ISSN: 1692-7257 - Volumen 2 - Número 26 - 2015

Revista Colombiana de Tecnologías de Avanzada

Recibido: 3 de septiembre de 2014
Aceptado: 4 de diciembre de 2014

SEGURIDAD DE LOS PROTOCOLOS DE VOTO ELECTRÓNICO A TRAVÉS DE INTERNET: UNA COMPARACIÓN

SECURITY OF ELECTRONIC VOTING PROTOCOLS THROUGH INTERNET: A COMPARISON

PhD. Isabel Cristina Satizábal Echavarría.

[*] **Universidad de Pamplona,** Facultad de Ingenierías y Arquitectura, Grupo LOGOS.
Km.1 vía a Bucaramanga, Pamplona, Norte de Santander, Colombia.
Tel.: (+577) 568 5303 Ext. 282.
E-mail: cristina.satizabal@unipamplona.edu.co

Resumen: En este artículo se analiza la seguridad de los protocolos utilizados en los sistemas SEAS y EVIV, determinando si cumplen con todas las características de seguridad que deberían incluir como son: elegibilidad, democracia, anonimato, verificabilidad, exactitud, imparcialidad, robustez, no recibo e incoercibilidad.

Palabras clave: EVIV (*End-to-end Verifiable Internet Voting system*), Protocolos, SEAS (*Secure E-voting Applet System*), Seguridad, Voto Electrónico a través de Internet.

Abstract: This paper discusses the security of the protocols used in SEAS and EVIV systems, determining whether they meet all the security features that they should include such as: eligibility, democracy, anonymity, verifiability, accuracy, fairness, robustness, receipt-freeness and incoercibility.

Keywords: EVIV (*End-to-end Verifiable Internet Voting system*), Protocols, Security, SEAS (*Secure E-voting Applet System*), Electronic Voting over Internet.

1. INTRODUCCIÓN

Actualmente, existen diferentes sistemas de voto electrónico tanto presencial como remoto, sin embargo, los usuarios suelen desconfiar de la seguridad de estos sistemas, especialmente cuando el voto se realiza, de manera remota, a través de una red pública como Internet.

Los sistemas de voto electrónico a través de Internet que existen actualmente se basan en redes combinadas (Chaum, 1981), cifrado homomórfico (Cohen & Fischer, 1985) (Joaquim, Ferreira, & Ribeiro, 2013) o firmas ciegas (Fujioka, Okamoto, & Ohta, 1992) (Baiardi et al., 2005). En este artículo se analiza la seguridad que ofrecen SEAS (Baiardi et al., 2005) y EVIV (Joaquim et al., 2013), representantes de dos de las categorías antes mencionadas, teniendo en cuenta los requerimientos de seguridad que deberían cumplir.

2. MARCO TEÓRICO

2.1 Requerimientos de Seguridad de los Sistemas de Votación Electrónica

Los requerimientos generales de seguridad que deben cumplir los esquemas de votación electrónica son (Sampigethaya & Poovendran, 2006) (Tubella i Casadevall & Vilaseca i Requena, 2005):

- **Elegibilidad:** Solo pueden votar quienes cumplan con ciertos criterios predeterminados, por lo que se debe poder verificar la validez de cada votante.

- **Democracia:** Cada elector puede votar una vez y nadie puede votar más de una vez
- **Anonimato:** No debe ser posible para nadie relacionar los votos con sus respectivos votantes, ni a corto ni a largo plazo.
- **Verificabilidad:** Cualquier votante tiene que poder verificar que el conteo final contiene su voto.
- **Resolución de Disputas:** Se debe proporcionar un mecanismo para resolver las disputas que se presenten en cualquier etapa del proceso de votación.
- **Exactitud:** El resultado final de la elección tiene que contener todos los votos válidos, por lo que estos deben ser correctamente registrados y contados.
- **Imparcialidad:** Para evitar cualquier interferencia en la conducta de los votantes, el conteo no puede empezar hasta que la elección no haya finalizado.

Para asegurar la resistencia frente a adversarios, el sistema debe cumplir, además, con los siguientes requisitos (Sampigethaya & Poovendran, 2006):

- **Robustez:** Debe ser robusto frente ataques pasivos y activos por parte de autoridades o votantes corruptos, como también frente a fallas (como dar acceso a autoridades o votantes no participantes)
- **No recibo:** No se le debería dar al votante ningún recibo que permita demostrar el sentido de su voto, para evitar la pérdida de anonimato.
- **Incoercibilidad:** El sistema no debe permitir posibles coerciones, como la extorsión por parte de adversarios.

3. PROTOCOLOS SEGUROS DE VOTO ELECTRÓNICO

3.1. Notación

La notación que se utiliza para expresar los protocolos que se describen a continuación, se muestra en la Tabla 1.

Tabla 1. Notación

SÍMBOLO	SIGNIFICADO
PK_i^j / SK_i^j	Claves pública y privada número j de la entidad i
K_{ij}	Clave secreta compartida de las entidades i y j
$SK_i^j\{m\}$	Mensaje m cifrado/descifrado con la clave privada número j de la entidad i
$PK_i^j\{m\}$	Mensaje *m* cifrado/descifrado con la clave pública número j de la entidad *i*.
$K_{ij}\{m\}$	Mensaje *m* cifrado con la clave secreta compartida de las entidades *i* y *j*.
$K_{ij}^{-1}\{m\}$	Mensaje m descifrado con la clave secreta compartida de las entidades *i* y *j*.
$[m]_{blind}$	Mensaje *m* cegado (ver Chaum, 1983).
h(m)	*Hash* del mensaje *m*.
ID^i	Identificador *i* del votante.
vote	Voto.
rec#	Número de recibo.
$CERT_i$	Certificado de la entidad *i*.

3.2 *SEAS*: Secure E-voting Applet System

Este protocolo fue definido por Baiardi et al. en el 2005 (Baiardi et al., 2005) y puede usarse en organizaciones distribuidas, que pueden tener hasta decenas de miles de miembros. En él intervienen 3 entidades:

- **Votante (V):** Es aquel que quiere votar de una forma segura.
- **Validador (Va):** Es el servidor que comprueba que el votante puede votar y habilita el voto.
- **Contador (C):** Es el servidor que se encarga de contar los votos válidos.

Se asume que cada votante, el validador y el contador poseen un certificado digital que contiene su clave pública PK_i^1 y que existen tres listas:

- **RVL1**: Es la lista de todas las personas que pueden votar, y contiene: el nombre del votante, el certificado digital de cada votante y el primer identificador ID^1 de cada votante. Esta lista es conocida por el validador Va y el contador C. C actualiza esta lista en el paso 2 del protocolo para indicar que ya ha firmado el par (PK_V^2,ID^2) del votante, mientras que Va actualiza esta lista en el paso 5 del protocolo para indicar que V ya votó.
- **RVL2:** Es una lista creada por el contador C, que contiene la pareja (PK_V^2, ID^2) de cada votante. Es actualizada en el paso 3 del protocolo.
- **RL:** Es una lista creada por el contador C, que contiene: los votos válidos cifrados $PK_V^3\{vote\}$, la clave de descifrado de cada uno de los votos SK_V^3, y el número de recibo de cada voto rec#. Es actualizada en los pasos 7 y 8 del protocolo.

En este protocolo, cada votante cuenta con dos identificadores ID^1 al que le corresponde el par de claves PK_V^1/SK_V^1 e ID^2 al que le corresponde el par de claves PK_V^2/SK_V^2. C, a pesar de conocer ambas identidades no puede relacionar una con la otra, lo que sirve para garantizar el anonimato de los votos.

La secuencia de mensajes que se envían estas entidades entre sí durante el proceso de votación es (Baiardi et al., 2005):

1. **V → C:** $SK_V^1\{[h(PK_V^2,ID^2)]_{blind,}\ ID^1\}$
2. **C → V:** $SK_C^1\{[h(PK_V^2,ID^2)]_{blind}\}$
3. **V → C:** $SK_C^1\{h(PK_V^2,ID^2)\}$, PK_V^2, ID^2
4. **V → Va:** $SK_V^1\{[h(PK_V^3\{vote\})]_{blind}\}$, ID^1
5. **Va → V:** $SK_{Va}^1\{[h(PK_V^3\{vote\})]_{blind}\}$
6. **V → C:** $SK_V^2\{SK_{Va}^1\{h(PK_V^3\{vote\})\}\}$, $PK_V^3\{vote\}$, ID^2
7. **C → V:** rec#, $SK_C^1\{PK_V^3\{vote\}\}$
8. **V → C:** rec#, SK_V^3

3.3. EVIV: End-to-end Verifiable Internet Voting system

Este protocolo fue definido por Joaquim et al. en el 2013 (Joaquim et al., 2013) y puede ser usado en pequeñas elecciones con un solo servidor como en grandes elecciones con cada servicio replicado varias veces, asegurando la escalabilidad y evitando problemas de bloqueos. En él intervienen 4 entidades:

- **Comisión Electoral (CE):** Se encarga del registro de los votantes, el sistema de votación y la autenticación de todos los datos públicos de las elecciones.
- **Votante (V):** Es un ciudadano con derecho a votar.
- **Administradores (A):** Se comparte el control sobre la privacidad del votante y la integridad de las elecciones entre estas entidades. Los administradores pueden ser los partidos políticos u otra autoridad autorizada (p.e. un observador de las elecciones de un organismo no gubernamental).
- **Organizaciones Independientes (OI):** Se encargan de determinar, de una manera independiente, que los datos públicos de las elecciones sean correctos. Cualquier persona u organización puede desempeñar el rol de organización independiente, siempre y cuando tenga los medios computacionales para hacerlo.

La arquitectura de EVIV está constituida por:

- **Servicio de Inscripción:** Es el responsable del proceso de inscripción de cada votante y es proporcionado por la comisión electoral. En este proceso se le asigna a cada votante un VST (*Token* de Seguridad). Con este *token*, el votante puede participar en varias elecciones hasta que expire.
- **Registro Electoral (RE):** Les permite a los votantes registrarse en línea a una elección determinada y está a cargo de la comisión electoral.
- **Urna Electoral (UE):** Realiza la autenticación del votante y la verificación del correcto cifrado del voto antes de aceptarlo.
- **Tablón de Anuncios (TA):** Es el lugar donde se publican todos los datos públicos de la elección. Los datos publicados no se pueden borrar y son siempre autenticables
- **Servicio de Verificación (SV):** Verifica que los votos y recibos sean correctos y válidos.
- ***Token* de Seguridad del Votante (VST):** Se encarga de cifrar el voto y de firmar digitalmente la información emitida por el votante (el par de claves del votante (PK_V^1/SK_V^1) y el certificado del votante ($CERT_V$), firmado por la comisión electoral, están dentro del VST). Este *token* puede ser una tarjeta inteligente.
- **Plataforma del Cliente:** Es el PC o cualquier otro tipo de máquina que interactúa con el lector del VST, y que tiene el sistema operativo y los programas que el votante usa durante el proceso electoral.

Antes de todo, es bueno tener en cuenta, que EVIV utiliza el criptosistema conocido como ElGamal exponencial donde los parámetros de la clave pública de la elección (PK_E) son *p*, *q* y *g*. Este criptosistema tiene homomorfismo (ver Apéndice A de (Joaquim et al., 2013)). Además, la clave privada de la elección (SK_E) es compartida entre un conjunto de *n* administradores para proteger la privacidad del votante. Por tanto, para descifrar un mensaje es necesaria la colaboración de $t<=n$ administradores.

El protocolo de EVIV se divide en 4 fases:

- **Fase de Inscripción del Votante:** Se realiza fuera de línea. El votante va personalmente a la Comisión Electoral y presenta una prueba de su identidad ID^1.
  1. **V → CE:** ID^1
  2. **CE → V:** VST
  3. **CE → TA:** $CERT_V$.

- **Fase de Registro en la Elección:** Se realiza algún tiempo antes de la elección (p.e. un mes) y se divide en dos estados: el estado de instalación (pasos 4 a 6) (llevado a cabo por la comisión electoral y los administradores), donde se anuncia la elección publicando parámetros (datos públicos) como: la lista de candidatos (LC), fecha de la elección (Date) y los parámetros de la clave pública *(p,q,g)*; y el estado de registro (pasos 7 a 11), donde cada votante se registra para participar en la elección (el votante se conecta de manera segura con el registro electoral, usando SSL/TLS, y genera una boleta (*ballot*) que contiene *k* votos cifrados ($cvote_i$, i=1 ... k), en orden aleatorio, y las correspondientes pruebas de validez de cada voto ($voteValidity_i$), donde k es el número de candidatos. La boleta tiene k-1 votos NO y un voto SI. Cada $cvote_i = (u,v) = (PK_E(b,t), PKE(q,d))$, donde b=1 para el voto SI y b= -1 para el voto NO, q es el código de confirmación aleatorio, t y d son parámetros de aleatorización. Tras el paso 10, el VST crea una tarjeta de códigos (*codecard*) compuesta por un código de votación aleatorio para cada candidato y un código de confirmación que debe corresponder al q_i del voto SI. El votante debe imprimir esta tarjeta en papel y mantenerla secreta.
  4. **CE** → **TA:** SK_{CE}^{1}{Date, *p*, *q*, *g*}, SK_{CE}^{1}{LC},
  5. **A** → **TA:** SK_{A}^{1}{*KeyGenerationData*, PK_E}
  6. **CE** → **TA:** SK_{CE}^{1} {PK_E}
  7. **RE** → **V:** SK_{CE}^{1}{LC}, SK_{CE}^{1} {PK_E}
  8. **V** → **RE:** SK_{V}^{1}{*ballot*}
  9. **RE** → **TA:** $SK_{RE}^{1}{SK_{V}^{1}${*ballot*}}$
  10. **RE** → **V:** $SK_{RE}^{1}{SK_{V}^{1}${*ballot*}}$
  11. **CE** → **TA:** SK_{CE}^{1}{*ballotList*}

- **Fase de Votación:** Esta fase también se compone de dos estados: el estado de inicialización (pasos 12 y 13), donde se genera un desafío (*electionChallenge* = h(*randomNumber*||*electoralRoll*||*ballotList*)) aleatorio que garantiza la verificabilidad extremo a extremo de EVIV y el estado de votación (pasos 14 a 18), donde el votante se conecta de manera segura a la urna electoral, introduce el código correspondiente al candidato por el que quiere votar indicado en su tarjeta de códigos y el VST genera el voto cifrado. El voto (*vote*) es la rotación (l veces), de la boleta del votante (*ballot*) hasta que el voto SI coincida con la posición del candidato elegido ($vote = \|_i^k cvote_{(i+l) \bmod k}$). Además, la concatenación de los códigos de verificación y de las pruebas correspondientes crean el recibo de votación (rec#) y el recibo de validez (*recValidity*).
  12. **A** → **TA:** SK_{A}^{1}{*generationData*, *randomNumber*}
  13. **CE** → **TA:** SK_{CE}^{1}{*electionChallenge*}
  14. **UE** → **V:** SK_{CE}^{1}{LC}, SK_{CE}^{1}{*electionChallenge*}
  15. **V** → **UE:** SK_{V}^{1}{*vote*, rec#, *recValidity*}
  16. **UE** → **TA:** $SK_{UE}^{1}{SK_{V}^{1}${*vote*, rec#, *recValidity*}}$
  17. **UE** → **V:** $SK_{UE}^{1}{SK_{V}^{1}${*vote*, rec#, *recValidity*}}$
  18. **CE** → **TA:** SK_{CE}^{1}{*electoralRoll*, *ballotList*, *voteList*, *receiptList*}

- **Fase de Verificación Pública y Conteo de Votos:** En esta fase, los administradores realizan el conteo anónimo homomórfico de los votos y cualquiera puede verificar todos los datos públicos de la elección, sin comprometer la privacidad de los votantes. Esta fase tiene 3 estados: el estado de verificación de los datos de la elección (pasos 19 a 21), el estado de conteo de los votos (pasos 22 a 24), y el estado de verificación de conteo de votos (paso 25).
  19. **OI_i** → **TA:** SK_{OIi}^{1}{electoralRoll, ballotList, voteList, receiptList}
  20. **V** → **SV_i:** ID^2
  21. **SV_i** → **V:** SK_{OIi}^{1}{*verifiedReceipt*}
  22. **CE** → **TA:** SK_{CE}^{1}{*homomorphicVotesAggregation*}
  23. **A_t** → **TA:** SK_{At}^{1}{*voteTally*, *decryptionProof*}
  24. **CE** → **TA:** SK_{CE}^{1}{*homomorphicVotesAggregation*, *voteTally*, *decryptionProof* }
  25. **OI_i** → **TA:** SK_{OIi}^{1}{*homomorphicVotesAggregation*, *voteTally*, *decryptionProof* }

4. COMPARACIÓN DE PROTOCOLOS DE VOTO ELECTRÓNICO

4.1 Elegibilidad

En la Tabla 2 se observa la comparación de la característica de elegibilidad de los dos protocolos de voto electrónico explicados en la sección 3.

4.2 Democracia

En la Tabla 3 se observa la comparación de la característica de democracia de los dos protocolos de voto electrónico explicados en la sección 3.

Tabla 2. Elegibilidad.

PROTOCOLO	ELEGIBILIDAD
SEAS	Si la incluye, pues el validador verifica que el identificador del votante ID^1 esté en la lista de votantes RVL1 y si es así firma el voto cifrado.
EVIV	Si la incluye, pues la urna electoral verifica que es un votante válido cuando descifra el mensaje que recibe con la clave pública del votante.

4.3 Anonimato

En la Tabla 4 se observa la comparación de la característica de anonimato de los dos protocolos de voto electrónico explicados en la sección 3.

4.4 Verificabilidad

En la Tabla 5 se observa la comparación de la característica de verificabilidad de los dos protocolos de voto electrónico explicados en la sección 3.

4.5 Exactitud

En la Tabla 6 se observa la comparación de la característica de exactitud de los dos protocolos de voto electrónico explicados en la sección 3.

Tabla 3. Democracia.

PROTOCOLO	DEMOCRACIA
SEAS	Si la incluye, pues el validador verifica que el votante no ha votado antes de firmar el voto y actualiza la lista de votantes RVL1 indicando que ya votó. El contador también actualiza la lista de votantes una vez ha firmado el par (PK_V^2, ID^2) del votante para no registrar dos veces al mismo votante en RVL2.
EVIV	No queda claro como se introduce esta característica, pues en la descripción del protocolo no se especifica si la urna electoral verifica si el votante ya ejerció su derecho al voto, e incluso en la fase de verificación, si el votante detecta que ha habido un error en su voto, puede volver a votar antes de que se realice el conteo.

Tabla 4. Anonimato.

PROTOCOLO	ANONIMATO
SEAS	Si la incluye, ya que cada votante posee dos identificadores ID^1 e ID^2, con su respectivo par de claves y el contador no puede relacionar uno con otro.
EVIV	Si la incluye, ya que solo el votante y su VST saben quién fue el candidato elegido, siempre y cuando el votante mantenga secreta su tarjeta de códigos. De esta manera, en la fase de verificación, el votante puede solicitar al servicio de verificación de cualquier organización independiente una copia verificada de su recibo de votación y comprobar que el código de confirmación es el mismo que el valor de verificación que aparece en su recibo de votación.

4.6 Imparcialidad

En la Tabla 7 se observa la comparación de la característica de imparcialidad de los dos protocolos de voto electrónico explicados en la sección 3.

Tabla 5. Verificabilidad.

PROTOCOLO	VERIFICABILIDAD
SEAS	Si la incluye, ya que después de la elección, el contador publica las listas RL, RVL1 y RVL2, y el validador publica su lista RVL1. Por tanto, con el número de recibo rec#, cada votante puede consultar la lista RL, descifrar el voto, saber si corresponde al candidato por quien votó y verificar que su voto fue tenido en cuenta en el conteo final..
EVIV	Si la incluye, ya que las organizaciones independientes y los votantes, a través de estas, pueden verificar que toda la información publicada en el tablón de anuncios es correcta. Incluso, si el votante detecta durante la fase de verificación que hubo algún error en su voto, puede volver a votar.

Tabla 6. Exactitud.

PROTOCOLO	EXACTITUD
SEAS	Si la incluye, ya que el contador descifra el voto, una vez recibe la clave SK_V^3 e incrementa el conteo.
EVIV	Si la incluye, ya que la comisión electoral calcula homomórficamente la agregación de votos, que es luego descifrada por un conjunto de administradores, quienes realizan el conteo y firman el resultado para publicarlo en el tablón de anuncios. Finalmente, tanto la comisión electoral como las organizaciones independientes pueden verificar que el conteo sea correcto.

4.7 Robustez

En la Tabla 8 se observa la comparación de la característica de robustez de los dos protocolos de voto electrónico explicados en la sección 3.

4.8 No Recibo

En la Tabla 9 se observa la comparación de la característica de no recibo de los dos protocolos de voto electrónico explicados en la sección 3.

Tabla 7. Imparcialidad.

PROTOCOLO	IMPARCIALIDAD
SEAS	Si la incluye, ya que solo se publica el resultado del conteo cuando se han cerrado las elecciones, aunque el contador va contando los votos a medida que recibe las claves para descifrarlos.
EVIV	Si la incluye, ya que solo se pública el resultado del conteo tras la fase de verificación.

4.9 Incoercibilidad

En la Tabla 10 se observa la comparación de la característica de incoercibilidad de los dos protocolos de voto electrónico explicados en la sección 3.

Tabla 8. Robustez.

PROTOCOLO	ROBUSTEZ
SEAS	La incluye parcialmente, ya que el protocolo es resistente a diferentes ataques, gracias a que los mensajes son firmados y se puede comprobar su autenticidad, además la información crítica viaja cegada. Sin embargo, hay un error en el primer mensaje que se envía, ya que ID^1 viaja cifrado y el contador no sabe qué clave utilizar para descifrar el mensaje, lo que no le permitiría realizar el proceso de registro del votante y que no se puedan llevar a cabo los demás pasos.
EVIV	Si la incluye, ya que el protocolo es resistente a diferentes ataques, gracias a que los mensajes son firmados y se puede comprobar su autenticidad. Además, se establece un canal seguro entre el votante y las otras entidades, lo que garantiza que la información viaje cifrada y no pueda ser utilizada por los atacantes. Finalmente, los votos solo pueden ser descifrados por un conjunto de administradores, gracias a que son cifrados con la clave pública de la elección.

Tabla 9. No Recibo.

PROTOCOLO	NO RECIBO
SEAS	Si la incluye, ya que con el número de recibo rec#, se puede consultar la lista RL, descifrar el voto y saber si corresponde al candidato por quien votó. Dicho recibo no está vinculado con la identidad del votante.
EVIV	La incluye parcialmente, ya que el código de confirmación de la tarjeta de códigos debe coincidir con el código de verificación del recibo, pero la única forma de no relacionarlo con el votante es que la tarjeta de códigos se mantenga en secreto.

Tabla 10. Incoercibilidad.

PROTOCOLO	INCOERCIBILIDAD
SEAS	No la incluye, pues un atacante puede obligar al votante a votar por quién él desee, sin que el protocolo lo detecte y el número de recibo ayuda a verificar que fue así.
EVIV	Trata de incluirla dándole al votante la posibilidad de votar varias veces, pero esto va en contra de la característica de democracia, y el votante puede proporcionar una prueba de su voto al que lo coacciona, su tarjeta de códigos.

5. CONCLUSIONES

Como se puede apreciar en las tablas de comparación, los protocolos analizados (SEAS e EVIV) no cumplen con la totalidad de las características de seguridad que deberían tener. La mayor falencia que presentan se relaciona con la resistencia a la coerción, pues siempre hay formas de que los atacantes obliguen a los votantes a votar por un determinado candidato, dado que la elección se realiza remotamente, y de comprobar que fue así.

Esta característica va un poco en contraposición con la característica de verificabilidad, porque el votante debe poder comprobar que su voto fue incluido en el conteo, y si el votante lo puede hacer, el que coacciona también puede comprobar por quién votó el votante.

También se evidencia en este análisis, que aunque el protocolo de EVIV es más complejo criptográficamente que el de SEAS, pues se lleva a cabo en una mayor cantidad de fases y pasos, no incluye la característica de democracia, pues le da la posibilidad a los votantes de votar varias veces como estrategia de incoercibilidad, e incluye parcialmente el no recibo, porque si la tarjeta de códigos cae en manos diferentes a las del votante, se puede vincular a ese votante con su voto.

Por tanto, SEAS tiene un protocolo más seguro y fácil de implementar que EVIV, aunque se debe corregir el error de cifrar la identidad del votante en el primer paso, ya que al utilizar un canal anónimo no sería posible identificar de qué votante se trata, e incluir la característica de incoercibilidad.

REFERENCIAS

Baiardi, F., Falleni, A., Granchi, R., Martinelli, F., Petrocchi, M., & Vaccarelli, A. (2005). SEAS, a Secure E-voting Protocol: Design and Implementation. *Computers & Security*, *24*, 642-652.

Chaum, D. (1981). Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. *Communications of the ACM*, *24*(2), 84-88.

Chaum, D. (1983). *Blind Signatures for Untraceable Payments.* Paper presented at the CRYPTO'82.

Cohen, J. D., & Fischer, M. J. (1985). *A Robust and Verifiable Cryptographically Secure Ellection Scheme.* Paper presented at the FOCS'85.

Fujioka, A., Okamoto, T., & Ohta, K. (1992). *A Practical Secret Voting Scheme for Large Scale Elections.* Paper presented at the AUSCRYPT'92.

Joaquim, R., Ferreira, P., & Ribeiro, C. (2013). EVIV: An End-to-End Verifiable Internet Voting System. *Computers & Security*, *32*, 170-191.

Sampigethaya, K., & Poovendran, R. (2006). A Framework and Taxonomy for Comparison of Electronic Voting Schemes. *Computers & Security*, *25*, 137-153.

Tubella i Casadevall, I., & Vilaseca i Requena, J. (2005). *Sociedad del Conocimiento, Cómo Cambia el Mundo ante Nuestros Ojos.* Barcelona: Editorial UOC.