+10 anys gestionant

La seguretat de la informació

Módulo de Criptografía Aplicada

MTSI 5a edició

2006-2007

Profesor: Jordi Puiggalí

Índice

01 Protección de la propiedad intelectual

- Esteganografía
- Watermarking
- Fingerprinting

01 01 Protección de la propiedad intelectual (PI)

Aumento del volumen de bienes digitales disponibles: imágenes, películas, programas, etc..

Protección de la PI de bienes en formato digital:

- Impedir el acceso a los contenidos:
  - Content Scramble System (CSS)
  - Windows Media
- Impedir la copia de los contenidos
  - Macrovision: VHS, DVD
  - Juegos de consola: Playstation 2, XBox
- Detección de copia
  - Marcar el objeto digital

01 02 Esteganografía

La esteganografía es el arte de esconder un mensaje dentro de otro, de manera que una tercera parte no pueda saber el contenido, o la presencia, del mensaje ocultado*

Utilizamos la esteganografía para proteger la PI de datos multimedia.

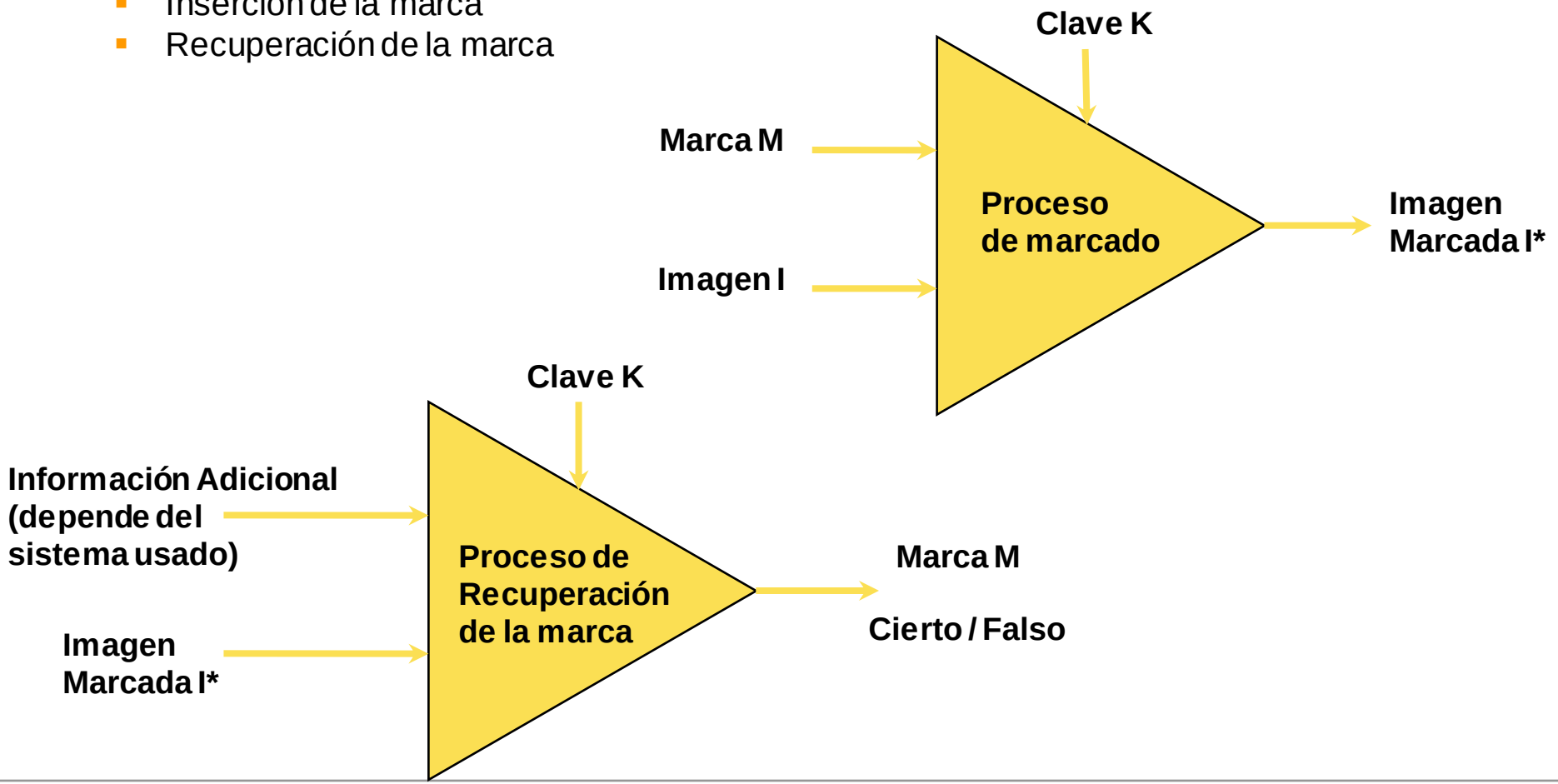
Utilización de Criptografía y esteganografía conjuntamente

*[Katzenbeisser et al 00]

01 03 Esquema de marcado de imágenes

Algoritmos de un esquema de marcado:

- Inserción de la marca
- Recuperación de la marca



01 04 Ejemplo de marcado de imágenes

Pixel 24bits

Red	1	0	0	1	0	1	1	0
Green	1	0	0	1	0	1	1	0
Blue	1	0	0	1	0	1	1	0

Si utilizamos los 2 últimos bits para almacenar una información (p.e., 101101)

1	0	0	1	0	1	1	0
1	0	0	1	0	1	1	1
1	0	0	1	0	1	0	1

Diferencia no perceptible

En una imagen de 1 Megapixel podríamos almacenar hasta 6Megabits de información

01 05

Tipos de marcas:

Watermarking: Identifica al propietario del contenido

Fingerprinting: Identifica al propietario de la copia del contenido

Watermarking

La copia incluye una marca que identifica al propietario del contenido

Todas las copias del producto tienen la misma marca

Propiedades que debe cumplir un esquema de watermarking:

- Impercibilidad
- Resistencia
- Tasa de información
- Información secreta

01 07 Watermarking: Impercibilidad vs Resistencia

En las imágenes modificamos los píxeles para insertar la marca

Alteraciones	Resistencia	Impercibilidad
Bajas	Baja	Alta
Altas	Alta	Baja

Modificar directamente los píxeles de la imagen

- Calcular la máxima alteración posible [Herrera 00]

Modificar los coeficientes de un dominio transformado

- Hallar los coeficientes susceptibles de modificación [Herrigel 98] [Caramma 00]

01 08 Watermarking: clasificación de los esquemas

Clasificación según la información necesaria para recuperar la marca:

- Privado:
  - Entrada: imagen marcada (I*), imagen original (I), clave secreta (K), marca (M)
  - Salida: Cierto / Falso
- Semi-público:
  - Entrada: I*, K, M -- Salida: Cierto / Falso
  - Entrada: I*,K, I -- Salida: M
- Publico:
  - Entrada: I*, K
  - Salida:M

01 09 Watermarking: Oblivious watermarking

No necesitan la imagen marcada para recuperar la marca

Desventajas:

- Necesitan la secuencia de marcaje
- Poca resistencia a los ataques de escalado, o distorsión geométrica

Ejemplos comerciales:

- Digimarc (www.digimarc.com)
  - Algoritmos secretos (no cumplen el principio de Kerckhoffs)

01 10 Fingerprinting

La copia incluye una marca que identifica al comprador de ésta.

Si se halla una copia distribuida ilegalmente se identifica al comprador que la ha distribuido.

Propiedades:

- Las mismas que los esquemas de Watermarking
- Seguridad contra confabulaciones
- Seguridad para el comprador
- Anonimato del comprador

01 11 Fingerprinting: Propiedades

Seguridad contra confabulaciones

- Comparación de los objetos digitales para hallar las marcas

Seguridad para el comprador

- Redistribución de los objetos digitales por el vendedor
- Esquemas simétricos
- Esquemas asimétricos
- Confabulaciones de compradores

Anonimato para el comprador

- Solo se debe desvelar si el comprador no es honesto

02 Voto electrónico

- Propiedades
- Protocolos

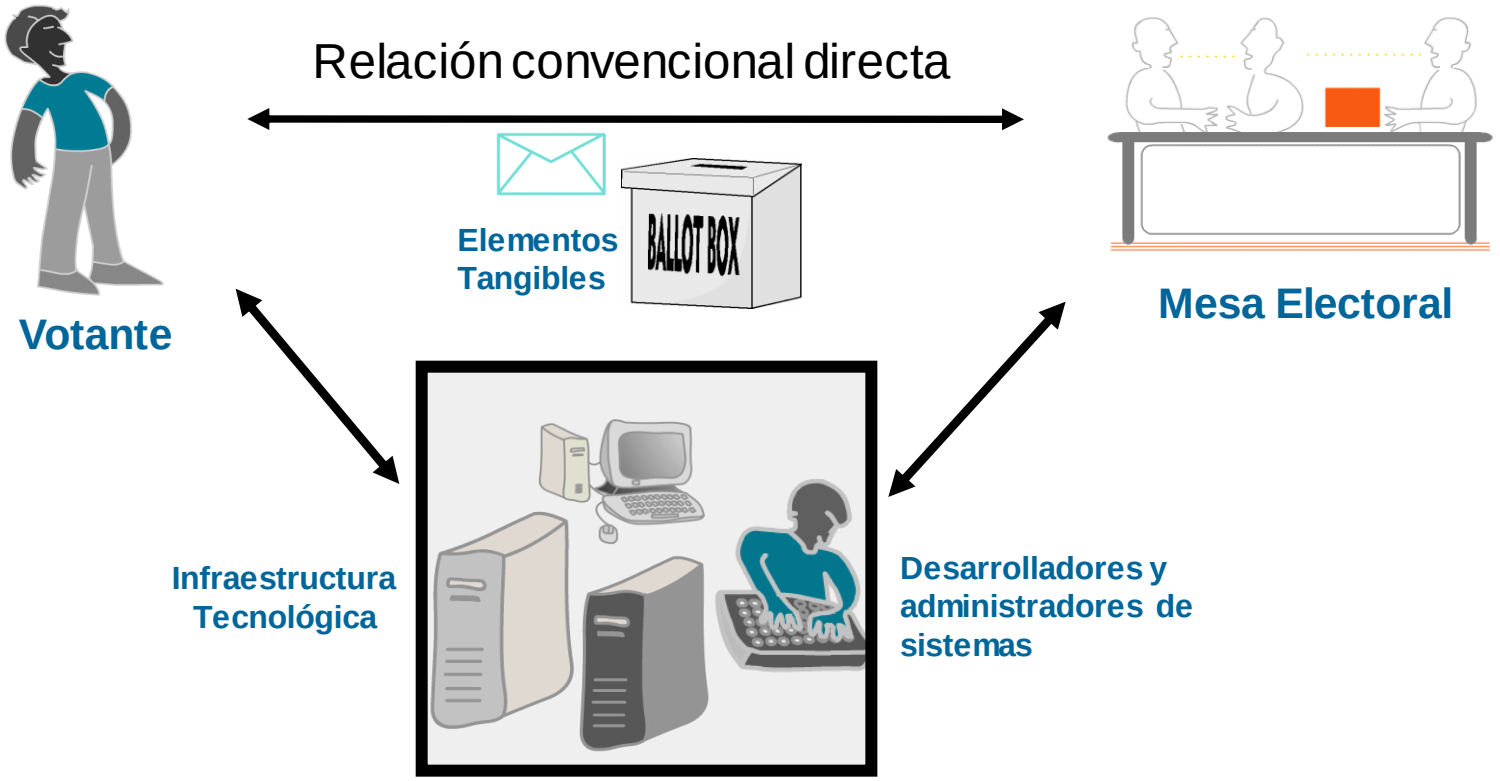
02 01 Voto Electrónico

Realizar el proceso de votación convencional mediante medios electrónicos

Tipos de e-Voting

- Poll-site: el votante debe desplazarse a un colegio electoral
- Remoto: el votante puede ejercer su derecho desde cualquier ubicación

02 02 Voto Electrónico: Cambio de paradigma



El voto electrónico introduce una nueva capa entre el votante y la mesa electoral, que implica **nuevos riesgos de seguridad** y reduce la confianza en el proceso electoral.

02 03 Voto Electrónico: Propiedades

Seguridad:

- Autenticidad de los votos
- Privacidad de los votantes
- Corrección de los resultados de la elección
- Privacidad de los resultados intermedios
- Verificabilidad de los votos
- No coerción

02 04

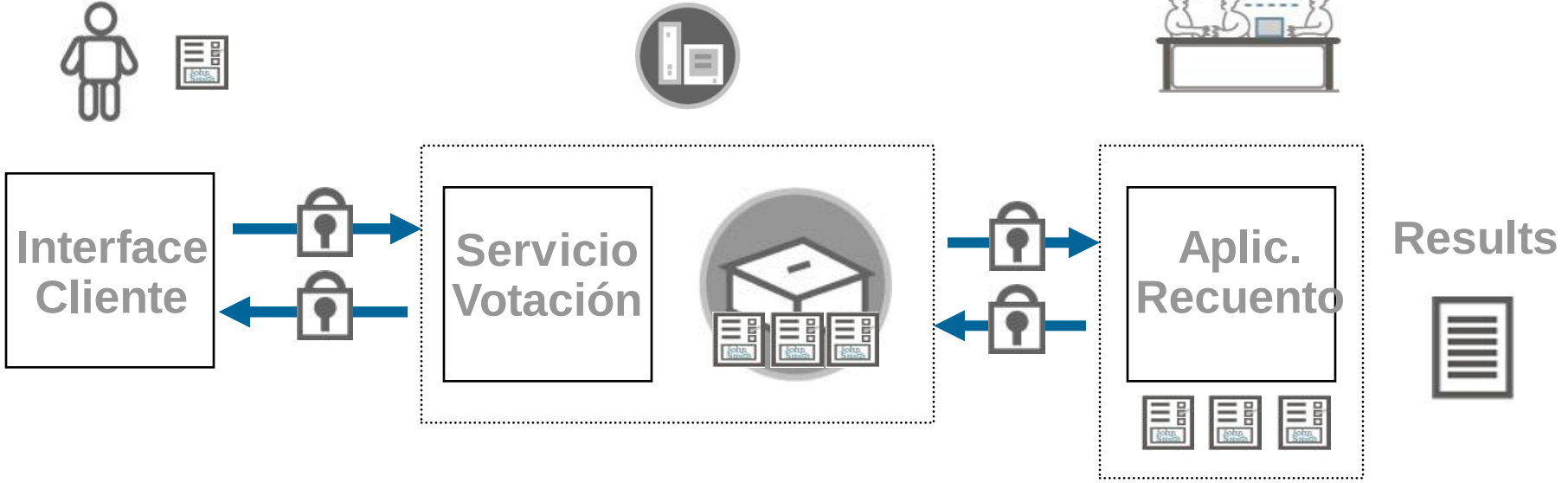
Voto electrónico: Propiedades (ii)

Conveniencia

- Flexibilidad
- Movilidad
- Escalabilidad
- Eficiencia

02 05

Voto electrónico: Elementos



- SV: Servicio de votación, recoge los votos
- ME: Mesa electoral, tabula los votos
- V: Votante

02 06 Voto electrónico: Protocolo simple

Votante

- Obtiene un identificador único Id
- Envía su voto con su Id al Servicio de Votación

Servicio Votación

- Verifica si el votante pertenece al censo y no ha votado préviamente
- Almacena el voto

Mesa Electoral

- Realiza la tabulación de los votos

02 07 Voto electrónico: Protocolo simple

Autenticidad de los votos ✗

Privacidad de los votantes ✗

Corrección de los resultados de la elección ✗

Privacidad de los resultados intermedios ✗

Verificabilidad de los votos ✗

No coerción ✓

02 08

Voto electrónico: Protocolos criptográficos

Protocolos basados en el modelo de las dos agencias

- Objetivo: separar la autenticación del votante del proceso de emisión del voto
- Generalmente utilizan la firma ciega para conseguir un voto válido y anónimo

Protocolos basados en las propiedades aditivas homomórficas

- Objetivo: obtener los resultados finales de la elección operando los votos cifrados
- Generalmente basados en El Gamal

Protocolos basados en técnicas de Mixing

- Objetivo: conseguir romper la correlación de los votantes y votos mediante el uso de una Mix-Net
- Actualmente los más estudiados

02 09 Voto electrónico: Modelo de las dos agencias

Obtener un voto validado por el sistema de votación sin que se sepa cuál es su contenido

Dos servidores:

- Servidor de validación de los votos
- Servidor de almacenaje de los votos

Suelen basarse en el uso de la firma ciega

Firma ciega

El concepto de firma ciega fue introducido por Chaum en 1982

Permite obtener la firma digital de un mensaje de un tercero sin que éste sepa el contenido de lo que está firmando

Recordatorio RSA:

- Clave pública: (e,n) -- clave privada: (d)
- Firma "s", de un mensaje *m:* $s = m^d \bmod n$,
- Verificación de la firma s: $s^e \bmod n = m$

02 11 Firma ciega (ii)

Firma ciega con RSA:

- C realiza los pasos siguientes:
  - genera un número aleatorio: $r \bmod n$
  - tapa el mensaje m:
    - $m' = m\, r^e \bmod n$
- B recibe m', y lo firma:
  - $s' = (m')^d \bmod n = m^d (r^e)^d \bmod n = m^d r \bmod n$
- *C recibe s' y destapa la firma:*
  - $s = s'/r = (m^d r)/r \bmod n = m^d \bmod n$

02 12 Voto electrónico: Modelo de las dos agencias - protocolo

Votante

- Escoge sus opciones de voto, los cifra y solicita una firma ciega del voto cifrado al servidor de validación

Servidor de validación

- Verifica si el votante que hace la solicitud de firma ciega esta en el censo y no ha votado
- Si todo es correcto realiza la firma ciega y envía ésta al votante

Votante

- Deshace la firma ciega y verifica que se corresponde con el voto cifrado
- Envía el voto cifrado con la firma recuperada al servidor de almacenaje de votos

Servidor de almacenaje

- Recibe el voto cifrado y firmado, y lo almacena

Mesa Electoral

- Descifra los votos y hace el recuento

02 13 Voto electrónico: Modelo de las dos agencias - análisis

Autenticidad de los votos !

Privacidad de los votantes ✓

Corrección de los resultados de la elección !

Privacidad de los resultados intermedios ✓

Verificabilidad de los votos !

No coerción ✓

Protocolos basados en las propiedades aditivas homomórficas

Obtener el resultado de la elección sin necesidad de descifrar los votos individualmente

Verificación universal

Suelen basarse en las propiedades de operación aditiva de los algoritmos homomórficos

- El Gammal
- Palier

Sólo funciona cuando el voto se puede representar de forma numérica. No sirve si hay opciones escritas

02 15 Propiedades aditivas algoritmos homomórficos

El concepto se basa en que el resultado de operar dos mensajes cifrados da como resultado el cifrado de la operación de los contenidos de los mensajes:

$$P(m_1) \cdot P(m_2) = P(m_1 \, o \, m_2)$$

En el caso de El Gammal estamos hablando de un cifrado homomórfico con propiedades aditivas. El producto de los mensajes cifrados da como resultado el cifrado de la suma de los mensajes:

$$P(m_1) * P(m_2) = P(m_1 + m_2)$$

De este modo, se pueden operar los votos cifrados y obtenemos el cifrado de la suma de los votos. La Mesa Electoral sólo debe descifrar esta suma y obtiene el resultado

02 16 Voto electrónico: Protocolo basado en algoritmos homomórficos

Votante

- Escoge sus opciones de voto, los con un algoritmo homomórfico, lo firma digitalmente y lo envía al servicio de votación

Servicio de votación

- Verifica si el votante esta en el censo y no ha votado
- Almacena el voto cifrado y firmado

Mesa Electoral

- Opera los votos cifrados
- Descifra el resultado

Voto electrónico: Protocolo basado en algoritmos homomórficos - análisis

Autenticidad de los votos ✓

Privacidad de los votantes ✓

Corrección de los resultados de la elección !

Privacidad de los resultados intermedios ✓

Verificabilidad de los votos ✓

No coerción ✓

Protocolos basados en Mixing

Romper la correlación entre los votos y los votantes

Facilitar la verificación de los votantes

Facilitar la auditoría

Tipos de Mixing

- Mixing con descifrado
- Mixing con cifrado

02 19 Mixing

El concepto se basa en hacer un cifrado o descifrado de los votos y a la vez mezclar de forma aleatoria los votos.

Este mecanismo permite romper la correlación entre los votos cifrados y los votos en claro.

Mixing con descifrado:

- Los votos son cifrados de forma anidada por los votantes utilizando primero la clave de la Mesa Electoral y luego las claves de los nodos del mix-net
- Los diferentes nodos del Mix-net descifran cada capa con sus claves

Mixing con cifrado:

- Basados en las propiedades de los protocolos homórficos: si se cifra más de una vez un mensaje sólo se necesita un solo descifrado para obtenerlo
- Los votos son cifrados por los votantes con la clave de la Mesa Electoral
- Los diferentes nodos del Mix-net vuelven a cifrarlos con la clave de la Mesa Electoral
- La Mesa Electoral descifra los votos en un único paso

Voto electrónico: Protocolo basado en Mixing

Votante

- Escoge sus opciones de voto y la cifra con la clave de la mesa electoral
- Si utiliza un mix-net con cifrado cifra de forma anidada el voto con las claves de los distintos nodos
- Firma el voto cifrado y lo envía al servicio de votación

Servicio de votación

- Verifica si el votante esta en el censo y no ha votado
- Almacena el voto cifrado y firmado

Mixing

- Cada nodo descifra o vuelve a cifrar los votos y los mezcla
- Los votos cifrados/descifrados son enviados al siguiente nodo

Mesa Electoral

- Recibe los votos cifrados y mezclados del último paso del mixing
- Descifra los votos
- Hace el recuento

02 21 Voto electrónico: Protocolo basado en Mixing - análisis

- Autenticidad de los votos ✓
- Privacidad de los votantes ✓
- Corrección de los resultados de la elección ✓
- Privacidad de los resultados intermedios ✓
- Verificabilidad de los votos ✓
- No coerción ✓

03 Dinero digital (e-cash)

- Propiedades
- Esquema de pago con e-cash

03 01 E-Cash

Representación de la moneda física en formato digital

Ejemplos de dinero digital:

- Tarjetas de crédito/débito
- Cuentas en el comercio previamente abiertas
- Sistemas de pago P2P

No confundir con sistemas de pago de transacciones bancarias:

- SET (Secure Electronic Transacion)

03 02 E-Cash: Propiedades*

Independencia del soporte físico

Seguridad

- Infalsificable
- Evitar el gasto múltiple

Privacidad de las compras

Mínimas operaciones online

Transferencia a otros usuarios

Divisibilidad*

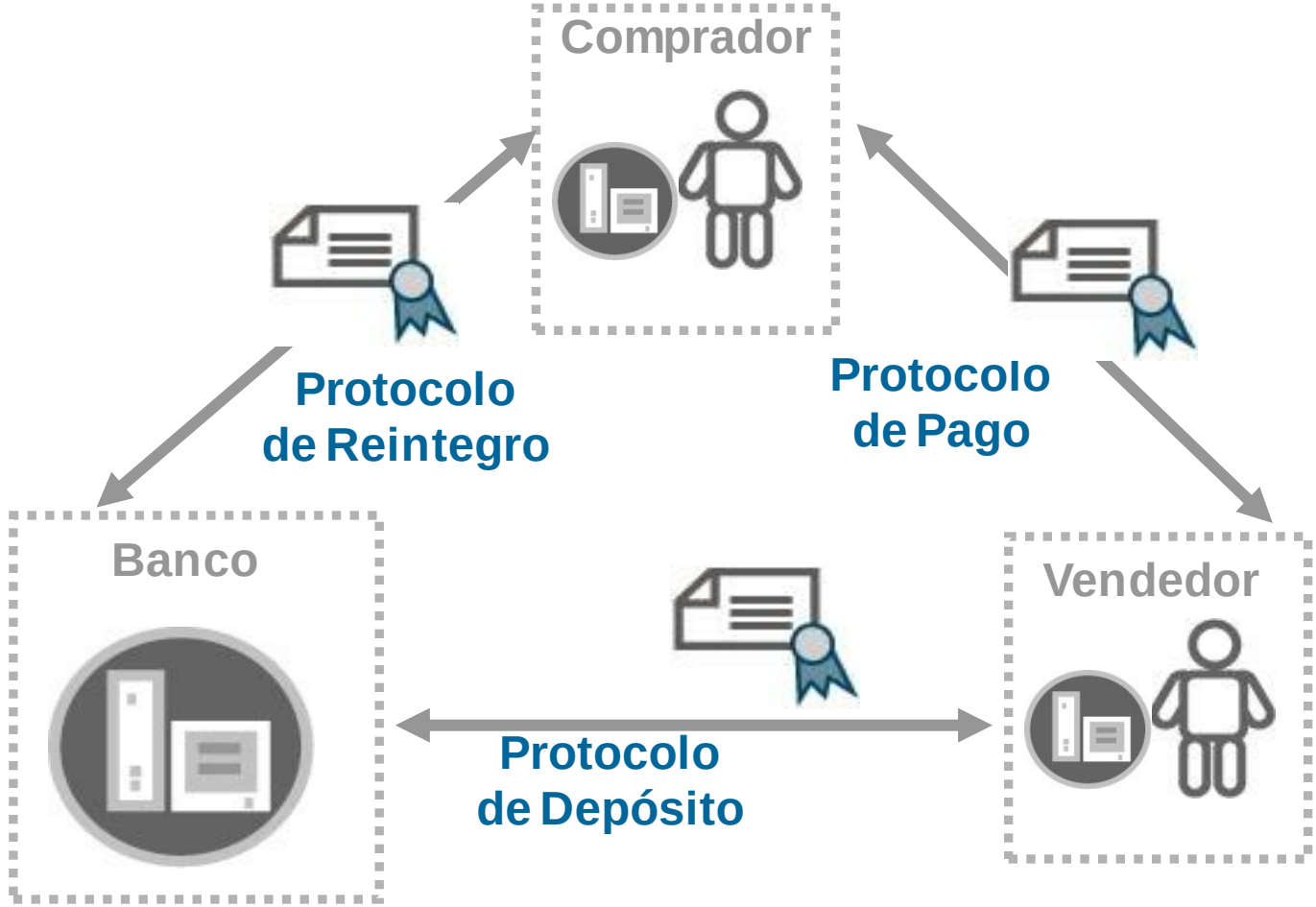
*[Okamoto et al 91]

03 03 E-Cash: Esquema de pago

Un esquema de pago consta básicamente de tres protocolos:

- Protocolo de Reintegro: el comprador C, obtiene las monedas del banco B
- Protocolo de Pago: el comprador entrega la moneda al vendedor V
- Protocolo de Depósito: El vendedor deposita las monedas en el banco B

E-Cash: Esquema de pago



E-Cash: Protocolo de Reintegro

El comprador *C* quiere retirar 20€ del banco *B*

B realiza las operaciones siguientes:

- extrae 20€ de la cuenta de C
- construye un billete mediante la firma con su clave privada K, (billete 20€, #serie):
  - S_K (billete 20€, #serie)
  - *#serie* es diferente para cada billete

C comprueba la firma del billete, y si es correcta, acepta el billete

E-Cash: Protocolo de Pago

Protocolo de pago:

- *C* paga al vendedor *V* con el billete obtenido previamente
- *V* comprueba la firma del billete, y si es correcta, lo acepta

03 07 E-Cash: Protocolo de Depósito

Protocolo de deposito:

- *V* deposita el billete en el banco (B)
- B comprueba la firma del billete, y si es válida, ingresa su valor en la cuenta de *V*

03 08 E-Cash: Propiedades del Esquema de Pago

Independencia del soporte físico ✓

Seguridad

- Infalsificable ✓
- Evitar el gasto múltiple ✗

Privacidad de las compras ✗

Mínimas operaciones online ✓

Transferencia a otros usuarios ✗

Divisibilidad de la moneda ✗

E-Cash: Esquema de pago II

B firma el billete sin conocer su contenido, mediante una firma ciega.

El comprador *C* "enmascara" el billete, y lo envia al banco *B*

B emite el billete (firma) sin conocer exactamente su contenido

El vendedor V ingresa el billete en *B, pero B* no puede saber quien lo retiró

E-Cash: Propiedades Esquema de pago II

- Independencia del soporte físico ✓
- Seguridad
  - Infalsificable **!**
  - Evitar el gasto múltiple ✗
- Privacidad de las compras ✓
- Mínimas operaciones online ✓
- Transferencia a otros usuarios ✗
- Divisibilidad de la moneda ✗

03 11 E-Cash: Evitar la alteración del importe de los billetes

Infalsificable !

- *B* tiene un par de claves para cada importe de billete diferente.
- Protocolo de remover y escoger

E-Cash: Remover y escoger

C :

- fabrica *n* billetes de 20€
- enmascara los billetes, usando un valor aleatorio "*r*" diferente para cada billete
- envía los *n* billetes enmascarados a *B*

B :

- escoge un billete al azar
- pide a *C* que desenmascare el resto (n-1)
- Si todos los n-1 billetes desenmascarados son correctos, *B* firma el billete que ha escogido
- La probabilidad de engaño a B por parte de C es de *1/n*.

E-Cash: Propiedades Esquema de pago III

- Independencia del soporte físico ✓
- Seguridad
  - Infalsificable ✓
  - Evitar el gasto múltiple ✗
- Privacidad de las compras ✓
- Mínimas operaciones online ✓
- Transferencia a otros usuarios ✗
- Divisibilidad de la moneda ✗

E-Cash: Evitar el gasto múltiple

Sistema online:

- B registra los billetes recibidos en una BD
- V envía el billete B durante el protocolo de Pago
- B comprueba si el billete ya ha sido usado
- V acepta el billete si la respuesta de B es afirmativa.

Requiere muchas comunicaciones y gestionar una gran base de datos

E-Cash: Propiedades Esquema de pago IV

- Independencia del soporte físico ✓
- Seguridad
  - Infalsificable ✓
  - Evitar el gasto múltiple ✓
- Privacidad de las compras ✓
- Mínimas operaciones online **!**
- Transferencia a otros usuarios ✗
- Divisibilidad de la moneda ✗

E-Cash: Evitar el gasto múltiple

Sistema offline:

- El comprador *C* crea una *Tira Aleatoria de Identificación* (TAI) diferente para cada billete
- Dos TAI diferentes sobre el mismo billete permiten recuperar el nombre del comprador *C*
- *C* es el único que puede crear una TAI válida

E-Cash: Evitar el gasto múltiple

- Si *B* recibe dos billetes idénticos con TAIs diferentes, entonces *C* ha hecho trampas y se le puede identificar
- Si *B* recibe dos billetes idénticos con la misma TAI, entonces el vendedor *V* es quien ha hecho trampas

E-Cash: Protocolo de reintegro con TAIs

C realiza las operaciones siguientes:

- prepara *n* billetes de 20€:
  - $m_i = (billete\ 20€, \#nserie, y_{i,1}, y'_{i,1}, \ldots, y_{i,K}, y'_{i,K})$
  - $y_{i,j} = H(x_{i,j})$, $y'_{i,j} = H(x'_{i,j})$,
  - $x_{i,j}$ e $x'_{i,j}$ son elegidos aleatoriamente
  - $x_{i,j} \oplus x'_{i,j} = Id\ de\ C\ para\ \forall i,j$
- tapa los billetes m_i, obteniendo m'_i, y los envía a *B*

E-Cash: Protocolo de reintegro con TAIs

B realiza las operaciones siguientes:

- *Pide a C* que destape *n-1* billetes, y revele los $x_{i,j}$ y $x'_{i,j}$ de cada billete
- *B* comprueba que son billetes de 20€ y los $y_{i,j}$, $y'_{i,j}$, $x_{i,j}$ y $x'_{i,j}$ cumplen las condiciones anteriores
- Si todo es correcto, *B* envía a C la firma *s'* para el billete tapado *m' que ha escogido*

C obtiene el billete firmado *s a partir de m'*

E-Cash: Protocolo de pago con TAIs

C envía *m* y *s* al vendedor *V*

V comprueba la firma de *B* sobre el billete

Si es correcta, genera una tira aleatoria de *k* bits $(b_1,\ldots,b_k)$ que envía como reto a *C*

Si $b_j = 0$, *C* revela x_j; sino, *C* revela x'_j

El vendedor *V* comprueba

- $y_j = H(x_j)$ o $y'_j = H(x'_j)$, según el caso.

Si todas las comprobaciones son correctas, *V* acepta el billete

La TAI es la secuencia de x_j y x'_j seleccionadas aleatoriamente por *V* con la tira de *k* bits

03 21 E-Cash: Protocolo de pago con TAIs

La probabilidad de que el mismo billete en otro pago genere la misma TAI es de 2^{-k}

Las funciones hash son unidireccionales, sólo *C* puede generar TAIs válidas

Dos TAIs diferentes sobre el mismo billete revelan el nombre de *C*, ya que para algún índice *j* tendremos x_j y x'_j

E-cash: Protocolo de depósito con TAIs

V entrega el billete "*m*", *la firma "s"* y la TAI generada, a *B*

B comprueba *s*, y verifica si el billete ya había sido depositado

Si el billete está en la base de datos, *B* compara las TAIs de ambos billetes.

- Si son diferentes, *C* ha usado el billete dos veces, y es identificado
- Si son iguales, *V* intenta depositar el billete dos veces

E-Cash: Propiedades Esquema de pago V

- Independencia del soporte físico ✓
- Seguridad
  - Infalsificable ✓
  - Evitar el gasto múltiple ✓
- Privacidad de las compras ✓
- Mínimas operaciones online ✓
- Transferencia a otros usuarios ✗
- Divisibilidad de la moneda ✗

E-Cash:

Esquema de pago que cumple todas las propiedades [Okamoto 91]

- Patentado por la NTT: Electronic cash implementing method using a trustee US PT OFFICE 5,091,229

DigiCash:

- Empresa fundada por David Chaum.

04

Juego online (e-gambling)

- Honestidad y Auditoria
- Generación Colaborativa
- Protocolo de compromiso

04 01 Juego online:

El juego se desarrolla a través de una red de comunicación

Tipos de juegos:

- Acción: Quake Arena
- Estrategia: Age of Empires
- Casino: Black Jack, Poker

Nos centraremos en la seguridad de los juegos de tipo Casino

04 02 Juego online: Seguridad

Seguridad en el juego electrónico remoto:

- Honestidad en el juego remoto
- Auditoria de las acciones del juego remoto

04 03 Juego online: Honestidad

Reproducción honesta del azar:

- Obtener un evento al azar: cara de un dado, posición de la ruleta, carta de una baraja, etc..
- Garantizar la imparcialidad
- Secreto de los eventos

Detectar las “trampas” con gran probabilidad

04 04 Juego online: Honestidad

Juegos de cartas:

- Unicidad de las cartas
- Confidencialidad de las cartas
- Confidencialidad de la estrategia
- Minimizar el efecto de las confabulaciones de jugadores

04 05 Juego online: Auditoria

Registrar la secuencia de acciones sucedidas durante el juego

Garantizar la integridad de la secuencia:

- Inserción
- Eliminación

Seguridad de las acciones registradas:

- Autoría (Autenticidad)
- Integridad
- No repudio

Juego online: TTP

El juego es gestionado por una tercera parte de confianza (TTP)

La TTP utiliza un Generador de Números Pseudo-Aleatorios (PRNG) para obtener los eventos del juego

La TTP guarda las acciones sucedidas durante la partida

Juego online: TTP

Ejemplo: Ruleta

- El jugador apuesta 20€ al 10
- La TTP realiza las operaciones siguientes:
  - Obtiene un valor mediante el PRNG: 292211992
  - Escala el valor obtenido: 292211992 mod 38 = 10
  - Envía el resultado al cliente: 10
- El jugador comprueba si ha ganado, o perdido

04 08

Juego online: TTP

Reproducción honesta del azar:

- Obtener un evento al azar ✗
- Garantizar la imparcialidad ✗
- Secreto de los eventos ✗

Detectar las “trampas” con gran probabilidad ✗

04 09 Juego online: Generación colaborativa

Todos los jugadores participan en la obtención del evento azaroso

Cada jugador genera un valor

El evento se obtiene operando todos los valores de los jugadores

Garantizar la generación independiente de los valores de los jugadores

- Utilización de un Protocolo de compromiso

04 10 Juego online: Protocolo de Compromiso

Concepto introducido por M. Blum (Coin flipping by telephone, 1982)

El protocolo consta de dos fases:

- Fase de compromiso
- Fase de liberación

04 11 Juego online: Protocolo de Compromiso

Fase de de compromiso de un valor V:

- Transformar el valor V, Cp=F(V)
- Enviar Cp al resto de participantes
- No se puede hallar V a partir de Cp sin información adicional
- Cp es único para cada V

04 12 Juego online: Protocolo de Compromiso

Fase liberación:

- Enviar la información adicional para hallar V a partir de Cp, y /o V
- Verificar que con la información podemos obtener V a partir de Cp

04 13 Juego online: Protocolo de Compromiso

Métodos para implementar un protocolo de compromiso.

- Cifrado simétrico
- Cifrado asimétrico
- Función hash

Juego online: Protocolo de Compromiso

Generación conjunta entre A y B utilizando una función hash

A se quiere comprometer al valor 60:

- genera un número aleatorio *R*
- calcula Cp= *H(R,60)*
- envía Cp a B

B envía su valor, 120 a A

Juego online: Protocolo de Compromiso

A libera el compromiso y obtiene el resultado:

- envía los valores *R* y 60 a B
- calcula el resultado de la ruleta: 60+120 mod 38 = 28

B verifica el compromiso y obtiene el resultado:

- *H(R,60) = Cp' =?= Cp*
- Si la verificación es correcta calcula el resultado de la ruleta 60 + 120 mod 38 = 28

Juego online: Protocolo de Compromiso

Reproducción honesta del azar:

- Obtener un evento al azar ✓
- Garantizar la imparcialidad ✓
- Secreto de los eventos ✓

Detectar las “trampas” con gran probabilidad ✓

Juego online: Juegos de Cartas

Juegos de cartas descubiertas

- El protocolo de compromiso es suficiente

Juegos de cartas tapadas: Mental Poker

- El propietario es el único que debe conocer el valor de la carta
- Protocolos con un elevado coste computacional debido a su complejidad

Juego online: Mental Poker

1.- El jugador A que reparte las cartas: las mezcla, las cifra con su clave pública P_A, obteniendo $P_A[c_1, c_2, c_3, \ldots c_{50}, c_{51}, c_{52}]$, y las envía a B.

2.- B elige sus cartas (supongamos 5), las cifra con su clave pública y devuelve a A las cartas que ha cifrado: $P_B\{P_A[c_{B1}, c_{B2}, c_{B3}, c_{B4}, c_{B5}]\}$.

3.- A descifra las cartas cifradas por B usando su clave privada S_A y se le envía el resultado a B: $P_B[c_{B1}, c_{B2}, c_{B3}, c_{B4}, c_{B5}]$.

4.- B descifra ahora con su clave privada S_B lo recibido y obtiene su mano $c_{Bi} = c_{B1}, c_{B2}, c_{B3}, c_{B4}, c_{B5}$.

5.- El jugador B pasa las restantes 47 cartas al jugador C y se repiten los pasos 2 al 4 anteriores entre C y A, usando ahora las claves e_C, d_A y d_C.

Juego online: Mental Poker

6.- Terminado el paso 5, el jugador C tendrá entonces como mano $c_{Ci} = c_{C1}, c_{C2}, c_{C3}, c_{C4}, c_{C5}$.

7.- El jugador C pasa las restantes 42 cartas que quedan y que están cifradas con su clave pública: $P_c\{P_A[c_1, c_2, c_3, \ldots c_{36}, c_{37}]\}$ al jugador A.

8.-El jugador A elige 5 cartas entre las 42 y devuelve al jugador C: $P_c\{P_A[c_{A1}, c_{A2}, c_{A3}, c_{A4}, c_{A5}]\}$.

9.- El jugador C descifra con su clave privada S_C lo recibido y envía a A: $P_A[c_{A1}, c_{A2}, c_{A3}, c_{A4}, c_{A5}]$.

10.- El jugador A descifra con su clave privada d_A lo recibido y se queda con su mano $c_{Ai} = c_{A1}, c_{A2}, c_{A3}, c_{A4}, c_{A5}$.

Juego online: Mental Poker

[Shamir 81]: Mental Poker con dos jugadores

[Lipton 81]: Debilidades protocolo de Shamir

[Goldwasser 82]: Mental poker con dos jugadores

[Barany 83]: Más de dos jugadores, pero permite confabulaciones

[Fortune 84]: Utiliza una TTP al inicio del juego

[Crepeau 87]: Solución teórica, pero con un elevado coste computacional

Juego online: Auditoria

Autenticidad, integridad, no repudio de las acciones:

- Cada jugador dispone de un par de claves certificadas
- Cada jugador firma los mensajes que envía

Integridad de la secuencia de juego

- Copia de los mensajes en otro sistema remoto
- Cada jugador firma su mensaje y el mensaje anterior

Contacto

Cualquier duda, consulta o sugerencia, podéis encontrarme en:

Jordi.Puiggali@scytl.com

Secured by scytl

www.scytl.com

Barcelona
C/Gran Capitán, 2-4 Desp. 202
08034 Barcelona
T: (+34) 932 303 500

http://escert.upc.es_