# Chương 1. MỞ ĐẦU

**Tóm tắt chương:**

* *Nội dung chương mở đầu trình bày tổng quan về nhu cầu cần đến mã dòng hiện nay, mục tiêu và yêu cầu của luận văn. Nội dung tóm tắt của từng chương trong luận văn được trình bày trong phần bố cục luận văn ở phía cuối của chương*.

## Bố cục luận văn

Nội dung của luận văn được trình bày gồm:

**Chương 1. MỞ ĐẦU** trình bày nhu cầu cần đến mã dòng hiện nay trong thực tế, lý do và mục tiêu thực hiện đề tài mã dòng, đồng thời xác định được các yêu cầu đặt ra của luận văn.

**Chương 2. LÝ THUYẾT MÃ DÒNG** trình bày và hệ thống các kiến thức căn bản của mã dòng, đồng thời so sánh sự khác nhau giữa mã dòng và mã khối, nêu ra các loại kiến trúc mã dòng, các loại bộ sinh dòng khóa; trình bày lý thuyết về trường hữu hạn (trường Galois) đóng vai trò cơ sở toán học quan trọng để hiểu rõ các khái niệm liên quan đến mã dòng như: dòng khóa được sinh ra bởi bộ sinh, LFSR, S-box; trình bày các khía cạnh mật mã của dòng khóa: độ phức tạp tuyến tính và đa thức cực tiểu, phân phối mẫu, hàm tương quan, độ phức tạp cầu; sau cùng là trình bày và hệ thống phần rất quan trọng, đó là tính an toàn của mô hình mã dòng với các ý tưởng: tính an toàn dựa vào kiến trúc mã dòng, tính an toàn dựa vào các khía cạnh mật mã của dòng khóa, đặc biệt là tính an toàn dựa vào kiến trúc của bộ sinh sẽ đi sâu phân tích và khảo sát các đặc tính mật mã quan trọng của hàm Boolean và S-box ảnh hướng đến tính an toàn của bộ sinh như: tính phi tuyến (nonlinearity) và tiêu chuẩn SAC (Strict Avalanche Criterion) của hàm Boolean, tính đồng nhất sai phân của S-box.

**Chương 3. MÃ DÒNG TRÊN MẠNG DI ĐỘNG** trình bày giới thiệu về mạng di động và các thuật toán bảo mật đã có trên mạng di động; trình bày lại mô hình mã dòng ZUC và các ứng dụng của nó trong hai thuật toán bảo mật là: thuật toán mã hóa 128-EEA3 và thuật toán chứng thực thông điệp 128-EIA3; trình bày các tiêu chuẩn thiết kế các lớp (layer) trong cấu tạo của ZUC, đặc biệt đi sâu phân tích và thực nghiệm đo đạc để kiểm tra các đặc tính mật mã quan trọng của hai S-box *S*0 và *S*1 trong hàm phi tuyến *F* là: tính phi tuyến của S-box, tính đồng nhất sai phân của S-box, tiêu chuẩn SAC và tính cân bằng (balance) của các hàm thành phần của S-box.

**Chương 4. CHƯƠNG TRÌNH THỰC HIỆN** trình bày kết quả về ứng dụng thử nghiệm Voice Chat, được hiện thực thông qua thuật toán mã hóa 128-EEA3 dùng generator ZUC để đảm bảo bí mật dữ liệu trên đường truyền giữa những người thực hiện cuộc hội thoại với nhau; trình bày mô hình của ứng dụng với các yêu cầu chức năng và mô hình hoạt động; tổng kết các kết quả đạt được và chưa đạt được về mặt ứng dụng của chương trình thực hiện.

**Phụ lục A** trình bày một số đặc tính mật mã khác của hàm Boolean và của S-box ảnh hướng đến tính an toàn của bộ sinh là: bậc đại số (algebraic degree) và độ miễn đại số (algebraic immunity).

**Phụ lục B** trình bày lại cấu trúc và sự an toàn của S-box trong thuật toán mã khối AES.

**Phụ lục C** trình bày một số khái niệm khác như: lượng tin, các tiên đề ngẫu nhiên Golomb.

**Tài liệu tham khảo chương:**

[1] M.J.B. Robshaw, *“Stream Ciphers”*, RSA Laboratories Technical Report TR-701, 1995, pp. 1 – 3.

[2] Trang web của hiệp hội GSMA, *“GSM Security Algorithms”*, <http://gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/gsm_security_algorithms.htm>

[4] Thomas W.Cusick, Cunsheng Ding, Ari Renvall *,“Stream Ciphers and Number Theory”*, North-Holland Mathematical Library, 2003.

[6] Adi Shamir, *“Stream Ciphers: Dead or Alive?”*, ASIACRYPT, 2004, pp. 22 – 41.

[7] Steve Babbage, *“Stream Ciphers – What does industry want?”*, The State of the Art of Stream Ciphers, Thursday October 14, 2004, pp. 9 – 11.

# Chương 2. LÝ THUYẾT MÃ DÒNG

**Tóm tắt chương:**

* *Chương 2 hệ thống và khảo sát các lý thuyết liên quan đến mã dòng. Nội dung chương này trình bày các vấn đề chính sau:*
  + *Trình bày khái niệm mã dòng và so sánh sự khác nhau giữa mã dòng và mã khối.*
  + *Trình bày các loại mã dòng: mã dòng đồng bộ và mã dòng tự đồng bộ; trình bày và phân tích tính chất của các kiến trúc mã dòng: mã dòng đồng bộ cộng, mã dòng tự đồng bộ cộng, mã dòng đồng bộ không cộng, phương pháp mã dòng sử dụng mã khối, mã phân phối hợp tác; trình bày các loại bộ sinh có thể được dùng trong mô hình mã dòng.*
  + *Trình bày và hệ thống các kiến thức cần thiết về trường hữu hạn (trường Galois), đóng vai trò nền tảng để hiểu rõ các khái niệm liên quan đến mã dòng như: dòng khóa được sinh ra bởi bộ sinh, LFSR, S-box*
  + *Trình bày và hệ thống các khía cạnh mật mã của dòng khóa được sinh ra bởi bộ sinh như: độ phức tạp tuyến tính và đa thức cực tiểu, phân phối mẫu, hàm tương quan, độ phức tạp cầu.*
  + *Hệ thống và phân tích các vấn đề liên quan đến tính an toàn của mô hình mã dòng, với 3 ý tưởng là: tính an toàn dựa trên kiến trúc mã dòng, tính an toàn dựa trên các khía cạnh mật mã của dòng khóa, tính an toàn dựa trên kiến trúc của bộ sinh. Ý tưởng về tính an toàn dựa trên kiến trúc của bộ sinh được khảo sát và phân tích kỹ lưỡng về các đặc tính mật mã quan trọng của hàm Boolean và S-box ảnh hướng đến tính an toàn của bộ sinh như: tính phi tuyến (nonlinearity) và tiêu chuẩn SAC (Strict Avalanche Criterion) của hàm Boolean, tính đồng nhất sai phân của S-box*.

**Tài liệu tham khảo chương:**

[1] M.J.B. Robshaw, *“Stream Ciphers”*, RSA Laboratories Technical Report TR-701, 1995, pp. 1 – 3.

[16] Richard A. Mollin, *“An Introduction to Cryptography – 2nd ed”*, Taylor & Francis Group, LLC, 2007.

[9] W. Diffie, M. Hellman, *“Privacy and authentication – An introduction to cryptography”*, Proc. IEEE 67(3), 1979, pp. 415 – 417.

[10] Joseph Lano, *“CRYPTANALYSIS AND DESIGN OF SYNCHRONOUS STREAM CIPHERS”*, Katholieke Universiteit Leuven – Faculteit Ingenieurswetenschappen Arenbergkasteel, B-3001 Heverlee (Belgium), 2006.

[11] Joan B. Plumstead, *“Inferring a sequence generated by a linear congruence”*, Springer, 1998, pp. 317 – 318.

[12] Chung-Chih Li, Bo Sun, *“Using Linear Congruential Generators for Cryptographic Purposes”*, Computer Science Department – Lamar University – Beaumont, TX 77710, pp. 2 – 3.

[13] Werner Alexi, Benny Chor, Oded Goldreich, Claus P. Schnorr, *“RSA and Rabin functions: certain parts are as hard as the whole”*, Society for Industrial and Applied Mathematics Philadelphia, PA, USA, ISSN: 0097-5397, 1988, pp. 197 – 208.

[14] Edgar Ferrer, *“Acceleration of Finite Field Arithmetic with an Application to Reverse Engineering Genetic Networks”*, University of Puerto Rico at Mayaguez, 2008.

[15] J. Guajardo, S. S. Kumar, C. Paar, J. Pelzl, *“Efficient Software-Implementation of Finite Fields with Applications to Cryptography”*, Springer Science + Business Media B.V. 2006, pp. 3 – 9.

[17] James L. Massey, *“Shift-Register Synthesis and BCH Decoding”*, IEEE TRANSACTIONS ON INFORMATION THEORY, 1969, pp. 122 – 125.

[18] A. Menezes, P. van Oorschot, S. Vanstone, *“Handbook of Applied Cryptography”*, CRC Press, 1997.

[19] E. Kowalski, “*Exponential sums over finite fields, I: elementary methods*”, ETH Zurich – D-MATH, Ramistrasse 101, 8092 Zurich, Switzerland, pp. 1 – 15.

[21] Nguyễn Chánh Tú, *“Lí thuyết mở rộng trường và Galois”*, Giáo trình điện tử, Khoa Toán ĐHSP Huế, 12 – 2006.

[23] T.Beth and F.Piper. “*The stop-and-go generator*”, T. Beth and N. Cot and I. Ingemarsson, editors, Advances in Cryptology – Eurocrypt '84, pp. 88-92, Springer-Verlag, Berlin, 1984, pp. 88 – 92.

[24] D. Gollmann, “*Pseudo-random properties of cascade connections of clock controlled shift registers*”, T. Beth, N. Cot, and I. Ingemarsson, editors, Advances in Cryptology – Eurocrypt '84, pp. 93-98, Springer-Verlag, Berlin, 1985, pp. 93 – 98.

[25] W. Meier and O. Staffelbach, “*The self-Shrinking generator*”, Advances in Cryptology – Eurocrypt '94, Springer-Verlag, 1995, pp. 205 – 214.

[26] Dong Hoon Lee, Jaeheon Kim, Jin Hong, Jae Woo Han, Dukjae Moon, “*Algebraic Attacks on Summation Generators*”,Fast Software Encryption  2004, 2004, pp. 34 – 48.

[27] Martin Hell, Thomas Johansson, Willi Meier, “*Grain - a stream cipher for constrained environments*”, International Journal of Wireless and Mobile Computing, Vol. 2, No. 1, 2007, pp. 86 – 93.

[32] Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng, *“Nonlinearity and Propagation Characteristics of Balanced Boolean Functions”*, Department of Computer Science – The University of Wollongong, pp. 2 – 25.

[33] Trần Minh Triết, *“Nghiên cứu và phát triển các phương pháp bảo vệ thông tin dựa trên AES”*, Luận án Tiến sĩ, Đại học Khoa học Tự nhiên Tp.HCM, 2009.

[34] K. Nyberg, *“Differentially uniform mappings for cryptography”*, EUROCRYPT ’93, LNCS vol. 765, Springer-Verlag, 1993, pp. 57 – 65.

# Chương 3. MÃ DÒNG TRÊN MẠNG DI ĐỘNG

**Tóm tắt chương:**

* *Chương 3 hệ thống và khảo sát các vấn đề liên quan đến mã dòng trên mạng di động. Nội dung chương này trình bày các vấn đề chính sau:*
  + *Hệ thống giới thiệu sơ lược về mạng di động, các thuật toán bảo mật đã có trên mạng di động.*
  + *Hệ thống lại mô hình mã dòng ZUC với cấu tạo của ZUC cũng như kiến trúc và hoạt động của 3 lớp: LFSR, BR, hàm phi tuyến F; trình bày hoạt động của ZUC.*
  + *Trình bày hai ứng dụng của ZUC là thuật toán mã hóa 128-EEA3 và thuật toán chứng thực thông điệp 128-EIA3.*
  + *Hệ thống, phân tích các tiêu chuẩn thiết kế và tính an toàn của ZUC: trình bày và phân tích tiêu chuẩn thiết kế của lớp LFSR; trình bày tiêu chuẩn thiết kế của lớp BR; hệ thống và phân tích tiêu chuẩn thiết kế và tính an toàn của hàm phi tuyến F, đặc biệt đi sâu phân tích và thực nghiệm đo đạc để kiểm tra các đặc tính mật mã quan trọng của hai S-box S0 và S1 là: tính phi tuyến của S-box, tính đồng nhất sai phân của S-box, tiêu chuẩn SAC và tính cân bằng (balance) của các hàm thành phần của S-box*.

**Tài liệu tham khảo chương:**

[28] Paul Yousef, *“GSM-Security a Survey and Evaluation of the Current Situation*” , Master's thesis, Linkoping Institute of Technology, 5-Mar-2004.

[29] 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, “*Specification of the A5/3 Encryption Algorithms for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS*”. Document 1: “*A5/3 and GEA3 Specifications*” (Release 6), Sep-2003.

[30] 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, “*Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3*”. Document 1: “*128-EEA3 and 128-EIA3 Specification*”, 4-Jan-2011.

[31] 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, “*Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3*”. Document 2: “*ZUC Specification*”, 4-Jan-2011.

[35] 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, *“Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3”*. Document 4: *“Design and Evaluation Report”*, 18-Jan-2011.

[37] Josef Pieprzyk, Chris Charnes, Jennifer Seberry, *“On the Immunity of S-boxes against Linear Cryptanalysis”*, Center for Computer Security Research, Department of Computer Science, University of Wollongong, pp. 1 – 9.

[38] Xian-Mo Zhang, Yuliang Zheng, *“On Nonlinear Resilient Functions”*, EUROCRYPT’95, France, May 1995, pp. 3 – 15.

# Chương 4. CHƯƠNG TRÌNH THỰC HIỆN

**Tóm tắt chương:**

* *Chương 4 trình bày kết quả của ứng dụng do chúng tôi thực hiện, với mô hình ứng dụng thử nghiệm mã dòng thông qua thuật toán mã hóa 128-EEA3 sử dụng generator ZUC. Nội dung chương này trình bày các vấn đề chính sau:*
  + *Giới thiệu tổng quan về ứng dụng Voice Chat dùng thuật toán mã hóa 128-EEA3 để đảm bảo tính bí mật của dữ liệu cuộc hội thoại trên đường truyền.*
  + *Trình bày mô hình của ứng dụng với các nội dung: các yêu cầu chức năng của chương trình; mô hình hoạt động của chương trình bao gồm: mô hình hoạt động ở chế độ công khai, mô hình hoạt động ở chế độ riêng tư; giao diện chương trình và hướng dẫn thực thi.*
  + *Tổng kết, đánh giá các kết quả đạt được và chưa đạt được về mặt ứng dụng của chương trình thực hiện*.