利用模糊簽名達成線上公平遊戲之研究

Online Fair Games based on Oblivious Signatures

左瑞麟	吳佩穎	黃齡葦	張莞純
國立政治大學	國立政治大學	國立政治大學	國立政治大學
資訊科學系	資訊科學系	資訊科學系	資訊科學系
Email: raylin@cs.nccu.edu.tw	Email: 95703055@nccu.edu.tw	Email: 95703052@nccu.edu.tw	Email: 95703051@nccu.edu.tw

摘要：

由於網路的蓬勃發展，帶動了線上遊戲的興起。線上公平遊戲(online fair games)，如：猜拳遊 戲、樂透遊戲 …等。因為輸贏可能牽涉到個人利益等等的商業行為，所以遊戲的公平與公正性變得非常重要。目前這些線上的公平遊戲大多需要可信賴的第三機構來執行，或利用密碼學中的模糊傳輸(OT)的方式來達成。另外，利用模糊傳輸的方式，為了達到不可否認性，有時可能還要再加上簽名機制才能構造出一個完整可信賴的線上公平遊戲。本研究利用模糊簽名(OS)來實現同樣的公平遊戲。和利用模糊傳輸(OT)及簽名的方式相比較，因為利用 OS 可一次達到遊戲的公平、公正與不可否認性，因此本研究方式會較為有效率。另外，因為不需用到 OT 及簽名兩套密碼系統，所以在實作上也將較為簡捷。

關鍵字：

密碼學(cryptography)、公平遊戲(fair game)、模糊簽名(oblivious signature) 、模糊傳輸(oblivious transfer)、線上遊戲(online game)。

壹、前言

由於網路的蓬勃發展，使得人與人之間溝通無界線，也帶動了線上遊戲的興起，線上博亦遊戲的資料大部份也都經由網路的傳輸，使得資料的安全性、正確性和遊戲本身的公平性備受考驗。

以最簡單的遊戲”猜拳”來說，在現實中，我們玩猜拳遊戲會同時出拳，因為這樣就無法先得知對方所要出的拳而再來改變自己的拳，即可達到公平性，謂為 online fair game。但在網路上，同時出拳是不可能的，因為網路上傳輸是有先後順序的，所以必須要有一方要先選擇自己所要出的拳，再

由另一方出拳，此時，公平性就面臨爭議了。舉例來說，使用者先出剪刀，因為網路上傳輸的先後順序問題，server 端即可先知道使用者的拳是剪刀，進而改變 server 端的拳為石頭，不管使用者怎麼選，server 端永遠是贏的一方，這種遊戲並非公平的遊戲。

再由樂透遊戲來探討，使用者選擇了六個號碼，而 server 端知道了使用者所選的號碼，下次中獎號碼公佈時，即不會公佈這六個號碼，這也是不公平的遊戲。

基於上述的缺點，實有必要提出安全的保護方法，保護使用者在遊戲中所選擇的拳以及樂透號碼在網路上傳送給 server 端時的安全性，使其不被竊取竄改，即使被截取了，也只是一堆被加密後的亂碼，而無法得知使用者的選擇。server 端也無法解密得知使用者所選的選擇，之後 server 簽名，達到不可否認性。

本研究的目的在探討如何運用 oblivious signature 達成一個 online fair game。另外，將針對提案方式及其它用 oblivious transfer 的 fair game 在效率及公平性方面作比較。

二、背景與文獻探討:

線上公平遊戲(Online fair game)目前並不如實體店面興盛，大多人購買各種彩券皆是到一般彩券行，透過電視轉播，或是公平、公正、公開的機構達到彩券的公信力，其中樂透通常是用紙張印刷，讓購買樂透者以畫卡的方式選號，目前樂透這類型的公平遊戲較少在線上進行，因為線上進行遊戲的同時性、公平性較難做到。目前的線上樂透遊戲(online lottery)大多利用模糊傳送(oblivious transfer)[2,3,6]的方式達成。

Oblivious transfer 是一種很特殊的訊息傳遞方式。以 1-out-n oblivious transfer 為例，其概念是：

(1). 提供者(Sender)有 n 個機密訊息欲傳送給接收者(Receiver),
(2). Receiver 只能選擇得到 n 個訊息當中之其中一個機密訊息，
(3). 在提供資訊服務過程中，Sender 無法獲知使用者選擇得到哪一個機密訊息，
(4). 另一方面,Sender 確信 Receiver 最終只能得到 n 個訊息中的其中一個。

以[6]為例，簡單介紹 oblivious transfer 的傳遞方式。假設 Sender 有 n 個訊息，依序為 M_1，M_2， …，至 M_n。Sender 欲將 n 個訊息中的其中一個傳送給 Receiver。假設 Receiver 欲接收第 α 個訊息 M_α。為了防止 α 值被 Sender 知道，Receiver 隨機選取一個亂數 r，利用 r 將 α 加密成 y 並將 y 回傳給 Sender。Sender 再利用 y 將所有 messages M_i 加密成 C_i，$1 \leqq i \leqq n$，並傳給 Receiver。此時 Receiver 可以由 Sender 傳回的 n 個 C_i，$1 \leqq i \leqq n$，中計算出 M_α，取得想得到的訊息，但無法取得 M_α 以外的其他訊息。

詳細演算法如圖 2.1 所示:

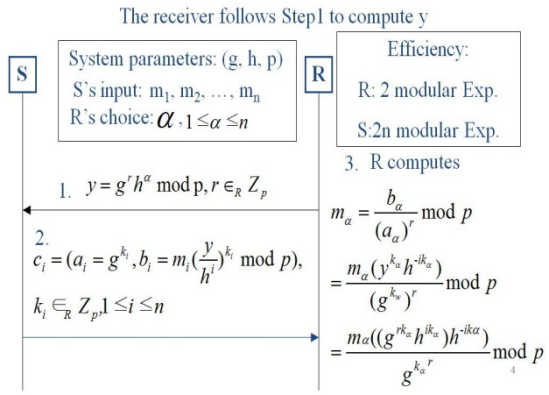

圖 2-1.Oblivious Transfer Algorithm

以下用猜拳遊戲為例，介紹如何利用 oblivious transfer 構造 online fair game。假設訊息 M_1,M_2,M_3 分別代表剪刀,石頭以及布。Dealer 先公開 M_1,M_2,M_3。Player 選擇第 α 個 message，$\alpha \in \{1,2,3\}$，利用亂數 r 將 α 加密為 y 後送回 y 給 Dealer。此時 Dealer 不知道 Player 選擇了那一個 message。Dealer 再將三個訊息都用 y 做加密後傳給 Player，Player 經由計算後可得 M_α。開獎時只要 Dealer 公布自己所選的拳，Player 再將 Dealer 公布的結果與自己手上的 M_α 作比較即可判斷輸贏。

過程簡圖如下:

圖 2-2.Oblivious Transfer Algorithm

Oblivious Transfer 可以使 Player 無法得到其選擇以外的其他 message，也保障 Player 選擇的訊息不會讓 Dealer 知道，故能防止 Dealer 作弊。

2.1 利用 Oblivious Transfer 的缺點

Oblivious Transfer(OT)不具不可否認性，因為在演算法過程中，並不包含 Sender 簽名的部分，Sender 可能否認訊息並不是由該端所發出，若要具備不可否認性，必須事先對每個訊息做簽名，因此 OT 需與其他簽名驗證系統配合，如此一來，每個使用者需有兩套系統(OT 系統及簽名驗證系統)，會在效率上花更多時間。

公平性方面，Oblivious Transfer 中 Sender 可能有 1/n 的機率作弊成功。例如:在猜拳遊戲裡，若 Sender 事先猜測 Player 可能會選擇”布”的 message，則 M_1,M_2,M_3 傳的皆是 message”布”。當 Receiver 的選擇為”布”時，Receiver 不會發現遊戲有問題。此時 Sender 也可得知 Receiver 選擇”布”(因為 M_1,M_2,M_3 皆是”布”)，因此只要出”剪刀”，即可作弊成功，導致公平性方面產生問題。

2.2 基於模糊簽名的線上公平遊戲

- **模糊簽名基本介紹:**

模糊簽名是電子簽章的一種類型，是由 D. Chen[1]在 1994 年所提出的。完整的模糊簽名包括了三個成員：一個簽名者(a signer S)，一個接受者 (a recipient R) 及一個認證者 (a

verifier V)。模糊簽名的特性就是接受者可以在 L 個訊息中選擇一個訊息給簽名者簽署，而簽名者不知道 L 個訊息中何者為接受者所需要的，只能確定接受者所選的訊息確實在 L 個訊息中的其中一個。因此，使用這個方法可以保障使用者的隱私而同時又能保護簽名者不會簽到任何他不願意簽署的文件。R. Tso 等學者[5]認為先前的方法沒有很清楚的顯現出模糊簽名的正規化的概念，於是於 2008 年將模糊簽名的模型及安全性明確的定義了出來。另外，由於 D. Chen[1]的方法架構對於通訊和計算方面缺乏效率，因此 R. Tso 等學者在[5]中另外提出了新的方案"1-out-of-n oblivious signatures"來改善這些問題。本研究將利用到 R. Tso 等學者的 1-out-of-n oblivious signatures 來實作我們的線上公平遊戲。以下首先針對 R. Tso 等學者的 1-out-of-n oblivious signatures 作一個詳盡的介紹。

- **1-out-of-n oblivious signatures**

(n 中選 1 的模糊簽名)的演算法

系統設定(System Setting)：

主要包含一個簽名者 S，一個接受者 R 及一個認證者 V。S 首先選取以下在產生簽名及驗證簽名時會用到的參數：

***p*、*q*:**兩個很大的質數，其中 $q|(p-1)$

***g*、*h*:** 循環群 Zp* 中的兩個元素，其序(order)為 q。另外，在 Zp*中的離散對數問題 $\log_g h$ 是（計算量上）困難的.

***H*:** $\{0,1\}^* \rightarrow Z_q^*$: 輸入為$\{0,1\}^*$的字串，輸出為 Z_q^*中的元素的單向雜湊函數 (one way hash function)

鑰匙生成(Key Generation):

簽名者 *S* 任意選取一數 $x \in Z_q^*$

然後計算 $y \leftarrow g^x \bmod p$.

S 的公開鑰匙(public key): y

S 的私密鑰匙(secret key): x

簽名階段（Signature Generation）:

假設接收者 *R* 欲得到訊息

$m_l \in \{m_1, \cdots, m_i, \cdots m_n\}$的簽名，其步驟如下:

步驟 1:

R 先選擇 $l \in \{1, \cdots, n\}$，然後計算 $c = g^r h^l \bmod p$ 並且把 c 與 n 個 message 傳給 S 作簽名。此 l 及表他所選擇的 m_l。

步驟 2:

S 也會選擇 n 個亂數 $k_i \in_R Zq^*$ ，$1 \le i \le n$，計算下列式子

- $K_i \leftarrow g^{ki} \bmod p$,
- $e_i \leftarrow H(m_i, K_i c/(gh)^i \bmod p)$,及
- $s_i \leftarrow K_i - x e_i \bmod q$.

最後 S 將$(e_i, s_i), 1 \le i \le n$ 送回 R。

步驟 3:

R 會先計算 $\delta_i \leftarrow g^{(r-i)} h^{(l-i)} \bmod p$, $1 \le i \le n$。然後藉由檢查下列公式驗證 S 的簽名。

$e_i = H(m_i, g^{e_i} y^{s_i} \delta_i \bmod p)$

， $1 \le i \le n$.

步驟 4:

如果$(e_i, s_i), 1 \le i \le n$,皆通過步驟三的驗證，代表 S 在簽名過程中沒

有造假。此時R即可利用以下方法得到關於m_l的簽名。亦即，可將模糊簽章轉換成正常的Schnorr簽章 (Schnorr signiture) [4]。其方法如下：

$e \leftarrow e_l$ 及

$s \leftarrow r\text{-}l + s_l \bmod q$,

所得到的$\sigma \leftarrow (e,s)$.即是m_l的簽章。

驗證階段(Signature Verification):

R將訊息m_l及得到的簽名$\sigma=(e,s)$公開後，驗證者V即可以利用下面的公式驗證這個簽名的有效性

$e = H(m_l, g^s y^e \bmod p)$.

基於離散對數問題，由於計算$\log_g h$是困難的，所以l一經決定後就無法再更改。所以確保了接收者R只能得到一個（事先決定好的）訊息的簽名。另一方面，此離散對數問題同時確保了簽名者無法得知l，亦即無法得知最終會簽到哪一個訊息。

以猜拳為例，Dealer先公開3個訊息M_1,M_2,M_3，分別代表剪刀、石頭及布，Player選擇第l個訊息，加密l並把加密後的訊息c送回給Dealer，此時Dealer不知道Player選擇了那一個message，Dealer再利用模糊簽名，將此三個訊息M_1,M_2,M_3都利用亂數c做簽名後傳給Player，Player經由計算後可得m_l的簽名，開獎時只要公布Dealer所選的拳與m_l作比較即可判斷輸贏。另外，因為簽名具有不可否認性，所以如果Dealer輸了，得到的m_l的簽名可以防止Dealer的事後否認。

參、分析與比較:

	公平性	不可否認性	效率
OT	○	需配合簽名系統	較差
OS	○	○	較好

OT過程中Sender將訊息傳給Receiver後，因為OT演算法中並沒有任何簽名，R無法辨認是否訊息為Sender傳送，造成OT不具不可否認性，若OT與其他簽名驗證系統配合，雖然可以解決此問題，但卻會造成效能降低；而OS則是將所有messages連同α加密成的c一起傳給S，再由S對全部訊息做模糊簽名。R在得到最終的簽名前，會對S的模糊簽名做驗證。如此S便沒有作弊的可能性，因此具有不可否認性，且R可以藉由驗證方式確定Mα上的簽名是合法的。

OT與OS兩者皆可以做到基本的安全性，可以保護Receiver選擇的訊息不被Sender看到，且除了被Receiver選擇的訊息外，Sender的其他訊息也不會被Receiver得到，但Oblivious Transfer有公平性上的問題，使得Sender有1/n的機率可以作弊成功，因此Oblivious Signature比Oblivious Transfer更具公正性。

效率方面，因為目前學界對OT的研究遠較OS為多，因此在OT中不乏許多非常有效率的方案。但OT因不具不可否認性，為了達到不可否認性，在OT方面，Sender端需加上n個簽名，而Receiver端需對n個簽名做驗證。此時，OS會較OT＋簽名有效率。尤其當OS及OT利用相同手法構造出來時，如W.Tzeng[6]的OT-Scheme和Tso

et al. [5] 的 OS 作比較時，此差異更為明顯。

由上述分析可得知，OS 比 OT 更為安全、具不可否認性、效率較佳，也更公平。

3.1 實做

利用 JAVA 對 Oblivious Signature 時做猜拳及樂透遊戲，實作方面:先由 Player 輸入其 ID 及 password，選擇要玩猜拳或是樂透遊戲，並且投注虛擬貨幣，Dealer 端驗證 Player 身分成功後，則傳送系統參數給 Player 端，Player 再將欲選擇的數字或猜拳符號加密後傳回，Dealer 端收到訊息後利用 Oblivious Signature 演算法將所有訊息簽名後回傳給 Player，Player 驗證並接受其選擇數字的簽名，到開獎日期，Dealer 公開開獎結果(即 Dealer 所出之拳或開獎號碼)，Player 即可得知猜拳遊戲輸贏或樂透遊戲是否中獎，即完成一回合的遊戲過程。

遊戲流程圖如下:

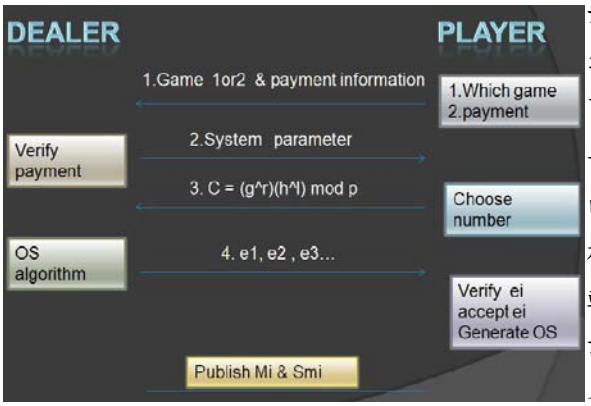

圖:5-1.project 流程圖

遊戲畫面如下:

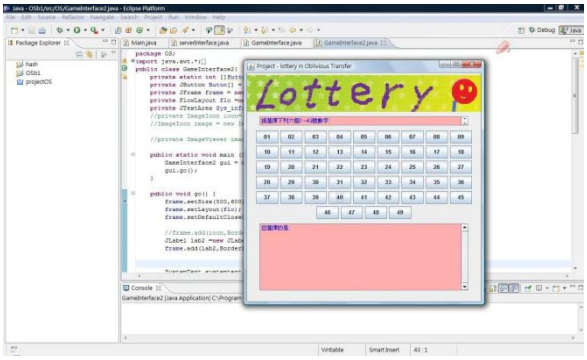

圖:5-2.lottery 遊戲畫面

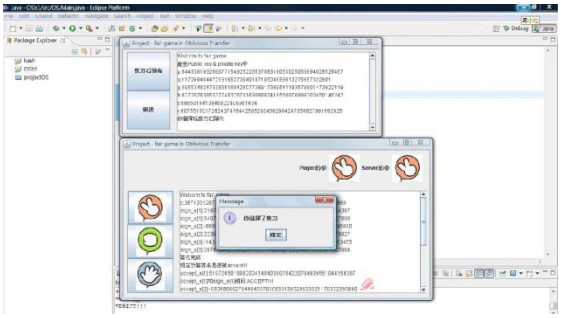

圖:5-3.猜拳遊戲畫面

肆、結論

本研究利用模糊簽名(Oblivious Signature)來實作線上公平的遊戲，如：猜拳遊戲、樂透遊戲…等。由於這類的線上博奕戲多牽涉到金錢等的商業交易行為，所以遊戲的公平性與安全性是非常重要的。目前這些線上的公平遊戲大多需要可信賴的第三機構來執行，或利用密碼學中的模糊傳輸來達成。由於模糊傳輸不具不可否認性，所以這類方式還需再利用電子簽名才能完整達到公平、公正及不可否認性。利用模糊簽名，可一次達到遊戲的公平、公正及不可否認性。因此，比利用 Oblivious Transfer 加簽名的方式更為有效率。

參考文獻

[1]. D. Chaum,“Blind signatures for untraceable payments”,Advances in Cryptology --CRYPTO'82, Sringer-Verlag, pp.199--203,1983.

[2]. S. Even, O. Glodreich and A. Lempel, “A randomized protocol for signing constructs”, Communications of the ACM 28 pp.637-647, 1985.

[3]. M. O. Rabin, “How to exchange secrets by oblivious transfer”, Tech. Memo TR-81, Aiken Computation Laboratory, 1981.

[4]. C. P. Schnorr, “Efficient signature generation by smart cards”, Journal of Cryptology, Vol. 4(3), pp.161-174, 1991.

[5]. R. Tso, T. Okamoto and E. Okamoto, “1-out-of-n oblivious signatures”, In Proceedings of ISPEC2008, Lectures Notes in Computer Science, Vol. 4991, pp.45-55, 2008.

[6]. W. Tzeng, “Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters”, IEEE Transactions on Computers, Vol. 53, No. 2, pp.232-240, 2004.