LƯỢC ĐỒ BẦU CỬ ĐIỆN TỬ KHÔNG TRUY VẾT DỰA TRÊN LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ MÙ

Nguyễn Tấn Đức, Ngô Đức Thiện[*], Nguyễn Hiếu Minh[+]
[*] Học viện Công nghệ Bưu chính Viễn thông
[+]Học viện kỹ thuật mật mã

Tóm tắt: Hiện nay, nhiều quốc gia trên thế giới đang có xu hướng triển khai hệ thống bầu cử điện tử, vì nó có một số lợi thế nổi bật so với cách bầu cử truyền thống, bao gồm bảo mật khi bỏ phiếu, tính chính xác của việc kiểm tra và phân tích phiếu bầu. Bài báo này đề xuất một lược đồ bầu cử điện tử (E-Voting) ẩn danh dựa trên lược đồ chữ ký số tập thể mù trên cơ sở bài toán DLP và ECDLP. Lược đồ đề xuất đảm bảo được các tính chất cơ bản của một lược đồ bầu cử điện tử như tính riêng tư của cử tri, không lộ thông tin bầu cử, chống cưỡng chế, chính xác, công bằng, khả năng kiểm chứng, dân chủ và tính an toàn của hệ thống.

Từ khóa: chữ ký số tập thể mù, lược đồ bầu cử điện tử, cử tri, phiếu bầu, bài toán khó.

I. MỞ ĐẦU

Bầu cử điện tử là một lĩnh vực nghiên cứu sinh động trong vài thập kỷ qua, các nhà nghiên cứu mong muốn thiết kế và sử dụng các hệ mật mã để khắc phục những hạn chế của các hệ thống bỏ phiếu dựa trên giấy truyền thống như bảo mật khi bỏ phiếu, tính chính xác của việc kiểm tra và phân tích phiếu bầu, tính xác minh, phát hiện lỗi và chi phí cao. Các hệ thống bầu cử điện tử có khả năng cung cấp một nền tảng là niềm tin, thân thiện với môi trường, kinh tế và ít xảy ra lỗi khi bỏ phiếu.

Hiện nay, trong khi xã hội hiện đại hoàn toàn dựa vào CNTT cho các hoạt động của Chính phủ, kinh doanh, công việc và giải trí…, thì việc sử dụng CNTT để ra quyết định dân chủ vẫn còn ở giai đoạn nghiên cứu và hoàn thiện. Đã có một số nước sử dụng bầu cử điện tử để người dân thực hiện quyền dân chủ của mình, tuy nhiên thách thức chính trong các hệ thống bầu cử điện tử hiện có là vấn đề bảo đảm tính bảo mật và tính ẩn danh cho cử tri. Cho đến nay, nhiều giải pháp thiết kế hệ thống bầu cử điện tử đã được đề xuất. Tuy nhiên, không có một giải pháp nào hoàn chỉnh trong cả lý thuyết và thực tiễn. Vì vậy, các nhà nghiên cứu cố gắng dựa trên các hệ mật cơ bản để xây dựng các chương trình bầu cử điện tử với hiệu quả cao để đáp ứng các yêu cầu đó. Trong đó, việc ứng dụng chữ ký số mù vào hệ thống bầu cử điện tử đang là một hướng nghiên cứu được các nhà nghiên cứu quan tâm vì nó bảo đảm được tính ẩn danh của cử tri khi đi bầu giống như bỏ phiếu truyền thống, vì không một cử tri nào muốn việc mình bỏ phiếu cho ai bị người khác biết được.

Một lược đồ bầu cử điện tử an toàn phải đảm bảo đáp ứng các tính chất như riêng tư, không lộ thông tin bầu cử, chống cưỡng chế, chính xác, công bằng, khả năng kiểm chứng, dân chủ và tính mạnh mẽ của hệ thống [1]. Tuy nhiên, đạt được tất cả các yêu cầu trên là một thách thức lớn. Bài báo này đề xuất một lược đồ bầu cử điện tử mới sử dụng 2 chữ ký của cơ quan có thẩm quyền bầu cử. Một chữ ký trên phiếu bầu đã được cử tri làm mù được tạo ra bởi nhiều thành viên của cơ quan có thẩm quyền để đảm bảo tính chính xác của việc xây dựng phiếu bầu. Ngoài ra, còn có một chữ ký khác trên mỗi cử tri như là ký trên token chứa thông tin cá nhân đã được làm mù cho phép cử tri thực hiện bầu cử trong các giai đoạn bầu cử ẩn danh. Đồng thời, để cho phép một cử tri đăng ký được ẩn danh, sử dụng lược đồ thông qua chứng chỉ dựa trên thông tin ẩn danh được đề xuất trong [2].

Phần còn lại của bài báo được tổ chức như sau. Phần 2 trình bày tổng quan việc nghiên cứu về hệ thống bầu cử điện tử. Phần 3 trình bày về các lược đồ chữ ký số được sử dụng để xây dựng lược đồ bầu cử điện tử. Phần 4 trình bày về thiết kế hệ thống. Phần 5 trình bày về đánh giá và phân tích lược đồ đề xuất và phần cuối cùng là kết luận.

II. CÁC NGHIÊN CỨU LIÊN QUAN

Bầu cử điện tử đã thu hút nhiều sự quan tâm gần đây và có nhiều lược đồ đã được đề xuất. Các lược đồ có thể được chia thành ba cách tiếp cận chính là (i) dựa trên các lược đồ chữ ký mù [3], [4], (ii) các lược đồ dựa trên mã hóa đồng cấu [5], [6], [7] và (iii) các lược đồ dựa trên mạng hỗn hợp [8], [9], [10]. Đồng thời cũng có một số lược đồ dựa trên cơ sở lai ghép giữa mã hóa đồng cấu và mạng hỗn hợp [11], [12]. Ngoài ra cũng có một số công bố gần đây như đề xuất các yêu cầu, thiết kế và thực hiện khi thiết kế hệ thống bầu cử điện tử [13], đề xuất chữ ký số mù an toàn ứng dụng cho bầu cử điện tử [14], hệ thống bầu cử điện tử dựa trên nền tảng android [15], hệ thống bầu cử điện tử sử dụng cho điện thoại di động android [16], ứng dụng bầu cử điện tử cải tiến sử dụng hạ tầng android [17], cơ chế kiểm tra bầu cử sử dụng mã hóa mới cho hệ thống bầu cử điện tử trên cơ sở cam kết bit và chữ ký số mù [18], sử dụng chữ ký số mù dựa trên định danh sử dụng cho hệ thống bầu cử điện tử [19] và lược đồ bầu cử điện tử không truy vết dựa trên cặp chữ ký số [20].

Trong các loại tiếp cận trên thì các lược đồ bầu cử dựa trên chữ ký số mù được cho là đơn giản, hiệu quả và phù

Tác giả liên hệ: Nguyễn Tấn Đức
Email: tanducslc@gmail.com
Đến tòa soạn: 11/2019, chỉnh sửa: 12/2019, chấp nhận đăng: 12/2019.

hợp cho các cuộc bầu cử quy mô lớn. Ngoài ra, vì mọi phiếu bầu đều được làm mù và giải mù chỉ bởi cử tri tương ứng nên có thể được xác minh một cách công khai, rộng rãi [21], [22]. Lược đồ bầu cử đề xuất trong [4] dựa trên chữ ký số mù của Chaum, trong đó, khi bỏ phiếu, cử tri đã đăng ký sẽ gửi phiếu bầu ẩn danh, sau đó danh sách các lá phiếu nhận được sẽ được công bố cho tất cả các cử tri. Cuối cùng, để giải mã phiếu bầu, mỗi cử tri cần phải tương tác với cơ quan kiểm phiếu bằng cách gửi khóa riêng của mình. Hạn chế của lược đồ này là cơ quan đăng ký có thể phát hiện những cử tri đã đăng ký bỏ phiếu và có thể thêm phiếu bầu vào danh sách phiếu bầu đã được bỏ phiếu. Lược đồ được đề xuất trong [23] sử dụng lược đồ chữ ký số mù ngưỡng để có được phiếu bầu, nó cũng sử dụng hệ thống mật mã ngưỡng để đảm bảo sự công bằng cho các ứng cử viên. Mặc dù nó đáp ứng tính thực tế, khả năng mở rộng và mạnh mẽ, nhưng để nó đáp ứng sự công bằng và chính xác thì cần có điều kiện. Một lược đồ khác [24] triển khai giải pháp nhận diện cử tri giả, phát triển trên cơ sở lược đồ chữ ký số mù của Chaum để đảm bảo sự ẩn danh của cử tri, tuy nhiên do việc tạo phiếu bầu, tạo khóa và kiểm phiếu cùng làm việc chung với nhau nên có thể dẫn đến gian lận như sửa đổi phiếu bầu.

Lược đồ bầu cử của chúng tôi đề xuất cũng dựa trên lược đồ chữ ký số mù nhưng sử dụng lược đồ chữ ký số tập thể mù và các lược đồ này đã được chứng minh là mù vô điều kiện. Ngoài ra, do có nhiều cơ quan có thẩm quyền độc lập và mỗi cơ quan gồm nhiều người tham gia trong lược đồ bầu cử nên lược đồ bầu cử hoàn toàn tin cậy, trừ khi tất cả các thành viên trong mỗi cơ quan và tất cả các cơ quan liên kết với nhau để phá hoại cuộc bầu cử.

III. CÁC LƯỢC ĐỒ CHỮ KÝ SỐ SỬ DỤNG TRONG LƯỢC ĐỒ BẦU CỬ ĐỀ XUẤT

Phần này trình bày sơ lược về các lược đồ chữ ký số được sử dụng trong lược đồ bầu cử điện tử đề xuất. Đó là lược đồ chữ ký số tập thể mù dựa trên lược đồ Schnorr [25] và dựa trên lược đồ EC-Schnorr [26]. Việc sử dụng lược đồ Schnorr dựa trên bài toán DLP trong việc xác thực cử tri sẽ dễ thực hiện hơn sử dụng các lược đồ dựa trên bài toán ECDLP trong khi vẫn đảm bảo được độ an toàn cần thiết. Lược đồ đề xuất trong phần này dựa trên mô hình được trình bày trong [20], tuy nhiên khác biệt ở đây là [20] sử dụng lược đồ chữ ký số mù đơn của Chaum [4] cho việc ký lên token đã được làm mù và lược đồ chữ ký số mù của Hwang [27] để xây dựng phiếu bầu. Trong khi bài báo này sử dụng lược đồ chữ ký số tập thể mù dựa trên EC-Schnorr [26] để xây dựng phiếu bầu và lược đồ chữ ký số tập thể mù dựa trên Schnorr [25] để ký mù trên token xác minh thông tin cử tri.

A. Lược đồ chữ ký số tập thể mù dựa trên Schnorr

Lược đồ chữ ký số tập thể mù trong [25] có 5 pha được mô tả như sau:

Pha tạo khóa: Người ký (*ở đây là Ban kiểm phiếu* - BKP), chọn tham số hệ thống là (*p, q, g*), trong đó *p*, *q* là hai số nguyên tố, *g* là phần tử sinh bậc *q*, và khoá bí mật $1 < d < q$.

Mỗi thành viên của BKP là BKP_i tính khoá công khai ρ_i của mình và gửi cho bên thứ ba tin cậy (*ở đây là ban điều hành bầu cử* - BĐH) để tính khoá công khai của tập thể BKP là ρ , với:

$$\rho_i = g^{d_i} \bmod p, i = 1,2,...,m \quad \rho = \prod_{i=1}^{n} \rho_i \bmod p$$

Mỗi BKP_i chọn một số ngẫu nhiên $k_i \in Z_q^*$, tính c_i và gửi tới BĐH để tính $\overline{c}$, $\overline{c}$ được gửi tới cử tri, với:

$$c_i = g^{k_i} \bmod p, i = 1,2,...,m$$

$$\overline{c} = \prod_{i=1}^{m} c_i \bmod p = g^{\sum_{i=1}^{m} k_i \bmod q} \bmod p$$

Khoá công khai là $(\rho, g, \overline{c})$ và khoá bí mật là (*d*). BKP giữ bí mật (*p,q,d*) và công khai $(\rho, g, \overline{c})$.

Pha làm mù: Cử tri V_j có một thông điệp (*ở đây là token* T_j), và V_j muốn BKP ký lên token T_j của mình. V_j làm mù T_j bằng cách chọn hai số ngẫu nhiên $\alpha, \beta \in \{1,2,...,q-1\}$ và tính:

$$\begin{cases} c = \overline{c} g^{\alpha} \rho^{\beta} \bmod p; h = H(T_j \| c) \\ r = h \bmod q; \overline{r} = (r - \beta) \bmod q \end{cases}$$

V_j gửi $\overline{r}$ cho BKP, $\overline{r}$ là token của V_j đã được làm mù.

Pha ký số : Khi nhận $\overline{r}$ từ V_j, mỗi BKP_i sử dụng các tham số riêng của mình là (k_i, d_i) để tính s_i : $s_i = k_i - d_i \overline{r} \bmod q$, và gửi tới BĐH để tính chữ ký số tập thể $\overline{s} = \sum_{i=1}^{m} s_i \bmod q$ và gửi $\overline{s}$ tới V_j.

Pha giải mù: Khi nhận $\overline{s}$ từ BĐH, V_j giải mù bằng cách tính $s = (\overline{s} + \alpha) \bmod q$. Cặp số (*r,s*) là chữ ký trên token của cử tri V_j.

Pha kiểm tra: Cặp (*r,s*) là chữ ký trên token T_j. Để thể kiểm tra tính hợp lệ của chữ ký, tính c' và r' và so sánh, nếu $r' = r$ thì chữ ký được chấp nhận, với: $c' = g^s \rho^r \bmod p$; $r' = H(T_j \| c') \bmod q$

B. Lược đồ chữ ký số tập thể mù dựa trên ECSchnorr

Lược đồ chữ ký số tập thể mù đề xuất trong [26] sử dụng đường cong elliptic có dạng như sau: $y^2 = x^3 + ax + b \bmod p$; p là số nguyên tố lớn tạo trường *GF*(*p*) của đường cong elliptic; q là số nguyên tố chỉ số lượng nhóm điểm của đường cong elliptic; P là điểm của đường cong có bậc *q;* G là điểm khác gốc O của đường cong elliptic và có toạ độ là (x_G, y_G) ; $H(M)$ là giá trị của hàm băm; d' là khoá riêng của người ký và $1 < d' < q$. Lược đồ này gồm 5 pha và được mô tả như sau:

Pha tạo khóa: BKP thực hiện như sau: Mỗi thành viên BKP_i (*trong mô hình này xem như có m thành viên*) tính giá trị khóa công khai $P_i = d'_i \times G$ của mình và gửi đến BĐH để tính khóa công khai tập thể là P: $P = P_1 + P_2 + ... + P_m = \sum_{i=1}^{m} d'_i \times G$ với *i=1,2...m*

Mỗi BKP_i chọn ngẫu nhiên $k_i \in Z_q$ và tính $C_i = k_i \times G$, sau đó gửi đến BĐH để tính $\overline{C}$ chung:

$\overline{C} = \sum_{i=1}^{m} C_i = \sum_{i=1}^{m} k_i \times G$. Khóa công khai của BKP là $(P, G, \overline{C})$ và khóa bí mật là (d').

Pha làm mù: Cử tri V_j có thông điệp (*ở đây là phiếu bầu* v_j) và muốn có chữ ký của BKP. V_j chọn ngẫu nhiên 2 số $\alpha, \beta \in \{1,2,...,q-1\}$, tính $C = \overline{C} + \alpha \times G + \beta \times P$; $r = H(v_j, x_C) \bmod q; \overline{r} = (r - \beta) \bmod q$ và gửi $\overline{r}$ cho BKP.

Pha ký số: Sau khi nhận $\overline{r}$ từ V_j, BKP thực hiện ký như sau: Mỗi BKP_i sử dụng (d_i, k_i) của mình để tính $s_i = k_i - d_i \overline{r} \bmod q$, và gửi đến BĐH để tính $\overline{s} = \sum_{i=1}^{m} s_i \bmod q$, và gửi cho V_j.

Pha giải mù: Sau khi nhận $\overline{s}$ từ BĐH, V_j tính $s = (\overline{s} + \alpha) \bmod q$, cặp (r,s) là chữ ký số trên phiếu bầu v_j. Sau đó V_j chuyển (v_j, r, s) cho BKP.

Pha kiểm tra: Kết quả cặp (r,s) là chữ ký trên phiếu bầu v_j. Để kiểm tra tính hợp lệ của chữ ký, tính $C' = s \times G + r \times P$ và $r' = H(v_j, x_{C'})$. Nếu $r' = r$ thì chữ ký là đúng.

C. Chữ ký số trên Token được làm mù

+ Cử tri có thể bầu cử mà không tiết lộ danh tính của mình khi chứng minh tính hợp lệ (*đủ điều kiện bỏ phiếu*) bằng cách sử dụng token. Để chứng minh tính hợp lệ bằng cách ẩn danh, cử tri V_j làm mù token T_j của mình bằng cách chọn hai số ngẫu nhiên $\alpha_j, \beta_j \in \{1,2,...,q-1\}$ và sử dụng các tham số công khai của tập thể BKP là $(\rho, g, \overline{c})$ để tính:

$$\begin{cases} c_j = \overline{c} g^{\alpha_j} \rho^{\beta_j} \bmod p; h_j = H(T_j \| c_j) \\ r_j = h_j \bmod q; \overline{r}_j = (r_j - \beta_j) \bmod q \end{cases}$$

Việc xác nhận định danh của V_j bởi thông tin xác thực dựa trên thông tin ẩn danh $T_j(A, ID_j, Z_j)$ của V_j.

+ Các BKP_i sẽ ký trên token đã được làm mù là $\delta_j(\alpha_j, \beta_j, T_j) = \overline{r}_j$ bằng cách sử dụng các tham số riêng của mình là (k_i, d_i) và tính $s_i = k_i - d_i \overline{r}_j \bmod q$, và gửi tới BĐH để tính chữ ký số tập thể $\overline{s}_j = \sum_{i=1}^{m} s_i \bmod q$.

V_j giải mù token đã được BKP ký bằng cách tính: $s_j = (\overline{s}_j + \alpha_j) \bmod q$. Cặp số (r_j, s_j) là chữ ký trên token mù của V_j.

Gọi $s_1(T_j) = r_j$ là thành phần thứ nhất và $s_2(T_j) = s_j$ là thành phần thứ hai của chữ ký của BKP trên token T_j. Do các thành viên BKP_i đã ký mà không biết T_j nên không ai ngoài V_j biết được (s_j, r_j) là từ V_j.

D. Chữ ký số trên phiếu bầu được làm mù

+ Trong pha gửi phiếu bầu, cử tri V_j sử dụng các hệ số làm mù của mình là (α'_j, β'_j) và khóa công khai của tập thể BKP là $(P, G, \overline{C})$ để làm mù phiếu bầu v_j của mình bằng cách tính:

$C_j = \overline{C} + \alpha'_j \times G + \beta'_j \times P$; $r'_j = H(v_j, x_{C_j}) \bmod q$; $\overline{r}'_j = (r'_j - \beta'_j) \bmod q$.

+ BKP_i ký lên $\gamma_j(\alpha'_j, \beta'_j, v_j) = \overline{r}'_j$ bằng cách sử dụng (d'_i, k'_i) để tính chữ ký là $s'_i = k'_i - d'_i \overline{r}'_j \bmod q$, sau đó gửi BĐH để tính chữ ký chung của BKP là: $\overline{s}'_j = \sum_{i=1}^{m} s'_i \bmod q$.

+ V_j giải mù phiếu bầu bằng cách tính $s'_j = (\overline{s}'_j + \alpha'_j) \bmod q$, cặp (s'_j, r'_j) là chữ ký số trên phiếu bầu v_j của cử tri V_j.

E. Xác thực thông tin dựa trên thông tin ẩn danh

Chứng chỉ dựa trên thông tin ẩn danh $T_j(A, ID_j, Z_j)$ được đề xuất trong [2] do cơ quan phát hành chứng chỉ (CQPHCC) cung cấp cho phép cử tri V_j chứng minh mình đủ điều kiện bỏ phiếu với bất kỳ cơ quan nào. Đầu tiên V_j cung cấp số định danh của mình cho CQPHCC, sau đó CQPHCC cung cấp thông tin xác thực $T_j(A, ID_j, Z_j)$ nếu cử tri V_j đủ điều kiện bỏ phiếu. Sau này, bất kỳ cơ quan có thẩm quyền nào đều có thể buộc V_j tính toán $U_j^{Z_j} \bmod n$ từ một số nguyên U_j sử dụng Z_j trong $T_j(A, ID_j, Z_j)$ mà không cần biết Z_j của V_j. Sau này, bất kỳ cơ quan có thẩm quyền nào đều có thể sử dụng con dấu $U_j^{Z_j} \bmod n$ để xác thực V_j chính là cử tri tương ứng với $T_j(A, ID_j, Z_j)$.

IV. XÂY DỰNG LƯỢC ĐỒ BẦU CỬ ĐIỆN TỬ

A. Cấu hình của lược đồ đề xuất

Lược đồ bầu cử điện tử đề xuất gồm các thông số chính như sau:

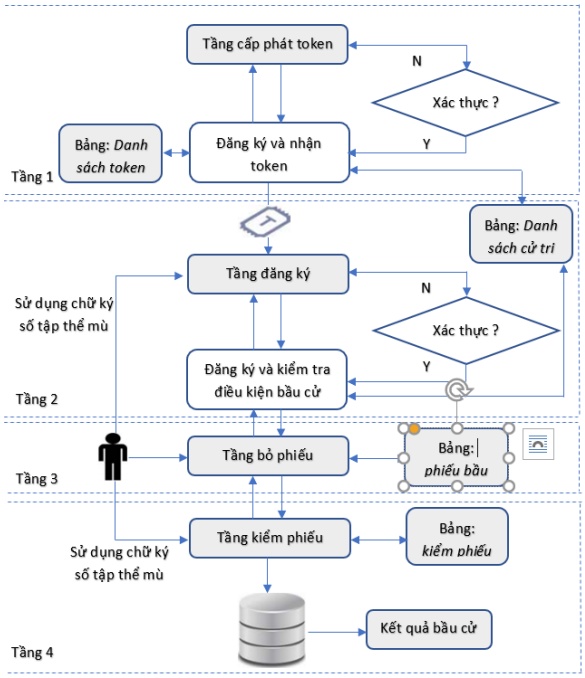
+ Gọi N là số cử tri được quyền đi bầu, cử tri thứ j được ký hiệu là $V_j (j = 1,...,N)$

+ Ban điều hành bỏ phiếu: gồm một hoặc nhiều người, ký hiệu là BĐH

+ Ban kiểm phiếu: gồm m người, ký hiệu là $BKP_i (i = 1,...,m)$, $m \geq 2$, ký hiệu là BKP

+ Cơ quan phát hành chứng chỉ xác thực thông tin: Ký hiệu là CQPHCC

+ Bốn bảng dữ liệu chính của hệ thống là: *danhsachcutri* (danh dách cử tri), *danhsachtoken* (danh sách token chứa thông tin xác thực cử tri), *bangphieubau* (chứa thông tin phiếu bầu) và *bangkiemphieu* (chứa thông tin phiếu bầu được giải mù). Lược đồ này xem như các dữ liệu chứa thông tin công dân đã có và được cơ quan có thẩm quyền quản lý và được truy vấn trong phần cấp quyền bầu cử.



Hình 1. Kiến trúc tổng quan của lược đồ bầu cử điện tử đề xuất

Hoạt động của các bên tham gia chính trong lược đồ được mô tả như sau:

Cử tri (V_j): Mỗi cử tri V_j có mã định danh ID_j để chứng minh tính hợp lệ của mình với cơ quan phát hành chứng chỉ CQPHCC và nhận thông tin ẩn danh $T_j(A, ID_j, Z_j)$ từ CQPHCC.

+ V_j sử dụng thông tin $U_j^{Z_j}$ để chứng minh việc mình nhận được token T_j chưa được sử dụng bỏ phiếu và sử dụng hệ số làm mù α_j, β_j để làm mù token T_j thành $\delta_j(\alpha_j, \beta_j, T_j)$

+ V_j cũng sử dụng các tham số (α'_j, β'_j) để làm mù và giải mù phiếu bầu v_j của mình thành $\gamma_j(\alpha'_j, \beta'_j, v_j)$.

Ban điều hành bỏ phiếu (BĐH): BĐH kiểm tra tính hợp lệ ẩn danh V_j sử dụng $T_j(A, ID_j, Z_j)$, chuyển $U_j^{Z_j}$ của cử tri vào bảng *danhsachtoken*, chuyển phiếu bầu đã được làm mù vào *bangphieubau* và chuyển dữ liệu về cử tri, token và phiếu bầu làm mù vào các bảng *danhsachcutri* và *bangkiemphieu*. BĐH cũng ký trên các T_j trước khi chuyển vào bảng *danhsachtoken*.

Ban kiểm phiếu (BKP): Có $m \geq 2$ người trong BKP. Mỗi thành viên BKP_i có trách nhiệm ký trên token được làm mù của cử tri và gửi cho BĐH tính chữ ký chung là $t_j(\alpha_j, \beta_j, T_j)$ và phiếu bầu đã được làm mù là $t_j(\alpha'_j, \beta'_j, v_j)$ bằng cách:

+ Mỗi BKP_i sử dụng khóa (k_i, d_i) để ký token mù $\delta_j(\alpha_j, \beta_j, T_j)$ và gửi cho BĐH để tính chữ ký chung là $t_j(\alpha_j, \beta_j, T_j)$.

+ Mỗi BKP_i sử dụng khóa (d'_i, k'_i) để ký phiếu bầu được làm mù là $\gamma_j(\alpha'_j, \beta'_j, v_j)$ và gửi BĐH tính chữ ký chung là $t_j(\alpha'_j, \beta'_j, v_j)$.

Cơ quan phát hành chứng chỉ xác thực (CQPHCC): CQPHCC có nhiệm vụ tạo và phát hành chứng chỉ xác thực dựa trên thông tin ẩn danh $T_j(A, ID_j, Z_j)$ cho V_j (*với A là thông tin của cơ quan phát hành chứng chỉ A*).

Bảng danh sách cử tri (*danhsachcutri*): Gồm 3 phần là "*ID*", "*thongtinxacthuc*" và "*token-mu*"

+ Trường "*ID*": ID_j là thông tin mã định danh của cử tri hợp lệ V_j;

+ Trường "*thongtinxacthuc*": chứa thông tin về chứng chỉ xác thực $T_j(A, ID_j, Z_j)$ của cử tri hợp lệ V_j;

+ Trường "*token-mu*": chứa giá trị token đã được làm mù là $\delta_j(\alpha_j, \beta_j, T_j)$.

Bảng 1. Bảng danh sách cử tri (danhsachcutri)

ID	*thongtinxacthuc*	*token-mu*
ID_1	$T_1(A, ID_1, Z_1)$	$\delta_1(\alpha_1, \beta_1, T_1)$
…	…	…
ID_j	$T_j(A, ID_j, Z_j)$	$\delta_j(\alpha_j, \beta_j, T_j)$
…	…	…
ID_N	$T_N(A, ID_N, Z_N)$	$\delta_N(\alpha_N, \beta_N, T_N)$

Bảng chứa thông tin token (*danhsachtoken*): gồm thông tin token, con dấu $U_j^{Z_j}$ như là quyền ẩn danh của V_j đã có T_j

+ Trường *"token"*: Chứa thông tin là một số duy nhất mà BĐH đã chuẩn bị trước để cấp cho cử tri.

+ Trường "*token-ttad*": Chứa thông tin ẩn danh của V_j. Khi V_j chọn T_j, BĐH chuyển thông tin $U_j^{Z_j}$ vào phần "*token-ttad* "

Bảng 2. 1Bảng danh sách token (danhsachtoken)

token	*token-ttad*
T_1	$U_1^{Z_1}$
…	…
T_j	$U_j^{Z_j}$
…	…
T_N	$U_N^{Z_N}$

Bảng thông tin về phiếu bầu (*bangphieubau*): Chứa thông tin phiếu bầu đã được làm mù và phần xác nhận phiếu bầu đó.

+ Trường "*phieubau-mu*": Chứa thông tin phiếu bầu đã được ký mù của cử tri thứ *j* tương ứng với T_j. Do đó mà ở phần bỏ phiếu, chữ ký của BKP trên phiếu bầu làm mù là $t_j(\alpha'_j, \beta'_j, v_j)$

+ Trường "*xacthuc*": Chứa phần thứ nhất của chữ ký trên T_j là $s_1(T_j)$ như là phần xác thực phiếu bầu

Bảng 3. Bảng danh sách phiếu bầu đã làm mù (bangphieubau)

phieubau-mu	*xacthuc*
$t_1(\alpha'_1, \beta'_1, v_1)$	$s_1(T_1) = r_1$
…	…
$t_j(\alpha'_j, \beta'_j, v_j)$	$s_1(T_j) = r_j$
…	…
$t_N(\alpha'_N, \beta'_N, v_N)$	$s_1(T_N) = r_N$

Bảng kiểm phiếu (*bangkiemphieu*): bảng này chứa phần phiếu bầu đã giải mù và phần xác thực.

+ Trường "*phieubau-giaimu*": Chứa thông tin phiếu bầu đã được giải mù bởi chính cử tri đó là: $s_j(\alpha'_j, \beta'_j, v_j)$

+ Trường "*xacthuc*": Chứa phần thứ hai của chữ ký trên T_j là $s_2(T_j)$, xem như là phần xác nhận của cử tri về tính chính xác của chữ ký BKP trên phiếu bầu đã được làm mù của mình.

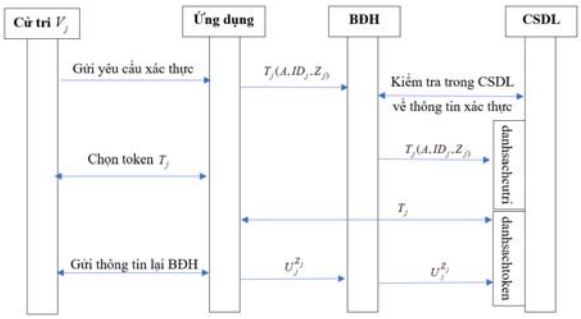
Bảng 4. Bảng danh sách phiếu bầu đã được giải mù (bangkiemphieu)

phieubau-giaimu	*xacthuc*
$s_1(\alpha'_1, \beta'_1, v_1)$	$s_2(T_1) = s_1$
…	…
$s_j(\alpha'_j, \beta'_j, v_j)$	$s_2(T_j) = s_j$
…	…
$s_N(\alpha'_N, \beta'_N, v_N)$	$s_2(T_N) = s_N$

B. Các tầng hoạt động của lược đồ đề xuất

Lược đồ đề xuất bao gồm 4 tầng được trình bày như sau:

1) Tầng cấp phát token



Hình 2. 1Sơ đồ luồng dữ liệu của tầng cấp phát token

Trong tầng này, mỗi cử tri V_j nhận được token T_j là duy nhất trong hệ thống trong khi vẫn duy trì tính ẩn danh của mình. Để đảm bảo tính ẩn danh cho cử tri, ít nhất N token được tạo trước (N *là số cử tri đủ điều kiện bỏ phiếu*) và được đặt vào bảng *danhsachtoken* để cử tri chọn token cho mình. Mỗi T_j trong bảng *danhsachtoken* đều có chữ ký của BĐH (chữ ký này khác với chữ ký của BKP là $\{s_1(T_j), s_2(T_j)\}$ để đảm bảo T_j đã được chọn từ bảng *danhsachtoken*). Trong tầng này, V_j và BĐH tương tác nhau như sau:

+ BĐH xác thực ẩn danh về tính hợp lệ của cử tri V_j bằng thông tin ẩn danh [2].

+ Sau khi xác thực, BĐH chuyển $T_j(A, ID_j, Z_j)$ vào bảng *danhsachcutri* .

+ Cử tri V_j đã được xác thực sẽ chọn token T_j chưa sử dụng trong bảng *danhsachtoken* (*token* T_j *đã có chữ ký của* BĐH *và chữ ký này không thể hiện trong lược đồ đề xuất*), và chuyển $U_j^{Z_j}$ của mình cho BĐH.

+ Vì T_j đã được V_j chọn nên BĐH chuyển tham số $U_j^{Z_j}$ của V_j tương ứng vào bảng *danhsachtoken*.

Các vấn đề bảo mật của tầng này như sau:

+ Mỗi V_j có thể nhận được nhiều token: BĐH đặt tham số $U_j^{Z_j}$ của V_j tương ứng với T_j của cử tri đó trên bảng *danhsachtoken* để đổi lấy thông tin xác thực. Do đó V_j không thể yêu cầu nhiều token.

+ Mỗi V_j có thể không nhận được token: Vì có ít nhất N token được tạo nên mọi cử tri đều có thể nhận được token. Nếu bất kỳ V_j nào không thể nhận được token, cử tri đó có thể yêu cầu nhiều lần.

+ Cử tri có thể sử dụng token do mình tự tạo: Trên T_j có chữ ký của BĐH và BĐH chỉ chấp nhận token có chữ ký của BĐH. Do đó V_j không thể sử dụng T_j của riêng mình tự tạo.

2) Tầng đăng ký:

Trong tầng này, ban kiểm phiếu ký trên T_j được làm mù của cử tri là $\delta_j(\alpha_j, \beta_j, T_j)$. Đầu tiên, V_j làm mù T_j của mình và sau đó các BKP_i ký mù trên T_j như được mô tả trong phần 3.3. Các BKP_i ký vào T_j mà không biết nội dung của nó. T_j đã được làm mù và được ký để chứng minh V_j đủ điều kiện bỏ phiếu và ẩn danh trong các giai đoạn sau. Vì bảng *danhsachcutri* là công khai nên bất kỳ ai cũng có thể kiểm tra một V_j đã đăng ký nhưng không biết nội dung T_j vì T_j trên bảng *danhsachcutri* ở dạng mù. Trong tầng này, V_j và BĐH tương tác như sau:

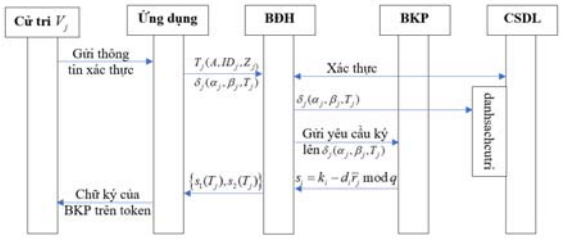
+ V_j làm mù token T_j của mình bằng cách sử dụng các tham số bí mật bằng cách tính $\delta_j(\alpha_j, \beta_j, T_j)$

+ V_j chuyển $T_j(A, ID_j, Z_j)$ và token được làm mù là $\delta_j(\alpha_j, \beta_j, T_j)$ tới BĐH

+ Sau khi xác thực, BĐH chuyển $\delta_j(\alpha_j, \beta_j, T_j)$ vào bảng *danhsachcutri*. BĐH cũng gửi $\delta_j(\alpha_j, \beta_j, T_j)$ tới các BKP_i để yêu cầu ký lên T_j

+ Các BKP_i ký vào $\delta_j(\alpha_j, \beta_j, T_j)$ và gửi cho BĐH tính chữ ký số chung là $\{s_1(T_j), s_2(T_j)\}$ và gửi đến V_j

+ V_j kiểm tra tính hợp lệ của chữ ký trên T_j được làm mù.



Hình 3. Sơ đồ luồng dữ liệu của tầng đăng ký

Các vấn đề bảo mật của tầng này như sau: BĐH có thể đặt chữ ký không hợp lệ trên T_j được làm mù, V_j có thể chứng minh sự không trung thực của BĐH bằng cách chỉ ra $\delta_j(\alpha_j,\beta_j,T_j)$ và token đã được ký là không chính xác.

3) Tầng bỏ phiếu:

Trong tầng bỏ phiếu, cử tri V_j sử dụng thành phần thứ nhất của chữ ký trên token là $\{s_1(T_j)\}=(r_j)$ để xác thực. BĐH kiểm tra tính hợp lệ của V_j bằng cách xác minh chữ ký BKP trên T_j là $\{s_1(T_j)\}$. Sau đó, V_j làm mù phiếu bầu v_j của mình thành $\gamma_j(\alpha'_j,\beta'_j,v_j)$ như được mô tả trong phần 3.4. Sau đó V_j gửi $\gamma_j(\alpha'_j,\beta'_j,v_j)$ đến BĐH để đưa vào bảng *bangphieubau*. Sau đó V_j xác nhận phiếu bầu đó bằng cách gửi $\{s_1(T_j)\}$ tới BĐH để được đưa vào phần xác thực (*xacthuc*) của bảng *bangphieubau*. Do đó, bất kỳ ai cũng có thể kiểm tra một cử tri đã gửi phiếu bầu mà không biết danh tính của cử tri và phiếu bầu thực tế. Cuối cùng, BKP ký vào phiếu bầu được làm mù của V_j và đưa vào bảng *bangphieubau* như được mô tả trong phần 3.4 là $t_j(\alpha'_j,\beta'_j,v_j)$. Trong tầng này, V_j và BĐH tương tác như sau:

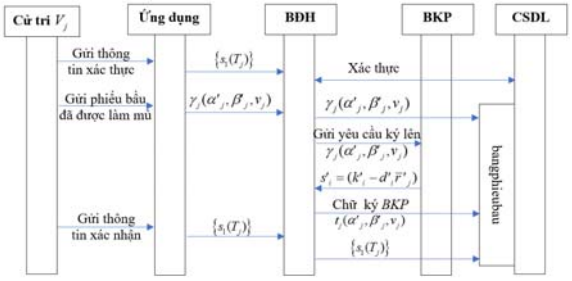
+ V_j gửi $\{s_1(T_j)\}$ cho BĐH. Bằng cách kiểm tra tính hợp lệ của chữ ký trên T_j để đảm bảo T_j không được sử dụng nhiều lần

+ V_j làm mù phiếu bầu của mình bằng cách tính $\gamma_j(\alpha'_j,\beta'_j,v_j)$ như được trình bày trong phần 3.4

+ V_j gửi $\gamma_j(\alpha'_j,\beta'_j,v_j)$ như là lá phiếu bầu được làm mù cho BĐH để đăng lên bảng *bangphieubau* (*tuy nhiên, nó không được hiển thị trên bảng bangphieubau trong bài báo này*).

+ V_j kiểm tra phiếu bầu trên bảng *bangphieubau*, V_j xác nhận bằng cách gửi thành phần thứ nhất của chữ ký trên T_j là $\{s_1(T_j)\}$ để đăng lên phần xác thực (*xacthuc*) trên bảng *bangphieubau*.

+ BKP ký vào phiếu bầu được làm mù $\gamma_j(\alpha'_j,\beta'_j,v_j)$ như được trình bày trong phần 3.4 và BĐH tính chữ ký tập thể là $t_j(\alpha'_j,\beta'_j,v_j)=\bar{s}'_j$ và đăng lên bảng *bangphieubau* .



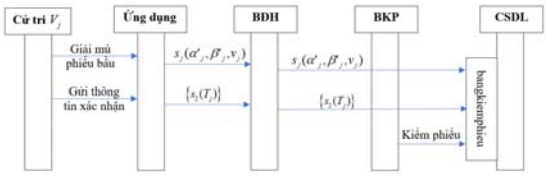
Hình 4. Sơ đồ luồng dữ liệu của tầng bỏ phiếu

Các vấn đề bảo mật của tầng này như sau:

+ BĐH không chuyển phiếu hoặc chuyển phiếu không chính xác vào bảng *bangphieubau*: Vì bảng *danhsachcutri* mở cho mọi người xem nên V_j có thể yêu cầu BĐH bỏ phiếu của mình vào bảng *bangphieubau* bằng cách gửi phiếu trước đây đã được chấp thuận. Nếu BĐH cập nhật không chính xác trên bảng *bangphieubau* thì V_j có thể từ chối việc bỏ phiếu đó.

+ Phiếu bầu trong bảng *bangphieubau* có thể được sửa đổi bởi kẻ tấn công: Vì bảng *bangphieubau* mở công khai cho mọi người nên không ai có thể sửa đổi nội dung của nó một cách bất hợp pháp.

4) Tầng kiểm phiếu:



Hình 5. Sơ đồ luồng dữ liệu của tầng kiểm phiếu

Tất cả các phiếu bầu trên bảng *bangphieubau* đều ở dạng mù. Khi quá trình bỏ phiếu kết thúc, mỗi cử tri cần giải mù phiếu bầu của mình bằng cách tính $s_j(\alpha'_j,\beta'_j,v_j)$ như được mô tả trong phần 3.4. V_j kiểm tra tính chính xác chữ ký của BKP trên phiếu bầu được làm mù của mình bằng cách gửi $s_j(\alpha'_j,\beta'_j,v_j)$ cho BĐH để đưa lên bảng *bangkiemphieu*. Sau đó, V_j xác nhận chúng bằng cách gửi thành phần thứ hai của chữ ký trên T_j là $s_2(T_j)=s_j$ lên phần xác thực (*xacthuc*) của bảng *bangkiemphieu*.

Ở đây, dữ liệu của cử tri V_j trên bảng *bangphieubau* và bảng *bangkiemphieu* có thể giống nhau hoặc không. Nếu giống nhau thì phiếu bầu được ký và được làm mù và giải mù là giống nhau trên bảng *bangphieubau* và bảng *bangkiemphieu* và được xác nhận bởi cùng một T_j. Nếu không giống nhau sẽ không có sự xác nhận nào được đưa vào bảng *bangkiemphieu*, không ai bao gồm BKP có thể biết được mối liên kết giữa chúng vì sử dụng lược đồ chữ ký số tập thể mù. Do đó mà liên kết của phiếu bầu đã ký bị mù trên bảng *bangphieubau*, phiếu bầu được ký và được giải mù trên bảng *bangkiemphieu* và danh tính của V_j đăng ký trên bảng *danhsachcutri* cũng bị xóa đi.

Các bước thực hiện của giai đoạn này như sau:

+ V_j giải mù phiếu bầu thành $s_j(\alpha'_j,\beta'_j,v_j)$ và kiểm tra tính chính xác chữ ký của BKP trên phiếu bầu.

+ V_j gửi $s_j(\alpha'_j, \beta'_j, v_j)$ cho BĐH để đăng lên bảng *bangkiemphieu*.

+ V_j xác nhận việc bỏ phiếu của mình bằng cách gửi thành phần thứ hai của chữ ký trên T_j là $s_2(T_j) = s_j$ cho BĐH đưa lên phần xác thực (*xacthuc*) của bảng *bangkiemphieu*.

Các vấn đề bảo mật của tầng này như sau: BKP có thể thêm hoặc xóa phiếu bầu, nếu làm như thế thì số lượng phiếu bầu trên bảng *bangphieubau* và bảng *bangkiemphieu* sẽ khác nhau mà bất kỳ ai cũng có thể phát hiện được

V. PHÂN TÍCH HIỆU NĂNG

A. Thiết lập thực nghiệm

Trong phần này sẽ tính thời gian thực hiện của các pha trong lược đồ. Thời gian tính toán cho các pha đăng ký, bỏ phiếu và kiểm phiếu là 3 trình độc lập được phát triển, hay tất cả thời gian tính toán không bao gồm thời gian giao tiếp. Ngoài ra, phần này được giả định rằng các yếu tố gây mù, số nguyên bí mật, số nguyên tố,… của các thực thể liên quan được chuẩn bị trước. Đồng thời, hoạt động của các thực thể không liên quan đến mật mã không được xem xét.

Lược đồ được thực hiện trong môi trường bộ xử lý Intel Core i7-4500U @ 1.80GHz với RAM 8 GB chạy trên hệ điều hành Windows 10. Đối với các hoạt động mã hóa, sử dụng khóa 1024 bit cho lược đồ ký token và 192 bit cho lược đồ ký phiếu bầu. Lược đồ chữ ký số mù cũng sử dụng số thành viên ban kiểm phiếu là m=3. Kết quả được tính trung bình của 1000 lần chạy và được chỉ ra như trong bảng 5 bên dưới.

B. Đánh giá hiệu năng của lược đồ đề xuất

Bảng 5 chỉ ra rằng, tổng thời gian cho phần đăng ký, bỏ phiếu và kiểm phiếu của lược đồ đề xuất khoảng: 4.0697+12.1233+11.9533=28.1463 mili giây.

Bảng 5. Chi phí thời gian yêu cầu cho các tầng của lược đồ bầu cử

	Các tầng của lược đồ (mili giây)		
Pha	Đăng ký	Bỏ phiếu	Kiểm phiếu
Làm mù	3.4074	9.9621	-
Tạo chữ ký	0.6619	2.1612	-
Giải mù	0.0004	-	0.0009
Kiểm tra	-	-	11.9524
Tổng	4.0697	12.1233	11.9533

Ví dụ: Nếu có 1,000 phiếu bầu thì có thể được tính trong khoảng 28 giây; Nếu có khoảng một triệu cử tri tham gia bỏ phiếu thì cần (28.1463 *1,000,000 = 28,146,300 mili giây) hay (28,146,300/1000)/60/60 = 7.8 giờ. Như vậy lược đồ đề xuất có độ phức tạp về thời gian là tương đối thấp, đủ khả thi để thực hiện trong thực tế, nhất là với việc triển khai trên các hệ thống CNTT tốc độ cao thì lược đồ bầu cử đề xuất hoàn toàn có thể triển trong thực tế.

C. So sánh, đánh giá:

Lược đồ bầu cử điện tử đề xuất trong [20] sử dụng các lược đồ chữ ký số mù đơn trong hệ thống có nhiều người ký (là các thành viên của ban điều hành, ở đây xem như có m người). Trong giai đoạn đăng ký, cử tri làm mù token T_j thành hai phần khác nhau, các thành viên ban kiểm phiếu ký vào cả hai phần đó, sau đó cử tri giải mù để được chữ ký trên T_j. Giả sử 3 thành viên ban kiểm phiếu thì cử tri V_j phải làm mù token của mình thành 6 phần khác nhau. Các thành viên BKP_i ký lên 6 phần đó, sau đó cử tri giải mù cả 6 phần chữ ký đó. Ở giai đoạn bỏ phiếu, lá phiếu v_j của cử tri V_j cũng được làm mù thành hai phần khác nhau, do đó mà với 3 BKP_i thì cử tri phải làm mù phiếu bầu thành 6 phần khác nhau bằng cách sử dụng hai bộ khóa công khai của 3 BKP_i, do đó phiếu bầu v_j cũng được ký thành 6 phần khác nhau do 3 BKP_i ký. Trong giai đoạn kiểm phiếu, cử tri phải giải mù phiếu bầu đã được ký của mình thành 6 phần khác nhau. Do đó mà thời gian tính toán để làm mù token, phiếu bầu, ký vào token và phiếu bầu đã được làm mù và giải mù token, phiếu bầu mù đã được ký là tỷ lệ thuận với số lượng thành viên ban kiểm phiếu BKP_i tham gia vào lược đồ bầu cử. Đồng thời hệ thống cũng yêu cầu dung lượng lưu trữ phải lớn và băng thông đường truyền khi triển khai thực tế (*gồm nhiều thực thể ở những nơi khác nhau về địa lý*) cũng phải cao để truyền tải số lượng lớn các thành phần, và độ phức tạp tính toán và lưu trữ cao ở cả phía cử tri và phía ban điều hành bầu cử.

Trong khi đó, lược đồ bầu cử điện tử đề xuất sử dụng các lược đồ chữ ký số tập thể mù nên cử tri không quan tâm đến số lượng thành viên ban điều hành, ban kiểm phiếu mà chỉ gửi một token hoặc một phiếu bầu được làm mù cho tập thể thành viên đó và các cơ quan đó tạo chữ ký tập thể và gửi lại cử tri chỉ một chữ ký nên sẽ giảm thời gian tính toán và dung lượng lưu trữ của hệ thống.

Ngoài ra, theo Sharon Levy trong [28] chỉ ra rằng, với cùng mức độ an toàn thì độ dài khóa của lược độ dựa trên bài toán IFP và DLP yêu cầu là 1024 bit, trong khi bài toán ECDLP chỉ yêu cầu khoảng 192 bit. Do đó, với việc sử dụng lược đồ ký số dựa trên bài toán ECDLP nên độ dài khóa cũng sẽ ngắn hơn bài toán RSA và DLP nên có thể sử dụng được trong các mạng có năng lực xử lý thấp như tốc độ đường truyền, khả năng lưu trữ và năng lực tính toán của hệ thống như ứng dụng trong các thiết bị Iot, thẻ thông minh,…

D. Phân tích độ an toàn của lược đồ bầu cử đề xuất

+ Tính riêng tư của cử tri: Việc sử dụng các lược đồ chữ ký số mù cho việc ký token và phiếu bầu của cử tri nên các bên khác, kể cả các thành viên của ban kiểm phiếu đều không thể biết được nội dung bầu cử của cử tri.

+ Không lộ thông tin bầu cử: Do phiếu bầu được xây dựng gồm nhiều thành phần tham gia như cử tri, ban điều hành và ban kiểm phiếu nên mặc dù cử tri biết phiếu bầu đã ký của mình trên bảng *bangphieubau*, nhưng cử tri không thể chứng minh điều đó với người cưỡng chế.

+ Tính chính xác: Chỉ những phiếu bầu đã được ký và được giải mù và được xác nhận của cử tri có trên bảng *bangkiemphieu* thì mới được đưa vào kiểm phiếu. Ngoài ra, nếu ban điều hành không chuyển phiếu hoặc chuyển phiếu không chính xác vào bảng *bangphieubau* thì cử tri có thể từ chối việc bỏ phiếu đó.

+ Tính mạnh mẽ: Do phiếu bầu được giải mù được xác nhận của cử tri trên bảng *bangphieubau* nên cử tri không thể cho rằng phiếu bầu của mình bị phá hoại. Ngoài ra thì ban điều hành và ban kiểm phiếu cũng không thể phá vỡ được lược đồ bầu cử, trừ khi tất cả các thành viên và các cơ quan đó đều liên kết với nhau để phá vỡ lược đồ.

+ Công bằng: Do mọi phiếu bầu trên bảng *bangphieubau* đều bị làm mù và được ký bởi các thành viên của ban kiểm phiếu nên không ai có thể biết kết quả bỏ phiếu trước khi kiểm phiếu. Chỉ cử tri mới có thể giải mù phiếu bầu của mình.

+ Khả năng kiểm chứng: Mọi cử tri đều phải xác nhận phiếu bầu được ký và được làm mù của mình trên bảng *bangphieubau* và phiếu bầu đã được giải mù của mình trên bảng *bangkiemphieu*. Do đó, lược đồ bầu cử đảm bảo rằng tất cả những phiếu bầu có sự xác nhận của cử tri tương ứng mới được đưa vào kiểm phiếu.

+ Dân chủ: Cử tri được xác thực bằng các thông tin ẩn danh. Đồng thời để gửi và xác nhận phiếu bầu của mình, thông tin định danh của cử tri được đảm bảo bởi token đã được giải mù là duy nhất. Hơn nữa, token của mỗi cử tri được ký bởi nhiều cơ quan nên không ai có thể giả mạo chữ ký trên token và do đó nên tất cả cử tri đủ điều kiện đều được tham gia bỏ phiếu.

+ Chống cưỡng chế: Lược đồ bầu cử được cho là ngăn chặn việc cưỡng ép vì người bỏ phiếu phải đảm bảo nhiều lần xác thực và phải xác nhận phiếu bầu được ký và được làm mù của mình trên bảng *bangphieubau* và phiếu bầu đã được giải mù của mình trên bảng *bangkiemphieu*. Người có thẩm quyền như ban điều hành hoặc ban kiểm phiếu cũng không thể ép buộc cử tri.

VI. KẾT LUẬN

Lược đồ bầu cử điện tử đề xuất bảo đảm các yêu cầu của một cuộc bầu cử công bằng do sử dụng token không thể liên kết được cử tri với phiếu bầu của cử tri đó, và các cơ quan có thẩm quyền trong cuộc bầu cử cũng không thể liên kết được phiếu bầu đã được làm mù của cử tri với phiếu bầu đã được giải mù của cử tri đó do sử dụng lược đồ chữ ký số tập thể mù, và do đó mà lược đồ bầu cử đề xuất hoàn toàn không thể truy vết hay lược đồ bầu cử là hoàn toàn ẩn danh. Ngoài ra, do sử dụng chữ ký số tập thể trên token chứa thông tin của cử tri đã được làm mù nên cho phép cử tri xuất hiện trước các cơ quan có thẩm quyền một cách ẩn danh. Hơn nữa, do sử dụng chữ ký số tập thể mù (*với số thành viên lớn hơn 1*) trên cùng một phiếu bầu đã chứng minh sự công bằng của chính quyền. Ngoài ra, lược đồ đề xuất cũng đảm bảo hầu hết tất cả các yêu cầu thiết yếu của một hệ thống bầu cử điện tử. Thực nghiệm cũng chứng minh rằng thời gian tính toán của các tầng trong lược đồ đề xuất là đủ nhỏ và như thế có thể sử dụng được trong thực tế, và do đó có thể mở rộng lược đồ khi mà có nhiều cơ quan được bổ trí ở nhiều nơi khác nhau và cử tri có thể bỏ phiếu ở bất kỳ đâu chỉ cần có kết nối mạng internet.

Ngoài ra có thể thấy rằng, việc sử dụng lược đồ chữ ký số tập thể mù trong lược đồ bầu cử điện tử sẽ làm giảm độ phức tạp tính toán và dung lượng lưu trữ so với việc sử dụng các lược đồ chữ ký số mù đơn. Đồng thời, việc sử dụng lược đồ chữ ký số dựa trên bài toàn ECDLP sẽ có nhiều ưu điểm hơn các lược đồ dựa trên bài toán IIFP, DLP khi yêu cầu về độ an toàn tăng cao.

TÀI LIỆU THAM KHẢO

[1] A. Fujioka, T. Okamoto, and K. Ohta (1993), "A practical secret voting scheme for large scale elections", in Advances in Cryptology (AUSCRYPT'92), pp. 244–251

[2] Shinsuke Tamura and Shuji Taniguchi (2014), "Enhanced anonymous tag based credentials", Information Security and Computer Fraud, vol. 2, no. 1, pp. 10-20

[3] J. Wen-Shenq, L. Chin-Laung and L. Horng-Twu (2002), "A verifiable multi-authority secret election allowing abstention from voting," The Computer Journal, Vol. 45(6), pp. 672– 82.

[4] D. Chaum (1998), "Elections with unconditionally- secret ballots and disruption equivalent to breaking RSA", Advances in Cryptology – Eurocrypt'88, LNCS 330, Springer-Verlag, pp. 177–182.

[5] J. Benaloh and D. Tuinstra (1994), "Receipt-free secret-ballot elections," Proceedings of 26th Symposium on Theory of Computing, pp. 544–553.

[6] M. Hirt and K. Sako (200), "Efficient Receipt-Free Voting Based on Homomorphic Encryption," Proceedings of EUROCRYPT, LNCS, Vol. 1807, pp. 539-556. Springer.

[7] B. Lee, and K. Kim (2002), "Receipt-free electronic voting scheme with a tamperresistant randomizer", ICISC 2002, LNCS 2587, Springer-Verlag, pp. 389–406.

[8] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang and S. Yoo (2004), "Providing receipt-freeness in Mixnet-based voting protocols," in Proceedings of the information Security and Cryptology (ICISC '03), pp. 245–258.

[9] A. Neff (2001), "A verifiable secret shuffle and its application to E-voting", ACM CCS 2001, ACM Press, pp. 116–125.

[10] H. A. Haddad. N. Islam S. Tamura and A. K. Md. Rokibul (2015), "An incoercible e- voting scheme based on revised simplified verifiable re-encryption mix-nets", Information Security and Computer Fraud, vol. 3, no. 2, pp. 32–38.

[11] J. Schweisgut (2006), "Coercion-resistant electronic elections with observer," 2nd International Workshop on Electronic Voting, Bregenz.

[12] A. Juels and M. Jakobsson (2002), "Coercion-resistant electronic elections," Cryptology ePrint Archive, Report 2002/165, <http://eprint.iacr.org/>.

[13] Ghassan Z. Qadah, Rani Taha (2007), "Electronic voting systems: Requirements, design, and implementation", Computer Standards & Interfaces 29 (2007) 376 – 386

[14] Nidhi Gupt, Praveen Kumar, Satish Chhokar (2011), "A Secure Blind Signature Application in E Voting", Proceedings of the 5 th National Conference; INDIACom-2011.

[15] Rahul Patil, Pritam Bhor, George Ebenez, Ashish Rasal (2014), "E-Voting System on Android Platform", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 3 Issue 2.

[16] P.Manivannan1, K.Ramesh2 (2015), "E-VOTING SYSTEM USING ANDROID SMARTPHONE", International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395-0056, Volume: 02 Issue: 06.

[17] Ganaraj K (2017), "ADVANCED E-VOTING APPLICATION USING ANDROID PLATFORM ", International Journal of Computer- Aided Technologies (IJCAx) Vol.4, No.1/2.

[18] Ashraf Darwish, Maged M El-Gendy (2017), "A New Cryptographic Voting Verifiable Scheme for E-Voting System Based on Bit Commitment and Blind Signature", Int J Swarm Intel Evol Comput 2017, 6:2 DOI: 10.4172/2090-4908.1000158.

[19] Mahender Kumar, C.P. Katti, P. C. Saxena (2017), "An Identity-based Blind Signature Approach for E-voting System", I.J. Modern Education and Computer Science, 10, 47-54.

[20] Kazi Md. Rokibul Alam, Adnan Maruf, Md. Rezaur Rahman Rakib, G. G. Md. Nawaz Ali, Peter Han Joo Chong and Yasuhiko Morimoto (2018), "An Untraceable Voting Scheme Based on Pairs of Signatures", International Journal of Network Security, Vol.20, No.4, PP.774-787.

[21] L. Huian, A. R. Kankanala, and X. Zou (2014), "A taxonomy and comparison of remote voting schemes," in 23rd International Conference on Computer Communication and Networks (ICCCN'14), pp. 1–8.

[22] A. K. Md. Rokibul and S. Tamura (2012), "Electronic voting: Scopes and limitations," in Proceedings of International Conference on Informatics, Electronics & Vision (ICIEV12), pp. 525–529.

[23] Wen shenq Juang, Chin laung Lei, and Pei ling Yu (2002), "A verifiable multi-authorities secret election allowing abstaining from voting," Computer Journal, vol. 45, no. 6, pp. 672–682.

[24] O. Cetinkaya and M. L. Loc (2009), "Practical aspects of dynavote e-voting protocol," Electronic Journal of E-government, vol. 7, no. 4, pp. 327–338.

[25] Duc Nguyen Tan, Hai Nguyen Nam, Minh Nguyen Hieu, Hiep Nguyen Van, Lam Tran Thi (2017), "New Blind Multisignature Schemes based on Signature Standards", The International Conference on Advanced Computing and Applications (ACOMP 2017), DOI: 10.1109/ACOMP.2017.4, page:23-27, IEEE Catalog Number:CFP17E01-POD, ISBN:978-1-5386-0608-7

[26] Duc Nguyen Tan, Hai Nguyen Nam, Minh Nguyen Hieu, Hiep Nguyen Van, Lam Tran Thi (2018), "New Blind Muti-signature Schemes Based on ECDLP", IJECE, Vol.8, No.2, April 2018, pp.1074~1083,ISSN: 2088-8708, DOI:10.11591/ijece.v8i2, pp1074-1083.

[27] C. C. Lee M. S. Hwang and Y. C. Lai (2003), "An untraceable blind signature scheme", IEICE Transaction on Fundamentals, vol. E86-A, no. 7, pp. 1902–1906.

[28] Sharon Levy (2015), "Performance and Security of ECDSA", http://www.semanticscholar.org

AN UNTRACEABLE ELECTRONIC VOTING SCHEME BASED ON BLIND MULTISIGNATURE SCHEME

Abstract: Recently many countries moved to electronic voting instead of a traditional one for many prominent advantages compared, including security, accuracy of ballot checking and analysis. In this paper, we propose an untraceable electronic voting scheme (E-Voting) based on blind multisignature schemes based on DLP and ECDLP. The proposed scheme achieves major security aspects such as voter privacy, non-disclosure of election information, anti-coercion, accuracy, fairness, verifiable ability, democracy and system security.

Nguyễn Tấn Đức, Nhận học vị Thạc sỹ năm 2006 tại Học viện Công nghệ Bưu chính Viễn thông. Hiện là NCS, khóa 2015 của Học viện Công nghệ Bưu chính Viễn thông. Đang công tác tại Sở Thông tin và Truyền thông tỉnh Tây Ninh. Lĩnh vực nghiên cứu: Công nghệ bảo mật, an toàn thông tin mạng.

Nguyễn Hiếu Minh, Nhận học vị Tiến sỹ chuyên ngành An toàn thông tin, tại Đại học Tổng hợp Kỹ thuật điện (Saint Petersburg Electrotechnical University "LETI" (ETU)) - Liên bang Nga, năm 2006; Nhận học hàm Phó Giáo sư, ngành truyền thông và mạng máy tính năm 2010. Đang công tác tại Học viện Kỹ thuật mật mã. Lĩnh vực nghiên cứu: An ninh mạng; Mật mã; Truyền thông và mạng máy tính.

Ngô Đức Thiện, Nhận học vị Tiến sỹ năm 2010. Hiện công tác tại Học viện Công nghệ Bưu chính Viễn thông.

Lĩnh vực nghiên cứu: Lý thuyết thông tin và mã hóa, mật mã.