HỆ MÃ HÓA DỰA TRÊN THUỘC TÍNH MỚI HỖ TRỢ TÍNH CHẤT PHI TẬP TRUNG HÓA

Lê Phi Thường[1], Lê Đình Hải[2], Trịnh Viết Cường[3], Lê Xuân Lâm[4]

TÓM TẮT

Mã hóa dựa trên thuộc tính (attribute-based encryption) là hệ mã hóa quan trọng hiện nay, được sử dụng rộng rãi trong lưu trữ dữ liệu trên điện toán đám mây, cũng như trong nhiều ứng dụng khác như truyền hình trả tiền, chia sẻ files,... Mã hóa dựa trên thuộc tính cho phép phân quyền truy cập dữ liệu của người dùng dựa trên thuộc tính. Trong các hệ mã hóa dựa trên thuộc tính hiện nay, hệ mã do hai tác giả Riepel và Wee đề xuất năm 2022 được xem là một trong những hệ mã quan trọng nhất. Hệ mã này có tính hiệu quả rất cao cũng như tính an toàn tốt, tuy nhiên điểm thiếu sót của hệ mã này là chưa hỗ trợ tính phi tập trung hóa. Trong bài báo này chúng tôi đề xuất giải pháp bổ sung tính phi tập trung hóa cho hệ mã của Riepel-Wee và đánh giá so sánh ưu nhược điểm của hệ mã đề xuất với một số hệ mã hóa dựa trên thuộc tính có hỗ trợ tính chất phi tập trung hóa khác.

Từ khóa: *Mã hóa dựa trên thuộc tính, phi tập trung hóa, điện toán đám mây.*

1. GIỚI THIỆU CHUNG VỀ MÃ HÓA DỰA TRÊN THUỘC TÍNH

Điện toán đám mây ngày nay đem lại rất nhiều lợi thế cho doanh nghiệp và người dùng, chúng giúp tiết giảm chi phí, tăng khả năng đáp ứng và do đó tăng lợi nhuận cho doanh nghiệp. Điện toán đám mây được dùng mọi nơi để lưu trữ và xử lý dữ liệu, từ việc lưu trữ cập nhật danh bạ điện thoại cho mỗi người dùng điện thoại di động, cho đến lớn hơn là lưu trữ và xử lý những dữ liệu khổng lồ của các doanh nghiệp. Các doanh nghiệp và người dùng không cần phải lưu trữ dữ liệu trên thiết bị của mình vốn hạn chế về khả năng lưu trữ và tính toán. Song song với những ưu thế, vấn đề an toàn của điện toán đám mây luôn được đặt ra. Hai câu hỏi lớn nhất về độ an toàn đối với điện toán đám mây là làm thế nào để chắc chắn rằng dữ liệu của chúng tôi không bị đánh cắp và bị sử dụng nếu như các máy chủ lưu dữ liệu (Cloud Servers) bị tấn công? Làm thế nào để đảm bảo quyền truy cập hiệu quả dữ liệu của các người dùng trong hệ thống? Để trả lời câu hỏi thứ nhất kỹ thuật mã hóa thông thường có thể là một giải pháp. Dữ liệu trước khi được đưa lên Cloud Servers sẽ được mã hóa. Khi các Cloud Servers bị tấn công và dữ liệu bị lấy cắp, kẻ tấn công không có khóa giải mã vẫn không thể nào truy cập được vào dữ liệu gốc (raw data) và do đó dữ liệu vẫn an toàn. Tuy nhiên, phương pháp dùng kỹ thuật mã hóa thông thường không thể giải quyết được vấn

[1] *NCS khoá 1 ngành Khoa học máy tính, Khoa CNTT&TT, Trường Đại học Hồng Đức*

[2] *Học viên Cao học khoá 13, ngành Khoa học máy tính, Khoa CNTT&TT, Trường Đại học Hồng Đức*

[3] *Khoa Công nghệ Thông tin và Truyền thông, Trường Đại học Hồng Đức; Email: trinhvietcuong@hdu.edu.vn*

[4] *Sở Thông tin và Truyền thông Thanh Hoá*

đề thứ hai, lý do là dữ liệu dùng kỹ thuật mã hóa thông thường (ví dụ hệ mã hóa AES hay RSA) chỉ có một khóa giải mã dữ liệu duy nhất, do đó không thể phân quyền truy cập dữ liệu cho các người dùng trong hệ thống một cách hiệu quả.

Kỹ thuật mã hóa dựa trên thuộc tính do Sahai and Waters [1] giới thiệu đã giải quyết tốt cả hai câu hỏi trên. Một hệ mã hóa dựa trên thuộc tính (Attribute-based encryption) có quá trình mã hóa và giải mã được dựa trên thuộc tính, và cứ miễn là tập các thuộc tính (attributes) thỏa mãn một chính sách (policy) là có thể giải mã thành công. Có hai loại mã hóa dựa trên thuộc tính, thứ nhất là mã hóa dựa trên chính sách ở bản mã (ciphertext policy attribute-based encryption: CP-ABE), trong hệ thống này mỗi người dùng sẽ được cấp một tập các thuộc tính (attributes), khi mã hóa người lập mã sẽ mã hóa dựa trên một chính sách (policy) nào đó, và chỉ có người dùng sở hữu tập các thuộc tính thỏa mãn chính sách đó mới có thể giải mã được. Ví dụ: Nếu xem mỗi bộ môn KHMT, HTTT, KTMT, TƯD là các thuộc tính, giới tính Nam, Nữ là các thuộc tính; các huyện trong tỉnh Thanh Hóa là các thuộc tính. Dựa vào từng cán bộ cụ thể ta có thể cấp cho họ sở hữu các thuộc tính tương ứng, khi mã hóa ta có thể mã hóa một thông báo dựa trên một chính sách mà chỉ có thể có một số người nhất định mới có thể giải mã được, chính sách thường được dựa trên một biểu thức boolean (biểu thức logic). Ví dụ mã hóa cho những cán bộ thuộc bộ môn KHMT, là Nam và thuộc 2 huyện Triệu Sơn, Thiệu Hóa mới có thể giải mã được, khi đó chính sách (được biểu diễn bởi biểu thức boolean) sẽ là: KHMT *và* Nam *và* (Triệu Sơn *hoặc* Thiệu Hóa). Loại mã hóa dựa trên thuộc tính thứ hai đó là mã hóa thuộc tính dựa trên chính sách ở khóa (key policy attribute-based encryption: KP-ABE), ngược lại với loại ở trên lúc này mỗi người dùng sẽ được cấp một chính sách (policy), và khi lập mã người lập mã sẽ chọn một tập các thuộc tính để mã hóa, và miễn là tập các thuộc tính này thỏa mãn chính sách là người dùng có thể giải mã được.

Với một hệ mã hóa dựa trên thuộc tính, mỗi người dùng sẽ sở hữu một tập thuộc tính (hoặc một chính sách giải mã policy) và được quản trị hệ thống (authority) tạo khóa tương ứng với tập thuộc tính (hoặc policy). Authority sở hữu một khóa bí mật của hệ thống (master secret key) để tạo khóa bí mật cho từng người dùng, hệ thống như vậy gọi là hệ thống *tập trung hóa*. Hệ thống tập trung hóa có hai điểm yếu. Điểm yếu đầu tiên cũng là quan trọng nhất là do authority là người tạo khóa, do đó authority biết tất cả khóa bí mật của người dùng trong hệ thống. Điều này dẫn đến nguy cơ mất an toàn đối với người dùng khi authority gian dối hoặc bị tấn công lấy mất master secret key. Điểm yếu thứ hai là do chỉ có một authority tạo khóa cho người dùng, nên nếu authority bị quá tải hay bị tấn công hệ thống sẽ không thể tạo khóa cho người dùng. Tuy nhiên do số lượng người dùng mới tham gia vào hệ thống là ít và không thường xuyên đối với đa số ứng dụng, do vậy điểm yếu thứ hai thường không được coi trọng bằng điểm yếu đầu tiên. Một hệ thống có tính chất *phi tập trung hóa* là hệ thống giải quyết tốt được ít nhất điểm yếu đầu tiên.

Mã hóa dựa trên thuộc tính là hướng nghiên cứu được các nhà nghiên cứu quan tâm, có rất nhiều các hệ mã hóa dựa trên thuộc tính với các tính chất khác nhau [1-9] đã được công bố. Trong đó hệ mã của hai tác giả Riepel-Wee đề xuất năm 2022 [6] (được công bố

tại một trong những hội nghị lớn nhất của ngành an toàn bảo mật thông tin ACM CCS) được xem là quan trọng nhất. Trong bài báo này đóng góp của chúng tôi là cải tiến hệ mã này bằng cách bổ sung thêm tính chất phi tập trung hóa cho hệ mã này. Đồng thời chúng tôi cũng đưa ra sự so sánh hệ mã đề xuất với các hệ mã dựa trên thuộc tính có hỗ trợ tính chất phi tập trung hóa khác.

2. HỆ MÃ DỰA TRÊN THUỘC TÍNH CỦA RIEPEL-WEE

2.1. Phép ghép cặp đôi

Phép ghép cặp đôi Pairings được mô tả như sau:

Gọi $\mathbb{G}_1$, $\mathbb{G}_2$ là hai nhóm cyclic có bậc nguyên tố p.

g_1 là phần tử sinh của tập $\mathbb{G}_1$, g_2 là phần tử sinh của tập $\mathbb{G}_2$.

Ψ là một ánh xạ từ $\mathbb{G}_2$ vào $\mathbb{G}_1$ trong đó $\Psi(g_2) = g_1$.

e là một ánh xạ song tuyến tính ký hiệu $e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$.

Trong đó phép *e* thỏa mãn hai tính chất sau:

Tính song tuyến tính: Với mọi $u \in \mathbb{G}_1$, $v \in \mathbb{G}_2$ và a, b $\in \mathbb{Z}$ ta có: $e(u^a, v^b) = e(u, v)^{a.b}$

Tính không suy biến: $e(g_1, g_2) \neq 1$.

Trong đó $\mathbb{G}_1$, $\mathbb{G}_2$ có thể trùng nhau, khi cài đặt với đường cong Eliptic thì $\mathbb{G}_1$, $\mathbb{G}_2$ sẽ là tập các điểm trên đường cong với tọa độ các điểm thuộc tập $\mathbb{Z}_p$, p là số nguyên tố, tập $\mathbb{G}_T$ sẽ là tập $\mathbb{Z}_q$ với $q = p^\tau$, trong đó tùy việc thiết lập thông số an toàn mà τ có thể là 2, 4, hoặc 6.

2.2. Ma trận chia sẻ tuyến tính

Ma trận chia sẻ tuyến tính (linear secret sharing matrix - LSS) được mô tả như sau: Giả sử p là số nguyên tố và $\mathcal{U}$ là tập các thuộc tính. Nếu $\mathbb{A}$ là một chính sách mã hóa dựa trên $\mathcal{U}$, thì ta có thể tìm một ma trận LSS, $M \in \mathbb{Z}_p^{n1 \times n2}$ và một hàm π ánh xạ các hàng trong ma trận *M* với các thuộc tính trong $\mathcal{U}$, các thuộc tính này xuất hiện trong $\mathbb{A}$, tức là hàm π có dạng $\pi \in \mathcal{F}([n1] \rightarrow \mathcal{U})$, với $n1$ là số hàng trong ma trận.

Cặp *(M, π)* được gọi là một chính sách mã hóa LSS. Và khi vector $\vec{y} = (s, y_2, \dots, y_{n2})^\perp \xleftarrow{\$} \mathbb{Z}_p^{n2}$ với số bí mật *s* cần chia sẻ, thì vector chia sẻ bí mật sẽ là $\vec{\lambda} = M.\vec{y}$. Đặt *S* là một tập các thuộc tính mà thỏa mãn chính sách mã hóa $\mathbb{A}$ (hay chính là *(M, π))*, *I* là tập các dòng của ma trận *M* mà ánh xạ qua hàm π xuất hiện trong *S*, tức là $I = \{i | i \in [n1] \wedge \pi(i) \in S\}$.

Người ta đã chứng minh được rằng: Tồn tại các hằng số $\{\gamma_i\}_{i \in I}$ trong $\mathbb{Z}_p$ sao cho với mọi giá trị chia sẻ hợp lệ $\left\{\lambda_i = (M.\vec{y})_i\right\}_{i \in I}$ của thành phần bí mật *s* thì $\sum_{i \in I} \gamma_i \lambda_i = s$ hay tương đương với:

$$\sum_{i \in I} \gamma_i \, \mathrm{M}_i = (1, 0, \dots, 0)$$

các hằng số $\{\gamma_i\}_{i \in I}$ có thể được tính toán được một cách hiệu quả.

2.3. Hệ mã dựa trên thuộc tính của Riepel và Wee

Hệ mã ở dạng dựa trên chính sách ở bản mã bao gồm 4 giải thuật:

Khởi tạo: khởi tạo các tham số chung cho toàn bộ hệ thống như khóa công khai của toàn bộ hệ thống, khóa bí mật của hệ thống (master secret key).

Tạo khóa: giải thuật tạo ra khóa bí mật cho người dùng mới tham gia vào hệ thống dựa trên đầu vào là tập thuộc tính của người dùng và khóa bí mật của hệ thống.

Mã hóa: đầu vào là chính sách mã hóa và khóa công khai của hệ thống, đầu ra là khóa phiên K của hệ thống và bản mã tương ứng với khóa phiên K. Lưu ý rằng khóa phiên K sẽ được dùng như khóa bí mật (với hệ mã AES) để mã hóa dữ liệu thực sự cần mã hóa.

Giải mã: đầu vào là bản mã và khóa bí mật, nếu tập thuộc tính của khóa bí mật thỏa mãn chính sách mã hóa, giải thuật cho đầu ra là khóa phiên K. Ngược lại thông báo không giải mã được. Lưu ý rằng khóa phiên K được dùng như khóa bí mật để giải mã (với hệ mã AES) ra dữ liệu bản rõ.

Các giải thuật cụ thể như sau:

Khởi tạo (1^{λ}).

Dựa trên tham số đầu vào λ, tạo ra hệ thống Pairings G:=$(p,\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T,e,g_1,g_2)$. Trong đó g_1, g_2 là các phần tử sinh của nhóm $\mathbb{G}_1$, $\mathbb{G}_2$; chọn ngẫu nhiên $\alpha \xleftarrow{\$} \mathbb{Z}_p$ và hàm băm H : $[|\mathcal{U}|+ 1] \rightarrow \mathbb{G}_1$, trong đó $\mathcal{U}$ là tập các thuộc tính của hệ thống. Tính khóa công khai mpk của hệ thống:

mpk:= (G,H, $e(g_1, g_2)^{\alpha}$)

Khóa bí mật của hệ thống msk := α.

Tạo khóa (msk, *S là tập con của tập* $\mathcal{U}$).

Chọn ngẫu nhiên $r \xleftarrow{\$} \mathbb{Z}_p$.Tính khóa bí mật với mỗi $u \in S$:

$\mathrm{sk}_1 := g_1^{\alpha}.\mathrm{H}(|\mathcal{U}| +1)^r$, $\mathrm{sk}_{2,u} = \mathrm{H}(u)^r$, $\mathrm{sk}_3 := g_2^r$

Đầu ra là khóa bí mật sk := $(\mathrm{sk}_1,\{\mathrm{sk}_{2,u}\}_{u \in S}, \mathrm{sk}_3)$

Mã hóa (mpk,(M,π) - là chính sách mã hóa dạng ma trận chia sẽ tuyến tính).

Chọn ngẫu nhiên $s_1 \xleftarrow{\$} \mathbb{Z}_p$, $\mathbf{v} \xleftarrow{\$} \mathbb{Z}_p^{n_2-1}$, $\mathbf{s'} \xleftarrow{\$} \mathbb{Z}_p^{\tau}$.

Tính $\mathrm{ct}_1 := g_2^{s_1}$ $\mathrm{ct}_{2,\mathrm{j}} := g_2^{s'[j]}$ for j $\in [\tau]$, và

$\mathrm{ct}_3 := \mathrm{H}([|\mathcal{U}| + 1)^{\mathrm{M}_i(s_1||v)^{\mathrm{T}}}.\mathrm{H}(\pi(i))^{s'[p(i)]}$

Với mỗi dòng $i \in [n_1]$. Phép toán || là phép ghép hai véc tơ.

Cuối cùng cho đầu ra là bản mã ct và khóa phiên K như sau:

$\mathrm{ct} := (\mathrm{ct}_1, (\mathrm{ct}_{2,j})_{j\in[\tau]}, (\mathrm{ct}_{3,i})_{i\in[n_1]})$ và $K := e(g_1, g_2)^{\alpha s_1}$.

Lưu ý rằng bản mã ct bao gồm cả chính sách mã hóa (M,π).

Giải mã (mpk,(M,π), *S*, ct, sk*)*.

Nếu tập thuộc tính của người dùng *S không* thỏa mãn chính sách mã hóa (M,π) cho đầu ra là thông báo không giải mã được. Ngược lại, theo tính chất của ma trận chia sẻ tuyến tính M tồn tại $\{\gamma_i\}_{i \in I}$ sao cho:

$$\sum_{i \in I} \gamma_i \mathrm{M}_i = (1,0, \dots ,0)$$

Tính khóa phiên: $K = e(sk_1, ct_1).\frac{\prod_{j\in[\tau]} e(\prod_{i\in I, p(i)=j}(sk_{2,\pi(i)})^{\gamma_i}, ct_{2,j})}{e(\prod_{i\in I}(ct_{3,i})^{\gamma_i}, sk_3)}$

3. HỆ MÃ DỰA TRÊN THUỘC TÍNH ĐỀ XUẤT

Trong mục này, trước tiên chúng tôi trình bày ý tưởng xây dựng hệ mã, sau đó trình bày chi tiết hệ mã cũng như những phân tích đánh giá về tính an toàn của hệ mã đề xuất.

3.1. Ý tưởng xây dựng

Trong hệ mã của Riepel-Wee khóa bí mật của hệ thống là α, khóa bí mật của từng người dùng sẽ được tính dựa trên α và tập thuộc tính của từng người dùng. Ý tưởng đầu tiên để giảm sự phụ thuộc vào duy nhất α (ngăn kẻ tấn công hay authority gian dối biết α) là ta tách α ra thành nhiều giá trị con $\alpha = \alpha_1 + \alpha_2 + \ldots + \alpha_n$, sau đó tách authority ra thành n authority con, mỗi authority con sở hữu một giá trị α_i. Khi cấp khóa, mỗi authority con sẽ cấp một khóa con tương ứng với từng giá trị α_i, người dùng sau đó sẽ gộp các khóa con lại thành khóa chính tương ứng với α và giải mã như thông thường. Với phương pháp này hệ thống có thể giải quyết tốt được vấn đề gây mất an toàn khóa bí mật của người dùng (vấn đề thứ nhất). Cụ thể, do lúc này hệ thống có n authority con, do đó trừ phi cả n authority con gian dối hay kẻ tấn công phải tấn công thành công cả n authority con mới có thể tính được khóa bí mật của người dùng. Như vậy hệ thống đã giảm thiểu được khả năng lộ khóa bí mật của người dùng, đặc biệt khi n đủ lớn. Tuy nhiên nhược điểm của phương pháp này là sẽ làm trầm trọng thêm nhược điểm thứ hai của hệ thống tập trung hóa bởi vì vai trò của từng authority con cũng tương tự như authority trong hệ thống tập trung hóa. Do đó hệ thống thay vì phải đảm bảo một authority không quá tải hoặc không bị tấn công như trong trường hợp tập trung hóa, ở đây hệ thống phải đảm bảo điều đó cho n authority.

Để giải quyết vấn đề thứ hai, ý tưởng tiếp theo là dùng kỹ thuật chia sẻ thành phần bí mật (secret sharing). Cụ thể, ta vẫn dựa trên ý tưởng chia α thành các α_i con như ở trên, tuy nhiên ta dùng kỹ thuật secret sharing thay vì việc chia đơn giản như ý tưởng đầu tiên. Trong kỹ thuật secret sharing để chia sẻ thành phần bí mật α, ta dùng một đa thức P có bậc là τ, trong đó $P(0) = \alpha$ (khi xây dựng hệ ta chọn P trước tính P(0), sau đó chọn $\alpha = P(0)$). Bằng phương pháp nội suy đa thức, nếu ta biết $\tau + 1$ giá trị khác nhau của đa thức P, ví dụ $P(x_1)$, $P(x_2)$, …, $P(x_{t+1})$, ta có thể tính được giá trị P(0). Áp dụng kỹ thuật này vào hệ Riepel-Wee, ta tạo ra n authority con ($n > \tau$), mỗi authority con được cấp một giá trị bí mật $P(x_i)$ khác nhau. Trong giải thuật tạo khóa, từng người dùng sẽ xin cấp khóa từ các authority con này. Tuy nhiên thay vì phải xin đủ n khóa từ n authority con như ý tưởng đầu tiên, ở đây người dùng chỉ cần xin đủ $\tau + 1$ khóa từ $\tau + 1$ authority con là có thể tính được khóa chính để giải mã (bằng phương pháp nội suy đa thức). Như vậy ý tưởng này giải quyết được cả hai vấn đề đối với hệ thống tập trung hóa, cụ thể:

Do tách thành nhiều authority con, nên kẻ tấn công hay authority gian dối phải có đủ ít nhất $\tau + 1$ khóa bí mật của authority con mới có thể tính được khóa của người dùng. Như vậy sẽ giảm thiểu được xác suất bị lộ khóa bí mật của người dùng nếu ta đặt τ đủ lớn.

Trong trường hợp một vài (nhỏ hơn -1) authority con bị quá tải hay bị tấn công dẫn đến không hoạt động, hệ thống vẫn có thể thực hiện chức năng cung cấp khóa cho người dùng như thông thường. Như vậy sẽ giảm thiểu xác suất hệ thống không hoạt động chức năng cung cấp khóa nếu ta đặt *n* đủ lớn.

3.2. Hệ mã đề xuất

Hệ mã dựa trên chính sách ở bản mã bao gồm 4 giải thuật:

Khởi tạo: khởi tạo các tham số chung cho toàn bộ hệ thống như khóa công khai của toàn bộ hệ thống, khóa bí mật của n authority của hệ thống. Lưu ý giải thuật chỉ chạy một lần duy nhất khi khởi tạo hệ thống.

Tạo khóa: giải thuật tạo ra khóa bí mật cho người dùng mới tham gia vào hệ thống dựa trên đầu vào là tập thuộc tính của người dùng và khóa bí mật của tối thiểu $\tau + 1$ authority của hệ thống.

Mã hóa: như hệ Doreen Riepel-Hoteck Wee.

Giải mã: như hệ Doreen Riepel-Hoteck Wee.

Các giải thuật cụ thể như sau:

Khởi tạo $(1^\lambda, \tau, n)$.

Dựa trên tham số đầu vào λ, tạo ra hệ thống Pairings G:=(p,$\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$,e,g_1,g_2). Chọn ngẫu nhiên một đa thức P có bậc là τ, đặt α = P(0), chọn hàm băm H : $[|\mathcal{U}|+ 1] \rightarrow \mathbb{G}_1$, trong đó $\mathcal{U}$ là tập các thuộc tính của hệ thống. Chọn ngẫu nhiên $x_1, x_2, \dots, x_n \xleftarrow{\$} \mathbb{Z}_p$ và khác 0, tính khóa bí mật của *n* authority lần lượt là P(x_1), P(x_2), …, P(x_n).

Khóa công khai mpk của hệ thống:

mpk:= (G,H,$e(g_1,g_2)^\alpha$, x_1, x_2, …, x_n)

Lưu ý giải thuật khởi tạo chạy một lần duy nhất khi khởi tạo hệ thống, đa thức P sau đó bị hủy không thực thể nào biết đa thức P.

Tạo khóa (P(x_1), P(x_2), …, P(x_t), $S \in \mathcal{U}$).

Không mất tính tổng quát, giả sử người dùng liên hệ với $\tau + 1$ authority từ 1 đến $\tau + 1$ để lấy khóa bí mật thành phần (trong thực tế người dùng có thể lựa chọn ngẫu nhiên các authortiy để lấy khóa bí mật thành phần). Từng authority i ($i = 1, \dots, \tau + 1$) chọn ngẫu nhiên $r_i \xleftarrow{\$} \mathbb{Z}_p$.Tính khóa bí mật với mỗi $u \in S$:

$$\mathrm{sk}_{1,i} := g_1^{P(x_i)}.\mathrm{H}(|\mathcal{U}| + 1)^{r_i}, \mathrm{sk}_{2,u,i} = \mathrm{H}(u)^{r_i}, \mathrm{sk}_{3,i} := g_2^{r_i}$$

Sau khi nhận đủ $\tau + 1$ khóa bí mật, người dùng thực hiện phép nội suy đa thức để tính lại khóa bí mật chính:

$$\mathrm{sk}_1 := g_1^{\sum_{i=1}^{\tau+1} \lambda_i P(x_i)}.\mathrm{H}(|\mathcal{U}| + 1)^{\sum_{i=1}^{\tau+1} \lambda_i r_i} = g_1^{\alpha}.\mathrm{H}(|\mathcal{U}| + 1)^{r}$$

$$\mathrm{sk}_{2,u} = \mathrm{H}(u)^{\sum_{i=1}^{\tau+1} \lambda_i r_i} = \mathrm{H}(u)^{r}$$

$$\mathrm{sk}_3 := g_2^{\sum_{i=1}^{\tau+1} \lambda_i r_i} = g_2^{r}$$

Trong đó $\lambda_i = \Pi_{j \neq i, j=1,\dots,\tau+1} \frac{x_j}{x_j - x_i}$.

Đầu ra là khóa bí mật sk := (sk_1,{$\mathrm{sk}_{2,u}$}$_{u \in S}$, sk_3)

Mã hóa (mpk,(M,π)). Như thuật toán mã hóa hệ mã Riepel-Wee

Giải mã (mpk,(M,π), *S*, ct, sk*).* Như thuật toán giải mã hệ mã Riepel-Wee

3.3. An toàn của hệ mã đề xuất

An toàn của hệ mã đề xuất được suy ra một cách tự nhiên từ an toàn của hệ mã Riepel-Wee và kỹ thuật chia sẻ thành phần bí mật (secret sharing). Do hệ mã đề xuất giữ nguyên giải thuật mã hóa của hệ Riepel - Wee, trong khi đó kẻ tấn công không có thêm bất cứ thông tin gì về khóa bí mật chính α của hệ thống nếu không tấn công đủ $\tau + 1$ authority con (theo tính chất của kỹ thuật secret sharing). Do vậy an toàn của hệ mã đề xuất được suy ra một cách tự nhiên từ an toàn của hệ mã Riepel-Wee và kỹ thuật secret sharing.

4. SO SÁNH VỚI MỘT SỐ HỆ MÃ DỰA TRÊN THUỘC TÍNH CÓ HỖ TRỢ TÍNH PHI TẬP TRUNG HÓA HIỆN CÓ

Tiêu chuẩn chính khi so sánh các hệ mã bao gồm: chức năng của hệ mã, tính an toàn của hệ mã, tốc độ của hệ mã (tốc độ mã hóa, tốc độ giải mã), dung lượng (độ dài bản mã, độ dài khóa bí mật, độ dài khóa công khai). Hệ mã đề xuất được xây dựng dựa trên hệ mã Riepel-Wee, do vậy được kế thừa các đặc tính của hệ mã trên. Lưu ý rằng hệ mã Riepel-Wee được phát triển gần đây được xem là một trong những hệ mã tốt nhất hiện nay. So sánh các tiêu chuẩn cụ thể của hệ mã đề xuất và các hệ mã có cùng chức năng (tính phi tập trung hóa) được trình bày trong bảng 1 sau.

Hệ mã	Bản mã	Khóa bí mật	Khóa công khai	Mã hóa	Giải mã
[4]	$3l+1$	$\|S\|k_{max}$ +6	$2Nk_{max}$ +2	$(3l+1)$exp	2I pairing
[2]	$3l+1$	$\|S\|k_{max}$	$2Nk_{max}$ +3	$(3l+1)$exp	2I pairing
[3]	$l+2$	$\|S\|k_{max}$ +2	Nk_{max} +5	$(l+2)$exp	2 pairing
Hệ đề xuất	$l+ k_{max}$ +1	$\|S\|+2$	n+1	$(l+ k_{max}$ +1)exp	$(k_{max}$ +2) pairing

Bảng 1. So sánh một số hệ mã hóa dựa trên thuộc tính hỗ trợ tính chất phi tập trung hóa

Trong bảng so sánh trên: l là số thuộc tính có trong một chính sách (policy). Ví dụ với chính sách là KHMT *và* Nam *và* (Triệu Sơn *hoặc* Thiệu Hóa), ta có $l = 4$.

k_{max} là số lần tối đa một thuộc tính có thể xuất hiện trong một chính sách. Ví dụ với chính sách (KHMT *và* Nam *và* Triệu Sơn) *hoặc* (KHMT *và* Nam *và* Thiệu Hóa), thuộc tính Nam xuất hiện hai lần. Lưu ý rằng k_{max} được khởi tạo cố định ngay từ đầu, do vậy khi khởi tạo hệ ta phải chọn k_{max} đủ lớn để người lập mã thoải mái chọn chính sách.

$|\boldsymbol{S}|$ là số thuộc tính mà người dùng u sở hữu.

N là tổng số thuộc tính có trong hệ thống

n là số authority con

I là số thuộc tính để thỏa mãn một chính sách khi giải mã của người dùng. Ví dụ với chính sách (KHMT *và* Nam *và* Triệu Sơn) *hoặc* (KHMT *và* Nam *và* Thiệu Hóa), I =3, vì cần 3 thuộc tính KHMT *và* Nam *và* Triệu Sơn để giải mã.

exp là phép lũy thừa;

pairing là phép tính song tuyến tính. Một phép tính pairing bằng khoảng 50 lần một phép lũy thừa.

Lưu ý rằng N sẽ rất lớn (lớn hơn nhiều so với n), k_{max} thường nhỏ hơn *l*. Do vậy hệ đề xuất có độ dài khóa bí mật và khóa công khai tốt nhất trong các hệ hiện có. Trong khi các chỉ số khác tiệm cận với các chỉ số của hệ tốt nhất có hỗ trợ tính phi tập trung hóa hiện nay là hệ [4].

5. KẾT LUẬN

Hệ mã dựa trên thuộc tính có ứng dụng rộng rãi trong đảm bảo an toàn thông tin cho hệ thống điện toán đám mây, cũng như trong nhiều loại ứng dụng khác hiện nay như truyền hình trả tiền, chia sẻ files,... Trong nhiều tính chất của hệ mã, tính phi tập trung hóa là tính chất quan trọng đang được quan tâm, đặc biệt trong bối cảnh sự riêng tư (privacy) của người dùng đang là vấn đề nóng hiện nay. Trong bài báo này chúng tôi dựa trên hệ mã nổi tiếng gần đây của Riepel-Wee và kỹ thuật secret sharing đề xuất một hệ mã mới hỗ trợ tính phi tập trung hóa. Hệ mã đề xuất có các tính chất có thể so sánh được với các hệ mã hỗ trợ tính phi tập trung hóa hiện có, đặc biệt với các tính chất như độ dài khóa bí mật và độ dài khóa công khai.

TÀI LIỆU THAM KHẢO

[1] A. Sahai and B. R. Waters (2005), *Fuzzy identity-based encryption*, In R. Cramer, editor, Advances in Cryptology - EUROCRYPT, vol.3494 of Lecture Notes in Computer Science, pages 457-473, Aarhus, Denmark, May 22-26, Springer, Berlin, Germany.

[2] S. Agrawal and M. Chase (2017), *Simplifying design and analysis of complex predicate encryption schemes*, Advances in Cryptology EUROCRYPT.

[3] A. B. Lewko, B. Waters (2011), *Decentralizing attribute-based encryption*, In K. G. Paterson, editor, Advances in Cryptology EUROCRYPT, vol.6632 of Lecture Notes in Computer Science, pages 568-588, Tallinn, Estonia, May 15-19, Springer, Berlin, Germany.

[4] Qutaibah M Malluhi, Abdullatif Shikfa, Vinh Duc Tran, Viet Cuong Trinh (2019), *Decentralized ciphertext-policy attribute-based encryption schemes for lightweight devices*, Computer Communications Journal, vol.145, 113-125, Elsvier.

[5] Chuangui Ma, Aijun Ge, Jie Zhang (2019), *Fully Secure Decentralized Ciphertext-Policy Attribute-Based Encryption in Standard Model*, Proceedings of Information Security and Cryptology: Inscrypt January 2019. DOI: 10.1007/978-3-030-14234-6-23, Springer Berlin Heidelberg, Berlin, Heidelberg.

[6] D. Riepel, H. Wee (2022), *FABEO: Fast Attribute-Based Encryption with Optimal Security*, In C. Cremers and E. Shi editors, ACM CCS: 29th Conference on Computer and Communications Security, p.2491-2054, Los Angeles CA USA, Nov.7-11. ACM Press.

[7] Y. Rouselakis, B. Waters (2013), *Practical constructions and new proof methods for large universe attribute-based encryption*, In A.-R. Sadeghi, V. D. Gligor, and M. Yung, editors, ACM CCS 13: 20th Conference on Computer and Communications Security, p.463-474, Berlin, Germany, Nov. 4-8, ACM Press**.**

[8] Ong Wang, Biwen Chen, Lei Li, Qiang Ma, Huicong Li, Debiao He (2020), *Efficient and Secure Ciphertext-Policy Attribute Based Encryption Without Pairing for Cloud-Assisted Smart Grid*, IEEE Access, Digital Object Identifier 10.1109/ACCESS.2020.2976746.

[9] B. Waters (2011), *Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization*, In D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, editors, PKC 2011: 14th International Workshop on Theory and Practice in Public Key Cryptography, vol.6571, Lecture Notes in Computer Science, p.53-70, Taormina, Italy, Mar. 6-9, Springer, Berlin, Germany.

A NEW DECENTRALIZED ATTRIBUTE-BASED ENCRYPTION SCHEME

Le Phi Thuong, Le Dinh Hai, Trinh Viet Cuong, Le Xuan Lam

ABSTRACT

Attribute-based encryption (ABE) is an important encryption system nowadays, widely used in data storage on cloud computing, as well as in many other applications such as pay TV and file sharing. Attribute-based encryption allows for access control to user data based on attributes. Among the current attribute-based encryption systems, the system proposed by authors Riepel and Wee in 2022 is considered one of the most important. This system is highly efficient and has good security features; however, its drawback is the lack of support for decentralization. In this paper, we propose a solution to enhance the decentralization feature for the Riepel-Wee encryption system. We then provide a comparative analysis of the strengths and weaknesses of our proposed encryption system with some other attribute-based encryption systems that support decentralization features.

Keywords: *Attribute-based encryption, decentralized, cloud storage.*

** Ngày nộp bài: 16/11/2023; Ngày gửi phản biện: 25/11/2023; Ngày duyệt đăng: 10/12/2023*