Revista Facultad de Ciencias Universidad Nacional de Colombia, Sede Medellín
V 4 N°2 julio-diciembre de 2015 • ISSN 0121-747X / ISSN-e 2357-5749 • Artículo Investigación
Páginas 83 a 102

EL VOTO ELECTRÓNICO Y RETOS CRIPTOGRÁFICOS RELACIONADOS[a]

ELECTRONIC VOTING AND RELATED CRYPTOGRAPHIC CHALLENGES

DANIEL CABARCAS JARAMILLO[b]

Recibido 03-07-2015, aceptado 09-12-2015, versión final 10-12-2015.
Artículo Investigación

RESUMEN: En este artículo se presenta una visión general del estado del arte del voto electrónico como opción para llevar a cabo elecciones populares. Se discuten requerimientos prototípicos, historia, efectos en la opinión pública, retos y oportunidades del voto electrónico. Se hace un especial énfasis en los retos criptográficos y en las tecnologías existentes.

PALABRAS CLAVE: Voto electrónico, criptografía.

ABSTRACT: We present an overview of the state of the art of electronic voting as an option for running popular elections. We discuss common requirements, history, public opinion, challenges and opportunities. We provide a more in depth analysis of cryptographic challenges and existing technologies.

KEYWORDS: Electronic voting, cryptography.

1. INTRODUCCIÓN

Parece sorprendente que en el mundo computarizado en que vivimos, las elecciones populares se lleven a cabo todavía marcando con una equis y contando manualmente los votos. Naturalmente existe un creciente interés en utilizar avances tecnológicos para mejorar los procesos de elección popular. Pero existen buenas razones para que el avance de dichas tecnologías haya sido lento. El problema del voto electrónico es un problema sumamente difícil desde el punto de vista computacional y tecnológico. Adicionalmente, las elecciones populares son sumamente delicadas para la estabilidad de los estados democráticos, lo que justifica todas las precauciones para introducir cambios al proceso.

Cuando hablamos de voto electrónico nos referimos a un sistema en el que los votantes registran su voto en un computador, y los votos se contabilizan electrónicamente. En el contexto de elecciones

[a]Cabarcas, D. (2015). El voto electrónico y retos criptográficos relacionados. *Revista de la Facultad de Ciencias*, 4 (**2**), 83–102.

[b]Facultad de Ciencias, Universidad Nacional de Colombia, sede Medellín. dcabarc@unal.edu.co

populares se han ensayado dos alternativas, un sistema en el que los votantes acuden a estaciones de votación administradas por una autoridad electoral, o un sistema de votación por internet, en el que los votantes pueden votar desde cualquier aparato conectado a la red. La primera alternativa ha sido la más explorada, pues preserva la tradicional entidad de "mesa de votación", al tiempo que ofrece mejores garantías de seguridad. La identificación de los votantes suele considerarse como un problema independiente al del voto electrónico.

El voto electrónico no sólo ofrece una manera conveniente de realizar elecciones, la criptografía aplicada a elecciones ofrece también oportunidades revolucionarias. Por ejemplo, la precisión del conteo puede ser garantizada por la imposibilidad de resolver un problema matemático, en lugar de que dependa de la honestidad de funcionarios públicos. También es posible que cada votante pueda comprobar que su voto ha sido tenido en cuenta, o que cualquier ciudadano pueda verificar el conteo. Protocolos criptográficos como las firmas ocultas o el cifrado homomórfico hacen posible tales garantías.

Sin embargo, computarizar el proceso de votación en elecciones a gran escala es un problema complejo. Los retos se desprenden de una compleja lista de requisitos. Mantener el voto secreto, y al mismo tiempo garantizar la integridad de la votación es un problema computacionalmente difícil. Adicionalmente, la complejidad de la plataforma computacional hace casi imposible garantizar su seguridad. Más allá de los problemas técnicos, existe también el problema humano de generar la confianza suficiente en el votante para que ejerza libremente el derecho al voto, y para que confíe en el resultado.

Este artículo busca dar a conocer el estado del arte del voto electrónico. Aunque buscamos hacer un especial énfasis en los retos criptográficos, la naturaleza de este tema implica una discusión más amplia. En la sección 2 se explora un amplio espectro de los temas que han caracterizado la discusión acerca del voto electrónico tales como requisitos de seguridad, auditoría del sistema, plataforma computacional y complejidad del software. En la sección 3 estudiamos el papel que juega la criptografía en el voto electrónico mediante la descripción detallada de tres protocolos criptográficos. Finalmente, en la sección 4 se concluye y se listan lineas de investigación en torno al voto electrónico.

2. GENERALIDADES

La historia reciente de los intentos por implementar elecciones populares utilizando voto electrónico ha dejado enseñanzas importantes. Es fundamental establecer estándares de seguridad adecuados como los que existen en otras áreas informáticas (Mercuri & Neumann, 2002). A la vez es importante forjar una masa crítica capaz de evaluar sistemas de voto electrónico. Los gobiernos deben proceder con cautela en su adopción, manteniendo los requerimientos democráticos por encima de los intereses privados y exigiendo una evaluación rigurosa de cualquier nueva tecnología. El voto electrónico es un área de investigación nueva y abierta en la que hay mucho por hacer (Chaum, Jakobsson, Rivest,

Ryan, Benaloh, Kutylowski & Adida, 2010). A continuación se describe el panorama histórico, seguido de una discusión de los requerimientos básicos, el papel de la criptografía y finalmente se mencionan algunos problemas de seguridad informática relacionados.

2.1. Breve panorama histórico

La forma en que los diferentes países han asumido la discusión del voto electrónico es muy variada. Brasil e India han sido pioneros en incorporar sistemas de voto electrónico y otros países suramericanos han seguido sus pasos como Venezuela. Por su lado Estados Unidos, Holanda y Noruega han dado pasos adelante y atrás. Otros países Europeos han sido muy cautelosos en la incorporación de esta tecnología con la excepción de Estonia.

La rápida adopción de Brasil obedece principalmente a tres factores: la necesidad de mejorar la confiabilidad y eficiencia de su sistema electoral; la capacidad económica para invertir en el desarrollo tecnológico; y la alta centralización de su sistema electoral. Desde 1996, Brasil ha llevado a cabo sus elecciones utilizando un sistema de voto electrónico. El sistema ha sido desarrollado y controlado a puerta cerrada por la autoridad única electoral de Brasil, el Tribunal Superior Electoral (TSE), y hasta hace poco, no se conocía su funcionamiento interno. Aunque algunas alarmas en cuanto al proceso se han encendido (Krimmer, 2006; Rezende, 2010), las elecciones se llevan a cabo en relativa tranquilidad. Más recientemente, se revelaron múltiples vulnerabilidades en el sistema, a partir de una prueba pública convocada por el TSE (Aranha, Karam, Miranda & Scarel, 2014).

La India ha pasado por un proceso similar al de Brasil. Desde 1982, La comisión electoral de La India viene utilizando maquinas electrónicas de votación (EVMs) para llevar a cabo elecciones populares. La comisión logró mantener el diseño de sus EVMs oculto durante décadas, hasta que en 2010, un grupo de expertos pudo analizar el aparato, y revelar múltiples defectos en su seguridad (Wolchok, Wustrow, Halderman, Prasad, Kankipati, Sakhamuri, Yagati & Gonggrijp, 2010). Desde entonces, el gobierno viene haciendo un esfuerzo por mejorar su seguridad.

El sistema de voto electrónico Venezolano también ha sido duramente criticado, pese a que los gobiernos han hecho todo lo posible por mantener en secreto el funcionamiento interno del sistema (Carriquiry, 2011).

En contraste, en Estados Unidos cada condado tiene la autonomía y responsabilidad de elegir su propio sistema de votación, generando debate y diversidad en los sistemas utilizados. En las elecciones presidenciales del año 2000, las cuales se llevaron a cabo en su mayoría con sistemas de voto no electrónico, se presentaron problemas, agravados por un estrecho margen en los resultados del estado de Florida. La legitimidad de las elecciones fue duramente cuestionada generando incertidumbre política. El congreso reaccionó a la crisis con el llamado "Help America Vote Act" del 2002 (United States Department of Justice, 2002), una ley que incentivaba a los estados de la unión a reemplazar su obsoleta tecnología electoral y autorizaba 3900 millones de dólares para comprar nuevos equipos. Esta ley dio un gran impulso a sistemas de voto electrónico que fueron adquiridos a lo largo y ancho de los Estados Unidos. Sin embargo, el remedio probó ser tan malo

como la enfermedad. Escándalos como la desaparición de 18000 votos en la disputa para el congreso de 2006 en el distrito 13 de Florida, prendieron las alarmas de la opinión pública. En el mundo académico, Kohno, Stubblefield, Rubin & Wallach (2004) ya habían expuesto graves problemas de seguridad en un popular sistema de voto electrónico. Uno a uno, los estados de la unión han venido abandonando estos sistemas al comprobar que no se ajustan a los mínimos estándares de seguridad. Por ejemplo, la gobernación de California contrató en 2007 una auditoría independiente de los sistemas previamente certificados para uso en elecciones (Blaze, Cordero, Engle, Karlof, Sastry, Sherr, Stegers & Yee, 2007; Calandrino, Feldman, Halderman, Wagner, Yu & Zeller, 2007; Inguva, Rescorla, Shacham & Wallach, 2007). Cada estudio demostró graves falencias lo que causó que se les retirara la certificación a todos los sistemas de voto electrónico (Bowen, 2007). De forma similar el estado de Ohio invirtió 1.9 millones de dólares en el proyecto EVEREST (Evaluation & Validation of Election-Related Equipment, Standards, & Testing) que concluyó que "Los sistemas de voto electrónico de Ohio tienen fallas de seguridad críticas que podrían impactar la integridad de las elecciones" (Brunner, 2007). El más reciente experimento, por parte de las autoridades electorales de Washington DC, permitir a votantes votar por internet, mostró ser un completo desastre (Wolchok, Wustrow, Isabel & Halderman, 2012).

El proceso en Holanda no ha sido más fácil que en Estados Unidos. Tras casi una década de votaciones electrónicas, en 2006, la fundación "Wij vertrouwen stemcomputers niet" (No confiamos en computadores para votar) demostró en televisión cómo manipular las máquinas de votación más usadas en el país (Gonggrijp & Hengeveld, 2006). Esto causó que se vetara su uso y se regresara a votaciones en papel. Estonia y Noruega han sido pioneros en ofrecer votación por internet (Heiberg, Laud & Villemson, 2012), pero tras un experimento de dos años, Noruega desistió de continuar la iniciativa (Stenerud & Bull, 2012).

2.2. Requisitos

La adopción de un sistema de voto electrónico comienza por establecer los requerimientos. Para ello es importante entender la tradición electoral del país, ajustarse a la ley, explorar las capacidades de la tecnología, distinguir prioridades, sopesar el costo beneficio y estudiar el impacto social de su implantación. Aunque éste es un ejercicio que cada autoridad electoral debe llevar a cabo, múltiples autores han identificado una serie de requerimientos mínimos (Internet Policy Institute, 2001; Lambrinoudakis, Gritzalis, Tsoumas, Karyda & Ikonomopoulos, 2002):

- Elegibilidad. Unicamente votantes autorizados deben poder votar.
- Unicidad. Ningún votante debe poder votar más de una vez.
- Precisión. Los votos deben ser registrados correctamente y el conteo debe corresponder con los votos depositados.
- Verificabilidad. Debe ser posible verificar que todos los votos han sido tenidos en cuenta en el conteo final, y debe existir un registro confiable y auténtico de la elección.

- Privacidad. Nadie debe poder determinar como votó ningún individuo.
- No coercible. Los votantes no deben poder probar como votaron.
- Otros: justicia, confianza, flexibilidad, escalabilidad, conveniencia, certificable, transparencia, participación verificable, rentabilidad.

La dificultad para implementar un sistema de voto electrónico se debe en parte a que algunos de estos requerimientos están en conflicto los unos con los otros. Por ejemplo, cualquier esfuerzo para mejorar la seguridad, tiende a incrementar costos, reducir conveniencia y transparencia, dificultar la escalabilidad y complicar la implementación.

El conflicto entre integridad y privacidad del voto es quizás el más importante reto tecnológico que enfrenta el voto electrónico. Mantener el voto privado y no coercible son requerimientos que van de la mano y que son claves para el libre ejercicio del voto. Sin embargo, estos dos requerimientos son posiblemente los más difíciles de mantener desde el punto de vista criptográfico. Preservar la privacidad dificulta dejar un registro de la transacción verificable y no falsificable como en otras aplicaciones de la seguridad informática. Además, para evitar la compra de votos, el requerimiento de que el votante no pueda probar como votó, convierte al votante en enemigo de su propia transacción.

Debido a dichos conflictos, no es suficiente con establecer requerimientos, sino que también es importante priorizar. Distintos investigadores dan prioridad a unos requerimientos sobre otros, por ejemplo, Shamos, reconocido por su experiencia como auditor de sistemas de votación para gobiernos, considera que el más importante de sus 6 "mandamientos" es la privacidad (Shamos, 1993). Mientras tanto, Rivest, reconocido por sus diversos aportes en criptografía opina que "es más importante que nadie tenga su pulgar en la balanza, a tener una balanza fácil de usar o inclusive muy precisa" (Rivest, 2002). Por su parte Peralta (2002) argumenta que se debería evitar complicar el sistema para resolver problemas que tengan una incidencia esperada menor al error estadístico.

2.3. Opinión pública y el papel de la criptografía

La importancia de las elecciones populares en las sociedades democráticas convierte al voto electrónico en una infraestructura crítica. El temor más generalizado acerca del voto electrónico, es que la automatización de los sistemas de voto y conteo abra la puerta a fraudes a gran escala. Dicho temor contrasta con la experiencia en otras áreas como en el comercio electrónico o con la falta de pruebas y los pocos casos de fraude que se han presentado en las experiencias con voto electrónico en muchas partes del mundo. Sin embargo, por el carácter crítico de las votaciones, la comparación con el comercio electrónico no es satisfactoria.

La sensibilidad del voto en el proceso democrático ha llevado a explorar alternativas de verificación y auditoría que ofrezcan niveles altos de confiabilidad. En los últimos 30 años, se han desarrollado protocolos que permiten por ejemplo preservar principios como: la *verificabilidad individual* que dice

que cada votante puede verificar si su voto fue contado; la *verificabilidad universal* – introducido por Benaloh (1987)–, dice que cualquier observador puede comprobar que el conteo sea calculado con precisión a partir de los votos depositados correctamente.

Los protocolos criptográficos que hacen posible dichos niveles de confiabilidad son: las *firmas ocultas* (blind signatures), las *redes de mezclado* (mixnets), y el *cifrado homomórfico* (homomorphic encryption). En la Sección 3 describimos en detalle cada uno de estos protocolos.

A partir de estos protocolos criptográficos, se han diseñado sistemas de voto electrónico más completos (Burmester & Magkos, 2002; Neff, 2004; Benaloh, 2007; Sandler, Derr & Wallach, 2008; Adida, 2008; Ryan, Bismark, Heather, Schneider & Xia, 2009; Clarkson, Chong & Myers, 2008; Ryan & Teague, 2013). Estos no sólo abordan el problema criptográfico, sino también otros problemas computacionales asociados.

Pese a importantes avances en criptografía, hay quienes rechazan cualquier sistema de voto electrónico que no produzca un registro en papel que el votante pueda comprobar y que pueda ser usado para reconteos y auditorías (Stark, 2008). Mercuri (1992) fue la primera en proponer los llamados *Audit paper Trails*. Dicho requerimiento surge por la inevitable mediación del software entre el votante y su voto, que impide tener plena confianza en el registro electrónico. En ésta linea de pensamiento, Chaum (2004) propone un sistema de voto que combina un registro impreso que usa criptografía en lo impreso para ofrecer otras garantías de verificabilidad.

La opinión pública es sensible a esta discusión, pero como explica Peralta (2002), la apariencia de seguridad suele ser más importante que la seguridad real para imprimir confianza en el público. Las experiencias con sistemas de votación van forjando la confianza. Un estudio realizado en Colombia muestra una actitud positiva frente a la perspectiva de utilizar sistemas de voto electrónico (Alvarez, Katz, Llamosa & Martinez, 2009). Mientras tanto, los mismos sistemas de voto electrónico, cuando fueron puestos a prueba en elecciones reales en Estados Unidos, generaron aversión del público, cf. (Thomson, 2008).

2.4. Periféricos

En la implementación de un sistema de voto electrónico no es despreciable el problema de la plataforma computacional (Rivest, 2002) que incluye los computadores, sistemas operativos, y redes para las cuales hoy en día es difícil garantizar un nivel de seguridad adecuado. Estas dificultades han desestimulado iniciativas para utilizar infraestructura existente, por ejemplo cajeros electrónicos, o computadores personales de uso general que podrían ser utilizados por entidades educativas entre elección y elección (Cranor, 2002). Los fabricantes de equipos para voto electrónico han sabido aprovechar esta situación para producir computadores dedicados específicamente para registrar votos, lo que incrementa su costo pero no necesariamente resuelve el problema, cf. (Feldman, Halderman & Felten, 2007). Así mismo, en países como Estados Unidos y Brasil, por miedo a ataques cibernéticos, se ha restringido el uso de redes públicas para la transmisión de resultados electorales, optando por el tradicional transporte físico de los resultados, que tampoco ofrece garantías de

seguridad adecuadas.

La complejidad inherente a cualquier proyecto de software es otro factor adverso. Mientras más complejo sea el software, más difícil es su control y auditoría, abriendo la puerta para errores voluntarios o involuntarios. Dificultades que en otras aplicaciones suelen ser aceptables, cuando se presentan en elecciones populares pueden generar inestabilidad política. Para combatir este problema, se han propuesto diseños específicos para sistemas de voto electónico en arquitecturas innovadoras como SAVE "Secure Architecture for Voting Electronically" (Goler & Selker, 2010) y AMVA "A modular Voting Architecture" (Bruck, Jefferson & Rivest, 2010). SAVE es una arquitectura modular y robusta que según sus autores hace un sistema de voto electrónico más confiable y resistente a fallas y ataques. La principal característica de AMVA es la separación entre el acto de seleccionar candidatos y el acto de votar, y sus autores aseguran que tiene el potencial de convertirse en el estándar para futuros equipos de votación.

Muchos expertos consideran que la confianza en el voto electrónico se puede lograr mediante un escrutinio meticuloso del software por parte de autoridades electorales, expertos independientes o por la comunidad en general. En particular muchos expertos opinan que el código usado para votaciones en procesos democráticos, debe ser abierto, para asegurar transparencia. Dicha opinión se sustenta en un axioma fundamental y ampliamente aceptado en la comunidad criptográfica, conocido como el Principio de Kerckhoffs, que dice que un sistema criptográfico debe ser seguro incluso si todo acerca del sistema, excepto la llave, es conocido (Kahn, 1996). Los fabricantes de equipos y software para voto electrónico rechazan tal exigencia porque consideran que esto pone en riesgo su negocio. Lo cierto es que, ya sea a través de expertos que firmen acuerdos de confidencialidad o sea la comunidad misma, el código debe ser examinado independientemente para evitar, en lo posible, errores y/o código malicioso.

Incluso con el escrutinio de toda la comunidad científica, no es posible garantizar que no se cuelen errores en el software. Por eso, Rivest propone el principio de *independencia del software*, que dice que un cambio o error no detectado en el software no puede causar un cambio o error indetectable en el resultado de una elección (Rivest & Wack, 2008). Aunque éste todavía es un principio teórico, se han logrado avances en esta dirección.

3. PROTOCOLOS CRIPTOGRÁFICOS

Los protocolos criptográficos juegan un papel fundamental en la conformación de un sistema de voto electrónico. A través del uso cuidadoso de funciones criptográficas, es posible garantizar algunos de los requerimientos de seguridad descritos arriba con una confianza muy alta y sin depender de la honestidad de los funcionarios electorales; en cambio, su seguridad se basa en la dificultad de resolver ciertos problemas matemáticos ámpliamente estudiados. Es por eso que la criptografía yace en la base del voto electrónico.

En esta sección describimos tres protocolos que el paso del tiempo y el escrutinio de la comunidad

científica han consolidado como pilares para construir sistemas de voto electrónico.

3.1. Firmas ocultas

Chaum (1982) propone un protocolo que produce firmas ocultas para proteger la seguridad en pagos electrónicos. Chaum explica:

> El análogo en papel a una firma oculta puede ser implementado con sobres alineados con papel carbón. Escribir una firma en la parte exterior de tal sobre deja una copia de la firma en una hoja de papel dentro del sobre.

Fujioka, Okamoto & Ohta (1993) propone un esquema de votación que utiliza el protocolo de Chaum. Este permite que cada votante obtenga una firma sobre su voto que demuestra que la votante está autorizada para votar sin que su voto pueda ser conectado a su identidad. Dos autoridades independientes son necesarias, un administrador y un contador. El administrador conoce quien puede votar y es el encargado de firmar. El contador únicamente se encarga de verificar si las firmas son correctas y de contabilizar los votos.
El protocolo se basa en tres funciones criptográficas:

1. Una función de cifrado ξ junto con su inverso ξ' sólo conocidas por la votante. Dado un mensaje v, debe ser inviable obtener v a partir de $\xi(v)$ y se debe satisfacer que $\xi'(\xi(v))$ sea igual a v.

2. Una función de firma digital σ que sólo es conocida por el administrador y su correspondiente inverso σ' conocido públicamente. Dado un mensaje x, debe ser inviable obtener $\sigma(x)$ sin conocer la llave privada pero cualquiera debe poder verificar que $\sigma'(\sigma(x))$ es igual a x.

3. Una función χ que sirve para ocultar la firma y su inverso χ' sólo conocidas por la votante. Dado cualquier mensaje x debe ser inviable obtener x a partir de $\chi(x)$ y se debe satisfacer que $\chi'(\sigma(\chi(x)))$ sea igual a $\sigma(x)$.

Sea v el valor del voto de una votante. La votante cifra su voto usando la función de cifrado y obtiene $x = \xi(v)$. La votante desea obtener una firma del administrador sobre su voto cifrado x que demuestre su elegibilidad sin que el administrador conozca x. Entonces calcula $\chi(x)$ y lo envía al administrador junto con prueba de su identidad. El administrador verifica la identidad, calcula $\sigma(\chi(x))$ y lo envía a la votante. Entonces la votante calcula $\chi'(\sigma(\chi(x)))$ que es igual a $\sigma(x)$. A continuación, la votante envía $(x, \sigma(x), \xi')$ al contador de forma anónima. El contador verifica que $\sigma'(\sigma(x)) = x$, lo que certifica que el voto proviene de un votante autorizado por el administrador y extrae el voto aplicando $\xi'(x)$ que es igual a v y publica $(x, \sigma(x), \xi', v)$ de modo que el votante pueda comprobar que su voto fue tenido en cuenta, y cualquiera pueda comprobar el conteo.
Una posible implementación del protocolo utiliza RSA (Rivest, Shamir & Adleman, 1978) para las firmas digitales. Sean p, q primos, $N = pq$, e un entero primo relativo a $\phi(N)$, donde ϕ es la función

de Euler y d un entero tal que $de \equiv 1 (\mathrm{mod}\, \phi(N))$. Los valores e y N componen la llave pública y d la llave privada sólo conocida por el administrador. La función de firma digital está dada por $\sigma(m) \coloneqq m^d (\mathrm{mod}\, N)$ y su inverso $\sigma'(c) \coloneqq c^e (\mathrm{mod}\, N)$. La función para ocultar la firma está dada por $\chi(x) \coloneqq xr^e (\mathrm{mod}\, N)$ donde r es un entero primo relativo con $\phi(N)$ escogido aleatoriamente, y $\chi'(y) \coloneqq yr^{-1}$. Nótese que la aleatoriedad de r esconde el valor de x para el administrador, mientras que se satisface que $\chi'(\sigma(\chi(x))) = \sigma(x)$. Para la función de cifrado ξ se puede utilizar cualquier cifrado de llave privada como por ejemplo AES (Daemen & Rijmen, 1999).

Según Fujioka, el protocolo es escalable, asegura la privacidad de los votantes (incluso si ambos el administrador y el contador conspiran), protege la justicia de la votación, y hace imposible fraude por parte del administrador o el votante.

3.2. Función homomórfica para conteo secreto

Este protocolo se basa en una función de cifrado que posee la propiedad de ser homomórfica. En abstracto, lo que buscamos es una función $E : M \to C$, donde M es el espacio de posibles mensajes, y C el espacio de posibles mensajes cifrados, junto con dos operaciones binarias, $\oplus$ definida en M y $\otimes$ definida en C, tales que para cualesquier mensajes $v_1, v_2 \in M$, se satisface que $E(v_1) \otimes E(v_2) = E(v_1 \oplus v_2)$.

La idea es que cada voto pueda ser cifrado individualmente y que la suma de votos se pueda computar sin que sea necesario descifrar cada voto. Una vez todos los votos han sido sumados, el total es descifrado. Cramer, Gennaro & Schoenmakers (1997) proponen un protocolo para voto electrónico basado en una función de cifrado homomórfica utilizando una variante del esquema de cifrado de llave pública ElGamal (ElGamal, 1985).

Recordemos ElGamal: Sea G un grupo cíclico de orden q y un elemento $g \in G$ de orden q. La llave privada es un entero $0 \leq x \leq q-1$ y la llave pública $h = g^x$. Para cifrar un mensaje $m \in G$ escogemos un entero $0 \leq y \leq q-1$ aleatoriamente, calculamos $s = h^y = g^{xy}$ y producimos el mensaje cifrado (g^y, ms). Utilizando la llave privada se puede reconstruir el mensaje original a partir de un mensaje cifrado (c_1, c_2) calculando $c_1^x = g^{yx} = s$ y $c_2/s = m$.

La manera de usar ElGamal para establecer un sistema de voto electrónico es el siguiente. Dados votos $v_1, v_2 \in \{1, -1\}$ (si/no) los votantes construyen $m_i = g^{v_i}$, elijen enteros y_1, y_2 aleatoriamente, calculan $s_i = h^{y_i}$ y publican $(g^{y_i}, m_i s_i)$. Estos votos se combinan mediante la operación

$$(g^{y_1}, m_1 s_1) \otimes (g^{y_2}, m_2 s_2) = (g^{y_1} g^{y_2}, m_1 s_1 m_2 s_2) = (g^{y_1+y_2}, g^{v_1+v_2} h^{y1+y2})$$

que es precisamente el resultado de cifrar el voto $v_1 + v_2$ utilizando el entero aleatorio $y_1 + y_2$.

Nótese que al final de la elección y después de combinar todos los votos, quien posee la llave privada x puede obtener el valor de $m = g^{v_1+\cdots+v_l}$ donde l es el número de votantes. Para obtener el total $T = v_1 + \cdots + v_l$ es necesario resolver un logaritmo discreto que es un problema difícil en general. Sin embargo, como el número de votantes es relativamente pequeño, basta comparar m con cada

uno de los valores $\{g^{-l}, \ldots, g^{l}\}$. Esta solución puede llegar a ser costosa computacionalmente en elecciones a gran escala.

En el protocolo descrito arriba, la autoridad que posee la llave privada x, tiene la capacidad de descifrar cada voto y así violar la privacidad de los votantes. Para prevenir esta situación, la llave puede ser distribuida entre n autoridades utilizado un esquema de umbral (Shamir, 1979). Un umbral u hace imposible que un voto pueda ser descifrado a menos que un número u de autoridades conspiren. Las autoridades podrían incluir representantes de los distintos poderes públicos, partidos políticos, entidades no gubernamentales, auditores y observadores internacionales, entre otros.

La aplicabilidad del protocolo depende de que cada voto v pertenezca al conjunto de votos permitidos ($\{1, -1\}$ en el ejemplo de arriba). Para asegurarse de ésto, y al mismo tiempo preservar la privacidad del votante, se puede usar una prueba de conocimiento nulo (zero knowledge proof). Esto es un protocolo que permite al votante demostrar que su voto es válido ante una autoridad sin dar a conocer el valor del voto. Existe una basta literatura acerca de pruebas de conocimiento nulo (Goldwasser, Micali & Rackoff, 1985; Feige & Shamir, 1990), y de su aplicación en esquemas de voto electrónico (Hirt & Sako, 2000*a*; Magkos, Burmester & Chrissikopoulos, 2001). Cramer et al. (1997) propone una prueba de conocimiento nulo para su esquema de votación homomórfica basada en una prueba de conocimiento de la igualdad entre logaritmos discretos (Chaum & Pedersen, 1992) y en una prueba de conocimiento de testigo indistinguible (Cramer, Damgård & Schoenmakers, 1994).

Cramer asegura que su protocolo garantiza privacidad, verificabilidad universal, y robustez.

3.3. Mixnet

Una red de mezclado (mix network o mixnet) es un protocolo criptográfico propuesto por Chaum (1981) que permite establecer un canal anónimo. La red de mezclado está conformada por una serie de servidores. Cada servidor a su turno recibe un conjunto de mensajes, lo mezcla y lo entrega al siguiente servidor. Solo el servidor conoce cuál entrada corresponde a cuál salida, de manera que al final del proceso, nadie puede determinar cual entrada corresponde a cual salida, siempre y cuando todos los servidores no conspiren para determinarlo.

En el contexto del voto electrónico, una red de mezclado se puede usar para mezclar los votos de manera que se pierda la conexión entre el votante y su voto y así se respete la privacidad.

La idea básica de una red de mezclado utiliza un esquema de cifrado de llave pública (G, E, D), donde $(pk, sk) \leftarrow G()$ genera una pareja de llaves pública y secreta, $c \leftarrow E_{pk}(v)$ cifra el mensaje v usando la llave pública pk, y $D_{sk}(c)$ descifra el texto cifrado c usando la llave secreta sk. El esquema debe ser correcto y seguro, es decir, para todo mensaje v, $D_{sk}(E_{pk}(v)) = v$ y debe ser inviable saber algo acerca de v a partir de c.

La red de mezclado consiste de n servidores cada uno de los cuales genera una pareja de llaves pública y secreta $(pk_1, sk_1), \ldots (pk_n, sk_n)$. Supongamos que m usuarios quieren enviar mensajes

$v_1, \ldots, v_m$ a través de la red. Entonces, cada usuario prepara un texto cifrado de la forma

$$c_i = E_{pk_1}(E_{pk_2}(\cdots(E_{pk_n}(v_i)\cdots)$$

y lo escribe en un tablero público. A continuación el primer servidor descifra la primera capa de cada texto cifrado mediante $D_{sk_1}(c_i)$ para obtener

$$c_i' = E_{pk_2}(\cdots(E_{pk_n}(v_i)\cdots),$$

reordena los c_i' en orden lexicográfico y escribe el resultado en un tablero público. En este punto, solo el primer servidor que conoce sk_1 conoce cual c_i corresponde a cual c_i'. Cada servidor realiza la misma tarea, de manera que al final del proceso, el último servidor obtiene los mensajes originales $v_1, \ldots, v_m$ en un orden arbitrario y los hace públicos.

A este modelo original propuesto por Chaum se le conoce como red de mezclado de descifrado porque cada servidor descifra un texto cifrado. Park, Itoh & Kurosawa (1994) introdujeron la red de mezclado de *recifrado*, la cual no solo es más eficiente, sino que además hace posible que un tercero verifique que los mensajes que entran son los mismos que los que salen de cada servidor. Otras variaciones al modelo original incluyen los trabajos de Jakobsson & Juels (2001), Neff (2001), y Golle, Jakobsson, Juels & Syverson (2004).

Existen varios esquemas de votación electrónica que utilizan redes de mezclado, cf. (Chaum, 1981; Park et al., 1994; Sako & Kilian, 1995; Hirt & Sako, 2000*b*; Neff, 2001; Jakobsson, Juels & Rivest, 2002; Ryan et al., 2009). No basta con mezclar los votos para lograr un sistema de votación seguro. Es necesario un mecanismo para que los votantes certifiquen sus credenciales. También es importante que cada votante firme digitalmente su voto para garantizar la integridad, pero que lo haga de manera anónima para que no sea posible conectar su identidad a su voto.

4. CONCLUSIONES

Existen herramientas basadas en criptografía que hacen posible que el voto electrónico sea seguro. Sin embargo, en la realidad lo que ha prevalecido son implementaciones inseguras que no utilizan tales herramientas. Esto se debe en parte a que los intereses de los políticos, de las empresas encargadas para implementarlo, y de los ciudadanos no necesariamente coinciden. También se debe a que lograr una implementación segura de un sistema de voto electrónico es un problema sumamente difícil. Incluso si se implementara la criptografía necesaria para garantizar los requisitos de seguridad, hay muchos otros factores que podrían hacer inseguro el sistema. Más aun, si acaso se pudieran controlar muchos de tales factores, la confianza del público no está garantizada.

Consideramos que el voto electrónico puede ser una tecnología valiosa para fortalecer la democracia. Sin embargo, en este punto, hace falta más investigación para implementarla en votaciones populares de manera responsable. Así que para concluir, presentamos una lista de líneas de investigación relacionadas al voto electrónico. La lista no es completa, y responde a nuestro estudio del estado

del arte. Algunas de las líneas han alimentado el desarrollo del área durante décadas, otras apenas empiezan a jugar un papel. Algunas atañen únicamente al voto electrónico, otras aparecen en distintos contextos. La mayoría fueron discutidas en las secciones anteriores. Proveemos bibliografía relacionada para cada una. Al separar los diferentes temas, no desconocemos la necesidad de estudios comprensivos o interdisciplinarios que aborden varios de los temas propuestos y sus relaciones.

- Marco teórico que permita modelar diferentes sistemas de votación y comparar su rendimiento frente a diferentes requisitos (Lambrinoudakis et al., 2002; Gerck, 2010).
- Identificación de riesgos asociados a la plataforma computacional y formas de mitigarlos (Rivest, 2002; Cranor, 2002).
- Arquitectura y diseño de sistemas de voto electrónico (Bruck et al., 2010; Goler & Selker, 2010).
- Verificabilidad individual y universal (Benaloh, 1987; Chevallier-Mames, Fouque, Pointcheval, Stern & Traoré, 2010).
- Verificación de software (independencia del Software) (Rivest & Wack, 2008).
- Protocolos para el voto electrónico (Chaum, 1982; Fujioka et al., 1993; Cramer et al., 1997; Kiayias & Yung, 2002; Benaloh, 2007; Sandler et al., 2008; Neff, 2004; Burmester & Magkos, 2002).
- Pruebas de conocimiento nulo (Goldwasser et al., 1985; Feige & Shamir, 1990; Chaum & Pedersen, 1992; Cramer et al., 1994; Hirt & Sako, 2000*a*; Magkos et al., 2001).
- Estándares de seguridad para el voto electrónico y certificación (Federal Election Commission, 2001; IFES,UN-DESA,IDEA, 1998–2010; IEEE, 2010; NIST,NSA,NIAP, 2010; National Institute of Standards and Technology, 1996).
- Privacidad eterna del voto (Moran & Naor, 2010; Demirel, Graaf & Araújo, 2012; Buchmann, Demirel & van de Graaf, 2013; Cuvelier, Pereira & Peters, 2013).
- Identificación de problemas de seguridad en el actual sistema de votación, y cuantificación del nivel de injerencia de cada problema (Registraduría Nacional del Estado Civil, 2010).
- Modelos de contratación y legislación apropiados para el voto electrónico (Presidencia de la República, Colombia, n.d.; Departamento Nacional de Planeación, Dirección de Justicia y Seguridad, Grupo de Estudios de Gobierno y Asuntos Internos, 2003; United States Department of Justice, 2002; Mitrou, Gritzalis, Katsikas & Quirchmayr, 2002).
- Traza de papel (Audit paper Trails) (Mercuri, 1992; Chaum, 2004; Benaloh, 2007).

- Auditorías y análisis forense de elecciones (Mebane Jr, 2007; Stark, 2008; Stark, 2010; McCarthy, Stanislevic, Lindeman, Ash, Addona & Batcher, 2008; Carriquiry, 2011).
- Afectación de la opinión pública (Thomson, 2008; Alvarez et al., 2009; Krimmer, 2006; Maneschy & Jacobiskind, 2002).
- Comprensibilidad del sistema de voto electrónico por parte de los votantes (Bannister & Connolly, 2007; Randell & Ryan, 2006; Casati, 2010; Budurushi, Neumann, Olembo & Volkamer, 2013).

Referencias

Adida, B. (2008), Helios: Web-based open-audit voting, *in* Proceedings of the 17th Conference on Security Symposium, SS'08, USENIX Association, Berkeley, CA, USA, 335–348.

Alvarez, R. M.; Katz, G.; Llamosa, R. & Martinez, H. E. (2009), Assessing voters' attitudes towards electronic voting in latin america: Evidence from colombia's 2007 e-voting pilot, *in* E-Voting and Identity, Lecture Notes in Computer Science, Springer-Verlag, Berlin / Heidelberg, 75–91.

Aranha, D. F.; Karam, M. M.; Miranda, A. & Scarel, F. (2014), (In)segurança do voto eletrônico no Brasil, 117 – 133.

Bannister, F. & Connolly, R. (2007), A risk assessment framework for electronic voting, *International Journal of Technology, Policy and Management* **7**, 190–208.

Benaloh, J. (1987), Verifiable Secret-Ballot Elections, PhD thesis, Yale University.

Benaloh, J. (2007), Ballot casting assurance via voter-initiated poll station auditing, *in* Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology.

Blaze, M.; Cordero, A.; Engle, S.; Karlof, C.; Sastry, N.; Sherr, M.; Stegers, T. & Yee, K.-P. (2007), Source code review of the sequoia voting system, Technical report, University of California, Berkeley under contract to the California Secretary of State.

Bowen, D. (2007), Secretary of state debra bowen moves to strengthen voter confidence in election security following top-to-bottom review of voting systems, News Release.

Bruck, S.; Jefferson, D. & Rivest, R. (2010), A modular voting architecture ("frog voting"), *in* D. Chaum, M. Jakobsson, R. Rivest, P. Ryan, J. Benaloh, M. Kutylowski & B. Adida, eds, 'Towards Trustworthy Elections', Vol. 6000 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, 97–106.

Brunner, J. L. (2007), Project everest (evaluation and validation of election related equipment, standards and testing), report of findings, Technical report, Ohio Secretary of State.

Buchmann, J., Demirel, D. & van de Graaf, J. (2013), Towards a publicly-verifiable mix-net providing everlasting privacy, *in* A.-R. Sadeghi, ed., Financial Cryptography and Data Security, Vol. 7859 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 197–204.

Budurushi, J.; Neumann, S.; Olembo, M. & Volkamer, M. (2013), Pretty understandable democracy - a secure and understandable internet voting scheme, *in* Availability, Reliability and Security (ARES), 2013 Eighth International Conference on, 198–207.

Burmester, M. & Magkos, E. (2002), *Secure Electronic Voting (Ed. Dimitris Gritzalis)*, Kluwer Academic Publishers, chapter Towards secure and practical e-elections in the new era, 63–76.

Calandrino, J. A.; Feldman, A. J.; Halderman, J. A.; Wagner, D.; Yu, H. & Zeller, W. P. (2007), Source code review of the diebold voting system, Technical report, University of California, Berkeley under contract to the California Secretary of State.

Carriquiry, A. L. (2011), Election forensics and the 2004 venezuelan presidential recall referendum as a case study, *Statistical Science*, 26(**4**), 471–478.

Casati, R. (2010), Trust, secrecy and accuracy in voting systems: the case for transparency, *Mind & Society* **9**(1), 19–23.

Chaum, D. (1981), Untraceable electronic mail, return addresses, and digital pseudonyms, *Communications of the ACM*, 24 (**2**).

Chaum, D. (1982), Blind signatures for untraceable payments, *in* 'CRYPTO', Plenum Press, 199–203.

Chaum, D. (2004), Secret-ballot receipts: true voter-verifiable elections, *IEEE Security and Privacy*, 2 (**1**).

Chaum, D.; Jakobsson, M.; Rivest, R. L.; Ryan, P. Y. A.; Benaloh, J.; Kutylowski, M. & Adida, B., eds (2010), *Towards Trustworthy Elections*, Springer Berlin / Heidelberg, chapter Foreword.

Chaum, D. & Pedersen, T. P. (1992), Wallet databases with observers, *in* Advances in Cryptology - CRYPTO '92', Springer-Verlag, 89–105.

Chevallier-Mames, B., Fouque, P.-A., Pointcheval, D., Stern, J. & Traoré, J. (2010), On some incompatible properties of voting schemes, *in* D. Chaum, M. Jakobsson, R. Rivest, P. Ryan, J. Benaloh, M. Kutylowski & B. Adida, eds, 'Towards Trustworthy Elections', Vol. 6000 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, 191–199.

Clarkson, M.; Chong, S. & Myers, A. (2008), Civitas: Toward a secure voting system, *in* Security and Privacy, 2008. SP 2008. IEEE Symposium on, 354–368.

Cramer, R.; Damgård, I. & Schoenmakers, B. (1994), Proofs of partial knowledge and simplified design of witness hiding protocols, *in* 'CRYPTO '94: Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology', Springer-Verlag, London, UK, 174–187.

Cramer, R.; Gennaro, R. & Schoenmakers, B. (1997), A secure and optimally efficient multi-authority election scheme, *in* W. Fumy, ed., Advances in Cryptology – EUROCRYPT '97', Vol. 1233 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, 103–118.

Cranor, L. F. (2002), *Secure Electronic Voting (Ed. Dimitris Gritzalis)*, Kluwer Academic Publishers, chapter In search of the perfect voting technology: no easy answers, 17–30.

Cuvelier, E.; Pereira, O. & Peters, T. (2013), Election verifiability or ballot privacy: Do we need to choose?, *in* J. Crampton, S. Jajodia & K. Mayes, eds, 'Computer Security – ESORICS 2013', Vol. 8134 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 481–498.

Daemen, J. & Rijmen, V. (1999), 'Aes proposal: Rijndael'.

Demirel, D., Graaf, J. V. D. & Araújo, R. (2012), Improving helios with everlasting privacy towards the public, *in* In International conference on Electronic Voting Technology/Workshop on Trustworthy Elections (EVT/WOTE'12). USENIX Association.

Departamento Nacional de Planeación, Dirección de Justicia y Seguridad, Grupo de Estudios de Gobierno y Asuntos Internos (2003), Implicaciones de la adopción del voto electrónico en Colombia. Documento de Trabajo.

ElGamal, T. (1985), A public key cryptosystem and a signature scheme based on discrete logarithms, *in* G. Blakley & D. Chaum, eds, Advances in Cryptology, Vol. 196 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, 10–18.

Federal Election Commission (2001), Voting systems performance and test standards. Available at http://www.fec.gov/agenda/agendas2001/mtgdoc01-62/overview.pdf.

Feige, U. & Shamir, A. (1990), Witness indistinguishable and witness hiding protocols, *in* 'STOC '90: Proceedings of the twenty-second annual ACM symposium on Theory of computing', ACM, New York, NY, USA, 416–426.

Feldman, A. J.; Halderman, J. A. & Felten, E. W. (2007), Security analysis of the diebold accuvote-ts voting machine, *in* Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology, EVT'07, USENIX Association, Berkeley, CA, USA, 2–2.

Fujioka, A.; Okamoto, T. & Ohta, K. (1993), A practical secret voting scheme for large scale elections, *in* J. Seberry & Y. Zheng, eds, Advances in Cryptology – AUSCRYPT '92', Vol. 718 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, 244–251.

Gerck, E. (2010), The witness-voting system, *in* D. Chaum, M. Jakobsson, R. Rivest, P. Ryan, J. Benaloh, M. Kutylowski & B. Adida, eds, Towards Trustworthy Elections, Vol. 6000 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, 1–36.

Goldwasser, S.; Micali, S. & Rackoff, C. (1985), The knowledge complexity of interactive proof-systems, *in* STOC '85: Proceedings of the seventeenth annual ACM symposium on Theory of computing, ACM, New York, NY, USA, 291–304.

Goler, J. & Selker, E. (2010), A secure architecture for voting electronically (save), *in* D. Chaum, M. Jakobsson, R. Rivest, P. Ryan, J. Benaloh, M. Kutylowski & B. Adida, eds, Towards Trustworthy Elections, Vol. 6000 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, 83–96.

Golle, P.; Jakobsson, M.; Juels, A. & Syverson, P. (2004), Universal re-encryption for mixnets, *in* T. Okamoto, ed., Topics in Cryptology - CT-RSA 2004, Vol. 2964 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 163–178.

Gonggrijp, R. & Hengeveld, W.-J. (2006), Nedap/groenendaal es3b voting computer, Wij vertrouwen stemcomputers niet (The "We do not trust voting computers" foundation). Available at http://wijvertrouwenstemcomputersniet.nl/other/es3b-en.pdf.

Heiberg, S.; Laud, P. & Villemson, J. (2012), The application of i-voting for estonian parliamentary elections of 2011, *in* A. Kiyaias & H. Lipmaa, eds, 3rd international conference on e-voting and identity, Vol. 7187 of *Lecture Notes in Computer Science*, Springer-Verlag, Tallinn, Estonia, 208 – 223.

Hirt, M. & Sako, K. (2000*a*), Efficient receipt-free voting based on homomorphic encryption, *in* B. Preneel, ed., Advances in Cryptology – EUROCRYPT '2000', Vol. 1807 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, 539–556.

Hirt, M. & Sako, K. (2000*b*), Efficient receipt-free voting based on homomorphic encryption, *in* B. Preneel, ed., 'Advances in Cryptology - EUROCRYPT 2000', Vol. 1807 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 539–556.

IEEE (2010), Voting systems electronic data interchange, project 1622. Available at http://grouper.ieee.org/groups/1622/.

IFES,UN-DESA,IDEA (1998–2010), Administration and cost of elections. Available at http://aceproject.org.

Inguva, S.; Rescorla, E.; Shacham, H. & Wallach, D. S. (2007), Source code review of the hart intercivic voting system, Technical report, University of California, Berkeley under contract to the California Secretary of State.

Internet Policy Institute (2001), Report on the national workshop on internet voting.

Jakobsson, M. & Juels, A. (2001), An optimally robust hybrid mix network, *in* Proceedings of the Twentieth Annual ACM Symposium on Principles of Distributed Computing, PODC '01, ACM, New York, NY, USA, 284–292.

Jakobsson, M.; Juels, A. & Rivest, R. L. (2002), Making mix nets robust for electronic voting by randomized partial checking, *in* Proceedings of the 11th USENIX Security Symposium, USENIX Association, Berkeley, CA, USA, 339–353.

Kahn, D. (1996), *The Codebreakers: the story of secret writing*, second edn, Scribner.

Kiayias, A. & Yung, M. (2002), *Secure Electronic Voting (Ed. Dimitris Gritzalis)*, Kluwer Academic Publishers, chapter Robust verifiable non-interactive zero-sharing: A plug-in utility for enhanced voters' privacy, 139–152.

Kohno, T.; Stubblefield, A.; Rubin, A. D. & Wallach, D. S. (2004), Analysis of an electronic voting system, *Security and Privacy, IEEE Symposium on* **0**, 27.

Krimmer, R., ed. (2006), *E-Voting in Brazil- The Risks to Democracy*, Vol. 86 of *LNI*, GI.

Lambrinoudakis, C.; Gritzalis, D.; Tsoumas, V.; Karyda, M. & Ikonomopoulos, S. (2002), *Secure Electronic Voting (Ed. Dimitris Gritzalis)*, Kluwer Academic Publishers, chapter Secure electronic voting: The current landscape, 101–122.

Magkos, E.; Burmester, M. & Chrissikopoulos, V. (2001), Receipt-freeness in large-scale elections without untappable channels, *in* 'I3E '01: Proceedings of the IFIP Conference on Towards The E-Society', Kluwer, B.V., Deventer, The Netherlands, The Netherlands, 683–694.

Maneschy, O. & Jacobiskind, M. (2002), *Burla Eletrônica*, Fundacão Alberto Pasqualini.

McCarthy, J.; Stanislevic, H.; Lindeman, M.; Ash, A. S.; Addona, V. & Batcher, M. (2008), Percentage-based versus statistical-power-based vote tabulation audits, *The American Statistician* **62**(1), 11–16.

Mebane Jr, W. R. (2007), Election forensics: statistical interventions in election controversies, *in* Annual Meeting of the American Political Science Association, Vol. 13.

Mercuri, R. & Neumann, P. (2002), *Secure Electronic Voting (Ed. Dimitris Gritzalis)*, Kluwer Academic Publishers, chapter Verification for electronic balloting systems, 31–42.

Mercuri, R. T. (1992), Physical verifiability of computer systems. 5th International Computer Virus and Security Conference.

Mitrou, L.; Gritzalis, D.; Katsikas, S. & Quirchmayr, G. (2002), *Secure Electronic Voting (Ed. Dimitris Gritzalis)*, Kluwer Academic Publishers, chapter Electronic voting: Constitutional and legal requirements, and their technical implications, 43–62.

Moran, T. & Naor, M. (2010), Split-ballot voting: Everlasting privacy with distributed trust, *ACM Trans. Inf. Syst. Secur.* 13(**2**), 16:1–16:43.

National Institute of Standards and Technology (1996), Generally accepted principles and practices for securing information technology systems. Available at http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf.

Neff, C. A. (2001), A verifiable secret shuffle and its application to e-voting, *in* 'Proceedings of the 8th ACM Conference on Computer and Communications Security', CCS '01, ACM, New York, NY, USA, 116–125.

Neff, C. A. (2004), Practical high certainty intent verification for encrypted votes, Technical report, VoteHere.

NIST,NSA,NIAP (2010), Common criteria evaluation and validation scheme for it security (ccevs). Available at http://www.niap-ccevs.org/.

Park, C.; Itoh, K. & Kurosawa, K. (1994), Efficient anonymous channel and all/nothing election scheme, *in* T. Helleseth, ed., Advances in Cryptology - EUROCRYPT 1993, Vol. 765 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 248–259.

Peralta, R. (2002), *Secure Electronic Voting (Ed. Dimitris Gritzalis)*, Kluwer Academic Publishers, chapter Issues, non-issues, and cryptographic tools for Internet-based voting, 139–152.

Presidencia de la República, Colombia (n.d.), Ley 892 del 7 de julio de 2004. Disponible en http://www.presidencia.gov.co/sne/2004/julio/08/24082004.htm.

Randell, B. & Ryan, P. Y. (2006), Voting technologies and trust, *IEEE Security & Privacy*, 4 (**5**), 50–56.

Registraduría Nacional del Estado Civil (2010), Mapa de riesgo por fraude electoral 2002 y 2006. Available at http://www.registraduria.gov.co/Informacion/elec_pre_2010_presmapariesgo.htm.

Rezende, P. (2010), Electronic elections: A balancing act, *in* D. Chaum, M. Jakobsson, R. Rivest, P. Ryan, J. Benaloh, M. Kutylowski & B. Adida, eds, Towards Trustworthy Elections, Vol. 6000 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, 124–140.

Rivest, R. L. (2002), Electronic voting, *in* In Financial Cryptography '01', Lecture Notes in Computer Science, Springer-Verlag, Berlin / Heidelberg, 243–268.

Rivest, R. L.; Shamir, A. & Adleman, L. (1978), A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM*, 21 (**2**), 120–126.

Rivest, R. L. & Wack, J. P. (2008), On the notion of software independence in voting systems, *Trans. R. Soc. A* **366**(1881).

Ryan, P. Y. A.; Bismark, D.; Heather, J.; Schneider, S. & Xia, Z. (2009), Prêt à voter: a voter-verifiable voting system, *Information Forensics and Security, IEEE Transactions on*, 4 (**4**), 662–673.

Ryan, P. Y. & Teague, V. (2013), Pretty good democracy, *in* B. Christianson, J. A. Malcolm, V. Matyás & M. Roe, eds, Security Protocols XVII, Vol. 7028 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 111–130.

Sako, K. & Kilian, J. (1995), Receipt-free mix-type voting scheme, *in* L. Guillou & J.-J. Quisquater, eds, 'Advances in Cryptology - EUROCRYPT 1995', Vol. 921 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 393–403.

Sandler, D.; Derr, K. & Wallach, D. S. (2008), Votebox: a tamperevident, verifiable electronic voting system, *in* 'Proceedings of the 17th conference on Security symposium'.

Shamir, A. (1979), How to share a secret, *Commun. ACM*, 22(**11**), 612–613.

Shamos, M. (1993), Electronic voting–evaluating the threat, Presented at CFP '93. Available at http://cpsr.org/prevsite/conferences/cfp93/shamos.html/.

Stark, P. B. (2008), Conservative statistical post-election audits, *The Annals of Applied Statistics* 2 (**2**) , 550–581.

Stark, P. B. (2010), Risk-limiting vote-tabulation audits: The importance of cluster size, *CHANCE*, 23 (**3**), 9–12.

Stenerud, I. S. G. & Bull, C. (2012), When reality comes knocking norwegian experiences with verifiable electronic voting, International Conference on Electronic Voting (EVOTE2012).

Thomson, C. (2008), Can you count on voting machines?, *The New York Times* . Available at http://www.nytimes.com/2008/01/06/magazine/06Vote-t.html?_r=2&ore.

United States Department of Justice (2002), Help america vote act of 2002. Available at http://www.justice.gov/crt/voting/hava/hava.php.

Wolchok, S.; Wustrow, E.; Halderman, J. A.; Prasad, H. K.; Kankipati, A.; Sakhamuri, S. K.; Yagati, V. & Gonggrijp, R. (2010), Security analysis of india's electronic voting machines, *in* Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS '10, ACM, New York, NY, USA, 1–14.

Wolchok, S.; Wustrow, E.; Isabel, D. & Halderman, J. (2012), Attacking the washington, d.c. internet voting system, *in* A. Keromytis, ed., Financial Cryptography and Data Security, Vol. 7397 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 114–128.