數位內容公平交易協定之正規驗證

林熙禎
中央大學資訊管理研究所

鍾佑祥
中央大學資訊管理研究所

摘要

電子商務日漸普及，藉由網路進行電子交易亦為一種熱門新興的購物模式。但由於此交易模式尚未成熟，雙方皆憂慮在虛幻的網路中損失自身權益，因此交易公平性之疑慮成為電子商務發展瓶頸。近代學者提出許多公平交易相關協定，並以協定分析方式列舉情境來證明協定滿足公平特性。然而，情境模擬的方式無法提供嚴謹之驗證，仍可能有百密一疏的例外情況發生。因此本研究提供一個嚴謹且兼具效率的方式，使用正規驗證(Formal Verification)中模型檢測(Model Checking)，運用CSP (Communicating Sequential Processes)語言，針對欲檢驗的協定及公平特性進行建模(Modeling)，再搭配FDR (Failures-Divergence Refinement)以有限狀態自動機結構(Finite Automata-like Structure)的概念做狀態集合的檢驗，偵測協定中的缺失，並檢驗協定是否完全滿足公平交易特性。

關鍵字：線上交易協定、正規驗證、公平交易、電子現金、FDR

Formal Verification of a Fair: exchange Electronic Commerce Protocol for Digital Content Transactions

Shi-Jen Lin
Department of Information Management, National Central University

Yo-Shang Chung
Department of Information Management, National Central University

Abstract

Due to the growing popularity of e-commerce, electronic transactions through the Internet become one of the popular new shopping models. However, this model is immature enough to convince the participants that they won't ever suffer the loss of money or interests through the virtual dealing, so the fairness become the sticking point of e-commerce. Actually, many researchers propose some fair-exchange protocol lately, but they prove the fairness of their protocols by simulation and test including a few inevitable exceptions which can't provide a rigorous proof. Therefore, we provide a strict but efficient method by the model checking of formal verification. First, we model the protocol and the desired fair properties by CSP (Communicating Sequential Processes). Second, we verify the variety of all the states by FDR (Failures-Divergence Refinement) based on the finite state machine concept. Then we can detect the failures of protocol and make sure if the protocol satisfied the fairness exactly.

Key words : e-commerce protocol, formal verification, fair exchange, electronic cash, FDR

壹、導論

隨著網際網路的普及，全球線上購物市場規模高速成長，線上交易逐漸成為主要的購物管道。此外，其中的付款環節正加速電子化，再加上數位內容應用的興起，使得消費者得以透過網路進行完整交易，達到更高的操作便利性，未來相關線上交易市場規模可望隨之水漲船高。然而，線上交易以高效率、低成本的特性獲得消費者青睞，但安全性問題也隨之而來。根據eMarketer的調查，全美14歲以上的網路使用者中近三成七不願意在線上消費，主因在於「隱私權」及「安全性」等問題(Grau, 2005)。再以台灣地區為觀察焦點，資策會FIND指出，過半數使用者質疑網路交易的安全性（孫鴻業, 2005）。由此可知，線上交易的安全性備受消費者質疑，若消費者對安全性的疑慮不減，即成為電子商務窒礙難行的原因之一。

前述的安全性議題，無形地抑止線上交易的發展。此時，具有「交易公平性」的線上交易機制，即扮演著十分重要的角色，因其有助維護交易中每位成員之權益，商家必須保障其收益、消費者必須保障其獲取正確商品的權利。尤其現今網路詐騙不勝枚舉，利用機制漏洞獲取不義之財者大有人在，再論電子現金多採先付款後使用的預付(Pre-paid)模式，相較於後付(Post-paid)風險較大，為消費者較不樂意接受。若不能進一步保障其公平性，容易降低交易意願，令使用者望之怯步，成為線上交易發展的瓶頸。因此，「交易公平性」成為一個完善的線上交易協定必須具備的關鍵因素。

近代已有許多學者提出許多線上交易的相關協定，但如何證明這些協定確實具有公平特性？以往之研究多採傳統的協定分析方式，列舉可能受攻擊的情境進行模擬(Simulation)。模擬為經常使用的驗證方法，然而其複雜程度會隨著系統設計本身的複雜度成指數成長，因此在面對日益複雜、情境組合眾多的協定設計，純粹以模擬的驗證方法將無法提供足夠的驗證覆蓋率(Verification Coverage)（Wang, 2004），常有百密一疏。尤其許多正常情況下皆可如常運行的協定，一旦遇到特殊的意外，原本具有的公平特性就常難以維持。

有鑒於完善之交易機制須符合安全性與公平性考量，本研究的研究動機為：如何嚴密的驗證線上交易機制具有「交易公平性」？整個交易流程中是否有任何違背公平性的可能？或者當意外狀況發生時，是否仍得以保障交易雙方權易，或是產生不可預期的損失？統整上述，本研究欲建構的檢驗方式將符合以下目的：

（1）提供嚴密檢驗協定公平特性之方式

使用正規驗證技術，利用有限狀態自動機結構的概念，能夠兼具效率及嚴密性地檢驗一個線上交易協定：在整套交易流程當中，是否能完全滿足指定的公平特性，交易成員無法自其它成員獲取不法利益，亦無成員會損失自身權益，致使交易行為合法且公平。

（2）檢驗時能考量意外狀況的發生

若發生網路斷線、交易成員系統故障等意外狀況時，完善的線上交易機制必須依然

具備原有的公平特性，因而本研究能夠加入上述意外情境，更深入檢驗交易公平性。

協定公平性分析愈周全，愈能有完善的交易機制取信於消費者，最終有助於線上交易市場版圖的加速擴張，發展潛力指日可待。最後，統整本研究之研究方法。本研究將以正規驗證為基礎，瞭解各項正規驗證技術的類型與應用，並依循研究目的使用正規驗證中的模型檢測方式，搭配CSP語言，針對欲檢驗的協定及公平特性實地進行建模，再利用FDR檢驗協定是否完全滿足公平特性。最後分別透過加入網路斷線、交易成員系統故障等意外狀況，做進一步檢驗，並提出協定中的缺失，進而完成本研究。

貳、文獻探討

一、正規驗證

隨著資訊系統設計日趨複雜，最常被採用的模擬驗證方法，漸難涵蓋系統所有可能狀態，不僅導致驗證成為系統開發中最費時的步驟之一，結果亦無法令人信服。此時，正規驗證建構在時態邏輯(Temporal Logics)的概念之上，採用邏輯證明的方式，藉由檢查所有事件順序並發掘潛伏於系統中的錯誤，嚴謹並有效地探究系統設計之正確性，彌補模擬時可能欠缺的周全性(Wang, 2004)。正規驗證目前已成功運用於超大型積體電路(Very Large Scale Integration, VLSI)產業(Burch et al., 1990)，本研究將進一步應用於電子商務範疇。

正規驗證方式包括四種類型(Anderson *et al*., 2006)：手動證明(Manual Proofs)、理論證明(Theorem Proving)、模擬(Simulations)，以及模型檢測(Model Checking)。手動證明較具彈性卻也費時易錯，因此適用於非常關鍵且較不計成本的應用，例如精密的醫療器材的驗證；理論證明提供正規結講來驗證協定，較可避免人為失誤，但仍需要人工介入因而費時；模擬在驗證時需要頻繁地更新模型，但常無法涵蓋所有可能性，導致驗證覆蓋率不足；而模型檢測可藉由電腦工具輔助完成，能提供比上述三種方法更快速又兼具效率的強健驗證，另有提供反例協助除錯的優勢，在正規驗證中已廣為採用，故本研究將採用模型檢測的方式，驗證Lin and Liu (2007)提出的「公平交易與消費者匿名性之數位內容線上交易協定」。

模型檢測之步驟如圖1(Muller-Olm *et al*., 1999)：首先給定一個以有限狀態自動機結構(Finite Automata-like Structure)來表達的系統模型M，再給定數條以時態邏輯公式表達的欲檢驗規格S，然後使用自動化的模型檢測工具，驗證M是否滿足S，也就是證明指定的規格在此邏輯系統模型中是否永遠成立。

FDR是一個以CSP為基礎語言的模型檢測工具，而CSP是以數學式用來描述狀態間轉換的一種流程語言。Kim et al. (2005) 指出，自從Lowe (1996)使用FDR在Needham-Schroeder公鑰協定當中成功發現了中間人攻擊(Man-in-the-middle Attack)後，FDR就開始被廣泛應用於正規驗證，並頻繁地出現在與安全相關的文獻中。因此本研究採用FDR做為模型檢測的工具。

二、公平交易

一般而言，「公平交易」並無明確定義。根據Gartner et al.(1999)的研究，公平交易的概念為「平等對待每位交易中的參與者」，也就是保證每位參與者都不會從其他人手中獲取不正當的利益。Ray and Ray(2000)亦將公平交易定義為三種特性：(1) 金錢原子性(Money Atomicity)：金錢在交易過程中不會被憑空創造，也不會無端減少。(2) 貨品原子性(Goods Atomicity)：「商家收到貨款」與「消費者收到商品」這兩項事件必定同時成立，或同時不成立。(3) 有效接收性(Validated Receipt)：消費者在付款之前，擁有驗證商品正確性之能力。

三、驗證之協定

本研究以Lin and Liu(2007)提出的公平交易與消費者匿名性之數位內容線上交易協定為基礎，驗證其是否滿足公平特性。此協定為消費者持有電子現金透過網路購買某數位內容產品之線上交易協定，共有五類參與者：消費者、商家、銀行、仲裁者及製造商。整體交易包括以下四個階段： (1) 協商—消費者決定購買某商品、向商家接收商品資訊之過程。(2) 提款—消費者從銀行帳戶提領指定面額之電子現金的過程。(3) 購買—消費者使用電子現金向商家購買商品之過程。(4) 仲裁—當購買程序完成之後，卻發生消費者已付款，商家卻沒有在指定的時間內回應商品解密金鑰，導致消費者無法解密。付款卻沒有得到商品的消費者，此時得以向仲裁者申請仲裁，取得原本應得的權益。

Lin and Liu 利用協定分析的方式，列舉九個可能毀損公平性的情境進行分析，說明各類情境下協定的表現，最後宣稱此協定具備良好的公平性。這些分析加強了此協定的公平性品質，但其公平特性的涵蓋仍然不夠完整，並且未經嚴密的驗證。

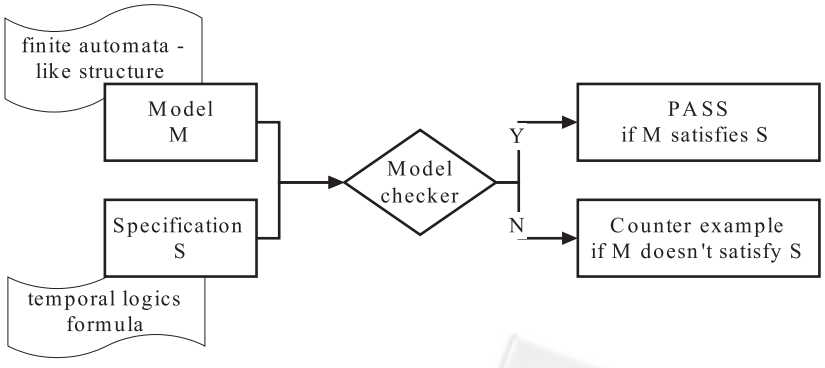

圖1：模型檢測運作示意圖

參、進行驗證

使用FDR進行驗證之前，必須先使用CSP做為狀態間轉換的描述工具，將欲驗證的

協定及欲驗證的特性分別建模成為一連串流程，前者稱為SYSTEM，後者為SPEC。建模完成後，再進入FDR分析，如果結果呈現SYSTEM的所有狀態完全包含於SPEC的狀態，也就是SYSTEM為SPEC的子集合，即可謂此協定滿足某種特性。

一、協定建模

協定共有四個階段，其中消費者與商家之間的購買與交貨過程，與公平特性最為緊密相關，因此本研究將以第三階段的購買流程為焦點進行建模。首先，如圖2針對上述流程進行傳送訊息的圖表分析，清楚界定交易成員之間所有的訊息傳遞。接下來使用CSP，針對每個交易成員所屬流程以及交易成員間的通道進行建模建模後，結合所有流程，協定即建模完成。

（一）交易成員所屬流程建模

以下就消費者流程中的購買階段為例進行建模，其中c代表消費者、m代表商家、b代表銀行。c在協定當中需先完成欲購商品之挑選，並向b提領電子現金後，才進入購買階段－c與m交換彼此的電子現金與商品（Lin and Liu, 2007）：

1. c→m：$E_{sek_{CM}}(tn,pid,E_{k_C}(s,m,v,c),kr_C,E_{pk_B}(tn,r_C))$

   c傳送交易編號(tn)、產品編號(pid)及加密的電子現金（$E_{k_C}(s,m,v,c)$）及銀行公鑰加密後的電子現金解密資訊（$E_{pk_B}(tn,r_C)$）給商家，其中$E_{sek_{CM}}$代表用消費者及商家共用的session key加密，E_{k_C}是以消費者的對稱式鑰匙加密，kr_C可用來算出K_C，r_C是消費者任選的亂數。將傳送的訊息精簡為加密的電子現金，建模如下：

   ```
   CONSUMER = coutm ! e_ecash -> E_ECASH_SENT
   ```

   其中CONSUMER代表消費者流程名稱，coutm代表c輸出m的通道、!代表傳送、e_ecash代表加密電子現金、-> 代表進入下一個流程、整句代表c向 m送出加密電子現金後進入下一步。

2. m→c：$E_{sek_{CM}}(tn,E_{k_{pid}}(DC_{pid}),kr_M,co_{tn},cert_{pid})$

   m接收到c的加密電子現金後，轉送給銀行檢驗其合法性及是否重覆花費。若成功b則將該筆電子現金記錄於資料庫，並將結果回傳給m。m檢視結果後無誤則回覆c 交易編號、加密的數位內容商品（$E_{k_{pid}}(DC_{pid})$）、承諾（co_{tn}）及產品憑證（$cert_{pid}$），其中k_{pid}為商家販售DC_{pid}所設的對稱式鑰匙，kr_M可以讓消費者算出k_{pid}，以便解密DC_{pid}。將傳送的訊息精簡為加密的數位內容商品，建模如下：

   ```
   E_ECASH_SENT = cinm ?a -> if (a==e_dc) then CHECK_EDC
   else E_ECASH_SENT
   ```

其中cinm代表c 從m輸入的通道、a代表接收的資訊、e_dc代表加密之商品、整句代表c從接收的訊息若為加密商品，則進行檢驗e_dc的動作，否則繼續靜待回覆。

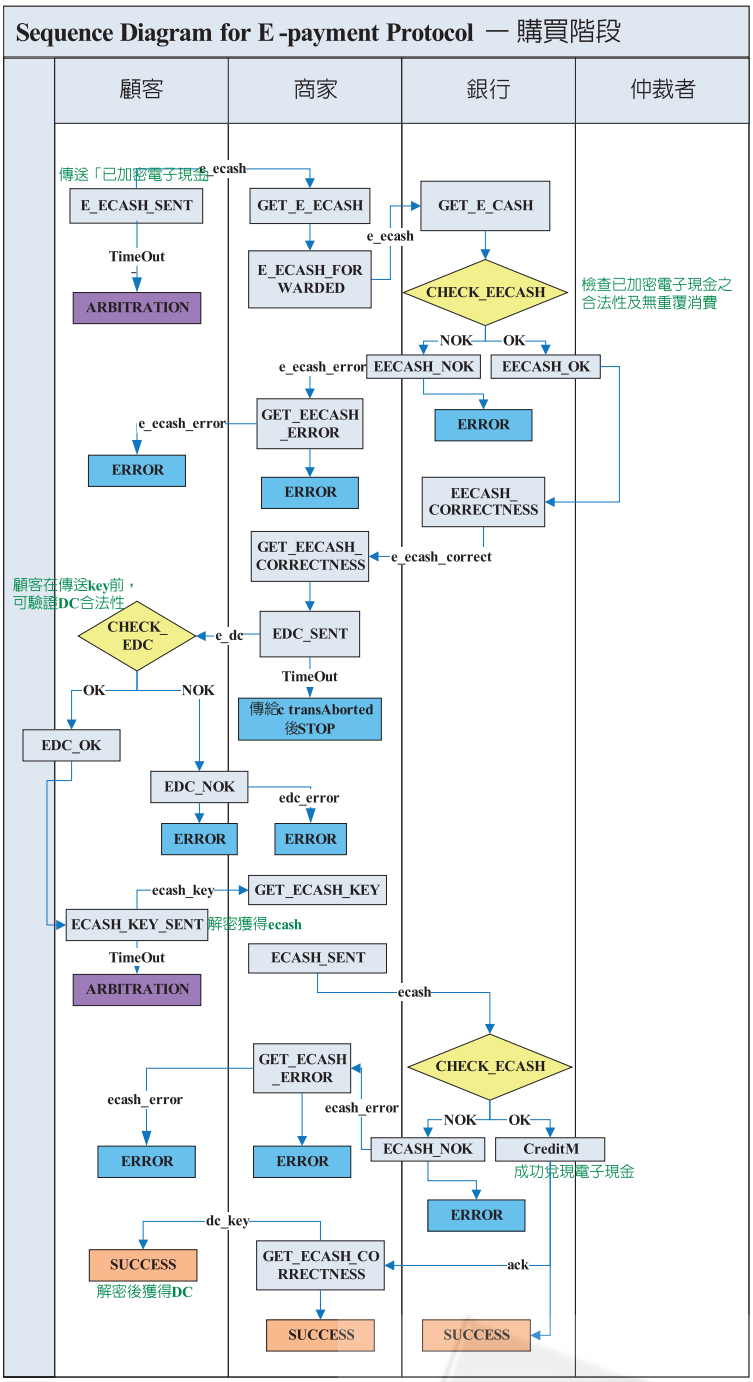

圖2：協定流程圖表分析

協定中整體購買流程共分為九個部份，在此列舉兩個部份呈現建模之關鍵，商家流程與銀行流程的建模方式也與此類似。其他如送出的電子現金為不合法時、收到的商品不正確時、等待逾時等例外情況在此不贅述，但都會包含於SYSTEM一同進行驗證。

（二）交易成員間通道之建模

兩兩交易成員之間均有傳送與接收兩個通道，例如在c與m之間，就有COMMcm與COMMmc兩條通道，如下所示：

```
COMMcm = []x: {e_cash, cash_key} @(coutm ?x -> (minc !x -> COMMcm))
COMMmc = []x: {e_dc,dc_key} @(moutc ?x -> (cinm !x -> COMMmc))
```

三個參與者間共有六條通道，其它五道通道在此亦不贅述，所有通道結合的描述如下所示：

```
COMM = (((( COMMcm [|{}|] COMMcb) [|{}|] COMMmc) [|{}|] COMMmb)
[|{}|]COMMbc) [|{}|] COMMbm
```

完成所有交易成員的流程與所有通道的建模之後，即可集結所有元素成SYSTEM，例完成協定建模，其中{coutm.e_cash,minc.e_cash}的內容將會隨著欲檢驗之特性而有所不同：

```
SYSTEM = (((CUSTOMER [|{}|] MERCHANT) [|{}|] BANK) [|COMMIO|]
COMM) \ diff(COMMIO,{coutm.e_cash,minc.e_cash})
```

二、特性建模

（一）金錢原子性：金錢在交易過程中不會被憑空創造，也不會無端減少。

由於c與m在使用電子現金交易時，並不直接傳送電子現金，而是先傳送加密電子現金，再傳送電子現金的解密金鑰由m自行解密。因此無論遺失上述任一訊息，也不會對金錢原子性造成威脅。然而，m解密電子現金後傳送到b兌現時若發生錯誤，可能導致電子現金無端減少。相關流程如下：(1) m接到c的電子現金解密金鑰。(2) m解密電子現金後轉送給b檢驗合法性。(3) 若檢驗成功，則將款項存入m帳戶並通知m。(4) 若檢驗失敗，則直接通知m失敗訊息。

若步驟1或2沒有達成，電子現金可能會無故減少，因此本特性建模如下：

```
SPEC1 = STOP |~| ((moutb.ecash -> binm.ecash -> boutm.ack -> STOP) []
 (moutb.ecash -> binm.ecash -> boutm.ecash_error -> STOP))
```

（二）貨品原子性：「商家收到款項」與「消費者收到商品」這兩項事件必定同時成立，或者同時不成立。

在交易過程中，c和m會先交換加密電子現金和商品，再互換解密金鑰。但金鑰的交換順序為c先傳送給m，m再傳送給c。這將導致c必需承受m收到金鑰且兌現成功後，拒傳其商品金鑰的風險。相關交易流程如下：(1) c傳送m加密電子現金。(2) m檢驗現金

後，回傳c加密商品。(3) c檢驗商品後，回傳m電子現金解密金鑰。(4) m收到金鑰兌現成功後，回傳c商品解密金鑰。若交易步驟3完成後，4卻沒有接續完成，將損害c之權益，因此本特性建模如下：

SPEC2 = STOP|~|((minc.e_ecash -> STOP) [](minc.e_ecash -> cinm.e_dc -> STOP)[] (minc.e_ecash -> cinm.e_dc -> minc.ecash_key -> cinm.dc_key -> STOP) [] (minc.e_ecash -> cinm.e_dc -> minc.ecash_key -> cinm.ecash_error -> STOP))

（三）有效接收性：消費者在付款之前，擁有驗證商品正確性的能力。

相關交易流程如下：(1) 消費者接收到商家的加密商品，開始檢驗其商品。(2) 若檢驗成功，回傳現金的解密金鑰。(3) 若檢驗失敗，通知商家失敗訊息，終止交易。若步驟2或3沒有達成，則表示消費者並沒有進行商品檢驗的能力，不符合公平性的定義，因此本特性建模如下：

SPEC3 = STOP |~|(cinm.e_dc -> ((coutm.ecash_key -> STOP) |~|(coutm.edc_error -> STOP)))

三、驗證結果

以上協定與公平特性皆建模完成之後，即可進入FDR進行驗證。驗證時FDR會載入先前建模的協定流程，包含消費者流程、商家流程及銀行流程，還有三方參與者之間的通道，及欲檢驗的三種特性，然後進行驗證。FDR驗證結果如圖3所示，上節的建模：金錢原子性(SPEC1)、貨品原子性(SPEC2)及有效接收性(SPEC3)，執行後均以打鉤顯示，代表通過驗證。亦即，滿足所述三個公平特性。

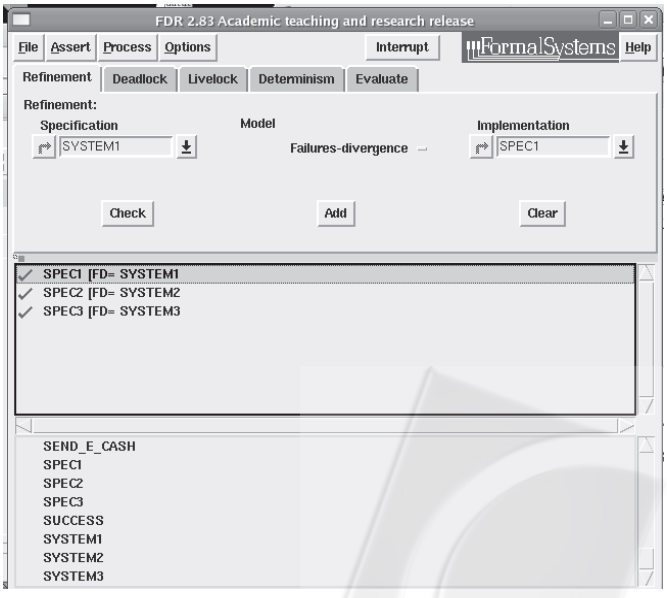

圖3：FDR驗證結果

肆、故障分析

最後分別加入網路斷線、交易成員系統故障等意外狀況，做進一步驗證。

一、網路斷線

三個交易成員間共有六條通道，但消費者與銀行互通的兩道通訊流程在購買階段未使用，因而此處將針對剩下四道較為關鍵的通訊流程進行網路故障情境的建模。網路斷線的情況具體可表示為各個交易成員之間的通道都可能發生故障，必需分別重新建模與驗證，例如消費者到商家間的通道建模如下：

```
COMMcm = []x: {pid, e_cash, cash_key} @(coutm ?x -> (COMMcm|~|(minc !x ->
COMMcm)))
```

其中的COMMcm|~|表示除了正常完成程序之外，也可能發生無法正常傳送訊息的可能。其它五條通道依此類推，驗證的結果如下表：

表1：網路斷線之驗證結果

通道故障	金錢原子性	貨品原子性	有效接收性
消費者→商　家	○	○	○
商　家→消費者	╳	╳	╳
商　家→銀　行	╳	╳	╳
銀　行→商　家	╳	╳	╳

○：該特性驗證通過、╳：該特性驗證不通過

根據特性違背數量統計資　顯示，不同成員之間若發生網路斷線，對公平性將產生不同影響。除了消費者至商家之間不會對公平性產生影響之外，其它通訊流程故障之時，皆會對原本滿足的公平特性造成影響。這是由於消費者至商家若發生斷線，消費者在一開始即無法傳送加密電子現金來啟始交易，因而不會發生不公平的情形，而其它路線卻是在交易啟始之後才被使用，會導致成員在送出某些敏感資訊後卻得不到回應，進而違背公平交易特性。

二、交易成員之系統故障

各交易成員之流程必需重新建模為故障模式，因此列舉消費者一部份的流程示範建模，其中程序起頭必須加入ABORT|~|，表示該道程序除了正常完成，也有隨時中斷的可能：

```
CUSTOMER = ABORT|~|coutm ! e_ecash -> E_ECASH_SENT
E_ECASH_SENT = ABORT |~|cinm ?a -> if (a==e_dc) then CHECK_EDC
else E_ECASH_SENT
```

不同交易成員系統分別故障時，驗證的結果如下：

表2：交易成員系統故障之驗證結果

交易成員系統故障	金錢原子性	貨品原子性	有效接收性
消費者	○	╳	╳
商　家	○	╳	○
銀　行	╳	╳	○

○：該特性驗證通過、╳：該特性驗證不通過

統計資料顯示不同成員的系統若發生故障，皆會對原本滿足的公平特性造成些許的影響，以下分別就三個特性的驗證結果進行探討。第一，金錢原子性在銀行系統故障之時，可能產生違背。是由於銀行在接收商家的兌現要求後，若發生系統故障，可能導致電子現金無故消失。第二，貨品原子性被影響最鉅，由於它牽涉的層面較廣，只要任一交易成員的系統故障，本特性即違背。第三，有效接收性在消費者系統故障之時，可能產生違背。是由於消費者系統故障，而無法進行商品的檢驗程序所致。

伍、結 論

本研究主要是探究如何驗證一個線上交易協定是否具有公平交易的特性，保障交易成員毋須擔憂自身權益受損，進而促進電子商務發展。相較於傳統的模擬或測試方法，本研究使用正規驗證方式，提供一完整的建模架構，成功的達成快速且效率驗證協定的目的。根據驗證結果，Lin and Liu (2007) 所提出的協定在正常運作下，皆能夠滿足基本公平特性。但倘若意外發生，例如任一方參與者系統當機時、或是任兩方網路斷線時，協定原先具備的金錢原子性、貨品原子性或有效接收性等公平特性無法如常保有，進而可能造成交易成員喪失電子現金等不可預期之損失。此時，如遇特性有所違背的情況，FDR會提供反例，協定設計者即可藉此進一步分析錯誤原因，以便修正協定缺失。因此加入反例分析，找出協定具體的缺失點後予以改進，將為本研究的下一階段重要目標。

除了本研究的三種特性，建議未來的研究可再拓展其它公平特性，甚至公平性外的其它安全特性，並擴增同質性交易成員的數量以複雜化協定，達到更嚴密完整的驗證結果。此外，正規驗證方法建構在時態邏輯的理論之上，主要應用於硬軟體的驗證，而非專為驗證線上交易協定所設計，因此應用於電子商務領域時產生一定的局限性：無法檢驗時間序列概念之外的特性，例如協定中經由加密機制帶來的安全特性等等，同時也受限於正規語言的表達性，使模型無法完全呈現真實的協定表現，建議未來研究可搭配其它方式輔助驗證，達到更完整的檢驗結果。

參考文獻

1. 孫鴻業，「美線上內容服務營收僅緩步成長 網路安全性為障礙」，FIND網路脈動，2006，http://www.find.org.tw/find/home.aspx?page=news&id=4195
2. Anderson, B.B., James V. Hansen, Paul Benjamin Lowry, and Scott L. Summers, "The application of model checing for securing e-commerce model checking is an effective component for performing online transactions that build customer trust and confidence," *Communications of the ACM*, Vol. 49, No. 6, 97-101, 2006.
3. Formal Systems (Europe) Ltd, "Failures-Divergence Refinement: FDR2 User Manual", 2005.
4. Gartner, F.C., H. Pagnia, and H. Vogt., "Approaching a formal definition of fairness in electronic commerce," *In Proceedings of the International Workshop on Electronic Commerce*, pages 354-359, Lausanne, Switzerland, IEEE Computer Society Press.454-459, 1999
5. Grau, Jeffrey, "Online Privacy and Security: The Fear Factor," eMarketer Reports, 2006. (available online at http://www.emarketer.com/Report.aspx?privacy_retail_apr06)
6. Kim, I.G. and Choi, J.Y., "Model Checking of RADIUS Protocol inWireless Networks," *IEICE Trans. Commun.*, Vol. E88-B. No.1, 397-398, 2005.
7. Lin, S.J. and Liu, D.C., "A Fair-Exchange and Customer-Anonymity Electronic Commerce Protocol for Digital Content Transactions," *Lecture Notes in Computer Science (4882)*, pp. 321-326, 2007.
8. Lowe, G., "Breaking and fixing the Needham-Schroeder public-key protocol using FDR," *Proc. TACAS*, no.1055 in LNCS, Springer-Verlag, 1996.
9. Muller-Olm, Markus, David Schmidt, and Bernhard Steffen, "Model-Checking a Tutorial Introduction," *A. Cortesi, G. File (Eds.): SAS'99*, LNCS 1694, pp. 330-354, 1999.
10. Ray, Indrakshi and Indrajit Ray, "Failure Analysis of an E-commerce Protocol Using Model Checking", *Proceedings of the Second International Workshop on Advanced Issues of E-Commerce and Web-based Information Systems*, Milpitas, CA, 2000.
11. Wang, F., "Formal Verification of Timed Systems: A Survey and Perspective," *Proceedings of the IEEE*, Vol. 92, Nr. 8, 1283-1307, 2004.