Taoyuan, Taiwan, 2020, pp. 1-2

#提出RNS自動化設計流程與RNS神經網路硬體加速

D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the importance of checking cryptographic protocols for faults," in \*Advances in Cryptology - EUROCRYPT '97\*, Lecture Notes in Computer Science, vol. 1233, W. Fumy, Ed. Berlin, Germany: Springer-Verlag, 1997, pp. 37–51.

#探討了故障攻擊對加密系統（包括 RSA）的影響，提出檢查錯誤的重要性

R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

#原始的RSA演算法論文，介紹了其理論基礎和應用，包括質數選取和模運算的重要性

W. Stallings, "Cryptography and Network Security: Principles and Practice," 7th ed., Pearson, 2016.

#詳細討論 RSA 加密的運作原理和實現，適合學術引用

RSA涉及大量模除運算、大數運算

S. Y. Sun Yile and W. X. Wu Xingjun, "An area efficient modular arithmetic processor," 2003 5th International Conference on ASIC Proceedings, Beijing, China, 2003, pp. 1273-1276 Vol.2

#提出一種基於**改良型加速技術**的模乘算法和硬體架構

Xin Zhou and Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption," Proceedings of 2011 6th International Forum on Strategic Technology, Harbin, Heilongjiang, 2011, pp. 1118-1121

#提出了基於**模指數運算的改進方法及**不同RSA碼長(如1024-bit、2048-bit等)對安全性與運算效率的影響

##############################################################################################

T. Blum and C. Paar, "Montgomery modular exponentiation on reconfigurable hardware," Proceedings 14th IEEE Symposium on Computer Arithmetic (Cat. No.99CB36336), Adelaide, SA, Australia, 1999, pp. 70-77,

#專為可重組硬體、FPGA提出了一種高效的蒙哥馬利模指數運算架構

M. -D. Shieh, J. -H. Chen, H. -H. Wu and W. -C. Lin, "A New Modular Exponentiation Architecture for Efficient Design of RSA Cryptosystem," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 16, no. 9, pp. 1151-1161, Sept. 2008

#設計高效能的模指數運算架構，提升RSA系統的運算效率

#提出了改進版的蒙哥馬利模乘(Montgomery Modular Multiplication)演算法

########################################################################################################

RSA和故障注入攻擊(Fault Injection Attack)→產生算術錯誤

M. Joye and M. Tunstall, "Fault Analysis in Cryptography," Springer, 2012.

#專注於故障分析在加密系統(包括 RSA)中的應用，深入探討算術錯誤的影響及應對方法。

########################################################################################################

T. Chiu and W. Xiong, "SoK: Fault Injection Attacks on Cryptosystems," in Proceedings of the Hardware and Architectural Support for Security and Privacy (HASP '23), 2023.

#這篇綜述性文章系統性地分析了故障注入攻擊對各種加密系統的影響，包括RSA，並討論了相應的防護措施。

C. Giraud, "An RSA Implementation Resistant to Fault Attacks and to Simple Power Analysis," in IEEE Transactions on Computers, vol. 55, no. 9, pp. 1116-1120, Sept. 2006

#提出了一種改進的RSA簽名演算法，能夠同時抵禦故障攻擊和簡單功率分析攻擊

Berzati, Alexandre et al. “Fault Attacks on RSA Public Keys: Left-To-Right Implementations Are Also Vulnerable.” The Cryptographer's Track at RSA Conference (2009).

# RSA加密左至右模指數運算實現的潛在漏洞

########################################################################################################