MỘT LƯỢC ĐỒ CHỮ KÝ TẬP THỂ CÓ CẤU TRÚC TỔNG QUÁT DỰA TRÊN MẬT MÃ ĐỊNH DANH

***Vũ Tất Điệp*[1]**
Email: diepvt@hou.edu.vn

Ngày tòa soạn nhận được bài báo: 02/06/2025
Ngày phản biện đánh giá: 08/09/2025
Ngày bài báo được duyệt đăng: 15/10/2025

DOI: 10.59266/houjs.2025.731

Tóm tắt: *Trong môi trường nghiệp vụ hiện đại, các quy trình phức tạp đòi hỏi sự tham gia của nhiều bên với vai trò và trách nhiệm khác nhau, khiến các lược đồ chữ ký tập thể truyền thống trở nên thiếu linh hoạt. Bài báo này kiến nghị một mô hình chữ ký tập thể với cấu trúc tổng quát, cho phép thiết lập một mối quan hệ ký "nhiều-nhiều"giữa một nhóm người ký và các thành phần của văn bản. Để hiện thực hóa mô hình, một lược đồ chữ ký cụ thể được xây dựng dựa trên mật mã định danh (IBC) và phép ghép cặp song tuyến tính. Việc áp dụng IBC không chỉ giúp loại bỏ gánh nặng trong việc quản lý và phân phối chứng thư số của hạ tầng khóa công khai (PKI) mà còn cung cấp khả năng miễn nhiễm tự nhiên trước các cuộc tấn công khóa lừa đảo (rogue-key attack). Một chứng minh an toàn hình thức được cung cấp trong mô hình tiên tri ngẫu nhiên, cho thấy lược đồ đạt được tính không thể giả mạo hiện hữu trước tấn công lựa chọn thông điệp và định danh thích ứng (EUF-CMA-ID), dựa trên độ khó của bài toán tính toán Diffie-Hellman (CDHP). Phân tích so sánh về hiệu năng cho thấy lược đồ đề xuất có chi phí tính toán và kích thước chữ ký cạnh tranh, trong khi vẫn đảm bảo tính linh hoạt vượt trội, phù hợp với các ứng dụng thực tiễn như hợp đồng điện tử, quy trình phê duyệt tài chính, và quản lý chuỗi cung ứng.*

Từ khóa: *chữ ký tập thể, chữ ký đa chữ ký, mật mã dựa trên định danh, cặp song tuyến tính, an toàn có thể chứng minh*

I. Đặt vấn đề

Trong bối cảnh chuyển đổi số, các quy trình nghiệp vụ phức tạp như phê duyệt hợp đồng đa phương, quản lý chuỗi cung ứng, hay bỏ phiếu điện tử ngày càng đòi hỏi sự tham gia và ràng buộc trách nhiệm của nhiều bên (Jinila & Komathy, 2015). Điều này tạo ra một nhu cầu cấp thiết về một cơ chế chữ ký số linh hoạt, có khả năng phản ánh chính xác các mối quan hệ trách nhiệm phức tạp này.

[1] Khoa Điện - Điện Tử, Trường Đại học Mở Hà Nội

Các lược đồ chữ ký tập thể truyền thống thường giả định vai trò của các thành viên là ngang hàng (Bellare & Neven, 2006), trong khi các mô hình cải tiến như của Harn (1999) chỉ hỗ trợ mối quan hệ ký ’một-một’ giữa người ký và thành phần văn bản (Li et al., 2000). Khoảng trống nghiên cứu hiện nay chính là sự thiếu vắng một lược đồ hiệu quả cho phép một mối quan hệ ký ’nhiều-nhiều’ (many-to-many) – tức là một người có thể ký nhiều phần, và một phần có thể yêu cầu nhiều người cùng ký (Gentry & Ramzan, 2006).

Để giải quyết triệt để vấn đề này, bài báo đề xuất một mô hình chữ ký tập thể có cấu trúc tổng quát và hiện thực hóa nó bằng một lược đồ cụ thể dựa trên mật mã định danh (IBC). Ưu điểm vượt trội của giải pháp này là: (1) Hỗ trợ đầy đủ mối quan hệ ký ’nhiều-nhiều’ thông qua ma trận trách nhiệm linh hoạt (Micali, Ohta, & Reyzin, 2001). (2) Loại bỏ sự phức tạp của hạ tầng khóa công khai (PKI) và miễn nhiễm tự nhiên với tấn công khóa lừa đảo (rogue-key attack) nhờ sử dụng IBC (Shamir, 1985; Boneh & Franklin, 2001). (3) Đạt được an toàn có thể chứng minh và hiệu năng cạnh tranh (Pointcheval & Stern, 2000; Cha & Cheon, 2003).

Hiện tượng này ảnh hưởng đến khoảng 80% bệnh nhân trong các giai đoạn tiến triển của bệnh (Pérez-López et al., 2016), thường xuất hiện khi bắt đầu đi, quay người, hoặc đi qua các không gian hẹp, từ đó làm gia tăng đáng kể nguy cơ té ngã, hạn chế tính tự chủ và suy giảm nghiêm trọng chất lượng cuộc sống (Walton et al., 2015; Creaby & Cole, 2012).

II. Cơ sở lý thuyết

2.1. Cặp song tuyến tính (Bilinear Pairings)

Phép ghép cặp song tuyến tính là một công cụ toán học nền tảng, cho phép thiết kế nhiều giao thức mật mã hiện đại (Menezes1993). Một ánh xạ song tuyến tính e: $G_1 \times G\_1 \rightarrow G_T$ (với G_1, G_T là các nhóm cyclic cùng cấp nguyên tố q) phải thỏa mãn đồng thời ba thuộc tính cốt lõi (Galbraith2008):

1. **Tính song tuyến tính:** Cho phép thực hiện các phép toán mũ trên các phần tử của nhóm, thể hiện qua đẳng thức $e(aP, bQ) = e(P, Q)^{ab}$.

2. **Tính không suy biến:** Đảm bảo ánh xạ không tầm thường ($e(P, P) \neq 1_{G_T}$), giúp tạo ra các giá trị có ý nghĩa trong nhóm đích.

3. **Khả năng tính toán hiệu quả:** Tồn tại thuật toán để tính giá trị $e(P, Q)$ trong thời gian chấp nhận được.

Các cấu trúc này thường được xây dựng từ cặp Weil hoặc Tate trên đường cong elliptic Barreto2006.

2.2. Các Giả định Độ phức tạp

Độ an toàn của lược đồ đề xuất dựa trên độ khó của bài toán tính toán Diffie-Hellman (CDHP) trong các nhóm được trang bị phép ghép cặp. Định nghĩa 2 (CDHP): Cho một nhóm cyclic G_1 cấp q, một phần tử sinh $P \in G_1$ và các phần tử aP, $bP \in G_1$ với $a, b \in Z_q$ chưa biết. Bài toán CDHP là tính toán phần tử $abP \in G_1$. Giả định CDHP cho rằng không có thuật toán thời gian đa thức nào có thể giải bài toán CDHP với xác suất đáng kể.

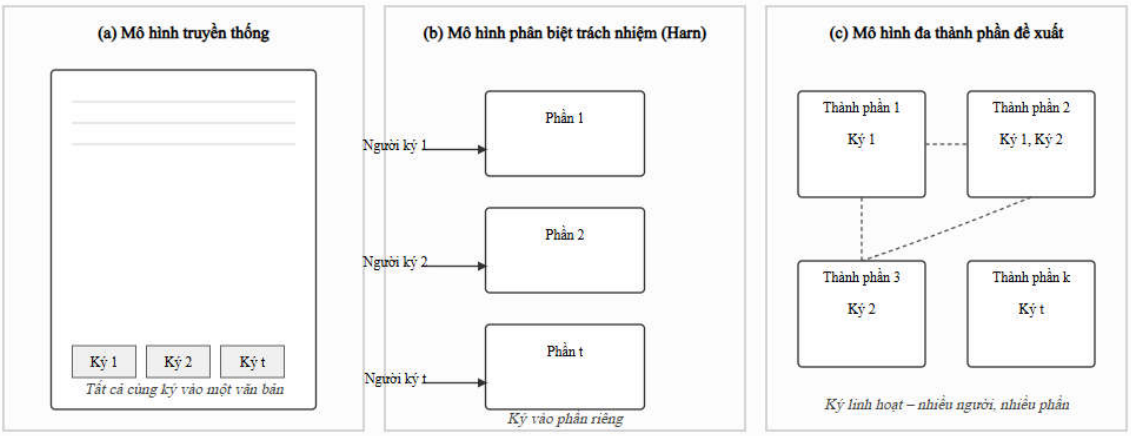
2.3. Mô hình An toàn

Lược đồ của chúng tôi được chứng minh an toàn trong mô hình tiêu chuẩn, cụ thể là Tính không thể giả mạo hiện hữu trước tấn công lựa chọn thông điệp và định danh thích ứng (EUF-CMA-ID) (*Boldyreva2003, Boldyreva2003; *Cha2003, Cha2003). Mô hình này được định nghĩa qua một trò chơi tương tác giữa một Kẻ tấn công A và một Người thách đố C. Kẻ tấn công được cấp quyền truy vấn oracle để lấy khóa bí mật và tạo chữ ký. A được xem là thành công nếu có thể tạo ra một chữ ký giả mạo hợp lệ cho một thông điệp mới, dưới một định danh mà khóa bí mật tương ứng chưa từng bị truy vấn trước đó.

III. Phương Pháp Nghiên Cứu

3.1. Mô hình Hệ thống

Hệ thống bao gồm ba thực thể: Trung tâm tạo khóa (PKG), Người ký (Signers), và Người xác thực (Verifier). Văn bản M được chia thành t thành phần, $M = \{m_1, \ldots, m_t\}$. Một nhóm gồm n người ký $U = \{u_1, \ldots, u_n\}$ sẽ tham gia ký. Mối quan hệ giữa người ký và các thành phần văn bản được định nghĩa bởi một ma trận trách nhiệm **A**, là một ma trận nhị phân kích thước $n \times t$. Phần tử $\mathbf{A}[i, j] = 1$ nếu người ký u_i chịu trách nhiệm ký thành phần m_j, và ngược lại.



Hình 1: Mô hình ký tập thể có cấu trúc tổng quát. Một tập hợp n người ký và k thành phần văn bản có mối quan hệ ký nhiều-nhiều linh hoạt, được định nghĩa bởi ma trận trách nhiệm.

3.2. Xây dựng Lược đồ

Lược đồ được xây dựng dựa trên năm thuật toán sau:

1. **Setup(1^λ):** Giai đoạn này do PKG khởi tạo với các bước:

• Chọn một cặp song tuyến tính (e, G_1, G_T) bậc q, một phần tử sinh $P \in G_1$.

Chọn một khóa bí mật chủ $s \in Z^*$ và tính khóa công khai chủ $P_{pub} = sP$.

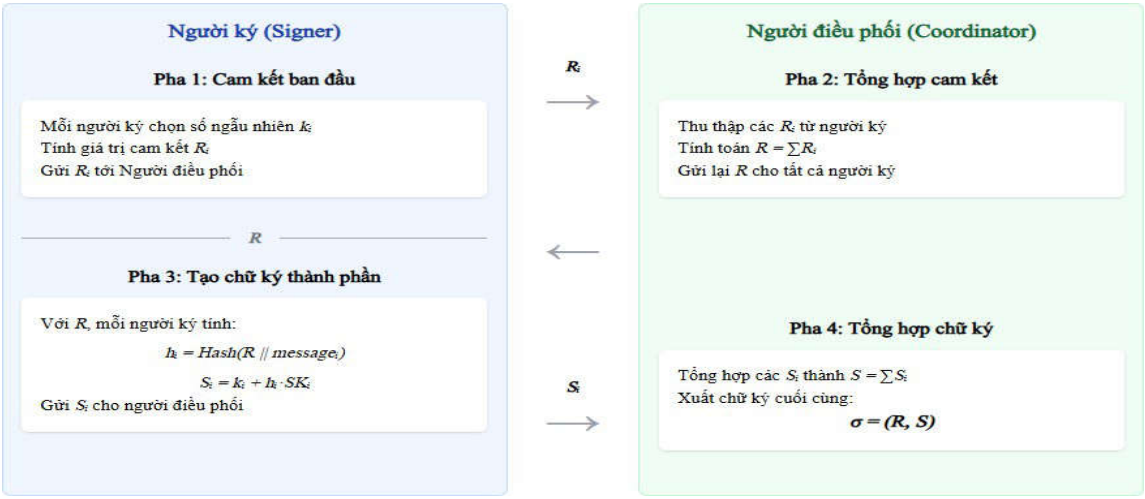
Chọn hai hàm băm mật mã: $H_1 : \{0, 1\}^* \rightarrow G_1$ và $H_2 : \{0, 1\}^* \rightarrow Z^*$.

• Công bố các tham số công khai $params = \{q, e, P, P_{pub}, H_1, H_2\}$. Giữ bí mật $msk = s$.

2. **Extract($params, s, ID_i$):** PKG tính và gửi khóa bí mật $SK_i = s \cdot H_1(ID_i)$ cho người dùng

u_i có định danh ID_i.

3. **Sign($params$, $\{SK_i\}$, M, $\mathbf{A}$):**



Hình 2: Mô hình lưu đồ thuật toán tạo chữ ký tập thể

Bước 1 (Cam kết): Mỗi người ký u_i chọn ngẫu nhiên $k_i \in Z^*$ và tính cam kết $R_i = k_i P$.

Các R_i được quảng bá.

• *Bước 2 (Tính toán tổng hợp):* Một người điều phối (hoặc mỗi thành viên) tính cam

kết tổng hợp $R = \sum_{i=1}^{n} R_i$.

• *Bước 3 (Tạo chữ ký thành phần):* Mỗi người ký u_i tính tổng giá trị băm của các thành phần mình chịu trách nhiệm: $h_i = \sum^{t} H_2(m_j, R) \pmod q$. Sau đó, u_i tính chữ ký thành phần: $S_i = k_i P + h_i SK_i$.

• *Bước 4 (Tạo chữ ký tập thể):* Người điều phối thu thập các S_i và tính chữ ký tập thể cuối cùng: $S = \sum^{n} S_i$. Chữ ký cuối cùng là $\sigma = (R, S)$.

4. **Verify** (*params*, $\{ID_i\}$, M, **A**, σ **):** Để xác thực chữ ký $\sigma = (R, S)$, người xác thực thực hiện:

• Tính khóa công khai $Q_i = H_1(ID_i)$ cho mỗi u_i.

• Tính khóa công khai tổng hợp dựa trên cấu trúc ký:

$$Q_{agg} = \sum_{i=1}^{n} \left(\left(\sum_{j=1, A[i,j]=1}^{t} H_2(m_j, R) \right) \cdot Q_i \right) \quad (1)$$

• Kiểm tra phương trình xác thực:

$$[e(S, P) \backslash overset? = e(R, P) \cdot e\left(\underline{O_{\text{agg}}}, P_{\text{pub}}\right)] \quad (2)$$

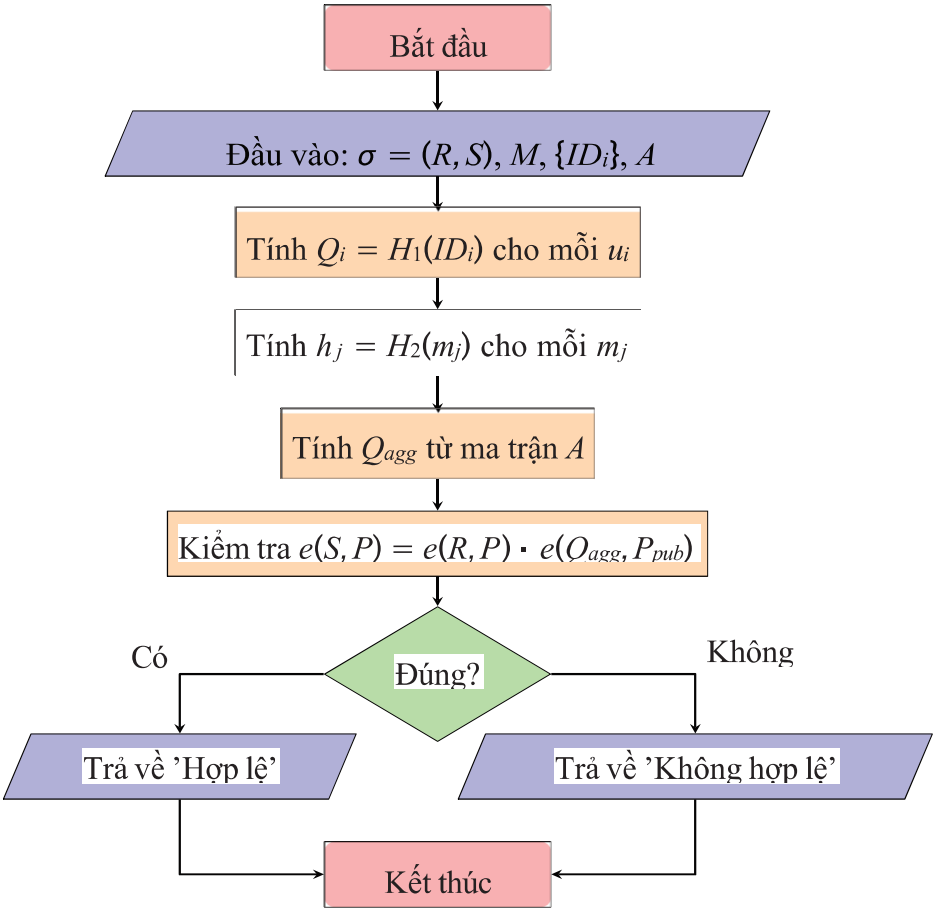
Nếu đẳng thức đúng, chữ ký hợp lệ.

Đẳng thức trên chứng tỏ lược đồ là đúng đắn về mặt toán học.

Chứng minh Tính đúng đắn:

$$\begin{aligned} e(S, P) &= e(\sum (k_i P + h_i SK_i), P) \\ &= e(\sum k_i P, P) \cdot e(\sum h_i (sQ_i), P) \\ &= e(R, P) \cdot e(\sum h_i Q_i, sP) \\ &= e(R, P) \cdot e(Q_{agg}, P_{pub}) \end{aligned}$$

3.3. Lưu đồ Thuật toán Xác thực



Hình 3: Lưu đồ thuật toán xác thực chữ ký

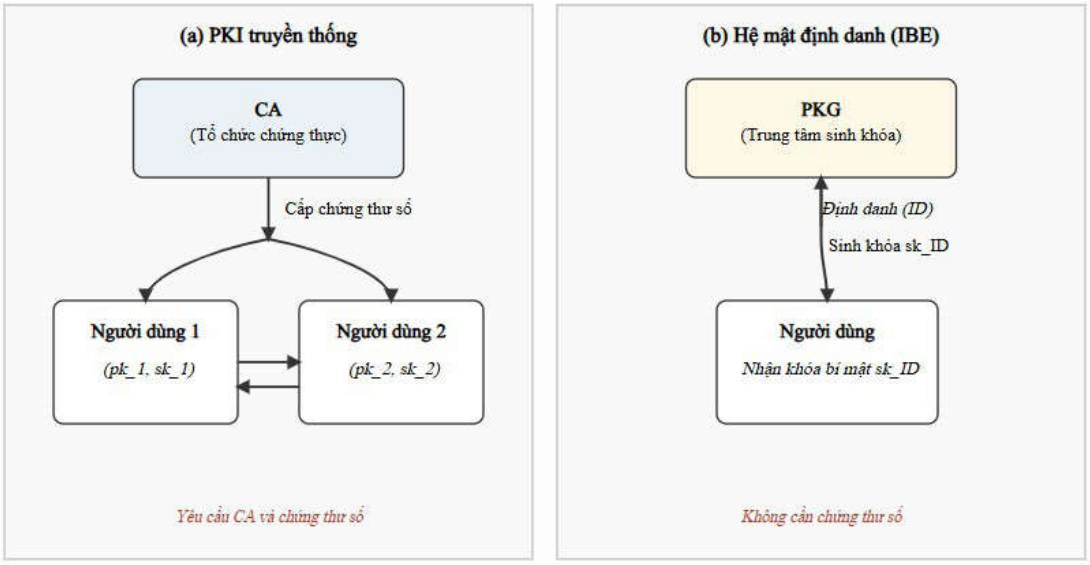
IV. Phân tích và Thảo luận

4.1. Phân tích An toàn

Định lý 1. *Lược đồ đề xuất đạt được an toàn EUF-CMA-ID trong mô hình tiên tri ngẫu nhiên, với giả định rằng bài toán CDHP là khó giải trong nhóm* G_1.

Sơ lược ý tưởng chứng minh: Chứng minh được thực hiện bằng kỹ thuật quy giản. Một thuật toán *B* được xây dựng để giải bài toán CDHP (*P, aP, bP*) bằng cách tương tác với kẻ tấn công *A* như một chương trình con. *B* sẽ mô phỏng môi trường cho *A* và sử dụng kỹ thuật Rẽ nhánh (Forking Lemma) của Pointcheval2000 (Pointcheval2000). Khi *A* tạo ra một chữ ký giả mạo thành công, *B* có thể lợi dụng kết quả này để trích xuất và giải được giá trị *abP*. Sự tồn tại của một kẻ tấn công *A* hiệu quả sẽ dẫn đến một thuật toán hiệu quả để giải CDHP, điều này mâu thuẫn với giả định ban đầu về độ khó của bài toán.

Một ưu điểm an toàn nổi bật của việc sử dụng IBC là khả năng kháng lại tấn công khóa lừa đảo (Rogue-Key Attack) một cách tự nhiên. Trong các lược đồ dựa trên PKI, kẻ tấn công có thể chọn khóa công khai của mình một cách khéo léo để mạo danh cả nhóm Bellare2006. Trên lược đồ của chúng tôi, khóa công khai $Q_i = H_1(ID_i)$ được xác định một cách tất định, ngăn chặn hoàn toàn loại tấn công này.



Hình 4: So sánh quy trình quản lý khóa. (a) PKI truyền thống yêu cầu CA và chứng thư số. (b) Hệ mật định danh (IBC) đơn giản hóa quy trình, loại bỏ nhu cầu về chứng thư.

4.2. Phân tích Hiệu năng và So sánh

Bảng 1 so sánh chi phí tính toán và các tính năng của lược đồ đề xuất với các công trình tiêu biểu.

Lược đồ của chúng tôi có kích thước chữ ký không đổi, chỉ gồm hai phần tử của nhóm G_1. Chi phí ký của mỗi thành viên là rất hiệu quả, chỉ yêu cầu một phép nhân vô hướng. Chi phí xác thực phụ thuộc tuyến tính vào số lượng người ký, tuy nhiên các phép toán này có thể được thực hiện song song. Sự linh hoạt, quản lý khóa đơn giản và an toàn nội tại là những ưu điểm vượt trội bù đắp cho chi phí này.

Bảng 1: So sánh các Lược đồ Chữ ký Tập thể

Tính năng	Harn (Harn1999)	Gentry (Gentry2006)	Đề xuất
Giả định an toàn	DLP	CDH	CDH
Nền tảng	PKI	IBC	IBC
Kích thước chữ ký	$O(n)$	$O(1)$	$O(1)$
Kháng Rogue-Key	Không	Tự nhiên	Tự nhiên
Mô hình linh hoạt	Không (1-1)	Không (n-1)	Có (nhiều-nhiều)

V. Kết luận

Bài báo này đã trình bày một giải pháp cho vấn đề thiếu linh hoạt của các phương pháp chữ ký tập thể trước đây thông qua việc đề xuất một mô hình có cấu trúc tổng quát cùng một lược đồ hiện thực hóa nó. Bằng cách dựa trên nền tảng mật mã định danh, lược đồ không chỉ đáp ứng được các kịch bản ký kết phức tạp mà còn được chứng minh là an toàn và hiệu quả. Các hướng phát triển trong tương lai có thể bao gồm việc mở rộng tính năng (ví dụ như tích hợp chữ ký mù, chữ ký ngưỡng), thực hiện chứng minh an toàn trong mô hình chuẩn, và nghiên cứu các phiên bản kháng tấn công lượng tử dựa trên những bài toán khó như bài toán trên lưới.

Tài liệu tham khảo:

[1]. Barreto, P. S. L. M., & Naehrig, M. (2006). Pairing-friendly elliptic curves

of prime order. In B. Preneel & S. Tavares (Eds.), *Selected Areas in Cryptography* (pp. 319–331). Springer.

[2]. Bellare, M., & Neven, G. (2006). Multi-signatures in the plain public-key model and a general forking lemma. In *Proceedings of the 13th ACM Conference on Computer and Communications Security* (pp. 390-399). ACM.

[3]. Boldyreva, A. (2003). Efficient threshold signature, multisignature and blind signature schemes based on the Gap-Diffie-Hellman-group. In Y. Desmedt (Ed.), *Public Key Cryptography - PKC 2003* (pp. 31-46). Springer.

[4]. Boneh, D., & Franklin, M. (2001). Identity-based encryption from the Weil pairing. In J. Kilian (Ed.), *Advances in Cryptology - CRYPTO 2001* (pp. 213-229). Springer.

[5]. Cha, J. C., & Cheon, J. H. (2003). An identity-based signature from gap Diffie-Hellman groups. In Y. Desmedt (Ed.), *Public Key Cryptography - PKC 2003* (pp. 18-30). Springer.

[6]. Creaby, M. W., & Cole, M. H. (2012). Gait stability in Parkinson's disease: a systematic review. *Neuroscience & Biobehavioral Reviews, 36*(6), 1444–1450.

[7]. Gentry, C., & Ramzan, Z. (2006). Identity-based aggregate signatures. In M. Yung, Y. Dodis, A. Kiayias, & T. Malkin (Eds.), *Public Key Cryptography - PKC 2006* (pp. 257-273). Springer.

[8]. Harn, L. (1999). Digital multisignature with distinguished signing authorities. *Electronics Letters, 35*(4), 294-295.

[9]. Jinila, B., & Komathy, K. (2015). Cluster oriented id based multi signature scheme for traffic congestion warning in vehicular ad hoc networks. In *Proceedings of the International Conference on Emerging ICT for Bridging the Future*, volume 2, (pp. 337- 345). Springer.

[10]. Li, Z., Hui, L., Chow, K., Chong, C., Tsang, W., & Chan, H. (2000). Cryptanalysis of harn digital multisignature scheme with distinguished signing authorities. *Electronics Letters, 36*(4), 294-295.

[11]. Micali, S., Ohta, K., & Reyzin, L. (2001). Accountable-subgroup multisignatures. In *Proceedings of the 8th ACM Conference on Computer and Communications Security* (pp. 245-254). ACM.

[12]. Pérez-López, C., et al. (2016). Freezing of gait in Parkinson's disease: a review of the state of the art. *Revista de Neurologia, 63*(11), 509-517.

[13]. Pointcheval, D., & Stern, J. (2000). Security arguments for digital signatures and blind signatures. *Journal of Cryptology, 13*(3), 361-396.

[14]. Shamir, A. (1985). Identity-based cryptosystems and signature schemes. In G. R. Blakley & D. Chaum (Eds.), *Advances in Cryptology - CRYPTO '84* (pp. 47-53). Springer.

[15]. Walton, C. C., et al. (2015). The major impact of freezing of gait on quality of life in Parkinson's disease. *Journal of Neurology, 262*(1), 108–114.

A GENERAL-STRUCTURED COLLECTIVE SIGNATURE SCHEME BASED ON IDENTITY-BASED CRYPTOGRAPHY

Vu Tat Diep[2]

Abstract: *In modern business environments, complex processes often require the involvement of multiple parties with distinct roles and responsibilities, which makes traditional collective signature schemes lack flexibility. This paper proposes a general-structured collective signature model that supports a many-to-many signing relationship between a group of signers and the components of a document. To instantiate this model, we construct a concrete scheme based on identity-based cryptography (IBC) and bilinear pairings. The use of IBC not only eliminates the burden of certificate management and distribution inherent in public key infrastructure (PKI) but also provides natural resistance to rogue-key attacks. A formal security proof is given in the random oracle model, showing that the scheme achieves existential unforgeability against adaptive chosen-message and chosen-identity attacks (EUF-CMA-ID), under the assumption of the hardness of the Computational Diffie–Hellman Problem (CDHP). Performance analysis indicates that the proposed scheme achieves competitive computational cost and signature size while offering enhanced flexibility, making it well-suited for practical applications such as electronic contracts, financial approval workflows, and supply chain management.*

Keywords: *collective signature, multi-signature, identity-based cryptography, bilinear pairing, provable security*

[2] Faculty of Electrical and Electronics Engineering, Hanoi Open University