A Cryptographic Solution to a Game Theoretic Problem.

Yevgeniy Dodis, Shai Halevi and Tal Rabin

17th May 2002

An essay for the Seminar on Theoretical Computer Science (Tik-79.194) by
Maarit Hietalahti
Helsinki University of Technology
Laboratory for Theoretical Computer Science

Abstract

This essay deals with the cryptographic solutions to a game theoretic problem presented in a paper by Dodis et al. [1]. Specifically, the problem of removing the trusted third party, ie. the mediator, in two-player games with correlated strategies. The problem and the use of cryptographic primitives is explained and demonstrated by examples.

Contents

1 Introduction

The problem considered here belongs to the area of two player strategic games: Two players, each with a set of possible actions, are assumed to be selfish and rational. They both choose an action from their respective sets and then execute them simultaneously. A player's only objective is to maximize its (expected) payoff.

A Nash equilibrium [4] is a state where neither player can improve their respective payoffs if the other player does not change its strategy. It is assumed that the players have chosen their moves independently of the other player.

1.1 Correlates Strategies

In a Nash equilibrium, the players cannot improve their payoffs if the other parties do not change their strategies as well. However, the payoffs received in a Nash equilibrium are not necessarily optimal. It has been shown that both players can receive better payoffs if they use correlated strategies [2]. This means that the players are assisted by a trusted third party, a *mediator*. The mediator chooses a pair of moves and privately tells each player its designated move. Since the strategies are correlated, the move of one player carries some information on the move of the other. However, this extra information brings them no advantage, because the designated move is always the best strategy if the other party also follows the directions. Players have no incentive to deviate from their designated moves, in other words, they have achieved a *correlated equilibrium*. A correlated equilibrium is not always a Nash equilibrium and without the help of an inpartial outsider the players would deviate from the strategy in search of a local optimum.

1.2 Problem: Removing the mediator

The problem in using a mediator is that the game can no longer be run with two players. A question arises: Can the mediator be replaced by some method, using cryptography? The answer is yes, but the models of game theory and cryptography are different. Therefore the setting must be modified a bit. An obvious additional requirement is that the players can interact and they are computationally bounded, so that they can crack the underlying cryptographic primitives with only a negligible probability. We must also remember that in cryptography, it is usually assumed that at least one player is honest and wants to complete the protocol correctly. In game theory, all players are selfish and rational, and will cheat if they see they will benefit from it.

1.3 Related work

There exists some related work done in game theory. Various methods have been presented to remove the mediator, for example, in an information-theoretic setting, Barany [3] substituted the mediator with four players. In cryptography, similar solutions have been applied in generic two-party secure computations [5] [6], mix-networks [7] [8], encryption schemes with blinding properties [10] [9] and so on.

2 Problem definition

2.1 Correlated equilibrium

The results of the paper are demonstrated on finite (two-player) strategic games with perfect information. Such games have two players 1 and 2, and a finite set of possible actions A_1 and A_2. The payoff functions $u_i : A_1 \times A_2 \to R(i = 1, 2)$ are known to both players.

Correlated strategy means that the mediator samples a pair of actions (a_1, a_2) according to a *joint* probability distribution $s(A_1 \times A_2)$ and recommends the action a_i to player i. $u_1(a'_1, s_2|a_1)$ is the expected payoff of player 1 if he plays a'_1 and his recommended action was a_1.

Definition 2.1 (Correlated equilibrium) *is a strategy profile* $s^* = s^*(A_1 \times A_2) = (s^*_1, s^*_2)$*, such that for any* (a^*_1, a^*_2) *that has non-zero probability, and any* $a_1 \in A_1$ *and* $a_2 \in A_2$*, we have* $u_1(a^*_1, s^*_2|a^*_1) \geq u_1(a_1, s^*_2|a^*_1)$ *and* $u_2(s^*_1, a^*_2|a^*_2) \geq u_2(s^*_1, a_2|a^*_2)$.

Example 2.2 *We consider a* 3×3 *game of two players shown in the table below. Each player can play one of the actions x,y, or z.*

	x	*y*	*z*
x	*5,5*	*1,6*	*1,1*
y	*6,1*	*0,0*	*2,0*
z	*1,1*	*0,2*	*3,3*

This game has (at least) the following Nash equilibria:

strategy	*payoff*
(x, y)	$[1, 6]$
(y, x)	$[6, 1]$
$(0.5x + 0.5y, 0.5x + 0.5y)$	$[3, 3]$
(z, z)	$[3, 3]$

The first two strategies are unfair. The highest payoffs are (3,3). But a correlated strategy can do better. If we choose the set of actions: $\{(x, x), (x, y), (y, x), (z, z)\}$*, each of which is played with equal probability, the payoffs achieved are much* *higher. The table below shows the expected payoffs of actions recommended to player 1, and the expected payoffs if player 1 deviates from its given action. For example, from the first row we see that if player 1 is recommended to play x, the other player recommended to play x or y with equal probabilities. The expected payoff is 3 if player 1 follows the recommendation. Payoffs from deviations are 3 and 0.5, which does not motivate player 1 to cheat. As the game table is symmetric, the same actions and payoffs applies to player 2 as well.*

a_1^*	s_2^*	$u_1(a_1^*, s_2^*\|a_1^*)$	$u_1(a_1, s_2^*\|a_1^*)$
x	$0.5x + 0.5y$	*3*	$u_1(y, s_2^*\|x) = 3$,$u_1(z, s_2^*\|x) = 0.5$
y	x	*6*	$u_1(x, s_2^*\|y) = 5$,$u_1(z, s_2^*\|y) = 1$
z	z	*3*	$u_1(y, s_2^*\|y) = 2$,$u_1(x, s_2^*\|y) = 1$

2.2 Extended games

In order to include the cryptographic model in the game-theoretic setting, the notion of two-player games has to be extended with the extra requirements from cryptography. These are 1) the players are computationally bounded, and 2) can communicate prior to playing the game.

The extended game is carried out as follows.

1. players exchange messages
2. choose their moves
3. execute them simultaneously

The formal defininition of the computational power of the players requires the introduction of a security parameter and that the strategies are restricted to probabilistic polynomial time (PPT). This means that it should be possible to compute the strategy with an algorithm that runs in polynomial time and that uses the outcome of a random process (a coin flip, for example) in making decisions. More information in, for example [11]

Definition 2.3 (Computational Nash equilibrium) *of an extended game G is an independent strategy profile (s_1^*, s_2^*), such that*

- *both s_1^*, s_2^* are PPT computable; and*
- *for any other PPT computable strategies s_1, s_2 there exists a negligible function μ such that on security parameter k, we have $u_1(s_1, s_2^*) \leq u_1(s_1^*, s_2^*) + \mu(k)$ and $u_2(s_1^*, s_2') \leq u_2(s_1^*, s_2^*) + \mu(k)$*

Removing the mediator is done so that the players must execute a cryptographic algorithm which securely computes the correlated equilibrium $s(A_1 \times A_2)$ and which helps the players to pick their moves without revealing them to the other player. This does not completely define the strategies of the players yet. We must remember that cryptography alone does not prevent the players from cheating. Therefore, it has to be made sure that the cheating player gains nothing by not following the protocol. A punishment for deviations is therefore introduced. The cheating player's payoff is reduced to its *minimax level*. The minimax level of player 2 is $\underline{v_2} = min_{s_1} max_{s_2} u_2(s_1, s_2)$. This is the smallest payoff that the other player can force on the cheating player. It can be shown that the expected payoff in the correlated equilibrium is always higher than the minimax level.

Theorem 2.4 *If secure two-party protocols exist for non-trivial functions, then for any Correlated equilibrium s of the original game G, there exists an extended game G' with a computational Nash equilibrium σ, such that the payoffs for both players are the same in σ and s.*

Cryptographic definition of the problem As the game is assumed to be with perfect information, it is probable that the players can negotiate a correlated strategy that is beneficial for both players. In the paper it has been assumed that a protocol for such a negotiation exists. The problem is not so much on finding a correlated equilibrium in the first place, but in making sure that the players actually follow the strategy. Therefore, the strategy (which is a probability distribution over the pairs of actions) is given as a set of pairs of actions $\{(a_1, b_1)...(a_n, b_n)\}$. As some pairs may be more probable than others in the strategy, the list may contain dublicates. Now, the problem can be defined cryptographically as follows.

Definition 2.5 (Correlated element selection (CES)) *Two players, A and B, know a list of pairs $(a_1, b_1), \ldots, (a_n, b_n)$. They need to jointly choose a random index i, and have player A learn only the value a_i and B only the value b_i.*

3 Replacing the mediator

The replacing of the mediator has to be done in several steps. In this section the building blocks, blindable encryption, zero knowledge proofs and key generation are explained briefly. In the following sections, the Preparer means the party who begins the protocol and the Chooser means the second participant.

3.1 Blindable encryption

A blindable encryption scheme is a public key encryption scheme with the following operations: Key-generation, Encryption, Decryption, Blind and Combine. Blind is a (PPT) algorithm $Blind_{pk}(c, m')$ that produces a random encryption of $m + m'$ The (PPT) algorithm Combine works so that

$$Blind_{pk}(Blind_{pk}(c, m_1; r_1), m_2; r2) = Blind_{pk}(c, m_1 + m_2; Combine_{pk}(r_1, r2))$$

when r_1, r_2 are random coins used by two successive blindings.

Thus, in a blindable encryption scheme it is possible to change the encryption of the underlying plaintext m to an encryption of a plaintext m+m' without being able to decrypt the message. The Combine operation, on the other hand, combines several blindings into one operation.

The blindable encryption scheme should be *semantically secure*. An encryption scheme is semantically secure, if the ciphertext does not reveal any extra information on the plaintext, i.e. information that the adversary does not know anyway. Many encryption schemes can be transformed into a blindable encryption scheme, for example, the ElGamal and the Goldwasser-Micali schemes have such a property. Blinding is often used in electronic voting. For more information on blindings, see [12].

The El Gamal blindable encryption scheme

1. key generation:
   - pick random k-bit prime $p = 2q + 1$, where q is prime
   - pick a generator g for the subgroup Q of quadratic residues modulo p.
   - pick random $x \in \mathcal{Z}_q$
   - set $h = g^x$
   - the secret key is x, the public key is h (and p)
2. encryption:
   - m =message
   - pick random $r \in \mathcal{Z}_q$
   - set $E(m) =< g^r, h^r \cdot m >$
3. blinding:
   - choose r' randomly from $\mathcal{Z}_q$
   - ciphertext $< s, t >$ is blinded with factor m': $Blind(< s, t >, m') =< s \cdot g^{r'}, t \cdot h^{r'} \cdot m' >$

We note that if $s = g^r$ and $t = h^r \cdot m$ (for some unknown r and m) then $Blind(< s, t >, m') =< g^{r+r'}, h^{r+r'} \cdot (mm') >$, which is a random encryption of mm' since $(r + r' mod q)$ is random when r' is. The Combine (r_1, r_2) operatio n is just $(r_1 + r_2 mod q)$

3.2 Zero knowledge proofs

The protocol uses many zero knowledge proofs. A zero knowledge proof means that something, a possession of information for example, is proven to someone without revealing the contents of the information. The proofs usually follow a protocol, a series of questions, for example, that cannot be answered without knowing the information. There are many types of zero knowledge proofs, parallel and noninteractive ones for example. Good examples of zero knowledge proofs used in cryptography can be found in [12].

The following things in the protocol presented in the next section need to be proven in zero-knowledge: proper permutation, knowledge of the index l and the blinding factor and the proof of proper encryption. The appendix of [1] contains some protocols for these proofs.

3.3 Key generation

If the keys are not generated in advance by a trusted third party, but by P (Preparer), the beginner of the protocol, then the other party C (Chooser) has to ensure that P does a *committing* encryption. This means that P cannot open the encryption in more than one way and that the output of the blinding operation is independent of which ciphertext of a given message was used as an input. The way to do this depends on the encryption scheme. A protocol for The El-Gamal version can be found in the appendix of [1]. Another, a more generic way, is to have P prove in zero knowledge that it followed the key generation algorithm properly.

4 Complete protocol

This protocol solves the correlated element selection problem with only two players.

Protocol CES-2 Common inputs: List of pairs $\{(a_i, b_i)\}_{i=1}^n$,
public key pk. Preparer knows: secret key sk

1. P: Permute and Encrypt

   Pick a random permutation π over $[n]$, and random strings $\{(r_i, s_i)\}_{i=1}^n$. Let

   $$(c_i, d_i) = (Enc_{pk}(a_{\pi(i)}; r_{\pi(i)}), Enc_{pk}(b_{\pi(i)}; s_{\pi(i)}))$$

   for all $i \in [n]$. Send $\{(c_i, d_i)\}_{i=1}^n$ to C.

   Sub-protocol Π_1: p proves in zero-knowledge that it knows the randomness$\{(r_i, s_i)\}_{i=1}^n$ and permutation π that were used to obtain the list $\{(c_i, d_i)\}_{i=1}^n$.

2. C : Choose and Blind

   Pick a random index $l \in [n]$.
   Send to P the ciphertext $e = Blind_{pk}(c_l, 0)$.

   Sub-protocol Π_2: C proves in a witness-hiding manner that it knows the randomness and index l that were used to obtain e.

3. P : Decrypt and Output

Set $\alpha = Dec_{sk}(e)$. Output a.
Send to C the list of pairs $\{(b_{\pi(i)}, s_{\pi(i)})\}_{i=1}^{n}$ (in this order)

4. C : Verify and Output
Denote by (b, s) the l'th entry in this list. If $d_l = Enc_{pk}(b; s)$ then output b.

5 Conclusions

The most interesting part of the paper is the combination of game theory and cryptography. The cryptographic solutions used were not new, therefore the focus of this essay was more on the advantages they bring to the game-theoretic world. Skipping the actual construction of the correlated equilibrium was unfortunate. The reason might be that the general case of finding all the equilibria is still somewhat an active field of research.

In the epilogue, the authors ponder if it were possible "to know what the players are up to" in some models. This would certainly simplify the design of secure protocols. However, usually in the cryptographic field, the adversaries manage to find new ways to attack protocols every time something like that is imagined to be achieved. Therefore, one should be cautious of such "silver bullet" solutions.

References

[1] Y. Dodis, S. Halevi and T. Rabin: A Cryptographic Solution to a Game Theoretic Problem. *Crypto 2000*.

[2] R. Aumann: Subjectivity and Correlation in Randomized Strategies. In *Journal of Mathematical Economics*, 1, pp. 67-95, 1974.

[3] I. Barany: Fair distribution protocols or how the players replace fortune. *Mathematics of Operations Research*, 17(2):327-340, 1992.

[4] J.F. Nash: Non-Cooperative Games. *Annals of Mathematics*, 54 pages 286-295.

[5] O. Goldreich, S. Micali, and A. Widgerson: How to play any mental game. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing*, pages 218-229.

[6] A.C. Yao: Protocols for secure computations (extended abstract). In *23rd Annual Symposium o n Foundations of Computer Science*, pages 160-164. IEEE, 1982.

[7] M. Abe: Universally verifiable Mix-net with Verification Work Independent on the number of Mix-canters. In *Proceedings of EUROCRYPT'98*, pages 437-447, 1998.

[8] M. Jakobsson: A practical Mix. In *Proceedings of EUROCRYPT'98*, pages 448-461, 1998.

[9] T. Sander, A. Young, and M. Yung: Non-interactive CryptoComputing for NC1. In *40th Annual Symposium on Foundations of Computer Science*, pages 554-567. IEEE, 1999.

[10] J. Garay, R. Gennaro, C. Jutla, T. Rabin: Secure distributed storage and retrieval. In *Proceedings of 11th International Workshop on Distributed Algorithms (WDAC'97)*, volume 1320 of *Lecture Notes in Computer Science*, pages 275-289. Springer-Verlag, 1997.

[11] Michael Sipser: Introduction to the Theory of Computation, PWS Publishing Company, 1997.

[12] Bruce Schneier: Applied Cryptography, John Wiley & sons, Inc. 1996.