THỰC HIỆN THUẬT TOÁN DES TRÊN FPGA

ThS. Bồ Quốc Bảo, ThS. Hà Quang Thanh
Đại học Công nghiệp Hà Nội
ThS. Nguyễn Trung Hiếu
Học viện Công nghệ Bưu chính Viễn thông

Trong những năm gần đây, do sự gia tăng nhanh chóng của dung lượng dữ liệu thông tin nên việc bảo mật và các thuật toán mã hoá cũng được phát triển để chống lại các tác nhân đe doạ sự an toàn thông tin, có thể nói bảo mật hiện đang được ứng dụng ở mọi nơi khi giao dịch dữ liệu số được thực hiện. Bài báo giới thiệu về các chuẩn bảo mật và cách thực hiện hiệu quả trên phần cứng với khả năng tái cấu hình thuật toán mật mã dữ liệu tiêu chuẩn DES (Data Encryption Standard). Thiết kế này được mô tả theo thiết kế số FPGA với phương thức sử dụng cấu trúc song song cho phép tính cả 8 DES S-box đồng thời nhằm giảm đường tới hạn thiết kế, kết quả này tối ưu khi so sánh với các cách thực hiện trên phần cứng tái cấu hình trước đây của DES.

1. GIỚI THIỆU

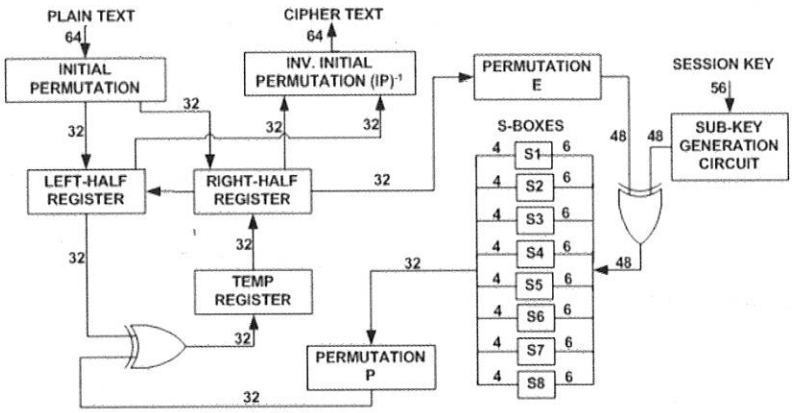
Việc thực hiện các thuật toán mã hoá trên phần cứng có thể tái cấu hình mang lại nhiều lợi ích hơn thực hiện trên VLSI (Very Large Scale Integrated circuits) và trên phần mềm vì nó có tốc độ cao tương tự như VLSI và độ linh hoạt cao tương tự như thực hiện trên phần mềm. Tuy nhiên phải thiết kế tất cả các phần từ mô tả hành vi đến bố cục vật lý. Đó là quá trình tốn nhiều thời gian và tiền bạc. Mã hoá thực hiện trên phần mềm có độ linh hoạt cao nhưng không đủ nhanh cho những ứng dụng thời gian thực. Nói cách khác, các thiết bị có thể tái cấu hình là lựa chọn tốt về vấn đề thời gian và giá thành so với VLSI nên việc thực hiện được giảm thiểu. Hơn nữa, nó có nhiều lợi thế về khả năng tái lập trình và thực nghiệm trên nhiều cấu trúc khác nhau hoặc các phiên bản khác nhau của cùng một cấu trúc.

Giữa các thuật toán giải mã khác nhau, ví dụ phổ biến nhất trong trường các mã đối xứng là thuật toán tiêu chuẩn mã hoá dữ liệu DES (Data Encryption Standard) của IBM trong giữa những năm 70. Thuật toán DES được cấu tạo bởi các vòng tuần hoàn dựa trên một số phép toán của bit như các phép toán logic, hoán vị, phép thay thế, phép toán dịch chuyển... Mặc dù các đặc điểm này phù hợp một cách tự nhiên với các cách thực hiện có hiệu quả trên các thiết bị FPGA có thể tái cấu hình, DES còn được thực hiện trên tất cả các dạng như như phần mềm, VLSI và các phần cứng có thể tái cấu hình sử dụng FPGA.

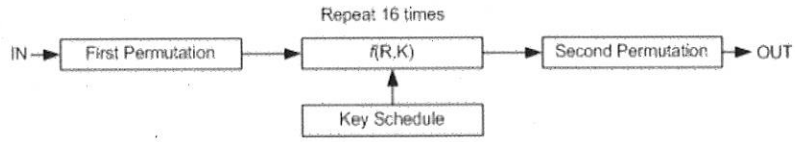
Bài báo này giới thiệu cấu trúc DES gọn và có hiệu quả được thiết kế đặc biệt cho dạng phần cứng có khả năng tái cấu hình. Việc thực hiện DES trong bài báo này khác trước, đó là nó sử dụng 8 bảng tra DES S-box có cấu trúc song song nên sẽ giảm đường tới hạn cho việc mã hoá và giải mã một cách có hiệu quả. Phần còn lại của bài báo gồm: phần 2 mô tả thuật toán DES; cấu trúc DES và cách thực hiện nó trên thiết bị phần cứng có thể tái cấu hình sẽ được giới thiệu trong phần 3. Phần 4 so sánh kết quả đạt được với các cách thực hiện DES trước đây. Kết luận và định hướng trong thời gian tới sẽ được đưa ra trong phần 5.

2. THUẬT TOÁN DES

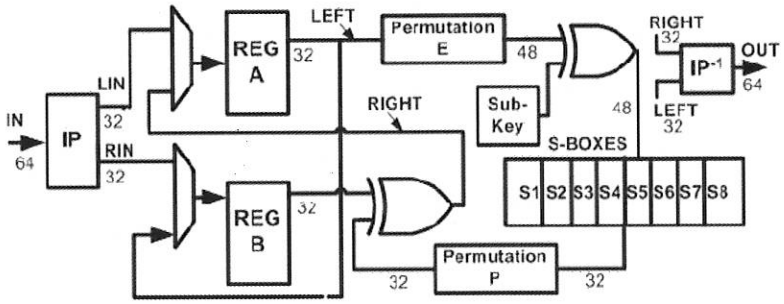
Tháng 8 năm 1974, IBM đã đưa ra ứng cử (dưới tên gọi là LUCIFER) một thuật toán mã hoá để đáp lại lời kêu gọi lần thứ hai của Cục tiêu chuẩn Liên bang Hoa Kỳ (NBS – National Bureau of Standard), và nay là Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST – National Institute of Standard & Technology) để bảo vệ dữ liệu khi truyền và lưu giữ. NBS đã đưa ra quy trình đánh giá với sự giúp đỡ của Cơ quan An ninh Quốc gia Hoa Kỳ (NSA – National Sercurity Agency)



Hình 1. Thuật toán DES



Hình 2. Thuật toán DES



Hình 3. Thực hiện thuật toán DES trên FPGA

và cuối cùng, tháng 7 năm 1977, thuật toán LUCIFER đã được chấp nhận như là một tiêu chuẩn mã hoá dữ liệu mới (NewDES – New Data Encryption Standard). Tiêu chuẩn giải mã dữ liệu, được biết đến như là thuật toán mã hoá dữ liệu (DEA - Data Encryption Algorithm) của ANSI và DEA-1 của ISO vẫn là một tiêu chuẩn phổ biến trên thế giới trong một thời gian dài trước khi bị thay thế bằng tiêu chuẩn mã hoá tiên tiến mới (NewAES – New Advanced Encryption Standard) vào tháng 10 năm 2000. Tuy nhiên, không loại trừ trường hợp là DES vẫn được dùng trong một số lĩnh vực trong vài năm nữa. DES đưa ra cơ sở so sánh các thuật toán mới và nó cũng được sử dụng trong các giao thức IPSec, mã hoá hộp ATM, giao thức SSL và TripleDES (thực hiện DES ba lần). Mô tả chi tiết thuật toán DES có thể tìm thấy trong [19-21].

DES là một mật mã khối: nó mã hoá/giải mã dữ liệu trong các khối 64 bit bằng cách sử dụng khoá 64 bit (mặc dù độ dài thực sự của khoá chỉ là 56 bit). DES là một thuật toán đối xứng: sử dụng cùng một thuật toán và khoá cho quá trình mã hoá và giải mã. DES là một mật mã lặp: cơ sở xây dựng các khối (phép thế được thực hiện sau phép hoán vị) gọi là một vòng và được lặp lại 16 lần. Trong mỗi vòng DES, khoá con được tạo ra từ khoá chính bằng cách sử dụng thuật toán chu trình tạo khoá con (key schedule). Chu trình tạo khoá con cho việc mã hoá và giải mã là giống nhau nhưng có trật tự ngược nhau. Thuật toán cơ sở cho việc mã hoá/giải mã một khối được chỉ ra trên hình 1. Mã hoá bắt đầu với việc hoán vị đầu (IP – Initial Permutation) bằng cách trộn ký tự 64 bit trong một mẫu xác định. Kết quả của việc hoán vị đầu được gửi vào hai thanh ghi 32 bit được gọi là thanh ghi dịch trái và thanh ghi dịch phải. Các thanh ghi này giữ hai nửa kết quả trung gian trong suốt 16 vòng lặp. Nội dung của thanh ghi phải được hoán vị (hoán vị E) và đưa vào một cổng XOR để cộng module 2 với khoá phụ trong mỗi vòng lặp. Chú ý là một số bit sẽ được chọn hai lần để cho phép các thanh ghi 32 bit mở rộng thành 48 bit. Đầu ra 48 bit của khối XOR được chia thành tám nhóm (mỗi nhóm 6 bit) đến địa chỉ của tám bộ nhớ thay thế (S-box). Hoán vị P nhận đầu ra 32 bit từ S-box và đưa đến khối XOR nội dung thanh ghi dịch trái. Đầu ra của khối này được đưa vào thanh ghi tạm thời, kết thúc vòng lặp thứ nhất.

Ở chu kỳ clock tiếp theo, nội dung của các thanh ghi tạm thời được viết vào thanh ghi dịch phải và nội dung trước đó của thanh ghi dịch phải được viết vào thanh ghi dịch trái. Quá trình này được lặp lại trong 16 vòng lặp DES. Sau 16 vòng lặp, các nội dung của thanh ghi dịch phải và trái được đưa đến hoán vị cuối IP-1, nó là nghịch đảo của hoán vị đầu. Đầu ra của IP-1 là ký tự mật mã 64 bit.

Bảng 1. Thực hiện DES trên phần cứng có thể tái cấu hình trong thời gian gần đây

Author	Device used	CLB slices (A)	Allowed Freq. (MHz)	Throughput (Mbits/s)(T)	T/A Factor
Wong et al. [10]	XC4020E	438	10	26.7	0.06
Kaps and Paar [11]	XC4028EX	741	25.18	402.7	0.54
Free-DES [12]	XCV400	5263	47.7	3052	0.57
McLoony, McCanny [13]	XCV1000	6446	59.5	3808	0.59
Sandia Laboratories [8]	ASIC	---	---	9280	---
Patterson (Jbits) [14]	XCV150	1584	168	10752	6.78
This work (FPGA)	XCV400e	117	68.05	274	2.34

3. THỰC HIỆN DES TRÊN PHẦN CỨNG CÓ THỂ TÁI CẤU HÌNH

Trên hình 1, 16 vòng lặp của các quá trình giống nhau được thực hiện dưới tên hàm f(R,K). DES kết hợp phép hoán vị thứ nhất, hàm f(R,K), phép hoán vị thứ hai và quy trình tạo khoá cho một phép mã hoá (được chỉ ra trên hình 2). Quy trình mã hoá và giải mã trong DES là giống nhau nhưng trật tự của khoá con là ngược nhau.

Thuật toán của quy trình tạo khoá đơn giản và nhanh. Hơn nữa, khoá được tạo ra một lần nhưng lại được dùng cho cả quá trình. Tuy nhiên, khi DES thực hiện trên FPGA thì các khoá con tính toán trước sẽ được lưu trong bộ nhớ.

Phần tiếp theo của bài báo sẽ giới thiệu cấu trúc của DES và cách thực hiện nó trên FPGA.

3.1 Cấu trúc khối của một vòng DES

Hình 3 giới thiệu cấu trúc sơ đồ khối của một vòng trong thuật toán DES. Cấu trúc này cũng hoàn toàn thích hợp cho việc thực hiện DES một cách có hiệu quả trên phần cứng có thể tái cấu hình.

Thuật toán DES dựa chủ yếu trên hai phép toán là các hoán vị cố định và phép thế. Cả hai phép toán này đều được thực hiện rất tốt trên FPGA. DES thực hiện bằng cách sử dụng 8 S-box (mỗi hộp có kích thước 64×4) chiếm tổng cộng 2Kbit. Dung lượng này tương đối nhỏ so với bộ nhớ và có thể thực hiện bằng cách phân chia bộ nhớ trong FPGA. Các phép hoán vị cố định thực chất không chiếm tài nguyên của FPGA khi nó được thực hiện bằng cách thay đổi dây. Các đặc điểm này được khai thác để có được một cách thực hiện DES có hiệu quả, như trên hình 3.

Ba đầu vào: Cho phép chip (CE - Chip Enable), Clock (CLK), dữ liệu vào (IN) và chỉ có một đầu ra (OUT) là bốn chân của một chip DES. Chân CE được kích hoạt (cho phép chip hoạt động) khi nó ở trạng thái thấp ('0'). Chân clock bên ngoài (CLK) là clock chính cho cả mạch, được dùng để tạo tất cả các tín hiệu điều khiển việc đồng bộ luồng dữ liệu.

Khi chân CE được kích hoạt, 64 bit đầu vào sẽ được hoán vị và được chia thành hai phần bằng nhau để đưa vào các chân RIN và LIN. Ở sườn lên đầu tiên của clock, cả hai nửa đó sẽ được chuyển đến đầu ra của hai thanh ghi REGA và REGB. Nửa bên phải (đầu ra REGA) sẽ thực hiện các phép toán là hoán vị E (PE), cộng module 2 với khoá con, phép thế (qua hộp S-box), hoán vị P (PP) và cộng module 2 với nửa bên trái (đầu ra REGB). Trước khi có chu kỳ clock tiếp theo, nửa bên phải cũ (RIGHT) là đầu vào của thanh ghi REGB và nửa bên trái mới (LEFT) là đầu vào của thanh ghi REGA. 16 vòng lặp sẽ được thực hiện. Sau 16 chu kỳ clock, hai nửa RIGHT và LEFT sẽ được nối vào nhau để đưa đến khối thực hiện hoán vị ngược (IP-1) tạo nên phép mã hoá cho khối 64 bit đầu vào. Chú ý là ở đây sử dụng 8 khối DES S-Box có cấu trúc song song nên sẽ giảm đáng kể đường tới hạn cho việc mã hoá và giải mã.

3.2 Tóm tắt việc thực hiện

Việc thực hiện thuật toán DES trên FPGA đã được hoàn thành trên thiết bị VirtexE XCV400e-8-bg560 vaf sử dụng Xilinx Foundation Series F4.1i như là một công cụ tổng hợp. Thiết bị được lập trình bằng ngôn ngữ VHDL. Nó chiếm 165 (3%) slice CLB, 117(1%) slice trigger và 129 (41%) các đường vào/ra (I/O). Thiết kế đạt tần số 68.05 MHz (14.7 µs), cần 16 chu kỳ clock để mã hoá một khối dữ liệu (64 bit). Vì vậy, tốc độ mã hoá là (68.05*64)/16 = 274 Mbit/s.

4. SO SÁNH ĐẶC TÍNH

Bảng 1 chỉ ra đặc điểm của một số cách thực hiện phần cứng DES đã được giới thiệu.Chú ý là kết quả đạt được là tốt so với các phương pháp trước đây.

Thực hiện VLSI của DES bằng công nghệ 0.6 micron tĩnh CMOS là phương pháp nhanh nhất từ trước đến nay. Sử dụng phương pháp Pipeline thì mã hoá đạt tốc độ ≥6.7 Gbs. Một số cách thực hiện trên FPGA của DES đạt được tốc độ trong khoảng từ 26 đến 10752 Mbit/s với các cách thiết kế khác nhau. Thực hiện DES bằng free DES core dùng phương pháp Pipeline ở chế độ ECB sẽ có được tốc độ dữ liệu là 3052 Mbit/s. Thực

hiện DES bằng Java (Jbit) sẽ có được tốc độ mã hoá nhanh nhất là 10752 Mbit/s. Thực hiện DES theo cả hai phương pháp Pipeline 2 giai đoạn và 4 giai đoạn sẽ đạt được tốc độ tương ứng là 183.3 Mbit/s và 402.7 Mbit/s. Hầu hết các cấu trúc FPGA cho thực hiện DES đều dùng phương pháp Pipeline từng phần hoặc toàn phần, chỉ có thiết kế trong [10] là thực hiện một vòng DES trên FPGA. Thiết kế được thực hiện trên XC4020E chiếm 438 slice CLB, nó cần 24 chu kỳ clock để hoàn thành việc mã hoá một khối dữ liệu đơn và đạt được tốc độ là 26.7 Mbit/s, do đó, hệ số tốc độ/số slice cần dùng là 0.06. Phương pháp thực hiện DES mà tác giả đưa ra ở đây cải thiện được cả hai hệ số là tốc độ và số slice cần dùng, cụ thể là nó cần 165 slice CLB trên XVC400 và đạt tốc độ 274 Mbit/s. Hệ số tốc độ/số slice cần dùng trong thiết kế là 2.34. So sánh với cấu trúc của thiết kế trong [10] thì phương pháp này tăng tốc độ lên 10 lần và giảm 4 lần slice CLB. Trên thực tế, xét về mặt cấu hình thì phương pháp này đứng thứ 2 nhưng hệ số tốc độ/số slice cần dùng thì thực sự đáng thuyết phục.

5. KẾT LUẬN

Bài báo này đã đưa ra phương pháp thực hiện DES nhanh và hiệu quả trên phần cứng có thể tái cấu hình. Thực hiện trên VLSI và FPGA sẽ có thể đạt được tốc độ rất cao phụ thuộc vào phương pháp thiết kế, tài nguyên thiết kế, tối ưu hoá cả thuật toán và mức thiết kế. Từ bảng 1 ta có thể thấy rằng phương pháp đưa ra có tính cạnh tranh so với các phương pháp thực hiện DES trên phần cứng có thể tái cấu hình trước đây.

Cấu trúc có thể được nâng cấp để đạt kết quả tốt hơn. Hầu hết các thiết kế trước đây đều sử dụng phương pháp Pipeline toàn phần để có được tốc độ tốt hơn khi số slice cần dùng không đổi.

TÀI LIỆU THAM KHẢO

[1]. Nguyễn Bình. Giáo trình Mật mã học - NXB Bưu điện, 2002.

[2]. Don Coppersmith. The data encryption standard (DES) and its strength against attacks. IBM Journal of Research and Development, 1994.

[3]. National Bureau of Standards, Data Encryption Standard, FIPS-Pub.46. National Bureau of Standards, U.S. Department of Commerce, Washington D.C., tháng 1/1977.

[4]. John Gilmore, "Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design", 1998, O'Reilly.

NGHIỆM THU ĐỀ TÀI NCKH

● Ngày 20/04/2011, Hội đồng khoa học nhà trường đã tổ chức họp nghiệm thu đề tài ***"Xây dựng hệ thống bài tập vật lý đại cương theo hướng tăng cường ứng dụng nghề nghiệp cho sinh viên các ngành kỹ thuật công nghiệp"*** chủ nhiệm đề tài ThS. Ngô Minh Đức.

Hiện nay, hệ thống các giáo trình, bài tập môn vật lý đại cương theo hướng tăng cường ứng dụng nghề nghiệp cho sinh viên còn rất thiếu và yếu. Sản phẩm của đề tài là cuốn sách bài tập vật lý đại cương A1&A2 với các bài tập có định hướng ứng dụng nghề nghiệp cho sinh viên các ngành kỹ thuật. Cuốn sách gồm 56 dạng bài toán gắn với nội dung của từng bài học lý thuyết theo chương trình. Cấu trúc mỗi bài gồm 4 phần: Tóm tắt lý thuyết, bài toán cơ bản và phương pháp giải, bài tập tự giải, hướng dẫn cách giải và đáp số. Cuốn sách được biên soạn công phu, sáng tạo, phù hợp cho sinh viên trong quá trình tự học theo hình thức học chế tín chỉ. Nhóm tác giả cũng đã triển khai dạy thử nghiệm ở các lớp ngành May và cho kết quả tốt. Hội đồng khoa học đánh giá cao những giá trị thực tiễn của đề tài và nhất trí cho đề tài được nghiệm thu loại xuất sắc.

● Ngày 20/05/2011, đề tài có mã số 18.2010.RD/HDD-ĐHCN ***"Nghiên cứu tổng hợp dược chất Oxalat sắt từ phoi sắt phế thải xưởng cơ khí trong trường, làm nguyên liệu sản xuất thuốc bổ máu trong dược phẩm và thức ăn chăn nuôi"*** do ThS. Hoàng Thanh Đức làm chủ nhiệm đã được Hội đồng khoa học nhà trường họp nghiệm thu và đánh giá cao những ý nghĩa khoa học, giá trị thực tiễn của đề tài.

Đề tài đã nghiên cứu, lựa chọn được phương pháp hiệu quả để tổng hợp Oxalat sắt từ phoi sắt phế thải bằng cách: cho phoi sắt tác dụng với axit sunfuric 15%, sau đó sắt II sunfat tổng hợp được cho tác dụng với axit oxalic để tạo thành oxalat sắt $FeC_2O_4.2H_2O$. Nhóm tác giả đã tiến hành khảo sát xác định các điều kiện phản ứng về nồng độ của axit H2SO4, lượng sắt II sunfat, thời gian và nhiệt độ phản ứng để xác lập quy trình công nghệ tổng hợp oxalat sắt hiệu quả. Kết quả thu được từ nghiên cứu của đề tài là sản phẩm dược chất Oxalat sắt có độ tinh khiết cao trên 99%, đạt yêu cầu chất lượng phục vụ nhu cầu sử dụng làm nguyên liệu cho sản xuất thuốc bổ máu trong dược phẩm và chăn nuôi, tiết kiệm chi phí, bước đầu đem lại các giá trị kinh tế cao. Đề tài đạt kết quả xuất sắc.