Cryptography meets Game Theory:

Utility Dependence in Correct and Fair Rational Secret Sharing (CRYPTO09)

Gilad Asharov and Yehuda Lindell

Department of Computer Science, Bar-Ilan University

אוניברסיטת בר-אילן

Game Theory and Cryptography

Game theory and cryptographic protocol design are concerned with "interactions" between mutually distrusting parties. These two subjects have developed almost independently.

In the standard model of **cryptography**, the parties are divided into two distinct sets: those that are *completely honest* and those that are *corrupt and malicious. Malicious* parties (also known as adversaries) are willing to do anything to break the protocol.

In **game theory**, the parties are considered to be *rational individuals* who try to maximize their utility. Each party has a utility function that specifies their gain in every possible outcome of the interaction (game), and the parties' aim is to obtain the highest possible gain.

Two main directions lie in the intersection between cryptography and game theory:

- **Applying cryptography to game theory**: solving game theoretic problems using cryptography (e.g., implementing a *mediator* using *secure computation*).
- **Applying game theory to cryptography:** constructing cryptographic protocols for *rational* parties. An example of this direction is *rational secret sharing*.

Rational Secret Sharing

Secret sharing is a central building block of modern cryptography. A ***t***-out-of-***n*** secret sharing scheme allows someone to share a secret ***s*** among ***n*** parties so that:

- ***Secrecy:*** no subset of less than ***t*** parties learn anything about the secret ***s***.
- ***Reconstruction:*** any subset of ***t*** parties can learn the secret ***s*** by combining their shares.

Rational secret sharing studies the *cryptographic* problem of secret sharing when all parties participating in the reconstruction are *rational*.

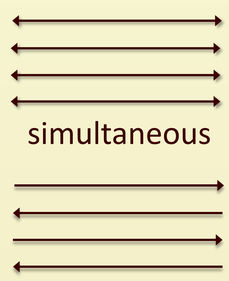
Preliminaries

Utility Functions: Knowledge is power and *exclusive* knowledge is even more power: the basic assumption is that parties gain more by learning than by not, and that they gain the most by being the only one to learn.

P_1 learns ***s***	P_2 learns ***s***	P_1's utility	P_2's utility
NO	NO	U_1^-	U_2^-
NO	YES	U_1^-	U_2^+
YES	NO	U_1^+	U_2^-
YES	YES	U_1	U_2

The formal assumption is that for every **i**, it holds that that $U_i^+ > U_i > U_i^-$

Communication Model: We assume that the parties are connected via a broadcast channel. There are two types of broadcast channels that have been considered:



- **Simultaneous**: parties can exchange messages "fairly"; each party sends its message independently of other messages.
- **Non-simultaneous**: essentially, only one party sends a message in any given time slot (this is the real-world model).

The Problem – Naïve Reconstruction

Consider 2-out-of-2 secret sharing, in the simultaneous channel model, and reconstruction that works by both parties simply sending their shares to one another. A party can send its share (*cooperate*) or can not send its share (*defect*). The utilities of the parties based on these possible actions are:

	P_2 cooperates	P_2 defects
P_1 cooperates	P_1 receives U_1 P_2 receives U_2	P_1 receives U_1^- P_2 receives U_2^+
P_1 defects	P_1 receives U_1^+ P_2 receives U_2^-	P_1 receives U_1^- P_2 receives U_2^-

It is never better to cooperate!

Previous Solutions – Fair Reconstruction

All previous solutions for this problem have the property that the *actual utility functions* of all parties are known. **This assumption is very problematic**.

All previous solutions in the *non-simultaneous* channel model have the property that one party can cause the other to output a wrong secret (at the expense of not learning the secret). We denote the utility of a party when it causes the above result to occur by U^f. If $U^f > U$, then these protocols **do *not* achieve correctness**.

Questions

1. Is it possible to construct a **single** fair reconstruction protocol that works irrespective of the actual values of the utility functions (as long as they fulfill the assumptions)? Such a solution would be ***utility independent***.
2. Is it possible to construct a protocol for the non-simultaneous model that achieves **correctness** (i.e., correct fair reconstruction even when $U^f > U$)?

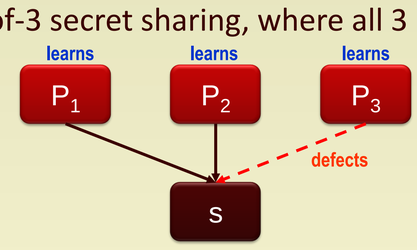
Our Results

1. Utility independent fair reconstruction is ***impossible*** in the 2-party case.
2. Utility independent is ***impossible*** in the t-out-of-n case with coalitions of size t/2 or greater.
3. Utility independent is ***possible*** in the t-out-of-n case with coalitions of size less than t/2, in the simultaneous channels model (*see protocol below*).
4. Correct fair reconstruction in the non-simultaneous channel model is possible **if and only if** the actual U^f utility values of all parties are known.

Utility Independent Fair Reconstruction (simultaneous channels)

The protocol is based on the observation that an **additional share** (beyond the minimum needed to reconstruct) helps to achieve fairness.

Consider the naïve reconstruction protocol for 2-out-of-3 secret sharing, where all 3 parties participate in the reconstruction phase. Even if one party defects, all the parties learn the secret. Therefore, there is *nothing to gain* by defecting when all others cooperate. However, it is still never worse to defect than cooperate (and can even be better, for example if one other party defects).

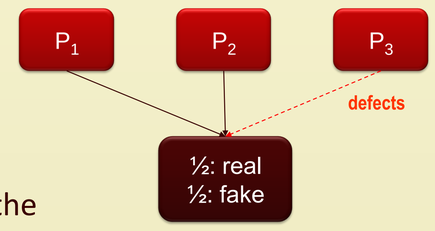


In order to utilize the above observation, we construct a protocol where **defecting can be worse than cooperating**. In this case, if defecting does not help (e.g., when there is an additional share), then it is better to cooperate.

Protocol: Consider an online dealer (implemented by secure computation) running many rounds. In every *round*:

- With probability ½ the dealer sends the parties shares of the real secret;
- With probability ½ the dealer send shares of a fake secret.

If any one of the parties defect in a round, then all the other parties halt immediately.



Analysis: If a party **defects** (and all other cooperate):

- With probability ½ all learn the secret (because of the additional share) and all gain utility **U**.
- With probability ½ the dealer sent shares of a fake secret and all parties stop the protocol. In this case, no one learns the secret and all gain U^-.

Thus, the expected utility when *defecting* is $\frac{1}{2}U + \frac{1}{2}U^-$.
In contrast, the expected utility when *cooperating is* **U**.
Since $U > U^-$, it follows that $U > \frac{1}{2}U + \frac{1}{2}U^-$ and so it is better to **cooperate**.

Obtaining an additional share: An additional share can be effectively obtained by sharing a random pad **r** with threshold **t**, and then sharing the secret XOR **r** with threshold less than **t**.