(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ

(11) **1-0052722**

(51)[2022.01] **H04N 19/31**

(13) **B**

(21) 1-2023-06707

(22) 27/09/2023

(45) 27/10/2025 451

(43) 25/01/2024 430A

(73) CÔNG TY TNHH MỘT THÀNH VIÊN TỔNG CÔNG TY SẢN XUẤT THIẾT BỊ VIETTEL (VN)
Thôn An Bình, Xã An Khánh, Huyện Hoài Đức, Thành phố Hà Nội

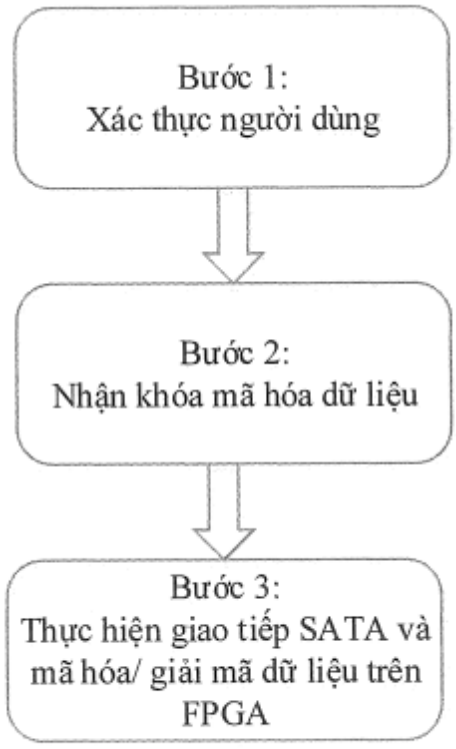
(72) NGUYỄN TUẤN TÚ (VN).

(74) Công ty TNHH NACILAW (NACILAW)

(54) PHƯƠNG PHÁP XÁC THỰC VÀ MÃ HÓA THỜI GIAN THỰC DỮ LIỆU Ổ CỨNG BẰNG FPGA QUA GIAO TIẾP SATA 3

(21) 1-2023-06707

(57) Sáng chế đề xuất phương pháp xác thực và mã hóa thời gian thực dữ liệu ổ cứng bằng FPGA qua giao tiếp SATA 3 sử dụng các giải pháp lưu trữ bằng phần tử an toàn, các giải thuật mã hóa/giải mã phần mềm trên nền tảng FPGA. Phương pháp bao gồm các bước: bước 1: xác thực người dùng khi máy tính được khởi động; bước 2: mô-đun mã hóa sẽ thực hiện lấy khóa mã hóa dữ liệu DEK được lưu trong mô-đun xác thực; bước 3: thực hiện giao tiếp SATA cùng với mã hóa/ giải mã dữ liệu trên FPGA.




Hình 2

**Lĩnh vực kỹ thuật được đề cập**

Sáng chế đề cập đến phương pháp xác thực và mã hóa thời gian thực dữ liệu ổ cứng bằng FPGA (Field-Programmable Gate Array – Mạch tích hợp có cấu trúc là các mảng phần tử logic lập trình được) áp dụng trong các lĩnh vực: xác thực người dùng; mã hóa dữ liệu lưu trữ trong ổ cứng qua giao tiếp SATA 3 (Serial Advanced Technology Attachment – Chuẩn kết nối ổ đĩa cứng nối tiếp tiên tiến) phục vụ đối tượng người dùng yêu cầu cao về bảo mật, an toàn thông tin.

**Tình trạng kỹ thuật của sáng chế**

Ngày nay, nhu cầu về các giải pháp an ninh, xác thực và mã hóa dữ liệu lưu trữ trong ổ cứng (đặc biệt là với các thiết bị phục vụ người dùng cá nhân) ngày càng tăng. Để đáp ứng nhu cầu của người sử dụng, các nhà sản xuất ổ cứng đã đưa ra nhiều giải pháp kỹ thuật khác nhau. Giải pháp phổ biến nhất hiện nay là ổ cứng tự mã hóa (SED - Self-Encrypting Drive). SED là loại ổ cứng có thể tự động mã hóa và giải mã dữ liệu trong quá trình làm việc mà không cần đến một tác động nào khác. Việc mã hóa/giải mã dữ liệu được thực hiện thông qua một khóa mã hóa dữ liệu (DEK - Data Encrytion Key).

Ưu điểm:

- Toàn bộ dữ liệu vào/ra ổ cứng đều phải đi qua bộ mã hóa/giải mã này. Do đó, chỉ cần đặt một DEK mới, toàn bộ dữ liệu cũ trên ổ đĩa sẽ trở nên vô nghĩa, không thể phục hồi được nữa. Thay vì phải mất nhiều giờ để ghi/xóa nhiều lần trên ổ cứng thông thường, thao tác này chỉ cần vài giây để có kết quả tương tự.
- SED cho phép người dùng đặt thêm một khóa chứng thực (AK - Authentication Key), làm việc như một mật khẩu để khóa ổ cứng lại. Khi khóa này được thiết lập, hệ thống sẽ yêu cầu mật khẩu khi khởi động lần đầu tiên. Tùy thuộc vào loại bo mạch chủ, nếu nhập sai ba hoặc bốn lần hệ thống

sẽ tự động bỏ qua và khởi động bình thường với ổ cứng đó ở trạng thái khóa. Trong trường hợp này, ổ đĩa sẽ không sử dụng được cho tới khi hệ thống được tắt đi, bật lại và nhập đúng AK. Trên thực tế, cho dù ổ SED bị tháo ra khỏi máy và cắm sang máy khác, nó sẽ vẫn đòi phải nhập AK để truy cập. Nhưng nếu máy mới không hỗ trợ ổ SED, ổ đĩa sẽ trở nên vô dụng vì không thể mở khóa để thực hiện đọc/ghi dữ liệu, không có bất kỳ cách nào để vượt qua.

Nhược điểm:

- Khi ổ đĩa đã được mở khóa bằng cách nhập đúng AK, nó sẽ giữ nguyên trạng thái đó cho tới khi nguồn điện bị cắt. Ví dụ như khi để máy tính vào trạng thái chờ (stand by) hay trạng thái ngủ (sleep), ổ đĩa sẽ không bị khóa lại, nó chỉ bị khóa khi máy tính được tắt hoàn toàn. Nói một cách khác, nếu người dùng mất máy tính khi đang để ở trạng thái ngủ (sleep), dữ liệu trên ổ cứng hoàn toàn có thể bị truy cập trái phép. Nếu có mật khẩu của hệ điều hành, kẻ trộm chỉ cần thực hiện khởi động lại máy tính bằng một hệ điều hành khác từ USB hay đĩa CD là có thể truy cập được dữ liệu. Thậm chí nếu người dùng thiết lập cả mật khẩu cho BIOS, dữ liệu vẫn có thể bị lấy cắp bằng cách di chuyển ổ cứng sang máy tính khác mà không cắt nguồn điện. Do đó, nếu cần tính bảo mật thật cao, người dùng cần có thói quen tắt máy tính mỗi khi không sử dụng chứ không phải là trạng thái ngủ (sleep).
- AK được lưu trữ bên trong ổ cứng SED nên tồn tại nguy cơ lộ lọt AK dẫn đến mất quyền xác thực người dùng.
- Thuật toán mã hóa dữ liệu thường được các nhà sản xuất sử dụng trên ổ cứng SED là tiêu chuẩn mã hóa tiên tiến (Advanced Encryption Standard) AES-256. AES là thuật toán mã hóa đã được thế giới công nhận. Thuật toán này được thực hiện bởi các mạch tích hợp chuyên dụng nên với những đối tượng khách hàng có nhu cầu thay đổi thuật toán mã hóa theo đặc thù riêng của mình (Công an, Quân đội, Ngoại giao, Cơ yếu…) thì gần như hiện nay không thể thực hiện được.

**Bản chất kĩ thuật của sáng chế**

Mục đích của sáng chế là đề xuất phương pháp xác thực người dùng, mã hóa/giải mã dữ liệu ổ cứng có khả năng bảo mật tương tự như ổ cứng SED, đồng thời khắc phục được các nhược điểm của ổ cứng SED đã nêu ở trên.

Để đạt được mục đích trên, sáng chế đề xuất phương pháp sử dụng FPGA để thực hiện xác thực, mã hóa/giải mã dữ liệu thời gian thực với tốc độ cao đến 06 Gbps (tương thích với giao tiếp SATA 3). Quá trình mã hóa/giải mã đảm bảo khả năng thay thế thuật toán dễ dàng theo nhu cầu của từng đối tượng người dùng.

Phương pháp được đề xuất bao gồm các bước:

Bước 1: xác thực người dùng khi máy tính được khởi động;

Bước 2: mô-đun mã hóa sẽ thực hiện lấy khóa mã hóa dữ liệu (DEK) được lưu trong mô-đun xác thực;

Bước 3: thực hiện giao tiếp SATA cùng với mã hóa/ giải mã dữ liệu trên FPGA.

Phương pháp được đề xuất có khả năng ứng dụng rộng rãi và thích hợp với phần lớn thiết bị. Phương pháp cho kết quả tối ưu nhất khi được hiện thực hóa trên dòng chip FPGA Kintex-7 của Xilinx.

**Mô tả vắn tắt các hình vẽ**

Hình 1 là hình vẽ sơ đồ tổng quát tương tác giữa các thành phần của hệ thống trong quá trình thực hiện sáng chế;

Hình 2 là hình vẽ sơ đồ tổng quát các bước thực hiện sáng chế;

Hình 3 là hình vẽ sơ đồ tổng quát quá trình xác thực người dùng;

Hình 4 là hình vẽ sơ đồ tổng quát quá trình nhận khóa mã hóa dữ liệu từ Mô-đun xác thực;

Hình 5 là hình vẽ sơ đồ tổng quát quá trình mã hóa/giải mã dữ liệu trên FPGA.

**Mô tả chi tiết sáng chế**

Phần sau đây mô tả chi tiết phương pháp xác thực và mã hóa thời gian thực dữ liệu ổ cứng bằng FPGA qua giao tiếp SATA 3 thông qua các hình vẽ minh họa kèm theo. Bên cạnh đó, một số thuật ngữ chuyên môn được hiểu như sau:

FPGA: (Field-Programmable Gate Array – Mạch tích hợp có cấu trúc là các mảng phần tử logic lập trình được). Với mật độ cổng logic lớn và khả năng tái lập trình được, FPGA phù hợp để thực hiện những bài toán đòi hỏi khối lượng tính toán lớn, yêu cầu làm việc theo thời gian thực.

SATA 3 (Serial Advanced Technology Attachment): là chuẩn kết nối ổ đĩa cứng nối tiếp tiên tiến. Tiêu chuẩn này ra đời từ năm 2003 và là một trong những chuẩn kết nối phổ biến nhất hiện nay. Phiên bản mới nhất của tiêu chuẩn này là phiên bản thứ 3 hay còn gọi là SATA 3. SATA 3 cho phép tốc độ truyền tải lên đến 06 Gbps.

Phương pháp được đề xuất có khả năng ứng dụng rộng rãi và thích hợp với phần lớn thiết bị. Phương pháp cho kết quả tối ưu nhất khi được hiện thực hóa trên dòng chip FPGA Kintex-7 của Xilinx.

Tham chiếu Hình 1, phương pháp được đề xuất được triển khai thực hiện trên hệ thống gồm bốn thành phần chính:

- Mô-đun bảo mật: được thiết kế sử dụng FPGA. Có chức năng xác thực người dùng, mã hóa/giải mã dữ liệu ổ cứng;
- Mô-đun xác thực: được thiết kế sử dụng phần tử lưu trữ an toàn. Có chức năng lưu trữ khóa chứng thực người dùng (AK), khóa mã hóa dữ liệu (DEK). Mô-đun xác thực được kết nối trực tiếp đến mô-đun bảo mật thông qua giao tiếp I2C (Inter-Integrated Circuit – giao tiếp kết nối các vi mạch tích hợp). Dữ liệu truyền tải trên đường tín hiệu giữa mô-đun xác thực và mô-đun bảo mật là dữ liệu đã được mã hóa;
- Bo mạch chủ máy tính: kết nối với mô-đun bảo mật qua giao tiếp SATA 3. Dữ liệu truyền tải trên đường tín hiệu giữa bo mạch chủ và mô-đun bảo mật là dữ liệu rõ, không được mã hóa;
- Ổ cứng: kết nối với mô-đun bảo mật qua giao tiếp SATA 3. Dữ liệu truyền tải trên đường tín hiệu giữa ổ cứng và mô-đun bảo mật là dữ liệu đã được mã hóa. Thuật toán mã hóa, các tham số mã được sử dụng có thể thay đổi tùy theo từng đối tượng người dùng. Mặc định thuật toán sử dụng trong phương pháp là AES-256.

Tham chiếu Hình 2, các mô-đun xử lý tín hiệu chính với các bước thực hiện được mô tả cụ thể như sau:

Bước 1: xác thực người dùng khi máy tính được khởi động. Tại bước này, mô-đun mã hóa sẽ thực hiện xác thực khóa chứng thực người dùng (AK).

Tham chiếu Hình 3 thể hiện chi tiết quá trình xác thực giữa mô-đun xác thực và mô-đun bảo mật.

Khi máy tính khởi động, mô-đun bảo mật sẽ kiểm tra có mô-đun xác thực được kết nối vào không. Nếu mô-đun xác thực được kết nối thì mô-đun bảo mật sẽ thực hiện xác thực người dùng. Nếu vì một lý do nào đó mà mô-đun bảo mật không xác định được mô-đun xác thực được kết nối vào thì mô-đun bảo mật sẽ ngừng hoạt động. Bo mạch chủ của máy tính sẽ bỏ qua việc khởi động với mô-đun bảo mật và ổ cứng mã hóa.

Mô-đun bảo mật và mô-đun xác thực đều được thiết kế tích hợp phần tử lưu trữ an toàn sử dụng IC ATAES132 của hãng Microchip. Phần tử này sử dụng để lưu trữ khóa xác thực (AK) và khóa mã hóa dữ liệu (DEK).

Quá trình xác thực gồm các bước sau:

- FPGA gửi lệnh yêu cầu mô-đun xác thực sinh ra và gửi lại cho FPGA một số ngẫu nhiên (RNG - Random Number Generator) gồm 16 byte;
- Dựa trên số RNG này, phần tử lưu trữ an toàn ở trên mô-đun bảo mật và mô-đun xác thực sẽ thực hiện đồng bộ với nhau một số sử dụng một lần (NONCE - Number used once) có chiều dài 12 byte để đưa vào thực hiện tại các bước tiếp theo;
- FPGA yêu cầu phần tử lưu trữ an toàn trên mô-đun xác thực thực hiện mã hóa số RNG bằng số NONCE và mã xác thực AK1 được lưu trữ;
- Mô-đun xác thực thực hiện tính toán mã xác thực tin nhắn (MAC - Message Authentication Code) của giá trị mã hóa ở bước trên và gửi trả lại MAC cho FPGA (gọi là MAC1). Dữ liệu gửi đi không chứa mã khóa xác thực (AK) nên đảm bảo được tính an toàn của hệ thống;
- FPGA yêu cầu phần tử lưu trữ an toàn trên mô-đun bảo mật thực thực hiện mã hóa số RNG bằng số NONCE và mã xác thực AK2 được lưu trữ;

- Mô-đun xác thực thực hiện tính toán mã xác thực tin nhắn MAC của giá trị mã hóa ở bước trên và gửi trả lại MAC cho FPGA (gọi là MAC2);
- FPGA so sánh MAC1 và MAC2:

  + Nếu MAC1 và MAC2 giống nhau thì chứng tỏ AK1 và AK2 giống nhau và quá trình xác thực thành công. FPGA sẽ tiếp tục thực hiện quá trình nhận khóa mã hóa dữ liệu được lưu trong mô-đun xác thực;

  + Nếu MAC1 và MAC2 khác nhau thì chứng tỏ AK1 và AK2 khác nhau và quá trình xác thực thất bại. Mô-đun bảo mật sẽ ngừng hoạt động. Bo mạch chủ của máy tính sẽ bỏ qua việc khởi động với Mô-đun bảo mật và ổ cứng mã hóa.

Bước 2: mô-đun mã hóa sẽ thực hiện lấy khóa mã hóa dữ liệu (DEK) được lưu trong mô-đun xác thực.

Tham chiếu Hình 4 thể hiện chi tiết quá trình nhận khóa mã hóa dữ liệu được lưu trữ trong Mô-đun xác thực.

Để nâng cao tính bảo mật, khóa mã hóa dữ liệu không được truyền nhận trực tiếp mà được thực hiện thông qua một khóa bảo mật khác (gọi là *key0*). Khóa bảo mật *key0* là giống nhau giữa mô-đun bảo mật và mô-đun xác thực.

Chi tiết quá trình nhận khóa gồm các bước sau:

- FPGA gửi lệnh yêu cầu mô-đun xác thực sinh ra và gửi lại cho FPGA một số ngẫu nhiên (RNG) gồm 16 byte;
- Dựa trên số RNG này, phần tử lưu trữ an toàn ở trên mô-đun bảo mật và mô-đun xác thực sẽ thực hiện đồng bộ với nhau một số sử dụng một lần NONCE gồm 12 byte để đưa vào thực hiện tại các bước tiếp theo;
- FPGA gửi yêu cầu đến mô-đun xác thực thực hiện mã hóa khóa mã hóa dữ liệu bằng khóa bảo mật *key0* và số NONCE rồi gửi dữ liệu sau mã hóa cho phần tử lưu trữ an toàn trên mô-đun bảo mật thông qua FPGA. Dữ liệu trao đổi giữa mô-đun bảo mật và mô-đun xác thực là dữ liệu đã được mã hóa nên giảm thiểu được nguy cơ lọt lộ thông tin;

- Phần tử lưu trữ an toàn trên mô-đun bảo mật thực hiện giải mã dữ liệu mã hóa trên bằng số NONCE được đồng bộ trước đó và khóa *key0* được lưu trữ. Giá trị thu được là khóa mã hóa dữ liệu (DEK).

Bước 3: thực hiện giao tiếp SATA cùng với mã hóa/ giải mã dữ liệu trên FPGA.

Tham chiếu Hình 5 thể hiện chi tiết các khối chức năng được thực hiện. Chi tiết gồm:

- Lớp vật lý ở phía thiết bị gốc (PHY Host) và lớp vật lý ở phía thiết bị ngoại vi (PHY Device): thực hiện giao tiếp vật lý giữa FPGA với bo mạch chủ máy tính và với ổ cứng. PHY Host và PHY Device là mô-đun phần mềm đảm nhiệm các chức năng:

  + Cấu hình các khối chức năng phần cứng giao tiếp số tốc độ cao (MGTs - Multi Gigabit Transceivers) của FPGA về tham số vật lý. Các khối MGTs thực hiện chuyển đổi tín hiệu vi sai trên đường truyền SATA thành tín hiệu số và ngược lại.

  + Thực hiện mã hóa/giải mã 8 bit/10 bit để đưa sang lớp kết nối (Link Layer).

  + Thực hiện khởi tạo giao tiếp SATA với bo mạch chủ máy tính và với ổ cưng.

  Khối này yêu cầu tần số xung nhịp đầu vào đến 150 MHz để đảm bảo đáp ứng được tốc độ 6 Gbps của giao tiếp SATA 3.
- Lớp kết nối (Link Layer) là khối chức năng thực hiện mã hóa/giải mã dữ liệu số từ lớp vật lý ở phía thiết bị gốc (PHY Host)/lớp vật lý ở phía thiết bị ngoại vi (PHY Device) thành dữ liệu theo định dạng khung (FIS - Frame Information Struct) đáp ứng tiêu chuẩn SATA.
- Cầu dữ liệu (Bridge Data): là mô-đun phần mềm đóng vai trò cầu nối truyền dữ liệu từ bo mạch chủ máy tính tới ổ cứng và ngược lại. Thực hiện quá trình điều khiển luồng dữ liệu tránh các tranh chấp khi truyền dữ liệu.
- Khối mã hóa/giải mã: thực hiện mã hóa đường dữ liệu từ bo mạch chủ máy tính xuống ổ cứng; giải mã dữ liệu từ ổ cứng gửi lên bo mạch chủ máy tính. Quá trình thực hiện khối này dựa trên nguyên tắc:

+ Không giải mã dữ liệu với FIS về dữ liệu định danh thiết bị lưu trữ (identify) và FIS về dữ liệu tự phân tích, giám sát, báo cáo (S.M.A.R.T – Self Monitoring Analysis and Reporting Technology) từ ổ cứng lên bo mạch chủ máy tính;

+ Không mã hóa với các FIS điều khiển;

+ Thuật toán mã hóa và giải mã có thể thay thế linh hoạt khi có yêu cầu. Khóa mã hóa được sử dụng từ bước 2 – nhận khóa mã hóa dữ liệu bên trên.

Tham chiếu Hình 5, quá trình ghi dữ liệu từ bo mạch chủ máy tính đến ổ cứng thực hiện các bước như sau:

- Bo mạch chủ máy tính gửi dữ liệu chưa mã hóa đến lớp vật lý ở phía thiết bị ngoại vi;
- Lớp vật lý ở phía thiết bị ngoại vi chuyển tín hiệu vật lý thành luồng dữ liệu số tốc độ cao;
- Lớp kết nối bóc tách các FIS dữ liệu theo tiêu chuẩn SATA;
- Cầu dữ liệu bóc tách dữ liệu và giải quyết các mâu thuẫn trong quá trình vận hành luồng dữ liệu SATA;
- Khối mã hóa dữ liệu thực hiện mã hóa dữ liệu theo thuật toán mong muốn;
- Lớp kết nối đóng gói dữ liệu sau mã hóa thành các FIS dữ liệu theo tiêu chuẩn SATA;
- Lớp vật lý ở phía thiết bị gốc chuyển tín hiệu số đã mã hóa thành tín hiệu vật lý và ghi vào ổ cứng.

Tham chiếu Hình 5, quá trình bo mạch chủ máy tính đọc dữ liệu từ ổ cứng thực hiện các bước như sau:

- Lớp vật lý ở phía thiết bị gốc chuyển tín hiệu vật lý từ ổ cứng thành luồng dữ liệu số tốc độ cao. Dữ liệu số này là dữ liệu đang được mã hóa;
- Lớp kết nối bóc tác dữ liệu mã hóa thành các FIS dữ liệu theo tiêu chuẩn SATA;
- Cầu dữ liệu bóc tách dữ liệu và giải quyết các mâu thuẫn trong quá trình vận hành luồng dữ liệu SATA;
- Khối giải mã dữ liệu thực hiện giải mã dữ liệu theo thuật toán mong muốn;

- Lớp kết nối đóng gói dữ liệu đã giải mã thành các FIS dữ liệu theo tiêu chuẩn SATA;
- Lớp vật lý ở phía thiết bị ngoại vi chuyển luồng dữ liệu số tốc độ cao đã giải mã thành tín hiệu vật lý và gửi lên bo mạch chủ máy tính.

Sáng chế đề xuất khác biệt ở chỗ, giải pháp được phát triển với sự mềm dẻo, linh động dựa trên nền tảng FPGA. Cụ thể, sáng chế thực hiện việc mã hóa/giải mã dữ liệu ổ cứng tốc độ cao với khả năng thay thế phương pháp mã hóa dễ dàng theo nhu cầu của từng đối tượng người sử dụng.

Các phần mô tả nêu trên chỉ là các phương án cụ thể của sáng chế, mà không dự định giới hạn phạm vi bảo hộ của sáng chế. Bất kỳ sự sửa đổi hoặc sự thay thế dễ dàng được tìm ra bởi người có trình độ trung bình trong lĩnh vực kỹ thuật tương ứng trong phạm vi kỹ thuật được bộc lộ theo sáng chế sẽ nằm trong phạm vi bảo hộ của sáng chế. Do đó, phạm vi bảo hộ của sáng chế sẽ thuộc phạm vi bảo hộ của yêu cầu bảo hộ.

## Yêu cầu bảo hộ

1. Phương pháp xác thực và mã hóa thời gian thực dữ liệu ổ cứng bằng FPGA qua giao tiếp SATA 3 bao gồm các bước:

bước 1: xác thực người dùng khi máy tính được khởi động; tại bước này, Mô-đun mã hóa sẽ thực hiện xác thực khóa chứng thực người dùng AK; cụ thể:

sử dụng phần tử lưu trữ an toàn ATAES132 của hãng microchip;

thực hiện sinh và xác thực số ngẫu nhiên sử dụng một lần (NONCE);

FPGA (mạch tích hợp có cấu trúc là các mảng phần tử logic lập trình được) yêu cầu phần tử lưu trữ an toàn trên mô-đun xác thực thực hiện mã hóa số RNG bằng số NONCE và mã xác thực AK1 được lưu trữ;

mô-đun xác thực thực hiện tính toán mã xác thực tin nhắn (MAC) của giá trị mã hóa ở bước trên và gửi trả lại MAC cho FPGA (gọi là MAC1);

FPGA yêu cầu phần tử lưu trữ an toàn trên mô-đun bảo mật thực hiện mã hóa số RNG bằng số NONCE và mã xác thực AK2 được lưu trữ;

mô-đun xác thực thực hiện tính toán mã xác thực tin nhắn MAC của giá trị mã hóa ở bước trên và gửi trả lại MAC cho FPGA (gọi là MAC2);

FPGA so sánh MAC1 và MAC2 để quyết định xác thực thành công hay không;

bước 2: mô-đun mã hóa sẽ thực hiện lấy khóa mã hóa dữ liệu DEK được lưu trong mô-đun xác thực; cụ thể:

FPGA gửi lệnh yêu cầu mô-đun xác thực sinh ra và gửi lại cho FPGA một số ngẫu nhiên RNG gồm 16 byte;

dựa trên số RNG này, phần tử lưu trữ an toàn ở trên mô-đun bảo mật và mô-đun xác thực sẽ thực hiện đồng bộ với nhau một số sử dụng một lần (NONCE) để đưa vào thực hiện tại các bước tiếp theo;

FPGA gửi yêu cầu đến mô-đun xác thực thực hiện mã hóa khóa mã hóa dữ liệu bằng khóa bảo mật *key0* và số NONCE rồi gửi dữ liệu sau mã hóa cho phần tử lưu trữ an toàn trên mô-đun bảo mật thông qua FPGA;

phần tử lưu trữ an toàn trên mô-đun bảo mật thực hiện giải mã dữ liệu mã hóa trên bằng số none được đồng bộ trước đó và khóa *key0* được lưu trữ; giá trị thu được là khóa mã hóa dữ liệu DEK;

bước 3: thực hiện giao tiếp SATA cùng với mã hóa/ giải mã dữ liệu trên FPGA; trong đó thực hiện các khối chức năng sau trên nền tảng FPGA:

lớp vật lý ở phía thiết bị gốc (PHY host) và lớp vật lý ở phía thiết bị ngoại vi (PHY device) thực hiện giao tiếp vật lý giữa FPGA với bo mạch chủ máy tính và với ổ cứng;

lớp kết nối (link layer) là khối chức năng thực hiện mã hóa/giải mã dữ liệu số từ tầng PHY Host/PHY Device thành dữ liệu theo định dạng khung FIS (frame information struct) đáp ứng tiêu chuẩn SATA;

cầu dữ liệu (bridge data) là khối chức năng đóng vai trò cầu nối truyền dữ liệu từ bo mạch chủ máy tính tới ổ cứng và ngược lại; thực hiện quá trình điều khiển luồng dữ liệu tránh các tranh chấp khi truyền dữ liệu;

khối mã hóa/giải mã: thực hiện mã hóa đường dữ liệu từ bo mạch chủ máy tính xuống ổ cứng; giải mã dữ liệu từ ổ cứng gửi lên bo mạch chủ máy tính.

2. Phương pháp xác thực và mã hóa thời gian thực dữ liệu ổ cứng bằng FPGA qua giao tiếp SATA 3 theo điểm 1, tại bước ghi dữ liệu từ bo mạch chủ máy tính đến ổ cứng, trong đó:

lớp vật lý ở phía thiết bị ngoại vi chuyển tín hiệu vật lý thành luồng dữ liệu số tốc độ cao;

lớp kết nối bóc tách, đóng gói dữ liệu sau mã hóa thành các FIS dữ liệu theo tiêu chuẩn SATA;

cầu dữ liệu bóc tách dữ liệu và giải quyết các mâu thuẫn trong quá trình vận hành luồng dữ liệu SATA;

khối mã hóa dữ liệu thực hiện mã hóa dữ liệu theo thuật toán mong muốn;

lớp vật lý ở phía thiết bị gốc chuyển tín hiệu số đã mã hóa thành tín hiệu vật lý và ghi vào ổ cứng.

3. Phương pháp xác thực và mã hóa thời gian thực dữ liệu ổ cứng bằng FPGA qua giao tiếp SATA 3 theo điểm 1, tại bước bo mạch chủ máy tính đọc dữ liệu từ ổ cứng, trong đó:

lớp vật lý ở phía thiết bị gốc chuyển tín hiệu vật lý từ ổ cứng thành luồng dữ liệu số tốc độ cao; dữ liệu số này là dữ liệu đang được mã hóa;

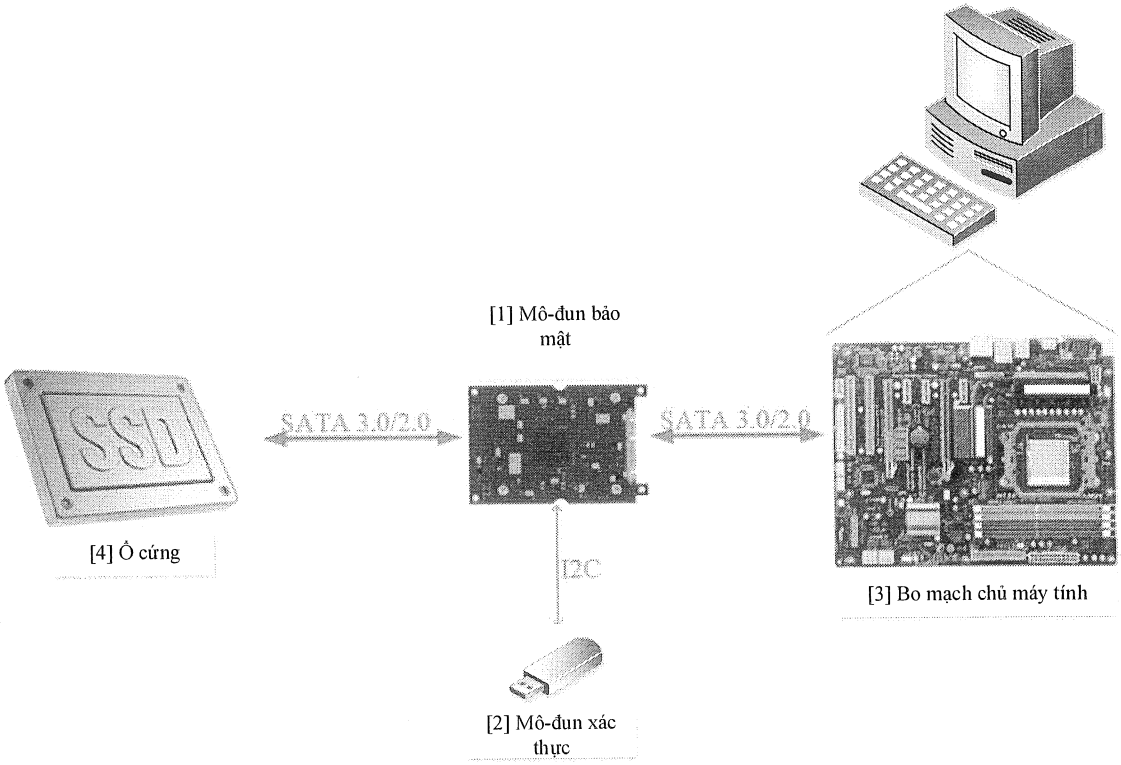
lớp kết nối bóc tác dữ liệu mã hóa thành các FIS dữ liệu theo tiêu chuẩn SATA;

cầu dữ liệu bóc tách dữ liệu và giải quyết các mâu thuẫn trong quá trình vận hành luồng dữ liệu SATA;

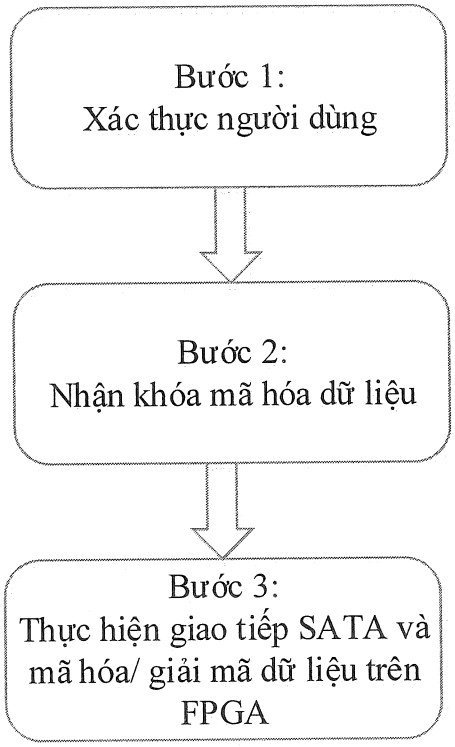
khối giải mã dữ liệu thực hiện giải mã dữ liệu theo thuật toán mong muốn;

lớp kết nối đóng gói dữ liệu đã giải mã thành các FIS dữ liệu theo tiêu chuẩn SATA;

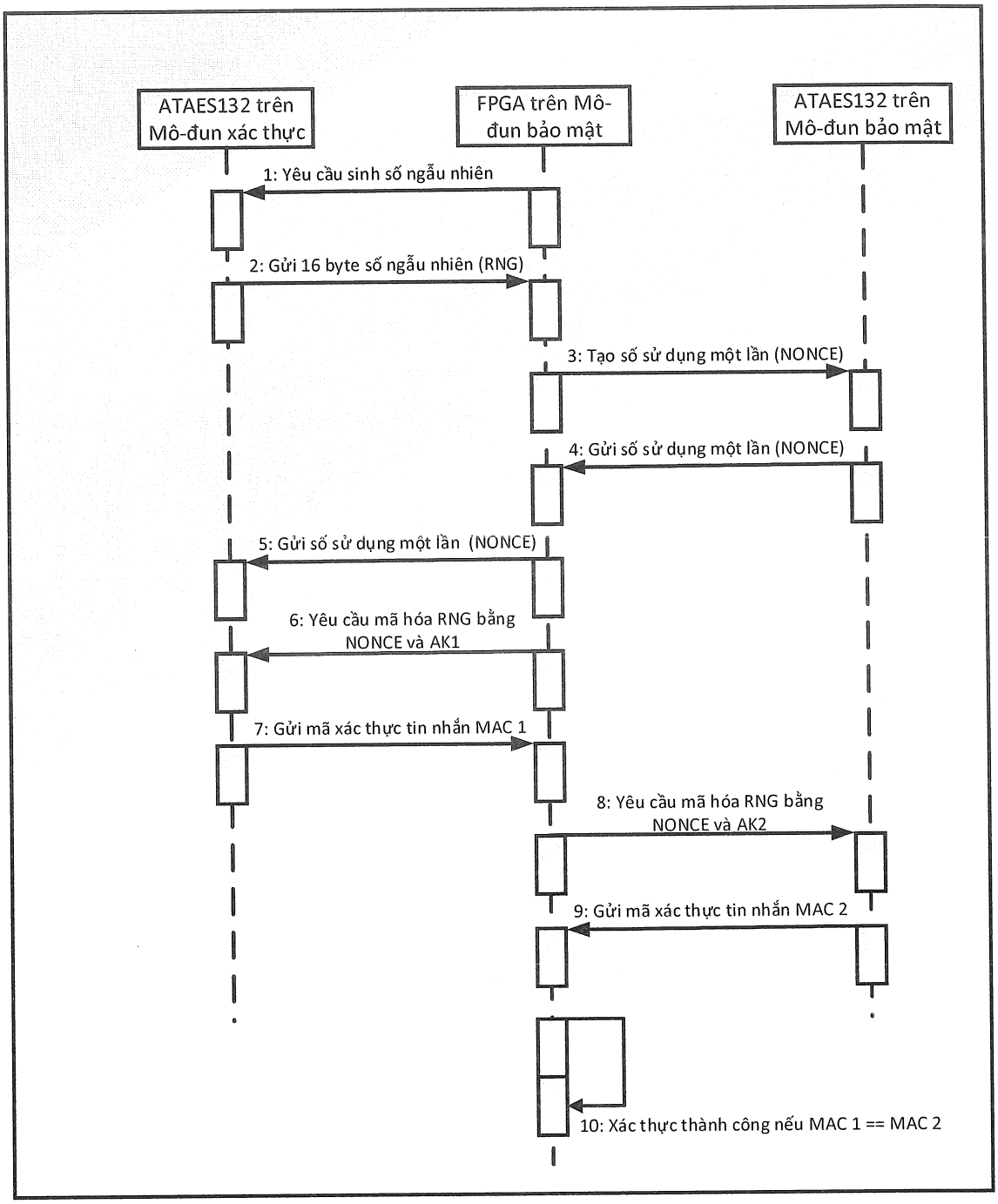
lớp vật lý ở phía thiết bị ngoại vi chuyển luồng dữ liệu số tốc độ cao đã giải mã thành tín hiệu vật lý và gửi lên bo mạch chủ máy tính.


[1] Mô-đun bảo mật
SSD
SATA 3.0/2.0
SATA 3.0/2.0
I2C
[4] Ổ cứng
[3] Bo mạch chủ máy tính
[2] Mô-đun xác thực

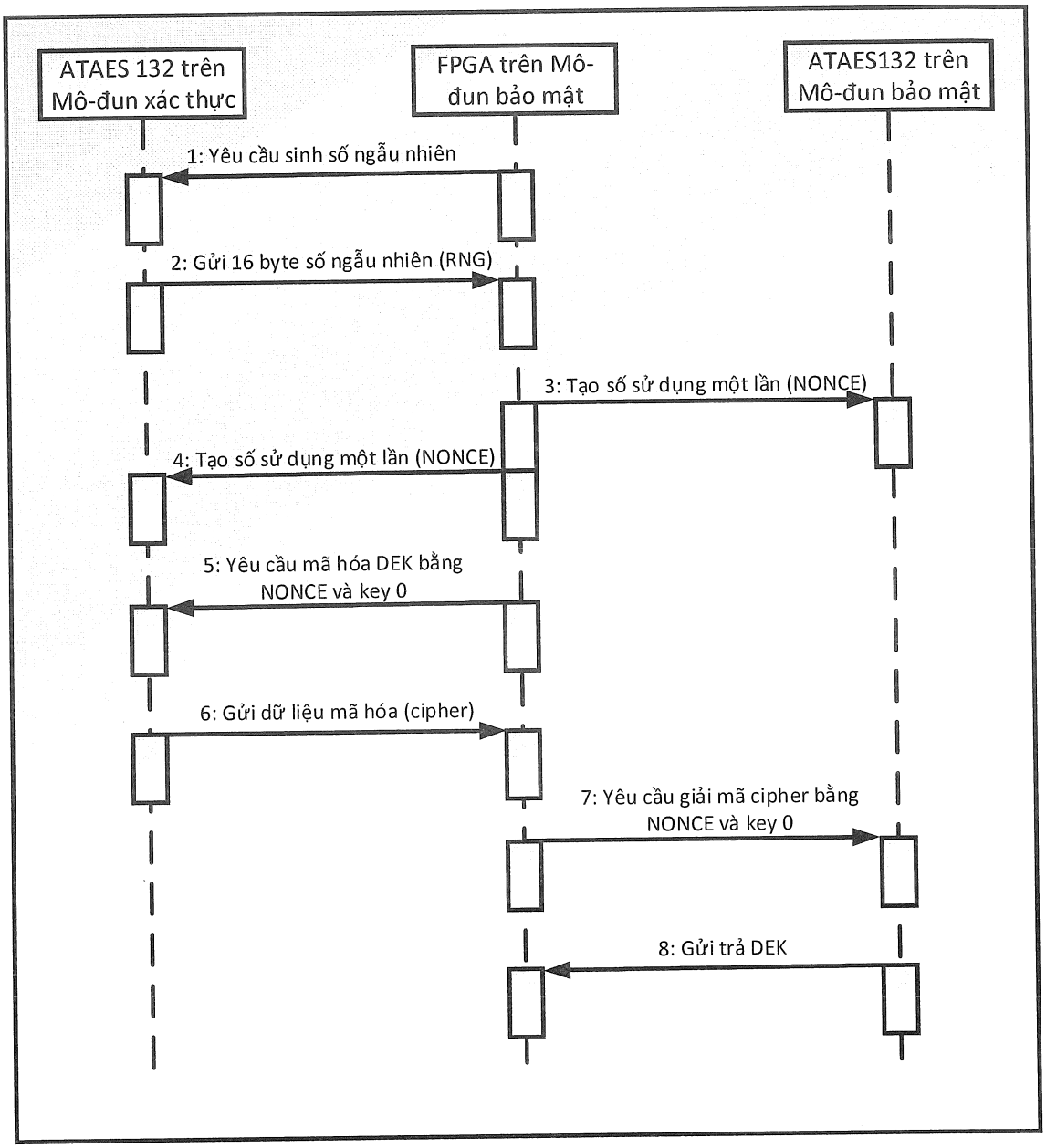
Hình 1


Bước 1:
Xác thực người dùng
Bước 2:
Nhận khóa mã hóa dữ liệu
Bước 3:
Thực hiện giao tiếp SATA và mã hóa/ giải mã dữ liệu trên FPGA

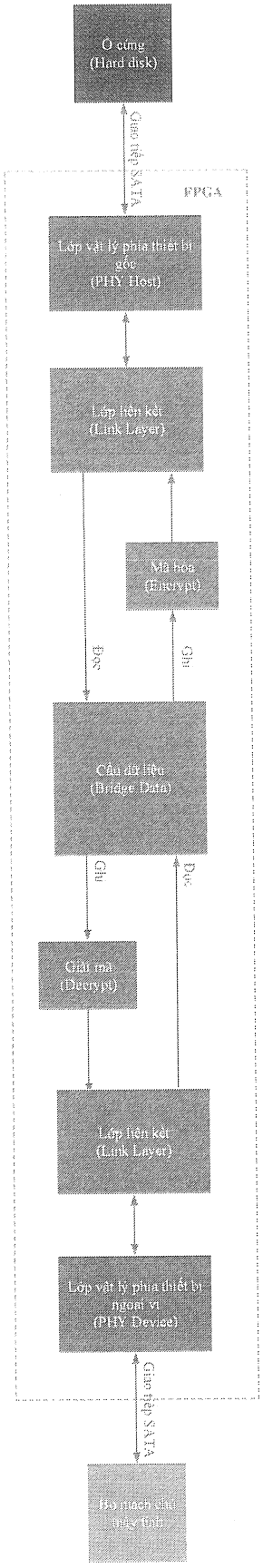
Hình 2


ATAES132 trên Mô-đun xác thực
FPGA trên Mô-đun bảo mật
ATAES132 trên Mô-đun bảo mật
1: Yêu cầu sinh số ngẫu nhiên
2: Gửi 16 byte số ngẫu nhiên (RNG)
3: Tạo số sử dụng một lần (NONCE)
4: Gửi số sử dụng một lần (NONCE)
5: Gửi số sử dụng một lần (NONCE)
6: Yêu cầu mã hóa RNG bằng NONCE và AK1
7: Gửi mã xác thực tin nhắn MAC 1
8: Yêu cầu mã hóa RNG bằng NONCE và AK2
9: Gửi mã xác thực tin nhắn MAC 2
10: Xác thực thành công nếu MAC 1 == MAC 2

Hình 3


ATAES 132 trên Mô-đun xác thực
FPGA trên Mô-đun bảo mật
ATAES132 trên Mô-đun bảo mật
1: Yêu cầu sinh số ngẫu nhiên
2: Gửi 16 byte số ngẫu nhiên (RNG)
3: Tạo số sử dụng một lần (NONCE)
4: Tạo số sử dụng một lần (NONCE)
5: Yêu cầu mã hóa DEK bằng NONCE và key 0
6: Gửi dữ liệu mã hóa (cipher)
7: Yêu cầu giải mã cipher bằng NONCE và key 0
8: Gửi trả DEK

Hình 4


Ổ cứng
(Hard disk)
Giao tiếp SATA
FPGA
Lớp vật lý phía thiết bị gốc
(PHY Host)
Lớp liên kết
(Link Layer)
Mã hóa
(Encrypt)
Đọc
Ghi
Cầu dữ liệu
(Bridge Data)
Ghi
Đọc
Giải mã
(Decrypt)
Lớp liên kết
(Link Layer)
Lớp vật lý phía thiết bị ngoại vi
(PHY Device)
Giao tiếp SATA
Bo mạch chủ máy tính

Hình 5