Voto Electrónico, Boleta Electrónica y otras disquisiciones

D. Penazzi

Famaf-Universidad Nacional de Córdoba

Contenidos

Argentina y el voto electrónico

Teorema de Hosp-Vora

Tipos de Voto Electrónico

Sistemas Avanzados

Conclusiones

La hora del Voto Electrónico ha llegado

Ante diversos problemas del sistema de votación argentino, algunas personas promueven el Voto Electrónico (VE) como la gran solución.

Algunos de los Problemas Prácticos del Voto Electrónico

- Cualquier programa complejo tendrá inevitablemente bugs.

Algunos de los Problemas Prácticos del 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.

Algunos de los Problemas Prácticos del 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:

Algunos de los Problemas Prácticos del 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.

Algunos de los Problemas Prácticos del 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.

Ejemplos de Problemas con el Voto Electrónico

- Se cuentan mal los votos.

Ejemplos de Problemas con el Voto Electrónico

- Se cuentan mal los votos.
- Se registran mal los votos. (el elector elige A pero el sistema registra B, o nada).

Ejemplos de Problemas con el Voto Electrónico

- Se cuentan mal los votos.
- Se registran mal los votos. (el elector elige A pero el sistema registra B, o nada).
- Se cuentan múltiples votos para un mismo elector.

Ejemplos de Problemas con el Voto Electrónico

- Se cuentan mal los votos.
- Se registran mal los votos. (el elector elige A pero el sistema registra B, o nada).
- Se cuentan múltiples votos para un mismo elector.
- Se registran votos no emitidos por ninguna persona. (análogo a la “urna embarazada”).

Ejemplos de Problemas con el Voto Electrónico

- Se cuentan mal los votos.
- Se registran mal los votos. (el elector elige A pero el sistema registra B, o nada).
- Se cuentan múltiples votos para un mismo elector.
- Se registran votos no emitidos por ninguna persona. (análogo a la “urna embarazada”).
- Máquinas o software que han sido examinados son reemplazados en la elección por otros que no han sido auditados.

Ejemplos de Problemas con el Voto Electrónico

- Se cuentan mal los votos.
- Se registran mal los votos. (el elector elige A pero el sistema registra B, o nada).
- Se cuentan múltiples votos para un mismo elector.
- Se registran votos no emitidos por ninguna persona. (análogo a la “urna embarazada”).
- Máquinas o software que han sido examinados son reemplazados en la elección por otros que no han sido auditados.
- Se revela el voto de uno o mas electores.

Ejemplos de Problemas con el Voto Electrónico

- Se cuentan mal los votos.
- Se registran mal los votos. (el elector elige A pero el sistema registra B, o nada).
- Se cuentan múltiples votos para un mismo elector.
- Se registran votos no emitidos por ninguna persona. (análogo a la “urna embarazada”).
- Máquinas o software que han sido examinados son reemplazados en la elección por otros que no han sido auditados.
- Se revela el voto de uno o mas electores.
- Y en realidad todo esto no es el mayor problema con el Voto Electrónico (mas adelante explicaremos)

EEUU

Cientos de errores en diversos estados. Algunos destacados:

- 2003: Boone County, Iowa: sobre 50.000 votantes registrados, el equipo electrónico contó 140.000 votos.

EEUU

Cientos de errores en diversos estados. Algunos destacados:

- 2003: Boone County, Iowa: sobre 50.000 votantes registrados, el equipo electrónico contó 140.000 votos.
- 2007: California: se descertificaron todas las maquinas de votación electrónicas por considerarse inseguras.

EEUU

Cientos de errores en diversos estados. Algunos destacados:

- 2003: Boone County, Iowa: sobre 50.000 votantes registrados, el equipo electrónico contó 140.000 votos.
- 2007: California: se descertificaron todas las maquinas de votación electrónicas por considerarse inseguras.
- 2007 “no system used in Ohio is without significant and serious risks to voting integrity"(Secretario de Estado)

EEUU

Cientos de errores en diversos estados. Algunos destacados:

- 2003: Boone County, Iowa: sobre 50.000 votantes registrados, el equipo electrónico contó 140.000 votos.
- 2007: California: se descertificaron todas las maquinas de votación electrónicas por considerarse inseguras.
- 2007 “no system used in Ohio is without significant and serious risks to voting integrity"(Secretario de Estado)
- 2015: el sistema AVS WinVote:

EEUU

Cientos de errores en diversos estados. Algunos destacados:

- 2003: Boone County, Iowa: sobre 50.000 votantes registrados, el equipo electrónico contó 140.000 votos.
- 2007: California: se descertificaron todas las maquinas de votación electrónicas por considerarse inseguras.
- 2007 “no system used in Ohio is without significant and serious risks to voting integrity"(Secretario de Estado)
- 2015: el sistema AVS WinVote:
  - Tiene password débiles que no pueden ser cambiadas

EEUU

Cientos de errores en diversos estados. Algunos destacados:

- 2003: Boone County, Iowa: sobre 50.000 votantes registrados, el equipo electrónico contó 140.000 votos.
- 2007: California: se descertificaron todas las maquinas de votación electrónicas por considerarse inseguras.
- 2007 “no system used in Ohio is without significant and serious risks to voting integrity"(Secretario de Estado)
- 2015: el sistema AVS WinVote:
  - Tiene password débiles que no pueden ser cambiadas
  - Usa Wired Equivalent Privacy (WEP) (mostrado inseguro en 2001 y reemplazado por WPA desde 2003).

EEUU

Cientos de errores en diversos estados. Algunos destacados:

- 2003: Boone County, Iowa: sobre 50.000 votantes registrados, el equipo electrónico contó 140.000 votos.
- 2007: California: se descertificaron todas las maquinas de votación electrónicas por considerarse inseguras.
- 2007 “no system used in Ohio is without significant and serious risks to voting integrity"(Secretario de Estado)
- 2015: el sistema AVS WinVote:
  - Tiene password débiles que no pueden ser cambiadas
  - Usa Wired Equivalent Privacy (WEP) (mostrado inseguro en 2001 y reemplazado por WPA desde 2003).
  - Usa una versión de Windows XP Embedded que no ha sido patcheada desde 2004.

EEUU

Cientos de errores en diversos estados. Algunos destacados:

- 2003: Boone County, Iowa: sobre 50.000 votantes registrados, el equipo electrónico contó 140.000 votos.
- 2007: California: se descertificaron todas las maquinas de votación electrónicas por considerarse inseguras.
- 2007 “no system used in Ohio is without significant and serious risks to voting integrity"(Secretario de Estado)
- 2015: el sistema AVS WinVote:
  - Tiene password débiles que no pueden ser cambiadas
  - Usa Wired Equivalent Privacy (WEP) (mostrado inseguro en 2001 y reemplazado por WPA desde 2003).
  - Usa una versión de Windows XP Embedded que no ha sido patcheada desde 2004.
- 2000: Volusia County, Florida: Gore recibió -16.022 votos.

EEUU

Cientos de errores en diversos estados. Algunos destacados:

- 2003: Boone County, Iowa: sobre 50.000 votantes registrados, el equipo electrónico contó 140.000 votos.
- 2007: California: se descertificaron todas las maquinas de votación electrónicas por considerarse inseguras.
- 2007 “no system used in Ohio is without significant and serious risks to voting integrity"(Secretario de Estado)
- 2015: el sistema AVS WinVote:
  - Tiene password débiles que no pueden ser cambiadas
  - Usa Wired Equivalent Privacy (WEP) (mostrado inseguro en 2001 y reemplazado por WPA desde 2003).
  - Usa una versión de Windows XP Embedded que no ha sido patcheada desde 2004.
- 2000: Volusia County, Florida: Gore recibió —-16.022

Brasil

- Falla en la protección del secreto del voto:

Brasil

- Falla en la protección del secreto del voto:
  - Se puede saber quien votó a quien por una mala implementación del mecanismo de aleatoriedad que supuestamente oculta el orden en el cual los votos fueron emitidos por los votantes.

Brasil

- Falla en la protección del secreto del voto:
  - Se puede saber quien votó a quien por una mala implementación del mecanismo de aleatoriedad que supuestamente oculta el orden en el cual los votos fueron emitidos por los votantes.
  - El sistema de verificación de identidad del votante esta enlazado con la máquina de votación.

Brasil

- Falla en la protección del secreto del voto:
  - Se puede saber quien votó a quien por una mala implementación del mecanismo de aleatoriedad que supuestamente oculta el orden en el cual los votos fueron emitidos por los votantes.
  - El sistema de verificación de identidad del votante esta enlazado con la máquina de votación.
- Uso de algoritmos criptográficos obsoletos.

Brasil

- Falla en la protección del secreto del voto:
  - Se puede saber quien votó a quien por una mala implementación del mecanismo de aleatoriedad que supuestamente oculta el orden en el cual los votos fueron emitidos por los votantes.
  - El sistema de verificación de identidad del votante esta enlazado con la máquina de votación.
- Uso de algoritmos criptográficos obsoletos.
- Vulnerables a amenazas internas.

Brasil

- Falla en la protección del secreto del voto:
  - Se puede saber quien votó a quien por una mala implementación del mecanismo de aleatoriedad que supuestamente oculta el orden en el cual los votos fueron emitidos por los votantes.
  - El sistema de verificación de identidad del votante esta enlazado con la máquina de votación.
- Uso de algoritmos criptográficos obsoletos.
- Vulnerables a amenazas internas.
- Falla en el uso de mecanismos de cifrado.

Otros paises

Alemania los sistemas usados hasta ese momento se declararon inconstitucionales.

Otros paises

Alemania los sistemas usados hasta ese momento se declararon inconstitucionales.

Holanda dejó de usarse en 2007 al probarse que los votos podian ser leidos (en algunas máquinas) a varios metros de distancia usando *Van Eck Phreaking* (lectura a distancia del monitor captando las radiaciones electromágneticas de la pantalla), y que los programas podían ser alterados (en las otras máquinas).

Otros paises

Alemania los sistemas usados hasta ese momento se declararon inconstitucionales.

Holanda dejó de usarse en 2007 al probarse que los votos podian ser leidos (en algunas máquinas) a varios metros de distancia usando *Van Eck Phreaking* (lectura a distancia del monitor captando las radiaciones electromágneticas de la pantalla), y que los programas podían ser alterados (en las otras máquinas).

India hackers lograron manipular los resultados con un celular.

Otros paises

Alemania los sistemas usados hasta ese momento se declararon inconstitucionales.

Holanda dejó de usarse en 2007 al probarse que los votos podian ser leidos (en algunas máquinas) a varios metros de distancia usando *Van Eck Phreaking* (lectura a distancia del monitor captando las radiaciones electromágneticas de la pantalla), y que los programas podían ser alterados (en las otras máquinas).

India hackers lograron manipular los resultados con un celular.

Irlanda evaluaron un sistema en elecciones piloto y determinaron que no se podía garantizar la integridad de ninguna elección que usara ese sistema. Costo del experimento: 54 millones de euros.

La propuesta Argentina

- Pero, se sostiene que tanto el sistema BUE usado en CABA y Salta, como el marco general propuesto en Diputados, resuelven estos problemas.

La propuesta Argentina

- Pero, se sostiene que tanto el sistema BUE usado en CABA y Salta, como el marco general propuesto en Diputados, resuelven estos problemas.
- Y se dicen cosas tales como:

La propuesta Argentina

- Pero, se sostiene que tanto el sistema BUE usado en CABA y Salta, como el marco general propuesto en Diputados, resuelven estos problemas.
- Y se dicen cosas tales como:
  - “no es voto electrónico, es boleta electrónica"

La propuesta Argentina

- Pero, se sostiene que tanto el sistema BUE usado en CABA y Salta, como el marco general propuesto en Diputados, resuelven estos problemas.
- Y se dicen cosas tales como:
  - “no es voto electrónico, es boleta electrónica"
  - “Sólo es una impresora, no es una computadora"

La propuesta Argentina

- Pero, se sostiene que tanto el sistema BUE usado en CABA y Salta, como el marco general propuesto en Diputados, resuelven estos problemas.
- Y se dicen cosas tales como:
  - “no es voto electrónico, es boleta electrónica"
  - “Sólo es una impresora, no es una computadora"
  - “Se imprime un papel, asi que no hay problemas"

La propuesta Argentina

- Pero, se sostiene que tanto el sistema BUE usado en CABA y Salta, como el marco general propuesto en Diputados, resuelven estos problemas.
- Y se dicen cosas tales como:
  - “no es voto electrónico, es boleta electrónica"
  - “Sólo es una impresora, no es una computadora"
  - “Se imprime un papel, asi que no hay problemas"
  - “El conteo electrónico es sólo para el conteo provisorio, el definitivo se hace con boletas"

La propuesta Argentina

- Pero, se sostiene que tanto el sistema BUE usado en CABA y Salta, como el marco general propuesto en Diputados, resuelven estos problemas.
- Y se dicen cosas tales como:
  - “no es voto electrónico, es boleta electrónica"
  - “Sólo es una impresora, no es una computadora"
  - “Se imprime un papel, asi que no hay problemas"
  - “El conteo electrónico es sólo para el conteo provisorio, el definitivo se hace con boletas"
  - “Si podemos sacar plata de un cajero, ¿porqué no podemos hacer un sistema de VE"?

La propuesta Argentina

- Pero, se sostiene que tanto el sistema BUE usado en CABA y Salta, como el marco general propuesto en Diputados, resuelven estos problemas.
- Y se dicen cosas tales como:
  - “no es voto electrónico, es boleta electrónica"
  - “Sólo es una impresora, no es una computadora"
  - “Se imprime un papel, asi que no hay problemas"
  - “El conteo electrónico es sólo para el conteo provisorio, el definitivo se hace con boletas"
  - “Si podemos sacar plata de un cajero, ¿porqué no podemos hacer un sistema de VE"?
  - “Hay que confiar en la buena fe del Estado".

La propuesta Argentina

- Pero, se sostiene que tanto el sistema BUE usado en CABA y Salta, como el marco general propuesto en Diputados, resuelven estos problemas.
- Y se dicen cosas tales como:
  - “no es voto electrónico, es boleta electrónica"
  - “Sólo es una impresora, no es una computadora"
  - “Se imprime un papel, asi que no hay problemas"
  - “El conteo electrónico es sólo para el conteo provisorio, el definitivo se hace con boletas"
  - “Si podemos sacar plata de un cajero, ¿porqué no podemos hacer un sistema de VE"?
  - “Hay que confiar en la buena fe del Estado".
- Todas mentiras.

Requerimientos Básicos de un sistema de votación

- Los dos objetivos básico de un sistema de votación son:

Requerimientos Básicos de un sistema de votación

- Los dos objetivos básico de un sistema de votación son:
  - Determinar un ganador y:

Requerimientos Básicos de un sistema de votación

- Los dos objetivos básico de un sistema de votación son:
  - Determinar un ganador y:
  - **convencer al perdedor** de que realmente perdió la elección.

Requerimientos Básicos de un sistema de votación

- Los dos objetivos básico de un sistema de votación son:
  - Determinar un ganador y:
  - **convencer al perdedor** de que realmente perdió la elección.
- En cualquier sistema de votación debe garantizarse, entre otras cosas:

Requerimientos Básicos de un sistema de votación

- Los dos objetivos básico de un sistema de votación son:
  - Determinar un ganador y:
  - **convencer al perdedor** de que realmente perdió la elección.
- En cualquier sistema de votación debe garantizarse, entre otras cosas:
  - La **fidelidad** del voto (el resultado final debe reflejar la voluntad de los electores), lo cual se logra con un sistema que sea íntegro (el resultado obtenido es el que debería obtenerse) y verificable (que esto se pueda verificar)

Requerimientos Básicos de un sistema de votación

- Los dos objetivos básico de un sistema de votación son:
  - Determinar un ganador y:
  - **convencer al perdedor** de que realmente perdió la elección.
- En cualquier sistema de votación debe garantizarse, entre otras cosas:
  - La **fidelidad** del voto (el resultado final debe reflejar la voluntad de los electores), lo cual se logra con un sistema que sea íntegro (el resultado obtenido es el que debería obtenerse) y verificable (que esto se pueda verificar)
  - El **secreto** del voto. (privacidad).

Requerimientos Básicos de un sistema de votación

- Los dos objetivos básico de un sistema de votación son:
  - Determinar un ganador y:
  - **convencer al perdedor** de que realmente perdió la elección.
- En cualquier sistema de votación debe garantizarse, entre otras cosas:
  - La **fidelidad** del voto (el resultado final debe reflejar la voluntad de los electores), lo cual se logra con un sistema que sea íntegro (el resultado obtenido es el que debería obtenerse) y verificable (que esto se pueda verificar)
  - El **secreto** del voto. (privacidad). Esto incluye la no coercibilidad del voto.

Requerimientos Básicos de un sistema de votación

- Los dos objetivos básico de un sistema de votación son:
  - Determinar un ganador y:
  - **convencer al perdedor** de que realmente perdió la elección.
- En cualquier sistema de votación debe garantizarse, entre otras cosas:
  - La **fidelidad** del voto (el resultado final debe reflejar la voluntad de los electores), lo cual se logra con un sistema que sea íntegro (el resultado obtenido es el que debería obtenerse) y verificable (que esto se pueda verificar)
  - El **secreto** del voto. (privacidad). Esto incluye la no coercibilidad del voto.Es decir, no basta conque no se pueda averiguar el voto contra la voluntad del elector, sino que no se pueda hacer aún con la colaboración del elector.

Problemas Teóricos (para cualquier sistema de votación)

- El requerimiento de privacidad diferencia un sistema de votación de un cajero automático, donde la identidad del extractor de dinero es conocida, y las transacciones quedan registradas.

Problemas Teóricos (para cualquier sistema de votación)

- El requerimiento de privacidad diferencia un sistema de votación de un cajero automático, donde la identidad del extractor de dinero es conocida, y las transacciones quedan registradas.
- Estos requerimientos conflictúan entre sí pues para preservar la privacidad no es deseable guardar mucha información , pero para garantizar la verificabilidad se necesitan muchos registros.

Problemas Teóricos (para cualquier sistema de votación)

- El requerimiento de privacidad diferencia un sistema de votación de un cajero automático, donde la identidad del extractor de dinero es conocida, y las transacciones quedan registradas.
- Estos requerimientos conflictúan entre sí pues para preservar la privacidad no es deseable guardar mucha información , pero para garantizar la verificabilidad se necesitan muchos registros.
- Veamos un poco mas esto.

Integridad y Verificabilidad

- Dados votos v_i, denotemos por $\vec{V}$ el vector de votos v_i y $\sum(\vec{V})$ al resultado (teórico) de sumar todos los votos y contar cuántos votos fueron para cada candidato.

Integridad y Verificabilidad

- Dados votos v_i, denotemos por $\vec{V}$ el vector de votos v_i y $\sum(\vec{V})$ al resultado (teórico) de sumar todos los votos y contar cuántos votos fueron para cada candidato.
- Por ejemplo, “51234 votos para A, 3456 votos para B", etc.

Integridad y Verificabilidad

- Dados votos v_i, denotemos por $\vec{V}$ el vector de votos v_i y $\sum(\vec{V})$ al resultado (teórico) de sumar todos los votos y contar cuántos votos fueron para cada candidato.
- Por ejemplo, “51234 votos para A, 3456 votos para B", etc.
- Cualquier sistema de votación deberá tener algun algoritmo que tome como entrada $\vec{V}$ y posiblemente algunas otras variables $\vec{X}$, algunas de las cuales pueden ser aleatorias y devuelva una suma de votos. Llamemos *Conteo* a ese algoritmo.

Integridad

Definición

Un sistema tendrá integridad perfecta si $Conteo(\vec{V}, \vec{X}) = \sum(\vec{V}) \; \forall \vec{V}, \vec{X}$.

Integridad

Definición

Un sistema tendrá integridad perfecta si $Conteo(\vec{V}, \vec{X}) = \sum(\vec{V}) \; \forall \vec{V}, \vec{X}$.

- Los sistemas de conteo manual **no** tienen integridad perfecta, por los errores naturales del conteo manual.

Integridad

Definición

Un sistema tendrá integridad perfecta si $Conteo(\vec{V}, \vec{X}) = \sum(\vec{V}) \; \forall \vec{V}, \vec{X}$.

- Los sistemas de conteo manual **no** tienen integridad perfecta, por los errores naturales del conteo manual.
- Los sistemas de conteo electrónico tienen mejor integridad y esta es una de las razones por las cuales se apoya el uso del VE.

Integridad

Definición

Un sistema tendrá integridad perfecta si $Conteo(\vec{V}, \vec{X}) = \sum(\vec{V}) \; \forall \vec{V}, \vec{X}$.

- Los sistemas de conteo manual **no** tienen integridad perfecta, por los errores naturales del conteo manual.
- Los sistemas de conteo electrónico tienen mejor integridad y esta es una de las razones por las cuales se apoya el uso del VE.
- Pero hay que distinguir entre el resultado $Conteo(\vec{V}, \vec{X})$ que se **obtendría** si usaramos *Conteo* del resultado que **efectivamente produce** el sistema.

Verificabilidad

- Denotaremos por $\mathit{ConteoOficial}(\vec{V}, \vec{X})$ al resultado que el sistema realmente produce como output.

Verificabilidad

- Denotaremos por $\mathit{ConteoOficial}(\vec{V}, \vec{X})$ al resultado que el sistema realmente produce como output.
- Sea $R(\vec{V}, \vec{X})$ el conjunto de registros que el sistema produce durante su operación.

Verificabilidad

- Denotaremos por $\mathit{ConteoOficial}(\vec{V}, \vec{X})$ al resultado que el sistema realmente produce como output.
- Sea $R(\vec{V}, \vec{X})$ el conjunto de registros que el sistema produce durante su operación.
- Esto no sólo incluye $\mathit{ConteoOficial}(\vec{V}, \vec{X})$ sino todo otro registro que permita demostrar que el sistema funcionó correctamente.

Verificabilidad

- Denotaremos por $\mathit{ConteoOficial}(\vec{V}, \vec{X})$ al resultado que el sistema realmente produce como output.
- Sea $R(\vec{V}, \vec{X})$ el conjunto de registros que el sistema produce durante su operación.
- Esto no sólo incluye $\mathit{ConteoOficial}(\vec{V}, \vec{X})$ sino todo otro registro que permita demostrar que el sistema funcionó correctamente.

Verificabilidad

- Denotaremos por $\mathit{ConteoOficial}(\vec{V}, \vec{X})$ al resultado que el sistema realmente produce como output.
- Sea $R(\vec{V}, \vec{X})$ el conjunto de registros que el sistema produce durante su operación.
- Esto no sólo incluye $\mathit{ConteoOficial}(\vec{V}, \vec{X})$ sino todo otro registro que permita demostrar que el sistema funcionó correctamente.

Definición

Un sistema tendrá verificabilidad perfecta si $R(V, X)$ permite determinar con certeza si $\mathit{ConteoOficial}(\vec{V}, \vec{X}) = \mathit{Conteo}(\vec{V}, \vec{X})$ o no.

Integridad y Verificabilidad

- Ejemplo: los vendedores de algúnos sistemas de VE proponen una “black box" en la cual entran sólo los votos $\vec{V}$ y sale sólo la suma $\sum(\vec{V})$.

Integridad y Verificabilidad

- Ejemplo: los vendedores de algúnos sistemas de VE proponen una “black box" en la cual entran sólo los votos $\vec{V}$ y sale sólo la suma $\sum(\vec{V})$.
- Como $R(\vec{V}, \vec{X}) = \emptyset$, estos sistemas tienen verificabilidad nula, asi que aún si tuvieran integridad perfecta, no nos interesan.

Integridad y Verificabilidad

- Ejemplo: los vendedores de algúnos sistemas de VE proponen una “black box" en la cual entran sólo los votos $\vec{V}$ y sale sólo la suma $\sum(\vec{V})$.
- Como $R(\vec{V}, \vec{X}) = \emptyset$, estos sistemas tienen verificabilidad nula, asi que aún si tuvieran integridad perfecta, no nos interesan.
- Observar que en la definición de verificabilidad perfecta no se pide que $\mathit{ConteoOficial}(\vec{V}, \vec{X}) = \mathit{Conteo}(\vec{V}, \vec{X})$, sino que esa proposición pueda ser verificada a partir de $R(\vec{V}, \vec{X})$.

Privacidad

- Observemos que el voto nunca es 100% secreto pues $\sum(\vec{V})$ revela ALGUNA información sobre los votos.

Privacidad

- Observemos que el voto nunca es 100% secreto pues $\sum(\vec{V})$ revela ALGUNA información sobre los votos.
- Como ejemplo extremo, si todos los votos son para un mismo candidato, se saben todos los votos.

Privacidad

- Observemos que el voto nunca es 100% secreto pues $\sum(\vec{V})$ revela ALGUNA información sobre los votos.
- Como ejemplo extremo, si todos los votos son para un mismo candidato, se saben todos los votos.

Definición

Se dice que un sistema tiene privacidad perfecta si la ÚNICA información sobre $\vec{V}$ que se puede obtener de los registros del sistema es la información dada por $\sum(\vec{V})$.

El teorema de Hosp y Vora

- Hosp y Vora probaron un teorema que dice lo siguiente:

El teorema de Hosp y Vora

- Hosp y Vora probaron un teorema que dice lo siguiente:

Teorema

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

El teorema de Hosp y Vora

- Hosp y Vora probaron un teorema que dice lo siguiente:

Teorema

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

- (Hosp, Ben, y Poorvi L. Vora. 2008.“An information-theoretic model of voting systems". Mathematical and Computer Modelling 48 (9): 1628-45)

Limitaciones y Utilidad del teorema de Hosp y Vora

- El teorema de Hosp y Vora no habla específicamente del VE, sino de cualquier sistema de votación.

Limitaciones y Utilidad del teorema de Hosp y Vora

- El teorema de Hosp y Vora no habla específicamente del VE, sino de cualquier sistema de votación.
- Ademas, se refiere a los conceptos de integridad, verificabilidad y privacidad perfectas.

Limitaciones y Utilidad del teorema de Hosp y Vora

- El teorema de Hosp y Vora no habla específicamente del VE, sino de cualquier sistema de votación.
- Ademas, se refiere a los conceptos de integridad, verificabilidad y privacidad perfectas.
- Pero en general en la vida nos conformamos con probabilidades bajas aunque no sean cero.

Limitaciones y Utilidad del teorema de Hosp y Vora

- El teorema de Hosp y Vora no habla específicamente del VE, sino de cualquier sistema de votación.
- Ademas, se refiere a los conceptos de integridad, verificabilidad y privacidad perfectas.
- Pero en general en la vida nos conformamos con probabilidades bajas aunque no sean cero.
- Asi que en principio, se podría bypassear las limitaciones de HospVora, aceptando alguna disminución de requerimientos.

Limitaciones y Utilidad del teorema de Hosp y Vora

- El teorema de Hosp y Vora no habla específicamente del VE, sino de cualquier sistema de votación.
- Ademas, se refiere a los conceptos de integridad, verificabilidad y privacidad perfectas.
- Pero en general en la vida nos conformamos con probabilidades bajas aunque no sean cero.
- Asi que en principio, se podría bypassear las limitaciones de HospVora, aceptando alguna disminución de requerimientos.
- Pero pone en evidencia gente que dice cosas como las siguientes:

Declaraciones absurdas

Declaraciones absurdas

- “El sistema es 100% seguro" (ONPE, en Perú).

Declaraciones absurdas

- “El sistema es 100% seguro" (ONPE, en Perú).
- “El sistema no es vulnerable" (el presidente de MSA, sobre Vot.Ar)

Declaraciones absurdas

- “El sistema es 100% seguro" (ONPE, en Perú).
- “El sistema no es vulnerable" (el presidente de MSA, sobre Vot.Ar)
- “El sistema posee una invulnerabilidad..." (creadores del sistema de la UNCuyo)

Declaraciones absurdas

- “El sistema es 100% seguro" (ONPE, en Perú).
- “El sistema no es vulnerable" (el presidente de MSA, sobre Vot.Ar)
- “El sistema posee una invulnerabilidad..." (creadores del sistema de la UNCuyo)
- “El voto e’ inviolable, repito el voto e’ inviolable" (diputado Marcelo Wechsler, en el Congreso de la Nación)

Proceso de votación moderno

- Se pueden distinguir dos etapas en un proceso de votación moderno:

Proceso de votación moderno

- Se pueden distinguir dos etapas en un proceso de votación moderno:

  Creación del voto: el elector selecciona de alguna forma entre las opciones disponibles y “crea" el voto, en algún formato, por ejemplo, seleccionando boletas y colocandolas en un sobre, marcando una boleta única, o interactuando con una máquina

Proceso de votación moderno

- Se pueden distinguir dos etapas en un proceso de votación moderno:

  Creación del voto: el elector selecciona de alguna forma entre las opciones disponibles y “crea" el voto, en algún formato, por ejemplo, seleccionando boletas y colocandolas en un sobre, marcando una boleta única, o interactuando con una máquina

  Conteo de los votos: luego de cerrado el tiempo disponible para votar, se cuentan los votos resguardados.

Definición de Voto Eléctronico.

- Una definición posible es llamar “Voto Electrónico" a cualquier sistema que introduzca computadoras en **alguna** de esas etapas

Definición de Voto Eléctronico.

- Una definición posible es llamar “Voto Electrónico" a cualquier sistema que introduzca computadoras en **alguna** de esas etapas
- Otra definición posible es llamar

Definición de Voto Eléctronico.

- Una definición posible es llamar “Voto Electrónico" a cualquier sistema que introduzca computadoras en **alguna** de esas etapas
- Otra definición posible es llamar
  - “voto electrónico” a sistemas en donde la **emisión** del voto es electrónica.

Definición de Voto Eléctronico.

- Una definición posible es llamar “Voto Electrónico" a cualquier sistema que introduzca computadoras en **alguna** de esas etapas
- Otra definición posible es llamar
  - “voto electrónico” a sistemas en donde la **emisión** del voto es electrónica.
  - Y “conteo electrónico” si las computadoras sólo se usan en el conteo.

Definición de Voto Eléctronico.

- Una definición posible es llamar “Voto Electrónico" a cualquier sistema que introduzca computadoras en **alguna** de esas etapas
- Otra definición posible es llamar
  - “voto electrónico” a sistemas en donde la **emisión** del voto es electrónica.
  - Y “conteo electrónico” si las computadoras sólo se usan en el conteo.
- Esto, a nivel internacional. Algunas personas en Argentina clasifican el sistema propuesto no como “voto electrónico" sino como “boleta electrónica", pero es un sistema en el cual el voto es emitido electrónicamente.

Gran Problema con el voto electrónico

- Se llame como se llame, cualquier sistema en el cual la emisión del voto sea electrónica tiene un problema grave que debe resolver

Gran Problema con el voto electrónico

- Se llame como se llame, cualquier sistema en el cual la emisión del voto sea electrónica tiene un problema grave que debe resolver
- Y es que asi como se pide que la integridad sea verificable, tampoco basta con que se respete la privacidad del elector.

Gran Problema con el voto electrónico

- Se llame como se llame, cualquier sistema en el cual la emisión del voto sea electrónica tiene un problema grave que debe resolver
- Y es que asi como se pide que la integridad sea verificable, tampoco basta con que se respete la privacidad del elector.
- Sino que esta garantía de privacidad debe ser transparente para el elector.

Gran Problema con el voto electrónico

- Se llame como se llame, cualquier sistema en el cual la emisión del voto sea electrónica tiene un problema grave que debe resolver
- Y es que asi como se pide que la integridad sea verificable, tampoco basta con que se respete la privacidad del elector.
- Sino que esta garantía de privacidad debe ser transparente para el elector.
- De lo contrario, ¿cuanta gente va a poder votar libremente si se esparce el rumor de que el gobernador (pej) introdujo código en las máquinas que permitiría vulnerar la privacidad?

Requerimiento Fundamental

Requerimiento Fundamental

El votante debe contar con la certeza de la confidencialidad de su voto. Es decir, poder estar razonablemente seguro que la máquina que lo crea no puede revelarlo de ninguna forma.

Requerimiento Fundamental

Requerimiento Fundamental

El votante debe contar con la certeza de la confidencialidad de su voto. Es decir, poder estar razonablemente seguro que la máquina que lo crea no puede revelarlo de ninguna forma.

Esta seguridad debe ser una seguridad *del votante* en el momento de emisión del voto. No basta con afirmar “los expertos dijeron”, “la auditoría fue buena”, “el presidente de la compañía asegura”, etc.

Requerimiento Fundamental

Requerimiento Fundamental

El votante debe contar con la certeza de la confidencialidad de su voto. Es decir, poder estar razonablemente seguro que la máquina que lo crea no puede revelarlo de ninguna forma.

Esta seguridad debe ser una seguridad *del votante* en el momento de emisión 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, y darle al votante suficientes armas para derrotarla.

DREs y IREs

- En algunos sistemas de Voto Electrónico tanto la emisión como el conteo de votos se hacen en **una sola máquina**.

DREs y IREs

- En algunos sistemas de Voto Electrónico tanto la emisión como el conteo de votos se hacen en **una sola máquina**.
- Estos sistemas suelen llamarse de **registro directo**.(Direct-Recording Electronic voting machines (DRE).)

DREs y IREs

- En algunos sistemas de Voto Electrónico tanto la emisión como el conteo de votos se hacen en **una sola máquina**.
- Estos sistemas suelen llamarse de **registro directo**.(Direct-Recording Electronic voting machines (DRE).)
- Otros sistemas separan físicamente la generación del voto del conteo del voto, permitiendo que el elector realice una creación de un objeto físico que representa su voto (un "token" o "boleta"), la cual es depositada en una urna para ser contada posteriormente, ya sea manual o electrónicamente.

DREs y IREs

- En algunos sistemas de Voto Electrónico tanto la emisión como el conteo de votos se hacen en **una sola máquina**.
- Estos sistemas suelen llamarse de **registro directo**.(Direct-Recording Electronic voting machines (DRE).)
- Otros sistemas separan físicamente la generación del voto del conteo del voto, permitiendo que el elector realice una creación de un objeto físico que representa su voto (un "token" o "boleta"), la cual es depositada en una urna para ser contada posteriormente, ya sea manual o electrónicamente.
- Suelen ser llamados de **registro indirecto** (Indirect-Recording Electronic voting machines (IRE)) o también Electronic Ballot Printers (EBP).

Voto Electrónico vs “Boleta Electrónica"

- Varias personas pretenden restringir la denominación “voto electrónico" a los sistemas de registro directo, mientras que para los sistemas indirectos usan “boleta electrónica."

Voto Electrónico vs “Boleta Electrónica"

- Varias personas pretenden restringir la denominación “voto electrónico" a los sistemas de registro directo, mientras que para los sistemas indirectos usan “boleta electrónica."
- Llamenle hipopótamo azul si quieren, pero “a rose by any other name would smell as sweet"

Voto Electrónico vs “Boleta Electrónica"

- Varias personas pretenden restringir la denominación “voto electrónico" a los sistemas de registro directo, mientras que para los sistemas indirectos usan “boleta electrónica."
- Llamenle hipopótamo azul si quieren, pero “a rose by any other name would smell as sweet"
- Es cierto que algunos argumentos contra los sistemas directos no son válidos para sistemas indirectos, pero eso no significa que estos automáticamente serán buenos.

Voto Electrónico vs “Boleta Electrónica"

- Varias personas pretenden restringir la denominación “voto electrónico" a los sistemas de registro directo, mientras que para los sistemas indirectos usan “boleta electrónica."
- Llamenle hipopótamo azul si quieren, pero “a rose by any other name would smell as sweet"
- Es cierto que algunos argumentos contra los sistemas directos no son válidos para sistemas indirectos, pero eso no significa que estos automáticamente serán buenos.
- Y de todos modos, aunque le llamemos “boleta electrónica" (que en realidad es un mejor nombre que “sistemas de voto electrónico de registro indirecto") el hecho es que:

Voto Electrónico vs “Boleta Electrónica"

- Varias personas pretenden restringir la denominación “voto electrónico" a los sistemas de registro directo, mientras que para los sistemas indirectos usan “boleta electrónica."
- Llamenle hipopótamo azul si quieren, pero “a rose by any other name would smell as sweet"
- Es cierto que algunos argumentos contra los sistemas directos no son válidos para sistemas indirectos, pero eso no significa que estos automáticamente serán buenos.
- Y de todos modos, aunque le llamemos “boleta electrónica" (que en realidad es un mejor nombre que “sistemas de voto electrónico de registro indirecto") el hecho es que:
- $\{\text{sistemas de boleta electrónica}\} \subset \{\text{voto electrónico}\}$.

“VISMSE"

- En Diputados incluso ante ciertas críticas ahora han eliminado la expresión “boleta electrónica", y ahora lo denominan“votación con impresión de sufragio mediante sistema electrónico".

“VISMSE"

- En Diputados incluso ante ciertas críticas ahora han eliminado la expresión “boleta electrónica", y ahora lo denominan“votación con impresión de sufragio mediante sistema electrónico".
- Todo esto puede parecer una discusión semántica sin mucho sentido, excepto que:

“VISMSE"

- En Diputados incluso ante ciertas críticas ahora han eliminado la expresión “boleta electrónica", y ahora lo denominan“votación con impresión de sufragio mediante sistema electrónico".
- Todo esto puede parecer una discusión semántica sin mucho sentido, excepto que:
- Es un intento deliberado de engañar a la población, pues si el sistema usado en CABA se declara como “voto electrónico", fue ilegal que el gobierno de la ciudad lo usara.

“VISMSE"

- En Diputados incluso ante ciertas críticas ahora han eliminado la expresión “boleta electrónica", y ahora lo denominan“votación con impresión de sufragio mediante sistema electrónico".
- Todo esto puede parecer una discusión semántica sin mucho sentido, excepto que:
- Es un intento deliberado de engañar a la población, pues si el sistema usado en CABA se declara como “voto electrónico", fue ilegal que el gobierno de la ciudad lo usara.
- Pero entonces no pueden luego venir a decirnos que tengamos “buena fe en el Estado".

“VISMSE"

- En Diputados incluso ante ciertas críticas ahora han eliminado la expresión “boleta electrónica", y ahora lo denominan“votación con impresión de sufragio mediante sistema electrónico".
- Todo esto puede parecer una discusión semántica sin mucho sentido, excepto que:
- Es un intento deliberado de engañar a la población, pues si el sistema usado en CABA se declara como “voto electrónico", fue ilegal que el gobierno de la ciudad lo usara.
- Pero entonces no pueden luego venir a decirnos que tengamos “buena fe en el Estado".
- Tampoco es cierto que los IRE sean un invento argentino.

DREs vs IREs

- Por otro lado, algunos en el “bando anti-VE" aseguran que el sistema de Argentina es “como el de Venezuela".

DREs vs IREs

- Por otro lado, algunos en el “bando anti-VE" aseguran que el sistema de Argentina es “como el de Venezuela".
- Esto no es correcto.

DREs vs IREs

- Por otro lado, algunos en el “bando anti-VE" aseguran que el sistema de Argentina es “como el de Venezuela".
- Esto no es correcto.
- La característica técnica que distingue los sistemas de registro directo de los indirectos NO ES la emisión o no de una boleta impresa.

DREs vs IREs

- Por otro lado, algunos en el “bando anti-VE" aseguran que el sistema de Argentina es “como el de Venezuela".
- Esto no es correcto.
- La característica técnica que distingue los sistemas de registro directo de los indirectos NO ES la emisión o no de una boleta impresa.
- Algunos sistemas directos imprimen una boleta de papel:

DREs vs IREs

- Por otro lado, algunos en el “bando anti-VE" aseguran que el sistema de Argentina es “como el de Venezuela".
- Esto no es correcto.
- La característica técnica que distingue los sistemas de registro directo de los indirectos NO ES la emisión o no de una boleta impresa.
- Algunos sistemas directos imprimen una boleta de papel:
  - Algunos guardan esa boleta directamente en la misma máquina.

DREs vs IREs

- Por otro lado, algunos en el “bando anti-VE" aseguran que el sistema de Argentina es “como el de Venezuela".
- Esto no es correcto.
- La característica técnica que distingue los sistemas de registro directo de los indirectos NO ES la emisión o no de una boleta impresa.
- Algunos sistemas directos imprimen una boleta de papel:
  - Algunos guardan esa boleta directamente en la misma máquina.
  - otros se la proveen al votante para que la deposite en una urna común.

DREs vs IREs

- Por otro lado, algunos en el “bando anti-VE" aseguran que el sistema de Argentina es “como el de Venezuela".
- Esto no es correcto.
- La característica técnica que distingue los sistemas de registro directo de los indirectos NO ES la emisión o no de una boleta impresa.
- Algunos sistemas directos imprimen una boleta de papel:
  - Algunos guardan esa boleta directamente en la misma máquina.
  - otros se la proveen al votante para que la deposite en una urna común.
- La diferencia fundamental es que en los sistemas de registro directo la máquina que genera el voto lo cuenta

DREs vs IREs

- Por otro lado, algunos en el “bando anti-VE" aseguran que el sistema de Argentina es “como el de Venezuela".
- Esto no es correcto.
- La característica técnica que distingue los sistemas de registro directo de los indirectos NO ES la emisión o no de una boleta impresa.
- Algunos sistemas directos imprimen una boleta de papel:
  - Algunos guardan esa boleta directamente en la misma máquina.
  - otros se la proveen al votante para que la deposite en una urna común.
- La diferencia fundamental es que en los sistemas de registro directo la máquina que genera el voto lo cuenta
- los sistemas indirecto no necesitan guardar ningún dato sobre el voto que generan

Argentina: BUE (Vot.Ar)

- Emisión electónica del voto: la elección del votante es impresa en forma térmica y ademas grabada en un chip RFID.

Argentina: BUE (Vot.Ar)

- Emisión electónica del voto: la elección del votante es impresa en forma térmica y ademas grabada en un chip RFID.
- La boleta se deposita en una urna.

Argentina: BUE (Vot.Ar)

- Emisión electónica del voto: la elección del votante es impresa en forma térmica y ademas grabada en un chip RFID.
- La boleta se deposita en una urna.
- Al final del dia se cuentan electrónicamente, acercando la boleta a un lector RFID.

Argentina: BUE (Vot.Ar)

- Emisión electónica del voto: la elección del votante es impresa en forma térmica y ademas grabada en un chip RFID.
- La boleta se deposita en una urna.
- Al final del dia se cuentan electrónicamente, acercando la boleta a un lector RFID.
- La máquina genera un acta la cual es transmitida electrónicamente.

Argentina: BUE (Vot.Ar)

- Emisión electónica del voto: la elección del votante es impresa en forma térmica y ademas grabada en un chip RFID.
- La boleta se deposita en una urna.
- Al final del dia se cuentan electrónicamente, acercando la boleta a un lector RFID.
- La máquina genera un acta la cual es transmitida electrónicamente.
- Sólo se cuentan a mano los votos que no pudieron ser leidos electrónicamente. (en BsAs, en Salta hubo una auditoría postelección de algunas urnas).

Argentina: BUE (Vot.Ar)

- Al sistema de boleta con chip RFID se le encontraron los siguientes defectos:

Argentina: BUE (Vot.Ar)

- Al sistema de boleta con chip RFID se le encontraron los siguientes defectos:
  - El chip permite individualizar las boletas, pues vienen numerados.

Argentina: BUE (Vot.Ar)

- Al sistema de boleta con chip RFID se le encontraron los siguientes defectos:
  - El chip permite individualizar las boletas, pues vienen numerados.
  - Durante 7 años y varias auditorias no se detectó un error de programación que permitía generar una boleta que contuviera mas de un voto. (al parecer ahora lo corrigieron, gracias a un hacker que advirtió el error).

Argentina: BUE (Vot.Ar)

- Al sistema de boleta con chip RFID se le encontraron los siguientes defectos:
  - El chip permite individualizar las boletas, pues vienen numerados.
  - Durante 7 años y varias auditorias no se detectó un error de programación que permitía generar una boleta que contuviera mas de un voto. (al parecer ahora lo corrigieron, gracias a un hacker que advirtió el error).
  - Puede ser leido por un celular llevado por el votante con solo acercar el celular a la boleta, permitiendo la compra de votos, como fue demostrado ya el año pasado.

Argentina: BUE (Vot.Ar)

- Al sistema de boleta con chip RFID se le encontraron los siguientes defectos:
  - El chip permite individualizar las boletas, pues vienen numerados.
  - Durante 7 años y varias auditorias no se detectó un error de programación que permitía generar una boleta que contuviera mas de un voto. (al parecer ahora lo corrigieron, gracias a un hacker que advirtió el error).
  - Puede ser leido por un celular llevado por el votante con solo acercar el celular a la boleta, permitiendo la compra de votos, como fue demostrado ya el año pasado.
  - Este año esto fue mostrado en la Comisión de Asuntos Constitucionales de Diputados por Javier Smaldone.

Argentina: BUE (Vot.Ar)

- Al sistema de boleta con chip RFID se le encontraron los siguientes defectos:
  - El chip permite individualizar las boletas, pues vienen numerados.
  - Durante 7 años y varias auditorias no se detectó un error de programación que permitía generar una boleta que contuviera mas de un voto. (al parecer ahora lo corrigieron, gracias a un hacker que advirtió el error).
  - Puede ser leido por un celular llevado por el votante con solo acercar el celular a la boleta, permitiendo la compra de votos, como fue demostrado ya el año pasado.
  - Este año esto fue mostrado en la Comisión de Asuntos Constitucionales de Diputados por Javier Smaldone.
  - Con un simple "RFID burner" se pueden quemar los chips sin ser detectados.

Argentina: BUE (Vot.Ar)

- Se hicieron declaraciones tales como:

Argentina: BUE (Vot.Ar)

- Se hicieron declaraciones tales como:
  - “Ponemos un equipo, una máquina absolutamente boba, que no tiene disco rígido, que no tiene memoria, que no tiene capacidad de almacenamiento alguno" (Sergio Angelini, CEO de MSA)

Argentina: BUE (Vot.Ar)

- Se hicieron declaraciones tales como:
  - “Ponemos un equipo, una máquina absolutamente boba, que no tiene disco rígido, que no tiene memoria, que no tiene capacidad de almacenamiento alguno" (Sergio Angelini, CEO de MSA)
  - “No tiene memoria la máquina, porque es una impresora" (Guillermo Montenegro, Ministro de Justicia y Seguridad de CABA)

Argentina: BUE (Vot.Ar)

- Se hicieron declaraciones tales como:
  - “Ponemos un equipo, una máquina absolutamente boba, que no tiene disco rígido, que no tiene memoria, que no tiene capacidad de almacenamiento alguno" (Sergio Angelini, CEO de MSA)
  - “No tiene memoria la máquina, porque es una impresora" (Guillermo Montenegro, Ministro de Justicia y Seguridad de CABA)
- pero la emisora de votos tiene un 2do núcleo de CPU no declarado con suficiente memoria para guardar todos los votos, el cual nunca fue auditado.

Argentina: BUE (Vot.Ar)

- Cualquiera podía acceder a los certificados criptográficos que se iban a usar en la elección, pudiendo de esta forma alterar la transmisión de los resultados.

Argentina: BUE (Vot.Ar)

- Cualquiera podía acceder a los certificados criptográficos que se iban a usar en la elección, pudiendo de esta forma alterar la transmisión de los resultados.
- Joaquin Sorianello avisó de este problema, y MSA en vez de premiarlo lo denunció y le mandó la policia metropolitana.

Argentina: BUE (Vot.Ar)

- Cualquiera podía acceder a los certificados criptográficos que se iban a usar en la elección, pudiendo de esta forma alterar la transmisión de los resultados.
- Joaquin Sorianello avisó de este problema, y MSA en vez de premiarlo lo denunció y le mandó la policia metropolitana.
- Luego de un año, la justicia metropolitana absolvió a Sorianello, y declaro que la seguridad de MSA era “vaga".

Problemas con la propuesta de Diputados

- Ante las críticas al sistema Vot.Ar, ahora se dice que la propuesta de Diputados no indica que necesariamente se usará ese sistema. (esto es correcto).

Problemas con la propuesta de Diputados

- Ante las críticas al sistema Vot.Ar, ahora se dice que la propuesta de Diputados no indica que necesariamente se usará ese sistema. (esto es correcto).
- Los diputados agregaron numerosos cambios al proyecto original del PEN para obtener una mejora en la verificabilidad de la integridad.

Problemas con la propuesta de Diputados

- Ante las críticas al sistema Vot.Ar, ahora se dice que la propuesta de Diputados no indica que necesariamente se usará ese sistema. (esto es correcto).
- Los diputados agregaron numerosos cambios al proyecto original del PEN para obtener una mejora en la verificabilidad de la integridad.
- En la media sanción de diputados se especifica entre otras cosas:

Problemas con la propuesta de Diputados

- Ante las críticas al sistema Vot.Ar, ahora se dice que la propuesta de Diputados no indica que necesariamente se usará ese sistema. (esto es correcto).
- Los diputados agregaron numerosos cambios al proyecto original del PEN para obtener una mejora en la verificabilidad de la integridad.
- En la media sanción de diputados se especifica entre otras cosas:
  - Auditorías previas, posteriores y simultaneas con las elecciones

Problemas con la propuesta de Diputados

- Ante las críticas al sistema Vot.Ar, ahora se dice que la propuesta de Diputados no indica que necesariamente se usará ese sistema. (esto es correcto).
- Los diputados agregaron numerosos cambios al proyecto original del PEN para obtener una mejora en la verificabilidad de la integridad.
- En la media sanción de diputados se especifica entre otras cosas:
  - Auditorías previas, posteriores y simultaneas con las elecciones
  - La posibilidad de que el elector chequee su voto, mirando lo impreso

Problemas con la propuesta de Diputados

- Ante las críticas al sistema Vot.Ar, ahora se dice que la propuesta de Diputados no indica que necesariamente se usará ese sistema. (esto es correcto).
- Los diputados agregaron numerosos cambios al proyecto original del PEN para obtener una mejora en la verificabilidad de la integridad.
- En la media sanción de diputados se especifica entre otras cosas:
  - Auditorías previas, posteriores y simultaneas con las elecciones
  - La posibilidad de que el elector chequee su voto, mirando lo impreso
  - Un doble conteo, tanto manual como electrónico, el dia de la elección.

Problemas con la propuesta de Diputados

- No resolvieron todos los problemas, pero es cierto que hay mucho mas controles que en la versión original.

Problemas con la propuesta de Diputados

- No resolvieron todos los problemas, pero es cierto que hay mucho mas controles que en la versión original.
- Pero si bien mejoraron la verificabilidad de la integridad no hicieron nada respecto de mejorar las fallas que el proyecto tiene respecto de preservar el secreto del voto, ni de las fallas que tiene en no asegurarle al votante tal protección.

Problemas con la propuesta de Diputados

- No resolvieron todos los problemas, pero es cierto que hay mucho mas controles que en la versión original.
- Pero si bien mejoraron la verificabilidad de la integridad no hicieron nada respecto de mejorar las fallas que el proyecto tiene respecto de preservar el secreto del voto, ni de las fallas que tiene en no asegurarle al votante tal protección.
- La media sanción de diputados no especifica cómo será el sistema, por lo que a esta altura no podemos decir cuales serán los problemas concretos.

Problemas con la propuesta de Diputados

- No resolvieron todos los problemas, pero es cierto que hay mucho mas controles que en la versión original.
- Pero si bien mejoraron la verificabilidad de la integridad no hicieron nada respecto de mejorar las fallas que el proyecto tiene respecto de preservar el secreto del voto, ni de las fallas que tiene en no asegurarle al votante tal protección.
- La media sanción de diputados no especifica cómo será el sistema, por lo que a esta altura no podemos decir cuales serán los problemas concretos.
- (algunos abogados sostienen que por esta razón es inconstitucional, pues estaría delegando en el PEN atribuciones del Congreso).

Problemas con la propuesta de Diputados

- Lo que si podemos decir es que varios artículos que se podrían haber incluido para garantizar medidas mínimas de seguridad no fueron incluidos.

Problemas con la propuesta de Diputados

- Lo que si podemos decir es que varios artículos que se podrían haber incluido para garantizar medidas mínimas de seguridad no fueron incluidos.
- Otra vez, esto no significa que el sistema que finalmente proponga el PEN no tenga estas medidas, pero:

Problemas con la propuesta de Diputados

- Lo que si podemos decir es que varios artículos que se podrían haber incluido para garantizar medidas mínimas de seguridad no fueron incluidos.
- Otra vez, esto no significa que el sistema que finalmente proponga el PEN no tenga estas medidas, pero:
  - Por un lado es significativo que rehusaran escribir esos articulos a pesar de las sugerencias explícitas

Problemas con la propuesta de Diputados

- Lo que si podemos decir es que varios artículos que se podrían haber incluido para garantizar medidas mínimas de seguridad no fueron incluidos.
- Otra vez, esto no significa que el sistema que finalmente proponga el PEN no tenga estas medidas, pero:
  - Por un lado es significativo que rehusaran escribir esos articulos a pesar de las sugerencias explícitas
  - Esta ley no caduca automáticamente el 9/12/2019. Aún aquellos que consideran que el gobierno actual es la maravilla mas maravillosa, deberían pensar qué va a pasar cuando otros sean gobierno

Algunas garantías que NO pusieron

- No se específica que la máquina que emita el voto no guarde ninguna información.

Algunas garantías que NO pusieron

- No se específica que la máquina que emita el voto no guarde ninguna información.
- No se específica que las boletas no deben estar numeradas. (en el sistema BUE lo están)

Algunas garantías que NO pusieron

- No se específica que la máquina que emita el voto no guarde ninguna información.
- No se específica que las boletas no deben estar numeradas. (en el sistema BUE lo están)
- No se específica que la máquina emisora y las boletas deben tener protección contra lecturas no autorizadas. (en vez de ello, se penaliza realizar esa acción, lo cual es una admisión que el sistema no tendrá tal protección)

Algunas garantías que NO pusieron

- No se específica que la máquina que emita el voto no guarde ninguna información.
- No se específica que las boletas no deben estar numeradas. (en el sistema BUE lo están)
- No se específica que la máquina emisora y las boletas deben tener protección contra lecturas no autorizadas. (en vez de ello, se penaliza realizar esa acción, lo cual es una admisión que el sistema no tendrá tal protección)
- Se fuerza al elector a emitir el voto en una máquina determinada, sólo pudiendo emitirlo en otra en forma excepcional.

Algunas garantías que NO pusieron

- No se específica que la máquina que emita el voto no guarde ninguna información.
- No se específica que las boletas no deben estar numeradas. (en el sistema BUE lo están)
- No se específica que la máquina emisora y las boletas deben tener protección contra lecturas no autorizadas. (en vez de ello, se penaliza realizar esa acción, lo cual es una admisión que el sistema no tendrá tal protección)
- Se fuerza al elector a emitir el voto en una máquina determinada, sólo pudiendo emitirlo en otra en forma excepcional.
- Si bien se establece el doble conteo, no se dice que hacer si las sumas de estos dos conteos dan distinto.

Otras cosas

- No hay plan B:

Otras cosas

- No hay plan B:
  - Si el sistema falla el dia de la elección en algún lugar, no se lleva a cabo la elección y se repite el proceso en 30 dias.

Otras cosas

- No hay plan B:
  - Si el sistema falla el dia de la elección en algún lugar, no se lleva a cabo la elección y se repite el proceso en 30 dias.
  - Mas grave, la CNE, luego de sólo 30 dias de haber puesto a disposición el sistema a los partidos y algunas universidades, debe “resolver sobre la aprobación" del VISMSE pero no está específicado qué se debe hacer si concluye que no lo aprueba.

Otras cosas

- No hay plan B:
  - Si el sistema falla el dia de la elección en algún lugar, no se lleva a cabo la elección y se repite el proceso en 30 dias.
  - Mas grave, la CNE, luego de sólo 30 dias de haber puesto a disposición el sistema a los partidos y algunas universidades, debe “resolver sobre la aprobación" del VISMSE pero no está específicado qué se debe hacer si concluye que no lo aprueba.
- Si bien se ha hecho mucha propaganda que este sistema “evita el voto cadena", el dictamen aprobado en Diputados **no garantiza esto**, pues no se especificó ningún mecanismo de verificación de que la boleta que el elector deposite en la urna sea la misma que le fue entregada.

Otras cosas

- No hay plan B:
  - Si el sistema falla el dia de la elección en algún lugar, no se lleva a cabo la elección y se repite el proceso en 30 dias.
  - Mas grave, la CNE, luego de sólo 30 dias de haber puesto a disposición el sistema a los partidos y algunas universidades, debe “resolver sobre la aprobación" del VISMSE pero no está específicado qué se debe hacer si concluye que no lo aprueba.
- Si bien se ha hecho mucha propaganda que este sistema “evita el voto cadena", el dictamen aprobado en Diputados **no garantiza esto**, pues no se especificó ningún mecanismo de verificación de que la boleta que el elector deposite en la urna sea la misma que le fue entregada.
- (El sistema BUE usado en Salta y CABA si evita el voto cadena, pues tiene un sistema de troquelado que cumple esa función. Pero los diputados aparentemente se olvidaron de agregarlo en la ley)

Otras cosas

- El proyecto original enviado por el PEN forzaba al elector a depositar en la urna el voto generado por el dispositivo de votación, aún si habia error en la impresión.

Otras cosas

- El proyecto original enviado por el PEN forzaba al elector a depositar en la urna el voto generado por el dispositivo de votación, aún si habia error en la impresión.
- Personalmente argumenté que esto era un error grave. No sé si fue por mi insistencia o por alguna otra causa, pero ahora al menos se le permite al elector desechar el voto si no esta de acuerdo con lo impreso, y pedir una nueva boleta

Otras cosas

- El proyecto original enviado por el PEN forzaba al elector a depositar en la urna el voto generado por el dispositivo de votación, aún si habia error en la impresión.
- Personalmente argumenté que esto era un error grave. No sé si fue por mi insistencia o por alguna otra causa, pero ahora al menos se le permite al elector desechar el voto si no esta de acuerdo con lo impreso, y pedir una nueva boleta
- Aún mejor sería que se le dieran al elector varias boletas, que el o ella pudiera generar diversos votos, destruir todos menos uno, y depositar ese en la urna, pero esto no esta contemplado.

Otras cosas

- El proyecto original enviado por el PEN forzaba al elector a depositar en la urna el voto generado por el dispositivo de votación, aún si habia error en la impresión.
- Personalmente argumenté que esto era un error grave. No sé si fue por mi insistencia o por alguna otra causa, pero ahora al menos se le permite al elector desechar el voto si no esta de acuerdo con lo impreso, y pedir una nueva boleta
- Aún mejor sería que se le dieran al elector varias boletas, que el o ella pudiera generar diversos votos, destruir todos menos uno, y depositar ese en la urna, pero esto no esta contemplado.
- Esta es una forma posible de “engañar" a la máquina emisora del voto para que no pueda saber a quien votamos.

Otras cosas

- El proyecto original enviado por el PEN forzaba al elector a depositar en la urna el voto generado por el dispositivo de votación, aún si habia error en la impresión.
- Personalmente argumenté que esto era un error grave. No sé si fue por mi insistencia o por alguna otra causa, pero ahora al menos se le permite al elector desechar el voto si no esta de acuerdo con lo impreso, y pedir una nueva boleta
- Aún mejor sería que se le dieran al elector varias boletas, que el o ella pudiera generar diversos votos, destruir todos menos uno, y depositar ese en la urna, pero esto no esta contemplado.
- Esta es una forma posible de “engañar" a la máquina emisora del voto para que no pueda saber a quien votamos.
- (aunque sería inútil si las boletas están numeradas)

Real research

- Hay varios sistemas propuestos en la literatura para tratar de resolver los problemas del VE.

Real research

- Hay varios sistemas propuestos en la literatura para tratar de resolver los problemas del VE.
- (Todos estan a años luz del sistema propuesto en Argentina)

Real research

- Hay varios sistemas propuestos en la literatura para tratar de resolver los problemas del VE.
- (Todos estan a años luz del sistema propuesto en Argentina)
- Estos sistemas usan herramientas criptográficas avanzadas.

Real research

- Hay varios sistemas propuestos en la literatura para tratar de resolver los problemas del VE.
- (Todos estan a años luz del sistema propuesto en Argentina)
- Estos sistemas usan herramientas criptográficas avanzadas.
- Veamos algunos conceptos.

Software Independence

Software Independence (Rivest,Wack)

Un sistema de votación electrónico es software-independent si un cambio indetectado en su software no puede producir un cambio indetectado en el resultado de la elección

Software Independence

Software Independence (Rivest,Wack)

Un sistema de votación electrónico es software-independent si un cambio indetectado en su software no puede producir un cambio indetectado en el resultado de la elección

- En la práctica, basta con que la probabilidad de que un cambio indetectado en el software pueda producir un cambio indetectado en el resultado sea lo suficientemente baja.

Software Independence

Software Independence (Rivest,Wack)

Un sistema de votación electrónico es software-independent si un cambio indetectado en su software no puede producir un cambio indetectado en el resultado de la elección

- En la práctica, basta con que la probabilidad de que un cambio indetectado en el software pueda producir un cambio indetectado en el resultado sea lo suficientemente baja.
- Requiere la producción de algún registro que sea verificable por el votante independientemente del software que lo produjo.

Software Independence

Software Independence (Rivest,Wack)

Un sistema de votación electrónico es software-independent si un cambio indetectado en su software no puede producir un cambio indetectado en el resultado de la elección

- En la práctica, basta con que la probabilidad de que un cambio indetectado en el software pueda producir un cambio indetectado en el resultado sea lo suficientemente baja.
- Requiere la producción de algún registro que sea verificable por el votante independientemente del software que lo produjo.
- Suele ir de la mano con Risk Limiting Post Election Audits, que intentan auditar a mano un cierto porcentaje de urnas o votos al azar para comprobar si el conteo fue bien hecho, calculando en base a herramientas probabilísticas cuantas hay que auditar, basandose en los resultados obtenidos.

Cifrado Homomórfico

- En estos sistemas el contador cuenta los votos **sin saber** lo que está contando.

Cifrado Homomórfico

- En estos sistemas el contador cuenta los votos **sin saber** lo que está contando.
- Varios posibles ataques son eliminados.

Cifrado Homomórfico

- En estos sistemas el contador cuenta los votos **sin saber** lo que está contando.
- Varios posibles ataques son eliminados.
- ¿Cómo puede el contador contar sin saber lo que está contando?

Cifrado Homomórfico

- En estos sistemas el contador cuenta los votos **sin saber** lo que está contando.
- Varios posibles ataques son eliminados.
- ¿Cómo puede el contador contar sin saber lo que está contando?

Cifrado Homomórfico Un sistema de cifrado E es homomórfico si $E : (G, +) \mapsto (H, .)$, donde $(G, +)$ y $(H, .)$ son grupos, y

$$E(x + y) = E(x).E(y)$$

Cifrado Homomórfico

- En estos sistemas el contador cuenta los votos **sin saber** lo que está contando.
- Varios posibles ataques son eliminados.
- ¿Cómo puede el contador contar sin saber lo que está contando?

Cifrado Homomórfico Un sistema de cifrado E es homomórfico si $E : (G, +) \mapsto (H, .)$, donde $(G, +)$ y $(H, .)$ son grupos, y

$$E(x + y) = E(x).E(y)$$

- En el caso de voto electrónico, se toman G y H como los residuos módulo algún número muy grande, y $+$ es la suma modular y . es la multiplicación modular.

Cifrado Homomórfico

- Esto permite que el contador **multiplique** los votos encriptados, sin saber cuales son y por lo tanto sin poder cambiarlos intencionalmente de uno a otro.

Cifrado Homomórfico

- Esto permite que el contador **multiplique** los votos encriptados, sin saber cuales son y por lo tanto sin poder cambiarlos intencionalmente de uno a otro.
- Luego de que se multiplicaron todos los votos encriptados, el resultado final se descifra para obtener la suma.

Cifrado Homomórfico

- Esto permite que el contador **multiplique** los votos encriptados, sin saber cuales son y por lo tanto sin poder cambiarlos intencionalmente de uno a otro.
- Luego de que se multiplicaron todos los votos encriptados, el resultado final se descifra para obtener la suma.
- Con algunas técnicas triviales de formateo, esa suma da la suma individual para cada candidato.

El Gamal Exponencial

- Un sistema de cifrado homomórfico es el sistema de El Gamal exponencial.

El Gamal Exponencial

- Un sistema de cifrado homomórfico es el sistema de El Gamal exponencial.
- p, q son primos grandes con $q|(p-1)$ (a veces se requiere $2q = p-1$).

El Gamal Exponencial

- Un sistema de cifrado homomórfico es el sistema de El Gamal exponencial.
- p, q son primos grandes con $q|(p-1)$ (a veces se requiere $2q = p-1$).
- g es generador de un subgrupo grande de $\mathbb{Z}_p - \{0\}$. (en general se toma un $\alpha \neq 0, 1$ y se calcula $g = \alpha^{\frac{p-1}{q}}$. Si no da 1, se usa ese g, si no se toma otro α).

El Gamal Exponencial

- Un sistema de cifrado homomórfico es el sistema de El Gamal exponencial.
- p, q son primos grandes con $q|(p-1)$ (a veces se requiere $2q = p-1$).
- g es generador de un subgrupo grande de $\mathbb{Z}_p - \{0\}$. (en general se toma un $\alpha \neq 0, 1$ y se calcula $g = \alpha^{\frac{p-1}{q}}$. Si no da 1, se usa ese g, si no se toma otro α).
- La clave privada es $x \in \mathbb{Z}_q - \{0, 1\}$

El Gamal Exponencial

- Un sistema de cifrado homomórfico es el sistema de El Gamal exponencial.
- p, q son primos grandes con $q|(p-1)$ (a veces se requiere $2q = p-1$).
- g es generador de un subgrupo grande de $\mathbb{Z}_p - \{0\}$. (en general se toma un $\alpha \neq 0, 1$ y se calcula $g = \alpha^{\frac{p-1}{q}}$. Si no da 1, se usa ese g, si no se toma otro α).
- La clave privada es $x \in \mathbb{Z}_q - \{0, 1\}$
- La clave pública es $h = g^x \mod p$

El Gamal Exponencial

- Un sistema de cifrado homomórfico es el sistema de El Gamal exponencial.
- p, q son primos grandes con $q|(p-1)$ (a veces se requiere $2q = p-1$).
- g es generador de un subgrupo grande de $\mathbb{Z}_p - \{0\}$. (en general se toma un $\alpha \neq 0, 1$ y se calcula $g = \alpha^{\frac{p-1}{q}}$. Si no da 1, se usa ese g, si no se toma otro α).
- La clave privada es $x \in \mathbb{Z}_q - \{0, 1\}$
- La clave pública es $h = g^x \mod p$
- Para cifrar m, generar r al azar, y tomar $E(m) = (g^r, g^m h^r) \mod p$.

El Gamal Exponencial

- Un sistema de cifrado homomórfico es el sistema de El Gamal exponencial.
- p, q son primos grandes con $q|(p-1)$ (a veces se requiere $2q = p-1$).
- g es generador de un subgrupo grande de $\mathbb{Z}_p - \{0\}$. (en general se toma un $\alpha \neq 0, 1$ y se calcula $g = \alpha^{\frac{p-1}{q}}$. Si no da 1, se usa ese g, si no se toma otro α).
- La clave privada es $x \in \mathbb{Z}_q - \{0, 1\}$
- La clave pública es $h = g^x \mod p$
- Para cifrar m, generar r al azar, y tomar $E(m) = (g^r, g^m h^r) \mod p$.
- Para descifrar (a, b) hacer $b(a^x)^{-1} \mod p$, lo cual da $g^m \mod p$, pues (en $\mathbb{Z}_p$):

El Gamal Exponencial

- Un sistema de cifrado homomórfico es el sistema de El Gamal exponencial.
- p, q son primos grandes con $q|(p-1)$ (a veces se requiere $2q = p-1$).
- g es generador de un subgrupo grande de $\mathbb{Z}_p - \{0\}$. (en general se toma un $\alpha \neq 0, 1$ y se calcula $g = \alpha^{\frac{p-1}{q}}$. Si no da 1, se usa ese g, si no se toma otro α).
- La clave privada es $x \in \mathbb{Z}_q - \{0, 1\}$
- La clave pública es $h = g^x \mod p$
- Para cifrar m, generar r al azar, y tomar $E(m) = (g^r, g^m h^r) \mod p$.
- Para descifrar (a, b) hacer $b(a^x)^{-1} \mod p$, lo cual da $g^m \mod p$, pues (en $\mathbb{Z}_p$):
  - $b = g^m h^r = g^m (g^x)^r = g^m (g^r)^x = g^m a^x$

El Gamal Exponencial

- La clave del sistema es que obtener x a partir de g^x (o r a partir de g^r) es dificil si x y r son aleatorios.

El Gamal Exponencial

- La clave del sistema es que obtener x a partir de g^x (o r a partir de g^r) es dificil si x y r son aleatorios.
- Pero entonces ¿cómo calculamos m a partir de g^m?

El Gamal Exponencial

- La clave del sistema es que obtener x a partir de g^x (o r a partir de g^r) es dificil si x y r son aleatorios.
- Pero entonces ¿cómo calculamos m a partir de g^m?
- Si m no es muy grande se puede obtener m a partir de g^m en tiempo $O(\sqrt{m})$.

El Gamal Exponencial

- La clave del sistema es que obtener x a partir de g^x (o r a partir de g^r) es dificil si x y r son aleatorios.
- Pero entonces ¿cómo calculamos m a partir de g^m?
- Si m no es muy grande se puede obtener m a partir de g^m en tiempo $O(\sqrt{m})$.
- De todos modos, esto es una debilidad del sistema de ElGamal Exponencial.

El Gamal Exponencial

- La clave del sistema es que obtener x a partir de g^x (o r a partir de g^r) es dificil si x y r son aleatorios.
- Pero entonces ¿cómo calculamos m a partir de g^m?
- Si m no es muy grande se puede obtener m a partir de g^m en tiempo $O(\sqrt{m})$.
- De todos modos, esto es una debilidad del sistema de ElGamal Exponencial.
- Otro sistema homomórfico que no tiene esta debilidad es el sistema Paillier, pero como es mas complicado explico nada mas que ElGamal.

Desconfiando de la máquina emisora

- Puesto que desconfiamos de la máquina emisora, en algunos papers se sugiere que el voto sea creado por el votante en una máquina independiente.

Desconfiando de la máquina emisora

- Puesto que desconfiamos de la máquina emisora, en algunos papers se sugiere que el voto sea creado por el votante en una máquina independiente.
- Un problema es que el votante podría cifrar cualquier cosa, es decir, traer un voto no válido.

Desconfiando de la máquina emisora

- Puesto que desconfiamos de la máquina emisora, en algunos papers se sugiere que el voto sea creado por el votante en una máquina independiente.
- Un problema es que el votante podría cifrar cualquier cosa, es decir, traer un voto no válido.
- Pero esto se resuelve de varias formas ingeniosas, veamos una:

Desconfiando de la máquina emisora

- Puesto que desconfiamos de la máquina emisora, en algunos papers se sugiere que el voto sea creado por el votante en una máquina independiente.
- Un problema es que el votante podría cifrar cualquier cosa, es decir, traer un voto no válido.
- Pero esto se resuelve de varias formas ingeniosas, veamos una:
- Problema:

Desconfiando de la máquina emisora

- Puesto que desconfiamos de la máquina emisora, en algunos papers se sugiere que el voto sea creado por el votante en una máquina independiente.
- Un problema es que el votante podría cifrar cualquier cosa, es decir, traer un voto no válido.
- Pero esto se resuelve de varias formas ingeniosas, veamos una:
- Problema:
  - Peggy cifra un voto para un candidato extraido de un conjunto $S = \{m_1, ..., m_n\}$.

Desconfiando de la máquina emisora

- Puesto que desconfiamos de la máquina emisora, en algunos papers se sugiere que el voto sea creado por el votante en una máquina independiente.
- Un problema es que el votante podría cifrar cualquier cosa, es decir, traer un voto no válido.
- Pero esto se resuelve de varias formas ingeniosas, veamos una:
- Problema:
  - Peggy cifra un voto para un candidato extraido de un conjunto $S = \{m_1, ..., m_n\}$.
  - Victor quiere verificar que el voto cifrado es realmente el cifrado de algún elemento de S.

Desconfiando de la máquina emisora

- Puesto que desconfiamos de la máquina emisora, en algunos papers se sugiere que el voto sea creado por el votante en una máquina independiente.
- Un problema es que el votante podría cifrar cualquier cosa, es decir, traer un voto no válido.
- Pero esto se resuelve de varias formas ingeniosas, veamos una:
- Problema:
  - Peggy cifra un voto para un candidato extraido de un conjunto $S = \{m_1, ..., m_n\}$.
  - Victor quiere verificar que el voto cifrado es realmente el cifrado de algún elemento de S.
  - Peggy podría probarlo mostrando cual es el cifrado, pero obviamente no quiere hacer eso.

Desconfiando de la máquina emisora

- Puesto que desconfiamos de la máquina emisora, en algunos papers se sugiere que el voto sea creado por el votante en una máquina independiente.
- Un problema es que el votante podría cifrar cualquier cosa, es decir, traer un voto no válido.
- Pero esto se resuelve de varias formas ingeniosas, veamos una:
- Problema:
  - Peggy cifra un voto para un candidato extraido de un conjunto $S = \{m_1, ..., m_n\}$.
  - Victor quiere verificar que el voto cifrado es realmente el cifrado de algún elemento de S.
  - Peggy podría probarlo mostrando cual es el cifrado, pero obviamente no quiere hacer eso.
  - Mas aún, no quiere revelar NADA mas allá del hecho que su cifrado es válido.

Desconfiando de la máquina emisora

- Veamos como se puede hacer esto, tomando como ejemplo el cifrado ElGamal.

Desconfiando de la máquina emisora

- Veamos como se puede hacer esto, tomando como ejemplo el cifrado ElGamal.
- Necesitaremos usar una función de hash criptográfica, que es una función H que, básicamente, toma cadenas de bits de longitud arbitraria y devuelve una cadena de bits de longitud fija b, con las propiedades que

Desconfiando de la máquina emisora

- Veamos como se puede hacer esto, tomando como ejemplo el cifrado ElGamal.
- Necesitaremos usar una función de hash criptográfica, que es una función H que, básicamente, toma cadenas de bits de longitud arbitraria y devuelve una cadena de bits de longitud fija b, con las propiedades que
  - Dado $H(x)$, encontrar x requiere tiempo $O(2^b)$.

Desconfiando de la máquina emisora

- Veamos como se puede hacer esto, tomando como ejemplo el cifrado ElGamal.
- Necesitaremos usar una función de hash criptográfica, que es una función H que, básicamente, toma cadenas de bits de longitud arbitraria y devuelve una cadena de bits de longitud fija b, con las propiedades que
  - Dado $H(x)$, encontrar x requiere tiempo $O(2^b)$.
  - Dado x, encontrar un $y \neq x$ con $H(x) = H(y)$ requiere tiempo $O(2^b)$.

Desconfiando de la máquina emisora

- Veamos como se puede hacer esto, tomando como ejemplo el cifrado ElGamal.
- Necesitaremos usar una función de hash criptográfica, que es una función H que, básicamente, toma cadenas de bits de longitud arbitraria y devuelve una cadena de bits de longitud fija b, con las propiedades que
  - Dado $H(x)$, encontrar x requiere tiempo $O(2^b)$.
  - Dado x, encontrar un $y \neq x$ con $H(x) = H(y)$ requiere tiempo $O(2^b)$.
  - Hallar x, y con $x \neq y$ y $H(x) = H(y)$ requiere tiempo $O(2^{b/2})$

Peggy: generación del voto

- (Todas las cuentas son en $\mathbb{Z}_p$)

Peggy: generación del voto

- (Todas las cuentas son en $\mathbb{Z}_p$)
- El voto de Peggy es de la forma $(a, b) = (g^r, g^{m_t} h^r)$ para algún r y algún t.

Peggy: generación del voto

- (Todas las cuentas son en $\mathbb{Z}_p$)
- El voto de Peggy es de la forma $(a, b) = (g^r, g^{m_t} h^r)$ para algún r y algún t.
- Ademas de esto, Peggy genera un w al azar y $(a_t, b_t) = (g^w, h^w)$.

Peggy: generación del voto

- (Todas las cuentas son en $\mathbb{Z}_p$)
- El voto de Peggy es de la forma $(a, b) = (g^r, g^{m_t} h^r)$ para algún r y algún t.
- Ademas de esto, Peggy genera un w al azar y $(a_t, b_t) = (g^w, h^w)$.
- Y para todos los $i \neq t$, Peggy genera numeros d_i, r_i al azar.

Peggy: generación del voto

- (Todas las cuentas son en $\mathbb{Z}_p$)
- El voto de Peggy es de la forma $(a, b) = (g^r, g^{m_t} h^r)$ para algún r y algún t.
- Ademas de esto, Peggy genera un w al azar y $(a_t, b_t) = (g^w, h^w)$.
- Y para todos los $i \neq t$, Peggy genera numeros d_i, r_i al azar.
- Y calcula $(a_i, b_i) = (a^{d_i} g^{r_i}, (bg^{-m_i})^{d_i} h^{r_i})$

Peggy: generación del voto

- (Todas las cuentas son en $\mathbb{Z}_p$)
- El voto de Peggy es de la forma $(a, b) = (g^r, g^{m_t} h^r)$ para algún r y algún t.
- Ademas de esto, Peggy genera un w al azar y $(a_t, b_t) = (g^w, h^w)$.
- Y para todos los $i \neq t$, Peggy genera numeros d_i, r_i al azar.
- Y calcula $(a_i, b_i) = (a^{d_i} g^{r_i}, (bg^{-m_i})^{d_i} h^{r_i})$
- Calcula $c = H(a_1, b_1, ..., a_n, b_n)$.

Peggy: generación del voto

- (Todas las cuentas son en $\mathbb{Z}_p$)
- El voto de Peggy es de la forma $(a, b) = (g^r, g^{m_t} h^r)$ para algún r y algún t.
- Ademas de esto, Peggy genera un w al azar y $(a_t, b_t) = (g^w, h^w)$.
- Y para todos los $i \neq t$, Peggy genera numeros d_i, r_i al azar.
- Y calcula $(a_i, b_i) = (a^{d_i} g^{r_i}, (bg^{-m_i})^{d_i} h^{r_i})$
- Calcula $c = H(a_1, b_1, ..., a_n, b_n)$.
- Calcula $d_t = c - \sum_{i \neq t} d_i$, $r_t = w - r d_t$.

Peggy: generación del voto

- (Todas las cuentas son en $\mathbb{Z}_p$)
- El voto de Peggy es de la forma $(a, b) = (g^r, g^{m_t} h^r)$ para algún r y algún t.
- Ademas de esto, Peggy genera un w al azar y $(a_t, b_t) = (g^w, h^w)$.
- Y para todos los $i \neq t$, Peggy genera numeros d_i, r_i al azar.
- Y calcula $(a_i, b_i) = (a^{d_i} g^{r_i}, (bg^{-m_i})^{d_i} h^{r_i})$
- Calcula $c = H(a_1, b_1, ..., a_n, b_n)$.
- Calcula $d_t = c - \sum_{i \neq t} d_i$, $r_t = w - r d_t$.
- Su voto contiene (a, b) y ademas todos los a_i, b_i, d_i, r_i y c.

Victor. verificación

1. Verifica si $c = H(a_1, b_1, ..., a_n, b_n)$.

Victor. verificación

1. Verifica si $c = H(a_1, b_1, ..., a_n, b_n)$.
2. Verifica si $\sum_{i=1}^{n} d_i = c$

Victor. verificación

1. Verifica si $c = H(a_1, b_1, ..., a_n, b_n)$.
2. Verifica si $\sum_{i=1}^{n} d_i = c$
3. Verifica si $a_i = a^{d_i} g^{r_i}\ \forall i$.

Victor. verificación

1. Verifica si $c = H(a_1, b_1, ..., a_n, b_n)$.
2. Verifica si $\sum_{i=1}^{n} d_i = c$
3. Verifica si $a_i = a^{d_i} g^{r_i} \ \forall i$.
4. Verifica si $b_i = (bg^{-m_i})^{d_i} h^{r_i} \ \forall i$.

Correctitud

- Si Peggy realmente cifró bien, 3 y 4 son automaticamente ciertas para los $i \neq t$.

Correctitud

- Si Peggy realmente cifró bien, 3 y 4 son automaticamente ciertas para los $i \neq t$.
- Para $i = t$:

Correctitud

- Si Peggy realmente cifró bien, 3 y 4 son automaticamente ciertas para los $i \neq t$.
- Para $i = t$:
  - $a^{d_t} g^{r_t} = (g^r)^{d_t} g^{r_t} = g^{rd_t + r_t} = g^w = a_t$

Correctitud

- Si Peggy realmente cifró bien, 3 y 4 son automaticamente ciertas para los $i \neq t$.
- Para $i = t$:
  - $a^{d_t} g^{r_t} = (g^r)^{d_t} g^{r_t} = g^{rd_t + r_t} = g^w = a_t$
  - $bg^{-m_t} = g^{m_t} h^r g^{-m_t} = h^r$.

Correctitud

- Si Peggy realmente cifró bien, 3 y 4 son automaticamente ciertas para los $i \neq t$.
- Para $i = t$:
  - $a^{d_t} g^{r_t} = (g^r)^{d_t} g^{r_t} = g^{rd_t + r_t} = g^w = a_t$
  - $bg^{-m_t} = g^{m_t} h^r g^{-m_t} = h^r$.
  - $(bg^{-m_t})^{d_t} h^{r_t} = h^{rd_t + r_t} = h^w = b_t$

Correctitud

- Si Peggy realmente cifró bien, 3 y 4 son automaticamente ciertas para los $i \neq t$.
- Para $i = t$:
  - $a^{d_t} g^{r_t} = (g^r)^{d_t} g^{r_t} = g^{rd_t + r_t} = g^w = a_t$
  - $bg^{-m_t} = g^{m_t} h^r g^{-m_t} = h^r$.
  - $(bg^{-m_t})^{d_t} h^{r_t} = h^{rd_t + r_t} = h^w = b_t$
- Peggy no puede crear estos números si no conoce r y t.

Zero Knowledge

- Pero Victor no aprende nada que no pudiera aprender por su cuenta, mas allá de que Peggy cifró bien.

Zero Knowledge

- Pero Victor no aprende nada que no pudiera aprender por su cuenta, mas allá de que Peggy cifró bien.
- Esto pues todos los registros de los a_i, b_i, etc los podría haber generado Victor si eliminamos el requerimiento de que $c = H(a_1, b_1, ..., a_n, b_n)$, por lo que el resto de los registros no revela nada sobre x ni sobre t.

Zero Knowledge

- Pero Victor no aprende nada que no pudiera aprender por su cuenta, mas allá de que Peggy cifró bien.
- Esto pues todos los registros de los a_i, b_i, etc los podría haber generado Victor si eliminamos el requerimiento de que $c = H(a_1, b_1, ..., a_n, b_n)$, por lo que el resto de los registros no revela nada sobre x ni sobre t.
- Simplemente, Victor genera todos los d_i, r_i y calcula todos los a_i, b_i como $a_i = a^{d_i} g^{r_i}$ y $b_i = (bg^{-m_i})^{d_i} h^{r_i}$ y calcula $c = sum_{i=1}^{n} d_i$.

Zero Knowledge

- Pero Victor no aprende nada que no pudiera aprender por su cuenta, mas allá de que Peggy cifró bien.
- Esto pues todos los registros de los a_i, b_i, etc los podría haber generado Victor si eliminamos el requerimiento de que $c = H(a_1, b_1, ..., a_n, b_n)$, por lo que el resto de los registros no revela nada sobre x ni sobre t.
- Simplemente, Victor genera todos los d_i, r_i y calcula todos los a_i, b_i como $a_i = a^{d_i} g^{r_i}$ y $b_i = (bg^{-m_i})^{d_i} h^{r_i}$ y calcula $c = sum_{i=1}^{n} d_i$.
- Pero como en realidad no conoce x ni r ni t, la probabilidad que $c = H(a_1, b_1, ..., a_n, b_n)$ es muy baja.

Mas complicaciones

- Este esquema no es completamente libre de coerción, por lo que hay que complicar aún mas el protocolo.

Mas complicaciones

- Este esquema no es completamente libre de coerción, por lo que hay que complicar aún mas el protocolo.
- Esto muestra otro problema a nivel teórico del VE que tiene que ver con la esencia del proceso democrático.

Mas complicaciones

- Este esquema no es completamente libre de coerción, por lo que hay que complicar aún mas el protocolo.
- Esto muestra otro problema a nivel teórico del VE que tiene que ver con la esencia del proceso democrático.
- No sirve de nada un sistema seguro, rápido, verificable, etc., si **los únicos que lo pueden entender son miembros de una elite técnica**.

Mas complicaciones

- Este esquema no es completamente libre de coerción, por lo que hay que complicar aún mas el protocolo.
- Esto muestra otro problema a nivel teórico del VE que tiene que ver con la esencia del proceso democrático.
- No sirve de nada un sistema seguro, rápido, verificable, etc., si **los únicos que lo pueden entender son miembros de una elite técnica**.
- Pero por su naturaleza misma, eso es lo que suele pasar con el VE.

Mas complicaciones

- Este esquema no es completamente libre de coerción, por lo que hay que complicar aún mas el protocolo.
- Esto muestra otro problema a nivel teórico del VE que tiene que ver con la esencia del proceso democrático.
- No sirve de nada un sistema seguro, rápido, verificable, etc., si **los únicos que lo pueden entender son miembros de una elite técnica**.
- Pero por su naturaleza misma, eso es lo que suele pasar con el VE.
- Por lo tanto hay que agregar elementos que permitan al votante, aún sin entender todos los detalles, estar razonablemente seguro que las partes fundamentales del acto de votar se cumplen.

Mas complicaciones

- Este esquema no es completamente libre de coerción, por lo que hay que complicar aún mas el protocolo.
- Esto muestra otro problema a nivel teórico del VE que tiene que ver con la esencia del proceso democrático.
- No sirve de nada un sistema seguro, rápido, verificable, etc., si **los únicos que lo pueden entender son miembros de una elite técnica**.
- Pero por su naturaleza misma, eso es lo que suele pasar con el VE.
- Por lo tanto hay que agregar elementos que permitan al votante, aún sin entender todos los detalles, estar razonablemente seguro que las partes fundamentales del acto de votar se cumplen.
- Y esto no es fácil de hacer, especialmente si queremos un sistema que tenga la propiedad de usabilidad.

Conclusiones

- ¿Es posible crear un sistema de VE razonablemente seguro, entendible, usable en una elección masiva?

Conclusiones

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

Conclusiones

- ¿Es posible crear un sistema de VE razonablemente seguro, entendible, usable en una elección masiva?
- Todavía no sabemos, quizas si, quizas no.
- El sistema propuesto por Diputados no es tal sistema.

Conclusiones

- ¿Es posible crear un sistema de VE razonablemente seguro, entendible, usable en una elección masiva?
- Todavía no sabemos, quizas si, quizas no.
- El sistema propuesto por Diputados no es tal sistema.
- Aún si se pudiera hacer tal sistema, se debe contrastar sus ventajas respecto de otros sistemas.

Conclusiones

- ¿Es posible crear un sistema de VE razonablemente seguro, entendible, usable en una elección masiva?
- Todavía no sabemos, quizas si, quizas no.
- El sistema propuesto por Diputados no es tal sistema.
- Aún si se pudiera hacer tal sistema, se debe contrastar sus ventajas respecto de otros sistemas.
- Por ejemplo, el sistema de Boleta Única en Papel (BUP).

Conclusiones

- ¿Es posible crear un sistema de VE razonablemente seguro, entendible, usable en una elección masiva?
- Todavía no sabemos, quizas si, quizas no.
- El sistema propuesto por Diputados no es tal sistema.
- Aún si se pudiera hacer tal sistema, se debe contrastar sus ventajas respecto de otros sistemas.
- Por ejemplo, el sistema de Boleta Única en Papel (BUP).
- Dadas las ventajas de la BUP en costos y seguridad, debería ser responsabilidad de los proponentes de un sistema de VE explicar porqué prefieren tal sistema al sistema BUP.

¿Por que no la BUP?

- Bueno, no sé.

¿Por que no la BUP?

- Bueno, no sé.
- Una explicación mas o menos coherente que me han dado es la siguiente:

¿Por que no la BUP?

- Bueno, no sé.
- Una explicación mas o menos coherente que me han dado es la siguiente:
- Los políticos insisten con “Debemos eliminar las boletas sabanas", pero en realidad no quieren esto: quieren el efecto arrastre entre categorias.

¿Por que no la BUP?

- Bueno, no sé.
- Una explicación mas o menos coherente que me han dado es la siguiente:
- Los políticos insisten con “Debemos eliminar las boletas sabanas", pero en realidad no quieren esto: quieren el efecto arrastre entre categorias.
- La BUP tiende a disminuir el efecto arrastre.

¿Por que no la BUP?

- Bueno, no sé.
- Una explicación mas o menos coherente que me han dado es la siguiente:
- Los políticos insisten con “Debemos eliminar las boletas sabanas", pero en realidad no quieren esto: quieren el efecto arrastre entre categorias.
- La BUP tiende a disminuir el efecto arrastre.
- En el proyecto de Diputados la primera opción es “Lista completa"

¿Por que no la BUP?

- Bueno, no sé.
- Una explicación mas o menos coherente que me han dado es la siguiente:
- Los políticos insisten con “Debemos eliminar las boletas sabanas", pero en realidad no quieren esto: quieren el efecto arrastre entre categorias.
- La BUP tiende a disminuir el efecto arrastre.
- En el proyecto de Diputados la primera opción es “Lista completa"
- Y esto parece que gusta.