**KHẢO SÁT MÃ DÒNG VÀ ỨNG DỤNG**

**BẢNG TÓM TẮT ĐỌC TÀI LIỆU THAM KHẢO**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Reference** | **Chương** | **Main ideas** |
| 01 | Adi Shamir, *“Stream Ciphers: Dead or Alive?”*, ASIACRYPT, 2004 | 1  Giới thiệu  [2-3 pp] | * Sự mất ưu thế của mã dòng so với mã khối ngày nay. * Tương lai của mã dòng: ứng dụng trong RFID. * Đặt niềm tin vào việc ứng dụng mã dòng. |
| 02 | M.J.B. Robshaw, *“Stream Ciphers”*, RSA Laboratories Technical Report TR-701, 1995 | 2 | * Khái niệm mã dòng đồng bộ: state (là giá trị của một tập hợp các biến mang lại duy nhất một sự mô tả cho trạng thái của thiết bị), next state. * ~~Phần tử~~ bộ sinh số học: *generator số giả ngẫu nhiên* (pseudo – random number generator). |
| 03 | Thomas W.Cusick, Cunsheng Ding, Ari Renvall *,“Stream Ciphers and Number Theory”*, North-Holland Mathematical Library, 2003. | 2 | * Thành phần ~~Khái niệm~~ mã dòng: dòng khóa (keystream), phần tử sinh dòng khóa (generator). * Tính chất ~~Mã dòng đồng bộ cộng~~ (additive synchronous stream ciphers): tính đồng bộ và tính cộng. * Mã dòng tự đồng bộ cộng (additive self-synchronous stream ciphers): giải thích tính tự đồng bộ (quá trình lan truyền lỗi và sự tự đồng bộ sau đó). * Mã dòng đồng bộ không cộng (nonadditive synchronous stream cipher): kết hợp giữa mà khối và mã dòng cộng. Cơ chế dùng khóa động. Phần tử sinh khóa động phải dữ bí mật. Ưu điểm của mã dòng đồng bộ không cộng. * Mã dòng sử dụng mã khối thông qua 3 mode of operation: CBC, CFB, OFB. * Mã phân phối hợp tác: sử dụng nhiều thuật toán mã khối và thành phần sinh khóa (generator) điểu khiển hoạt động. * Khái niệm về các khía cạnh mật mã của sequence được sinh ra bởi phần tử sinh: độ phức tạp tuyến tính, đa thức cực tiểu, phân phối mẫu, hàm tương quan, độ phức tạp cầu.   + Khái niệm chung về độ phức tạp tuyến tính của một sequence bất kỳ.  + Độ phức tạp tuyến tính của sequence được sinh ra bởi LFSR  + Độ phức tạp cầu dựa vào độ phức tạp tuyến tính. |
| 04 | James L. Massey, *“Shift-Register Synthesis and BCH Decoding”*, IEEE TRANSACTIONS ON INFORMATION THEORY, 1969. | 2 | * Định lý: *Nếu một số LFSR với chiều dài LN(s), sinh ra dãy sN = s0, s1, …, sN-1 và cả dãy sN+1 = s0, s1, …, sN-1, sN, thì . Ngược lại, nếu một số LFSR với chiều dài LN(s) sinh ra dãy sN nhưng không sinh được dãy sN+1, thì* * Thuật toán Berlekamp-Massey để tìm ra một LFSR ngắn nhất với chiều dài *Ln*(*s*) sinh ra dãy *s0, s1, …, sn-1*. Đồng thời là thuật toán xác định độ phức tạp tuyến tính của dãy được sinh ra bởi LFSR. |
| 05 | A. Menezes, P. van Oorschot, S. Vanstone, *“Handbook of Applied Cryptography”*, CRC Press, 1997. | 2 | * Đa thức hồi quy (đa thức kết nối) của LFSR có dạng: * *maximum-length* LFSR: khi *C*(*D*) là đa thức cơ bản (primitive polynomial). m-sequence được sinh ra bởi LFSR này. Nó thỏa *tiên đề ngẫu nhiên Golomb*. * Tấn công LFSR:Chỉ cần một dòng khóa con của nó có chiều dài ít nhất hai lần độ phức tạp tuyến tính là đủ để xác định được đầy đủ dòng khóa ban đầu. * Định nghĩa miễn tương quan bậc *m* (*mth*-order correlation immune). Hàm kết hợp của generator kết hợp phi tuyến được lựa chọn sao cho thỏa mãn miễn tương quan thì sẽ không có sự *phụ thuộc xác suất* nào *giữa bất kỳ tập con nhỏ nào của n dãy LFSR và dòng khóa*. |
| 06 | Edgar Ferrer, *“Acceleration of Finite Field Arithmetic with an Application to Reverse Engineering Genetic Networks”*, University of Puerto Rico at Mayaguez, 2008. | 2 | * Định nghĩa trường hữu hạn (trường Galois):   *Một trường hữu hạn  gồm có một tập hữu hạn F, và hai phép toán + và  thỏa mãn các tính chất sau:*  *1.*  *2.*  *3.*  *4.*  *5.*  *6.  sao cho*  *sao cho*   * Số phần tử trong một trường Galois có thể là *một số nguyên tố* hoặc *lũy thừa của một số nguyên tố*. * Định nghĩa đa thức bất khả quy: *Một đa thức trên  là bất khả quy nếu nó không thể được phân tích thành nhân tử của các đa thức không tầm thường trên trường tương tự* ()*.* * Các cách biểu diễn phần tử trong trường hữu hạn   + Biểu diễn lũy thừa (power representation).  + Biểu diễn cơ sở thông thường (normal basis).  + Biểu diễn cơ sở chuẩn (standard basis). |
| 07 | 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. | 2 | * Thuật toán Shift-and-Add Most Significant Bit (MSB): dùng để nhân hai phần tử trong trường *GF*(2*m*). Giải thích tính “Shift” và “Add” trong thuật toán: biểu thức  có thể được thực hiện với phép Shift bit. Sở dĩ như vậy là bởi vì có thể xem một phần tử thuộc *GF*(2*m*) là một chuỗi bit bao gồm *m* bit mà giá trị của bit thứ *i* là giá trị của hệ số  trong cách biểu diễn cơ sở chuẩn. Còn biểu thức  rõ ràng có bản chất thực hiện bởi phép cộng. * Thuật toán Euclid nhị phân mở rộng (Binary Extended Euclidean Algorithm - BEA): để tính nghịch đảo của một phần tử trong *GF*(2*m*). |
| 08 | Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng, *“Nonlinearity and Propagation Characteristics of Balanced Boolean Functions”*, Department of Computer Science – The University of Wollongong. | 2 | * Định nghĩa hàm Boolean: *Hàm Boolean là hàm f ánh xạ GF(2)n thành GF(2). Còn gọi đơn giản f là hàm trên GF(2)n.* * Các khái niệm:   + Truth table của hàm Boolean: Dãy nhị phân định nghĩa bởi  được gọi là *truth table* của *f*. Ở đây  với  là các vector trong *GF(2)n* mà số nguyên do nó biểu diễn là *i* (xem vector như chuỗi bits).  + Hàm affine và tuyến tính: hàm *affine* *f* trên *GF*(*p*)*n* là hàm có dạng , ở đây . *f* được gọi là *hàm tuyến tính* nếu *c* = 0. Sequence của hàm affine (hoặc tuyến tính) được gọi là *affine (linear) sequence*.  + Khoảng cách Hamming (Hamming distance) giữa hai hàm Boolean: chúng được định nghĩa như , ở đây  và  tương ứng là các *truth table* của *f* và *g*.   * Định nghĩa độ phi tuyến của hàm Boolean: *Độ phi tuyến (nonlinearity) của f, ký hiệu bởi Nf , là khoảng cách Hamming nhỏ nhất giữa f và tất cả hàm affine trên GF(2)n. Nghĩa là , ở đây , , …,  là các ký hiệu của các hàm affine trên GF(2)n*. * Có nhiều cách để cải thiện độ lớn độ phi tuyến của hàm Boolean như: *kết nối, phân chia, điều chỉnh* các dãy. * Ma trận *Walsh-Hadamard*: *H*0 = 1,  ở đây  là *tích Kronecker*. |
| 09 | K. Nyberg, *“Differentially uniform mappings for cryptography”*, EUROCRYPT ‟93, LNCS vol. 765, Springer-Verlag, 1993. | 2 | * Định nghĩa tính đồng nhất sai phân của S-box: *Cho G*1 *và G*2 *là các nhóm Abel hữu hạn. Ánh xạ*  *được gọi là* ***đồng nhất sai phân*** *(differential uniformity) mức*  *nếu:*     *ở đây  được gọi là mức đồng nhất sai phân của f*. |
| 10 | 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. | 2 | * Định nghĩa tiêu chuẩn SAC: *Hàm  thỏa tiêu chuẩn SAC khi và chỉ khi  thỏa WH(a) =* 1. * Một trong những tiêu chí đánh giá độ an toàn của S-box là từng hàm *fj* phải đạt hay “gần đạt” tiêu chuẩn SAC, tức là nếu 1 bit đầu vào của S-box bị thay đổi thì mỗi bit đầu ra sẽ bị thay đổi với xác suất xấp xỉ ½. * Đối với S-box AES, khi 1 bit đầu vào bị thay đổi, mỗi bit đầu ra sẽ thay đổi với xác suất xấp xỉ ½. |
| 11 | 3rd Generation Partnership Project, “*Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3*”. Document 1: “*128-EEA3 and 128-EIA3 Specification*”, 4-Jan-2011. | 3 | * Đặc tả cách cài đặt giải thuật mã hõa *128-EEA3* và giải thuật chứng thực *128-EIA3* dựa trên ZUC. |
| 12 | Paul Yousef, *“GSM-Security a Survey and Evaluation of the Current Situation*” , Master's thesis, Linkoping Institute of Technology, 5-Mar-2004. | 3 | * Cặp thuật toán *A3* và *A8* được dùng để chứng thực thông tin trên mạng GSM. Các thuật toán này được cài trên SIM và dựa trên thuật toán khác tên là *COMP128*. * Giải thuật A5/1 là giải thuật mã hóa dòng dùng trên hệ thống GSM đang được sử dụng ở nhiều quốc gia. Giải thuật này sử dụng khóa có kích thước 64 bits được tạo từ giải thuật *COMP128*. * Giải thuật A5/2 cũng được dùng trên hệ thống GSM nhưng ít phổ biết do độ an toàn thấp hơn A5/1. Sử dụng phương pháp tấn công biết trước bản rõ đối với A5/2, ta có thể thu được khóa với độ phức tạp là 216. |
| 13 | 3rd Generation Partnership Project, “*Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3*”. Document 2: “*ZUC Specification*”, 4-Jan-2011. | 3 | * Đặc tả cách cài đặt giải thuật mã hóa ZUC bao gồm :   + Kiến trúc tổng quan của giải thuật ZUC.   + Cấu trúc và hoạt động của thanh ghi dịch chuyển hồi quy tuyến tính.   + Hàm lọc thông tin từ thanh ghi.   + Hàm biến đổi phi tuyến và kiến trúc của các S-box.   + Cách khởi tạo và thực thi chương trình mã hóa băng ZUC. |
| 14 | Claude Carlet, *“Boolean Functions for Cryptography and Error Correcting Codes”*, University of Paris 8, France. | 3 | * Bậc đại số của hàm Boolean:   ở đây *P*(*N*) là ký hiệu *tập lũy thừa* (power set) của  (tập lũy thừa của *N* là tập bao gồm tất cả các tập con của *N*). Dạng biểu diễn này được gọi là *dạng chuẩn đại số* (Algebraic Normal Form – ANF) của hàm Boolean.  Bậc của ANF được ký hiệu là  và được gọi là ***bậc đại số*** (algebraic degree) của hàm *f* : , ở đây  là ký hiệu kích thước của *I*. Bậc đại số còn có tên gọi khác là *bậc phi tuyến* (nonlinear order).   * Bậc đại số của hàm Boolean càng cao thì khả năng generator (sử dụng hàm Boolean này) bị tấn công sai phân càng thấp. |
| 15 | Xian-Mo Zhang, Yuliang Zheng, *“On Nonlinear Resilient Functions”*, EUROCRYPT’95, France, May 1995. | 3 | Không chỉ có khái niệm bậc đại số của hàm Boolean, mà còn có khái niệm bậc đại số của S-box (xuất phát từ khái niệm hàm có nhiều hàm thành phần )   * Bậc đại số của S-box:   Bậc đại số của S-box là bậc đại số nhỏ nhất trong số các bậc đại số của các tổ hợp tuyến tính khác không của các hàm thành phần S-box. Nghĩa là:    trong đó,  là hàm ánh xạ từ  thành  (các fi với i = 0, 1, …, m là các hàm Boolean ánh xạ từ  thành ). F chính là một  S-box. |

Sau đây là cấu trúc bài viết của cuốn Khóa luận:

**Chương 1. Mở đầu.**

**Tóm tắt: mục tiêu của chương, nội dung chính do mình thực hiên trong chương, cấu trúc chương**

**Tài liệu tham khảo chương**

**Chương 2. Lý thuyết mã dòng.**

**Chương 3. Mã dòng trên mạng di động.**

**Chương 4. Chương trình thực hiện.**

**Kết luận.**

**Phụ lục.**