Từ tác động nhóm, nửa nhóm đến mã hóa đồng cấu và những vấn đề bảo mật có liên quan

- **Đặng Tuấn Thương**
- **Nguyễn Anh Tuấn**
- **Ngô Thị Bảo Trân**

Trường Đại học Khoa học Tự nhiên, ĐHQG-HCM

(Bài nhận ngày 05 tháng 12 năm 2014, nhận đăng ngày 23 tháng 09 năm 2015)

TÓM TẮT

Trong những bài báo gần đây, các tác giả đã chứng tỏ rằng một số hệ mã đồng cấu là trường hợp riêng của dãy khớp ngắn chẻ ra trên nhóm. Trong bài báo này, bằng cách chỉ ra sự liên quan giữa những ý tưởng này với khái niệm tác động nhóm và nửa nhóm, chúng tôi xây dựng một giao thức trao đổi khóa dựa trên tác động kép từ nhóm tự đẳng cấu và nửa nhóm nhân $\mathbb{Z}$ lên chính nhóm đó.

Từ khóa: *mã hóa đồng cấu, dãy khớp chẻ ra, tích nửa trực tiếp, tác động nhóm, giao thức trao đổi khóa.*

GIỚI THIỆU

Mã hóa đồng cấu là một loại mã hóa bảo toàn các phép toán trên cấu trúc đại số giữa bản rõ và bản mã. Hiểu theo một nghĩa nào đó, thì tồn tại một đồng cấu từ cấu trúc đại số của bản rõ vào cấu trúc đại số của bản mã. Trong [3] và [8], các tác giả đã chỉ ra mối quan hệ mật thiết giữa dãy khớp ngắn chẻ ra trên nhóm và mô hình mã hóa đồng cấu.

Theo ngôn ngữ của lý thuyết nhóm, một dãy khớp ngắn: $1 \to H \to G \to K \to 1$ là chẻ ra nếu và chỉ nếu $G = H \rtimes K$, tức G là tích nửa trực tiếp của H bởi K, và điều này tương đương với mệnh đề: tồn tại một đồng cấu từ K lên $Aut(H)$, do đó tồn tại một tác động nhóm từ K lên H. Như vậy xét trên một khía cạnh nào đó thì mã hóa đồng cấu chính là một trường hợp riêng của khái niệm tác động nhóm.

Dựa trên những nhận xét này, chúng tôi xây dựng một mô hình trao đổi khóa dựa trên tác động kép từ nửa nhóm nhân $\mathbb{Z}$ và nhóm tuyến tính tổng quát $\mathrm{GL}(n, \mathrm{F_p})$ lên tích trực tiếp của n nhóm cyclic cấp pvới p là một số nguyên tố.

MÔ HÌNH MÃ HÓA ĐỒNG CẤU DỰA TRÊN DÃY KHỚP

Trước khi đề cập đến mối liên quan giữa mã hóa đồng cấu và dãy khớp ngắn chẻ ra trên nhóm, chúng tôi nhắc lại một số kiến thức về lý thuyết nhóm.

Định nghĩa 2.1. Cho G_i là các nhóm, và $f_i$là các đồng cấu nhóm từ $G_i$lên G_{i+1}. Dãy

$$\dots \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \xrightarrow{f_{i+1}} G_{i+2} \xrightarrow{f_{i+2}} \dots$$

được gọi là dãy khớp nếu như với mọi i đều có: $Ker(f_{i+1}) = Im(f_i)$. Một dãy khớp được gọi là dãy khớp ngắn nếu như nó có dạng sau

$$1 \to H \to G \to K \to 1$$

Thí dụ 2.2. Nếu H là nhóm con chuẩn tắc của G, khi đó sẽ có dãy khớp ngắn sau đây.

$$1 \to H \xrightarrow{i} G \xrightarrow{\phi} G/H \to 1$$

trong đó i là ánh xạ nhúng chính tắc, và ϕ là toàn cấu chính tắc từ G lên G/H.

Định nghĩa 2.3.*Một dãy khớp ngắn*

$$1 \to H \xrightarrow{e} G \xrightarrow{d} K \to 1$$

được gọi là chẻ ra nếu tồn tại một đồng cấu ϵ từ $K \to G$ sao cho: $d \circ \epsilon = id_K$ trong đó $\circ$ là phép hợp thành các ánh xạ và id_K là ánh xạ đồng nhất trên K.

Dựa trên dãy khớp chẻ ra, trong [8], tác giả đã áp dụng khái niệm này để giải thích lại một số mô hình mã hóa đồng cấu, có thể mô tả ngắn gọn như sau

$$1 \to H \xrightarrow{e} G \xrightarrow{d} K \to 1$$

Với các ký hiệu được dùng như trong định nghĩa. Trong mô hình này, Alice giữ bí mật ánh xạ d, công khai H, G, K, e, ϵ.

Để mã hóa, Bob làm như sau: chọn văn bản $m \in K$, và giá trị $h \in H$ ngẫu nhiên, sau đó tính: $C = \epsilon(m).e(h)$.

Để giải mã, Alice sử dụng d để tính: $d(C) = d\big(\epsilon(m).e(h)\big) = d\big(\epsilon(m)\big)d\big(e(h)\big)$. Theo tính chất của dãy khớp chẻ ra, có: $d \circ \epsilon = id_K \Rightarrow d\big(\epsilon(m)\big) = m$. Và vì: $Im(e) = Ker(d)$, nên sẽ có: $d\big(e(h)\big) = 1$. Do vậy, $d(C) = m$ và điều này bao hàm tính đúng đắn của mô hình.

Tuy nhiên, mô hình này còn có tính chất đẹp đẽ hơn, chính vì ϵ là đồng cấu. nên nếu chọn 2 văn bản $m_1, m_2 \in K$, và mã hóa:

$$C_1 = \epsilon(m_1)e(h_1) \text{và} C_2 = \epsilon(m_2)e(h_2)$$

Theo tính chất của dãy khớp ngắn, sẽ có:

$$d(C_1C_2) = d\big(\epsilon(m_1)e(h_1)\epsilon(m_2)e(h_2)\big) = m_1m_2$$

Và điều này cũng chứng tỏ sự bảo toàn các cấu trúc đại số giữa bản rõ và bản mã, đúng như tên gọi của mô hình mã hóa này, là *mã đồng cấu*. Cũng trong [8], tác giả đã chỉ ra mô hình dãy khớp trong một số hệ mã đồng cấu thông dụng, như ElGamal, Goldwasser-Micali và Paillier. Ưu điểm của loại mã này chính là việc cho phép so khớp trên các dữ liệu mã hóa, mà một thí dụ của nó được đề cập ở [2] trong mô hình so khớp hồ sơ DNA.

Theo kết quả từ lý thuyết nhóm, có định lý sau đây.

Định lý 2.4 [7-Lemma 7.20, Theorem 7.22, Theorem 7.23]. *Dãy khớp ngắn: $1 \to H \to G \to K \to 1$ là chẻ ra khi và chỉ khi: G là tích nửa trực tiếp của H bởi K(Ký hiệu: $G = H \rtimes K$). Điều này cũng tương đương với sự tồn tại của một đồng cấu nhóm từ K lên $Aut(H)$ và phép toán trên G sẽ tương thích với đồng cấu này.*

Với K, H là các nhóm được đề cập trong định lý trên,khi đó sẽ tồn tại một đồng cấu ϕ được định nghĩa:

$$\phi: K \to Aut(H)$$
$$k \mapsto \phi_k$$

thế thì theo tính chất của đồng cấu, sẽ có:

$$\phi(1_K) = \phi_{1_K} = id_H \quad (2.1)$$
$$\phi(k_1k_2) = \phi_{k_1k_2} = \phi(k_1)\phi(k_2) = \phi_{k_1}\phi_{k_2} \quad (2.2)$$

Sử dụng những nhận xét này, trong phần 3, sẽ thấy sự kết nối rất tự nhiên từ mô hình mã hóa đồng cấu đến khái niệm tác động nhóm.

CÁC MÔ HÌNH TRAO ĐỔI KHÓA DỰA TRÊN TÁC ĐỘNG

Trước hết ta sẽ nhắc lại khái niệm về tác động nửa nhóm và các vấn đề mã hóa có liên quan.

Định nghĩa 3.1. *Cho G là một nửa nhóm và X là một tập hợp. Vậy: G tác động lên X nếu tồn tại một ánh xạ*

$$G \times X \to X$$
$$(g, x) \mapsto gx$$

thỏa mãn với mọi $g, h \in G, x \in X$:$(gh)x = g(hx)$. Trong trường hợp G là nhóm, hoặc nửa

nhóm có đơn vị thì $1_G x = x$ *trong đó* 1_G *là đơn vị của* G.

Giả sử G là một nhóm, ký hiệu $Inn(G) = \{\phi_g | g \in G, \phi_g(h) = ghg^{-1}, \forall h \in G\}$ là tập các tự đẳng cấu nội của G, thế thì G sẽ tác động lên chính nó thông qua ánh xạ

$$G \times G \to G$$
$$(g, x) \mapsto \phi_g(x) = gxg^{-1}$$

Dựa trên tác động này, trong [5], các tác giả đã mô tả một mô hình trao đổi khóa trên nhóm braid dựa trên bài toán liên hợp như sau:

Mô hình 3.2 (Mô hình trao đổi khóa dựa trên bài toán liên hợp). Alice và Bob chọn nhóm G không giao hoán, H là một tập con của G thỏa mãn: $h_1h_2 = h_2h_1 (\forall h_1, h_2 \in H)$, cùng với một phần tử $g \in G$.

Sau đó, Alice chọn bí mật $a \in H$, và tính $\phi_a(g) = aga^{-1}$ và gửi cho Bob.

Bob cũng chọn $b \in H$ bí mật, và tính $\phi_b(g) = bgb^{-1}$ và gửi cho Alice.

Và cả hai cùng thống nhất khóa $K = \phi_{ab}(g) = \phi_a(\phi_b(g)) = \phi_b(\phi_a(g))$.

Tính đúng đắn của mô hình được suy ra từ tính chất của tác động: $\phi_{ab} = \phi_a\phi_b$ và tính chất giao hoán của các phần tử trong H, vì lúc đó $ab = ba$. Độ an toàn của mô hình hoàn toàn phụ thuộc vào bài toán: tách ϕ_a từ cặp giá trị $(\phi_a(g), g) (3.1)$.

Trong trường hợp G là một nhóm, và $\mathbb{Z}$ là một nửa nhóm với phép nhân thông thường, xét ánh xạ sau đây:

$$\mathbb{Z} \times G \to G$$
$$(k, g) \mapsto g^k$$

Khi đó, với mọi $k, h \in \mathbb{Z}, g \in G$, có:$(kh, g) = g^{kh} = (g^k)^h$, và $(1, g) = g^1 = g$. Như vậy, $\mathbb{Z}$ tác động lên G thông qua ánh xạ trên. Và cũng dễ dàng xây dựng được mô hình trao đổi khóa của Diffie-Hellman, với độ khó dựa trên bài toán logarit rời rạc trên nhóm G: tách k từ cặp giá trị (g, g^k) (3.2).

Từ (3.1), và (3.2), có thể xây dựng một mô hình trao đổi khóa dựa trên tác động (nửa) nhóm như sau:

Mô hình 3.3 (Mô hình trao đổi khóa dựa trên tác động nửa nhóm). Alice và Bob thống nhất một nửa nhóm G và một nhóm K sao cho G tác động lên K, đồng thời với đó là một tập con H của G thỏa: $h_1h_2 = h_2h_1 (\forall h_1, h_2 \in H)$, cùng với một phần tử $k \in K$.

Alice chọn $a \in H$ bí mật, và tính ak và gửi cho Bob

Bob cũng chọn bí mật $b \in H$ và tính bk và gửi cho Alice.

Alice sau đó tính: $a(bk) = (ab)k$, và Bob cũng tính: $b(ak) = (ba)k$, vì $ab = ba$ nên: $(ab)k = (ba)k$ và cả hai sẽ thống nhất khóa $K = abk$. Độ an toàn của mô hình cũng dựa trên bài toán: tách a từ (k, ak), tức sau khi cho $a \in G$ tác động lên một phần tử $k \in K$ đã biết để thu được ak, hỏi có cách nào phục hồi lại a hay không?

Sử dụng Mô hình 3.3, các tác giả trong [6] đã mô tả một giao thức trao đổi khóa dựa trên lý thuyết bất biến, khi cho nửa nhóm nhân ma trận $M_{n\times n}(K)$ tác động lên vành đa thức $K[x_1, x_2 \ldots x_n]$ trong đó K là một trường. Ngoài ra, với ý tưởng tương tự, các tác giả trong [4] cũng nêu ra một mô hình dựa trên khái niệm *toàn hình* (holomorph) của một nhóm (tức là tích nửa trực tiếp của một nhóm với chính nhóm tự đẳng cấu của nhóm đó). Trong phần tiếp theo của bài báo, chúng tôi sẽ xây dựng một giao thức trao đổi khóa dựa trên tác động kép từ nhóm tự đẳng cấu và nửa nhóm nhân $\mathbb{Z}$ lên một nhóm.

MỘT GIAO THỨC TRAO ĐỔI KHÓA DỰA TRÊN TÁC ĐỘNG KÉP

Trở lại với các kết quả (2.1) và (2.2) ở cuối phần hai, định nghĩa một ánh xạ:

$$K \times H \to H$$

$$(k, h) \mapsto kh = \phi_k(h)$$

Khi đó, theo (2.1), sẽ có:

$$(k_1k_2)h = \phi_{k_1k_2}(h) = \phi_{k_1}\left(\phi_{k_2}(h)\right) = k_1(k_2h)(\forall k_1k_2 \in K, h \in H)$$

Và theo (2.2), sẽ có:

$$1_K h = \phi_{1_K}(h) = id_H(h) = h(\forall h \in H)$$

Do đó, K tác động lên H thông qua ánh xạ được định nghĩa ở trên. Và như một hệ quả trực tiếp cũng có: $Aut(H)$ tác động lên H qua ánh xạ:

$$Aut(H) \times H \to H$$

$$(\phi, h) \mapsto \phi(h)$$

Và trên tinh thần của Mô hình 3.3, sẽ đưa ra mô hình trao đổi khóa dựa trên tác động kép của nhóm tự đẳng cấu $Aut(G)$ và nửa nhóm nhân $\mathbb{Z}$ lên nhóm G. Về bản chất, đây chính là tác động tử nửa nhóm $Aut(G) \times \mathbb{Z}$ lên tập G thông qua ánh xạ.

$$(Aut(G) \times \mathbb{Z}) \times G \to G$$

$$\left((\phi, k), x\right) \to \phi(x)^k$$

Mô hình 4.1. Alice và Bob công khai nhóm $G, Aut(G)$, tập con H của $Aut(G)$ sao cho: $\phi_1\phi_2 = \phi_2\phi_1(\forall\phi_1, \phi_2 \in H)$ cùng với một phần tử $g \in G$.

Alice chọn bí mật $\phi \in H, a \in \mathbb{Z}$ và tính: $\phi(g^a)$ sau đó gửi qua cho Bob.

Bob chọn bí mật $\psi \in H, b \in \mathbb{Z}$ và tính: $\psi(g^b)$sau đó gửi qua cho Alice.

Alice tiếp theo tính: $K = \phi\left(\psi(g^b)\right)^a = \phi(\psi(g)^b)^a = \phi\left(\psi(g)\right)^{ba} = \psi\left(\phi(g)\right)^{ab}$

Bob cũng tính: $K = \psi\left(\phi(g^a)\right)^b = \psi(\phi(g)^a)^b = \psi\left(\phi(g)\right)^{ab}$

Cả hai cùng thống nhất khóa K.

Tính đúng đắn của mô hình được suy ra từ tính giao hoán giữa các phần tử trong H và tính chất của tự đẳng cấu.

Tính bảo mật. Về độ an toàn của mô hình 4.1, kẻ tấn công phải bị buộc phải tách hai lớp tác động, một từ nhóm tự đẳng cấu, và một từ nửa nhóm nhân $\mathbb{Z}$, do đó mô hình trên có độ bảo mật không thấp hơn mô hình trao đổi khóa của Diffie-Hellman (3.2). Đồng thời, đây cũng chính là một mở rộng của mô hình trao đổi khóa liên hợp trên nhóm braid (3.1), vì như đã biết, $Inn(G) \leq Aut(G)$.

Thế nhưng, sẽ nảy sinh những câu hỏi như: liệu xây dựng các nhóm tự đẳng cấu có dễ không? Và trong điều kiện nào thì mô hình trao đổi khóa có thể hiện thực được? Trong phần 5 dưới đây, chúng tôi sẽ đề xuất một cách hiện thực mô hình này.

MỘT CÁCH HIỆN THỰC MÔ HÌNH 4.1

Trước hết, chúng tôi chọn nhóm cyclic cấp p là nhóm điểm trên đường cong elliptic [1], và ký hiệu nhóm này là C_p. Nhóm G trong mô hình 4.1 sẽ là tích trực tiếp của ba nhóm C_p, tức:

$$G = C_p \times C_p \times C_p$$

Gọi $P_i(i = 1,2,3)$ lần lượt là các phần tử sinh của ba nhóm C_p ở trên. Khi đó, với mọi phần tử $Q \in G$, tồn tại $b_i \in \mathbb{Z}_p(i = 1,2,3)$, sao cho

$$Q = b_1P_1 + b_2P_2 + b_3P_3$$

Dễ dàng nhận thấy G là một không gian véctơ 3 chiều trên $\mathbb{F}_p$, và như vậy mỗi một tự đẳng cấu ϕ của G chính là một phép chuyển cơ sở. Do đó, theo những kết quả từ đại số tuyến tính, để chuyển cơ sở, chỉ cần nhân một ma trận A khả nghịch vào cơ sở cho trước. Sử dụng nhận xét này, sẽ chỉ ra một thuật toán xây dựng tự đẳng cấu của G.

Thuật toán 5.1 (Xây dựng một tự đẳng cấu của G)

Input. Nhóm $G = C_p \times C_p \times C_p$ và cơ sở $< P_1, P_2, P_3 >$của G.

Output. Tự đẳng cấu ϕcủa G.

Bước 1. Chọn một ma trận khả nghịch $\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \in GL(3, \mathbb{F}_p)$.

Bước 2. Đặt $P_{1\phi} = a_{11}P_1 + a_{12}P_2 + a_{13}P_3$, $P_{2\phi} = a_{21}P_1 + a_{22}P_2 + a_{23}P_3$, $P_{3\phi} = a_{31}P_1 + a_{32}P_2 + a_{33}P_3$. Định nghĩa ánh xạ ϕ thỏa

$$\phi: G \to G$$

$$b_1P_1 + b_2P_2 + b_3P_3 \mapsto b_1P_{1\phi} + b_2P_{2\phi} + b_3P_{3\phi}$$

Bước 3. Trả về ϕ.

Theo những kết quả từ lý thuyết nhóm [7-Example 7.4], sẽ có: $Aut(G) \cong GL(3, \mathbb{F}_p)$. Do đó, sử dụng Thuật toán 5.1 có thể sinh ra toàn bộ các tự đẳng cấu của nhóm G. Và như vậy, việc lựa chọn hai tự đẳng cấu giao hoán với nhau theo phép hợp thành các ánh xạ hoàn toàn có thể thực hiện được dựa trên việc lựa chọn ma trận.

KẾT LUẬN

Trong bài báo này, chúng tôi đã nêu ra sự liên quan giữa mã hóa đồng cấu và khái niệm tác động nhóm. Từ đó, bằng cách sử dụng một tác động kép lên nhóm abel sơ cấp có cấp p^3 (là tích trực tiếp của ba nhóm cyclic có cấp p trên đường cong elliptic) từ nhóm tự đẳng cấu và nửa nhóm nhân $\mathbb{Z}$, chúng tôi đã trình bày một mô hình trao đổi khóa có độ bảo mật không thấp hơn mô hình trao đổi khóa của Diffie-Hellman, và đây đồng thời cũng là mở rộng của mô hình trao đổi khóa dựa trên nhóm braid. Tính khả thi của mô hình, mà cụ thể là việc xây dựng các phần tử của nhóm tự đẳng cấu cũng đã được chỉ ra trong phần cuối của bài báo.

From semigroup action to homomorphic encryption and some related problems in cryptography

- **Dang Tuan Thuong**
- **Nguyen Anh Tuan**
- **Ngo Thi Bao Tran**

University of Science, VNU-HCM

ABSTRACT

In some recent papers, the authors have showed some homomorphic cryptosystems which are particular cases of split exact sequences of groups. By connecting the relation between these ideas to the concept of group action, in this paper, we build a public key exchange protocol based on actions to a group, from its automorphism group and semigroup $\mathbb{Z}$ under usual multiplication.

Keywords: *homomorphic encryption, split exact sequence, semidirect product, group action, public key exchange protocol.*

TÀI LIỆU THAM KHẢO

[1]. D. Boneh, X. Boyen, H. Shacham, Short group signatures, *Advances in Cryptography-CRYPTO* 2004, *Lecture Notes in Computer Science*, 3152, Springer-Verlag, 41-55 (2004).

[2]. F. Bruekers, S. Katzenbeisser, K. Kursawe, P. Tuyls, Privacy-preserving matching of DNA profiles, available from *eprint.iacr.org* (2008).

[3]. D. Grigoriev, Public-key cryptography and invariant theory, *Journal of Mathematical Sciences*, Volume 126, Issue 3, Springer Science and Business Media, 1152-1157 (2005).

[4]. M. Habbeb, D. Kahrobaei, C. Koupparis, V. Shpilrain, Public key exchange using semidirect product of (semi)groups, *Applied Cryptography and Network Security ACNS* 13, Canada, 475-486 (2013).

[5]. K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang, C. Park, New public key cryptosystem using braids group, In *Advances in cryptography-CRYPTO* 2000 (Santa Barbara, CA), volume 1880 of *Lecture Notes In Computer Science*, Springer, Berlin, 166-183 (2000).

[6]. G. Maze, C. Monico, J. Rosenthal, Public key cryptography based on semigroup actions, *Journal of Advances in Mathematics Communications* (AMC), 24, 489-502 (2007).

[7]. J.J. Rotman, An introduction to the theory of groups, 4th edition, Graduate Texts in Mathematics, *Springer* (1994).

[8]. A. Yainamura, Homomorphic encryptions of sums of groups, 17th *International Symposium*, AAECC -17 Proceedings, *Lecture Notes in Computer Science*, Springer-Verlag, 357-366 (2007).