JOURNAL OF ECONOMIC THEORY **83**, 69–89 (1998)
ARTICLE NO. ET982444

Secure Protocols or How Communication Generates Correlation

Olivier Gossner*

CORE, Voie du Roman Pays 34, B-1348 Louvain-la-Neuve, Belgium
gossner@core.ucl.ac.be

Received November 19, 1996; revised May 1, 1998

Correlated equilibria and communication equilibria are useful notions to understand the strategic effects of information and communication. Between these two models, a protocol generates information through communication. We define a secure protocol as a protocol from which no individual may have strategic incentives to deviate and characterize these protocols. *Journal of Economic Literature* Classification Numbers: 072. © 1998 Academic Press

1. INTRODUCTION

A series of papers ([2, 4, 5, 8, 9, 11, 12, 17, 18, 21] is not an exhaustive list) shows how a group of players can generate shared information through communication by the use of a communication protocol. The main advantage of such a protocol is to replace the central mediator of Aumann's [1] model of correlated equilibrium by a decentralized procedure in which the players themselves generate the corresponding information.

While doing so, one also introduces possibilities for players to cheat during that procedure. Therefore, the authors generally prove that their protocols fulfill some properties that make them intuitively immune against player's deviations. Nevertheless, different papers use different conditions, and it is not obvious which set of conditions should be used instead of another. The aim of this paper is to introduce a strategic definition of a secure protocol.

A communication mechanism (see [10, 20]) is a technology used by the players to communicate. It can be seen as a device to which players send messages and which sends them back private, stochastically drawn signals (public messages or deterministic signals are particular cases). In a jointly

* Part of this work was done at Universitat Pompeu Fabra in Barcelona with financial support of H.C.M. grant number ERB CHBGCT 93 0462. The author thanks Françoise Forges, Sylvain Sorin, and Nicolas Vieille for stimulating discussions and enriching comments. Insightful comments from an associate editor and a referee are gratefully acknowledged.

0022-0531/98 $25.00

controlled lottery [3], players repeatedly announce simultaneous public messages. In polite talk [2], players send public messages one after the other. Bárány [4] and Forges [11] make the assumption that players communicate through private phone lines.

In Aumann's [1] model of correlated equilibrium and in Forge's [10] model of communication equilibrium, information structures and communication mechanisms define preplay phases that take place before a game is played.[1] Given a strategic form game G and an information structure $\mathscr{I}$, the game G extended by $\mathscr{I}$ is defined as the extended game in which players get information from $\mathscr{I}$, then play in G. Similarly, if $\mathscr{C}$ is a communication mechanism, G extended by $\mathscr{C}$ is the game in which players first communicate through $\mathscr{C}$, then play in G.

A protocol P consists of two phases. First, players communicate. During that phase players send messages to the communication mechanism $\mathscr{C}$ (communication can be sequential, in this case a message represents a "strategy" used to communicate). In return, $\mathscr{C}$ sends back signals to the players. Second, each player computes from his signal a translated (or new) signal, that corresponds to his relevant information after communication. The distribution of the interpreted signals is summarized in an information structure $\mathscr{I}(P)$ called the information structure generated by the protocol.

Imagine that players rely on P in order to play in a game G. Some players may have incentives to change their messages or to compute their translated signal differently in order to get a better payoff in G. To define such incentives, we compare Nash equilibria of G extended by $\mathscr{C}$ with Nash equilibria of G extended by $\mathscr{I}(P)$. More precisely, we say that P is a secure protocol when for every game G and all Nash equilibrium f of G extended by $\mathscr{I}(P)$, the following procedure is Nash equilibrium of G extended by $\mathscr{C}$:

- Follow the protocol, therefore generating signals that could have been issued by $\mathscr{I}(P)$;
- Play in G according to f (as if the obtained signals had been sent by $\mathscr{I}(P)$).

The definition of a secure protocol allows to study games and their communication possibilities separately. For a fixed G, the revelation principle (see Myerson [19]) characterizes all distributions on the actions of G that can be implemented by Nash equilibria of $\Gamma(\mathscr{C}, G)$ when $\mathscr{C}$ varies. Here, we instead fix $\mathscr{C}$ and study the protocols P which are self-enforcing for all G. Because they do not depend on G, secure protocols are "Universal" in the sense of Forges [11].

[1] We do not consider extensive form correlated equilibria or extensive form communication equilibria. For the general model, see Forges [10, 11].

We obtain different characterizations of secure protocols. Mainly, we prove that a protocol is secure if and only if two conditions are fulfilled:

- No player can change the distribution of the translated signals of other players by changing his messages;
- No player can gain information about the translated signals of the others, either by considering his original signal instead of his translated one, or by changing his messages.

Intuitively, if a player can affect the distribution of translated signals of the others, he can also change the distribution of their actions in some game played after $\mathscr{C}$ and can get a better payoff from this. Also, if no player can change the distribution of translated signals of the others, one may still gain if it is possible to obtain more information on these. In common words, a protocol is secure when no player has the possibility either to mislead other players, or to spy their private information.

Our characterization allows to check which protocols proposed in the literature are secure, and which are not. Bárány [4] shows that if there are at least 4 players communicating through “phone lines,” then any information structure with rational coefficients can be generated. The protocols used are not secure, since it has to be assumed that all the messages are recorded by the mechanism and can be checked later. Lehrer [17] and Lehrer and Sorin [18] prove that for any information structure $\mathscr{I}$ with rational coefficients, there exists a mechanism and a protocol for that mechanism that generates $\mathscr{I}$. The mechanisms considered are public (each player knows his message and a public signal) and deterministic (the signals depend deterministically on the messages), and the properties obtained on these protocols imply that they are secure. Using tools from modern cryptography, Urbano and Vila [21] exhibit secure protocols with public communication and two players. Their protocols are secure under some assumptions of bounded rationality.

In a repeated game with imperfect monitoring, each player is partially informed about the past actions of the others. Lehrer [16] shows how players may use the signals of the game as a communication mechanism in order to correlate (see also Tomala [22]). Gossner [14] for protocols in finite time and Gossner and Vieille [15] for protocols in infinite time prove that Lehrer’s [16] internal correlation protocols are not secure. Still, these protocols are successfully used to build equilibria in repeated games because they are “statistically secure”: any profitable deviation is detectable in the long run.

We introduce the notations and the main definitions in Section 2. The characterization of secure protocols is presented in Section 3, and some examples are studied in Section 4. Sections 5, 6, and 7 are devoted to the proof of the main result. In Section 8, we simplify this characterization using Blackwell's reduction to standard experiments. In Section 9, we study the relationship between translations and interpretations (as introduced in [13]). To keep notations simple, the definition and the characterizations of secure protocols are fist given for games with complete information. The extension to the general case of incomplete information is presented with other extensions in Section 10. We finally conclude in Section 11.

2. THE MODEL

2.1. *Basic Definitions*

I is the finite set of players. A *compact game* $G=((S^i)_i, g)$ is given by a compact set of strategies S^i for each player i and by a continuous payoff function $g\colon S \to \mathbb{R}^I$. The set of mixed strategies for player i is $\Sigma^i = \Delta(S^i)$, and g is extended to Σ by $g(\sigma)=\mathbf{E}_\sigma g(s)$. (We write S and Σ for $\prod_i S^i$ and $\prod_i \Sigma^i$, S^{-i} and Σ^{-i} for $\prod_{j\neq i} S^j$ and $\prod_{j\neq i} \Sigma^j$, and we shall use similar notations whenever convenient.)

An *information structure* $\mathscr{I}=((X^i)_i, \mu)$ is given by a finite set of signals X^i for each i and by a probability measure μ over X. When x is drawn according to μ, player i is informed about the coordinate x^i.

A *communication mechanism* is a triple $\mathscr{C}=((T^i)_i, (Y^i)_i, l)$, where T^i is i's finite set of messages, Y^i is i's finite set of signals, and $l\colon T \to \Delta(Y)$ is the signal function. When t is the profile of messages sent by the players, $y \in Y$ is drawn according to $l(t)$ and player i is informed of y^i. $\mathscr{T}^i = \Delta(T^i)$ represents the set of mixed messages for player i and l is extended to $\mathscr{T}$ by $l(\tau)(y) = \mathbf{E}_\tau l(t)(y)$.

2.2. *Extended Games*

Games extended by information structures were first defined by Aumann [1].

Definition 2.1. Given a compact game G and an information structure $\mathscr{I}$, $\Gamma(\mathscr{I}, G)$ is the game G *extended by* $\mathscr{I}$ that unfolds as follows:

- $x \in X$ is drawn according to μ, each player i is informed about x^i;
- each player i chooses $\sigma^i \in \Sigma^i$ according to x^i;
- the vector payoff is $g(\sigma)$.

A strategy for player i is a mapping $f^i\colon X^i \to \Sigma^i$, and the payoff function of $\Gamma(\mathscr{I}, G)$ is given by $g_{\mathscr{I}}(f) = \mathbf{E}_\mu g(f(x))$. See Fig. 1.

$$\begin{tikzcd} \mathscr{I} \arrow[r, "x^i"] & i \arrow[r, "f^i(x^i)"] & G \end{tikzcd}$$

FIG. 1. The extended game $\Gamma(\mathscr{I}, G)$.

$$\begin{tikzcd}
\mathscr{C} \arrow[r, "y^i"] & i \arrow[r, "F^i(y^i)"] \arrow[l, bend left, "t^i"] & G
\end{tikzcd}$$

FIG. 2. The extended game $\Gamma(\mathscr{C}, G)$.

A game extended by a communication mechanism is defined similarly (see Forges [10]):

Definition 2.2. Given a compact game G and a communication mechanism $\mathscr{C}$, $\Gamma(\mathscr{C}, G)$ is the game G *extended by* $\mathscr{C}$ that unfolds as follows:

- each player i sends a message t^i to the mechanism;
- $y \in Y$ is drawn according to $l(t)$ and each player i is informed of y^i;
- each player i chooses $\sigma^i \in \Sigma^i$ according to y^i;
- the vector payoff is $g(\sigma)$.

A strategy for player i is given by a mixed message $\tau^i \in \mathscr{T}^i$ and by a mapping F^i: $Y^i \to \Sigma^i$. The payoff function writes $g_{\mathscr{C}}(\tau, F) = \mathbf{E}_{l(\tau)}\, g(F(y))$. See Fig. 2.

In Section 10.1, we examine the model in which σ^i is chosen according to y^i and to t^i.

2.3. *Protocols and Secure Protocols*

Lehrer [16] introduced protocols to generate an information structure through a communication mechanism. We formally define a protocol by:

Definition 2.3. For a given mechanism $\mathscr{C}$:

- A *translation* is a family $\phi = (\phi^i)_i$ of mappings ϕ^i from Y^i to the set of probability measures $\Delta(X^i)$ over a finite set X^i.
- A *protocol* (or $\mathscr{C}$*-protocol*) (τ, ϕ) is given by $\tau \in \mathscr{T}$ and by a translation ϕ.

Using the protocol (τ, ϕ), player i first sends a message t^i drawn according to τ^i to the mechanism. Then, if y^i is the signal received from $\mathscr{C}$, i computes the translated signal x^i with probability $\phi^i(y^i)(x^i)$. See Fig. 3. Note that a translation ϕ defines an application from Y to $\Delta(X)$ and that $\phi^{-i} = (\phi^j)_{j \neq i}$ defines an application from Y^{-i} to $\Delta(X^{-i})$ for every i.

$$\begin{tikzcd}
\mathscr{C} \arrow[r, "y^i"] & i \arrow[r, "x^i"] \arrow[l, bend left, "t^i"] & \mathscr{I}
\end{tikzcd}$$

FIG. 3. The protocol (τ, ϕ).

$$\begin{tikzcd}
\mathscr{C} \arrow[r, "y^i"] & i \arrow[rr, "F^i(y^i)"] \arrow[dr, "x^i"'] \arrow[l, bend left=60, "t^i"] & & G \\
& & i \arrow[ur, "f^i(x^i)"'] & \\
& & \mathscr{I} \arrow[u, "x^i"] &
\end{tikzcd}$$

FIG. 4. Construction of strategies in $\Gamma(\mathscr{C}, G)$ from strategies in $\Gamma(\mathscr{I}, G)$ and (τ, ϕ).

Definition 2.4. A protocol (τ, ϕ) *generates* the information structure $\mathscr{I} = (X, \mu)$ defined by the spaces of signals $(X^i)_i$ and by the probability μ image of $l(\tau)$ by ϕ. Explicitly, we have $\mu(x) = \mathbf{E}_{l(\tau)}\phi(y)(x)$.

From the protocol (τ, ϕ) generating $\mathscr{I}$ and from a strategy f^i in $\Gamma(\mathscr{I}, G)$, there exists a natural way to define a strategy in $\Gamma(\mathscr{C}, G)$. Let $(\tau^i, (f \circ \phi)^i)$ be the strategy that corresponds to:

- send messages to the mechanism according to τ^i;
- draw a translated signal x^i according to $\phi^i(y^i)$ when y^i is the signal received from the mechanism;
- play $f^i(x^i)$ in G (as if x^i had been sent by $\mathscr{I}$).

Formally, $(f \circ \phi)^i$ is given by the formula $(f \circ \phi)^i\,(y^i)(\mathscr{S}^i) = \mathbf{E}_{\phi^i(y^i)}\, f^i(x^i)(\mathscr{S}^i)$ for $\mathscr{S}^i$ Borelian of S^i. See Fig. 4.

Definition 2.5. Given a game G, a $\mathscr{C}$-protocol (τ, ϕ) generating an information structure $\mathscr{I}$ is *secure for* G if for every Nash equilibrium f of $\Gamma(\mathscr{I}, G)$, $(\tau, f \circ \phi)$ is a Nash equilibrium of $\Gamma(\mathscr{C}, G)$. (τ, ϕ) is *secure* when it is secure for every compact game G.

From now on, (τ, ϕ) represents a $\mathscr{C}$-protocol generating the information structure $\mathscr{I} = ((X^i)_i, \mu)$.

3. CHARACTERIZATION OF SECURE PROTOCOLS

Our main result is that a protocol (τ, ϕ) is secure if and only if:

- No player i may change the distribution of translated signals of other players by changing the distribution of his messages;
- No player may gain information on the translated signal of other players either:
  - — by changing the distribution of his messages;
  - — by considering his original signal y^i instead of his translated one x^i.

To formalize this, we need a few more notations:

When (τ'^i, τ^{-i}) is the profile of mixed messages, $l(\tau'^i, \tau^{-i})$ and ϕ induce some probability $P_{(\tau'^i, \tau^{-i})}$ on $Y \times X$. Namely, $P_{(\tau'^i, \tau^{-i})}(y, x) = l(\tau'^i, \tau^{-i})(y)\, \phi(y)(x)$.

Let $m(\tau'^i) \in \Delta(X^{-i})$ denote the marginal of $P_{(\tau'^i, \tau^{-i})}$ on X^{-i}. $m(\tau'^i)$ is the probability over players other than i's translated signals when they follow the protocol (τ, ϕ) and when i's messages are distributed according to τ'^i. Precisely we have $m(\tau'^i)(x^{-i}) = \mathbf{E}_{l(\tau'^i, \tau^{-i})} \phi^{-i}(y^{-i})(x^{-i})$. In particular, $m(\tau^i)$ is the marginal of μ on X^{-i}.

To compare different informations of a player on other's signals, we use the comparison of statistical experiments due to Blackwell [6, 7]. For a reminder on these, see Appendix A. We just recall here that the notation $\alpha \supset \beta$ means that the statistical experiment α is more informative than β.

The statistical experiment that characterizes the information given by y^i about x^{-i} when players $j \neq i$ follow the protocol (τ, ϕ) and when i's messages are distributed according to τ'^i writes $\gamma_{\tau'^i} = (w_{x^{-i}})_{x^{-i},\, P_{(\tau'^i, \tau^{-i})}(x^{-i}) > 0}$, with $w_{x^{-i}}(y^i) = P_{(\tau'^i, \tau^{-i})}(y^i \mid x^{-i})$.

On the other hand, the statistical experiment that characterizes the information given by x^i about x^{-i} when (τ, ϕ) is followed by all the players is $\alpha^i = (u_{x^{-i}})_{x^{-i},\, \mu(x^{-i}) > 0}$, with $u_{x^{-i}}(x^i) = \mu(x^i \mid x^{-i})$. Equivalently, α^i characterizes the information of i given by x^i about x^{-i} when x is the profile of signals sent by $\mathscr{I}$.

We are now ready to state our main result:

Theorem 3.1. *(τ, ϕ) is secure if and only if:*

(1) *For every player i and $\tau'^i \in \mathscr{T}^i$, $m(\tau'^i) = m(\tau^i)$.*

(2) *For every player i and $\tau'^i \in \mathscr{T}^i$, $\alpha^i \supset \gamma_{\tau'^i}$.*

Examples of secure and non-secure protocols are presented in next section.

To prove Theorem 3.1, we first provide in Section 5 a useful characterization of secure protocols. Then we prove in Section 6 that (1) holds when (τ, ϕ) is secure. Finally, in Section 7 we show that under (1), (τ, ϕ) is secure if and only if (2) holds.

4. EXAMPLES

Example 4.1. Consider the mechanism $\mathscr{C}$ (Example 2 of [18]) in which the sets of messages are $\{T, M, B\}$ for player 1 and $\{l, m, r\}$ for player 2. Each player receives as signal his message and a public signal defined by the matrix:

$$\begin{array}{cccc} & l & m & r \\ T & a & b & a \\ M & b & b & c \\ B & a & c & c \end{array}$$

A $\mathscr{C}$-protocol (τ, ϕ) is defined by $\tau = ((1/3)\,T + (1/3)\,M + (1/3)B,\ (1/3)\,l + (1/3)\,m + (1/3)\,r)$ and by:

$$\phi^1: \quad \left|\begin{array}{l}(T, a)\\(M, b) \to T\\(B, c)\end{array}\right. \qquad \left|\begin{array}{l}(T, b)\\(M, c) \to B\\(B, a)\end{array}\right.$$

$$\phi^2: \quad \left|\begin{array}{l}(l, a)\\(m, b) \to L\\(r, c)\end{array}\right. \qquad \left|\begin{array}{l}(l, b)\\(m, c) \to R.\\(t, a)\end{array}\right.$$

(τ, ϕ) generates the information structure $\mathscr{I}$ represented by:

	L	R
T	1/3	1/3
B	1/3	0

Lines are signals to player 1, columns are signals to player 2, and the corresponding entry is the probability of the signals profile.

Now consider the following games:

	L	R
T	6, 6	2, 7
B	7, 2	0, 0

G_1

	L	R
T	6, 6	6, 7
B	6, 2	0, 0

G_2

G_1 is known as the game of Chicken, and G_2 is a modified version of G_1. Both G_1 and G_2 possess the correlated equilibrium distribution $1/3(T, L) + 1/3(T, R) + 1/3(B, L)$.

One can check directly that following the $\mathscr{C}$-protocol (τ, ϕ), then playing in G_1 or G_2 according to the translated signals ($T \to T$, $B \to B$, $L \to L$, $R \to R$) constitute Nash equilibria of $\Gamma(\mathscr{C}, G_1)$ and of $\Gamma(\mathscr{C}, G_2)$.

One can also see that, by a property of circular permutation over signals and over translations, neither the probability over player 2's translated signals, nor player 1's information about player 2's translated signals, depend on the message of player 1. A symmetric property also holds for player 2. Therefore, Theorem 3.1 implies that (τ, ϕ) is secure.

Example 4.2. We now consider the communication mechanism $\mathscr{C}'$ constructed from $\mathscr{C}$ in which 1 has another message U. If 1 sends U, his signal reveals 2's message and 2 distinguishes U from T, M, and B. In $\mathscr{C}'$, each player receives as signal his message and a public signal given by:

$$\begin{array}{cccc} & l & m & r \\ T & \mathrm{a} & \mathrm{b} & \mathrm{a} \\ M & \mathrm{b} & \mathrm{b} & \mathrm{c} \\ B & \mathrm{a} & \mathrm{c} & \mathrm{c} \\ U & \mathrm{d} & \mathrm{e} & \mathrm{f} \end{array}$$

If we set:

$$\phi'^1(y^1) = \begin{cases} \phi^1(y^1) & \text{if} \quad y^1 \neq (U, d), (U, e), (U, f) \\ U & \text{otherwise} \end{cases}$$

$$\phi'^2(y^2) = \begin{cases} \phi^2(y^1) & \text{if} \quad y^2 \neq (l, d), (m, e), (r, f) \\ L & \text{if} \quad y^2 = (l, d) \text{ or } (m, e) \\ R & \text{if} \quad y^2 = (r, f). \end{cases}$$

(τ, ϕ') is a $\mathscr{C}'$-protocol that generates $\mathscr{I}$. We prove that (τ, ϕ') is not secure by two different ways.

In $\Gamma(\mathscr{C}, G_2)$, it is a Nash equilibrium to follow (τ, ϕ'), then to play in G_2 according to the translated messages as in Example 4.1. Nevertheless, this is not a Nash equilibrium of $\Gamma(\mathscr{C}, G_1)$. In fact, player 1 would have incentives to send message U, then to play B if his signal is (U, d) or (U, e), and T if his message is (U, f). Therefore, (τ, ϕ) is not secure from the definition.

Player 1 cannot change the distribution of player 2's translated messages. But if 1 sends message U, 1 learns the translated message of player 2, which is strictly more informative that in $\mathscr{I}$. Hence, (τ, ϕ) is not secure from the characterization.

5. TEST GAMES

We introduce games where player $j \neq i$'s payoff functions are zero and where their strategies are identified to their signals in $\mathscr{I}$. Then we show that these games are sufficient to identify player i's possible incentives to deviate from (τ, ϕ).

Let I_{X^i} denote the identical mapping of X^i.

Definition 5.1. For $i \in I$,

- An *i-test game* is a compact game $\tilde{G} = ((\tilde{S}^j)_{j \in I}, \tilde{g})$ with $\tilde{S}^j = X^j$ and $\tilde{g}^j \equiv 0$ for $j \neq i$.
- An *i-test* is a pair $(\tilde{G}, f)$, where $\tilde{G}$ is an i-test game and f is a Nash equilibrium of $\Gamma(\mathscr{I}, \tilde{G})$ such that $f^j = I_{X^j}$ for $j \neq i$.

The definition depends on $\mathscr{I}$, but it is assumed to be fixed. An i-test game is given by a compact set $\tilde{S}^i$ and a continuous mapping $\tilde{g}^i$: $\tilde{S}^i \times X^{-i} \to \mathbb{R}$. Given an i-test game $\tilde{G}$, $\tilde{g}_{\mathscr{I}}$ and $\tilde{g}_{\mathscr{C}}$ represent the payoff functions of $\Gamma(\mathscr{I}, \tilde{G})$ and of $\Gamma(\mathscr{C}, \tilde{G})$ respectively.

To construct an i-test $(\tilde{G}, f)$ from an i-test game $\tilde{G}$, set $f^j = I_{X^j}$ for $j \neq i$ and choose $f^i \in \arg\max_{f'^i: X^i \to \Sigma^i} \tilde{g}^i_{\mathscr{I}}(f^{-i}, f'^i)$. Such f is a Nash equilibrium of $\Gamma(\mathscr{I}, \tilde{G})$ since $\tilde{g}^j_{\mathscr{I}} \equiv 0$ for $j \neq i$.

Definition 5.2. Given an i-test $(\tilde{G}, f)$, the protocol (τ, ϕ) is *test secure for* $(\tilde{G}, f)$ when $(\tau, f \circ \phi)$ is a Nash equilibrium of $\Gamma(\mathscr{C}, \tilde{G})$. (τ, ϕ) is *test secure* when it is test secure for every i and for every i-test.

Note that (τ, ϕ) is test secure for $(\tilde{G}, f)$ whenever it is secure for $\tilde{G}$.

Lemma 5.1. *(τ, ϕ) is secure if and only if it is test secure.*

Proof. If (τ, ϕ) is secure, it is in particular test secure for every i-test.

Conversely, assume that (τ, ϕ) is test secure. Consider a compact game G and a Nash equilibrium f of $\Gamma(\mathscr{I}, G)$. Define an i-test game $\tilde{G}$ by $\tilde{S}^i = S^i$ and $\tilde{g}^i(s^i, x^{-i}) = g^i(f^{-i}(x^{-i}), s^i)$. Hence $\tilde{g}(s^i, x^{-i})$ is the expected payoff of player i in $\Gamma(\mathscr{I}, G)$ if players $j \neq i$ get signals x^j, use strategies f^j and if i plays s^i. For every f'^i: $X^i \to \Sigma^i$:

$$g^i_{\mathscr{I}}(f^{-i}, f'^i) = \tilde{g}^i_{\mathscr{I}}((I_{X^j})_{j \neq i}, f'^i)$$

therefore f^i is a best reply against $(I_{X^j})_{j \neq i}$ in $\Gamma(\mathscr{I}, \tilde{G})$. Hence, $(\tilde{G}, ((I_{X^j})_{j \neq i}, f^i))$ is an i-test. As (τ, ϕ) is test secure, $(\tau, (\phi^{-i}, (f \circ \phi)^i))$ is a Nash equilibrium of $\Gamma(\mathscr{C}, \tilde{G})$. Now, see that for every $\tau'^i \in \mathscr{T}^i$ and F^i: $Y^i \to S^i$:

$$g^i_{\mathscr{C}}((\tau^{-i}, \tau'^i), ((f \circ \phi)^{-i}, F^i)) = \tilde{g}^i_{\mathscr{C}}((\tau^{-i}, \tau'^i), (\phi^{-i}, F^i))$$

Therefore,

$$(\tau^i, (f \circ \phi)^i) \in \arg\max_{\tau'^i, F^i} g^i_{\mathscr{C}}((\tau^{-i}, \tau'^i), ((f \circ \phi)^{-i}, F^i))$$

In words, $(\tau^i, (f \circ \phi)^i)$ is a best response against $(\tau^{-i}, (f \circ \phi)^{-i})$ in $\Gamma(\mathscr{C}, G)$ for every i. Hence $(\tau, f \circ \phi)$ is a Nash equilibrium of $\Gamma(\mathscr{C}, G)$. ▮

6. STABILITY OF THE MARGINALS

In this section we prove that if a protocol is secure, no player may change the distribution of the translated signals of the others by changing the distribution of his messages.

LEMMA 6.1. *If (τ, ϕ) is secure, then for every player i and for all $\tau'^i \in \mathscr{T}^i$, $m(\tau'^i) = m(\tau^i)$.*

Proof. Assume (τ, ϕ) is secure and consider a mapping $h: X^{-i} \rightarrow \mathbb{R}$. Define an i-test game $\tilde{G}$ by $\tilde{S}^i = \{s_0^i\}$ (s_0 is arbitrarily chosen) and by $\tilde{g}^i(s_0^i, x^{-i}) = h(x^{-i})$. A Nash equilibrium f of $\Gamma(\mathscr{I}, \tilde{G})$ is given by $f^j = I_{X^j}$ for $j \neq i$ and by $f^i(x^i) = s_0$. So $(\tau, f \circ \phi)$ is a Nash equilibrium of $\Gamma(\mathscr{C}, \tilde{G})$. Hence, for all $\tau'^i \in \mathscr{T}^i$ and F^i: $Y^i \rightarrow \tilde{S}^i$:

$$\tilde{g}^i_{\mathscr{C}}(\tau^{-i}, (f \circ \phi)^{-i}, \tau'^i, F^i) \leqslant \tilde{g}^i_{\mathscr{C}}(\tau, (f \circ \phi))$$

This writes explicitly:

$$\mathbf{E}_{l(\tau^{-i}, \tau'^i)} \mathbf{E}_{\phi^{-i}(y^{-i})} h(x^{-i}) \leqslant \mathbf{E}_{l(\tau)} \mathbf{E}_{\phi^{-i}(y^{-i})} h(x^{-i})$$

which is also:

$$\mathbf{E}_{m(\tau'^i)} h(x^{-i}) \leqslant \mathbf{E}_{m(\tau^i)} h(x^{-i})$$

Since this is true for every mapping h, $m(\tau'^i) = m(\tau^i)$. ▮

7. SECURE PROTOCOLS AND STATISTICAL EXPERIMENTS

In this section, we complete the proof of Theorem 3.1 by proving:

LEMMA 7.1. *Assume condition* (1) *of Theorem* 3.1 *holds, then* (τ, ϕ) *is secure if and only if for every i and every $\tau'^i \in \mathscr{T}^i$, $\alpha^i \supset \gamma_{\tau'^i}$.*

Proof. From lemma 5.1, (τ, ϕ) is secure if and only if for every i and every $\tau'^i \in \mathscr{T}^i$:

For every i-test $(\tilde{G}, f)$

$$\max_{F^i:\, Y^i \rightarrow S^i} \tilde{g}^i_{\mathscr{C}}(\tau^{-i}, (f \circ \phi)^{-i}, \tau'^i, F^i) \leqslant \tilde{g}^i_{\mathscr{I}}(f) \quad \mathbf{TC}(\tau'^i).$$

We shall prove that, assuming (1), $\mathbf{TC}(\tau'^i)$ holds if and only if $\alpha^i \supset \gamma_{\tau'^i}$. Fix $\tau'^i \in \mathscr{T}^i$ and write $\gamma^i = \gamma_{\tau'^i}$. For every i-test game $\tilde{G} = (\tilde{S}^i, \tilde{g}^i)$ we denote

$$v(\alpha^i, f^i) = (\mathbf{E}_{u_{x^{-i}}} \tilde{g}^i(f^i(x^i)), x^{-i})_{x^{-i} \in X^{-i}}$$

for a mapping f^i: $X^i \rightarrow \tilde{S}^i$, and

$$V(\gamma^i, F^i) = (\mathbf{E}_{w_{x^{-i}}} \tilde{g}^i(F^i(y^i), x^{-i}))_{x^{-i} \in X^{-i}}$$

for a mapping F^i: $Y^i \rightarrow \tilde{S}^i$.

These notations call for interpretations:

- The x^{-i}-th coordinate $v_{x^{-i}}(\alpha^i, f^i)$ of $v(\alpha^i, f^i)$ is the expected payoff of player i in $\Gamma(\mathcal{I}, \tilde{G})$ if i uses the strategy f^i, if other players use strategies (I_{X^j}), and if x^{-i} is the profile of their actions.
- The x^{-i}-th coordinate $V_{x^{-i}}(\gamma^i, F^i)$ of $V(\gamma^i, F^i)$ is the expected payoff of player i in $\Gamma(\mathcal{C}, \tilde{G})$ if i uses the strategy (τ'^i, F^i), if other players use strategies (τ^{-i}, ϕ^{-i}), and if x^{-i} is the profile of their actions.

Note that in both cases, the probability that players $j \neq i$ take actions x^{-i} is $\mu(x^{-i})$.

Then, $\mathbf{TC}(\tau'^i)$ holds if and only if for every $\tilde{G}$:

$$\max_{F^i\colon Y^i \to \tilde{S}^i} \sum_{x^{-i} \in X^{-i}} \mu(x^{-i})\, V_{x^{-i}}(\gamma^i, F^i) \leqslant \max_{f^i\colon X^i \to \tilde{S}^i} \sum_{x^{-i} \in X^{-i}} \mu(x^{-i})\, v_{x^{-i}}(\alpha^i, f^i).$$

Writing $A = \{(\tilde{g}^i(\tilde{s}^i, x^{-i}))_{x^{-i} \in X^{-i}}, \tilde{s}^i \in \tilde{S}^i\}$, we have $R_1(\alpha^i, A) = \{v(\alpha^i, f^i), f^i\colon X^i \to \tilde{S}^i\}$ and $R_1(\gamma^i, A) = \{V(\gamma^i, F^i), F^i\colon Y^i \to \tilde{S}^i\}$ (with the notations of Appendix A). Furthermore, A describes all the compact subsets of $\mathbb{R}^{X^{-i}}$ as $\tilde{G}$ describes all the i-test games. Therefore $\mathbf{TC}(\tau'^i)$ holds if and only if for every compact subset A of $\mathbb{R}^{X^{-i}}$:

$$\max_{V \in R_1(\gamma^i, A)} \sum_{\mu(x^{-i}) > 0} \mu(x^{-i})\, V_{x^{-i}} \leqslant \max_{v \in R_1(\alpha^i, A)} \sum_{\mu(x^{-i}) > 0} \mu(x^{-i})\, v_{x^{-i}}.$$

From Lemma A.1, this is equivalent to $\alpha^i \supset \gamma^i$. ▌

8. SECURE PROTOCOLS AND STANDARD EXPERIMENTS

Theorem 3.1 fully characterizes secure protocols. Nevertheless, the conditions it uses are not easily tractable, since properties (1) and (2) have to be fulfilled for all $\tau'^i \in \mathcal{T}'^i$. Furthermore, it is not always easy to check if some experiment is more informative than another.

8.1. *Equivalent Comparison of Experiments*

When player i sends messages according to τ'^i and receives a signal y^i, his conditional probability over the translated signals of other players is given by $P_{(\tau'^i, \tau^{-i})}(x^{-i} \mid y^i) \in \Delta(X^{-i})$. Let $\rho^i(\tau'^i) \in \Delta(\Delta(X^{-i}))$ be the distribution of $P_{(\tau'^i, \tau^{-i})}(x^{-i} \mid y^i)$ when y^i is distributed according to $l(\tau'^i, \tau^{-i})$. $\rho^i(\tau'^i)$ characterizes the distribution of the information of i on the translated signals of other players when he sends messages according to τ'^i and relies on y^i.

When i receives the signal x^i from $\mathcal{I}$, the conditional probability on x^i to x^{-i} is given by $\mu(x^{-i} \mid x^i) \in \Delta(X^{-i})$. Let $\pi^i \in \Delta(\Delta(X^{-i}))$ be the distribution of $\mu(x^{-i} \mid x^i)$ when x^i is distributed according to μ. π^i characterizes the distribution of the information of i on the signals of other players when he gets his signal from $\mathscr{I}$, or equivalently his information on the translated signals of other players when he sends messages to $\mathscr{C}$ according to τ^i and relies on his translated signal x^i.

π^i and $\rho^i(\tau^i)$ are called the *standard measures* associated to the experiments α^i and $\gamma_{\tau'^i}$.

LEMMA 8.1. *$\alpha^i \supset \gamma_{\tau'^i}$ if and only if for any continuous convex mapping H from $\Delta(X^{-i})$ to $\mathbb{R}$, $\int H\, d\pi^i \geqslant \int H\, d\rho^i(\tau'^i)$.*

Proof. The Lemma is a consequence of Theorem 4 of Blackwell [6]. ▮

Remarks. • Since both $\rho^i(\tau'^i)$ and π^i have finite support, the condition also writes: For all continuous convex mapping H: $\Delta(X^{-i}) \to \mathbb{R}$

$$\sum_{x^i \in X^i} H(\mu(x^{-i} \mid x^i))\, \mu(x^i) \geqslant \sum_{y^i \in Y^i} H(P_{(\tau'^i,\, \tau^{-i})}(x^{-i} \mid y^i))\, l(\tau'^i, \tau^{-i})(y^i).$$

• A consequence of the lemma is that α^i and $\gamma_{\tau'^i}$ are equivalent if and only if $\pi^i = \rho^i(\tau'^i)$.

LEMMA 8.2. *For every continuous convex mapping H from $\Delta(X^{-i})$ to $\mathbb{R}$, the mapping $\tau'^i \mapsto \int H\, d\rho^i(\tau'^i)$ is convex.*

Proof. Take $\tau_1^i, \tau_2^i \in \mathscr{T}^i$ and $p \in [0, 1]$. Set $\tau_0^i = p\tau_1^i + (1-p)\,\tau_2^i$ and $\tau_0 = (\tau_0^i, \tau^{-i})$, $\tau_1 = (\tau_1^i, \tau^{-i})$, $\tau_2 = (\tau_2^i, \tau^{-i})$. For every $y^i \in Y^i$,

$$\begin{aligned} &P_{\tau_0}(x^{-i} \mid y^i)\, l(\tau_0)(y^i) \\ &\qquad = pP_{\tau_1}(x^{-i} \mid y^i)\, l(\tau_1)(y^i) + (1-p)\, P_{\tau_2}(x^{-i} \mid y^i)\, l(\tau_2)(y^i) \end{aligned}$$

with $l(\tau_0)(y^i) = pl(\tau_1)(y^i) + (1-p)\, l(\tau_2)(y^i)$, so that, by convexity of H,

$$\begin{aligned} &H(P_{\tau_0}(x^{-i} \mid y^i))\, l(\tau_0)(y^i) \\ &\qquad \leqslant pH(P_{\tau_1}(x^{-i} \mid y^i))\, l(\tau_1)(y^i) + (1-p)\, H(P_{\tau_2}(x^{-i} \mid y^i))\, l(\tau_2)(y^i). \end{aligned}$$

And the result obtains by summing over $y^i \in Y^i$. ▮

8.2. *Another Characterization of Secure Protocols*

We are now able to provide another characterization of secure protocols that involves a finite number of conditions only. Also, the only comparisons of experiments that have to be checked are $\alpha^i \supset \gamma_{t^i}$ for t^i a message sent with null probability under τ^i.

THEOREM 8.1. *(τ, ϕ) is secure if and only if:*

(1′) *For all i and $t^i \in T^i$ such that $\tau^i(t^i) = 0$, $m(t^i) = m(\tau^i)$;*

(2′) *For all i and $t^i \in T^i$ such that $\tau^i(t^i) > 0$, $\rho^i(t^i) = \pi^i$;*

(2″) *For All i and $t^i \in T^i$ such that $\tau^i(t^i) = 0$, $\alpha^i \supset \gamma_{t^i}$.*

Proof. We compare the conditions of Theorems 8.1 with those of Theorem 3.1. Obviously (1) implies (1′) and (2) implies (2″).

(2) ⇒ (2’). Consider $t^i \in T^i$ such that $\tau^i(t^i) > 0$. Choose $p \in]0, 1[$ and $\tau'^i \in \mathscr{T}^i$ such that $\tau^i = pt^i + (1-p)\,\tau'^i$. Take $H\colon \Delta(X^{-i}) \to \mathbb{R}$ continuous convex. Since $\alpha^i \supset \gamma_{t^i}$ and $\alpha^i \supset \gamma_{\tau'^i}$, $\int H\, d\pi^i \geqslant \int H\, d\rho^i(t^i)$ and $\int H\, d\pi^i \geqslant \int H\, d\rho^i(\tau'^i)$. On the other hand, Lemma 8.2 shows that $\int H\, d\pi^i \leqslant p \int H\, d\rho^i(t^i) + (1-p) \int H\, d\rho^i(\tau'^i)$. This implies that $\int H\, d\pi^i = \int H\, d\rho^i(t^i) = \int H\, d\rho^i(\tau'^i)$. Since this is true for all H, $\pi^i = \rho^i(t^i)$.

(1′) and (2′) ⇒ (1). First see that (2′) implies $m(t^i) = m(\tau^i)$ for t^i such that $\tau^i(t^i) > 0$. Indeed for $x^{-i} \in X^{-i}$:

$$m(t^i)(x^{-i}) = \int p_{x^{-i}}\, d\rho^i(t^i) = \int p_{x^{-i}}\, d\pi^i = m(\tau^i)(x^{-i})$$

where $p_{x^{-i}}(\delta) = \delta(x^{-i})$ for $\delta \in \Delta(X^{-i})$. Therefore $m(t^i) = m(\tau^i)$ for all $t^i \in T^i$, which implies $m(\tau'^i) = m(\tau^i)$ for all $\tau'^i \in \mathscr{T}^i$.

(2′) and (2″) ⇒ (2). (2′) and (2″) imply that for all $t^i \in T^i$, $\alpha^i \supset \gamma_{t^i}$. Lemma 8.2 shows that the set $\{\tau'^i \in \mathscr{T}^i, \alpha^i \supset \gamma_{\tau'^i}\}$ is convex. Hence $\alpha^i \supset \gamma_{\tau^i}$ for all $\tau^i \in \mathscr{T}^i$. ∎

9. TRANSLATIONS AND INTERPRETATIONS

The notion of translation is closely related to the one of interpretation introduced in Gossner [13].

9.1. *Faithful Interpretations*

Recall from [13] that an *interpretation* from an information structure $\mathscr{I}_0 = ((X_0^i)_i, \mu_0)$ to another $\mathscr{I}_1 = ((X_1^i)_i, \mu_1)$ is a family of mappings $\psi = (\psi^i)_i$ from X_0^i to $\Delta(X_1^i)$. ψ is a *compatible interpretation* whenever the probability image of μ_0 by ψ is μ_1. Moreover, ψ is *faithful* whenever no player loses information about the translated signal of the other players x_1^{-i} when computing his translated signal x_1^i and forgetting his original one x_0^i. Formally, if P_ψ denotes the probability induced on $X_0 \times X_1$ by μ_0 and ψ, ψ is faithful if it is compatible and if for all i and $x_1^{-i} \in X_1^{-i}$, $P_\psi(x_1^{-i} \mid x_0^i) = P_\psi(x_1^{-i} \mid x_1^i)$ P_ψ-almost surely.

Consider a $\mathscr{C}$-protocol (τ, ϕ) generating $\mathscr{I} = ((X^i)_i, \mu)$, and let $\mathscr{J}$ be the information structure defined by the sets of signals $(Y^i)_i$ and by the probability $l(\tau)$ on Y. ϕ defines an interpretation from $\mathscr{J}$ to $\mathscr{I}$. Since μ is the probability image of $l(\tau)$ by ϕ, ϕ is a compatible interpretation from $\mathscr{J}$ to $\mathscr{I}$.

PROPOSITION 9.1. *If a protocol (τ, ϕ) is secure, ϕ is a faithful interpretation from $\mathscr{J}$ to $\mathscr{I}$.*

Proof. We use property (ii) of Theorem 7.1 of [13]. The experiment before interpretation for player i is γ_{τ^i} and the experiment after interpretation for player i is α^i. $\gamma_{\tau^i} \supset \alpha^i$ since γ_{τ^i} is always sufficient for α^i as noted in [13]. Assuming (τ, ϕ) is secure, Theorem 3.1 implies $\alpha^i \supset \gamma_{\tau^i}$. Then, the experiment before interpretation and the experiment after interpretation for player i are equivalent, so ϕ is faithful. ▮

Consider a $\mathscr{C}$-protocol (τ, ϕ) generating $\mathscr{I}$, and an interpretation ψ from $\mathscr{I}$ to $\mathscr{I}'$. We define the $\mathscr{C}$-protocol $(\tau, \psi \circ \phi)$ by the relations $(\psi \circ \phi)(y^i) = \sum_{x^i} \phi(y^i)(x^i)\, \psi(x^i)$. Note that $(\tau, \psi \circ \phi)$ generates $\mathscr{I}'$ whenever ψ is compatible. Moreover, one can easily check the following:

PROPOSITION 9.2. *If (τ, ϕ) is secure and if ψ is faithful, then $(\tau, \psi \circ \phi)$ is secure.*

Proposition 9.2 formalizes the approach used in Lehrer [16]: To generate $\mathscr{I}'$, one first generates $\mathscr{I}$, then a faithful transformation from $\mathscr{I}$ to $\mathscr{I}'$ is used.

9.2. *Deterministic Translations*

A transformation ψ from $\mathscr{I}_0 = ((X_0^i)_i, \mu_0)$ to $\mathscr{I}_1 = ((X_1^i)_i, \mu_1)$ is *deterministic* when for every $x_0^i \in X_0^i$ such that $\mu_0(x_0^i) > 0$, the support of $\phi^i(x_0^i)$ is a singleton. An information structure $\tilde{\mathscr{I}}_1$ is *minimal* when any faithful interpretation from an information structure $\mathscr{I}_0$ to $\tilde{\mathscr{I}}_1$ is deterministic.

Consider the equivalence relation on information structures: "there exists a faithful transformation from $\mathscr{I}_1$ to $\mathscr{I}_0$ and there exists a faithful transformation from $\mathscr{I}_0$ to $\mathscr{I}_1$". In [13], we proved the existence for any information structure $\mathscr{I}$ of an information structure $\tilde{\mathscr{I}}$ that is minimal and equivalent to $\mathscr{I}$.

To some extent, a similar property holds for translations.

DEFINITION 9.1. A translation ϕ is *deterministic on the support of* $l(\tau)$ when for every y^i such that $l(\tau)(y^i) > 0$, the support of $\phi^i(y^i)$ is reduced to a point.

Proposition 9.3. *Let (τ, ϕ) be a secure protocol generating $\mathscr{I}$ and let $\mathscr{I}'$ be minimal and equivalent to $\mathscr{I}$. There exists a translation ϕ' that is deterministic on the support of $l(\tau)$ such that (τ, ϕ') is secure and generates $\mathscr{I}'$.*

Proof. Let ψ be a deterministic faithful interpretation from $\mathscr{I}$ to $\mathscr{I}'$. With $\phi' = \psi \circ \phi$, (τ, ϕ') is secure and generates $\mathscr{I}'$ from Proposition 9.2. Then Proposition 9.1 shows that ϕ' is faithful. As $\mathscr{I}'$ is minimal this implies that for all y^i such that $l(\tau)(y^i) > 0$, the support of $\phi'^i(y^i)$ is reduced to a point. ▌

It is not true in general that if there exists a secure protocol (τ, ϕ) that generates a minimal information structure $\mathscr{I}$, there also exists a secure protocol (τ', ϕ') that generates $\mathscr{I}$ and such that ϕ' is deterministic.

Example 9.1. Consider again the mechanism $\mathscr{C}'$ defined in Example 4.2. A $\mathscr{C}'$ protocol is defined by the mixed message τ of Example 4.1 and by:

$$\phi''^1(y^1) = \begin{cases} \phi^1(y^1) & \text{if} \quad y^1 \neq (U, d), (U, e), (U, f), \\ U & \text{otherwise,} \end{cases}$$

$$\phi''^2(y^2) = \begin{cases} \phi^2(y^2) & \text{if} \quad y^2 \neq (l, d), (m, e), (r, f), \\ \frac{2}{3}L + \frac{1}{3}R & \text{otherwise.} \end{cases}$$

(τ, ϕ'') is a $\mathscr{C}'$-protocol that generates $\mathscr{I}$. If 1 sends message U, it does not change the probability of translated signals of 2, and 1 gets with probability 1 a conditional probability $\frac{2}{3}L + \frac{1}{3}R$ on 2's translated messages, which is less informative than if he sends messages according to τ^1. Therefore (τ, ϕ'') is a secure $\mathscr{C}'$-protocol that generates $\mathscr{I}$. Furthermore, $\mathscr{I}$ is minimal as proved in [13].

Now take any $\mathscr{C}'$-protocol (τ', ϕ'). If the translation ϕ'^2 of player 2 is deterministic (even for signals (l, d), (m, e), and (r, f)), then if 1 sends the message U, 1's signal reveals the signal of 2, and therefore also reveals the translated signal of 2. Hence if (τ', ϕ') generates $\mathscr{I}$, (τ', ϕ') is not secure.

10. EXTENSIONS AND DISCUSSION ON THE MODEL

10.1. *Perfect Recall of the Messages Sent*

We assumed that players peg their action only on their signals, not on their messages. For the actions of the players in G to depend also on their messages, we construct from G and from $\mathscr{C}$ the extended game $\bar{\Gamma}(\mathscr{C}, G)$ "with perfect recall" in which:

- each player i sends a message t^i to the mechanism;
- $y \in Y$ is drawn according to $l(t)$ and each player i is informed of y^i;

- each player i chooses σ^i according to t^i and y^i;
- the vector payoff is $g(\sigma)$.

A strategy for player i in $\bar{\Gamma}(\mathscr{C}, G)$ is given by a mixed message $\tau^i \in \mathscr{T}^i$ and by an application F^i: $T^i \times Y^i \to \Sigma^i$. The payoff function of $\bar{\Gamma}(\mathscr{C}, G)$ is $\bar{g}_{\mathscr{C}}(\tau, F) = \mathbf{E}_{l(\tau)}\, g(F(t, y))$.

Given $\mathscr{C}$, we define a mechanism $\overline{\mathscr{C}} = ((T^i)_i, (\bar{Y}^i)_i, \bar{l})$ with $\bar{Y}^i = T^i \times Y^i$ and $\bar{l}(\tau)(t, y) = \tau(t)\, l(t)(y)$. In $\overline{\mathscr{C}}$ each player receives as signal the message he has sent to the mechanism and a signal drawn as in $\mathscr{C}$.

We see that the sets of strategies in $\bar{\Gamma}(\mathscr{C}, G)$ and in $\Gamma(\overline{\mathscr{C}}, G)$ are equal and that $\bar{g}_{\mathscr{C}}(l, t) = g_{\overline{\mathscr{C}}}(l, t)$. This shows the equivalence between G extended by $\mathscr{C}$ with perfect recall and G extended by $\overline{\mathscr{C}}$ without perfect recall.

10.2. *Finite Games*

We could have defined a secure protocol as a protocol that is secure for all finite games without affecting our characterizations. In fact, the proof of Lemma 6.1 needs only the strategy spaces to be finite, and Blackwell [6, p. 96] notes that the comparison of experiments remains unchanged of the sets A of choices opened to the statistician are finite.

10.3. *Infinite Mechanisms*

We considered communication mechanisms with finite sets of messages and signals. Actually, the model and Theorem 3.1 easily extend to the case where Hwa sets are taken compact.

10.4. *The Incomplete Information Case*

For simplicity, we assumed complete information in the sense that player's payoffs depend only on their actions. Actually, the definition of a secure protocol and its characterizations naturally extend to the case of incomplete information.

Fix a (finite) set of states of nature Ω.

A (*Bayesian*) *game* $G = (\pi, (S^i)_i, g)$ is given by a probability distribution π on Ω, by a compact set of actions S^i for each player i, and by a continuous payoff function g: $\Omega \times S \to \mathbb{R}^I$. The set of mixed strategies for i is $\Sigma^i = \Delta(S^i)$.

An *information structure* $\mathscr{J} = ((X^i_{\mathscr{J}})_i, \mu_{\mathscr{J}})$ is now given by a (finite) set of signals $X^i_{\mathscr{J}}$ for each player i and by a signal function $\mu_{\mathscr{J}}$: $\Omega \to \Delta(X_{\mathscr{J}})$. When $\omega \in \Omega$ is the state of nature, $\mu_{\mathscr{J}}(\omega)$ is the distribution of signal profiles to the players.

A *communication mechanism* is a triple $\mathscr{C} = ((T^i)_i, (Y^i)_i, l)$, where T^i is i's finite set of messages, Y^i is i's finite set of signals, and l: $\Omega \times T \to \Delta(Y)$

$$\begin{tikzcd} \mathscr{J} \arrow[r, "x^i_{\mathscr{J}}"] & i \arrow[r, "f^i(x^i_{\mathscr{J}})"] & G \end{tikzcd}$$

FIG. 5. The extended game $\Gamma(\mathscr{J}, G)$.

$$\begin{tikzcd}
 & G & \\
\mathscr{I} \arrow[r, "x^i_{\mathscr{I}}"] & i \arrow[u, "F^i(x^i_{\mathscr{I}}, y^i)"] \arrow[r, "t^i"] & \mathscr{C} \arrow[l, bend left=90, "y^i"]
\end{tikzcd}$$

FIG. 6. The extended game $\Gamma(\mathscr{J}, \mathscr{C}, G)$.

is the signal function (the signal in $\mathscr{C}$ may depend on ω). The set of mixed messages for player i is $\mathscr{T}^i = \Delta(T^i)$.

Given a Bayesian game G and an information structure $\mathscr{J}$, $\Gamma(\mathscr{J}, G)$ represents the extended game in which:

- $\omega \in \Omega$ is drawn according to π;
- Players are informed according to $\mathscr{J}$;
- G is played.

A strategy of i in $\Gamma(\mathscr{J}, G)$ is a mapping f^i: $X^i_{\mathscr{J}} \to \Sigma^i$. See Fig. 5.

Given G, $\mathscr{J}$ and a communication mechanism $\mathscr{C}$, let $\Gamma(\mathscr{J}, \mathscr{C}, G)$ be the extended game in which:

- $\omega \in \Omega$ is drawn according to π
- Players are informed according to $\mathscr{J}$;
- Players communicate through $\mathscr{C}$;
- G is played.

A strategy of i in $\Gamma(\mathscr{J}, \mathscr{C}, G)$ is given by a (message) mapping τ^i: $X^i_{\mathscr{J}} \to \mathscr{T}^i$ and by an (action) mapping F^i: $X^i_{\mathscr{J}} \times Y^i \to \Sigma^i$. See Fig. 6.

A *communication protocol* (or $\mathscr{J}$-$\mathscr{C}$-protocol) is given by a (message) mapping τ^i: $X^i_{\mathscr{J}} \to \mathscr{T}^i$, by a finite set of translated signals $X^i_{\mathscr{I}}$ for each player i and by a translation ϕ^i: $X^i_{\mathscr{J}} \times Y^i \to \Delta(X^i_{\mathscr{I}})$. See Fig. 7.

For $\omega \in \Omega$ being fixed, $\mu_{\mathscr{J}}$, $\tau = (\tau^i)_i$ and $\phi = (\phi^i)_i$ induce a probability distribution on $X_{\mathscr{J}} \times Y \times X_{\mathscr{I}}$. Let $\mu_{\mathscr{I}}(\omega)$ be its marginal on $X_{\mathscr{I}}$. $\mathscr{I} = ((X^i_{\mathscr{I}_i}, \mu_{\mathscr{I}})$ is the information structure generated by the protocol (τ, ϕ).

$$\begin{tikzcd}
 & \mathscr{I} & \\
\mathscr{J} \arrow[r, "x^i_{\mathscr{J}}"] & i \arrow[u, "x^i_{\mathscr{I}}"] \arrow[r, "t^i"] & \mathscr{C} \arrow[l, bend left=90, "y^i"]
\end{tikzcd}$$

FIG. 7. The protocol (τ, ϕ).

We say that (τ, ϕ) is secure when for every Bayesian game G and every Nash equilibrium f of $\Gamma(\mathcal{I}, G)$, it is a Nash equilibrium of $\Gamma(\mathcal{I}, \mathcal{C}, G)$ to:

- Receive information according to $\mathcal{I}$;
- Follow the protocol, thus generating signal profiles $x_{\mathcal{I}} \in X_{\mathcal{I}}$;
- Play in G according to $f(x_{\mathcal{I}})$.

For a fixed $\omega \in \Omega$ and $\tau'^i\colon X^i_{\mathcal{I}} \to \mathcal{T}^i$, let $m(\omega, \tau'^i) \in \Delta(X^{-i})$ be the distribution of players $j \neq i$'s translated signals when the state of nature is ω, players $j \neq i$ follow (τ, ϕ) and when i's messages are sent according to τ'^i.

Let α^i be the statistical experiment that characterizes the information on $(\omega, x^{-i}_{\mathcal{I}})$ given by $x^i_{\mathcal{I}}$ in the information structure $\mathcal{I}$. Let also $\gamma_{\tau'^i}$ be the statistical experiment that characterizes the information on $(\omega, x^{-i}_{\mathcal{I}})$ given by $(x^i_{\mathcal{I}}, y^i)$ when players $j \neq i$ follow (τ, ϕ) and when i's messages are sent according to τ'^i.

Theorem 3.1 extends to:

THEOREM 10.1. (τ, ϕ) *is secure if and only if:*

(1) *For every player i, $\tau'^i \in \mathcal{T}^i$ and $\omega \in \Omega$, $m(\omega, \tau'^i) = m(\omega, \tau^i)$*

(2) *For every player i and $\tau'^i \in \mathcal{T}^i$, $\alpha^i \supset \gamma_{\tau'^i}$*

The proof of Theorem 10.1 is a simple extension of the proof of Theorem 3.1.

11. CONCLUSION

In our approach, instead of looking both for a mechanism and for a protocol securely generating a given information structure, we start with a mechanism $\mathcal{C}$ and wonder which $\mathcal{C}$-protocols are secure.

We obtained different characterizations of a secure protocol. Now, it would be interesting to know which information structures can be securely generated through a given protocol or through its repetitions. Ideally, results in the spirit of the Folk Theorem that classify communication mechanisms according to the information structures securely generated through their repetitions could be obtained. Proposition 9.2 gives a positive result in this direction, since if there exists a faithful transformation from $\mathcal{I}$ to $\mathcal{I}'$ and if $\mathcal{I}$ can be securely generated through a $\mathcal{C}$-protocol, $\mathcal{I}'$ can also be securely generated through a $\mathcal{C}$-protocol.

A. BLACKWELL'S COMPARISON OF STATISTICAL EXPERIMENTS

Recall from Blackwell [6, 7] that an *experiment* α is a family of probability measure $u_1, ..., u_N$ on the Borel field of a space Z. u_k is the probability over the signals received by the statistician when the state of nature is k. A *decision problem* is a pair (α, A), where A is a compact subset of $\mathbb{R}^N$. Points in A are possible choices for the statistician, the gain[2] from action $a = (a_1, ..., a_N)$ is a_k if the actual state of nature is k. A *decision procedure* for (α, A) is a measurable mapping from Z to A, it associates a choice of action to every signal. To every decision procedure f such that $f(z) = (a_1(z), ..., a_n(z))$ is associated a gain vector:

$$v(f) = \left(\int a_1(z)\, du_1, ..., \int a_N(z)\, du_N \right)$$

The kth coordinate of $v(f)$ is the expected gain if the state of nature is k and the decision procedure is f. $R_1(f)$ denotes the range of $v(f)$ and $R(f)$ is the convex closure of $R_1(f)$.

Given two statistical experiments α and β, α is *more informative* than β, and we write $\alpha \supset \beta$, when $R(\alpha, A) \supset R(\beta, A)$ for all A. The experiments α and β are *equivalent* when $\alpha \supset \beta$ and $\beta \supset \alpha$.

We use the following characterization of $\alpha \supset \beta$:

LEMMA A.1. *Let $c_1, ..., c_N$ be positive real numbers, $\alpha \supset \beta$ if and only if for any compact subset A of $\mathbb{R}^N$:*

$$\max_{v \in R_1(\beta, A)} \sum_k c_k v_k \leqslant \max_{v \in R_1(\alpha, A)} \sum_k c_k v_k.$$

Remark. The lemma comes from the condition (3) of Theorem 2 of Blackwell [6]. In Blackwell's result the numbers $c_1, ..., c_N$ are all equal to 1, but the proof remains unchanged for all $c_k > 0$.

REFERENCES

1. R. J. Aumann, Subjectivity and correlation in randomized strategies, *J. Math. Econ.* **1** (1974), 67–95.
2. R. J. Aumann and S. Hart, Polite talk isn't cheap, handout, 1993.
3. R. J. Aumann, M. Maschler, and R. Stearns, Repeated games with incomplete information: An approach to the nonzero sum case, *in* "Reports to the U.S. Arms Control and Disarmament Agency," Chapter IV, pp. 117–216, ST-143, 1968.

[2] In Blackwell's work, and in statistics in general, the statistician minimizes an expected loss. In a game theoretic approach, it is more natural to say that she maximizes an expected gain.

4. L. Bárány, Fair distribution protocols or how the players replace fortune, *Math. Oper. Res.* **17** (1992), 327–340.
5. L. Bárány and Z. Füredi, Mental poker with three or more players, *Inform. Control* **59** (1983), 84–93.
6. D. Blackwell, Comparison of experiments, *in* "Proceedings of the Second Berkeley Symposium on Mathematical Statistics and Probability," pp. 93–102, University of California Press, Berkeley, 1951.
7. D. Blackwell, Equivalent comparison of experiments, *Ann. Math. Statist.* **24** (1953), 265–272.
8. S. Crépeau, A secure poker protocol that minimizes the effect of player coalitions, *in* "Advances in Cryptology: Proceedings of CRYPTO'85," pp. 73–86, Springer-Verlag, Berlin, 1986.
9. J. Farrell, Cheap talk, coordination, and entry, *Rand J. Econ.* **18** (1987), 34–39.
10. F. Forges, An approach to communication equilibria, *Econometrica* **54** (1986), 1375–1385.
11. F. Forges, Universal mechanisms, *Econometrica* **58** (1990), 1341–1364.
12. S. Fortune and Merritt, Poker protocols, *in* "Advances in Cryptology: Proceedings of CRYPTO'84," pp. 454–464, NATO ASI Series, 1985.
13. O. Gossner, "Comparison of Information Structures," CORE, DP 9791, 1997.
14. O. Gossner, "Jeux répétés et mécanismes de communication," Ph.D. thesis, Université Paris 6, Paris, 1996.
15. O. Gossner and N. Vieille, work in progress, 1998.
16. E. Lehrer, Internal correlation in repeated games, *Internat. J. Game Theory* **19** (1991), 431–456.
17. E. Lehrer, Mediated talk, *Internat. J. Game Theory* **25** (1996), 177–188.
18. E. Lehrer and S. Sorin, One shot public mediated talk, *Games Econ. Behav.* **20** (1997), 131–148.
19. R. B. Myerson, Optimal coordination problems in generalized principal-agent problems, *J. Math. Econ.* **10** (1982), 67–81.
20. R. B. Myerson, "Game Theory; Analysis of Conflict," Harvard Univ. Press, Cambridge, MA, 1991.
21. A. Urbano and J. E. Vila, Pre-play communication and coordination in two-player games, handout, 1997.
22. T. Tomala, "Équilibres de jeux répétés á observation imparfaite," Ph.D. thesis, Université Paris I, Paris, 1996.