G. Draper-Gil, et al., "Un protocolo para la firma de contratos en escenarios multi-two-party con atomicidad", *XII Reunión Española de Criptología y Seguridad de la Información*, pp. 357-362, 2012.
NICS Lab. Publications: https://www.nics.uma.es/publications

Un Protocolo para la Firma de Contratos en escenarios Multi-Two-Party con Atomicidad

Gerard Draper-Gil*, Josep-Lluís Ferrer-Gomila*, M. Francisca Hinarejos*, Jose A. Onieva†, Javier López†
*Universitat de les Illes Balears (UIB), Email:{gerard.draper, jlferrer, xisca.hinarejos}@uib.es
†Universidad de Málaga (UMA), Email: {onieva, jlm}@lcc.uma.es

***Resumen*—Los avances tecnológicos que está experimentando el mundo digital (Internet, comunicaciones, etc.) están acercando a consumidores y proveedores. Los proveedores pueden ofrecer sus productos directamente a los consumidores finales, y éstos son capaces de acceder a los proveedores desde cualquier lugar y en cualquier momento. A la hora de adquirir productos o servicios, esta facilidad de acceso permite a los consumidores consultar distintas ofertas de diferentes proveedores. Pero en el caso de que el consumidor quiera múltiples productos, como los paquetes turísticos, formados por vuelos, hoteles, excursiones, etc, los consumidores carecen de herramientas que les permitan realizar la contratación multi-two-party de manera atómica. En este artículo presentamos un protocolo de firma de contratos multi-two-party con atomicidad que garantiza la equitatividad de todas las partes.**

I. Introducción

La rápida evolución de Internet y los avances en tecnologías de comunicación están facilitando la interacción entre proveedores y compradores finales (de aquí en adelante consumidores). Mediante Internet, los proveedores pueden ofrecer sus productos directamente a los consumidores finales, aumentando su catálogo de opciones; y gracias a los avances en las tecnologías de comunicación, los consumidores son capaces de acceder a los proveedores desde cualquier lugar y en cualquier momento. En algunos sectores (por ejemplo, el sector ocio) este canal de comunicación directo entre proveedores y consumidores es especialmente interesante cuando estos últimos deciden adquirir un producto multi-servicio, como los paquetes turísticos, donde los consumidores adquieren productos formados por varios servicios: hoteles, vuelos, excursiones, etc. Los consumidores pueden fácilmente comparar el precio ofrecido para un mismo servicio en distintos proveedores (existen incluso webs específicas para estos servicios) y escoger el que más les convenga. Al final, el paquete que compra el consumidor puede estar formado por servicios de diferentes proveedores: el vuelo en el proveedor A, el hotel en el proveedor B, etc. El problema aparece en el momento de ejecutar la compra de los servicios: para que el consumidor obtenga el producto que desea, tiene que comprar servicios diferentes de proveedores distintos, por lo tanto, quiere comprometerse con todos los proveedores o con ninguno; sino fuera así, su paquete no estaría completo. Sin pérdida de generalidad y para facilitar la explicación del problema, supondremos que el consumidor adquiere un único producto/servicio de cada proveedor.

Cuando compramos un producto/servicio a un proveedor *online*, estamos realizando un proceso de firma digital de contratos. La firma digital de contratos es un caso particular de intercambio equitativo, donde los objetos a intercambiar son firmas digitales sobre un contrato: el usuario A tiene un objeto que el usuario B quiere, pero A no quiere darle su objeto a B sin tener la seguridad de que B le dará el objeto que ella quiere. Si en el intercambio intervienen más de 2 participantes, hablamos de Intercambio Equitativo Multi-Party.

En un escenario clásico Multi-Party tenemos a un grupo de N participantes $\{N_1, ..., N_N\}$ que quieren firmar un contrato M compartido entre todos ellos, pero ninguno quiere dar su firma sin tener la seguridad de que recibirá las $N-1$ firmas del resto de participantes. Un escenario Multi-Two-Party es un caso distinto al Multi-Party, en el que tenemos un conjunto de $(N-1)$ pares de participantes $\{C, P_1\}, \{C, P_2\}..., \{C, P_{(N-1)}\}$, que quieren firmar un conjunto de $(N-1)$ contratos $\{M_1, M_2, ..., M_{(N-1)}\}$ dos a dos, es decir, C y P_1 quieren firmar el contrato M_1, C y P_2 el contrato M_2, etc. En este escenario, ni C ni P_i quieren dar su firma sin tener la seguridad que el otro participante enviará la suya. Finalmente, un escenario *Multi-Two-Party Atómico* es un caso restrictivo del Multi-Two-Party en el que C no quiere enviar su firma sin tener la seguridad que recibirá la firma de *todos* los proveedores $P_1, ..., P_{(N-1)}$, ni P_i quiere enviar la suya si no recibe la correspondiente firma de C sobre el contrato M_i.

El problema del intercambio equitativo Multi-Party ha sido ampliamente estudiado, dando como resultado un gran número de soluciones heterogéneas, por ejemplo las que encontramos en [1], [2]. Las podemos clasificar de acuerdo al uso que hacen de una tercera parte de confianza (TTP del inglés Trusted Third Party): *inline*, *online* y *offline*; de acuerdo al tipo de arquitectura del protocolo: anillo, serie, paralelo; y de acuerdo a su aplicación: correo electrónico certificado, firma digital de contratos o intercambio de bienes digitales. Pese al esfuerzo dedicado al estudio del Intercambio Equitativo Multi-Party, hay muy pocas propuestas [3], [4] que traten, en mayor o menor medida, el problema que presentamos en este artículo, la firma digital de contratos en escenarios Multi-Two-Party Atómicos, y de hecho el problema aún no está resuelto.

Contribución: En este artículo presentamos una propuesta de protocolo para firma digital de contratos orientada a un tipo de escenarios Multi-Party, los *Multi-Two-Party Atómicos*, donde tenemos un consumidor y múltiples proveedores que quieren firmar un contrato dos a dos (consumidor-proveedor), con la particularidad de que el consumidor necesita la firma

de todos los proveedores.

Organización: El artículo está organizado de la siguiente manera. En la sección II se describen los requisitos de seguridad del protocolo *Multi-Two-Party Atómico*. En la sección III discutimos el trabajo previo realizado en el ámbito de protocolos de firma digital *Multi-Two-Party Atómicos*. Nuestra propuesta se define en las secciones IV y V. En la sección VI analizamos si nuestra propuesta cumple con los requisitos de seguridad. Finalmente, las conclusiones aparecen en la sección VII.

II. Requisitos de Seguridad

Los requisitos de seguridad para el intercambio equitativo de valores fueron establecidos por Asokan *et al.* [5], y más tarde reformulados por Zhou *et al.* [6]: *efectividad, equitatividad, temporalidad, no-repudio* y *verificabilidad de la TTP*. La *confidencialidad* es otra propiedad deseable: el contrato en claro sólo debe ser revelado a las partes interesadas, el consumidor y los proveedores. Ni siquiera durante la resolución de disputas debe revelarse el contenido de este a la TTP. Además, en nuestro escenario, es posible que un consumidor quiera que los proveedores sólo tengan acceso a su contrato (el que firman con el cliente).

La equitatividad es un requisito especialmente importante, que puede dividirse en equitatividad *fuerte* y *débil* (la definición que hacen Zhou *et al.* [6] corresponde con la definición de Asokan *et al.* de equitatividad fuerte). El objetivo principal de la equitatividad es asegurar que al terminar un intercambio los participantes honestos obtienen los objetos que esperaban, o sino, nadie tendrá suficiente información como para obtener una ventaja sobre el resto de participantes. La equitatividad es un requisito que los protocolos de intercambio equitativo deben cumplir (ya sea en su versión fuerte o en su versión débil). A continuación detallaremos los requisitos para los protocolos de intercambio equitativo Multi-Two-Party Atómicos, aplicados a la firma digital de contratos:

- **Efectividad.** Si todas las partes involucradas en una firma Multi-Two-Party Atómica se comportan correctamente, el consumidor recibirá la firma de todos los proveedores, y los proveedores recibirán la correspondiente firma del consumidor, sin que intervenga la TTP.
- **Equitatividad Débil Multi-Two-Party Atómica.** Al finalizar una firma Multi-Two-Party Atómica, el consumidor honesto tendrá la firma de todos los proveedores, y los proveedores honestos tendrán la correspondiente firma del consumidor; o todas las partes honestas conseguirán evidencias suficientes para demostrar, ante un árbitro, que se han comportado correctamente.
- **Temporalidad.** Todos los participantes en una firma Multi-Two-Party Atómica tienen la seguridad de que la ejecución del protocolo de firma tendrá una duración finita. Una vez finalizada, no se puede degradar el nivel de equitatividad obtenida por los participantes honestos, independientemente del comportamiento del resto de participantes.
- **No-Repudio.** En una firma Multi-Two-Party Atómica en la que hay involucrados un consumidor y $N-1$ proveedores, ni el consumidor ni los proveedores pueden negar haber estado involucrados. En particular, dado un contrato firmado M_i, ni el consumidor C ni el proveedor P_i pueden negar haberlo firmado.
- **Confidencialidad.** Sólo los participantes involucrados en una firma, el consumidor C y el proveedor P_i, pueden conocer el contenido del contrato M_i. Ni siquiera la TTP debe tener acceso al contrato en claro.
- **Verificabilidad de la TTP.** Si la TTP actúa de manera deshonesta, provocando la pérdida de equitatividad de un participante honesto (consumidor o proveedor), este puede probar el comportamiento deshonesto de la TTP frente a un árbitro externo.

III. Trabajo Previo

Pese a los muchos esfuerzos dedicados al estudio del intercambio equitativo, existen muy pocas propuestas [3], [4] que traten el problema que presentamos en este artículo.

En [4] Onieva *et. al* presentan la extensión de un protocolo Multi-Party de no-repudio con TTP online, que permite a un emisor enviar distintos mensajes a múltiples destinatarios. En su artículo, Onieva *et al.* [4] clasifican los escenarios Multi-Party en dos tipos: escenarios con un emisor y varios receptores, en los que el emisor envía el mismo mensaje a todos (*Simple Origin with Many Recipients* para el intercambio de un mismo mensaje, $SOMR-M$); y escenarios en los que un emisor envía un mensaje distinto a cada receptor (*Simple Origin with Many Recipients* para diferentes mensajes $SOMR-M_i$). Este segundo tipo de escenarios, $SOMR-M_i$, es parecido al que nosotros presentamos, el Multi-Two-Party Atómico, aunque en su caso el objetivo del protocolo es el intercambio de mensajes, y el nuestro es el intercambio de evidencias de firmas de contratos. Es más, la atomicidad no se contempla en el artículo. Por lo tanto, su propuesta no puede aplicarse a protocolos de firma de contratos Multi-Two-Party con Atomicidad.

En [3], Liu propone un protocolo optimista Atómico Multi-Two-Party para el intercambio de pagos por bienes digitales, compuesto por un sub-protocolo de intercambio con 2 fases: negociación y pago; y 3 sub-protocolos de resolución. La fase de negociación es un ciclo de 4 pasos donde el consumidor y los proveedores se ponen de acuerdo en los términos del intercambio (precio y producto). Si el consumidor y los proveedores se comportan correctamente, la fase de pago necesita del intercambio de 5 mensajes entre el consumidor y cada proveedor, sin que intervenga la TTP, por lo que cumple con el requisito de efectividad. La propuesta también cumple con los requisitos de no-repudio y equitatividad, pero no cumple con la verificabilidad de la TTP ni con la temporalidad. Además, el problema al que va enfocado es distinto al que presentamos en este artículo.

Respecto a la temporalidad en [3], una vez la fase de pago ha sido iniciada, el protocolo no puede ser cancelado; y los sub-protocolos de resolución sólo pueden aplicarse durante la

segunda fase, la fase de pago. Por lo tanto, no podemos afirmar que el protocolo de firma de contratos terminará en un tiempo limitado. Es más, al terminar la ejecución del protocolo, un proveedor puede contactar con la TTP reclamando que no ha recibido el objeto de pago y recibir una prueba de pago de la TTP, cambiando el estado final de la ejecución. Por lo tanto, la propuesta de Liu [3] no cumple con el requisito de temporalidad. El problema es que la resolución de los sub-protocolos de reclamación requiere que la TTP contacte con las partes involucradas. Si el consumidor ejecuta el último paso del protocolo, puede creer que el intercambio ha terminado. En este caso, la TTP no será capaz de contactar con el consumidor para solucionar posibles reclamaciones de proveedores, por lo que enviará una prueba de pago al proveedor.

Respecto a la verificabilidad en [3], los sub-protocolos de reclamación no generan evidencias del contacto entre la TTP y el consumidor o los proveedores. Por ello, cuando la TTP genera una evidencia como solución a una reclamación, ni el consumidor, ni la TTP, ni los proveedores pueden probar que la evidencia ha sido generada correctamente. Por ejemplo, la TTP genera una evidencia sin intentar contactar con la otra parte involucrada. Por lo tanto, el protocolo propuesto por Liu [3] no cumple con el requisito de verificabilidad.

Por lo tanto, ninguna de las referencias que hemos encontrado en la literatura en relación con intercambios Atómicos Multi-Two-Party ([3], [4]) cumple con los requisitos de seguridad necesarios (sección II), para nuestro escenario.

IV. Visión general de la propuesta Multi-Two-Party

En este artículo proponemos un protocolo optimista para la firma de contratos Atómicos Multi-Two-Party, inspirado en una propuesta previa [7] para firma electrónica de contratos Multi-Party. La propuesta original [7] tiene una arquitectura en anillo y requiere N rondas y $(N+1)(N-1)$ mensajes (donde N es el número de partes involucradas) para ejecutar el protocolo, sin intervención de la TTP. Para nuestro escenario, el Atómico Multi-Two-Party, hemos tenido que cambiar la arquitectura del protocolo, porque no permite dar solución a nuestro problema donde los proveedores no tienen relación ninguna entre ellos y en lugar de un mismo contrato para todas las partes, se tiene uno diferente por cada par $\{C, P_i\}$.

Nuestra propuesta tiene una arquitectura en paralelo, donde el consumidor contacta con todos los proveedores "a la vez", y espera su respuesta antes de continuar con otra ronda, es decir, el consumidor envía $N-1$ compromisos (COMmitment) al mismo tiempo, y espera a recibir las $N-1$ aceptaciones (ACCeptance) antes de continuar. Si el consumidor deja de recibir una o más aceptaciones, contactará con la TTP.

Los compromisos son los mensajes enviados desde el consumidor a los proveedores, y las aceptaciones son los mensajes enviados de los proveedores al consumidor. Los $COM_{(n,i)}$ y $ACC_{(n,i)}$ (n = número de ronda, i = número de proveedor) son las evidencias que el proveedor P_i y el consumidor C deben recibir, respectivamente.

Sub-Protocolo de Intercambio

Ronda		
1	$C \rightarrow P_i$	$CID, M_i, 1, COM_{(1,i)}$
1	$C \leftarrow P_i$	$CID, 1, ACC_{(1,i)}$
⋮	⋮	⋮
n	$C \rightarrow P_i$	$CID, n, COM_{(n,i)}$
n	$C \leftarrow P_i$	$CID, n, ACC_{(n,i)}$
⋮	⋮	⋮
N	$C \rightarrow P_i$	$CID, N, COM_{(N,i)}$
N	$C \leftarrow P_i$	$CID, N, ACC_{(N,i)}$

N = número de participantes; n = ronda
$COM_{(n,i)} = S_C[CID, h(M_i), n]$
$ACC_{(n,i)} = S_{P_i}[CID, h(M_i), n]$

Tabla I
SUB-PROTOCOLO DE INTERCAMBIO ATÓMICO MULTI-TWO-PARTY

A continuación se presenta la notación que se va a utilizar a lo largo del artículo:

- **N** Número de participantes: 1 Consumidor y $N-1$ Proveedores.
- $\overline{\mathbf{X}}_{\mathbf{Z}} = \{\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x}_{(\mathbf{Z})}\}$ Vector con Z elementos.
- **C** Consumidor.
- $\mathbf{P_i}$ Proveedor i, $1 \leq i \leq (N-1)$.
- $\mathbf{M_i}$ Mensaje (contrato) intercambiado entre el consumidor C y el proveedor P_i.
- **CID** Identificador de Contrato único (Unique Contract IDentifier).
- $\mathbf{h}(\mathbf{M_i})$ Función de Hash del mensaje M_i.
- $\mathbf{S_j}[\mathbf{M_i}] = \mathbf{SK_j}[\mathbf{h}(\mathbf{M_i})]$ Firma Digital de j sobre M_i (donde SK_j es la clave privada de j).

V. Protocolo

Nuestra propuesta de protocolo optimista de firma electrónica de contratos Multi-Two-Party Atómicos está dividida en dos sub-protocolos: *intercambio* (sección V-A) y *resolución* (sección V-B). Si todas las partes involucradas se comportan correctamente, el sub-protocolo de *intercambio* terminará después de N rondas, se intercambiarán $2N(N-1)$ mensajes y la TTP no intervendrá.

V-A. Sub-Protocolo de Intercambio

La tabla I muestra el flujo de ejecución del sub-protocolo de *intercambio* y los correspondientes valores intercambiados. Cada ejecución completa del sub-protocolo está compuesta de N rondas, y cada ronda requiere el intercambio de $N-1$ pares de mensajes {compromiso, aceptación}, lo que hace un total de $2N(N-1)$ mensajes. Las evidencias de firma son las correspondientes a la ronda N ($COM_{(N,i)}$ y $ACC_{(N,i)}$).

En cada ronda el consumidor envía, en paralelo, el compromiso correspondiente a cada proveedor y espera a que cada proveedor envíe su mensaje de aceptación como respuesta. Una vez el consumidor ha recibido todos los mensajes de aceptación de los proveedores, continúa con la siguiente ronda. Si fallase en la recepción de uno o más mensajes de aceptación, ejecutará el sub-protocolo de *resolución* (V-B); de lo contrario podría perder la atomicidad en la firma del contrato.

Sub-Protocolo de Resolución

Consumidor peticionResolucion$_{(n,i)}$
$CID, h(M_i), n$
$COM_{(1,1)}, ACC_{(1,1)}, ..., COM_{(1,(N-1))}, ACC_{(1,(N-1))}$
$\vdots \quad \vdots \quad \vdots$
$COM_{(n,1)}, ACC_{(n,1)}, ..., COM_{(n,i)}$, $EVRES_{(n,i)}$

Proveedor P$_i$ peticionResolucion$_{(n,i)}$
$CID, h(M_i), n$
$COM_{(1,i)}, ACC_{(1,i)}, ..., COM_{(n,i)}, ACC_{(n,i)}$, $EVRES_{(n,i)}$

TTP RespuestaResolucionCancelada$_{(n,i)}$
$Canceled_{TK}$ = $S_{TTP}[CID, h(M_i), n, canceled]$

TTP RespuestaResolucionFirmada$_{(n,i)}$
Consumer $Signed_{TK}$ = $S_{TTP}[CID, h(M_i), n, COM_{(n,i)}]$
Provider $Signed_{TK}$ = $S_{TTP}[CID, h(M_i), n, ACC_{(n,i)}]$

N = número de participantes; n = ronda
$COM_{(n,i)}$ = $S_C[CID, h(M_i), n]$
$ACC_{(n,i)}$ = $S_{P_i}[CID, h(M_i), n]$
$EVRES_{(n,i)}$ = $S_{(C\ or\ P_i)}[CID, h(M_i), n, ...]$, firma sobre el mensaje enviado.

Tabla II
SUB-PROTOCOLO DE RESOLUCIÓN MULTI-TWO-PARTY ATÓMICO

V-B. Sub-Protocolo de Resolución

En cualquier momento, el consumidor y los proveedores pueden contactar con la TTP para resolver la ejecución del protocolo. Durante la primera ronda ($n = 1$), cualquier participante puede contactar con la TTP y solicitar que se cancele la firma, mientras que si $n > 1$, la petición tendrá como objetivo finalizar el protocolo (firmar el contrato). En la tabla II podemos ver como se construyen las peticiones del sub-protocolo de *resolución*.

V-B1. Reglas de la TTP: La TTP utiliza un conjunto de reglas para solucionar correctamente las peticiones de *resolución* recibidas. Las reglas se basan en un grupo de variables que la TTP actualiza cada vez que recibe una petición, indicando el estado de una ejecución del protocolo identificada por su CID. A continuación presentamos estas variables, su definición y la notación utilizada:

- $\overline{X}_N = \{C, P_1, ..., P_{(N-1)}\}$; conjunto de participantes de una firma electrónica de contratos.
- $\overline{XC}$ conjunto de participantes que han pedido la resolución de una ejecución del protocolo con identificador "CID".
- $\overline{XA}$ conjunto de participantes que han recibido una evidencia de cancelación de la TTP, junto con el número de ronda en que la solicitaron ($\{X_i, n\}$).
- *canceled* variable booleana que indica si el estado de la ejecución es cancelado (*canceled = true*) o no (*canceled = false*).
- *signed* variable booleana que indica si el estado de la ejecución es firmado (*signed = true*) o no (*signed = false*).

Las reglas deben aplicarse en un cierto orden, como mostramos a continuación (en la tabla III podemos ver las reglas en pseudo-código):

If ($X_i \in \overline{XC}$ **)**
  rechazar petición
else
  $\overline{XC}$ = $X_i \cup \overline{XC}$
  If (k=1 and signed == false **)**
    canceled = true; $\overline{XA}$ = $\{X_i, 1\} \cup \overline{XA}$;
    $TTP \longrightarrow X_i\ Canceled_{TK}$
  else If($k = 1$ and signed == true **)**
    $TTP \longrightarrow X_i\ Signed_{TK}$
  else If($k > 1$ and signed == false **)**
    signed = true; $TTP \longrightarrow X_i\ Signed_{TK}$
  else If($k > 1$ and signed == true **)**
    $TTP \longrightarrow X_i\ Signed_{TK}$
  else If($k > 1$ and canceled == true **)**
    If ($\forall\{X_i, r\} \in \overline{XA} \rightarrow r < k - 1$ **)**
      canceled = false; signed = true;
      $TTP \longrightarrow X_i\ Signed_{TK}$
    else
      $\overline{XA}$ = $\{X_i, k\} \cup \overline{XA}$;
      $TTP \longrightarrow X_i\ Canceled_{TK}$
    end If
  end If
end If

Tabla III
ALGORITMO DE RESOLUCIÓN DE LA TTP

R0 La TTP sólo aceptará una petición de resolución por participante y CID.

R1 Si la TTP recibe una petición de un participante X_i durante la ronda $n = 1$, y la ejecución no ha sido previamente finalizada (*signed=true*) por otro participante, la TTP cancelará la firma y le enviará a X_i una prueba de que la firma ha sido cancelada.

R2 Si la TTP recibe una petición de X_i durante la ronda $n > 1$, y la ejecución no ha sido previamente cancelada por otro participante, la TTP la finalizará (*signed=true*) y le enviará a X_i una prueba de que el contrato está firmado.

R3 Si la TTP recibe una petición de X_i durante la ronda $n = 1$, y la ejecución ha sido previamente finalizada (*signed=true*) por otro participante, la TTP enviará a X_i una prueba de que el contrato está firmado.

R4 Si la TTP recibe una petición de X_i durante la ronda $n > 1$, y la ejecución ha sido previamente cancelada por otro participante, la TTP revisará las peticiones previamente recibidas para comprobar si alguien ha hecho trampas. Si la TTP decide que todas las peticiones anteriores eran incorrectas, cambiará el estado de la ejecución a *signed=true* y enviará la correspondiente prueba de firma a X_i. De lo contrario, el estado continuará siendo *canceled=true* y la TTP enviará a X_i la correspondiente prueba de cancelación.

En la regla **R4**, la TTP comprueba la validez de las peticiones recibidas anteriormente, en comparación con la nueva petición. En particular, la TTP comprobará los números de ronda en los que las peticiones fueron recibidas, y el número de ronda en el que la nueva petición ha sido recibida: $\forall\{X_i, r\} \in \overline{XA} \rightarrow r < n - 1$. Si las peticiones previamente recibidas fueron enviadas dos o más rondas antes de la recepción de la nueva petición, quiere decir que son "erróneas", ya

que los participantes tenían más evidencias de las presentadas en la petición de cancelación. Esto implica que el protocolo había superado la ronda $n = 1$, por lo que la TTP debería de haber finalizado (*signed=true*), en lugar de haber cancelado (*canceled=true*).

Como ejemplo para explicar **R4**, consideremos la siguiente situación. Tenemos un consumidor y 3 proveedores, $N = 4$, por lo que necesitaremos 4 rondas y 24 mensajes para ejecutar el sub-protocolo de *intercambio*. Durante la ronda $n = 2$, P_1 decide cancelar el protocolo de firma, después de haber enviado su mensaje de aceptación, $ACC_{(2,1)}$. Para ello, envía una petición de resolución $RES_{(1,1)}$ en la que omite las evidencias de la segunda ronda ($COM_{(2,1)}, ACC_{(2,1)}$), por lo que enviará a la TTP: "$CID, M_1, 1, COM_{(1,1)}, ACC_{(1,1)}, EVRES_{(1,1)}$". Siguiendo las reglas: P_1 nunca ha contactado con la TTP en referencia a la firma con identificador CID, ronda $n = 1$ y la variable *signed = false*, por lo tanto, la TTP cancela la firma y envía prueba de ello a P_1. Como el consumidor ha recibido todas las evidencias de la ronda $n = 2$, enviará los compromisos de la siguiente ronda, pero esta vez P_1 no enviará su mensaje de aceptación, por lo que el consumidor contactará a la TTP enviando una petición de resolución $RES_{(3,1)}$. Cuando la TTP reciba la petición comprobará el valor de ronda recibido con el de las peticiones recibidas anteriormente $RES_{(1,1)}$, porque la variable *canceled = true*. Al compararlos tendremos: $1 < (3 - 1)$, por lo tanto la conclusión de la TTP es que P_1 ha mentido, por lo que cambiará su resolución previa de cancelado a firmado, y enviará la correspondiente prueba al consumidor.

VI. Análisis de Seguridad

En esta sección comprobaremos si nuestra propuesta cumple con los requisitos de seguridad para protocolos de Intercambio Equitativo Multi-Two-Party Atómicos, aplicados a la firma digital de contratos, definidos en la sección II: efectividad, equitatividad, temporalidad, no-repudio, verificabilidad de la TTP y confidencialidad.

Efectividad. La ejecución del sub-protocolo de *intercambio* (tabla I) nos asegura que, si todos los participantes actúan correctamente, el consumidor recibirá la firma de los $N - 1$ proveedores, y cada proveedor P_i recibirá su correspondiente firma del consumidor C después de N rondas y sin intervención de la TTP. Por lo tanto, el protocolo cumple con el requisito de efectividad.

Equitatividad Débil Multi-Two-Party Atómica. Si consideramos al consumidor honesto, con independencia del comportamiento del proveedor, el consumidor mantendrá la equitatividad. Hay dos posibilidades en las que un proveedor P_i (con $1 \leq i \leq (N - 1)$) puede obtener una prueba de firma del consumidor:

- Después de recibir el N-ésimo compromiso $COM_{(N,i)}$, $(1 < i < (N - 1))$, lo que significa que el consumidor tiene $N-1$ aceptaciones del proveedor, con lo que puede contactar con la TTP y obtener una evidencia de firma.
- Después de contactar con la TTP, lo que implica que la variable *signed* es igual a *true*, por lo tanto, el consumidor puede obtener una evidencia de firma del proveedor o de la TTP, si el proveedor decide no continuar la secuencia de N rondas.

En ambas situaciones, el consumidor mantiene la equitatividad.

Si consideramos un proveedor honesto P_i $(1 \leq i \leq (N - 1))$, con independencia del comportamiento del consumidor, el proveedor mantendrá la equitatividad. El consumidor puede obtener una prueba de firma del proveedor de 2 maneras distintas:

- Después de recibir la N-ésima aceptación del proveedor $ACC_{(N,i)}$, lo que implica que el proveedor ya tiene la prueba de firma del consumidor $COM_{(N,i)}$.
- Contactando con la TTP en la ronda $n > 1$, lo que quiere decir que la TTP tiene la variable *signed = true*. Por lo tanto, el proveedor podrá obtener la prueba de firma del mismo consumidor, o de la TTP si el consumidor decide interrumpir la secuencia de N rondas.

En todas las situaciones, el proveedor mantiene la equitatividad. Por lo tanto, podemos afirmar que el protocolo cumple con el requisito de Equitatividad Débil Multi-Two-Party Atómica.

Temporalidad. En cualquier momento durante la ejecución del protocolo, cualquier participante puede ejecutar el sub-protocolo de *resolución* y finalizar su ejecución, obteniendo una prueba o bien de firma, o bien de cancelación. Si todos los participantes se comportan de manera correcta el protocolo requiere de N rondas y $2N(N - 1)$ mensajes, siendo N un número finito y conocido. Por lo tanto, podemos afirmar que el protocolo tiene una duración finita, ya sea porque interviene la TTP, o con la ejecución normal de este. Es más, una vez el protocolo ha terminado, su estado final no puede cambiar. Si el protocolo finaliza con la intervención de la TTP, esta se encargará de mantener la coherencia entre las distintas peticiones posibles recibidas (siguiendo las reglas de la TTP). Si el protocolo ha finalizado después de la N-ésima ronda, las evidencias obtenidas por proveedor y consumidor servirán como prueba de su estado final. Por tanto, podemos afirmar que el protocolo cumple con el requisito de temporalidad.

No-repudio. Durante la firma de un contrato Multi-Two-Party Atómico, se generan, en cada ronda, evidencias de la participación del consumidor y de los proveedores. El $COM_{(n,i)}$ y el $ACC_{(n,i)}$ relacionan a consumidores y proveedores con la firma de un contrato. En particular, el N-ésimo compromiso y la N-ésima aceptación, son considerados como la firma del contrato. Si un consumidor intenta desvincularse de la firma de un contrato M_i con el proveedor P_i, este puede probar la implicación del consumidor utilizando la firma realizada por el propio consumidor, o una

evidencia obtenida de la TTP. De la misma manera, si el proveedor intenta desvincularse, el consumidor puede probar su implicación utilizando la firma generada por el proveedor, o las evidencias recibidas de la TTP.

Verificabilidad. La TTP puede comportarse de forma deshonesta y generar evidencias erróneas, dando como resultado, que algún participante honesto pueda perder su equitatividad. Suponiendo que el consumidor es honesto y la TTP deshonesta, pueden darse las siguientes situaciones:

- El consumidor envía una petición de *resolución* en la ronda $n = 1$, y la TTP contesta con una evidencia de firma. De acuerdo a las reglas de la TTP, durante la ronda $n = 1$ los participantes sólo pueden obtener prueba de cancelación. Por lo que el consumidor sabrá que la TTP ha enviado una respuesta equivocada (el consumidor no ha enviado ningún mensaje de ronda 2). Para probarlo, el consumidor puede pedirle a la TTP que presente las pruebas de la petición de resolución recibida previamente, esto es, pruebas de la ronda 2.
- El consumidor envía una petición durante la ronda $n \geq 2$ porque uno o más proveedores no han enviado su mensaje de aceptación, y la TTP responde con una evidencia de cancelación (sin que haya habido una cancelación previa), o de firma (habiendo recibido una cancelación previa). Como estamos en la ronda $n \geq 2$, las reglas de la TTP establecen que la respuesta debe ser una evidencia de firma a no ser que algún otro participante la haya cancelado, por lo tanto, cualquier respuesta es válida. Pero las evidencias contradictorias que la TTP haya enviado al consumidor y a uno o más proveedores probará la irregularidad en el comportamiento de la TTP.

Suponiendo un proveedor honesto y la TTP deshonesta, puede darse la siguiente situación:

- El proveedor envía una petición de *resolución* durante la ejecución de la ronda n porque no ha recibido el compromiso de la ronda $(n+1)$ y la TTP responde con una cancelación (sin que haya habido una cancelación previa), o una firma (habiendo recibido una cancelación previa). Ambos resultados son coherentes con las reglas de la TTP, pero en ambos casos el proveedor y el consumidor tendrán evidencias contradictorias enviadas y firmadas por la TTP, lo que probará su mal comportamiento.

Confidencialidad. La ejecución del sub-protocolo de *resolución* no requiere el envío del texto en claro del contrato (M_i), es decir, sin cifrar. La TTP sólo recibe el resultado de aplicar una función de "hash" sobre M_i. Además, las comunicaciones entre consumidor y proveedor son punto-a-punto: del consumidor al proveedor P_i. Estrictamente hablando, para conseguir la confidencialidad deberíamos cifrar el contrato M_i, para prevenir que una tercera parte pueda monitorizar el canal de comunicaciones, y obtener su contenido. Pero esto puede evitarse utilizando algún tipo de protocolo de transporte, como Secure Socket Layer (SSL), por lo que podemos afirmar que el protocolo cumple con el requisito de confidencialidad.

VII. Conclusiones

En este artículo hemos presentado un protocolo optimista para la firma electrónica de contratos en escenarios Multi-Two-Party Atómicos. Con un breve análisis de seguridad, hemos probado que cumple con los requisitos de seguridad necesarios: efectividad, equitatividad, temporalidad, no-repudio y verificabilidad de la TTP. Se trata, de acuerdo a nuestro conocimiento, de la primera propuesta de protocolo de firma para escenarios de este tipo.

Agradeceimientos

Este trabajo ha sido financiado por una beca FPI ligada al proyecto de investigación TSI2007-62986 del Ministerio de Ciencia e Innovación (MICINN) de España, cofinanciada por el Fondo Social Europeo y el proyecto de investigación Consolider, con referencia CSD2007-00004, del MICINN.

Referencias

[1] S. Kremer, O. Markowitch, and J. Zhou, "An intensive survey of fair non-repudiation protocols," *Elsevier Computer Communications*, vol. 25, pp. 1606 – 1621, 2002.

[2] J. A. Onieva, J. Lopez, and J. Zhou, "Multi-party non-repudiation applications," in *Secure Multi-Party Non-Repudiation Protocols and Applications*, vol. 43 of *Advances in Information Security*, pp. 1 – 21, Springer US, 2009.

[3] Y. Liu, "An optimistic fair protocol for aggregate exchange," in *Proceedings of the 2009 Second International Conference on Future Information Technology and Management Engineering*, FITME'09, (Los Alamitos, CA, USA), pp. 564–567, IEEE Computer Society, 2009.

[4] J. A. Onieva, J. Zhou, M. Carbonell, and J. Lopez, "A multi-party non-repudiation protocol for exchange of different messages," in *18th IFIP International Information Security Conference. Security and Privacy in the Age of Uncertainty (IFIP SEC'03)*, IFIP Conference Proceedings, pp. 37–48, IFIP, 2003.

[5] N. Asokan, V. Shoup, and M. Waidner, "Optimistic fair exchange of digital signatures," in *Advances in Cryptology - EUROCRYPT'98*, vol. 1403 of *Lecture Notes in Computer Science*, pp. 591 – 606, Springer Berlin / Heidelberg, 1998.

[6] J. Zhou, R. Deng, and F. Bao, "Some remarks on a fair exchange protocol," in *Public Key Cryptography*, vol. 1751 of *Lecture Notes in Computer Science*, pp. 46 – 57, Springer Berlin / Heidelberg, 2000.

[7] J. Ferrer-Gomila, M. Payeras-Capellà, and L. Huguet-Rotger, "Optimality in asynchronous contract signing protocols," in *Trust and Privacy in Digital Business*, vol. 3184 of *Lecture Notes in Computer Science*, pp. 200–208, Springer Berlin / Heidelberg, 2004.