p-ISSN 3030 - 4628
e-ISSN 3030 - 4636

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

Lê Xuân Lâm[1], Lưu Vũ Nam[2], Trịnh Viết Cường[3]

TÓM TẮT

Kỹ thuật dựa trên định danh được phát triển gần đây để thay thế cơ sở hạ tầng khóa công khai (PKI) kém hiệu quả. Tuy nhiên, kỹ thuật này có nhược điểm là khóa bí mật của người dùng do duy nhất một trung tâm cấp khóa tạo ra, dẫn đến rủi ro trong việc lộ khóa bí mật của người dùng. Để khắc phục nhược điểm này hướng nghiên cứu hiện nay là phi tập trung hóa trung tâm cấp khóa. Trong bài báo này chúng tôi đề xuất một hệ mã hóa mới dựa trên định danh hỗ trợ tính chất phi tập trung hóa của trung tâm cấp khóa. Hệ mã đề xuất có thể so sánh về tính hiệu quả và an toàn so với các hệ mã có cùng tính chất hiện có.

Từ khóa: *Mã hóa dựa trên định danh, phi tập trung hóa, cơ sở hạ tầng khóa công khai.*

DOI: *https://doi.org/10.70117/hdujs.72.03.2025.657*

1. GIỚI THIỆU CHUNG VỀ MÃ HÓA DỰA TRÊN ĐỊNH DANH

Mã hóa khóa công khai được giới thiệu vào thập niên 70 và ngày nay nó đã đóng vai trò không thể thiếu trong việc đảm bảo an toàn thông tin cho các giao dịch trên mạng, chính phủ điện tử, lưu trữ dữ liệu an toàn… Trong các mô hình đó mỗi cá nhân, đơn vị, tổ chức được cấp một cặp khóa công khai/bí mật đại diện cho chính bản thân mình để làm việc, tuy nhiên vấn đề đặt ra là mỗi khóa công khai chỉ là một dãy số ngẫu nhiên không cho biết chính xác nó đại diện cho ai, điều đó dẫn đến khả năng bị giả mạo trong giao dịch và làm việc. Để giải quyết vấn đề trên cơ sở hạ tầng khóa công khai (Public key Infrastructure - PKI) được phát triển, mục tiêu của nó là chứng minh một cách công khai về mặt pháp lý rằng một khóa công khai nhất định thuộc về một cá nhân, tổ chức, đơn vị nhất định, và mọi người có thể kiểm tra điều đó một cách dễ dàng. Khi một khóa công khai được xác thực thuộc về một thực thể khi đó các thực thể mới có thể dùng nó để thực hiện các công việc như lưu trữ dữ liệu, truyền dữ liệu trên mạng, và kiểm tra chữ ký điện tử. Trong bài báo này chúng tôi gọi tắt tất cả các vấn đề trên là Cryptography.

Có nhiều kỹ thuật để xây dựng PKI, kỹ thuật truyền thống là cần một trung tâm chứng thực có uy tín (Central Authority - CA) *đảm bảo* rằng một khóa công khai thuộc về một thực thể nhất định, đảm bảo ở đây thực tế là CA dùng chữ ký điện tử của mình để ký xác nhận rằng một khóa công khai thuộc về một thực thể nhất định, do vậy mọi thực thể khác hoàn toàn yên tâm khi làm việc với thực thể này. Lúc này mỗi khóa công khai sẽ kèm theo một chữ ký của CA, gọi là chứng thực số (certificate). Kỹ thuật này được dùng phổ biến trong thực tế hiện nay mà tiêu biểu là chuẩn X509. Mặc dù chữ ký điện tử đang được nghiên cứu mạnh trong thời gian gần đây, tuy nhiên độ dài của mỗi chữ ký vẫn là đáng kể,

[1] *Học viên cao học lớp K16 chuyên ngành Khoa học Máy tính, Khoa Kỹ thuật, Công nghệ và Truyền thông*
[2] *Trường Đại học Văn hóa, Thể thao và Du lịch Thanh Hóa*
[3] *Khoa Kỹ thuật, Công nghệ và Truyền thông, Trường Đại học Hồng Đức; Email: trinhvietcuong@hdu.edu.vn*

p-ISSN 3030 - 4628
e-ISSN 3030 - 4636

điều đó dẫn tới hạn chế của chuẩn X509 là độ dài của chứng thực số lớn không hiệu quả khi truyền trên mạng. Ngoài ra việc duy trì trung tâm CA để quản lý các chứng thực số và quá trình xin cấp chứng thực số cũng gây tốn kém và lãng phí. Để giải quyết vấn đề này nhiều kỹ thuật thay thế đã và đang được nghiên cứu bao gồm Identity-based Cryptography [1,2,3], Implicit Certificate Cryptography [4], Certificateless Cryptography [5], Registration-based Cryptography [6]. Trong đó với kỹ thuật Identity-based Cryptography ta không còn cần thiết phải xây dựng PKI, cụ thể ta có thể dùng một thông tin gì đó gắn với chính thực thể đó làm khóa công khai, khóa công khai lúc này không còn là một dãy số ngẫu nhiên. Ví dụ, ta có thể dùng số chứng minh thư hay địa chỉ email chính thức của một thực thể để làm khóa công khai, với khóa công khai như vậy dĩ nhiên ta không còn cần một CA để *đảm bảo* rằng khóa công khai này thuộc về ai đó, do đó ở đây ta không còn cần phải có chứng thực số hay không còn cần phải xây dựng PKI. Tuy nhiên, để từ một địa chỉ email hay chứng minh thư bất kỳ dùng làm khóa công khai có thể tạo ra được một khóa bí mật tương ứng, trong mô hình Identity-based Cryptography ta cần phải có một thực thể làm công việc đó gọi là trung tâm tạo khóa (Private Key Generator-PKG). Không như trong mô hình truyền thống, do CA không biết khóa bí mật của từng thực thể nên CA (hay những kẻ tấn công thành công CA) không có khả năng giả mạo thực thể đó để làm việc, ví dụ dùng khóa bí mật của một thực thể để đọc dữ liệu mà thực thể khác mã hóa cho thực thể này, hay dùng khóa bí mật để ký một văn bản. Ở đây PKG tạo ra khóa bí mật cho thực thể nên PKG (hay những kẻ tấn công thành công PKG) hoàn toàn có khả năng này. Do vậy, rủi ro đối với người dùng là cao hơn so với mô hình PKI truyền thống. Để giải quyết vấn đề này phương pháp phổ biến hiện nay là phi tập trung hóa trung tâm PKG. Với phương pháp này thay vì chỉ có duy nhất một trung tâm PKG cấp khóa bí mật cho người dùng, ta phân chia PKG thành các trung tâm con, mỗi trung tâm chịu trách nhiệm cấp một phần khóa bí mật cho người dùng, do vậy nếu một vài PKG con bị tấn công hay gian dối sẽ không gây rủi ro đối với khóa bí mật của người dùng.

Đóng góp của bài báo: Mã hóa dựa trên định danh (Identity-based encryption-IBE) là hướng nghiên cứu được các nhà nghiên cứu quan tâm, có rất nhiều các hệ mã hóa dựa trên định danh đã được công bố. Trong đó hệ mã của tác giả Hoteck Wee đề xuất năm 2016 [3] (được công bố tại một trong những hội nghị lớn nhất của ngành an toàn bảo mật thông tin Theory of Cryptography-TCC) vẫn được đánh giá là hệ mã dựa trên định danh hiệu quả và an toàn nhất hiện nay. 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. Chúng tôi cũng đồng thời đưa ra sự so sánh hệ mã đề xuất với các hệ mã dựa trên định danh có hỗ trợ tính chất phi tập trung hóa khác. Chúng tôi cũng lưu ý rằng bài báo của chúng tôi là nghiên cứu đầu tiên nghiên cứu tính phi tập trung hóa cho hệ mã của tác giả Hoteck Wee.

2. HỆ MÃ DỰA TRÊN ĐỊNH DANH CỦA HOTECK WEE

2.1. Phép ghép cặp đôi

Phép ghép cặp đôi Pairings được mô tả như sau:
Gọi $\mathbb{G}$, $\mathbb{G}_T$ là hai nhóm cyclic có bậc nguyên tố p.
g là phần tử sinh của tập $\mathbb{G}$.
e là một ánh xạ song tuyến tính ký hiệu $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$.
Trong đó phép *e* thỏa mãn hai tính chất sau:

p-ISSN 3030 - 4628
e-ISSN 3030 - 4636

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

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

Khi cài đặt với đường cong Eliptic thì $\mathbb{G}$, 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.

Nhóm có bậc là hợp số (Composite order group): Các nhóm $\mathbb{G}$, $\mathbb{G}_T$ có bậc là một số nguyên hợp (composite), tức là không phải là số nguyên tố p. Điều này có nghĩa là bậc của các nhóm $\mathbb{G}_1$, $\mathbb{G}_T$ là tích của ít nhất hai số nguyên tố. Trong bài báo này chúng tôi dùng $\mathbb{G}$ và $\mathbb{G}_T$ có bậc là số nguyên hợp N là tích của ba số nguyên tố p_1, p_2, p_3, tức là $\mathbb{G} = \mathbb{G}_1 \times \mathbb{G}_2 \times \mathbb{G}_3$, với g_1, g_2, g_3 lần lượt là phần tử sinh của ba nhóm con $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_3$.

2.2. Hệ mã dựa trên định danh của Hoteck Wee

Hệ mã dựa trên định danh 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 định danh của người dùng và khóa bí mật của hệ thống.

Mã hóa: đầu vào là định danh của người dùng, 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 tương ứng với định danh được dùng để mã hóa, giải thuật cho đầu ra là khóa phiên K. 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:=($N, \mathbb{G}, \mathbb{G}_T, e, g_1, g_2, g_3$). Trong đó g_1, g_2, g_3, lần lượt là phần tử sinh của ba nhóm con $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_3$. Chọn ngẫu nhiên $\alpha \xleftarrow{\$} \mathbb{Z}_N$, u, $\xleftarrow{\$} \mathbb{G}_1$ và hàm băm

H : $\mathbb{G}_T$, $\rightarrow \{0,1\}^\lambda$. Tính khóa công khai mpk của hệ thống:

mpk:= (G,H, g_1, g_1^α, e(g_1, u))

Khóa bí mật của hệ thống msk := (α, u, g_3)

Tạo khóa (msk, ID $\in \mathbb{Z}_N$)

$sk_{ID} = u^{1/(\alpha+ID)}$

Mã hóa (mpk, ID $\in \mathbb{Z}_N$)

Chọn ngẫu nhiên $s \xleftarrow{\$} \mathbb{Z}_N$

Tính bản mã của khóa phiên CP = $g_1^{(\alpha+ID)s}$

Khóa phiên K = H(e(g_1,u)^s).

Lưu ý bản mã CP không cần bao gồm ID, do vậy hệ mã có tính chất ẩn danh người nhận.

Giải mã (sk_{ID}, CP)

Tính: K' = e(CP, sk_{ID}) = e($g_1^{(\alpha+ID)s}$, $u^{1/(\alpha+ID)}$) = e(g_1,u)^s

Tính khóa phiên K = H(K').

p-ISSN 3030 - 4628
e-ISSN 3030 - 4636

3. HỆ MÃ DỰA TRÊN ĐỊNH DANH 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 dựa trên định danh của Hoteck Wee khóa bí mật của hệ thống là α, khóa bí mật của từng người dùng sẽ được tính dựa trên α và định danh 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 trung tâm cấp khóa PKG ra thành n PKG con, mỗi PKG con sở hữu một giá trị α_i. Khi cấp khóa, mỗi PKG 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. Tuy nhiên, do α nằm dưới mẫu số của khóa nên ý tưởng như trên sẽ không thực hiện được. Do đó, thay vì tách α, chúng tôi bổ sung thêm một giá trị mới là β ở trên tử số và thực hiện tách β thành các β_i con. Việc bổ sung này không làm ảnh hưởng đến tính hiệu quả của hệ mã do vẫn giữ nguyên độ dài khóa và bản mã.

3.2. Hệ mã đề xuất

Hệ mã dựa trên định danh đề xuất bao gồm bốn 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* PKG 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 định danh của người dùng và khóa bí mật của *n* PKG của hệ thống.

Mã hóa: tương tự như hệ Hoteck Wee.

Giải mã: tương tự như hệ Hoteck Wee.

Các giải thuật cụ thể như sau:

Khởi tạo (1^{λ}).

Dựa trên tham số đầu vào λ và *n* (số các trung tâm cấp khóa) tạo ra hệ thống Pairings $G:=(N, \mathbb{G}, \mathbb{G}_T, e, g_1, g_2, g_3)$. Trong đó g_1, g_2, g_3, lần lượt là phần tử sinh của ba nhóm con $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_3$. Chọn ngẫu nhiên $\alpha, \beta, \beta_1, \ldots, \beta_n \xleftarrow{\$} \mathbb{Z}_N$, $u, \xleftarrow{\$} \mathbb{G}_1$ và hàm băm $H : \mathbb{G}_T, \rightarrow \{0,1\}^{\lambda}$ sao cho $\beta = \beta_1 + \ldots + \beta_n$ Tính khóa công khai mpk của hệ thống:

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

Khóa bí mật của trung tâm cấp khóa thứ i (với i đi từ 1 đến *n*) là $msk_i := (\alpha, \beta_i, u, g_3)$.

Tạo khóa (msk_i, $ID \in \mathbb{Z}_N$)

Người dùng nhận khóa thành phần thứ i từ trung tâm cấp khóa thứ i

$sk_{ID-i} = u^{\beta i/(\alpha+ID)}$, với i = 1, …, *n*

Sau khi nhận đủ *n* khóa thành phần, tính khóa bí mật

$sk_{ID} = sk_{ID-1} . sk_{ID-2} \ldots sk_{ID-n} = u^{\beta/(\alpha+ID)}$

Mã hóa (mpk, $ID \in \mathbb{Z}_N$)

Chọn ngẫu nhiên $s \xleftarrow{\$} \mathbb{Z}_N$

Tính bản mã của khóa phiên $CP = g_1^{(\alpha+ID)s}$

Khóa phiên $K = H(e(g_1,u)^{s\beta})$.

Lưu ý bản mã CP không cần bao gồm ID, do vậy hệ mã có tính chất ẩn danh người nhận.

p-ISSN 3030 - 4628
e-ISSN 3030 - 4636

Giải mã (sk_{ID}, CP)

Tính: $K' = e(CP, sk_{ID}) = e(g_1^{(\alpha+ID)s}, u^{\beta/(\alpha+ID)}) = e(g_1,u)^{s\beta}$

Tính khóa phiên $K = H(K')$.

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 Hoteck Wee. Do hệ mã đề xuất giữ nguyên giải thuật mã hóa của hệ Hoteck Wee, trong khi đó kẻ tấn công không có thêm bất cứ thông tin gì về khóa bí mật chính β của hệ thống nếu không tấn công đủ *n* PKG con. Do vậy, an toàn của hệ mã đề xuất được suy ra một cách tự nhiên từ an toàn của hệ mã Hoteck Wee.

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

Mã hóa dựa trên thuộc tính (Attribute-based encryption - ABE) [7,8,9] là mở rộng của mã hóa dựa trên định danh. Trong đó, nếu như mỗi người dùng trong hệ ABE sở hữu duy nhất một thuộc tính chính là định danh (ID) của mình thì khi đó hệ ABE sẽ trở thành hệ mã dựa trên định danh (IBE). Do đó, hiển nhiên các hệ ABE hỗ trợ tính chất phi tập trung hóa cũng quy về hệ IBE hỗ trợ tính chất phi tập trung hóa. Ngoài ra, chúng tôi cũng lưu ý rằng để giải quyết vấn đề trung tâm cấp khóa PKG biết khóa bí mật của người dùng, hiện nay có một vài kỹ thuật được đề xuất để giải quyết vấn đề này như kỹ thuật chứng thư số ẩn (Implicit certificate encryption) [4], kỹ thuật không chứng chỉ (Certificateless encryption) [5] hay gần đây là kỹ thuật dựa trên đăng ký (Registration-based encryption) [6]. Tuy nhiên, bài báo này chỉ tập trung trong phạm vi so sánh các hệ mã dựa trên định danh hỗ trợ tính phi tập trung hóa, không đi sâu vào so sánh ưu, nhược điểm của các loại kỹ thuật khác nhau.

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 Hoteck Wee, do vậy được kế thừa các đặc tính của hệ mã trên. Lưu ý rằng hệ mã Hoteck Wee đến nay vẫn được xem là một trong những hệ mã dựa trên định danh hiệu quả 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.

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

Hệ mã	Bản mã	Khóa bí mật	Khóa công khai	Mã hóa	Giải mã
[7]	4	7	2 + N	4 exp	2 pairing
[5]	4	1	3 + N	4 exp	2 pairing
[6]	3	3	5 +N	3 exp	2 pairing
Hệ đề xuất	1	1	3	2 exp	1 pairing

Trong bảng so sánh trên:

exp là phép lũy thừa;

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

N là số người dùng trong hệ thống;

p-ISSN 3030 - 4628
e-ISSN 3030 - 4636

Hệ mã của chúng tôi dùng nhóm là hợp số $\mathbb{G} = \mathbb{G}_1 \times \mathbb{G}_2 \times \mathbb{G}_3$, do vậy kích thước một phần tử của chúng tôi tương đương khoảng 3 phần tử của các hệ khác; an toàn hệ mã chúng tôi dựa trên hệ mã Hoteck Wee do vậy đạt an toàn adaptive security. Các hệ mã khác chỉ đạt an toàn mức yếu hơn là selective security (yêu cầu kẻ tấn công phải chọn trước định danh của người dùng để tấn công trước khi biết các thông tin khác).

5. KẾT LUẬN

Kỹ thuật dựa trên định danh là kỹ thuật quan trọng dùng để thay thế cơ sở hạ tầng khóa công khai. Tuy nhiên, điểm yếu hiện nay của kỹ thuật này là việc trung tâm cấp khóa PKG biết khóa bí mật của người dùng. Hướng nghiên cứu hiện nay để giải quyết vấn đề này là phi tập trung hóa trung tâm cấp khóa của người dùng. Trong bài báo này chúng tôi nghiên cứu đề xuất một hệ mã hóa dựa trên định danh có hỗ trợ tính phi tập trung hóa. Hệ mã đề xuất của chúng tôi có tính an toàn và hiệu quả có thể so sánh được với các hệ mã dựa trên định danh có hỗ trợ tính phi tập trung hóa hiện có.

TÀI LIỆU THAM KHẢO

[1] D. Boneh, M. K. Franklin (2001), *Identity-based encryption from the weil pairing*, In CRYPTO, Lecture Notes in Computer Science, J. Kilian, Ed., Springer, vol. 2139, pp. 213-229.

[2] A. Shamir (1984), *Identity-based cryptosystems and signature schemes*, In G. R. Blakley and D. Chaum, editors, Advances in Cryptology - CRYPTO'84.

[3] Hoteck Wee (2016), *DéJà Q Uncore!Un Petit IBE*, In Eyal Kushilevitz and Tal Malkin, editors, TCC 2016: 13th International Conference, TCC 2016-A, Tel Aviv, Israel, Springer LNCS Proceedings, Part II.

[4] Daniel R. L. Brown, Matthew J. Campagna and Scott A. Vanstone (2011), *Security of ECQV-Certified ECDSA Against Passive Adversaries*.

[5] S. Al-Riyami, K. G. Paterson (2003), *Certificateless public key cryptography*, In C.-S. Laih, editor, Advances in Cryptology - ASIACRYPT.

[6] Noemi Glaeser, Dimitris Kolonelos, Giulio Malavolta, Ahmadreza Rahimi (2023), *Efficient Registration-based encryption*, CCS '23: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, pp.1065-1079,

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

[8] 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, pp.113-125, Elsvier.

[9] Chuangui Ma, Aijun Ge, Jie Zhang (2019), *Fully Secure Decentralized Ciphertext-Policy Attribute-Based Encryption in Standard Model*, Proceedings of Information Security and Cryptology.

p-ISSN 3030 - 4628
e-ISSN 3030 - 4636

A NEW DECENTRALIZED IDENTITY-BASED ENCRYPTION SCHEME

Le Xuan Lam, Luu Vu Nam, Trinh Viet Cuong

ABSTRACT

Identity-based cryptography is an important technique since it can replace the inefficient public key infrastructure. This technique, however, has a shortcoming that the authority can know the secret key of users. To deal with this shortcoming of Identity-based cryptography, researchers try to decentralize the authority. Continuing with this line of work, in this paper we propose a new identity-based encryption scheme supporting decentralized property. Our proposed scheme can be comparable to other existing identity-based encryption schemes supporting decentralized property.

Keywords: *Identity-based encryption, decentralized, public key infrashstructure.*

** Ngày nộp bài: 07/11/2024; Ngày gửi phản biện: 21/11/2024; Ngày duyệt đăng: 10/03/2025*