Algunas Consideraciones sobre el Voto Electrónico y la Boleta Electrónica

D. Penazzi, N Wolovick

Famaf-Universidad Nacional de Córdoba

Requerimientos Básicos de un sistema de votación

- **Integridad** del voto

Requerimientos Básicos de un sistema de votación

- **Integridad** del voto
- **Privacidad** del voto.

Requerimientos Básicos de un sistema de votación

- **Integridad** del voto
- **Privacidad** del voto. Incluyendo:
  - no coercibilidad del voto:

Requerimientos Básicos de un sistema de votación

- **Integridad** del voto
- **Privacidad** del voto. Incluyendo:
  - no coercibilidad del voto: el elector **no debe poder demostrarle a nadie** como votó, para evitar amenazas o compra de votos.

Requerimientos Básicos de un sistema de votación

- **Integridad** del voto
- **Verificabilidad** de la integridad
- **Privacidad** del voto. Incluyendo:
  - no coercibilidad del voto: el elector **no debe poder demostrarle a nadie** como votó, para evitar amenazas o compra de votos.

Requerimientos Básicos de un sistema de votación

- **Integridad** del voto
- **Verificabilidad** de la integridad
- **Privacidad** del voto. Incluyendo:
  - no coercibilidad del voto: el elector **no debe poder demostrarle a nadie** como votó, para evitar amenazas o compra de votos.
- **Certeza individual de la privacidad**

Problemas Teóricos (para cualquier sistema de votación)

- Privacidad $\Rightarrow$ sistema de votación $\neq$cajero automático

Problemas Teóricos (para cualquier sistema de votación)

- Privacidad $\Rightarrow$ sistema de votación $\neq$cajero automático
- Conflicto :

Problemas Teóricos (para cualquier sistema de votación)

- Privacidad $\Rightarrow$ sistema de votación $\neq$cajero automático
- Conflicto :
  - privacidad $\Rightarrow$ no es deseable guardar mucha información.

Problemas Teóricos (para cualquier sistema de votación)

- Privacidad $\Rightarrow$ sistema de votación $\neq$cajero automático
- Conflicto :
  - privacidad $\Rightarrow$ no es deseable guardar mucha información.
  - verificabilidad de la integridad $\Rightarrow$ se necesitan muchos registros.

Problemas Teóricos (para cualquier sistema de votación)

- Privacidad $\Rightarrow$ sistema de votación $\neq$cajero automático
- Conflicto :
  - privacidad $\Rightarrow$ no es deseable guardar mucha información.
  - verificabilidad de la integridad $\Rightarrow$ se necesitan muchos registros.

Teorema de Hosp y Vora

No existe ningún sistema de votación (electrónico o no) que tenga al mismo tiempo las propiedades de integridad perfecta, verificabilidad perfecta y privacidad perfecta.

Requerimiento Fundamental

Certeza individual de privacidad

El votante debe contar con una garantía razonable de la confidencialidad de su voto. Es decir, poder estar razonablemente seguro que su voto no puede ser revelado de ninguna forma, ni aún contando con su propia colaboración.

Requerimiento Fundamental

Certeza individual de privacidad

El votante debe contar con una garantía razonable de la confidencialidad de su voto. Es decir, poder estar razonablemente seguro que su voto no puede ser revelado de ninguna forma, ni aún contando con su propia colaboración.

Esta seguridad debe ser una seguridad **del votante** en el momento de emisión del voto. En el caso de un sistema que use emisión electrónica del voto, no basta con afirmar “los expertos dijeron”, “la auditoría fue buena”, “el presidente de la compañía asegura”, etc.

Requerimiento Fundamental

Certeza individual de privacidad

El votante debe contar con una garantía razonable de la confidencialidad de su voto. Es decir, poder estar razonablemente seguro que su voto no puede ser revelado de ninguna forma, ni aún contando con su propia colaboración.

Esta seguridad debe ser una seguridad **del votante** en el momento de emisión del voto. En el caso de un sistema que use emisión electrónica del voto, no basta con afirmar “los expertos dijeron”, “la auditoría fue buena”, “el presidente de la compañía asegura”, etc.

- Se debe pensar que el votante y la máquina son "adversarios". (en el sentido de seguridad informática)

Problemas generales con sistemas de Voto Electrónico

- Cualquier programa complejo tendrá inevitablemente bugs.

Problemas generales con sistemas de Voto Electrónico

- Cualquier programa complejo tendrá inevitablemente bugs.
- En el caso del VE, además de los errores, tenemos que lidiar con posibles ataques internos que traten de esconder un fragmento de código malicioso intencional.

Problemas generales con sistemas de Voto Electrónico

- Cualquier programa complejo tendrá inevitablemente bugs.
- En el caso del VE, además de los errores, tenemos que lidiar con posibles ataques internos que traten de esconder un fragmento de código malicioso intencional.
- También se tiene el problema de la escalabilidad de las amenazas:

Problemas generales con sistemas de Voto Electrónico

- Cualquier programa complejo tendrá inevitablemente bugs.
- En el caso del VE, además de los errores, tenemos que lidiar con posibles ataques internos que traten de esconder un fragmento de código malicioso intencional.
- También se tiene el problema de la escalabilidad de las amenazas:
  - En un sistema tradicional, para crear cambios a una escala suficiente para cambiar una elección deben estar involucrados muchos individuos.

Problemas generales con sistemas de Voto Electrónico

- Cualquier programa complejo tendrá inevitablemente bugs.
- En el caso del VE, además de los errores, tenemos que lidiar con posibles ataques internos que traten de esconder un fragmento de código malicioso intencional.
- También se tiene el problema de la escalabilidad de las amenazas:
  - En un sistema tradicional, para crear cambios a una escala suficiente para cambiar una elección deben estar involucrados muchos individuos.
  - En el VE, los individuos necesarios son mucho menos, y un par de líneas de código hábilmente ocultas pueden cambiar cientos de miles de votos.

Voto Electrónico vs "Boleta Electrónica"

- Algunas personas en Argentina definen "voto electrónico" exclusivamente como aquellos sistemas en los cuales tanto la emisión como el conteo de votos se hacen en **una sola máquina**.

Voto Electrónico vs "Boleta Electrónica"

- Algunas personas en Argentina definen "voto electrónico" exclusivamente como aquellos sistemas en los cuales tanto la emisión como el conteo de votos se hacen en **una sola máquina**.
- Estos sistemas a nivel internacional suelen llamarse de **registro directo**.(Direct-Recording Electronic voting machines (DRE).)

Voto Electrónico vs "Boleta Electrónica"

- Algunas personas en Argentina definen "voto electrónico" exclusivamente como aquellos sistemas en los cuales tanto la emisión como el conteo de votos se hacen en **una sola máquina**.
- Estos sistemas a nivel internacional suelen llamarse de **registro directo**.(Direct-Recording Electronic voting machines (DRE).)
- En algunos sistemas de voto electrónico directo se produce algún registro en papel.

Voto Electrónico vs "Boleta Electrónica"

- Algunas personas en Argentina definen "voto electrónico" exclusivamente como aquellos sistemas en los cuales tanto la emisión como el conteo de votos se hacen en **una sola máquina**.
- Estos sistemas a nivel internacional suelen llamarse de **registro directo**.(Direct-Recording Electronic voting machines (DRE).)
- En algunos sistemas de voto electrónico directo se produce algún registro en papel.
- Estos sistemas son llamados internacionalmente como "DRE with VVPAT" es decir, sistemas de registro directo con un "Voter Verified Paper Audit Trail".

Boleta Electrónica

- Algunas personas denominan "boleta electrónica" a un sistema en donde:

Boleta Electrónica

- Algunas personas denominan "boleta electrónica" a un sistema en donde:
  - se separan la generación del voto del conteo del voto

Boleta Electrónica

- Algunas personas denominan "boleta electrónica" a un sistema en donde:
  - se separan la generación del voto del conteo del voto
  - El elector registra su elección en la "boleta", la cual guarda esa elección no sólo en forma impresa sino digital

Boleta Electrónica

- Algunas personas denominan "boleta electrónica" a un sistema en donde:
  - se separan la generación del voto del conteo del voto
  - El elector registra su elección en la "boleta", la cual guarda esa elección no sólo en forma impresa sino digital
  - La boleta es depositada en una urna para ser contada posteriormente en forma electrónica.

Boleta Electrónica

- Algunas personas denominan "boleta electrónica" a un sistema en donde:
  - se separan la generación del voto del conteo del voto
  - El elector registra su elección en la "boleta", la cual guarda esa elección no sólo en forma impresa sino digital
  - La boleta es depositada en una urna para ser contada posteriormente en forma electrónica.
- A nivel internacional estos sistemas suelen ser llamados sistemas **de voto electrónico** de **registro indirecto** (Indirect-Recording Electronic voting machines (IRE)) o también Electronic Ballot Printers (EBP).

Boleta Electrónica

- Algunas personas denominan "boleta electrónica" a un sistema en donde:
  - se separan la generación del voto del conteo del voto
  - El elector registra su elección en la "boleta", la cual guarda esa elección no sólo en forma impresa sino digital
  - La boleta es depositada en una urna para ser contada posteriormente en forma electrónica.
- A nivel internacional estos sistemas suelen ser llamados sistemas **de voto electrónico** de **registro indirecto** (Indirect-Recording Electronic voting machines (IRE)) o también Electronic Ballot Printers (EBP).
- Uno de los primeros que propuso sistemas de este tipo fue Ronald Rivest. (el lo llamó "frogs" por una analogía con un sapito que lleva el voto de un lado a otro)

Ventajas del sistema "Frog" (Boleta Electrónica) sobre DREs

- Separación del proceso de emisión del proceso del conteo $\Rightarrow$:

Ventajas del sistema "Frog" (Boleta Electrónica) sobre DREs

- Separación del proceso de emisión del proceso del conteo $\Rightarrow$:
  - programa complejo que debe mostrar los candidatos, realizar la selección, etc, **separado** de:

Ventajas del sistema "Frog" (Boleta Electrónica) sobre DREs

- Separación del proceso de emisión del proceso del conteo $\Rightarrow$:
  - programa complejo que debe mostrar los candidatos, realizar la selección, etc, **separado** de:
  - programa que cuenta los votos, que puede ser muy simple.

Ventajas del sistema "Frog" (Boleta Electrónica) sobre DREs

- Separación del proceso de emisión del proceso del conteo $\Rightarrow$:
  - programa complejo que debe mostrar los candidatos, realizar la selección, etc, **separado** de:
  - programa que cuenta los votos, que puede ser muy simple.
  - Ademas, programa que emite votos no guarda ningún registro.

Ventajas del sistema "Frog" (Boleta Electrónica) sobre DREs

- Separación del proceso de emisión del proceso del conteo $\Rightarrow$:
  - programa complejo que debe mostrar los candidatos, realizar la selección, etc, **separado** de:
  - programa que cuenta los votos, que puede ser muy simple.
  - Ademas, programa que emite votos no (debería) guarda(r) ningún registro.

Ventajas del sistema "Frog" (Boleta Electrónica) sobre DREs

- Separación del proceso de emisión del proceso del conteo $\Rightarrow$:
  - programa complejo que debe mostrar los candidatos, realizar la selección, etc, **separado** de:
  - programa que cuenta los votos, que puede ser muy simple.
  - Ademas, programa que emite votos no (debería) guarda(r) ningún registro.
- De hecho Rivest sugería que cada partido político tuviera su propio programa de conteo.

Ventajas del sistema "Frog" (Boleta Electrónica) sobre DREs

- Separación del proceso de emisión del proceso del conteo $\Rightarrow$:
  - programa complejo que debe mostrar los candidatos, realizar la selección, etc, **separado** de:
  - programa que cuenta los votos, que puede ser muy simple.
  - Ademas, programa que emite votos no (debería) guarda(r) ningún registro.
- De hecho Rivest sugería que cada partido político tuviera su propio programa de conteo.
- Esto incrementa la integridad y verificabilidad del sistema, respecto de los DREs

Ventajas del sistema "Frog" (Boleta Electrónica) sobre DREs

- Separación del proceso de emisión del proceso del conteo $\Rightarrow$:
  - programa complejo que debe mostrar los candidatos, realizar la selección, etc, **separado** de:
  - programa que cuenta los votos, que puede ser muy simple.
  - Ademas, programa que emite votos no (debería) guarda(r) ningún registro.
- De hecho Rivest sugería que cada partido político tuviera su propio programa de conteo.
- Esto incrementa la integridad y verificabilidad del sistema, respecto de los DREs
- **Privacidad:** puede no mejorar o incluso empeorar este punto respecto de un DRE, si no se implementa bien.

Una ventaja del sistema usado en la ciudad de BsAs sobre el actual

- Una propiedad que es correcta del sistema usado en la ciudad de BsAs es que previene el voto cadena y votos especialmente marcados entregados por algún puntero.

Una ventaja del sistema usado en la ciudad de BsAs sobre el actual

- Una propiedad que es correcta del sistema usado en la ciudad de BsAs es que previene el voto cadena y votos especialmente marcados entregados por algún puntero.
- No es debido **a nada especial electrónico**

Una ventaja del sistema usado en la ciudad de BsAs sobre el actual

- Una propiedad que es correcta del sistema usado en la ciudad de BsAs es que previene el voto cadena y votos especialmente marcados entregados por algún puntero.
- No es debido **a nada especial electrónico**
- Usa un sistema de **troquelado** que es usado en otros lados, por ejemplo en Canadá, para sistemas de votación en papel y que podría ser usado en el sobre de la boleta tradicional.

Una ventaja del sistema usado en la ciudad de BsAs sobre el actual

- Una propiedad que es correcta del sistema usado en la ciudad de BsAs es que previene el voto cadena y votos especialmente marcados entregados por algún puntero.
- No es debido **a nada especial electrónico**
- Usa un sistema de **troquelado** que es usado en otros lados, por ejemplo en Canadá, para sistemas de votación en papel y que podría ser usado en el sobre de la boleta tradicional.
- **El proyecto de ley** no tiene ninguna provisión especial que garantize protección contra este ataque.

Ataques a la privacidad

- En el Congreso se mostraron varias formas de violar la privacidad con el sistema usado en la ciudad de BsAs:

Ataques a la privacidad

- En el Congreso se mostraron varias formas de violar la privacidad con el sistema usado en la ciudad de BsAs:
  - leer con un celular lo grabado en el chip

Ataques a la privacidad

- En el Congreso se mostraron varias formas de violar la privacidad con el sistema usado en la ciudad de BsAs:
  - leer con un celular lo grabado en el chip
  - leer con una radio el voto en el momento de emisión

Ataques a la privacidad

- En el Congreso se mostraron varias formas de violar la privacidad con el sistema usado en la ciudad de BsAs:
  - leer con un celular lo grabado en el chip
  - leer con una radio el voto en el momento de emisión
  - aún sin chip, codificar en la boleta el momento en el cual el voto fue emitido.

Ataques a la privacidad

- En el Congreso se mostraron varias formas de violar la privacidad con el sistema usado en la ciudad de BsAs:
  - leer con un celular lo grabado en el chip
  - leer con una radio el voto en el momento de emisión
  - aún sin chip, codificar en la boleta el momento en el cual el voto fue emitido.
- Los dos primeros problemas se resuelven cifrando el voto, pero:

Ataques a la privacidad

- En el Congreso se mostraron varias formas de violar la privacidad con el sistema usado en la ciudad de BsAs:
  - leer con un celular lo grabado en el chip
  - leer con una radio el voto en el momento de emisión
  - aún sin chip, codificar en la boleta el momento en el cual el voto fue emitido.
- Los dos primeros problemas se resuelven cifrando el voto, pero:
  - se añade la complejidad de mantener las claves seguras, quienes estarán a cargo de ellas, etc.

Ataques a la privacidad

- En el Congreso se mostraron varias formas de violar la privacidad con el sistema usado en la ciudad de BsAs:
  - leer con un celular lo grabado en el chip
  - leer con una radio el voto en el momento de emisión
  - aún sin chip, codificar en la boleta el momento en el cual el voto fue emitido.
- Los dos primeros problemas se resuelven cifrando el voto, pero:
  - se añade la complejidad de mantener las claves seguras, quienes estarán a cargo de ellas, etc.
  - Para poder mantener la propiedad de que el votante pueda comprobar su voto, son necesarias técnicas mas complicadas que enlentecerán el proceso de emisión del voto.

Ataques a la privacidad

- En el Congreso se mostraron varias formas de violar la privacidad con el sistema usado en la ciudad de BsAs:
  - leer con un celular lo grabado en el chip
  - leer con una radio el voto en el momento de emisión
  - aún sin chip, codificar en la boleta el momento en el cual el voto fue emitido.
- Los dos primeros problemas se resuelven cifrando el voto, pero:
  - se añade la complejidad de mantener las claves seguras, quienes estarán a cargo de ellas, etc.
  - Para poder mantener la propiedad de que el votante pueda comprobar su voto, son necesarias técnicas mas complicadas que enlentecerán el proceso de emisión del voto.
  - Algunas de esas técnicas requieren que el votante pueda generar mas de un voto, solo uno de los cuales es depositado en la urna.

Técnicas Avanzadas a nivel mundial

- Desconfiar de máquinas. ("Software independence", "Trust Math")

Técnicas Avanzadas a nivel mundial

- Desconfiar de máquinas. ("Software independence", "Trust Math")
- En general los sistemas son complicados y algunos no pueden ser usados en elecciones masivas por los requerimientos computacionales o porque las complicaciones no escalan adecuadamente.

Técnicas Avanzadas a nivel mundial

- Desconfiar de máquinas. ("Software independence", "Trust Math")
- En general los sistemas son complicados y algunos no pueden ser usados en elecciones masivas por los requerimientos computacionales o porque las complicaciones no escalan adecuadamente.
- Muchos de estos sistemas requerirían votaciones separadas por categorías, que es algo que en Argentina varios no quieren

Técnicas Avanzadas a nivel mundial

- Desconfiar de máquinas. ("Software independence", "Trust Math")
- En general los sistemas son complicados y algunos no pueden ser usados en elecciones masivas por los requerimientos computacionales o porque las complicaciones no escalan adecuadamente.
- Muchos de estos sistemas requerirían votaciones separadas por categorías, que es algo que en Argentina varios no quieren
- Requieren criptografía y no está claro que se puedan explicar al público general en forma adecuada.

Técnicas Avanzadas a nivel mundial

- Desconfiar de máquinas. ("Software independence", "Trust Math")
- En general los sistemas son complicados y algunos no pueden ser usados en elecciones masivas por los requerimientos computacionales o porque las complicaciones no escalan adecuadamente.
- Muchos de estos sistemas requerirían votaciones separadas por categorías, que es algo que en Argentina varios no quieren
- Requieren criptografía y no está claro que se puedan explicar al público general en forma adecuada.
- Es otro problema del VE:

Técnicas Avanzadas a nivel mundial

- Desconfiar de máquinas. ("Software independence", "Trust Math")
- En general los sistemas son complicados y algunos no pueden ser usados en elecciones masivas por los requerimientos computacionales o porque las complicaciones no escalan adecuadamente.
- Muchos de estos sistemas requerirían votaciones separadas por categorías, que es algo que en Argentina varios no quieren
- Requieren criptografía y no está claro que se puedan explicar al público general en forma adecuada.
- Es otro problema del VE:
- No sirve de nada un sistema seguro, rápido, verificable, etc., si **los únicos que lo pueden entender son miembros de una elite técnica**.

Ejemplo: fragmento de parte de uno de los sistemas propuestos

- (Todas las cuentas son en $\mathbb{Z}_p$)
- Peggy elige su candidato m_t, toma r al azar y calcula $(a, b) = (g^r, g^{m_t} y^r)$.
- Para todos los $i \neq t$, Peggy genera numeros d_i, e_i al azar.
- Calcula $(\rho_i, \sigma_i) = (a^{d_i} g^{e_i}, (bg^{-m_i})^{d_i} y^{e_i})$
- Para $i = t$, Peggy genera un w al azar y $(\rho_t, \sigma_t) = (g^w, y^w)$.
- El voto de Peggy es (a, b) y todos los (ρ_i, σ_i).
- Recibido el voto, Victor produce challenge c. Peggy calcula $d_t = c - \sum_{i \neq t} d_i$, $e_t = w - r d_t$ y revela todos los (d_i, e_i) a Victor, quien:
  1. Verifica si $\sum_{i=1}^{n} d_i = c$
  2. Verifica si $\rho_i = a^{d_i} g^{e_i}$ $\forall i$.
  3. Verifica si $\sigma_i = (bg^{-m_i})^{d_i} y^{e_i}$ $\forall i$.

Conclusiones

- ¿Es posible crear un sistema de emisión electrónica del voto razonablemente seguro, entendible, usable en una elección masiva?

Conclusiones

- ¿Es posible crear un sistema de emisión electrónica del voto razonablemente seguro, entendible, usable en una elección masiva?
- Todavía no sabemos, quizas si, quizas no.

Conclusiones

- ¿Es posible crear un sistema de emisión electrónica del voto razonablemente seguro, entendible, usable en una elección masiva?
- Todavía no sabemos, quizas si, quizas no.
- Aún si se pudiera hacer tal sistema, se debe contrastar sus ventajas respecto de otros sistemas.

Conclusiones

- ¿Es posible crear un sistema de emisión electrónica del voto razonablemente seguro, entendible, usable en una elección masiva?
- Todavía no sabemos, quizas si, quizas no.
- Aún si se pudiera hacer tal sistema, se debe contrastar sus ventajas respecto de otros sistemas.
- Ademas, el mejor sistema del mundo no sirve de nada si no funciona el dia de la elección.

Conclusiones

- ¿Es posible crear un sistema de emisión electrónica del voto razonablemente seguro, entendible, usable en una elección masiva?
- Todavía no sabemos, quizas si, quizas no.
- Aún si se pudiera hacer tal sistema, se debe contrastar sus ventajas respecto de otros sistemas.
- Ademas, el mejor sistema del mundo no sirve de nada si no funciona el dia de la elección.
- Esto es inherente a todo sistema de EMISIÓN electrónica del voto. $\Rightarrow$ deben tener plan de contingencia no electrónico.

Conclusiones

- ¿Es posible crear un sistema de emisión electrónica del voto razonablemente seguro, entendible, usable en una elección masiva?
- Todavía no sabemos, quizas si, quizas no.
- Aún si se pudiera hacer tal sistema, se debe contrastar sus ventajas respecto de otros sistemas.
- Ademas, el mejor sistema del mundo no sirve de nada si no funciona el dia de la elección.
- Esto es inherente a todo sistema de EMISIÓN electrónica del voto. $\Rightarrow$ deben tener plan de contingencia no electrónico.
- Sistemas en donde la tecnología es puesta LUEGO de la emisión no son tan problemáticos ante una falla.

Conclusiones

- ¿Es posible crear un sistema de emisión electrónica del voto razonablemente seguro, entendible, usable en una elección masiva?
- Todavía no sabemos, quizas si, quizas no.
- Aún si se pudiera hacer tal sistema, se debe contrastar sus ventajas respecto de otros sistemas.
- Ademas, el mejor sistema del mundo no sirve de nada si no funciona el dia de la elección.
- Esto es inherente a todo sistema de EMISIÓN electrónica del voto. $\Rightarrow$ deben tener plan de contingencia no electrónico.
- Sistemas en donde la tecnología es puesta LUEGO de la emisión no son tan problemáticos ante una falla.
- Si de todos modos se necesitá un sistema de back-up ¿porqué no usarlo directamente y ahorrarnos las complicaciones?