



(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)



1-0025371

(51)⁷ H03M 13/00

(13) B

(21) 1-2016-02700

(22) 24/12/2013

(86) PCT/CN2013/090285 24/12/2013

(87) WO 2015/096021 A1 02/07/2015

(45) 25/09/2020 390

(43) 26/09/2016 342A

(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)

Huawei Administration Building, Bantian, Longgang, Shenzhen, Guangdong 518129, China

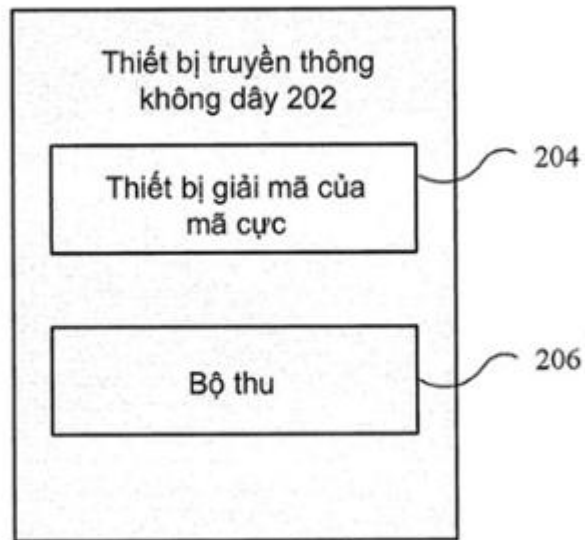
(72) LI, Bin (CA); TONG, Wen (CA); SHEN, Hui (CN); SHI, Yuchen (CN).

(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) THIẾT BỊ THU VÀ PHƯƠNG PHÁP GIẢI MÃ CHUỖI MÃ

(57) Sáng chế đề cập đến thiết bị thu và phương pháp giải mã chuỗi mã. Phương pháp bao gồm các bước: thu chuỗi mã có độ dài N bit đầu vào, trong đó chuỗi mã thu được bằng cách mã hóa một lượng bit thông tin trong bộ mã hóa ở thiết bị truyền trong hệ thống truyền thông không dây; chia chuỗi mã thành m mã con mà được ghép với nhau, trong đó mỗi mã con có độ dài N/m , và mỗi trong số N và m là các lũy thừa nguyên của 2, và $N > m$; tính toán riêng biệt, đối với m mã con của chuỗi mã, các khoảng cách Oclit được lấy bình phương của các bit đầu vào mà là độc lập với nhau trong m mã con, để thu được các khoảng cách Oclit được lấy bình phương tối thiểu của các bit đầu vào mà độc lập với nhau trong m mã con, trong đó các khoảng cách Oclit được lấy bình phương tối thiểu của các bit đầu vào mà độc lập với nhau trong m mã con được gọi chung là các khoảng cách Oclit được lấy bình phương tối thiểu độc lập; thu được, theo m khoảng cách Oclit được lấy bình phương tối thiểu độc lập, khoảng cách Oclit được lấy bình phương tối thiểu của các bit đầu vào mà được ghép với nhau trong m mã con, trong đó khoảng cách Oclit được lấy bình phương tối thiểu của các bit đầu vào mà được ghép với nhau trong m mã con được gọi là khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp; và thu được các bit đầu vào mà nằm trong m mã con và thỏa mãn các khoảng cách Oclit được lấy bình phương tối thiểu độc lập và khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp, và thu được kết quả giải mã của chuỗi mã theo các quan hệ giữa m mã con và chuỗi mã.

200



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực mã hóa-giải mã, và cụ thể, đề cập đến phương pháp giải mã cho mã cực (Polar code).

Tình trạng kỹ thuật của sáng chế

Trong hệ thống truyền thông, mã hóa kênh thường được sử dụng để cải thiện độ tin cậy của việc truyền dữ liệu và đảm bảo chất lượng truyền thông. Mã cực đã được chứng minh là mã hiệu quả mà có thể đạt được dung lượng Shannon và có độ phức tạp mã hóa và giải mã thấp. Mã cực là mã khối tuyến tính. Ma trận sinh của nó là G_N , và xử lý mã hóa của nó là $x_1^N = u_1^N G_N$, trong đó $G_N = B_N F^{\otimes n}$, và độ dài mã $N = 2n$, trong đó $n \geq 0$. u_1^N là các bit đầu vào, bao gồm các bit thông tin và các bit đóng băng. Ở đây, $F = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, và B_N là ma trận chuyển vị, ví dụ, ma trận hoán vị bit. $F^{\otimes n}$ là lũy thừa Kronecker của F và được xác định là $F^{\otimes n} = F \otimes F^{\otimes(n-1)}$. Mã cực có thể được biểu diễn bằng cách sử dụng mã tập hợp (N, K, A, u_{A^c}) , và xử lý mã hóa của nó là $x_1^N = u_A G_N(A) \oplus u_{A^c} G_N(A^c)$, trong đó A là tập các chỉ số của các bit thông tin, $G_N(A)$ là ma trận con của G_N và thu được bằng cách sử dụng các hàng mà tương ứng với các chỉ số trong tập A , và $G_N(A^c)$ là ma trận con của G_N và thu được bằng cách sử dụng các hàng mà tương ứng với các chỉ số trong tập A^c . u_{A^c} là các bit đóng băng, trong đó số lượng bit đóng băng là $(N - K)$ và số lượng bit đóng băng là các bit đã biết. Nhằm đơn giản, các bit đóng băng này có thể được thiết lập là 0.

Mã cực cũng có thể được giải mã bằng cách giải mã ML (hợp lý tối đa), và

bộ giải mã hợp lý tối đa để giải mã ML tìm được chuỗi bit thông tin, để tối thiểu hóa khoảng cách Oclit được lấy bình phương:

$$E_{\min} = \min_{u_k} \|y_1^N - z_1^N(u_1, u_2, \dots, u_N)\|^2$$

trong đó z_k là ký tự thu được sau khi ánh xạ BPSK, trong đó $z_k = (1 - 2x_k), k = 1, \dots, N$.

Độ phức tạp của giải mã ML là $O(2^K)$.

Có thể thấy rằng, theo kỹ thuật đã biết, việc giải mã ML đối với mã cực có độ phức tạp quá cao.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là đề xuất phương pháp giải mã và thiết bị giải mã cho mã cực, để làm giảm độ phức tạp giải mã.

Theo một khía cạnh, sáng chế đề xuất thiết bị giải mã cho mã cực, bao gồm:

môđun chia, có cấu trúc để thu mã cực cần được giải mã có độ dài N, và chia mã cực cần được giải mã thành m mã con của mã cực mà được ghép với nhau, trong đó mỗi mã con của mã cực có độ dài N/m, N và m là các lũy thừa nguyên của 2, và $N > m$;

m môđun xử lý độc lập, có cấu trúc tách biệt để tính toán, đối với m mã con của mã cực, các khoảng cách Oclit được lấy bình phương của các bit đầu vào mà là độc lập với nhau trong m mã con của mã cực, để thu được các khoảng cách Oclit được lấy bình phương tối thiểu của các bit đầu vào mà là độc lập với nhau trong m mã con của mã cực, trong đó các khoảng cách Oclit được lấy bình

phương tối thiểu của các bit đầu vào mà là độc lập với nhau trong m mã con của mã cực được gọi là các khoảng cách Oclit được lấy bình phương tối thiểu độc lập;

môđun xử lý kết hợp, có cấu trúc để thu được, theo m khoảng cách Oclit được lấy bình phương tối thiểu độc lập, khoảng cách Oclit được lấy bình phương tối thiểu của các bit đầu vào mà được ghép với nhau trong m mã con của mã cực, trong đó khoảng cách Oclit được lấy bình phương tối thiểu của các bit đầu vào mà được ghép với nhau trong các mã con của mã cực được gọi là khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp; và

môđun xuất kết quả, có cấu trúc để thu được các bit đầu vào mà nằm trong m mã con của mã cực và thỏa mãn các khoảng cách Oclit được lấy bình phương tối thiểu độc lập và khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp, và thu được kết quả giải mã của mã cực cần được giải mã dựa vào các quan hệ giữa m mã con của mã cực và mã cực cần được giải mã.

Theo khía cạnh khác, sáng chế đề xuất phương pháp giải mã được thực hiện bởi thiết bị nêu trên.

Theo các phương án của sáng chế, mã cực cần được giải mã được chia, và xử lý hợp lý tối đa kết hợp được thực hiện, mà làm giảm độ phức tạp giải mã và độ trễ giải mã của mã cực, và cải thiện tốc độ thông lượng của bộ giải mã ML đối với mã cực.

Mô tả vắn tắt các hình vẽ

FIG.1 là sơ đồ giản lược của hệ thống truyền thông không dây 100 trong môi trường ứng dụng theo cách thức thực hiện của sáng chế;

FIG.2 là sơ đồ giản lược của hệ thống 200 theo cách thức thực hiện của sáng chế;

FIG.3 là sơ đồ giản lược của thiết bị giải mã cho mã cực 300 theo cách thức thực hiện cụ thể;

FIG.4 là sơ đồ giản lược của phương pháp giải mã cho mã cực theo cách thức thực hiện cụ thể;

FIG.5 là sơ đồ giản lược của việc giải mã song song hai tầng trong cách thức thực hiện được thể hiện trên FIG.4;

FIG.6 là sơ đồ giản lược của phương pháp giải mã cho mã cực trong cách thức thực hiện cụ thể khác;

FIG.7 là sơ đồ giản lược của việc giải mã song song ba tầng trong cách thức thực hiện được thể hiện trên FIG.6;

FIG.8 là sơ đồ giản lược của phương pháp giải mã theo cách thức thực hiện cụ thể; và

FIG.9 là sơ đồ giản lược của thiết bị giải mã theo cách thức thực hiện cụ thể.

Mô tả chi tiết sáng chế

Phần sau đây mô tả rõ ràng và toàn bộ các giải pháp kỹ thuật trong các phương án của sáng chế có viện dẫn tới các hình vẽ kèm theo trong các phương án của sáng chế. Rõ ràng, các phương án được mô tả là một vài phương án của sáng chế mà không phải tất cả các phương án của sáng chế. Tất cả các phương án khác được thực hiện bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật

dựa trên các phương án của sáng chế mà không cần cố gắng sáng tạo sẽ nằm trong phạm vi bảo hộ của sáng chế.

Sau đây, các phương án được mô tả có viện dẫn tới các hình vẽ kèm theo, trong đó các ký hiệu chỉ dẫn giống nhau trên hình vẽ sẽ chỉ báo cùng bộ phận ở đây. Nhằm dễ dàng minh họa, phần mô tả sau đây sẽ đề xuất nhiều chi tiết, để cho một hoặc nhiều phương án được hiểu rõ ràng. Tuy nhiên, rõ ràng rằng, các phương án cũng có thể được thực hiện mà không có các chi tiết này. Trong ví dụ khác, cấu trúc và thiết bị đã biết được thể hiện dưới dạng các sơ đồ khối, để mô tả một hoặc nhiều phương án.

Các thuật ngữ như "bộ phận", "môđun", và "hệ thống" trong bản mô tả này được sử dụng để biểu diễn thực thể, phần cứng, vi chương trình, kết hợp của phần cứng và phần mềm, phần mềm, hoặc phần mềm thực hiện liên quan đến máy tính. Ví dụ, bộ phận này có thể là, nhưng không bị giới hạn ở, xử lý chạy trên bộ xử lý, bộ xử lý, đối tượng, tệp có thể chạy được, tập lệnh thực thi, và chương trình và/hoặc máy tính. Bằng cách minh họa, cả ứng dụng chạy trên thiết bị tính toán và thiết bị tính toán có thể là các bộ phận. Một hoặc nhiều bộ phận có thể nằm trong xử lý và/hoặc tập lệnh thực thi, và các bộ phận có thể nằm trên một máy tính và/hoặc được phân phối giữa hai máy tính hoặc nhiều hơn. Ngoài ra, các bộ phận này có thể được thực hiện từ các phương tiện lưu trữ đọc được bởi máy tính khác nhau có các cấu trúc dữ liệu được lưu trữ trên đó. Các bộ phận này có thể thực hiện việc truyền thông bằng xử lý cục bộ và/hoặc từ xa và theo, ví dụ, tín hiệu có một hoặc nhiều gói dữ liệu (ví dụ, dữ liệu từ hai bộ phận tương tác với bộ phận khác trong hệ thống cục bộ, hệ thống phân phối, và/hoặc

truyền trong mạng như Internet mà tương tác với hệ thống khác bằng tín hiệu).

Ngoài ra, thiết bị đầu cuối truy nhập trong mỗi phương án cũng có thể được gọi là hệ thống, bộ phận người dùng, trạm người dùng, trạm vô tuyến di động, trạm di động, trạm từ xa, thiết bị đầu cuối từ xa, thiết bị di động, thiết bị đầu cuối người dùng, thiết bị đầu cuối, thiết bị truyền thông không dây, trạm người dùng, thiết bị người dùng, hoặc UE (User Equipment - Thiết bị người dùng). Thiết bị đầu cuối truy nhập có thể là điện thoại di động tế bào, điện thoại không dây, điện thoại SIP (Session Initiation Protocol - Giao thức khởi tạo phiên), trạm WLL (Wireless Local Loop - Vòng lặp cục bộ không dây), PDA (Personal Digital Assistant - thiết bị số hỗ trợ cá nhân), thiết bị cầm tay có chức năng truyền thông không dây, thiết bị tính toán, hoặc thiết bị xử lý khác được kết nối tới modem không dây. Ngoài ra, mỗi phương án được mô tả có viện dẫn tới trạm gốc. Trạm gốc có thể có cấu trúc để truyền thông với thiết bị di động. Trạm gốc có thể là BTS (Base Transceiver Station - Trạm thu phát gốc) trong GSM (Global System of Mobile communication - Hệ thống truyền thông di động toàn cầu) hoặc CDMA (Code Division Multiple Access - Đa truy nhập phân chia theo mã), hoặc có thể là NB (NodeB - nút B) trong WCDMA (Wideband Code Division Multiple Access - Đa truy nhập phân chia theo mã băng rộng), hoặc có thể còn là eNB hoặc eNodeB (Evolutional Node B - Nút B cải tiến) trong LTE (Long Term Evolution - Phát triển dài hạn), trạm chuyển tiếp hoặc điểm truy nhập, hoặc thiết bị trạm gốc trong mạng 5G tương lai.

Ngoài ra, tất cả khía cạnh hoặc các đặc điểm của sáng chế có thể được áp dụng như là phương pháp, thiết bị, hoặc sản phẩm mà sử dụng kỹ thuật mã hóa

và/hoặc thiết kế tiêu chuẩn. Thuật ngữ "sản phẩm" trong bản mô tả này bao hàm các chương trình máy tính mà có thể được truy nhập từ thiết bị, vật mang, phương tiện lưu trữ đọc được bởi máy tính bất kỳ. Ví dụ, phương tiện lưu trữ đọc được bằng máy tính có thể bao gồm, nhưng không bị giới hạn ở, bộ nhớ từ (như đĩa cứng, đĩa mềm, hoặc băng từ), đĩa quang (như CD (Compact Disk - Đĩa nén), hoặc DVD (Digital Versatile Disk - Đĩa đa năng số)), thẻ thông minh, và bộ nhớ chớp (như EPROM (Erasable Programmable Read-Only Memory - Bộ nhớ chỉ đọc khả tình có thể xóa), hoặc thẻ, thẻ nhớ, hoặc đầu đọc đĩa). Ngoài ra, các phương tiện lưu trữ khác nhau được mô tả ở đây có thể bao gồm một hoặc nhiều thiết bị để lưu trữ thông tin và/hoặc phương tiện lưu trữ đọc được bởi máy tính khác. Thuật ngữ "phương tiện lưu trữ đọc được bởi máy tính" có thể bao gồm, nhưng không bị giới hạn ở, kênh vô tuyến và các phương tiện lưu trữ khác có khả năng lưu trữ, chứa, và/hoặc mang các lệnh và/hoặc dữ liệu.

Sau đây, phần mô tả được viện dẫn tới FIG.1, mà là sơ đồ giản lược của hệ thống truyền thông không dây 100 theo cách thức thực hiện của sáng chế. Hệ thống 100 bao gồm trạm gốc 102, trong đó trạm gốc 102 có thể bao gồm nhiều nhóm anten. Ví dụ, một nhóm anten có thể bao gồm các anten 104 và anten 106, và nhóm anten khác có thể bao gồm các anten 108 và anten 110, và nhóm bổ sung có thể bao gồm các anten 112 và anten 114. Hai anten được thể hiện trong mỗi nhóm anten. Tuy nhiên, đối với mỗi nhóm, nhiều anten hơn hoặc ít anten hơn có thể được sử dụng. Trạm gốc 102 có thể bao gồm thêm chuỗi bộ truyền và chuỗi bộ thu. Có thể được hiểu bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật rằng cả chuỗi bộ truyền và chuỗi bộ thu có thể bao gồm nhiều bộ phận

(như bộ xử lý, bộ điều chế, bộ ghép kênh, modem, bộ giải ghép kênh, hoặc anten) liên quan đến việc gửi và thu tín hiệu.

Trạm gốc 102 có thể truyền thông với một hoặc nhiều thiết bị đầu cuối truy nhập (ví dụ, thiết bị đầu cuối truy nhập 116 và thiết bị đầu cuối truy nhập 122). Tuy nhiên, có thể được hiểu rằng, trạm gốc 102 có thể truyền thông với hầu hết các thiết bị đầu cuối truy nhập tương tự các thiết bị đầu cuối truy nhập 116 và thiết bị đầu cuối truy nhập 122. Các thiết bị đầu cuối truy nhập 116 và thiết bị đầu cuối truy nhập 122 có thể là, ví dụ, điện thoại di động tế bào, điện thoại thông minh, máy tính di động, thiết bị truyền thông cầm tay, thiết bị tính toán cầm tay, thiết bị vô tuyến vệ tinh, hệ thống định vị toàn cầu, PDA, và/hoặc bất kỳ thiết bị thích hợp khác được sử dụng cho việc truyền thông trên hệ thống truyền thông không dây 100. Như được thể hiện trên hình vẽ, thiết bị đầu cuối truy nhập 116 truyền thông với các anten 112 và anten 114, trong đó các anten 112 và anten 114 gửi thông tin tới thiết bị đầu cuối truy nhập 116 thông qua đường kết nối xuôi 118 và thu thông tin từ thiết bị đầu cuối truy nhập 116 thông qua đường kết nối ngược 120. Ngoài ra, thiết bị đầu cuối truy nhập 122 truyền thông với các anten 104 và anten 106, trong đó các anten 104 và anten 106 gửi thông tin tới thiết bị đầu cuối truy nhập 122 thông qua đường kết nối xuôi 124 và thu thông tin từ thiết bị đầu cuối truy nhập 122 thông qua đường kết nối ngược 126. Trong hệ thống FDD (Frequency Division Duplex - Song công phân chia theo tần số), ví dụ, đường kết nối xuôi 118 có thể sử dụng băng tần số mà khác với băng tần số mà được sử dụng bởi đường kết nối ngược 120, và đường kết nối xuôi 124 có thể sử dụng băng tần số khác với băng tần số mà được sử

dụng bởi đường kết nối ngược 126. Ngoài ra, trong hệ thống TDD (Time Division Duplex - Song công phân chia theo thời gian), đường kết nối xuôi 118 và đường kết nối ngược 120 có thể sử dụng băng tần số chung, và đường kết nối xuôi 124 và đường kết nối ngược 126 có thể sử dụng băng tần số chung.

Mỗi nhóm anten và/hoặc mỗi vùng được thiết kế cho việc truyền thông được gọi là phân vùng của trạm gốc 102. Ví dụ, nhóm anten có thể được thiết kế để truyền thông với thiết bị đầu cuối truy nhập trong phân vùng của vùng phủ sóng của trạm gốc 102. Trong việc truyền thông bằng các đường kết nối xuôi 118 và đường kết nối xuôi 124, anten truyền của trạm gốc 102 có thể cải thiện, bằng cách tạo chùm tín hiệu, các tỷ lệ tín hiệu trên tạp âm của các đường kết nối xuôi 118 và đường kết nối xuôi 124 mà tương ứng với các thiết bị đầu cuối truy nhập 116 và thiết bị đầu cuối truy nhập 122. Ngoài ra, so với trường hợp trong đó trạm gốc gửi thông tin tới tất cả thiết bị đầu cuối truy nhập của trạm gốc bằng cách sử dụng một anten, khi trạm gốc 102 gửi, bằng cách tạo chùm tín hiệu, thông tin tới các thiết bị đầu cuối truy nhập 116 và thiết bị đầu cuối truy nhập 122 mà được phân phối ngẫu nhiên trong vùng phủ sóng liên quan, thiết bị di động trong tế bào lân cận ít bị nhiễu hơn.

Trong thời gian đã định, trạm gốc 102, thiết bị đầu cuối truy nhập 116, và/hoặc thiết bị đầu cuối truy nhập 122 có thể là thiết bị gửi kiểu truyền thông không dây, và/hoặc thiết bị thu kiểu truyền thông không dây. Khi gửi dữ liệu, thiết bị gửi kiểu truyền thông không dây có thể mã hóa dữ liệu và truyền dữ liệu được mã hóa. Cụ thể, thiết bị gửi kiểu truyền thông không dây có thể có (ví dụ, tạo ra, thu nhận, và lưu trữ trong bộ nhớ) lượng bit thông tin cụ thể mà cần được

gửi tới thiết bị thu kiểu truyền thông không dây thông qua kênh. Các bit thông tin này có thể được chứa trong khối truyền (hoặc nhiều khối truyền) của dữ liệu, trong đó nhiều khối truyền có thể được tạo ra bằng cách phân đoạn. Ngoài ra, thiết bị gửi kiểu truyền thông không dây có thể mã hóa mỗi khối truyền bằng cách sử dụng bộ mã hóa mã cực (mà không được thể hiện). Một cách tương ứng, khi thu dữ liệu, thiết bị thu kiểu truyền thông không dây có thể thực hiện giải mã cho mã cực trên dữ liệu, để cải thiện độ tin cậy của truyền thông dữ liệu.

FIG.2 thể hiện hệ thống 200 mà thực hiện phương pháp giải mã cho mã cực trong môi trường truyền thông không dây. Hệ thống 200 bao gồm thiết bị truyền thông không dây 202. Được thể hiện rằng thiết bị truyền thông không dây 202 thu dữ liệu thông qua kênh thu. Mặc dù được thể hiện rằng thiết bị truyền thông không dây 202 thu dữ liệu, nhưng thiết bị truyền thông không dây 202 cũng có thể gửi dữ liệu thông qua kênh (ví dụ, thiết bị truyền thông không dây 202 có thể gửi và thu dữ liệu tại cùng thời điểm, thiết bị truyền thông không dây 202 có thể gửi và thu dữ liệu tại các thời điểm khác nhau, hoặc thiết bị truyền thông không dây 202 gửi và thu dữ liệu tại cùng thời điểm và thiết bị truyền thông không dây 202 gửi và thu dữ liệu tại các thời điểm khác nhau được kết hợp). Thiết bị truyền thông không dây 202 có thể là, ví dụ, trạm gốc (như trạm gốc 102 trên FIG.1), hoặc thiết bị đầu cuối truy nhập (như thiết bị đầu cuối truy nhập 116 trên FIG.1 hoặc thiết bị đầu cuối truy nhập 122 trên FIG.1).

Thiết bị truyền thông không dây 202 có thể bao gồm bộ giải mã cho mã cực 204 và bộ thu 206. Bộ giải mã cho mã cực 204 có cấu trúc để chia, theo đặc điểm cấu trúc của mã cực mà được thu bởi bộ thu 206 và có độ dài N, mã cực

thành m mã con của mã cực mà được ghép với nhau, trong đó mỗi mã con của mã cực có độ dài N/m , N và m là các lũy thừa nguyên của 2, và $N > m$; đầu tiên, thực hiện tối thiểu hóa tỷ lệ hợp lý tối đa trên các bit đầu vào mà là độc lập với nhau trong m mã con của mã cực (tức là, đối với m mã con của mã cực, tính toán các khoảng cách Oclit được lấy bình phương của các bit đầu vào mà là độc lập với nhau, để thu được các khoảng cách Oclit được lấy bình phương tối thiểu của các bit đầu vào mà là độc lập với nhau trong m mã con của mã cực), và sau đó thực hiện tối thiểu hóa tỷ lệ hợp lý tối đa theo cách được kết hợp, để thu được kết quả của việc giải mã hợp lý tối đa đối với mã cực mà độ dài gốc của nó là N .

Viện dẫn tới FIG.3, mà là sơ đồ giản lược của thiết bị giải mã cho mã cực 300 theo cách thức thực hiện của sáng chế, thiết bị giải mã cho mã cực bao gồm:

môđun chia 302, có cấu trúc để thu mã cực cần được giải mã có độ dài N , và chia mã cực cần được giải mã thành m mã con của mã cực mà được ghép với nhau, trong đó mỗi mã con của mã cực có độ dài N/m , N và m là các lũy thừa nguyên của 2, và $N > m$;

m môđun xử lý độc lập 304, có cấu trúc tách biệt để tính toán, đối với m mã con của mã cực, các khoảng cách Oclit được lấy bình phương của các bit đầu vào mà là độc lập với nhau trong m mã con của mã cực, để thu được các khoảng cách Oclit được lấy bình phương tối thiểu của các bit đầu vào mà là độc lập với nhau trong m mã con của mã cực, trong đó các khoảng cách Oclit được lấy bình phương tối thiểu của các bit đầu vào mà là độc lập với nhau trong m mã con của mã cực được gọi là các khoảng cách Oclit được lấy bình phương tối thiểu độc lập;

môđun xử lý kết hợp 306, có cấu trúc để thu được, theo m khoảng cách Oclit được lấy bình phương tối thiểu độc lập, khoảng cách Oclit được lấy bình phương tối thiểu của các bit đầu vào mà được ghép với nhau trong m mã con của mã cực, trong đó khoảng cách Oclit được lấy bình phương tối thiểu của các bit đầu vào mà được ghép với nhau trong m mã con của mã cực được gọi là khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp; và

môđun xuất kết quả 308, có cấu trúc để thu được các bit đầu vào nằm trong m mã con của mã cực và thỏa mãn các khoảng cách Oclit được lấy bình phương tối thiểu độc lập và khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp, và thu được kết quả giải mã của mã cực cần được giải mã dựa vào các quan hệ giữa m mã con của mã cực và mã cực cần được giải mã.

Theo ví dụ ưu tiên của sáng chế, các môđun xử lý độc lập thực hiện xử lý theo cách song song. m có thể là 2, 4, 8, hoặc tương tự. Trong các cách thức thực hiện sau đây, các ví dụ trong đó m bằng 2 và 4 được sử dụng, nhưng không bị giới hạn như vậy trong các cách thức thực hiện khác, mã cực được chia thành số lượng môđun khác theo giải pháp của sáng chế. Rõ ràng, trong cách thức thực hiện nêu trên, độ phức tạp giải mã của mã cực có thể được làm giảm bằng xử lý chia và kết hợp.

Viện dẫn tới FIG.4, mà là cách thức thực hiện của phương pháp giải mã khác theo sáng chế, ví dụ được sử dụng, trong đó m trong cách thức thực hiện của FIG.3 bằng 2 và cách thức giải mã song song được sử dụng. Theo cách thức thực hiện cụ thể này, xử lý giải mã về cơ bản được hoàn thành trong hai tầng. Thiết bị giải mã được gọi là bộ giải mã song song hai tầng 400 (hoặc ngắn gọn

là Bộ giải mã tìm kiếm hai tầng).

Theo cách thức thực hiện nêu trên được thể hiện trên FIG.4, nói chung, giải mã ML đối với mã cực có thể được hoàn thành trong hai tầng, làm giảm đáng kể độ phức tạp của việc giải mã ML đối với mã cực. Mã giả của bộ giải mã song song hai tầng (Bộ giải mã ML tìm kiếm hai tầng) nêu trên được biểu diễn ngắn gọn như sau:

Bộ giải mã ML tìm kiếm hai tầng

For (any realization of $a_k = b_k, k \in \Omega_{01}^{(1)}$)

{

Exhaustive search

$$\text{Exhaustive search } E_b(b_k, k \in \Omega_{01}^{(1)}) = \min_{b_k, k \in \Omega_{01}^{(1)}} D_{N/2+1}^N$$

$$\text{Combine } E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)}) = E_a(a_k, k \in \Omega_{01}^{(1)}) + E_b(b_k, k \in \Omega_{01}^{(1)})$$

}

$$\text{Exhaustive search } \min_{a_k = b_k, k \in \Omega_{01}^{(1)}} E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)})$$

Đầu tiên, nhằm dễ dàng cho việc mô tả, trong các xử lý và các hình vẽ kèm theo của các cách thức thực hiện, mã cực cần được giải mã được biểu diễn bằng

$$x_1^N = v_1^N \times \begin{bmatrix} F^{\otimes(n-1)} & 0 \\ F^{\otimes(n-1)} & F^{\otimes(n-1)} \end{bmatrix}$$

cách sử dụng công thức $= \left[\left(v_1^{N/2} \oplus v_{N/2+1}^N \right) F^{\otimes(n-1)} \quad v_{N/2+1}^N F^{\otimes(n-1)} \right]$; tập chỉ số $\Omega_{01}^{(1)}$ biểu

diễn rằng v_k là bit đóng băng và $v_{k+N/2}$ là bit thông tin; và tập chỉ số $\Omega_{11}^{(1)}$ biểu

diễn rằng v_k là bit thông tin và $v_{k+N/2}$ là bit thông tin. Nói cách khác, nếu

$k \in \Omega_{01}^{(1)}$, a_k và b_k được ghép với nhau, mà được biểu diễn bằng cách sử dụng

công thức $a_k = b_k$; và nếu $k \in \Omega_{11}^{(1)}$, a_k, b_k là độc lập với nhau. Lưu ý rằng, đối

với mã cực, không có tập chỉ số $\Omega_{10}^{(1)}$, tức là, v_k là bit thông tin và $v_{k+N/2}$ là bit

đóng bằng. Trong một vài ví dụ, $\Omega_{11}^{(1)}$ nêu trên có thể được chia thành ba tập con: $\Omega_{11}^{(1)} = \{\Omega_{01}^{(2)} + N/4\} \cup \Omega_{11}^{(2)} \cup \{\Omega_{11}^{(2)} + N/4\}$, trong đó tập chỉ số $\Omega_{01}^{(2)}$ biểu diễn tất cả các chỉ số thỏa mãn $k \notin \Omega_{11}^{(1)}$ và $k + N/4 \in \Omega_{11}^{(1)}$, trong đó $1 \leq k \leq N/4$, và tập chỉ số $\Omega_{11}^{(2)}$ biểu diễn tất cả các chỉ số thỏa mãn $k \in \Omega_{11}^{(1)}$ và $k + N/4 \in \Omega_{11}^{(1)}$, trong đó $1 \leq k \leq N/4$. Tương tự, không có chỉ số thỏa mãn các điều kiện sau đây: $k \in \Omega_{11}^{(1)}$ và $k + N/4 \notin \Omega_{11}^{(1)}$, trong đó $1 \leq k \leq N/4$.

Viện dẫn tới nguyên tắc hoạt động của việc giải mã hợp lý tối đa, dựa vào FIG.4, xử lý hoạt động của cách thức thực hiện giải mã được thể hiện trên FIG.4 bao gồm:

S401: Thu mã cực cần được giải mã có độ dài N, trong đó mã cực cần được giải mã được biểu diễn bằng cách sử dụng công thức $x_1^N = v_1^N \times \begin{bmatrix} F^{\otimes(n-1)} & 0 \\ F^{\otimes(n-1)} & F^{\otimes(n-1)} \end{bmatrix} = \left[\left(v_1^{N/2} \oplus v_{N/2+1}^N \right) F^{\otimes(n-1)} \quad v_{N/2+1}^N F^{\otimes(n-1)} \right]$, và chia mã cực cần được giải mã thành hai mã con của mã cực: mã con thứ nhất của mã cực và mã con thứ hai của mã cực, trong đó các bit đầu vào tương ứng với hai mã con của mã cực là a_k và b_k một cách tương ứng, và được biểu diễn riêng biệt bằng cách sử dụng các công thức $a_1^{N/2} = v_1^{N/2} \oplus v_{N/2+1}^N$ và $b_1^{N/2} = v_{N/2+1}^N$.

S402: Đối với bit đầu vào $a_k, k \in \Omega_{11}^{(1)}$ mà nằm trong mã con thứ nhất của mã cực và độc lập với bit đầu vào bất kỳ trong mã con thứ hai của mã cực, thực hiện việc tính toán để thu được khoảng cách Oclit được lấy bình phương tối

thiểu độc lập thứ nhất $E_a(a_k, k \in \Omega_{11}^{(1)}) = \min_{a_k, k \in \Omega_{11}^{(1)}} D_1^{N/2}$; và đối với bit đầu vào $b_k, k \in \Omega_{11}^{(1)}$ mà nằm trong mã con thứ hai của mã cực và độc lập với bit đầu vào

bất kỳ trong mã con thứ nhất của mã cực, thực hiện việc tính toán để thu được khoảng cách Oclit được lấy bình phương tối thiểu độc lập thứ hai

$$E_b(b_k, k \in \Omega_{01}^{(1)}) = \min_{b_k, k \in \Omega_{11}^{(1)}} D_{N/2+1}^N$$

S403: Kết hợp khoảng cách Oclit được lấy bình phương tối thiểu độc lập thứ nhất và khoảng cách Oclit được lấy bình phương tối thiểu độc lập thứ hai E_a, E_b , để thu được E_{sum} mà được biểu diễn bằng cách sử dụng công thức $E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)}) = E_a(a_k, k \in \Omega_{01}^{(1)}) + E_b(b_k, k \in \Omega_{01}^{(1)})$.

S404: Thực hiện việc tìm kiếm để thu được khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp thứ nhất mà được biểu diễn bằng cách sử dụng công thức $\min_{a_k=b_k, k \in \Omega_{01}^{(1)}} E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)})$, tức là, $\min_{a_k=b_k, k \in \Omega_{01}} E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)})$.

S405: Thu được các bit đầu vào $a_k = b_k, k \in \Omega_{01}^{(1)}$ mà được ghép với nhau trong mã con thứ nhất của mã cực và mã con thứ hai của mã cực và thỏa mãn khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp thứ nhất; và thu được các bit đầu vào $a_k, b_k, k \in \Omega_{11}^{(1)}$ mà là độc lập với nhau trong mã con thứ nhất của mã cực và mã con thứ hai của mã cực và thỏa mãn khoảng cách Oclit được lấy bình phương tối thiểu độc lập thứ nhất E_a và khoảng cách Oclit được lấy bình phương tối thiểu độc lập thứ hai E_b (tức là, thực hiện việc tìm kiếm để thu được các bit đầu vào $a_k, b_k, k \in \Omega_{11}^{(1)}$ mà tối thiểu hóa E_a hoặc E_b).

S406: Sau khi tất cả a_k, b_k thu được thông qua việc tính toán, thực hiện việc tính toán theo các quan hệ $b_1^{N/2} = v_{N/2+1}^N$ và $a_1^{N/2} = v_1^{N/2} \oplus v_{N/2+1}^N$ giữa hai mã con của mã cực và mã cực cần được giải mã, để thu được các bit đầu vào $v_1^{N/2}$ và $v_{N/2+1}^N$ của mã cực cần được giải mã.

Phần mô tả sẽ được viện dẫn tới FIG.5, mà là sơ đồ giản lược của việc giải mã song song hai tầng trong cách thức thực hiện nêu trên. Có thể thấy được từ sơ đồ này rằng, bằng việc giải mã song song, độ phức tạp được làm giảm đáng kể.

Phần mô tả sẽ được viện dẫn tới FIG.6, mà là cách thức thực hiện cụ thể khác theo sáng chế. Cách thức thực hiện cụ thể này được phát triển tiếp dựa trên giải pháp giải mã song song nêu trên, để thực hiện cách thức giải mã trong đó m trong cách thức thực hiện được thể hiện trên FIG.3 bằng 4. Cách thức giải mã này được gọi ngắn gọn là giải mã ML song song ba tầng. Viện dẫn tới nguyên tắc hoạt động của giải mã hợp lý tối đa, viện dẫn tới FIG.6, xử lý hoạt động của cách thức thực hiện nêu trên bao gồm:

S601: Thu mã cực cần được giải mã có độ dài N, và chia mã cực cần được giải mã thành bốn mã con của mã cực mà được ghép với nhau, trong đó mỗi mã con của mã cực có độ dài N/4, N và m là các lũy thừa nguyên của 2, và $N > 4$.

Cụ thể, mã cực cần được giải mã được biểu diễn bằng cách sử dụng công thức $x_1^N = v_1^N \times \begin{bmatrix} F^{\otimes(n-1)} & 0 \\ F^{\otimes(n-1)} & F^{\otimes(n-1)} \end{bmatrix}$, và bốn mã con của mã cực được gọi là mã con thứ ba của mã cực, mã con thứ tư của mã cực, mã con thứ năm của mã cực, và mã con thứ sáu của mã cực. Phương pháp chia cụ thể có thể là như sau: đầu tiên, mã cực cần được giải mã được chia, bằng cách sử dụng phương pháp trong S401 trên FIG.4, thành hai mã con của mã cực, tức là, mã con thứ nhất của mã cực và mã con thứ hai của mã cực, trong đó các bit đầu vào tương ứng với hai mã con của mã cực là a_k và b_k lần lượt, và được biểu diễn riêng biệt bằng

cách sử dụng các công thức $a_1^{N/2} = v_1^{N/2} \oplus v_{N/2+1}^N$ và $b_1^{N/2} = v_{N/2+1}^N$; và sau đó, mã con thứ nhất của mã cực được chia thành mã con thứ ba của mã cực và mã con thứ tư của mã cực, và mã con thứ hai của mã cực được chia thành mã con thứ năm của mã cực và mã con thứ sáu của mã cực.

Các bit đầu vào của mã con thứ ba nêu trên của mã cực, mã con thứ tư của mã cực, mã con thứ năm của mã cực, và mã con thứ sáu của mã cực là c_k mà được biểu diễn bằng cách sử dụng công thức $c_k = a_k \oplus a_{k+N/4}$, d_k mà được biểu diễn bằng cách sử dụng công thức $d_k = a_{k+N/4}$, e_k mà được biểu diễn bằng cách sử dụng công thức $e_k = b_k \oplus b_{k+N/4}$, và f_k một cách lần lượt, trong đó $f_k = b_{k+N/4}$, $1 \leq k \leq N/4$, $a_1^{N/2} = v_1^{N/2} \oplus v_{N/2+1}^N$, và $b_1^{N/2} = v_{N/2+1}^N$.

Nguyên tắc cụ thể của giải pháp chia nêu trên là như sau:

$x_1^{N/2} = a_1^{N/2} F^{\otimes(n-1)}$ có thể còn được chia thành:

$$x_1^{N/2} = \begin{bmatrix} c_1^{N/4} F^{\otimes(n-2)} & d_1^{N/4} F^{\otimes(n-2)} \end{bmatrix}$$

Tương tự, có thể thu được rằng:

$$x_1^N = \begin{bmatrix} c_1^{N/4} F^{\otimes(n-2)} & d_1^{N/4} F^{\otimes(n-2)} & e_1^{N/4} F^{\otimes(n-2)} & f_1^{N/4} F^{\otimes(n-2)} \end{bmatrix}; \text{ và theo cấu}$$

trúc của mã cực được thể hiện trong công thức nêu trên, rõ ràng rằng, phương pháp chia nêu trên có thể được thực hiện một cách hiệu quả.

S602: Đối với các bit đầu vào mà là độc lập với nhau trong bốn mã con nêu trên của mã cực, tính toán riêng biệt các khoảng cách Ôclit được lấy bình phương tối thiểu độc lập, để thu được khoảng cách Ôclit được lấy bình phương

tối thiểu độc lập thứ nhất $E_c = \min_{c_k, k \in \Omega_{11}^{(2)}} D_1^{N/4}$, khoảng cách Ôclit được lấy bình

phương tối thiểu độc lập thứ hai $E_d = \min_{d_k, k \in \Omega_{11}^{(2)}} D_{N/4+1}^{N/2}$, khoảng cách Ôclit được lấy

bình phương tối thiểu độc lập thứ ba $E_e = \min_{e_k, k \in \Omega_{11}^{(2)}} D_{N/2+1}^{3N/4}$, và khoảng cách Öclit

được lấy bình phương tối thiểu độc lập thứ tư $E_f = \min_{f_k, k \in \Omega_{11}^{(2)}} D_{3N/4+1}^N$, trong đó tập chỉ số $\Omega_{11}^{(2)}$ biểu diễn tất cả các chỉ số thỏa mãn $k \in \Omega_{11}^{(1)}$ và $k + N/4 \in \Omega_{11}^{(1)}$, và tập chỉ số $\Omega_{11}^{(1)}$ biểu diễn rằng v_k là bit thông tin và $v_{k+N/2}$ là bit thông tin, trong đó $1 \leq k \leq N/4$.

S603: Thực hiện việc tính toán để thu được tổng khoảng cách Öclit được lấy bình phương của mã con thứ ba của mã cực và mã con thứ tư của mã cực, trong đó tổng này được biểu diễn bằng cách sử dụng công thức $E_{sum1} = E_e + E_d$, và đối với các bit đầu vào mà được ghép với nhau trong mã con thứ ba của mã cực và mã con thứ tư của mã cực, thực hiện việc tìm kiếm để thu được khoảng cách Öclit được lấy bình phương tối thiểu được kết hợp thứ nhất mà được biểu diễn bằng cách sử dụng công thức $E_{sum2} = \min_{a_k, k \in \Omega_{01}^{(2)}} E_{sum1}$, trong đó $\Omega_{01}^{(2)}$ biểu diễn tất cả các chỉ số thỏa mãn $k \notin \Omega_{11}^{(1)}$ và $k + N/4 \in \Omega_{11}^{(1)}$, trong đó $1 \leq k \leq N/4$.

S604: Thực hiện việc tính toán để thu được tổng khoảng cách Öclit được lấy bình phương của mã con thứ năm của mã cực và mã con thứ sáu của mã cực, trong đó tổng này được biểu diễn bằng cách sử dụng công thức $E_{sum3} = E_e + E_f$, và đối với các bit đầu vào mà được ghép với nhau trong mã con thứ năm của mã cực và mã con thứ sáu của mã cực, thực hiện việc tìm kiếm để thu được khoảng cách Öclit được lấy bình phương tối thiểu được kết hợp thứ hai mà được biểu diễn bằng cách sử dụng công thức $E_{sum4} = \min_{b_k, k \in \Omega_{01}^{(2)}} E_{sum3}$, trong đó $\Omega_{01}^{(2)}$ biểu diễn tất cả các chỉ số thỏa mãn $k \notin \Omega_{11}^{(1)}$ và $k + N/4 \in \Omega_{11}^{(1)}$, trong đó $1 \leq k \leq N/4$.

S605: Đối với các bit đầu vào mà được ghép với nhau trong tất cả các mã

con của mã cực, tính toán tổng khoảng cách Oclit được lấy bình phương mà được biểu diễn bằng cách sử dụng công thức $E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)}) = E_{sum2} + E_{sum4}$, và thực hiện việc tìm kiếm để thu được khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp thứ ba $\min_{a_k=b_k, k \in \Omega_{01}^{(1)}} E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)})$, trong đó tập chỉ số $\Omega_{01}^{(1)}$ biểu diễn rằng v_k là bit đóng băng, và $v_{k+N/2}$ là bit thông tin.

S606: Thu được các bit đầu vào $a_k = b_k, k \in \Omega_{01}^{(1)}$ thỏa mãn khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp thứ ba $\min_{a_k=b_k, k \in \Omega_{01}^{(1)}} E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)})$, và thay thế một cách riêng biệt các bit đầu vào $a_k = b_k, k \in \Omega_{01}^{(1)}$ vào khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp thứ nhất E_{sum2} và khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp thứ hai E_{sum4} thu được các bit đầu vào khác.

S607: Sau khi tất cả các bit đầu vào c_k, d_k, e_k , và f_k thu được, thu được các bit đầu vào v_1^N của mã cực cần được giải mã theo các quan hệ

$$\begin{cases} v_k = c_k \oplus d_k \oplus e_k \oplus f_k \\ v_{k+N/4} = d_k \oplus f_k \\ v_{k+N/2} = e_k \oplus f_k \\ v_{k+3N/4} = f_k \end{cases}$$

giữa bốn mã con của mã cực và mã cực cần được giải mã.

Theo cách thức thực hiện nêu trên được thể hiện trên FIG.6, nói chung, việc giải mã ML đối với mã cực có thể được hoàn thành trong ba tầng, làm giảm đáng kể độ phức tạp của việc giải mã ML đối với mã cực. Mã của bộ giải mã song song ba tầng nêu trên (Bộ giải mã ML tìm kiếm ba tầng) được biểu diễn ngắn gọn như sau:

Bộ giải mã ML tìm kiếm ba tầng

For (any realization of $a_k = b_k, k \in \Omega_{01}^{(1)}$)

{

For (any realization of $a_k, k \in \Omega_{01}^{(2)} + N/4$)

{

Calculate $c_k = a_k \oplus a_{k+N/4}$, and $d_k = a_{k+N/4}$,

where $1 \leq k \leq N/4$, $k \notin \Omega_{11}^{(2)}$

Search $E_c = \min_{c_k, k \in \Omega_{11}^{(2)}} D_1^{N/4}$

Search $E_d = \min_{d_k, k \in \Omega_{11}^{(2)}} D_{N/4+1}^{N/2}$

Combine $E_{sum1} = E_c + E_d$

}

Search $E_{sum2} = \min_{a_k, k \in \Omega_{01}^{(2)}} E_{sum1}$

For (any realization of $b_k, k \in \Omega_{01}^{(2)} + N/4$)

{

Calculate $e_k = b_k \oplus b_{k+N/4}$, and $f_k = b_{k+N/4}$,

where $1 \leq k \leq N/4$, $k \notin \Omega_{11}^{(2)}$

Search $E_e = \min_{e_k, k \in \Omega_{11}^{(2)}} D_{N/2+1}^{3N/4}$

Search $E_f = \min_{f_k, k \in \Omega_{11}^{(2)}} D_{3N/4+1}^N$

Hiệu quả kỹ thuật của cách thức thực hiện này được mô tả chi tiết dưới đây, trong đó độ phức tạp của việc giải mã hợp lý tối đa song song ba tầng là $2^{|\Omega_{01}^{(1)}| + |\Omega_{11}^{(1)}| + |\Omega_{11}^{(2)}|}$. Việc dẫn tới bảng 1 dưới đây, mà là sự so sánh giữa độ phức tạp của việc giải mã hợp lý tối đa song song ba tầng và độ phức tạp của việc giải mã hợp lý tối đa gốc trong các trường hợp của độ dài mã N khác nhau, trong đó Comp 1 là độ phức tạp của việc giải mã ML song song ba tầng và Comp 2 là độ phức tạp

của việc giải mã ML gốc.

N	$ \Omega_{01}^{(1)} $	$ \Omega_{11}^{(1)} $	$ \Omega_{11}^{(2)} $	Comp 1	Comp 2
32	4	2	2	2^8	2^{16}
64	4	4	5	2^{13}	2^{32}
128	8	6	11	2^{25}	2^{64}
256	16	10	23	2^{49}	2^{128}

Bảng 1

Phân mô tả sẽ được viện dẫn tới FIG.7, mà là sơ đồ giản lược của việc giải mã song song ba tầng nêu trên. Có thể được thấy từ FIG.7 rằng, độ phức tạp của việc giải mã hợp lý tối đa trong cách thức thực hiện này của sáng chế có thể được làm giảm đáng kể.

Trong các cách thức thực hiện nêu trên, m bằng 2 hoặc 4. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể biết rằng m cũng có thể bằng 8, hoặc lũy thừa nguyên của 2 khác. Trong các cách thức thực hiện nêu trên, bằng cách làm giảm độ phức tạp giải mã, và đặc biệt, bằng cách sử dụng cách thức giải mã song song, thông lượng giải mã có thể được cải thiện đáng kể và độ trễ giải mã có thể được làm giảm.

Phương pháp giải mã ML được mô tả trong mỗi cách thức thực hiện của sáng chế có thể được sử dụng kết hợp với phương pháp giải mã bất kỳ mà không xung đột logic với phương pháp giải mã ML, mà không bị giới hạn trong các cách thức thực hiện của sáng chế.

Theo ví dụ của sáng chế, cách thức thực hiện cụ thể khác của sáng chế đề xuất phương pháp giải mã. Theo phương pháp này, đầu tiên, việc giải mã SC được thực hiện độc lập (tốt hơn là, theo cách song song) trên m mã con của mã

cực, và sau đó, xử lý kết hợp của việc giải mã ML hợp lý tối đa được thực hiện trên các mã con của mã cực, tức là, việc giải mã của mã cực hoàn thiện được thực hiện bằng cách kết hợp việc giải mã song song SC và phương pháp giải mã ML song song nêu trên (ví dụ, phương pháp giải mã ML song song hai tầng hoặc phương pháp giải mã ML song song ba tầng).

Thiết bị giải mã cho mã cực được thể hiện trên FIG.3 được sử dụng như là ví dụ. Một cách tùy chọn, thiết bị này còn bao gồm môđun giải mã độc lập SC, có cấu trúc để chia mã cực có độ dài S thành N mã con của mã cực, trong đó mỗi mã con có độ dài S/N, và thực hiện riêng biệt việc giải mã SC để thu được N kết quả giải mã SC (ví dụ, các tỷ lệ hợp lý), trong đó S và N là các lũy thừa nguyên của 2 và $S > N$,

sao cho môđun chia, m môđun xử lý độc lập, môđun xử lý kết hợp, và môđun xuất kết quả theo bất kỳ trong số cách thức thực hiện nêu trên hoàn thành hoạt động tương ứng bằng cách sử dụng tất cả các bit đầu vào trong N kết quả giải mã SC như là mã cực cần được giải mã có độ dài N;

và

thu được, theo tất cả các bit đầu vào, kết quả giải mã của mã cực có độ dài S.

Theo ví dụ cụ thể khác, theo đơn xin cấp bằng sáng chế Trung Quốc số 201310073607.8, cách thức thực hiện trong đó việc giải mã SC có thể được thực hiện song song trên tám mã con của mã cực được đề xuất (viện dẫn tới FIG.4 trong đơn xin cấp bằng sáng chế Trung Quốc số 201310073607.8). So với cách thức thực hiện trong đơn xin cấp bằng sáng chế Trung Quốc số 201310073607.8,

trong ví dụ này, sau khi giải mã song song SC, không còn cần thiết phải dịch chuyển $(a_i, b_i, c_i, d_i, e_i, f_i, g_i, h_i)$ để ra quyết định. Thay vì đó, nguyên tắc ML được sử dụng để thực hiện việc giải mã kết hợp. Việc dẫn tới FIG.8, xử lý của nó bao gồm:

Đầu tiên, mã cực có độ dài S được chia thành tám mã cực có độ dài S/8, tức là, tám vector tín hiệu thu $y_1^{S/8}$, $y_{S/8+1}^{2S/8}$, $y_{2S/8+1}^{3S/8}$, ..., và $y_{7S/8+1}^S$. Các bit đầu vào tương ứng thỏa mãn:

$$\begin{cases} a_i = v_i \oplus v_{i+S/8} \oplus v_{i+2S/8} \oplus v_{i+3S/8} \oplus v_{i+4S/8} \oplus v_{i+5S/8} \oplus v_{i+6S/8} \oplus v_{i+7S/8} \\ b_i = v_{i+S/8} \oplus v_{i+3S/8} \oplus v_{i+5S/8} \oplus v_{i+7S/8} \\ c_i = v_{i+2S/8} \oplus v_{i+3S/8} \oplus v_{i+6S/8} \oplus v_{i+7S/8} \\ d_i = v_{i+3S/8} \oplus v_{i+7S/8} \\ e_i = v_{i+4S/8} \oplus v_{i+5S/8} \oplus v_{i+6S/8} \oplus v_{i+7S/8} \\ f_i = v_{i+5S/8} \oplus v_{i+7S/8} \\ g_i = v_{i+6S/8} \oplus v_{i+7S/8} \\ h_i = v_{i+7S/8} \end{cases} \quad 1 \leq i \leq S/8$$

Tám bộ giải mã thành phần (các bộ giải mã SC có độ dài S/8) sử dụng riêng biệt $y_1^{S/8}$, $y_{S/8+1}^{2S/8}$, $y_{2S/8+1}^{3S/8}$, ..., và $y_{7S/8+1}^S$ như là các đầu vào. Tám bộ giải mã thành phần tính toán một cách độc lập các tỷ lệ hợp lý logarit một cách riêng biệt: $L(a_i) = L_{S/8}^{(i)}(y_1^{S/8}, \hat{a}_1^{i-1})$, $L(b_i) = L_{S/8}^{(i)}(y_{S/8+1}^{2S/8}, \hat{b}_1^{i-1})$, $L(c_i) = L_{S/8}^{(i)}(y_{2S/8+1}^{3S/8}, \hat{c}_1^{i-1})$, ..., và $L(h_i) = L_{S/8}^{(i)}(y_{7S/8+1}^S, \hat{h}_1^{i-1})$.

Thứ hai, theo các tỷ lệ hợp lý logarit nêu trên thu được bằng cách tính toán, việc giải mã song song ML được thực hiện trên các bit đầu vào $(v_k, v_{k+S/8}, v_{k+2S/8}, \dots, v_{k+7S/8})$, mà được biểu diễn cụ thể bằng cách sử dụng công thức sau đây:

$$\begin{bmatrix} a_k \\ b_k \\ c_k \\ d_k \\ e_k \\ f_k \\ g_k \\ h_k \end{bmatrix} = \begin{bmatrix} v_k \\ v_{k+S/8} \\ v_{k+2S/8} \\ v_{k+3S/8} \\ v_{k+4S/8} \\ v_{k+5S/8} \\ v_{k+6S/8} \\ v_{k+7S/8} \end{bmatrix}^T \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Ma trận trên về phải của công thức nêu trên là ma trận sinh của mã cực có độ dài $N = 8$. Do đó, trong xử lý giải mã nêu trên, phương pháp giải mã song song ML đối với mã cực theo cách thức thực hiện nêu trên có thể được sử dụng.

$$\text{Cụ thể, } Y = \begin{bmatrix} L(a_i) = L_{S/8}^{(i)}(y_1^{S/8}, \hat{a}_1^{i-1}) & , & L(b_i) = L_{S/8}^{(i)}(y_{S/8+1}^{2S/8}, \hat{b}_1^{i-1}) \\ L(c_i) = L_{S/4}^{(i)}(y_{2S/8+1}^{3S/8}, \hat{c}_1^{i-1}) & , \dots, & L(h_i) = L_{S/8}^{(i)}(y_{7S/8+1}^S, \hat{h}_1^{i-1}) \end{bmatrix},$$

các bit đầu vào là $(v_k, v_{k+S/8}, v_{k+2S/8}, \dots, v_{k+7S/8})$, và

sau khi $\hat{v}_i, \hat{v}_{i+S/8}, \hat{v}_{i+2S/8}, \dots, \hat{v}_{i+7S/8}$ ($i = 1, 2, \dots, S/8$) thu được, kết quả giải mã u_i^N của mã cực gốc có thể thu được bằng cách thay thế vị trí.

Theo cách thức thực hiện nêu trên, mã cực có độ dài S được chia thành tám mã cực có độ dài $S/8$, việc giải mã SC được thực hiện riêng biệt trên tám mã cực, và sau đó, cách thức giải mã kết hợp ML như giải mã ML song song hai tầng hoặc giải mã ML song song ba tầng được đề xuất trong các cách thức thực hiện của sáng chế được sử dụng, nhờ đó làm giảm hơn nữa độ phức tạp giải mã và cải thiện thông lượng giải mã.

Có thể được hiểu rằng, các phương án được mô tả trong bản mô tả này có thể được thực hiện bằng cách sử dụng phần cứng, phần mềm, vi chương trình,

phần mềm trung gian, vi mã, hoặc kết hợp của chúng. Để áp dụng sáng chế bằng cách sử dụng phần cứng, bộ xử lý có thể được bố trí trong một hoặc nhiều ASIC (Application Specific Integrated Circuits - Mạch tích hợp riêng cho ứng dụng), DSP (Digital Signal Processing - Bộ xử lý tín hiệu số), DSPD (DSP Device - Thiết bị xử lý tín hiệu số), PLD (Programmable Logic Device - Thiết bị logic khả trình), FPGA (Field-Programmable Gate Array - Mảng cổng khả trình dạng trường), các bộ xử lý, các bộ điều khiển, các bộ vi điều khiển, các bộ vi xử lý, hoặc các bộ phận điện tử khác có cấu trúc để thực hiện các chức năng của bản mô tả này, hoặc kết hợp của chúng.

Khi các phương án được thực hiện trong phần mềm, vi chương trình, phần mềm trung gian hoặc vi mã, mã chương trình hoặc các đoạn mã, chúng có thể được lưu trữ trong phương tiện lưu trữ đọc được bởi máy tính như bộ phận lưu trữ. Đoạn mã có thể biểu diễn thủ tục, chức năng, chương trình con, chương trình, đoạn chương trình, đoạn chương trình con, môđun, nhóm phần mềm, lớp, hoặc kết hợp bất kỳ của các lệnh, các cấu trúc dữ liệu, hoặc các câu lệnh chương trình. Đoạn mã có thể được ghép với đoạn mã khác hoặc mạch phần cứng bằng cách truyền và/hoặc thu thông tin, dữ liệu, các đối số, các tham số, hoặc nội dung bộ nhớ. Thông tin, các đối số, các tham số, dữ liệu, và loại tương tự có thể được truyền, chuyển tiếp, hoặc được truyền sử dụng cách thức thích hợp bất kỳ bao gồm chia sẻ bộ nhớ, truyền bản tin, truyền thẻ, truyền qua mạng, và loại tương tự.

Để áp dụng sáng chế bằng cách sử dụng phần mềm, kỹ thuật được mô tả trong bản mô tả này có thể được thực hiện bằng cách sử dụng các môđun (ví dụ,

các thủ tục và các chức năng) mà thực hiện các chức năng được mô tả trong bản mô tả này. Mã phần mềm có thể được lưu trữ trong bộ nhớ và được thực hiện bởi bộ xử lý. Bộ nhớ có thể được bố trí trong bộ xử lý hoặc phía ngoài bộ xử lý. Trong trường hợp bộ nhớ được bố trí phía ngoài bộ xử lý, bộ nhớ có thể được ghép nối với bộ xử lý bằng các cách thức đã biết.

Viện dẫn tới FIG.9, mà thể hiện hệ thống 900 mà có thể sử dụng phương pháp xử lý mã cực trong môi trường truyền thông không dây. Ví dụ, hệ thống 900 có thể ít nhất một phần nằm trong trạm gốc hoặc thiết bị đầu cuối truy nhập. Sẽ được hiểu rằng, hệ thống 900 có thể được biểu diễn là bao gồm các khối chức năng, mà có thể là các khối chức năng mà các chức năng của nó được thực hiện bởi bộ xử lý, phần mềm, hoặc kết hợp của nó (ví dụ, vi chương trình). Hệ thống 900 bao gồm nhóm logic 902 có các thành phần điện tử mà được hoạt động theo cách thức kết hợp.

Ví dụ, nhóm logic 902 có thể bao gồm: môđun chia 904, có cấu trúc để thu mã cực cần được giải mã có độ dài N , và chia mã cực cần được giải mã thành m mã con của mã cực mà được ghép với nhau, trong đó mỗi mã con của mã cực có độ dài N/m , N và m là các lũy thừa nguyên của 2, và $N > m$;

m môđun xử lý độc lập 906, không được thể hiện tất cả trên hình vẽ, có cấu trúc tách biệt để tính toán, đối với m mã con của mã cực, các khoảng cách Óclit được lấy bình phương của các bit đầu vào mà là độc lập với nhau trong m mã con của mã cực, để thu được các khoảng cách Óclit được lấy bình phương tối thiểu của các bit đầu vào mà là độc lập với nhau trong m mã con của mã cực, trong đó các khoảng cách Óclit được lấy bình phương tối thiểu của các

bit đầu vào mà là độc lập với nhau trong m mã con của mã cực được gọi là các khoảng cách Oclit được lấy bình phương tối thiểu độc lập;

môđun xử lý kết hợp 908, có cấu trúc để thu được, theo m khoảng cách Oclit được lấy bình phương tối thiểu độc lập, khoảng cách Oclit được lấy bình phương tối thiểu của các bit đầu vào mà được ghép với nhau trong m mã con của mã cực, trong đó khoảng cách Oclit được lấy bình phương tối thiểu của các bit đầu vào mà được ghép với nhau trong m mã con của mã cực được gọi là khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp; và

môđun xuất kết quả 910, có cấu trúc để thu được các bit đầu vào nằm trong m mã con của mã cực và thỏa mãn các khoảng cách Oclit được lấy bình phương tối thiểu độc lập và khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp, và thu được kết quả giải mã của mã cực cần được giải mã dựa vào các quan hệ giữa m mã con của mã cực và mã cực cần được giải mã.

Ngoài ra, hệ thống 900 có thể bao gồm bộ nhớ 912, trong đó bộ nhớ 912 lưu trữ các chỉ dẫn được sử dụng để thực hiện các chức năng liên quan đến các thành phần điện tử 904, 906, 908, và 910. Mặc dù được thể hiện rằng các thành phần điện tử 904, 906, 908, và 910 được bố trí nằm ngoài bộ nhớ 912, có thể được hiểu rằng, một hoặc nhiều thành phần điện tử 904, 906, 908, và 910 có thể được bố trí trong bộ nhớ 912. Một cách tương ứng, các cách thức thực hiện của phương pháp nêu trên có thể còn được ưu tiên sử dụng trên các bộ phận nêu trên. Các chi tiết của nó không được mô tả lại ở đây lần nữa

Phần mô tả nêu trên bao gồm các ví dụ của một hoặc nhiều phương án. Rõ ràng là, không thể mô tả, cho việc mô tả các phương án này, tất cả kết hợp khả

thi của các bộ phận hoặc các phương pháp. Tuy nhiên, người có hiểu biết trung bình trong lĩnh vực kỹ thuật sẽ nhận ra rằng các phương án này có thể còn được kết hợp và được thay đổi. Do đó, các phương án được mô tả trong bản mô tả này nhằm mục đích bao gồm tất cả các thay đổi, cải biến, và các sửa đổi nằm trong phạm vi bảo hộ của bộ yêu cầu bảo hộ kèm theo. Ngoài ra, đối với thuật ngữ "bao gồm", "có", hoặc loại tương tự được sử dụng trong phần mô tả hoặc yêu cầu bảo hộ, thuật ngữ này nhằm mục đích được hiểu theo ý nghĩa là bao gồm theo cách tương tự như thuật ngữ "gồm có" khi được sử dụng trong yêu cầu bảo hộ.

Người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể nhận ra rằng, kết hợp với các ví dụ được mô tả trong các phương án được bộc lộ trong bản mô tả này, các bộ phận và các bước thuật toán có thể được thực hiện bởi phần cứng điện tử hoặc kết hợp của phần mềm máy tính và phần cứng điện tử. Các chức năng này được thực hiện bởi phần cứng hay phần mềm phụ thuộc vào các ứng dụng cụ thể và các điều kiện ràng buộc thiết kế của các giải pháp kỹ thuật. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể sử dụng các phương pháp khác nhau để thực hiện các chức năng được mô tả đối với mỗi ứng dụng cụ thể, nhưng sẽ không được xem rằng việc thực hiện này vượt quá phạm vi của sáng chế.

Có thể được hiểu rõ ràng bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật rằng, nhằm mục đích mô tả thuận tiện và vắn tắt, đối với xử lý chi tiết của hệ thống, thiết bị, và bộ phận nêu trên, việc tham chiếu có thể được thực hiện tới xử lý tương ứng trong các phương án về phương pháp nêu trên, và các chi tiết không được mô tả lại lần nữa.

Trong một vài phương án được đề xuất bởi sáng chế, sẽ được hiểu rằng hệ thống, thiết bị, và phương pháp được bộc lộ có thể được thực hiện theo các cách khác. Ví dụ, phương án về thiết bị được mô tả chỉ là ví dụ. Ví dụ, việc phân chia bộ phận chỉ là việc phân chia chức năng logic và có thể là việc phân chia khác theo phương án thực tế. Ví dụ, các bộ phận hoặc các thành phần có thể được kết hợp hoặc được tích hợp vào hệ thống khác, hoặc một vài đặc điểm có thể được bỏ qua hoặc không được thực hiện. Ngoài ra, các ghép nối liên quan được mô tả hoặc thể hiện hoặc các ghép nối trực tiếp hoặc các kết nối truyền thông có thể được thực hiện bằng cách sử dụng một vài giao diện. Các ghép nối không trực tiếp hoặc các kết nối truyền thông giữa các thiết bị hoặc các bộ phận có thể được thực hiện dưới dạng điện tử, cơ học, hoặc các dạng khác.

Các bộ phận được mô tả như là các thành phần riêng biệt có thể hoặc không phải là được tách biệt về mặt vật lý, và các phần được thể hiện như là các bộ phận có thể hoặc không phải là các bộ phận vật lý, có thể nằm trong một vị trí, hoặc có thể được phân phối trên các bộ phận mạng. Một vài hoặc tất cả bộ phận có thể được lựa chọn theo nhu cầu thực tế để đạt được mục đích của các giải pháp của các phương án.

Ngoài ra, các bộ phận chức năng trong các phương án của sáng chế có thể được tích hợp vào một bộ xử lý, hoặc mỗi bộ phận có thể tồn tại riêng lẻ về mặt vật lý, hoặc hai bộ phận hoặc nhiều hơn được tích hợp vào một bộ phận.

Khi các chức năng được thực hiện dưới dạng đơn vị chức năng phần mềm và được bán hoặc được sử dụng như là sản phẩm độc lập, các chức năng có thể được lưu trữ trong phương tiện lưu trữ đọc được bởi máy tính. Dựa trên cách

hiểu này, các giải pháp kỹ thuật của sáng chế về cơ bản, hoặc một phần theo kỹ thuật đã biết, hoặc một vài giải pháp kỹ thuật có thể được thực hiện dưới dạng sản phẩm phần mềm. Sản phẩm phần mềm máy tính được lưu trữ trong phương tiện lưu trữ và bao gồm các chỉ lệnh để chỉ dẫn thiết bị máy tính (mà có thể là máy tính cá nhân, máy chủ, hoặc thiết bị mạng) thực hiện tất cả hoặc một vài bước của các phương pháp được mô tả trong các phương án của sáng chế. Phương tiện lưu trữ nêu trên bao gồm: bất kỳ phương tiện mà có thể lưu trữ mã chương trình, như ổ chớp USB, đĩa cứng tháo rời, bộ nhớ chỉ đọc (ROM-Read Only Memory), bộ nhớ truy nhập ngẫu nhiên (RAM-Random Access Memory), đĩa mềm, hoặc đĩa quang.

Phần mô tả nêu trên chỉ là các cách thức thực hiện cụ thể của sáng chế, nhưng không nhằm mục đích giới hạn phạm vi bảo hộ của sáng chế. Bất kỳ thay đổi hoặc thay thế được thực hiện bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật nằm trong phạm vi kỹ thuật được bộc lộ trong sáng chế sẽ nằm trong phạm vi bảo hộ của sáng chế. Do đó, phạm vi bảo hộ của sáng chế sẽ được đưa vào phạm vi bảo hộ của yêu cầu bảo hộ.

YÊU CẦU BẢO HỘ

1. Thiết bị thu trong hệ thống truyền thông không dây, bao gồm:

bộ xử lý; và

phương tiện lưu trữ đọc được bởi máy tính loại không tạm thời mà lưu trữ mã chương trình để thực thi bởi bộ xử lý, trong đó các mã chương trình bao gồm các lệnh để:

thu chuỗi mã có độ dài N bit đầu vào, trong đó chuỗi mã này thu được bằng cách mã hóa một lượng bit thông tin trong bộ mã hóa ở thiết bị truyền trong hệ thống truyền thông không dây;

chia chuỗi mã thành m mã con mà được ghép với nhau, trong đó mỗi mã con có độ dài N/m , và trong đó mỗi trong số N và m là các lũy thừa nguyên của 2, và $N > m$;

tính toán một cách riêng biệt, đối với m mã con, các khoảng cách Ôclit được lấy bình phương của các bit đầu vào mà là độc lập với nhau trong m mã con, để thu được các khoảng cách Ôclit được lấy bình phương tối thiểu của các bit đầu vào mà là độc lập với nhau trong m mã con, trong đó các khoảng cách Ôclit được lấy bình phương tối thiểu của các bit đầu vào mà là độc lập với nhau trong m mã con được gọi chung là các khoảng cách Ôclit được lấy bình phương tối thiểu độc lập;

thu được, theo m khoảng cách Ôclit được lấy bình phương tối thiểu độc lập, khoảng cách Ôclit được lấy bình phương tối thiểu của các bit đầu vào mà được ghép với nhau trong m mã con, trong đó khoảng cách Ôclit được lấy bình

phương tối thiểu của các bit đầu vào mà được ghép với nhau trong các mã con được gọi là khoảng cách Óclit được lấy bình phương tối thiểu được kết hợp; và

thu được các bit đầu vào mà nằm trong m mã con và thỏa mãn các khoảng cách Óclit được lấy bình phương tối thiểu độc lập và khoảng cách Óclit được lấy bình phương tối thiểu được kết hợp, và thu được kết quả giải mã của chuỗi mã theo các quan hệ giữa m mã con và chuỗi mã.

2. Thiết bị thu theo điểm 1, trong đó việc tính toán một cách riêng biệt các khoảng cách Óclit được lấy bình phương tối thiểu độc lập bao gồm:

tính toán các khoảng cách Óclit được lấy bình phương tối thiểu độc lập theo cách song song.

3. Thiết bị thu theo điểm 1 hoặc 2, trong đó m bằng 2, 4 hoặc 8.

4. Thiết bị thu theo điểm 3, trong đó m bằng 2,

trong đó chuỗi mã được biểu diễn bằng công thức:

$$\begin{aligned} x_1^N &= v_1^N \times \begin{bmatrix} F^{\otimes(n-1)} & 0 \\ F^{\otimes(n-1)} & F^{\otimes(n-1)} \end{bmatrix} \\ &= \left[\left(v_1^{N/2} \oplus v_{N/2+1}^N \right) F^{\otimes(n-1)} \quad v_{N/2+1}^N F^{\otimes(n-1)} \right], \end{aligned}$$

trong đó việc chia chuỗi mã thành m mã con bao gồm:

chia chuỗi mã thành mã con thứ nhất và mã con thứ hai, trong đó các bit đầu vào tương ứng với hai mã con lần lượt là a_k và b_k , và được biểu diễn bằng các công thức $a_1^{N/2} = v_1^{N/2} \oplus v_{N/2+1}^N$ và $b_1^{N/2} = v_{N/2+1}^N$;

trong đó việc tính toán một cách riêng biệt các khoảng cách Óclit được lấy bình phương tối thiểu độc lập bao gồm:

đối với các bit đầu vào $a_k, k \in \Omega_{11}^{(1)}$ mà nằm trong mã con thứ nhất và độ

lập với bit đầu vào bất kỳ trong mã con thứ hai, thực hiện việc tính toán để thu được khoảng cách Oclit được lấy bình phương tối thiểu độc lập thứ nhất

$$E_a(a_k, k \in \Omega_{01}^{(1)}) = \min_{a_k, k \in \Omega_{11}^{(1)}} D_1^{N/2}; \text{ và}$$

đối với các bit đầu vào $b_k, k \in \Omega_{11}^{(1)}$ mà nằm trong mã con thứ hai và độc lập với bit đầu vào bất kỳ trong mã con thứ nhất, thực hiện việc tính toán để thu được khoảng cách Oclit được lấy bình phương tối thiểu độc lập thứ hai

$$E_b(b_k, k \in \Omega_{01}^{(1)}) = \min_{b_k, k \in \Omega_{11}^{(1)}} D_{N/2+1}^N;$$

trong đó việc thu được khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp bao gồm:

kết hợp khoảng cách Oclit được lấy bình phương tối thiểu độc lập thứ nhất và khoảng cách Oclit được lấy bình phương tối thiểu độc lập thứ hai E_a, E_b , để thu được E_{sum} mà được biểu diễn bằng công thức $E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)}) = E_a(a_k, k \in \Omega_{01}^{(1)}) + E_b(b_k, k \in \Omega_{01}^{(1)});$ và

thực hiện việc tìm kiếm để thu được khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp mà được biểu diễn bằng công thức

$$\min_{a_k = b_k, k \in \Omega_{01}^{(1)}} E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)}); \text{ và}$$

trong đó việc thu được các bit đầu vào mà nằm trong các mã con thứ nhất và thứ hai và thỏa mãn khoảng cách Oclit được lấy bình phương tối thiểu độc lập và khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp, và thu được kết quả giải mã của chuỗi mã bao gồm:

thu được các bit đầu vào $a_k = b_k, k \in \Omega_{01}^{(1)}$ mà được ghép với nhau trong mã con thứ nhất và mã con thứ hai và thỏa mãn khoảng cách Oclit được lấy bình

phương tối thiểu được kết hợp thứ nhất;

thu được các bit đầu vào $a_k, b_k, k \in \Omega_{11}^{(1)}$ mà là độc lập với nhau trong mã con thứ nhất và mã con thứ hai và thỏa mãn khoảng cách Oclit được lấy bình phương tối thiểu độc lập thứ nhất E_a và khoảng cách Oclit được lấy bình phương tối thiểu độc lập thứ hai E_b ; và

thu được các kết quả giải mã $v_1^{N/2}$ và $v_{N/2+1}^N$ của chuỗi mã bằng cách sử dụng các quan hệ $b_1^{N/2} = v_{N/2+1}^N$ và $a_1^{N/2} = v_1^{N/2} \oplus v_{N/2+1}^N$ giữa hai mã con và chuỗi mã;

trong đó trong các công thức nêu trên,

N là độ dài của chuỗi mã, v_1^N là các bit đầu vào, bit 1 đến bit N , trong chuỗi mã này, bao gồm các bit thông tin và các bit đóng băng;

$\begin{bmatrix} F^{\otimes(n-1)} & 0 \\ F^{\otimes(n-1)} & F^{\otimes(n-1)} \end{bmatrix}$ là ma trận sinh cho chuỗi mã,

và trong đó $v_1^{N/2}$ là các bit đầu vào của mã con thứ nhất, mà là bit 1 đến bit $N/2$ trong chuỗi mã, $v_{N/2+1}^N$ là các bit đầu vào của mã con thứ hai, mà là bit $N/2+1$ đến bit N trong chuỗi mã;

tập chỉ số $\Omega_{01}^{(1)}$ biểu diễn rằng v_k là bit đóng băng và $v_{k+N/2}$ là bit thông tin; và tập chỉ số $\Omega_{11}^{(1)}$ biểu diễn rằng v_k là bit thông tin và $v_{k+N/2}$ là bit thông tin.

5. Thiết bị thu theo điểm 3, trong đó m bằng 4,

trong đó việc thu và chia chuỗi mã thành m mã con bao gồm:

thu chuỗi mã, và chia chuỗi mã thành bốn mã con mà được ghép với nhau, trong đó mỗi mã con có độ dài $N/4$, N là lũy thừa nguyên của 2, và chuỗi mã

được biểu diễn bằng công thức

$$x_1^N = v_1^N \times \begin{bmatrix} F^{\otimes(n-1)} & 0 \\ F^{\otimes(n-1)} & F^{\otimes(n-1)} \end{bmatrix} = \left[\left(v_1^{N/2} \oplus v_{N/2+1}^N \right) F^{\otimes(n-1)} \quad v_{N/2+1}^N F^{\otimes(n-1)} \right],$$

và trong đó bốn mã con là mã con thứ ba, mã con thứ tư, mã con thứ năm, và mã con thứ sáu, và các bit đầu vào của mã con thứ ba, mã con thứ tư, mã con thứ năm, và mã con thứ sáu lần lượt là: c_k , d_k , e_k , và f_k ;

trong đó việc tính toán riêng biệt các khoảng cách Oclit được lấy bình phương tối thiểu độc lập bao gồm:

tính toán riêng biệt các khoảng cách Oclit được lấy bình phương tối thiểu độc lập đối với các bit đầu vào mà là độc lập với nhau trong mã con thứ ba, mã con thứ tư, mã con thứ năm, và mã con thứ sáu, để thu được khoảng cách Oclit

được lấy bình phương tối thiểu độc lập thứ nhất $E_c = \min_{c_k, k \in \Omega_{11}^{(2)}} D_1^{N/4}$, khoảng cách

Oclit được lấy bình phương tối thiểu độc lập thứ hai $E_d = \min_{d_k, k \in \Omega_{11}^{(2)}} D_{N/4+1}^{N/2}$, khoảng

cách Oclit được lấy bình phương tối thiểu độc lập thứ ba $E_e = \min_{e_k, k \in \Omega_{11}^{(2)}} D_{N/2+1}^{3N/4}$, và

khoảng cách Oclit được lấy bình phương tối thiểu độc lập thứ tư

$E_f = \min_{f_k, k \in \Omega_{11}^{(2)}} D_{3N/4+1}^N$, trong đó tập chỉ số $\Omega_{11}^{(2)}$ biểu diễn tất cả các chỉ số thỏa mãn

$k \in \Omega_{11}^{(1)}$ và $k + N/4 \in \Omega_{11}^{(1)}$, và tập chỉ số $\Omega_{11}^{(1)}$ biểu diễn rằng v_k là bit thông tin

và $v_{k+N/2}$ là bit thông tin, trong đó $1 \leq k \leq N/4$;

trong đó việc thu được khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp bao gồm:

thực hiện việc tính toán để thu được tổng các khoảng cách Oclit được lấy bình phương của mã con thứ ba và mã con thứ tư, trong đó tổng này được biểu

diễn bằng công thức $E_{sum1} = E_c + E_d$, và

đối với các bit đầu vào mà được ghép với nhau trong mã con thứ ba và mã con thứ tư, thực hiện việc tìm kiếm để thu được khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp thứ nhất mà được biểu diễn bằng công thức $E_{sum2} = \min_{a_k, k \in \Omega_{01}^{(2)}} E_{sum1}$, trong đó $\Omega_{01}^{(2)}$ biểu diễn tất cả các chỉ số thỏa mãn $k \notin \Omega_{11}^{(1)}$ và $k + N/4 \in \Omega_{11}^{(1)}$, trong đó $1 \leq k \leq N/4$;

thực hiện việc tính toán để thu được tổng các khoảng cách Oclit được lấy bình phương của mã con thứ năm và mã con thứ sáu, trong đó tổng này được biểu diễn bằng công thức $E_{sum3} = E_e + E_f$, và

đối với các bit đầu vào mà được ghép với nhau trong mã con thứ năm và mã con thứ sáu, thực hiện việc tìm kiếm để thu được khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp thứ hai mà được biểu diễn bằng công thức $E_{sum4} = \min_{b_k, k \in \Omega_{01}^{(2)}} E_{sum3}$, trong đó $\Omega_{01}^{(2)}$ biểu diễn tất cả các chỉ số thỏa mãn $k \notin \Omega_{11}^{(1)}$ và $k + N/4 \in \Omega_{11}^{(1)}$, trong đó $1 \leq k \leq N/4$;

đối với các bit đầu vào mà được ghép với nhau trong các mã con từ thứ ba đến thứ sáu, tính toán tổng khoảng cách Oclit được lấy bình phương mà được biểu diễn bằng công thức $E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)}) = E_{sum2} + E_{sum4}$, và thực hiện việc tìm kiếm để thu được khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp thứ ba $\min_{a_k = b_k, k \in \Omega_{01}^{(1)}} E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)})$, trong đó tập chỉ số $\Omega_{01}^{(1)}$ biểu diễn rằng v_k là bit đóng băng và $v_{k+N/2}$ là bit thông tin; và trong đó việc thu được kết quả giải mã của chuỗi mã bao gồm:

thu được các bit đầu vào $a_k = b_k, k \in \Omega_{01}^{(1)}$ thỏa mãn khoảng cách Oclit được

lấy bình phương tối thiểu được kết hợp thứ ba $\min_{a_k=b_k, k \in \Omega_{01}^{(1)}} E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)})$;

thay thế một cách riêng biệt các bit đầu vào $a_k = b_k, k \in \Omega_{01}^{(1)}$ vào khoảng cách Öclit được lấy bình phương tối thiểu được kết hợp thứ nhất E_{sum2} và khoảng cách Öclit được lấy bình phương tối thiểu được kết hợp thứ hai E_{sum4} để thu được các bit đầu vào khác; và

sau khi tất cả các bit đầu vào c_k, d_k, e_k , và f_k thu được, thu được các bit đầu vào v_1^N của chuỗi mã theo các quan hệ

$$\begin{cases} v_k = c_k \oplus d_k \oplus e_k \oplus f_k \\ v_{k+N/4} = d_k \oplus f_k \\ v_{k+N/2} = e_k \oplus f_k \\ v_{k+3N/4} = f_k \end{cases} \quad \text{giữa các mã con từ thứ ba đến thứ sáu và chuỗi mã;}$$

trong đó trong các công thức nêu trên, N là độ dài của chuỗi mã, v_1^N là các bit đầu vào, bit 1 đến bit N, trong chuỗi mã này, bao gồm các bit thông tin và các bit đóng băng; $\begin{bmatrix} F^{\otimes(n-1)} & 0 \\ F^{\otimes(n-1)} & F^{\otimes(n-1)} \end{bmatrix}$ là ma trận sinh cho chuỗi mã,

và trong đó $v_1^{N/2}$ là các bit đầu vào của mã con thứ nhất, mà là bit 1 đến bit N/2 trong chuỗi mã, $v_{N/2+1}^N$ là các bit đầu vào của mã con thứ hai, mà là bit N/2+1 đến bit N trong chuỗi mã.

6. Thiết bị thu theo điểm bất kỳ trong số các điểm từ 1 đến 5, trong đó các mã chương trình còn bao gồm các lệnh để:

chia chuỗi mã có độ dài S thành N mã con, trong đó mỗi mã con có độ dài S/N, và thực hiện một cách riêng biệt việc giải mã hủy bỏ liên tiếp (successive cancellation, SC) trên N mã con để thu được N kết quả giải mã SC, trong đó mỗi trong số S và N là các lũy thừa nguyên của 2, trước khi chia chuỗi mã có độ dài N thành m mã con;

trong đó tất cả các bit đầu vào trong N kết quả giải mã SC được sử dụng làm chuỗi mã có độ dài N.

7. Thiết bị thu theo điểm 5, trong đó việc chia chuỗi mã thành bốn mã con bao gồm:

chia chuỗi mã thành mã con thứ nhất và mã con thứ hai, trong đó các bit đầu vào tương ứng với hai mã con này lần lượt là a_k và b_k , và được biểu diễn bởi các công thức

$$a_1^{N/2} = v_1^{N/2} \oplus v_{N/2+1}^N \quad \text{và} \quad b_1^{N/2} = v_{N/2+1}^N; \text{ và}$$

chia mã con thứ nhất thành mã con thứ ba và mã con thứ tư, và chia mã con thứ hai thành mã con thứ năm và mã con thứ sáu, trong đó các bit đầu vào của mã con thứ ba, mã con thứ tư, mã con thứ năm, và mã con thứ sáu lần lượt là:

$$c_k \text{ mà được biểu diễn bằng công thức } c_k = a_k \oplus a_{k+N/4},$$

$$d_k \text{ mà được biểu diễn bằng công thức } d_k = a_{k+N/4},$$

$$e_k \text{ mà được biểu diễn bằng công thức } e_k = b_k \oplus b_{k+N/4},$$

$$f_k \text{ mà được biểu diễn bằng công thức } f_k = b_{k+N/4},$$

$$\text{trong đó } 1 \leq k \leq N/4, \quad a_1^{N/2} = v_1^{N/2} \oplus v_{N/2+1}^N, \text{ và } b_1^{N/2} = v_{N/2+1}^N.$$

8. Phương pháp giải mã chuỗi mã, bao gồm:

thu chuỗi mã có độ dài N bit đầu vào, trong đó chuỗi mã thu được bằng cách mã hóa một lượng bit thông tin trong bộ mã hóa ở thiết bị truyền trong hệ thống truyền thông không dây;

chia chuỗi mã thành m mã con mà được ghép với nhau, trong đó mỗi mã con có độ dài N/m, và trong đó mỗi trong số N và m là các lũy thừa nguyên của 2, và $N > m$;

tính toán riêng biệt, đối với m mã con của chuỗi mã, các khoảng cách Oclit được lấy bình phương của các bit đầu vào mà là độc lập với nhau trong m mã con, để thu được các khoảng cách Oclit được lấy bình phương tối thiểu của các bit đầu vào mà là độc lập với nhau trong m mã con, trong đó các khoảng cách Oclit được lấy bình phương tối thiểu của các bit đầu vào mà là độc lập với nhau trong m mã con được gọi chung là các khoảng cách Oclit được lấy bình phương tối thiểu độc lập;

thu được, theo m khoảng cách Oclit được lấy bình phương tối thiểu độc lập, khoảng cách Oclit được lấy bình phương tối thiểu của các bit đầu vào mà được ghép với nhau trong m mã con, trong đó khoảng cách Oclit được lấy bình phương tối thiểu của các bit đầu vào mà được ghép với nhau trong m mã con được gọi là khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp; và

thu được các bit đầu vào mà nằm trong m mã con và thỏa mãn các khoảng cách Oclit được lấy bình phương tối thiểu độc lập và khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp, và thu được kết quả giải mã của chuỗi mã theo các quan hệ giữa m mã con và chuỗi mã.

9. Phương pháp theo điểm 8, trong đó việc tính toán riêng biệt các khoảng cách Oclit được lấy bình phương tối thiểu độc lập bao gồm:

tính toán các khoảng cách Oclit được lấy bình phương tối thiểu độc lập theo cách song song.

10. Phương pháp theo điểm 8 hoặc 9, trong đó m bằng 2, 4 hoặc 8.

11. Phương pháp theo điểm 10, trong đó m bằng 2,

trong đó chuỗi mã được biểu diễn bằng công thức

$$x_1^N = v_1^N \times \begin{bmatrix} F^{\otimes(n-1)} & 0 \\ F^{\otimes(n-1)} & F^{\otimes(n-1)} \end{bmatrix} \\ = \left[\left(v_1^{N/2} \oplus v_{N/2+1}^N \right) F^{\otimes(n-1)} \quad v_{N/2+1}^N F^{\otimes(n-1)} \right],$$

trong đó việc chia chuỗi mã thành m mã con bao gồm:

chia chuỗi mã thành mã con thứ nhất và mã con thứ hai, trong đó các bit đầu vào tương ứng với hai mã con lần lượt là a_k và b_k , và được biểu diễn bằng các công thức $a_1^{N/2} = v_1^{N/2} \oplus v_{N/2+1}^N$ và $b_1^{N/2} = v_{N/2+1}^N$;

trong đó việc tính toán riêng biệt các khoảng cách Oclit được lấy bình phương tối thiểu độc lập bao gồm:

đối với các bit đầu vào $a_k, k \in \Omega_{11}^{(1)}$ mà nằm trong mã con thứ nhất và độc lập với bit đầu vào bất kỳ trong mã con thứ hai, thực hiện việc tính toán để thu được khoảng cách Oclit được lấy bình phương tối thiểu độc lập thứ nhất

$$E_a(a_k, k \in \Omega_{11}^{(1)}) = \min_{a_k, k \in \Omega_{11}^{(1)}} D_1^{N/2}; \text{ và}$$

đối với bit đầu vào $b_k, k \in \Omega_{11}^{(1)}$ mà nằm trong mã con thứ hai và độc lập với bit đầu vào bất kỳ trong mã con thứ nhất, thực hiện việc tính toán để thu được khoảng cách Oclit được lấy bình phương tối thiểu độc lập thứ hai

$$E_b(b_k, k \in \Omega_{11}^{(1)}) = \min_{b_k, k \in \Omega_{11}^{(1)}} D_{N/2+1}^N;$$

trong đó việc thu được khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp bao gồm:

kết hợp khoảng cách Oclit được lấy bình phương tối thiểu độc lập thứ nhất và khoảng cách Oclit được lấy bình phương tối thiểu độc lập thứ hai E_a, E_b , để

thu được $E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)}) = E_a(a_k, k \in \Omega_{01}^{(1)}) + E_b(b_k, k \in \Omega_{01}^{(1)})$; và

thực hiện việc tìm kiếm để thu được khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp thứ nhất mà được biểu diễn bằng công thức

$$\min_{a_k=b_k, k \in \Omega_{01}^{(1)}} E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)}) ; \text{ và}$$

trong đó việc thu được các bit đầu vào mà nằm trong các mã con thứ nhất và thứ hai và thỏa mãn khoảng cách Oclit được lấy bình phương tối thiểu độc lập và khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp, và thu được kết quả giải mã của chuỗi mã bao gồm:

thu được các bit đầu vào $a_k = b_k, k \in \Omega_{01}^{(1)}$ mà được ghép với nhau trong mã con thứ nhất và mã con thứ hai và thỏa mãn khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp thứ nhất, trong đó khoảng cách Oclit được lấy bình phương tối thiểu được kết hợp thứ nhất được biểu diễn bằng công thức

$$\min_{a_k=b_k, k \in \Omega_{01}^{(1)}} E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)}) ;$$

thu được các bit đầu vào $a_k, b_k, k \in \Omega_{11}^{(1)}$ mà là độc lập với nhau trong mã con thứ nhất và mã con thứ hai và thỏa mãn khoảng cách Oclit được lấy bình phương tối thiểu độc lập thứ nhất E_a và khoảng cách Oclit được lấy bình phương tối thiểu độc lập thứ hai E_b ; và

thu được các kết quả giải mã $v_1^{N/2}$ và $v_{N/2+1}^N$ của chuỗi mã bằng cách sử dụng các quan hệ $b_1^{N/2} = v_{N/2+1}^N$ và $a_1^{N/2} = v_1^{N/2} \oplus v_{N/2+1}^N$ giữa hai mã con và chuỗi mã,

trong đó trong các công thức nêu trên,

N là độ dài của chuỗi mã, v_1^N là các bit đầu vào, bit 1 đến bit N , trong

chuỗi mã này, bao gồm các bit thông tin và các bit đóng băng;

$$\begin{bmatrix} F^{\otimes(n-1)} & 0 \\ F^{\otimes(n-1)} & F^{\otimes(n-1)} \end{bmatrix} \text{ là ma trận sinh cho chuỗi mã,}$$

và trong đó $v_1^{N/2}$ là các bit đầu vào của mã con thứ nhất, mà là bit 1 đến bit $N/2$ trong chuỗi mã, $v_{N/2+1}^N$ là các bit đầu vào của mã con thứ hai, mà là bit $N/2+1$ đến bit N trong chuỗi mã;

tập chỉ số $\Omega_{01}^{(1)}$ biểu diễn rằng v_k là bit đóng băng và $v_{k+N/2}$ là bit thông tin; và tập chỉ số $\Omega_{11}^{(1)}$ biểu diễn rằng v_k là bit thông tin và $v_{k+N/2}$ là bit thông tin.

12. Phương pháp theo điểm 10, trong đó m bằng 4,

trong đó việc thu và chia chuỗi mã thành m mã con bao gồm:

thu chuỗi mã, và chia chuỗi mã này thành bốn mã con mà được ghép với nhau, trong đó mỗi mã con có độ dài $N/4$, N là lũy thừa nguyên của 2, và chuỗi

$$x_1^N = v_1^N \times \begin{bmatrix} F^{\otimes(n-1)} & 0 \\ F^{\otimes(n-1)} & F^{\otimes(n-1)} \end{bmatrix} \\ \text{mã được biểu diễn bằng công thức} = \left[\left(v_1^{N/2} \oplus v_{N/2+1}^N \right) F^{\otimes(n-1)} \quad v_{N/2+1}^N F^{\otimes(n-1)} \right],$$

và trong đó bốn mã con là mã con thứ ba, mã con thứ tư, mã con thứ năm, và mã con thứ sáu, và các bit đầu vào của mã con thứ ba, mã con thứ tư, mã con thứ năm, và mã con thứ sáu lần lượt là: c_k , d_k , e_k , và f_k ;

trong đó việc tính toán riêng biệt các khoảng cách Ôclit được lấy bình phương tối thiểu độc lập bao gồm:

tính toán riêng biệt các khoảng cách Ôclit được lấy bình phương tối thiểu độc lập đối với các bit đầu vào mà là độc lập với nhau trong mã con thứ ba, mã con thứ tư, mã con thứ năm, và mã con thứ sáu, để thu được khoảng cách Ôclit

được lấy bình phương tối thiểu độc lập thứ nhất $E_c = \min_{c_k, k \in \Omega_{11}^{(2)}} D_1^{N/4}$, khoảng cách

Öclit được lấy bình phương tối thiểu độc lập thứ hai $E_d = \min_{d_k, k \in \Omega_{11}^{(2)}} D_{N/4+1}^{N/2}$, khoảng

cách Öclit được lấy bình phương tối thiểu độc lập thứ ba $E_e = \min_{e_k, k \in \Omega_{11}^{(2)}} D_{N/2+1}^{3N/4}$, và

khoảng cách Öclit được lấy bình phương tối thiểu độc lập thứ tư

$E_f = \min_{f_k, k \in \Omega_{11}^{(2)}} D_{3N/4+1}^N$, trong đó tập chỉ số $\Omega_{11}^{(2)}$ biểu diễn tất cả các chỉ số thỏa mãn

$k \in \Omega_{11}^{(1)}$ và $k + N/4 \in \Omega_{11}^{(1)}$, và tập chỉ số $\Omega_{11}^{(1)}$ biểu diễn rằng v_k là bit thông tin

và $v_{k+N/2}$ là bit thông tin, trong đó $1 \leq k \leq N/4$;

trong đó việc thu được khoảng cách Öclit được lấy bình phương tối thiểu được kết hợp bao gồm:

thực hiện việc tính toán để thu được tổng các khoảng cách Öclit được lấy bình phương của mã con thứ ba và mã con thứ tư, trong đó tổng này được biểu diễn bằng công thức $E_{sum1} = E_c + E_d$, và

đối với các bit đầu vào mà được ghép với nhau trong mã con thứ ba và mã con thứ tư, thực hiện việc tìm kiếm để thu được khoảng cách Öclit được lấy bình phương tối thiểu được kết hợp thứ nhất mà được biểu diễn bằng công thức

$E_{sum2} = \min_{a_k, k \in \Omega_{01}^{(2)}} E_{sum1}$, trong đó $\Omega_{01}^{(2)}$ biểu diễn tất cả các chỉ số thỏa mãn $k \notin \Omega_{11}^{(1)}$ và $k + N/4 \in \Omega_{11}^{(1)}$, trong đó $1 \leq k \leq N/4$;

thực hiện việc tính toán để thu được tổng các khoảng cách Öclit được lấy bình phương của mã con thứ năm và mã con thứ sáu, trong đó tổng này được

biểu diễn bằng công thức $E_{sum3} = E_e + E_f$, và

đối với các bit đầu vào mà được ghép với nhau trong mã con thứ năm và

mã con thứ sáu, thực hiện việc tìm kiếm để thu được khoảng cách Ôclit được lấy bình phương tối thiểu được kết hợp thứ hai mà được biểu diễn bằng công thức $E_{sum4} = \min_{b_k, k \in \Omega_{01}^{(2)}} E_{sum3}$, trong đó $\Omega_{01}^{(2)}$ biểu diễn tất cả các chỉ số thỏa mãn $k \notin \Omega_{11}^{(1)}$ và $k + N/4 \in \Omega_{11}^{(1)}$, trong đó $1 \leq k \leq N/4$;

đối với các bit đầu vào mà được ghép với nhau trong các mã con từ thứ ba đến thứ sáu, tính toán tổng khoảng cách Ôclit được lấy bình phương mà được biểu diễn bằng công thức $E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)}) = E_{sum2} + E_{sum4}$, và thực hiện việc tìm kiếm để thu được khoảng cách Ôclit được lấy bình phương tối thiểu được kết hợp thứ ba $\min_{a_k = b_k, k \in \Omega_{01}^{(1)}} E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)})$, trong đó tập chỉ số $\Omega_{11}^{(1)}$ biểu diễn rằng v_k là bit đóng băng, và $v_{k+N/2}$ là bit thông tin; và

trong đó việc thu được kết quả giải mã của chuỗi mã bao gồm:

thu được các bit đầu vào $a_k = b_k, k \in \Omega_{01}^{(1)}$ thỏa mãn khoảng cách Ôclit được lấy bình phương tối thiểu được kết hợp thứ ba $\min_{a_k = b_k, k \in \Omega_{01}^{(1)}} E_{sum}(a_k = b_k, k \in \Omega_{01}^{(1)})$;

thay thế một cách riêng biệt các bit đầu vào $a_k = b_k, k \in \Omega_{01}^{(1)}$ vào khoảng cách Ôclit được lấy bình phương tối thiểu được kết hợp thứ nhất E_{sum2} và khoảng cách Ôclit được lấy bình phương tối thiểu được kết hợp thứ hai E_{sum4} để thu được các bit đầu vào khác; và

sau khi tất cả các bit đầu vào c_k, d_k, e_k , và f_k thu được, thu được các bit đầu vào v_1^N của chuỗi mã theo các quan hệ
$$\begin{cases} v_k = c_k \oplus d_k \oplus e_k \oplus f_k \\ v_{k+N/4} = d_k \oplus f_k \\ v_{k+N/2} = e_k \oplus f_k \\ v_{k+3N/4} = f_k \end{cases}$$
 giữa các mã con từ thứ ba đến thứ sáu và chuỗi mã;

trong đó trong các công thức nêu trên, N là độ dài của chuỗi mã, v_1^N là các

bit đầu vào, bit 1 đến bit N, trong chuỗi mã này, bao gồm các bit thông tin và các

bit đóng băng; $\begin{bmatrix} F^{\otimes(n-1)} & 0 \\ F^{\otimes(n-1)} & F^{\otimes(n-1)} \end{bmatrix}$ là ma trận sinh cho chuỗi mã,

và trong đó $v_1^{N/2}$ là các bit đầu vào của mã con thứ nhất, mà là bit 1 đến bit N/2 trong chuỗi mã, $v_{N/2+1}^N$ là các bit đầu vào của mã con thứ hai, mà là bit N/2+1 đến bit N trong chuỗi mã.

13. Phương pháp theo điểm bất kỳ trong số các điểm từ 8 đến 12, trong đó trước khi thu và chia chuỗi mã có độ dài N thành m mã con, phương pháp còn bao gồm:

chia chuỗi mã có độ dài S thành N mã con, trong đó mỗi mã con có độ dài S/N, và thực hiện một cách riêng biệt việc giải mã SC để thu được N kết quả giải mã SC, và

sử dụng tất cả các bit đầu vào trong N kết quả giải mã SC như là chuỗi mã có độ dài N;

trong đó kết quả giải mã của chuỗi mã có độ dài S thu được theo tất cả các bit đầu vào,

trong đó mỗi trong số S và N là lũy thừa nguyên của 2.

14. Phương pháp theo điểm 12, trong đó việc chia chuỗi mã thành bốn mã con bao gồm:

chia chuỗi mã thành mã con thứ nhất và mã con thứ hai, trong đó các bit đầu vào tương ứng với hai mã con này lần lượt là a_k và b_k , và được biểu diễn bởi các công thức :

$$a_1^{N/2} = v_1^{N/2} \oplus v_{N/2+1}^N \quad \text{và} \quad b_1^{N/2} = v_{N/2+1}^N; \text{ và}$$

chia mã con thứ nhất thành mã con thứ ba và mã con thứ tư, và chia mã con thứ hai thành mã con thứ năm và mã con thứ sáu, trong đó các bit đầu vào của mã con thứ ba, mã con thứ tư, mã con thứ năm, và mã con thứ sáu lần lượt là:

$$c_k \text{ mà được biểu diễn bằng công thức } c_k = a_k \oplus a_{k+N/4},$$

$$d_k \text{ mà được biểu diễn bằng công thức } d_k = a_{k+N/4},$$

$$e_k \text{ mà được biểu diễn bằng công thức } e_k = b_k \oplus b_{k+N/4},$$

$$f_k \text{ mà được biểu diễn bằng công thức } f_k = b_{k+N/4},$$

$$\text{trong đó } 1 \leq k \leq N/4, \quad a_1^{N/2} = v_1^{N/2} \oplus v_{N/2+1}^N, \text{ và } b_1^{N/2} = v_{N/2+1}^N.$$

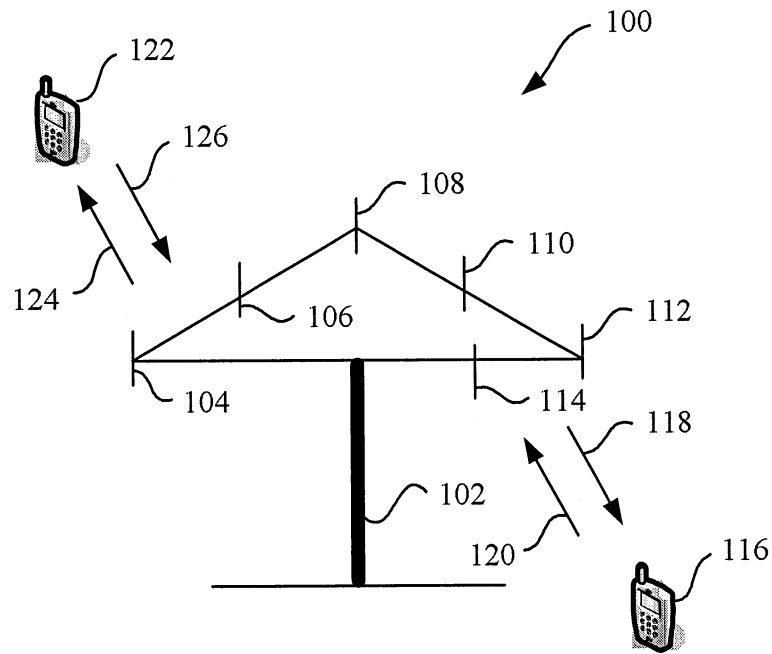


FIG. 1

200

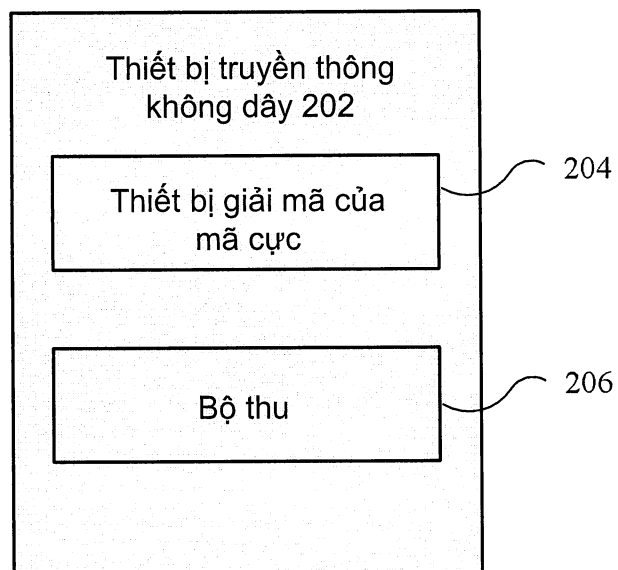


FIG. 2

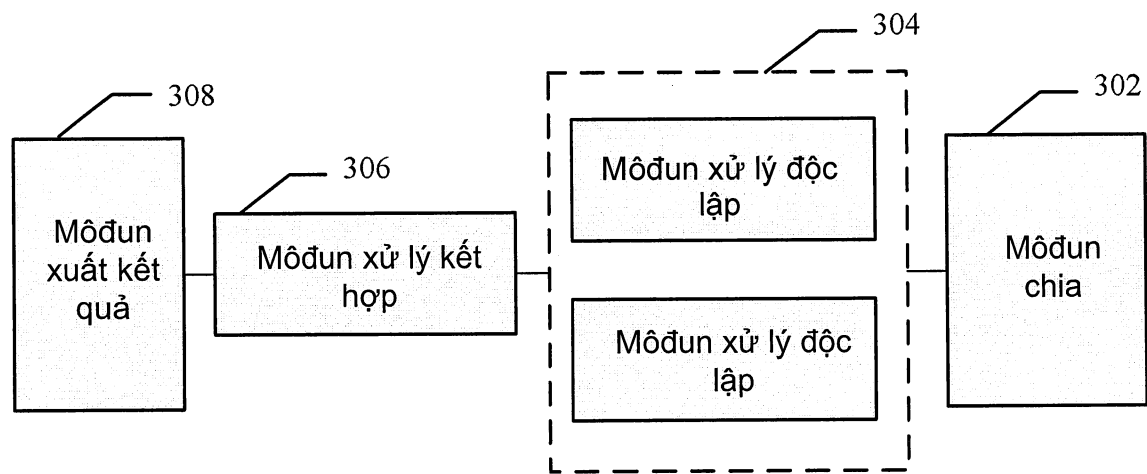


FIG. 3

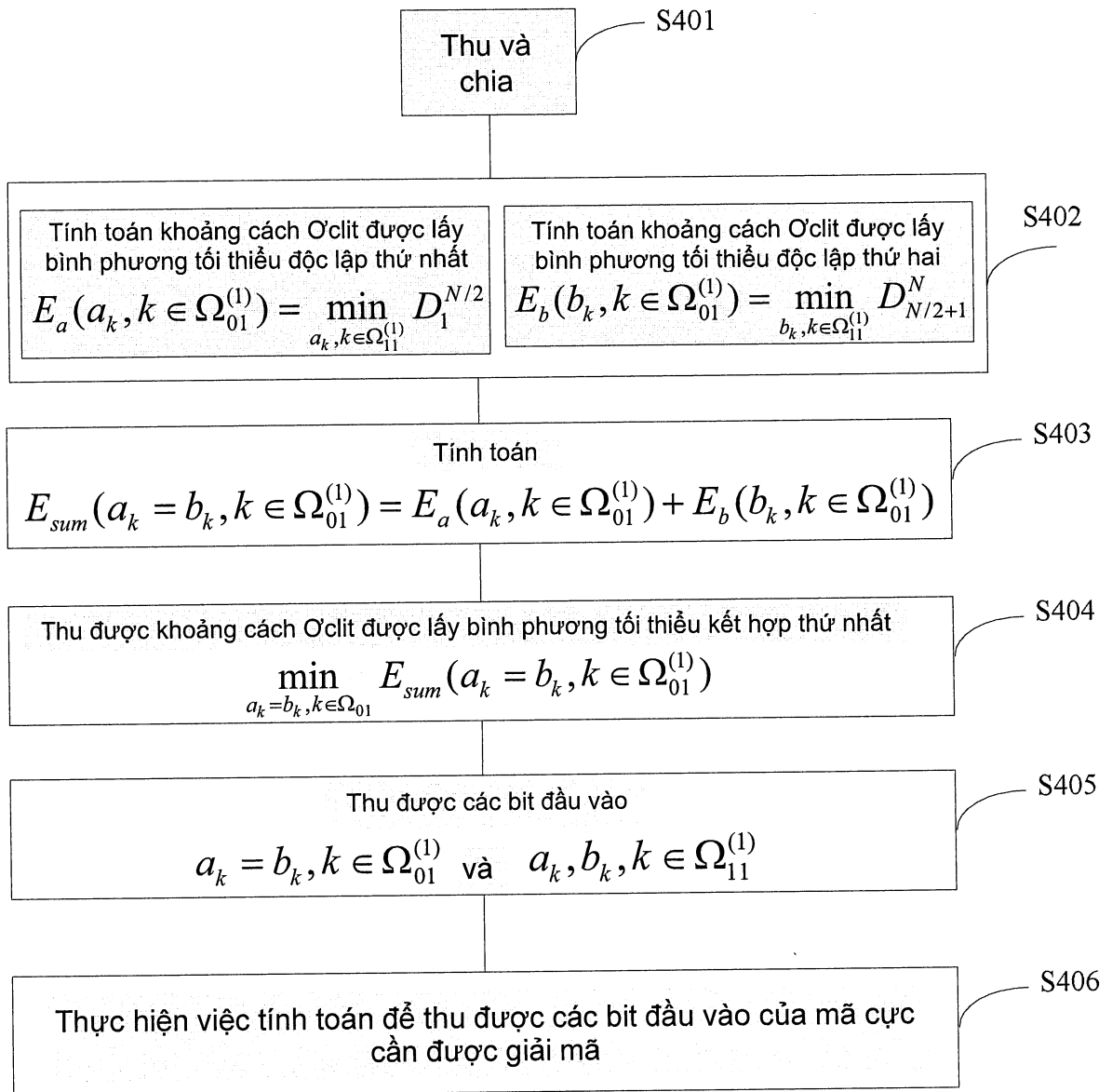


FIG. 4

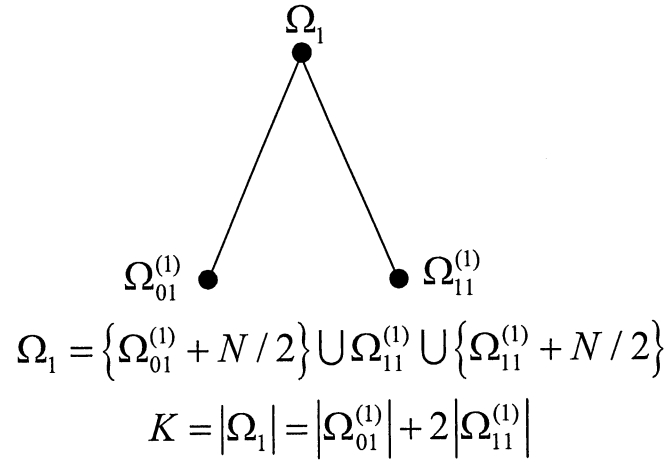


FIG. 5

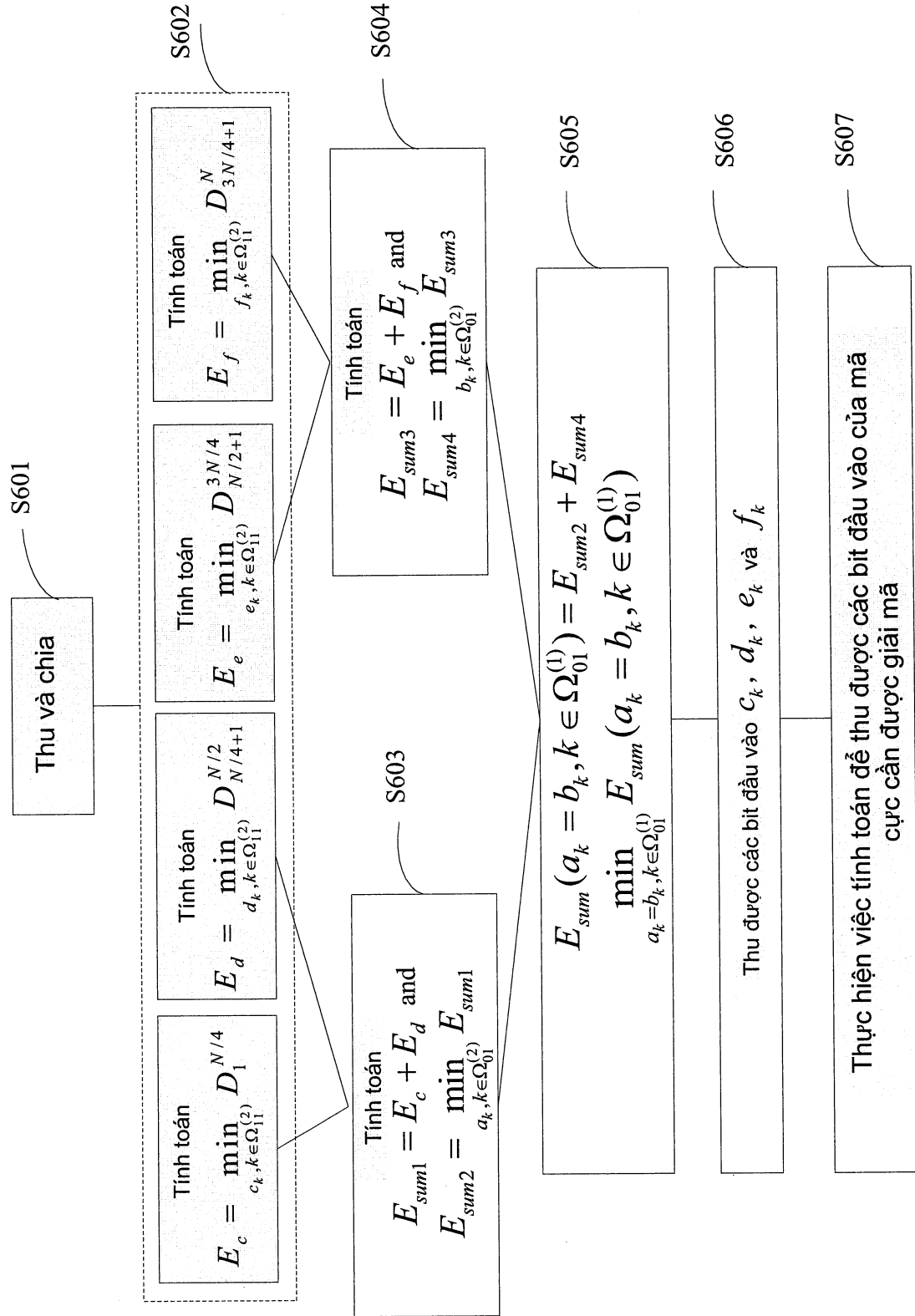


FIG. 6

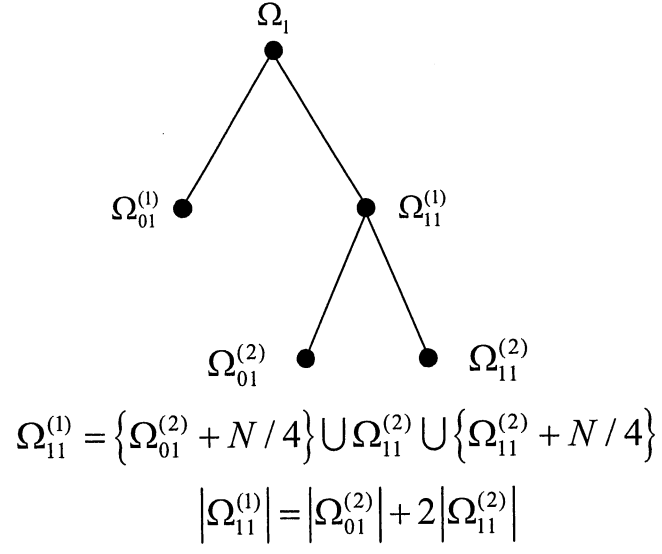


FIG. 7

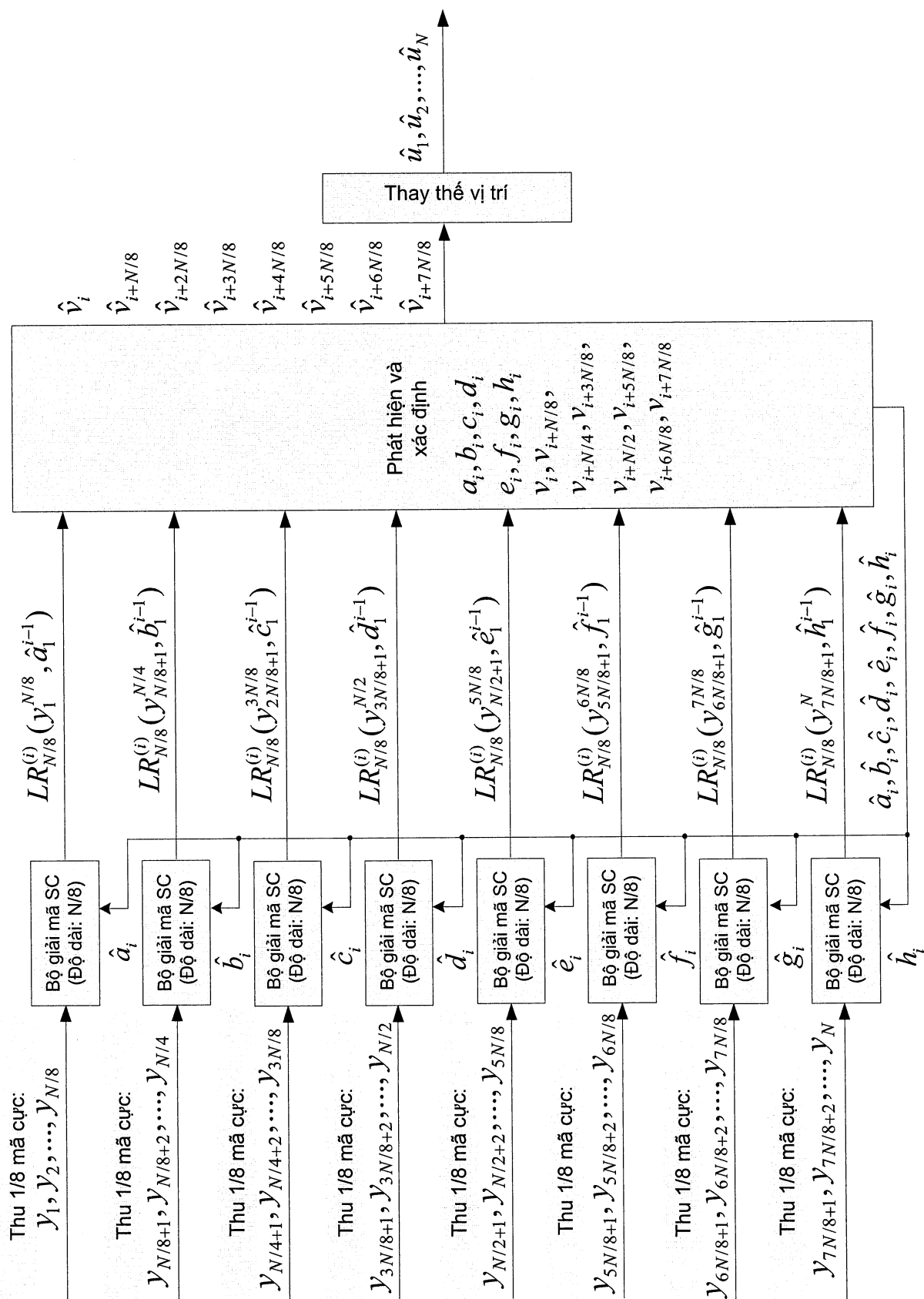


FIG. 8

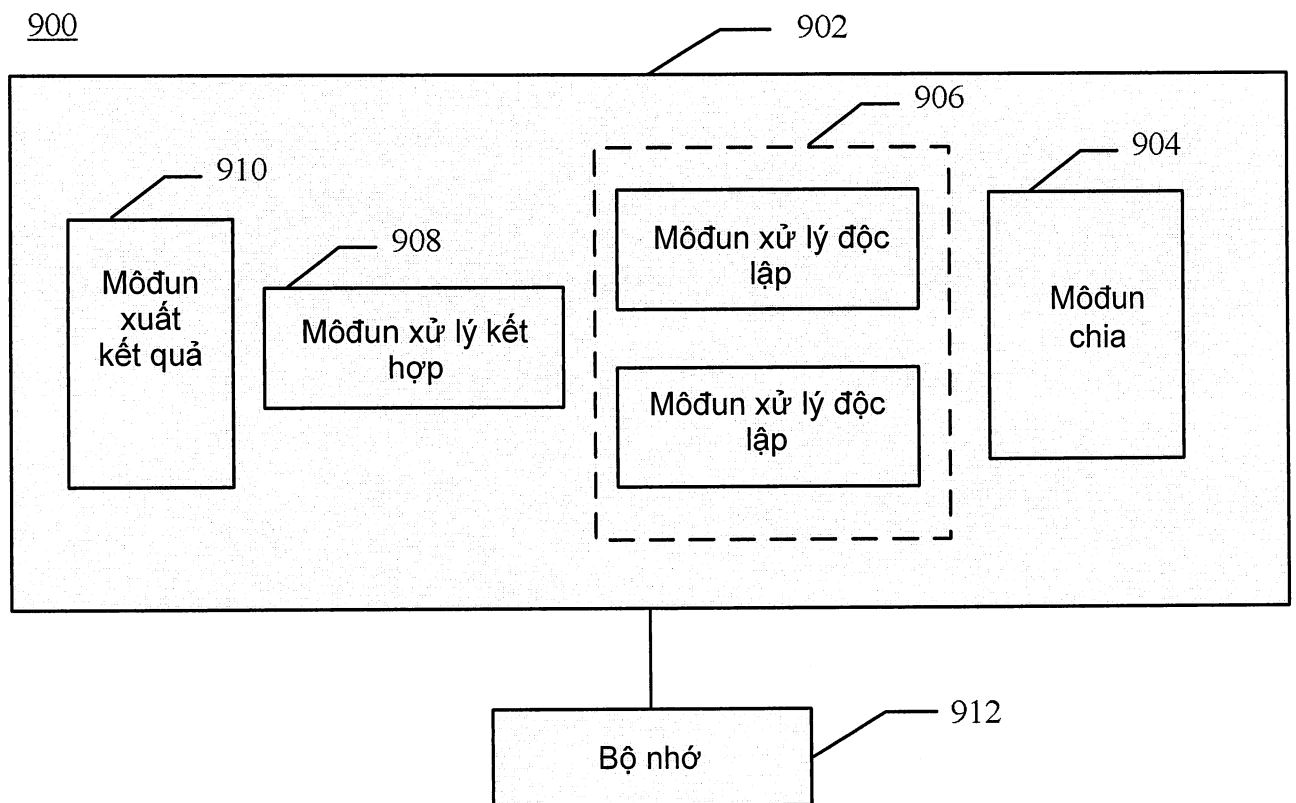


FIG. 9