Cryptographically Blinded Games: Leveraging Players' Limitations for Equilibria and Profit

PAVEL HUBÁČEK, Aarhus University
SUNOO PARK, MIT

In this work we apply methods from cryptography to enable mutually distrusting players to implement broad classes of mediated equilibria of strategic games without trusted mediation. Our implementation uses a pre-play "cheap talk" phase, consisting of non-binding communication between players prior to play in the original game. In the cheap talk phase, the players run a secure multi-party computation protocol to sample from an equilibrium of a "cryptographically blinded" version of the game, in which actions are encrypted.

Coarse correlated equilibrium. Coarse correlated equilibria (CCE) are a generalization of correlated equilibria (CE), invoking a notion of commitment. Suppose a mediator samples an action profile a from a distribution α. We say α is a CCE if no player has incentive not to "promise" in advance – *before seeing his advice* a_i – to play according to the advice, if he believes that all other players will commit to do the same. Note that players who do not commit will not see the advice at all, and hence must play an independent strategy.

In this paper, we address the following question:

How can the players of a strategic game implement any CCE via (cryptographic) pre-play communication without trusting each other or a mediator?

In the computational setting, we give an implementation for general strategic games, in the form of an extended game comprising a cryptographic protocol in the pre-play phase, which securely samples an action profile for a "cryptographically blinded" version of the game. The blinded game's action space consists of *encryptions* of the original game's actions. Our implementation has the strong property that any computational CCE of the original game corresponds to a payoff-equivalent Nash equilibrium of the extended game. Furthermore, it achieves *strategic equivalence*, in that every computational Nash equilibrium of the extended game corresponds to a computational CCE of the original game.

In the information-theoretic setting, we give an implementation for strategic games with four or more players, using a similar cryptographically blinded pre-play phase given pairwise communication channels. This also achieves strategic equivalence. Both the restriction to four or more players and the need for a stronger communication model are unavoidable in this setting, as shown by impossibility results of [Bárány 1992; Ben-Or et al. 1988; Pease et al. 1980; Aumann and Hart 2003].

Relation to prior work. The *pre-play* literature considers the problem of implementing equilibria without mediation. Our work generalizes that of [Bárány 1992] in the information-theoretic setting and [Dodis et al. 2000] in the computational setting. It has long been recognized that the possibility to *commit* to strategies in advance can increase payoffs achievable in a game, starting with [von Stackelberg 1934]; in this work, we achieve the payoffs of CCE without resorting to the usual assumption of binding contracts. Our results are achieved using a very weak (and necessary [Hubáček et al. 2013]) notion of mediation, where the mediator's actions are publicly verifiable, and moreover the mediator's output does not affect players' strategic choices.

Categories and Subject Descriptors: F.0 [**Theory of Computation**]: General; J.4 [**Social and Behavioral Sciences**]: Economics

Additional Key Words and Phrases: blinded games; cheap talk; coarse correlated equilibria; cryptographic protocols; encryption; multi-party computation; power of commitment.

Full version available at: `http://people.csail.mit.edu/sunoo/blindedgames`
Pavel was supported by the ERC Starting Grant 279447 and the CTIC and the CFEM research centers.
Authors' addresses: P. Hubáček, Department of Computer Science, Aarhus University, Aabogade 34, DK-8200 Aarhus, Denmark; S. Park, MIT CSAIL, 32 Vassar Street, Cambridge, MA 02139, USA.

EC'14, June 8–12, 2014, Stanford, CA, USA. ACM 978-1-4503-2565-3/12/06.
http://dx.doi.org/10.1145/2600057.2602903

REFERENCES

Robert J. Aumann and Sergiu Hart. 2003. Long cheap talk. *Econometrica* 71, 6 (2003), 1619–1660.

Imre Bárány. 1992. Fair distribution protocols or how the players replace fortune. *Mathematics of Operations Research* 17, 2 (1992), 327–340.

Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. 1988. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*. ACM, 1–10.

Yevgeniy Dodis, Shai Halevi, and Tal Rabin. 2000. A cryptographic solution to a game theoretic problem. In *CRYPTO (Lecture Notes in Computer Science)*, Mihir Bellare (Ed.), Vol. 1880. Springer, 112–130.

Pavel Hubáček, Jesper Buus Nielsen, and Alon Rosen. 2013. Limits on the power of cryptographic cheap talk. In *CRYPTO (1) (Lecture Notes in Computer Science)*, Ran Canetti and Juan A. Garay (Eds.), Vol. 8042. Springer, 277–297.

Marshall Pease, Robert Shostak, and Leslie Lamport. 1980. Reaching agreement in the presence of faults. *Journal of the ACM (JACM)* 27, 2 (1980), 228–234.

Heinrich von Stackelberg. 1934. *Marktform und Gleichgewicht.-Wien & Berlin: Springer 1934. VI, 138 S. 8*. J. Springer.