(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) **1-0032803**

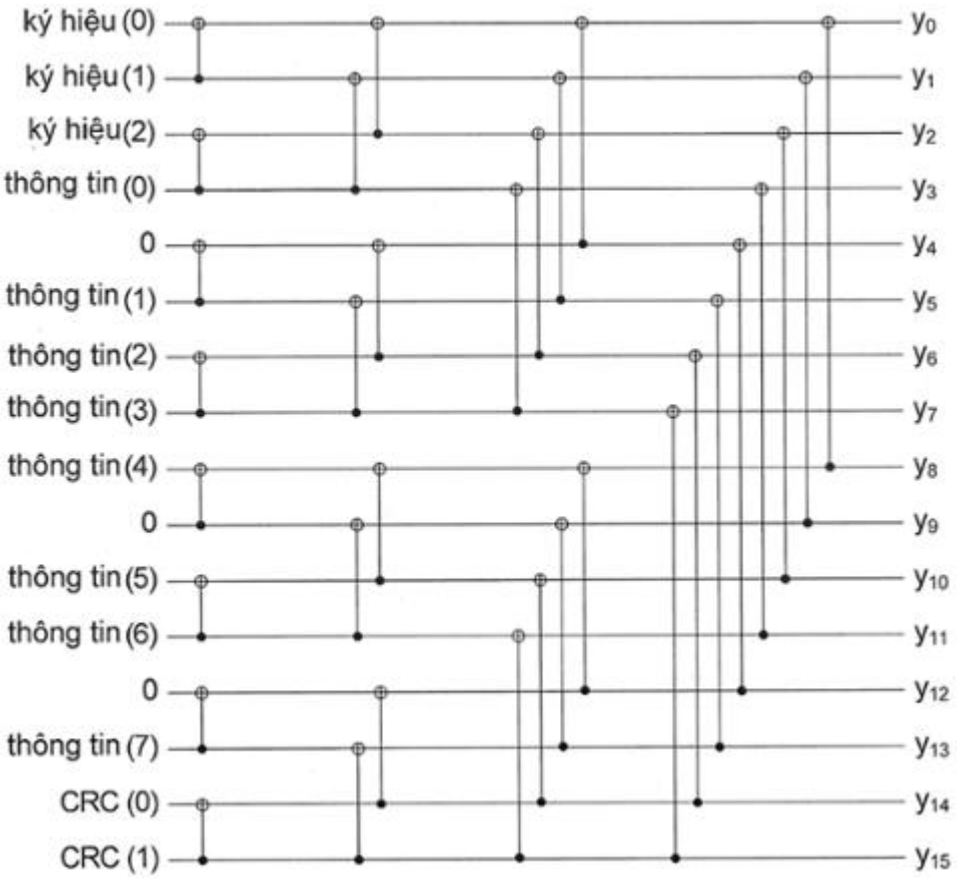
(51)[8] **H03M 13/29**

(13) **B**

(21) 1-2018-02784 (22) 01/12/2016
(86) PCT/CN2016/108234 01/12/2016 (87) WO 2017/092693 A1 08/06/2017
(30) 62/261,590 01/12/2015 US; 15/364,521 30/11/2016 US
(45) 25/08/2022 413 (43) 25/09/2018 366A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District Shenzhen, Guangdong 518129, P. R. China
(72) GE, Yiqun (CN); SHI, Wuxian (CN).
(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) THIẾT BỊ TRUYỀN CÁC BIT THÔNG TIN, THIẾT BỊ THU CÁC TỪ MÃ, PHƯƠNG PHÁP TRUYỀN CÁC BIT THÔNG TIN VÀ PHƯƠNG PHÁP THU CÁC TỪ MÃ

(57) Sáng chế đề cập đến thiết bị và phương pháp truyền các bit thông tin, thiết bị và phương pháp thu các từ mã, dùng trong bộ mã hóa và bộ giải mã mã cực được cho phép ký hiệu. Các bit ký hiệu được chèn vào một vài vị trí bit không tin cậy. Các bit ký hiệu khác nhau được chèn dùng cho các bộ thu khác nhau. Đối với từ mã định trước, chỉ bộ thu đã biết về ký hiệu có thể giải mã từ mã. Các bit kiểm tra dư vòng (Cyclic redundancy check, CRC) có thể được bao gồm trong vectơ đầu vào để hỗ trợ việc giải mã.


ký hiệu (0)
ký hiệu (1)
ký hiệu(2)
thông tin (0)
0
thông tin (1)
thông tin(2)
thông tin (3)
thông tin (4)
0
thông tin (5)
thông tin (6)
0
thông tin (7)
CRC (0)
CRC (1)
y0
y1
y2
y3
y4
y5
y6
y7
y8
y9
y10
y11
y12
y13
y14
y15

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến các mã cực, và đề cập đến các bộ mã hóa và các bộ giải mã dùng cho các mã cực.

Tình trạng kỹ thuật của sáng chế

Các mã cực dựa vào các ma trận tích Kronecker. $\mathbf{G} = \mathbf{F}^{\otimes m} = \mathbf{F} \otimes \cdots \otimes \mathbf{F}$ là tích Kronecker gập m của ma trận hạt nhân **F**.

Nếu là **A** ma trận $m \times n$ **A** và **B** là ma trận $p \times q$, sau đó tích Kronecker **A** $\otimes$ **B** là ma trận khối $mp \times nq$:

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} a_{11}\mathbf{B} & \cdots & a_{1n}\mathbf{B} \\ \vdots & \ddots & \vdots \\ a_{m1}\mathbf{B} & \cdots & a_{mn}\mathbf{B} \end{bmatrix},$$

rõ ràng hơn:

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & \cdots & a_{11}b_{1q} & \cdots & \cdots & a_{1n}b_{11} & a_{1n}b_{12} & \cdots & a_{1n}b_{1q} \\ a_{11}b_{21} & a_{11}b_{22} & \cdots & a_{11}b_{2q} & \cdots & \cdots & a_{1n}b_{21} & a_{1n}b_{22} & \cdots & a_{1n}b_{2q} \\ \vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \ddots & \vdots \\ a_{11}b_{p1} & a_{11}b_{p2} & \cdots & a_{11}b_{pq} & \cdots & \cdots & a_{1n}b_{p1} & a_{1n}b_{p2} & \cdots & a_{1n}b_{pq} \\ \vdots & \vdots & & \vdots & \ddots & & \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots & & \ddots & \vdots & \vdots & & \vdots \\ a_{m1}b_{11} & a_{m1}b_{12} & \cdots & a_{m1}b_{1q} & \cdots & \cdots & a_{mn}b_{11} & a_{mn}b_{12} & \cdots & a_{mn}b_{1q} \\ a_{m1}b_{21} & a_{m1}b_{22} & \cdots & a_{m1}b_{2q} & \cdots & \cdots & a_{mn}b_{21} & a_{mn}b_{22} & \cdots & a_{mn}b_{2q} \\ \vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \ddots & \vdots \\ a_{m1}b_{p1} & a_{m1}b_{p2} & \cdots & a_{m1}b_{pq} & \cdots & \cdots & a_{mn}b_{p1} & a_{mn}b_{p2} & \cdots & a_{mn}b_{pq} \end{bmatrix}.$$

Fig.1 thể hiện cách làm thế nào ma trận tích Kronecker có thể được tạo ra từ ma trận hạt nhân $\mathbf{G_2}$ 102. Được thể hiện trên Fig.1 là ma trận tích Kronecker gập-2 $\mathbf{G_2}^{\otimes 2}$ 102 và ma trận tích Kronecker gập-3 $\mathbf{G_2}^{\otimes 3}$ 104, trong đó $\mathbf{G_2} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Phương pháp này có thể được mở rộng để tạo ra ma trận tích Kronecker gập-m $\mathbf{G_2}^{\otimes m}$.

Mã cực có thể được tạo nên từ ma trận tích Kronecker dựa vào ma trận $\mathbf{G_2}$. Đối với mã cực có các từ mã có độ dài $N = 2^m$, ma trận sinh là $\mathbf{G_2}^{\otimes m}$. Ví dụ về việc sử dụng ma trận tích Kronecker $\mathbf{G_2}^{\otimes 3}$ để tạo ra các từ mã có độ dài 8 được mô tả trên Fig.2. Từ mã **x** được tạo nên bởi tích của vectơ đầu vào **u** và ma trận tích Kronecker $\mathbf{G_2}^{\otimes 3}$ 104 như được chỉ ra ở 110. Vectơ đầu vào **u** được bao gồm các bit phong tỏa và các bit thông tin. Theo ví dụ cụ thể, N=8, vì vậy vectơ đầu vào **u** là 8 bit vectơ, và từ mã x là 8 bit vectơ. Vectơ đầu vào có các bit phong tỏa ở các vị trí 0, 1, 2 và 4, và có các bit thông tin ở các vị trí 3, 5, 6 và 7. Cách thực hiện ví dụ của bộ mã hóa mà tạo ra các từ mã được chỉ ra ở 112, trong đó các bit phong tỏa tất cả được thiết đặt tới 0, trong đó vòng tròn xung quanh ký hiệu cộng chỉ ra sự bổ sung môđulô 2. Đối với ví dụ trên Fig.2, N=8 bit vectơ đầu vào được tạo nên từ K=4 bit thông tin và N-K=4 bit phong tỏa. Các mã của dạng thức này được gọi là các mã cực và bộ mã hóa được gọi là bộ mã hóa cực.

Tổng quát hơn, trong "Sự phân cực kênh: phương pháp xây dựng các mã đạt được dung lượng dùng cho các kênh không nhớ đầu vào nhị phân đối xứng" của E. Arikan, IEEE các giao dịch về lý thuyết thông tin, tập 55, ấn phẩm 7, được xuất bản vào tháng 7 năm 2009, lý thuyết "sự phân cực kênh" đã được chứng minh ở chương IV. Sự phân cực kênh là thao tác mà tạo ra các kênh N từ các bản sao độc lập N của kênh không nhớ rời rạc đầu vào nhị phân (B-DMC - binary-input discrete memoryless channel) W sao cho các kênh song song mới được phân cực theo nghĩa là thông tin tương hỗ của chúng hoặc sát với 0 (các kênh SNR tương hỗ thấp) hoặc sát với 1 (các kênh SNR tương hỗ cao). Nói cách khác, một vài vị trí bit bộ mã hóa sẽ trải qua kênh với SNR tương hỗ cao, và sẽ có độ tin cậy tương đối thấp/khả năng thấp được giải mã chính xác, và đối với một vài vị trí bit bộ mã hóa, chúng sẽ trải qua kênh với SNR tương hỗ cao, và sẽ có độ tin cậy cao/khả năng cao được giải mã chính xác. Trong việc xây dựng mã, các bit thông tin được đặt ở các vị trí tin cậy và các bit phong tỏa (các bit được biết tới cả bộ mã hóa và bộ giải mã) được đặt ở các vị trí không tin cậy. Theo lý thuyết, các bit phong tỏa có thể được thiết đặt tới bất kỳ trị số nào miễn

là chuỗi bit phong tỏa được biết tới cả bộ mã hóa và bộ giải mã. Trong các ứng dụng thông thường, các bit phong tỏa tất cả được thiết đặt tới "0".

Theo trường hợp truyền thông trong đó bộ truyền có thể muốn gửi dữ liệu chỉ cho một hoặc nhiều bộ thu cụ thể, khối được mã hóa được truyền qua không khí có thể được thu bởi bất kỳ bộ thu không đúng mục tiêu nào khác. Các phương pháp khác nhau có thể được sử dụng để ngăn ngừa các bộ thu không đúng mục tiêu này khỏi giải mã thông tin. Một vài hệ thống sử dụng giao thức bảo mật/mã hóa nổi tiếng trên các lớp cao hơn để cung cấp sự bảo mật. Tuy nhiên, các phương pháp này bao gồm một vài tài nguyên lập lịch lớp cao hơn, và dẫn đến sự trì hoãn xử lý dài. Hơn nữa, các thuật toán lập lịch lớp cao hơn có thể không cung cấp đủ bảo mật trong điều kiện SNR tương đối thấp.

Sẽ có ưu điểm là có phương pháp tương đối đơn giản để cung cấp bảo mật cho các mã cực.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là đề xuất bộ mã hóa và bộ giải mã mã cực được cho phép ký hiệu. Các bit ký hiệu được chèn vào một vài vị trí bit không tin cậy. Các bit ký hiệu khác nhau được chèn dùng cho các bộ thu khác nhau. Đối với từ mã định trước, chỉ bộ thu đã biết về ký hiệu có thể giải mã từ mã. Các bit kiểm tra dư vòng (CRC - Cyclic redundancy check) có thể được bao gồm trong vectơ đầu vào để hỗ trợ việc giải mã.

Khía cạnh khái quát của sáng chế đề xuất phương pháp trong bộ mã hóa. Phương pháp này bao gồm việc tạo ra N bit vectơ đầu vào cho việc mã hóa cực, vectơ đầu vào có các vị trí bit tin cậy mã cực và các vị trí bit không tin cậy mã cực, bằng cách chèn mỗi trong số ít nhất một bit thông tin vào vị trí bit tin cậy mã cực tương ứng, và mỗi trong số ít nhất một bit ký hiệu vào vị trí bit không tin cậy mã cực tương ứng, trong đó $N = 2^m$ trong đó $m>=2$. N bit vectơ đầu vào được nhân với ma trận sinh mã cực để tạo ra từ mã mã cực, và sau đó từ mã mã cực được truyền hoặc được lưu trữ.

Một cách tùy chọn, ít nhất một bit thông tin bao gồm K bit thông tin, K>=1, và phương pháp còn bao gồm việc xử lý K bit thông tin để tạo ra u bit CRC, trong đó u >=1, và tạo ra N bit vectơ đầu vào bằng cách chèn mỗi trong số u bit CRC ở vị trí bit tin cậy mã cực tương ứng. Kết quả là, từ mã cực là từ mã cực được kiểm tra CRC.

Một cách tùy chọn, phương pháp này còn bao gồm việc truyền thông ít nhất một bit ký hiệu tới bộ thu một cách tách biệt từ sự truyền của từ mã.

Khía cạnh khái quát khác của sáng chế đề xuất phương pháp trong bộ mã hóa mà bao gồm các bước:

tạo ra vectơ đầu vào bằng cách:

đối với mỗi trong số các khối thông tin P, trong đó P>=2, tạo ra phần tương ứng của vectơ đầu vào, phần tương ứng bắt đầu với tập hợp tương ứng của ít nhất một bit ký hiệu và cũng chứa khối thông tin, mỗi trong số các tập hợp của các bit ký hiệu khác với nhau;

kết hợp các phần tương ứng để tạo ra vectơ đầu vào;

nhân vectơ đầu vào với ma trận sinh mã cực để tạo ra từ mã mã cực;

và sau đó truyền hoặc lưu trữ từ mã.

Một cách tùy chọn, việc tạo ra vectơ đầu vào còn bao gồm việc xử lý mỗi khối thông tin để tạo ra tập hợp tương ứng của các bit CRC, và đối với mỗi trong số các khối thông tin P, bao gồm tập hợp tương ứng của các bit CRC trong phần tương ứng của vectơ đầu vào.

Khía cạnh khái quát khác của sáng chế đề xuất phương pháp trong bộ giải mã. Phương pháp bao gồm việc thu từ mã mà đã được mã hóa với mã cực trong đó ít nhất một bit phong tỏa được thay bằng ít nhất một bit ký hiệu tương ứng cụ thể tới bộ giải mã và được biết tới bộ giải mã tách biệt với việc thu từ mã. Việc giải mã của từ mã thu được được thực hiện bằng cách thiết đặt ít nhất một bit phong tỏa để bằng ít nhất một trị số bit ký hiệu tương ứng.

Một cách tùy chọn, phương pháp này còn bao gồm việc thu thông tin trên các bit ký hiệu được sử dụng trong mã cực tách biệt với việc thu từ mã.

Một cách tùy chọn, từ mã đã được mã hóa với mã cực được cho phép ký hiệu được kiểm tra CRC, trường hợp trong đó phương pháp còn bao gồm việc xác nhận kết quả của việc giải mã nhờ sử dụng việc kiểm tra CRC.

Khía cạnh khái quát khác của sáng chế đề xuất thiết bị mà có bộ tạo vectơ đầu vào được tạo cấu hình để tạo ra N bit vectơ đầu vào cho việc mã hóa cực, vectơ đầu vào có các vị trí bit tin cậy mã cực và các vị trí bit không tin cậy mã cực, bằng cách chèn mỗi trong số ít nhất một bit thông tin vào vị trí bit tin cậy mã cực tương ứng, và mỗi trong số ít nhất một bit ký hiệu vào vị trí bit không tin cậy mã cực tương ứng, trong đó $N = 2^m$ trong đó m>=2. Ngoài ra, thiết bị có bộ mã hóa mã cực được tạo cấu hình để nhân vectơ đầu vào với ma trận sinh mã cực để tạo ra từ mã cực.

Khía cạnh khái quát khác của sáng chế đề xuất thiết bị có bộ tạo vectơ đầu vào được tạo cấu hình để tạo ra N bit vectơ đầu vào cho việc mã hóa cực bằng cách:

đối với mỗi trong số các khối thông tin P, trong đó P>=2, tạo ra phần tương ứng của vectơ đầu vào, phần tương ứng bắt đầu với tập hợp tương ứng của ít nhất một bit ký hiệu và cũng chứa khối thông tin, mỗi trong số các tập hợp của các bit ký hiệu khác với nhau; và

kết hợp các phần tương ứng để tạo ra vectơ đầu vào.

Thiết bị cũng có bộ mã hóa mã cực được tạo cấu hình để nhân vectơ đầu vào với ma trận sinh mã cực để tạo ra từ mã cực.

Một cách tùy chọn, thiết bị có bộ xử lý CRC được tạo cấu hình để xử lý mỗi khối thông tin để tạo ra tập hợp tương ứng của các bit CRC. Trong trường hợp này, bộ tạo ra vectơ đầu vào bao gồm tập hợp tương ứng của các bit CRC đối với mỗi trong số các khối thông tin P trong phần tương ứng của vectơ đầu vào.

Khía cạnh khái quát khác của sáng chế đề xuất thiết bị có bộ thu để thu từ mã mà đã được mã hóa với mã cực, và bộ giải mã được tạo cấu hình để giải mã

mã cực của từ mã thu được bằng cách xử lý ít nhất một bit ký hiệu như bit phong tỏa có trị số bit ký hiệu đã biết.

Một cách tùy chọn, thiết bị được tạo cấu hình để thu thông tin trên các bit ký hiệu được sử dụng trong mã cực tách biệt với việc thu từ mã.

Một cách tùy chọn, thiết bị cũng có bộ kiểm tra CRC được tạo cấu hình để xác nhận kết quả của việc giải mã nhờ sử dụng việc kiểm tra CRC.

Mô tả vắn tắt các hình vẽ

Các phương án của sáng chế tới đây sẽ được mô tả dựa vào các hình vẽ kèm theo trong đó:

Fig.1 là ví dụ về ma trận sinh mã cực thông thường;

Fig.2 là ví dụ về bộ mã hóa mã cực thông thường;

Fig.3 là lưu đồ của phương pháp mã hóa mã cực được cho phép ký hiệu được kiểm tra CRC theo một phương án của sáng chế;

Fig.4 là sơ đồ khối của trường hợp ứng dụng ví dụ theo một phương pháp trên Fig.3;

Fig.5 là cách thực hiện mạch ví dụ theo một phương pháp trên Fig.3;

Fig.6 là lưu đồ của phương pháp giải mã từ mã của mã cực được cho phép ký hiệu được kiểm tra CRC;

Fig.7A là lưu đồ của phương pháp mã hóa mã cực được cho phép ký hiệu được kiểm tra CRC với nhiều ký hiệu theo một phương án của sáng chế;

Fig.7B là sơ đồ khối của trường hợp ứng dụng ví dụ theo một phương pháp trên Fig.7;

Fig.8 là cách thức thực hiện mạch ví dụ theo một phương pháp trên Fig.7A;

Fig.9 là sơ đồ khối của thiết bị để thu và giải mã các từ mã của mã cực được cho phép ký hiệu được kiểm tra CRC; và

Fig.10 là sơ đồ khối của thiết bị để mã hóa và truyền các từ mã của mã cực được cho phép ký hiệu được kiểm tra CRC.

Mô tả chi tiết sáng chế

Khi các mã cực được sử dụng, các bit kiểm tra dư vòng (CRC - Cyclic redundancy check) có thể được bao gồm trong vectơ đầu vào để hỗ trợ việc giải mã. Các bit CRC được tạo ra dựa vào các bit thông tin được truyền. Các bit CRC được bao gồm trong các vị trí tin cậy (nghĩa là, các vị trí với kênh tin cậy). Các bit CRC có thể được bổ sung để nâng cao hiệu suất mã cực cho độ dài khối từ ngắn đến trung bình. Đối với bộ mã hóa cực độ dài khối rất dài, việc kiểm trad ư vòng là không cần thiết. Trong trường hợp trong đó các bit CRC được bao gồm, N bit vectơ đầu vào được tạo nên từ K bit thông tin, u bit CRC, và N-K-u bit phong tỏa. Ví dụ được mô tả trên Fig.3. Bắt đầu với k bit khối thông tin 200, u bit CRC được cộng thêm ở 202 để tạo ra vectơ với K bit khối thông tin, và u bit CRC ở 204. Ở 206, N-K-u bit phong tỏa được chèn để tạo ra N bit vectơ đầu vào với K bit khối thông tin, và u bit CRC và N-K-u bit phong tỏa, trong đó N là luỹ thừa của 2. Vectơ 208 sau đó được nhân với ma trận tích Kronecker ở 210 để tạo ra N bit từ mã 212.

Cách thực hiện ví dụ được mô tả trên Fig.4, trong đó N=16, K=8, u=2 và có sáu bit phong tỏa cho tốc độ mã hóa 0,5 các bit phong tỏa được chèn ở các ví trí 0, 1, 2, 4, 9 và 12. Ở bộ giải mã, các bit CRC được xem như các bit thông tin cho đến khi vào thời điểm khi chúng được sử dụng để kiểm tra các bit thông tin khác.

Đặc điểm của bộ giải mã cực là khi bit thông tin được giải mã, bit không bao giờ có cơ hội được điều chỉnh. Bit mà đã được thiết đặt ở bước i không thể được thay đổi ở bước $j > i$. Ngoài ra, sự nhận biết của trị số của các bit phong tỏa tương lai hoặc các bit ký hiệu tương lai không được xem xét nghĩa là, các bit tương lai này, thậm chí được biết dùng cho bộ giải mã, sẽ không giúp giải mã bit thông tin hiện thời.

Theo trường hợp truyền thông trong đó bộ truyền có thể muốn gửi dữ liệu chỉ cho một hoặc nhiều bộ thu cụ thể, khối được mã hóa trên không khí có thể được thu bởi bất kỳ bộ thu không đúng mục tiêu nào khác. Để ngăn ngừa các bộ thu không đúng mục tiêu này khỏi giải mã thông tin, ký hiệu mà được biết bởi bộ truyền và (các) bộ thu đúng mục tiêu chỉ được sử dụng để bảo vệ dữ liệu

được mã hóa. Nghĩa là, ký hiệu "được nhúng" vào dữ liệu được mã hóa bởi phương tiện định trước mà chỉ (các) bộ thu đúng mục tiêu có thể sử dụng nó để giải mã dữ liệu. Độ dài của ký hiệu có thể, ví dụ, là hàng chục bit lên đến hàng trăm bit. Ký hiệu càng dài, nó càng có thể cung cấp nhiều sự bảo mật hơn, và không gian ký hiệu kết quả càng lớn. Ví dụ với ký hiệu đủ dài, không gian ký hiệu có thể chứa hàng nghìn hoặc thậm chí hàng triệu ký hiệu. Ngoài ra, một cách lý tưởng, dấu hiệu cho phép ký hiệu này sẽ có thể làm việc trong môi trường tỉ lệ tín hiệu trên tạp nhiễu tương đối thấp.

Một vài hệ thống sử dụng giao thức bảo mật/mã hóa nổi tiếng trên các lớp cao hơn để hỗ trợ sự bảo mật. Tuy nhiên, nó bao gồm một vài tài nguyên lập lịch lớp cao hơn, và dẫn đến sự trì hoãn xử lý dài. Hơn nữa, thuật toán lập lịch lớp cao hơn có thể không cung cấp đủ chức năng chống nhiễu ở điều kiện SNR tương đối thấp.

Để khắc phục các nhược điểm của các phương pháp bao gồm các tài nguyên lập lịch lớp cao hơn, phương pháp khác sử dụng các thông số FEC dựa vào ký hiệu ở lớp vật lý. Ví dụ, việc đan xen hoặc tỉa của mã Turbo được thực hiện chức năng của ký hiệu. Theo ví dụ khác, ma trận LDPC bằng cách nào đó là chức năng của ký hiệu. Các phương pháp này có xu hướng không những có tác động tiêu cực lên hiệu suất FEC mà còn làm tăng độ phức tạp của bộ giải mã và độ trễ xử lý. Hơn nữa, không gian ký hiệu của chúng thường chứa số lượng rất hạn chế của các ký hiệu và có thể được giải mã bởi thuật toán.

Phương pháp khác bao gồm sự sử dụng của việc giả xáo trộn dựa vào ký hiệu ở lớp vật lý. Phương pháp này yêu cầu thêm các tài nguyên (tính toán và đệm) để giải xáo trộn và có thể khiến độ trễ xử lý tăng lên.

Theo một vài trường hợp, ký hiệu có thể là sự kết hợp của nhiều ký hiệu mà bao gồm ký hiệu nhóm và ký hiệu cá nhân. Theo trường hợp này, một phần của khối dữ liệu được kết hợp với ký hiệu nhóm có thể được giải mã bởi tất cả các bộ thu của nhóm. Một phần của khối dữ liệu được kết hợp với ký hiệu cá nhân có thể chỉ được giải mã bởi bộ thu này của nhóm này.

Các phương pháp để đạt được nhiều ký hiệu bao gồm việc lập lịch lớp cao hơn, và vì vậy sử dụng nhiều tài nguyên hơn cho việc lập lịch lớp cao và có thể dẫn đến thời gian xử lý dài. Ngoài ra, phương pháp này sẽ chia khối dữ liệu dài thành nhiều khối dữ liệu nhỏ hơn. Tuy nhiên, việc tách biệt khối thành nhiều khối nhỏ hơn có thể khiến hiệu suất FEC (BLER so với SNR) giảm xuống do các khối nhỏ hơn (Turbo và LDPC).

Phương án của sáng chế đề xuất mã cực được cho phép ký hiệu đơn. Theo một vài phương án, các bit kiểm tra dư vòng (CRC - Cyclic redundancy check) được bao gồm trong vectơ đầu vào để hỗ trợ việc giải mã. Các bit CRC được tạo ra dựa vào các bit thông tin được truyền. Các bit CRC được bao gồm trong các vị trí tin cậy (nghĩa là, các vị trí với kênh tin cậy). Các bit CRC có thể được bổ sung để nâng cao hiệu suất mã cực cho độ dài khối từ ngắn đến trung bình. Đối với bộ mã hóa cực độ dài khối rất dài, CRC có thể là không cần thiết. Mã cực được cho phép ký hiệu với các bit CRC ở đây được gọi là mã cực được cho phép ký hiệu được kiểm tra CRC. Mặc dù phương án với CRC được bộc lộ ở đây, tổng quát hơn, theo các phương án khác, một vài bit kiểm tra chẵn lẻ dùng cho việc phát hiện lỗi và/hoặc việc phát hiện có thể được bao gồm trong các vị trí bit tương đối tin cậy.

Dựa vào Fig.3, thể hiện lưu đồ của phương pháp về việc thực hiện mã cực được cho phép ký hiệu được kiểm tra CRC cho việc thực hiện bởi bộ mã hóa. Ở khối 200, K bit khối thông tin để mã hóa được thu hoặc nếu không được chứa. Ở khối 202, u bit CRC được tính toán và được chèn để tạo ra vectơ với K bit khối thông tin, và u bit CRC ở 204. Ở 206, M bit ký hiệu được chèn, và N-K-u-M bit phong tỏa được chèn để tạo ra N bit vectơ đầu vào 208 với K bit khối thông tin, và u bit CRC, M bit ký hiệu và N-K-u-M bit phong tỏa, trong đó N là luỹ thừa của 2. Vectơ 208 sau đó được nhân với ma trận tích Kronecker ở 210 để tạo ra N bit từ mã được đưa ra (hoặc được lưu trữ) ở khối 212. Ma trận tích Kronecker là $\mathbf{G_2}^{\otimes m}$, trong đó $N = 2^m$.

Các bit thông tin và các bit CRC được chèn vào từ mã ở các vị trí tương ứng với các vị trí bit tin cậy dùng cho mã cực. Các bit CRC không cần tới tất cả cùng nhau hoặc cuối cùng, miễn là bộ truyền và bộ thu biết các vị trí của các bit CRC và các bit thông tin. Tương tự như vậy, các bit phong tỏa và các bit ký hiệu được chèn vào các vị trí bit không tin cậy dùng cho mã cực. Theo một vài phương án, tất cả các vị trí bit phong tỏa được sử dụng cho các bit ký hiệu.

Các độ dài ký hiệu khác nhau có thể được sử dụng. Độ dài của ký hiệu có thể là hàng chục bit lên đến hàng trăm bit. Ký hiệu càng dài, nó có thể cung cấp bảo mật càng nhiều. Ký hiệu có thể đủ dài sao cho có hàng nghìn hoặc thậm chí hàng triệu ký hiệu duy nhất.

Fig.4 thể hiện trường hợp ví dụ trong đó phương án trên Fig.3 có thể được sử dụng, trong đó bộ truyền 350 (Thiết bị người dùng của Alice (UE - User equipment)) có dữ liệu đúng mục tiêu cho việc thu bởi bộ thu đúng mục tiêu 352 (UE của Bob) và không muốn bộ thu không đúng mục tiêu 354 (UE của Carol) có thể giải mã dữ liệu. Khối dữ liệu 356 dùng cho UE của Bob 352 được truyền qua không khí sau khi việc mã hóa cực cho phép ký hiệu được kiểm tra CRC. Bằng cách chỉ thông báo bộ thu đúng mục tiêu về các bit ký hiệu, bộ thu không đúng mục tiêu sẽ không thể giải mã dữ liệu.

Cách thực hiện ví dụ được mô tả trên Fig.7, trong đó N=16, K=8, u=2, và M=3, và có ba bit phong tỏa cho tốc độ mã hóa 0,5. Các bit ký hiệu được chèn ở các vị trí bit 0, 1 và 2. Các bit phong tỏa được chèn ở các vị trí 4, 9 và 12, các bit thông tin ở các vị trí 3, 5, 6, 7, 8, 10, 11, 13, và các bit CRC ở các vị trí 14 và 15.

Bộ giải mã cực được cho phép ký hiệu được kiểm tra CRC không yêu cầu độ phức tạp thêm đáng kể so với bộ giải mã cực thông thường. Bộ giải mã sử dụng các bit ký hiệu để giải mã các bit thông tin bằng các cách giống như các bit phong tỏa được sử dụng trong các bộ giải mã cực thông thường. Không có sự nhận biết của các bit ký hiệu này, bộ giải mã gần như không thể giải mã các bit thông tin một cách thành công. Không có sự suy giảm hiệu suất BER/BLER do

sự có mặt của các bit ký hiệu, như được xác nhận bởi cả lý thuyết và sự mô phỏng. Ngoài ra, có thể có khả năng điều chỉnh lỗi và chống nhiễu mạnh.

Trong trường hợp trong đó khối dữ liệu có số lượng lớn các bit (ví dụ, theo thứ tự của hàng nghìn bit) với R=1/2~1/3, có chỗ để chèn hàng trăm hoặc thậm chí hàng nghìn bit ký hiệu, dẫn đến khả năng cản trở và bảo mật mạnh.

Fig.8A thể hiện việc giải mã hủy bỏ liên tiếp đối với mã cực có tất cả bit đóng băng (nghĩa là, mã cực với các bit phong tỏa nhưng không có các bit ký hiệu nào).

Fig.6 thể hiện lưu đồ của phương pháp dùng cho cách thực hiện trong bộ giải mã về việc giải mã hủy bỏ liên tiếp dùng cho từ mã cực cho phép ký hiệu được kiểm tra CRC có N bit ở các vị trí bit i = 0 đến N-1. Phương pháp bắt đầu ở khối 300 với việc thu nhận thông tin bit phong tỏa và thông tin bit ký hiệu. Thông tin này chỉ ra các vị trí M bit đóng băng (Đóng băng được thiết đặt), và các vị trí K bit ký hiệu (Ký hiệu được thiết đặt), và các trị số của các bit phong tỏa (các bit phong tỏa thường không là bộ thu cụ thể, $Frozen_m$, m =0 đến M-1, thường không cho tất cả các bộ thu), và các bit ký hiệu (ký $hiệu_k$, k= 0, K-1, bộ thu cụ thể). Thông tin này được thu nhận tách biệt với từ mã thu được. Ví dụ, thông tin này có thể được truyền thông bởi bộ truyền tới bộ thu trong khi thiết lập kết nối ban đầu. Theo ví dụ cụ thể, N=16, M=3 và K=3, và các bit phong tỏa ở các vị trí 4, 9 và 12 và có các trị số 0,0,0, và các bit ký hiệu ở các vị trí 0, 1, 2 và có các trị số 1,0,0, như được chỉ ra ở 302. Việc giải mã bắt đầu ở vị trí bit 0, bằng cách thiết đặt chỉ số i = 0 ở khối 304. Ở khối 306, nếu chỉ số i là chỉ số của vị trí bit ký hiệu, sau đó $\widehat{u_i}$ được thiết đặt tới trị số bit ký hiệu đã biết tương ứng. Ở khối 308, nếu chỉ số i là chỉ số của vị trí bit phong tỏa, sau đó $\widehat{u_i}$ được thiết đặt tới trị số bit đóng băng đã biết tương ứng. Ở khối 310, nếu chỉ số I không là chỉ số của vị trí bit ký hiệu hoặc vị trí bit phong tỏa, sau đó vị trí bit được giải mã tới trị số của 0 hoặc 1, ví dụ sử dụng thao tác so sánh đường dẫn. Nếu chỉ số i bằng N-1 ở khối 312, sau đó phương pháp kết thúc. Nếu không, chỉ số i được tăng lên ở khối 314 và phương pháp tiếp tục quay lại ở khối 306.

Các bit CRC được xem như các bit dữ liệu ở bộ giải mã ở các khối từ 300 đến 314. Tiếp theo, khi tất cả các bit được giải mã bao gồm các bit dữ liệu và các bit CRC, việc kiểm tra CRC được thực hiện ở khối 316. Nếu việc kiểm tra CRC thành công sau đó các bit dữ liệu được giải mã chính xác với xác suất cao.

Có thể nhận thấy rằng khối so sánh đường dẫn 310 được thực hiện chỉ cho các bit mà hoặc không là các bit đóng băng hoặc không là các bit ký hiệu. Cách tiếp cận trên Fig.6 không tùy thuộc vào ký hiệu cụ thể và các vị trí bit phong tỏa.

Phương án khác của sáng chế đề xuất bộ mã hóa cực cho phép nhiều ký hiệu được kiểm tra CRC. Với bộ mã hóa như vậy, nhiều ký hiệu được chèn, và các bộ thu khác nhau có thể giải mã các tập hợp con dữ liệu khác nhau tùy thuộc vào sự nhận biết của chúng của các ký hiệu.

Dựa vào Fig.7A, bắt đầu ở khối 400, K1 bit khối thông tin thứ nhất và K2 bit khối thông tin thứ nhất được thu nhận. Ở 402 u1 bit CRC thứ nhất được tính toán dựa vào K1 bit khối thông tin thứ nhất, và u2 bit CRC thứ hai được tính toán dựa vào K2 bit khối thông tin thứ nhất để tạo ra vectơ 404 với K1 bit khối thông tin thứ nhất, và u1 bit CRC thứ nhất, K2 bit khối thông tin thứ nhất, và u2 bit CRC thứ hai. Ở 406, M1 bit ký hiệu thứ nhất được chèn trước K1 bit khối thông tin thứ nhất, và M2 bit ký hiệu thứ hai được chèn sau K1 bit khối thông tin thứ nhất và u1 bit CRC thứ nhất và trước K2 bit khối thông tin thứ nhất. Ngoài ra, N-K1-u1-M1-K2-u2-M2 bit phong tỏa được chèn để tạo ra N bit vectơ đầu vào 408 trong đó N là luỹ thừa của 2. Vectơ 408 sau đó được nhân với ma trận tích Kronecker ở khối 410 để tạo ra N bit từ mã mà được đưa ra (hoặc được lưu trữ) ở khối 412.

Bộ thu với sự nhận biết của chỉ M1 bit ký hiệu thứ nhất có thể chỉ giải mã các bit của K1 bit khối thông tin thứ nhất. Nó không thể giải mã các bit của K2 bit khối thông tin thứ hai. Bộ thu với sự nhận biết của cả M1 bit ký hiệu thứ nhất và M2 bit ký hiệu thứ hai có thể giải mã tất cả các bit thông tin. Cách tiếp cận giải mã giống như cách tiếp cận 402 trên Fig.8, nhưng bộ thu mà không có tất cả

các bit ký hiệu sẽ dừng việc giải mã cho các vị trí bit tiếp theo vị trí chứa bit ký hiệu không được biết.

Fig.7B thể hiện trường hợp ví dụ trong đó phương án trên Fig.9A có thể được sử dụng, trong đó bộ truyền 950 (UE của Alice) có dữ liệu 960 đúng mục tiêu cho việc thu bởi bộ thu thứ nhất 952 (UE của Bob) và muốn chỉ một vài trong số dữ liệu 962 được giải mã bởi bộ thu thứ hai 954 (UE của Carol) sao cho phần còn lại của dữ liệu 964 có thể chỉ được giải mã bởi bộ thu thứ nhất 952. Bằng cách thông báo bộ thu đúng mục tiêu (UE của Bob theo ví dụ trên Fig.9B) về tất cả các bit ký hiệu, bộ thu đúng mục tiêu có thể giải mã tất cả dữ liệu 960. Bằng cách chỉ thông báo bộ thu (UE của Carol theo ví dụ trên Fig.9B) về chỉ ký hiệu thứ nhất, bộ thu có thể chỉ giải mã phần thứ nhất 962 của dữ liệu 960.

Nhiều cách tiếp cận ký hiệu có thể được dễ dàng kéo dài để chứa được P>=2 khối thông tin, bằng cách tạo ra vectơ đầu vào với các phần P, mỗi phần chứa các bit ký hiệu tương ứng, một trong số các khối thông tin với ít nhất một bit phong tỏa được chèn, và CRC qua khối thông tin.

Ví dụ cụ thể về bộ mã hóa mà sử dụng các ký hiệu được mô tả trên Fig.8, trong đó N=16, K1=3, u1=2, M1=3, và K2=3, u2=2 và M2=1. Đối với khối thông tin thứ nhất, các bit 0,1,2 chứa M1 bit ký hiệu thứ nhất. Các bit 3,5,6 chứa K1 bit thông tin. Các bit 7 và 8 chứa u1 bit CRC, và bit 4 là bit phong tỏa. Đối với khối thông tin thứ hai, bit 9 chứa M2 bit ký hiệu thứ hai. Các bit 10,11,13 chứa K2 bit thông tin. Các bit 14 và 15 chứa u2 bit CRC, và bit 12 là bit phong tỏa.

Các ưu điểm của mã cực được cho phép ký hiệu được kiểm tra CRC mà có thể được thực hiện theo một vài cách thực hiện bao gồm:

không bao gồm việc mã hóa lớp cao và giao thức lập lịch để đạt được sự truyền thông cho phép ký hiệu;

không có tài nguyên tính toán thêm nào được bổ sung để hỗ trợ việc phát hiện ký hiệu;

không có độ trễ thêm nào được bổ sung để phát hiện ký hiệu;

không có tổn thất hiệu suất BER/BLER cực nào do sự có mặt của ký hiệu;

sự có mặt của ký hiệu và kích cỡ của ký hiệu khó để phát hiện;

kích cỡ ký hiệu lớn có thể chứa được;

nhiều ký hiệu được hỗ trợ với mỗi ký hiệu được kết hợp với một phần của thông tin.

Mã cực được cho phép ký hiệu được kiểm tra CRC có thể hoàn toàn được xác định rõ bởi tám bộ dữ liệu (N, K, F, $\boldsymbol{vF}$, S, $\boldsymbol{vS}$, C, $\boldsymbol{vC}$), trong đó:

N là độ dài mã trong các bit (hoặc độ dài khối),

K là số lượng của các bit thông tin được mã hóa mỗi từ mã (hoặc kích thước mã);

vF là vectơ nhị phân có độ dài Nf (các bit phong tỏa) và F là tập hợp con của các chỉ số N − K từ {0, 1, . . ., N − 1} (các vị trí bit phong tỏa).

vS là vectơ nhị phân có độ dài Ns (các bit ký hiệu) và S là tập hợp con của các chỉ số N − K từ {0, 1, . . ., N − 1} (các vị trí bit ký hiệu).

vC là vectơ nhị phân có độ dài Nc (các bit CRC) và C là tập hợp con của các chỉ số N − K từ {0, 1, . . ., N − 1} (các vị trí bit CRC)

trong đó Nf + Ns + Nc = N-K

và lưu ý I = {0, 1, . . ., N − 1}\(F,S,C) tương ứng với các chỉ số bit thông tin.

Trong phần trên, các vị trí bit K + C tương ứng với các vị trí bit tin cậy dùng cho mã cực, và các vị trí bit Nf + Nc tương ứng với các vị trí bit không tin cậy dùng cho mã cực. Cách thực hiện không có CRC đạt được nhờ sử dụng tất cả các vị trí bit tin cậy như các bit thông tin. Cách thực hiện không có các bit phong tỏa đạt được nhờ sử dụng tất cả các vị trí bit không tin cậy như các bit ký hiệu, mặc dù cần lưu ý rằng các bit ký hiệu có chức năng giống như các bit phong tỏa; sự khác nhau là không phải tất cả các bộ thu nhận biết được các bit ký hiệu.

Được đưa ra bất kỳ tập hợp con nào của các chỉ số từ vectơ **x**, vectơ con tương ứng được biểu thị là $\mathbf{x}_A$.

Đối với mã cực (N, K, *F*, **vF**, *S*, **vS**, *C*, **vC**), thao tác mã hóa cho vectơ của các bit thông tin u có độ dài K tới đây sẽ được mô tả. Để m = log2 (N) và $\mathbf{G} = \mathbf{F}^{\otimes n} = \mathbf{F} \otimes \cdots \otimes \mathbf{F}$ là tích Kronecker gập m của ma trận hạt nhân **F**, Trong đó F là $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Tiếp theo, từ mã được tạo ra là

$\boldsymbol{x} = \mathbf{G}\,\mathbf{d}$ trong đó **d** là vectơ cột $\in \{0, 1\}^N$ sao cho $\mathbf{d}_F = \mathbf{vF}$ và $\mathbf{d}_I = \mathbf{u}$, $\mathbf{d}_C = \mathbf{vC}$ và $\mathbf{d}_S = \mathbf{vS}$.

hoặc $\boldsymbol{x} = \mathbf{d}\,\mathbf{G}^T$ trong đó $()^T$ chỉ ra ma trận chuyển vị, và **d** là vectơ hàng $\in \{0, 1\}^N$ sao cho $\mathbf{d}_F = \mathbf{vF}$ và $\mathbf{d}_I = \mathbf{u}$, $\mathbf{d}_C = \mathbf{vC}$ và $\mathbf{d}_S = \mathbf{vS}$.

Một cách tương đương, nếu ma trận hạt nhân như các ví dụ nêu trên,

$\boldsymbol{x} = \mathbf{d}\,\mathbf{G}$ và **d** là vectơ hàng $\in \{0, 1\}^N$ sao cho $\mathbf{d}_F = \mathbf{vF}$ và $\mathbf{d}_I = \mathbf{u}$, $\mathbf{d}_C = \mathbf{vC}$ và $\mathbf{d}_S = \mathbf{vS}$.

Ở các mã cực mà không cho phép ký hiệu, sự lựa chọn của tập hợp F của các vị trí bit phong tỏa (nghĩa là, các vị trí bit không tin cậy) là bước trong việc mã hóa cực thường được gọi là sự xây dựng mã cực. Ví dụ, tham chiếu tới bài báo của Arikan, được đề cập trước đó. Tổng quát hơn, bất kỳ phương pháp nào lựa chọn tập hợp của các vị trí bit tạp âm mã cực có thể được sử dụng thay vì lựa chọn tập hợp của các vị trí mà sẽ được sử dụng cho các bit ký hiệu, hoặc các bit ký hiệu và các bit phong tỏa. Như được lưu ý trước đó, trong một vài trường hợp, tất cả các vị trí bit phong tỏa được sử dụng cho các bit ký hiệu. Ứng dụng này không giới hạn ở vị trí bit phong tỏa/các vị trí bit ký hiệu cụ thể. Tuy nhiên, nằm trong tập hợp của các vị trí vì vậy được lựa chọn, bit ký hiệu được đưa ra cần được bao gồm trước khi các bit thông tin được kết hợp với bit ký hiệu được đưa ra. Ngoài ra, các bit CRC, khi được bao gồm, được đặt ở các vị trí bit tin cậy mã cực. Ma trận tích Kronecker dựa vào ma trận hạt nhân cụ thể được đề cập ở trên là ví dụ cụ thể về ma trận sinh mã cực. Tổng quát hơn, bất kỳ ma trận sinh

mã cực nào có thể được sử dụng mà tạo ra các từ mã với các vị trí tin cậy và không tin cậy. Theo một vài phương án, ma trận sinh mã cực được dựa vào ma trận tích Kronecker của ma trận hạt nhân khác. Ví dụ, ma trận hạt nhân có thể là ma trận các kích thước số nguyên tố, chẳng hạn như 3x3 hoặc 5x5. Ma trận hạt nhân có thể là nhị phân hoặc không là nhị phân.

Tổng quát hơn, bất kỳ phương pháp mã hóa nào mà về mặt toán học tương đương với các phương pháp được mô tả có thể được sử dụng. Ví dụ, khi tập hợp của các từ mã được xác định như được mô tả ở đây, nhiều cấu trúc bộ mã hóa khác nhau được biết trong lĩnh vực kỹ thuật có thể được sử dụng để mã hóa dữ liệu đầu vào để tạo ra các từ mã. Thông thường, bộ mã hóa được mô tả ở đây được bao gồm như một phần của thiết bị mà bao gồm các bộ phận khác. Các bộ phận này có thể, ví dụ, bao gồm bộ điều biến để điều biến các bit được đưa ra bởi bộ mã hóa để tạo ra các ký hiệu, và bộ truyền để truyền các ký hiệu qua kênh chẳng hạn như kênh không dây. Chức năng ngược tương tự sẽ ở bộ thu cùng với bộ giải mã.

Fig.9 là sơ đồ khối của thiết bị để thu và giải mã các từ mã. Thiết bị 1100 bao gồm bộ thu 1104 được ghép nối với anten 1102 để thu các tín hiệu từ kênh không dây, và bộ giải mã 1106. Bộ nhớ 1108 được ghép nối với bộ giải mã 1106. Theo một vài phương án, bộ thu 1104 bao gồm bộ giải điều biến, bộ khuếch đại, và/hoặc các bộ phận khác của chuỗi thu RF. Bộ thu 1104 thu, qua anten 1102, từ mà dựa vào từ mã của mã cực. Các bit được giải mã được đưa ra ở 1120 để xử lý thu thêm.

Bộ giải mã 1106 được thực hiện trong hệ mạch, chẳng hạn như xử lý hoặc, nó được tạo cấu hình để đánh giá các bit trong từ thu được như được bộc lộ ở đây. Bộ nhớ 1108 có thể bao gồm một hoặc nhiều thiết bị bộ nhớ trạng thái rắn và/hoặc các thiết bị bộ nhớ với vật ghi có thể di động và di chuyển được. Theo cách thực hiện dựa vào bộ xử lý của bộ giải mã 1106, các lệnh thực hiện được bởi bộ xử lý để tạo cấu hình bộ xử lý để thực hiện các thao tác giải mã được lưu trữ trong phương tiện đọc được bởi bộ xử lý bất biến. Phương tiện bất biến có

thể bao gồm (các) thiết bị bộ nhớ giống nhau được sử dụng cho bộ nhớ 1108, hoặc một hoặc nhiều thiết bị bộ nhớ tách biệt. Phương pháp giải mã trên Fig.6 thể hiện một cách thực hiện có thể của bộ giải mã 1106 và bộ nhớ 1108.

Bộ nhớ 1008 có thể được sử dụng để lưu trữ các kết quả xử lý bởi các thành phần xử lý của bộ giải mã 1106. Bộ giải mã 1106 cũng có thể bao gồm bộ ghép kênh địa chỉ được ghép nối giữa các thành phần xử lý và bộ nhớ 1008. Theo phương án, bộ giải mã 1106 được tạo cấu hình để lưu trữ các kết quả xử lý bởi các thành phần xử lý tới các vùng bộ nhớ tương ứng trong bộ nhớ 1008 mà mỗi vùng có thể truy cập để cung cấp, theo thao tác truy cập bộ nhớ đơn, các đầu vào tới mỗi trong số các thành phần xử lý dùng cho các phép tính toán tiếp theo. Các phương án khác còn có thể bao gồm, ít hơn, hoặc các bộ phận khác nhau và/hoặc các sự thay đổi về thao tác thu các bộ phận thiết bị.

Theo ví dụ cụ thể, bộ giải mã 1106 bao gồm bộ giải mã mã cực 1116 được tạo cấu hình để thực hiện việc giải mã mã cực của từ mã thu được bằng cách xử lý ít nhất một bit ký hiệu như bit phong tỏa có trị số bit ký hiệu đã biết. Thiết bị có thể được tạo cấu hình để thu thông tin trên các bit ký hiệu được sử dụng trong mã cực được cho phép ký hiệu tách biệt với việc thu từ mã. Trong khi CRC được sử dụng, bộ giải mã 1106 bao gồm bộ kiểm tra CRC 1112 được tạo cấu hình để xác nhận kết quả của việc giải mã nhờ sử dụng việc kiểm tra CRC.

Fig.10 là sơ đồ khối của thiết bị ví dụ để mã hóa và truyền các từ mã. Thiết bị 1200 bao gồm bộ mã hóa 1204 được ghép nối với bộ truyền 1206. Bộ mã hóa 1204 được thực hiện trong hệ mạch mà được tạo cấu hình để mã hóa dòng bit đầu vào 1202 nhờ sử dụng mã cực được cho phép ký hiệu, hoặc mã cực được cho phép ký hiệu được kiểm tra CRC. Theo phương án được minh họa, thiết bị 1200 cũng bao gồm anten 1208, được ghép nối với bộ truyền 1206, để truyền các tín hiệu qua kênh không dây. Theo một vài phương án, bộ truyền 1206 bao gồm bộ điều biến, bộ khuếch đại, và/hoặc các bộ phận khác của chuỗi truyền RF.

Theo một vài phương án, thiết bị 1200, và tương tự như vậy thiết bị 1100 trên Fig.11, bao gồm phương tiện đọc được bởi máy tính bất biến mà bao gồm các lệnh dùng cho việc thực hiện bởi bộ xử lý để thực hiện và/hoặc điều khiển thao tác của bộ mã hóa 1204 trên Fig.12, để thực hiện và/hoặc điều khiển thao tác của bộ giải mã 1106 trên Fig.11, và/hoặc nếu không điều khiển việc thực hiện của các phương pháp được mô tả ở đây. Theo một vài phương án, bộ xử lý có thể là bộ phận của nền tảng (platform) phần cứng dùng cho mục đích chung. Theo các phương án khác, bộ xử lý có thể là bộ phận của nền phần cứng chuyên dụng. Ví dụ, bộ xử lý có thể là bộ xử lý được nhúng, và các lệnh có thể được cung cấp như phần sụn. Một vài phương án có thể được thực hiện nhờ sử dụng chỉ phần cứng. Theo một vài phương án, các lệnh dùng cho việc thực hiện bởi bộ xử lý có thể được bao gồm dưới dạng sản phẩm phần mềm. Sản phẩm phần mềm có thể được lưu trữ trong vật ghi bất khả biến hoặc bất biến, mà có thể là, ví dụ, bộ nhớ chỉ đọc dạng đĩa nén (CD-ROM - compact disc read-only memory), đĩa chớp dạng kênh truyền nối tiếp đa năng (USB - universal serial bus), hoặc đĩa cứng di động.

Thiết bị truyền thông có thể bao gồm thiết bị 1100, thiết bị 1200, hoặc cả bộ truyền và bộ thu và cả bộ mã hóa và bộ giải mã. Thiết bị truyền thông như vậy có thể là thiết bị người dùng hoặc thiết bị mạng truyền thông. Theo ví dụ cụ thể, bộ mã hóa 1204 bao gồm bộ tạo vectơ đầu vào 1210 được tạo cấu hình để tạo ra N bit vectơ đầu vào cho việc mã hóa cực, vectơ đầu vào có các vị trí bit tin cậy mã cực và các vị trí bit không tin cậy mã cực bằng cách chèn mỗi trong số ít nhất một bit thông tin vào vị trí bit tin cậy mã cực tương ứng, và mỗi trong số ít nhất một bit ký hiệu vào vị trí bit không tin cậy mã cực tương ứng, trong đó $N = 2^m$ trong đó m>=2. Bộ mã hóa 1202 cũng bao gồm bộ mã hóa mã cực 1214 được tạo cấu hình để nhân vectơ đầu vào với ma trận sinh mã cực để tạo ra từ mã cực cho phép ký hiệu. Bộ truyền 1206 truyền từ mã cực cho phép ký hiệu. Ngoài ra, hoặc hơn nữa, có thể có bộ nhớ (không được thể hiện) để lưu trữ từ mã cực cho phép ký hiệu.

Theo các phương án mà bao gồm CRC, thiết bị cũng bao gồm bộ xử lý CRC 1214 được tạo cấu hình để xử lý K bit thông tin để tạo ra u bit CRC, trong đó u >=1. Trong trường hợp này, bộ tạo vectơ đầu vào 1210 tạo ra N bit vectơ đầu vào bằng cách chèn mỗi trong số u bit CRC ở vị trí bit tin cậy mã cực tương ứng.

Theo một vài phương án, bộ tạo ra vectơ đầu vào sử dụng nhiều cách tiếp cận ký hiệu được mô tả trước đó, có hoặc không có CRC.

Theo ví dụ của sáng chế, phương pháp theo bộ mã hóa được bộc lộ. Theo ví dụ thứ nhất, phương pháp này bao gồm bước tạo ra N bit vectơ đầu vào cho việc mã hóa cực, vectơ đầu vào có các vị trí bit tin cậy mã cực và các vị trí bit không tin cậy mã cực, bằng cách chèn mỗi trong số ít nhất một bit thông tin vào vị trí bit tin cậy mã cực tương ứng, và mỗi trong số ít nhất một bit ký hiệu vào vị trí bit không tin cậy mã cực tương ứng, trong đó $N = 2^m$ trong đó m>=2; nhân N bit vectơ đầu vào với ma trận sinh mã cực để tạo ra từ mã mã cực; và bước truyền hoặc lưu trữ từ mã mã cực.

Theo ví dụ thứ hai, phương pháp của ví dụ nêu trên được đề xuất trong đó việc nhân N bit vectơ đầu vào với ma trận sinh mã cực để tạo ra từ mã mã cực bao gồm bước: xử lý N bit vectơ đầu vào để tạo ra kết quả tương đương với phép nhân vectơ đầu vào như vectơ hàng với ma trận tích Kronecker gập m $\mathbf{G_2}^{\otimes m}$, trong đó $\mathbf{G_2} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ để tạo ra từ mã cực hoặc nó tương đương với việc nhân ma trận tích Kronecker gập m $\mathbf{G_2}^{\otimes m}$ với vectơ đầu vào như vectơ cột, trong đó $\mathbf{G_2} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ để tạo ra từ mã cực.

Theo ví dụ thứ ba, phương pháp của ví dụ bất kỳ trong số các ví dụ nêu trên được đề xuất trong đó ít nhất một bit thông tin bao gồm K bit thông tin, K>=1, phương pháp này còn bao gồm bước: xử lý K bit thông tin để tạo ra u-bit CRC, trong đó u >=1; và tạo ra N bit vectơ đầu vào bằng cách chèn mỗi trong số u bit CRC ở vị trí bit tin cậy mã cực tương ứng, sao cho từ mã cực là từ mã cực được kiểm tra CRC.

Theo ví dụ thứ tư, phương pháp của ví dụ bất kỳ trong số các ví dụ nêu trên còn bao gồm bước chèn ít nhất một bit phong tỏa ở vị trí bit không tin cậy mã cực.

Theo ví dụ thứ năm, phương pháp của ví dụ bất kỳ trong số các ví dụ nêu trên được đề xuất trong đó N bit vectơ đầu vào có M bit ký hiệu, K bit thông tin, u bit CRC với ít nhất một bit phong tỏa, trong đó $N = 2^m$ trong đó m>=2, và số lượng các bit phong tỏa là N-K-u-M.

Theo ví dụ thứ sáu, phương pháp của ví dụ bất kỳ trong số các ví dụ nêu trên còn bao gồm bước truyền thông ít nhất một bit ký hiệu tới bộ thu một cách tách biệt từ sự truyền của từ mã.

Theo ví dụ thứ bảy, phương pháp này bao gồm bước tạo ra vectơ đầu vào bằng cách: đối với mỗi trong số P khối thông tin, trong đó P>=2, tạo ra phần tương ứng của vectơ đầu vào, phần tương ứng bắt đầu với tập hợp tương ứng của ít nhất một bit ký hiệu và cũng chứa khối thông tin, mỗi trong số các tập hợp của các bit ký hiệu khác với nhau; và kết hợp các phần tương ứng để tạo ra vectơ đầu vào; nhân vectơ đầu vào với ma trận sinh mã cực để tạo ra từ mã mã cực; và truyền hoặc lưu trữ từ mã.

Theo ví dụ thứ tám, phương pháp của ví dụ nêu trên được đề xuất trong đó việc tạo ra vectơ đầu vào còn bao gồm bước: xử lý mỗi khối thông tin để tạo ra tập hợp tương ứng của các bit CRC; và, đối với mỗi trong số các khối thông tin P, bao gồm tập hợp tương ứng của các bit CRC trong phần tương ứng của vectơ đầu vào.

Theo ví dụ thứ chín, phương pháp của ví dụ nêu trên được đề xuất trong đó P=2, và trong đó việc xử lý mỗi khối thông tin để tạo ra tập hợp tương ứng của các bit CRC bao gồm các bước: xử lý K1 bit thông tin để tạo ra u1 bit CRC; và xử lý K2 bit thông tin để tạo ra u2 bit CRC; sao cho vectơ đầu vào bao gồm: N bit vectơ đầu vào với phần thứ nhất chứa M1 bit ký hiệu, K1 bit thông tin, và u1 bit CRC và ít nhất một bit phong tỏa, và với phần thứ hai chứa M2 bit ký hiệu,

K2 bit thông tin, u2 bit CRC và ít nhất một bit phong tỏa, trong đó N = 2^m trong đó m>=3.

Theo ví dụ thứ mười, phương pháp của ví dụ nêu trên còn bao gồm các bước: chuyển M1 bit ký hiệu tới bộ thu thứ nhất; và chuyển M1 bit ký hiệu và M2 bit ký hiệu tới bộ thu thứ hai.

Theo ví dụ thứ mười một, phương pháp theo bộ giải mã bao gồm các bước: thu từ mã mà đã được mã hóa với mã cực trong đó ít nhất một bit phong tỏa được thay bằng ít nhất một bit ký hiệu tương ứng cụ thể tới bộ giải mã và được biết tới bộ giải mã tách biệt với việc thu từ mã; và thực hiện việc giải mã của từ mã thu được bằng cách thiết đặt ít nhất một bit phong tỏa để bằng ít nhất một trị số bit ký hiệu tương ứng.

Theo ví dụ thứ mười hai, phương pháp của ví dụ nêu trên còn bao gồm bước thu thông tin trên các bit ký hiệu được sử dụng trong mã cực tách biệt với việc thu từ mã.

Theo ví dụ thứ mười ba, phương pháp của ví dụ nêu trên được đề xuất trong đó từ mã đã được mã hóa với mã cực được cho phép ký hiệu được kiểm tra CRC, và trong đó phương pháp này còn bao gồm bước xác nhận kết quả của việc giải mã nhờ sử dụng việc kiểm tra CRC.

Theo ví dụ thứ mười bốn, thiết bị bao gồm: bộ tạo vectơ đầu vào được tạo cấu hình để tạo ra N bit vectơ đầu vào cho việc mã hóa cực, vectơ đầu vào có các vị trí bit tin cậy mã cực và các vị trí bit không tin cậy mã cực, bằng cách chèn mỗi trong số ít nhất một bit thông tin vào vị trí bit tin cậy mã cực tương ứng, và mỗi trong số ít nhất một bit ký hiệu vào vị trí bit không tin cậy mã cực tương ứng, trong đó $N = 2^m$ trong đó m>=2; bộ mã hóa mã cực được tạo cấu hình để nhân vectơ đầu vào với ma trận sinh mã cực để tạo ra từ mã cực.

Theo ví dụ thứ mười lăm, thiết bị của ví dụ nêu trên còn bao gồm bộ truyền để truyền từ mã cực, hoặc bộ nhớ để lưu trữ từ mã cực.

Theo ví dụ thứ mười sáu, thiết bị của ví dụ nêu trên được đề xuất trong đó ít nhất một bit thông tin bao gồm K bit thông tin, K>=1, thiết bị này còn bao

gồm: bộ xử lý CRC được tạo cấu hình để xử lý K bit thông tin để tạo ra u bit CRC, trong đó u >=1; trong đó bộ tạo vectơ đầu vào tạo ra N bit vectơ đầu vào bằng cách chèn mỗi trong số u bit CRC ở vị trí bit tin cậy mã cực tương ứng.

Theo ví dụ thứ mười bảy, thiết bị của ví dụ nêu trên được đề xuất trong đó N bit vectơ đầu vào có M bit ký hiệu, K bit thông tin, u bit CRC với ít nhất một bit phong tỏa, trong đó $N = 2^m$ trong đó m>=2 , và số lượng của các bit phong tỏa là N-K-u-M.

Theo ví dụ thứ mười tám, thiết bị của ví dụ nêu trên được đề xuất trong đó bộ truyền được tạo cấu hình để chuyển ít nhất một M bit ký hiệu tới bộ thu một cách tách biệt từ sự truyền của từ mã.

Theo ví dụ thứ mười chín, thiết bị bao gồm: bộ tạo vectơ đầu vào được tạo cấu hình để tạo ra N bit vectơ đầu vào cho việc mã hóa cực bằng cách: đối với mỗi trong số các khối thông tin P, trong đó P>=2, tạo ra phần tương ứng của vectơ đầu vào, phần tương ứng bắt đầu với tập hợp tương ứng của ít nhất một bit ký hiệu và cũng chứa khối thông tin, mỗi trong số các tập hợp của các bit ký hiệu khác với nhau; và kết hợp các phần tương ứng để tạo ra vectơ đầu vào; và bộ mã hóa mã cực được tạo cấu hình để nhân vectơ đầu vào với ma trận sinh mã cực để tạo ra từ mã cực.

Trong ví dụ thứ hai mươi, thiết bị của ví dụ nêu trên còn bao gồm bộ xử lý CRC được tạo cấu hình để xử lý mỗi khối thông tin để tạo ra tập hợp tương ứng của các bit CRC; trong đó bộ tạo ra vectơ đầu vào bao gồm tập hợp tương ứng của các bit CRC đối với mỗi trong số các khối thông tin P trong phần tương ứng của vectơ đầu vào.

Theo ví dụ thứ hai mươi mốt, thiết bị bao gồm: bộ thu để thu từ mã mà đã được mã hóa với mã cực; và bộ giải mã được tạo cấu hình để giải mã mã cực của từ mã thu được bằng cách xử lý ít nhất một bit ký hiệu như bit phong tỏa có trị số bit ký hiệu đã biết.

Theo ví dụ thứ hai mươi hai, thiết bị của ví dụ nêu trên còn được tạo cấu hình để thu thông tin trên các bit ký hiệu được sử dụng trong mã cực tách biệt với việc thu từ mã.

Theo ví dụ thứ mười ba, thiết bị của ví dụ nêu trên còn bao gồm bộ kiểm tra CRC được tạo cấu hình để xác nhận kết quả của việc giải mã nhờ sử dụng việc kiểm tra CRC.

Phần mô tả trước đó của một vài phương án được đề xuất để cho phép bất kỳ người nào có hiểu biết trung bình trong lĩnh vực kỹ thuật thực hiện hoặc sử dụng thiết bị, phương pháp, hoặc phương tiện đọc được bởi bộ xử lý theo sáng chế. Các sự cải biến khác nhau tới các phương án này sẽ dễ dàng rõ ràng với những người có hiểu biết trung bình trong lĩnh vực kỹ thuật, và các nguyên tắc chung của các phương pháp và các thiết bị được mô tả ở đây có thể được áp dụng tới các phương án khác. Vì vậy, sáng chế không được dự định giới hạn ở các phương án được thể hiện ở đây nhưng phải được bao hàm với phạm vi rộng nhất phù hợp với các nguyên tắc và các dấu hiệu mới được bộc lộ ở đây.

YÊU CẦU BẢO HỘ

1. Thiết bị truyền các bit thông tin, thiết bị này bao gồm:

ít nhất một bộ xử lý được tạo cấu hình để: tạo ra vectơ đầu vào để mã hóa cực, vectơ đầu vào bao gồm các bit thông tin, một hoặc nhiều bit ký hiệu, và một hoặc nhiều bit phong tỏa, trong đó mỗi bit của một hoặc nhiều bit ký hiệu được đặt ở vị trí bit tương ứng của vectơ đầu vào mà có độ tin cậy thấp hơn so với độ tin cậy của vị trí bit bất kỳ trong số các vị trí bit đối với các bit thông tin; và để mã hóa cực vectơ đầu vào để tạo ra từ mã; và

bộ truyền được tạo cấu hình để truyền từ mã qua kênh không dây cho việc thu bởi ít nhất một thiết bị thu.

2. Thiết bị theo điểm 1, trong đó bộ truyền còn được tạo cấu hình để truyền thông tin về một hoặc nhiều bit ký hiệu đến ít nhất một thiết bị thu tách biệt với việc truyền từ mã.

3. Thiết bị theo điểm 1, trong đó một hoặc nhiều bit ký hiệu bao gồm ít nhất một bit mà dành riêng cho ít nhất một thiết bị thu và một hoặc nhiều bit phong tỏa bao gồm các bit của cùng giá trị cố định.

4. Thiết bị theo điểm 1, trong đó ít nhất một bit ký hiệu của một hoặc nhiều bit ký hiệu được đặt tại vị trí bit tương ứng ở vectơ đầu vào mà trước vị trí bit bất kỳ trong số các vị trí bit đối với các bit thông tin.

5. Thiết bị theo điểm 1, trong đó vectơ đầu vào còn bao gồm các bit kiểm tra dư vòng (cyclic redundancy check - CRC) được tạo ra dựa vào các bit thông tin, trong đó các bit CRC được đặt tại các vị trí bit với các độ tin cậy cao hơn so với các độ tin cậy của các vị trí bit đối với một hoặc nhiều bit ký hiệu.

6. Thiết bị theo điểm 1, trong đó vectơ đầu vào còn bao gồm các bit kiểm tra dư vòng (CRC) được tạo ra dựa vào các bit thông tin, và ít nhất một bit ký hiệu của một hoặc nhiều bit ký hiệu được đặt tại vị trí bit tương ứng ở vectơ đầu vào mà trước vị trí bit bất kỳ trong số các vị trí bit đối với các bit thông tin và các bit CRC.

7. Thiết bị theo điểm 1, trong đó vectơ đầu vào còn bao gồm các bit kiểm tra dư vòng (CRC) được tạo ra dựa vào các bit thông tin, và ít nhất một bit ký hiệu của một hoặc nhiều bit ký hiệu được đặt tại vị trí bit tương ứng ở vectơ đầu vào mà sau vị trí bit đối với ít nhất một trong số các bit CRC.

8. Thiết bị để thu từ mã, thiết bị này bao gồm:

bộ thu để thu, qua kênh không dây từ thiết bị truyền, từ mã được tạo ra dựa vào việc mã hóa cực vectơ đầu vào bao gồm các bit thông tin, một hoặc nhiều bit ký hiệu, và một hoặc nhiều bit phong tỏa, trong đó mỗi bit của một hoặc nhiều bit ký hiệu là ở vị trí bit tương ứng mà có độ tin cậy thấp hơn so với độ tin cậy của vị trí bit bất kỳ trong số các vị trí bit đối với các bit thông tin, và

bộ giải mã mã cực được tạo cấu hình để giải mã từ mã được thu để tạo ra các bit được giải mã.

9. Thiết bị theo điểm 8 còn được tạo cấu hình để thu, từ thiết bị truyền, thông tin về một hoặc nhiều bit ký hiệu tách biệt với việc thu từ mã.

10. Thiết bị theo điểm 8, trong đó một hoặc nhiều bit ký hiệu bao gồm ít nhất một bit mà dành riêng cho nhóm các thiết bị thu mà bao gồm thiết bị thu và một hoặc nhiều bit phong tỏa bao gồm các bit của cùng giá trị cố định.

11. Thiết bị theo điểm 8, trong đó ít nhất một bit ký hiệu của một hoặc nhiều bit ký hiệu được đặt tại vị trí bit tương ứng ở vectơ đầu vào mà trước vị trí bit bất kỳ trong số các vị trí bit đối với các bit thông tin.

12. Thiết bị theo điểm 8 trong đó vectơ đầu vào còn bao gồm các bit kiểm tra dư vòng (CRC) được tạo ra dựa vào các bit thông tin, trong đó các bit CRC được đặt tại các vị trí bit với các độ tin cậy cao hơn so với các độ tin cậy của các vị trí bit đối với một hoặc nhiều bit ký hiệu.

13. Thiết bị theo điểm 8, trong đó vectơ đầu vào còn bao gồm các bit kiểm tra dư vòng (CRC) được tạo ra dựa vào các bit thông tin, và ít nhất một bit ký hiệu của một hoặc nhiều bit ký hiệu được đặt tại vị trí bit tương ứng ở vectơ đầu vào mà trước vị trí bit bất kỳ trong số các vị trí bit đối với các bit thông tin và các bit CRC.

14. Thiết bị theo điểm 8, trong đó vectơ đầu vào còn bao gồm các bit kiểm tra dư vòng (CRC) được tạo ra dựa vào các bit thông tin, và ít nhất một bit ký hiệu của một hoặc nhiều bit ký hiệu được đặt tại vị trí bit tương ứng ở vectơ đầu vào mà sau vị trí bit đối với ít nhất một trong số các bit CRC.

15. Phương pháp dùng cho thiết bị truyền để truyền các bit thông tin, phương pháp bao gồm:

tạo ra, bởi bộ xử lý của thiết bị truyền, vectơ đầu vào để mã hóa cực, vectơ đầu vào bao gồm các bit thông tin, một hoặc nhiều bit ký hiệu, và một hoặc nhiều bit phong tỏa;

trong đó mỗi bit của một hoặc nhiều bit ký hiệu được đặt tại vị trí bit tương ứng của vectơ đầu vào mà có độ tin cậy thấp hơn so với độ tin cậy của vị trí bit bất kỳ trong số các vị trí bit đối với các bit thông tin;

mã hóa cực, bởi bộ xử lý của thiết bị truyền, vectơ đầu vào để tạo ra từ mã; và

truyền, bởi bộ truyền của thiết bị truyền, từ mã qua kênh không dây cho việc thu bởi ít nhất một thiết bị thu.

16. Phương pháp theo điểm 15 còn bao gồm:

truyền, bởi thiết bị truyền, thông tin về một hoặc nhiều bit ký hiệu đến ít nhất một thiết bị thu tách biệt với việc truyền từ mã.

17. Phương pháp theo điểm 15 trong đó một hoặc nhiều bit ký hiệu bao gồm ít nhất một bit mà dành riêng cho ít nhất một thiết bị thu và một hoặc nhiều bit phong tỏa bao gồm các bit của cùng giá trị cố định.

18. Phương pháp theo điểm 15 trong đó ít nhất một bit ký hiệu của một hoặc nhiều bit ký hiệu được đặt tại vị trí bit tương ứng ở vectơ đầu vào mà trước vị trí bit bất kỳ trong số các vị trí bit đối với các bit thông tin.

19. Phương pháp theo điểm 15 trong đó vectơ đầu vào còn bao gồm các bit kiểm tra dư vòng (CRC) được tạo ra dựa vào các bit thông tin, trong đó các bit CRC được đặt tại các vị trí bit với các độ tin cậy cao hơn so với các độ tin cậy của các vị trí bit đối với một hoặc nhiều bit ký hiệu.

20. Phương pháp theo điểm 15, trong đó vectơ đầu vào còn bao gồm các bit kiểm tra dư vòng (CRC) được tạo ra dựa vào các bit thông tin, và ít nhất một bit ký hiệu của một hoặc nhiều bit ký hiệu được đặt tại vị trí bit tương ứng ở vectơ đầu vào mà trước vị trí bit bất kỳ trong số các vị trí bit đối với các bit thông tin và các bit CRC.

21. Phương pháp theo điểm 15, trong đó vectơ đầu vào còn bao gồm các bit kiểm tra dư vòng (CRC) được tạo ra dựa vào các bit thông tin, và ít nhất một bit ký hiệu của một hoặc nhiều bit ký hiệu được đặt tại vị trí bit tương ứng ở vectơ đầu vào mà sau vị trí bit đối với ít nhất một trong số các bit CRC.

22. Phương pháp dùng cho thiết bị thu để thu từ mã, phương pháp bao gồm:

thu qua kênh không dây, bởi thiết bị thu từ thiết bị truyền, từ mã được tạo ra dựa vào việc mã hóa cực vectơ đầu vào bao gồm các bit thông tin, một hoặc nhiều bit ký hiệu, và một hoặc nhiều bit phong tỏa, trong đó mỗi bit của một hoặc nhiều bit ký hiệu là ở vị trí bit tương ứng mà có độ tin cậy thấp hơn so với độ tin cậy của vị trí bit bất kỳ trong số các vị trí bit đối với các bit thông tin; và

giải mã cực, bởi thiết bị thu, từ mã được thu để tạo ra các bit được giải mã.

23. Phương pháp theo điểm 22 còn bao gồm thu, từ thiết bị truyền, thông tin về một hoặc nhiều bit ký hiệu tách biệt với việc thu từ mã.

24. Phương pháp theo điểm 22 trong đó một hoặc nhiều bit ký hiệu bao gồm ít nhất một bit mà dành riêng cho nhóm các thiết bị thu mà bao gồm thiết bị thu và một hoặc nhiều bit phong tỏa bao gồm các bit của cùng giá trị cố định.

25. Phương pháp theo điểm 22 trong đó ít nhất một bit ký hiệu của một hoặc nhiều bit ký hiệu được đặt tại vị trí bit tương ứng ở vectơ đầu vào mà trước vị trí bit bất kỳ trong số các vị trí bit đối với các bit thông tin.

26. Phương pháp theo điểm 22 trong đó vectơ đầu vào còn bao gồm các bit kiểm tra dư vòng (CRC) được tạo ra dựa vào các bit thông tin, trong đó các bit CRC bit được đặt tại các vị trí bit với các độ tin cậy cao hơn so với các độ tin cậy của vị trí bit bất kỳ trong số các vị trí bit đối với một hoặc nhiều bit ký hiệu.

27. Phương pháp theo điểm 22, trong đó vectơ đầu vào còn bao gồm các bit kiểm tra dư vòng (CRC) được tạo ra dựa vào các bit thông tin, và ít nhất một bit ký hiệu của một hoặc nhiều bit ký hiệu được đặt tại vị trí bit tương ứng ở vectơ đầu vào mà trước vị trí bit bất kỳ trong số các vị trí bit đối với các bit thông tin và các bit CRC.

28. Phương pháp theo điểm 22, trong đó vectơ đầu vào còn bao gồm các bit kiểm tra dư vòng (CRC) được tạo ra dựa vào các bit thông tin, và ít nhất một bit ký hiệu của một hoặc nhiều bit ký hiệu được đặt tại vị trí bit tương ứng ở vectơ đầu vào mà sau vị trí bit đối với ít nhất một trong số các bit CRC.

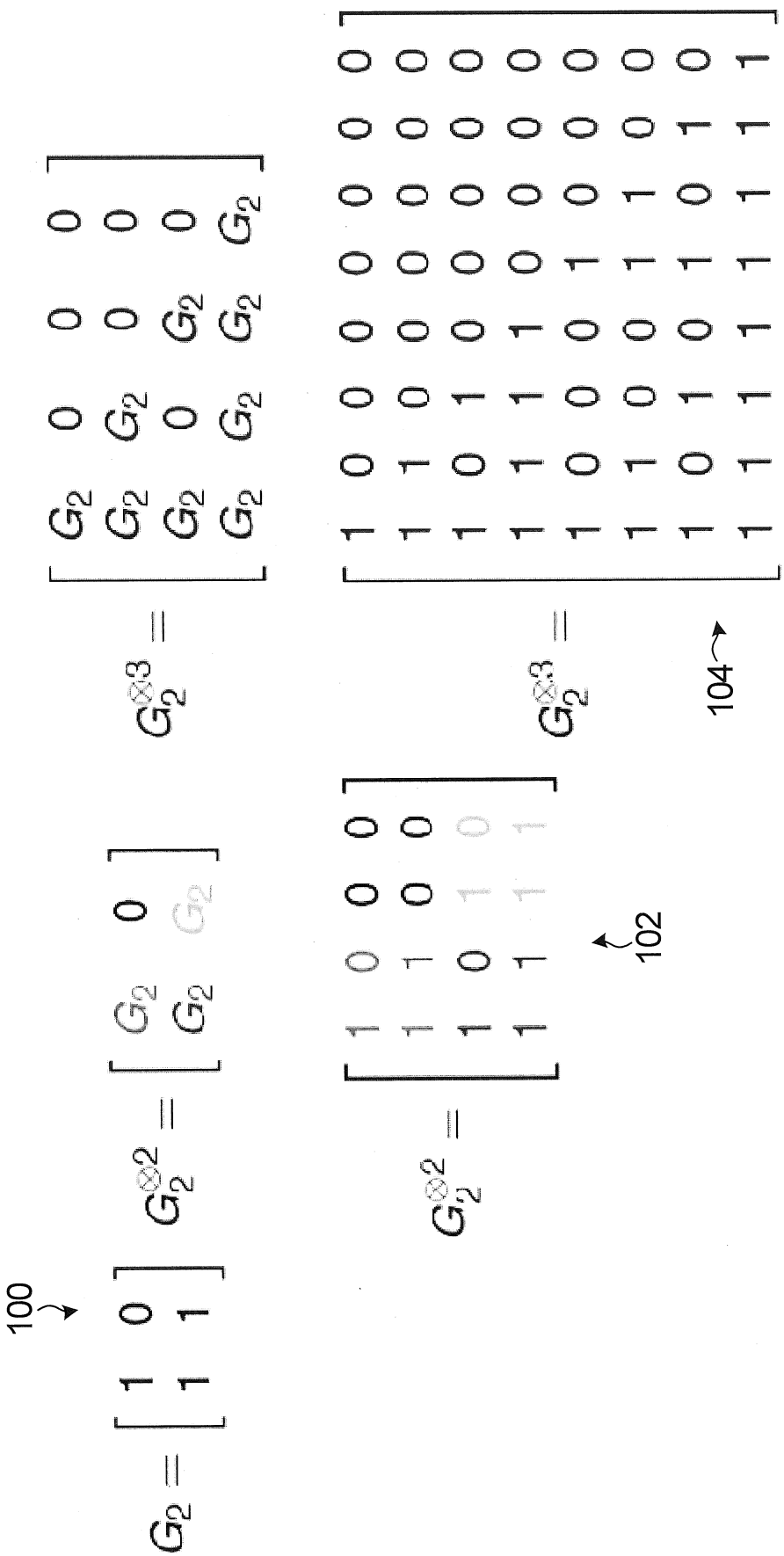


FIG. 1
(Kỹ thuật đã biết)

Độ dài $N = 2^m$, $m \in \mathbb{N}$

Ma trận sinh: Các cột của $G_2^{\otimes m}$

104

$$G_2^{\otimes 3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

bit phong tỏa
bit phong tỏa
bit phong tỏa
bit thông tin
bit phong tỏa
bit thông tin
bit thông tin
bit thông tin

$$\bar{x} = [0\ 0\ 0\ u_3\ 0\ u_5\ u_6\ u_7]G_2^{\otimes 3}$$

110

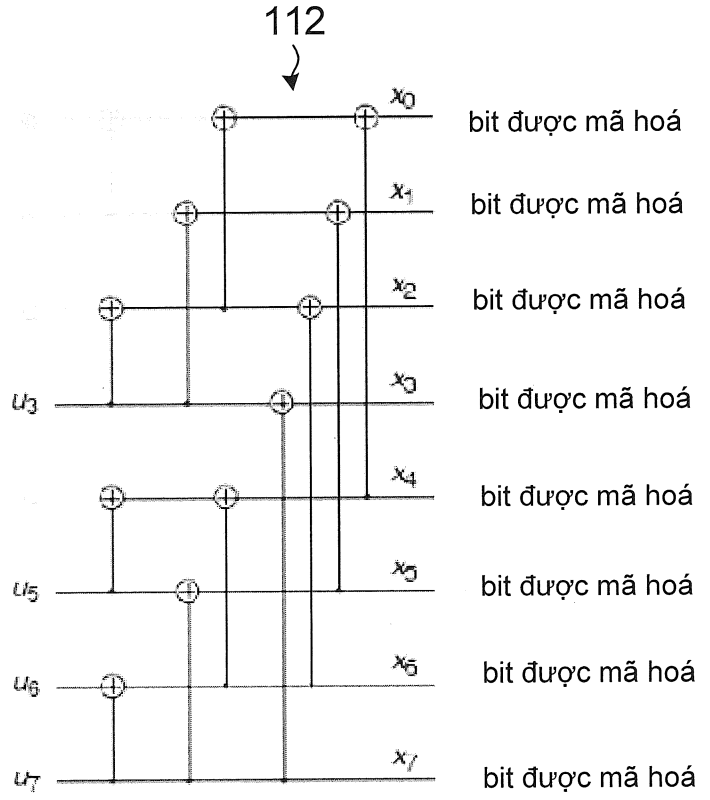


FIG. 2

(Kỹ thuật đã biết)

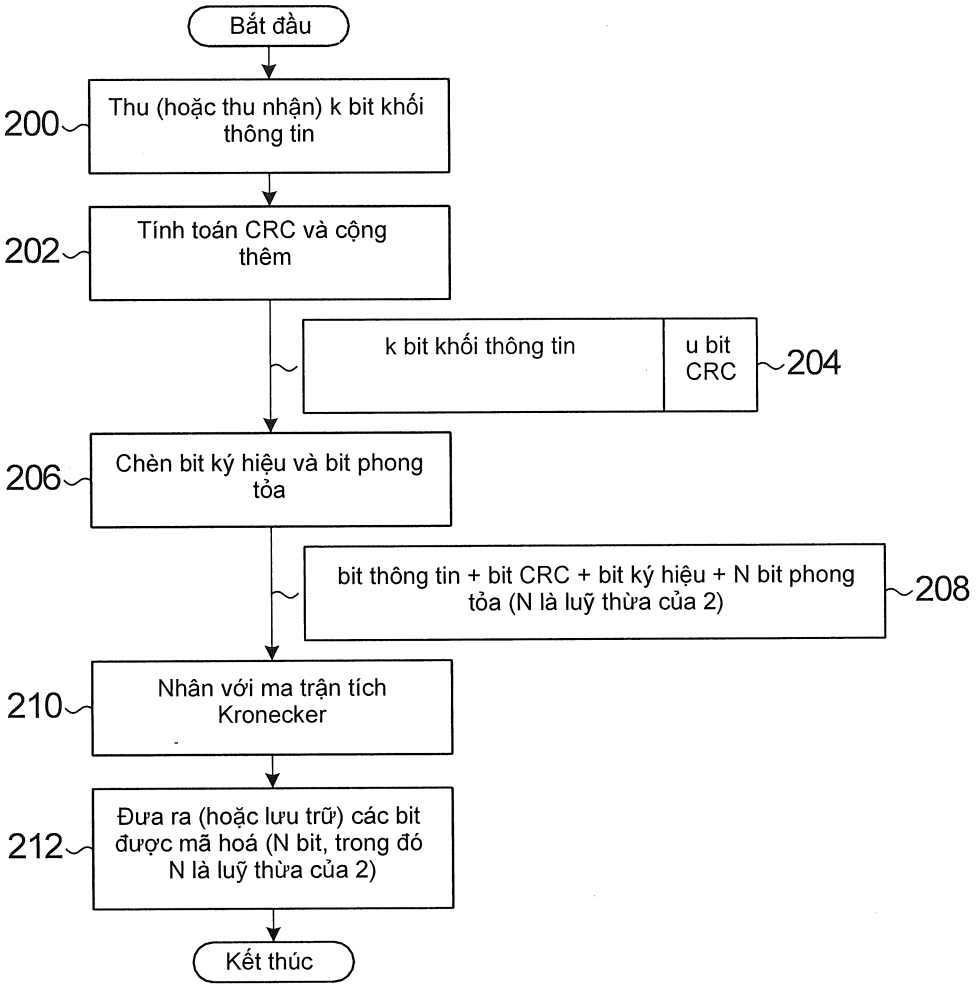

Bắt đầu
200
Thu (hoặc thu nhận) k bit khối thông tin
202
Tính toán CRC và cộng thêm
k bit khối thông tin
u bit CRC
204
206
Chèn bit ký hiệu và bit phong tỏa
bit thông tin + bit CRC + bit ký hiệu + N bit phong tỏa (N là luỹ thừa của 2)
208
210
Nhân với ma trận tích Kronecker
212
Đưa ra (hoặc lưu trữ) các bit được mã hoá (N bit, trong đó N là luỹ thừa của 2)
Kết thúc

FIG. 3

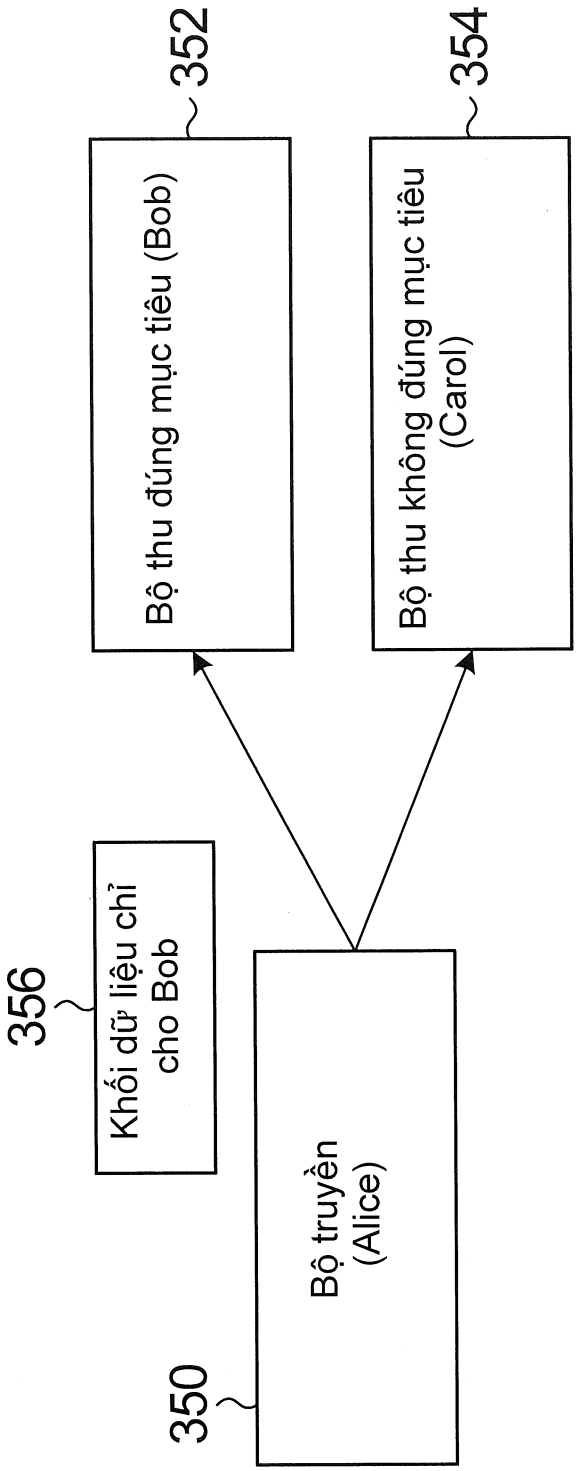

352
354
Bộ thu đúng mục tiêu (Bob)
Bộ thu không đúng mục tiêu (Carol)
356
Khối dữ liệu chỉ cho Bob
Bộ truyền (Alice)
350

FIG. 4

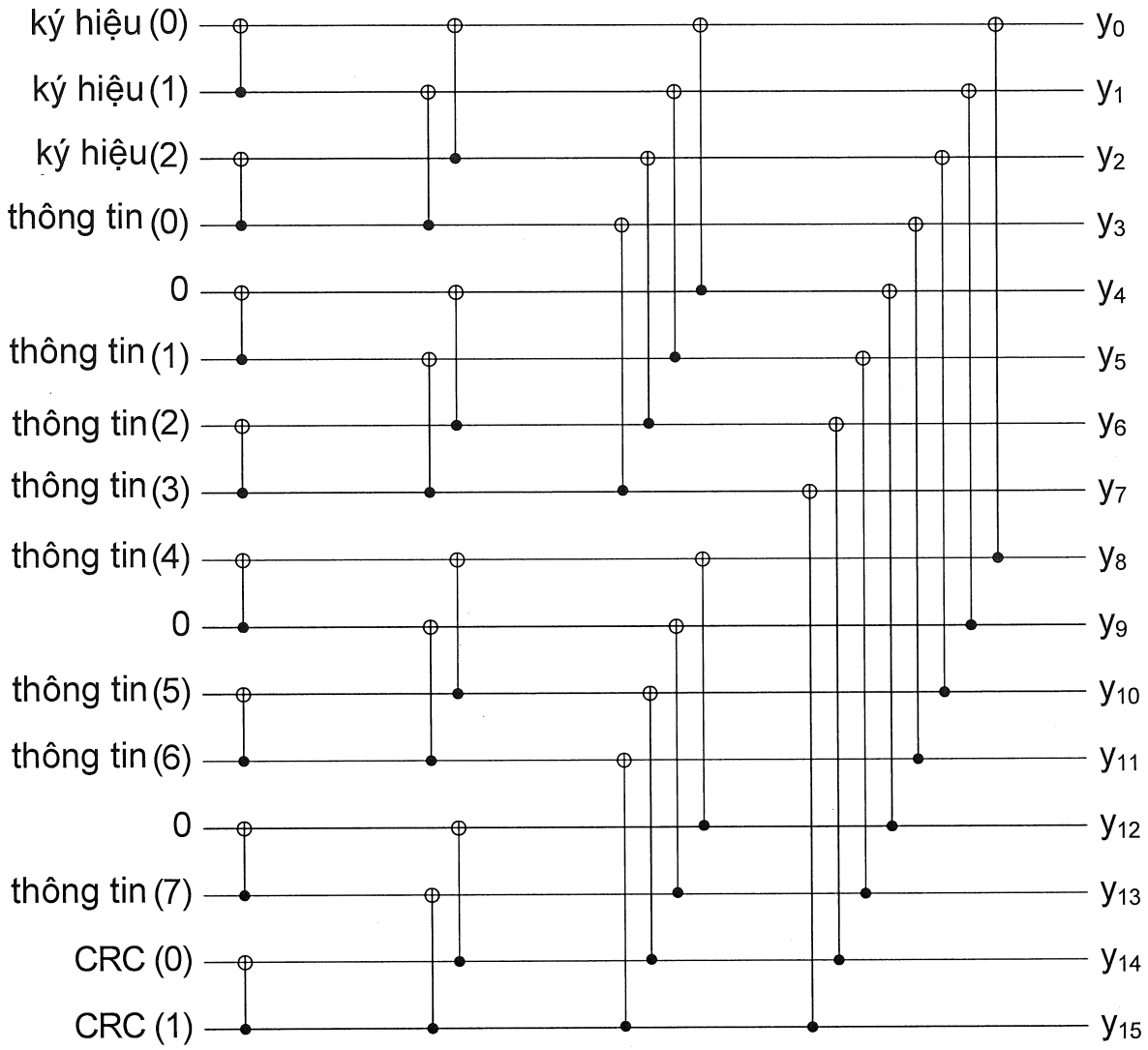

ký hiệu (0)
ký hiệu (1)
ký hiệu (2)
thông tin (0)
0
thông tin (1)
thông tin (2)
thông tin (3)
thông tin (4)
0
thông tin (5)
thông tin (6)
0
thông tin (7)
CRC (0)
CRC (1)
y0
y1
y2
y3
y4
y5
y6
y7
y8
y9
y10
y11
y12
y13
y14
y15

FIG. 5

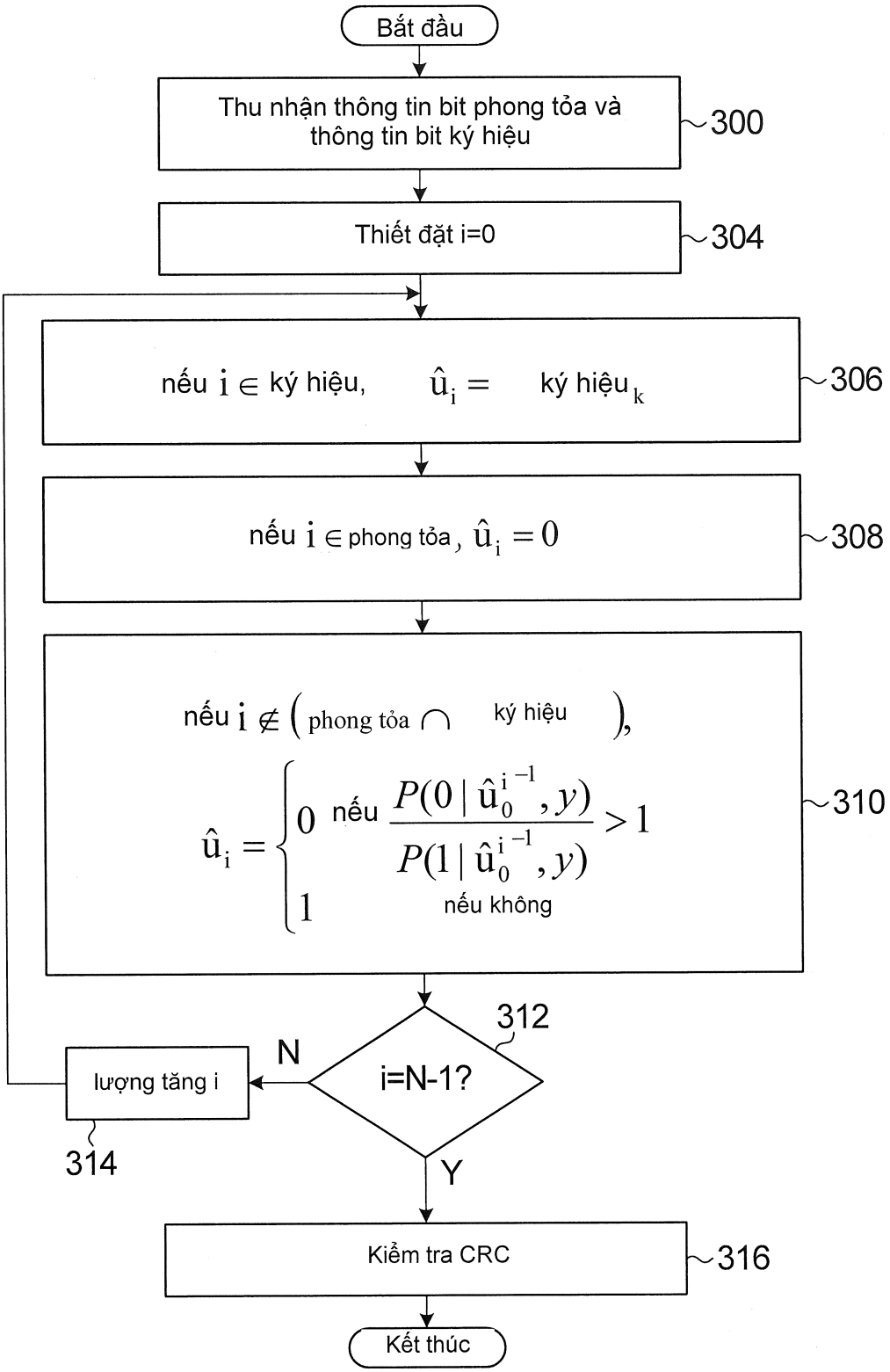

Bắt đầu
Thu nhận thông tin bit phong tỏa và thông tin bit ký hiệu
300
Thiết đặt i=0
304
nếu $i \in$ ký hiệu, $\hat{u}_i =$ ký hiệu$_k$
306
nếu $i \in$ phong tỏa, $\hat{u}_i = 0$
308
nếu $i \notin$ (phong tỏa $\cap$ ký hiệu),
$\hat{u}_i = \begin{cases} 0 & \text{nếu } \frac{P(0 \mid \hat{u}_0^{i-1}, y)}{P(1 \mid \hat{u}_0^{i-1}, y)} > 1 \\ 1 & \text{nếu không} \end{cases}$
310
312
i=N-1?
N
Y
lượng tăng i
314
Kiểm tra CRC
316
Kết thúc

FIG. 6

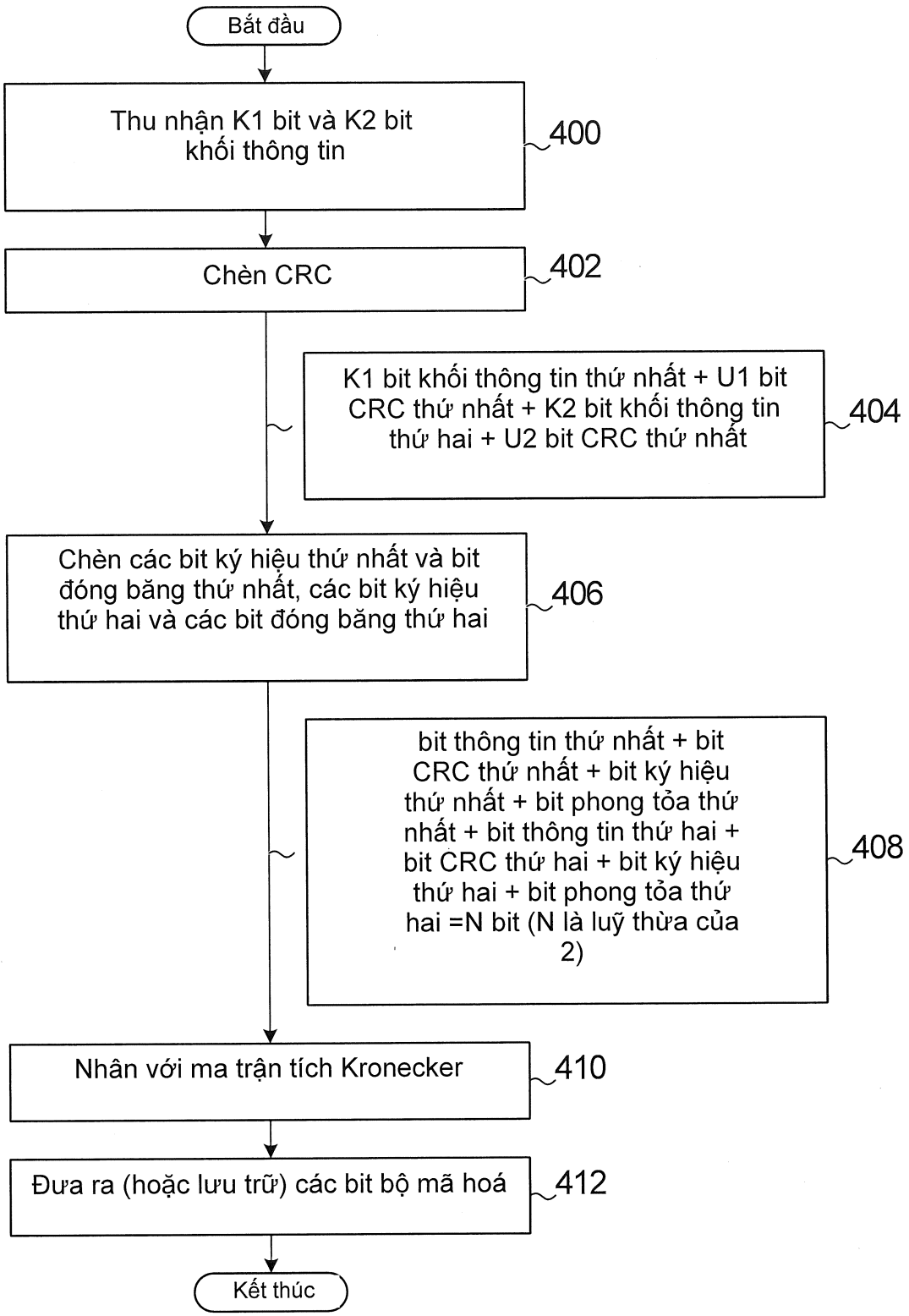

Bắt đầu
Thu nhận K1 bit và K2 bit khối thông tin
400
Chèn CRC
402
K1 bit khối thông tin thứ nhất + U1 bit CRC thứ nhất + K2 bit khối thông tin thứ hai + U2 bit CRC thứ nhất
404
Chèn các bit ký hiệu thứ nhất và bit đóng băng thứ nhất, các bit ký hiệu thứ hai và các bit đóng băng thứ hai
406
bit thông tin thứ nhất + bit CRC thứ nhất + bit ký hiệu thứ nhất + bit phong tỏa thứ nhất + bit thông tin thứ hai + bit CRC thứ hai + bit ký hiệu thứ hai + bit phong tỏa thứ hai =N bit (N là luỹ thừa của 2)
408
Nhân với ma trận tích Kronecker
410
Đưa ra (hoặc lưu trữ) các bit bộ mã hoá
412
Kết thúc

FIG. 7A

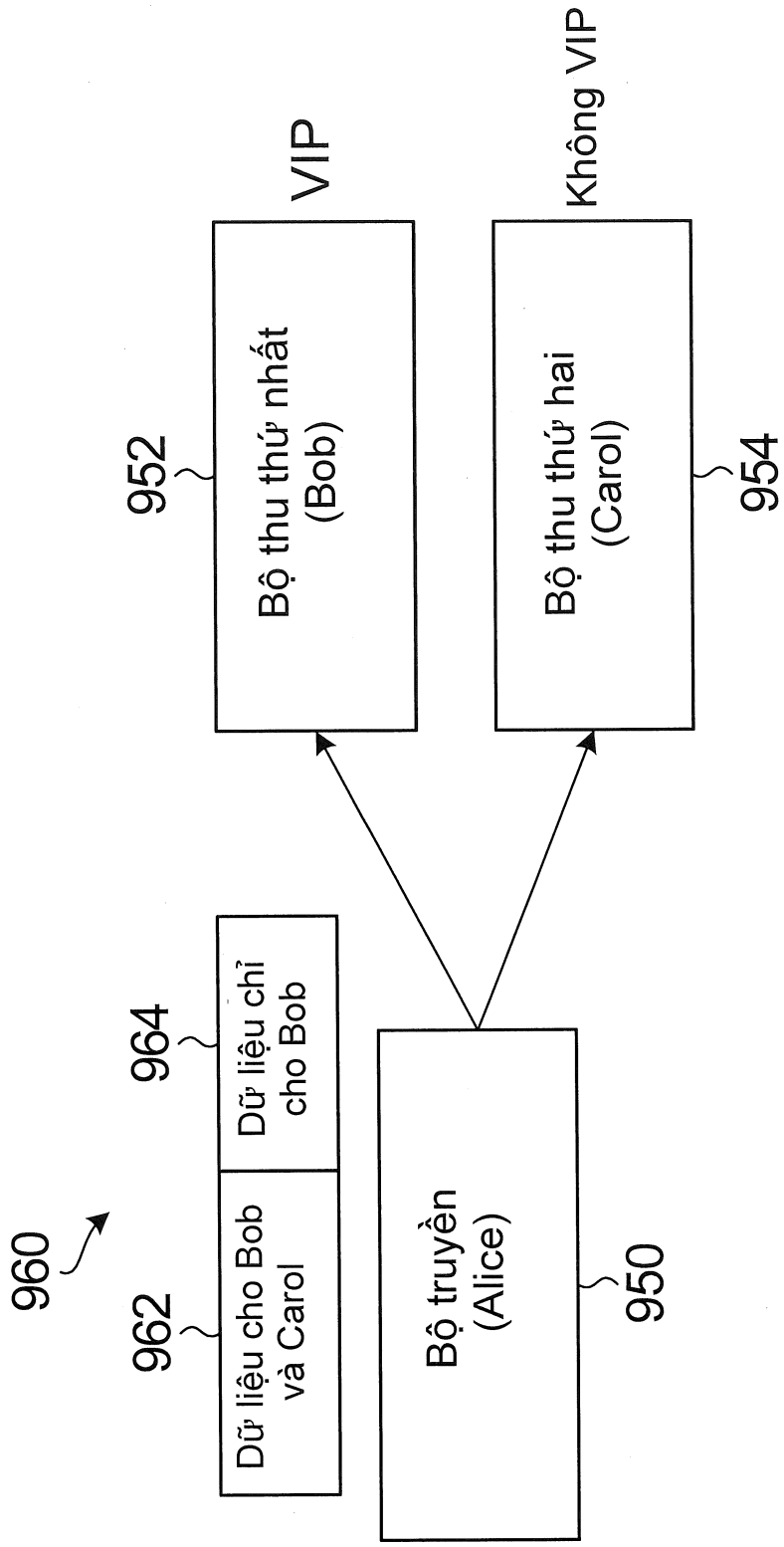

960
962
Dữ liệu cho Bob và Carol
964
Dữ liệu chỉ cho Bob
Bộ truyền (Alice)
950
952
Bộ thu thứ nhất (Bob)
VIP
954
Bộ thu thứ hai (Carol)
Không VIP

FIG. 7B

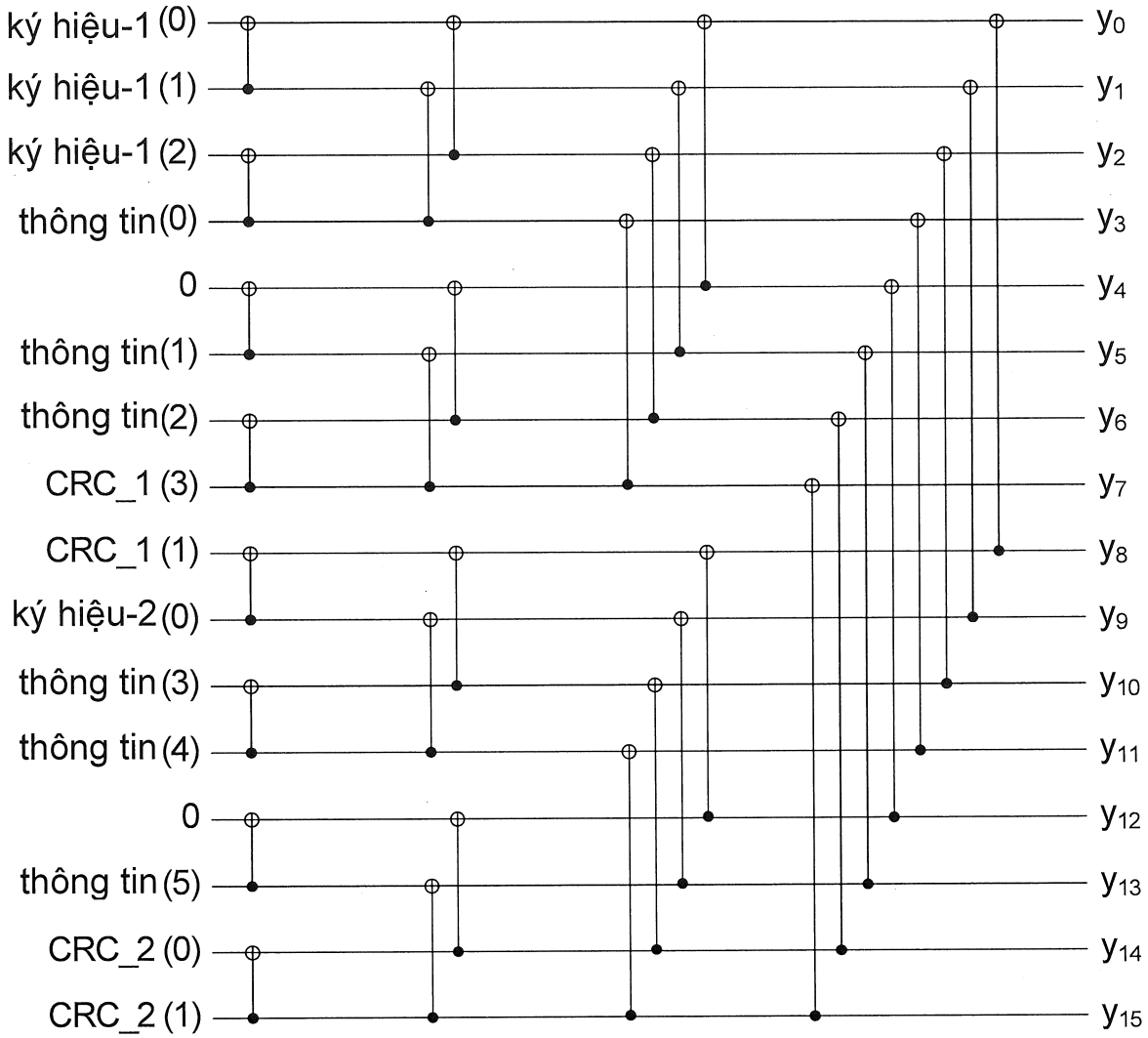

ký hiệu-1 (0)
ký hiệu-1 (1)
ký hiệu-1 (2)
thông tin (0)
0
thông tin (1)
thông tin (2)
CRC_1 (3)
CRC_1 (1)
ký hiệu-2 (0)
thông tin (3)
thông tin (4)
0
thông tin (5)
CRC_2 (0)
CRC_2 (1)
y0
y1
y2
y3
y4
y5
y6
y7
y8
y9
y10
y11
y12
y13
y14
y15

FIG. 8

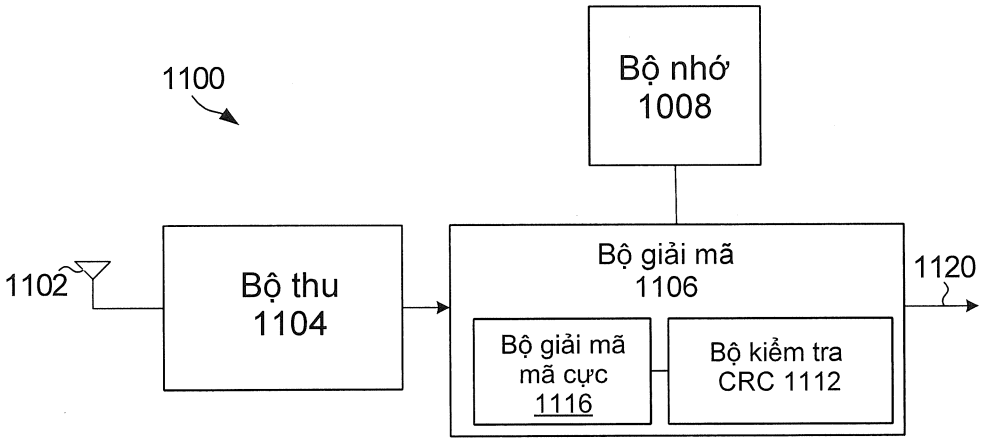

1100
Bộ nhớ
1008
1102
Bộ thu
1104
Bộ giải mã
1106
1120
Bộ giải mã
mã cực
1116
Bộ kiểm tra
CRC 1112

FIG. 9

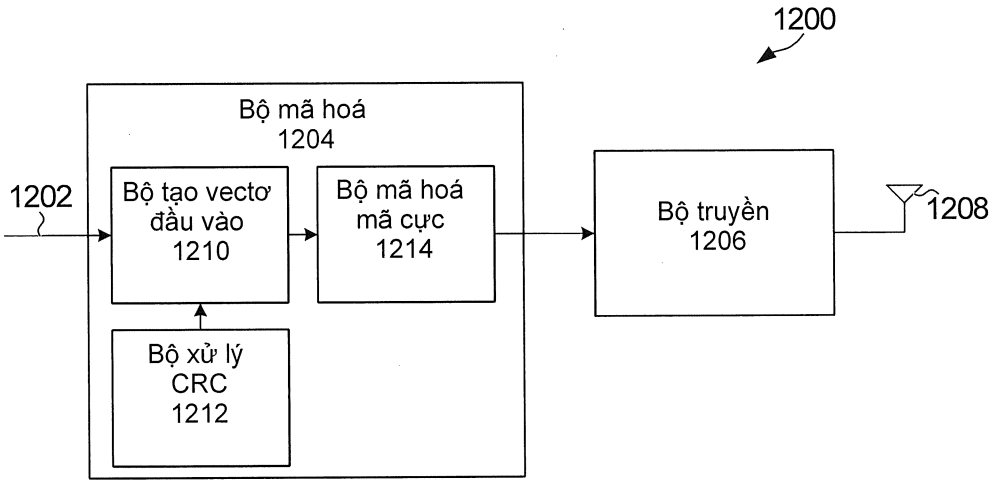

1200
Bộ mã hoá
1204
1202
Bộ tạo vectơ
đầu vào
1210
Bộ mã hoá
mã cực
1214
Bộ truyền
1206
1208
Bộ xử lý
CRC
1212

FIG. 10