TÍNH AN TOÀN IND-CPA CỦA PHƯƠNG PHÁP MÃ HÓA CÓ THỂ CHỐI TỪ DỰA TRÊN GIAO THỨC BA BƯỚC SHAMIR

Nguyễn Đức Tâm*

* Học viện Kỹ thuật mật mã – Ban Cơ yếu Chính phủ

Tóm tắt: Nội dung bài báo phân tích và chứng minh tính đúng đắn, chối từ thuyết phục và an toàn IND-CPA của một phương pháp mã hóa có thể chối từ với quá trình truyền tin mật dựa trên giao thức ba bước Shamir sử dụng thuật toán mã hóa lũy thừa modulo Pohlig-Hellman. Phương pháp mã hóa có thể chối từ này đã được đề xuất trong bài báo [11], nhưng chưa được chứng minh các tính chất cơ bản của một giao thức mã hóa có thể chối từ.

Từ khóa: Mã hóa có thể chối từ, mã hóa xác suất, mã hóa giả xác suất, mã hóa giao hoán, giao thức ba bước Shamir, thuật toán Pohlig-Hellman, IND-CPA.

I. PHẦN MỞ ĐẦU

Các kỹ thuật mã hóa thông thường hiện nay nhằm bảo vệ tính bí mật, an toàn, xác thực của thông tin khi lưu trữ và truyền thông, chống lại các tấn công nhằm thu tin thám mã. Mã hóa có thể chối từ (MHCTCT) là một kỹ thuật mật mã với một cách tiếp cận kỹ thuật khác biệt với mã hóa thông thường. Trong mã hóa thông thường, mỗi bản mã là một cam kết duy nhất của một bản rõ và khóa mã. MHCTCT cho phép giải mã một bản mã cho ra hai bản rõ có ý nghĩa khác nhau, định nghĩa MHCTCT được Canetti và cộng sự công bố lần đầu tại bài báo [1]. MHCTCT được ứng dụng chống lại dạng tấn công cưỡng ép trong trong kịch bản mà kẻ thứ ba chặn thu bản mã truyền trên kênh truyền công cộng và cưỡng ép bên gửi hoặc bên nhận hoặc cả hai bên phải trình ra thuật toán mã hóa, bản rõ và các khóa mã đã sử dụng [1], ứng dụng trong lưu trữ ẩn giấu các hệ thống tệp dữ liệu nhạy cảm [2-4], ứng dụng trong các môi trường giao dịch đa bên không cam kết nội dung như các giao thức bỏ phiếu điện tử, đấu giá điện tử [5].

MHCTCT đã được nghiên cứu và đề xuất cụ thể một số giao thức sử dụng khóa công khai [6], hoặc sử dụng khóa bí mật [7]. Gần đây, một giải pháp MHCTCT được đề xuất sử dụng thuật toán mã hóa giao hoán và khóa bí mật dùng chung trong [8]. Bài toán đảm bảo an toàn của các giao thức MHCTCT chống tấn công cưỡng ép được thảo luận trong các bài báo [9,10]. Ngoài ra, để đảm bảo an toàn chống lại các tấn công cưỡng ép chủ động, cần bổ sung vào trong các giao thức MHCTCT thủ tục xác thực bên gửi và bên nhận [10].

Trong bài báo [11] đã đề xuất phương pháp mã hóa có thể chối từ sử dụng thuật toán lũy thừa modulo Pohlig-Hellman có tính chất giao hoán, trong đó thuật toán mới được mô tả tổng quát về phương pháp còn các tính chất chưa được chứng minh.

Bài báo này sẽ đi mô tả chi tiết quá trình thực hiện giao thức mã hóa, giải mã và thực hiện chối từ khi bị tấn công cưỡng ép, đồng thời phân tích và chứng minh tính đúng đắn, tính chối từ thuyết phục và an toàn IND-CPA của phương pháp được đề xuất trong [11]. Trong nội dung bài báo, Phần II mô tả mô hình truyền tin và ngữ cảnh tấn công. Phần III giới thiệu một số thuật toán sử dụng trong phương pháp đề xuất. Phần IV mô tả lại chi tiết giao thức thực hiện phương pháp mã hóa có thể chối từ trong bài báo [11]. Phần V là một số định nghĩa quan trọng về độ an toàn không phân biệt tính toán. Phần VI chứng minh tính đúng đắn, chối từ và an toàn IND-CPA của phương pháp. Phần VII kết luận.

II. MÔ HÌNH TRUYỀN TIN VÀ NGỮ CẢNH TẤN CÔNG

Mô hình truyền tin và ngữ cảnh tấn công khi hai bên A và B truyền tin mật bằng giao thức ba bước Shamir như sau:

- Giả sử A và B truyền thông điệp bí mật T và ngụy trang một thông điệp giả mạo M cùng kích thước trên cùng bản mã C (trong giao thức ba bước Shamir, quá trình truyền tin thực hiện mã hóa gồm ba bước, tạo ra các bản mã C_1, C_2, C_3). Đối phương tấn công có trong tay các bản mã truyền trên kênh truyền, tiến hành cưỡng ép các bên truyền tin phải trình ra thông điệp rõ, các khóa mã sử dụng và thuật toán mã hóa/giải mã. Một kịch bản thường gặp khác là đối phương tiến hành giả mạo là một trong các bên liên lạc để tấn công giả mạo tích cực.

- Khi bị tấn công cưỡng ép, A (hoặc B, hoặc cả hai bên) để bảo vệ thông điệp bí mật T, các bên sẽ trình ra thông điệp giả mạo M phù hợp hoàn toàn với các bản mã (C_1, C_2, C_3), khóa mã và thuật toán mã hóa/giải mã.

- Nguồn tin đầu vào để mã hóa là (T, M) thay vì chỉ là T. M ở đây đóng vai trò như một lượng thông tin ngẫu nhiên thêm vào. Cách thức thực hiện này giống hệt như các giao thức mã hóa xác suất, khi người ta bổ sung thêm

Tác giả liên lạc: Nguyễn Đức Tâm,
Email: nguyenductamkma@gmail.com
Đến tòa soạn: 2/2020, chỉnh sửa: 4/2020, chấp nhận đăng: 4/2020.

nguồn ngẫu nhiên kết hợp với thông điệp ban đầu trước khi thực hiện mã hóa. Do vậy, để giao thức MHCTCT một cách thuyết phục, thiết kế của nó thường dựa trên giao thức mã hóa xác suất tương ứng.

Các tiêu chí thiết kế hướng tới nhằm mục đích giao thức phải đảm bảo an toàn, chống lại các tình huống tấn công cưỡng ép bởi cả đối phương thụ động hoặc đối phương chủ động giả mạo, các tình huống tấn công được đặt ra là:

- Đối phương chặn được mọi bản mã gửi trên kênh.
- Đối phương cưỡng ép tấn một bên hoặc cả hai bên sau khi các bản mã đã được gửi nhận.
- Mỗi bên hoặc cả hai bên đều buộc phải trình ra: thông điệp rõ, khóa bí mật sử dụng, thuật toán thực hiện trong quá trình truyền tin và phải đảm bảo các bản mã phù hợp hoàn toàn với những thành phần này.
- Đối phương có thể chủ động đóng giả là một trong các bên để tiến hành tấn công giả mạo.

III. MỘT SỐ THUẬT TOÁN SỬ DỤNG

3.1 Giao thức ba bước Shamir

Để thực hiện giao thức ba bước Shamir, thuật toán sử dụng phải có tính chất giao hoán một cách liên tiếp [12], nghĩa là nó cho phép một thông điệp được mã hóa hai bước với bất kỳ một thứ tự nào đều cho ra kết quả như nhau. Với T là thông điệp đầu vào và K_A, K_B là hai khóa mã của hai lần mã khác nhau, thuật toán mã hóa phải đảm bảo:

$$E_{K_A}\left(E_{K_B}(T)\right) = E_{K_B}\left(E_{K_A}(T)\right)$$

do tính chất giao hoán, người nhận luôn nhận được bản rõ chính xác, vì:

$$D_{K_B}\left(D_{K_A}\left(E_{K_A}\left(E_{K_B}(T)\right)\right)\right) = T$$

Mô tả giao thức chi tiết được thực hiện như sau:

1. A cần gửi thông điệp T, A tạo khóa ngẫu nhiên K_A và tính bản mã $C_1 = E_{K_A}(T)$. A gửi C_1 cho B qua kênh mở;

2. B tạo một khóa ngẫu nhiên K_B, mã hóa bản mã C_1 bằng khóa K_B : $C_2 = E_{K_B}(C_1) = E_{K_B}\left(E_{K_A}(T)\right)$, gửi C_2 cho A;

3. A, sử dụng thủ tục giải mã $D = E^{-1}$, tính bản mã $C_3 = D_{K_A}(C_2) = D_{K_A}\left(E_{K_B}\left(E_{K_A}(T)\right)\right) = D_{K_A}\left(E_{K_A}\left(E_{K_B}(T)\right)\right) = E_{K_B}(T)$, gửi C_3 cho B;

B nhận được được C_3, giải mã $M = D_{K_B}(C_3) = D_{K_B}\left(E_{K_B}(T)\right) = T.$

Vì A và B không cần trao đổi khóa trước khi thực hiện liên lạc, nên giao thức ba bước Shamir còn được gọi là giao thức không khóa ba bước Shamir.

3.2 Trao đổi khóa Diffie-Hellman

Giao thức Diffie-Hellman [13], được sử dụng để hai bên A và B thỏa thuận một bí mật chung với nhau (Z_{AB}) thông qua kênh công khai:

$$Z_{AB} = y_B^{x_A} = \left(g^{x_B}\right)^{x_A} = y_A^{x_B} = \left(g^{x_A}\right)^{x_B} = g^{x_B x_A} \bmod p$$

Trong đó: p là một số nguyên tố mạnh ≥ 2048 bít; g là phần tử sinh của $\mathbb{Z}_p^*$; $x_A, x_B \geq 256$ bít là khóa bí mật của A, B; $y_B = g^{x_B} \bmod p, y_A = g^{x_A} \bmod p$ là khóa công khai của A, B.

3.3 Thuật toán mã hóa Pohlig-Hellman

Thuật toán mã hóa giao hoán Pohlig–Hellman [14] sử dụng phép toán lũy thừa modulo để biến đổi thông điệp rõ với một số mũ bí mật e (độ dài tối thiểu của e là 256 bit) sau đó chia modulo cho số nguyên tố p (với p là số nguyên tố an toàn có kích thước đủ lớn). Quá trình mã hóa và giải mã được thực hiện với phép lũy thừa modulo cùng các số mũ e và d tương ứng.

Với thông điệp $M < p,$ các thủ tục mã hóa $E_K(M)$ và giải mã $D_K(C)$ được mô tả như sau:

Thủ tục mã hóa $E_K(M)$:

$$C = E_K(M) = M^e \bmod p$$

Thủ tục giải mã $D_K(C)$:

$$M = D_K(C) = C^d \bmod p = M^{ed} \bmod p$$

Với $D_K = E_K^{-1}$ và khóa mã $K = (e, d)$.

Trong đó cần chọn số e thỏa mãn nguyên tố cùng nhau với $(p-1)$. Tiếp theo, sử dụng thuật toán Eclid mở rộng để tính nghịch đảo tương ứng của e là $d = e^{-1} \bmod (p-1)$.

Mức độ an toàn của thuật toán Pohlig-Hellman chống lại tấn công lựa chọn bản rõ được tính bằng độ phức tạp tính toán của bài toán logarit rời rạc.

IV. PHƯƠNG PHÁP MÃ HÓA CÓ THỂ CHỐI TỪ DỰA TRÊN GIAO THỨC BA BƯỚC SHAMIR

Phương pháp MHCTCT dựa trên giao thức ba bước Shamir được đề xuất trong [11], Phần IV này sẽ đi mô tả lại chi tiết phương pháp này:

Để đảm bảo an toàn cho mã hóa dựa trên phép lũy thừa modulo cần chọn số nguyên tố p là số nguyên tố an toàn, thỏa mãn $(p-1)/2$ là một số nguyên tố. Đồng thời để đảm bảo an toàn ngữ nghĩa cho bản mã, cần bổ sung thêm yếu tố ngẫu nhiên vào nguồn tin ban đầu [15-16] khi đó giao thức mã hóa là giao thức mã hóa xác suất. Nếu thay thế một cách có chủ đích nguồn ngẫu nhiên bằng một thông điệp bí mật, mã hóa xác suất lúc này trở thành mã hóa giả xác suất.

Phương pháp đề xuất cụ thể là sự kết hợp của các thuật toán:

1. Quá trình truyền tin thực hiện theo giao thức ba bước Shamir;

2. Khi bắt đầu thực hiện phiên truyền tin mật, hai bên sử dụng giao thức trao đổi khóa Diffe-Hellman thống nhất với nhau một tham số bí mật dùng chung để thực hiện giao thức chối từ;

3. Thuật toán mã hóa sử dụng là thuật toán lũy thừa modulo Pohlig-Hellman, thuật toán này đảm bảo tính chất giao hoán.

Các bước thực hiện chi tiết:

Bước 1 thống nhất tham số: A và B sử dụng giao thức

Diffie-Hellman tạo khóa phiên công khai (sử dụng một lần) và trao đổi với nhau. Tiếp theo, họ chia sẻ tham số bí mật dùng chung Z_{AB}.

Bước 2 mã hóa: A cần truyền thông điệp mật T, A tạo một thông điệp giả mạo M có cùng kích thước với T. A và B thực hiện quá trình mã hóa truyền tin theo giao thức ba bước không khóa Shamir, sử dụng thuật toán lũy thừa modulo Pohlig-Hellman được trình bày ở mục 3.3 để mã hóa đồng thời (T, M).

Bước 3 giải mã: B có hai chế độ giải mã, chế độ giải mã mật để khôi phục thông điệp mật T; chế độ giải mã chối từ khi bị tấn công cưỡng ép để trình ra cho đối phương tấn công thông điệp giả mạo M.

Trong quá trình mã hóa, A và B sẽ sử dụng giao thức MHCTCT đảm bảo các bản mã (C_1, C_2, C_3) được tạo ra bằng giao thức mã hóa không khóa có thể chối từ (mã hóa đồng thời hai thông điệp M và T) không phân biệt được về mặt tính toán với các bản mã (C_1, C_2, C_3) được tạo ra bằng giao thức mã hóa xác suất khi mã hóa thông điệp M.

Khi bị tấn công cưỡng ép:

A hoặc B hoặc cả hai bên A, B sẽ trình ra thông điệp giả mạo M, các bản mã (C_1, C_2, C_3), giao thức mã hóa xác suất và các khóa giả, đảm bảo mọi thành phần này phù hợp với nhau. Do đó, A và B có đủ lý lẽ hợp lý rằng mình đang sử dụng giao thức mã hóa xác suất để truyền thông điệp (trong khi thực tế là giao thức MHCTCT được hai bên thực sự sử dụng).

Như vậy, phương pháp chối sử dụng hai giao thức:

- *Giao thức thứ nhất là giao thức mã hóa xác suất sử dụng thuật toán Pohlig-Hellman*, đây sẽ là giao thức dùng để trình ra khi bị tấn công cưỡng ép, giao thức được mô tả chi tiết tại 4.1 và được ký hiệu là *giao thức EncPH_F*.

- *Giao thức thứ hai là giao thức mã hóa có thể chối từ giả xác suất sử dụng thuật toán Pohlig-Hellman*, đây là giao thức mà hai bên A, B thực sự dùng để truyền tin mật, giao thức được mô tả chi tiết tại 4.2 và được ký hiệu là giao thức *DenEncPH*.

4.1 Giao thức mã hóa xác suất sử dụng thuật toán Pohlig-Hellman

Giao thức EncPH_F:

A cần truyền thông điệp $M < p$ cho B (để đảm bảo mức an toàn 112 bit, p là số nguyên tố có kích thước *2048 bit* [16] và được hai bên công khai).

** Bước 1: thống nhất tham số*

A tạo một giá trị ngẫu nhiên $k_A < p-1$, đóng vai trò là khóa bí mật sử dụng một lần của A, tính khóa công khai sử dụng một lần của A là $R_A = \alpha^{k_A} \bmod p$, và gửi R_A cho B.

B tạo một giá trị ngẫu nhiên $k_B < p-1$, đóng vai trò là khóa bí mật sử dụng một lần của B, tính khóa công khai sử dụng một lần của B là $R_B = \alpha^{k_B} \bmod p$, và gửi R_B cho A. Lúc này B có giá trị bí mật dủng chung $Z = Z_{AB} = {R_A}^{k_B} \bmod p = \alpha^{k_A \cdot k_B} \bmod p$.

A nhận R_B, ính giá trị dùng chung $Z = Z_{AB} = {R_B}^{k_A} \bmod p = \alpha^{k_B \cdot k_A} \bmod p$.

** Bước 2: mã hóa theo giao thức ba bước Shamir*

B2.1. A tạo khóa riêng $K_A = (e_A, d_A)$, với $\gcd(e_A, p-1) = 1, d_A = e_A^{-1} \bmod (p-1)$, tạo một giá trị ngẫu nhiên ρ_1 với mục đích thêm vào nguồn tin rõ ban đầu, và tính bản mã $C_1 = (C_1', C_1'')$ bằng hệ các hệ phương trình đồng dư tuyến tính sau đây (có sự hiện diện của các tham số Z, ρ_1) với C_1' và C_1'' chưa biết:

$$\begin{cases} C_1' + C_1'' = \rho_1 \bmod p \quad = U_1 \\ C_1' + ZC_1'' = M^{e_A} \bmod p = S_1 \end{cases} \quad (1)$$

Hệ phương trình đồng dư bậc nhất hai ẩn (1) có hai nghiệm C_1', C_1'':

$(C_1' = D^{-1} D_{C_1'} \bmod p; C_1'' = D^{-1} D_{C_1''} \bmod p)$. Với:

D^{-1} là phần tử nghịch đảo của $D = (Z-1) \bmod p$;

$D_{C_1'} = (U_1 Z - S_1) \bmod p$; $D_{C_1''} = (S_1 - U_1) \bmod p$;

Sau đó, A gửi bản mã C_1 cho B.

B2.2. B tạo khóa riêng $K_B = (e_B, d_B)$, với $\gcd(e_B, p-1) = 1, d_B = e_B^{-1} \bmod (p-1)$, tính giá trị $S_1 = M^{e_A} \bmod p = (C_1' + ZC_1'') \bmod p$, tạo một giá trị ngẫu nhiên ρ_2, và tính bản mã $C_2 = (C_2', C_2'')$ bằng hệ phương trình đồng dư tuyến tính sau đây với C_2', C_2'' chưa biết:

$$\begin{cases} C_2' + C_2'' = \rho_2 \bmod p \quad = U_2 \\ C_2' + ZC_2'' = S_1^{e_B} \bmod p = S_2 \end{cases} \quad (2)$$

Hệ phương trình đồng dư bậc nhất hai ẩn (2) có hai nghiệm C_2', C_2'':

$(C_2' = D^{-1} D_{C_2'} \bmod p; C_2'' = D^{-1} D_{C_2''} \bmod p)$. Với:

D^{-1} là phần tử nghịch đảo của $D = (Z-1) \bmod p$;

$D_{C_2'} = (U_2 Z - S_2) \bmod p$; $D_{C_2''} = (S_2 - U_2) \bmod p$;

Tiếp theo, B gửi bản mã C_2 cho A.

B2.3. A tạo một giá trị ngẫu nhiên ρ_3 và tính giá trị $S_2 = S_1^{e_B} \bmod p = (C_2' + ZC_2'') \bmod p$ và bản mã $C_3 = (C_3', C_3'')$ bằng hệ phương trình đồng dư tuyến tính sau với C_3', C_3'' chưa biết:

$$\begin{cases} C_3' + C_3'' = \rho_3 \bmod p \quad = U_3 \\ C_3' + ZC_3'' = S_2^{d_A} \bmod p = S_3 \end{cases} \quad (3)$$

Hệ phương trình đồng dư bậc nhất hai ẩn (3) có hai nghiệm C_3', C_3'':

$(C_3' = D^{-1} D_{C_3'} \bmod p; C_3'' = D^{-1} D_{C_3''} \bmod p)$. Với:

$D_{C_3'} = (U_3 Z - S_3) \bmod p$; $D_{C_3''} = (S_3 - U_3) \bmod p$;

Sau đó, A gửi bản mã C_3 đến B.

** Bước 3: giải mã*

B nhận được C_3, B tính thông điệp M như sau:

$$M = (C_3' + ZC_3'')^{d_B} \bmod p \quad (4)$$

Lưu ý rằng, trong giao thức, các giá trị ρ_i

$(i = 1, 2, 3)$ ngẫu nhiên thêm vào trong quá trình mã hóa với giả thiết 1 như sau:

Giả thiết 1 *Các giá trị* $\rho_i\,(i=1,2,3)$ *thêm vào trong quá trình mã hóa ba bước của giao thức EncPH_F nhằm mục đích tăng tính ngẫu nhiên của các bản mã, các giá trị ngẫu nhiên này không lưu nhớ trong bộ nhớ của máy tính (máy lập mã và máy giải mã).*

Mệnh đề 1 *Nếu A, B sử dụng giao thức DenEncPH thực hiện mã hóa và truyền tin thông điệp* M *bằng quá trình thực hiện ba bước có bổ sung các giá trị ngẫu nhiên* $\rho_i\,(i=1,2,3)$. *Thì khi B thực hiện giải mã sẽ khôi phục chính xác thông điệp* M *mà không phụ thuộc các giá trị* ρ_i *thêm vào.*

Chứng minh:

Trong giao thức *EncPH_F*, có các công thức sau không có sự tham gia của các ngẫu nhiên ρ_i:

$S_1 = M^{e_A} \bmod p;$

$S_2 = S_1^{e_B} \bmod p = M^{e_A e_B} \bmod p;$

$C_3' + ZC'' = S_2^{d_A} \bmod p = M^{e_A e_B d_A} \bmod p = M^{e_B} \bmod p;$

khi B thực hiện giải mã bằng công thức (4):

$$M = \left(C_3' + ZC_3''\right)^{d_B} \bmod p = M^{e_B d_B} \bmod p = M \qquad (5)$$

Ta có mệnh đề 1 được chứng minh.

4.2 Giao thức mã hóa có thể chối từ sử dụng thuật toán Pohlig-Hellman

A cần truyền thông điệp $T < p$ sang cho B, A ngụy trang bằng thông điệp giả mạo M có cùng kích thước với T, giao thức truyền tin được mô tả chi tiết các bước thực hiện như sau:

Giao thức DenEncPH:

Bước 1: thống nhất tham số

Hoàn toàn tương tự như giao thức *EncPH_F*, A và B dùng giao thức trao đổi Diffie-Hellman thống nhất tham số bí mật dùng chung Z:

$$Z = Z_{AB} = R_B{}^{k_A} \bmod p = (\alpha^{k_B})^{k_A} \bmod p$$
$$= R_A{}^{k_B} \bmod p = (\alpha^{k_A})^{k_B} \bmod p$$

Bước 2: mã hóa theo giao thức ba bước Shamir

B 2.1. A tạo các khóa riêng $K_A = (e_A, d_A)$, với $\gcd(e_A, p-1) = 1, d_A = e_A^{-1} \bmod (p-1)$, và $Q_A = (\varepsilon_A, \delta_A)$, với $\gcd(\varepsilon_A, p-1) = 1$, $\delta_A = \varepsilon_A^{-1} \bmod (p-1)$, tính bản mã $C_1 = (C_1', C_1'')$ bằng cách giải hệ phương trình sau đây để tìm (C_1', C_1''):

$$\begin{cases} C_1' + Z^2 C_1'' = T^{\varepsilon_A} \bmod p = U_1 \\ C_1' + ZC_1'' = M^{e_A} \bmod p = S_1 \end{cases} \qquad (6)$$

Hệ phương trình đồng dư bậc nhất hai ẩn (6) có hai nghiệm C_1', C_1'':

$(C_1' = D^{-1} D_{C_1'} \bmod p; C_1'' = D^{-1} D_{C_1''} \bmod p)$. Với:

D^{-1} là phần tử nghịch đảo của $D = (Z - Z^2) \bmod p;$

$D_{C_1'} = (U_1 Z - S_1 Z^2) \bmod p;\ D_{C_1''} = (S_1 - U_1) \bmod p;$

Tiếp theo, A gửi bản mã C_1 sang B.

B 2.2. B, tạo khóa riêng $K_B = (e_B, d_B)$, với $\gcd(e_B, p-1) = 1, d_B = e_B^1 \bmod (p-1)$, $Q_B = (\varepsilon_B, \delta_B)$, với $\gcd(\varepsilon_B, p-1) = 1, \delta_B = \varepsilon_B^{-1} \bmod (p-1)$, tính các giá trị $U_1 \equiv T^{\varepsilon_A} \equiv \left(C_1' + Z^2 C_1''\right) \bmod p,$ $S_1 \equiv M^{e_A} \equiv \left(C_1' + ZC_1''\right) \bmod p,$ tính $C_2 = (C_2', C_2'')$ bằng hệ phương trình đồng dư tuyến tính sau đây với (C_2', C_2'') chưa biết:

$$\begin{cases} C_2' + Z^2 C_2'' = U_1^{e_B} \bmod p = U_2 \\ C_2' + ZC_2'' = S_1^{e_B} \bmod p = S_2 \end{cases} \qquad (7)$$

Hệ phương trình đồng dư bậc nhất hai ẩn (7) có hai nghiệm C_2', C_2'':

$(C_2' = D^{-1} D_{C_2'} \bmod p; C_2' = D^{-1} D_{C_2''} \bmod p)$. Với:

D^{-1} là phần tử nghịch đảo của $D = (Z - Z^2) \bmod p;$

$D_{C_2'} = (U_2 Z - S_2 Z^2) \bmod p;\ D_{C_2''} = (S_2 - U_2) \bmod p;$

Tiếp theo, B gửi bản mã C_2 sang cho A.

B 2.3. A tính giá trị $U_2 \equiv U_1^{e_B} \equiv \left(C_2' + Z^2 C_2''\right) \bmod p,$ $S_2 \equiv S_1^{e_B} \equiv \left(C_2' + ZC_2''\right) \bmod p,$ và bản mã $C_3 = (C_3', C_3'')$ bằng hệ phương trình đồng dư tuyến tính sau với C_3', C_3'' chưa biết:

$$\begin{cases} C_3' + Z^2 C_3'' = U_2^{\delta_A} \bmod p = U_3 \\ C_3' + ZC_3'' = S_2^{d_A} \bmod p = S_3 \end{cases} \qquad (8)$$

Hệ phương trình đồng dư bậc nhất hai ẩn (8) có hai nghiệm C_3', C_3'':

$(C_3' = D^{-1} D_{C_3'} \bmod p; C_3' = D^{-1} D_{C_3''} \bmod p)$. Với:

$D_{C_3'} = (U_3 Z - S_3 Z^2) \bmod p;\ D_{C_2''} = (S_3 - U_3) \bmod p;$

Tiếp theo, A gửi bản mã C_3 sang B.

Bước 3:giải mã

+ Giải mã ở chế độ truyền tin mật

B nhận được C_3, B giải mã ở chế độ truyền tin mật để khôi phục thông điệp bí mật T như sau:

$$T = \left(C_3' + Z^2 C_3''\right)^{\delta_B} \bmod p \qquad (9)$$

+ Giải mã ở chế độ bị tấn công cưỡng ép

Nếu bị tấn công cưỡng ép, B trình ra thông điệp giả mạo M như sau:

$$M = \left(C_3' + ZC_3''\right)^{d_B} \bmod p \qquad (10)$$

V. MỘT SỐ ĐỊNH NGHĨA QUAN TRỌNG VỀ ĐỘ AN TOÀN KHÔNG PHÂN BIỆT TÍNH TOÁN

Định nghĩa 1 *[17] Một thuật toán* ϕ *được gọi là chạy trong thời gian đa thức nếu tồn tại một đa thức* $p(n)$ *sao cho với mọi chuỗi đầu vào* x *có độ dài* n *bít, thuật toán* $\phi(x)$ *kết thúc sau nhiều nhất là* $p(n)$ *bước.*

Định nghĩa 2 *[17] Một hàm* $\delta(n)$ *được gọi là không đáng kể (negligible) theo biến n, nếu với mọi đa thức* $p(n)$, *luôn tồn tại một số nguyên* n_0 *sao cho*

$\delta(n) < \frac{1}{p(n)}$ *khi* $n > n_0$.

Một hàm không đáng kể hay sử dụng là [17]: $\frac{1}{2^n}$

Định nghĩa 3 *[1] Cho* $A = \{A_n\}_{n\in N}$ *và* $B = \{B_n\}_{n\in N}$ *là hai phân bố xác suất và* $\delta : N \to [0,1]$. *Chúng ta nói* A *và* B *là* $\delta(n)-$*đóng nếu với mỗi bộ phân biệt thời gian đa thức D và với* $\forall n$ *đủ lớn,* $\left|\text{Prob}(D(A_n)=1) - \text{Prob}(D(B_n)=1)\right| < \delta(n)$. *Nếu* $\delta(n)$ *là không đáng kể thì chúng ta nói rằng* A *và* B *là không phân biệt tính toán và được viết là* $A \overset{c}{\approx} B$.

Định nghĩa 4 *[17] Một đánh giá độ an toàn không phân biệt tính toán với tấn công CPA của một hệ mật khóa bí mật với giao thức truyền tin mật* $\pi(Gen, Enc, Dec)$ *gồm các thủ tục tạo khóa Gen, mã hóa Enc, giải mã Dec, với ký hiệu là* $SecK^{CPA}_{E.\pi}(n)$ *được mô tả như sau:*

Đối phương tấn công E chọn một cặp bản rõ m_0, m_1 *có cùng độ dài đưa vào thủ tục mã hóa.*

Một khóa bí mật k ngẫu nhiên có kích thước n *bít và một bít ngẫu nhiên* $b \in \{0,1\}$ *được chọn để mã hóa* m_b *và trả lại cho E bản mã* $C = Enc_k(m_b)$ *được gọi là bản mã thách thức.*

E có quyền truy cập không giới hạn tới thủ tục mã hóa Enc

Sau khi nhận được bản mã C, *để đoán bít* b, *E thực hiện một thuật toán nào đó và có giá trị* b'.

Kết quả của đánh giá là 1 nếu $b' = b$ *và là 0 nếu khác nhau.*

Định nghĩa 5 *[17] Một hệ mật khóa bí mật có kích thước khóa bí mật* n *bít được gọi là có độ an toàn không phân biệt tính toán bằng tấn công bản rõ chọn trước (IND-CPA) nếu với mọi thuật toán trong thời gian đa thức, xác suất để* $SecK^{CPA}_{E.\pi}(n)$ *có kết quả là 1 là:*

$$\Pr[SecK^{CPA}_{E.\pi}(n) = 1] \le \frac{1}{2} + \delta(n), \quad \text{với } \delta(n) \text{ là một hàm không đáng kể của } n.$$

VI. TÍNH ĐÚNG ĐẮN, CHỐI TỪ THUYẾT PHỤC VÀ AN TOÀN IND-CPA CỦA PHƯƠNG PHÁP ĐỀ XUẤT

6.1 Tính đúng đắn

Mệnh đề 2 *Nếu A, B dùng giao thức DenEncPH để mã hóa điệp bí mật* T *và ngụy trang bằng thông điệp giả mạo* M *cùng kích thước. Thì khi B giải mã ở chế độ truyền tin mật luôn khôi phục được chính xác thông điệp bí mật* T.

Chứng minh:

- Khi B giải mã ở chế độ truyền tin mật, khôi phục thông điệp bí mật T, Ta có: trong giao thức *DenEncPH*, từ các công thức:

$U_1 = T^{\varepsilon_A} \bmod p$;

$U_2 = U_1^{\varepsilon_B} \bmod p = T^{\varepsilon_A \varepsilon_B} \bmod p$;

$C_3' + Z^2 C_3'' = U_2^{\delta_A} \bmod p = T^{\varepsilon_A \varepsilon_B \delta_A} \bmod p$

B thay các công thức này vào công thức giải mã (9) tại giao thức *DenEncPH*:

$$\begin{aligned} T &= \left(C_3' + Z^2 C_3''\right)^{\delta_B} \bmod p \\ &= \left(T^{\varepsilon_A \varepsilon_B \delta_A}\right)^{\delta_B} \bmod p = T \bmod p \end{aligned} \quad (11)$$

Ta có mệnh đề 2 được chứng minh.

6.2 Tính chối từ thuyết phục

Mệnh đề 3 *Khi hai bên A, B sử dụng giao thức DenEncPH để truyền thông điệp bí mật* T *và ngụy trang bằng thông điệp giả mạo* M *cùng kích thước. Nếu đối phương tấn công chặn thu được các bản mã* (C_1, C_2, C_3) *và tiến hành cưỡng ép A hoặc B hoặc cả hai bên:*

1. Khi đối phương cưỡng ép bên nhận B, B sẽ trình ra bí mật dùng chung Z, *khóa mã giả mạo* (e_B, d_B), *giao thức mã hóa xác suất EncPH_F, các thành phần này hoàn toàn phù hợp với các bản mã* (C_1, C_2, C_3) *và thực hiện giải mã* (C_1, C_2, C_3) *bằng giao thức EncPH_F khôi phục được chính xác thông điệp giả mạo* M. *(CM 3-1)*

2. Khi đối phương tấn công cưỡng ép bên gửi A, A sẽ trình ra tham số bí mật dùng chung Z, *khóa mã giả mạo* (e_A, d_A) *và dùng giao thức mã hóa xác suất EncPH_F mã hóa thông điệp giả mạo* M *tạo ra các bản mã* (C_1^*, C_2, C_3^*) *hoàn toàn phù hợp với giao thức mã hóa xác suất và thuật toán mã hóa. (CM 3-2)*

3. Khi đối phương cưỡng ép đồng thời hai bên. B sẽ trình ra bí mật dùng chung Z, *khóa mã giả mạo* (e_B, d_B), *giao thức mã hóa xác suất EncPH_F hoàn toàn phù hợp với các bản mã* (C_1, C_2, C_3) *và thực hiện giải mã* (C_1, C_2, C_3) *bằng giao thức DenEncPH khôi phục được chính xác thông điệp giả mạo* M. *Đồng thời A sẽ trình ra tham số bí mật dùng chung* Z, *khóa mã giả mạo* (e_A, d_A) *và dùng giao thức mã hóa xác suất EncPH_F mã hóa thông điệp giả mạo* M *tạo ra các bản mã* (C_1^*, C_2, C_3^*) *hoàn toàn phù hợp với giao thức mã hóa xác suất và thuật toán mã hóa. (CM 3-3)*

Chứng minh:

CM 3-1. Khi B bị tấn công cưỡng ép, B sử dụng các bản mã (C_1, C_2, C_3) (được tạo ra từ giao thức *DenEncPH* và đã có trong tay đối phương tấn công), tham số bí mật dùng chung Z, khóa mã giả mạo (e_B, d_B), thuật toán giải mã trong giao thức *DenEncPH* khôi phục chính xác thông điệp giả mạo M và trình ra cho đối phương như sau:

Ta có, do trong cả hai giao thức *EncPH_F* và giao thức *DenEncPH* đều sử dụng chung các giá trị: tham số bí mật Z, các khóa giả mạo $(e_A, d_A), (e_B, d_B)$ và các công thức tính các giá trị trung gian giống nhau:

$S_1 = M^{e_A} \bmod p$;

$S_2 = S_1^{e_B} \bmod p = M^{e_A e_B} \bmod p$;

$\left(C_3' + Z^2 C_3''\right) = S_2^{d_A} \bmod p = M^{e_A e_B d_A} \bmod p$;

B sử dụng công thức (10) trong giao thức *DenEncPH* (trùng hoàn toàn với công thức (4) của giao thức *EncPH_F*) để giải mã khôi phục chính xác M :

$$M = \left(C_3' + ZC_3''\right)^{d_B} \bmod p = \left(M^{e_A e_B d_A}\right)^{d_B} \bmod p = M \bmod p \quad (12)$$

Ta có điều phải chứng minh (CM 3-1)

CM 3-2. Khi A bị ép buộc thực hiện lại quá trình mã hóa, A sử dụng tham số bí mật dùng chung Z, khóa mã giả mạo (e_A, d_A), giao thức *EncPH_F* để mã hóa thông điệp giả mạo M:

- Đầu vào bước 1 mã hóa của giao thức *EncPH_F* lúc này là M và ρ_1^*, với ρ_1^* là giá trị ngẫu nhiên do A tạo ra (theo *giả thiết 1*), dựa vào hệ phương trình (1), A tính bản mã $C_1^* = (C_1^{*'}, C_1^{*''})$:

$$\begin{cases} C_1^{*'} + C_1^{*''} = \rho_1^* \bmod p \\ C_1^{*'} + ZC_1^{*''} = M^{e_A} \bmod p \end{cases}$$

- Đầu vào bước 3 mã hóa của giao thức *EncPH_F* lúc này là $C_2 = (C_2', C_2'')$ và ρ_3^*, với C_2 là bản mã A nhận được từ B khi thực hiện giao thức *DenEncPH* lúc trước, ρ_3^* là giá trị ngẫu nhiên do A tạo ra (theo *giả thiết 1*), A tính giá trị trung gian $S_2 = S_1^{e_B} \bmod p = \left(C_2' + ZC_2''\right) \bmod p$, tiếp đó dựa vào hệ phương trình (3), A tính bản mã $C_3^* = (C_3^{*'}, C_3^{*''})$:

$$\begin{cases} C_3^{*'} + C_3^{*''} = \rho_3^* \bmod p \\ C_3^{*'} + ZC_3^{*''} = S_2^{d_A} \bmod p \end{cases}$$

Như vậy các bản mã do A trình ra cho đối phương sẽ là $\left(C_1^*, C_2, C_3^*\right)$ khác với các bản mã đang có trong tay của đối phương là $\left(C_1, C_2, C_3\right)$. Điều này được lý giải hoàn toàn hợp lý bằng *giả thiết 1*, do các giá trị ngẫu nhiên $\rho_i\ (i = 1,2,3)$ thêm vào quá trình mã hóa ba bước của giao thức mã hóa xác suất *EncPH_F* và không lưu nhớ trong máy tính, nên mỗi lần thực hiện lại quá trình mã hóa với cùng một bản rõ M, các bản mã tạo ra sẽ khác nhau.

Ta có điều phải chứng minh (CM 3-2).

CM 3-3. Từ chứng minh (CM 3-1) kết hợp đồng thời với (CM 3-2), có điều phải chứng minh (CM 3-3)

Kết hợp các chứng minh (CM 3-1), (CM 3-2), (CM 3-3) ta có mệnh đề 3 được chứng minh.

6.3 Tính an toàn IND-CPA

Mệnh đề 4 *Với cùng một thông điệp giả mạo M và cùng một khóa giả mạo $K_A = (e_A, d_A), K_B = (e_B, d_B)$. Với khóa thật bí mật $Q_A = (\varepsilon_A, \delta_A), Q_B = (\varepsilon_B, \delta_B)$ cùng các giá trị ngẫu nhiên ρ_i trong giao thức EncPH_F được chọn ngẫu nhiên và có phân phối xác suất đều trong $\square_p$, thì khi thực hiện mã hóa truyền tin thông điệp bí mật T, các bản mã (C_1, C_2, C_3) tạo ra từ giao thức EncPH_F thỏa mãn tính chất không phân biệt tính toán với các bản mã (C_1, C_2, C_3) tạo ra từ giao thức DenEncPH.*

Như vậy ta phải đi chứng minh: khi kẻ tấn công E có các bản mã (C_1, C_2, C_3) trong tay, xác suất để các bản mã này được tạo ra từ việc mã hóa (M, ρ_i) bằng giao thức *EncPH_F* hoặc được tạo ra từ việc mã hóa (M, T) bằng giao thức *DenEncPH* là $\left(\frac{1}{2} + \delta(n)\right)$.

Để tiện chứng minh, do p là một số nguyên tố cỡ n bit, ta đặt $p = 2^{n-1} + \omega$, trong đó ω là một số cụ thể nào đó.

Chứng minh:

Bản mã (C_1, C_2, C_3) gồm ba bản mã ở ba bước mã hóa của quá trình thực hiện mã hóa theo giao thức ba bước Shamir. Ở mỗi bước thứ i, mỗi bản mã gồm hai thành phần là C_i', C_i''.

Ta có: *Tại Bước 1 của quá trình mã hóa theo giao thức ba bước Shamir:*

Để chứng minh, trong thủ tục tấn công bản rõ lựa chọn, sau khi nhận được bản mã thách thức C_1 tương ứng với bản rõ m_b. Kẻ tấn công E chỉ có thể đoán đúng $b' = b$ bằng một trong hai cách sau:

1. Đoán ngẫu nhiên với xác suất bằng 1/2.

2. Chọn ngẫu nhiên $b' \in \{0,1\}$ và truy vấn bộ mã hóa (*EncPH_F* hoặc *DenEncPH*) với $p(n)$ lần, sử dụng đầu vào là m_b và các khóa bí mật ngẫu nhiên để có bản mã C_1^* cho đến khi $C_1^* = C_1$. Ở đây $p(n)$ là một đa thức của n để đảm bảo chắc chắn tấn công này có thể thực thi trong thời gian đa thức.

Khi đó xác suất để E đoán thành công là:

$$\Pr[SecK_{E.\pi}^{CPA}(n) = 1] = \frac{1}{2} + p(n).\Pr[C_1^* = C_1] \quad (11)$$

do bản mã tại mỗi bước gồm hai thành phần nên, công thức (11) tương đương với hai công thức:

$$\Pr[SecK_{E.\pi}^{CPA}(n) = 1] = \frac{1}{2} + p(n).\Pr[C_1^{*'} = C_1'] \quad (11a)$$

$$\Pr[SecK_{E.\pi}^{CPA}(n) = 1] = \frac{1}{2} + p(n).\Pr[C_1^{*''} = C_1''] \quad (11b)$$

* *Khi* E *truy vấn bộ mã hóa EncPH_F:*

Với $m_b = (M_b, \rho_{bi}); b \in \{0,1\}$, Ta có, dựa vào công thức tính nghiệm của hệ phương trình (1):

$$\Pr[C_1^{*'} = C_1'] =$$
$$= \Pr[(U_{1EncPH\_F} Z - S_{1EncPH\_F})(Z-1)^{-1} \bmod p = C_1']$$
$$= \Pr[(\rho_b Z - M_b^{e_A}) \bmod p = C_1'(Z\text{-}1) \bmod p]$$
$$= \Pr[M_b^{e_A} \bmod p = (\rho_b Z - C_1'(Z\text{-}1)) \bmod p]$$
$$= \Pr[e_A = \log_{M_b}(\rho_b Z - C_1'(Z\text{-}1))]$$

do e_A được bộ mã hóa chọn ngẫu nhiên trong $\square_p$, và M_b, ρ_b, Z, C_1' không đổi nên:

$$\Pr[e_A = \log_{M_b}((\rho_b \bmod p)Z - C_1')] = \Pr[e_A] = \frac{1}{p-1} = \frac{1}{(2^{n-1} + \omega) - 1}$$

Do $\frac{1}{(2^{n-1} + \omega) - 1} < \frac{1}{2^{n-1}}$, theo định nghĩa (2) thì $\frac{1}{2^{n-1}}$ là một hàm không đáng kể theo biến n, nên

$\frac{1}{(2^{n-1}+\omega)-1}$ cũng là hàm không đáng kể theo biến n.

Do $p(n)$ là một đa thức nên: $\frac{p(n)}{(2^{n-1}+\omega)-1}$ cũng là một hàm không đáng kể của n, thay vào biểu thức (11a) ta có điều phải chứng minh $(C_1^{*'},C_1^{'})$ thỏa mãn IND-CPA.

Lập luận hoàn toàn tương tự cho biểu thức:

$\Pr[C_1^{*''}=C_1^{''}]$

$=\Pr[(S_{1EncPH\_F}-U_{1EncPH\_F})(Z-1)^{-1} \bmod p = C_1^{''}]$

$=\Pr[(M_b^{e_A}-(\rho_b \bmod p))(Z-1)^{-1} \bmod p = C_1^{''}]$

$=\Pr[(M_b^{e_A}-(\rho_b \bmod p)) \bmod p = C_1^{''}(Z-1) \bmod p]$

$=\Pr[M_b^{e_A} \bmod p = (C_1^{''}(Z-1)+\rho_b) \bmod p]$

$=\Pr[e_A=\log_{M_b}(C_1^{''}(Z-1)+\rho_b)]$

$=\Pr[e_A]=\frac{1}{p-1}=\frac{1}{2^{n-1}+\omega-1}$

Như đã chứng minh, do $\frac{1}{(2^{n-1}+\omega)-1}$ là hàm không đáng kể theo biến n, do $p(n)$ là một đa thức nên: $\frac{p(n)}{(2^{n-1}+\omega)-1}$ cũng là một hàm không đáng kể của n, thay vào biểu thức (11b), ta có điều phải chứng minh $(C_1^{*''},C_1^{''})$ thỏa mãn IND-CPA.

* *Khi* E *truy vấn bộ mã hóa DenEncPH:*

Ta có, từ việc giải nghiệm của hệ phương trình đồng dư (1), (6), và các giá trị $(Z,S_1=M^{e_A} \bmod p)$ ở cả hai giao thức là hoàn toàn giống hệt nhau và được coi như là hằng số khi E chọn lựa bản rõ m_b để thực hiện thủ tục tấn công CPA, với $m_b=(M,T_b); b\in\{0,1\}$. Từ (6):

$\Pr[C_1^{*'}=C_1^{'}]=$

$=\Pr[(U_{1DenEncPH}Z-S_{1DenEncPH}Z^2)(Z-Z^2)^{-1} \bmod p = C_1^{'}]$

$=\Pr[(T_b^{\varepsilon_A}Z-M^{e_A}Z^2)(Z-Z^2)^{-1} \bmod p = C_1^{'}]$

$=\Pr[(T_b^{\varepsilon_A}-M^{e_A}Z)Z.Z^{-1}(1-Z)^{-1} \bmod p = C_1^{'}]$

$=\Pr[(T_b^{\varepsilon_A}-M^{e_A}Z) \bmod p = C_1^{'}(1-Z) \bmod p]$

$=\Pr[T_b^{\varepsilon_A} \bmod p = (C_1^{'}(1-Z)+M^{e_A}) \bmod p]$

$=\Pr[\varepsilon_A=\log_{T_b}(C_1^{'}(1-Z)+M^{e_A})]$

do ε_A được bộ mã hóa chọn ngẫu nhiên trong $\square_p$, và $T_b, M, e_A, Z, C_1^{'}$ không đổi nên:

$=\Pr[\varepsilon_A]=\frac{1}{p-1}=\frac{1}{2^{n-1}+\omega-1}$

Như đã chứng minh, do $\frac{1}{(2^{n-1}+\omega)-1}$ là hàm không đáng kể theo biến n, do $p(n)$ là một đa thức nên: $\frac{p(n)}{(2^{n-1}+\omega)-1}$ cũng là một hàm không đáng kể của n, thay vào biểu thức (11a) ta có điều phải chứng minh $(C_1^{*'},C_1^{'})$ thỏa mãn IND-CPA.

Lập luận hoàn toàn tương tự cho:

$\Pr[C_1^{*''}=C_1^{''}]=$

$=\Pr[(S_{1DenEncPH}-U_{1DenEncPH})(Z-Z^2)^{-1} \bmod p = C_1^{''}]$

$=\Pr[(M^{e_A}-T_b^{\varepsilon_A}) \bmod p = C_1^{''}(Z-Z^2) \bmod p]$

$=\Pr[T_b^{\varepsilon_A} \bmod p = (M^{e_A}-C_1^{''}(Z-Z^2)) \bmod p]$

$=\Pr[\varepsilon_A=\log_{T_b}(M^{e_A}-C_1^{''}(Z-Z^2))]$

$=\Pr[\varepsilon_A]=\frac{1}{p-1}=\frac{1}{2^{n-1}+\omega-1}$

Như đã chứng minh, do $\frac{1}{(2^{n-1}+\omega)-1}$ là hàm không đáng kể theo biến n, do $p(n)$ là một đa thức nên: $\frac{p(n)}{(2^{n-1}+\omega)-1}$ cũng là một hàm không đáng kể của n, thay vào biểu thức (11b), ta có điều phải chứng minh $(C_1^{*''},C_1^{''})$ thỏa mãn IND-CPA.

Như vậy ta có điều phải chứng minh về tính không phân biệt tính toán giữa bản mã tạo ra ở Bước 1 của giao thức mã hóa xác suất *EncPH_F* và bản mã tạo ra ở Bước 1 của giao thức mã hóa có thể chối từ *DenEncPH*.

Trong quá trình mã hóa ba bước, do định dạng hệ phương trình đồng dư tuyến tính ở Bước 2 và Bước 3 hoàn toàn tương tự như Bước 1, với cách lập luận tương tự như trên để chứng minh IND-CPA cho các cặp bản mã (C_2^*,C_2), (C_3^*,C_3).

Ta có điều phải chứng minh phương pháp mã hóa giả xác suất như trình bày thỏa mãn tính chất IND-CPA.

6.4 Nhận xét độ an toàn của giao thức mã hóa

1. Như chứng minh ở mệnh đề 3, phương pháp MHCTCT đề xuất có khả năng chối từ thuyết phục bên gửi hoặc bên nhận hoặc đồng thời cả hai bên. Như chứng minh tại mệnh đề 4, phương pháp đề xuất đảm bảo tính an toàn IND-CPA của các bản mã đầu ra.

2. Khi bị cưỡng ép bởi đối phương tấn công thụ động (đã thu được các bản mã C_1,C_2,C_3), bên gửi hoặc bên nhận hoặc cả hai bên trình ra thông điệp giả mạo M, thuật toán mã hóa, các khóa $k_A,R_A,Z,(e_A,d_A)$ hoặc $k_B,R_B,Z,(e_B,d_B)$ hoặc $k_A,R_A,k_B,R_B,Z,(e_A,d_A)$, (e_B,d_B) hoàn toàn phù hợp với nhau. Hai bên cũng chứng minh rằng đã dùng giao thức mã hóa xác suất để gửi an toàn thông điệp M. Và theo mệnh đề 4, các bản mã có trong tay đối phương tấn công đảm bảo không phân biệt tính toán với các bản mã do hai bên trình ra.

Đối phương tấn công có hai cách để có các bản mã (C_1,C_2,C_3), cách thứ nhất là thu được trên kênh truyền công cộng (các bản mã này được tạo ra từ giao thức mã hóa có thể chối từ giả xác suất – giao thức *DenEncPH*), cách thứ hai dựa vào bộ tham số và thuật toán do hai bên liên lạc trình ra với đối phương tấn công (các bản mã được tạo ra từ giao thức mã hóa xác suất – giao thức *EncPH_F*). Đối phương tấn công có hai khả năng sau: *i) đồng ý với những người dùng* và *ii) chứng minh các bản mã được tạo ra bằng giao thức MHCTCT*. Tuy nhiên, khả năng thứ hai không khả thi vì không có manh mối. Từ các bản mã (C_1,C_2,C_3) có trong tay, đối phương tấn công có

thể khôi phục lại các giá trị ngẫu nhiên thêm vào $\rho_i = (C_i^{'} + C_i^{''}) \bmod p \ \ (i = 1,2,3)$ (thực chất là các giá trị $T^{\varepsilon_A} \bmod p, U_1^{\varepsilon_B} \bmod p, U_2^{\delta_A} \bmod p$ được tạo ra từ giao thức *DenEncPH*), để từ các giá trị này để tính ra thông điệp bí mật T, đối phương tấn công phải tính một trong các khóa riêng $Q_A(\varepsilon_A, \delta_A), Q_B(\varepsilon_B, \delta_B)$. Việc tính ra một trong các khóa riêng Q_{A} hoặc Q_{B} được thực hiện bằng cách giải bài toán logarith rời rạc modulo p, với cách chọn p như mô tả thì độ khó bài toán đủ đảm bảo an toàn cho giao thức.

3. Để chống lại tấn công giả mạo tích cực, khi mà đối phương tấn công giả mạo là một trong các bên tham gia truyền tin, giao thức có thể được bổ sung thủ tục xác thực giữa hai bên trước khi thực hiện quá trình trao đổi tham số bí mật và mã hóa như cách thức thực hiện trong bài báo [18]. Hoặc một cách đơn giản để xác thực giữa hai bên đó là hai bên thống nhất trước một thuật toán bí mật để rút trích ra bộ tham số bí mật sử dụng trong thiết lập các hệ phương trình (1) đến (10) từ tham số bí mật dùng chung Z_{AB} được thỏa thuận ở phiên liên lạc, kỹ thuật này được giới thiệu trong bài báo [19]. Tuy nhiên, nếu có quá trình thống nhất thuật toán bí mật này từ trước, khi đó lược đồ mã hóa trở thành một lược đồ mã hóa có chia sẻ trước một quy ước bí mật.

VII. KẾT LUẬN

Giao thức đề xuất trong [11] sử dụng thuật toán mã hóa Pohlig-Hellman có tính chất giao hoán, thực hiện quá trình truyền tin mật như một quá trình không trao đổi khóa trước phiên liên lạc, mã hóa đồng thời thông điệp mật và thông điệp giả mạo, sử dụng kỹ thuật thỏa thuận khóa Diffie-Hellman chia sẻ tham số bí mật dùng chung sử dụng một lần. Để có thể ngụy trang được trong quá trình thực hiện truyền tin, cùng với giao thức MHCTCT thực sự dùng thật trong truyền tin mật, một giao thức mã hóa xác suất được xây dựng để trình ra cho đối phương tấn công. Do giao thức MHCTCT xây dựng dựa trên giao thức mã hóa xác suất với việc thay thế nguồn ngẫu nhiên bằng thông điệp giả bí mật có chủ đích vào quá trình mã hóa, vì vậy nó được coi như là một giao thức mã hóa giả xác suất.

Như chứng minh tại bài báo này, giao thức MHCTCT sử dụng thuật toán mã hóa Pohlig-Hellman thỏa mãn đầy đủ tính chất của một lược đồ MHCTCT theo định nghĩa của Canetti [1] đó là tính đúng đắn, tính an toàn IND-CPA và tính chối từ thuyết phục. Các bản mã tạo ra từ giao thức MHCTCT mà hai bên sử dụng truyền tin mật đảm bảo tính không phân biệt tính toán với các bản mã do hai bên sử dụng giao thức giả mạo trình diễn lại quá trình mã hóa khi bị tấn công cưỡng ép.

Với việc sử dụng các nguyên thủy mật mã an toàn và đã được chứnh minh đầy đủ tính chất của một giao thức MHCTCT, phương pháp hoàn toàn có khả năng ứng dụng được trong thực tế.

REFERENCES

[1] Ran Canetti, Cynthia Dwork, Moni Naor, and Rafail Ostrovsky, "Deniable Encryption," Proceedings Advances in Cryptology – CRYPTO 1997. Lectute Notes in Computer Science. Springer – Verlag. Berlin, Heidelberg, New York, pp. 90-104, 1997.

[2] Truecrypt: Free open-source on-the-fly encryption. [Online]. http://truecrypt.org.

[3] Roger Needham, and Adi Shamir Ross Anderson, "The steganographic file system. In Information Hiding," Springer, pp. 73-82, 1998.

[4] AndrewD. McDonald and MarkusG. Kuhn. Stegfs, "A steganographic file system for linux. In Andreas Pfitzmann, editor, Information," Springer Berlin Heidelberg, pp. 463–477, 2000.

[5] B. Meng, "A Secure Internet Voting Protocol Based on Non-interactive Deniable Authentication Protocol and Proof Protocol that Two Ciphertexts are Encryption of the Same Plaintext," Journal of Networks, pp. 370–377, 2009.

[6] I. Yu, E. Kushilevits, and R. Ostrovsky, "Efficient Non-interactive Secure Computation," Advances in Cryptology -- EUROCRYPT 2011. Lectute Notes in Computer Science. Springer – Verlag. Berlin, Heidelberg, New York, pp. 406-425, 2011.

[7] C. Wang and J.A. Wang , "Shared-key and Receiver-deniable Encryption Scheme over Lattice," Journal of Computational Information Systems, pp. 747-753, 2012.

[8] [8] N.A. Moldovyan, A.A. Moldovyan, and A.V. Shcherbacov, "Deniable-encryption protocol using commutative transformation," Workshop on Foundations of Informatics, pp. 285-298, 2016.

[9] N.A. Moldovyan, A.N. Berezin, A.A. Kornienko, and A.A. Moldovyan, "Bi-deniable Public-Encryption Protocols Based on Standard PKI," Proceedings of the 18th FRUCT & ISPIT Conference, Technopark of ITMO University, Saint-Petersburg, Russia. FRUCT Oy, Finland, pp. 212-219, 2016.

[10] A.A. Moldovyan, N.A. Moldovyan, and V.A. Shcherbakov, "Bi-Deniable Public-Key Encryption Protocol Secure Against Active Coercive Adversary," Buletinul Academiei de Stiinte a Republicii Moldova. Mathematica, pp. 23-29, 2014.

[11] Nam Hai Nguyen, N. A. Moldovyan, A. V. Shcherbacov., Hieu Minh Nguyen, Duc Tam Nguyen, "No-Key Protocol for Deniable Encryption" Information Systems Design and Intelligent Applications: Proceedings of Fourth International Conference INDIA 2017.: Springer, Singapore, 2018, pp. 96-104.

[12] Ulf Carlsen, "Cryptographic protocol flaws:know your enemy," in Computer Security Foundations Workshop VII. Proceedings., 1994.

[13] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, p. 644–654, 1976.

[14] M. Hellman and S. Pohlig, "Exponentiation Cryptographic Apparatus and Method," U.S. Patent # 4,424,414, 1984.

[15] N. Moldovyan and A. Moldovyan, Innovative cryptography 2nd Edition, Boston: Charles River Media, 2007, pp. 50-57.

[16] Douglas Robert Stinson, Maura Paterson, Cryptography Theory and Practice, 4th ed., CRC Press, 2019.

[17] J. Katz and Y. Lindell, "Introduction to Modern Cryptography: Principles and Protocols," in Cryptography and Network Security Series, Chapman & Hall/CRC, 2007.

[18] Nguyễn Đức Tâm, Lê Mỹ Tú, "Phương pháp kết hợp ẩn mã với mã hóa khóa công khai có thể chối từ" Tạp chí nghiên cứu KH&CN quân sự, vol. Số đặc san An toàn thông tin, pp. 100-108, 8 2019.

[19] Nguyễn Đức Tâm, Lê Mỹ Tú, "Đề xuất giao thức mã hóa không khóa có thể chối từ giả xác suất sử dụng thuật toán RSA" Tạp chí nghiên cứu KH&CN quân sự, vol. 62, pp. 37-45, 8 2019.

IND-CPA SECURITY OF DENIABLE ENCRYPTION METHOD BASE ON SHAMIR THREE-PASS PROTOCOL

Abstract: This paper analyzes and prove the correct, security, deniable and IND-CPA secùity of a deniable encrypiton method, this method base on Shamir three-pass protocol using Pohlig-Hellman encrypion algorithm. This deniable encryption method has been proposed in the paper [11], but it not been proven the properties of a deniable encryption protocol.

Keyword: Deniable encryption, Shamir three-pass protocol, commutative encrypion, probabilistic encryption, pseudo probabilistic encryption.

SƠ LƯỢC VỀ TÁC GIẢ

Nguyễn Đức Tâm

Sinh năm 1974 tại Bắc Giang. Tốt nghiệp chuyên ngành Kỹ thuật mật mã tại Học viện KTMM. Hiện đang công tác tại Học viện Kỹ thuật mật mã. Hướng nghiên cứu: mã hóa có thể chối từ.

Email:nguyenductamkma@gmail.com