Estudio de los Sistemas de Verificación para Votaciones Electrónicas Presenciales

Roger Jardí Cedó, Jordi Pujol Ahulló y Jordi Castellà Roca
Departament d'Enginyeria Informàtica i Matemàtiques
UNESCO Chair in Data Privacy
Universitat Rovira i Virgili
Av. Països Catalans 26. E-43007 Tarragona, Spain
Email: {roger.jardi, jordi.pujol, jordi.castella}@urv.cat

***Resumen*—Las elecciones son una parte muy importante de una democracia. Mediante éstas, la sociedad puede elegir a sus representantes, tomar una decisión o expresar una opinión. Alguien podría estar interesado en manipular los resultados de dichas elecciones sin ser descubierto. Por este motivo es necesario un control del proceso de votación que detecte y evite cualquier tipo de alteración. En este trabajo se estudian los principales sistemas de verificación (académicos y comerciales), que realizan dicho control en los sistemas de votación electrónica presencial. Con este fin, se ha diseñado un marco comparativo común con el que se analizan todos los sistemas de verificación de votación electrónica. Este marco comparativo agrupa diferentes propiedades, cubriendo importantes áreas tales como la interacción con el usuario o la seguridad.**

I. Introducción

Un proceso electoral consiste en elegir a una persona o partido, es decir, un representante de todos los miembros de una comunidad (p.e., una empresa, un estado o un país). Para un candidato esto supone una gran responsabilidad pero a la vez un gran poder (p.e., fondos, capacidad de cambiar leyes).

Por este motivo, existe la necesidad de comprobar la corrección del proceso de votación y de los resultados, asegurando así que los votos corresponden a las intenciones reales de los votantes. Puesto que debe mantenerse el secreto de voto y el anonimato del votante en todo momento, la verificación puede resultar difícil. A pesar de esto, cualquier sistema de votación debe proporcionar algún tipo de verificación.

Los sistemas de votación tradicionales usan papeletas electorales de papel como soporte para emitir el voto. Actualmente las nuevas tecnologías han propiciado la aparición de los sistemas de votación electrónica o "e-voting", que usan dispositivos electrónicos. Estos sistemas proporcionan ventajas respecto a los sistemas convencionales como una aceleración del proceso de escrutinio o un ahorro de papel con consecuencias económicas, logísticas y ecológicas. Las primeras iniciativas fueron en EE.UU., en 1964, donde se utilizaron tarjetas perforadas y máquinas de recuento, aunque más recientemente se han utilizado escáneres ópticos y técnicas criptográficas.

La aparición de estos nuevos sistemas ha hecho replantear un conjunto de problemáticas, ya conocidas en los sistemas antiguos, para solucionarlas y mejorarlas. Estas viejas problemáticas derivan de la seguridad, como es el caso del secreto de voto, el anonimato del votante, etc.. Éstas afectan directamente el proceso de verificación. Para ello se definen tres tipos de verificación: *individual*, *universal* y *extremo-a-extremo* (del inglés "end-to-end"). El primer tipo, definido desde el punto de vista del votante, permite que éste pueda comprobar que su voto ha sido emitido y contabilizado correctamente. La verificación universal permite comprobar que los votos de las urnas no han sido manipulados y que se han escrutado correctamente. Su objetivo es el de garantizar que el proceso que va desde la emisión del voto hasta el recuento se haya realizado correctamente. En los sistemas tradicionales (basados en papeletas en papel y procesos manuales), se realizan ambos tipos de verificación por medio de un conjunto de procesos manuales. En cambio, para realizar dichas verificaciones en sistemas de *e-voting* es necesaria una combinación de nuevas tecnologías y nuevos procesos. La verificación extremo-a-extremo es un tipo de verificación individual que permite comprobar que el voto ha sido emitido y contado correctamente en cualquier momento de la votación. Su objetivo es el de aumentar la confianza del votante en el sistema y, consecuentemente, en la veracidad e integridad de los resultados electorales. Los nuevos sistemas de votación, a diferencia de los tradicionales, facilitan este tipo de verificación.

Este estudio presenta un análisis de los sistemas de verificación de votaciones electrónicas (SVV de ahora en adelante) y muestra como éstos consiguen alguno de los tres tipos de verificación antes descritos. En particular, se centra el enfoque en los SVVs del tipo presencial, en inglés "poll site", ya que éstos son los más comunes actualmente. No obstante, en los siguientes capítulos, se verá la evolución que sufren los SVVs presenciales hacia el modelo remoto, adoptando modelos intermedios como el presencial-remoto. En este tipo de sistemas, el voto se emite de forma controlada, como en los presenciales, aunque el escrutinio se realiza remotamente, como en el tipo remoto (es decir, en un centro o sitio distinto al de la emisión). Los sistemas incluidos en este trabajo son los más relevantes del mundo comercial y académico de la última década. Por lo tanto, la contribución de éste trabajo es doble: (i) la *definición de un marco de evaluación común* para una justa comparación de todos los sistemas y, (ii) el *estudio y comparación de los sistemas de votación electrónica* más importantes.

Estructura del documento. La siguiente sección introduce los conocimientos necesarios y las bases para entender el estudio. La Sección 3 presenta el marco de evaluación y la Sección 4 el análisis de todos los sistemas de verificación de votación (SVVs) incluidos. La Sección 5 analiza globalmente todos los sistemas, y por último, la Sección 6 presenta las conclusiones finales de este trabajo.

II. Conocimientos Previos

En este estudio se considera que el proceso de votación estándar está compuesto por tres fases: (i) el *registro del votante y su identificación*, (ii) la *emisión de voto* y (iii) el *escrutinio de votos*, dónde todos los votos son contabilizados de manera segura y los resultados son imparciales y públicos. El proceso de votación incluye todos los procedimientos y tecnologías necesarios para confiar en la votación.

II-A. Tipos de Votación

A continuación se presenta la clasificación de los sistemas de votación según el lugar donde el votante emite el voto (Sección II-A1) y la clasificación que realiza la legislación de EE.UU. llamada "HAVA classification"(Sección II-A2) sobre los sistemas de verificación de votaciones (SVVs). Esta última se utilizará más adelante para organizar los sistemas de votación analizados.

II-A1. Clasificación según el entorno: Según el sitio de votación y su entorno inmediato, donde el votante puede ejercer su voto, los sistemas de votación se pueden clasificar en sistemas **presenciales** y **remotos**. Para emitir un voto en el *primer tipo*, los votantes tienen que ir a un sitio dedicado a este propósito (p.e., colegio electoral) y con algún tipo de control físico (entorno controlado). En los *sistemas remotos*, los votantes pueden votar desde un sitio lejano al sitio donde se efectúa el escrutinio. Los ejemplos más importantes son el **voto postal** y el **voto por Internet**.

Recientemente se ha propuesto un nuevo tipo de sistemas que pretende aprovechar las ventajas tanto de los sistemas presenciales como de los remotos; el **presencial remoto**. Este tipo de sistemas permiten emitir el voto en un entorno controlado, aunque su escrutinio se realiza en otro sitio destinado específicamente al recuento seguro y centralizado de todos los votos.

II-A2. Clasificación HAVA: Esta clasificación fue promovida por la *Election Assistance Commission* (EAC), una agencia independiente del Gobierno de EE.UU. creada por *Help America Vote Act* 2002 (HAVA). La agencia EAC definió las *Voluntary Voting System Guidelines* (VVSG) en 2005 [1], que consistían en unas directrices que clasifican los SVVs en cuatro tipos: (i) los **SVVs basados en separación de procesos** tienen una arquitectura modular que separa el sistema en dos procesos diferentes, la generación del voto, y su emisión; (ii) los **SVVs basados en evidencias** registran todas las acciones realizadas por los votantes durante la emisión del voto; (iii) los **SVVs directos o de verificación directa** generan un registro paralelo al del voto que permite la verificación directa del votante, es decir, que el votante no requiera de ninguna tecnología para interpretar el contenido del registro; Finalmente, (iv) los **SVVs basados en criptografía extremo a extremo** usan métodos criptográficos para la construcción de recibos. Éstos permiten a los votantes verificar, sin comprometer su privacidad, que su voto no ha sido modificado.

III. Marco de Evaluación Común

Esta sección establece la clasificación que se utilizará para organizar los sistemas de verificación a estudiar y también define y clasifica las propiedades de éstos. Todo ello constituye el marco común que se usará más adelante para analizar y comparar los SVVs.

III-A. Clasificación de los SVVs

En esta sección se presentan los criterios la clasificación de los SVVs. El **año de** su primera **publicación** es la última propiedad usada para organizarlos.

1. Entre los sistemas **electrónicos** y los **basados en papel**, sólo se consideran los electrónicos. Éstos requieren que el voto esté en formato electrónico en vez de papel.
2. Se usa la *clasificación HAVA* antes mencionada para diferenciar los SVVs en sistemas basados en **separación de procesos**, en **evidencias**, en **criptografía extremo a extremo** (E2E) y **directos**.
3. Se distingue entre sistemas **integrales** e **independientes**. Los primeros son sistemas completos que realizan todo el proceso de votación, incluido el de verificación. En cambio, los independientes están diseñados únicamente para verificar la votación sin estar supeditados a un sistema de votación determinado.

III-B. Propiedades Evaluadas de los SVVs

A continuación se presentan las características consideradas importantes para evaluar los sistemas de verificación. Su clasificación obedece a los aspectos del proceso de votación al que conciernen: *interacción con el usuario*, *seguridad*, *integrabilidad* (con un sistema de votación existente) y *aspectos técnicos*.

Interacción con el usuario. La interacción con el votante determina en gran medida la impresión y la confianza que da el sistema:

1. **Accesibilidad.** Facilidad de uso del sistema (p.e., usuarios con algún tipo de discapacidad).
2. **Impacto de uso.** Complejidad del proceso de emisión de voto comparado con el proceso habitual.
3. **Confiabilidad.** Confianza en el proceso de votación desde el punto de vista de los votantes.

Seguridad. Las propiedades de seguridad están relacionadas con el *votante* y con el *proceso de votación*:

Relacionados con el votante:

4. **Secreto de voto.** El sistema impide que una tercera persona conozca el contenido del voto.
5. **Anonimato.** El sistema impide que se mantenga cualquier relación entre el voto y el votante.

6. **Resistencia a la coacción.** El sistema impide que el votante pueda probar a una tercera persona el contenido de su voto.
7. **Verificación individual.** El sistema permite que el votante pueda comprobar que su voto se ha contabilizado correctamente.

Relacionados con el proceso de votación:

- **Verificación universal.** Ésta se descompone en:
  8. **Integridad de la urna.** Únicamente los votos de votantes autorizados pueden estar en la urna de manera inalterada hasta el final del proceso de votación (antes del escrutinio).
  9. **Precisión del escrutinio.** El escrutinio debe contar todos los votos emitidos de manera correcta no antes del final de la votación.
10. **Auditabilidad.** El sistema de votación electrónica permite a una tercera persona, sin comprometer otras propiedades de seguridad, analizar lo sucedido en las elecciones.

Integración. El SVV, sea integral o independiente, tiene la posibilidad y la efectividad de adaptarse/integrarse con otros sistemas de votación, actuando el SVV de forma independiente (de la misma forma que se realizó en [2]). Se tiene en cuenta la sincronización de las operaciones, especialmente la emisión de votos, entre el sistema de votación y el SVV.

11. **Integración**. Facilidad de implementación/adaptación del sistema evaluado como sistema verificador independiente de otras infraestructuras de votación.
12. **Gestión de la información.** Evalúa cuando el subsistema de emisión de votos de los sistemas de votación y el sistema evaluado garantizan tanto atomicidad de operaciones, como resistencia a fallos (p.e., errores de usuarios, desconexiones de cables).

Aspectos técnicos. Se analiza el rendimiento de los SVVs desde un punto de vista técnico:

13. **Simplicidad.** Cuando el SVV es directo y sencillo.
14. **Disponibilidad.** El votante debe poder emitir su voto sólo cuando se le permita, durante el tiempo establecido para ello, y previniendo que pueda emitir más de un voto (si no está permitido).
15. **Escalabilidad.** El sistema verificador escala computacionalmente.
16. **Flexibilidad.** Esta propiedad evalúa el nivel de libertad que ofrece el sistema verificador (p.e., número de candidatos, modo escritura –"write-in").

Representación. Por simplicidad, a continuación se muestra la notación usada en cada una de las 16 propiedades evaluadas en los sistemas estudiados.

IV. Estudio y Comparación de los SVVs

En esta sección se presentan los SVVs (Sección IV-A), su análisis (Sección IV-B) y el estudio de las sinergias entre los sistemas de votación electrónica y las técnicas criptográficas (Sección IV-C).

Cuadro I
Lista de valores de las propiedades evaluadas.

Interacción con el Usuario	↑ / ↓ / ∼: Buena/Débil/Aceptable.
Seguridad	**S/N/∼**: **S**í/**N**o/Parcialmente.
Integración	**NT**: **N**o existen requisitos **T**écnicos adicionales (en terminales de votación, etc.). **T**: Existen requisitos **T**écnicos adicionales. **NSW**: **N**o existen requisitos **S**oft**W**are adicionales (en terminales de votación, etc.). **SW**: Existen requisitos **S**oft**W**are adicionales.
Gestión de la información	**NA**: **N**o existe **A**tomicidad en las operaciones. **A**: Existe **A**tomicidad en las operaciones. **PD**: Existe **P**érdida de **D**atos. **NPD**: **N**o existe **P**érdida de **D**atos.
Aspectos Técnicos	↑ / ↓: Propiedad Alta/Baja.
En cualquier caso	"N/A": La propiedad no fue considerada por el sistema.

IV-A. Presentación y Clasificación de los SVVs

Por razones de espacio, a continuación se listan brevemente los sistemas de mayor relevancia, y que han estado incluidos en el presente estudio. Para mayor detalle, se invita al lector a visitar las referencias externas indicadas.

Siguiendo la categorización HAVA, en el conjunto de *SVVs basados en separación de procesos* se incluye **Modular Voting Architecture ("Frog")** [3]. En la categoría de *SVVs basados en evidencias* se han estudiado **VVAATT** [4] y **VVVAT** [5]. Finalmente, en el grupo de *SVVs basados en criptografía extremo a extremo* se han analizado **VoteHere** [6], **VoteBox** [7], **Three-Ballot** [8] y **E-valg** [9].

IV-B. Análisis y Evaluación de los SVVs

Para analizar y valorar los SVVs se siguen las propiedades antes descritas en el marco común de evaluación. En la Cuadro III se puede ver el resumen de este análisis.

Interacción con el usuario. Dado que todos los SVVs usan DREs (del inglés "**d**irect **r**ecording **e**lectronic voting terminals") para emitir los votos, todos ellos tienen un cierto grado de **accesibilidad**. No obstante, algunos lo mejoran usando audioguías (VVAATT) o añadiendo otras tecnologías de asistencia (como el ratón o el teclado) (VoteBox y E-valg). En el caso del E-valg, esto ya fue probado en los estudios [2], [10]. En cuanto al **impacto de uso**, sistemas como Frog, VoteBox y Three-Ballot presentan mayor complejidad y un proceso de votación ligeramente más largo. Por ejemplo, en el Frog existe una separación estricta entre los procesos de generación y emisión de voto (a pesar de que un votante pueda traer la papeleta llena de casa); VoteBox permite a los votantes realizar un "immediate ballot challenge" [11], que es una manera de alertar del mal funcionamiento del equipo de emisión e inutilizar el terminal de votación; o Three-Ballot que usa una multi-papeleta compuesta por tres partes. Además, todos ellos incorporan tres técnicas distintas con el fin de incrementar la **confianza** en el sistema: (i) *frogs* (Frog) y *recibos* (VoteHere, VoteBox, Three-Ballot y

E-valg) son elementos tangibles para el votante, (ii) *audio guías* (VVAATT), y *boletines* publicados en Internet (excepto VVAATT).

Seguridad. VVAATT/VVVAT no garantizan la confidencialidad de voto, dado que todas las grabaciones (audio o vídeo) muestran el orden *secuencial* de votación. Además, el equipo de grabación del VVAATT/VVVAT tiene una *protección* muy débil (ya que se accede a menudo) y unas técnicas de *extracción* de información de los registros de grabación poco fiables y lentas. A pesar que este sistema no garantiza el anonimato del votante y *no es fiable* en su conjunto, se ha incluido en el estudio por ser el referente de los sistemas basados en evidencias. A continuación se analizan el resto de sistemas.

Seguridad relacionada con el votante. A excepción de Frog, todos los sistemas usan una infraestructura de clave pública (PKI), la mayoría de ellos ElGamal, para garantizar el **secreto de voto**. Sin embargo, los SVVs usan técnicas muy diferentes para proteger el **anonimato del votante**. Mientras que Frog utiliza un simple algoritmo aleatorio, Three-Ballot separa cada una de las tres partes del voto y las almacena usando sus valores hash. También aparecen técnicas más complejas: mixing (VoteHere), criptografía homomórfica aditiva (VoteBox) o un esquema híbrido (E-valg), que combina criptografía homomórfica multiplicativa con mixing. El uso de esquemas umbral, extendido en gran parte de estos sistemas, previene ataques de seguridad procedentes de partes teóricamente confiables. Por otro lado, los sistemas que utilizan recibos pueden permitir la **coacción** y la **venta de votos**, ya que pueden reflejar la opción de voto en el resguardo. Para solucionar esta problemática se usan los códigos de retorno que impiden adivinar el voto; es el caso de VoteBox, Three-Ballot, E-valg y VoteHere. Sin embargo, este último puede tener un defecto, ya que el votante podría evidenciar su intención de voto dado que dispone del voto cifrado junto con los códigos de retorno [12]. Frog, a pesar de no utilizar recibos, tampoco cumple con dichas propiedades, ya que no asegura el secreto de voto. Además, los sistemas que usan recibos *mejoran* la **verificación individual** a *E2E*.

Seguridad relacionada con el sistema. A excepción de Frog, todos los sistemas garantizan la **integridad de la urna** mediante diferentes tecnologías (como pruebas de conocimiento nulo –*ZKPs*–, firmas digitales o esquemas umbral). Ver el Cuadro II para mayor detalle. VoteHere, VoteBox, Three-Ballot y E-valg avalan la **precisión del escrutinio**. Los sistemas homomórficos hacen un recuento más eficiente que las técnicas de mixing [13], [14]. En cuanto a la **auditabilidad**, Three-Ballot crea unos registros o pistas de auditoría para cualquier operación relacionada con los votantes, aunque ninguna sobre el proceso de recuento. Los sistemas evaluados que ofrecen más prestaciones en éste ámbito son VoteBox y E-valg, ya que usan trazas inmutables. VoteBox construye un sistema de auditoría totalmente distribuido, mientras que E-valg sólo audita los elementos críticos del sistema.

Integración. En general todos los SVVs evaluados tienen alguna dependencia, ya sea de software o hardware (ver Cuadro III para más detalles), para integrarlos en los DREs. Los únicos sistemas que implementan algún tipo de **gestión de datos** son VoteBox y E-valg [2], ya que garantizan la atomicidad del voto, son resistentes a pérdidas, y manipulación de datos.

Cuadro II
TÉCNICAS DE SEGURIDAD USADAS POR LOS SVVS

		Técnicas de Seguridad			
		ZKPs	Firma Digital	Esquema Umbral	Sistema Auditoría
SVV	Frog	No	Sí	No	No
	VoteHere	Sí	Sí	Sí	No
	VoteBox	Sí	Sí	Sí	Sí
	Three-Ballot	No	Sí	No	No
	E-valg	Sí	Sí	Sí	Sí

Aspectos técnicos. VoteBox y Frog son más **complejos** que el resto de sistemas estudiados, puesto que tienen una estructura distribuida –el último debido a la separación de procesos. Sin embargo, VoteBox es el único que estructuralmente proporciona *replicación* de la información sensible, susceptible de ser objeto de algún tipo de ataque. Esta característica otorga al sistema un alto grado de **disponibilidad**. Otra buena propiedad de VoteBox es su **escalabilidad** (debida a su arquitectura), además de un escrutinio rápido de votos (como consecuencia del uso de criptografía homomórfica). VoteBox y E-valg comparten esta propiedad. A pesar de ello, ambos deben abordar el voto presencial remoto con cautela, garantizando la infraestructura necesaria a fin de no sobrecargar el sistema. Finalmente, sólo Frog, VoteHere y E-valg dan **flexibilidad** al tipo votación y al formato del voto. Por el contrario, VoteBox, que usa las propiedades homomórficas *aditivas* de ElGamal, no soporta tipos de elecciones muy complejas. Three-Ballot sólo es adecuado para papeletas formadas por tres partes, a pesar de que el contenido de la papeleta es flexible.

IV-C. Estudio de Tendencias en SVVs

Del análisis anterior se extraen *tres tendencias claras* relativas a los siguientes aspectos: (i) ámbito de votación, (ii) tecnología de la votación y (iii) grado de verificabilidad.

Estudio del ámbito de votación. En este estudio se ha analizado SVVs *presenciales*, y todos ellos usan DREs como terminales de votación. Claramente, los DREs resultan de gran utilidad, puesto que permiten la gestión electrónica de los votos. En este sentido cabe destacar la tendencia existente de migración de sistemas electorales *presenciales* a *presenciales remotos*. Dicha tendencia es consecuencia no sólo de la tecnología, sino también de la evolución natural de las reglas democráticas. A pesar de ello, mientras que VoteBox se *adaptó* para soportar esquemas de voto presenciales remotos, E-valg *fue estructuralmente diseñado* para tal propósito.

Estudio de la tecnología de votación. En este caso se considera la tecnología de votación usada desde la emisión de los votos hasta su escrutinio, por lo que los sistemas VVAATT/VVVAT no se incluyen en este estudio. El objetivo de estas tecnologías es el de proveer seguridad (tales como anonimato, integridad de la urna o precisión del escrutinio). La

tendencia que presentan estas soluciones, de las más simples a las más complejas y fiables, es tal como sigue. Mientras que Frog usa meros algoritmos *aleatorios* en el tratamiento de los votos para garantizar el *anonimato de los votantes*, VoteHere usa técnicas de *mixing* más fiables. VoteBox y Three-Ballot usan criptografía *homomórfica aditiva* (que es computacionalmente intensiva) para garantizar el *anonimato*, a la par que facilitan el *escrutinio*. La tecnología más compleja, pero más flexible y fiable, es la usada por E-valg: el *esquema híbrido*. Dicho esquema se compone de criptografía homomórfica multiplicativa (menos intensiva computacionalmente que la aditiva [13], [14]) y mecanismos de mixing. Claramente, estas tecnologías de votación llegan a un *compromiso* entre (i) garantizar que sean más seguras y fiables, y (ii) asegurar que sean rápidas y eficientes en el uso de recursos. Es claro que esta tendencia desde simples técnicas de aleatoriedad a esquemas híbrido es una consecuencia directa de la continua permeabilidad de los sistemas de votación con respecto a los últimos avances criptográficos.

Estudio de la verificabilidad. Los sistemas analizados se organizan como sigue. (i) Sistemas basados en VVAATT/VVVAT y Frog proveen una verificabilidad deficiente y básica respectivamente de los procesos de votación. Principalmente se centran en garantizar únicamente un cierto grado de verificación individual y desatendiendo la universal y la E2E. (ii) VoteHere y Three-Ballot ofrecen un grado aceptable de verificabilidad (individual, universal y E2E). Finalmente, (iii) E-valg y VoteBox aseguran un buen nivel de verificabilidad, a la vez que definen un sistema de auditoría robusto.

En conclusión, VoteBox y E-valg son las mejores alternativas estudiadas como sistemas de votación. No obstante, E-valg ofrece unas características que lo hacen atractivo. La razón de ello es porque E-valg provee aplicaciones comerciales usadas alrededor del mundo, un alto grado de verificabilidad y una suave transición de sistemas de votación tradicionales a electrónicos, y mejorando así su accesibilidad y facilidad de uso.

Cuadro III
DETALLE DE LAS PROPIEDADES DE LOS SVVS.

				Frog	VVAATT VVVAT	VoteHere	Vote Box	Three-Ballot	E-valg
Interacción con el Usuario	Accesibilidad			→	≀	→	←	N/A	←
	Impacto de Uso			≀	←	←	→	→	←
	Confiabilidad			←	←	←	←	←	←
Seguridad	**Relacionado con el Votante**	Secreto de Voto		N	N	Y	Y	Y	Y
		Anonimato		Y	N	Y	Y	Y	Y
		Resistencia Coacción		N	N	N	Y	Y	Y
		Verificación Individual		≀	N	Y	Y	Y	Y
	Relacionado con la Votación	Verificación Universal	Integridad de la Urna	≀	N	Y	Y	Y	Y
			Precisión Escrutinio	N	N	Y	Y	Y	Y
		Auditabilidad		N	≀	N	Y	Y	Y
Integración	Integración			T/SW	T	SW	T/SW	N/A	N/A
	Gestión de la Información			N/A	NA/PD	N/A	A/NPD	N/A	A/NPD
Aspectos Técnicos	Simplicidad			→	←	←	→	←	←
	Disponibilidad			N/A	N/A	N/A	←	N/A	N/A
	Escalabilidad			→	→	≀	←	≀	←
	Flexibilidad			←	→	←	→	→	←

V. CONCLUSIONES

En este trabajo se ha definido un marco de evaluación, común para todos los sistemas de verificación de votación electrónica (SVVs), y se ha elaborado un estudio comparativo de una selección de dichos sistemas. Para ello se han seguido los siguientes pasos: (i) se ha definido una *clasificación* de SVVs, (ii) se han definido las *propiedades* a estudiar de los SVVs, (iii) se han *elegido y analizado* un conjunto representativo de SVVs tanto del mundo académico como comercial, y finalmente, (iv) se ha hecho un *estudio de tendencias*.

La clasificación de los SVVs se ha hecho combinando varios criterios con el propósito de conseguir una agrupación natural y completa adecuada a nuestro enfoque. No se consideran los sistemas de votación basados en papel. Se usa la clasificación HAVA [1] de EE.UU., que agrupa los SVVs en función del tipo de verificación. Se distingue también si el método de verificación es independiente del sistema de votación o si ha sido desarrollado para un sistema concreto de votación. A pesar de que existen muchas categorizaciones correctas, ésta ha sido la más adecuada para nuestros propósitos.

Las propiedades elegidas para evaluar los SVVs han sido la seguridad del sistema, la confianza del votante, y en menor medida la flexibilidad de voto. Aspectos como el secreto de voto, el anonimato del votante y la precisión de los resultados son sumamente importantes e imprescindibles en unas votaciones. No es menos importante la confianza que deben tener los votantes en el sistema de votación. En una democracia hace falta confiar en ella y en los mecanismos que la sustentan.

Como ya se ha indicado anteriormente, este estudio se ha centrado en sistemas de verificación de elecciones elec-

trónicas. Más concretamente, en los SVVs sin dependencia del papel, dado que los sistemas de votación han evolucionado progresivamente hacia el uso de la tecnología digital y la criptografía. Teniendo en cuenta este subconjunto, se han elegido los sistemas más relevantes.

A partir de este estudio se puede concluir que los SVVs pretenden facilitar el voto a personas sordas mediante audio guías, así como aumentar la seguridad y la confianza del votante en el sistema. Estas últimas con la ayuda técnicas criptográficas, como son (i) el *cifrado* del voto, (ii) la *firma digital* y el *esquema umbral*, (iii) el *mixing* o los *homomorfismos*, (iv) las *ZKPs*, (v) los *códigos de retorno* y *recibos*, y (vi) la *auditoría* del sistema.

El cifrado del voto mediante RSA o ElGamal garantiza el secreto de voto. Con la firma digital y el esquema umbral se protege la autenticidad de los votos y se aumenta el secreto de voto. El mixing o las propiedades homomórficas derivadas de ElGamal sirven para conseguir el anonimato del votante. Este último tiene importantes consecuencias en el sistema, ya que aumenta la eficiencia del escrutinio [13], [14] y reduce la flexibilidad tanto en el tipo como en el formato del voto. En cambio, el uso del mixing proporciona un escrutinio ligeramente más lento [13], [14]. Ambas técnicas tienen sus ventajas y sus inconvenientes, pero las dos necesitan del uso de ZKPs para conseguir una verificación universal (también el anonimato en los que utilizan mixing). La gran mayoría de SVVs utilizan códigos de retorno y recibos para conseguir una verificación individual (E2E), evitar la coacción del votante y a su vez, aumentar la confianza del votante en el sistema. En la actualidad existe la tendencia de auditar, cada vez más, los sistemas informáticos de cualquier tipo por motivos de seguridad. Sólo los SVVs más nuevos auditan todo lo sucedido a lo largo del proceso electoral.

Se puede observar cierta evolución en el uso del mixing y/o de homomorfismos. Los primeros sistemas homomórficos utilizaban las propiedades aditivas. En cambio, sistemas más contemporáneos emplean sus propiedades multiplicativas con el objetivo de aumentar la flexibilidad del voto. Otros sistemas llamados híbridos, aún más recientes, van más allá y combinan el mixing con la criptografía homomórfica multiplicativa para aprovechar las ventajas de ambos, y ganar en eficiencia y flexibilidad.

Los sistemas de votación electrónica actuales, como E-valg y VoteBox, hacen posible el voto *presencial remoto*. Esta posibilidad supone un nuevo paso hacia el voto plenamente *remoto*. De hecho, ya se han realizado experiencias de voto por *Internet*. Se argumenta que la implantación de los *sistemas remotos* facilitaría la realización de consultas, aumentando la participación ciudadana en la toma de decisiones. Por consiguiente acercaría un poco más la democracia a la sociedad. No obstante, la aceptación de estos esquemas dependerá del cumplimiento al mismo tiempo de dos requisitos: ofrecer un elevado nivel de *seguridad* y una gran facilidad de *acceso* a los votantes. En el apartado de la seguridad de la votación remota preocupa especialmente que el entorno de votación no esté supervisado, es decir, no se controla ni la plataforma del votante ni su entorno. Este hecho facilita la posibilidad de la coerción de los votantes y la venta masiva de votos.

AGRADECIMIENTOS

Los autores agradecen las ayudas del MICINN (proyectos eAEGIS TSI2007-65406-C03-01, ARES-CONSOLIDER INGENIO 2010 CSD2007-00004), del Ministerio de Industria, Comercio y Turismo (proyecto TSI-020100-2009-720), y del Govern de la Generalitat de Catalunya (ajuda 2009 SGR 1135). Los autores son responsables de las ideas expresadas en este artículo, que no reflejan necesariamente la posición de la UNESCO ni comprometen a dicha organización.

REFERENCIAS

[1] Election Assistance Commission (USA), "Voluntary voting system guidelines," 2005. Last visit: April 2010. [Online]. Available: http://www.eac.gov/voting%20systems/docs/vvsgvolumei.pdf/attachment_download/file

[2] A. T. Sherman, A. Gangopadhyay, S. H. Holden, G. Karabatis, A. G. Koru, C. M. Law, D. F. Norris, J. Pinkston, A. Sears, and D. Zhang, "An examination of vote verification technologies: findings and experiences from the Maryland study," in *Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop (EVT'06)*. Berkeley, CA, USA: USENIX Association, 2006, pp. 10–10.

[3] S. Bruck, D. Jefferson, and R. Rivest, "A modular voting architecture ("FROGS")," August 2001. [Online]. Available: http://www.vote.caltech.edu/drupal/files/working_paper/vtp_wp3.pdf

[4] T. Selker, "The voter verified audio audit transcript trail," September 2004. Last visit: February 2010. [Online]. Available: http://www.dos.state.pa.us/election_reform/lib/election_reform/VVAATT_CalTech.pdf

[5] E. Cross, G. Rogers, J. McClendon, W. Mitchell, K. Rouse, P. Gupta, P. Williams, I. Mkpong-Ruffin, Y. McMillian, E. Neely, J. Lane, H. Blunt, and J. Gilbert, "Prime III: One machine, one vote for everyone," in *Proceedings of 2007 Voting Competition Conference*, 2007, July.

[6] P. E. Varner, "Vote early, vote often, and VoteHere: A security analysis of VoteHere," Ph.D. dissertation, University of Virginia, March 2001.

[7] D. Sandler, K. Derr, and D. S. Wallach, "Votebox: a tamper-evident, verifiable electronic voting system," in *Proceedings of the 17th conference on Security symposium (SS'08)*. Berkeley, CA, USA: USENIX Association, 2008, pp. 349–364.

[8] A. O. Santin, R. G. Costa, and C. A. Maziero, "A Three-Ballot-based secure electronic voting system," *IEEE Security and Privacy*, vol. 6, no. 3, pp. 14–21, 2008.

[9] Norwegian Ministry of Local Gobernment and Regional Development, "E-vote 2011: Contractor solution specification," December 2009. Last visit: February 2010. [Online]. Available: http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/e_valg_systemlosning/Tilbud_ergogroup/SSA-U_Appendix_2A_Contractor_Solution_Specification.pdf

[10] Norwegian Ministry of Local Gobernment and Regional Development, "E-vote 2011: Accessibility and usability evaluation of e-vote prototypes," November 2009. Last visit: February 2010. [Online]. Available: http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/e_valg_systemlosning/report_evoting_usability_accessibility_eval_nr_iter2_final.pdf

[11] J. Benaloh, "Ballot casting assurance via voter-initiated poll station auditing," in *Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology (EVT'07)*. Berkeley, CA, USA: USENIX Association, 2007, pp. 14–14.

[12] R. Barnes, "VoteHere VHTi: A verifiable e-voting protocol," 2004. Last visit: April 2010. [Online]. Available: http://www.cs.virginia.edu/crab/VoteHere.pdf

[13] K. Peng, R. Aditya, C. Boyd, E. Dawson, and B. Lee, "Multiplicative homomorphic e-voting," in *Proceedings of 5th International Conference on Cryptology in India (INDOCRYPT 2004)*, 2004, pp. 61–72.

[14] K. Peng, "A hybrid e-voting scheme," in *Proceedings of the 5th International Conference on Information Security Practice and Experience (ISPEC '09)*. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 195–206.