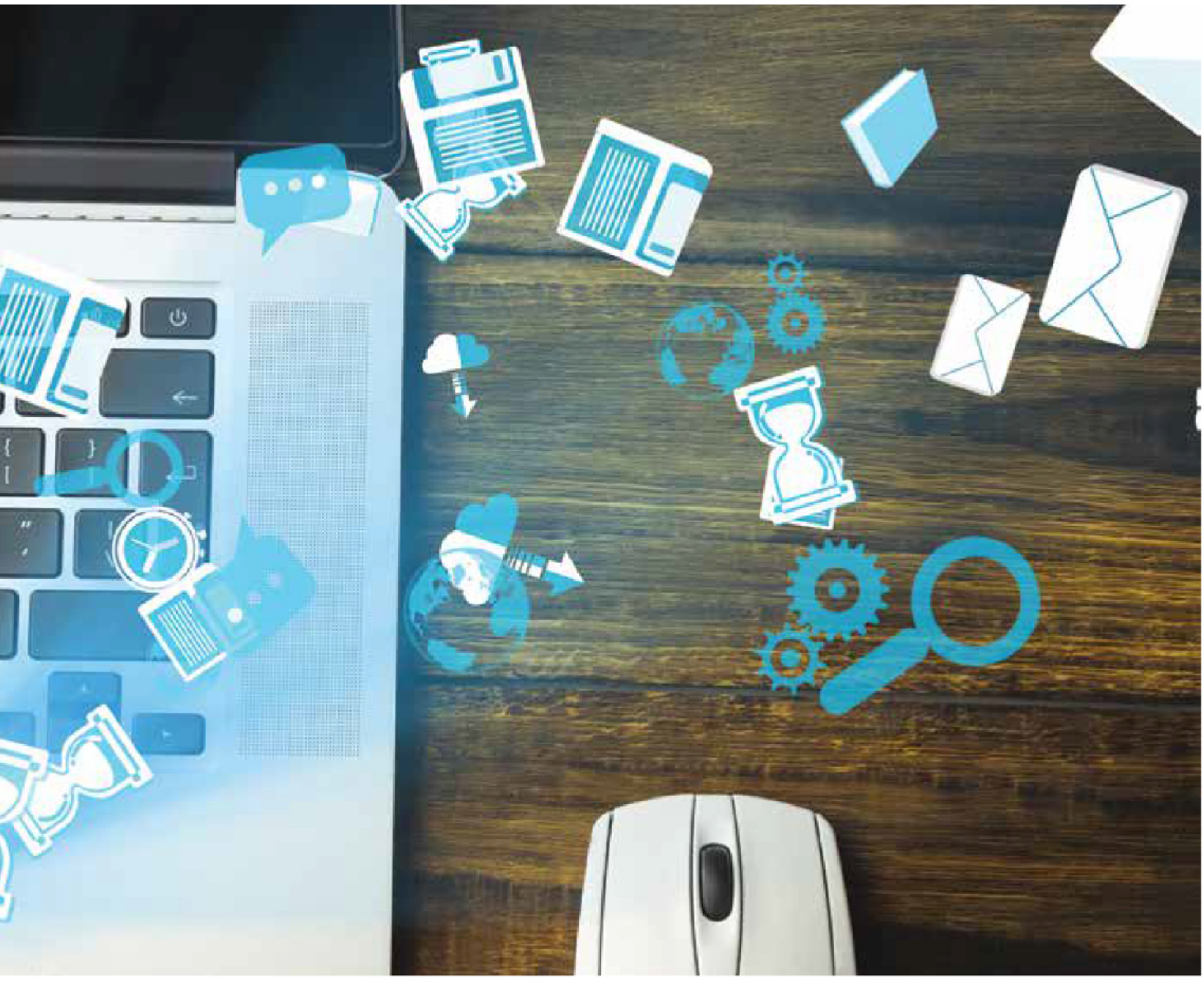
NIST SP 800-22 VÀ NHỮNG CẨN TRỌNG KHI SỬ DỤNG (PHẦN I)

TS. Trần Duy Lai[1], ThS. Hoàng Đình Linh[2]
[1]Nguyên Viện trưởng Viện Khoa học Công nghệ mật mã
[2]Viện Khoa học công nghệ mật mã

Trong các ứng dụng mật mã, việc đánh giá chất lượng của bộ sinh số ngẫu nhiên và giả ngẫu nhiên đóng vai trò cực kỳ quan trọng, và việc đánh giá tính ngẫu nhiên theo thống kê là một yêu cầu cơ bản nhất trong quá trình đánh giá đó. NIST SP 800-22 đã được đưa ra và trở thành một công cụ hữu ích, phổ biến nhất cho việc đánh giá tính ngẫu nhiên theo thống kê đối với các bộ sinh trên. Tuy nhiên, cho đến nay dù được sử dụng khá rộng rãi nhưng vẫn còn những điểm bất cập trong bộ kiểm tra này, khi một số kiểm tra thống kê còn chưa chính xác. Trong nội dung của bài báo, chúng tôi sẽ đưa ra một góc nhìn chung về bộ kiểm tra tính ngẫu nhiên theo thống kê NIST SP 800-22 cho các bộ tạo số ngẫu nhiên và giả ngẫu nhiên, đồng thời trình bày các vấn đề còn tồn tại và đưa ra một vài lưu ý đối với việc sử dụng công cụ này.

MỞ ĐẦU

Các số ngẫu nhiên và giả ngẫu nhiên đã và đang đóng một vai trò quan trọng trong nhiều lĩnh vực, chẳng hạn như cơ học lượng tử, lý thuyết trò chơi, mật mã… Trong mật mã, các số có tính ngẫu nhiên (gồm các số ngẫu nhiên hoặc giả ngẫu nhiên) lại càng quan trọng hơn và được sử dụng nhiều. Chẳng hạn, các hệ mật thường sử dụng các khóa được tạo ra như một đại lượng ngẫu nhiên. Nhiều giao thức mật mã cũng yêu cầu các dầu vào có tính ngẫu nhiên, ví dụ đối với các tham số bổ trợ trong việc sinh chữ ký số hoặc trong việc tạo ra các thách thức ngẫu nhiên trong các giao thức xác thực.



Hơn nữa, độ an toàn của nhiều lược đồ và giao thức mật mã phụ thuộc chủ yếu vào các thành phần (có tính) ngẫu nhiên đó.

Có hai loại bộ sinh số ngẫu nhiên (RNGs) cơ bản được sử dụng để sinh các dãy số ngẫu nhiên: các bộ sinh số ngẫu nhiên thực sự (True Random Number Generators (TRNGs)) và các bộ sinh số giả ngẫu nhiên (Pseudo/Deterministic Random Number Generators (PRNGs)). Trong các ứng dụng mật mã, cả hai loại bộ sinh này tạo ra một chuỗi các bit 0 và 1 mà có thể chia thành các chuỗi con hoặc các khối của các số ngẫu nhiên. Đối với việc kiểm tra tính ngẫu nhiên, các kiểm tra dựa trên giả thiết thống kê được sử dụng rộng rãi để đánh giá chất lượng của các bộ sinh số ngẫu nhiên, trong đó kiểm tra xem khi nào các dãy đầu ra có phù hợp với giả thiết cho trước, tức là dãy có tính ngẫu nhiên hoàn thiện (perfect randomness) hay không. Hơn nữa các kiểm tra tính ngẫu nhiên theo thống kê cũng được sử dụng để đánh giá đầu ra của các nguyên thủy mật mã, chẳng hạn như các mã khối, hàm băm để bước đầu đánh giá tính không thể phân biệt được giữa các đầu ra của chúng với đầu ra được chọn ngẫu nhiên. Một số bộ kiểm tra thống kê được sử dụng phổ biến bao gồm: bộ tiêu chuẩn kiểm tra được đề xuất bởi Knuth [1], Dichard [2] được đề xuất bởi Marsaglia và sử dụng phổ biến nhất hiện nay chính là NIST SP 800-22 [3] và được chuẩn hóa bởi Viện Tiêu chuẩn và Công nghệ quốc gia Hoa kỳ (NIST). Theo chúng tôi, một trong những lý do là bởi vì NIST công bố mã nguồn của bộ kiểm tra này. Bộ kiểm tra của NIST ban đầu gồm 16 tiêu chuẩn kiểm tra, sau đó trong bản cập nhật mới

nhất năm 2010 rút xuống còn 15 tiêu chuẩn, khi loại bỏ đi tiêu chuẩn nén Lempel-Ziv. Đã có nhiều nghiên cứu chỉ ra rằng, một số tiêu chuẩn kiểm tra của NIST là chưa chính xác và cần phải chỉnh sửa hoặc thay thế bằng cách tiêu chuẩn khác.

Đối với người dùng khi tiếp cận bộ tiêu chuẩn này sẽ có 3 vấn đề chính được đặt ra. Thứ nhất, đọc hiểu và nắm được chi tiết và chính xác nội dung trong tài liệu mà NIST đã công bố. Các nội dung chính trong tài liệu này sẽ được chúng tôi trình bày sơ lược trong phần II. Vấn đề thứ hai đó là việc khai thác sử dụng chính xác mã nguồn của bộ kiểm tra, đồng thời kiểm tra tính đúng đắn, đối chiếu giữa mã nguồn và mô tả lý thuyết trong tài liệu. Ở mức cao hơn, người dùng có thể tùy chỉnh mã nguồn để chính xác hóa các công thức hoặc bổ sung các kiểm tra khác theo ý muốn. Vấn đề cuối cùng, cũng là khó khăn nhất đó chính là đảm bảo cơ sở lý thuyết cho các kiểm tra của bộ kiểm tra này. Trong tài liệu mà NIST công bố, họ không đưa ra cơ sở lý thuyết một cách rõ ràng mà chỉ liệt kê các tài liệu liên quan đến kiểm tra tương ứng. Theo đánh giá của chúng tôi, có những kiểm tra đã có cơ sở lý thuyết một cách rõ ràng như kiểm tra tần số, kiểm tra tần số trong một khối; lại có những kiểm tra có thể làm rõ được cơ sở lý thuyết theo các tài liệu công bố như kiểm tra loạt, hạng ma trận, so khớp mẫu, độ phức tạp tuyến tính, tổng tích lũy; nhưng cũng có những kiểm tra không dễ để có thể làm rõ cơ sở lý thuyết như kiểm tra DFT, Serial, phổ quát của Maurer, entropy xấp xỉ, viếng thăm ngẫu nhiên và biến thể viếng thăm ngẫu nhiên.

CÁC NỘI DUNG CHÍNH TRONG NIST SP 800-22

Như đã trình bày, vấn đề đầu tiên đối với người dùng là đọc hiểu và nắm được chi tiết tài liệu báo cáo mà NIST công bố. Tài liệu NIST SP 800-22 Revision 1a dài 131 trang, được chia làm 5 Mục và 7 Phụ lục. Mục 1 của tài liệu đưa ra một số khái niệm về tính ngẫu nhiên, độ bất định, các bộ sinh số ngẫu nhiên và giả ngẫu nhiên cùng với một số khái niệm và ký hiệu toán học. Mục 2 chiếm phần lớn nội dung khi trình bày về mục đích, cách gọi hàm, mô tả, phân phối tham chiếu, mức ý nghĩa, tham số khuyến cáo và ví dụ cho 15 kiểm tra thống kê. Trong tài liệu này, NIST không trình bày chi tiết về cơ sở lý thuyết cho các kiểm tra mà chỉ trích dẫn đến các tài liệu đã được công bố. Mục 3 liệt kê các tài liệu trên đối với mỗi kiểm tra thống kê. Mục 4 trình bày chiến lược phân tích thống kê cho một RNG (Random Number Generators). Mục 5 trình bày hướng dẫn sử dụng mã nguồn cài đặt của bộ kiểm tra này.

Ngoài ra, một số thông tin khác được trình bày trong các phụ lục: Phụ lục A trình bày về mã nguồn cài đặt của bộ kiểm tra. Phụ lục B trình bày một số kết quả thực nghiệm đối với các dữ liệu mẫu. Phụ lục C giúp người dùng có thể tùy chỉnh mã nguồn để bổ sung các kiểm tra khác. Phụ lục D mô tả của các bộ sinh số giả ngẫu nhiên có sẵn trong mã nguồn cài đặt của bộ kiểm tra. Phụ lục E trình bày một số hàm số học tính toán được sử dụng trong các kiểm tra như hàm gamma, hàm lỗi. Phụ lục F trình bày một số phần mềm hỗ trợ tính toán như Mathematica để tính toán một số hàm trung gian trong các kiểm tra.

Quy trình cho việc phân tích thống kê đối với một bộ sinh số ngẫu nhiên RNG

Để đánh giá và phân tích thống kê đối với các bộ sinh số ngẫu nhiên hoặc giả ngẫu nhiên, NIST đã đưa ra một quy trình gồm 5 giai đoạn như sau:

Giai đoạn 1: Lựa chọn một bộ sinh

Lựa chọn bộ sinh số dựa trên phần cứng hoặc phần mềm, phải tạo ra một dãy nhị phân có độ dài n cho trước.

Giai đoạn 2: Sinh dãy nhị phân

Với kích thước n cho trước và bộ sinh đã chọn, tiến hành xây dựng một tập m dãy nhị phân và lưu vào một tệp dữ liệu.

Giai đoạn 3: Thực hiện các tiêu chuẩn kiểm tra

Thực hiện lựa chọn các tiêu chuẩn kiểm tra cùng với các tham số đầu vào và áp dụng các tiêu chuẩn kiểm tra đó lên tệp dữ liệu đã tạo.

Giai đoạn 4: Kiểm tra các giá trị *P-value*

Một tệp đầu ra sẽ được tạo từ các tiêu chuẩn kiểm tra với các giá trị trung gian, chẳng hạn các giá trị thống

kê, các giá trị *P-value* cho mỗi tiêu chuẩn kiểm tra. Dựa trên các giá trị *P-value* đó, chúng ta có thể đưa ra một kết luận đối với chất lượng của các dãy được kiểm tra.

Giai đoạn 5: Đánh giá, khẳng định vượt qua hay không vượt qua

Đối với mỗi tiêu chuẩn kiểm tra thống kê, một tập các giá trị *P-value* được đưa ra. Đối với một mức ý nghĩa cho trước, một lượng nhất định các giá trị *P-value* được kỳ vọng là không vượt qua. Ví dụ, nếu mức ý nghĩa được chọn là 0.01 $(\alpha - 0.01)$ thì khoảng 1% của số dãy được kiểm tra là không vượt qua. Một dãy vượt qua một kiểm tra thống kê khi $P - value \geq \alpha$ và ngược lại thì không vượt qua.

Phân tích các kết quả thực nghiệm

Việc phân tích các kết quả thực nghiệm có thể được thực hiện theo nhiều cách. NIST đã sử dụng hai cách tiếp cận để phân tích kết quả thực nghiệm như sau:

(1) *Kiểm tra tỷ lệ số dãy vượt qua một tiêu chuẩn kiểm tra thống kê:*

Đếm số lượng các dãy trong mẫu mà có giá trị *P-value* $\geq \alpha$ và ký hiệu là m_p. Khi đó, dưới giả thiết về tính ngẫu nhiên, m_p tuân theo phân phối nhị thức $B(m,1-\alpha)$ là xấp xỉ theo phân phối chuẩn $N(m(1-\alpha), m\alpha(1-\alpha))$ khi n đủ lớn. Do đó, tỷ lệ dãy vượt qua một kiểm tra (m_p/m) xấp xỉ theo $N\left((1-\alpha), \frac{\alpha(1-\alpha)}{m}\right)$.

Khoảng chấp nhận được của m_p/m được xác định sử dụng mức ý nghĩa như sau:

$$1-\alpha-3\sqrt{\frac{\alpha(1-\alpha)}{m}} < \frac{m_p}{m} < 1-\alpha+3\sqrt{\frac{\alpha(1-\alpha)}{m}}.$$

Nếu tỷ lệ dãy vượt qua nằm ngoài khoảng trên thì có bằng chứng là dữ liệu là không ngẫu nhiên.

(2) *Kiểm tra phân phối của các giá trị P-value để kiểm tra tính phân phối đều:*

Phân phối của các *P-value* được giả sử là phân phối đều. Tính đều có thể được xác định bằng cách áp dụng một kiểm tra χ^2 và đưa ra một giá trị *P-value* tương ứng với kiểm tra so khớp tính tốt (goodness-of-fit) trên các giá trị *P-value* thu được từ một tiêu chuẩn kiểm tra thống kê (tức là *P-value* của các *P-value)*. Đầu tiên, đoạn [0,1] được chia thành 10 khoảng con đều nhau. Kiểm tra được thực hiện bằng công thức tính:

$$\chi^2 = \sum_{i=1}^{10} \frac{(F_i - m/10)^2}{m/10},$$

trong đó F_i là số lượng các *P-value nằm trong khoảng thứ i. Giá trị* ***P-value*** P_T mới được tính là:

$$P_T = igamc\left(\frac{9}{2}, \frac{\chi^2}{2}\right),$$

trong đó igamc là hàm phần bù gamma không đầy đủ. Nếu $P_T \geq \alpha_{II} (:= 0.0001)$ thì các dãy có thể được coi là được phân phối đều, trong đó α_{II} là mức ý nghĩa đối với P_T.

Nếu một trong hai điều kiện trên không thỏa mãn thì vẫn cần thực hiện kiểm tra trên các bộ mẫu khác của bộ sinh để xác định xem đó là một bằng chứng rõ ràng của tính không ngẫu nhiên hay không.

KẾT LUẬN

Trong phần này, chúng tôi đã trình bày tóm lược về các nội dung chính trong chuẩn NIST SP 800-22. Nội dung phần tiếp theo, chúng tôi sẽ trình bày các nghiên cứu liên quan đến NIST SP 800-22 và chỉ ra những lưu ý cần phải cẩn trọng khi sử dụng bộ công cụ này.❖

TÀI LIỆU THAM KHẢO

1. MacLaren, M.D., The art of computer programming. Volume 2: Seminumerical algorithms (Donald E. Knuth). SIAM Review, 1970. 12(2): p. 306-308.
2. Marsaglia, G., The marsaglia random number cdrom including the dichard battery of tests of randomness, 1995. URL http://www. stat. fsu. edu/pub/dichard, 2008.
3. Rukhin, A.L., et al., SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, National Institute of Standards & Technology, Gaithersburg, MD, 2001.