Protocolo de votación electrónica basado en emparejamientos bilineales

Electronic voting protocol from bilinear pairings

Gina Gallegos-García[*1], *Roberto Gómez-Cárdenas*[2], *Gonzalo Duchén-Sánchez*[3]

[1,3] IPN ESIME Culhuacan. Sta. Ana Núm. 1000, 04430, México D. F. México

[2] ITESM-CEM, Carretera Lago de Guadalupe Km 3.5, Atizapán de Zaragoza, 52926, Estado de México, México

(Recibido el 23 de noviembre de 2009. Aceptado el 13 de septiembre de 2010)

Resumen

Desde hace dos décadas la votación electrónica ha sido un campo de investigación activo, el cual involucra el uso de sistemas de información y de esquemas criptográficos con la finalidad de reducir costos y errores humanos, así como incrementar la velocidad de procesamiento, sin descuidar la seguridad del proceso. Las propuestas existentes basan dicha seguridad en la dificultad de resolver problemas matemáticos tales como la factorización en números primos ó el problema de logaritmo discreto de la Criptografía de Llave Pública. En el presente artículo se describe un protocolo de votación electrónica que garantiza privacidad, transparencia y robustez mediante el uso de un esquema de Criptografía Basada en Identidad. El protocolo propuesto está dividido en cuatro fases principales: establecimiento, autenticación, votación y conteo, e involucra un modelo de responsabilidad distribuida, dónde *t* de *n* entidades son necesarias durante la etapa de conteo para descifrar los votos. El trabajo incluye una prueba de exactitud del funcionamiento del protocolo.

----- *Palabras clave:* Emparejamientos bilineales, esquema de umbral, esquemas de firma ciega, votación electrónica

Abstract

Electronic voting has been an active research area since two decades, which involves using information systems and cryptographic schemes in order to reduce costs and human mistakes as well as increase process speed, without discard its security. In the literature there exist some proposals,

* Autor de correspondencia: teléfono: + 52 + 55 + 565 62 058, fax: + 52 + 55 + 565 62 058, correo electrónico: gina@calmecac.esimecu.ipn.mx. (G. Gallegos)

which are based on the difficult to resolve mathematical problems such as: prime factorization or discrete logarithm, both of them from Public Key Cryptography. In this paper we describe an electronic voting protocol that meets privacy, transparency and robustness by using a scheme from Identity Based Cryptography. The proposed protocol is divided in four main phases: set-up, authentication, voting and counting and involves a distributed responsibility model, with *t* out of *n* entities that are required during the counting phase to decrypt the votes. The paper includes a correctness test to show how the protocol works.

----- *Keywords:* Bilinear pairings, threshold schemes, blind signature schemes, electronic voting

Introducción

En la actualidad es natural escuchar el término *votación electrónica,* el cual se empezó a utilizar en 1964, cuando por vez primera en Estados Unidos de Norteamérica se utilizaron computadoras para desarrollar funciones relacionadas a un proceso de votación. Desde entonces y gracias al rápido crecimiento de las tecnologías de la información, la votación electrónica, es ahora una alternativa aplicable a la votación convencional.

La votación electrónica, al igual que la convencional, involucra la intervención de diferentes entidades, como: los votantes, los contadores de votos, los centros de registro, las boletas de voto y casillas de votación, por mencionar algunas. Estas entidades interactúan entre sí durante cuatro etapas principales: registro, en donde un ciudadano debe registrarse como votante; autenticación, en dónde el ciudadano garantiza que es un votante registrado, convirtiéndolo en votante auténtico; votación, dónde el votante auténtico emite su voto: y conteo, desarrollada por los contadores o un centro especial que cuenta los votos y publica los resultados. Estas fases se desarrollan por medio del uso de sistemas informáticos y dispositivos electrónicos con la finalidad de reducir costos, errores humanos y aumentar velocidad en el procesamiento de los datos. Sin embargo, en este tipo de procesos, es necesario garantizar las siguientes propiedades [1]: a) Privacidad: El voto no debe asociarse con el votante. b) Elegibilidad: Solo votantes elegibles participan en el proceso de votación. c) Unicidad: Solo debe ser contado un voto por cada votante. d) No-coercibilidad: Ninguna entidad debe ser capaz de conocer la decisión del votante ó de ejercer coerción sobre el mismo para obligar a que vote por algún candidato en particular. e) Transparencia: El proceso de votación debe ser transparente ante cualquier entidad participante. f) Exactitud: Todos los votos emitidos deben ser considerados en la cuenta final. g) Robustez: Ninguna entidad dentro del proceso de votación debe tener la posibilidad de interrumpir el proceso desde principio hasta que llegue a su fin.

Las propuestas de solución encaminadas a garantizar dichas propiedades, se enfocan en el uso de primitivas criptográficas basadas en Criptografía de Llave Pública PKC, la cual ofrece alta flexibilidad en protocolos de acuerdo de llave y mecanismos de autenticación. Sin embargo, cuando la PKC es usada, es necesaria una Infraestructura de Llave Pública PKI [2], para unir las llaves públicas con sus propietarios y para permitir a otras entidades verificar dichas uniones. Como consecuencia de esto, los componentes de cada protocolo se incrementan considerablemente, y una gran cantidad de tiempo computacional y de almacenamiento es requerido cuando el número de entidades incrementa.

La Criptografía de Llave Pública Basada en Identidad PKC-IBC, propuesta por Shamir en 1984 [3], es una alternativa de solución al

problema antes mencionado, la cual permite contar con las ventajas de la PKC, sin necesidad de sin la necesidad de utilizar certificados digitales, componentes de una PKI. En la IBC existe una entidad Generadora de Llaves Privadas GLP, quién posee una llave maestra pública y una llave maestra privada. Esta última, es útil para generar las llaves privadas de las entidades participantes dentro de un esquema de cifrado ó de firma digital basado en identidad. Es decir, el par de llaves de dichas entidades se genera con información que identifica a una entidad como lo es un correo electrónico, una dirección IP ó un número de serie, la cual no tiene relevancia con el uso de la llave. Con esto, la información que identifica a una entidad puede ser usada como llave pública para cifrar información ó para verificar una firma digital. En 2001, Boneh [4] implementó la PKC-IBC haciendo uso de emparejamientos bilineales. Desde entonces y gracias a dicha implementación, la PKC-IBC es actualmente un medio para diseñar nuevos protocolos criptográficos.

En este artículo se presenta un protocolo de votación electrónica que garantiza privacidad, transparencia y robustez haciendo uso de las propiedades de los emparejamientos bilineales.

El artículo está dividido en nueve secciones. La fundamentación matemática en que están basados los esquemas utilizados, es dada en la segunda sección. La sección tres detalla los esquemas utilizados en nuestro protocolo criptográfico de votación electrónica. El trabajo relacionado con nuestro protocolo de votación electrónica se describe en la sección cuatro. En la sección cinco se describe el funcionamiento de las cuatro fases en que se divide nuestro protocolo. En la sección seis se detalla el protocolo propuesto. En la sección siete se hace un análisis al protocolo, considerando los requisitos que un protocolo de este tipo debe cumplir. En la sección ocho se muestran los resultados obtenidos en este diseño. Finalmente en la sección nueve se dan las conclusiones y se plantea el trabajo fututo. La sección diez enlista las referencias utilizadas.

Fundamentación matemática

Un emparejamiento bilineal es una función racional $\hat{e}$ que mapea un par de elementos de un grupo hacia un elemento grupo , ambos de orden q, tal como se describe en la Ecuación (1).

$$\hat{e}: G_1 \times G_1 \rightarrow G_2 \quad (1)$$

Las leyes del grupo G_1 son aditivas y su elemento neutro es el ∞. Las leyes del grupo G_2 son multiplicativas y su elemento neutro es el 1. Los dos grupos son de orden primo q y sea P un elemento generador arbitrario de G_1. Se asume que el Problema de Logaritmo Discreto PLD, es difícil en G_1 y en G_2. Con esto, se define que el emparejamiento sobre (G_1, G_2) es un mapeo descrito por la Ecuación (1) que satisface las siguientes propiedades:

1. Bilinealidad: El término bilineal denota que el mapeo ê mantiene la dicha propiedad en los términos que se expresan en la Ecuación (2) y la Ecuación (3), dónde $P, Q, R \in G_1$, $a,b \in \Gamma q$ y $\hat{e}(P,Q)$ G_2

$$\hat{e}: (aP, bQ) = \hat{e}: (P, Q)^{ab} \quad (2)$$

$$\hat{e}: (P + Q,R) = \hat{e}: (P, R)\hat{e}(Q,R) \quad (3)$$

2. No degenerativo: Esta propiedad indica que si P es un generador de G_1, entonces $\hat{e}(P_1, P)$ es un generador de G_2, por lo que la diferencia de la Ecuación (4) existe, siempre y cuando $P \neq 0$.

$$\hat{e}(P,P) \neq 1 \quad (4)$$

3. Calculable: Para todo $P, Q \in G_1$, existen algoritmos eficientes [4] [5], que permiten calcular $\hat{e}(P,Q)$, los cuales basan su seguridad en la dificultad de resolver los siguientes problemas:

   - Problema Computacional de Diffie-Hellman (DHC). Considerando un grupo G_1, dado el generador P y (aP, bP), es computacionalmente intratable obtener el valor $(abP) \in G_1$.

- Problema de Decisión de Diffie-Hellman (DHD). Considerando un grupo G_1 de orden q, dados (aP, bP, cP), es computacionalmente indistinguible decidir si $c \equiv ab \bmod q$ o no.
- Problema Bilineal de Diffie-Hellman (DHB). Considerando los grupos G_1 y G_2 de orden q, un mapeo bilineal y ê: G_1 x $G_1 \rightarrow G_2$ un generador P de G_1 y dados (P, aP, bP, cP), es computacionalmente intratable obtener $\hat{e}(P, P)^{abc}$.

Actualmente no se sabe si el problema Bilineal de Diffie-Hellman es más fácil que el problema de Decisión de Diffie-Hellman. Sin embargo, no se conoce ningún algoritmo que pueda resolver estos problemas en tiempo polinomial.

Preliminares

Nuestra propuesta hace uso de dos primitivas criptográficas, la firma y el cifrado. La firma considera la propuesta hecha en [6] y la primitiva de cifrado contempla el esquema propuesto en [7]. A continuación se revisan aquellos conceptos básicos que permitirán entender el funcionamiento del protocolo propuesto.

Esquemas de firma ciega

En un esquema de Firma Ciega la entidad firmante no conoce el contenido del mensaje que está firmando, debido a que el emisor del mensaje realiza un proceso para ocultar su mensaje. A este proceso se le conoce como *cegar* el mensaje. Estos esquemas se usan en escenarios dónde el firmante y el emisor del mensaje son entidades diferentes.

Esquemas de umbral

En un esquema de umbral *(t, n)*, información secreta denotada como *"s"* y dividida con la ayuda de una entidad Generadora de Llaves Públicas GLP, no se revela a menos que t de n entidades propietarias de sombras, junten dichas sombras para reconstruir *"s"*.

Shamir desarrolló un esquema de umbral basado en la interpolación de Lagrange [8], el cual está dividido en dos fases: distribución y reconstrucción. La idea básica en la fase de distribución es la siguiente: Sea q un número primo, la información $s \varepsilon Z_q$ es generada por la entidad GLP y debe ser distribuida entre un grupo de n entidades G_i (i = 1,2..., n). Para esto, la GLP elige al azar un polinomio $f(x)$, definido mediante la Ecuación (5) con $a_1 x, \ldots a_{t-1} x^{t-1} \varepsilon Z_q^+$.

$$f(x) = s + a_1 x + \ldots + a_{t-1} x^{t-1} \tag{5}$$

Después, considerando el polinomio $f(x)$ de la Ecuación (5), la GLP calcula las *sombras* x_i con base en la Ecuación (6) y envía (i, x_i) a cada entidad G_1.

$$_{x1}x = f(i) \varepsilon Z_q^+ \tag{6}$$

Por otro lado, en la fase de reconstrucción, es necesario utilizar el coeficiente de la interpolación de Lagrange de la siguiente forma: Sea $S \subseteq \{1, \ldots, n\}$ un conjunto tal que $|S|$ denota la cardinalidad de un conjunto dado. La función $f(x)$ puede ser reconstruida haciendo uso de la Ecuación (7) dónde $L_j \varepsilon Z_q^+$, corresponde al coeficiente de la interpolación de Lagrange usado en el esquema de Shamir y se expresa mediante la Ecuación (8).

$$f(x) = \sum_{j \in S} L_j x_j \tag{7}$$

$$L_j \prod_{j \in S, j \neq i} \frac{-xj}{x_i - x_j} \tag{8}$$

La combinación de esquemas de umbral y la Criptografía Basada en Identidad forma un esquema de cifrado de umbral basado en identidad.

Esquemas de cifrado de umbral basado en identidad

En los esquemas de Cifrado de Umbral basado en Identidad [7], se tiene una llave maestra pública y una llave maestra privada, las cuales son divididas en n *sombras* entre n entidades.

Para cifrar un mensaje, las entidades utilizan la llave maestra pública, mientras que el proceso de descifrado requiere de un subconjunto de al t menos usuarios, dónde $t \leq n$.

Trabajo relacionado

Las primeras propuestas de protocolos criptográficos de votación electrónica tienen sus inicios en los años 80´s [9], y a la fecha se tienen propuestas recientes [10-12]. Todas ellas basadas en esquemas de firma ciega, con excepción de la propuesta [9], basada en [13]. De igual forma al final de los 90´s, diferentes protocolos para votación electrónica basados en esquemas de umbral fueron diseñados [14-15].

El protocolo propuesto en este artículo retoma algunas de las ideas principales de los protocolos antes mencionados en cuanto a utilizar dos bloques principales de construcción: esquemas de firmas ciegas y esquemas de umbral. Sin embargo, la mayoría de los protocolos propuestos basan su seguridad en la dificultad de resolver el problema de la factorización en números primos y el problema de logaritmo discreto. Nuestra propuesta mejora a las anteriores haciendo uso de la propiedad de bilinealidad de los emparejamientos bilineales, como consecuencia de ello, la seguridad de nuestro protocolo recae en la dificultad de resolver el problema de logaritmo discreto bilineal [3] y como se mencionó antes, a la fecha no se conoce ningún algoritmo que pueda resolver dicho problema en tiempo polinomial. Además, debido a que hacemos uso de la Criptografía Basada en Identidad, se elimina la administración de certificados digitales necesaria en [13-15].

Protocolo de votación electrónica propuesto

Nuestra propuesta se divide en cuatro fases: establecimiento, autenticación, votación y conteo, las cuales se describen en términos generales a continuación, para posteriormente ser detalladas en la siguiente sección.

Etapa de establecimiento

En esta etapa se generan las llaves utilizadas para cifrar y firmar los votos, para ello la entidad GLP genera su llave maestra privada s y su respectiva llave maestra pública P_{Pub}. La llave maestra pública de la entidad GLP se distribuye entre las entidades E_i con $1 \leq i \leq n$, haciendo uso del procedimiento que se detalló en la sección de Preliminares. Adicionalmente a esto, en esta etapa se genera el par de llaves útiles para firmar ciegamente los votos, para ello, el presidente de casilla genera su par público/privado, PBB_p y PBB_s respectivamente. Envía su PBB_p a una entidad llamada Entidad Combinadora EC, quien participa durante la etapa de conteo para verificar la firma σ de cada voto y posteriormente para descifrarlos haciendo uso de t sombras de descifrado de las entidades E_i.

Etapa de autenticación

En la etapa de autenticación, el votante debe mostrar su tarjeta de identificación para que las autoridades electorales verifiquen que se encuentra en la lista de votantes registrados. En caso contrario, el votante no tiene permitido emitir su voto.

Etapa de votación

El votante selecciona al candidato de su elección y cifra su elección con la llave pública P_{pub} de la entidad GLP. Posteriormente, mediante un factor ciego a, el votante oculta su voto cifrado y solicita al presidente de casilla la firma ciega sobre su voto.

Etapa de conteo

En esta etapa, los votos son verificados, descifrados y contados. La verificación de las firmas de cada voto la lleva a cabo la entidad EC, haciendo uso de la llave pública PBB_p del presidente de casilla. Después, para descifrar los votos, la EC selecciona t de n sombras de descifrado, con $t<n$ (los cuales son generados por cada entidad E_i por medio de un emparejamiento

bilineal considerando el voto y la llave privada S_{ID_i} como parámetros), calcula el producto de dichas sombras y descifra los votos. Finalmente, los votos son contados y el conteo es publicado.

Especificación del protocolo de votación electrónica

En esta sección se describe detalladamente el proceso desarrollado en cada una de las etapas del protocolo descrito con anterioridad.

La notación usada en el protocolo propuesto se muestra en la Tabla 1.

Tabla 1 Notación de nuestro protocolo

Abreviatura	*Significado*
$E_i =$	Entidades políticas, guardias civiles, presidente de la casilla, un representante de cada partido político participante y un ciudadano, todos ellos registrados en el proceso de voto electrónico $1 \leq i \leq n$.
$\frac{Ppub}{s} =$	Llave maestra pública/privada de la entidad Generadora de Llaves Privadas
$t =$	Umbral a utilizarse dentro del protocolo propuesto
$Q_{ID} =$	Llave pública obtenida a partir de la identidad de E_i
dID_i	Sombra privada de la entidad E_i
$\frac{PBB_p}{PBB_s} =$	Llave pública/privada del presidente de casilla

Etapa de establecimiento

1) En esta etapa se genera el par de llaves utilizado en la etapa de votación para cifrar y descifrar votos, por lo que la entidad GLP considera lo siguiente: Sean G_1 y G_2 dos grupos cíclicos del mismo orden primo q, que satisface un emparejamiento bilineal $\hat{e}$: G_1 x $G_1 \rightarrow G_2$. Sea $P \in G_1$ un elemento generador y sean, H: $\{0,1\}^* \rightarrow Z_q$, H_1: $\{0,1\}^* \rightarrow G_1$ y H_2: $G_2 \rightarrow \{0,1\}^n$ tres funciones hash criptográficas.

2) La entidad GLP selecciona al azar una llave maestra privada $s \in Z_q^*$ y un polinomio de grado *t-1,* como lo expresa la Ecuación (5), dónde *t* es el umbral necesario para descifrar los votos y $a_1, \ldots, a_{t-1} \in Z_q^*$ y son elegidos al azar.

3) La entidad GLP calcula su llave maestra pública P_{pub} con base en la Ecuación (9).

$$P_{pub} = sP \in G_1 \tag{9}$$

4) Para cada entidad *Ei*, con $1 \leq i \leq n$, la entidad GLP calcula las *i*-sombra denotadas por $P_{pub}^{(i)}$ de acuerdo a la Ecuación (10).

$$P_{pub}^{(i)} = (f(i))P \in G_1 \tag{10}$$

5) Por último, la entidad GLP publica los parámetros presentados en la Ecuación (11).

$$Parámetros = \{G_1, G_2, \hat{e}, H_1, H_2, P, P_{pub}^{(1)}, \ldots, P_{pub}^{(n)}, P_{pub}\} \tag{11}$$

6) Para cualquier subconjunto $S \in \{1, \ldots, n\}$ tal que $|S| \geq t$ dónde L_i denota el coeficiente de Lagrange expresado en la Ecuación (8), cada entidad E_i verifica que se cumpla la Ecuación (12)

$$\sum_{i \in S} L_i P_{pub}^{(i)} = P_{pub} \tag{12}$$

7) Dada la identidad *ID* de una entidad E_i, la entidad GLP hace lo siguiente:

   a) Con base en la Ecuación (13), y haciendo uso de la función hash H_i, calcula la llave pública Q_{ID} de cada entidad E_i.

$$Q_{ID} = H_1(ID) \in G_1 \tag{13}$$

   b) Entrega a cada entidad E_i su respectiva sombra privada dID_i, de acuerdo a la Ecuación (14).

$$d_{iD_i} = f(i)Q_{ID} \in .\mathrm{G}_1 \quad (14)$$

c) Cuando la entidad E_i recibe su sombra d_{iD_i} verifica se cumpla la Ecuación (15)

$$\hat{e}(P_{pub}^{(i)}, Q_{ID}) = \hat{e}(P, d_{iD_i}) \quad (15)$$

Si la verificación de alguna entidad E_i falla, ésta se queja con la entidad GLP, quién emite una nueva sombra privada.

8) El par de llaves útil para firmar ciegamente y verificar dichas firmas, es calculada por el presidente de casilla de la siguiente manera:

a) Selecciona al azar su llave privada denotada por PBB_s, dónde $PBB_s = x \in Z_q^*$.

b) Calcula su llave pública PBB_p con base en la Ecuación (16), dónde P quedó definido en el paso 1) de esta misma etapa.

$$PBB_p = [(PBB)]_s)P \quad (16)$$

Etapa de autenticación

1) Con el objetivo de verificar si el votante es un votante válido, los observadores solicitan al votante su tarjeta de identificación y revisan que el nombre del votante aparezca en una lista de votantes válida.

2) El votante es auténtico y autorizado para votar siempre y cuando aparezca en dicha lista. En caso contrario, es rechazado.

Etapa de votación

1) El votante elige un candidato y cifra su voto *v* como sigue:

a) *v* es codificado como un elemento de G_2.

b) Dada la identidad *ID* de cualquier entidad *Ei*, el votante calcula Q_{ID}, con base en la Ecuación (13)

c) Elige al azar un parámetro *r*, dónde $r \in Z_q$.

b) Cifra el voto con base en la Ecuación (17)

$$<U, W> = <rP, \upsilon \oplus H_2[(\hat{e}(P_{pub}, Q_{ID})]^r) > \quad (17)$$

2) Dado el voto cifrado $<U, W> \in \{0,1\}^*$, el votante obtiene la firma de su voto de la siguiente forma:

a) El votante elige al azar $a \in Z_q^*$ como factor ciego y calcula υ' utilizando la función H_1 que eligió la entidad GLP, tal como lo indica la Ecuación (18).

$$\upsilon' = aH_1(<U, W>) \quad (18)$$

b) Con base en la Ecuación (19), el presidente de casilla calcula la firma ciega σ′ del voto y se la envía al votante.

$$\sigma'[(PBB]_s)\upsilon' \quad (19)$$

c) El votante obtiene la firma σ de su voto mediante la Ecuación (20) y forma el par $(<U, W>, \sigma)$, dónde *<U, W>* es el voto y σ es la firma del voto.

$$\sigma = a^{-1}\sigma' \quad (20)$$

3) Para fines de comprobación en la etapa de conteo y haciendo uso de la función hash *H* que se definió en la etapa de establecimiento, el votante obtiene el valor hash del par $(<U, W>, \sigma)$, denotado por $H(<U, W>, \sigma)$ y lo guarda como un recibo de comprobación.

4) Considerando el uso de un dispositivo de almacenamiento, se almacena el par $(<U, W>, \sigma)$ y el valor hash antes obtenido $H(<U, W>, \sigma)$.

5) Finalmente, la tarjeta de identificación del votante es invalidada con el fin de que no pueda votar nuevamente.

Etapa de conteo

1) Para realizar el conteo de los votos, primero es necesario verificar la firma de cada voto y después descifrar los mismos, por lo que la Entidad Combinadora (EC) hace lo siguiente para cada voto emitido:

a) Con base en la Ecuación (21), verifica la firma de cada voto. Es decir, si la igualdad se mantiene, el voto es auténtico en caso contrario el voto se considera como falso.

$$\hat{e}(PBB_p, H_1(<U,W>)) = \hat{e}(P,\sigma) \quad (21)$$

b) Las entidades E_i calculan sus sombras de descifrado $\hat{e}(U, s_{iD_i})$ y se las entregan a la EC, quién selecciona un conjunto $S \subset \{1, 2, \ldots i \ldots n\}$de t sombras, tal que $|S| = t$ y calcula el producto de las mismas mediante la Ecuación (22).

$$g = \prod_{i \in S} \hat{e}(U, d_{ID_i})^{L_i} \quad (22)$$

Dónde L_i denota el coeficiente de Lagrange detallado en la Ecuación (8).

c) Una vez que se tiene g, la EC obtiene su valor hash utilizando la función hash H_2 y opera dicho valor con la parte W del voto emitido. Todo esto, con base en la Ecuación (23).

$$v = W \oplus H_2(g) \quad (23)$$

4) Los votos se cuentan y los resultados se publican. El votante puede verificar si su voto fue contado comparando su recibo denotado por $H(<U,W>,\sigma)$ con los resultados publicados.

Análisis del protocolo

A continuación se analiza el protocolo propuesto desde el punto de vista de los requisitos de seguridad, privacidad, eligibilidad, unicidad, no-coercibilidad, transparencia, exactitud y robustez, que éste cumple.

El protocolo propuesto garantiza la *privacidad* del votante durante y después de la votación gracias al uso del esquema de cifrado de umbral, el cual basa su seguridad en la dificultad para resolver los problemas de Diffie-Hellman Computacional y Bilineal. Además, en el protocolo propuesto, la *privacidad* se mantiene aún cuando el votante obtiene un recibo al término de la emisión de su voto, ya que éste no contiene información referente al votante ni a su elección.

Nuestro protocolo cumple con el requisito de *elegibilidad* debido a que durante la fase de votación, únicamente pueden emitir votos los votantes elegibles ó auténticos. Es decir, quienes fueron definidos como tal en un registro previo al día de la elección.

Adicionalmente a esto, en esta propuesta solo se considera la emisión de un voto por votante. Es decir, cada votante solo puede emitir un voto una sola vez, debido a que su tarjeta de identificación se marca, de tal forma que el votante no pueda volver a votar. Con esto, se cumple con el requisito de *unicidad* en el protocolo propuesto.

Se asegura la *no-coercibilidad* debido a que el recibo que se entrega al votante no asocia al votante con el voto. La información contenida en el recibo es el valor hash del voto cifrado y firmado por el presidente de casilla, razón por la cual el votante puede votar libremente.

Se garantiza la *transparencia* en el protocolo gracias al uso de dos esquemas criptográficos: esquema de firma ciega y esquema de cifrado de umbral basado en identidad, ambos basados en emparejamientos bilineales. La seguridad de dichos mecanismos se basa en la dificultad de resolver los problemas de Diffie-Hellman, Computacional y Bilineal. Con lo cual, nuestro protocolo no recae en la seguridad de la red, la cual no puede ser garantizada. Además, el recibo entregado a los votantes se publica al final de proceso de votación para verificar, de manera transparente, que todos los votos fueron considerados en la etapa de conteo.

Este protocolo cumple con el requisito de *exactitud*, debido a que la Entidad Combinadora puede recuperar los votos al momento de verificar la firma y descifrar los votos. En la siguiente sección se hace una prueba de exactitud al protocolo.

Aún cuando algunas entidades E_i actúen de manera deshonesta y no publiquen sombras de descifrado válidas, el protocolo propuesto cumple con la característica de ser *robusto* debido al uso del esquema de cifrado de umbral basado en identidad. Para conseguir la *robustez* en nuestro protocolo, cada entidad E_i hace lo siguiente:

a) Elige al azar $R \in \mathrm{G}_1$ y calcula W_1 y W_2 con base en las Ecuaciones (24) y (25).

$$w = \hat{e}(P,R) \in \mathrm{G}_2 \quad (24)$$

$$w_2 = \hat{e}(U,R) \in \mathrm{G}_2 \quad (25)$$

b) Haciendo uso de la función hash H, calcula el valor hash h de: $\hat{e}(U, d_{ID_i}), \hat{e}(Q, q_{ID}), w_1, w_2$ y obtiene X de acuerdo a la Ecuación (26)

$$X = R + hd_{ID_i} \in \mathrm{G}_1 \quad (26)$$

c) Genera la tupla (w_1, w_2 h, X) y la concatena con su parte de descifrado, de esta forma las otras entidades E_j pueden verificar las Ecuaciones (27) y (28).

$$\hat{e}(P,X) = \hat{e}(P,R)\hat{e}(P_{pub}^{(i)}, Q_{ID})^h \quad (27)$$

$$\hat{e}(U,X) = \hat{e}(U,R)\hat{e}(U, d_{ID_i})^h \quad (28)$$

La igualdad de la Ecuación (27) queda comprobada mediante el uso de las Ecuaciones (2) y (3) de la siguiente manera: al sustituir la Ecuación (26) en la Ecuación (27), resulta la Ecuación (29) y al utilizar las Ecuación (3) y (13), se obtiene la Ecuación (30). Finalmente haciendo uso de la Ecuación (2) y despejando d_{ID_i} de la Ecuación (14), se obtiene la Ecuación (31).

$$\hat{e}(P, R + hd_{ID_i}) = \hat{e}(P,R)\hat{e}(P_{pub}^{(i)}, Q_{ID})^h \quad (29)$$

$$\hat{e}(P,R)\hat{e}(P, hd_{ID_i}) = \hat{e}(P,R)\hat{e}(f(i)P, d_{ID_i} f(i)^{-1})^h \quad (30)$$

$$\hat{e}(P,R)\hat{e}(P, d_{ID_i})^h = \hat{e}(P,R)\hat{e}(P, d_{ID_i})^h \quad (31)$$

Por otro lado, la igualdad de la Ecuación (28) queda comprobada de la siguiente manera: al sustituir la Ecuación (26) en la Ecuación (28), se obtiene la Ecuación (32) De igual forma, al utilizar la Ecuación (3), resulta la Ecuación (33) y finalmente utilizando la Ecuación (2), se obtiene la Ecuación (34).

$$\hat{e}(U, R + hd_{ID_i}) = \hat{e}(U,R)\hat{e}(U, d_{ID_i})^h \quad (32)$$

$$\hat{e}(U,R)\hat{e}(U, hd_{ID_i}) = \hat{e}(U,R)\hat{e}(U, d_{ID_i})^h \quad (33)$$

$$\hat{e}(U,R)\hat{e}(U, d_{ID_i})^h = \hat{e}(U,R)\hat{e}(U, d_{ID_i})^h \quad (34)$$

Resultados en el protocolo propuesto

En esta sección se describe una prueba de funcionamiento del protocolo propuesto en términos de su exactitud. Para ello, es necesario probar que la Entidad Combinadora, puede descifrar y verificar la firma de cada voto emitido, primero se prueba la exactitud de la Ecuación (21), lo que indica que el voto es válido únicamente si dicha Ecuación se cumple. Para esto, se sustituyen las Ecuaciones (16) y (20) en la Ecuación (21), lo que da como resultado la Ecuación (35). Después, se sustituye la Ecuación (19) en dicha Ecuación (35), por lo que se obtiene la Ecuación (36). Posteriormente al sustituir la Ecuación (18) en la Ecuación (36), se obtiene la Ecuación (37). Finalmente, al hacer uso de la propiedad de la bilinealidad expresada en la Ecuación (2), se obtiene la Ecuación (38).

$$\hat{e}(xP, H_1(U,W)) = \hat{e}(P, a^{-1}\sigma') \quad (35)$$

$$\hat{e}(xP, H_1(U,W)) = \hat{e}(P, a^{-1} PBB_s \upsilon') \quad (36)$$

$$\hat{e}(xP, H_1(U,W)) = \hat{e}(P, a^{-1} xaH_1(U,W))^x \quad (37)$$

$$\hat{e}(P, H_1(<U, W>))^x = \hat{e}(P, H_1(<U, W>))^x \quad (38)$$

Como se puede ver, la Ecuación (38) prueba que la verificación funciona siempre y cuando la igualdad de la Ecuación (21) exista.

De igual forma, se prueba la exactitud de la Ecuación (23) la cual muestra que la sombra de descifrado es válida, solo sí es aceptable. Para ello, se sustituye en dicha Ecuación, la Ecuación (22), con lo que se obtiene la Ecuación (39). Considerando las propiedades de los grupos y sustituyendo la Ecuación (17) en la Ecuación (39), se obtiene la Ecuación (40), en la cual al sustituir la Ecuación (14) se llega a la Ecuación (41). En ésta última, al sustituir la Ecuación (7), da como resultado la Ecuación (42). En dónde, al sustituir la Ecuación (9), se obtiene la Ecuación (43). Al despejar W de la Ecuación (23), se obtiene la Ecuación (44), en la cual, si se realizan la operaciones or-exclusiva se obtiene la Ecuación (45).

$$\upsilon = W \oplus H_2(\prod_{i \in S} \hat{e}(U, d_{ID_i})^{L_i}) \quad (39)$$

$$\upsilon = W \oplus H_2(\hat{e}(rP, \sum_{i \in S} L_i d_{ID_i})) \quad (40)$$

$$\upsilon = W \oplus H_2(\hat{e}(rP, \sum_{i \in S} L_i f(i) Q_{ID})) \quad (41)$$

$$\upsilon = W \oplus H_2(\hat{e}(rP, s Q_{ID})) \quad (42)$$

$$\upsilon = W \oplus H_2(\hat{\in}(rP_{pub^{s-1}}, s Q_{ID}) \quad (43)$$

$$\upsilon = \upsilon \oplus H_2(\hat{e}(P_{pub}, Q_{ID})^r) \oplus H_2(\hat{e}(P_{Pub}, Q_{ID})^r) \quad (44)$$

$$\upsilon = \upsilon \quad (45)$$

Con base en la Ecuación (45) se prueba que la Entidad Combinadora puede descifrar el voto emitido por cada votante, siempre y cuando la igualdad de la Ecuación (22) sea correcta.

Conclusiones y trabajo futuro

En este trabajo se detalló un protocolo de votación electrónica que cumple con los requisitos propios de un protocolo de este tipo: privacidad, eligibilidad, únicidad, no coercibilidad, transparencia, exactitud y robustez, siendo éste el primer protocolo de votación electrónica que utiliza esquemas basados en emparejamientos bilineales para garantizar 3 de los requisitos antes mencionados: privacidad, transparencia y robustez. El protocolo propuesto mejora las propuestas anteriores desde el punto de vista de las premisas de seguridad que tiene el hecho de trabajar con esquemas que basen su funcionamiento en emparejamientos bilineales. Otra mejora de nuestro protocolo comparado con propuestas existentes, es la eliminación de una Infraestructura de Llave Pública. Por último es importante mencionar que el funcionamiento del protocolo propuesto fué probando mediante una prueba de exactitud. Como trabajo a futuro se considera utilizar esquemas de firma de umbral basados en identidad, con la finalidad de continuar trabajando con la idea de distribuir la llave privada, de tal forma que cualquier subconjunto de t entidades con $t<n$, sea capaz de obtener sombras de firmas. Es importante mencionar que todas las firmas tienen que ser hechas de manera ciega para evitar que las entidades firmantes actúen como entidades maliciosas dentro del protocolo de votación electrónica, con lo que se propone continuar investigaciones sobre la idea de una responsabilidad distribuida durante la etapa de emisión y conteo de votos electrónicos.

Referencias

1. O. Cetinkaya, D. Cetinkaya, "Verification and Validation Issues in Electronic Voting" *The Electronic Journal of e-Government,* Vol. 5. 2007, pp 117 – 126.
2. D.R. Kuhn, V. C. Hu, W. T. Polk, S-J. Chang, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, National Institute of Standards and Technology, SP 800-32, 2001, pp. 5-27.
3. A. Shamir, "Identity-based cryptosystems and signature schemes", *Advances in Cryptology-*

Crypto´84, Springer-Verlag, LNCS 196. Santa Bárbara (CA). 1985. pp. 47-53.

4. D. Boneh, M. Franklin, "Identity-based encryption from the Weil Pairing", *SIAM Journal of Computing*, Vol. 32. 2003. pp. 586-615.

5. M. Scott, N. Benger, M. Charlemagne, L. J. Dominguez and E. J. Kachisa, "On the Final Exponentiation for Calculating Pairings on Ordinary Elliptic Curves". *Pairing 2009*. Springer-Verlag. LNCS 5671. 2009. pp. 78-88.

6. A. Boldyreva, "Efficient Threshold Siganture, Multisignature and Blind Signature Schemes based on the Gap-Diffie-Hellman-Group Siganture Scheme". *PKC 2003*. Springer-Verlag, LNCS 2139. Miami (FL). 2003. pp. 31-46.

7. B. Libert and J. Quisquarter, "Efficient Revocation and Threshold Pairing Based Cryptosystems", *ACM Annual Symposium on Principles of Distributed Computing,* PODC. Boston (MA). 2003. pp. 163-171.

8. A. Shamir. *How to share a secret*. Ed. Communications ACM 22. New York. 1979. pp. 612-613.

9. A. Fujioka, T. Okamoto and Ohta K., "A practical secret voting scheme for large scale elections*", Advances in Cryptology – AUSCRYPT '92*, LNCS 718, Springer – Verlag. Queensland (Australia). 1993. pp. 244-251.

10. Lourdes López-García, Francisco Rodríguez-Henríquez and Miguel Ángel, León-Chávez, "An E-Voting Protocol Based on Pairing Blind Signatures" *Poster Session of International Conference on Security and Cryptography*, *Secrypt 2008*. Porto (Portugal).

11. Sung-Hyun Yun Sung-Jin Lee, "An electronic voting scheme based on undeniable blind signature scheme", *Proc. of the 37th Annual 2003 International Carnahan Conference on Security Technology,* IEEE Computer Society. Taipei (Taiwan). 2003. pp. 163-167.

12. B. Kharchineh and M. Ettelaee, "A New Electronic Voting Protocol Using a New Blind Signature Scheme", *Proc. of the Second International Conference on Future Networks, 2010, IEEE Computer Society.* Sanya (China). 2010. pp. 190-194.

13. D. Chaum, "Elections with unconditionally secrets ballots and disruption equivalent to breaking RSA", *Proc. of Eurocrypt '88,* Davos. Switzerland. 1988. pp. 177-182

14. R. Cramer, R. Gennaro and B. Schoenmrkers, "A Secure and Optimally Efficient Multi-Authority Election Scheme", *Proc. of EUROCRYPT '97,* Springer – Verlag, LNCS 1233. Konstanz (Germany). 1997. pp. 103-118.

15. O. Baudron, P. Fouque, D. Pointcheval, G. Poupard and J. Stern, "Practical multi-candidate election system", *ACM Annual Symposium on Principles of Distributed Computing,* PODC 2001. New Port (RI). 2001. pp 274-283.