Unmediated communication in games with (in)complete information: the 4-player case

Helmuts Āzacis, Marie Laclau, Péter Vida

Unmediated communication in games with (in)complete information: the 4-player case

Helmuts Āzacis[*], Marie Laclau,[†] and Péter Vida[‡]

January 17, 2025

Abstract

We show that essentially every correlated equilibrium of any finite game with complete information and four players can be implemented as a sequential equilibrium of an extended game, in which before choosing actions in the underlying game, players exchange cheap talk messages. In particular, we improve on the result of Bárány (1992) and Gerardi (2004). Our result can be generalized to games with incomplete information, i.e., to the set of regular communication equilibria.

Keywords: unmediated communication; sequential equilibrium; correlated equilibria; communication equilibria; communication protocols.

JEL Classification: C72; D82.

1 Introduction

A well-known result of game theory demonstrates that access to a trusted mediator can broaden the set of equilibrium outcomes in Bayesian games (Forges (1986); Myerson (1982)). In such settings, players can send messages to an impartial mediator, who then (randomly) generates private recommendations to communicate back to the players. This leads to the concept of correlated equilibrium (or communication equilibrium in the case of players with privately known types). This raises a natural question: under what conditions can a mediator

[*]Cardiff Business School, Cardiff University, Cardiff, UK and Corvinus University of Budapest, Institute of Economics, Budapest, Hungary. E-mail: azacish@cf.ac.uk

[†]HEC Paris and CNRS, 1 rue de la Libération, 78351 Jouy-en-Josas, France; laclau@hec.fr. Marie Laclau gratefully acknowledges the support of the French National Research Agency, under grant ANR CIGNE (ANR-15-CE38-0007-01), grant ANR StratCom (ANR-19-CE26-0010-01), and through ORA Project "Ambiguity in Dynamic Environments" (ANR-18-ORAR-0005), and the program Investissements d'Avenir (ANR-11-IDEX-0003/Labex Ecodec/ANR-11-LABX-0047).

[‡]Corresponding author: Université Cergy Pontoise, THEMA, 33 boulevard du Port, 95011 Cergy-Pontoise Cedex, France and Corvinus University of Budapest, CIAS; vidapet@gmail.com.

be effectively replaced by direct communication between players? By "direct communication", we refer to the exchange of cheap-talk (costless) messages among the players, possibly over several stages, prior to taking any actions. Unlike the mediated setup, this form of interaction relies solely on the players themselves and excludes the use of a trusted intermediary. The resulting multi-stage communication process is called a cheap-talk extension of the original static game. Our paper addresses this question for the case of four players assuming sequential rationality and consistency of beliefs in the multistage communication game.

Before presenting our results, let us highlight some related results in the literature (for an extensive overview, the reader is referred to the survey by Forges (2010)). Without sequential rationality, Bárány (1992) and Forges (1990) provide a complete characterization of unmediated communication when the solution concept is Nash equilibrium for games with four or more players: namely, they show that in games of at least four players, every (rational) correlated equilibrium outcome of a strategic form game can be achieved as a Nash equilibrium of a cheap-talk extension of the game with finitely many stages. However, Bárány (1992) assumes the existence of a recording machine (PVR)[1] and punishment strategies are used when a deviation is detected. Forges (1990) extends the analysis to the Nash implementation of communication equilibria.[2]

Assuming sequential rationality, Ben-Porath (2003) shows that, in games with at least three players, every rational communication equilibrium outcome can be achieved as a sequential equilibrium of a cheap-talk extension of the game with finitely many stages, provided that there exists a *Nash threat* (a Nash equilibrium that can be used to punish *all* players of *all* types when there is a deviation). Gerardi (2004) extends this result without assuming a Nash threat but considering games with at least five players. The case of four players was an open question until very recently, when Geffner and Halpern (2024) extended the result of Gerardi (2004) to the case of four players. (They also consider extensions where several players might deviate at the same time.) Their result relies on the use of two primitives as blackboxes: *verifiable secret sharing* (VSS) and *circuit computation* (CC). Though, they do not construct communication protocols verifying these primitives and refer to Ben-Or et al. (1988).

In this paper, we show that every rational correlated equilibrium of any finite game with complete information and four players can be implemented as a sequential equilibrium of cheap-talk extension with finitely many stages. More precisely, players communicate with each other

[1]Bárány (1992) assumes that *Public Verification of the Record (PVR)* is possible: at each stage, each player can ask for the revelation of all exchanged messages.

[2]Formally, Forges (1990) shows that every communication equilibrium outcome can be achieved as a correlated equilibrium of a two stage cheap-talk extension of the original Bayesian game. Combining this result with the fact that PVR is not necessary for Bárány's result (Ben-Or, Goldwasser, and Wigderson (1988); Vida (2007)), one gets that, in games of at least four players, every rational communication equilibrium outcome can be implemented as a Nash equilibrium of a cheap-talk extension of the game with finitely many stages.

for finitely many stages either through pairwise private communication channels and by making public announcements. Our result can be generalized to games with incomplete information, i.e., to the set of regular communication equilibria. Coming back to the existing literature, we do not assume the existence of a Nash threat like Ben-Porath (2003), nor a PVR like Bárány (1992). Unlike Bárány (1992), we impose sequential rationality and we are thus in the same setup as Gerardi (2004) but with four players, with the exception that we allow for public announcements in addition to private messages.[3] Finally, we assume that we have access to a large enough, but finite message space (defined by construction given our communication protocol).

Contrary to Geffner and Halpern (2024), our proof is completely constructive both in terms of strategies after on and off-path histories (even after multilateral deviations) as well as in terms of beliefs. We check the sequential rationality of players in each and every information set given the beliefs and the strategies of the other players. Our protocol satisfies the following properties. First, no player have incentives to deviate unilaterally from the prescribed (continuation) equilibrium strategies no matter in which information set she finds herself. Second, the protocol is *secure* (see Gossner (1998)), in the sense that even after any unilateral deviation, each player learns the correct action she is supposed to play afterwards and no player learns anything more about recommended actions of other players than what she learns when receiving her recommended action from the trusted third party. That is, even after unilateral deviation the given correlated equilibrium is still implemented.

The main insights of our communication protocol are as follows. First, we construct an auxiliary protocol which is a modification of Bárány's protocol (Bárány (1992)) using only private communication. Then, we use this auxiliary protocol to construct several other subprotocols which all will be parts of a grand protocol, where all the constructed protocols are assumed to be run simultaneously. Intuitively, the subprotocols are such that during the private communication phase, no player (even a deviator) is ever surprised until the first public communication phase in stage $n-1$ and, in some of the subprotocols, which we call checkable protocols, unilateral deviations are detected with probability one at stage $n-1$. However, the identity of the deviator may remain unknown. If there is no deviation detected in any one of the checkable protocols, then players can play according to this protocol. On the other hand, in case of deviations in all the checkable protocols, players are able to identity the deviator in stage n by truthfully and publicly reporting the private messages sent and received in the past in the checkable protocols. This is achieved by the means of checkable protocols $\mathcal{P}_{ij}$ designed for each pair of players i and j. These protocols are such that i and j do not exchange private messages with each other but they communicate through players k and l, and hence, they cannot contradict to each other. The intuition is that when there are two suspects of a deviation, i and j, the protocol $\mathcal{P}_{ij}$ can be

[3]Public messages can be replaced by very simple and secure broadcasting protocols using only private communication channels similar to byzantine agreement (see e.g. Lamport, Shostak, and Pease (1982)).

used to identify the deviator. Also, for every player i, there is a non-checkable subprotocol $\mathcal{P}_i$ in which player i is silent, i.e., does not send messages to anyone and hence, cannot manipulate that protocol. Intuitively, $\mathcal{P}_i$ will be used by the players when i has been identified as the deviator. The main difficulty is the construction of consistent beliefs off the equilibrium path, given the protocols, which gives incentives to the players to be truthful in stage n no matter in which information set they find themselves. The protocols in turn must be designed in such a way that these beliefs can be constructed. The key property of the beliefs that we use is that every player, even deviators, in any information set believe that the other players were not manipulating any of the protocols during the private communication.

The remaining of the paper is as follows. Section 2 introduces the model and the main result. Section 3 presents the construction of communication protocol and the proof of the main result. All proofs that are not in the text are in the Appendix. Important terms and definitions are *emphasized in blue*.

2 The setup and the main result

Let $\Gamma =< I = \{1,2,3,4\}, (A_i)_{i\in I}, (g_i)_{i\in I} >$ be a finite 4-player game of complete information, where $I = \{1,2,3,4\}$ is the set of players, A_i is the finite set of actions available to player $i \in I$, $A = \prod_{i\in I} A_i$ is the set of action profiles, and $g_i : A \to \mathbb{R}$ is the payoff function of player $i \in I$. We let $A_{-i} = \prod_{j\neq i} A_i$ denote the set of profiles of actions of players different from i. The set of probability distributions over a finite set X is denoted by $\Delta(X)$.

We consider the cheap talk extension of Γ, where before choosing actions in Γ (the action phase), players communicate with each other for finitely many stages either through pairwise private communication channels or by making public announcements (the communication phase). During the communication phase, players exchange "cheap" messages in that they do not affect directly their payoffs. More precisely, at each stage of the communication phase, each player simultaneously[4] sends private messages from a finite set $\mathcal{M}$ to all the other players, and make a public announcement from the same set $\mathcal{M}$. This specification of the extended game is without loss of generality, since players can send an "empty" message by mixing with positive probability among all the possible messages. The description of the set $\mathcal{M}$ will be part of the construction. A history of length $t \geq 0$ for player i is given by $h_i^{t-1} = (m^k_{-i,i}, m^k_{i,-i}, p^k)_{-1\leq k\leq t-1}$ where $m^k_{-i,i} = (m^k_{j,i})_{j\in I\setminus\{i\}}$ denotes the private messages received by player i from players $-i$, $m^k_{i,-i} = (m^k_{i,j})_{j\in I\setminus\{i\}}$ denotes the private messages sent by player i to players $-i$, $p^k = (p^k_j)_{j\in I}$ denotes the profile of public announcements made at stage

[4]This assumption is not necessary; only the penultimate and last stage of communication must be done simultaneously.

$k \geq 0$ by all players, and $(m_{-i,i}^{-1}, m_{i,-i}^{-1}, p^{-1}) \equiv \emptyset$. The set of histories of length t for player i is denoted by H_i^{t-1} with $H_i^{-1} = \{\emptyset\}$, and let $H^{t-1} = \prod_{i \in N} H_i^{t-1}$.

A communication protocol or a communication strategy profile $c = (c_i)_{i \in I}$ of length $n+1$, where $c_i = (c_i^0, \ldots, c_i^t, \ldots, c_i^n)$, specifies for each player i which private message to send to each player $m_{i,-i}^t \in \mathcal{M}^{I-1}$ and which public announcement to make $p_i^t \in \mathcal{M}$ at stage t for $0 \leq t \leq n$ given a history $h_i^{t-1} \in H_i^{t-1}$, that is, for each player i and each $t : 0 \leq t \leq n$, $c_i^t : H_i^{t-1} \to \Delta(\mathcal{M}^I)$.

In stage $n+1$ players choose actions according to the decision rule $d_i \ : \ H_i \to \Delta(A_i)$ in Γ as a function of the realized and observed communication history $h_i \in H_i$, where we use the abbreviations $h_i^n = h_i, H_i^n = H_i, H^n = H$. Let $d = (d_i)_{i \in I}$. Each player i then receives his payoff according to g_i. Clearly, there is an induced distribution on $H \times A$ which we denote by P.

Solution concept. Our solution concept is sequential equilibrium as defined in Kreps and Wilson (1982), henceforth SE.

Let $SE(\Gamma)$ be the set of outcomes in Γ induced by sequential equilibria of finite cheap talk extensions of Γ: a probability distribution $\mu \in \Delta(A)$ is in $SE(\Gamma)$ if and only if there exists a cheap-talk extension of Γ and a sequential equilibrium of that extension that induces μ.

A probability distribution $\mu \in \Delta(A)$ is a correlated equilibrium of Γ if and only if:

$$\sum_{a \in A} \mu(a) \left(g_i(a) - g_i(a_{-i}, \delta_i(a_i)) \right) \geq 0 \, \forall i \in I, \, \forall \delta_i \ : \ A_i \to A_i.$$

We say that a correlated equilibrium μ is *rational* if for every action profile in A, the probability $\mu(a)$ is a rational number. Let $C(\Gamma)$ be the set of rational correlated equilibria of Γ.

The main result. Our theorem is the following.

Theorem 1. *Let Γ be a finite normal-form game with four players, and let $\mu \in C(\Gamma)$. Then $\mu \in SE(\Gamma)$.*

Corollary 1. *Our result can be generalized to the case of incomplete information games, i.e., to the set of regular communication equilibria.*

Proof. The proof of the corollary can be found in the Appendix in section D. □

3 Proof of the theorem

The proof is constructive. First we introduce an auxiliary protocol à la Bárány (1992) and state some of its properties. Then we use this auxiliary protocol to construct several other

protocols which all will be parts of the grand protocol. When a public message of a player or his private message to another player at a certain stage is not specified then it is assumed that this player babbles, i.e., uses a completely mixed behavioral strategy over $\mathcal{M}$. $\mathcal{M}$ is chosen to be finite but large enough so that players can send all the messages specified by the equilibrium at once at any stage of the communication. Note however that most of the communication can be done sequentially (politely). We will point out those stages where simultaneity is important, basically the last two stages of the communication. The length of the communication phase is chosen to be large enough and is determined by the length of the longest protocol. It is because all the protocols are assumed to be run simultaneously. What is important however, is that their last two stages are performed simultaneously (within and across the protocols) at stages $n-1$ and n.

We summarize the important properties of the different protocols in several lemmas which are then used to prove that our construction is indeed a sequential equilibrium and that it induces the desired correlated equilibrium outcome. Importantly, we discuss players beliefs and equilibrium (continuation) strategies out of equilibrium as well.

Let $\mu \in \Delta A$ be an arbitrary correlated equilibrium distribution of Γ with rational entries. Let E be a finite set which is partitioned into $(E_a)_{a\in A}$ in such a way that $|E_a|/|E| = \mu(a)$ for all $a \in A$. For all $i \in I$ let $pr_i : E \to A_i$ be such that $pr_i(e) = a_i$ if and only if $e \in E_a$. Latin letters are elements of E (e.g. $e \in E$) and Greek letters are bijections (or permutations) from E to itself so their inverse exists. We write $\alpha\beta$ for the composition of two such functions (or the product of two permutations) and by abusing notation we write $\alpha e \in E$ denoting the image of e under α (i.e. instead of $\alpha(e)$). All random choices are specified to be uniform over the specified finite sets. From know on, let i, j, k, and l denote different players unless stated explicitly otherwise.

3.1 Auxiliary protocol à la Bárány (1992): $\mathcal{B}^+$

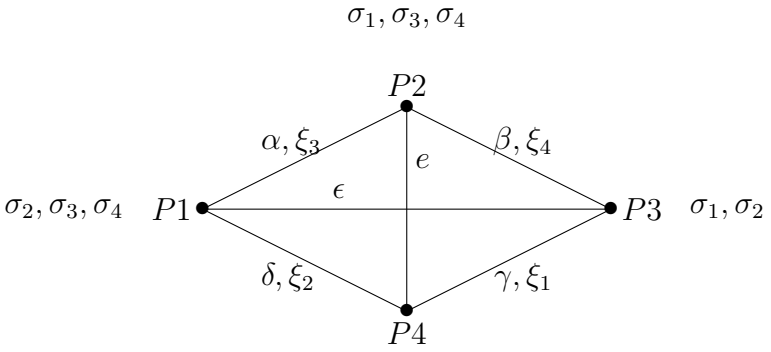
In what follows all the messages are sent through private channels.

Stage 0: free random choices of $\alpha, \beta, \gamma, \delta, \epsilon, (\sigma_i, \xi_i)_{i\in I}$ and $e \in E$:

- 1 chooses $\alpha, \sigma_3, \sigma_4, \xi_3$ and sends them to 2
- 1 chooses ϵ, σ_2 and sends them to 3
- 1 chooses δ, ξ_2 and sends them to 4
- 2 chooses β, σ_1, ξ_4 and sends them to 3
- 2 chooses e and sends it to 4
- 3 chooses γ, ξ_1 and sends them to 4

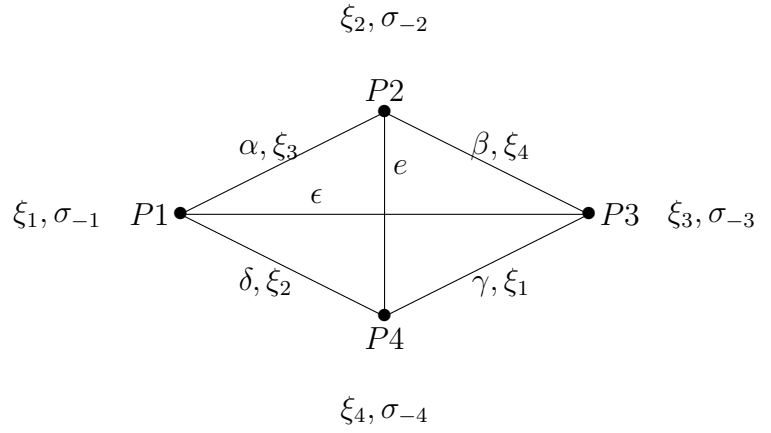
So we have the following picture representing the knowledge of the players:

Figure 1: Random permutations known by the players at the end of **stage 0**.



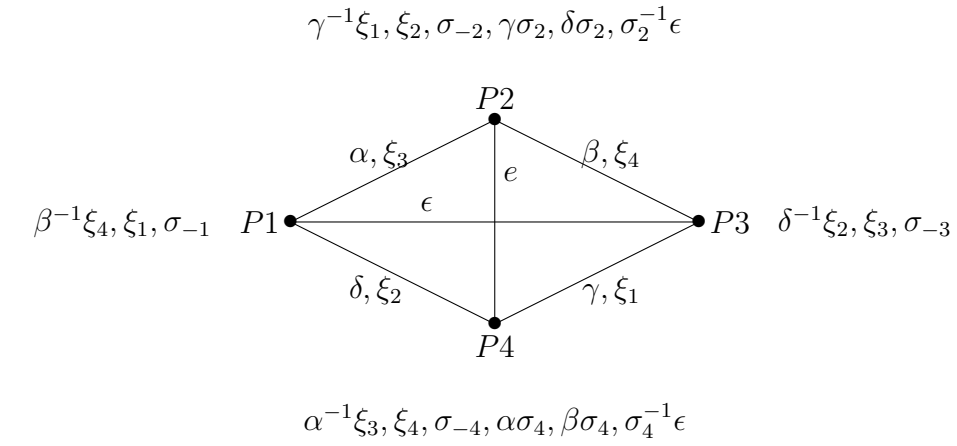
In stages 1 to 3 all the messages are sent by two players. First, in stage 1 σ_i-s and ξ_i-s are distributed in such a way that i learns ξ_i and only $-i$ learn σ_i and we denote the knowledge of i about the σ_j-s with σ_{-i}. So we get to the following figure:

Figure 2: Random permutations known by the players at the end of **stage 1**.



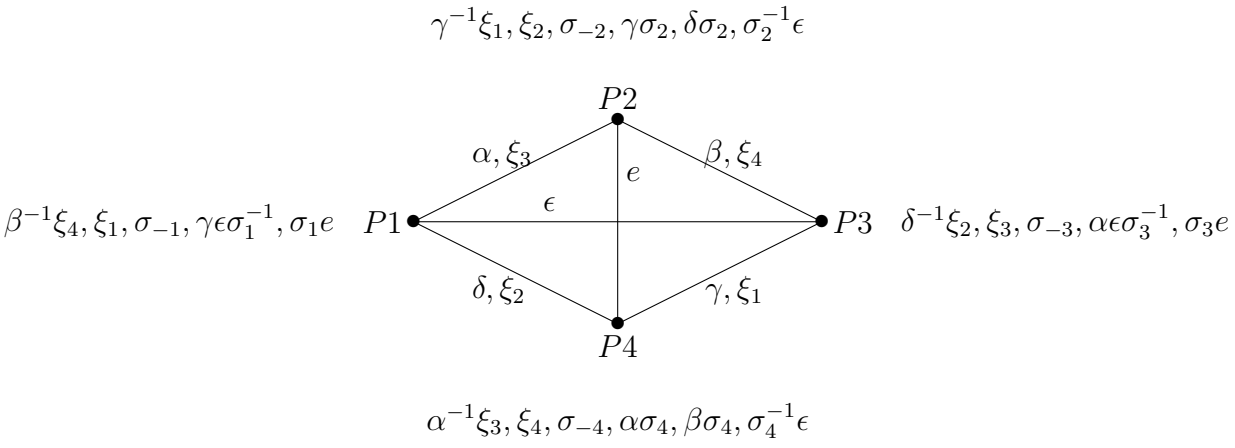
After stage 2 we get to the following figure:

Figure 3: Random permutations known by the players at the end of **stage 2**.



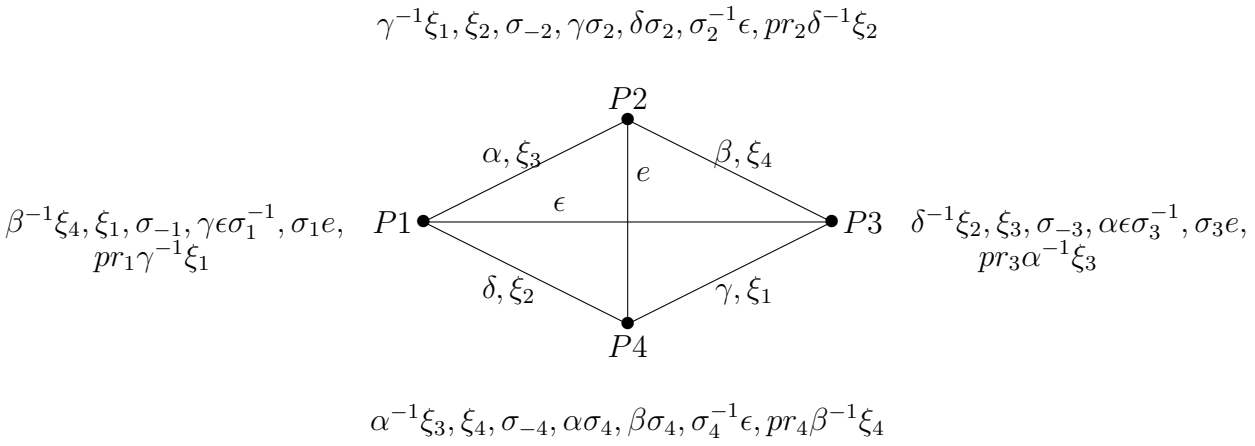
Notice that players 2 and 4 can already calculate $\delta\epsilon e$ and $\beta\epsilon e$ respectively and they can also calculate $\gamma\epsilon$ and $\alpha\epsilon$ respectively. In the third stage players 1 and 3 learn what they need to calculate $\gamma\epsilon e$ and $\alpha\epsilon e$ respectively:

Figure 4: Random permutations known by the players at the end of **stage 3**.



Finally, in the last stage (stage 4) player i learns the appropriate transformation of ξ_i from players $-i$ to be able to calculate $pr_i\epsilon e$. For example, player 1 receives the function $pr_1\gamma^{-1}\xi_1$ from players 2,3, and 4 and calculates $pr_1\gamma^{-1}\xi_1\xi_1^{-1}\gamma\epsilon\sigma_1^{-1}\sigma_1 e$.

Figure 5: Random permutations known by the players at the end of **stage 4**.



We denote by $\mathcal{B}$ the protocol $\mathcal{B}^+$ without the last stage (4) messages which we call the *codes for decision rules*. To distinguish later from other type of sent objects, in the rest of the paper the word *message* will refer to objects which are sent in protocol $\mathcal{B}^+$. Suppose that every player i chooses his own computed action $pr_i\epsilon e$ at the action stage of the extended game. Then the protocol, together with these *induced decision rules* d, induces a distribution $P \in \Delta(H \times A)$. We have the following lemma:

Lemma 1. *1. $P(a) = \mu(a)$ for all $a \in A$.*

2. *(1) For every i, a_{-i} and h_i which has positive probability under P: $P(a_{-i}|h_i) = \mu(a_{-i}|d_i(h_i))$, and (2) for any history h_i^t with $t < n$: $P(a|h_i^t) = \mu(a)$.*

3. *Unilateral deviations in randomization (which can only happen in stage 0) do not affect properties 1. and 2. above.*

4. *From stage 1 on any message which is sent by some player i to player k, is also sent by some player $j \neq i$ to player k and, hence,* unilateral *deviations from stage 1 on are detected instantaneously with probability 1 by receiver k.*

5. *Messages in the last stage (4), i.e., the codes for decision rules are sent by three players to the fourth one. Unilateral deviations in stage 4 are immaterial in that the receiver can always calculate her correct action using the information from the majority of the players .*

Proof. The proof can be found in the Appendix in section A. □

In what follows we derive 11 protocols from $\mathcal{B}$, all of which are run independently in an arbitrary order. When all these protocols terminate (in stage $n-2$) we add another stage (stage $n-1$) to each of them in which the players communicate simultaneously and publicly. This stage allows the players to check whether there has been any deviation or not in the preceding stages. All of these protocols will be run independently so any stage 0 randomization is independent across the protocols. Finally, we add one more stage, the nth stage, of communication to handle certain deviations which may have happened before. In this stage, players also learn their actions. More precisely, in stage n players communicate simultaneously publicly and privately. Their public communication is used to identify the deviator, if possible, and to pin down according to which protocol's induced decision rule they will calculate their actions. In their private communication, they communicate according to the last stage of $\mathcal{B}^+$, in each protocol, and players $-i$ send the information to player i, for all i, so that i can compute her induced, recommended actions in all the protocols.

3.2 The master protocol: $\mathcal{P}0$

We define now a master protocol $\mathcal{P}0$ from which the rest of the protocols will be derived. Consider the protocol $\mathcal{B}$ and modify it as follows. Leave stage 0 messages unchanged. If a message m in a later stage is sent by players i and j to k in $\mathcal{B}$, say $i < j$, then in $\mathcal{P}0$ let only i send the message m to k and let j choose a random permutation λ_m, which we call *key generators*, and send it to k. We say that in this case m *was sent by i to k with the key $\lambda_m m$ shared between j and k*. A detailed description of messages in $\mathcal{P}0$ without the key generators can be found in the Appendix in section B.

Let $\mathcal{P}0^+$ denote the protocol in which after $\mathcal{P}0$ is over, the players do the following:

1. **in stage $n-1$ publicly and simultaneously announce:** for all the messages m-s, which were sent with a key in $\mathcal{P}0$ shared between some j and k, players j, k compute and announce the key $\lambda_m m$. We say that the protocol is *faulty* if there is a message m which was sent with a key shared between j and k such that these players publicly disagree in stage $n-1$ about the corresponding $\lambda_m m$ key, i.e., the announced keys are inconsistent.

2. **in stage n publicly and simultaneously:**

   (a) if the protocol is not faulty, then babble.

   (b) if the protocol is faulty, then announce all the private messages and the key generators they have sent and received before stage $n-1$, including stage 0 messages as well.

3. **in stage n privately and simultaneously send:** their messages as in the last stage (4) of $\mathcal{B}^+$, i.e., the codes for decision rules.

In case of unilateral deviation in $\mathcal{P}0$, one of the pairs of keys must be inconsistent with probability one, i.e., there must be a message which was sent with a key shared between j and k and the publicly announced keys for this message differ between these players and, hence, the protocol is faulty. In case of no deviation in $\mathcal{P}0$, all the keys of all the messages must coincide in stage $n-1$ provided players do not deviate in stage $n-1$. Unilateral deviations only during the public announcement of stage $n-1$ are also detected by these inconsistent keys. In case of no deviation in $\mathcal{P}0^+$, the code for every player decision is sent by three other players and they must also coincide. Consider the corresponding decision rules and the induced distribution. Hence, we have the following lemma.

Lemma 2. *All the properties of $\mathcal{B}^+$ but property 4., as stated in lemma 1, are inherited by $\mathcal{P}0^+$. Instead of property 4. we have that:*

4.1 *Any player at any of her information sets can believe that the others are or were following the protocol before stage $n-1$.*

4.2 *Any unilateral deviation in $\mathcal{P}0$, though not necessarily the identity of the deviator, is detect with probability 1 in $\mathcal{P}0^+$ at stage $n-1$ publicly by all the players.*

Proof. The formal statement of 4.1 and its proof of can be found in the Appendix in section B where we also show that these are the only consistent beliefs. The proof of 4.2 is trivial by construction. □

Remark 1. In case no unilateral deviation is detected in $\mathcal{P}0^+$, i.e., when the protocol is not faulty, which will be the case in equilibrium, players' stage n public communication is babbling and then they choose their actions according to the induced decision rules of $\mathcal{P}0^+$. In case the protocol is faulty, it becomes useless for action choices because in the continuation equilibrium strategies, in stage n, all the past private messages and the key generators will be announced publicly. Hence, the need to introduce further protocols below. However, these public announcements will be useful to identify the deviator and determine that according to which of the protocols below the players will eventually choose their actions.

3.3 The protocol when i and j do not talk to each other: $\mathcal{P}ij$

We define now the protocol $\mathcal{P}ij$ in which i and j will never communicate with each other directly. So fix the players i and j.

First, we modify $\mathcal{P}0$ into $\mathcal{P}0'$ in such a way that no key is shared between i and j. Whenever in $\mathcal{P}0$ a message m was sent by k to i with the key $\lambda_m m$ shared between i and j, let now m be sent by j to i with the key $\lambda_m m$ shared between i and k in $\mathcal{P}0'$. Similarly, whenever in $\mathcal{P}0$ a

message m was sent by k to j with the key $\lambda_m m$ shared between j and i, let now m be sent by i to j with the key $\lambda_m m$ shared between j and k in $\mathcal{P}0'$.

Second, to get $\mathcal{P}ij$, we further modify $\mathcal{P}0'$ so that any message sent between i and j is sent in a split through k and l. More precisely, in $\mathcal{P}ij$, whenever a message m is sent from i to j in $\mathcal{P}0'$, let i choose a random permutation η_m and send η_m to k and send $\eta_m m$ to l. We refer to these objects as *splits* of m. Then the protocol requires k and l to forward these splits to j. Let us stress that m refers to stage 0 messages as well. However, key generators are never shared in a split between i and j in $\mathcal{P}ij$ because in $\mathcal{P}0'$ i and j never shares a key. We say that such a message m is *sent in a split* $(\eta_m, \eta_m m)$ from i to j through k and l (with a key $\lambda_m m$ shared between j and k or l). Notice that in $\mathcal{P}ij$ there are new objects, the splits, which are sent relative to $\mathcal{P}0'$, but there are no new key generators associated to these splits. There are only the old key generators associated to messages m-s, which were also sent in $\mathcal{P}0'$. Let us apply similar changes when a message is sent from j to i in $\mathcal{P}0'$. Notice that $\mathcal{P}ij$ lasts necessarily longer than $\mathcal{P}0$.

Let $\mathcal{P}ij^+$ denote the protocol in which after $\mathcal{P}ij$ is over, the players do the following just as in $\mathcal{P}0^+$:

1. **in stage** $n-1$ **publicly and simultaneously:** for all the messages m-s, which were sent with a key in $\mathcal{P}0'$, and hence, also in $\mathcal{P}ij$ (possibly in a split), let the corresponding players compute and announce the key $\lambda_m m$.

2. **in stage** n **publicly and simultaneously:**

   (a) if the protocol is not faulty, then babble.

   (b) if the protocol is faulty, then announce all the private messages, the key generators, and the splits, for short, the *objects*, they have sent and received before stage $n-1$, including stage 0 messages as well.

3. **in stage** n **privately and simultaneously send:** their messages as in the last stage (4) of $\mathcal{B}^+$, i.e., the codes for decision rules.

Consider the corresponding decision rules and the induced distribution.

Lemma 3. *All the properties of* $\mathcal{P}0, \mathcal{P}0^+$*, as stated in lemma 2, are inherited by* $\mathcal{P}ij, \mathcal{P}ij^+$ *respectively. An additional property we have is that* i *and* j *never communicates directly to each other in* $\mathcal{P}ij$ *and* i *and* j *never shares (even indirectly) a key.*

Remark 2. If $\mathcal{P}0^+$ is faulty, but there are i, j such that $\mathcal{P}ij^+$ is not faulty, then (after publicly babbling in stage n) players will choose their actions according to that protocol. If there are several such protocols, then players play according to the first (according to some commonly

known order) such protocol. If $\mathcal{P}0^+$ and all the $\mathcal{P}ij^+$, henceforth *checkable protocols*, are faulty, then they become useless for action choices. Hence, the need to introduce further protocols. We show later, however, that in this case the identity of the deviator, if unique, can already be discovered.

3.4 The protocol when i does not talk: $(\mathcal{P}i)$

We define now the protocol in which player i remains silent. Consider again the protocol $\mathcal{P}0$ but now players, who are supposed to send the λ_m key generators, stay silent. Given that in stage 0, player 4 does not send any message and that in later stages, it is always the player with the smaller index who sends the message, we have that in this version of $\mathcal{P}0$ player 4 remains silent. Let us denote this protocol by $\mathcal{P}4$. Let $\mathcal{P}i$ be the protocol where we permute the roles of the players in $\mathcal{P}4$ so that it is now player i who remains silent.

Let $\mathcal{P}i^+$ denote the protocol in which after $\mathcal{P}i$ is over, players publicly babble in stages $n-1$ and n, and all the players privately send the codes for decision rules in stage n (here player i also communicates). Consider the corresponding decision rules and the induced distribution.

Lemma 4. *All the properties of $\mathcal{P}0, \mathcal{P}0^+$, as stated in lemma 2, are inherited by $\mathcal{P}i, \mathcal{P}i^+$ respectively for all i with the qualification of 4.2: necessarily, given the absence of key generators, no deviation is ever detected before stage n private communication. We additionally have that player i only sends messages in stage n privately, because otherwise she babbles, i.e., she remains silent.*

Remark 3. If all the checkable protocols are faulty, then, in case of unilateral deviation, the players will be able to identify the deviator using stage n public communication. Suppose player i was identified as the unique deviator. Players then choose actions according to the protocol in which the deviator was sending private messages only in stage n, i.e., according to $\mathcal{P}i^+$ and choose their actions accordingly.

3.5 The grand protocol

It is immaterial in which order the protocols are run and in which order the private communication of the objects happens in the first $n-2$ stages (as long as players have the necessary information to send the required objects). We only have to make sure that all the six $\mathcal{P}ij$, all the four $\mathcal{P}i$, and $\mathcal{P}0$ are terminated before stage $n-1$ public announcements which must be simultaneous within and across protocols. Finally, stage n public and private communication must also happen simultaneously within and across the protocols. In stage $n+1$ players choose actions according to one of the protocols as already hinted by remarks 2, 3 and 4 above on which

we elaborate now and fully describe the equilibrium strategy profile by defining the decision rules $(d_i)_{i\in I}$ which use information from all the protocols. Before proceeding we need the following central terminologies.

We say that a player is *obedient* if she does not deviate before stage $n-1$ from the grand protocol. An obedient player is called *super-obedient* if she does not deviate from the grand protocol before stage n and *semi-obedient* if she deviates in stage $n-1$. One can also use these categories *relative to any given checkable protocol*, namely, whether a player was obedient, super-obedient or semi-obedient in a given checkable protocol.

Actions

So suppose now that we are in stage $n+1$ when the players choose their actions. In what follows, we select a protocol for each possible public history. The selection depends only on the public communication in stages $n-1$ and n. Then the decision rule for obedient players will be the induced (by majority) decision rule of the selected protocol. We have to further extend these rules to the case when the majority does not exist, i.e., to the case when all three codes for the decision rule received by a player in stage n private communication are different. We specify that in such a case the given obedient player should use the code received from the smallest indexed player. From now on we simply refer to this as the *extended majority rule*. Non-obedient players will choose actions which will be sequentially rational given their beliefs, to be specified later, about other players' actions.

The selected protocol

Case 0: there is a non-faulty checkable protocol in stage $n-1$.

The selection rule for Case 0: Let the selected protocol be the first, according to some order which is commonly known by the players starting with $\mathcal{P}0^+$, non-faulty protocol.

Remark 4. Note that in stage n public communication of such a protocol, the players are babbling so the protocol is suitable for determining actions. Notice also that this case covers the case of being on the equilibrium path, but also the case when the players have only followed this particular protocol. But it also covers cases of multilateral deviations within this protocol. E.g., at stage $n-1$ two players, who a shared a key, deviate and announce the same key for a message m which, however, is not the key prescribed by the protocol. Or the case when a player deviates before stage $n-1$ so in stage $n-1$ there should be inconsistent keys, but another player who shared the corresponding key deviates in stage $n-1$ in such a way that the keys become consistent etc.

Case 1: all of the checkable protocols are faulty in stage $n-1$.

The selected protocol will be one of the $\mathcal{P}i^+$ protocols. Recall that all the checkable protocols prescribe that players in stage n should announce (truthfully) all the objects, i.e. the messages, the key generators, and the splits they have sent and received before stage $n-1$ within these protocols but of course this may not be the case. To proceed and categorize all the possible stage $n-1$ and stage n public histories that we have to cover, it is useful to introduce the following terminology.

We say that *two players are in conflict about the past of a checkable protocol* in stage n if there is an object in this protocol about which they disagree: the receiver of an object reports a received object m and the sender of that object reports a sent object $m' \neq m$ about some stage $t < n-1$ private communication in stage n. *Two players are in conflict* if they are in conflict about the past of some checkable protocol.

Let us now consider stage n reports separately for each player. Taking them on their face value, they can be interpreted as a *self-classification*: they represent, for each player, a claim about themselves being obedient or non-obedient. Several comments are in order. First, the truth behind face value might be different since a player can lie while reporting in stage n. Second, nothing is claimed about players' behavior in the non-checkable $\mathcal{P}i$ protocols. Third, among players who self-classified themselves as obedient, we can further classify them by using their own stage $n-1$ announcements into claims (self-classification) to be super-obedient or semi-obedient. Finally, contrary to self-classification, we define the *classification* of a player i based on stage n reports of players $-i$ if players in $-i$ are not in conflict with each other.

The selection rule for Case 1: if $\exists i$ such that $\forall j \in -i$ is self-classified as super-obedient, $-i$ are not in conflict with each other and classify i as not super-obedient in *all* the checkable protocols. Then let the selected protocol be $\mathcal{P}i^+$. Otherwise let it be $\mathcal{P}1^+$.

Remark 5. Notice that the selection rule is unambiguously defined because such an i, if exists, must be unique. It is not possible to have another $j \neq i$ for which the same properties are true because of the presence of protocol $\mathcal{P}ij^+$.

We have finished the description of the grand protocol, i.e., the full description of the equilibrium strategies. We have specified how the players should communicate and choose actions at each and every possible information set.

3.6 Beliefs and the verification of equilibrium conditions

In this section, we describe the players' beliefs at each and every information set. We verify that the described equilibrium strategies specify sequentially rational moves at each and every

information set given the beliefs and other players' strategies. Finally, we conclude that we implement the desired correlated equilibrium distribution in SE of our extended game.

Beliefs

1. ***Obedience, beliefs about moves before stage*** $n-1$: Any player at any of her information sets believes that all the other players are obedient. Hence, beliefs before stage $n-1$ moves are pinned down by the Bayes rule.

2. **Beliefs about moves in stage** $n-1$ **of obedient players**: The beliefs of an obedient player after stage $n-1$ public announcements are immaterial, i.e., it can be arbitrary, as long as she believes in obedience (see below: Verifying equilibrium conditions, sequential rationality).

3. **Beliefs about moves in stage** $n-1$ **of non-obedient players**: (1) Non-obedient players believe that all the other players are super-obedient whenever it is possible. (2) Suppose that such beliefs of a non-obedient player i are not possible because stage $n-1$ public announcements contradict to these beliefs. Given such a situation we define now the beliefs of player i after stage $n-1$ public announcements are made. We must specify i's beliefs only when all the checkable protocols are faulty. (Otherwise her beliefs are immaterial, i.e. it can be arbitrary, as long as she believes in obedience because the play will follow one of the non-faulty protocols.) Hence, given that all the checkable protocols are faulty, player i believes that she is not able to change the outcome of the selection rule of case 1 by not telling the truth in stage n.

4. **Beliefs about moves in stage** n **of obedient players**: Obedient players believe that the extended majority rule gives them the message which was supposed to be sent by the other three players in the selected protocol and they believe that this is true for the other players as well. In short, when an obedient player i calculates that her action is a_i by using the extended majority rule of the selected protocol, she believes that the other (obedient) players choose actions according to $\mu(a_{-i}|a_i)$ because she believes that the selected protocol was not manipulated.

5. **Beliefs about moves in stage** n **of non-obedient players**: Non-obedient players, given the strategy they have followed, calculate (using the Bayes rule) the induced distribution of obedient players' actions, which may not coincide with the one corresponding to μ, and form their beliefs accordingly.

Lemma 5. *These beliefs are consistent in the sense of Kreps and Wilson (1982).*

Proof. The proof can be found in the Appendix in Section C. □

Verifying equilibrium conditions, sequential rationality

First, we check the incentives of an obedient player from stage $n-1$ on but backwards. Stage $n+1$ action choices of an obedient player are sequentially rational given their beliefs (points 1 and 4 in beliefs) because μ is a correlated equilibrium and because of points 1. and 2. (1) of lemmas 2,3 and 4 (see the corresponding statements in lemma 1). It is immaterial for an obedient player how she communicates publicly in stage n. In case 0, the selected protocol is already determined; in case 1, it does not matter for her that according to which $\mathcal{P}i^+$ protocol the actions will be chosen, her expected payoff in all these terminations is equal, according to point 2. (2) of lemma 4 (see again lemma 1), to her (ex ante) correlated equilibrium payoff. Hence her beliefs in point 2 can be arbitrary. Deviations in stage n private communication have no effect on the outcome due to the majority rule. In stage $n-1$, it is sequentially rational for an obedient player to follow the grand protocol and report her calculated $\lambda_m m$-s keys truthfully for the same reason and, hence, to behave super-obediently in stage $n-1$.

Second, we check the incentives of a non-obedient player i from stage $n-1$ on but backwards. Stage $n+1$ action choices of a non-obedient player are defined to be sequentially rational given her beliefs that the other players are obedient, obedient players' strategies, and her own private and public communication. It is immaterial for a non-obedient player how she communicates publicly in stage n. In case 0, the selected protocol is already determined in stage $n-1$ (see selection rule for case 0). In case 1 (see selection rule for case 1), suppose that her beliefs are as in beliefs point 3 (1). Then she knows that she will be identified as a deviator no matter what she publicly says in stage n and play will follow $\mathcal{P}i^+$. Suppose that beliefs point 3 (1) is not possible, but then by definition of beliefs point 3 (2), she believes that she cannot change the selected protocol by deviating from telling the truth. Deviations in stage n private communication have no effect on the outcome due to the majority rule. Just before stage $n-1$ public announcements, a non-obedient player believes that the others are obedient and hence they follow their equilibrium strategy and behave super-obediently in stage $n-1$. It is then immaterial for her how to communicate in stage $n-1$ because the selected protocol cannot be one in which she behaved non-obediently. The selected protocol will be either $\mathcal{P}i^+$ (in case 1) that she is unable to manipulate or one of the non-faulty checkable protocols (in case 0) in which she must have behaved obediently because deviations in these protocols are detected in stage $n-1$ with probability one by inconsistent keys. Her expected payoff from any stage $n-1$ communication are equal to her (ex ante) correlated equilibrium payoff.

Finally, we consider the incentives of a player to deviate during the first $n-2$ stages. But we have just seen that such a deviation results in the same expected payoff as in equilibrium.

It follows that it is sequentially rational for all the players to behave super-obediently, babble publicly and transmit privately the messages required by the protocols in stage n, and finally

calculate and choose actions according to $\mathcal{P}0^+$ given that the others do so. By the properties of $\mathcal{P}0^+$ established in lemma 2, and the consistency of the beliefs, the given correlated equilibrium is implemented in SE. Q.E.D.

References

Bárány, I. (1992): "Fair distribution protocols or how the players replace fortune," *Mathematics of Operations Research*, 17, 327–340.

Ben-Or, M., S. Goldwasser, and A. Wigderson (1988): "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation (Extended Abstract)," *Proceedings 20 STOC ACM*, 1–10.

Ben-Porath, E. (2003): "Cheap talk in games with incomplete information," *Journal of Economic Theory*, 108, 45–71.

Forges, F. (1986): "An Approach to Communication Equilibria," *Econometrica*, 1375–1385.

——— (1990): "Universal Mechanisms," *Econometrica*, 58, 1341–64.

——— (2010): "Communication in Bayesian Games: Overview of Work on Implementing Mediators in Game Theory," *Open Access publications from Université Paris-Dauphine*.

Geffner, I. and J. Y. Halpern (2024): "Communication Games, Sequential Equilibrium, and Mediators," *Journal of Economic Theory*, 221, 105890.

Gerardi, D. (2002): "Unmediated Communication in Games with Complete and Incomplete Information," Cowles Foundation Discussion Papers 1371, Cowles Foundation for Research in Economics, Yale University.

——— (2004): "Unmediated communication in games with complete and incomplete information," *Journal of Economic Theory*, 114, 104–131.

Gossner, O. (1998): "Secure Protocols or How Communication Generates Correlation," *Journal of Economic Theory*, 83, 69–89.

Kreps, D. M. and R. Wilson (1982): "Sequential Equilibria," *Econometrica*, 50, 863–894.

Lamport, L., R. Shostak, and M. Pease (1982): "The Byzantine generals problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4, 382–401.

Myerson, R. B. (1982): "Optimal Coordination Mechanisms in Generalized Principal–Agent Problems," *Journal of Mathematical Economics*, 10, 67–81.

Vida, P. (2007): "From Communication Equilibria to Correlated Equilibria," *Unpublished paper, University of Vienna*.

A Proof of Lemma 1

Proof of Lemma 1, point 1:

This point follows trivially by construction.

Proof of Lemma 1, point 2 (1): Players' information before the decision stage is given in Figure 5. For example, the information set of player 1 is:

$$h_1 = \left\{\beta^{-1}\xi_4, \xi_{-4}, \sigma_{-1}, \alpha, \delta, \epsilon, \gamma\epsilon\sigma_1^{-1}, \sigma_1 e, pr_1\gamma^{-1}\xi_1\right\}$$

The players calculate their actions as follows:

$$\begin{aligned}
d_1(h_1) &= pr_1\gamma^{-1}\xi_1\xi_1^{-1}\gamma\epsilon\sigma_1^{-1}\sigma_1 e = pr_1\epsilon e = a_1 && (1)\\
d_2(h_2) &= pr_2\delta^{-1}\xi_2\xi_2^{-1}\delta\sigma_2\sigma_2^{-1}\epsilon e = pr_2\epsilon e = a_2 && (2)\\
d_3(h_3) &= pr_3\alpha^{-1}\xi_3\xi_3^{-1}\alpha\epsilon\sigma_3^{-1}\sigma_3 e = pr_3\epsilon e = a_3 && (3)\\
d_4(h_4) &= pr_4\beta^{-1}\xi_4\xi_4^{-1}\beta\sigma_4\sigma_4^{-1}\epsilon e = pr_4\epsilon e = a_4 && (4)
\end{aligned}$$

We look at player 1. Let $h' := h_1 \setminus \{\sigma_1 e\}$. Thus,

$$\begin{aligned}
&\Pr\left(pr_2\epsilon e = a_2, \ldots, pr_4\epsilon e = a_4 | pr_1\epsilon e = a_1, h', \sigma_1 e\right)\\
=\ &\frac{\Pr\left(pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4, h', \sigma_1 e\right)}{\Pr\left(pr_1\epsilon e = a_1, h', \sigma_1 e\right)}\\
=\ &\frac{\Pr\left(\sigma_1 e | pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4, h'\right)\Pr\left(pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4, h'\right)}{\Pr\left(\sigma_1 e | pr_1\epsilon e = a_1, h'\right)\Pr\left(pr_1\epsilon e = a_1, h'\right)}.
\end{aligned}$$

We claim that

$$\Pr\left(\sigma_1 e | pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4, h'\right) = \Pr\left(\sigma_1 e | pr_1\epsilon e = a_1, h'\right)$$

holds. To show it, we argue that both conditional probability distributions are uniform with the same support. Consider all realizations of $\sigma_1 e$ that are compatible with $pr_1\epsilon e = a_1$ and h'. Suppose there are Q such compatible realizations of $\sigma_1 e$. Because each compatible realization is equally likely,

$$\Pr\left(\sigma_1 e | pr_1\epsilon e = a_1, h'\right) = \frac{1}{Q}.$$

Now, we ask what realizations of $\sigma_1 e$ are compatible, in the sense of having a positive probability, with $pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4$ and h'.[5] We claim that the same Q realizations of $\sigma_1 e$ are still compatible. If we look at (2)-(4), the realizations of $a_2, \ldots, a_4$ do not depend on the realization of σ_1. Therefore, any realization of $\sigma_1 e$ that can occur given $pr_1\epsilon e = a_1$ and h', can still occur given $pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4$ and h' and so, because each compatible realization is equally likely,

$$\Pr\left(\sigma_1 e | pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4, h'\right) = \frac{1}{Q}.$$

Thus,

$$\begin{aligned}
& \Pr\left(pr_2\epsilon e = a_2, \ldots, pr_4\epsilon e = a_4 | pr_1\epsilon e = a_1, h', \sigma_1 e\right) \\
= & \frac{\Pr\left(pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4, h'\right)}{\Pr\left(pr_1\epsilon e = a_1, h'\right)} \\
= & \frac{\Pr\left(pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4\right)}{\Pr\left(pr_1\epsilon e = a_1\right)} \\
= & \Pr\left(pr_2\epsilon e = a_2, \ldots, pr_4\epsilon e = a_4 | pr_1\epsilon e = a_1\right)
\end{aligned}$$

where the second equality is because ϵe is independent of h'. To see it,

$$\Pr(\epsilon e = \hat{e}, h') = \Pr(e = \epsilon^{-1}(\hat{e}), h') = \Pr(e = \epsilon^{-1}(\hat{e}))\Pr(h') = \Pr(\epsilon e = \hat{e})\Pr(h')$$

where the second equality follows from the fact that h' does not contain e and the latter was drawn independently of other variables.

We now consider player 2. His information set is:

$$h_2 = \left\{\gamma^{-1}\xi_1, \xi_{-1}, \sigma_{-2}, \alpha, \beta, e, \gamma\sigma_2, \delta\sigma_2, \sigma_2^{-1}\epsilon, pr_2\delta^{-1}\xi_2\right\}.$$

[5] It is enough to consider realizations $pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4$ that have a positive probability. If $pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4$ have zero probability, then

$$\begin{aligned}
\Pr\left(pr_2\epsilon e = a_2, \ldots, pr_4\epsilon e = a_4 | pr_1\epsilon e = a_1, h', \sigma_1 e\right) &= \\
\Pr\left(pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4 | pr_1\epsilon e = a_1\right) &= 0.
\end{aligned}$$

With some abuse of notation, let $h' := h_2 \backslash \left\{\sigma_2^{-1}\epsilon\right\}$. Thus,

$$\begin{aligned}
& \Pr\left(pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4 | pr_2\epsilon e = a_2, h', \sigma_2^{-1}\epsilon\right) \\
= & \frac{\Pr\left(pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4, h', \sigma_2^{-1}\epsilon\right)}{\Pr\left(pr_2\epsilon e = a_2, h', \sigma_2^{-1}\epsilon\right)} \\
= & \frac{\Pr\left(\sigma_2^{-1}\epsilon | pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4, h'\right) \Pr\left(pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4, h'\right)}{\Pr\left(\sigma_2^{-1}\epsilon | pr_2\epsilon e = a_2, h'\right) \Pr\left(pr_2\epsilon e = a_2, h'\right)}.
\end{aligned}$$

We claim that

$$\Pr\left(\sigma_2^{-1}\epsilon | pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4, h'\right) = \Pr\left(\sigma_2^{-1}\epsilon | pr_2\epsilon e = a_2, h'\right)$$

holds. To show it, we argue that both conditional probability distributions are uniform with the same support. Consider all realizations of $\sigma_2^{-1}\epsilon$ that are compatible with $pr_2\epsilon e = a_2$ and h'. Suppose there are Q such compatible realizations of $\sigma_2^{-1}\epsilon$. Because each compatible realization is equally likely,

$$\Pr\left(\sigma_2^{-1}\epsilon | pr_2\epsilon e = a_2, h'\right) = \frac{1}{Q}.$$

Now, we ask what realizations of $\sigma_2^{-1}\epsilon$ are compatible, in the sense of having a positive probability, with $pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4$ and h'. We claim that the same Q realizations of $\sigma_2^{-1}\epsilon$ are still compatible. If we look at (1), (3), (4), the realizations of a_1, a_3, a_4 do not depend on the realization of σ_2. Therefore, any realization of $\sigma_2^{-1}\epsilon$ that can occur given $pr_2\epsilon e = a_2$ and h', can still occur given $pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4$ and h' and so, because each compatible realization is equally likely,

$$\Pr\left(\sigma_2^{-1}\epsilon | pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4, h'\right) = \frac{1}{Q}.$$

Thus,

$$\begin{aligned}
& \Pr\left(pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4 | pr_2\epsilon e = a_2, h', \sigma_2^{-1}\epsilon\right) \\
= & \frac{\Pr\left(pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4, h'\right)}{\Pr\left(pr_2\epsilon e = a_2, h'\right)} \\
= & \frac{\Pr\left(pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4\right)}{\Pr\left(pr_2\epsilon e = a_2\right)} \\
= & \Pr\left(pr_1\epsilon e = a_1, \ldots, pr_4\epsilon e = a_4 | pr_2\epsilon e = a_2\right)
\end{aligned}$$

where the second equality is because ϵe is independent of h'. To see it, note that h' does not contain ϵ and the latter was drawn independently of other variables.

The proofs for players 3 and 4 are analogous to those of players 1 and 2 respectively. Q.E.D.

Proof of Lemma 1, point 2 (2):

It is enough to consider the stage right before the one when the players receive projections. Thus, in case of player 1, his information is

$$h_1 = \left\{\beta^{-1}\xi_4, \xi_{-4}, \sigma_{-1}, \alpha, \delta, \epsilon, \gamma\epsilon\sigma_1^{-1}, \sigma_1(e)\right\}.$$

We want to show that

$$\Pr(\epsilon e|h_1) = \frac{1}{|E|}$$

which would imply that $\Pr(a|h_1) = \mu(a)$.

The joint distribution of ϵe and h_1 is

$$\begin{aligned}
\Pr(\epsilon e, h_1) &= \Pr(\gamma\epsilon\sigma_1^{-1})\Pr(\epsilon e, \beta^{-1}\xi_4, \xi_{-4}, \sigma_{-1}, \alpha, \delta, \epsilon, \sigma_1 e) \\
&= \Pr(\sigma_1 e)\Pr(\gamma\epsilon\sigma_1^{-1})\Pr(\epsilon e, \beta^{-1}\xi_4, \xi_{-4}, \sigma_{-1}, \alpha, \delta, \epsilon) \\
&= \Pr(\epsilon e)\Pr(\sigma_1 e)\Pr(\gamma\epsilon\sigma_1^{-1})\Pr(\beta^{-1}\xi_4, \xi_{-4}, \sigma_{-1}, \alpha, \delta, \epsilon) \\
&= \Pr(\epsilon e)\Pr(h_1)
\end{aligned}$$

where the first equality follows because γ is independent of $\{\epsilon e, h_1\}\backslash\{\gamma\epsilon\sigma_1^{-1}\}$; the second equality because σ_1 is independent of $\{\epsilon e, h_1\}\backslash\{\gamma\epsilon\sigma_1^{-1}, \sigma_1 e\}$; the third equality because e is independent of $h_1\backslash\{\gamma\epsilon\sigma_1^{-1}, \sigma_1 e\}$.

Hence, we have

$$\Pr(\epsilon e|h_1) = \Pr(\epsilon e) = \frac{1}{|E|}$$

as was required to show. The proof for the other players is analogous.Q.E.D.

Proof of Lemma 1, point 3:

The action profile depends on the realized value of ϵe, which is jointly controlled by players 1 and 2. Hence, neither of these players can gain by a unilateral deviation when drawing ϵ and e. Besides ϵ, player 1 also chooses other permutations like α and δ but they do not determine his action according to (1). The choices of these permutations enter in (2)-(4). However, if player 1 deviates by choosing these permutations differently from the uniform distribution or even have them correlated, such a deviation would not be detected by the other players and so would not affect what they know and their actions would still only depend on projections of ϵe. The same comment applies to players 2 and 3 who choose permutations β, γ and so on. Q.E.D.

Proof of Lemma 1, points 4 and 5:

These points follow trivially by construction.

B Proof of Lemma 2

We only have to prove point 4.1. First we formally state point 4.1. Consider a history of player i after the communication in stage $n-2$ is over, i.e., $h_i^{n-2} = (m_{-i,i}^k, m_{i,-i}^k, p^k)_{-1 \leq k \leq n-2}$ and split it into sent s_i^{n-2} and received r_i^{n-2} messages. Denote the corresponding sets of histories by S_i^{n-2} and R_i^{n-2} respectively. Consider the communication strategy profile c given by $\mathcal{P}0$ and let player i follow some communication strategy c_i' which can be equal to c_i. Then (c_i', c_{-i}) induces a distribution $P \in \Delta(H^{n-2})$. We claim that for any i, for any c_i', for any $r_i^{n-2} \in R_i^{n-2}$, and for any $s_i^{n-2} \in S_i^{n-2}$ for which $P(s_i^{n-2}) > 0$ we have that $P(r_i^{n-2}|s_i^{n-2}) > 0$. In words, it does not matter how player i communicates, she will never be surprised by any message that she receives from the others. Namely, player i can always believe that players $-i$ follow the protocol $\mathcal{P}0$. In fact, given that this is the equilibrium strategy of the other players, these are the only consistent beliefs of player i no matter whether she herself has followed the protocol or not.

We report here the messages sent and received in $\mathcal{P}0$ by the players without the key generators which obviously do not make a difference.[6]

Player 1		
Stage	Sent	Received
0	$\sigma_{-1}, \xi_2, \xi_3, \alpha, \delta, \epsilon$	$-$
1	$\sigma_{-1}, \xi_2, \xi_3$	ξ_1
2	$\delta\sigma_2, \sigma_2^{-1}\epsilon, \alpha\sigma_4, \sigma_4^{-1}\epsilon$	$-$
3	$\delta^{-1}\xi_2, \alpha^{-1}\xi_3, \alpha\epsilon\sigma_3^{-1}$	$\beta^{-1}\xi_4, \gamma\epsilon\sigma_1^{-1}, \sigma_1 e$

Player 2		
Stage	Sent	Received
0	$\sigma_1, \xi_4, \beta, e$	$\sigma_3, \sigma_4, \xi_3, \alpha$
1	σ_1, ξ_4	ξ_2
2	$\beta\sigma_4$	$\gamma\sigma_2, \delta\sigma_2, \sigma_2^{-1}\epsilon$
3	$\beta^{-1}\xi_4, \gamma\epsilon\sigma_1^{-1}, \sigma_1 e, \sigma_3 e$	$\gamma^{-1}\xi_1$

Player 3		
Stage	Sent	Received
0	ξ_1, γ	$\sigma_1, \sigma_2, \xi_4, \beta, \epsilon$
1	ξ_1	σ_4, ξ_3
2	$\gamma\sigma_2$	$-$
3	$\gamma^{-1}\xi_1$	$\delta^{-1}\xi_2, \alpha\epsilon\sigma_3^{-1}, \sigma_3 e$

[6]The proof of the corresponding point of lemma 3 for $\mathcal{P}ij$ is similar. The proof of the corresponding point of 4 for $\mathcal{P}i$ for $i \neq 4$ is the same given that $\mathcal{P}0$ without key generators is identical to $\mathcal{P}4$ and in $\mathcal{P}i$ only the players' roles change.

Player 4		
Stage	Sent	Received
0	–	$\xi_1, \xi_2, \gamma, \delta, e$
1	–	ξ_4, σ_{-4}
2	–	$\alpha\sigma_4, \beta\sigma_4, \sigma_4^{-1}\epsilon$
3	–	$\alpha^{-1}\xi_3$

Consider the case of $i = 1$ and first for simplicity assume that $c_1' = c_1$. Let (v, w, z, y) be an arbitrary element of R_1^{n-2} corresponding to the four messages received by player 1. Now the question is whether there exist some $\xi_1, \beta, \xi_4, \gamma, \sigma_1, e$ such that given ϵ we have that $v = \xi_1, w = \beta^{-1}\xi_4, z = \gamma\epsilon\sigma_1^{-1}, y = \sigma_1 e$. The answer is obviously positive, hence, player 1 can believe that others' random choices in stage 0 were exactly these objects (which have positive probability) and they have followed the protocol.

The situation is a bit more subtle when $c_1' \neq c_1$ because player 1 instead of $\sigma_2^{-1}\epsilon$ can send a different message, say m, to player 2 in stage 2, which may now even depend on the message v she received in stage 1, and player 2 then sends back $\gamma\sigma_2 m\sigma_1^{-1}$ to player 1 in stage 3. Nevertheless, the question is whether there exist some $\xi_1, \beta, \xi_4, \gamma, \sigma_1, e$ for any m such that we have that $v = \xi_1, w = \beta^{-1}\xi_4, z = \gamma\sigma_2 m\sigma_1^{-1}, z = \sigma_1 e$ given σ_2 and m. Again, the answer to this question is obviously positive.

One can do the same argument for the rest of the players. In fact, for players 2 and 3 the argument becomes much simpler. Q.E.D.

C Proof of Lemma 5: consistency

We have to prove that out of equilibrium beliefs in our equilibrium as specified in section 3.6 are consistent in the sense of sequential equilibrium.

The completely mixed communication strategies converging to the equilibrium communication strategies, i.e., the justifying sequence, are given as follows. Errors will be made independently across the protocols so we describe these only for one given protocol. Each player is non-obedient with probability in the order of $\varepsilon^{p(\varepsilon)}$, where we choose later $p(\varepsilon)$ to be large enough. By this we mean that with this probability the player chooses a completely mixed behavioral strategy and with the remaining probability she behaves obediently in that protocol. It is sufficient to consider such mixing because by point 4.1 of lemma 2, the players before stage $n-1$ must believe that the others are obedient and beliefs can always be calculated using the Bayes rule.

In $\mathcal{P}0^+$, conditional on being obedient before stage $n-1$, in stage $n-1$ each player is semi-obedient (i.e., they report wrong keys) with probability in the order of ε and non-obedient players

report the keys dishonestly in the same order. Players send a wrong code for decision rules to another player in stage n private communication, independently across receivers, independently of stage n public communication and independently in which information set they are with probabilities in the following orders: Player 1 with ε^5, player 2 with ε^4, players 3 and 4 with ε^3. Given that players babble if the protocol is non-faulty, we only have to require that players deviate from their sequentially rational stage n public communication when the protocol was faulty, with probability in the order of ε. In $\mathcal{P}ij^+$ the mixing is the same with the difference that in stage $n-1$, players k and l report wrong keys in the order of $\sqrt{\varepsilon}$. Hence, when i (j) observes an inconsistent key in $\mathcal{P}ij^+$ announced by k and j (i), conditional on obedience and that she was obedient relative to $\mathcal{P}ij^+$, she believes that it is k who has reported the wrong key.

Beliefs in point 1 (obedience) are consistent because the probability, right after stage $n-1$, that the other three players are obedient converges to 0 in a weakly slower order than $(\varepsilon^7)^3$ (all the three players were obedient but deviated in stage $n-1$ in all the 7 checkable protocols), and this probability right after stage n converges to 0 in a weakly slower order than $((\varepsilon^7)^3)^2((\varepsilon^5)^3)^{11} = \varepsilon^{207}$ (all the three players were obedient but are deviating in stage $n-1$ and in stage n in the public messages of all the 7 checkable protocols and in stage n all the three players are sending wrong codes for decisions to the given player in the private communication in all the 11 protocols) whereas the probability that some players are non-obedient converges to 0 in a weakly faster order than $1-((1-\varepsilon^{p(\varepsilon)})^3)^{11}$ (at least one player is non-obedient at least in one of the protocols). Hence, if $p(\varepsilon)$ is large enough, so that $1-((1-\varepsilon^{p(\varepsilon)})^3)^{11}$ converges to 0 in a weakly faster order than ε^{208} as ε is going to 0, then the beliefs will be concentrated on histories in which the other players are obedient.

Beliefs in point 2 can be arbitrary and hence will follow from the justifying sequence.

We prove now the consistency of beliefs in point 3. Beliefs in point 3 (1) are clearly consistent because being super-obedient in every protocol is the equilibrium strategy in stage $n-1$. For point 3 (2) we have to consider two cases and we proceed by contradiction. (1) Assume that i can believe that she can change the selected protocol from $\mathcal{P}1^+$ to $\mathcal{P}j^+$, for some j, by not telling the truth in stage n about the past of some checkable protocol while players $-i$ tell the truth. (2) Assume that i can believe that she can change the selected protocol from $\mathcal{P}j^+$ to $\mathcal{P}1^+$, for some j, by not telling the truth in stage n about the past of some checkable protocol while players $-i$ tell the truth.

Consider case (1). It must be then that players $-j$ can classify j as non-super-obedient in all the checkable protocols with a public announcement in stage n and self-classify themselves as super-obedient without being in conflict between each other (see selection rule case 1). It must be then that i is super-obedient relative to $\mathcal{P}ij^+$ (to be able to agree with k and l and self-classify as super-obedient), k and l must be believed to be super-obedient, and hence, there must be

a player k and a message in $\mathcal{P}ij^+$ such that j and k announce different keys for this message because $\mathcal{P}ij^+$ is faulty. But then, because of the specified justifying sequence (see above), i have to believe that k is semi-obedient relative to $\mathcal{P}ij^+$ which is a contradiction to the super-obedience of k.

Consider case (2). It must be the case that player i was super-obedient relative to all the checkable protocols (but was non-obedient in some non-checkable protocol) and she believes that player j is the unique semi-obedient player who deviated in all the checkable. But then in $\mathcal{P}ij^+$ there must be a message such that j and k announce different keys for this message because $\mathcal{P}ij^+$ is faulty. However, in this case player i will have to believe, because of the specified justifying sequence (see above), that player k is semi-obedient relative to $\mathcal{P}ij^+$ which is a contradiction to the super-obedience of k.

We prove now the consistency of beliefs in point 4. We already know that obedient players believe that the others were also obedient, hence, they believe that the selected protocol is not manipulated. No matter which code the players use to calculate their actions, by construction the calculated action has positive probability under μ. Now, conditional on that the selected protocol is not manipulated, the probability that all the three players send the wrong code converges in a faster order to 0 than two of them send the wrong code which converges in a faster order to 0 than one of them sends the wrong code (see the chosen orders of errors) and hence, the majority rule is consistent. In case all the codes for decision rules differ, simple calculation shows that it is the smallest indexed player among the three who sends the wrong code with probability converging in the fastest order to 0. Finally, even if the smallest indexed player sends a wrong code to a receiver, she believes that the other two will send the correct code to the same receiver, hence, believes that the receiver will choose actions according to the correct code for her decision rule (see similar construction in Gerardi (2004)).

Finally, beliefs in point 5 are defined to be calculated according to the Bayes rule conditional on the other players being obedient, hence, these beliefs are consistent. Q.E.D.

D Proof of Corollary 1: Regular Communication Equilibria

See the discussion in Gerardi (2004) after Theorem 2 on page 119 and Gerardi (2002) who uses Forges (1990) to prove the same result when the number of players is at least 5. Given the properties of our protocol and that Forges (1990) only needs 4 players, the proof of our remark is the same as that of Theorem 2 in Gerardi (2004).