Un Esquema de Pago Seguro mediante Multicupones para Escenarios Multi-Comerciante

Andreu Pere Isern-Deyà*, M. Francisca Hinarejos*, Josep Lluís Ferrer-Gomila*, Magdalena Payeras-Capellà*
Carlos Gañán†, José Luis Muñoz†, Jordi Forné†, Oscar Esparza†
*Universitat de les Illes Balears (UIB), Email: {andreupere.isern, xisca.hinarejos, jlferrer, mpayeras}@uib.es
†Universitat Politècnica de Catalunya (UPC), Email: {carlos.ganan, jose.munoz, jforne, oscar.esparza}@entel.upc.edu

***Resumen*—Un multicupón electrónico es el equivalente al bloc de cupones del mundo en papel, ofrecido por comerciantes a clientes para que puedan obtener descuentos o regalos. Hasta la fecha, muchas de las soluciones propuestas se han centrado en escenarios donde múltiples clientes pueden interactuar con un único comerciante. Pero esta restricción es un serio inconveniente para la expansión en el uso de cupones electrónicos, ya que cada cliente necesita una relación preestablecida con cada comerciante. En este artículo proponemos un nuevo esquema de multicupón para escenarios multi-comerciante, preservando las propiedades de seguridad de las soluciones previas con un único comerciante, y mejorando la eficiencia y la seguridad de las propuestas anteriores para escenarios multi-comerciante.**

***Index Terms*—cupón electrónico, no falsificable, anonimato, revocación del anonimato, afiliación de comerciantes**

I. Introducción

Un cupón es un documento impreso que permite al consumidor conseguir descuentos u obsequios cuando adquire bienes o servicios de un comerciante. Los comerciantes pueden usar los cupones para incrementar las ventas (atrayendo a nuevos consumidores, recompensando su fidelidad, etc.) o los empleados pueden recibir cupones de sus empresas (por ejemplo, talonarios de cupones para restaurantes [1], [2]). Por lo tanto, los cupones en papel son una herramienta útil tanto para los comerciantes como para los clientes. De hecho, los cupones electrónicos son una de las áreas donde el comercio electrónico ha recibido una especial atención en los últimos años [3]–[10].

Existen diferentes tipos de cupones en papel. Los hay anónimos o nominales, emitidos por comercios o por un emisor común para un conjunto de comerciantes, pueden gastarse por un único consumidor o este consumidor puede darlos o venderlos a otros consumidores, etc. Por tanto, tenemos que definir qué tipo de cupones queremos trasladar a la versión electrónica, ya que la solución dependerá del escenario de aplicación.

En nuestro escenario un conjunto de comercios delegan la tarea de emitir cupones a una entidad emisora; esta entidad emite cupones que pueden gastarse en esos comercios. De esta manera, identificamos tres tipos de actores: consumidores o clientes (interesados en obtener bienes o servicios a mejor precio); comerciantes (interesados en incrementar sus ventas con nuevos clientes o clientes ya fidelizados); y el emisor (entidad que emite cupones a los clientes quienes podrán gastarlos en diferentes comercios). Por otro lado, los comerciantes prefieren que los clientes compren blocs de cupones, más que cupones individuales. Por su parte, los clientes quieren un precio menor al comprar un bloc. En la versión electrónica, al bloc de cupones se le conoce como multicupón: un conjunto de cupones que se manejan como una sola unidad [7]. Aunque inicialmente los cupones tienen que ser gastados por el cliente que los ha solicitado, un cliente puede entregar a otro cliente de su confianza unos cupones como regalo.

Contribución. En este artículo proponemos un esquema de multicupones para un escenario donde los clientes pueden gastar cupones de un mismo multicupón en diferentes comercios afiliados a una entidad emisora. La propuesta usa multicupones anónimos y no rastreables, permitiendo que nadie pueda determinar quién gasta un cupón ni dónde se ha gastado. Nuestra solución proporciona un alto grado de privacidad para los clientes honestos y protege a los comercios frente a posibles comportamientos fraudulentos de los clientes, pudiendo llegar a revocar su anonimato. Además, nuestra propuesta mejora la eficiencia de soluciones previas durante el proceso de pago. Finalmente, y especialmente novedoso, los comercios pueden unirse y abandonar la afiliación sin problemas de seguridad ni para los clientes ni para los emisores de multicupones, a diferencia de [9].

Organización. El artículo está organizado de la siguiente forma. En la Sección II describimos los requisitos de seguridad necesarios para nuestro escenario. En la Sección III presentamos un análisis sobre las propuestas previas. En la Sección IV se resume el protocolo propuesto y se define la estructura del multicupón y su ciclo de vida. La especificación completa de la propuesta se explica en la Sección V. En la Sección VI proporcionamos un análisis de los requisitos de seguridad. Finalmente, en la Sección VII, se presentan las conclusiones.

II. Requisitos de Seguridad

A continuación, describimos los requisitos básicos de seguridad que tiene que cumplir una solución para multicupones [4]–[6]:

- *No falsificable*. Un cupón lleva asociado un valor monetario, explícita o implícitamente. Por lo tanto, un multicupón no debería poder ser falsificado, es decir, un cliente o una coalición de clientes no deberían poder gastar más cupones de los que contiene un multicupón, emitir nuevos multicupones o modificar su contenido.

- *Doble uso*. Además de detectar cupones falsos, también se debería detectar el uso de una copia de un cupón válido.
- *No enlazable*. Un comerciante no debería poder enlazar dos procedimientos de pago al procedimiento de emisión, o enlazar dos procedimientos diferentes de pago a un mismo cliente.
- *No divisible*. Podemos agrupar en dos las definiciones existentes sobre no divisibilidad. Por una parte se define la *no divisibilidad débil* [7], en la que compartir cupones requiere compartir toda la información secreta asociada a un multicupón. Esta solución está diseñada para disuadir a los clientes de compartir cupones. Por otro lado, se define la *no divisibilidad fuerte* cuando un único cliente puede utilizar a la vez cupones de un mismo multicupón. Esto hace que los clientes que compartan un mismo multicupón deban ser de confianza [9].

Además de los requisitos de seguridad anteriores, la privacidad es cada vez más importante ya que los comerciantes intentan obtener datos personales de los clientes. De esta manera, la privacidad trata sobre la información que revela un cliente sobre sí mismo, y de controlar quién puede acceder a esa información. Por otra parte, la seguridad de una solución de multicupón no puede verse comprometida cuando un comerciante abandona el escenario. A continuación definimos unos requisitos adicionales:

- *Anonimato del cliente*. La identidad del cliente tiene que ser preservada, es decir, los clientes han de poder obtener y gastar cupones sin necesidad de revelar su identidad. Ni el emisor ni los comerciantes han de poder obtener información acerca de la identidad de los clientes a través del uso de los cupones.
- *No rastreable*. Junto con el anonimato, la privacidad también está relacionada con la imposibilidad de rastrear las diferentes operaciones realizadas por un mismo cliente tanto en un mismo comercio como en diferentes comercios.
- *Confidencialidad de los datos intercambiados*. Los datos intercambiados entre las entidades participantes (clientes, comerciantes y emisor) sólo deben ser accesibles por las dos entidades finales que participan en la comunicación.
- *Revocación del anonimato del cliente*. Aunque se desea el anonimato de los clientes, el sistema debe proporcionar mecanismos para revelar su identidad cuando se comportan de forma deshonesta. Por ejemplo, cuando un cliente intenta utilizar un cupón falso o un mismo cupón dos veces.
- *Desafiliación de los comerciantes*. Si un comerciante abandona el sistema, la seguridad de la solución de multicupón no debe verse comprometida. Por lo tanto, el emisor y los comerciantes no pueden compartir información confidencial sobre los clientes, y el emisor no debe permitir a los comerciantes obtener beneficios de manera fraudulenta.

III. Trabajo Previo

En esta sección analizamos las propuestas existentes para multicupones electrónicos, considerando dos aspectos principales de las soluciones: funcionales y seguridad.

Con respecto a los aspectos funcionales, todas las soluciones analizadas [3]–[9] proporcionan los protocolos básicos necesarios para operar con multicupones (emitir y pagar) en escenarios con un único comerciante (simple-comerciante). Sin embargo, se necesitan más procedimientos para los escenarios más generales, como depositar y reembolsar. El protocolo de depósito es necesario cuando el comerciante no es el emisor de los multicupones. Este es el caso de un escenario multi-comerciante, como el propuesto en [9]. Por otro lado, un protocolo de reembolso permite a los clientes recuperar el valor de los cupones que no han sido gastados.

Otra funcionalidad interesante es el proceso de pago múltiple que puede definirse como el procedimiento que permite gastar más de un cupón en un mismo pago. Aunque éste es un proceso interesante, la gran mayoría de las soluciones analizadas requieren ejecutar el pago tantas veces como cupones individuales se necesiten utilizar. Este mecanismo es necesario para poder pagar de forma eficiente en un sistema multicupón, sin embargo, sólo lo contempla la solución en [6].

Con respecto a la seguridad, las soluciones deben tener en cuenta la privacidad de los clientes, y la detección y prevención del uso fraudulento de los multicupones. Casi todos los sistemas analizados cumplen con estos requisitos [3]–[9], sin embargo, el principal inconveniente de la inmensa mayoría de los sistemas es que están diseñados para escenarios con un único comerciante [4]–[8], donde toda la seguridad está controlada por el comerciante, ya que él es el responsable de la emisión y validación de los cupones. No obstante, en este tipo de esquemas, la utilidad de los multicupones y su difusión se ve reducida, ya que los clientes sólo pueden interactuar con el comerciante que emitió el multicupón. Esta limitación se solucionó en [9], en cuyo esquema los clientes pueden obtener y gastar multicupones en cualquiera de los comerciantes que pertenecen a una misma federación (asociación de comerciantes). Sin embargo, el comerciante que recibe un cupón, el cual fue expedido por otro comerciante, debe ponerse en contacto con el comerciante que emitió el multicupón con el fin de recuperar el descuento aplicado. Además, los comerciantes deben compartir la misma clave privada de la federación y una base de datos con la información sobre los cupones emitidos y gastados. De esta manera, cuando un comerciante deja la federación, tanto la clave privada como los datos compartidos pueden verse comprometidos. Éste es un problema de seguridad crítico y no resuelto por [9].

IV. Resumen de la Propuesta de 2D-multicupón

En esta sección presentamos un esquema multicupón, al que llamamos 2D-multicupón. El esquema cumple con todos los requisitos de seguridad en un escenario de múltiples comercios afiliados a una entidad emisora.

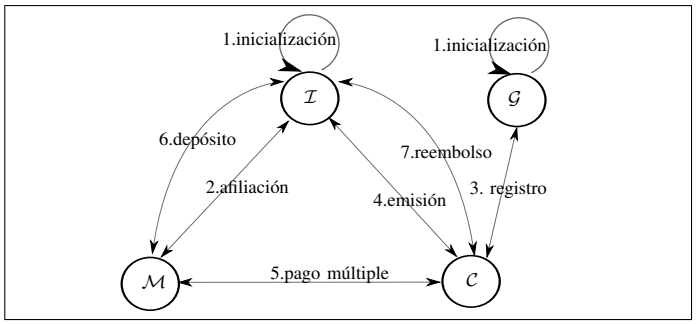

Figura 1: Escenario propuesto. Relación entre entidades y flujo de protocolo.

IV-A. Herramientas Criptográficas

Firma de grupo. Es una herramienta criptográfica cuyo objetivo es proporcionar anonimato a un firmante que pertenece a un grupo de usuarios. Cualquier miembro del grupo puede firmar mensajes, pero la firma resultante mantiene en secreto la identidad del usuario que ha firmado. Se define una tercera parte, llamada *Gestor de Grupo*, quien genera los parámetros necesarios para el funcionamiento del sistema y que además es capaz de revocar el anonimato y revelar la identidad del usuario que ha firmado. Para el desarrollo de nuestra solución, usamos el esquema de firma de grupo propuesto en [11]. A continuación definimos brevemente los procedimientos que usa:

- *KeyGen*$^G(n)$. Genera una clave pública de grupo (pk^G), una clave privada del Gestor de Grupo $(sk^G_{\mathcal{G}})$ y n claves privadas de usuario $(sk^G_1 ... sk^G_n)$.
- *Sign*$^G(pk^G, sk^G_u, M)$. Genera una firma de grupo σ sobre un mensaje M.
- *Verify*$^G(pk^G, M, \sigma)$. Verifica la validez de σ.
- *Open*$^G(pk^G, sk^G_{\mathcal{G}}, M, \sigma)$. Revela la identidad del firmante.

Firma parcial ciega. Está relacionada con la firma ciega [12], la cual se usa para firmar cierta información que está oculta para la entidad que la firma. Sin embargo, en [12], el firmante no tiene ningún control sobre los parámetros ocultos. En cambio, la firma parcial ciega agrega información común, previamente acordada entre firmante y solicitante, y que es visible para ambos. En nuestra propuesta usamos el esquema definido en [13] por su eficiencia y sencillez.

IV-B. Diseño y Estructura del 2D-multicupón

Siguiendo el escenario multi-comerciante considerado en §I, en la Fig. 1 se pueden distinguir las entidades consideradas, así como las interacciones entre las mismas: emisor $(\mathcal{I})$; comerciantes o vendedores $(\mathcal{M})$; y consumidores o clientes $(\mathcal{C})$. Además, introducimos una tercera parte de confianza, llamada Gestor de Grupo $(\mathcal{G})$, que genera, emite y gestiona pares de claves de grupo y que puede revelar la identidad de los clientes deshonestos.

En la Fig. 2 definimos una serie de marcas temporales para gestionar el ciclo de vida del 2D-multicupón y poder definir cuando se puede ejecutar cada protocolo. Estos valores

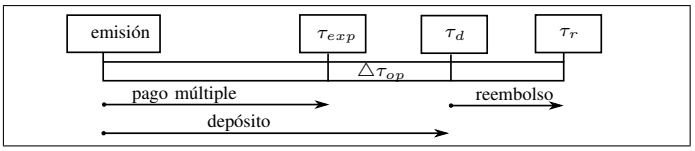

Figura 2: Ciclo de vida del 2D-multicupón

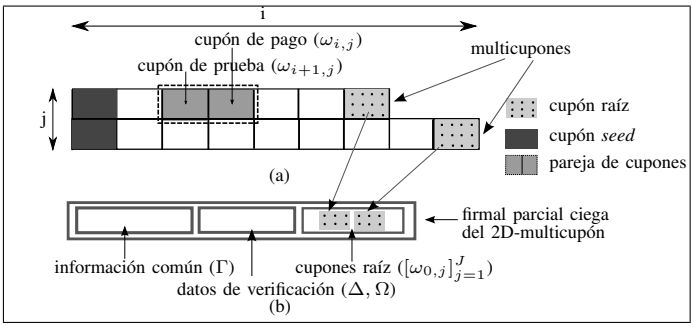

Figura 3: Estructura del 2D-multicupón $(\mathbb{MC}^{2D})$. (a) 2D-multicupones generados aplicando una cadena de hash $(\mathbb{MC}_{\omega})$. (b) Firma parcial ciega $(\mathbb{MC}_{\mathcal{PBS}})$ sobre los cupones raíz.

temporales están incluidos dentro de la información común del 2D-multicupón.

La Fig. 3 muestra la estructura del 2D-multicupón $(\mathbb{MC}^{2D})$. Como se puede observar, está compuesto por dos partes:

- Un número determinado de multicupones $(\mathbb{MC}_{\omega})$. Cada multicupón contiene una lista encadenada de cupones que puede tener diferente longitud y valor (Fig. 3.(a)). Estos cupones se obtienen aplicando un procedimiento de cadena de hash sobre un cupón inicial (*seed*) hasta el último elemento de la cadena llamado cupón raíz (*root*). Cada multicupón se divide conceptualmente en dos grupos de cupones: *cupones de pago* y *cupones de prueba*. El primero tiene valor monetario mientras que el segundo se usa para probar la posesión del primero. Los cupones se gastan en parejas, donde cada *cupón de pago* se usa junto con un *cupón de prueba*.
- La firma parcial ciega sobre los cupones raíz $(\mathbb{MC}_{\mathcal{PBS}})$. La firma parcial ciega (Fig. 3.(b)) se genera mediante la cooperación de $\mathcal{I}$ y $\mathcal{C}$ en la emisión del 2D-multicupón. Esta parte contiene tres datos: información común en claro (Γ) (ver Cuadro I); datos de verificación (Δ, Ω); y los cupones raíz de cada multicupón $([\omega_{0,j}]_{j=1}^{J})$.

V. Especificación Completa del Protocolo

En esta sección se definen todos los protocolos en detalle. El Cuadro I muestra la notación usada.

V-A. Inicialización del Sistema

Tanto $\mathcal{G}$ como $\mathcal{I}$ tienen que inicializar sus servicios (ver Fig. 1). Por una parte, $\mathcal{G}$ genera los parámetros para usar el esquema de firma de grupo. Por otra parte, $\mathcal{I}$ crea un par de claves RSA para usar el esquema de firma parcial ciega.

Cuadro I
NOTACIÓN USADA EN LA DESCRIPCIÓN DEL PROTOCOLO.

Notación General	
$\mathcal{H}(x)$	Función de hash resistente a colisión
$\mathcal{H}^i(x)$	Función de hash $\mathcal{H}()$ aplicada i veces
$\mathbb{SK}_{\mathcal{X}}$ y $\mathbb{PK}_{\mathcal{X}}$	Par de claves de un criptosistema de clave pública
$Cert_{\mathcal{X}}$	Certificado de clave pública de la entidad $\mathcal{X}$
$\mathbb{S}_{\mathcal{X}}(x)$	Firma sobre x realizada por $\mathcal{X}$
$x \overset{R}{\leftarrow} \mathbb{Z}_r$, $x \overset{R}{\leftarrow} \mathbb{Z}_n^*$	x obtenido aleatoriamente en $\mathbb{Z}_r$ o $\mathbb{Z}_n^*$
$\mathbb{K}_S$	Clave de cifrado simétrica
$\mathbb{E}_{\mathbb{K}_S}[x]$ y $\mathbb{D}_{\mathbb{K}_S}[x]$	Cifrado y descifrado de x usando $\mathbb{K}_S$
$\mathbb{SG}_{\mathcal{G}}(x)$	Firma de grupo sobre x generada mediante *Sign*^{G}
$A_k\|_{k=1}^K$	Concatenación de los elementos indexados A_k donde k puede tomar valores $1 \leq k \leq K$
$\omega_{i,j}$	Un cupón de $\mathbb{MC}^{2D}$ con índice i del multicupón j
$\triangle\tau_{op}$	Parámetro del sistema que define τ_d y τ_r
(e, n)	Clave pública RSA de $\mathcal{I}$
(d, p, q)	Clave privada RSA de $\mathcal{I}$
Contenido de la infomación común (Γ)	
$\mathcal{I}_{id}$	(Opcional) Identificador de $\mathcal{I}$
s_{id}	(Opcional) Identificador del servicio
N	Número de *cupones de pago* en un multicupón
v	Valor de cada *cupón de pago*
$[(N_j, v_j)]_{j=1}^J$	Número de *cupones de pago* y su valor para cada multicupón $j\ \forall\ 1 \leq j \leq J$. Todos los *cupones de pago* de cada multicupón j tienen igual valor v_j
τ_{exp}	Límite temporal hasta el que $\mathcal{C}$ puede gastar sus cupones en $\mathcal{M}$
τ_d	Tiempo máximo que tiene $\mathcal{M}$ para depositar en $\mathcal{I}$ los cupones recibidos de $\mathcal{C}$
τ_r (si aplica)	Marca temporal hasta la que $\mathcal{C}$ puede reembolsar los cupones que no ha gastado

V-B. Afiliación/Desafiliación

Cada comercio que desee aceptar cupones emitidos por $\mathcal{I}$ tiene que afiliarse a este, firmando un acuerdo que puede consistir en una lista de términos y condiciones. $\mathcal{I}$ y los comercios afiliados no comparten información sensible, ya que los comerciantes solo necesitan conocer la clave pública de $\mathcal{I}$ (e, n) y la clave pública de grupo (pk^G).

V-C. Registro en el Gestor de Grupo

Antes que $\mathcal{C}$ pueda usar un 2D-multicupón emitido por $\mathcal{I}$, $\mathcal{C}$ tiene que registrarse en $\mathcal{G}$ para obtener un par de claves de grupo. $\mathcal{G}$ autentica a $\mathcal{C}$ usando su certificado digital $Cert_{\mathcal{C}}$, enlaza una clave privada de cliente $(sk_{\mathcal{C}}^G)$ a la identidad de $\mathcal{C}$ y le envía el par de claves de grupo $\left(pk^G, sk_{\mathcal{C}}^G\right)$ y un certificado digital $Cert_{\mathcal{G}}$ (emitido por una autoridad de confianza) que autentica la clave pública de grupo.

V-D. Protocolo de Emisión

El protocolo de emisión (Fig. 4) permite a $\mathcal{C}$ obtener de $\mathcal{I}$ un 2D-multicupón anónimo y no rastreable. El proceso es anónimo ($\mathcal{C}$ no proporciona ningún dato sobre su identidad) y el 2D-multicupón no contiene ninguna información que permita identificar a $\mathcal{C}$. Además, gracias al uso de un esquema de firma parcial ciega, el listado de cupones raíz $([\omega_{0,j}]_{j=1}^J)$ está oculto para $\mathcal{I}$, pero este puede controlar la información común del 2D-multicupón (ver Cuadro I). Nadie (excepto $\mathcal{G}$) puede rastrear las actividades de $\mathcal{C}$.

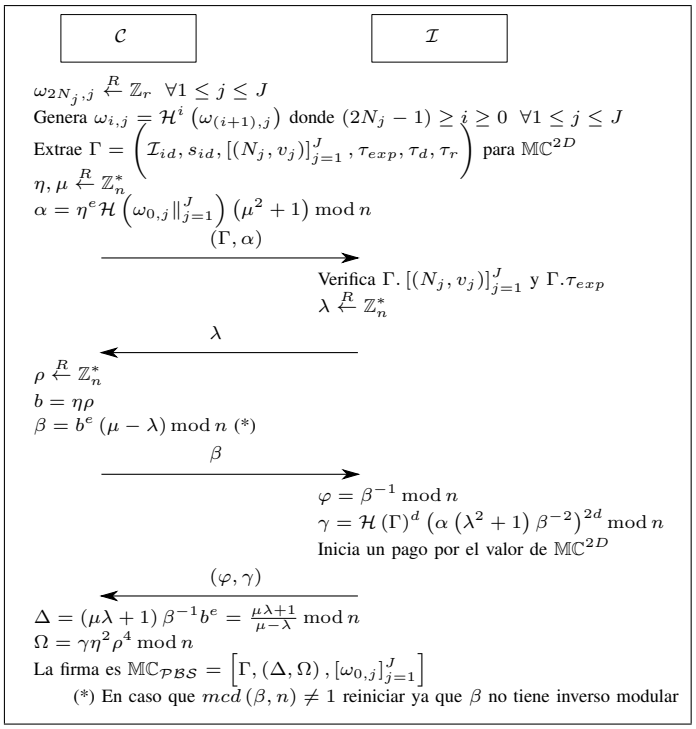

Figura 4: Protocolo de emisión de un 2D-multicupón.

$\mathbb{MC}_{\mathcal{PBS}}$ se define como $\left[\Gamma, (\Delta, \Omega), [\omega_{0,j}]_{j=1}^J\right]$ (ver Fig. 3) y se verifica evaluando la siguiente igualdad:

$$\Omega^e \overset{?}{\equiv} \mathcal{H}(\Gamma)\,\mathcal{H}\left(\omega_{0,j}\|_{j=1}^J\right)^2\left(\Delta^2 + 1\right)^2 \bmod n \qquad (1)$$

V-E. Protocolo de Pago Múltiple

El protocolo de *pago múltiple* (Fig. 5) es un protocolo entre $\mathcal{C}$ y $\mathcal{M}$ que permite a $\mathcal{C}$ gastar cupones de su 2D-multicupón a cambio de un servicio proporcionado por cualquier $\mathcal{M}$ de la afiliación. El pago múltiple puede ejecutarse mientras $\tau_{now} \leq \tau_{exp}$.

El protocolo define un intercambio de tres pasos donde $\mathcal{C}$ puede pagar a $\mathcal{M}$ con diversos pares de cupones en una única transacción. Para ejecutar el intercambio, $\mathcal{C}$ envía a $\mathcal{M}$ un conjunto de *cupones de pago* combinando cupones de diferentes multicupones hasta el valor del servicio requerido. Este conjunto se define como $A_{i,j,k_j} \subseteq \left[[\omega_{i,j}, (i, j), k_j]_{i=1}^{N_j}\right]_{j=1}^J$, es decir, la lista de los últimos cupones de cada multicupón seleccionado j de $\mathbb{MC}_{\omega}$, hasta conseguir el valor requerido para la obtención del servicio, junto con las correspondientes coordenadas (i, j) y el número de cupones necesario de cada multicupón j seleccionado. Después de diversas verificaciones, $\mathcal{M}$ envía a $\mathcal{C}$ el servicio solicitado. Finalmente, $\mathcal{C}$ envía el conjunto de *cupones de prueba* $B_{i+1,j,k_j} \subseteq \left[[\omega_{i+1,j}, (i + 1, j), k_j]_{i=1}^{N_j}\right]_{j=1}^J$ correspondiente a A_{i,j,k_j} para probar la validez de los *cupones de pago*.

V-F. Protocolo de Depósito

El protocolo de depósito (Fig. 6) permite a $\mathcal{M}$ pedir a $\mathcal{I}$ un ingreso a cambio de un conjunto de cupones recibidos de

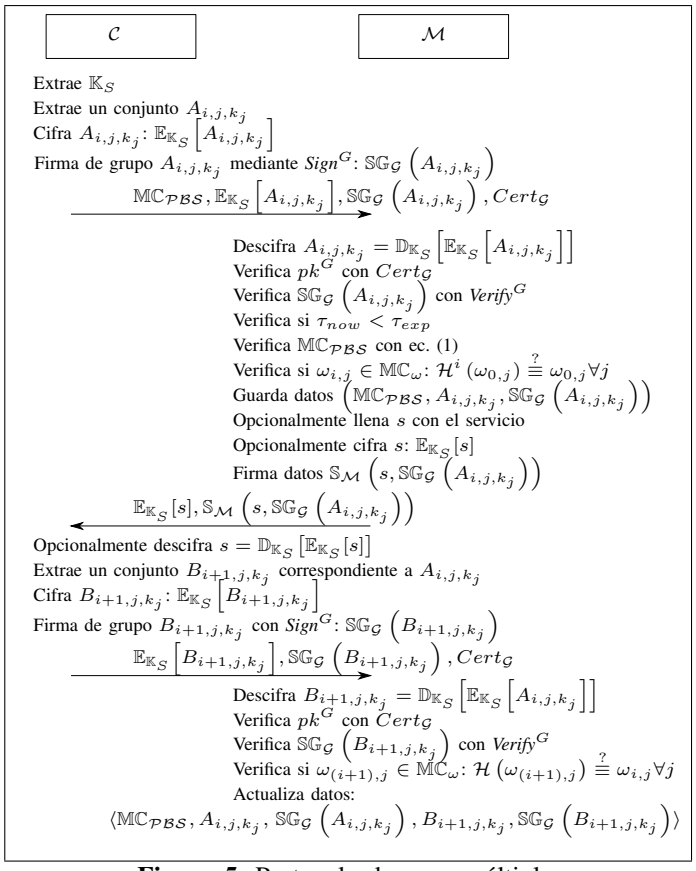

Figura 5: Protocolo de pago múltiple.

los clientes. Igual que el protocolo de emisión, el protocolo de depósito usa una única transacción para enviar múltiples cupones. Este protocolo puede usarse mientras $\tau_{now} \leq \tau_d$ aunque $\mathcal{M}$ no haya recibido todos los cupones del 2D-multicupón. Si $\mathcal{I}$ detecta un cupón reusado, contacta con $\mathcal{G}$ quien puede proceder a revocar el anonimato de la entidad que ha actuado de forma fraudulenta.

V-G. Protocolo de Reembolso

El protocolo de reembolso es un protocolo opcional aplicable si todos los participantes están de acuerdo. Permite a $\mathcal{C}$ solicitar a $\mathcal{I}$ un reembolso de un conjunto de cupones sin gastar cuando el 2D-multicupón ya no es válido. El protocolo puede usarse mientras $\tau_d < \tau_{now} \leq \tau_r$. Por problemas de espacio, omitimos la especificación del flujo del protocolo, ya que es similar al protocolo de depósito.

VI. Análisis de los Requisitos de Seguridad

En esta sección presentamos un análisis de nuestra propuesta para verificar que cumple con los requisitos de seguridad.

Proposición 1. *La privacidad de los clientes está garantizada. Se satisface el anonimato de los clientes respecto al comerciante y al emisor, y se cumple con las propiedades de no rastreable y no enlazable.*

Afirmación 1. **El cliente actúa de forma anónima**.

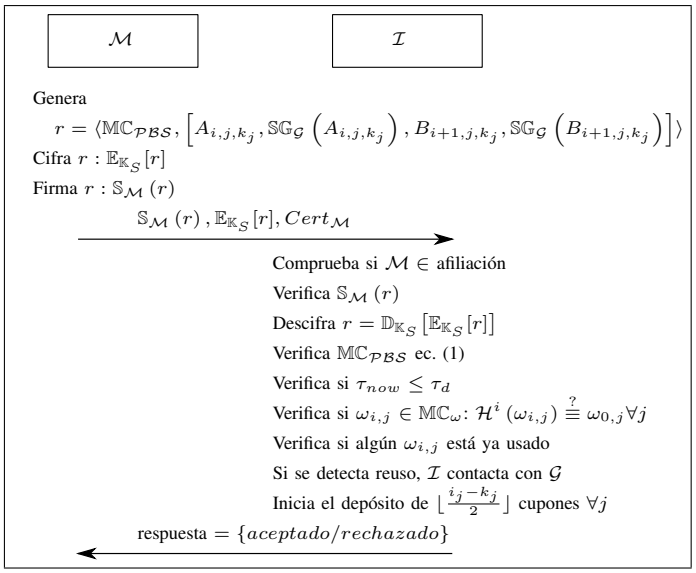

Figura 6: Protocolo de depósito.

Demostración. El 2D-multicupón contiene dos tipos de datos: información común, que puede ser leída por cualquiera y que no contiene información relacionada con su propietario; e información oculta (identificadores de cupones raíz $[\omega_{0,j}]_{j=1}^{J}$).

Cuando $\mathcal{C}$ envía un cupón o un conjunto de cupones (A_{i,j,k_j} o B_{i+1,j,k_j}) a $\mathcal{M}$, $\mathcal{C}$ firma los cupones con la clave privada de grupo (sk_c^G). $\mathcal{M}$ puede verificar la firma usando la clave pública de grupo (pk^G), pero no puede derivar la identidad de $\mathcal{C}$, ya que el gestor de grupo ($\mathcal{G}$) es el único que puede revelar dicha identidad.

Afirmación 2. **Los 2D-multicupones no son enlazables**.

Demostración. Los cupones de diferentes 2D-multicupones no pueden vincularse, ya que están asociados a cupones raíz (*root*) independientes, generados aplicando cadenas de hash a partir de cupones semilla (*seed*) elegidos aleatoriamente. Sin embargo, un conjunto de cupones perteneciente al mismo 2D-multicupón puede ser enlazado por las propiedades de las cadenas de hash.

Afirmación 3. **Los clientes no son rastreables**.

Demostración. Los cupones no pueden ser utilizados para rastrear la identidad de $\mathcal{C}$. $\mathcal{C}$ no necesita revelar su identidad a $\mathcal{I}$ en el protocolo de emisión, ni a $\mathcal{M}$ en el protocolo de pago múltiple. De esta forma nadie (excepto $\mathcal{G}$) puede determinar quién gasta un cupón o un conjunto de cupones ni dónde han sido gastados estos cupones.

Afirmación 4. **Las comunicaciones son confidenciales**.

Demostración. Los mensajes se protegen mediante el uso de una clave compartida $\mathbb{K}_S$ de un criptosistema seguro de clave simétrica.

Resultado de la Proposición 1: Las afirmaciones $1-4$ permiten concluir que la privacidad del cliente está asegurada.

Proposición 2. *El emisor y los comerciantes están protegidos ante posibles comportamientos fraudulentos por parte*

del cliente. Se detecta la reutilización y la falsificación de 2D-multicupones. Además la desafiliación de comerciantes no compromete la seguridad del sistema.

AFIRMACIÓN 5. **Se detecta el reuso de los cupones**.

DEMOSTRACIÓN. $\mathcal{I}$ no necesita almacenar ninguna información acerca de los 2D-multicupones durante el protocolo de emisión ya que estos están firmados con su clave privada y contienen toda la información necesaria para su verificación. Cuando $\mathcal{C}$ utiliza cupones en un determinado $\mathcal{M}$, le envía el conjunto de cupones (A_{i,j,k_j} o B_{i+1,j,k_j}) firmado con la clave privada de grupo ($\mathbb{SG}_{\mathcal{G}}\left(A_{i,j,k_j}\right)$ o $\mathbb{SG}_{\mathcal{G}}\left(B_{i+1,j,k_j}\right)$). Entonces, $\mathcal{M}$ puede obtener cada cupón individual y comprobar si algún cupón ya ha sido utilizado previamente, es decir, verificar si aparece en la base de datos local de $\mathcal{M}$ o de $\mathcal{I}$.

AFIRMACIÓN 6. **Los 2D-multicupones ni su contenido pueden falsificarse**.

DEMOSTRACIÓN. El número de cupones de cada 2D-multicupón se fija en el protocolo de emisión. Por tanto, el número de cupones no puede ser falsificado: $\mathcal{C}$ y $\mathcal{M}$ no pueden utilizar más cupones de los permitidos, generar nuevos multicupones o modificar su contenido, ya que la información es firmada por $\mathcal{I}$, y sólo $\mathcal{I}$ conoce la clave privada (d, p, q).

AFIRMACIÓN 7. **El anonimato de los clientes maliciosos puede revocarse**.

DEMOSTRACIÓN. Aunque tanto la falsificación como la reutilización se detectan, la identidad de $\mathcal{C}$ no se revela sin la participación de $\mathcal{G}$. Dado que los cupones gastados están firmados por $\mathcal{C}$ con su clave privada de grupo (sk_c^G), si un cupón ya ha sido utilizado o ha sido falsificado, se puede solicitar la revocación del anonimato de $\mathcal{C}$ a $\mathcal{G}$, quien utiliza $Open^G$ para revelar la identidad de $\mathcal{C}$.

AFIRMACIÓN 8. **Los comerciantes pueden desafiliarse de forma segura**.

DEMOSTRACIÓN. $\mathcal{M}$ sólo necesita conocer la clave pública de $\mathcal{I}$ (e, n) y la clave pública de grupo (pk^G) para participar en el sistema. Por tanto, los comerciantes no comparten ninguna información sensible, de manera que pueden abandonar el sistema sin que este se vea comprometido.

AFIRMACIÓN 9. **El 2D-multicupón no es divisible**.

DEMOSTRACIÓN. Nuestro esquema proporciona *no divisibilidad débil*, porque los clientes que comparten cupones de un mismo 2D-multicupón podrían ser falsamente acusados de comportamiento malicioso. Si $\mathcal{C}_1$ firma los cupones que comparte con $\mathcal{C}_2$, y $\mathcal{C}_2$ se comporta de forma maliciosa, el sistema acusaría a $\mathcal{C}_1$. Si $\mathcal{C}_2$ es quien firma, $\mathcal{C}_1$ podría, de la misma manera, utilizar los cupones compartidos de forma fraudulenta y el sistema acusaría a $\mathcal{C}_2$. Por lo tanto, si los clientes quieren compartir cupones, asumen el riesgo de ser falsamente acusados de comportamiento fraudulento. De esta manera se disuade a los clientes de compartir un mismo 2D-multicupón.

Resultado de la Proposición 2: Las afirmaciones $5-9$ permiten concluir que el sistema protege a los comerciantes y al emisor frente a los clientes deshonestos. Además, el sistema está protegido frente a la desafiliación de los comerciantes y disuade a los clientes de compartir un mismo 2D-multicupón.

VII. CONCLUSIONES

La solución multicupón presentada en este artículo cumple con todas las propiedades de seguridad necesarias para un escenario multi-comerciante, y mejora la seguridad y la eficiencia de las soluciones previas gracias al diseño del proceso de pago múltiple. El anonimato de los clientes está garantizado con la utilización de técnicas de firma de grupo que permiten la no rastreabilidad de las operaciones de los clientes, consiguiendo así preservar su privacidad. Por otra parte, tanto el emisor como los comerciantes, están protegidos frente al uso fraudulento de los multicupones por parte de los clientes, ya que se puede detectar su reutilización y falsificación, y en caso necesario, la identidad de los clientes deshonestos puede ser revelada. Además, a diferencia de las propuestas anteriores, los comerciantes pueden unirse y abandonar el sistema de forma segura.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por el Ministerio de Educación y Ciencia bajo el proyecto CONSOLIDER-ARES (CSD2007-00004).

REFERENCIAS

[1] Edenred. An international company for booklet coupons of restaurants. *[Online]. Available: http://www.edenred.com*.

[2] Gourmet. An international company for booklet coupons of restaurants. *[Online]. Available: http://www.cheque-dejeuner.com/*.

[3] C. Blundo, S. Cimato, and A. De Bonis. Secure e-coupons. *Electronic Commerce Research*, 5:117–139, January 2005.

[4] L. Chen, M. Enzmann, A. Sadeghi, M. Schneider, and M. Steiner. A Privacy-Protecting Coupon System. In *Financial Cryptography and Data Security*, volume 3570 of *LNCS*, pages 578–578. 2005.

[5] L. Nguyen. Privacy-protecting coupon system revisited. In *Financial Cryptography and Data Security*, volume 4107 of *LNCS*, pages 266–280. 2006.

[6] S. Canard, A. Gouget, and E. Hufschmitt. A handy multi-coupon system. In Jianying Zhou, Moti Yung, and Feng Bao, editors, *Applied Cryptography and Network Security*, volume 3989 of *LNCS*, pages 66–81. 2006.

[7] A. N. Escalante, H. Löhr, and A. Sadeghi. A non-sequential unsplittable privacy-protecting multi-coupon scheme. In *GI Jahrestagung (2)*, pages 184–188, 2007.

[8] L. Chen, A. N. Escalante, H. Löhr, M. Manulis, and A. Sadeghi. A privacy-protecting multi-coupon scheme with stronger protection against splitting. In *Proceedings of the 11th International Conference on Financial cryptography and 1st International Conference on Usable Security*, volume 4886 of *LNCS*, pages 29–44. 2007.

[9] F. Armknecht, A. N. Escalante, H. Löhr, M. Manulis, and A. Sadeghi. Secure multi-coupons for federated environments: privacy-preserving and customer-friendly. In *Proceedings of the 4th International Conference on Information Security Practice and Experience*, volume 4991 of *LNCS*, pages 29–44. 2008.

[10] S. Hsueh and J. Chen. Sharing secure m-coupons for peer-generated targeting via eWOM communications. *Electronic Commerce Research and Applications*, 9:283–293, July 2010.

[11] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *LNCS*, pages 227–242. 2004.

[12] D. Chaum. Blind Signatures for Untraceable Payments. *Advances in Cryptology Proceedings of Crypto 82*, pages 199–203, 1983.

[13] H. Chien, J. Jan, and Y. Tseng. RSA-based Partially Blind Signature with Low Computation. *International Conference on Parallel and Distributed Systems ICPADS 2001*, pages 385–389, 2001.