DOI: 10.6277/TER.202310_51(4).0001

Correlation with Forwarding

Chun-Ting Chen*

In this paper, I consider three-player complete information games augmented with pre-play communication. Players can privately communicate with others, but not through a mediator. I implement correlated equilibria by allowing players to authenticate their messages and forward the authenticated messages during communication. Authenticated messages, such as letters with signatures, cannot be forged but sent or received by players. With authenticated messages, I show that if a game G has an α as a point in the convex hull of Nash equilibrium, then any correlated equilibrium distribution in G, which has rational coefficients and gives each player a strictly higher payoff than what α does, can be implemented via a pre-play communication. The proposed communication protocol does not require perfect public recording, as has been used in Bárány (1992), and does not publicly expose players' private messages at any stage during communication.

Keywords: pre-play communication, correlated equilibrium, forwarding
JEL classification: C72, D83

*The author is an Assistant Professor at the Department of Economics at National Taipei University. The author thanks the editor, two anonymous referees, Kalyan Chatterjee, Chen-Ying Huang, Vijay Krishna, Melody Pei-Yu Lo, and Min-Hung Tsay, for their valuable comments. This work is financially supported by the Center for Research in Econometric Theory and Applications (Grant No. 110-L900-203) from the Featured Areas Research Center Program within the framework of the Higher Education Sprout Project by the Ministry of Education (MOE) in Taiwan, and by the Ministry of Science and Technology (MOST), Taiwan, under Grant No. 110-2634-F-002-045 and 107-2410-H-002-036.

臺灣大學學術期刊資料庫

經濟論文叢刊 (*Taiwan Economic Review*), 51:4 (2023), 429–462。
國立台灣大學經濟學系出版

1 Introduction

Suppose that there are three players, namely, *Int* (*Intermediator*), *S* (*Sender*), and *R* (*Receiver*), communicating with one another through writing letters. There are two ways for *Int* to send *S*'s messages to *R*: (1) writing letters without authentication or (2) forwarding letters with *S*'s authentication. In the first form, *Int* can privately rewrite *S*'s messages and then send the rewritten message to *R*. Contrary to the first form, in the second form, *Int* cannot rewrite the messages without *S*'s authentication; therefore, *Int* can only forward *S*'s letters to *R*. The first form can be interpreted as the *cheap talk*, whereas the second form, *forwarding*, is an added feature in this paper so that players can identify the origin of a message.

If players can communicate using forwarding, this paper examines whether the correlated equilibrium distribution (c.e.d.) of a game can be generated by an augmented pre-play communication procedure. The notion of correlation equilibrium (Aumann, 1974) is plausible since, in equilibrium, players have enforced themselves to act according to a c.e.d. When this c.e.d. assigns probability 0 to some outcomes that degrade players' welfare, players' welfare could be better off than Nash equilibrium. Nevertheless, a *mediator*, not a player herself, is well known to inhabit the notion of correlated equilibrium to enforce players' behaviors. Without a mediator, we may ask whether players can enforce themselves so that their outcomes can still be generated via a c.e.d.

Without a mediator, pioneering works have proposed different pre-play communication protocols to implement c.e.d. by cheap talk. Those protocols vary with each other regarding deviation-detection procedures and punishment schema. Notably, when the number of players is less than or equal to four, a procedure in their protocols seems indispensable — publicly exposing all previous messages. Bárány (1992) has four players. There, the way to detect unilateral deviation is by letting each player receive the same messages from two different players. *After* a deviation has been detected, the *public revealing procedure* — a procedure that publicly reveals all players' previous private messages — is activated. Every player then knows who has deviated and goes to the punishment phase. When there were less than four players, in Ben-Porath (1998), the public revealing procedure is randomly activated *no matter whether* a deviation has occurred. After this procedure is activated, players go to the punishment phase if deviations are detected; otherwise, they redo the protocol. Gerardi (2004) has five or more players

臺灣大學學術期刊資料庫

and used the majority rules to detect deviations. Each player receives the same messages sent from three different players, and therefore, the unilateral deviation can be identified. Since only unilateral deviation is considered, no punishment schema is needed in Gerardi (2004). For two-player complete information games, it is impossible to implement c.e.d., as shown in Ben-Porath (1998).

Using forwarding, in three-player complete information games with finite actions, this paper removes the public revealing procedure. It allows players to detect unilateral deviation without exposing players' private messages at any stage in the pre-play communication. Seeing public revealing as powerful is not hard. Such a procedure is powerful because it not only reveals all private messages, but also exposes all private messages publicly. Only the convex hull of Nash equilibrium can be implemented after this kind of deviation-detection procedure. Contrary to the public revealing procedure, the deviation-detection procedure proposed in this paper is a zero-knowledge proof. It is: conditional on each player's private message relevant to his action, information regarding other players' private messages is the same as that induced by a c.e.d. even after the deviation-detection procedure. To put it differently, in the terminology of computer science, the essence of this paper is a zero-knowledge proof to correlate actions for three-player games.

To replace the public revealing procedure, forwarding is used in my protocol. Intuitively, since players' messages can be authenticated, the forwarding enforces *Int* to deliver *S*'s true message to *R*. This aspect of forwarding is like to "record" players' messages. However, if *Int* indeed records *S*'s messages, then *Int* can manipulate *S*'s messages by sending recorded *S*'s messages. Messages circulated by forwarding have to be "identified" well to qualify themselves. Moreover, if all messages guiding players' actions are circulated by forwarding, since forwarding already involves three players, players' actions will become publicly known. Hence, private messages between two players are indispensable in implementing c.e.d. outside the convex hull of Nash equilibrium. Since private messages are indispensable, to detect deviations, messages circulated must be well "encoded" so that they can be detected if deviations occur.

Although the encoding rule in this paper is technical, the protocol itself is based on a simple fact: the joint distribution is the marginal distribution

臺灣大學學術期刊資料庫

multiplying the conditional distribution.[1] Recall what a mediator does in a c.e.d., q. This mediator recommends a_i to each player i while letting i's conditional distribution conditional on a_i over others' actions a_{-i} be $q(a_{-i} \mid a_i)$. The above idea suggests that if a protocol can implement q, then this protocol will let a_i be chosen with probability $q(a_i)$ and let a_{-i} be chosen with probability $q(a_{-i} \mid a_i)$. The remaining question is to ensure that i can only observe the messages that guide i to act a_i. Based on these ideas, in Section 3.1, Example 1 gives a protocol that implements a c.e.d. for a three-player game in which there is a player who has only one action. In Section 3.2, Example 2 shows a protocol with its deviation-detection procedure if players have two actions. The case for finite actions can be proved and shown in Appendix A.

Following is the positive result obtained by this paper. Suppose a finite game G has three players and has an α as a point in the convex hull of Nash equilibrium. Then, for any c.e.d. q in G, which has rational number coefficients and gives all players higher expected payoff than what α does, this q can be realized as a Nash equilibrium in a finite-period pre-play communication extension $ext(G)$ of G, in which forwarding is applied.

This paper is organized as follows. I describe my model in Section 2. I state my main result and depict my communication protocol by two examples in Section 3. In Section 4, I relate my paper to the current literature and compare the required assumptions in implementing correlated equilibria for future extensions. The proofs for my main result are all in Appendix A.

2 Model

For a set X, the cardinality of X is denoted by $|X|$, and the set of probability distributions over X is denoted by ΔX.

G is a three-player game in the strategic form. Let $I = \{1, 2, 3\}$ be the set of players. For each $i \in I$, A_i is i's set of actions with generic element a_i. The set of action profiles is denoted by $A = \times_{i \in I} A_i$ with generic element a. For each i, let $u_i : \times_{i \in I} A_i \to \mathbb{R}$ be i's payoff function. A randomized action for i is an element in $\triangle A_i$ and is denoted by σ_i. Denote $\sigma \in \times_{i \in I} \triangle A_i$ as a randomized action profile. For convenience, also denote a_{-i} as an element

[1] This multiplication of marginal probability and conditional probability argument is the main ingredient in implementing correlated equilibrium for two-player games, as in Ben-Porath (1998) or Dodis, Halevi, and Rabin (2000).

臺灣大學學術期刊資料庫

in $\times_{j\neq i} A_j$ and denote σ_{-i} as an element in $\times_{j\neq i} \triangle A_j$.

Definition 2.1. (Nash equilibrium) $\sigma = (\sigma_i)_{i\in I}$ is a Nash equilibrium (NE henceforth) if and only if

$$u_i(\sigma_i, \sigma_{-i}) \geq u_i\left(\sigma_i', \sigma_{-i}\right),$$

for all i and for all $\sigma_i' \in \triangle A_i$.

Definition 2.2. (Correlated equilibrium) $q \in \triangle A$ is a correlated equilibrium distribution if and only if, for all i, for all a_i, for all a_i',

$$\sum_{a_{-i}} q\left(a_{-i}|a_i\right) u_i(a_i, a_{-i}) \geq \sum_{a_{-i}} q\left(a_{-i}|a_i\right) u_i\left(a_i', a_{-i}\right),$$

where $q(a_{-i}|a_i)$ is the conditional distribution of a_{-i} conditional on a_i.

I then consider an extension $ext(G)$ of G such that it allows finite stages of communication before G is played. In these communication stages, players can send or receive costless messages. The question is whether players can enforce themselves to act according to q in G after the pre-play communication phase in $ext(G)$. I assume players can use forwarding in pre-communication to answer this question. Forwarding allows players to forward messages by assuming that the messages are encoded by players' authentication, such as their signatures.

Forwarding Without cost, each player i can send messages with his own authentication. Furthermore, j can pass i's authenticated messages to k; k can verify i's authentication, and j cannot forge i's authentication.

3 Result

In this section, I state my main result and illustrate my pre-play communication protocol using two examples. In Example 1, I consider a straightforward case also discussed by Bárány (1992) in which there is a player who has only one action. In this case, Bárány (1992) has shown that there is a c.e.d. that cannot be implemented by the pre-play communication so that deviations can be detected with probability 1. I will however show that such c.e.d. can be implemented by a pre-play communication with forwarding

臺灣大學學術期刊資料庫

so that deviations can be detected with probability 1. In Example 2, I consider a case in which each player has two actions. In this case, the c.e.d. can be implemented in finite steps in which deviations are detected with high probability. Appendix A shows the proof of my main result and the protocol for general cases. I first state my main result as follows.

Theorem 1. Let G be a three-player game in which α is a point in the convex hull of NE. For any c.e.d. in G that has rational number coefficients and gives all players strictly higher expected payoffs than what α does, if players can communicate with forwarding, then there exists an $ext(G)$ such that this c.e.d. can be realized as a NE in $ext(G)$.

proof. In Appendix A. □

I begin to show the main idea in my protocols using two examples. In the remainder of this paper, the term *jointly* refers to *jointly-controlled lottery* (j.c.l. henceforth) (Aumann and Maschler, 1995). The j.c.l. is a procedure to generate a targeting distribution by two or more players, in which unilateral deviation cannot change the distribution that is meant to be generated. The j.c.l. procedure will publicly inform an outcome drawn from the targeting distribution to players.

3.1 Example 1 — forwarding

I first consider a straightforward example discussed in Bárány (1992) to see how forwarding helps players correlate actions. Let G be a three-player game so that $A_1 = \{N, S\}$ ({"north","south"}), $A_2 = \{E, W\}$ ({"east","west"}), and $A_3 = \{0\}$ with payoff matrix

	W	E
N	(6,6,0.1)	(2,7,0)
S	(7,2,0)	(0,0,5)

in which Player i's payoff is indicated by the ith element in a payoff vector.[2] We may consider a c.e.d. q that gives a higher welfare than all points in the convex hull of NE do. This q assigns probabilities over action profiles such that

$$q(N, W, 0) = q(N, E, 0) = q(S, W, 0) = \frac{1}{3}.$$

[2] My example is a modified version of Bárány (1992). The original example can be represented by

臺灣大學學術期刊資料庫

Denote $q(a_1)$ as the marginal distribution of $a_1 \in A_1$; denote $q(a_2|a_1)$ as the conditional distribution of $a_2 \in A_2$ given a_1.[3]

To implement q via pre-play communication, we should first notice that Player 1 and Player 2 cannot communicate only by themselves. This is because q is outside the convex hull of NE. If Player 1 and Player 2's actions were solely contingent on the messages communicating between them, only the points in the convex hull of NE in G can be implemented, since they publicly know these messages.

In other words, Player 3 must be able to privately send messages to Player 1 and Player 2 to induce them to play q. However, Player 3 is not incentivized to do so. After all, he only can get the payoff of 1/30 from q, while deviating from q would get him a better payoff. Furthermore, it is nontrivial to detect Player 3's deviation. In fact, his deviation cannot be detected with probability 1 (as shown by Bárány (1992)). To see this, note that q assigns positive probabilities on $(N, E, 0)$ and $(S, W, 0)$. Thus, there is a pair of Player 3's messages, one of which, say m^{32}, privately sent to Player 2 to induce Player 2 to play E, and one of which, say m^{31}, privately sent to Player 1 to induce Player 1 to play S. However, $(S, E, 0)$ gives Player 3 the highest payoff. Therefore Player 3 can send this pair of messages without being detected with probability 1 to induce Player 1 and Player 2 to play $(S, E, 0)$, which gives Player 3 a higher payoff than that from q.

A pre-play communication should prevent Player 3 inducing E if he induces S. My protocol use forwarding to accomplish so. The key here is that, instead of freely sending private messages to Player 1 and Player 2, Player 3 correlates Player 1 and Player 2's actions by forwarding Player 1's messages to Player 2. First, let Player 1 and Player 3 conduct a j.c.l. in choosing Player

	W	E
N	(6,6,0)	(2,7,0)
S	(7,2,0)	(0,0,5)

in which Player 3 gets a strictly positive payoff only at the action profile $(S, E, 0)$. There exists, nevertheless, no point in the convex hull of NE in the original example that gives each player a strictly less expected payoff than q does. My example has a point α in the convex hull ($\alpha(S, W, 0) = \alpha(N, E, 0) = 1/2$) to give each player a strictly less expected payoff than q does.

[3]The c.e.d. q yields a payoff (5, 5, 1/30) with the corresponding welfare (301/30). The NE payoffs are (7, 2, 0), (2, 7, 0), and [4(2/3), 4(2/3), (54/90)] with corresponding welfare 9, 9, and (894/90).

臺灣大學學術期刊資料庫

1's action a_1 according to $q(a_1)$. Then, contingent on a_1, Player 1 sends a set of authenticated messages to Player 3, distributed as $q(a_2|a_1)$ and meant to induce Player 2's action a_2. Afterward, Player 3 privately forwards one of these authenticated messages to Player 2, determining Player 2's action. Using forwarding, Player 2 can verify Player 1's authentication, and Player 3 cannot forge it. Thus, the probability that $(a_1, a_2) = (S, E)$ is 0 since $q(E|S) = 0$. Furthermore, since $q(a_1, a_2) = q(a_1) \cdot q(a_2|a_1)$, if Player 1 acts a_1 and Player 2 acts a_2, then q is being generated.

In other words, the presence of Player 3 is a "virtual urn". Continent on Player 1's action, Player 1 can send different messages that induce Player 2's actions to Player 3 while letting Player 2 draw a message from Player 3 so that (1) Player 1 does not know which message has been drawn, and (2) Player 2 does not know the distribution of messages. Player 1 must not know which message has been drawn; otherwise, Player 1 will know Player 2's action. Player 2 must not know the distribution of messages held by Player 3. Otherwise, Player 2 will be able to infer Player 1's action. In the absence of Player 3, such an urn does not exist. However, since Player 3 is a player instead of an urn, Player 3 might have incentives to change the distribution of the received messages sent by Player 1. The authentication issued by Player 1 is meant to deter Player 3's manipulation.[4]

As follows, I show my protocol — F protocol (*Forwarding protocol*) — for this example.[5]

F protocol

[4]It is also crucial to enforce Player 1 to send the distribution $q(a_2|a_1)$ according to $q(a_1)$ instead of sending some other distribution. Since Player 3 is a player, Player 3 can monitor whether Player 1 has sent the legitimate distribution of messages.

[5] My result still holds in the case that Player 3 can forge Player 1's authentication but it can be detected by Player 2 with a probability very close to 1. The punishment schema will still be triggered if forging is detected. In computer science, authentication can be accomplished by digital signature. For a cheap talk implementation, one can consider the following scenario. Whenever Player 1 asks Player 3 to send a message, say the number "1", to Player 2, he also asks Player 3 to send it with its authentication code, say "apple". It will be very hard for Player 3 to send the number "2" instead without being caught if he has no idea about number "2"s authentication code. As long as Player 1 and Player 2 can privately decide the authentication code for each number, Player 3's manipulation can be detected with arbitrarily high probability.

臺灣大學學術期刊資料庫

1. **STEP 0** We first prepare random variables that are used to generate the intended distribution of messages in **STEP 2** and **STEP 3**. Let $Y = \{\bar{y}, \bar{\bar{y}}\}$ be an arbitrary set with two elements. Player 1 and Player 3 jointly and uniformly choose a permutation $\pi : Y \to Y$. Independently from π, Player 2 and Player 3 jointly and uniformly choose a number $y \in Y$. All random variables are chosen via j.c.l.
2. **STEP 1** Player 1's action is determined in this step. To do so, Player 1 and Player 3 jointly and randomly choose an element $a_1 \in A_1$ according to $q(a_1)$.
3. **STEP 2** Contingent on a_1 and given the chosen π, Player 1 sends a list of authenticated messages (authenticated by Player 1) to Player 3: if $a_1 = N$, Player 1 sends $([m]_{\pi(\bar{y})}, [m]_{\pi(\bar{\bar{y}})}) = ([W, \pi(\bar{y})], [E, \pi(\bar{\bar{y}})])$; otherwise, he sends $([m]_{\pi(\bar{y})}, [m]_{\pi(\bar{\bar{y}})}) = ([W, \pi(\bar{y})], [W, \pi(\bar{\bar{y}})])$.
4. **STEP 3** This step determines Player 2's action. Given the chosen y, Player 3 forwards the message $[m]_y$ to Player 2. ($[m]_y$ is the message authenticated by Player 1, of which the last element is y.)

   Player 2's action is the first element of $[m]_y$.
5. **STEP 4** The protocol ends. Player 1 and Player 2 play their recommended actions chosen in **STEP 1** and **STEP 3**, and Player 3 plays action 0.

If players follow the protocol, it is straightforward to check that Player 1 and Player 2's actions, as well as their information regarding each other's actions, are induced by q. In **STEP 1**, Player 1's action is chosen according to $q(a_1)$. In **STEP 3**, when Player 3 forwards Player 1's messages to Player 2, Player 1 does not know which message specified by y has been chosen. This is because Player 1 does not know the chosen y, Player 1 does not know Player 2's action. Meanwhile, Player 1's prescribed messages sent to Player 3 are distributed as $q(a_2|a_1)$. Therefore, in **STEP 3**, Player 2's action is induced by $q(a_2|a_1)$. Finally, since a_1 and π are chosen by Player 1 and Player 3, Player 2 does not know Player 1's action.

Players' deviations in the protocol can be detected with probability 1. In **STEP 2**, Player 3 is able to monitor whether Player 1 has sent the prescribed messages to him since a_1 is jointly chosen by Player 1 and Player 3. Furthermore, in **STEP 3**, Player 2 is able to verify whether Player 3 has sent the correct authenticated messages in which y is on the last element.

臺灣大學學術期刊著作權

To provide players the right incentives to follow the protocol, the deviation-detection procedure and the punishment schema for this example are below.

- Deviation-detection procedure (**DD1**): If Player i's deviation is detected by Player j, both Player i (the player who deviates) and Player j (the player who detects it) send the message **STOP** to all other players, and then all players go to the punishment schema; otherwise, both of them send the message **OK** to all other players.
- Punishment schema: Let α be the point in the convex hull of NE such that
$$\alpha(N, E, 0) = \alpha(S, W, 0) = 1/2.$$
Players first publicly perform a j.c.l. that generates α.[6] Players then play $(N, E, 0)$ or $(S, W, 0)$ according to α.

Since α gives a strictly lower payoff to every player than q does, players will not deviate from the protocol.

A downside of this protocol is that Player 3 will know Player 1 and Player 2's actions. Nevertheless, Player 3 has only one action in this example, and therefore his action in G still follows q. The next section discusses the general cases when Player 3 has multiple actions. The current protocol will be modified so that players' actions are not exposed to any other player, and deviations can be deterred with a probability larger than 1/2.

3.2 Example 2 — randomized-forwarding and deviation-detection

In this section, consider the game in which $A_1 = \{N, S\}$, $A_2 = \{E, W\}$, and $A_3 = \{0, 1\}$. Let q be the c.e.d. that assigns equal probabilities over the action profiles such that

$$q(N, W, 0) = q(N, E, 0) = q(N, E, 1) = q(S, W, 0) = \frac{1}{4}.$$

Assume that there is an α in the convex hull of NE so that α gives each player a strictly lower expected payoff than q does.

[6] As in Gerardi (2004), we can arbitrarily assign two players, say Player 1 and Player 2, to publicly perform a j.c.l. that generates α. That is, Players 3 is a witness in this j.c.l. process and informed about the outcome.

臺灣大學學術期刊資料庫

In this example, if Player 1 and Player 2's actions are exposed to Player 3 during pre-play communication, Player 3 would not follow the recommended actions generated by the protocol. Suppose the action profile $(a_1, a_2, a_3) = (N, E, 0)$ is being generated by the protocol. Player 3 would deviate from playing $a_3 = 0$ since, according to q, playing 1 is his best response given that $(a_1, a_2) = (N, E)$.

Using forwarding, we have a better protocol than Example 1 so that Player 1 and Player 2's actions are not exposed to Player 3. Consider the following procedure with T steps. In each step, contingent on some $a_1 \in A_1$, Player 1 authenticates a message $[a_2, y]$ and sends it to Player 3, where $a_2 \in A_2$ and y is an arbitrary number that indexes this message. Afterwards, Player 3 forwards this authenticated message to Player 2. Due to forwarding, Player 3 cannot manipulate $[a_2, y]$ contingent on a_1. After T steps, Player 2 should get a list of $([a_2^1, y^1], \cdots, [a_2^T, y^T])$ contingent on Player 1's list $(a_1^1, \cdots, a_1^T)$. Afterwards, Player 1 and Player 2 jointly and uniformly choose a $t^* \in \{1, \cdots, T\}$ without being known by Player 3. Player 3 would not know the chosen pair $(a_1^{t^*}, [a_2^{t^*}, y^{t^*}])$ since he does not know t^*, even if he has known $(a_1^1, \cdots, a_1^T)$ as well as $([a_2^1, y^1], \cdots, [a_2^T, y^T])$.

To generate Player 3's action, we can modify the above procedure so that Player 2 gets a list in the form of $([a_2^1, a_3^1, y^1], \cdots, [a_2^t, a_3^t, y^t], \cdots [a_2^T, a_3^T, y^T])$ in which the second element of a message, $a_3^t \in A_3$, determines Player 3's action. After that, Player 1 and Player 2 jointly and uniformly choose a $t^* \in \{1, \cdots, T\}$, and then Player 2 reports the chosen $a_3^{t^*}$ to Player 3. For our purpose, as an instance, contingent on Player 1's list

$$l_1 = (N, N, N, S), \tag{1}$$

we can let Player 2 get the list of

$$l_2 = \left(\left[W, 0, y^1\right], \left[E, 0, y^2\right], \left[E, 1, y^3\right], \left[W, 0, y^4\right]\right), \tag{2}$$

so that whenever $t^* \in \{1, 2, 3, 4\}$ is uniformly chosen by Player 1 and Player 2, players' actions are correlated according to q provided that Player i plays $a_i^{t^*}$.

The above procedure has generated q when players do not deviate. However, Player i's belief over others' actions is not the same as $q(a_{-i}|a_i)$. (For instance, Player 2 would know Player 1's action since he knows the order of Player 1's list.) As follows, Section 3.2.1 assumes players are honest (no deviation) and illustrates a protocol that prevents this situation. Section 3.2.2

臺灣大學學術期刊資料庫

incorporates the deviation-detection procedure to deter deviations with a probability no less than 1/2 when players might deviate.

3.2.1 Honest Players

In this section, I suppose that players would not deviate. Players, however, would be able to conceive the others' actions during the protocol. I modify the above procedure so that every Player i's belief over others' actions is the same as $q(a_{-i}|a_i)$.

We first see how to prevent Player 2 knowing Player 1's action. To fix the idea, let the original lists be l_1 for Player 1 and l_2 for Player 2. We can let Player 1 reorder his own list and, at the same time, randomly choose the indices of authenticated messages. To be precise, if Player 1 reorders his list $l_1 = (N, N, N, S)$ to $l_1' = (S, N, N, N)$ and indexes the sequence of his authenticated messages by (y^1, y^2, y^3, y^4), then Player 2 will get the list of

$$l_2 = \left(\left[W, 0, y^1\right], \left[E, 0, y^2\right], \left[E, 1, y^3\right], \left[W, 0, y^4\right]\right),$$

but contingent on

$$l_1' = (S, N, N, N),$$

instead of $l_1 = (N, N, N, S)$. Player 2 would not know Player 1's action since he does not know Player 1's reordering and indexing.

Next, we can prevent Player 1 from knowing Player 2 and Player 3's actions. Player 3 will reorder Player 2's list. To fix the idea, let the original lists be l_1' for Player 1 and l_2 for Player 2. At each step, instead of sending an authenticated message, Player 1 sends a set of authenticated messages to Player 3. More precisely, at each step when Player 1's action is S, Player 1 will send the set of messages $\{[W, 0, y^1]\}$ to Player 3; and contingent on N, Player 1 will send $\{[E, 0, y^2], [E, 1, y^3], [W, 0, y^4]\}$. At each step, Player 3 forwards one of Player 1's authenticated messages to Player 2 ordered by Player 3's own ordering over Player 1's messages. Precisely speaking, if Player 3 orders $\{[E, 0, y^2], [E, 1, y^3], [W, 0, y^4]\}$ (contingent on N) to $([W, 0, y^4], [E, 0, y^2], [E, 1, y^3])$, then contingent on Player 1's list,

$$l_1' = (S, N, N, N),$$

Player 2 will get the list of

$$l_2' = \left(\left[W, 0, y^1\right], \left[W, 0, y^4\right], \left[E, 0, y^2\right], \left[E, 1, y^3\right]\right)$$

臺灣大學學術期刊資料庫

by Player 3's ordering. Thus, Player 1 would not know Player 2 and Player 3's actions since Player 2's list has been reordered.

Furthermore, we can prevent Player 2 from knowing Player 3's action. Player 1's authenticated messages will "rotate" Player 3's actions on Player 2's list. That is, if $a_3 \in A_3$ is Player 3's recommended action, it will be uniformly rotated to some $a_3' \in A_3$ on Player 2's list. To accomplish so, Player 1's list is extended to be in the form of $((a_1^t, r^t))_t$, where $r^t \in \{0, 1\}$ indicates the rotation of Player 3's recommended action. To fix the idea in our context, let the original lists be l_1' for Player 1 and l_2' to Player 2. Player 1's list is extended to be

$$\begin{aligned} l_1'' &= \left(\left(a_1^t, r^t\right)\right)_t \\ &= ((S, 0), (N, 0), (N, 0), (N, 0), (S, 1), (N, 1), \\ &\quad (N, 1), (N, 1)), \end{aligned}$$

and contingent on l_1'', Player 2's original list, l_2', is extended to be in the form of $([a_2^t, a_3^t, y^t])_t$ so that

$$\begin{aligned} l_2'' &= \left(\left[a_2^t, a_3^t, y^t\right]\right)_t \\ &= \left(\left[W, 0, y^1\right], \left[W, 0, y^2\right], \left[E, 0, y^3\right], \left[E, 1, y^4\right], \left[W, 1, y^5\right], \right. \\ &\quad \left. \left[W, 1, y^6\right], \left[E, 1, y^7\right], \left[E, 0, y^8\right]\right). \end{aligned}$$

That is, for each message in l_2'', the second element, a_3^t, represents Player 3's rotated action such that Player 3's action will be determined to be

$$a_3^{t^*} + r^{t^*} (\text{mod} 2)$$

for some chosen t^*. Player 1 and Player 2 then choose $t^* \in \{1, \cdots, 8\}$, and then report r^{t^*} and $a_3^{t^*}$ to Player 3 respectively. Player 2 would not know Player 3's action, since he does not know the rotation r^{t^*} and since Player 3's action is uniformly rotated.

Finally, Player 3 does not know Player 1 and Player 2's actions, since he only knows about $a_3^{t^*}$ and r^{t^*} and since t^* is privately chosen by Player 1 and Player 2.

The following RF protocol (*Randomized-Forwarding protocol*) summarizes the above ideas (in **Step 0.1** and **Step 0.2** as follows). To begin with, I list the messages that will be authenticated by Player 1 for this protocol in Figure 1.

臺灣大學學術期刊資料庫

$(N,0)$	$(N,0)$	$(N,0)$	$(S,0)$	$(N,1)$	$(N,1)$	$(N,1)$	$(S,1)$
$[W,0,1]$	$[E,0,2]$	$[E,1,3]$	$[W,0,4]$	$[W,1,5]$	$[E,1,6]$	$[E,0,7]$	$[W,1,8]$

Figure 1: An example of Player 1's 8 authenticated messages in RF protocol

RF Protocol

1. **Step 0.1**: Player 1 prepares the authenticated messages. Each message has its own index randomly chosen by Player 1. Let $T = \{1, \cdots, 8\}$ be the set of steps and let $Y = T$ be the set of indices. Let $R = \{0, 1\}$ with generic element r. An example of these messages with their indices is listed in Figure 1. A box in Figure 1 has the form of

(a_1, r)
$[m]_y$

in which $a_1 \in A_1$, $r \in R$, and $[m]_y$ is the message in the form of $[a_2, a_3, y]$ so that $a_2 \in A_2$, $a_3 \in A_3$, and y is the index of this message. If $[m]_y$ is intended to be contingent on (a_1, r), then $[m]_y$ and (a_1, r) are within the same box.

2. **Step 0.2**: We prepare some random variables meant to prevent players' actions from being exposed to one another. These random variables will be used in **Step 1**. First, Player 1 and Player 3 jointly and uniformly choose a bijection (a permutation)

$$\phi : T \to Y.$$

Let

$$\chi : Y \to A_1 \times R$$

be the mapping such that, for each $y \in Y$, the authenticated message $[a_2, a_3, y]$ is contingent on $\chi(y)$. Notice that ϕ and χ will induce a mapping

$$\chi\phi : T \to A_1 \times R.$$

Restricted by $\chi\phi$, Player 3 uniformly chooses a bijection (a permutation)

$$\pi : T \to Y$$

臺灣大學學術期刊資料庫

so that

$$\chi\pi(t) = \chi\phi(t)$$

for each $t \in T$.

3. **Step 1**: Player 1 and Player 2 get their lists of messages in this step. There are $|T|$ steps. For each t-step, $t \in T$, Player 1 authenticates the set of messages contingent on $f(t|\phi)$ to Player 3. After that, Player 3 forwards the message $[m]_{\pi(t)}$ to Player 2.

   After $|T|$ steps, Player 1 should get a list of

$$l_1^* = (\chi\phi(t))_t;$$

   Player 2 gets a list of

$$l_2^* = ([a_2, a_3, \pi(t)])_t .$$

4. **Step 2**: Player 1 and Player 2 get their recommended actions in this step. Player 1 and Player 2 jointly and uniformly choose a $t^* \in T$. Player 1 knows

$$\chi\phi\left(t^*\right) = \left(a_1^{t^*}, r^{t^*}\right);$$

   Player 2 knows

$$[m]_{y^{t^*}} = \left[a_2^{t^*}, a_3^{t^*}, y^{t^*}\right].$$

5. **Step 3**: Player 3 gets his recommended action in this step. Player 2 reports $a_3^{t^*}$ to Player 3, and Player 1 reports r^{t^*} to Player 3.
6. **Step 4**: The protocol ends. Players' recommended actions are determined by:

   - Player 1's recommended action is $a_1^{t^*}$.
   - Player 2's recommended action is $a_2^{t^*}$.
   - Player 3's recommended action is $a_3^{t^*} + r^{t^*} (\mathrm{mod} 2)$.

3.2.2 Deviation-Detection

There are two kinds of deviations that might occur in **Step 3** in the RF protocol. The first one is that Player 2 might deviate from reporting $a_3^{t^*} \in A_3$ to Player 3. The second is that Player 1 might deviate from reporting $r^{t^*} \in \{0, 1\}$ to Player 3. In this section, I show how deviations can be deterred during communication.

臺灣大學學術期刊資料庫

The idea in tackling the first kind is a natural analog of a daily example: whenever a terminal user needs to log in to a server, she needs to enter her ID and passcode. It realizes in our context by adding a "tag" for every Player 3's rotated action on Player 2's list. For every $a_3 \in A_3$ on Player 2's list, a tagging is a permutation

$$\theta(\cdot|a_3) : U \to U,$$

where U is an arbitrary set of numbers with generic element u. Given this tagging, on every message on Player 2's list and for every $a_3 \in A_3$, a number $\theta(u|a_3)$ is attached. Whenever Player 2 needs to report a_3 — the ID, he also needs to report $\theta(u|a_3)$ — the passcode. Player 2 knows the number of $\theta(u|a_3)$ but not $\theta(\cdot|a_3)$ and u. Provided that Player 1 and Player 3 know $\theta(\cdot|a_3)$ and u for every $a_3 \in A_3$, if Player 2 deviates to report a_3' instead of a_3, then Player 2 might be also wrong in reporting the number of $\theta(u|a_3')$. Therefore, Player 2's deviation can be detected by Player 3 with a probability of $1 - 1/|U|$.

To prevent Player 1 misreporting $r \neq r^{t^*}$ is more involved. Let us examine an example first. Suppose that the RF protocol (in **Step 1**) has generated

$$\begin{aligned} l_1^* &= \left(\left(a_1^t, r^t\right)\right)_t \\ &= ((N,0),(N,0),(N,0),(S,0),(N,1),(N,1),(N,1),(S,1)) \end{aligned}$$

to Player 1 and

$$\begin{aligned} l_2^* &= \left(\left[a_2^t, a_3^t, y^t\right]\right)_t \\ &= \left(\left[W,0,y^1\right],\left[E,0,y^2\right],\left[E,1,y^3\right],\left[W,0,y^4\right],\left[W,1,y^5\right],\right. \\ &\quad \left.\left[E,1,y^6\right],\left[E,0,y^7\right],\left[W,1,y^8\right]\right) \end{aligned}$$

to Player 2. After $t^* \in \{1, \cdots, 8\}$ is chosen, Player 1 should report $r = r^{t^*}$ to Player 3. Since Player 2 knows t^* while Player 3 knows l_1^*, a straightforward way to detect Player 1's deviation by reporting $r \neq r^{t^*}$ is to allow Player 3 to ask Player 2 whether t^* is in the set of

$$T(r) = \left\{t \in T | r^t = r\right\}$$

by reporting $T(r)$ to Player 2. Apparently, $t^* \in T(r)$ if and only if $r = r^{t^*}$. Therefore, Player 1's deviation can be detected with probability 1 this way.

臺灣大學學術期刊資料庫

Table 1:

	$r=0$	$r=1$
$v=\bar{v}$	$t\in\{1,2,3,4\}$	$t\in\{5,6,7,8\}$
$v=\bar{\bar{v}}$	$t\in\{9,10,11,12\}$	$t\in\{13,14,15,16\}$

However, if Player 1 indeed reports $r=r^{t^*}$ truthfully, Player 2 will be able to infer r from $T(r)$, since $T(r)$ is dependent on r.[7] Note that Player 2 also knows $a_3^{t^*}$. Player 2 will then know Player 3's recommended action, which is $a_3^{t^*}+r^{t^*}(\text{mod}2)$. The question boils down to finding a way to hide the information about r^{t^*} but still be able to detect Player 1's deviation.

To accomplish so, let us duplicate Player 1 and Player 2's lists so that the lists become

$$l_1'''=\left(l_1^*,l_1^*\right)$$

for Player 1 and

$$l_2'''=\left(l_2^*,l_2^*\right)$$

for Player 2. Note that the length of l_1''' is 16. We can index the copies of l_1^* by its order in l_1'''. Let $v\in\{\bar{v},\bar{\bar{v}}\}$ be such an index: if t^* is chosen from the first copy of l_1''' (i.e. $t^*\in\{1,\cdots,8\}$), then $v=\bar{v}$; if it is chosen from the second (i.e. $t^*\in\{9,\cdots,16\}$), then $v=\bar{\bar{v}}$. In other words, the set of steps, $\{1,\cdots,16\}$, can be partitioned into a 2-by-2 table by $r\in\{0,1\}$ and $v\in\{\bar{v},\bar{\bar{v}}\}$ according to l_1''' as shown by Table 1.

To ease the exposition, let us first denote the entry in Table 1 by $T(r,v)$ for each $(r,v)\in\{0,1\}\times\{\bar{v},\bar{\bar{v}}\}$. Now suppose $t^*=3$ is chosen. To hide Player 3's information about r^{t^*}, consider the following procedure. Suppose that Player 1 reports $(r',v')=(r^{t^*},\bar{v})$ (since $t^*\in\{1,\cdots,8\}$) to Player 3.

[7] To see this, suppose that $t^*=3$. If Player 1 reports truthfully, then we have $T(r^{t^*})=\{1,2,3,4\}$. Given $T(r^{t^*})$ and Player 2's list l_2^*, Player 2 knows that, for some $a_1^{t^*}$ and r^{t^*}, Player 2's action and Player 3's rotated action can be only chosen from the list

$$\bar{l}=\left(\left[W,0,y^1\right],\left[E,0,y^2\right],\left[E,1,y^3\right],\left[W,0,y^4\right]\right).$$

Since Player 3's recommended action is 0 if Player 2's action is W (according to q), Player 2 knows that r^{t^*} must be equal to 0. Otherwise, there is no suitable r so that Player 3's roated actions are in $\bar{l}$.

臺灣大學學術期刊資料庫

Afterwards, Player 3 randomly chooses a $\tilde{v} \in \{\bar{v}, \bar{\bar{v}}\}$ with equal probability for the r that is *not* equal to r'. Let us say $\tilde{v} = \bar{\bar{v}}$. Player 3 then reports the set $T(\bar{v}, \tilde{v})$ to Player 2, where

$$\begin{aligned} T(\bar{v}, \tilde{v}) &\equiv T\left(r = r^{t^*}, v = \bar{v}\right) \cup T\left(r \neq r^{t^*}, v = \tilde{v}\right) \\ &= T(0, \bar{v}) \cup T(1, \bar{\bar{v}}) \\ &= \{1, 2, 3, 4, 13, 14, 15, 16\}. \end{aligned}$$

Since the set $T(\bar{v}, \tilde{v})$ does not depend on the specific value of r, Player 2 cannot infer r from $T(\bar{v}, \tilde{v})$.

I claim that Player 1's deviation by reporting $(r', v') \neq (r^{t^*}, \bar{v})$ can be detected with probability at least 1/2. To see this, notice that if Player 1 reports truthfully, then $T(\bar{v}, \tilde{v})$ must include t^* by the construction of $T(\bar{v}, \tilde{v})$. Furthermore, according to Table 1, since Player 2 knows t^*, the only successful deviation for Player 1 without being detected is when Player 1 reports $r' = 1$ and Player 3 chooses $\tilde{v} = \bar{v}$. Since Player 3 randomly chooses $\tilde{v}$ between $\bar{v}$ and $\bar{\bar{v}}$, Player 1's deviation can be detected with probability at least 1/2.

The following RF+DD protocol incorporates the above deviation-detection procedure into the RF protocol. To begin with, I list the messages that will be authenticated by Player 1 in this protocol in Figure 2.[8]

RF+DD Protocol

1. **Step 0.0**: We first prepare the permutation θ that will be used to detect deviations. Let $U = \{\bar{u}, \bar{\bar{u}}\}$ with generic element u. Player 1 and Player 3 jointly and uniformly choose a permutation

$$\theta(\cdot|a_3) : U \to U$$

   for each $a_3 \in A_3$.

2. **Step 0.1**: Player 1 prepares the authenticated messages indexed by numbers. Let $T = \{1, \cdots, 32\}$ be the set of steps and let $Y = T$ be the set of indices. Let $R = \{0, 1\}$ and $V = \{\bar{v}, \bar{\bar{v}}\}$ with generic

[8] My result still holds in the case that Player 3 can forge Player 1's authentication but it can be detected by Player 2 with a probability very close to 1. The punishment schema will still be triggered if forging is detected. Authentication can be achieved by digital signature. For a cheap talk implementation, readers are referred to Footnote 5.

臺灣大學學術期刊資料庫

$(N,0,\bar{u},\bar{v})$
$[W,0,\theta(\bar{u}\mid 0),1]$
$[E,0,\theta(\bar{u}\mid 0),2]$
$[E,1,\theta(\bar{u}\mid 1),3]$

$(N,1,\bar{u},\bar{v})$
$[W,1,\theta(\bar{u}\mid 1),5]$
$[E,1,\theta(\bar{u}\mid 1),6]$
$[E,0,\theta(\bar{u}\mid 0),7]$

$(N,0,\bar{\bar{u}},\bar{v})$
$[W,0,\theta(\bar{\bar{u}}\mid 0),17]$
$[E,0,\theta(\bar{\bar{u}}\mid 0),18]$
$[E,1,\theta(\bar{\bar{u}}\mid 1),19]$

$(N,1,\bar{\bar{u}},\bar{v})$
$[W,1,\theta(\bar{\bar{u}}\mid 1),21]$
$[E,1,\theta(\bar{\bar{u}}\mid 1),22]$
$[E,0,\theta(\bar{\bar{u}}\mid 0),23]$

$(S,0,\bar{u},\bar{v})$
$[W,0,\theta(\bar{u}\mid 0),4]$

$(S,1,\bar{u},\bar{v})$
$[W,1,\theta(\bar{u}\mid 1),8]$

$(S,0,\bar{\bar{u}},\bar{v})$
$[W,0,\theta(\bar{\bar{u}}\mid 0),20]$

$(S,1,\bar{\bar{u}},\bar{v})$
$[W,1,\theta(\bar{\bar{u}}\mid 1),24]$

$(N,0,\bar{u},\bar{\bar{v}})$
$[W,0,\theta(\bar{u}\mid 0),9]$
$[E,0,\theta(\bar{u}\mid 0),10]$
$[E,1,\theta(\bar{u}\mid 1),11]$

$(N,1,\bar{u},\bar{\bar{v}})$
$[W,1,\theta(\bar{u}\mid 1),13]$
$[E,1,\theta(\bar{u}\mid 1),14]$
$[E,0,\theta(\bar{u}\mid 0),15]$

$(N,0,\bar{\bar{u}},\bar{\bar{v}})$
$[W,0,\theta(\bar{\bar{u}}\mid 0),25]$
$[E,0,\theta(\bar{\bar{u}}\mid 0),26]$
$[E,1,\theta(\bar{\bar{u}}\mid 1),27]$

$(N,1,\bar{\bar{u}},\bar{\bar{v}})$
$[W,1,\theta(\bar{\bar{u}}\mid 1),29]$
$[E,1,\theta(\bar{\bar{u}}\mid 1),30]$
$[E,0,\theta(\bar{\bar{u}}\mid 0),31]$

$(S,0,\bar{u},\bar{\bar{v}})$
$[W,0,\theta(\bar{u}\mid 0),12]$

$(S,1,\bar{u},\bar{\bar{v}})$
$[W,1,\theta(\bar{u}\mid 1),16]$

$(S,0,\bar{\bar{u}},\bar{\bar{v}})$
$[W,0,\theta(\bar{\bar{u}}\mid 0),28]$

$(S,1,\bar{\bar{u}},\bar{\bar{v}})$
$[W,1,\theta(\bar{\bar{u}}\mid 1),32]$

Figure 2: An example of Player 1's 32 authenticated messages in RF+DD protocol

element r and v respectively. An example of these messages are listed in Figure 2. (Comparing to RF protocol, there are additional copies of authenticated messages for each $u \in U$ and $v \in V$.)

A box in Figure 2 has the form of

(a_1, r, u, v)
$[m]_y$
$\vdots$
$[m]_{y'}$

in which $a_1 \in A_1$, $r \in R$, $u \in U$, $v \in V$, and $[m]_y$ is the message in the form of $[a_2, a_3, \theta(u|a_3), y]$ so that $a_2 \in A_2$, $a_3 \in A_3$, and y is the index of this message. If $[m]_y$ is intended to be contingent on (a_1, r, u, v), then $[m]_y$ and (a_1, r, u, v) are within the same box.

3. **Step 0.2**: This step is the same as **Step 0.2** in RF protocol in which the permutations ϕ, π are chosen, and the mapping χ is determined. The only difference from **Step 0.2** in RF protocol is the codomain of χ. Now, the codomain of χ is $A_1 \times R \times U \times V$.

臺灣大學學術期刊資訊網

4. **Step 1**: The procedure in this step is the same as **Step 1** in RF protocol.
5. **Step 2**: The procedure in this step is the same as **Step 2** in RF protocol except for that, now, Player 1 knows

$$\chi\phi\left(t^*\right) = \left(a_1^{t^*}, r^{t^*}, u^{t^*}, v^{t^*}\right);$$

Player 2 knows

$$[m]_{y^{t^*}} = \left[a_2^{t^*}, a_3^{t^*}, \theta\left(u^{t^*}|a_3^{t^*}\right), y^{t^*}\right].$$

6. **Step 3** The procedure in this step is the same as **Step 3** in RF protocol except for that after t^* is chosen, Player 2 reports

$$m^{23} = \left(a_3^{t^*}, \theta\left(u^{t^*}|a_3^{t^*}\right)\right)$$

to Player 3; Player 1 reports

$$m^{13} = \left(r^{t^*}, u^{t^*}, v^{t^*}\right)$$

to Player 3.

7. **Deviation-Detection (Step 4)** This step is the deviation-detection procedure. Two kinds of deviations might be made in **Step 3**: Player 1 misreports m^{13} or Player 2 misreports m^{23}.

Suppose Player 2 reports $(a_3', u') \neq m^{23}$. This deviation is detected if $u' \neq \theta(u^{t^*}|a_3')$.

Next, suppose Player 1 reports $(r', u', v') \neq m^{13}$. First, define

$$T(r, u, v) \equiv \{t \in T | \chi\phi(t) = (a_1, r, u, v) \text{ for some } a_1\}.$$

Player 3 randomly chooses an element $\tilde{v} \in V$ with probability 1/2. Player 3 constructs the set $T(u', v', \tilde{v})$ so that

$$T\left(u', v', \tilde{v}\right) \equiv T\left(r', u', v'\right) \cup T\left(r \neq r', u', \tilde{v}\right),$$

and reports it to Player 2. Since Player 2 knows t^*, whenever $t^* \notin T(u', v', \tilde{v})$, Player 1's deviation is detected.

臺灣大學學術期刊資料庫

If Player i's deviation is detected by Player j in the above steps, both Player i (the player who deviates) and Player j (the player who detects it) send the message **STOP** to all other players, and then all players go to the punishment scheme; otherwise, both of them send the message **OK** to all other players.

8. **Step 5** The protocol ends. Players' recommended actions are determined as follows.

   - Player 1's recommended action is $a_1^{t^*}$.
   - Player 2's recommended action is $a_2^{t^*}$.
   - Player 3's recommended action is $a_3^{t^*} + r^{t^*} (\mathrm{mod} 2)$.

Now I can show that players' unilateral deviations can be detected with a probability of no less than 1/2.

Proposition 3.1. In the above RF+DD protocol, players' unilateral deviations can be detected with a probability no less than 1/2.

proof. **Step 0.0**, **Step 0.1**, **Step 0.2**, and **Step 2** are using j.c.l., and therefore players' deviations do not affect the distribution of permutations or elements intended to be generated in these steps. Deviations in **Step 1** will be detected with probability 1 since, in which, players use forwarding in transacting authenticated messages. I then check the possible deviations in **Step 3**.

I begin with Player 1's deviations in **Step 3**. Suppose that Player 1 reports $(r', u', v') \neq (r^{t^*}, u^{t^*}, v^{t^*})$. Then the probability of $t^* \in T(u', v', \tilde{v})$ is 0 if $u' \neq u^{t^*}$ by the construction of $T(u', v', \tilde{v})$. Furthermore, by the construction of $T(u', v', \tilde{v})$, the only successful deviation for Player 1 without being detected is when $u' = u^{t^*}$, $r' \neq r^{t^*}$ and $\tilde{v} = v^{t^*}$. Since Player 3 uniformly chooses $\tilde{v}$ from $\{\bar{v}, \bar{\bar{v}}\}$, this deviation can be detected with a probability no less than 1/2.

I then check Player 2's deviation in **Step 3**. Suppose that Player 2 follows the protocol, Player 2 should report $m^{23} = (a_3^{t^*}, \theta(u^{t^*}|a_3^{t^*}))$ to Player 3. If Player 2 reports $(a', u') \neq m^{23}$ instead, then Player 3 will detect this deviation if $(a', u') \neq (a', \theta(u^{t^*}|a'))$. Since $\theta(\cdot|a')$ is uniformly chosen without being known by Player 2, there is a probability of $1 - 1/|U| = 1/2$ so that $u' \neq \theta(u^{t^*}|a')$. Thus, this deviation can be detected with probability 1/2.

In summary, players' unilateral deviations can be detected with a probability no less than 1/2. □

臺灣大學學術期刊資料庫

I have to check further whether players' conditional probabilities conditional on their recommended actions over the others' is the same as that induced by q. The proof is straightforward but technical since the deviation-detection procedure in **Step 4** might leak information to players so that they can infer other players' recommended actions. The proof for Theorem 1 shows that this is not the case. Hence, I have the following proposition for Example 2.

Proposition 3.2. After the RF+DD protocol ends, if players has not yet received **STOP**, every player i's conditional probability conditional on his own recommended action a_i over others' recommended actions a_{-i} is the same as that induced by q.

proof. In the Appendix. □

4 Conclusion

The underlying question meant to be answered is whether the c.e.d. in a three-player game G can be implemented as a NE of a game $ext(G)$. This paper shows a positive result through the assumption that forwarding is possible. The benefit of forwarding is that the information regarding players' recommended actions is not exposed after the deviation-detection procedure. Players have the right incentive to play G according to q. It is in sharp contrast to using the public exposing procedure in Bárány (1992) or Ben-Porath (1998).

In the literature, for three or more players, Forges (1990), Gerardi (2004) and Ben-Porath (2003) use pre-play communication to implement communication equilibrium.[9] Gerardi (2004) uses majority rule for five players, and therefore no punishment schema is required. For three or four players, Forges (1990) assumes the existence of a correlation device; Ben-Porath (1998) and Ben-Porath (2003) do not assume a correlation device beforehand but use a public exposing procedure to prevent deviations.[10] Heller (2010) and Heller, Solan, and Tomala (2012) employ the technique in multiparty computation in computer science to implement correlated equilibrium or communication equilibrium. Multiparty computation is a protocol

[9]The notion of correlated equilibrium is extended to communication equilibrium for Bayesian games. Also, see Forges (1986) or Myerson (2004).

[10]Also, see Forges (2009).

臺灣大學學術期刊資料庫

to compute a multi-dimensional function so that players can only know the outputs projected to their own dimensions without knowing others'.[11] Their papers employ a public exposing procedure, as in Ben-Porath (1998), to detect deviations in the communication stage and require possibly infinite periods. My paper proposes forwarding to implement correlated equilibrium in finite periods. For a survey, further see Forges (2009).

Implementing correlation equilibrium or communication equilibrium is unattainable through cheap talk for two-player games, as shown in Ben-Porath (1998) or Vijay Krishna (2007). Nevertheless, it is possible if additional assumptions are added. Lehrer (1996), Lehrer and Sorin (1997), Gossner and Vieille (2001) and Vida and Āzacis (2013) consider an additional "mediated-talk" device. A mediated-talk device is a mediator that receives private inputs from players and sends public outputs. Lehrer and Sorin (1997) show that implementing correlated equilibrium can be accomplished in one-step pre-play communication through mediated-talk. Gossner and Vieille (2001) restrict the inputs or outputs to be 0 or 1 but gets the negative result. Vida and Āzacis (2013) also restrict the inputs or outputs to be 0 or 1 but further assumes that the mediated-talk can record players' private inputs and get the positive result. Ben-Porath (1998) implements correlated equilibrium by physical device "urns". One player can input private information, such as colored balls, to the urn, while the other can draw a ball from the urn without seeing the distribution of colors. Adopting a public exposing procedure, Ben-Porath (1998) implements correlated equilibrium in two-player cases.

Using cryptography, Dodis, Halevi, and Rabin (2000) (also see Urbano and Vila (2002) and Teague (2008)) attempt to implement correlated equilibria in two-player games, in which one player plays the role of a sender and the other as the role of a receiver. The sender encrypts and sends the action profiles to the receiver to choose an action profile to create correlation. Due to encryption, the sender's action is hidden from the receiver. In contrast, my protocol adds the third player to correlate players' actions. Using forwarding, the protocol is made to prevent one player's actions from being known by one another.

We may wonder if forwarding can replace the cryptography used in Dodis, Halevi, and Rabin (2000) or the urns used in Ben-Porath (1998) for two-player games. However, forwarding involves three players; therefore,

[11] See also Shamir (1979) and Ben-Or and Wigderson (1988) for multiparty computation.

臺灣大學學術期刊資料庫

forwarding is inapplicable in a two-player case. If there are only two players, forwarding is equivalent to cheap talk; therefore, implementing correlated equilibria is impossible. The difference between forwarding and the cryptography used in Dodis, Halevi, and Rabin (2000) or the urns is whether the content itself has been encrypted. In Dodis, Halevi, and Rabin (2000), the content of a message has been encrypted. By contrast, forwarding strengthens the ability to identify the origin of messages but not encrypt the content itself. Therefore, the power of forwarding is in the middle between urns and cheap talk.

Appendix

A.1 Proof for Theorem 1

The proof is constructive, and its essence is the same as that in Section 3.2. To begin with, I show my protocol in Section A.1.1, which is the same as the RF+DD protocol in Section 3.2. Then I check the deviation-detection probability in Section A.1.2, and check the conditional probabilities generated by the protocol in Section A.1.3.

For convenience, let us keep the following notations:

1. $A_i = \{1, \cdots, |A_i|\}$ be i's action set with generic element a_i for $i = 1, 2, 3$.
2. q is the targeting c.e.d. meant to be implemented. $q(a_i)$ is the marginal probability of a_i; $q(a_{-i}|a_i)$ is the conditional probability at a_{-i} conditional on a_i.
3. $R = A_3$ with generic element r. (R is just a copy of A_3 but with different interpretation: $r \in R$ is a rotation to rotate $a_3 \in A_3$ so that $r + a_3 (\text{mod} |A_3|)$ is an element in A_3).
4. $U = \{1, \cdots, |U|\}$ with generic element u. U is used in the deviation-detection procedure.
5. $V = \{1, \cdots, |V|\}$ with generic element v. V is used in the deviation-detection procedure.
6. $T = \{1, \cdots, |T|\}$ with generic element t. T is the set of steps used in **Step 1** in my protocol.
7. $Y = T$ with generic element y. (Y is just a copy of T but interpreted as the index set; $y \in Y$ is an index for Player 1 to index his authenticated messages. $|Y|$ is the total number of authenticated messages).

臺灣大學學術期刊授權

A.1.1 The protocol

We first determine $|Y|$. Since q has rational coefficients, it can be represented by its coefficients, i.e. $q = (q(a))_a$, in which each fraction has been reduced. Let lcm_q be the least common multiple of the denominators of q. The total number of authenticated messages $|Y|$ is determined by

$$|Y| = \text{lcm}_q \cdot |R| \cdot |U| \cdot |V|.$$

I begin to show my protocol.

- **Step 0.0**: We first prepare the permutation θ that will be used to detect deviations. Player 1 and Player 3 jointly and uniformly choose a permutation
$$\theta(\cdot|a_3) : U \to U$$
for each $a_3 \in A_3$,.
- **Step 0.1**: Player 1 prepares his authenticated messages. An arbitrary authenticated message is in the form of
$$[a_2, a_3, u, y],$$
where $a_2 \in A_2, a_3 \in A_3, u \in U, y \in Y$. Player 1 randomly and uniformly chooses y from Y so that each authenticated message has a distinct y. Let us call y the index of a message and denote $[m]_y$ as the message indexed by y.

  Let $M(a_1, r, u, v)$ be the set of authenticated messages contingent on $a_1 \in A_1, r \in R, u \in U, v \in V$. Let $(M(a_1, r, u, v))_{(a_1,r,u,v)}$ be a partition of Player 1's authenticated messages such that:

  1. The fraction of
  $$\frac{|M(a_1, r, u, v)|}{|Y|/(|R| \cdot |U| \cdot |V|)} = q(a_1),$$
  for every $a_1 \in A_1, r \in R, u \in U, v \in V$.
  2. The fraction of
  $$\frac{\left|\left\{[\bar{a}_2, \bar{a}_3, \bar{u}, \bar{y}] \in M(a_1, r, u, v) \,\middle|\, \bar{a}_2 = a_2, \bar{a}_3 + r \equiv a_3 \,(\text{mod}\,|A_3|)\right\}\right|}{|M(a_1, r, u, v)|} = q\left(a_2, a_3 \middle| a_1\right),$$
  for every $a_1 \in A_1, a_2 \in A_2, a_3 \in A_3, r \in R, u \in U, v \in V$.

臺灣大學學術期刊資料庫

3. For every authenticated message $[\bar{a}_2, \bar{a}_3, \bar{u}, \bar{y}]$, if

$$[\bar{a}_2, \bar{a}_3, \bar{u}, \bar{y}] \in M(a_1, r, u, v)$$

then

$$\bar{u} = \theta\left(u \middle| a_3\right),$$

for every $a_1 \in A_1, r \in R, u \in U, v \in V$.

Notice that, from the above construction, for every r, u, v,

$$\frac{\left|\left\{[\bar{a}_2, \bar{a}_3, \bar{u}, \bar{y}] \in M(a_1, r, u, v) \,\middle|\, \bar{a}_2 = a_2, \bar{a}_3 + r \equiv a_3 \,(\mathrm{mod}\,|A_3|)\right\}\right|}{|Y|/(|R| \cdot |U| \cdot |V|)} = q(a_1, a_2, a_3),$$

for every a_1, a_2 and a_3.

- **Step 0.2**: We prepare some random variables that will be used in **Step 1**. First, Player 1 and Player 3 jointly and uniformly choose a bijection (a permutation)

$$\phi : T \to Y.$$

Let χ be the mapping

$$\chi : Y \to A_1 \times R \times U \times V$$

such that $[a_2, a_3, \theta(u|a_3), y]$ is in the set of $M(\chi(y))$ for each $y \in Y$. Notice that ϕ and χ will induce a mapping

$$\chi\phi : T \to A_1 \times R \times U \times V.$$

Restricted by $\chi\phi$, Player 3 then uniformly choose a bijection (a permutation)

$$\pi : T \to Y$$

such that

$$\chi\pi(t) = \chi\phi(t),$$

for all $t \in T$.

臺灣大學學術期刊資料庫

- **Step 1**: Player 1 and Player 2 get their lists of messages in this step. There are $|T|$ steps. For each t-step, $t \in T$, Player 1 sends the set of authenticated messages $M(\chi\phi)$ to Player 3. After that, Player 3 forwards the message $[m]_{\pi(t)}$ to Player 2. ($[m]_{\pi(t)}$ is Player 1's authenticated message indexed by $\pi(t)$.)

  After $|T|$ steps, Player 1 should get a list of

$$l_1^* = (\chi\phi(t))_t;$$

  Player 2 gets a list of

$$l_2^* = \left(\left[a_2, a_3, \theta\left(u\middle|a_3\right), \pi(t)\right]\right)_t.$$

- **Step 2**: Player 1 and Player 2 get their recommended actions in this step. Player 1 and Player 2 jointly and uniformly choose a $t^* \in T$. Player 1 knows

$$\chi\phi\left(t^*\right) = \left(a_1^{t^*}, r^{t^*}, u^{t^*}, v^{t^*}\right);$$

  Player 2 knows

$$[m]_{y^{t^*}} = \left[a_2^{t^*}, a_3^{t^*}, \theta\left(u^{t^*}\middle|a_3^{t^*}\right), y^{t^*}\right].$$

- **Step 3** Player 3 gets his recommended action in this step. Player 2 reports

$$m^{23} = \left(a_3^{t^*}, \theta\left(u^{t^*}\middle|a_3^{t^*}\right)\right)$$

  to Player 3; Player 1 reports

$$m^{13} = \left(r^{t^*}, u^{t^*}, v^{t^*}\right)$$

  to Player 3.

- **Deviation-Detection (Step 4)** This step is the deviation-detection procedure. Two kinds of deviations might be made in **Step 3**: Player 1 misreports m^{13} or Player 2 misreports m^{23}.

  1. Suppose Player 2 reports (a_3', u'), which might be different from m^{23}. This deviation is detected if $u' \neq \theta(u^{t^*}|a_3')$.

臺灣大學學術期刊資料庫

2. Next, suppose Player 1 reports (r', u', v'), which might be different from m[13]. First, define

$$T(r, u, v) \equiv \{t \in T | \chi\phi(t) = (a_1, r, u, v) \text{ for some } a_1\}.$$

Player 3 randomly chooses an element $\tilde{v} \in V$ with probability $1/|V|$. Player 3 then constructs the set $T(u', v', \tilde{v})$ defined by

$$T\left(u', v', \tilde{v}\right) \equiv T\left(r', u', v'\right) \cup T\left(r \neq r', u', \tilde{v}\right) \quad (3)$$

where

$$T\left(r \neq r', u', v'\right) = \bigcup_{r \neq r'} T\left(r, u', v'\right).$$

Player 3 then reports $T(u', v', \tilde{v})$ to Player 2. Since Player 2 knows t^*, whenever $t^* \notin T(u', v', \tilde{v})$, Player 1's deviation is detected.

If Player i's deviation is detected by Player j in the above steps, both Player i (the player who deviates) and Player j (the player who detects it) send the message **STOP** to all other players; otherwise, both of them send the message **OK** to all other players.

- **Step 5** The protocol ends. Players' recommended actions are determined as follows.
  - Player 1's recommended action is $a_1^{t^*}$.
  - Player 2's recommended action is $a_2^{t^*}$.
  - Player 3's recommended action is $a_3^{t^*} + r^{t^*} (\text{mod} |A_3|)$.

I proceed to prove Theorem 1.

A.1.2 Deviation Detection

In the following lemma, I show that the unilateral deviation can be detected with a probability larger than or equal to $\min\{1 - 1/|U|, 1 - 1/|V|\}$. The proof is the same as the proof for Proposition 3.1.

Lemma A.1. The unilateral deviation can be detected with a probability larger than or equal to $\min\{1 - 1/|U|, 1 - 1/|V|\}$.

proof. The proof is the same as the proof for Proposition 3.1 except for now U and V can be made arbitrarily large. □

臺灣大學學術期刊資料庫

A.1.3 Conditional Probabilities

In the next three subsections, I will show that if players are on the equilibrium path, every player's conditional probability over other players' recommended actions conditional on his own recommended action is the same as that induced by q.

In **Step 5**, Player 1 has observed $(a_1^{t^*}, r^{t^*}, u^{t^*}, v^{t^*})$; Player 2 has observed an authenticated message $[m]_{y^*} = [a_2^{t^*}, a_3^{t^*}, \theta(u^{t^*}|a_3^{t^*}), y^{t^*}]$ and a subset of steps $T(u^{t^*}, v^{t^*}, \tilde{v})$ from Player 3; and Player 3 has observed $a_3^{t^*}$ and $(r^{t^*}, u^{t^*}, v^{t^*})$. Let

$$\Pr\left(a^{t^*}, r^{t^*}, u^{t^*}, v^{t^*}, a_2^{t^*}, a_3^{t^*}, \theta\left(u^{t^*}\middle|a_3^{t^*}\right), y^{t^*}, T\left(u^{t^*}, v^{t^*}, \tilde{v}\right)\right)$$

be the joint probability of these random variables generated by the protocol.

To begin with, recall that Player 1's recommended action is $a_1^{t^*}$, Player 2's is $a_2^{t^*}$, and Player 3's is $a_3^{t^*} + r^{t^*} (\mathrm{mod}|A_3|)$. I first check Player 2's conditional probability, and then Player 1's and then Player 3's.

Player 2's conditional probabilities over players' recommended actions

Lemma A.2. On the equilibrium path, the conditional probability over Player 1 and Player 3's recommended action profile (a_1, a_3) conditional on Player 2's recommended action a_2 is $q(a_1, a_3|a_2)$.

proof. Recall that Player 2 has observed $[m]_{y^{t^*}} = [a_2^{t^*}, a_3^{t^*}, \theta(u^{t^*}|a_3^{t^*}), y^{t^*}]$ and $T(u^{t^*}, v^{t^*}, \tilde{v})$. On the equilibrium path, by definition of $T(u^{t^*}, v^{t^*}, \tilde{v})$ (in (3)),

$$T\left(u^{t^*}, v^{t^*}, \tilde{v}\right) \equiv T\left(r^{t^*}, u^{t^*}, v^{t^*}\right) \cup T\left(r \neq r^{t^*}, u^{t^*}, \tilde{v}\right), \qquad (4)$$

where

$$T\left(r \neq r^{t^*}, u^{t^*}, \tilde{v}\right) = \bigcup_{r \neq r^{t^*}} T\left(r, u^{t^*}, \tilde{v}\right).$$

From $T(u^{t^*}, v^{t^*}, \tilde{v})$, Player 2 knows that $[m]_{y^{t^*}}$ is either chosen from $M(a_1, r^{t^*}, u^{t^*}, v^{t^*})$ for some a_1 or $M(a_1, r', u^{t^*}, \tilde{v})$ for some a_1 and some $r' \neq r^{t^*}$. Further recall that the authenticated messages are randomly and uniformly

臺灣大學學術期刊資料庫

indexed. Thus, $[m]_{y^{t^*}}$ can be only chosen from the set $\overline{M}$, where

$$\overline{M} = \bigcup_{a_1' \in A_1} \bigcup_{(r',v') \in \overline{R \times V}} \left\{ \left[\bar{a}_2, \bar{a}_3, \theta\left(u^{t^*} \middle| \bar{a}_3\right), \bar{y} \right] \in M\left(a_1', r', u^{t^*}, v'\right) \middle| \bar{a}_2 = a_2^{t^*}, \bar{a}_3 = a_3^{t^*} \right\},$$

in which

$$\overline{R \times V} = \left\{ \left(r^{t^*}, v^{t^*}\right) \right\} \cup \left(\left(R \setminus \left\{ r^{t^*} \right\} \right) \times \{\tilde{v}\} \right).$$

Since $(M(a_1, r, u, v))_{(a_1,r,u,v)}$ is a partition of authenticated messages, the total number of messages in $\overline{M}$ is

$$|\overline{M}| = \sum_{a_1' \in A_1} \sum_{(r',v') \in \overline{R \times V}} \left\{ \left[\bar{a}_2, \bar{a}_3, \theta\left(u^{t^*} \middle| \bar{a}_3\right), \bar{y} \right] \in M\left(a_1', r', u^{t^*}, v'\right) \middle| \bar{a}_2 = a_2^{t^*}, \bar{a}_3 = a_3^{t^*} \right\}.$$

By **Step 5** in the protocol, recall that Player 2's recommended action is $a_2^{t^*}$, while Player 1's is $a_1^{t^*}$ and Player 3's is $a_3^{t^*} + r^{t^*} (\mathrm{mod} |A_3|)$. Thus, conditional on Player 2's recommended action, the conditional probability over Player 1 and Player 3's recommended action profile $(a_1^{t^*}, a_3^{t^*} + r^{t^*} (\mathrm{mod}\ |A_3|))$ is just

$$\Pr\left(a_1^{t^*}, a_3^{t^*} + r^{t^*} \left(\mathrm{mod} \middle| A_3 \middle|\right) \middle| a_2^{t^*}, a_3^{t^*}, \theta\left(u^{t^*} \middle| a_3^{t^*}\right), y^{t^*}, T\left(u^{t^*}, v^{t^*}, \tilde{v}\right)\right) \tag{5}$$

$$= \frac{\left| \left\{ \left[\bar{a}_2, \bar{a}_3, \theta\left(u^{t^*} \middle| \bar{a}_3\right), \bar{y} \right] \in M\left(a_1^{t^*}, r^{t^*}, u^{t^*}, v^{t^*}\right) \middle| \bar{a}_2 = a_2^{t^*}, \bar{a}_3 = a_3^{t^*} \right\} \right|}{\left|\overline{M}\right|} \tag{6}$$

$$= \frac{\left| \left\{ \left[\bar{a}_2, \bar{a}_3, \bar{u}, \bar{y} \right] \in M\left(a_1^{t^*}, r^{t^*}, u^{t^*}, v^{t^*}\right) \middle| \bar{a}_2 = a_2^{t^*}, \bar{a}_3 = a_3^{t^*} \right\} \right|}{\left|\overline{M}\right|} \tag{7}$$

$$= \frac{q\left(a_1^{t^*}, a_2^{t^*}, a_3^{t*} + r^{t^*} \left(\mathrm{mod} \middle| A_3 \middle|\right)\right)}{q\left(a_2^{t^*}\right)} \tag{8}$$

$$= q\left(a_1^{t^*}, a_3^{t^*} + r^{t^*} \left(\mathrm{mod} \middle| A_3 \middle|\right) \middle| a_2^{t^*}\right). \tag{9}$$

The proof is done. □

臺灣大學學術期刊資料庫

Player 1's conditional probabilities over players' recommended actions

Lemma A.3. On the equilibrium path, the conditional probability over Player 2 and Player 3's recommended action profile (a_2, a_3) conditional on Player 1's recommended action a_1 is $q(a_2, a_3|a_1)$.

proof. Player 1 has observed $(a_1^{t^*}, r^{t^*}, u^{t^*}, v^{t^*})$. Therefore,

$$\begin{aligned}
&\Pr\left(a_2^{t^*}, a_3^{t^*} + r^{t^*} \left(\mathrm{mod}|A_3|\right) \middle| a_1^{t^*}, r^{t^*}, u^{t^*}, v^{t^*}\right) && (10)\\
&= \left\{\left|\left\{\left[\bar{a}_2, \bar{a}_3, \theta\left(u^{t^*}\middle|\bar{a}_3\right), \bar{y}\right] \in M\left(a_1^{t^*}, r^{t^*}, u^{t^*}, v^{t^*}\right)\middle|\bar{a}_2\right.\right.\\
&\quad \left.\left. = a_2^{t^*}, \bar{a}_3 = a_3^{t^*}\right\}\right| \Big/ \left\{\left|M\left(a_1^{t^*}, r^{t^*}, u^{t^*}, v^{t^*}\right)\right|\right\} && (11)\\
&= q\left(a_2^{t^*}, a_3^{t^*} + r^{t^*} \left(\mathrm{mod}|A_3|\right) \middle| a_1^{t^*}\right). && (12)
\end{aligned}$$

□

Player 3's conditional probabilities over players' recommended actions

Lemma A.4. On the equilibrium path, the conditional probability over Player 1 and Player 2's recommended action profile (a_1, a_2) conditional on Player 3's recommended action a_3 is $q(a_1, a_2|a_3)$.

proof. Player 3 has observed $a_3^{t^*}$ and $(r^{t^*}, u^{t^*}, v^{t^*})$. Therefore,

$$\begin{aligned}
&\Pr\left(a_1^{t^*}, a_2^{t^*} \middle| a_3^{t^*}, r^{t^*}, u^{t^*}, v^{t^*}\right) && (13)\\
&= \left\{\left|\left\{\left[a_2^{t^*}, \bar{a}_3, \theta\left(u^{t^*}\middle|\bar{a}_3\right), \bar{y}\right] \in M\left(a_1^{t^*}, r^{t^*}, u^{t^*}, v^{t^*}\right)\middle|\right.\right.\\
&\quad \left.\left.\bar{a}_3 = a_3^{t^*}\right\}\right| \Big/ \left\{\sum_{a_1' \in A_1} \left|\left\{\left[a_2^{t^*}, \bar{a}_3, \theta\left(u^{t^*}\middle|\bar{a}_3\right), \bar{y}\right]\right.\right.\\
&\quad \left.\left. \in M\left(a_1', r^{t^*}, u^{t^*}, v^{t^*}\right)\middle|\bar{a}_3 = a_3^{t^*}\right\}\right|\right\} && (14)\\
&= q\left(a_1^{t^*}, a_2^{t^*} \middle| a_3^{t^*} + r^{t^*} \left(\mathrm{mod}|A_3|\right)\right). && (15)
\end{aligned}$$

□

A.1.4 Summary

Now I can prove Theorem 1. Denote α as a point in the convex hull of NE in G. Let q be a c.e.d. in G, which has rational coefficients and gives each player a strictly higher payoff than α does.

臺灣大學學術期刊資料庫

If q is a point in the convex hull of NE, all players play q after the protocol the following way. Let Player 1 and Player 2 publicly perform a j.c.l. that generates q. Afterwards, players play q.

If q is outside the convex hull of NE, there is a η_i such that $u_i(q) > \eta_i u_i(\alpha) + (1-\eta_i)u_i(\beta)$, where $u_i(q)$, $u_i(\alpha)$, $u_i(\beta)$ are respectively player i's expected payoff in q, in α, and the maximum expected payoff. Then take

$$\eta^* = \arg \max_{i:u_i(q)>u_i(\alpha)} \{\eta_i | u_i(q) > \eta_i u_i(\alpha) + (1-\eta_i)\, u_i(\beta)\},$$

and V and U so that

$$\min\{1 - 1/|U|, 1 - 1/|V|\} = \eta^*.$$

If there is no deviation, players play their recommended actions generated by the protocol. If deviations are detected, players play α after the protocol the following way. Let Player 1 and Player 2 publicly perform a j.c.l. that generates α. Players then play the NE according to α. Players' deviations are then deterred by the construction of U and V.

If players are on the equilibrium path, each player's conditional probability conditional on his recommended action over others' is the same as that induced by q as shown by Lemma A.2, Lemma A.3, and Lemma A.4. I have proved Theorem 1. □

References

Aumann, Robert J. (1974), "Subjectivity and Correlation in Randomized Strategies," *Journal of Mathematical Economics*, 1(1), 67–96.

Aumann, Robert J. and Michael Maschler (1995), *Repeated Games With Incomplete Information*, Cambridge, MA: MIT Press.

Bárány, Imre (1992), "Fair Distribution Protocols or How The Players Replace Fortune," *Mathematics of Operations Research*, 17, 327–340.

Ben-Or, Michael and Avi Wigderson (1988), "Completeness Theorems for Non-cryptographic Fault-tolerant Distributed Computation," in *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, New York: ACM Press, 1–10.

Ben-Porath, Elchanan (1998), "Correlation without Mediation: Expanding the Set of Equilibrium Outcomes by 'Cheap' Pre-play Procedures," *Journal of Economic Theory*, 80(1), 108–122.

臺灣大學學術期刊資料庫

——— (2003), "Cheap Talk in Games with Incomplete Information," *Journal of Economic Theory*, 108(1), 45–71.

Dodis, Yevgeniy, Shai Halevi, and Tal Rabin (2000), "A Cryptographic Solution to a Game Theoretic Problem," in *Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology*, London: Springer-Verlag, 112–130.

Forges, Francoise (1990), "Universal Mechanisms," *Econometrica*, 58(6), 1341–1364.

Forges, Françoise (1986), "An Approach to Communication Equilibria," *Econometrica*, 54(6), 1375–1385.

——— (2009), "Correlated Equilibria and Communication in Games," in Robert A. Meyers (ed.), *Encyclopedia of Complexity and Systems Science*, New York: Springer New York, 1587–1596.

Gerardi, Dino (2004), "Unmediated Communication in Games with Complete and Incomplete Information," *Journal of Economic Theory*, 114(1), 104–131.

Gossner, Olivier and Nicolas Vieille (2001), "Repeated Communication through The Mechanism And," *International Journal of Game Theory*, 30(1), 41–60.

Heller, Yuval (2010), "Minority-proof Cheap-talk Protocol," *Games and Economic Behavior*, 69(2), 394–400.

Heller, Yuval, Eilon Solan, and Tristan Tomala (2012), "Communication, Correlation and Cheap-talk in Games with Public Information," *Games and Economic Behavior*, 74(1), 222–234.

Lehrer, Ehud (1996), "Mediated Talk," *International Journal of Game Theory*, 25(2), 177–188.

Lehrer, Ehud and Sylvain Sorin (1997), "One-shot Public Mediated Talk," *Games and Economic Behavior*, 20(2), 131–148.

Myerson, Roger B. (2004), *Game Theory*, Cambridge, MA: Harvard University Press.

Shamir, Adi (1979), "How to Share A Secret," *Communications of the ACM*, 22(11), 612–613.

Teague, Vanessa (2008), "Problems With Coordination in Two-Player Games: Comment on "Computational Complexity and Communication"," *Econometrica*, 76(6), 1559–1564.

Urbano, Amparo and Jose E. Vila (2002), "Computational Complexity and Communication: Coordination in Two-Player Games," *Econometrica*, 70(5), 1893–1927.

臺灣大學學術期刊資料庫

Vida, Péter and Helmuts Āzacis (2013), "A Detail-free Mediator," *Games and Economic Behavior*, 81, 101–115.

Vijay Krishna, R. (2007), "Communication in Games of Incomplete Information: Two Players," *Journal of Economic Theory*, 132(1), 584–592.

投稿日期: 2022年3月17日, 接受日期: 2022年5月23日

關聯性與訊息轉傳

陳俊廷

台北大學經濟系

我考慮三人完全資訊賽局的賽前溝通。賽前溝通可以讓玩家們在賽局開始前, 與其他玩家互相傳遞私有訊息。當玩家可以轉傳訊息並驗證訊息時, 我證明關聯性均衡可以被賽前溝通實現。可驗證的訊息, 比如簽了名的信件, 可以被傳遞但不能被僞造。當訊息可以被驗證時, 我證明: 如果一個賽局具有在其 Nash 均衡凸包上的點 α, 那麼, 對於任何一個此賽局的關聯性均衡, 若其係數皆爲有理數且給予任何玩家嚴格大於在 α 下的報酬, 此關聯性均衡就可以被賽前溝通實現。此文章所提出的賽前溝通過程, 不需要可以將訊息完美記錄的物件 (Bárány, 1992), 且在溝通過程中的任何階段, 玩家的私有訊息都不會被公開。

關鍵詞: 賽前溝通, 關聯性均衡, 轉傳

JEL 分類代號: C72, D83

臺灣大學學術期刊資料庫