# Implementation of Communication Equilibria by Correlated Cheap Talk: the Two-Player Case*

Péter Vida† and Françoise Forges‡

September 2011 (previous version: February 2011)

**Abstract**

We show that essentially every communication equilibrium of any finite Bayesian game with two players can be implemented as a strategic form correlated equilibrium of an extended game, in which before choosing actions as in the Bayesian game, the players engage in a possibly infinitely long (but in equilibrium almost surely finite), direct, cheap talk.

Keywords: Bayesian game, cheap talk, communication equilibrium, correlated equilibrium, pre-play communication.

JEL Classification Numbers: C72, D70.

*Péter Vida proved the main result of this paper as part of his doctorate thesis at the Universitat Autònoma de Barcelona. A preliminary version of the paper, by Péter Vida, circulated under the title "From Communication Equilibria to Correlated Equilibria". The two authors had discussions on this research in 2005-2006 and completed the present version in 2010-2011. We wish to thank Elchanan Ben-Porath, Antoni Calvó-Armengol, Olivier Gossner, Manfred Nermuth, Eilon Solan, Adam Szeidl and the participants of the workshop "Decentralized Mechanism Design, Distributed Computing and Cryptography" held at Princeton in June 2010. Finally, three referees and especially a co-editor of Theoretical Economics raised interesting questions which led us to establish additional results.

†University of Vienna, Department of Economics. peter.vida@univie.ac.at

‡CEREMADE and LEDa, Université Paris-Dauphine. francoise.forges@gmail.com

# 1 Introduction

Let us consider a standard Bayesian game, in which the players simultaneously choose actions as a function of their private information (or type). This framework is useful to identify the parameters of the basic interactive decision problem but does not account for possible nonbinding communication between the players, which enables them to exchange information and to coordinate their actions. Such communication typically takes place at the interim stage (namely, once the players know their type and before they choose an action) and is conveniently modelled in extensions of the Bayesian game.

As illustrated by a vast literature, communication may consist of a plain conversation between the players ("cheap talk") or be mediated by a third party; it may last for one or several stages or even involve no deadline (see, e.g., Forges and Koessler (2008) for a short survey). In spite of this variety, a generalized revelation principle holds: the set of all Nash equilibrium outcomes of all games that extend a given Bayesian game by allowing arbitrary communication is nicely characterized as the set of all "canonical communication equilibria". These are achieved with the help of a mediator who first invites the players to reveal their types and then performs a lottery, in order to privately recommend an action to each of them, as a function of their reported types (see Forges (1986), Myerson (1986) and Myerson (1991), chapter 6).

Canonical communication equilibria are very tractable but rely on a centralized mediator, who collects the private information of the players. Plain conversation between the players is much more natural and preserves the players' privacy. Hence the question:

*Can all canonical communication equilibrium outcomes be implemented by means of cheap talk, i.e., as Nash equilibrium outcomes of an appropriately designed extended game in which the players can talk?*

Partially or even fully positive answers have been given in finite Bayesian games, in which types and actions take finitely many values, as soon as the number of players is at least three[1]. However, for two players, the answer is in general negative. Consider for instance the particular case where every player has a single type (complete information); in a plain conversation,

[1] Game theoretical references involve, e.g., Bárány (1992), Forges (1990b), Ben Porath (1998, 2003, 2006) and Gerardi (2004). See, e.g., Halpern (2008) for references in computer science.

both players know all the messages that they exchange, hence they cannot simulate the private recommendations of a mediator. More precisely, in a bi-matrix game, communication equilibria coincide with Aumann (1974, 1987)'s correlated equilibria, while the set of Nash equilibrium outcomes of a cheap talk extension of the game is always included in the convex hull of the set of Nash equilibrium outcomes of the bi-matrix game.

As a very different particular case, consider a two-person (finite) Bayesian game with a single informed player, whose actions are not payoff relevant, and a decision maker. In the original Bayesian game, the players choose their actions simultaneously so that the informed player cannot transmit information to the decision maker. Allowing a single stage of cheap talk, from the informed player to the decision maker, transforms the game into a *sender-receiver game*[2]. Examples show that, in that framework, there may exist communication equilibrium outcomes which cannot be achieved as Nash equilibrium outcomes of the sender-receiver game (see, e.g., Forges (1985)[3]). Even more, some communication equilibrium outcomes cannot even be implemented by "long cheap talk", in which both players exchange costless messages for as many stages as they like (see Forges (1990a)[4]).

Should the previous negative results lead us to forget about implementing communication equilibrium outcomes by cheap talk in two-person Bayesian games? Of course, no: two-person games are *the* prototype of interactive decision problems, as illustrated by the most popular game theoretical ex-

[2]Sender-receiver games were first studied by Crawford and Sobel (1982) and Green and Stokey (2007). Their model involves types and actions in a real interval and thus does not pertain to the finite setup that will be adopted in this paper.

[3]The framework in Forges (1985) is an infinitely repeated game but the results are easily reformulated in one-shot games with cheap talk (see exercise 6.9 in Myerson (1991)). Krishna and Morgan (2004) concentrate on Crawford and Sobel (1982)'s uniform quadratic example. They show that two stages of cheap talk enable the players to Pareto improve on all equilibria achieved with a single stage of cheap talk, when the bias $b$ reflecting the conflict of interest between the sender and the receiver is not too large, namely when $b \leq \frac{1}{\sqrt{8}}$. Goltsman et al. (2009) show that, if $b \leq \frac{1}{8}$, Krishna and Morgan (2004)'s cheap talk equilibria are optimal communication equilibria. Goltsman et al. (2009) also establish that finitely many stages of cheap talk achieve the optimal communication equilibrium outcome if and only if $b \leq \frac{1}{8}$.

[4]The example in Forges (1990a) explicitly deals with *long cheap talk* before a *single* decision stage, but relies on techniques developed by Hart (1985) and Aumann and Hart (1986) for infinitely repeated games with incomplete information. Aumann and Hart (2003) use this approach to characterize *all* Nash equilibrium outcomes of any long cheap talk game with a single informed player.

amples. But the above counter-examples teach us that, to implement all communication equilibrium outcomes of a two-person game, we have to relax the notion of cheap talk in some way. For instance, Dodis, Halevy and Rabin (2000) and Urbano and Vila (2002) rely on cryptographic tools developed in computer science, namely assume that the computational ability of the players is limited. Under this assumption, they show that the correlated equilibrium outcomes of any two-person game with complete information can indeed be implemented as ($\epsilon-$) Nash equilibrium outcomes of a cheap talk extension of the game. Ben-Porath (1998) obtains a similar result by allowing the players not only to talk but also to make use of urns or envelopes. Generalizations to games with incomplete information have been proposed by R.V. Krishna (2007) and Izmalkov, Lepinski and Micali (2010) for the latter approach and by Urbano and Vila (2004) for the cryptographic one. The common feature of these solutions is that *at every stage*, cheap talk is relaxed in some way: limited computational ability or physical hard devices are used to exchange messages at every stage.

In this paper, we follow another avenue and maintain the standard notion of cheap talk. The players are not subject to any deadline and cannot use any common device (like urns, envelopes or recording machines) while they talk (but each player is of course free to use any personal device to make his own choices). However, we assume that, before they start to talk, the players can privately observe some signal, a sunspot, which is totally extraneous to the game (i.e., independent of the players' types and without any direct effect on the payoffs)[5]. Following Aumann (1974, 1987), the players' signals can be correlated and the set of all Nash equilibrium outcomes of the extended game in which the players first observe their signal has a tractable canonical representation. In our framework, the canonical signal of each player takes the form of a recommendation on how to talk and how to make a decision at the end of the cheap talk phase.

In other words, we consider strategic form correlated equilibria (in the sense of Aumann (1974, 1987)) of a long cheap talk game extending the original Bayesian game. Our main result can be stated as follows. Fix any two-person Bayesian game $\Gamma$ and any (strictly individually rational) communication equilibrium outcome of $\Gamma$; we design a long cheap talk extension

[5] As in Forges (1988), we do not reserve the term "sunspot" to a common, public, extraneous signal. The interpretation is that every player observes the sunspots in his own way.

$ext\Gamma$ of $\Gamma$, with finitely many messages at every stage, together with a correlation device for the cheap talk game $ext\Gamma$, with the following properties: (i) no player can gain by unilaterally deviating from the recommendation of the correlation device in $ext\Gamma$ and (ii) the outcome, namely the conditional probability distributions generated by the correlation device and strategies in $ext\Gamma$ over actions given types, are exactly the same as in the communication equilibrium. In this construction, the size of the finite set of messages depends on the parameters of the Bayesian game and on the underlying communication equilibrium. By considering a countable set of messages, we can get at once all (strictly individually rational) communication equilibrium outcomes of any Bayesian game as correlated equilibrium outcomes of a *universal* cheap talk game, as in Forges (1990b) for games with at least four players[6]. Our cheap talk game $ext\Gamma$ is possibly infinitely long in the sense that its length is not fixed in advance, in a deterministic way, but depends endogenously on the messages exchanged by the players.

Our result extends Forges (1985), which focuses on the case of a single informed player and a single decision maker. One stage of cheap talk suffices then to implement all communication equilibrium outcomes. Recently, Blume (2010) established a similar result in the context of Crawford and Sobel (1982)'s sender-receiver game. Forges (1985)'s construction goes through if payoff relevant actions are added for the single informed player. However, the general case, where *both* players are privately informed *and* make decisions, remained open until Vida (2006) proposed a first solution[7].

When trying to implement a given communication equilibrium by cheap talk in a two-person game in which both players have private information and must take actions, the main problem is to guarantee that no player learns useful information before the other. Full detection of possible deviations during the cheap talk phase can be of no help if it happens too late. Indeed, there may be no way to "punish" a deviator once he possesses the desired information. In order to solve the problem, the basic idea is that the correlation device selects a relevant stage $t^*$ of the cheap talk phase, without telling it directly to the players. How will the players figure out when they reach it? At the end of every stage $t$ of cheap talk, they simultaneously discover *from*

[6]Forges (1990b) also proposes a cheap talk game with a *continuum* of messages which is universal for all three person games.

[7]The main result in this paper can already be found in Vida (2006)'s unpublished doctoral dissertation (see also Vida (2007a)). The proof proposed in this paper is a simplification of the original one.

*their exchanged messages* whether stage $t$ was relevant (i.e., $t = t^*$) or not. Useful information is only exchanged at the relevant stage $t^*$, but the players realize this at the end of the stage. In addition, at every stage, each player can check whether the other's message was legitimate or not. If the stage is not relevant, the players' information is not updated so that illegitimate messages can give rise to punishments.

As indicated in the previous paragraphs, our construction makes use of possibly infinitely long cheap talk. To which extent does our implementation result rely on an infinite horizon? We prove that, at the correlated equilibrium which implements a given communication equilibrium, cheap talk lasts for finitely many stages almost surely. We also propose an example (in section 5) in which an efficient communication equilibrium outcome cannot be achieved as a correlated equilibrium outcome, in any cheap talk game with a bounded number of stages. Nonetheless, if the underlying game $\Gamma$ has a strictly individually rational Bayesian-Nash equilibrium (a condition which holds in the previous example), every (strictly individually rational) communication equilibrium payoff can be *approximated* by a correlated equilibrium payoff of a *sufficiently long* cheap talk game (proposition 1 in section 4).

The brief sketch above also suggests that our construction makes use of punishments. This should not be surprising in view of the literature on the implementation of a mediator by cheap talk (see Bárány (1992) for an early example, Heller et al. (2011) for a recent one, Ben-Porath (2003, 2006) and Gerardi (2004) for discussions and solutions to the problem, Forges (2009) for a survey). Are these punishments credible? To formulate this question more precisely, recall that, according to our result, every communication equilibrium of a Bayesian game $\Gamma$ can be implemented as a *Nash* equilibrium of an extended game $(ext\Gamma)^\mu$, in which a correlation device $\mu$ sends private signals to the players before they talk. Can we refine *this Nash equilibrium* so as to capture the players' sequential rationality, e.g., into a *perfect Bayesian equilibrium*? Proposition 2 (section 4) gives sufficient conditions for a positive answer.

We implement communication equilibria of a given Bayesian game as correlated equilibria of the game preceded by cheap talk. Hence we replace the communication device by a correlation device, that is to say, a mediator by another! What do we really gain from our construction? As argued by Forges (1985, 1988, 1990b) and recently by Blume (2010), the mediators implicitly involved in the two solution concepts are very different from each other. In a (canonical) communication equilibrium of the original game, the mediator gets to know the whole information of every player. However, in a correlated equilibrium of the cheap talk game, the mediator does not receive *any* information from the players. He makes recommendations on how to exchange messages but remains fully ignorant of the players' types. With such a mediator, players can preserve their privacy.

Let us turn to the organization of the paper. In the next section, we recall the concepts of Bayesian game and communication equilibrium. Then, in section 3, we describe the extension of the game in which the players can talk and we define correlated equilibrium in that game. In section 4, we state the main result as theorem 1 and the two propositions mentioned above; the reader familiar with our basic concepts can go to the statements right away. Section 5 is devoted to an example which illustrates our results. Section 6 contains the proofs. Finally, section 7 discusses some variants of the model.

## 2 Basic game, communication equilibrium

Let us fix a two-player finite Bayesian game $\Gamma \equiv < \{L^i, A^i, g^i\}_{i=1,2}, p >$: for every player $i = 1, 2$, $L^i$ is a finite set of possible types, $A^i$ is a finite set of actions and $g^i : L \times A \to \mathbb{R}$ is a von Neumann-Morgenstern utility function, where $L = L^1 \times L^2$ and $A = A^1 \times A^2$; $p \in \Delta L$ is the players' common prior over $L$.

$\Gamma$ starts with a move of nature, which selects $l = (l^1, l^2) \in L$ according to $p$; player $i$ is only informed of his own type $l^i$, $i = 1, 2$. Then the players simultaneously choose actions $a^1 \in A^1$ and $a^2 \in A^2$, respectively; let $a = (a^1, a^2)$. The respective payoffs are $g^1(l, a)$ and $g^2(l, a)$.

A (canonical) communication device[8] $q$ for $\Gamma$ is a transition probability from $L$ to $A$, $q : L \to \Delta A$, namely a system of probability distributions $q(.|l)$ over $A$ for every $l \in L$. By adding a communication device $q$ to the Bayesian game, one generates an extended game $\Gamma^q$, which is played as follows:

1. Every player $i$ learns his type $l^i$ as in $\Gamma$, $i = 1, 2$.

2. Every player $i$ sends a private message $\hat{l}^i \in L^i$ to the communication device $q$; let $\hat{l} = (\hat{l}^1, \hat{l}^2)$.

3. $q$ selects an action profile $a = (a^1, a^2)$ with probability $q(a|\hat{l})$.

[8] See Forges (1986, 1990b) and Myerson (1986, 1991).

4. $q$ sends $a^i$ privately to player $i$, $i = 1, 2$.

5. The players choose actions and receive payoffs as in $\Gamma$.

Some strategies are of special interest in $\Gamma^q$: player $i$ is *sincere* in $\Gamma^q$ if he reveals his type to the communication device at stage 2, namely $\hat{l}^i = l^i$ for every $l^i \in L^i$; player $i$ is *obedient* if at stage 5, he follows the recommendation $a^i$ made by the communication device at stage 4, whathever his type. When both players are sincere and obedient, the expected payoff of player $i$ of type $l^i$ is[9]:

$$G^i[q|l^i] = \sum_{l^{-i}} p(l^{-i}|l^i) \sum_a q(a|l^i, l^{-i}) g^i((l^i, l^{-i}), a) \quad l^i \in L^i, i = 1, 2. \qquad (1)$$

Let $G[q] = (G^i[q|l^i])_{l^i \in L^i, i=1,2}$ be the pair of vector payoffs associated with $q$.

**Definition 1** *Let $q$ be a (canonical) communication device for $\Gamma$. $q$ is a (canonical) communication equilibrium of $\Gamma$ if and only if the sincere and obedient strategies form a Nash equilibrium of $\Gamma^q$, namely, iff*

$$G^i[q|l^i] \geq \sum_{l^{-i}} p(l^{-i}|l^i) \sum_{a^i, a^{-i}} q(a^i, a^{-i}|\hat{l}^i, l^{-i}) g^i((l^i, l^{-i}), r^i(a^i), a^{-i})$$

*for $i = 1, 2, l^i, \hat{l}^i \in L^i$ and for all $r^i : A^i \to A^i$. $ME(\Gamma)$ denotes the set of communication equilibrium*[10] *payoffs of $\Gamma$, namely*

$$ME(\Gamma) = \{G[q] | q \textit{ is a communication equilibrium in } \Gamma\} \subset \mathbb{R}^{|L^1 \times L^2|}.$$

Thanks to the general *revelation principle* recalled in the introduction (see, e.g., Forges (1990b)), $ME(\Gamma)$ is the set of all payoffs that can be achieved at a Nash equilibrium of an arbitrary extension of $\Gamma$ allowing the players to communicate (possibly with infinitely many stages and relying on a mediator at every stage).

**Definition 2** *A payoff vector $(x^i(l^i))_{l^i \in L^i} \in \mathbb{R}^{|L^i|}$ is (strictly) interim individually rational for player $i = 1, 2$ (or interim supportable with (strict)*

[9] When the index $i$ refers to one of the two players, $-i$ refers to the other one.

[10] We use the notation $ME$ as a reminder of "mediated equilibrium"; we keep $CE$ for "correlated equilibrium".

*punishment) in $\Gamma$ if there is a strategy of the other player in $\Gamma$, namely, a transition probability $y^{-i} : L^{-i} \to \Delta A^{-i}$, such that for all $l^i \in L^i$,*

$$x^i(l^i) \geq (>) \max_{a^i \in A^i} \sum_{l^{-i}} p(l^{-i}|l^i) \sum_{a^{-i}} y^{-i}(a^{-i}|l^{-i}) g^i((l^i, l^{-i}), a^i, a^{-i}).$$

*$(S)INTIR(\Gamma)$ denotes the set of vectors in $\mathbb{R}^{|L^1 \times L^2|}$ that are (strictly) interim individually rational for both players.*

Observe that, in general, $(S)INTIR(\Gamma)$ depends on the prior probability distribution $p$ in $\Gamma$. In games with complete information (i.e., when $|L^1| = |L^2| = 1$), the definition reduces to the standard one, namely $x^i$ is (strictly) individually rational for player $i$ iff

$$x^i \geq (>) \min_{y^{-i} \in \Delta A^{-i}} \max_{a^i \in A^i} \sum_{a^{-i}} y^{-i}(a^{-i}) g^i(a^i, a^{-i})$$

The following lemma, which will be used later, states that interim individual rationality always holds at a communication equilibrium.

**Lemma 1** *$ME(\Gamma) \subseteq INTIR(\Gamma)$.*

**Proof**

Let $q$ be a communication equilibrium and $l^i \in L^i$ be a type of player $i$; for any $b^i \in A^i$ and $\hat{l}^i \in L^i$,

$$G^i[q|l^i] = \sum_{l^{-i}} p(l^{-i}|l^i) \sum_a q(a|l^i, l^{-i}) g^i((l^i, l^{-i}), a) \geq$$

$$\sum_{l^{-i}} p(l^{-i}|l^i) \sum_{a^i, a^{-i}} q(a^i, a^{-i}|\hat{l}^i, l^{-i}) g^i((l^i, l^{-i}), (b^i, a^{-i})) =$$

$$\sum_{l^{-i}} p(l^{-i}|l^i) \sum_{a^{-i}} q(a^{-i}|\hat{l}^i, l^{-i}) g^i((l^i, l^{-i}), (b^i, a^{-i}))$$

Hence one can set $y^{-i}(a^{-i}|l^{-i}) = q(a^{-i}|\hat{l}^i, l^{-i})$ for some $\hat{l}^i \in L^i$ as punishment.■

Observe that, in the previous proof, "punishment" is mostly a convenient terminology. More precisely, consider the following strategy of player $i$ in $\Gamma^q$: at stage 2, he reports type $\hat{l}^i$ whatever his type; at stage 5, he plays an arbitrary action $b^i$, independently of the recommendation of the communication device. This strategy of player $i$ can be interpreted as "non-participation". If player $j = -i$ plays the strategy $y^{-i}$ in the previous proof, player $i$'s payoff is the same as when he does not participate.

# 3 Cheap talk game, correlated equilibrium

In this section, we first extend the basic game $\Gamma \equiv < \{L^i, A^i, g^i\}_{i=1,2}, p >$ by means of a long cheap talk phase; then we define correlated equilibria in this extended game.

Let $M$ be a finite set of messages; let $c$ ("continue") and $s$ ("stop") be two additional messages available to the players. We define the multistage game $ext_M\Gamma$ as follows:

Stage 0: every player $i$ learns his type $l^i$ as in $\Gamma$, $i = 1, 2$.

Stage 1: the players simultaneously send the message $c$ or $s$ to each other. If they both selected $c$, they simultaneously send a message in $M$ to each other and they proceed to stage 2. Otherwise, every player $i$ chooses an action in $A^i$, payoffs are given as in $\Gamma$, the game stops.

Stage $t$ ($t = 2, 3, ...$): if the game has not stopped at an earlier stage, the players simultaneously send the message $c$ or $s$ to each other. If they both selected $c$, they simultaneously send a message in $M$ to each other and they proceed to stage $t + 1$. Otherwise, every player $i$ chooses an action in $A^i$, payoffs are given as in $\Gamma$, the game stops.

The previous scenario fully describes the players' possible moves in the game $ext_M\Gamma$, and the payoffs if the moves make the game stop at some stage $t$. The scenario also allows the game to go on forever, which is unavoidable if the length of communication is not fixed in advance (see, e.g., Forges (1990a), Gossner and Vieille (2001), Aumann and Hart (2003)). We thus have to define the payoffs in the case of infinitely long cheap talk, even if this event will typically be off the equilibrium path. Since there is no particular outcome to be identified in our general Bayesian game, we assume, as Gossner and Vieille (2001) and Aumann and Hart (2003), that, if communication goes on forever, the players make their decisions "at infinity".

Let $H_t = (M \times M)^{t-1}$, $t = 1, 2, ...$, be the set of all pairs of messages in $M$ possibly sent before stage $t$ and let $H_\infty = (M \times M)^{\mathbb{N}}$. We provide these sets with a measurable structure, in the standard way: let $\mathcal{H}_t$ be the algebra over $H_\infty$ generated by cylinder sets of the form $h_{t-1} \times H_\infty$, where $h_{t-1}$ is a sequence in $H_t$. Let $\mathcal{H}_\infty$ be the $\sigma$-algebra over $H_\infty$ generated by the algebras $\mathcal{H}_t, t = 1, 2, ...$ Finally, $N = \{\{1\}, \{2\}, \{1, 2\}\}$ describes the sets of players possibly choosing $s$ at some stage.

A pure strategy $\sigma^i$ for player $i$ $(i = 1, 2)$ in $ext_M\Gamma$ is a sequence of measurable mappings, $\sigma^i = [(\delta^i_t, m^i_t, d^i_t)_{t\geq 1}, d^i_\infty]$, where

$$\delta^i_t : L^i \times H_t \to \{c, s\}, \quad m^i_t : L^i \times H_t \to M, \qquad t = 1, 2, ...$$

$$d^i_t : L^i \times H_t \times N \to A^i,\ t = 1, 2, ... \quad d^i_\infty : L^i \times H_\infty \to A^i$$

These mappings are interpreted as follows: $\delta^i_t$ describes player $i$'s decision to continue or stop at stage $t$ if the game is still going on at that stage, $m^i_t$ describes which message in $M$ he sends if both players have decided to continue at stage $t$, $d^i_t$ describes the action he chooses according to which player(s) decided to stop at stage $t$; $d^i_\infty$ describes the action he chooses if communication goes on forever.

Let $\sigma = (\sigma^1, \sigma^2)$ be a pair of pure strategies in $ext_M\Gamma$ and let $l = (l^1, l^2)$ be a pair of types chosen at stage 0. If, for these types $l$, $\sigma$ induces the game to stop at stage $t$, namely if $\sigma$ leads one of the player to choose $s$ at stage $t$, as a function of the past history, then the payoffs associated with $l$ and $\sigma$ are computed using the mappings $d^i_t$ and the utility functions $g^i$. If for these types $l$, $\sigma$ induces cheap talk to last forever, the payoffs associated with $l$ and $\sigma$ are computed in a similar way, using the mappings $d^i_\infty$. Payoffs in $ext_M\Gamma$ are thus well-defined and the definition of the game is complete.

As explained in the introduction, the players cannot hope to implement all communication equilibrium outcomes of $\Gamma$ by cheap talk, namely as equilibrium outcomes of $ext_M\Gamma$ for some set of messages $M$, without randomizing their strategies in a correlated way.

A correlation device consists of a probability space $(\Omega, \mathcal{B}, \mu)$, together with sub-$\sigma$-algebras $\mathcal{B}^1$ and $\mathcal{B}^2$ of $\mathcal{B}$. $(\Omega, \mathcal{B}, \mu)$ represents extraneous events ("sunspots"), which happen independently of $\Gamma$ (and $ext_M\Gamma$), in particular independently of the types in $L$; $\mathcal{B}^i$, $i = 1, 2$, represents player $i$'s private information on the extraneous events. In order to achieve our implementation goal, we shall only make use of simple and well-behaved correlation devices, typically describing discrete random variables.

By adding a correlation device $[(\Omega, \mathcal{B}, \mu), \mathcal{B}^1, \mathcal{B}^2]$ to $ext_M\Gamma$, we get a new extended game, $(ext_M\Gamma)^\mu$, in which before stage 1 of $ext_M\Gamma$, every player $i$ gets private information in $\mathcal{B}^i$ on an extraneous event, selected in $(\Omega, \mathcal{B})$ according to $\mu$. This lottery can take place before or after stage 0, but is independent of the players' prior $p$. In $(ext_M\Gamma)^\mu$, every player $i$ makes his strategic choices as a function of his extraneous information, described by $\mathcal{B}^i$ $(i = 1, 2)$. Proceeding as in Aumann and Hart (2003), a pure strategy

$\boldsymbol{\sigma}^i$ for player $i$ ($i = 1, 2$) in $(ext_M\Gamma)^\mu$ is a sequence $\boldsymbol{\sigma}^i = [(\boldsymbol{\delta}^i_t, \mathbf{m}^i_t, \mathbf{d}^i_t)_{t\geq 1}, \mathbf{d}^i_\infty]$ of $L^i \times \mathcal{H}_t \times \mathcal{B}^i$-measurable mappings describing player $i$'s move at stage $t$ (including $\infty$), where

$$\boldsymbol{\delta}^i_t : L^i \times H_t \times \Omega \to \{c, s\}, \quad \mathbf{m}^i_t : L^i \times H_t \times \Omega \to M, \qquad t = 1, 2, ...$$

$$\mathbf{d}^i_t : L^i \times H_t \times N \times \Omega \to A^i, \; t = 1, 2, ... \quad \mathbf{d}^i_\infty : L^i \times H_\infty \times \Omega \to A^i$$

**Definition 3** *A correlated equilibrium of $ext_M\Gamma$ is a Nash equilibrium of $(ext_M\Gamma)^\mu$, for some correlation device $[(\Omega, \mathcal{B}, \mu), \mathcal{B}^1, \mathcal{B}^2]$. $CE(ext_M\Gamma)$ denotes the set ($\subset \mathbb{R}^{|L^1 \times L^2|}$) of all correlated equilibrium payoffs of $ext_M\Gamma$.*

# 4 Implementing communication equilibria by cheap talk

In this section, we first state the main theorem, in terms of the standard correlated equilibrium solution concept. After having deduced two immediate corollaries, we give a sketch of the proof, which clarifies the use of unboundedly long cheap talk and indicates the role of punishments. We then turn to "approximate implementation" with finitely long cheap talk (proposition 1). Finally, we give sufficient conditions for implementation in sequentially rational strategies (proposition 2).

The prior probability distribution $p$ over $L$, the probability distribution $\mu$ of a correlation device and strategies $(\boldsymbol{\sigma}^1, \boldsymbol{\sigma}^2)$ in $ext_M\Gamma$ induce a probability distribution over $\Omega \times L \times H_\infty \times A$ and thus also conditional probability distributions over $A$, given every $l \in L$.

**Theorem 1** *Let $\Gamma \equiv < \{L^i, A^i, g^i\}_{i=1,2}, p >$ be a two-person finite Bayesian game and $q$ be a communication equilibrium of $\Gamma$ such that $G[q] \in SINTIR(\Gamma)$. There exist a finite set of messages $M$ and a correlated equilibrium of $ext_M(\Gamma)$, the cheap talk extension of $\Gamma$ with messages in $M$, which induces the conditional probability distribution $q(.|l^1, l^2)$ over actions (i.e., over $A^1 \times A^2$) for every pair of types $(l^1, l^2) \in L^1 \times L^2$; in particular, the payoff of the correlated equilibrium is $G[q]$. Moreover, the correlated equilibrium of $ext_M(\Gamma)$ is such that cheap talk lasts for finitely many stages almost surely.*

In this statement, the set of messages depends on the parameters of $\Gamma$ and of $q$. If we allow for countably many messages, i.e., if we consider the extended cheap talk game $ext\Gamma$ in which $M = \mathbb{N}$, we can get all strictly individually rational communication equilibrium payoffs at once: $ME(\Gamma) \cap SINTIR(\Gamma) \subseteq CE(ext\Gamma)$. Recall that, by lemma 1, $ME(\Gamma) \subseteq INTIR(\Gamma)$; the restriction imposed on communication equilibrium outcomes is thus a relatively mild one. Conversely, by proceeding as in general versions of the revelation principle, one can show that $CE(ext\Gamma) \subseteq ME(\Gamma)$. Hence we get the following corollary[11]:

**Corollary 1** $ME(\Gamma) \cap SINTIR(\Gamma) = CE(ext\Gamma) \cap SINTIR(\Gamma)$

Remark that, once $\mathbb{N}$ is the set of messages, cheap talk in $ext\Gamma$ is described in a universal way, i.e., independently of the underlying Bayesian game $\Gamma$, as in Forges (1990b).

Corollary 1 can be interpreted as a characterization of the correlated equilibrium payoffs of the long cheap talk game $ext\Gamma$, since it states that $CE(ext\Gamma)$ and $ME(\Gamma)$ essentially coincide[12]. In order to make the relationship between the two sets more precise, let us denote the closure of $CE(ext\Gamma)$ as $\overline{CE(ext\Gamma)}$.

**Corollary 2** *If* $ME(\Gamma) \cap SINTIR(\Gamma) \neq \emptyset$, $\overline{CE(ext\Gamma)} = ME(\Gamma)$.

**Proof of corollary 2**

$ME(\Gamma)$ being closed, $\overline{CE(ext\Gamma)} \subseteq ME(\Gamma)$. In order to see the converse, we show that, if $ME(\Gamma) \cap SINTIR(\Gamma) \neq \emptyset$, then $ME(\Gamma) \subseteq \overline{ME(\Gamma) \cap SINTIR(\Gamma)}$. Let $x \in ME(\Gamma)$. By lemma 1, $x \in INTIR(\Gamma)$; let $x^* \in ME(\Gamma) \cap SINTIR(\Gamma)$, let $\alpha_n$ be a sequence in $(0,1)$ such that $\alpha_n \to 1$ and let $x_n = \alpha_n x + (1-\alpha_n)x^*$. $ME(\Gamma)$ being convex, $x_n \in ME(\Gamma)$ and from the inequalities in definition 2, it is readily checked that $x_n \in SINTIR(\Gamma)$; finally, $x_n \to x$.■

**Sketch of the proof of theorem 1**

Let $q$ be a communication equilibrium of $\Gamma$. We gradually construct a set of messages $M$, a correlation device $\mu$ for $ext_M(\Gamma)$ and equilibrium strategies

[11] In this statement and the next ones, we do not recall that $\Gamma$ is a finite two-person Bayesian game.

[12] Aumann and Hart (2003) show that, even if only one of the players has private information in $\Gamma$ (if, e.g., $|L^2| = 1$), the characterization of the *Nash* equilibrium payoffs of the game $ext\Gamma$ is fairly complex, as it relies on the martingales generated by the long cheap talk. On the contrary, most correlated equilibrium payoffs of $ext\Gamma$ are characterized in a tractable way, as communication equilibrium payoffs of the original Bayesian game $\Gamma$.

in $(ext_M\Gamma)^\mu$ which induce the transition probability $q$. The correlation device $\mu$ first selects, independently for every $l \in L$, a pair of actions $a_l = (a_l^1, a_l^2) \in A$ according to $q(.|l)$. If the players could reveal their types to each other, the correlation device could send them $(a_l)_{l \in L}$ before the beginning of $\Gamma$.

In order to keep the correlated equilibrium conditions as close as possible to the communication equilibrium conditions, the correlation device $\mu$ selects permutations $\eta^i$ of $L^i$ $(i = 1, 2)$ to encrypt player $i$'s type $l^i$ and permutations $\phi^i_{\eta(l)}$ of $A^i$ $(i = 1, 2,\ l \in L)$ to encrypt player $i$'s recommended action $a^i_{\eta(l)}$. Before the beginning of $\Gamma$, the device tells player $i$ how to encrypt his type (namely, $\eta^i$) and how to decrypt his recommended action (namely, $\phi^i_{\eta(l)}$, $l \in L$). Every player's encrypted, recommended action is transmitted by the other player. More precisely, the correlation device tells to player $i$ the encrypted actions $b^j_{\eta(l)} = \phi^j_{\eta(l)}(a^j_{\eta(l)})$, $l \in L$, $j \neq i$.

At the first stage of cheap talk, the players can simultaneously send their encrypted type to each other; let $\eta(l)$ be the pair of messages. Let us imagine that, at a second stage of cheap talk, the players send simultaneously the corresponding encrypted actions $b^j_{\eta(l)}$ to each other. The communication equilibrium conditions guarantee that a player cannot gain in lying on his type at the first stage nor on deviating (at the decision stage) from the action $(\phi^i_{\eta(l)})^{-1}(b^i_{\eta(l)})$ that he decrypts at the second stage. In other words, at this point, the correlation device mimics $q$.

However, the communication equilibrium conditions do not ensure that a player correctly transmits the encrypted action of the other player at the second stage. To fill this gap, the correlation device $\mu$ chooses a "code" $k^i(\eta(l), a^i)$ in some large set, independently and uniformly, for every pair of encrypted types $\eta(l)$ and every possible action $a^i$, $i = 1, 2$. The correlation device tells to player $i$ the whole mapping $k^i$ but only $k^j(\eta(l), b^j_{\eta(l)})$, $l \in L$, for $j \neq i$. If, given a pair of messages $\eta(l)$, player $i$ transmits $a^j \neq b^j_{\eta(l)}$ to player $j$, he will, with high probability, not guess correctly the corresponding code $k^j(\eta(l), a^j)$. In this case, he will be detected and punished by player $j$.[13]

The equilibrium strategies suggested in the previous paragraph raise two problems. The first one, which is not typical of our construction (see, e.g., Bárány (1992) and Heller et al. (2011)), is that punishments may appear as incredible threats. We will come back to this below. The second and most

[13] Similar codes were used in Forges (1990b) in order to allow a player to check with high probability whether another player correctly transmits information generated by a correlation device.

important issue is that, if player $i$ unilaterally deviates at the second stage of cheap talk and does not transmit the correct encrypted, recommended action $b^j_{\eta(l)}$ to player $j$, player $i$ typically receives a correct recommendation at the same stage. Player $i$ may thus have updated his beliefs in such a way that player $j$ cannot maintain player $i$'s payoff below the communication equilibrium payoff.[14]

In order to solve the second problem, we do not fix the number of stages of cheap talk in $ext_M(\Gamma)$. Encrypted types are still exchanged only once at the first stage, but the correlation device $\mu$ chooses a relevant stage $t^\star \geq 2$ according to a geometric distribution. The previous encrypted, recommended actions, whose distribution is determined by $q$, are selected for stage $t^\star$ only. For all stages $t \neq t^\star$, the correlation device $\mu$ selects encrypted, recommended actions uniformly. Codes are selected at every stage $t$, as described above.

The key is that the players only discover whether stage $t$ ($\geq 2$) is relevant or not, i.e., whether $t = t^\star$, at the end of stage $t$, after having exchanged messages. If one of the player $j$ detects an incorrect code in player $i$'s message at the end of stage $t$, then, with high probability, $t \neq t^\star$, so that player $i$'s belief over $L$ is still the prior $p$ and player $j$ can punish player $i$ (strictly) below his communication equilibrium payoff (which belongs to $SINTIR(\Gamma)$). Strict punishment takes care of the small probability that deviation luckily happens at $t^\star$.

There remains to explain how the players discover whether $t = t^\star$ at the end of every stage $t \geq 2$. The correlation device $\mu$ selects "labels" $\lambda^i_t$ such that $\lambda^1_t = \lambda^2_t$ if and only if $t = t^\star$. By exchanging their labels at the same time as the encrypted, recommended actions and their codes, the players can recognize $t^\star$. In order to prevent cheating on the labels, codes are associated to the labels as well. For every $t \geq 2$, the correlation device $\mu$ tells to player $i$ the code $\kappa^i(t, \lambda^i_t)$ of his own label $\lambda^i_t$ at stage $t$, together with the whole mapping $\kappa^j(t, .)$. This completes the description of the correlation device $\mu$. Regarding strategies, if player $j$ detects an incorrect label code in player $i$'s message, player $j$ punishes player $i$.■

Theorem 1 is proved in full details in section 6. In particular, we show how to compute precisely the size of the set of messages $M$ and the parameter of the geometric distribution choosing $t^\star$.

[14] Ben-Porath (2003) identifies this issue in games with three players or more, but does not provide a thorough solution (see Ben-Porath (2006)). We illustrate the difficulty on a two-person game in section 5.

**Approximation with finite cheap talk**

Theorem 1 is stated in terms of the *infinitely* long cheap talk game $ext_M(\Gamma)$. For $T \geq 2$, let us denote as $ext_M^T(\Gamma)$ the extension of $\Gamma$ in which the players cannot talk for more than $T$ stages. In section 5, we show on an example that there may exist a communication equilibrium payoff which cannot be achieved as a correlated equilibrium payoff of $ext_M^T(\Gamma)$, for any $T$. A natural question is thus whether every communication equilibrium payoff of a Bayesian game $\Gamma$ can be *approximated* by a correlated equilibrium payoff of a *sufficiently long* cheap talk game extending $\Gamma$. A positive answer is given in the following proposition and illustrated in section 5. The result is formally established after the proof of theorem 1, in section 6.

**Proposition 1** *Let us assume that* $\Gamma$ *has a Bayesian-Nash equilibrium payoff which belongs to* $SINTIR(\Gamma)$. *Let* $x = G[q] \in ME(\Gamma) \cap SINTIR(\Gamma)$ *and let* $\delta > 0$*; there exist a finite set of messages* $M$*, a finite number of stages* $T$ *and a payoff vector* $x_\delta$ $\delta-$*close to* $x$ *such that* $x_\delta \in CE(ext_M^T\Gamma)$.

**Implementation in sequentially rational strategies**

The proof of theorem 1 makes use of punishment strategies which may not be "credible", in the sense that they apply to any communication equilibrium payoff in $SINTIR(\Gamma)$ and are thus akin to minmax strategies. A standard way to guarantee credible punishments is to focus on communication equilibrium payoffs that are not only strictly individually rational, but even dominate a Bayesian-Nash equilibrium. Ben-Porath (2003, 2006) studies the implementation of such particular communication equilibria in Bayesian games with three players or more.

**Definition 4** *A payoff vector* $((x^i(l^i))_{l^i \in L^i})_{i=1,2} \in \mathbb{R}^{|L^1 \times L^2|}$ *in* $\Gamma$ *is Nash-dominating if there exists a Bayesian-Nash equilibrium payoff* $\xi = (\xi^i(l^i)_{l^i \in L^i})_{i=1,2}$ *in* $\Gamma$ *such that*

$$x^i(l^i) > \xi^i(l^i) \quad \text{for every } i = 1,2 \text{ and } l^i \in L^i.$$

For Nash-dominating payoffs[15], theorem 1 can be restated in terms of a version of the *perfect Bayesian equilibrium* (PBE) solution concept, which

[15] Nash domination is by no means a necessary condition as illustrated for instance by the sender-receiver case (see Forges (1985) and section 7.2).

we call *semi-weak* PBE[16]. More precisely, we require sequential rationality at every information set and Bayesian updating on the equilibrium path as in the *weak* PBE (see, e.g., Mas Colell et al. (1995) or Myerson (1991), who refers to "weak sequential equilibrium"). We further impose a natural restriction on the players' beliefs out off equilibrium path, in the vein of the condition of "action-determined beliefs" of Osborne and Rubinstein (1994) (see also Fudenberg and Tirole (1991)), which we define precisely below, after the statement of proposition 2.

**Proposition 2** *Let us assume that the prior $p$ of $\Gamma \equiv < \{L^i, A^i, g^i\}_{i=1,2}, p >$ has full support and that $x = G[q] \in ME(\Gamma)$ is Nash-dominating. There exist a finite set of messages $M$ and a correlation device $[(\Omega, \mathcal{B}, \mu), \mathcal{B}^1, \mathcal{B}^2]$ for $ext_M(\Gamma)$ such that $x$ is a semi-weak perfect Bayesian equilibrium payoff of $(ext_M\Gamma)^\mu$.*

The reason to restrict to a prior $p$ with full support is well explained in Gerardi (2004). As his example 1 illustrates, without full support of the prior $p$ in $\Gamma$, there may exist communication equilibria that can only be achieved by means of a communication device recommending a strictly dominated action to one of the players when a type profile of zero probability under $p$ is reported. Such communication equilibria cannot be implemented with sequentially rational strategies, even if the implementation process does not rely on any punishment.

In order to make precise the condition on beliefs behind our semi-weak PBE, let $\boldsymbol{\sigma}$ be an equilibrium of $(ext_M\Gamma)^\mu$ and let $h_{t-1}$ be a sequence of messages before stage $t$, i.e., $h_{t-1} \in H_t = (M \times M)^{t-1}$; let $m_t = (m_t^1, m_t^2)$ be a pair of messages at stage $t$. Assume that the probability of $h_{t-1}$ given $l^i$ and $\mathcal{B}^i$ is positive under the distribution induced by $p$, $\mu$ and $\boldsymbol{\sigma}$. Then the belief of player $i$ over $L^j$ given $l^i$, $\mathcal{B}^i$, $h_{t-1}$ and $m_t$ does not depend on $m_t^i$. This condition guarantees that, in the previous sketch of the proof of theorem 1, a "lucky deviator" (who does not transmit the correct encrypted action to the other player at stage $t$, but correctly guesses its code and then dicovers that $t^\star = t$) updates his belief on the other player's type.

[16] We limit ourselves to strengthening the rationality of the specific equilibrium strategies constructed in the proof of theorem 1, without addressing the question of an appropriate definition of refined correlated equilibrium (see, e.g., Dhillon and Mertens (1996) for a discussion of this topic).

In section 6.3., we establish proposition 2 by using the same correlation device $[(\Omega, \mathcal{B}, \mu), \mathcal{B}^1, \mathcal{B}^2]$ and the same set $M$ of messages as in the proof of theorem 1.

# 5 An example

We consider a variant of the "secret sharing" problem, which is well-known in computer science (see for instance Abraham et al. (2008)). The secret sharing game $\Gamma$ will be derived from an auxiliary game $\hat{\Gamma}$, in which both players have two equally likely possible types in $S^1 = S^2 = \{0, 1\}$, to be referred to as "payoff types". The payoff types of the players are chosen independently of each other. Every player has two possible actions: $A^1 = A^2 = \{0, 1\}$; the payoff functions $g^i : S^1 \times S^2 \times A^1 \times A^2 \to \mathbb{R}$, $i = 1, 2$, are summarized in the following table:

| $g$ | $s^2$ | 0 | | 1 | |
|---|---|---|---|---|---|
| $s^1$ | $A$ | 0 | 1 | 0 | 1 |
| | 0 | $3, 3$ | $6, -2$ | $0, 0$ | $-2, 6$ |
| 0 | 1 | $-2, 6$ | $0, 0$ | $6, -2$ | $3, 3$ |
| | 0 | $0, 0$ | $-2, 6$ | $3, 3$ | $6, -2$ |
| 1 | 1 | $6, -2$ | $3, 3$ | $-2, 6$ | $0, 0$ |

The interpretation is as follows : the secret is $s = s^1 + s^2$ ($mod$ 2). Given the secret $s \in \{0, 1\}$, the "right" (resp., "wrong") action is to play according to the secret, namely $a^i = s$ (resp., $a^i \neq s$); both players have the same preferences: being the only one to take the right action is preferred to both taking the right action, which is preferred to both taking the wrong action, which is itself preferred to being the only one to take the wrong action.

In the game $\hat{\Gamma}$, the pair of expected payoffs $(3, 3)$ can only be achieved as a completely revealing outcome, in which both players take the right action[17]. But complete revelation cannot be achieved at a communication *equilibrium* of $\hat{\Gamma}$: every player can gain in lying unilaterally about his payoff type in order to be the only one to take the right action.

[17] In order to see this, let $q(.|l)$, $l \in L$, be conditional probability distributions over actions given types achieving the pair of expected payoffs $(3, 3)$ in the game $\hat{\Gamma}$. Every $q(.|l)$ is a distribution over the *same* payoffs $\{(0, 0), (-2, 6), (3, 3), (6, -2)\}$, in which $(3, 3)$ is an extreme point.

We now modify $\hat{\Gamma}$ into a more complex game $\Gamma$. In $\Gamma$, the payoff type of every player is enriched into a "full type", which is highly correlated to the full type of the other player. More precisely, player $i$'s type in $\Gamma$ is denoted as $l^i$ and consists of a $4-$tuple; the first component of $l^i$ is player $i$'s payoff type $s^i$. In order to define the other three components of $l^i$, let $E$ be a finite set, and let $|E|$ denote the number of elements in $E$. $E$ will be interpreted as a set of "codes". The sets of types in $\Gamma$ are $L^i = \{0,1\} \times E \times E \times E$, $i = 1, 2$. In $\Gamma$, nature first makes the following choices:

1. a pair of payoff types $(s^1, s^2)$, as in $\hat{\Gamma}$

2. 4 codes $e_0^1, e_1^1, e_0^2, e_1^2$ in $E$, independently of each other, with probability $\frac{1}{|E|}$ each.

Player $i$'s type is $l^i = (s^i, e^i_{s^i}, e_0^{-i}, e_1^{-i})$, $i = 1, 2$, i.e., player $i$ is informed of his payoff type $s^i$, of the code $e^i_{s^i} \in E$ of his payoff type $s^i$ and of the codes $e_0^{-i}$ and $e_1^{-i}$ of the two possible payoff types of the other player. Player $i$ is not informed of the code of the other possible payoff type he might have, nor on the payoff type of the other player, of course. The action sets and the payoff functions in $\Gamma$ are the same as in $\hat{\Gamma}$, in the sense that payoffs only depend on payoff types and actions.

If player $i$ can talk to the other player $j = -i$ and wants to reveal his payoff type $s^i$ to him, player $i$ also sends the code $e^i_{s^i}$, so that player $j$, who knows the code of the two possible payoff types of player $i$, namely, $e_0^i$ and $e_1^i$, can check that player $i$'s reported payoff type is consistent with the codes. If player $i$ wants to lie on his payoff type, he has to guess the corresponding code, with a probability of $1 - \frac{1}{|E|}$ of being detected by player $j$.[18]

Even if no communication device is available, every player can detect a lie of the other with high probability, by checking the codes, but this typically happens *after* that useful information has been transmitted. The situation is very different when there is a communication device. In this case, the device does not release any information when it detects cheating, which protects the honest player. This effect cannot be simulated at a Nash equilibrium of a cheap talk game extending $\Gamma$.

[18] The technique of codes is also useful in the proof of theorem 1. However, in the current example, codes are not generated by a correlation device but as part of the types in the Bayesian game.

Let us show that the vector of conditional expected payoffs $((3,3),(3,3)) \in ME(\Gamma)$. For that, we describe a canonical communication device $q : L \rightarrow \Delta A$. Every player $i$, $i = 1, 2$, reports a type $(r^i, e^i, \varepsilon_0^{-i}, \varepsilon_1^{-i})$ to the communication device $q$, which then recommends actions as follows:

1. if $e^i = \varepsilon^i_{r^i}$ and $e^j = \varepsilon^j_{r^j}$, $q$ computes $r = r^1 + r^2$ $(mod\ 2)$ and sets $a^1 = a^2 = r$.

2. otherwise, $q$ chooses an action profile $(a^1, a^2)$ uniformly.

Let us check that $q$ defines a communication equilibrium. Assume that player $j$ is honest and obedient and consider player $i = -j$ with type $(s^i, e^i_{s^i}, e_0^{-i}, e_1^{-i})$. Suppose first that $r^i \neq s^i$, namely that player $i$ lies on his component of the secret. Player $i$ has no information on the code $e^i_{r^i}$, which has been chosen with probability $\frac{1}{|E|}$ in $E$; he will thus guess it correctly with probability $\frac{1}{|E|}$. In this case, the device recommends actions $a^1 = a^2 = r^i + s^j$; by playing against the recommendation of the device, player $i$ gets the highest possible payoff, 6. Otherwise, if player $i$ does not guess $e^i_{r^i}$ correctly, the device selects actions uniformly, and player $i$ can as well play against the recommendation of the device. His total expected payoff is $\frac{1}{|E|} \times 6 + (1 - \frac{1}{|E|}) \times \left[\frac{1}{4} \times 3 + \frac{1}{4} \times 6 + \frac{1}{4} \times (-2)\right]$, which is $< 3$ as soon as $|E| \geq 4$. All other possible deviations of player $i$, e.g., involving cheating in the other player's codes, either give rise to a higher probability of being detected and reduce his expected payoff, or have no effect on the payoffs. As we already observed above, while completely revealing in terms of the payoff types (in $S^1 \times S^2$), the communication equilibrium expected payoff $(3,3)$ cannot be achieved as a *Nash* equilibrium of a cheap talk game like $ext_M\Gamma$.

The vector of conditional expected payoffs $((3,3),(3,3))$ is in $SINTIR(\Gamma)$: by playing both actions with probability $\frac{1}{2}$, independently of his type, player $j$ guarantees that player $i = -j$'s payoff does not exceed $\frac{7}{4}$, whathever his type and his action[19]. Obviously, this punishment depends on the fact that player $i$ does not know player $j$'s share of the secret. By theorem 1, $((3,3),(3,3))$ can thus be achieved as a correlated equilibrium of a long cheap talk game $ext_M\Gamma$, for some finite set of messages $M$. We show below that in any extended cheap talk game in which the number of stages is fixed, the players cannot reach $((3,3),(3,3))$.

[19] In fact, the strategies consisting of playing both actions with the same probability, independently of the type, form a Bayesian-Nash equilibrium.

Let us fix an extension $ext_M^T\Gamma$ of $\Gamma$ in which the cheap talk phase cannot exceed $T$ stages. Every stage $t = 0, 1, ..., T$ of $ext_M^T\Gamma$ can be described as in $ext_M\Gamma$, for some set $M$ of messages, but the moves in $\{c, s\}$ are not necessary: the game goes on for $T + 1$ stages, with final decisions at stage $T + 1$, whatever the history[20]. Let us assume that $ext_M^T\Gamma$ has a correlated equilibrium achieving the expected payoff $(3, 3)$, namely complete revelation of the secret. At the last stage $T$, both players must know the secret on every possible history on the equilibrium path. Without loss of generality, this does not happen at stage $T - 1$, otherwise the deadline could be $T - 1$.

Thus, at the end of stage $T-1$, there exists a history $\mathbf{h}_{T-1} = (l, \omega, h_{T-1})$, where $h_{T-1}$ is the sequence of messages up to stage $T-1$, which has positive probability at equilibrium, for which at least one of the players, say player 1, does not know the secret, namely, player 1's posterior probability that player 2's type is 0 *is not* 0 *or* 1. Hence, on $\mathbf{h}_{T-1}$, player 1 relies on player 2's message at stage $T$ to learn the secret. Note that the history $\mathbf{h}_{T-1}$ involves the choice $\omega = (\omega^1, \omega^2)$ of the underlying correlation device, hence is not necessarily fully identified by player 2. But player 2 can select his message uniformly, independently of the past, at stage $T$. If player 2 deviates in this way (only at stage $T$), while player 1 does not deviate, player 2 learns the secret at stage $T$, on every possible history, while player 1 does not learn it at least on $\mathbf{h}_{T-1}$. In the next paragraph, we complete player 2's deviation by describing how he chooses his action and we show that his deviation is profitable.

At the end of stage $T - 1$, player 2's information consists of his type $l^2$, the private extraneous signal from the correlation device $\omega^2$ and the messages exchanged at stages $1, ..., T - 1$. Given his information, player 2 determines the message $m_T^2$ he should send at stage $T$ as if he did not deviate. Since there is no deviation at any stage $1, ..., T - 1$, player 1 sends his message $m_T^1$ at stage $T$ as in equilibrium. Even if player 2 deviates at stage $T$, he has the same information, at the end of stage $T$, as when he does not deviate. In particular, $m_T^1$ and $m_T^2$ are part of player 2's information. We complete his deviation as follows: after having sent his (uniformly selected) message $\widetilde{m}_T^2$ to player 1 and having received player 1's message $m_T^1$, he chooses his action in $A^2$ according to his equilibrium strategy as if the messages at stage $T$ were $(m_T^1, m_T^2)$. This guarantees him a payoff strictly higher than 3 if the history $\mathbf{h}_{T-1}$ identified above occurs and no less than 3 otherwise. Hence player 2's

[20] Hence, on some histories, cheap talk may become vacuous from some stage on.

deviation is profitable.

The constructive proof of theorem 1 avoids the obstacles of a bounded cheap talk phase, by introducing extra uncertainty for the players about the time $t^\star$ at which they reveal their part of the secret to each other. In such a construction, the number of conversation stages cannot be deterministically bounded. Nevertheless, in equilibrium, the players stop talking with probability one. The probability that a deviator can affect the conversation in a way that it lasts forever can be made arbitrarily small. The main idea is that, at every stage $t$, player $i$, say, does not know whether $t = t^\star$, i.e., whether he will receive useful information from player $j = -i$ at that stage. Hence player $i$ may not have any incentive to send a message which differs from the one prescribed by the correlation device. In particular, in our construction, with large probability, a deviation of player $i$ is detected by player $j$ before that player $i$ learns the secret, so that player $j$ can stop the conversation and punish player $i$ in the initial Bayesian game $\Gamma$, with prior $p$.

To sum up, the proof of theorem 1 will confirm that, in the secret sharing game, the players learn the secret with probability 1 after a random finite number $t^\star$ of stages of correlated cheap talk (namely, $x = ((3,3),(3,3)) \in CE(ext_M\Gamma)$). We have shown that this result cannot be true if $t^\star$ is imposed not to exceed a fixed, deterministic bound $T$, i.e., that $x \notin \cup_{T\geq 1} CE(ext_M^T\Gamma)$. The requirement that the players learn the secret *with probability 1* is essential to this observation, as will follow from proposition 1. To see that this proposition applies to the secret sharing game, let us set $\xi = ((2,2),(2,2))$. $\xi$ is the payoff of a Bayesian-Nash equilibrium, in which one of the players chooses the action 0, independently of his type, and the other player chooses the action 1, independently of his type. Furthermore, $\xi \in SINTIR(\Gamma)$, since as noticed above, every player can guarantee that the other's interim expected payoff does not exceed $\frac{7}{4}$. Thus, from proposition 1, for every $\delta > 0$, there is a finite number of stages $T$ such that the game $ext_M^T\Gamma$ has a correlated equilibrium at which the players learn the secret with probability at least $1-\delta$ and thus get approximately the desired payoff $x$, i.e., for every $\delta > 0$, there exist a finite number of stages $T$ and $x_\delta$ $\delta-$close to $x$ such that $x_\delta \in CE(ext_M^T\Gamma)$. Finally, observe also that the payoff $x$ Nash-dominates $\xi$ (or $((\frac{7}{4},\frac{7}{4}),(\frac{7}{4},\frac{7}{4}))$) so that, by proposition 2, it can be achieved with sequentially rational strategies.

# 6 Proof of the results

## 6.1 Proof of theorem 1

Let us fix a communication equilibrium $q$ of $\Gamma$, such that $G[q] \in SINTIR(\Gamma)$. We shall construct a set of messages $M$ and a correlated equilibrium of $ext_M\Gamma$ which satisfy the requirements of the theorem. The precise size of $M$ will be determined when we check the equilibrium conditions. We start by describing a correlation device, namely a probability space $(\Omega, \mathcal{B}, \mu)$, and private signals for every player, namely sub-$\sigma$-algebras $\mathcal{B}^1$ and $\mathcal{B}^2$; then we define the players' strategies.

*Items selected by the correlation device:* $(\Omega, \mathcal{B}, \mu)$

We make a list of the items selected by the correlation device. Unless specified otherwise, these items are selected uniformly in the finite set to which they belong and they are all selected independently of each other.

The correlation device selects:

1. for $i = 1, 2$, a permutation $\eta^i$ of $L^i$; let $\eta = (\eta^1, \eta^2)$ and $\eta(l) = (\eta^1(l^1), \eta^2(l^2))$, for every $l = (l^1, l^2) \in L$;
2. a stage $t^\star \in \{2, 3, ...\}$, according to a geometric distribution with success parameter $z > 0$ to be specified later;
3. for every $l \in L$, a pair of actions $a_{t^\star,\eta(l)} \in A$, according to $q(.|l)$;
4. for every $l \in L$ and every $t \in \{2, 3, ...\}$, $t \neq t^\star$, a pair of actions $a_{t,\eta(l)} \in A$;
5. for $i = 1, 2$, every $l \in L$ and every $t \in \{2, 3, ...\}$, a permutation $\phi^i_{t,\eta(l)}$ of $A^i$; let us set $b^i_{t,\eta(l)} = \phi^i_{t,\eta(l)}(a^i_{t,\eta(l)})$;
6. for $i = 1, 2$, every $l \in L$, every action $b^i \in A^i$ and every $t \in \{2, 3, ...\}$, a "code" $k^i(t, \eta(l), b^i) \in M$;
7. for $i = 1, 2$ and every $t \in \{2, 3, ...\}$, a pair of "labels" $\lambda^i_t \in M$ such that $\lambda^1_{t^\star} = \lambda^2_{t^\star}$ and $\lambda^1_t \neq \lambda^2_t$ if $t \neq t^\star$;
8. for $i = 1, 2$, every $l \in L$, every $t \in \{2, 3, ...\}$ and every label $\lambda \in M$, a "code" $\kappa^i(t, \lambda) \in M$.

To sum up, only $t^\star$ in 2. and $a_{t^\star,\eta(l)}$, $l \in L$, in 3. are selected according to a specific, non-uniform probability distribution. The stage $t^\star$ is the only random variable which is not finite. In 7., the labels $\lambda_t^1$ and $\lambda_t^2$ at stage $t$ are not independent from each other, nor from $t$. The parameter $z$ represents the probability that $t^\star$ be the next stage; $z$ and the size of $M$ will be computed at the end of the proof (see the expression (4) below).

*Private extraneous information:* $\mathcal{B}^i$, $i = 1, 2$.

The correlation device sends the following private signal[21] to player $i$, $i = 1, 2$:

- the permutation $\eta^i$ of $L^i$ selected in 1.
- the permutations $\phi^i_{t,\eta(l)}$ of $A^i$, $l \in L$, $t \in \{2, 3, ...\}$ selected in 5.
- the (encrypted, recommended) actions (for the other player, $-i$) $b^{-i}_{t,\eta(l)} \in A^{-i}$ for every $l \in L$, $t \in \{2, 3, ...\}$ defined in 5, together with their associated code $k^{-i}(t, \eta(l), b^{-i}_{t,\eta(l)})$ selected in 6.
- the code functions $k^i(t, \eta(l), .) : A^i \to M$ for every $l \in L$, $t \in \{2, 3, ...\}$, selected in 6.
- the labels $\lambda^i_t$, $t \in \{2, 3, ...\}$ selected in 7., together with their associated code $\kappa^i(t, \lambda^i_t)$ selected in 8.
- the code functions (of the other player, $-i$) $\kappa^{-i}(t, .) : M \to M$ for every $t \in \{2, 3, ...\}$, selected in 8.

We denote player $i$'s private signal as

$$\omega^i = \begin{bmatrix} \eta^i \\ (\phi^i_{t,\eta(l)})_{t\geq 2, l\in L} \\ (b^{-i}_{t,\eta(l)}, k^{-i}(t, \eta(l), b^{-i}_{t,\eta(l)}), k^i(t, \eta(l), .))_{t\geq 2, l\in L} \\ (\lambda^i_t, \kappa^i(t, \lambda^i_t), \kappa^{-i}(t, .))_{t\geq 2} \end{bmatrix} \tag{2}$$

At this point, the description of the game $(ext_M\Gamma)^\mu$ is complete.

[21] It is understood that functions over $L = L^1 \times L^2$ are described as $L^1 \times L^2$ tables, for a given order on $L^1$ and $L^2$.

*Equilibrium strategies* $(\boldsymbol{\sigma}^1, \boldsymbol{\sigma}^2)$ in $(ext_M\Gamma)^\mu$

We first give a rough description of the strategies $(\boldsymbol{\sigma}^1, \boldsymbol{\sigma}^2)$ and of the way in which they combine with each other. The basic idea is that the geometric random variable $t^\star$ describes the only relevant stage, in which players determine the actions $a^i_{t^\star,\eta(l)}$, $i = 1, 2$, to be played in the Bayesian game. For every $l$, the pair of actions $a_{t^\star,\eta(l)}$ selected in 3. is distributed according to $q(.|l)$. However, the players cannot fully reveal their types to each other nor know more than their own action. Hence permutations are applied both to the types ($\eta^i$, selected in 1.) and to the actions ($\phi^i_{t^\star,\eta(l)}$, selected in 5.). At stage 1, the players send hidden types, $\eta^i(l^i)$, $i = 1, 2$, to each other. At stage $t^\star$, every player $i$ sends the message $b^{-i}_{t^\star,\eta(l)}$ to the other player. If player $i$ indeed receives the message $b^i_{t^\star,\eta(l)}$ from the other player, he is able to evaluate his action as $a^i_{t^\star,\eta(l)} = ({\phi^i}_{t^\star,\eta(l)})^{-1}(b^i_{t^\star,\eta(l)})$, by applying the inverse of the permutation ${\phi^i}_{t^\star,\eta(l)}$, and this action will be distributed as in the communication equilibrium. There remains to make every player able to identify $t^\star$, *only after* having transmitted his recommended action $b^{-i}_{t^\star,\eta(l)}$ to the other player. This is the role of the labels selected in 7. By construction, as in the communication equilibrium, player $i$ will not gain by pretending another type at stage 1 or deviating from his recommended action $a^i_{t^\star,\eta(l)}$. But player $i$ must transmit a recommended action $b^{-i}_{t^\star,\eta(l)}$ to the other player, which has no counterpart in the communication equilibrium. This is the role of the codes[22] selected in 6. In order to prevent cheating in the labels, further codes are needed, selected in 8. We detail the equilibrium strategies in the next paragraph.

Given his private extraneous signal $\omega^i$ described above, player $i$'s equilibrium strategy in $ext_M\Gamma$ is as follows:

- at stage 1, player $i$ chooses $c$; if both players select $c$, player $i$ announces $\eta^i(l^i)$ if his type is $l^i$; otherwise, he plays a punishment action against the other player and the game stops (recall that $G[q] \in SINTIR(\Gamma)$, so that player $i$ can select a punishment[23] according to some $y^i(.|l^i) \in$

[22] Restricted to two stages, $t = 1$ and $t^\star$ chosen deterministically equal to 2, the correlation device is a variant of the one used in Forges (1990b) in the case of three players.

[23] To be consistent with our definition of strategies in $(ext_M\Gamma)^\mu$, in which all randomizations are made by the correlation device, possible punishment strategies should in fact be selected by the correlation device.

$\Delta A^{-i}$); let $\eta(l)$ be the pair of announcements at the first stage (if $(c, c)$ was chosen).

- at stage 2, player $i$ chooses $c$

- at every stage $t \geq 2$, if both players select $c$, player $i$ sends the message:

$$b^{-i}_{t,\eta(l)}, k^{-i}(t, \eta(l), b^{-i}_{t,\eta(l)}), \lambda^i_t, \kappa^i(t, \lambda^i_t)$$

- at stage 2, if $(c, c)$ was not selected, player $i$ punishes the other player, as in stage 1.

- at every stage $t \geq 2$, if $(c, c)$ was selected, then, right after having received the other player's last message, player $i$ checks whether the latter is consistent with the codes, namely that player $-i$'s announcement $(b^i_t, k^i_t, \lambda^{-i}_t, \kappa^{-i}_t)$ satisfies:

$$k^i_t = k^i(t, \eta(l), b^i_t), \kappa^{-i}_t = \kappa^{-i}(t, \lambda^{-i}_t)$$

  If these equalities do not hold at stage $t$, player $i$ stops the cheap talk, that is, he chooses $s$ at the beginning of stage $t+1$ and plays a punishment action against the other player as above.

- at every stage $t \geq 2$, if $(c, c)$ was selected, player $i$ also checks whether his label $\lambda^i_t$ coincides with the label sent by the other player, namely whether $\lambda^i_t = \lambda^{-i}_t$. If yes, and no deviation was detected, player $i$ concludes that $t = t^\star$; he chooses to stop (namely, $s$) at the beginning of stage $t+1$, the cheap talk ends and player $i$ determines his action $a^i$ by applying the inverse of the permutation ${\phi^i}_{t,\eta(l)}$ (which he received from the correlation device) to the message $b^i_t$ (which he received from the other player):

$$({\phi^i}_{t,\eta(l)})^{-1}(b^i_t) = a^i$$

- if, at the beginning of some stage $t \geq 3$, player $i$ chooses $c$ but the other player $j$ $(= -i)$ chooses $s$, player $i$ punishes player $j$ as above.

- should cheap talk last forever, $\mathbf{d}^i_\infty$ $(i = 1, 2)$ could be defined in an arbitrary way.

To sum up, if both players follow the prescribed strategies, the conversation lasts for at least 2 stages. Stage 1 is the only stage where the players send a type dependent message, but posteriors are not updated until stage $t^\star$ is reached. Stages $t \geq 2$ are used for possible coordination. Coordination happens when $\lambda_t^1 = \lambda_t^2$, namely when $t = t^\star$; in this case, final decisions are made at stage $t^\star + 1$.

In order to check that the prescribed strategies form an equilibrium in the game $(ext_M\Gamma)^\mu$, we assume for simplicity that player 2 does not deviate in $(ext_M\Gamma)^\mu$ and consider possible deviations of player 1. Let $l^1$ be his type and $\omega^1$ be his extraneous signal, described as in (2). Since player 1's payoff $G^1[q]$ is individually rational, he cannot benefit from choosing $s$ at the beginning of stage 1 of $(ext_M\Gamma)^\mu$; let thus $\eta^1(\hat{l}^1)$ be his further message at stage 1, with $\hat{l}^1$ possibly different from $l^1$. We shall distinguish between several deviations of player 1. We start with deviations which are already feasible in the communication equilibrium and we show that they are unprofitable, namely, that the correlated equilibrium of $(ext_M\Gamma)^\mu$ "mimics" the communication equilibrium.

*Equilibrium conditions: undetectable deviations*

Let us assume that from stage 2 on, player 1 sends all his messages as prescribed by his correlated strategy. More precisely, let $t \geq 2$ be a stage t at which the conversation is still going on. Given our current assumptions, it must be that $\lambda_r^1 \neq \lambda_r^2$ for every stage $r$ such that $2 \leq r < t$. At the beginning of stage $t$, player 1 has not learnt anything on $t^\star$, player 2's type nor recommended actions, since all items that player 1 can interpret in $\omega^1$ have been selected uniformly (this holds in particular for *every* action $b^2_{t,\eta^1(\hat{l}^1),\eta^2(l^2)}$, including $b^2_{t^\star,\eta^1(\hat{l}^1),\eta^2(l^2)}$, which is obtained by applying a random permutation to $a^2_{t,\eta^1(\hat{l}^1),\eta^2(l^2)}$). Furthermore, at the beginning of stage $t$, given $\omega^1$ and the sequence of moves in $(ext_M\Gamma)^\mu$ up to stage $t$ (including his first move $\eta^1(\hat{l}^1)$), player 1 anticipates that the pair of actions to be determined (but not necessarily played) at the further stage $t^\star$ will be

$$({\phi^i}_{t^\star,\eta^1(\hat{l}^1),\eta^2(l^2)})^{-1}(b^i_{t^\star,\eta^1(\hat{l}^1),\eta^2(l^2)}) = a^i_{t^\star,\eta^1(\hat{l}^1),\eta^2(l^2)} \quad i = 1, 2 \tag{3}$$

By construction, given player 1's information at the beginning of stage $t$, this pair of actions is distributed according to $q(.|\hat{l}^1, l^2)$. In other words, if player 2 does not deviate and player 1 of type $l^1$ sends $\eta^1(\hat{l}^1)$ at the first stage and all his other messages as prescribed, the actions computed by the players at stage $t^\star$, namely (3), are distributed exactly as the actions recommended by the communication device $q$ when player 1's reported type is $\hat{l}^1$ and player 2's type is $l^2$. Hence player 1 will not deviate at the first stage by lying on his type and/or at $t^\star + 1$ by choosing another action than the one computed in (3).

The previous paragraph also shows that, if both players follow the prescribed strategies at every stage, the conditional probability distribution over actions (i.e., over $A^1 \times A^2$) given types $(l^1, l^2) \in S^1 \times S^2$ is $q(.|l^1, l^2)$; in particular, the expected payoffs are $G[q]$.

We consider further possible deviations of player 1.

*Equilibrium conditions: deviations which are detectable with high probability*

Let $l^1$, $\omega^1$ and $\hat{l}^1$ be as above. As already observed for stage 1, if player 2 does not deviate, player 1 cannot gain in sending his messages as prescribed and choosing $s$ at the beginning of a stage at which he should choose $c$, since his payoff $G^1[q]$ is individually rational.

As above, let us consider a stage $t$ at which the conversation is still going on; assume that player 1 does not send (at least one of) the prescribed variables $b^2_{t,\eta^1(\hat{l}^1),\eta^2(l^2)}$ and $\lambda^1_t$ in his message to player 2. Then, since the codes are chosen uniformly in $M$, the corresponding codes $k^2(t, \eta^1(\hat{l}^1), \eta^2(l^2), b^2_{t,\eta^1(\hat{l}^1),\eta^2(l^2)})$ and $\kappa^1(t, \lambda^1_t)$, will be incorrect with probability (at least) $1-1/|M|$, in which case player 2 will detect an inconsistency, stop the conversation and choose his action according to a "punishment" strategy $y^2(.|l^2)$. If it turns out that $\lambda^1_t \neq \lambda^2_t$, player 1 will not have learnt anything; in particular his probability distribution over $L^2$ will still be $p(.|l^1)$. In this case, player 2 can pick the strategy $y^2(.|l^2)$ in such a way that player 1's payoff does not exceed $G^1[q|l^1] - \epsilon$, for some $\epsilon > 0$, since $G^1[q]$ is *strictly* individually rational in the original game $\Gamma$ (whose parameters involve the prior $p$). However, if $\lambda^1_t = \lambda^2_t$, so that $t = t^\star$, player 1 acquires new information; the effect of the "punishment" strategy becomes unclear, except for the fact that player 1's payoff cannot exceed the largest possible payoff in the game $\Gamma$, which we denote by $\alpha$. Finally, if player 1's deviation is not detected, his payoff can also be bounded by $\alpha$ (in this case, the conversation could be infinite). By recalling that, at every stage $t$ at which the game has not yet stopped, the probability that $t = t^\star$ is $z$, we compute the following upper bound on player 1's payoff $G^1_{dev}(l^1)$ when he deviates as described above:

$$G^1_{dev}(l^1) \leq (1 - 1/|M|)(z\alpha + (1-z)(G^1[q|l^1] - \epsilon)) + \alpha/|M| \qquad (4)$$

If the set $M$ of messages[24] is large enough and the probability $z > 0$ is small enough, the previous bound will not exceed $G^1[q|l^1]$, namely

$$G^1_{dev}(l^1) \leq G^1[q|l^1]$$

We have thus shown that the correlated strategies described above form an equilibrium of the game $(ext_M\Gamma)^\mu$ which achieves the conditional probability distributions $q(.|l)$ of the communication equilibrium, in particular, the payoff $G\,[q]$. At equilibrium, given the geometric distribution of $t^\star$, the conversation ends with probability one.■

## 6.2 Proof of proposition 1

Let $\xi$ be a Bayesian Nash equilibrium payoff such that $\xi \in SINTIR(\Gamma)$ and let $x \in ME(\Gamma) \cap SINTIR(\Gamma)$. There exists $\epsilon > 0$ such that player $i$ ($i = 1, 2$) has strategies $y^i_x$ and $y^i_\xi$ to punish player $j = -i$ in $\Gamma$ at the payoff vectors $(x^j(l^j) - \epsilon)_{l^j \in L^j}$ and $(\xi^j(l^j) - \epsilon)_{l^j \in L^j}$, respectively.

Let $\delta$ be given; let us choose $\rho \in (0, 1)$ such that

$$x_\delta \equiv (1 - \rho)x + \rho\xi$$

is $\delta-$close to $x$ (i.e., $\rho||\xi - x|| \leq \delta$).

We temporarily fix $T$. Let the correlation device make its choices as in the proof of theorem 1, in particular, let $t^\star$ be chosen as in 2., according to a geometric distribution with parameter $z$ (which is also fixed for the moment) and let actions be chosen as in 3., using $q$. Let player $i$'s prescribed strategy be as in the proof of theorem 1 as long as he does not detect any deviation, and if he deduces that $t^\star \leq T$. Let player $i$ play the Bayesian Nash equilibrium strategy associated with payoff $\xi$ if he detects no deviation until stage $T$ and concludes that $t^\star$ will be $> T$.

If the players follow the previous strategies, the expected payoff of player $j$ of type $l^j$, just before stage $t$, i.e., conditionally on $t^\star \geq t$, is

$$x^j_t(l^j) = x^j_t(z, T)(l^j) \equiv (1 - (1 - z)^{T-t+1})x^j(l^j) + (1 - z)^{T-t+1}\xi^j(l^j) \quad (5)$$

By the above properties of $x$ and $\xi$, player $i$ can punish player $j = -i$ at the payoff vector $(x^j_t(l^j) - \epsilon)_{l^j \in L^j}$ if player $j$ deviates at stage $t$, for every

[24] The bound (4) reflects the required size of $M$ as far as codes are concerned. The set $M$ should of course be also large enough to contain the other messages to be transmitted by the players (i.e., $|M| \geq \max\{|L^i|, |A^i|, i = 1, 2\}$).

$t \leq T$, by playing $y^i_x$ with probability $1-(1-z)^{T-t+1}$ and $y^i_\xi$ with probability $(1-z)^{T-t+1}$. Hence, by proceeding as in (4), if player $j$ deviates at stage $t$, his expected payoff cannot exceed

$$(1 - 1/|M|)(z\alpha + (1 - z)(x^j_t(l^j) - \epsilon)) + \alpha/|M|$$

We can choose $|M|$ and $z$ (as a function of $\epsilon$) in such a way that, for every $j, l^j$ and $t \leq T$, this bound be $\leq x^j_t(l^j)$.[25] This guarantees that no player can gain in deviating at any stage $t \leq T$. The corresponding equilibrium payoff is computed from (5) at $t = 1$. More precisely, we choose $z' < z$ and $T = T(z')$ such that $x_1(z', T) = x_1(z', T(z')) = x_\delta$, i.e., $\rho = (1 - z')^T$.■

**Remark: the assumption $\xi \in SINTIR(\Gamma)$ in proposition 1**

In the previous proof it is an essential assumption that $\xi \in SINTIR(\Gamma)$. Intuitively, just before the last stage of the game, i.e., when $t = T$, the players' equilibrium expected payoff becomes $x_T(z, T) = zx + (1 - z)\xi$ (omitting the indices $j$, $l^j$). If $\xi$ itself is in $SINTIR(\Gamma)$, we can choose the level of punishment to be $x_T - \epsilon$. When choosing $z$ to be sufficiently small the difference between the equilibrium payoff and the punishment stays constant at $\epsilon$. If $\xi \in INTIR(\Gamma) \setminus SINTIR(\Gamma)$, by proceeding as in corollary 2, $x_T(z, T)$ can still be supported by strict punishment, namely by $v_T = z(x - \epsilon) + (1-z)\xi$. However, in this case the difference $x_T(z, T) - v_T = z\epsilon$ converges to 0 as $z$ goes to 0. Hence choosing a smaller $z$ decreases the effectiveness of punishment, which in turn necessitates the choice of an even smaller $z$.

## 6.3 Proof of proposition 2

Let us fix a communication equilibrium $q$ of $\Gamma$ such that the associated payoff $G[q]$ is Nash-dominating, namely higher than the expected payoff of some Nash equilibrium $\zeta = (\zeta^1, \zeta^2)$ of $\Gamma$, for every type of every player. Let us consider the set of messages $M$ and the correlation device $\mu$ constructed in the proof of theorem 1; $\mu$ induces a scenario, namely, a prescribed plan of actions for every player. As in the proof of theorem 1, player $i$'s strategy $\boldsymbol{\sigma}^i$ in $ext_M(\Gamma)^\mu$ will first consist of following the prescribed plan of actions and of punishing player $j = -i$ if it appears that player $j$ did not follow the plan

[25] More precisely, $\forall\ \epsilon > 0\ \exists\ |M| \in \mathbb{N}$, $\exists\ 0 < z < 1$ such that for *any* feasible payoff $\gamma$ in $\Gamma$, $(1 - 1/|M|)\,[z\alpha + (1 - z)(\gamma - \epsilon)] + \alpha/|M| \leq \gamma$.

$(i = 1, 2)$[26]. Player $i$ will now play $\zeta^i$ if he has to punish the other player, but we have to further complete the description of strategies and beliefs in order to show that they form a semi-weak PBE. $\boldsymbol{\sigma}^i$ will consist of stopping the game and choosing an action in $\Gamma$ according to $\zeta^i$ at basically *all* information sets such that the prescribed plan of actions was not followed at some earlier stage, possibly by the player who has to move at that information set[27]. Such a specification of $\boldsymbol{\sigma}^i$ makes player $i$'s strategy sequentially rational provided that player $i$'s belief over $L^j$ is his prior and that he expects that player $j$ will play $\zeta^j$. There is only one class of information sets out off the equilibrium path at which the underlying player will update his belief over the other player's type. In the next paragraph, we describe these information sets for player $i$ and how $\boldsymbol{\sigma}^i$ operates at them.

Let $t \geq 2$. Assume that player $i$ followed the prescribed plan of actions at all stages $< t$ but does not follow it at stage $t$. Assume also that player $i$ observed correct codes in player $j$'s messages at all stages $\leq t$ and that player $j$'s reported label at stage $t$, $\lambda_t^j$, coincides with the label $\lambda_t^i$ that player $i$ received from the correlation device $\mu$. At such an information set, player $j$'s moves are exactly the same as on the equilibrium path. Since our semi-weak PBE requires that player $i$'s beliefs on player $j$'s type $l^j$ does not depend on player $i$'s own last move, player $i$ must update his belief over $L^j$. We also assume that player $i$ believes that player $j$ will detect his deviation and will thus punish him immediately, by stopping the game at the beginning of stage $t+1$ and playing $\zeta^j$. Note that semi-weak PBE does not restrict player $i$'s belief over $\omega^j$, so that player $i$ can indeed believe that his deviation is detected with probability 1, even if $M$ is finite. In order that player $i$ be sequentially rational at the described information set, $\boldsymbol{\sigma}^i$ specifies that he stops the game and plays a best response against $\zeta^j$ *given his updated belief* over $L^j$.

If at some stage, player $i$ updates his belief in the way just described and

[26] Player $i$ detects that player $j$ has deviated from the plan typically when he receives an incorrect code. If $q$ is such that some actions of player $i$ have zero probability given his type, player $i$ may also detect a deviation of player $j$ from his computed action when he concludes that $t^\star$ has been reached. We focus on the typical case but the second one can be handled similarly.

[27] To be complete, we must also consider the case of information sets occurring at the second substage of some stage $t \geq 2$, after that both players chose "continue" while the prescribed plan of actions was not followed at an earlier stage. In this case, $\boldsymbol{\sigma}^i$ prescribes to choose a message uniformly and to stop at the next stage.

the game goes on, even for infinitely many stages, player $i$ keeps his belief over $L^j$ without modifying it any further. At all other information sets out off the equilibrium path, player $i$ does not update his belief over $L^j$, stops the game and plays $\zeta^i$. In particular, consider the following situation: player $i$ first deviates at some stage $t$, then concludes that $t^\star > t$, but the game nevertheless goes on until stage $t' > t$ and player $i$ again deviates at stage $t'$; even if the labels at stage $t'$ lead player $i$ to the conclusion that $t^\star = t'$, player $i$ does not update his beliefs over $L^j$ at $t'$, stops the game and plays $\zeta^i$.[28]

Consider now the typical case where player $i$ followed the plan of actions induced by $\mu$ at all stages $\leq t$, for some $t \geq 2$, and discovers, through the codes that he receives from player $j$, that player $j$ did not follow the plan at stage $t$. This must be player $j$'s first observed defection since otherwise player $i$, who followed the scenario, would have stopped the game. As soon as player $j$ deviated from the prescribed scenario, no constraint must be imposed on player $i$'s belief over $L^j$, which can thus be kept at the prior. In particular, even if only player $j$'s code on player $i$'s encrypted action is incorrect while player $j$'s reported label $\lambda_t^j$ coincides with the label $\lambda_t^i$ that player $i$ received from the correlation device, player $i$ can believe that player $j$'s reported label $\lambda_t^j$ is in fact incorrect and that player $j$ luckily picked his label code. As a consequence, player $i$ can believe that player $j$ did not update his belief over $L^i$ and expects that player $j$ will play $\zeta^j$. Recall that, as detailed above, it is indeed sequentially rational for player $j$ to stop the game and play $\zeta^j$ after his deviation in this case. With these beliefs, player $i$ is sequentially rational by stopping the game at the beginning of stage $t+1$ and punishing player $j$ using $\zeta^i$.

The reasoning of the previous paragraphs can be applied to any information set occurring after some finite stage $t \geq 2$. Let us come to the case where cheap talk never stops. If player $i$ always followed the prescribed plan of actions, it means that he did not detect any incorrect code but could not identify $t^\star$. Player $j$ must thus have deviated from the prescribed scenario, say at stage $t'$, by not reporting the correct $\lambda_{t'}^j$, and must have been lucky in picking the associated code. Player $i$'s belief over $L^j$ is still the prior and furthermore, player $i$ can expect that player $j$ will play $\zeta^j$ because player $j$

[28] Player $i$'s beliefs over $L^j$ at stage $t'$ are not restricted by our semi-weak PBE but are coherent with the belief that player $j$ detected player $i$'s first deviation at stage $t$, failed to punish player $i$ and chose messages uniformly from then on.

himself did not update his belief over $L^i$. Indeed, player $i$ can believe that player $j$'s first deviation occurred at some stage $t < t'$ such that, just after stage $t$, player $j$ deduced that $t^\star > t$; player $j$ expected to be punished by player $i$ at stage $t+1$ and having realized that player $i$ did not follow the plan, player $j$ did not update his belief at stage $t'$ (player $i$'s belief is coherent with the fact that player $j$ only updates his belief over $L^i$ at his first deviation, as explained above). Finally, assume again that cheap talk never stops and that player $i$ did not follow the plan at some stage $t$. If he updated his belief over $L^j$ at the corresponding information set as described above, he kept this belief since stage $t$ and plays a best response against $\zeta^j$ given this belief. Otherwise, he plays $\zeta^i$.■

# 7 Discussion: variants of the model

We start with a variant of the strategic form correlated equilibria considered up to now. Then we consider two particular cases in which theorem 1 takes a much simpler form. Finally, we address a question mostly motivated by Ben-Porath (2003, 2006).

## 7.1 Extensive form correlated equilibria

The proof of theorem 1 makes use of typical correlation devices for the long cheap talk game $ext_M\Gamma$, which select, before the beginning of the game, an *infinite* sequence of extraneous signals to be used gradually by the players. The corresponding correlated equilibria can be denoted as "strategic form correlated equilibria". What if the players do not have access to (or cannot generate[29]) infinite sequences of correlated extraneous signals, at once, at the beginning of the game? One could then consider *extensive form, autonomous* correlation devices which send one private signal to every player at every stage of $ext_M\Gamma$ (see Forges (2006) and Myerson (2006, 1991)). Such devices generate sunspots every day. They are independent of the cheap talk game, in the sense that they do not receive any input from the players and do not get any information on the players' messages. They thus preserve the

[29] Players can simulate finite correlation devices by themselves by using simple machines (like Turing machines, see Dodis, Halevy and Rabin (2000) and Urbano and Vila (2002)) or the AND signalling function (see Vida (2007b)).

players' privacy. The previous proof shows that theorem 1 still holds if "correlated equilibrium" is replaced by "extensive form, autonomous correlated equilibrium using *finitely* many signals at every stage". Corollary 1 also holds for the set $\widetilde{CE}(ext\Gamma)$ of extensive form, autonomous correlated equilibrium payoffs, since $CE(ext\Gamma) \subseteq \widetilde{CE}(ext\Gamma) \subseteq ME(\Gamma)$.

## 7.2 Sender-Receiver games

As a particular case, let us assume that only player 1 possesses private information ($|L^2| = 1$) and that only player 2 makes a decision ($|A^1| = 1$). Under these asumptions, the cheap talk game becomes a "sender-receiver" game, in which the length of the players' conversation is not fixed in advance (as in, e.g., Forges (1990a), Aumann and Hart (2003)[30], Forges and Koessler (2008)). We shall deduce from the proof of theorem 1 that $t^\star$ can be chosen in a deterministic way, as $t^\star = 1$. Let us set $L = L^1$ and $A = A^2$ and let us consider a correlation device as above, which selects the following items

1. a permutation $\eta$ of $L$;
2. for every $l \in L$, an action $a_{\eta(l)} \in A$, according to $q(.|l)$;
3. for every $l \in L$, a permutation $\phi_{\eta(l)}$ of $A$; let us set $b_{\eta(l)} = \phi_{\eta(l)}(a_{\eta(l)})$;
4. for every $l \in L$ and every action $b \in A$, a "code" $k(\eta(l), b) \in M$;

The correlation device transmits
to player 1: $\eta$ and $(b_{\eta(l)}, k(\eta(l), b_{\eta(l)}))_{l \in L}$
to player 2: $(\phi_{\eta(l)}, k(\eta(l), .))_{l \in L}$

Given the signal from the correlation device and his type $l$, player 1's equilibrium strategy is to send $\eta(l)$, $b_{\eta(l)}$ and $k(\eta(l), b_{\eta(l)})$ to player 2 at a single stage of information transmission. Given his private signal $(\phi_{\eta(l)}, k(\eta(l), .))_{l \in L}$ and player 1's message $(\hat{l}, b, m)$, player 2 checks whether the code is correct, namely that $m = k(\hat{l}, b)$; if it is the case, he chooses the action $(\phi_{\hat{l}})^{-1}(b)$; otherwise he chooses his action according to $q(.|l)$, for some arbitrary $l \in L$. By proceeding as above, one shows that these correlated strategies form an equilibrium, which is equivalent to the communication equilibrium $q$. Forges

[30] Aumann and Hart (2003) assume one sided private information, namely, $|L^2| = 1$, but allow both players to make decisions.

(1985, lemma 2) establishes a slightly stronger result, namely that *every* communication equilibrium payoff (even not in $SINTIR(\Gamma)$) can be achieved as a correlated equilibrium payoff of the cheap talk game. As already pointed out, Blume (2010) proves an analog in Crawford and Sobel (1982)'s model.

## 7.3 Uniform punishments

The proof of theorem 1 dramatically simplifies if the communication equilibrium payoff of $\Gamma$ to be implemented as a correlated equilibrium payoff of $ext_M\Gamma$ is higher than a punishment payoff that can be achieved *for every probability distribution* $p \in \Delta L$. This happens for instance if $\Gamma$ has a "bad outcome" that every player can enforce, *whatever the types are*.

More precisely, recalling expression (1), let $G[q] = (G^i[q|l^i]_{l^i \in L^i})_{i=1,2} \in ME(\Gamma)$ be a communication equilibrium payoff for which there exist $y^i : L^i \to \Delta A^i$, $i = 1, 2$, such that, for every $i = 1, 2$, $l = (l^i, l^{-i}) \in L$, $a^i \in A^i$,

$$G^i[q|l^i] \geq \sum_{a^{-i}} y^{-i}(a^{-i}|l^{-i}) g^i((l^i, l^{-i}), a^i, a^{-i})$$

Then, in the proof of theorem 1, in order to achieve $G[q]$ as a payoff in $CE(ext_M\Gamma)$, $t^\star$ can be chosen in a deterministic way, as $t^\star = 2$. The correlation device can dispense with selecting the labels and all items associated with $t > 2$. Indeed, if player $i$'s code $k^{-i}(2, \eta(l), b^{-i}_{2,\eta(l)})$ at stage 2 is not correct, player $-i$ can punish him by playing the strategy $y^{-i}$ in $\Gamma$, which guarantees that player $i$'s payoff does not exceed $G^i[q|l^i]$, *independently of the information that player $i$ may have acquired at stage* 2, i.e., even if player $i$ learns the type $l^{-i}$ of player $-i$.

However, in many interesting situations, when a player has obtained further information on the other's type, it becomes impossible to punish him below his communication equilibrium payoff. This is exactly what happens in the example of section 5 once a player knows the secret.

## 7.4 "Cheap talk" with delayed messages

The terminology "cheap talk" has been used to cover more or less sophisticated forms of communication between the players. In this paper, we just allow the players to talk for as long as they like by sending simultaneous messages to each other. Bárány (1992) and Ben-Porath (2006) consider more flexible procedures, like the safe recording, at some stage $t$, of a message that can possibly be released at some further stage $t'$, as a function of the history at stage $t'$.

If such a relaxed form of cheap talk is allowed in the framework of the current paper, the proof of theorem 1 can easily be modified so as to achieve every payoff in $ME(\Gamma) \cap SINTIR(\Gamma)$ with *only four stages of cheap talk*. To see this, let us slightly modify the correlation device of the proof of theorem 1 by chosing $t^\star$ uniformly in some finite set $T$ and interpreting it as an index (rather than a stage). At the first stage of cheap talk, the players exchange information $\eta(l)$ on their types as before. Then every player $i$ secretly prepares $|T|$ envelopes, with envelope $t$ containing the encrypted recommended action $b^{-i}_{t,\eta(l)}$ of the other player, its code $k^{-i}(t, \eta(l), b^{-i}_{t,\eta(l)})$ and player $i$'s code function $k^i(t, \eta(l), .)$. At the second stage of cheap talk, the players exchange their extraneous signals on the labels for all $t \in T$ at once (namely, $(\lambda^i_t, \kappa^i(t, \lambda^i_t), \kappa^{-i}(t, .))_{t \in T}$ ). If no deviation is detected at this stage, they identify the index $t^\star$. At the third stage of "cheap talk", they reveal to each other the content of all envelopes with index $t \neq t^\star$ and check that the codes are consistent. If again no deviation is detected, they open the two envelopes with index $t^\star$.

The conclusion from this exercise is that allowing delayed messages in cheap talk is by no means innocuous. Indeed, in section 5, we have exhibited a communication equilibrium payoff which cannot be achieved as a correlated equilibrium payoff of any game in which cheap talk lasts for a fixed number of stages and does not involve any delayed message.

# References


[1] Abraham, I., Dolev, D. and Halpern, J.Y. (2008), "Lower Bounds on Implementing Robust and Resilient Mediators", Proceedings of the Fifth Theory of Cryptography Conference, Springer-Verlag, 302-319, and mimeo, Cornell University.

[2] Aumann, R.J. (1974), "Subjectivity and Correlation in Randomized Strategies", *Journal of Mathematical Economics* **1**, 67-96.

[3] Aumann, R.J. (1987), "Correlated Equilibrium as an Expression of Bayesian Rationality", *Econometrica* **55**, 1-18.

[4] Aumann, R. J. and Hart, S. (1986), "Bi-convexity and Bi-martingales", *Israel Journal of Mathematics* **54**, 159-180.

[5] Aumann, R.J. and Hart, S. (2003) "Long Cheap Talk", *Econometrica* **71**, 1619-1660.

[6] Bárány, I. (1992), "Fair Distribution Protocols or how the Players Replace Fortune", *Mathematics of Operation Research* **17**, 327-340.

[7] Ben-Porath, E. (1998), "Correlation without Mediation: Expanding the Set of Equilibrium Outcomes by "Cheap" Pre-play Procedures", *Journal of Economic Theory* **80**, 108-122.

[8] Ben-Porath, E. (2003), "Cheap talk in Games with Incomplete Information", *Journal of Economic Theory*, **108**, 45-71.

[9] Ben-Porath, E. (2006) "Corrigendum: Cheap talk in Games with Incomplete Information", mimeo, Hebrew University of Jerusalem.

[10] Blume, A. (2010) "Correlated Equilibria in Sender-Receiver Games", mimeo, University of Pittsburgh.

[11] Crawford, V. and Sobel, J. (1982) "Strategic Information Transmission", *Econometrica* **50**, 1431-1451.

[12] Dhillon, A. and Mertens, J.-F., (1996), "Perfect Correlated Equilibria", *Journal of Economic Theory* **68**, 279-302.

[13] Dodis, Y. Halev, S. and Rabin, T. (2000), "A Cryptographic Solution to a Game Theoretic Problem", CRYPTO 2000: 20th International Cryptology Conference, Springer-Verlag, 112-130.

[14] Forges, F. (1985) "Correlated Equilibria in a Class of Repeated Games with Incomlete Information", *International Journal of Game Theory* **14**, 129-150.

[15] Forges, F. (1986) "An Approach to Communication Equilibria", *Econometrica* **54**, 1375-1385.

[16] Forges, F. (1988), "Can Sunspots Replace a Mediator?", *Journal of Mathematical Economics* **17**, 347-368.

[17] Forges, F. (1990a), "Equilibria with Communication: A Job Market Example", *Quarterly Journal of Economics* **105**, 375-398.

[18] Forges, F. (1990b), "Universal Mechanisms", *Econometrica* **58**, 1341-1364.

[19] Forges, F. (2009), "Correlated Equilibrium and Communication in Games", R. Meyers (ed.), *Encyclopedia of Complexity and Systems Science*, Springer.

[20] Forges, F. and Koessler, F. (2008), "Multistage Communication with and without Verifiable Types", *International Game Theory Review* **10**, 145-164.

[21] Fudenberg, D. and Tirole, J. (1991), *Game Theory*, MIT Press.

[22] Gerardi, D. (2004) "Unmediated Communication in Games with Complete and Incomplete Information", *Journal of Economic Theory* **114**, 104-131.

[23] Goltsman, M., Hörner, J., Pavlov, G. and Squintani, F. (2009), "Mediation, Arbitration and Negotiation", *Journal of Economic Theory* **144**, 1397-1420.

[24] Gossner, O. and Vieille, N. (2001) "Repeated Communication through the *and* Mechanism", *International Journal of Game Theory* **30**, 41-61.

[25] Green, J.R. and Stokey, N.L. (2007), "A Two-person Game of Information Transmission", *Journal of Economic Theory*, **135**, 90-104.

[26] Halpern, J.Y. (2008), "Computer Science and Game Theory: A Brief Survey", Palgrave Dictionary of Economics (S. N. Durlauf and L. E. Blume, eds.), Palgrave MacMillan.

[27] Hart, S. (1985), "Nonzero-sum Two-person Repeated Games with Incomplete Information", *Mathematics of Operations Research* **10**, 117-153.

[28] Heller, Y., Solan, E. and T. Tomala (2011), "Communication, Correlation and Cheap Talk in Games with Public Information", *Games and Economic Behavior*, forthcoming.

[29] Izmalkov, S., Lepinski, M. and Micali, S. (2010) "Perfect Implementation", *Games and Economic Behavior*, to appear.

[30] Krishna, V. and Morgan, J. (2004), "The Art of Conversation: Eliciting Information from Experts through Multi-stage Communication", *Journal of Economic Theory* **117**, 147-79.

[31] Krishna, R. V. (2007), "Communication in Games of Incomplete Information: two Players", *Journal of Economic Theory* **132**, 584-592.

[32] Mas Colell, A.,M. Whinston and J. Green (1995), *Microeconomic Theory*, Oxford University Press.

[33] Myerson, R.B. (1986), "Multistage Games with Communication", *Econometrica* **54**, 323-358.

[34] Myerson, R.B. (1991), "Game Theory: Analysis of Conflict", *Harvard University Press.*

[35] Osborne, M. and A. Rubinstein (1994), "A Course in Game Theory", *MIT Press.*

[36] Urbano, A. and Vila, J.E. (2002), "Computational Complexity and Communication: Coordination in Two-player Games", *Econometrica* **70**, 1893-1927.

[37] Urbano, A. and Vila, J.E. (2004), "Computationally Restricted Unmediated Talk under Incomplete Information", *Economic Theory* **23**, 283-320.

[38] Vida, P. (2006), "Long Pre-play Communication in Games", *Doctorate Thesis*, mimeo, Universitat Autònoma de Barcelona.

[39] Vida, P. (2007a), "From Communication Equilibria to Correlated Equilibria", mimeo, University of Vienna.

[40] Vida, P. (2007b), "A Detail-free Mediator", mimeo, University of Vienna.