GIẢI PHÁP NÂNG CAO TỶ LỆ MÃ HÓA CỦA SƠ ĐỒ MẬT MÃ DỰA TRÊN MÃ

PROPOSED SOLUTIONS TO IMPROVE THE CODE RATE OF CODE-BASED CRYPTOGRAPHY

Lê Văn Thái

TÓM TẮT

Bài báo đề xuất hai giải pháp cải tiến hệ mật McEliece, giải pháp sử dụng vector lỗi mang tin và giải pháp sử dụng mã nối tiếp thay thế mã Goppa. Các giải pháp đề xuất cho phép tăng tỷ lệ mã hoá đến ~0,8, đạt độ lợi mã hóa 1,7dB, tăng khả năng sửa lỗi, khả năng chống nhiễu của hệ thống và độ bảo mật so với thuật toán đề xuất gốc.

Từ khóa: *Hệ mật McEliece, sơ đồ mật dựa trên mã, mã hóa công khai, mã Goppa.*

ABSTRACT

This paper is mainly to analyse the feature of the McEliece cryptosystem, in which it gives a variety of solutions in order to enhace the effect of the algorithm such as using error vector and replace Goppa code which use in the traditional by succeed concatenated coding. The algorithm improves the coding rate about ~0.8, gain encoding 1.7dB and the security ability of McEliece algorithm improves more greatly than the traditional.

Keywords*: McEliece cryptosystem, Code based cryptosystem, Public-key cryptography, Goppa codes.*

Trường Đai học Công nghiệp Hà Nội
Email: thailv@haui.edu.vn
Ngày nhận bài: 28/5/2018
Ngày nhận bài sửa sau phản biện: 30/6/2018
Ngày chấp nhận đăng: 25/10/2018

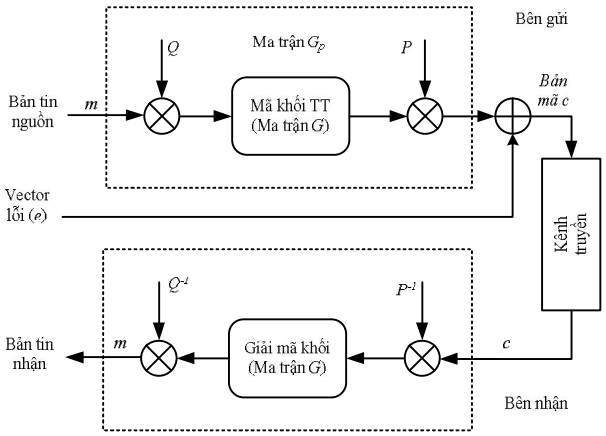
1. ĐẶT VẤN ĐỀ

Hệ mật McEliece là hệ mật mã khóa công khai đầu tiên dựa trên lý thuyết mã hóa đại số, được giới thiệu năm 1978 [1]. An ninh của hệ mật này dựa trên độ khó của bài toán giải mã theo syndrome và đã được chứng minh là bài toán NP đầy đủ [2]. Sơ đồ gốc ban đầu đề xuất sử dụng mã Goppa nhị phân và thuật toán giải mã Patterson. Ưu điểm nổi bật của hệ mật là tính bảo mật cao, thời gian thực hiện mã hoá và giải mã nhanh, yêu cầu thiết bị thực hiện đơn giản [3]. Trải qua 40 năm với mã Goppa chưa có thuật toán hiệu quả nào có thể phá vỡ được sơ đồ hệ mật McEliece với tham số được lựa chọn phù hợp. Vì vậy, hệ mật này được xếp vào nhóm mật mã sau lượng tử và những năm gần đây đã được cộng đồng các nhà mật mã học nghiên cứu rộng rãi. Tuy nhiên, hệ mật này chưa được đưa vào ứng dụng trong thực tế xuất phát từ nhược điểm cơ bản của nó là tỷ lệ mã hóa thấp (~1/2), kích thước khóa lớn (1024× 524 bit đối với hệ mật đề xuất ban đầu) do đó đòi hỏi dung lượng bộ nhớ lớn.

Nội dung bài báo này, đề xuất hai cải tiến áp dụng trên sơ đồ hệ mật McEliece nhằm khắc phục những điểm yếu trên của hệ mật gốc. Các thuật toán đề xuất mới cho phép tăng tỷ lệ mã hóa lên đến 0,8 mà vẫn đảm bảo độ an toàn của hệ mật. Phần còn lại của bài báo được tổ chức như sau: Trong phần 2, bài báo giới thiệu đặc điểm cơ bản của hệ mật mã khóa công khai McEliece, phần 3 trình bày thuật toán cải tiến sử dụng vector lỗi mang một phần thông tin, phần 4 trình bày thuật toán cải tiến sử dụng mã nối tiếp thay thế Goppa trong sơ đồ hệ mật gốc, cuối cùng phần kết luận được trình bày trong phần 5.

2. HỆ MẬT KHÓA CÔNG KHAI MCELIECE

Hệ mật McEliece được giới thiệu bởi R.McEliece vào năm 1978 [1]. Đây là sơ đồ hệ mật đầu tiên sử dụng tính ngẫu nhiên trong mã hóa. Thuật toán dựa trên độ khó của giải mã mã khối tuyến tính. Thuật toán ban đầu sử dụng mã nhị phân Goppa, dễ dàng trong việc giải mã nhờ thuật toán của Patterson [4]. Khóa công khai thu được từ khóa mật bằng cách che dấu từ mã đã chọn giống như một từ mã tuyến tính. Để thực hiện, ma trận sinh G của mã nhị phân được xáo trộn với hai ma trận khả nghịch ngẫu nhiên Q và P.



Hình 1. Sơ đồ khối thuật toán McEliece

Hệ mật McEliece bao gồm 3 thuật toán: thuật toán tạo khóa, nhằm tạo ra khóa công khai và khóa mật; thuật toán

mã hóa xác suất, sử dụng tính chất ngẫu nhiên trong thuật toán mã hóa và thuật toán giải mã. Hệ mật McEliece gốc sử dụng mã Goppa nhị phân, mã Goppa là một lớp con của mã sửa lỗi tuyến tính được dùng để sửa các lỗi ngẫu nhiên xảy ra khi truyền qua kênh có nhiễu. Sơ đồ khối hệ mật được biểu diễn trên hình 1 [5].

Trong đó: Bản tin nguồn được biểu diễn ở dạng một chuỗi thông tin số nhị phân được chia thành các khối con ký hiệu là *m* có độ dài là *k* bit. Các thuật toán của hệ mật được thực hiện như sau [1]:

Tạo khóa:

• Chọn một mã tuyến tính nhị phân *C* có khả năng sửa được *t* lỗi. Mã Goppa được đặc trưng bởi ma trận sinh *G* kích thước *k*×*n* và có khả năng sửa được một vector lỗi ngẫu nhiên dài *n* bit có trọng số nhỏ hơn hoặc bằng *t*.

• Chọn một ma trận nhị phân khả nghịch *Q* kích thước *k*×*k* có nghịch đảo là Q^{-1}.

• Chọn một ma trận hoán vị nhị phân ngẫu nhiên *P* kích thước *n*×*n* (chỉ có một phần tử "1" trên mỗi hàng và mỗi cột).

• Tính toán ma trận $G_p = Q.G.P$ kích thước *k*×*n*.

$$G_p = Q.G.P \quad (1)$$

• Khóa công khai là (G_p, *t*), khóa mật là (*Q*, *G*, *P*).

Mã hóa:

Quá trình mã hoá và giải mã một bản tin trên hệ mật McEliece được thực hiện như sau: Ở bên nhận muốn nhận được bản tin được mật hoá bằng thuật toán McEliece, sẽ thực hiện tính chìa khoá công khai G_p dựa trên các chìa khoá mật là các ma trận *Q*, *G* và *P*, sau đó gửi cặp khóa công khai (G_p, *t*) qua kênh truyền đến bên gửi.

• Khi muốn gửi bản tin *m* tới bên nhận thông qua khóa công khai (G_p, *t*).

• Biểu diễn bản tin *m* ở dạng một chuỗi nhị phân có độ dài *k* bit.

• Tạo một vector *e* ngẫu nhiên có độ dài *n* và có trọng số (số phần tử "1") $w(e) \le t$.

• Tính toán bản mã *c* sau đó gửi cho bên nhận

$$c = mG_p + e \quad (2)$$

Giải mã:

Sau khi nhận được từ mã *c*, bên nhận thực hiện giải mã bản tin:

• Tính phép toán cP^{-1}

$$\mathrm{cP}^{-1} = \mathrm{m}(\mathrm{QGP})\mathrm{P}^{-1} + \mathrm{eP}^{-1} = \mathrm{mQG} + \mathrm{eP}^{-1} \quad (3)$$

• Sử dụng thuật toán giải mã sửa lỗi đối với CP^{-1} để tìm được *mQ*

$$m' = mQ \quad (4)$$

• Xác định bản tin *m*

$$\mathrm{m} = \mathrm{m'Q}^{-1} = (\mathrm{mQ})\mathrm{Q}^{-1} \quad (5)$$

Ta có $cP^{-1} = mQG + eP^{-1}$ và *P* là ma trận hoán vị nên eP^{-1} có trọng số lớn nhất là *t*. Mã Goppa G_p có thể sửa được *t* lỗi và từ mã *mQG* có thể sửa được *t* lỗi nhờ thuật toán Patterson hoặc sử dụng các thuật toán khác. Do đó ta sẽ tính được từ mã $m' = mQ$. Để lấy bản tin gốc ta nhân *m'* với ma trận nghịch đảo của *Q* ta có $m'Q^{-1} = m$, đây chính là bản tin gốc ban đầu.

Từ bản chất của các thuật toán thực hiện trong hệ mật McEliece ta đưa ra một số nhận xét cơ bản về thuật toán này như sau:

- Hệ mật có độ bảo mật cao vì không phải thực hiện truyền các khóa mật (các khóa dùng để giải mã bản tin) qua kênh, các khóa này chỉ duy nhất bên thực hiện giải mã biết.

- Thiết kế các thiết bị mã hoá và giải mã đơn giản vì việc tính toán thực hiện trong các quá trình này là các phép tính nhị phân, do đó ta có thể thiết kế thiết bị bằng các linh kiện số khá phổ biến.

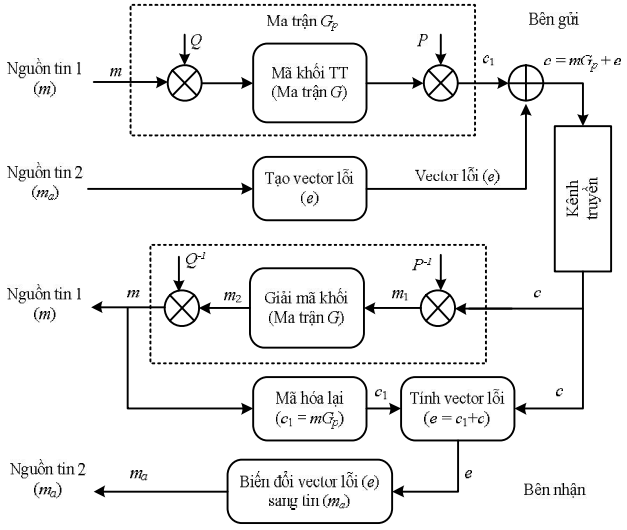
- Thời gian mã hoá và giải mã nhanh chỉ thực hiện tính toán trên các phép toán nhị phân, có thể đáp ứng được các thông tin yêu cầu thời gian thực.

- Nhược điểm cơ bản của hệ mật là tỷ lệ mã hoá thấp (~1/2) vì sử dụng mã kênh là mã khối tuyến tính, thuật toán McEliece gốc sử dụng mã Goppa (1024, 524) với tỷ lệ mã hoá $\mathrm{r} = \mathrm{k}/\mathrm{n} \approx 1/2$.

- Thông thường để đảm bảo độ mật cao, thuật toán McEliece yêu cầu kích thước khóa lên tới 1024 bit (tương đương với 2^{10}), hơn nữa, để khắc phục phương án tấn công theo kiểu vét cạn (tính tất cả các trường hợp có thể có của vector tín hiệu đầu vào), thuật toán McEliece yêu cầu kích thước bản tin đầu vào khá lớn ($k \ge 524$). Những vấn đề này dẫn đến việc đòi hỏi thiết bị mã hoá và giải mã phải có dung lượng bộ nhớ khá lớn, do đó làm chậm thời gian của quá trình xử lý tín hiệu.

Nội dung tiếp theo của bào báo trình bày hai đề xuất cải tiến thuật toán McEliece nhằm tăng tỷ lệ mã hóa và tăng khả năng chống nhiễu và độ bảo mật so với thuật toán gốc.

3. ĐỀ XUẤT TĂNG TỶ LỆ MÃ HÓA CỦA HỆ MẬT McELIECE SỬ DỤNG VECTOR LỖI MANG TIN



Hình 2. Sơ đồ khối hệ mật McEliece cải tiến

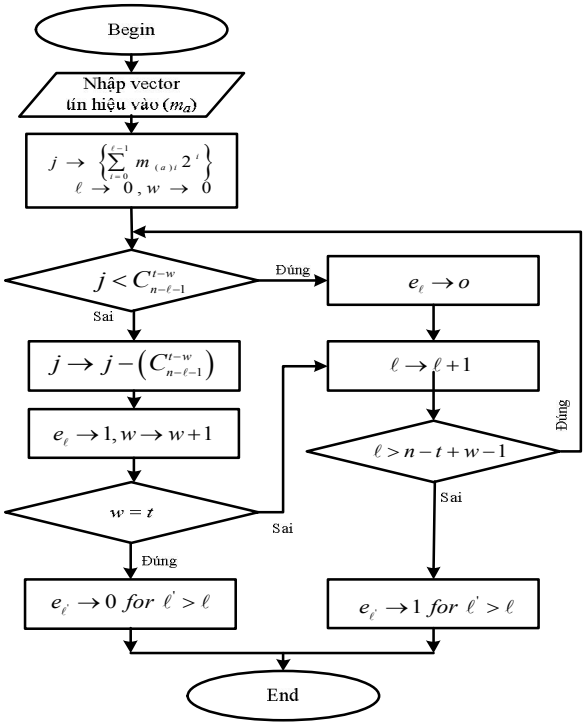
Điểm hạn chế của hệ mật McEliece là tỷ lệ mã hóa thấp (khoảng 0,5 với sơ đồ gốc). Để khắc phục điểm hạn chế này tác giả đề xuất giải pháp đưa một phần thông tin cần truyền vào vector lỗi. Thuật toán đề xuất nhằm tăng tỷ lệ mã hóa của thuật toán McEliece đồng thời nâng cao độ bảo mật của hệ mật McEliece. Sơ đồ khối hệ mật McEliece cải tiến đề xuất được thể hiện trên hình 2.

Giải pháp thực hiện là lấy một số bit thông tin cần truyền ánh xạ sang một vector lỗi trước khi được thêm vào từ mã. Bên nhận sau khi xác định được vector lỗi, có thể được khôi phục lại được phần thông tin bổ sung. Bằng cách sử dụng phương pháp này, tỷ lệ mã hóa cho hệ mật McEliece được tăng lên đến 0,8 hoặc cao hơn. Giải pháp cơ bản của thuật toán là tạo ra vector lỗi e có độ dài n và trọng lượng t từ các bit thông tin có độ dài l. Như vậy tổng số bít tin được gửi đi trong trường hợp này là (k+l), khi đó, tỷ lệ mã hoá tăng lên, (k + l)/n > k/n khi (l ≠ 0). Vấn đề cơ bản được đặt ra là lựa chọn độ dài của chuỗi tin bổ sung l bằng bao nhiêu và làm thế nào để tạo được vector lỗi thỏa mãn yêu cầu trên.

Để thực hiện ý tưởng này, ta dựa trên một thuật toán biến đổi nhị phân, nội dung chính của thuật toán là có thể biến đổi một chuỗi bít nhị phân có nội dung bất kỳ với độ dài l (vector tin bổ sung) thành một chuỗi bít có độ dài n và trọng lượng t (vector lỗi e) với điều kiện ràng buộc phải thoả mãn theo công thức (6) [6,7]:

$$l = \left\lfloor \log_2 C_n^t \right\rfloor. \quad (6)$$

Trong đó, C_n^t là tổ hợp của *t* trong *n*. Lưu đồ thuật toán biến đổi từ vector tin bổ sung m_a sang vector lỗi *e* được mô tả trên hình 3.



Hình 3. Lưu đồ thuật toán biến đổi từ vector tin bổ sung sang vector lỗi

Giả thiết bản tin cần truyền là $M = (m \| m_a)$, gồm hai bản tin con là *m* và m_a. Các thuật toán của hệ mật McEliece cải tiến được thực hiện như sau:

Tạo khóa:

Quá trình tạo khóa thực hiện tương tự trong thuật toán gốc (được trình bày trong phần 1), với khóa công khai (G_p, *t*) và khóa bí mật là ba ma trận *Q*, *G*, *P*. Thuật toán mã hóa và giải mã của sơ đồ đề xuất được thực hiện như sau:

Mã hóa:

Khi muốn gửi bản tin nguồn tới bên nhận thông qua khóa công khai G_P. Bên gửi thực hiện chia bản tin thành hai thành phần là bàn tin chính *m* (nguồn tin 1) và bản tin bổ sung m_a (nguồn tin 2) và thực hiện mã hóa như sau:

+ Đối với bản tin chính *m* (nguồn tin 1) được nhân với khóa công khai G_P (trong đó G_P là ma trận tích của ba ma trận *Q*, *G*, *P*) ta được từ mã c_1.

+ Đối với phần bản tin bổ sung m_a (nguồn tin 2), ở bên gửi thực hiện biến đổi bản tin này với độ dài l sang vector lỗi *e* có độ dài *n* và trọng lượng *t*, thực hiện theo thuật toán được trình bày trên hình 3; các tham số l, n, t phải thoả mãn công thức (6).

+ Tính từ mã $c = c_1 + e = mG_p + e$

Giải mã:

Sau khi nhận được bản mã *c*, bên nhận thực hiện giải mã bản tin như sau:

+ Xác định bản tin chính m. Thực hiện tính $m^1 = c.P^{-1}$ (P^{-1} là ma trận nghịch đảo của *P*), giải mã sửa sai tương ứng với ma trận sinh *G* ta xác định được vector m_2 và thực hiện tính $m = m_2Q^{-1}$.

$$\begin{aligned} m_1 &= c.P^{-1} \\ &= (mG_p + e)P^{-1} \\ &= (mQGP + e)P^{-1} \\ &= (mQ)G + eP^{-1} \end{aligned}$$

$$m_2 = mQ$$

Từ đó ta xác định được bản tin chính $m = m_2Q^{-1}$.

+ Xác nhận tin bổ sung m_a*, bên nhận tiến hành thực hiện khôi phục bản tin theo các bước sau:*

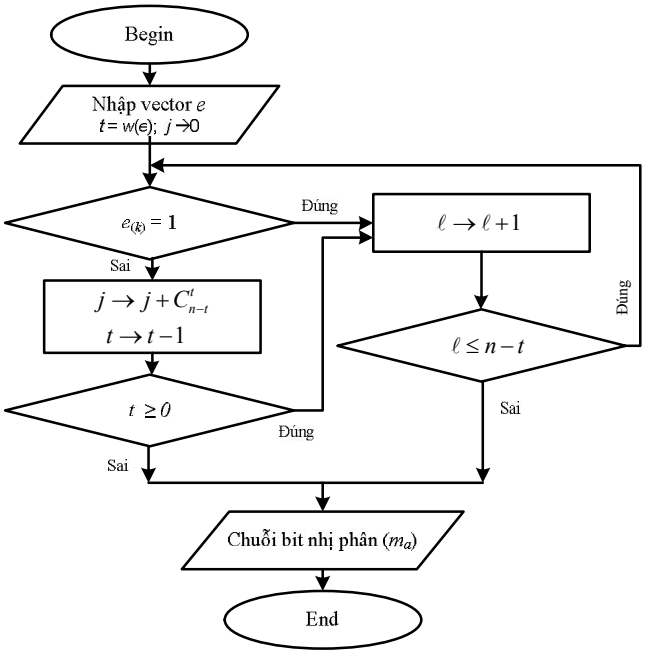
Bước 1: Thực hiện mã hoá lại, bằng cách tính:

$$c_1 = mG_p \quad (7)$$

Bước 2: Tính vector lỗi ở bên nhận theo công thức (8):

$$e = c_1 + c \quad (8)$$

Bước 3: Khôi phục phần bản tin bổ sung từ vector e bằng thuật toán biến đổi ngược so với bên gửi, thuật toán được trình bày chi tiết trên hình 4.



Hình 4. Thuật toán biến đổi vector lỗi thành chuỗi tín hiệu bổ sung m_a

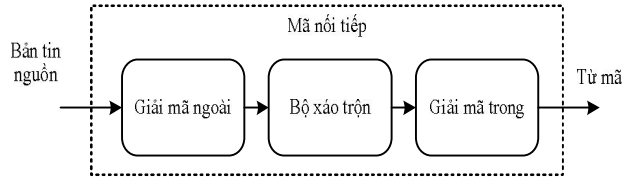
Nhận xét đặc điểm thuật toán McEliece cải tiến sử dụng vector lỗi mang tin:

+ Hệ mật đề xuất khi sử dụng vector lỗi mang một phần thông tin đã tăng được tỷ lệ mã hóa so với đề xuất của hệ mật gốc (tỷ lệ mã hoá có thể đạt tới ~0,8 trong khi thuật toán gốc chỉ đạt tỷ lệ mã hoá ~0,5). Mặt khác thông qua việc bổ sung một lượng thông tin vào vector lỗi đã làm tăng được độ bảo mật của hệ mật, vì bên thứ ba thường chỉ quan tâm đến phần thông tin chính (*m*) nằm trong thuật toán gốc.

+ Hệ mật McEliece cải tiến còn hạn chế là yêu cầu sự thống nhất thuật toán biến đổi phần thông tin bổ sung thành vector lỗi e, điều này dẫn đến sự phức tạp khi sử dụng hệ mật cải tiến này.

+ Với phương pháp cải tiến sử dụng vector lỗi mang tin, tỷ lệ mã hóa có thể được cải thiện từ 0,51 lên 0,79 khi chọn các tham số theo đề xuất gốc $k = 524$, $n = 1024$ và $t = 50$ khi đó l = 284 tính theo công thức (6) (mang 284 bit thông tin bổ sung) và từ 0,63 lên 0,87 khi chọn $k = 654$, $n = 1024$, $t = 37$ và l = 225.

4. ĐỀ XUẤT NÂNG CAO ĐỘ BẢO MẬT CỦA HỆ MẬT McELIECE SỬ DỤNG MÃ NỐI TIẾP THAY THẾ MÃ GOPPA TRONG SƠ ĐỒ GỐC



Hình 5. Sơ đồ khối mã nối tiếp

Giải pháp cơ bản của đề xuất này là sử dụng mã kênh nối tiếp thay thế cho mã Goppa trong thuật toán truyền thống nhằm tăng không gian chìa cho hệ mật McEliece, mà vẫn đảm bảo được độ bảo mật và tốc độ mã. Sơ đồ khối của mã nối tiếp được thể hiện trên hình 5 [8].

Cấu trúc của mã nối tiếp bao gồm một mã ngoài, một mã trong và bộ xáo trộn bít nằm giữa hai mã này có nhiệm vụ phá vỡ các lỗi cụm (lỗi dài) thành các lỗi đơn nhằm mục đích để tăng khả năng sửa lỗi của mã, kể cả trong trường hợp điều kiện kênh truyền quá xấu.

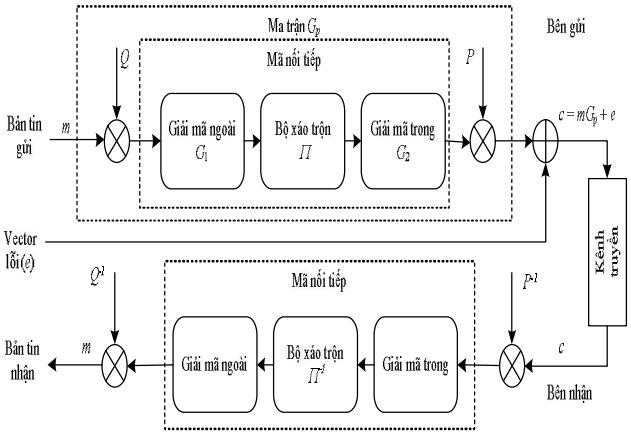
Để áp dụng mã nối tiếp vào hệ mật McEliece, ta cần phải chọn các mã thành phần là các mã khối tuyến tính có các đa thức sinh tương ứng là G_1 và G_2 với các khoảng cách Hamming cực tiểu tương ứng là d_{1min} và d_{2min}. Khi đó, mã nối tiếp có thể sửa được một lỗi cụm có độ dài là $\max(n_1t_2, n_2t_1)$, trong đó n_i là độ dài các từ mã thành phần và t_i là khả năng sửa lỗi của các mã thành phần, được tính theo công thức (9) [8].

$$t_i = \left\lfloor \frac{d_{imin} - 1}{2} \right\rfloor \text{ với } i = 1, 2 \quad (9)$$

Hoặc mã nối tiếp có thể sửa được *t* lỗi ở các vị trí bất kỳ trong từ mã với:

$$t = \left\lfloor \frac{d_{1min}.d_{2min} - 1}{2} \right\rfloor. \quad (10)$$

Sơ đồ khối hệ mật McEliece khi sử dụng mã nối tiếp được thể hiện trong hình 6.



Hình 6. Sơ đồ khối hệ mật McEliece cải tiến sử dụng mã nối tiếp

Các thuật toán của hệ mật McEliece cải tiến sử dụng mã nối tiếp thay thế mã Goppa trong sơ đồ gốc được thực hiện như sau:

Tạo *khóa*:

- Khóa bí mật bao gồm các ma trận Q, G_1, Π, G_2 và P (ở đây ta sử dụng bộ xáo trộn khối).

- Khóa công khai gồm cặp (G_p, *t*). Trong đó: *t* được xác định theo công thức (10) và G_p được xác định theo công thức (11).

$$G_p = QG_1\Pi G_2P \quad (11)$$

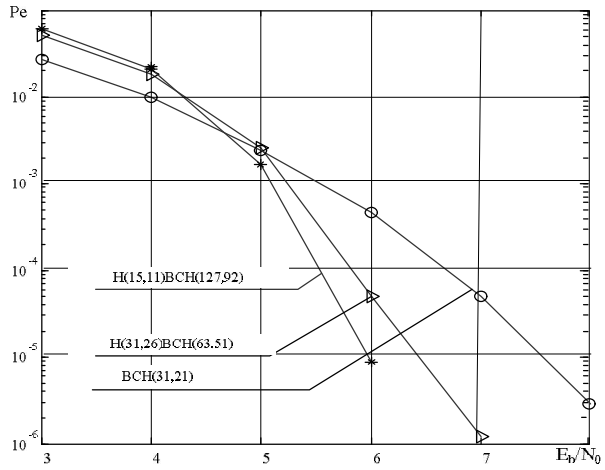
Mã hóa và giải mã:

Quá trình mã hoá và giải mã một bản tin của thuật toán cải tiến đề xuất về cơ bản tương tự như thuật toán McEliece

gốc. Tuy nhiên, khi giải mã kênh ta phải thực hiện qua hai lần giải mã các mã thành phần (mã trong và mã ngoài), với các ma trận kiểm tra được xác định $G_i H_i^T = 0$, trong đó, i = 1 ÷ 2. Đồng thời, sau khi giải mã trong ta phải thực hiện giải xáo trộn để sắp xếp lại vị trí các bit của từ mã trước khi đưa vào giải mã ngoài cho đúng với thứ tự như bên gửi.

Nhận xét đặc điểm thuật toán McEliece cải tiến sử dụng mã nối tiếp:

Thông qua việc sử dụng mã nối tiếp thay thế mã Goppa trong đề xuất gốc, khả năng sửa lỗi của hệ thống được cải thiện một cách đáng kể so với khi sử dụng các mã đơn, điều này thể hiện qua kết quả trên hình 7.



Hình 7. Khả năng sửa lỗi của mã nối tiếp so với các mã đơn

Từ kết quả hình 7 ta thấy, để đạt được xác suất lỗi bit $P_e = 10^{-5}$ trong trường hợp sử dụng mã nối tiếp với các mã thành phần là mã Hamming(31, 26) và mã BCH(63, 51) cần tỷ lệ $E_b/N_0 \approx 5,8$dB, đối với trường hợp sử dụng mã đơn BCH (31, 21) cần $E_b/N_0 \approx 7,5$dB. Tỷ lệ mã hóa trong cả hai trường hợp là $r = k/n \approx 0,67$. Như vậy độ lợi mã hoá đạt được là 1,7 dB. Tương tự như vậy, khi sử dụng mã nối tiếp với các mã thành phần là mã Hamming (15,11) và mã BCH(127, 92) độ lợi mã hoá của hệ thống cao hơn so với trường hợp sử dụng mã đơn. Đây là cơ sở để cải thiện độ mật của hệ thống khi sử dụng thuật toán McEliece, điều này được chứng minh qua phương pháp tính độ bền vững của hệ mật cải tiến theo thuật toán tấn công tìm vector lỗi *e* thể hiện qua công thức (12) [6].

$$k_c = C_n^t \quad (12)$$

Kết quả thuật toán McEliece cải tiến sử dụng mã nối tiếp thay cho mã Goppa so với thuật toán đề xuất gốc được thể hiện qua trong bảng 1.

Bảng 1. So sánh thuật toán McEliece cải tiến và thuật toán gốc

Sơ đồ hệ mật	Tỷ lệ mã hoá	Số lỗi có thể sửa	Độ bền mật mã
Hệ mật McEliece sử dụng mã Goppa(1024,524)	~0,5	50	$C_{1024}^{50} \approx 3,1.10^{88}$
Hệ mật McEliece sử dụng mã nối tiếp H(15,11)BCH(127,92)	~0,8	91	$C_{1905}^{91} \approx 4,46.10^{160}$

Chi phí của thuật toán cải tiến sử dụng mã nối tiếp thay thế mã Goppa thường yêu cầu từ mã có độ dài lớn hơn so với thuật toán gốc. Do đó yêu cầu dung lượng bộ nhớ trong các thiết bị giải mã lớn hơn, nhưng vấn đề này không còn là vấn đề khó khăn trong khoa học công nghệ hiện nay.

5. KẾT LUẬN

Phương pháp đề xuất cải tiến hệ mật McEliece sử dụng vector lỗi mang một phần thông tin đã tăng được tỷ lệ mã hoá từ 0,5 lên đến 0,8 so với thuật toán đề xuất gốc, đồng thời cũng làm tăng độ phức tạp của tấn công giải mã của hệ mật.

Hệ mật McEliece cải tiến sử dụng mã nối tiếp thay thế cho mã Goppa trong đề xuất gốc đã làm tăng được khả năng sửa lỗi và tăng khả năng chống nhiễu của hệ thống. Tỷ lệ mã hóa khi sử dụng mã nối tiếp thay thay thế mã Goppa là tăng 0,17 và độ lợi mã hóa đạt 1,7dB. Hai giải pháp cải tiến tác giả đề xuất trên đây kết hợp với những ưu điểm của hệ mật McEliece, giúp cho hệ mật này tăng thêm tính khả dụng cho các hệ thống truyền tin số.

TÀI LIỆU THAM KHẢO

[1]. McEliece R. J. (1978). A Public-Key Cryptosystem Based on Algebraic Coding Theory, The Deep Space Network Progress Report, pp: 114-116.

[2]. Berlekamp E., McEliece R., and Tilborg H. v. (1978), "On the Inherent Intractability of Certain Coding Problems", IEEE Transactions on Information Theory, 24(3), pp: 384-386.

[3]. Bernstein D. J., Buchmann J., and Dahmen E. (2009), Post-quantum cryptography, Springer-Verlag Berlin Heidelberg, pp: 95-145.

[4]. Patterson N. J. (1975), "The Algebraic Decoding of Goppa Codes", IEEE Transactions on Information Theory, IT-21(2), pp: 203-207.

[5]. Алферов А.П. Основы криптографии. М.: Гелиос АРВ, 2001. С. 321-323.

[6]. Hung min sun. Enhancing the security of the McEliece Public key Cryptosystem.Journal of inffomation science and engineering 16.2000. C 799-812.

[7]. C. S. Park. Improving code rate of McEliece's public key cryptosystem. Electronics letters, Vol. 25, No. 21, 1989, pp. 1466-1467.

[8]. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М: Техносфера, 2005.