Experiencias en el desarrollo de sistemas de votaciones electrónicas

Sergio Rajsbaum
Instituto de Matemáticas
Universidad Nacional Autónoma de México

CIBSI 2011
Bucaramanga, Colombia

Resumen

- Desde 2006 se han desarrollado en el IMate-UNAM varios sistemas de votaciones
- Sobre Plone
- Se han usado, con lo que se ha aprendido lo difícil que es tener un sistema útil
- Usando protocolos de votaciones existentes

Meta

- aprender acerca de sistemas de votaciones
- para grupos medianos: 100 a 1000 usuarios
- en comunidades: universidades, asociaciones, etc.
- Existen problemas adicionales en sistemas electorales, de escala, sociales, políticos, etc.

Antecedentes

- En la UNAM se hacen votaciones regularmente, tanto globales como internas a una dependencia, tradicionalmente en papel
- A partir de 2005 se ha trabajado en desarrollar un sistema de información integral sobre Plone: datos personales, CV, actividades académicas.

Objetivo

Implementación de un sistema de votación en un *sistema de administración de contenido* (Plone) usando:

- técnicas modernas de criptografía,
- en un proyecto de software abierto
- que busca lograr un balance entre seguridad, flexibilidad y facilidad de uso

Reto

- Hay más preocupación por que la gente vote que por la seguridad - debe ser muy sencillo para el votante
- flexible - que pueda adaptarse a los requerimientos legales
- Pero seguro- Convencer al perdedor de la validez de la elección

Facilidad

- Se puede votar remotamente, desde cualquier plataforma, en cualquier navegador
- Autenticación sencilla
- Claridad- candidatos, reglas, estado de la elección, resultados, etc.

Flexibilidad

Debe cumplir con la legalidad existente-

Existen diversas votaciones, cada una con sus reglas de tiempos, formas de votar, quien puede votar y quien puede ser candidato

Ejemplos de flexibilidad

Ejemplos de flexibilidad

Quien: "puede votar solamente quien tenga categoría al menos Titular, 3 años de antigüedad, y no tenga un puesto administrativo"

Ejemplos de flexibilidad

Quien: "puede votar solamente quien tenga categoría al menos Titular, 3 años de antigüedad, y no tenga un puesto administrativo"

Tiempos: "el padrón de elegibles y votantes se debe publicar el día 8, 5 días para correcciones, 3 días para aceptar candidatos, 5 días para publicarlos, elección abierta 2 días, ..."

Ejemplos de flexibilidad

Quien: "puede votar solamente quien tenga categoría al menos Titular, 3 años de antigüedad, y no tenga un puesto administrativo"

Tiempos: "el padrón de elegibles y votantes se debe publicar el día 8, 5 días para correcciones, 3 días para aceptar candidatos, 5 días para publicarlos, elección abierta 2 días, ..."

Forma: "cada quien tiene 3 votos y los puede distribuir sobre cualesquiera de los candidatos" o "se debe votar por una pareja de candidatos"

Seguridad - Verificable

requerimientos contradictorios:

- darle a cada votante suficiente información para convencerlo de que su voto ha sido contado correctamente,
- pero no tanta como para que pueda convencer a un tercero de por quien votó

Plone + criptografía

La clave

¿ Por qué Plone ?

1. IMate tiene el sistema con toda la información académica y de
2. autenticación
3. Corre en cualquier plataforma, se accesa desde cualquier navegador
4. abierto, en python
5. seguro
6. poderoso

I. Información académica

- Permite generar padrones de candidatos y votantes, y verificar su correctez:
- “puede votar solamente quien tenga categoría al menos Titular, 3 años de antigüedad, y no tenga un puesto administrativo”

2. Autenticación

- Sistemas típicos requieren de obtener claves para votar de manera complicada, y que cambian con frecuencia
- El sistema existente ya conoce a los usuarios

3. Acceso

- Corre en cualquier plataforma
- acceso remoto- se puede votar desde cualquier sede del IMate, y durante un viaje
- se accesa desde cualquier navegador

4. Proyecto académico

- Desarrollado por estudiantes principalmente
- abierto, desarrollo colaborativo, parte de la comunidad Plone
- Python es un lenguaje bien diseñado
- Harvard, Rice, Penn State, Utah, Yale, Columbia, ACM, etc.

Comunidad

Online

- IRC channel : #plone
- 54 Mailing lists en gmane.org
- Twitter: @plone
- LinkedIn Group

Offline

- 12 sprints en 2007
- 6 conferencias anuales
- 2 symposiums en 2008
- 25 User groups en 11 countries
- Ploneability events

PloneEdu

- “PloneEdu is a global community interested in promoting and supporting the adoption of the Plone open source content management solutions for all levels and types of educational uses”
- weblion.psu.edu/ploneedu/community/
- hemos colaborado en CV y Datos personales

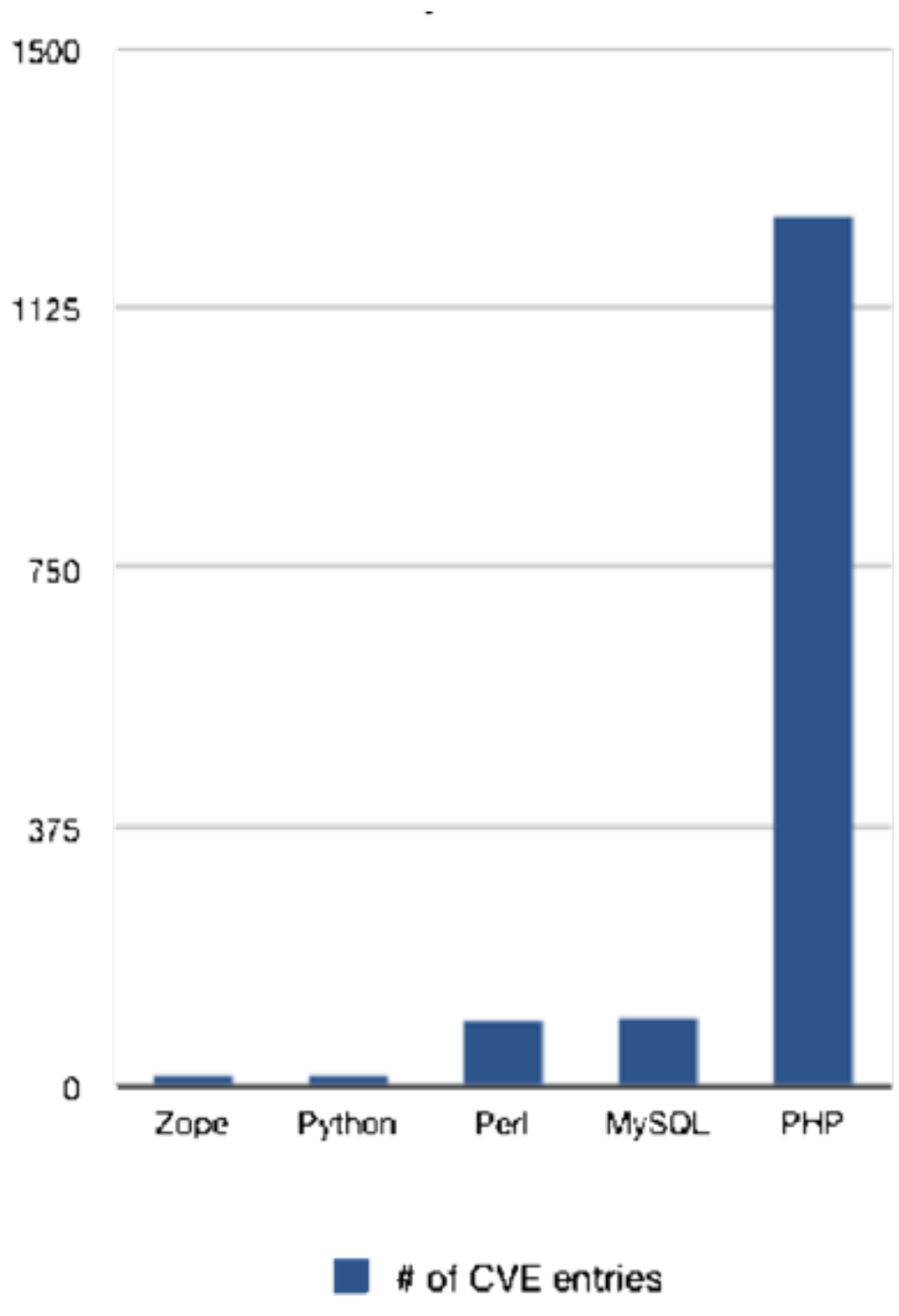
¿Existe?

- Aparentemente no existen sistemas de votaciones seguros sobre un CMS abierto
- y muy pocos sistemas abiertos

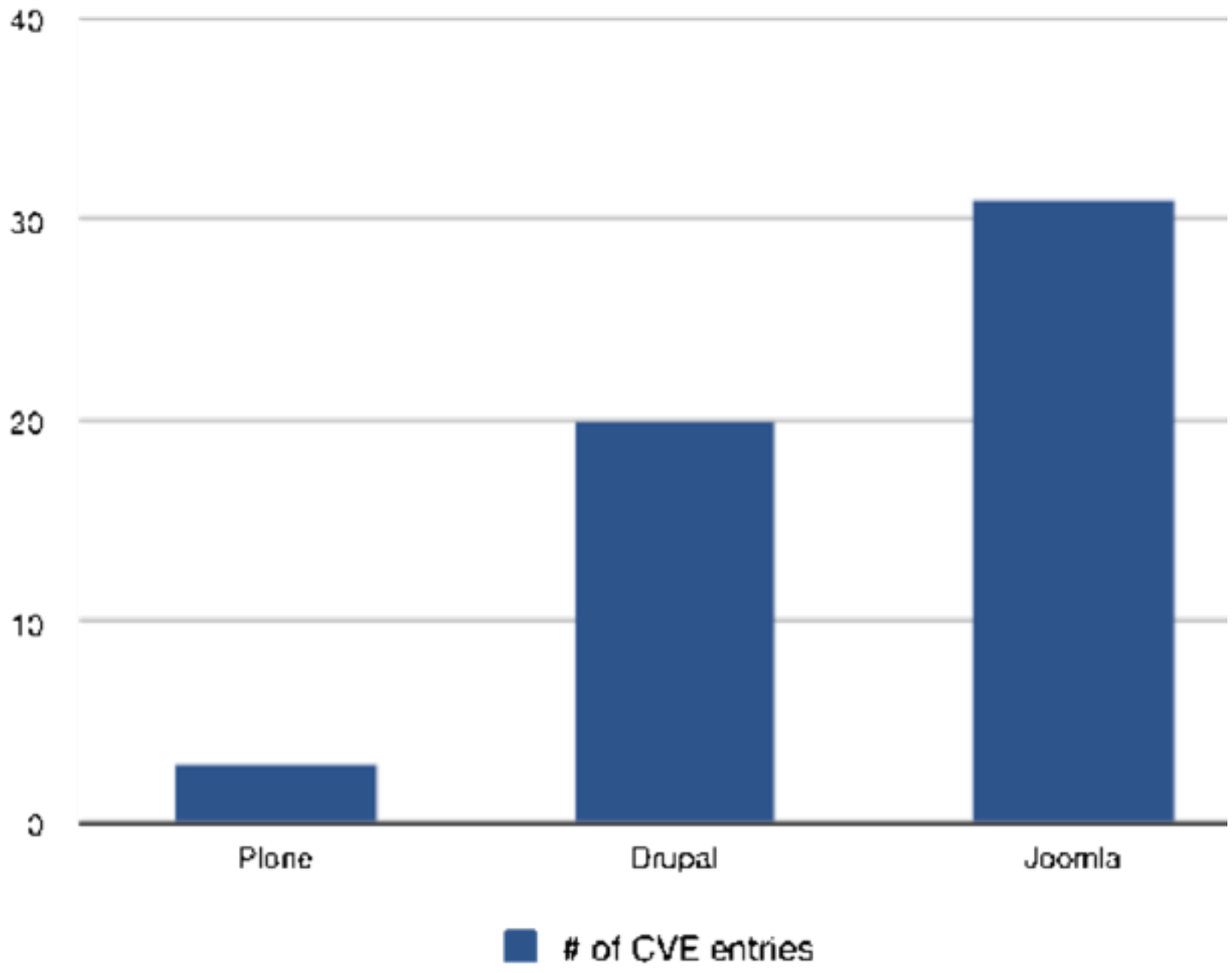
5. Seguridad

Entre los CMS, en todas las estadísticas
Plone queda hasta arriba en seguridad

Plataformas



Comparando seguridad de CMSs



http://plone.org/about/security/overview/security-overview-of-plone/

6. Plone es poderoso

- Sistema de control de accesos avanzado- cada contenido tiene bien definidos sus permisos, roles, etc
- Sistema de flujos avanzado
- Comunidad activa, usado en muchos sitios importantes del mundo, bien documentado
- Gobierno: Bélgica, Brasil, etc.

Interoperabilidad

- PlonePAS - Pluggable Authentication Service
- OpenID
- LDAP / Active Directory
- Apache
- RDBMS
- Salesforce
- Gmail

Plone es modular

- Esta diseñado para desarrollos colaborativos, módulos independientes se desarrollan e integran
- piramide: python, zope, plone

¿ Qué es Plone ?

Sistema de gestión de contenidos
content managment system

- Mantenimiento y producción colaborativa de sitios web
- Permite división de labores
- Herramientas para crear contenidos
- Facilita trabajar sistemáticamente
- Búsquedas rápidas y flexibles

La clave

- Plone (ya)

  +

- criptografía (ahora veamos)

Elecciones secretas

Elecciones secretas

- La palabra “boleta” viene del Italiano *ballotta*, pequeña bola, y eso eran: piedrita, frijol, bala

Elecciones secretas

- La palabra "boleta" viene del Italiano *ballotta*, pequeña bola, y eso eran: piedrita, frijol, bala
- En la Pennsylvania colonial se votaba lanzando frijoles en un sombrero. Votos en papel no se hacía para ocultar la identidad del votante, sino para facilitar el conteo de votos.

Elecciones secretas

- La palabra "boleta" viene del Italiano *ballotta*, pequeña bola, y eso eran: piedrita, frijol, bala
- En la Pennsylvania colonial se votaba lanzando frijoles en un sombrero. Votos en papel no se hacía para ocultar la identidad del votante, sino para facilitar el conteo de votos.
- Se consideraba cobarde la "boleta secreta"; citando a uno de Carolina del Sur, votar en secreto

Elecciones secretas

- La palabra "boleta" viene del Italiano *ballotta*, pequeña bola, y eso eran: piedrita, frijol, bala
- En la Pennsylvania colonial se votaba lanzando frijoles en un sombrero. Votos en papel no se hacía para ocultar la identidad del votante, sino para facilitar el conteo de votos.
- Se consideraba cobarde la "boleta secreta"; citando a uno de Carolina del Sur, votar en secreto

  destruiría esa apertura generosa y noble que es característica del caballero Inglés

Elecciones secretas

- La palabra "boleta" viene del Italiano *ballotta*, pequeña bola, y eso eran: piedrita, frijol, bala
- En la Pennsylvania colonial se votaba lanzando frijoles en un sombrero. Votos en papel no se hacía para ocultar la identidad del votante, sino para facilitar el conteo de votos.
- Se consideraba cobarde la "boleta secreta"; citando a uno de Carolina del Sur, votar en secreto

  destruiría esa apertura generosa y noble que es característica del caballero Inglés
- Antes de 1892 se votaba en público en EUA

Esta exhibición relata la historia de los métodos de votación en EUA, tan variados como los estados y sus distritos

http://americanhistory.si.edu/vote/

Bingham's (1852) ilustra un día de elecciones en Missouri. Solamente hombres blancos dueños de propiedades podían votar, y los candidatos y sus representantes podían solicitar votos inmediatamente antes de votar. Mucha bebida y votos anotados públicamente.

http://americanhistory.si.edu/vote/

Requiriendo secreto

- Sin el secreto todos podian verificar la correctez de la cuenta de votos
- En secreto, ¿¿cómo??
- Una vez echado el voto a la urna, pasamos a una caja negra ...

Coerción

- Los sistemas actuales, ¡no le entregan un recibo al votante!
- Debido al principio de que el votante no debe sacar nada absolutamente de la casilla de elecciones
- que pudiera servir de prueba de por quien votó

Elecciones verificables

Elecciones verificables

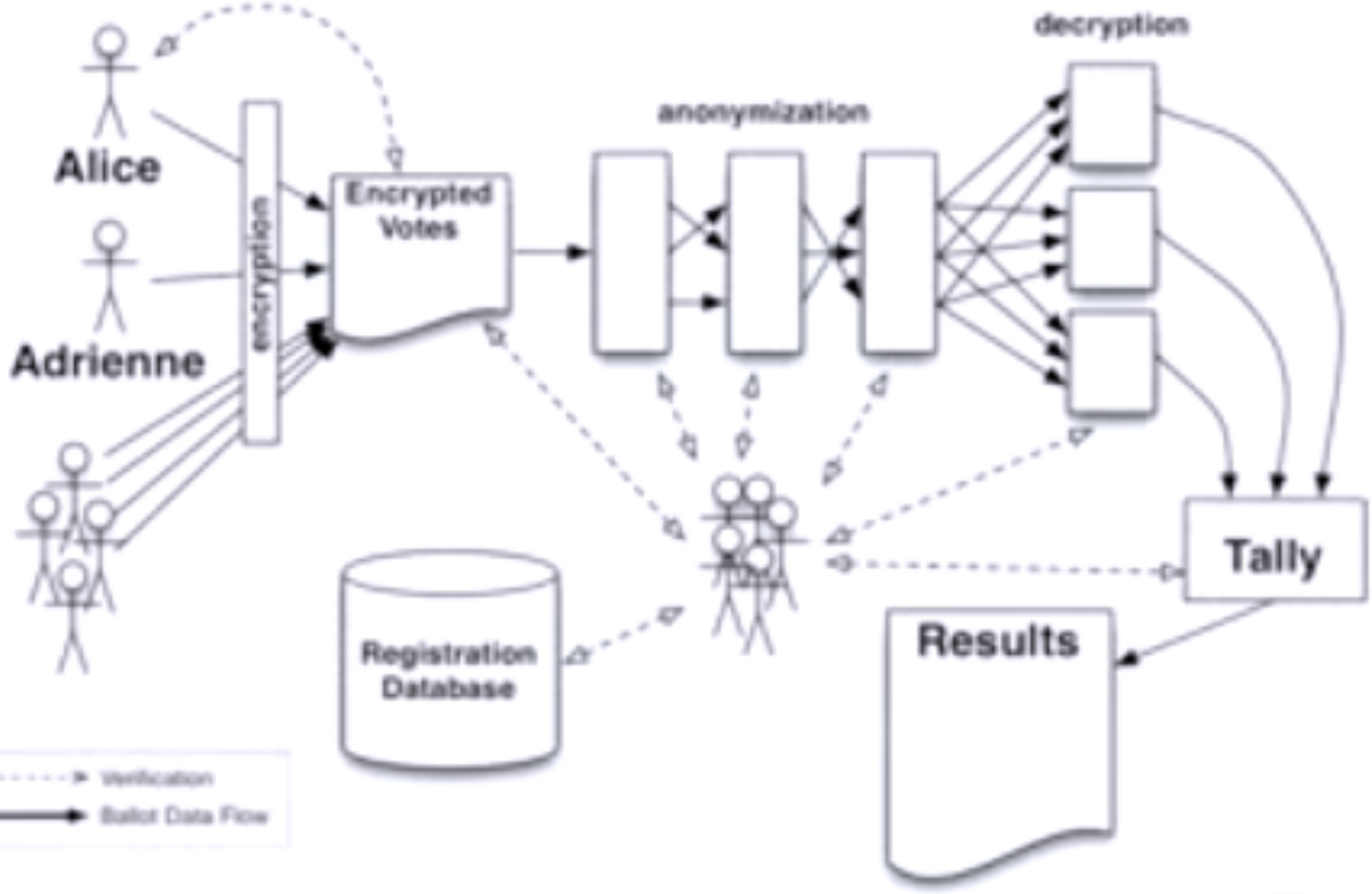
- Con criptografía se puede hacer magia: cada votante obtiene un recibo, este se publica en el web.
- El votante sabe que su voto se contó correctamente, sin que se pierda su anonimidad, y a la vez
- previniendo que alguien le pida una prueba de por quien votó

Principio básico

- Cada votante encripta su voto, y lo publica junto con su nombre en un pizarrón público
- Legislaciones requieren que los nombres aparezcan

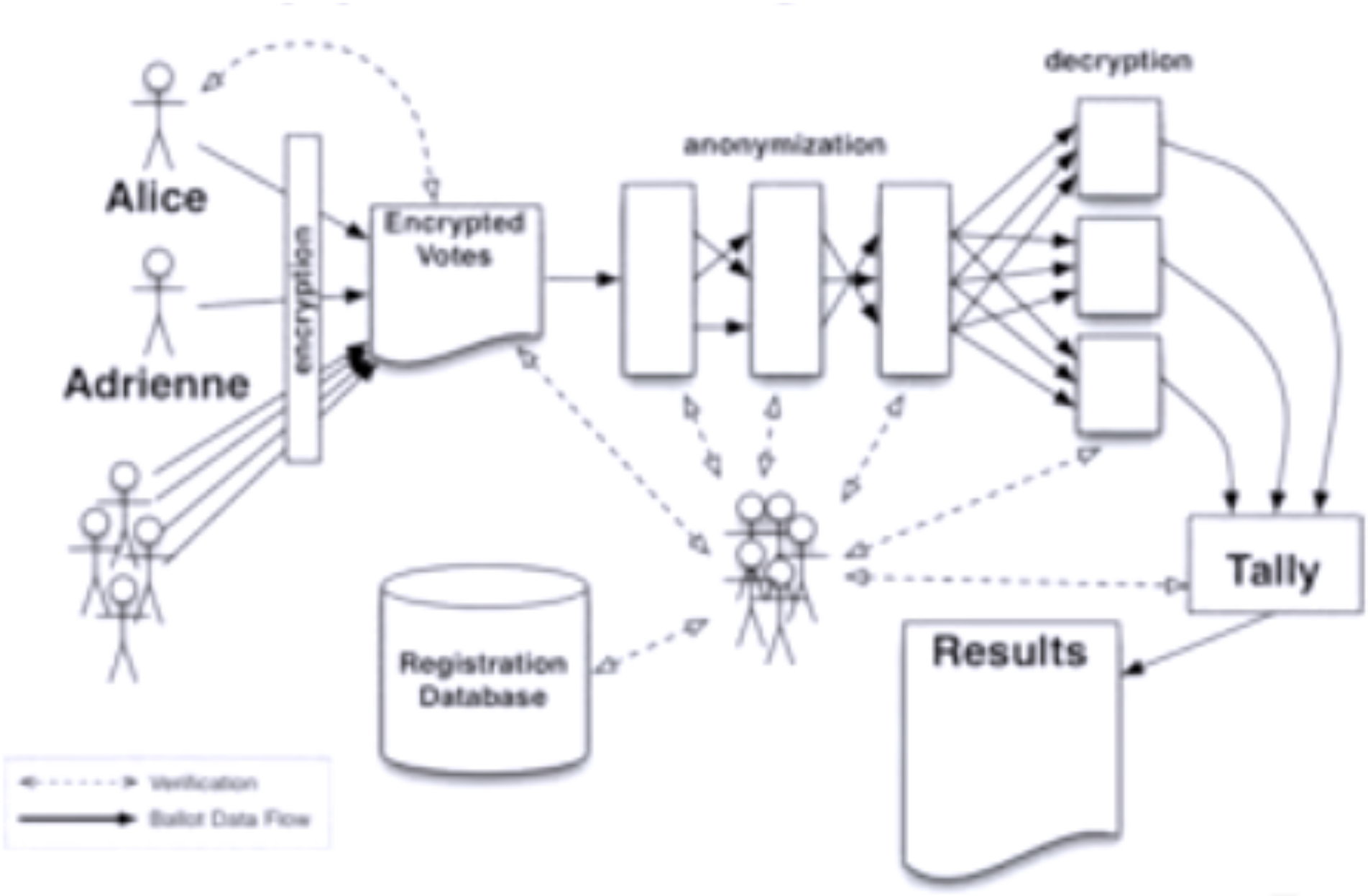
➡ se considera una propiedad de seguridad

Crypto Voting Schemes

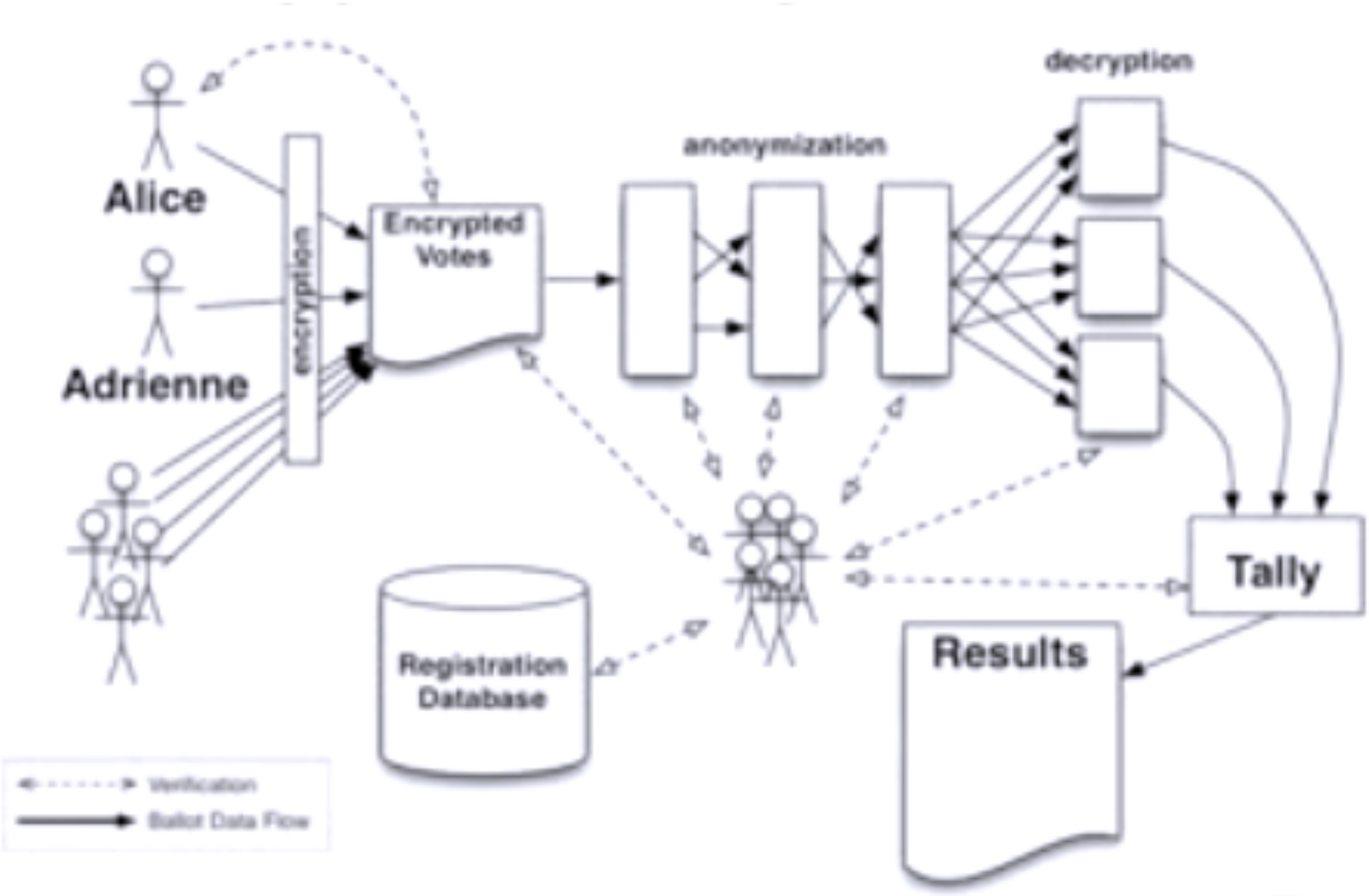


Ben Adida

criptografía para elecciones verificables

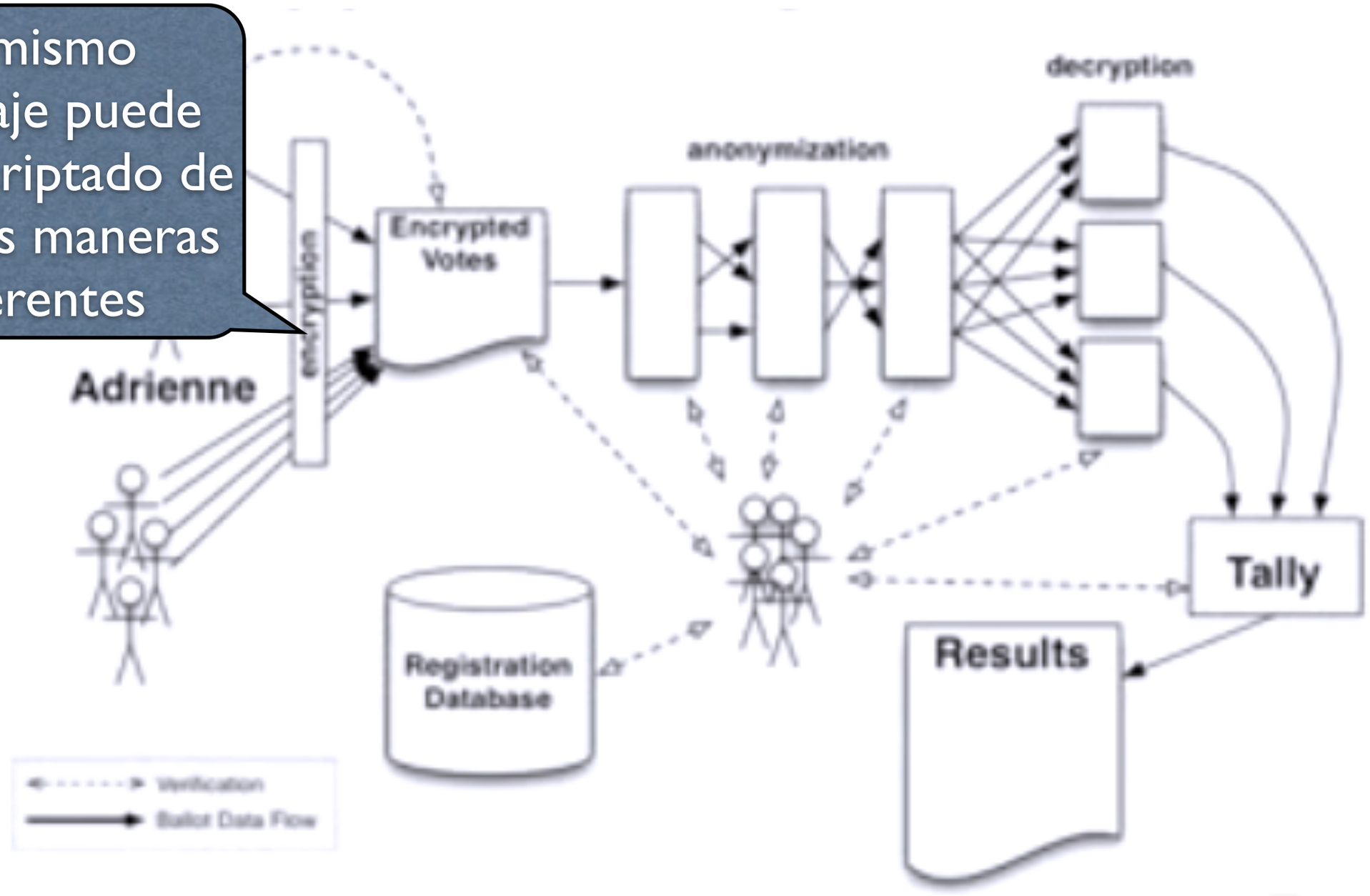


Ben Adida


Alice
Adrienne
encryption
Encrypted Votes
anonymization
decryption
Tally
Results
Registration Database
Verification
Ballot Data Flow

Ben Adida

el mismo mensaje puede ser encriptado de muchas maneras diferentes



Ben Adida

el mismo mensaje puede ser encriptado de muchas maneras diferentes

revolver los votos, de forma que en cada fase estén los mismos contenidos

Ben Adida

el mismo mensaje puede ser encriptado de muchas maneras diferentes

revolver los votos, de forma que en cada fase estén los mismos contenidos

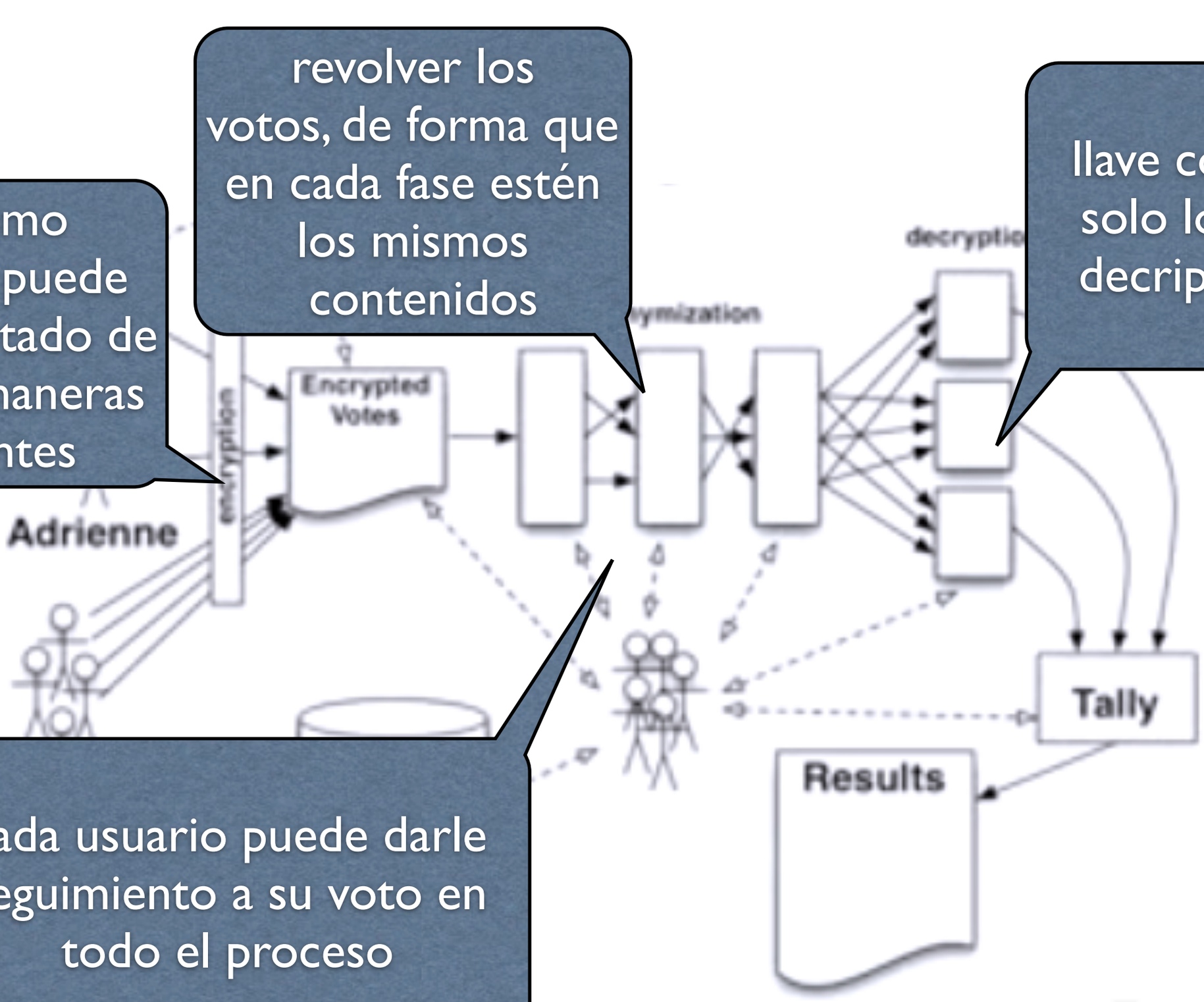
llave compartida: solo los pueden decriptar juntos

Ben Adida

el mismo mensaje puede ser encriptado de muchas maneras diferentes

revolver los votos, de forma que en cada fase estén los mismos contenidos

llave compartida: solo los pueden decriptar juntos



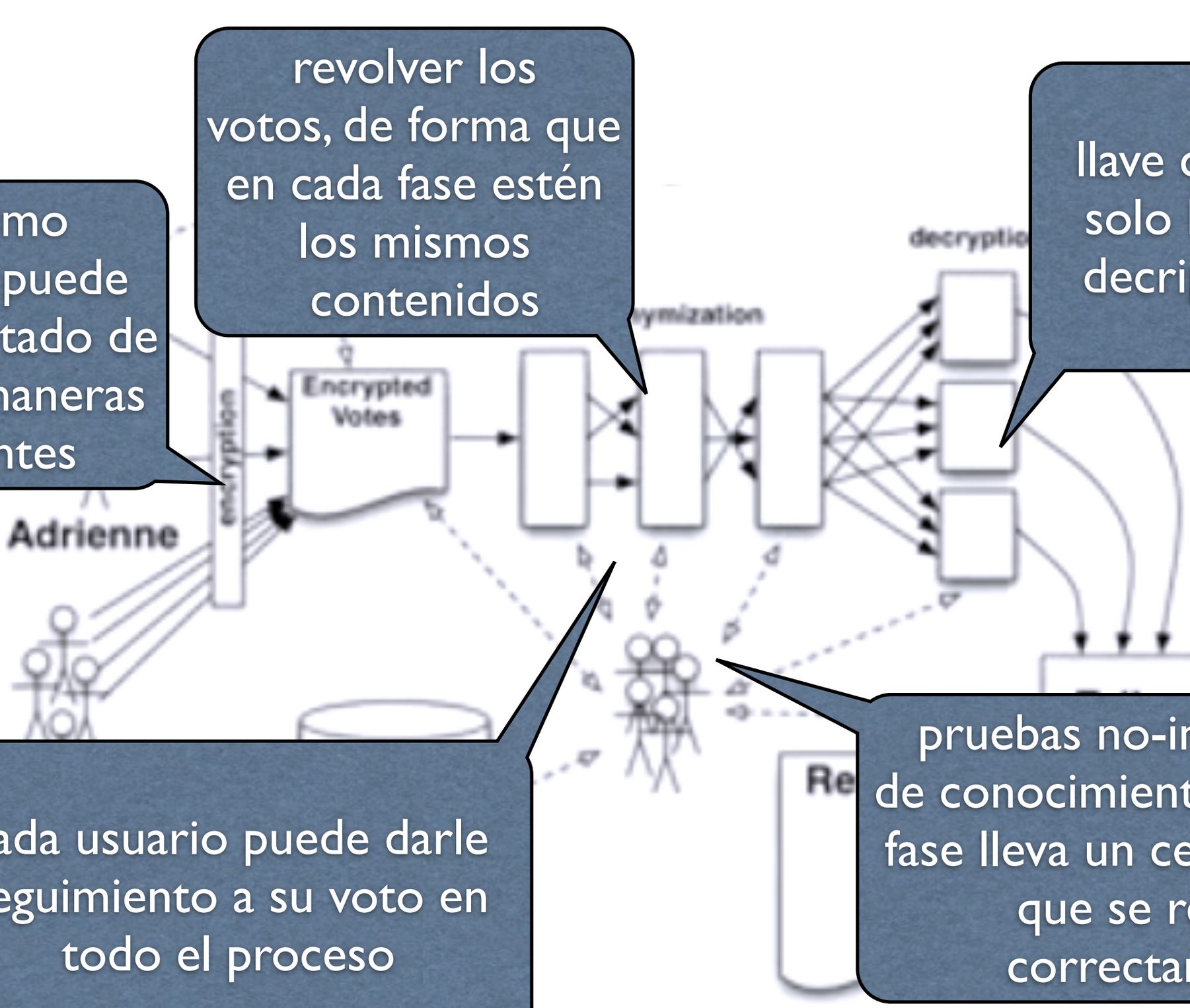
cada usuario puede darle seguimiento a su voto en todo el proceso

Ben Adida

el mismo mensaje puede ser encriptado de muchas maneras diferentes

revolver los votos, de forma que en cada fase estén los mismos contenidos

llave compartida: solo los pueden decriptar juntos



cada usuario puede darle seguimiento a su voto en todo el proceso

pruebas no-interactivas de conocimiento cero: cada fase lleva un certificado de que se realizó correctamente

Ben Adida

Ingredientes de Criptografía

1. El-Gamal : Sistema de llave pública asimétrica de encriptamiento
2. Mixnets para revolver votos
3. Pruebas de conocimiento cero
4. Distribución de llaves con umbral

1. El-Gamal

- Tiene muchas propiedades bonitas: el usuario incluye aleatoriedad en la encripción, es
- homomórfico- producto de mensajes encriptados es igual al encriptados del producto. Se puede modificar para sumas, aunque lento... hay otros sistemas (Pailler99)

2. Anonimización

Dos opciones:

- Usando propiedad homomórfica, se agregan los votos
- Mixnets, sin que se agreguen

3. Pruebas de conocimiento cero

(Esta es interactiva, es posible hacerlo de manera no-interactiva)

Alice desea convencer a Bob de que adentro de un sobre cerrado dice “Obama”, pero sin abrir el sobre

Una prueba

Una prueba

- Alice produce 1000 sobres, se los da a Bob para que elija uno solo que NO abrir

Una prueba

- Alice produce 1000 sobres, se los da a Bob para que elija uno solo que NO abrir
- Al abrir los 999 debe estar escrito “Obama”

Una prueba

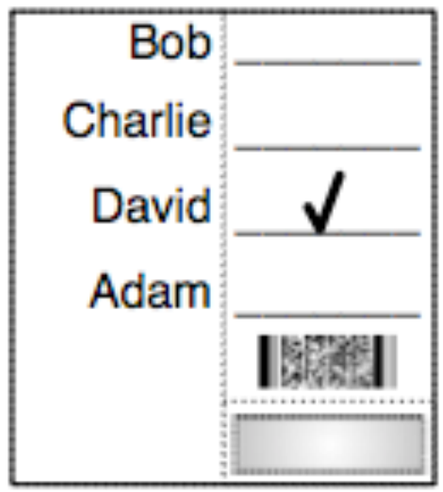
- Alice produce 1000 sobres, se los da a Bob para que elija uno solo que NO abrir
- Al abrir los 999 debe estar escrito “Obama”
- Se queda con el cerrado, deshecha los 999

Scratch & Vote

Elecciones verificables

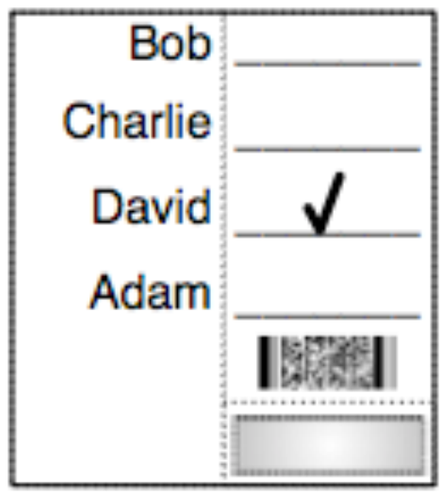
Scratch & Vote

(Ben Adida, Rivest CCS 2006)



Scratch & Vote

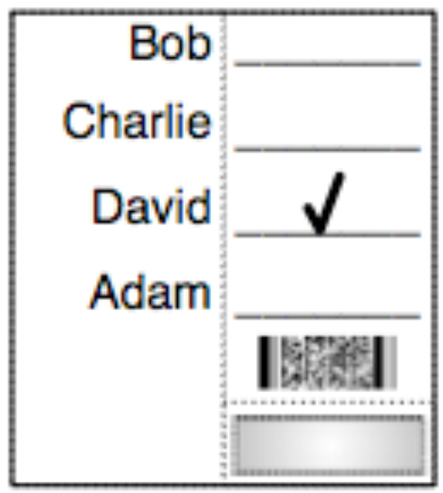
(Ben Adida, Rivest CCS 2006)



- Alice obtiene una boleta con los candidatos en orden aleatorio.

Scratch & Vote

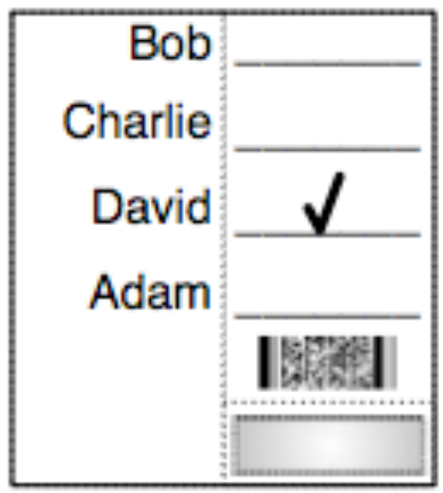
(Ben Adida, Rivest CCS 2006)



- Alice obtiene una boleta con los candidatos en orden aleatorio.
- Oficiales de la elección no deben ver este orden

Scratch & Vote

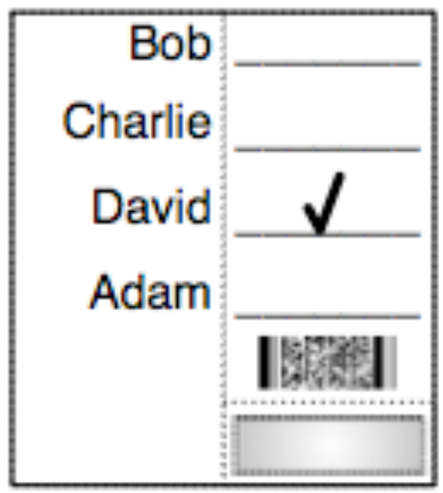
(Ben Adida, Rivest CCS 2006)



- Alice obtiene una boleta con los candidatos en orden aleatorio.
- Oficiales de la elección no deben ver este orden
- tiene bolitas escaneables a la derecha

Scratch & Vote

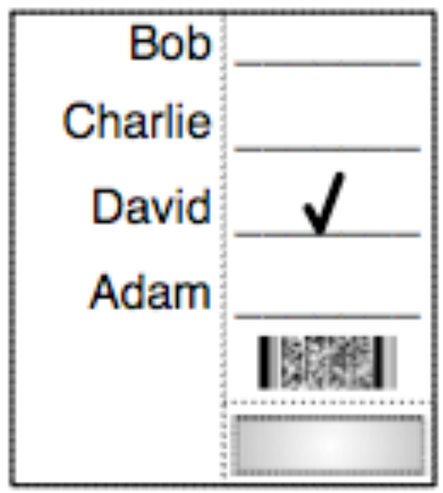
(Ben Adida, Rivest CCS 2006)



- Alice obtiene una boleta con los candidatos en orden aleatorio.
- Oficiales de la elección no deben ver este orden
- tiene bolitas escaneables a la derecha
- un código de barras con el orden encriptado

Scratch & Vote

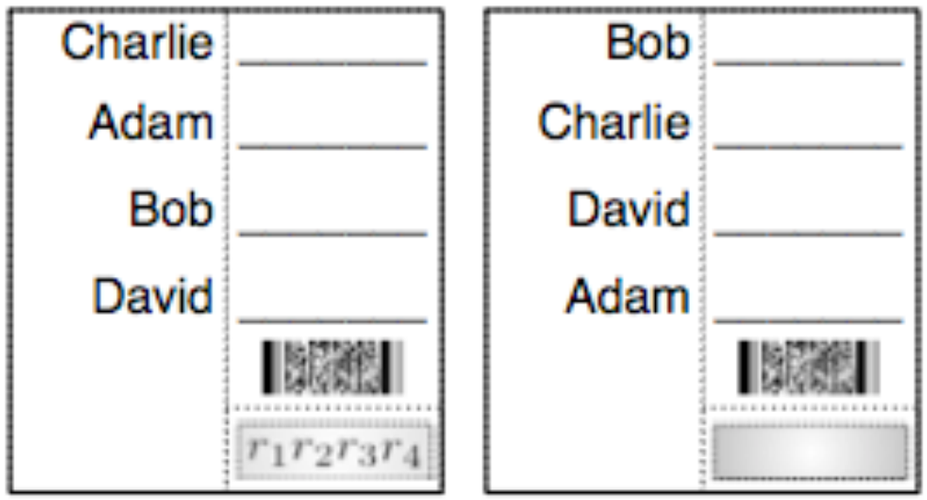
(Ben Adida, Rivest CCS 2006)



- Alice obtiene una boleta con los candidatos en orden aleatorio.
- Oficiales de la elección no deben ver este orden
- tiene bolitas escaneables a la derecha
- un código de barras con el orden encriptado
- una barra raspable con los números aleatorios que permiten decriptar

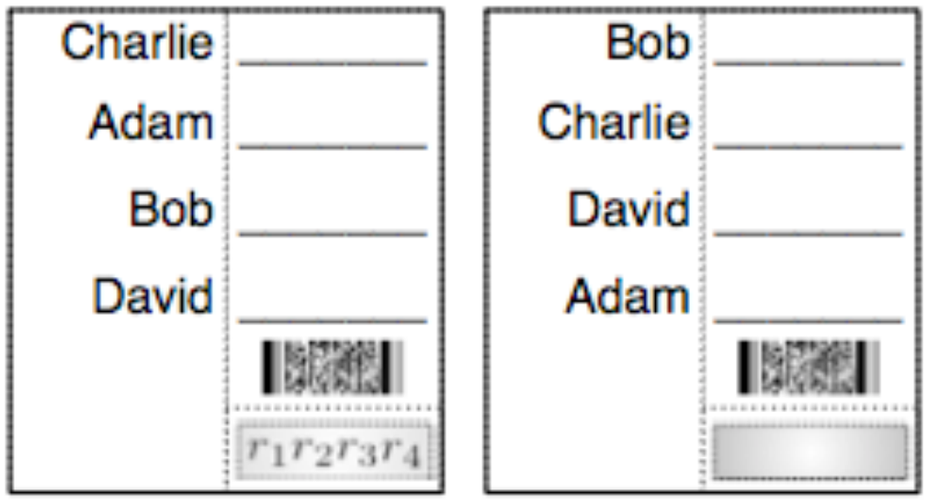
Auditando

(Ben Adida, Rivest CCS 2006)



Auditando

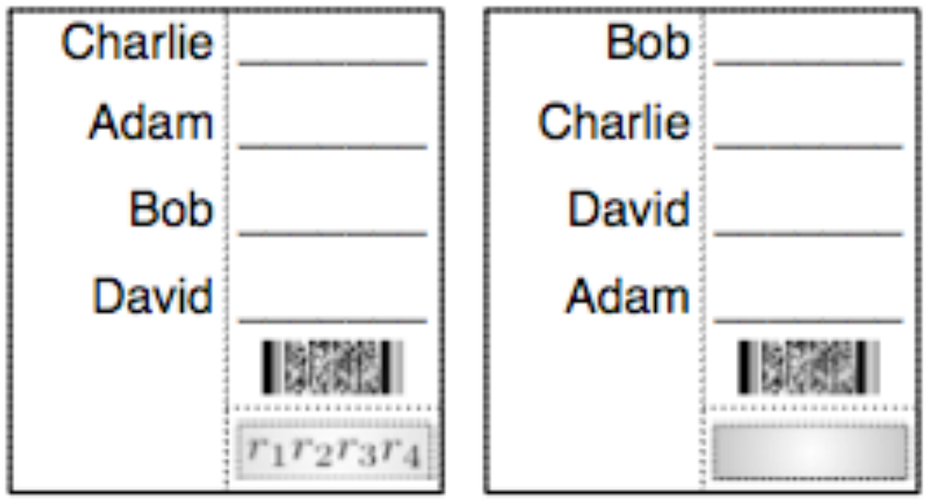
(Ben Adida, Rivest CCS 2006)



- Alice selecciona una segunda boleta

Auditando

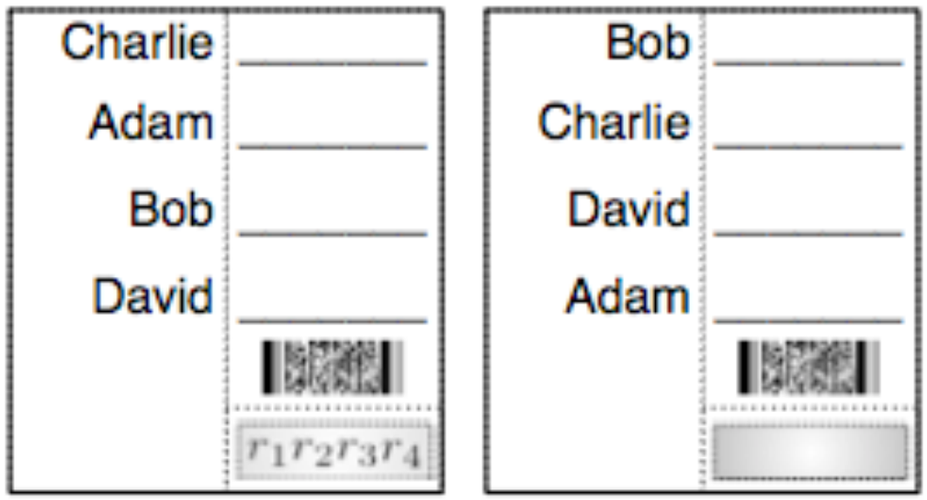
(Ben Adida, Rivest CCS 2006)



- Alice selecciona una segunda boleta
- raspa y entrega la boleta inválida a una organización de apoyo, para recibir confirmación de la validez del orden

Auditando

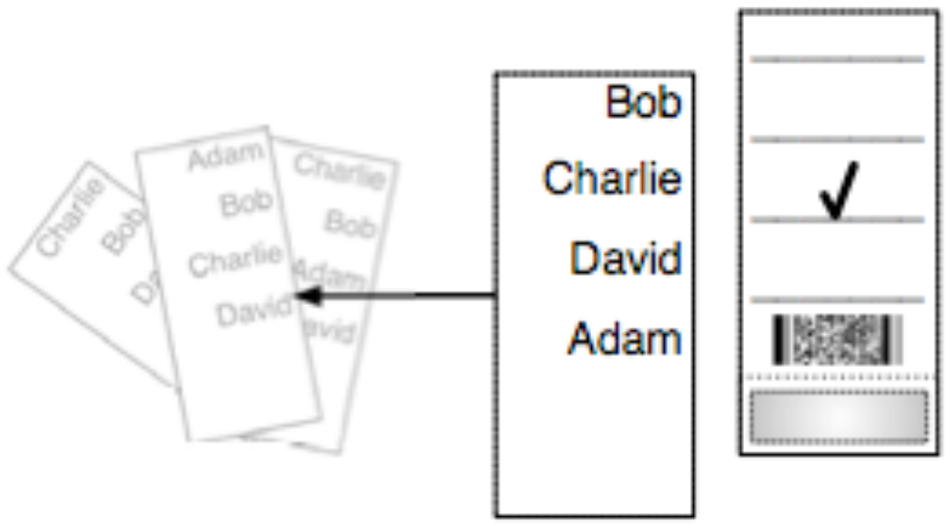
(Ben Adida, Rivest CCS 2006)



- Alice selecciona una segunda boleta
- raspa y entrega la boleta inválida a una organización de apoyo, para recibir confirmación de la validez del orden
- esto otorga confianza a Alice de la validez de su boleta

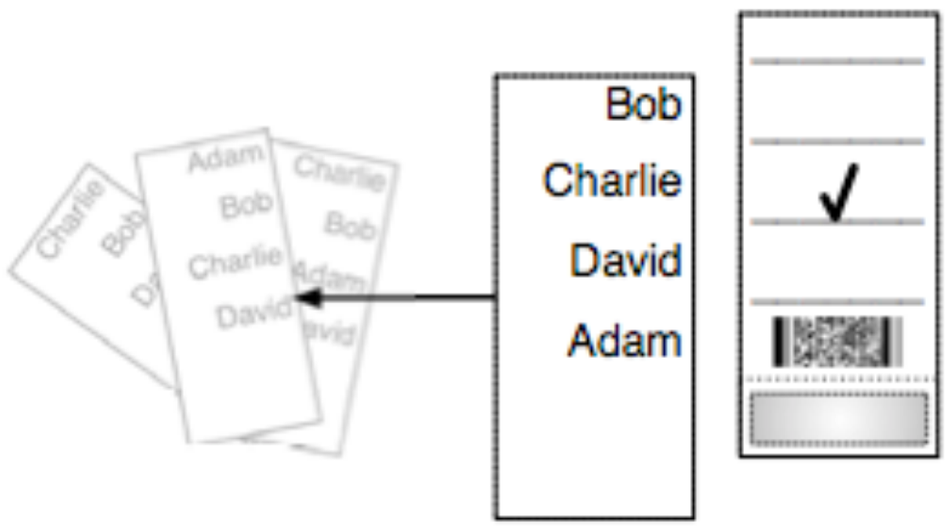
Selección

(Ben Adida, Rivest CCS 2006)



Selección

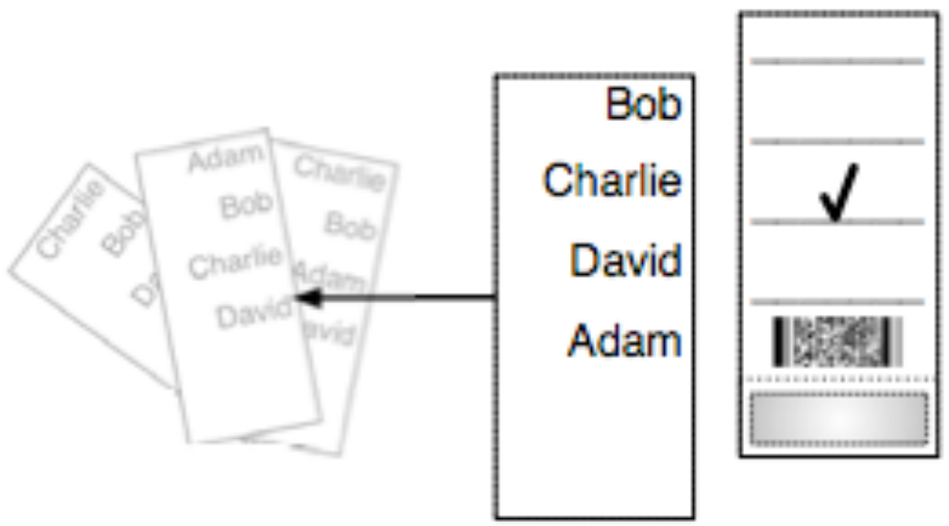
(Ben Adida, Rivest CCS 2006)



- En privado Alice marca su voto

Selección

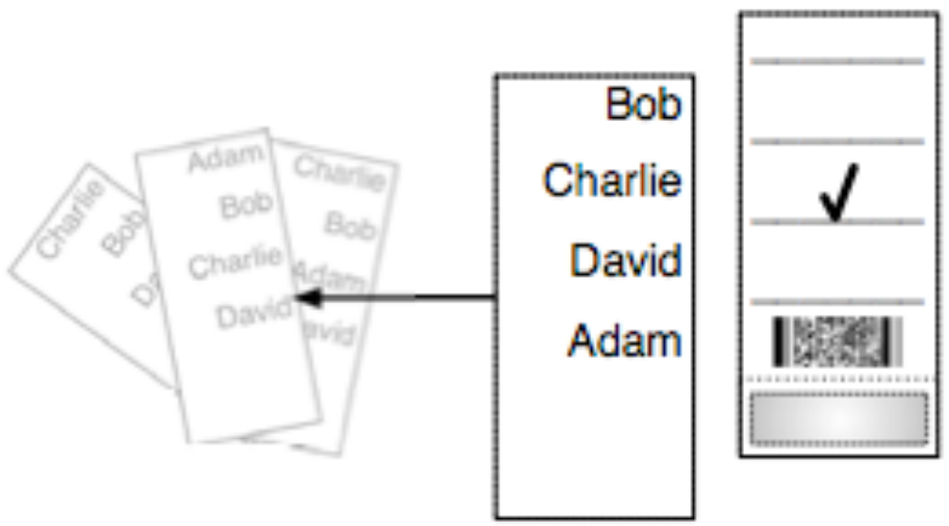
(Ben Adida, Rivest CCS 2006)



- En privado Alice marca su voto
- Separa las dos mitades, tira los nombres

Selección

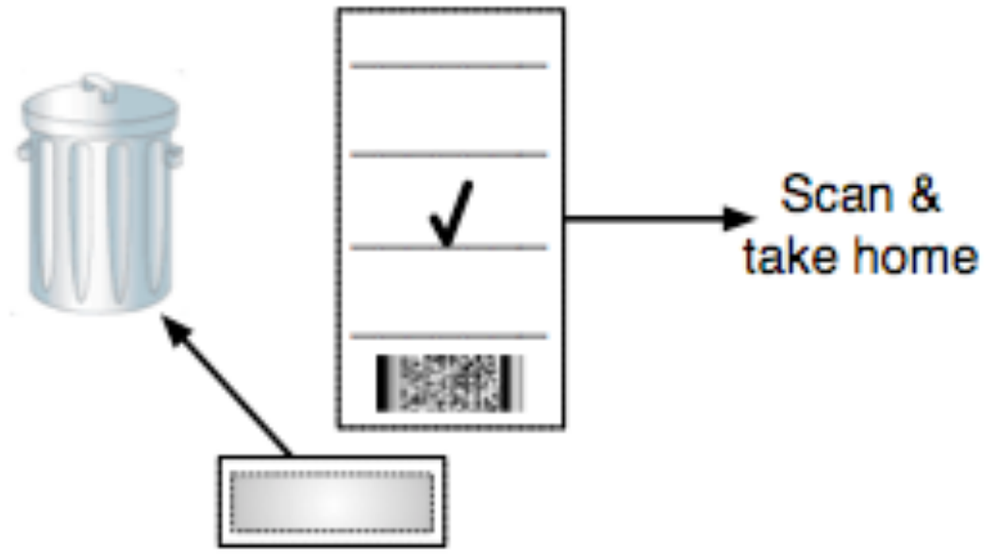
(Ben Adida, Rivest CCS 2006)



- En privado Alice marca su voto
- Separa las dos mitades, tira los nombres
- en el basurero hay solo listas de nombres en orden aleatorio

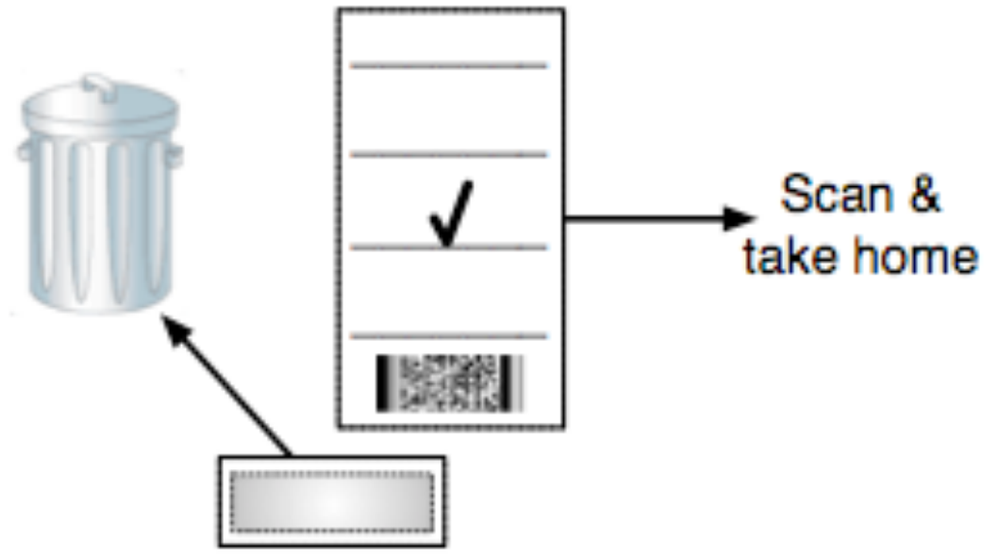
Votando

(Ben Adida, Rivest CCS 2006)



Votando

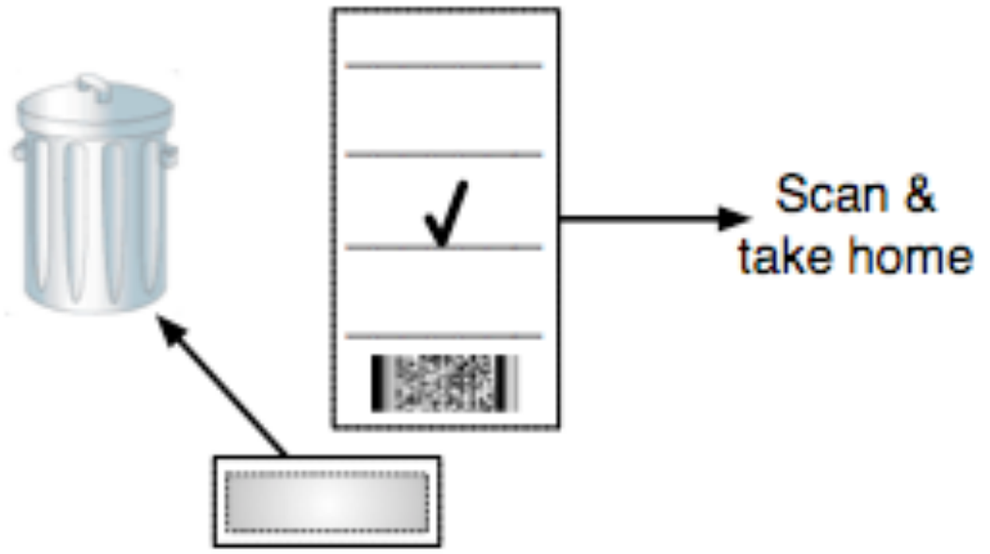
(Ben Adida, Rivest CCS 2006)



- Alice le presenta el lado derecho de su boleta al oficial de la elección, quien verifica que no esté raspada

Votando

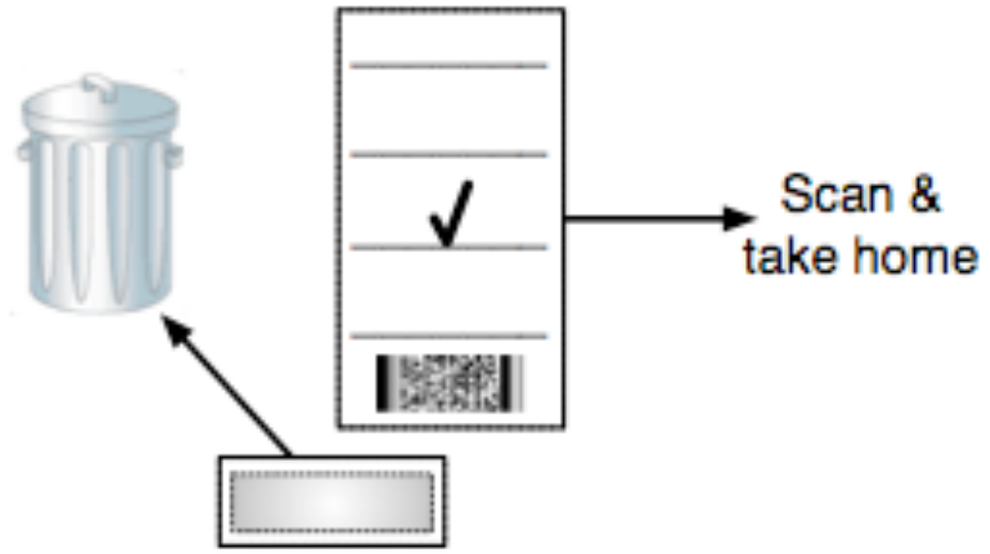
(Ben Adida, Rivest CCS 2006)



- Alice le presenta el lado derecho de su boleta al oficial de la elección, quien verifica que no esté raspada
- El oficial tira la parte raspada, en frente de testigos

Votando

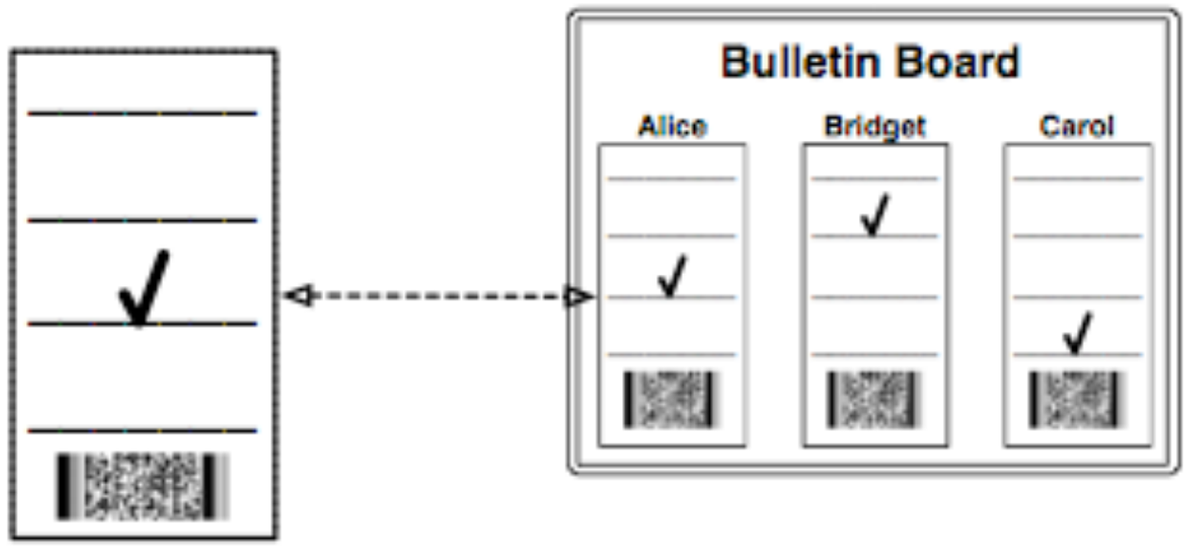
(Ben Adida, Rivest CCS 2006)



- Alice le presenta el lado derecho de su boleta al oficial de la elección, quien verifica que no esté raspada
- El oficial tira la parte raspada, en frente de testigos
- Alice mete al escaner el código de barras y su elección, y se lo lleva a casa

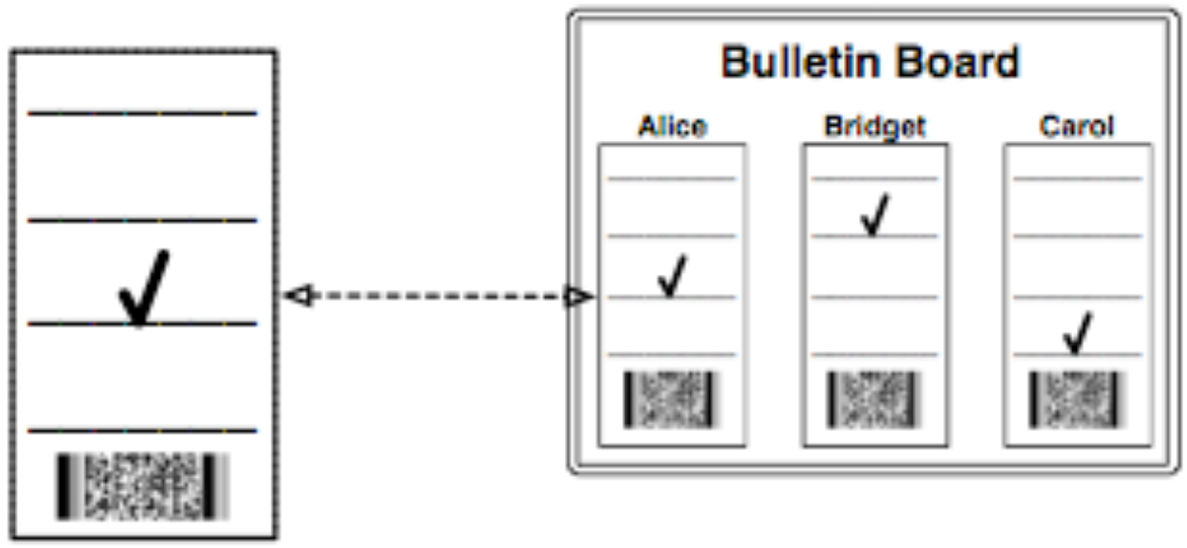
Verificando

(Ben Adida, Rivest CCS 2006)



Verificando

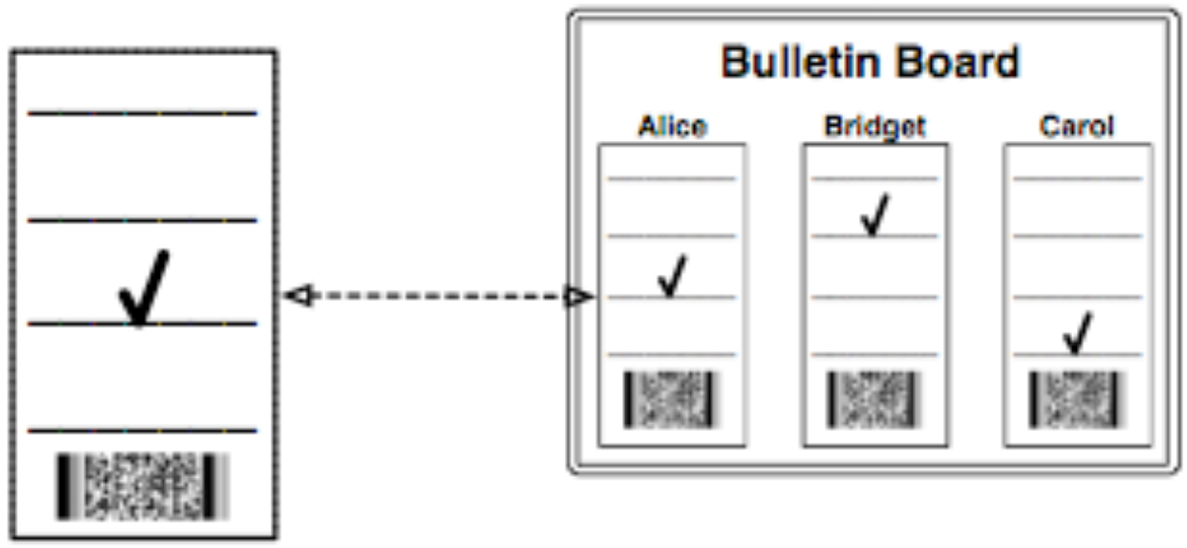
(Ben Adida, Rivest CCS 2006)



- Alice busca en el web su boleta

Verificando

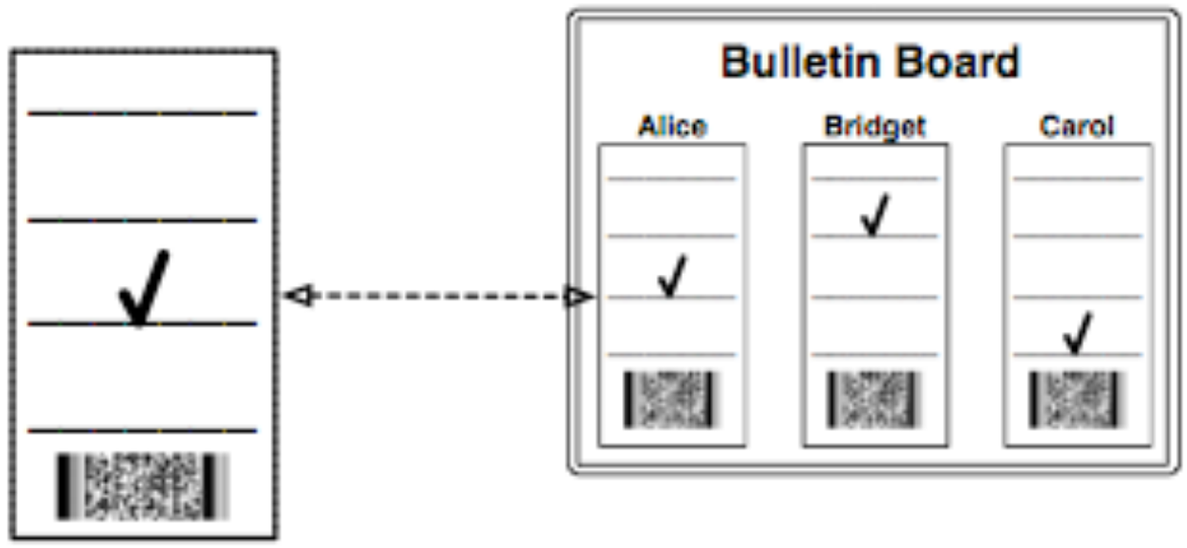
(Ben Adida, Rivest CCS 2006)



- Alice busca en el web su boleta
- Verifica que en la suma de votos es igual a todos los publicados en el web

Verificando

(Ben Adida, Rivest CCS 2006)



- Alice busca en el web su boleta
- Verifica que en la suma de votos es igual a todos los publicados en el web
- Alice verifica el decriptamiento hecho por los oficiales de la elección

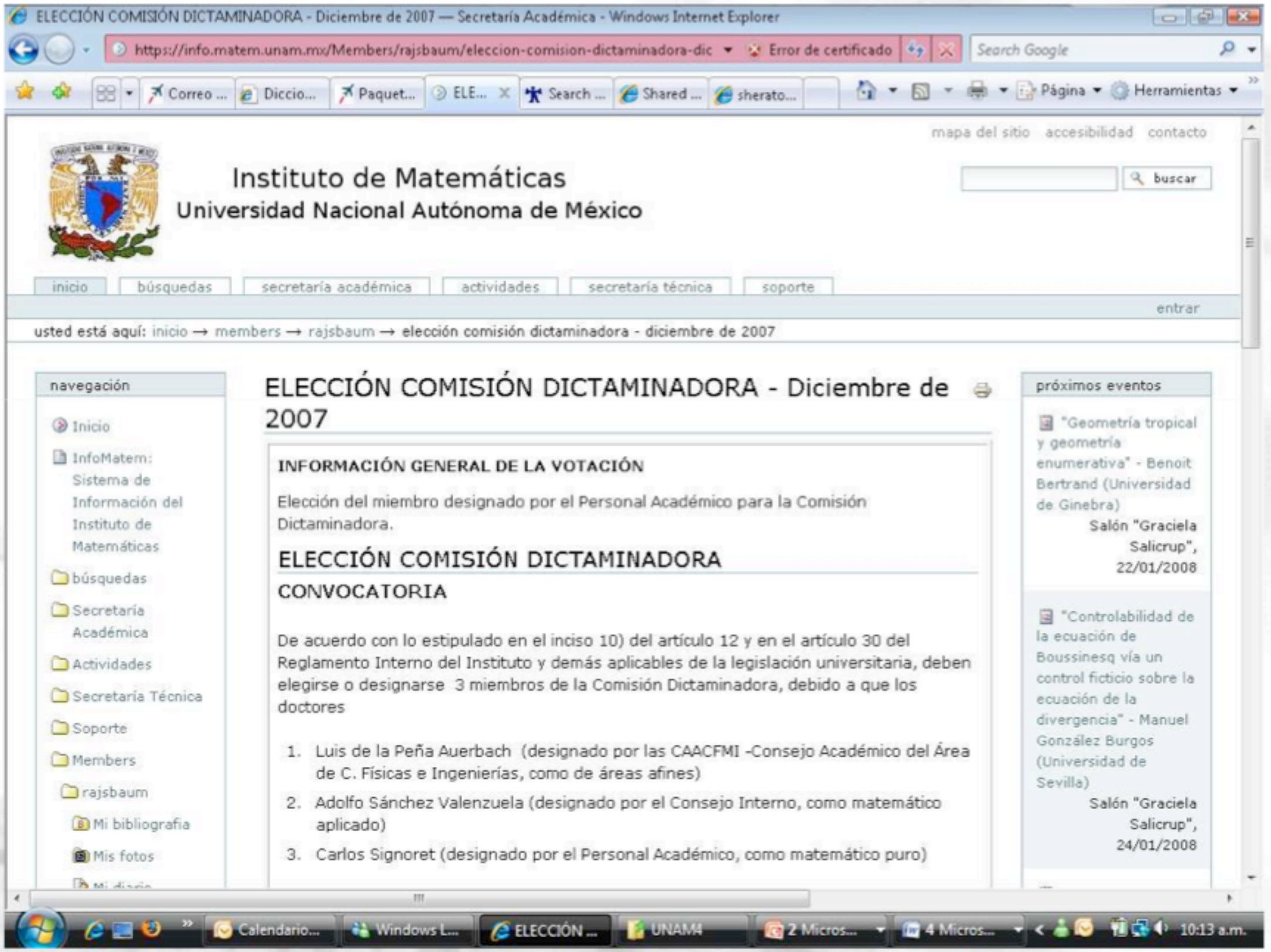
La experiencia en el IMate - UNAM

Experiencia

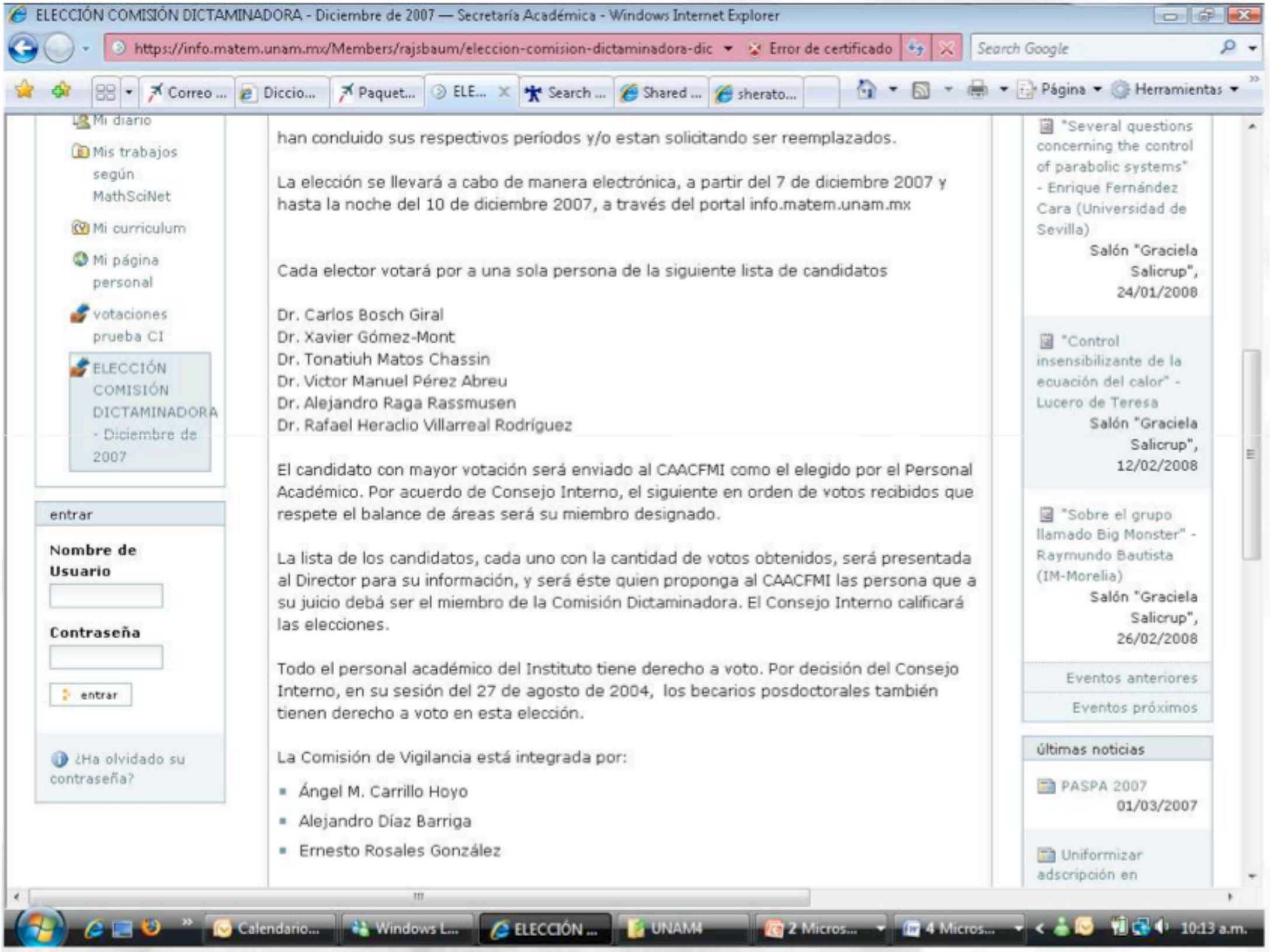
- Implementación del sistema sobre Plone, basado en KOA sistema remoto de votaciones, servidor confiable
- Varias tesis de licenciatura y maestría
- Utilización en varias elecciones reales
- En proceso de desarrollo de una nueva versión más flexible, con mixnets, y una biblioteca criptográfica en python, basado en Ben Adida 2008, Josh Benaloh 2006.

Elección de la Comisión Dictaminadora entre el 7 y el 10 de diciembre de 2007

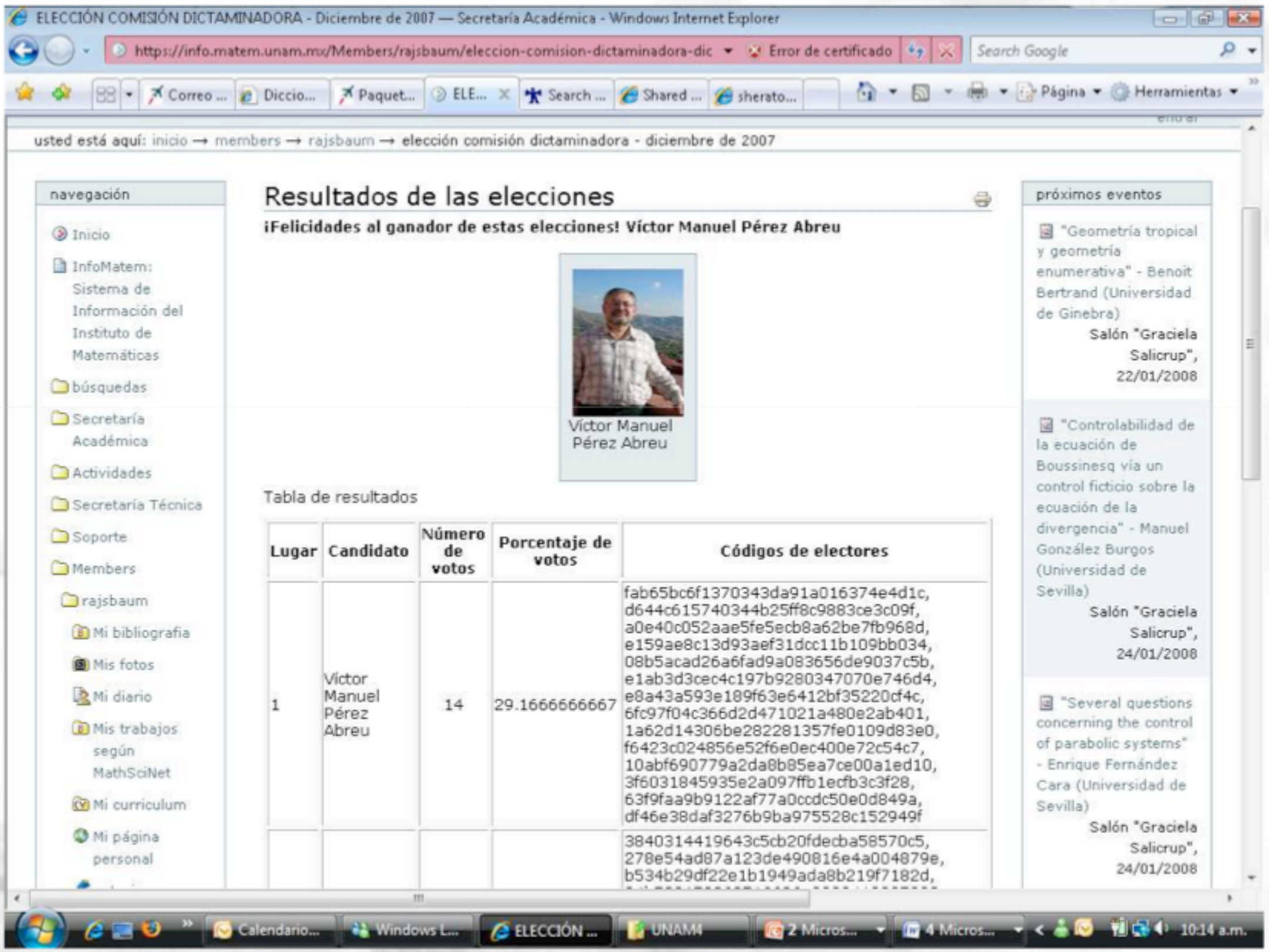
Convocatoria (1)



Convocatoria (II)



Resultados


ELECCIÓN COMISIÓN DICTAMINADORA - Diciembre de 2007 — Secretaría Académica - Windows Internet Explorer
https://info.matem.unam.mx/Members/rajsbaum/eleccion-comision-dictaminadora-dic
Error de certificado
Search Google
usted está aquí: inicio → members → rajsbaum → elección comisión dictaminadora - diciembre de 2007
navegación
Inicio
InfoMatem: Sistema de Información del Instituto de Matemáticas
búsquedas
Secretaría Académica
Actividades
Secretaría Técnica
Soporte
Members
rajsbaum
Mi bibliografia
Mis fotos
Mi diario
Mis trabajos según MathSciNet
Mi curriculum
Mi página personal
Resultados de las elecciones
¡Felicidades al ganador de estas elecciones! Víctor Manuel Pérez Abreu
Víctor Manuel Pérez Abreu
Tabla de resultados
Lugar
Candidato
Número de votos
Porcentaje de votos
Códigos de electores
1
Víctor Manuel Pérez Abreu
14
29.1666666667
fab65bc6f1370343da91a016374e4d1c, d644c615740344b25ff8c9883ce3c09f, a0e40c052aae5fe5ecb8a62be7fb968d, e159ae8c13d93aef31dcc11b109bb034, 08b5acad26a6fad9a083656de9037c5b, e1ab3d3cec4c197b9280347070e746d4, e8a43a593e189f63e6412bf35220cf4c, 6fc97f04c366d2d471021a480e2ab401, 1a62d14306be282281357fe0109d83e0, f6423c024856e52f6e0ec400e72c54c7, 10abf690779a2da8b85ea7ce00a1ed10, 3f6031845935e2a097ffb1ecfb3c3f28, 63f9faa9b9122af77a0ccdc50e0d849a, df46e38daf3276b9ba975528c152949f
3840314419643c5cb20fdecba58570c5, 278e54ad87a123de490816e4a004879e, b534b29df22e1b1949ada8b219f7182d,
próximos eventos
"Geometría tropical y geometría enumerativa" - Benoit Bertrand (Universidad de Ginebra)
Salón "Graciela Salicrup", 22/01/2008
"Controlabilidad de la ecuación de Boussinesq vía un control ficticio sobre la ecuación de la divergencia" - Manuel González Burgos (Universidad de Sevilla)
Salón "Graciela Salicrup", 24/01/2008
"Several questions concerning the control of parabolic systems" - Enrique Fernández Cara (Universidad de Sevilla)
Salón "Graciela Salicrup", 24/01/2008
Calendario...
Windows L...
ELECCIÓN ...
UNAM4
2 Micros...
4 Micros...
10:14 a.m.

Trabajo en proceso PloneVoteCryptoLib

- implementa en python todas las operaciones criptográficas requeridas para elecciones verificables:
- redes de mezcla verificables por recifrado sobre ElGamal, cifrado de umbral, generación de llaves distribuida, etc.

PloneVoteCryptoLib provee servicios para estas operaciones

- cifrado de votos con representación y longitud arbitraria, monitorización de progreso, configuración global centralizada, serialización a XML de objetos: instancias de ElGamal, llaves, textos cifrados, etc.
- Es la base para continuar la implementación del sistema PloneVote completo, basado en:
- Josh Benaloh, Simple Verifiable Elections, EVT'06 USENIX

PloneVote


Cliente web del elector
.js
Usado por el elector para emitir su voto.
Servidor de PloneVote
- Zope
- Plone
- Productos de Plone
PVCL
Cliente del auditor
Usado por los auditores para verificar la correctitud de la elección.
PVCL
Cliente de la comisión
Usado por la comisión de la elección para anonimizar y contar los votos.
PVCL

Conclusiones

Conclusiones

- Proyecto académico (no de desarrollo de software), aprendizaje para alumnos y profesores
- Tesis de licenciatura y maestría, participación en congresos internacionales e integración con la comunidad de Plone
- sistema Plone en: www.matem.unam.mx
- documentos en:

  /acerca-de/estructura-interna/secretaria-academica/documentos/plone

Conclusiones (I)

- La integración de un sistema de votaciones con Plone tiene muchos beneficios, ser parte de una comunidad (Python y Plone), así como permitir reuso de infraestructura de software y de datos de usuarios: autenticación, interfaz de usuarios, datos de usuarios, etc.
- Bien aceptado por la comunidad de usuarios: fácil, rápido y convenienteBasado en GnuPG

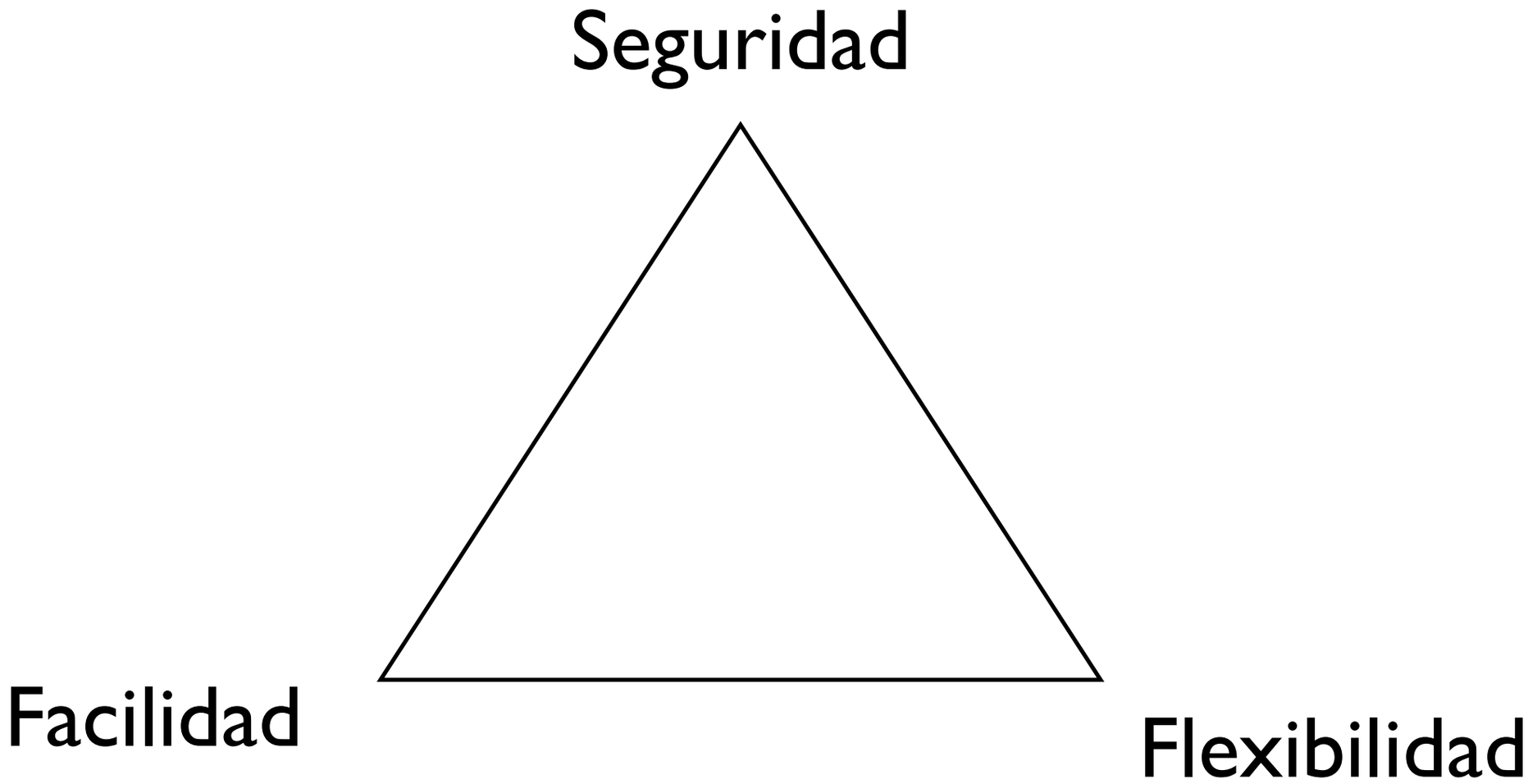
Conclusiones (II)

- Complicado y lento para los administradores de la votación: configuración y pruebas
- El primer sistema muestra un buen balance entre seguridad, eficiencia, facilidad de uso (ninguna implementación de criptografía, ningún requerimiento de parte de votantes)
- Trabajo futuro terminar la segunda versión, y evaluarla: desempeño, facilidad de uso

una vez más
observamos: la compleja
interacción entre la
tecnología y los procesos
sociales-sicológicos

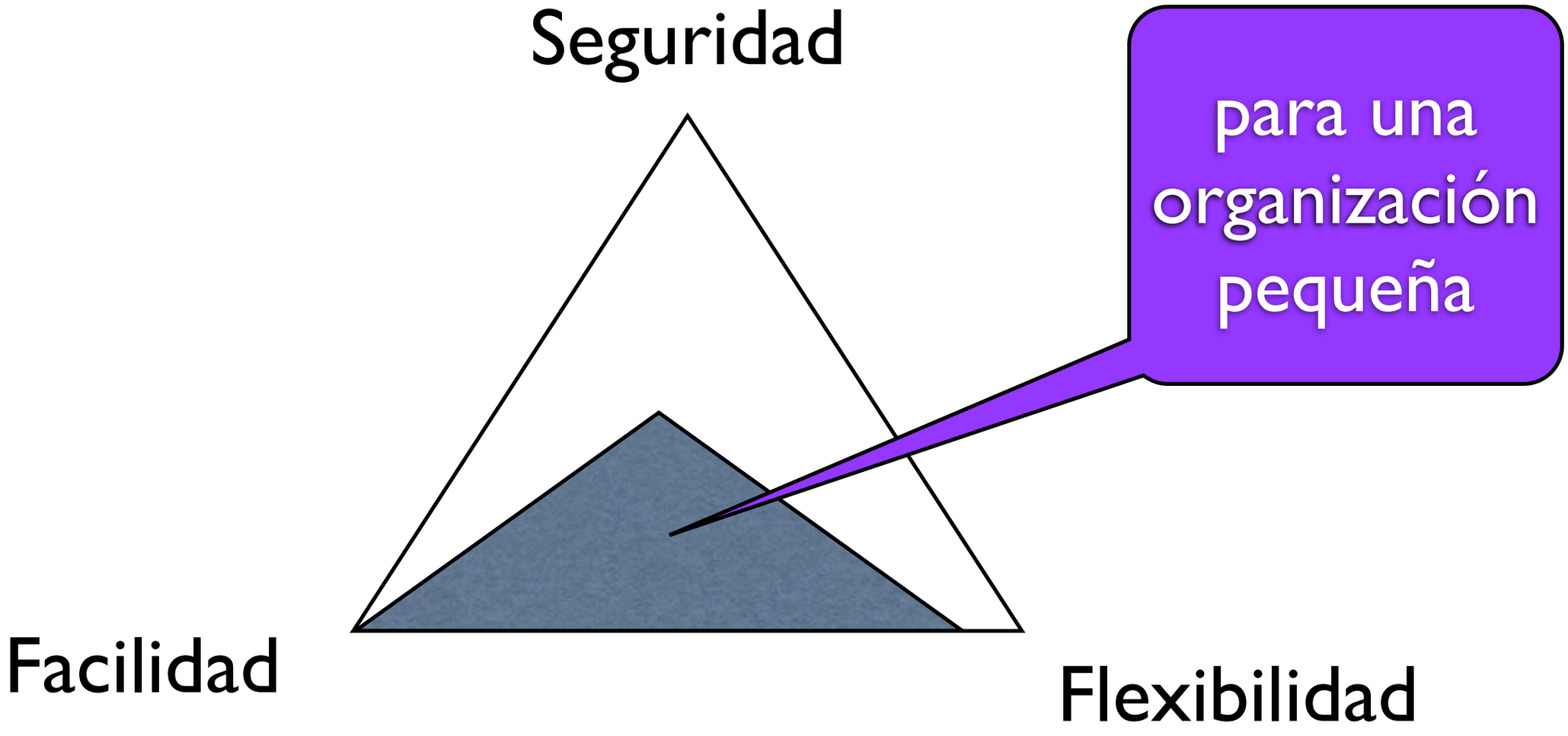
¿Donde esta el balance óptimo?

¿Donde esta el balance óptimo?

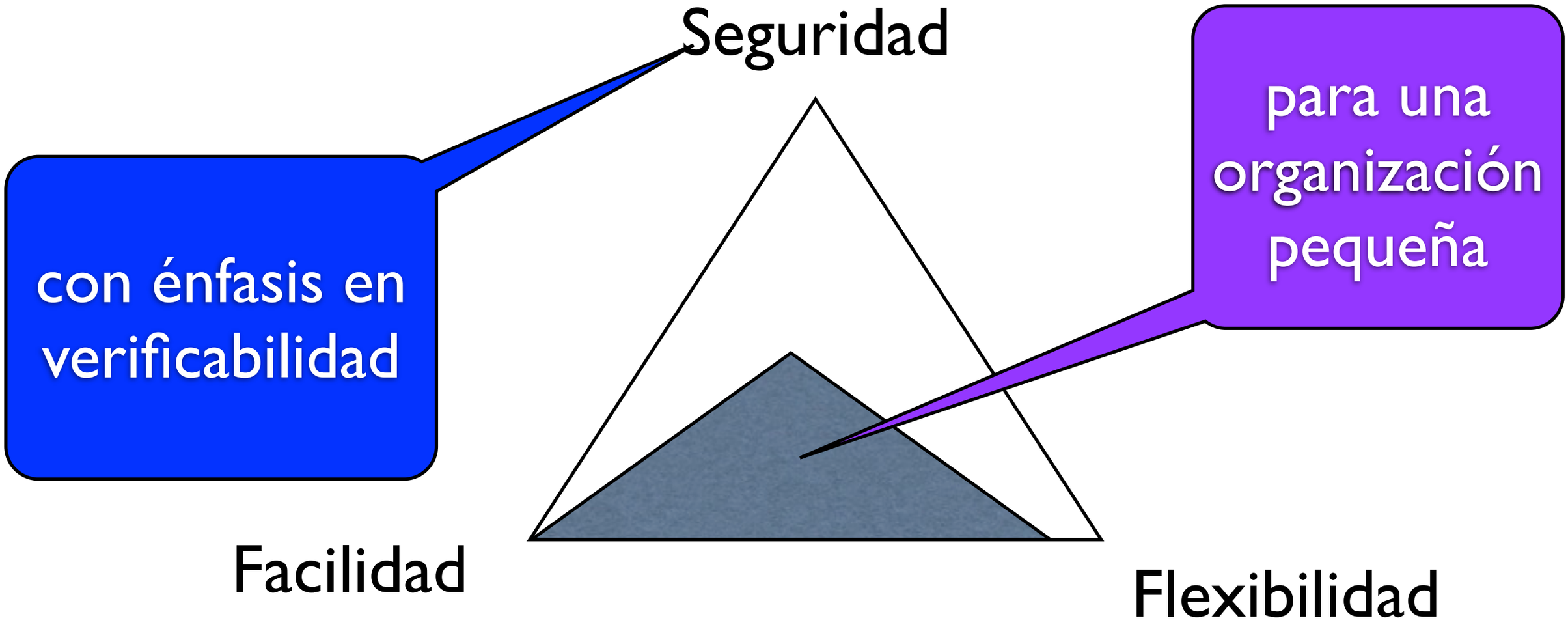


Depende de la situación

¿Donde esta el balance óptimo?



¿Donde esta el balance óptimo?



Gracias por su atención