ב"ה

JUBILEE: Secure Debt Relief and Forgiveness

David Cerezo Sánchez
david@calctopia.com

Yom Kippur
10th of Tishrei, 5782
Shmitah and Yovel [*]

Abstract

JUBILEE is a securely computed mechanism for debt relief and forgiveness in a frictionless manner without involving trusted third parties, leading to more harmonious debt settlements by incentivising the parties to truthfully reveal their private information. JUBILEE improves over all previous methods:

- individually rational, incentive-compatible, truthful/strategy-proof, ex-post efficient, optimal mechanism for debt relief and forgiveness with private information

- by the novel introduction of secure computation techniques to debt relief, the "*blessing of the debtor*" is hereby granted for the first time: debt settlements with higher expected profits and a higher probability of success than without using secure computation

A simple and practical implementation is included for "The Secure Spreadsheet".

Another implementation is realised using Raziel smart contracts on a blockchain with Pravuil consensus.

Keywords: secure computation, mechanism design, debt forgiveness

JEL classification: D82, G33, H63

1 Introduction

As it is written in the Torah, the Jubilee is the remission year at the end of seven cycles of seven years when slaves and prisoners are freed, properties are returned to their original owners and debts are forgiven [1] to prevent profiting

[*] According to Chatam Sofer's way of calculating the Yovel, 118*49=5782 (caveat: others may dispute the exact year, e.g., 5782+1).

[1] Deuteronomy 15:1–6, Leviticus 25:8–13, Isaiah 61:1-2

from the poor [2]. The first Jubilee was celebrated in AM 2553, starting the count 14 years after entering Eretz Yisrael [3], as it was previously commandeth [4]: Jubilees were announced with a *shofar* [5], an instrument made from a ram's horn (i.e., a *yobhel* or *yoveil,* from which the term Jubilee is derived [6]) and they provided a regulated and periodical "clean state" for debt forgiveness.

By setting debt forgiveness on a fixed and periodical calendar, the Jubilee resolved the age-old social problem of debt relief: modernly, governments enforce an intricate system of debt collectors, courts and legal procedures. In these cases, third parties are involved to handle conflicts of interests between distrusting parties:

- debtors request too much debt forgiveness
- creditors grant debt settlements as small as possible, trying to take as many assets as possible from debtors: in some instances, the true amount of debt relief needed is less than the expected revenue from the debtor to fulfil their debt obligations, but the stated debt recovery values from creditors exceed said expected revenue and/or continuation value of the debtor, making it financially impossible for the debtor to compensate the creditors. As a result, future projects from debtors will not be undertaken, even if socially desirable, sacrificed to satisfy the overstated demands from creditors.

For the first time, by combining mechanism design and secure computation we manage to reconcile the demands of debtors and creditors in to create a new debt relief mechanism in which the best course of action is the truthful revelation of their private information: removing most of the conflict from the situation, third parties are no longer needed and frictionless debt settlements can be reached.

1.1 Contributions

In summary, we make the following contributions:

- an individually rational, incentive-compatible, truthful/strategy-proof, ex-post efficient, optimal mechanism for debt relief and forgiveness with private information is introduced
- further, an implementation using secure computation is presented

In a nutshell, we contribute a new methodology for debt relief and forgiveness in a frictionless and strifeless way without resorting to third parties (i.e., courts, debt collectors), revamping an age-old problem with modern cryptographic techniques such that truthful revelation of private information is the best strategy for all parties involved.

[2] Exodus 22:25

[3] Rambam in Mishneh Torah, Sabbatical Year and the Jubilee 10:2

[4] Leviticus 25:2

[5] Ibn Ezra on Leviticus 25:9; Rashi on Leviticus 25:10

[6] Ramban on Leviticus 25:10

In section 2, we discuss related literature and prior work. In section 3, we first introduce our model, then proceed to describe a direct mechanism for debt settlements, and finally describe the optimal mechanism. In section 4, we describe our implementations of the optimal mechanism and then we conclude in section 5.

The reader interested in the most practical applications may skip to section 4,

2 Related Literature

The literature on the combination of secure computation and mechanism design is surprisingly scarce: it mostly focuses on the problems of secure computation with rational actors [ADGH06, IML05, HT04, GK06, OPRV08], and the combination of secure computation with the incentive-compatible Vickrey auction or its generalisation as the Vickrey–Clarke–Groves mechanism [EL03, NPS99, BS05]. Truthfulness is absolutely necessary for secure computation to gain acceptance in the real world: although any truthful mechanism can be securely computed [Xia11], the converse does not hold. Thus, further research is needed to devise securely computed mechanisms that encourage participants to report their information truthfully.

2.1 Prior Work in Cryptography

Previous literature considered the use of secure computation technologies for credit origination and rating [BP20, DDN$^+$15, AKL12, HFT21, FAZ05], but not for debt relief.

This paper also shows that the moral character of cryptographic work [Rog15] goes way beyond preventing "*mass surveillance*", as it's currently customary in the field of cryptography.

2.2 Prior Work in Game Theory

Some seminal papers [O'N81, AM85] started the game-theoretic study of bankruptcy problems in the Talmud: see [HV01, Tho13] for surveys of the extensive literature that followed, including alternative derivations of the Mishnah of the Talmud rule [7] using cooperative bargaining [DV93] and the strategic Nash cooperative solution [MTY20]. Note that the Talmud rule is so influential that it was adopted as law (*halakha*) in other contexts [8] and it became a source of great discussion[9] as Talmud scholars were trying to unravel and interpret it.

[7] Rabbi Nathan in Babylonian Talmud, Kethuboth 93a; Yerushalmi Talmud, Kethuboth 10,4

[8] Rambam in Mishneh Torah, Malveh veLoveh, Chapter 20, Section 4

[9] Rabbi Seadia Gaon in Responsa Sha'arei Zedeq part 4, gate 4; Rabbi Hai Gaon as quoted by Rabbi Isaac Alfasi on Kethuboth 93a; Rabbi Bezalel Ashkenazi in Shitah Mekubetzet on Kethuboth 93a; Piniles H.M. in Darka Shel Torah, p. 64; Rabbi Yehoshua Leib Diskin in Torat Ha'Ohel, vol. 1 page 2b

This paper fundamentally departs from this line of work found in the game-theoretic literature:

1. it focuses on debt relief via debt settlements, it's not restricted to equitable partitions between creditors
2. creditors are allowed to have private information (i.e., all information is not public)
3. it uses cryptography as a primary tool to achieve its goals
4. it performs better than the Talmud rule in neutralising creditor's conflict of interests

The ultimate reason for this innovation is "*mi-p'nei tikkun ha-olam*" (i.e., for the bettering of the world, and for repairing the world, as modernly interpreted): as participation is individually rational for creditors (see next condition 3.3), it is economically rational to participate even with the institution of the *prozbul* [10], a legal subterfuge to circumvent the commandeth forgiveness of loans even after the Shmitah and the Yovel.

3 Model and Design

This paper is primarily concerned with a setting of distrusting parties, a debtor entity and multiple creditors, holding asymmetric information used as input in a process to settle non-marketable debt (i.e., creditors are assumed not to trade between themselves). The debtor entity is an intentional generalisation in order to abstract away the more specific cases of a private party, a corporation or an indebted sovereign state: note that each of these specific cases may need further refinements to this general model. The results of this section are themselves based on these works: [Mye81].

3.1 Model Setup

A highly indebted entity with total outstanding debt D and no cash in hand needs funds from external sources for an investment of I (i.e., for debt service and to finance another project) that will generate future cash flows given by the Discounted Cash Flow of the current Asset continuation value plus the Investment value, $A + I$: if the entity files for bankruptcy, the opportunity of the investment in the other project will be lost. It is assumed that the entity is prohibited by existing covenants from issuing new higher priority debt senior to the existing outstanding debt: in other words, the entity can only undertake the investment if it settles the outstanding debt after successful negotiations with n risk-neutral creditors to fully or partially write down the principal of the debt since creditors would be the main beneficiaries of the investment I, thus avoiding bankruptcy and ensuring the continuation of the debtor entity.

[10] Gittin 4:3; Mishnah Sheviit 10

To ease exposition, we assume that the risk-free interest rate is zero and that each creditor has an identical share of the total outstanding debt, $d = (D/n)$, each with equal priority. The willingness to cancel some of the debt depends on two factors:

1. The estimated percentage of debt cancellation from other creditors.
2. The expected recovery value θ_i for each creditor i in case of bankruptcy if the entity does not receive any investments and/or debt cancellation, and we assume that θ_i represents the expected recovery value if the creditor owned claims to his proportional part n of the total entire value of the entity.

The creditor type θ_i is private information and everyone holds identical expectations about the possible value of θ_i, captured by the random variable

$$\Theta_i : \left[\underline{\theta}, \overline{\theta}\right] \rightarrow [0, 1]$$

with distribution $F(\theta_i)$, density $\phi(\theta_i)$, and $\overline{\theta} \leq D$. With each creditor acting as Bayesian decision-maker [Har67], creditor types are identically and independently distributed, its list denoted by the vector $\theta = (\theta_1, \dots, \theta_n)$ and the set of all possible types of $s = 1, 2, \dots, n$ creditors arise from their different preferences, given by

$$I_s = \left\{\theta \mid \underline{\theta} \leq \theta_j \leq \overline{\theta} \,\text{for}\, j = 1, 2, \dots, s\right\}$$

Remark 1. We assume that each creditor θ_i are the only private knowledge, that is, the vector $\theta = (\theta_1, \dots, \theta_n)$.

We further assume that $F(\theta_i)$, D, A, and I are common knowledge. There would be no uncertainty about how much debt forgiveness should be granted if the vector θ was publicly known.

Additionally, we define

$$\begin{aligned}\phi(\theta) &= \prod_{j=1}^{n} \phi(\theta_j) \\ \theta_{-i} &= (\theta_1, \dots, \theta_{i-1}, \theta_{i+1}, \dots, \theta_n) \\ \phi(\theta_{-i}) &= \prod_{j \neq i} \phi(\theta_j)\end{aligned}$$

Creditor i may also know the expected recovery by other creditors (i.e., using secure computation), in that case, the revised expected recovery value in bankruptcy would be given by the following liquidation value

$$l_i(\theta_i, \theta_{i-1}) = \theta_i + \sum_{j \neq i} e_i(\theta_j)$$

with non-decreasing revised estimation function $e_i : \left[\underline{\theta}, \overline{\theta}\right] \rightarrow \mathbb{R}$ defining how the creditor would revise his estimate if he knew the estimate of creditor j , and satisfying

$$\int_{\underline{\theta}}^{\overline{\theta}} e_i\left(\theta_j\right)\phi\left(\theta_j\right)d\theta_j = 0, \text{ such that } \forall j \neq i, \tag{3.1}$$

implying that θ_i would still be the expected recovery value of θ_i because

$$\int_{I_{n-1}} l_i\left(\theta_i, \theta_{-i}\right)\phi\left(\theta_{-i}\right)d\theta_{-i} = \theta_i.$$

As it is evident, the expected recovery value of θ_i cannot exceed the full value of the debt,

$$l_i\left(\theta_i, \theta_{-i}\right) \leq d \text{ such that } \forall\theta_i \in \left[\underline{\theta}, \overline{\theta}\right], \theta_{-i} \in I_{n-1}.$$

In this paper we use the following definition of efficiency:

Definition 2. (*Ex-post* efficiency). We consider a debt relief process by debt settlement to be *ex-post* efficient if and only if the entity remains solvent after the new investment is undertaken with probability one when

$$A \geq \sum_{i=1}^{n} l_i\left(\theta_i, \theta_{-i}\right),$$

and if the investment is undertaken with probability zero, the entity goes bankrupt. Debt settlement can only be efficient if there is a surplus in the difference between the value of an entity in solvency and the value of the entity in bankruptcy,

Finally, note that the problem of debt settlement is a problem of asymmetric information: if the debtor entity knew the true value of θ_i for every creditor, it would be individually rational to propose a settlement arrangement giving each creditor i his expected recovery value if and only if the settlement arrangement is *ex-post* efficient (i.e., continuation would be Pareto-efficient) and all creditors would accept. Thus, asymmetric information is a key feature of debt settlements and θ_i is assumed to be private information: hence the use of secure computation, to enable the privacy-preserving computation of said private information between the distrusting parties.

3.2 A Direct Mechanism for Debt Settlement

In this sub-section, we obtain an *ex-post* efficient revelation mechanism to settle the outstanding debt, by making use of the Revelation Principle:

Definition 3. (Revelation Principle [Mye81]). Every equilibrium outcome of any arbitrary mechanism can be implemented as an outcome in a truth-telling equilibrium of an incentive-compatible direct revelation mechanism.

For each creditor, it's the best response to report his true type in a truth-telling Bayesian equilibrium point of the revelation game, thus creditors and the debtor entity would follow the instructions of the following protocol:

Functionality $\mathcal{F}_{YOVEL}$

1. Each creditor privately reports their private information θ_i to a trusted party, at the same time.
2. Using the private reports, a trusted party calculates and instructs:

- the debtor entity to invest with probability k, or go bankrupt with probability $1-k$. In case of continuing solvent, the entity must make payments to the creditors as defined by the vector

$$t = (t_1, \ldots, t_n)$$

- each creditor i must forgive an amount of debt equal to $d - t_i$ if the debtor is not declared bankrupt.

Figure 3.1: Ideal functionality $\mathcal{F}_{YOVEL}$

The vector of reported types is defined by

$$\hat{\theta} = \left(\hat{\theta}_1, \hat{\theta}_2 \ldots, \hat{\theta}_n\right),$$

the recommended vector of transfer payments be denoted by $t : I_n \to \mathbb{R}^n$, and the recommended probability $k : I_n \to [0,1]$ of continuing solvent and receiving investment.

Let $\Gamma = (t, k)$ denote the mechanism implemented by the trusted party in the ideal model or a Secure Multi-Party Computation program in the real model, then $t_j\left(\hat{\theta}_i, \theta_{-i}\right)$ is the payment to creditor j, and $k\left(\hat{\theta}_i, \theta_{-i}\right)$ is the investment probability when creditor i reports $\hat{\theta}_i$ and all the creditors announce their true types. Note that for the mechanism to be truthful equilibrium, it must be individually rational for all players to participate and an equilibrium for each creditor to report their true θ_i.

The expected utility from a mechanism $\Gamma = (t, k)$ to creditor i such that it's an equilibrium to report their true type for every other creditor, is given by

$$\int_{I_{n-1}} \left\{k\left(\hat{\theta}_i, \theta_{-i}\right) t_i\left(\hat{\theta}_i, \theta_{-i}\right) + \left[1 - k\left(\hat{\theta}_i, \theta_{-i}\right)\right] l_i\left(\theta_i, \theta_{-i}\right)\right\} \phi\left(\theta_{-i}\right) d\theta_{-i},$$

rewritten as

$$\theta_i + \int_{I_{n-1}} k\left(\hat{\theta}_i, \theta_{-i}\right) \left[t_i\left(\hat{\theta}_i, \theta_{-i}\right) - l_i\left(\theta_i, \theta_{-i}\right)\right] \phi\left(\theta_{-i}\right) d\theta_{-i}.$$

using the definition of $l_i\left(\theta_i, \theta_{-i}\right)$ and the properties of the revised estimation function 3.1. The change in expected utility is given by

$$U\left(\theta_i, \hat{\theta}_i, t_i, k\right) = \int_{I_{n-1}} k\left(\hat{\theta}_i, \theta_{-i}\right) \left[t_i\left(\hat{\theta}_i, \theta_{-i}\right) - l_i\left(\theta_i, \theta_{-i}\right)\right] \phi\left(\theta_{-i}\right) d\theta_{-i} \quad (3.2)$$

because in case of no debt settlement, creditors get their expected recovery value θ_i and the entity goes bankrupt; but in case of staying solvent, creditors receive payments t_i but they lose the liquidation value. This change in expected utility must be positive for all creditors

$$\text{(IR)} \qquad U\left(\theta_i, \hat{\theta}_i, t_i, k\right) \geq 0, \text{ such that } \forall \theta_i \in \left[\underline{\theta}, \overline{\theta}\right], \tag{3.3}$$

for them to participate in the mechanism since debt relief can only be granted willfully outside of bankruptcy, defining the individually rational (IR) participation constraint: in other words, no party is forced to participate in the mechanism, and each creditor is granted veto power over the debt settlement via their joint control of the probability $k\left(\right)$ thus effectively imposing negative externalities on each other (note that extensions to this model introducing majority voting rules are also possible).

On the other hand, the expected utility of the debtor entity from the mechanism $\Gamma = (t, k)$ in a truth-telling equilibrium is

$$V\left(\theta, k, t\right) = \int_{I_n} k\left(\theta\right) \left(A - \sum_{i=1}^{n} t_i\left(\theta\right)\right) \phi\left(\theta\right) d\theta, \tag{3.4}$$

also subject to a positive Ex-Ante Budget Balance (EXABB) participation constraint

$$\text{(EXABB)} \qquad V\left(\theta, k, t\right) \geq 0 \tag{3.5}$$

An additional incentive-compatibility constraint (IC) for the mechanism $\Gamma = (t, k)$ must be satisfied for truthful reporting to be an equilibrium, which in conjunction with the individually rational (IR) participation constraint 3.3 define the mechanism as a feasible mechanism:

$$\text{(IC)} \quad U\left(\theta_i, \hat{\theta}_i, t_i, k\right) \geq U\left(\theta_i, \theta_j, t_i, k\right), \text{ such that } \forall \theta_i, \theta_j \in \left[\underline{\theta}, \overline{\theta}\right], \forall i, j. \tag{3.6}$$

To obtain incentive-compatibility [Mye81], it's a first necessary and sufficient condition that

$$K\left(\theta_i\right) = \int_{I_{n-1}} k\left(\theta_i, \theta_{i-1}\right) \phi\left(\theta_{-i}\right) d\theta_{-i}$$

must be decreasing in θ_i for all $\theta_i \in \left[\underline{\theta}, \overline{\theta}\right]$. In other words, the higher the expected recovery value of a creditor the smaller the probability that the entity will remain solvent as expected by that same creditor. The other second necessary and sufficient condition derived from [Mye81] is that $\forall \theta_i$,

$$U\left(\theta_i, \theta_i, t_i, k\right) = U\left(\bar{\theta}, \bar{\theta}, t_i, k\right) + \int_{I_{n-1}} \int_{\theta_i}^{\bar{\theta}} k\left(u, \theta_{-i}\right) du \phi\left(\theta_{-i}\right) d\theta_{-i} \geq 0, \tag{3.7}$$

granting, for the highest type $\overline{\theta}$, the expected change in utility to each creditor i plus a positive mark-up: the new rightmost term of the right-hand side is an economic incentive given to creditors of type $\theta_i < \overline{\theta}$ by the mechanism to induce them to reveal that they are the creditors more inclined to grant debt forgiveness (i.e., an "informational rent"). To derive the equation 3.7, we start denoting by $\hat{U}\left(\theta_{i,}\theta_{i,},k,t\right)$ as the maximum utility of creditor i from the mechanism (k,t): then, by the envelope theorem[Sam47, Mil04, MS02],

$$\frac{d\hat{U}}{d\theta_i} = -\int_{I_{n-1}} k\left(\theta_i,\theta_{-i}\right)\phi\left(\theta_{-i}\right)d\theta_{-i} \leq 0$$

Therefore, by reintegration we obtain the previous equation 3.7

$$\begin{aligned}\hat{U}\left(\theta_i,\theta_i,k,t\right) &= U\left(\bar{\theta},\bar{\theta},t,k\right) + \int_{I_{n-1}}\left(\int_{\theta_i}^{\bar{\theta}}\frac{d\hat{U}}{du}du\right)\phi\left(\theta_{-i}\right)d\theta_{-i} \\ &= U\left(\bar{\theta},\bar{\theta},t,k\right) + \int_{I_{n-1}}\int_{\theta_i}^{\bar{\theta}} p\left(u,\theta_{-i}\right)du\phi\left(\theta_{-i}\right)d\theta_{-i}\end{aligned}$$

Now let's look at the incentive-compatible mechanism most favourable to the debtor, that is, when $U\left(\bar{\theta},\bar{\theta},t_i,k\right)=0$: then, the amount the debtor will pay is the expected recovery value plus an additional economic incentive derived from 3.7,

$$\int_{I_n} k\left(\theta\right)t_i\left(\theta_i,\theta_{-i}\right)\phi\left(\theta\right)d\theta = \int_{I_n} k\left(\theta\right)\left[l_i\left(\theta_i,\theta_{-i}\right)+\frac{F\left(\theta_i\right)}{\phi\left(\theta_i\right)}\right]\phi\left(\theta\right)d\theta \tag{3.8}$$

To derive equation 3.8, we start from 3.2 and 3.7,

$$\begin{aligned}\int_{I_{n-1}} k\left(\theta_i,\theta_{-i}\right)t_i\left(\theta_i,\theta_{-i}\right)\phi\left(\theta_{-i}\right)d\theta_{-i} &= \int_{I_{n-1}} k\left(\theta_i,\theta_{-i}\right)l_i\left(\theta_i,\theta_{-i}\right)\phi\left(\theta_{-i}\right)d\theta_i \\ &+ \int_{I_{n-1}}\int_{\theta_i}^{\bar{\theta}} k\left(u,\theta_{-i}\right)du\phi\left(\theta_{-i}\right)d\theta_{-i}\end{aligned}$$

By taking expectations over all possible values of θ_i, we obtain

$$\begin{aligned}\int_{I_n} k\left(\theta\right)t_i\left(\theta_i,\theta_{-i}\right)\phi\left(\theta\right)d\theta &= \int_{I_n} k\left(\theta_i,\theta_{-i}\right)l_i\left(\theta_i,\theta_{-i}\right)\phi\left(x\right)d\theta \\ &+ \int_{I_{n.1}}\left[\int_{\underline{\theta}}^{\bar{\theta}}\int_{\theta_i}^{\bar{\theta}} k\left(u,\theta_{-i}\right)du\phi\left(\theta_i\right)d\theta_i\right]\phi\left(\theta_i\right)d\theta_{-i}\end{aligned} \tag{3.9}$$

Integrating by parts the term in brackets, we arrive at

$$\int_{\underline{\theta}}^{\bar{\theta}}\int_{\theta_i}^{\bar{\theta}} k\left(u,\theta_{-i}\right)du\phi\left(\theta_i\right)d\theta_i = \int_{\underline{\theta}}^{\bar{\theta}} k\left(\theta_i,\theta_{-i}\right)F\left(\theta_i\right)d\theta_i$$

Thus, equation 3.9 can be rewritten as the desired equation 3.8

$$\begin{aligned}\int_{I_n} k(\theta)\, t_i(\theta_i,\theta_{-i})\, f(\theta)\, d\theta &= \int_{I_n} k(\theta_i,\theta_{-i})\, l_i(\theta_i,\theta_{-i})\, f(\theta)\, d\theta \\ &+ \int_{I_n} k(\theta_i,\theta_{-i}) \left[F(\theta_i)/\phi(\theta_i)\right] \phi(\theta)\, d\theta \\ &= \int_{I_n} k(\theta) \left[l_i(\theta_i,\theta_{-i}) + \frac{F(\theta_i)}{\phi(\theta_i)}\right] \phi(\theta)\, d\theta\end{aligned}$$

By substituting the previous relation on the debtor's expected utility 3.4, it becomes

$$\int_{I_n} k(\theta) \left(A - \sum_{i=1}^{n} \left[l_i(\theta_i,\theta_{-i}) + \frac{F(\theta_i)}{\phi(\theta_i)} \right] \right) \phi(\theta)\, d\theta \tag{3.10}$$

Theorem 4. *A mechanism $\Gamma = (t,k)$ is incentive-compatible according to constraint 3.6 (IC) and satisfies the creditor's participation constraint 3.3 (IR) and the debtor's participation constraint 3.5 (EXABB) if and only if the debtor's expected utility is strictly positive,*

$$\int_{I_n} k(\theta) \left(A - \sum_{i=1}^{n} \left[l_i(\theta_i,\theta_{-i}) + \frac{F(\theta_i)}{\phi(\theta_i)} \right] \right) \phi(\theta)\, d\theta \geq 0 \tag{3.11}$$

Proof. Note that by the debtor's participation constraint 3.5 (EXABB),

$$V(\theta,k,t) \geq 0$$

and that 3.10 is derived from the debtor's expected utility 3.4, then it trivially follows that 3.11 must also be positive. □

Definition 5. (*Blessing of the debtor*). The willingness of creditors to grant debt forgiveness is higher when using secure computation for their private information. This paradoxical situation is the opposite of the "*winner's curse*" from auction theory [BBM19]: given that an agreement on debt forgiveness among creditors must be unanimous 3.3 , then debt forgiveness could only happen if all creditors are willing to grant forgiveness because their expected recovery value from bankruptcy is low, thus the willingness of each creditor gets reinforced from the private information obtained from other creditors.

Theorem 6. *The expected profits of the debtor are higher when there are differences in private information, and not just differences in preferences, for any incentive-compatible $k(\theta)$.*

Proof. A creditor is more willing to grant debt forgiveness when there are differences in private information (i.e., *the blessing of the debtor* 5) because the expected recovery value conditional on a successful settlement is smaller than the unconditional expected recovery value, given that all creditors consider that debt settlements will only prosper when other debtholders expect a low recovery value. This allows the debtor entity to extract more debt forgiveness from creditors under private information.

Debtor's expected profits are given by 3.8 if the investment rule $k(\theta)$ is incentive-compatible. When there are only differences in preferences, the revision functions are $e_i(\theta_j) = 0$ for all values of i, j, and θ_j, thus we only need to show that

$$\int_{I_n} k(\theta) \left[\sum_{i=1}^{n} e_i(\theta_{-i}) \right] \phi(\theta)\, d\theta < 0$$

with $e_i(\theta_{-i}) = \sum_{j \neq i} e_i(\theta_j)$. By the definition of $K(\theta_i)$, the inequality can be rewritten as

$$\sum_{i=1}^{n} \sum_{j \neq i} \left[\int_{\underline{\theta}}^{\bar{\theta}} K(\theta_j)\, e_i(\theta_j)\, \phi(\theta_j)\, d\theta_j \right] < 0.$$

Since $e_i(\theta_i)$ is increasing and by definition $\int_{\underline{\theta}}^{\bar{\theta}} e_i(\theta_j)\, \phi(\theta_j)\, d\theta_j = 0$ for all i and j, there exists an $\hat{\theta}_i$ such that $e_i(\theta_j) \lesseqgtr 0$ as $\theta_j \lesseqgtr \hat{\theta}_i$, and we can write

$$\int_{\underline{\theta}}^{\hat{\theta}_i} K\left(\hat{\theta}_i\right) e_i(\theta_j)\, \phi(\theta_j)\, d\theta_j + \int_{\hat{\theta}_i}^{\bar{\theta}} K\left(\hat{\theta}_i\right) e_i(\theta_j)\, \phi(\theta_j)\, d\theta_j = 0$$

Due to incentive-compatibility we know that $K(\theta_j)$ is decreasing, hence

$$\int_{\underline{\theta}}^{\hat{\theta}_i} K(\theta_i)\, e_i(\theta_j)\, \phi(\theta_j)\, d\theta_j < \int_{\underline{\theta}}^{\hat{\theta}_i} K\left(\hat{\theta}_i\right) e_i(\theta_j)\, \phi(\theta_j)\, d\theta_j,$$

and

$$\int_{\hat{\theta}_i}^{\bar{\theta}} K\left(\hat{\theta}_i\right) e_i(\theta_j)\, \phi(\theta_j)\, d\theta_j > \int_{\hat{\theta}_i}^{\bar{\theta}} K(\theta_i)\, e_i(\theta_j)\, \phi(\theta_j)\, d\theta_j.$$

But then

$$\int_{\underline{\theta}}^{\bar{\theta}} K(\theta_j)\, e_i(\theta_j)\, \phi(\theta_j)\, d\theta_j < K\left(\hat{\theta}_i\right) \int_{\underline{\theta}}^{\bar{\theta}} e_i(\theta_j)\, \phi(\theta_j)\, d\theta_j = 0.$$

□

A recent impossibility result [JM00] further limits mechanisms' ability to implement efficient allocations when creditors' private values aren't private information (i.e., with secure computation as used here).

Theorem 7. *(Jehiel-Moldovanu Impossibility Theorem [JM00, Mil04]). Let $\Gamma(\theta)$ be a mechanism where the liquidation value $l_i(\theta_i, \theta_{i-1})$ depends on the valuations of other creditors but without private information, and suppose that the function $E\left(\theta^i\right) \equiv E\left[\Gamma^i(\theta)\,|\theta^i\right]$ depends non-trivially on θ^i_{-i}. Then, no mechanism exists that implements Γ at any Bayes-Nash equilibrium.*

Corollary 8. *The use of secure computation techniques enables debt settlements with higher expected profits, thus attaining the "blessing of the debtor" 5 with efficient allocations for creditors.*

Proof. Follows from previous Theorem 6, since secure computation enables computation on private information between multiple distrusting parties. Additionally, efficient allocations for creditors are only possible with private information by Theorem 7. □

Additionally Theorem 6 implies that condition 3.11 of Theorem 4 will be satisfied with higher probability when there are differences in private information, making debt settlements more efficient.

3.3 An Optimal Revelation Mechanism

We start choosing the investment rule $k(\theta)$ to maximise the debtor's expected utility given by 3.10,

$$\hat{k}(\theta) = \begin{cases} 1 & \text{if } A \geq \sum_{i=1}^{n} \left[l_i(\theta_i, \theta_{-i}) + \frac{F(\theta_i)}{\phi(\theta_i)} \right] \\ 0 & \text{otherwise} \end{cases}$$

In other words, the entity will remain solvent if the continuation value is higher than the sum of the expected recovery values in bankruptcy, plus the terms $(F(x_i)/\phi(\theta_i))$: this investment rule $\hat{k}(\theta)$ and the condition that $U\left(\bar{\theta}, \bar{\theta}, t, k\right) = 0$ would set debtor's expected profits. But we also need an explicit solution for $t(\theta)$, thus the investment rule $\hat{k}(\theta)$ is rewritten as

$$\hat{k}(\theta) = \begin{cases} 1 & \text{if } C \geq B(\theta_i) + Q(\theta_{-i}) \\ 0 & \text{otherwise} \end{cases}$$

where

$$B(\theta_i) = \theta_i + \frac{F(\theta_i)}{\phi(\theta_i)} + \sum_{j \neq i} e_j(\theta_i)$$

and

$$Q(\theta_{-i}) = \sum_{j=1}^{n} \sum_{k \neq j, i} e_j(\theta_k) + \sum_{j \neq i} \left[\theta_j + \frac{F(\theta_j)}{\phi(\theta_j)} \right]$$

We make the following assumption so $B(x_i)$ is strictly increasing.

Assumption 1. *$F(\theta_i)/\phi(\theta_i)$ is strictly increasing (i.e., monotonically non-decreasing) for all $\theta_i \in \left[\underline{\theta}, \overline{\theta}\right]$ and all $i = 1, \ldots, N$.*

This assumption is satisfied by any uniform distribution on the interval $0 \leq \underline{\theta} < \overline{\theta} < \infty$, the Pareto, exponential, and positive normal distributions.

Thus, there exists a unique value of θ_i denoted by $\tilde{\theta} = \tilde{\theta}(\theta_{-i})$ for each vector θ_{-i} that solves

$$A = B(\theta_i) + Q(\theta_{-i})$$

The pivotal type $\tilde{\theta}(\theta_{-i})$ that creditor i can report without forcing bankruptcy according to investment rule $\hat{k}(\theta)$ is large when low types θ_{-i} are being reported by the other creditors: it measures the magnitude of the opportunities for holding out. It's defined by

$$\tilde{\theta}(\theta_{-i}) = \left\{ \min \theta_i | A = \sum_{i=1}^{n} \left[\theta_i + e(\theta_{-i}) + \frac{F(\theta_i)}{\phi(\theta_i)} \right] \right\}$$

Theorem 9. *The payment to creditor i is calculated according to*

$$\hat{t}_i(\theta_i, \theta_{-i}) = \hat{t}_i(\theta_{-i}) = \tilde{\theta}(\theta_{-i}) + e_i(\theta_{-i})$$

in the optimal mechanism.

Proof. The investment rule $\hat{k}(\theta)$ can be rewritten by the definition of $\tilde{\theta}(\theta_{-i})$ as

$$k(\theta) = \begin{cases} 1 & \text{for } \theta_i \le \tilde{\theta}(\theta_{-i}) \\ 0 & \text{otherwise} \end{cases}$$

Thus, the change in utility to creditor i from the optimal mechanism by constraint 3.6 is

$$\begin{aligned} U\left(\theta_i, \theta_i, \hat{k}, \hat{t}\right) &= \int_{I_{n-1}} \int_{\theta_i}^{\bar{\theta}} \hat{k}(u, \theta_{-i})\, du \phi(\theta_{-i})\, d\theta_{-i} & (3.12) \\ &= \int_{I_{n-1}} \max\left[\tilde{\theta}(\theta_{-i}) - \theta_i, 0\right] \phi(\theta_{-i})\, d\theta_{-i} & (3.13) \end{aligned}$$

From the previous equation 3.13 and the change in the expected utility from the non-optimal mechanism 3.2,

$$\begin{aligned} &\int_{I_{n-1}} \hat{k}(\theta_i, \theta_{-i})\, t_i(\theta_i, \theta_{-i})\, \phi(\theta_{-i})\, d\theta_{-i} & (3.14) \\ &= \int_{I_{n-1}} \left(\theta_i + e_i(\theta_{-i}) + \max\left[\tilde{\theta}(\theta_{-i}) - \theta_i, 0\right]\right) \phi(\theta_{-i})\, d\theta_{-i} & (3.15) \end{aligned}$$

Finally, we arrive to the solution to equation 3.15,

$$\hat{t}_i(\theta_i, \theta_{-i}) = \hat{t}_i(\theta_{-i}) = \tilde{\theta}(\theta_{-i}) + e_i(\theta_{-i})$$

since $\tilde{\theta}(\theta_{-i}) - \theta_i < 0$ when $\hat{k}(\theta_i, \theta_{-i}) = 0$, and $\tilde{\theta}(\theta_{-i}) - \theta_i > 0$ when $\hat{k}(\theta_i, \theta_{-i}) = 1$. □

In the optimal mechanism 9, a payment is received by creditor i which is independent of the reported type, but it will depend on the types declared by other creditors as explained in the following:

- the function $\tilde{\theta}(\theta_{-i})$ is decreasing in each component of θ_{-i} .

- the function $e_i\left(\theta_{-i}\right)$ is increasing in each component of θ_{-i} : if other creditors report high expected recovery values, then creditor i would increase his own expected recovery value.

If the holding out from $\tilde{\theta}\left(\theta_{-i}\right)$ dominates the revision of expectations from $e_i\left(\theta_{-i}\right)$, then transfers are decreasing in each component of θ_{-i} when using the optimal mechanism.

4 Practical Implementation

To ease exposition, we consider the simplest case: consider an example with $n = 2$ creditors and their private expected recovery value from bankruptcy θ_i be uniformly distributed on $[0, 1]$.

Assume that the revision function 3.1 is defined by

$$e_i\left(\theta_i\right) = \alpha\left(\theta_i - \frac{1}{2}\right)$$

such that when the constant $\alpha > 1$ creditors give more weight to the estimate of other creditors, and vice versa.

The optimal continuation value is given by

$$\hat{k}\left(\theta\right) = \begin{cases} 1 & \text{if } A \geq \left(\theta_1 + \theta_2\right)\left(1 + \alpha\right) - \alpha \\ 0 & \text{otherwise} \end{cases} \tag{4.1}$$

thus

$$\tilde{\theta}\left(\theta_2\right) = \left(\frac{4}{2 + \alpha}\right)\left(A - \frac{\alpha}{2}\right) - 2\theta_1$$

the payment to creditor 1 is

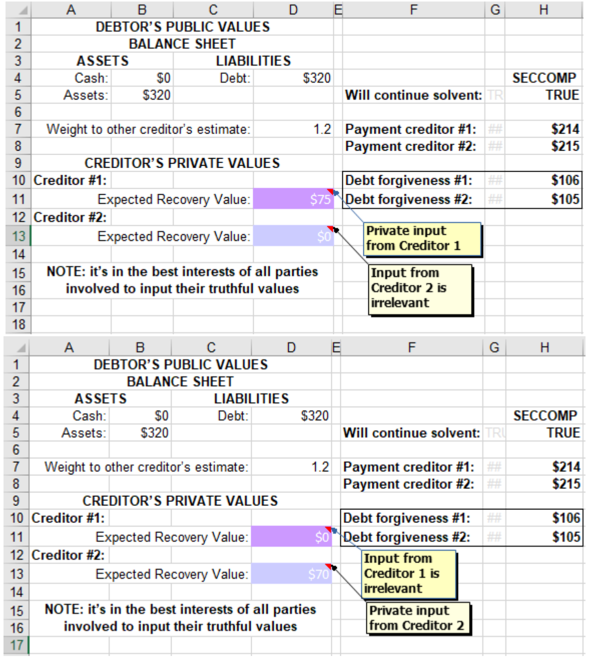
$$\hat{t}_1\left(\theta_2\right) = \tilde{\theta}\left(\theta_2\right) + e\left(\theta_2\right) = \left(\frac{4A - \alpha^2}{2\alpha + 4}\right) - \theta_2\left(1 - \alpha\right) \tag{4.2}$$

and the payment to creditor 2 is

$$\hat{t}_2\left(\theta_1\right) = \tilde{\theta}\left(\theta_1\right) + e\left(\theta_1\right) = \left(\frac{4A - \alpha^2}{2\alpha + 4}\right) - \theta_1\left(1 - \alpha\right) \tag{4.3}$$

Finally, the amount of debt forgiveness by each creditor i is given by $d - \theta_i$.

4.1 Implementation on "The Secure Spreadsheet"



	A	B	C	D	E	F	G	H
1	DEBTOR'S PUBLIC VALUES							
2	BALANCE SHEET							
3	ASSETS		LIABILITIES					
4	Cash:	$0	Debt:	$320				SECCOMP
5	Assets:	$320				Will continue solvent:	TR	TRUE
6								
7	Weight to other creditor's estimate:			1.2		Payment creditor #1:	##	$214
8						Payment creditor #2:	##	$215
9	CREDITOR'S PRIVATE VALUES							
10	Creditor #1:					Debt forgiveness #1:	##	$106
11	Expected Recovery Value:			$75		Debt forgiveness #2:	##	$105
12	Creditor #2:							
13	Expected Recovery Value:			$0				
14								
15	NOTE: it's in the best interests of all parties							
16	involved to input their truthful values							
17								
18								

Private input from Creditor 1

Input from Creditor 2 is irrelevant

	A	B	C	D	E	F	G	H
1	DEBTOR'S PUBLIC VALUES							
2	BALANCE SHEET							
3	ASSETS		LIABILITIES					
4	Cash:	$0	Debt:	$320				SECCOMP
5	Assets:	$320				Will continue solvent:	TRU	TRUE
6								
7	Weight to other creditor's estimate:			1.2		Payment creditor #1:	##	$214
8						Payment creditor #2:	##	$215
9	CREDITOR'S PRIVATE VALUES							
10	Creditor #1:					Debt forgiveness #1:	##	$106
11	Expected Recovery Value:			$0		Debt forgiveness #2:	##	$105
12	Creditor #2:							
13	Expected Recovery Value:			$70				
14								
15	NOTE: it's in the best interests of all parties							
16	involved to input their truthful values							
17								

Input from Creditor 1 is irrelevant

Private input from Creditor 2

Figure 4.1: Screenshots from "The Secure Spreadsheet". Top is creditor #1, bottom is creditor #2.

The previously derived closed-form formulae for the probability of the debtor to receive debt relief and continue being solvent 4.1, the payment to creditor #1 4.2 and to creditor #2 4.3 can be securely computed very easily on "The Secure Spreadsheet" (USPTO Patent 10,423,806[Cer14]), available online for download [Cer21b]: first precognised in the article "The G-d Protocols" [Sza97] from 1997, "The Secure Spreadsheet" is the first and only user program for general-purpose secure computation. For maximum performance at an affordable cost, the preferred secure computation protocol used by the "The Secure Spreadsheet" is the *dual-execution* protocol[MF06]:

Theorem 10. *(Dual-Execution protocol[HKE12]). If the garbled circuit construction is secure against semi-honest adversaries and the hash function M is modelled as a random oracle, then the Dual-Execution protocol securely computes f implementing the ideal functionality $\mathcal{F}_{YOVEL}$ 3.1 if for every non-uniform probabilistic polynomial-time adversary $\mathcal{A}$ in the real model, there exists a non-uniform probabilistic polynomial-time adversary $\mathcal{S}$ in the ideal model such that*

$$\left\{IDEAL_{f,S(aux)}\left(x,y,n\right)_{x,y,aux\in\{0,1\}^*}\right\} \overset{c}{\equiv} \left\{REAL_{\prod,\mathcal{A}(aux)}\left(x,y,n\right)\right\}_{x,y,aux\in\{0,1\}^n}$$

As pictured above on the captured screenshots 4.1, the public values for the debt D, the continuation value C and the weight α to the estimate to the other creditors must be the same on both spreadsheets for creditors 1 and 2. On the top spreadsheet for creditor 1, the only private that is taken into account is the one inputted by creditor 1 (et vice versa for the bottom spreadsheet for creditor 2). The final values computed using secure computation appear on the right-hand side of the captured screenshots, under the column "SECCOMP".

4.2 Implementation on a blockchain

The previous implementation on spreadsheets 4.1 is also realised on a blockchain using Raziel [Cer17] smart contracts and Pravuil [Cer21a] consensus: identical secure computations as the ones carried out on "The Secure Spreadsheet" are executed among creditors and debtors interfacing the blockchain with a mobile app.

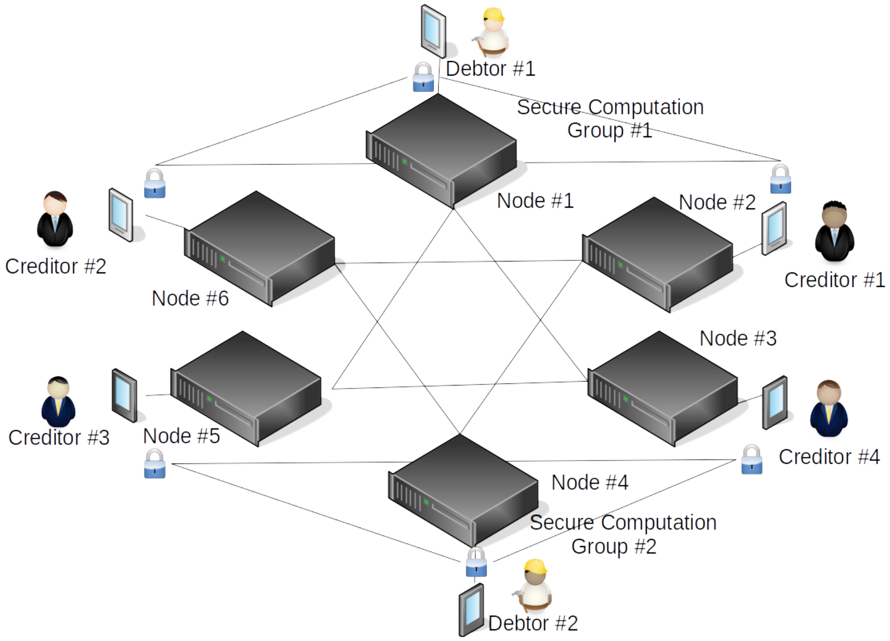


Figure 4.2: Two secure computation groups forgiving debts on a blockchain

Note the special suitability of Pravuil [Cer21a] consensus integrating real-world identity on this blockchain: debt management requires real-world identities, otherwise Sybil attacks could create unlimited fake debts. Due to this reason, this is the only valid blockchain consensus protocol [Cer21a] for the purpose of debt management.

5 Conclusion

The present paper has tackled and successfully solved the problem of debt relief and forgiveness by securely computing optimal debt settlements. The mathematical proofs hereby provided demonstrate that participation in the proposed mechanism is within the economically rational interests of all the involved parties by truthfully providing their private information, thus removing the need for third parties. Additionally, the provided implementations demonstrate the practicality of the securely computed mechanism.

References

[ADGH06] Ittai Abraham, Danny Dolev, Rica Gonen, and Joe Halpern. Distributed Computing Meets Game Theory: Robust Mechanisms for Rational Secret Sharing and Multiparty Computation, 2006. https://www.cs.cornell.edu/home/halpern/papers/podc06.pdf.

[AKL12] Emmanuel A. Abbe, Amir E. Khandani, and Andrew W. Lo. Privacy-Preserving Methods for Sharing Financial Risk Exposures, 2012. https://www.princeton.edu/~eabbe/publications/AKL_AER.pdf.

[AM85] Robert J. Aumann and Michael Maschler. Game Theoretic Analysis of a Bankruptcy Problem from the Talmud, 1985. https://www.cs.cmu.edu/~arielpro/15896s15/docs/paper8.pdf.

[BBM19] Dirk Bergemann, Benjamin Brooks, and Stephen Morris. Countering the Winner's Curse: Optimal Auction Design in a Common Value Model, 2019. https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/3/352/files/2020/11/TE3797-printed-version.pdf.

[BP20] David Byrd and Antigoni Polychroniadou. Differentially Private Secure Multi-Party Computation for Federated Learning in Financial Applications, 2020. https://arxiv.org/abs/2010.05867.

[BS05] Felix Brandt and Tuomas Sandholm. Efficient Privacy-Preserving Protocols for Multi-unit Auctions, 2005. http://dss.in.tum.de/files/brandt-research/fc2005.pdf.

[Cer14] David Cerezo Sánchez. Secure Multiparty Computation on Spreadsheets, 2014. https://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&p=1&u=/netahtml/PTO/srchnum.html&r=1&f=G&l=50&d=PALL&s1=10423806.PN.

[Cer17] David Cerezo Sánchez. Raziel: Private and Verifiable Smart Contracts on Blockchains, 2017. https://ia.cr/2017/878.

[Cer21a] David Cerezo Sánchez. Pravuil: Global Consensus for a United World, 2021. https://ia.cr/2021/669.

[Cer21b] David Cerezo Sánchez. The Secure Spreadsheet, 2021. https://www.calctopia.com.

[DDN$^+$15] Ivan Damgård, Kasper Damgård, Kurt Nielsen, Peter Sebastian Nordholt, and Tomas Toft. Confidential Benchmarking based on Multiparty Computation, 2015. https://eprint.iacr.org/2015/1006.

[DV93] Nir Dagan and Oscar Volij. The Bankruptcy Problem: A Cooperative Bargaining Approach, 1993. https://www.nirdagan.com/research/199301/full.pdf.

[EL03] Edith Elkind and Helger Lipmaa. Interleaving Cryptography and Mechanism Design: The Case of Online Auctions, 2003. https://eprint.iacr.org/2003/021.

[FAZ05] Keith Frikken, Mikhail Atallah, and Chen Zhang. Privacy-Preserving Credit Checking, 2005. https://www.cs.purdue.edu/homes/mja/sscc/documents/EC2005.pdf.

[GK06] S. Dov Gordon and Jonathan Katz. Rational Secret Sharing, Revisited, 2006. https://www2.cs.duke.edu/nicl/netecon06/papers/ne06-rational.pdf.

[Har67] John C. Harsanyi. Games with incomplete information played by Bayesian players, 1967. http://www.dklevine.com/archive/refs41175.pdf.

[HFT21] Marcella Hastings, Brett Hemenway Falk, and Gerry Tsoukalas. Privacy-Preserving Network Analytics, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3680000.

[HKE12] Yan Huang, Jonathan Katz, and David Evans. Quid-Pro-Quo-tocols: Strengthening Semi-Honest Protocols with Dual Execution, 2012. https://www.cs.virginia.edu/~evans/pubs/oakland2012/quidproquotocols.pdf.

[HT04] Joseph Halpern and Vanessa Teague. Rational Secret Sharing and Multiparty Computation: Extended Abstract, 2004. https://theory.stanford.edu/~vteague/STOC04.pdf.

[HV01] Carmen Herrero and Antonio Villar. The Three Musketeers: Four Classical Solutions to Bankruptcy Problems, 2001. http://www.ivie.es/downloads/docs/wpasad/wpasad-2000-23.pdf.

[IML05] Sergei Izmalkov, Silvio Micali, and Matt Lepinski. Rational Secure Computation and Ideal Mechanism Design, 2005. http://economics.mit.edu/files/1084.

[JM00] Philippe Jehiel and Benny Moldovanu. Efficient Design with Interdependent Valuations, 2000. https://philippe-jehiel.enpc.fr/wp-content/uploads/sites/2/2018/03/fineff3.pdf.

[MF06] Payman Mohassel and Matthew Franklin. Efficiency Tradeoffs for Malicious Two-Party Computation, 2006. https://www.iacr.org/archive/pkc2006/39580468/39580468.pdf.

[Mil04] Paul Milgron. Putting Auction Theory to Work, 2004. https://www.cambridge.org/us/academic/subjects/economics/microeconomics/putting-auction-theory-work.

[MS02] Paul Milgron and Ilya Segal. Envelope Theorems for Arbitrary Choice Sets, 2002. https://web.stanford.edu/~milgrom/publishedarticles/Envelope%20Theorems.pdf.

[MTY20] Juan D. Moreno-Ternero, Min-Hung Tsay, and Chun-Hsien Yeh. A Strategic Justification of the Talmud Rule Based on Lower and Upper Bounds, 2020. http://www.upo.es/serv/bib/wps/econ2002.pdf.

[Mye81] Roger B. Myerson. Optimal Auction Design, 1981. https://www.cs.princeton.edu/courses/archive/spr09/cos444/papers/myerson81.pdf.

[NPS99] Moni Naor, Benny Pinkas, and Reuben Sumner. Privacy preserving auctions and mechanism design. pages 129–139. ACM Press, 1999. http://www.wisdom.weizmann.ac.il/%7Enaor/PAPERS/nps.ps.gz.

[O'N81] Barry O'Neill. A Problem of Rights Arbitration from the Talmud, 1981. http://www.sscnet.ucla.edu/polisci/faculty/chwe/austen/oneill1982.pdf.

[OPRV08] Shien Jin Ong, David Parkes, Alon Rosen, and Salil Vadhan. Fairness with an Honest Minority and a Rational Majority, 2008. https://eprint.iacr.org/2008/097.

[Rog15] Phillip Rogaway. The Moral Character of Cryptographic Work. Cryptology ePrint Archive, Report 2015/1162, 2015. https://eprint.iacr.org/2015/1162.

[Sam47] Paul Samuelson. Foundations of Economic Analysis, 1947. https://www.hup.harvard.edu/catalog.php?isbn=9780674313033.

[Sza97] Nick Szabo. The God Protocols, 1997. https://nakamotoinstitute.org/the-god-protocols/.

[Tho13] William Thomson. Game-theoretic Analysis of Bankruptcy and Taxation Problems: Recent Advances, 2013. https://doi.org/10.1142/S0219198913400185.

[Xia11] David Xiao. Is privacy compatible with truthfulness?, 2011. https://eprint.iacr.org/2011/005.