DOI:10.1145/2574871

A solution to the persistent problem of preventing collusion in Vickrey auctions.

BY SILVIO MICALI AND MICHAEL O. RABIN

Cryptography Miracles, Secure Auctions, Matching Problem Verification

IN THIS ARTICLE, we extend the methods of Rabin et al.[10,11] in a major way and provide a solution to the long-standing important problem of preventing collusion in second-price (Vickrey) auctions. The new tools presented are deniable revelation of a secret value and uncontrollable deniable bidding. In Rabin et al.,[10,11] new highly efficient methods for proving correctness of announced results of computations were introduced. These proofs completely conceal input values and intermediate results of the computation. One application was to enable an Auctioneer to announce outcome of a sealed bid auction and provide verification of correctness of the outcome, while keeping bid values information-theoretically secret. We quickly survey these methods for completeness of the discussion and because of their wide applicability. Another example of an application is to prove to participants of a stable matching process such as the assignment residents to hospitals, of the correctness of the announced assignment without revealing any preferences of residents with respect to hospitals and vice-versa.

» key insights

- **Practically efficient secrecy of values preserving proofs of correctness of computations are useful for many financial and social processes.**
- **In particular, they supply a solution to the long-standing open problem of countering collusion of bidders in second-price (Vickrey) auctions.**
- **An important feature of these new methods is their understandability by a wide audience of potential users.**

By way of motivation, let us outline the main application given in this article for the extended method for secrecy preserving proofs of correctness. We consider Vickrey auctions where bidders $B_1, \ldots, B_n$ submit sealed bids $b_1, \ldots, b_n$ for a single item IT to a seller/auctioneer AU. At an announced end of bidding time T_1, the AU opens the bids and determines that, say, b_w was the highest bid value and b_s was the second highest bid. Bidder B_w will get the item IT and pay to AU the second-highest bid value b_s.

This bidding mechanism, absent collusion, makes it worth while for every bidder to bid his true value for the item IT. It thus assures the AU a return of the second highest private true value for the IT.[14]

When setting up the auction, AU specifies a reserve price r. If none of the bids is $\geq r$, then the IT is not sold. If the second price is smaller than r, then the winner (if there is one) pays r for the IT.

The possibility of collusion completely subverts the above advantage to the AU from the second price auction. Assume that all bidders form a Cartel to collude against AU. They determine ahead of closing time T that B_1's true value b_1 (as claimed by him) for the item IT is the largest among all true values as claimed by bidders. They agree that in the actual auction, B_1 will bid b_1 and each of the other bidders $B_2, \ldots, B_n$ will bid r. They also agree that if B_1 gets the IT, then he will make certain side payments to Cartel members $B_2, \ldots, B_n$. They also specify fines to be paid by cartel members who deviate from the agreement. Now, if all Cartel members keep to their agreement, then B_1 will get the IT and pay r to the AU. Thus, all of the seller's potential gain from conducting the auction is wiped out. Because of possibility of collusion, second-price auctions are rarely used despite their theoretical advantage.[5, 6, 12, 13]

We shall show how the use of cryptography enables prevention of collusion in *one-time* second-price auctions by making cartel agreements unenforceable and making it worthwhile for colluders to break those agreements. In repeated auctions involving the same bidders, the participants have an incentive to voluntarily keep collusion agreements so as to gain in the long run. The extent to which our methods can be applied to these cases and to other auctions is under study.

Using the methods of Rabin et al.[10,11] and the new tools of *deniable revelation of a secret value and uncontrollable deniable bidding*, we design an auction mechanism with the following properties.

1. Bidders submit sealed bids $b_1, \ldots, b_n$ to AU in an uncontrollable and deniable manner. This means that a bidder cannot be compelled by anybody to submit a specified bid value. Also, he cannot be compelled to reveal any information about his submitted bid.
2. The AU assigns to every bidder B_i a secret identifier id_i. Identifiers are known to AU but NOT known to bidders.
3. After the closing time of the auction, the AU determines that bidder B_w is the highest/winning bidder and that B_s is the second highest bidder with bid value b_s.
4. AU proves to the bidders, referring only to identifiers, that the bid by the bidder with identifier value id_w (say identifier value 10325) is the highest bid. Also that the bid by the bidder with identifier value id_s (say identifier value 21131) is the second highest bid.
5. The proof in 4 is information-theoretic hiding with respect to all bid values and with respect to the correlation between identifiers and bidders. Thus at this stage, bidders know nothing about who bid what and even the winner and second highest bidder do not know about their status as such.
6. The AU proves to B_w that his identifier is the above-mentioned id_w, that is, that he is the winner of the IT. AU proves to B_w that the bid value associated with the above-mentioned identifier id_s is b_s. AU collects from the winner B_w the price b_s. That is, the winner gets IT and pays to the AU the second highest bid value b_s (Vickrey). These proofs to B_w are again secrecy preserving with respect to the actual identity of B_s and any other bid value except b_s.
7. The AU proves to B_s that his identifier is id_s. The AU proves to every bidder B_j, $j \neq s$, that his identifier is different from id_s.
8. The proofs of 6–7 are again secrecy preserving and deniable by the bidders involved.
9. Every bidder B_i, if he so desires, can arrange that if he wins the item IT, then the fact he won will remain secret/unknown to the other bidders. This assumption holds, for example, for digital goods but may be difficult to implement for some physical goods such as radio spectrum. This issue is fully discussed later.

We shall prove that these properties 1–9 enable the Auctioneer to prevent collusion by promising, when announcing the auction, a kickback payment to the second highest bidder, whoever he may turn out to be.

The implementation of properties 1–8 requires of the Auctioneer proofs of correctness of announced results of computations while keeping input values and intermediate results secret. A new highly efficient tool for doing this was presented in Rabin et al.[10,11]

A new construct of a deniable proof of value presented in this paper is employed in implementing the properties 1 and 8.

Sealed Bid Auctions Implementation by Encryption and Secure Bulletin Board

In this article, we assume that the Auctioneer employs an electronic Secure Bulletin Board (SBB) with the following properties. The SBB is controllable by the AU who can post data. Posted data is time stamped and signed by the AU. Data cannot be erased. The SBB is viewable by all participants in the auction and they are assured that they all view the same content. Detailed implementations of a SBB use standard algorithmic tools and are not discussed herein.

Much of the data posted on the SBB will be in "sealed envelopes" created by bidders or by the AU. In Definition 3, we specify the Pedersen Commitment function which will be used in detailed proofs of the secrecy properties of our bidding mechanism. In practice, we implement sealed envelopes and commitments by an encryption function $E(\, , \,)$, say a 128-bit AES (Advanced Encryption Standard) used in authenticated encryption mode such as GCM.

Previous Results and Background

The method of value-secrecy preserving proofs of correctness in Rabin et al.[10,11] and in the present work was motivated by the ground-breaking methodology of Zero Knowledge Proofs (ZKP) innovated in Goldreich et al.[3] and Goldwasser et al.,[4] and the subject of thousands of subsequent papers. ZKP and other methods of verification of truth of claimed statements are, however, not sufficiently efficient for providing practical solutions for the auction-verification problems treated in Rabin et al.[10,11] and herein.

By way of example, in Parkes et al.[8] a method using Paillier homomorphic encryption[7] was employed for verification of claimed results of an auction while keeping bid values secret. Verification of a hundred-bidder second-price auction required several hundred minutes. By comparison, the new method of Rabin et al.[10] verifies a hundred-bidder second-price auction in two milliseconds. The use of multiparty computations (see Ben-David et al.[1]) provides secrecy of bids but no verification of correctness of announced results. It is also by far slower than that of Rabin et al.[10,11] and that presented in the present work.

The main innovation of Rabin et al.[10,11] is to work directly with the input values to a computation and its intermediate results as numbers rather than going down to the bit level. Furthermore, numbers are randomly represented by two-coordinate vectors.

The papers by Rabin et al.[10,11] consider a generalized form of straight line computations on elements of a finite field F_p. For our applications, a 128-bit prime p is completely adequate. Thus, the field operations $(x + y) \bmod p$ and $(x \times y) \bmod p$ are rapidly executable on an ordinary 64-bit processor.

A number of players $P_1, \ldots, P_n$ secretly submit to an *Evaluator Prover* EP input values $x_1, \ldots, x_n$ taken from F_p (i.e., $x \in \{0, 1, \ldots, p - 1\}$). The EP performs a computation on these inputs and announces the results of that computation.

Definition 1. *A Generalized Straight Line Computation (GSLC) on inputs $x_1, \ldots, x_n \in F_p$ with K outputs $x_{L+1}, \ldots, x_{L+K}$ is a sequence*

$$\mathrm{GSLC} = x_1, \ldots, x_n, x_{n+1}, \ldots, x_L, x_{L+1}, \ldots, x_{L+K} \qquad (1)$$

where for all $m > n$ there exist $i, j < m, L$, such that $x_m = (x_i + x_j) \bmod p$, or $x_m = (x_i \times x_j) \bmod p$, or $x_m = x_i$, or $x_m = \mathrm{TruthValue}\,(x_i \leq x_j)$.

An example of a GSLC for the output $x_{(2n-1)} = x_1 + \cdots + x_n$ is

$$x_1, \ldots, x_n, x_{(n+1)}, \ldots, x_{(2n-1)}, \quad \text{where } x_{(n+1)} = x_1 + x_2, x_{(n+2)} = x_{(n+1)} + x_3, \text{etc.} \qquad (2)$$

We show how the use of cryptography enables prevention of collusion in *one-time* second-price auctions by making cartel agreements unenforceable and making it worthwhile for colluders to break those agreements.

Random vector representations of values $x \in \mathbf{F_p}$. We now come to the main construct for enabling Secrecy Preserving Proofs for the correctness of the results $x_{L+1}, \ldots, x_{L+K}$ of the GSLC(1).

Definition 2. *Let $x \in F_p$ be a value. A random vector representation* RR(x) *of x is a vector $X = (u, v)$ where $u, v \in F_p$; u was chosen randomly (notation $u \leftarrow F_p$) and $x = (u + v) \bmod p$. For a vector $X = (u, v)$ we denote* $\mathrm{val}(X) = (u + v) \bmod p$.

The method for creating a RR(x) = (u, v) of x is to randomly choose $u \leftarrow F_p$ and set $v = (x - u) \bmod p$. Note that from u (or v) by itself, no information about x can be deduced.

Commitment functions. We shall use the Pedersen commitment function[9] for values $u \in F_p$. Let G be a group of prime order $q > p$ for which computing the discrete log function is intractable. Let g, h in G be two generators such that $\log_g(h) = e$ (i.e., $g^e = h$) is not known and by the intractability assumption not computable in, say, a thousand years.

Definition 3. *Let $u \in F_p$, the commitment* COM(u, r) *to u, using the help value $r \in [0, q - 1]$, is* $\mathrm{COM}(u, r) = g^u \times h^r$.

Note that under a random choice of the help value r, COM(u, r) is a random element of G. Consequently, the commitment function COM(u, r) is *information-theoretically hiding*. Since computation of $\log_g(h) = e$ is intractable, the commitment function is *computationally binding*. The latter means that for no commitment value C is it possible to compute two different pairs $(u, r) \neq (v, s)$ such that $C = \mathrm{COM}(u, r) = \mathrm{COM}(v, s)$. The reason is that $\log_g(h) = e$ is efficiently computable from the equation $g^u \times h^r = g^v \times h^s$. Consequently, a player who has created and posted a commitment COM(u, r) can open it only in one way to reveal the original value u.

Even the above strong binding property of the Pedersen commitment leaves it exposed to an attack by imitation. Assume that one bidder in an auction has committed to his bid using a value u committed to as $C = \text{COM}(u, r) = g^u \times h^r$. Another bidder who sees the posted C will post $D = C \times g \times h^s$. When the first bidder decommits the value u by revealing u and r, the second bidder will open D by revealing $u + 1$ and $r + s$, thus decommitting the value $u + 1$ and raising the bid by 1. In the following, such an attack will be enabled if there is collusion between the auctioneer and the second bidder.

To counter exposure to imitation, we assume that an independent agent, such as NIST, has created and signed randomly chosen pairs (g_i, h_i), $i = 0, 1, \ldots$, of generators of the group G. When setting up the auction, the AU and every participant are assigned a different pair of generators from the above list to be used for their commitments.

Proving claimed correctness of an addition $x + y = z$. We can now show how the EP can prove to a Verifier correctness of an equation $x + y = z$. The EP prepares random representations $X = (u_1, v_1)$, $Y = (u_2, v_2)$, and $Z = (u_3, v_3)$, of the values x, y, and z. Note that

$$\text{val}(X) + \text{val}(Y) = \text{val}(Z) \qquad (3)$$

if and only if there exists a $w \in F_p$ such that $X + Y = Z + (w, -w)$.
The EP prepares commitments

$$\begin{aligned} \text{COM}(X) &= [\text{COM}(u_1, r_1), \text{COM}(v_1, s_1)], \\ \text{COM}(Y) &= [\text{COM}(u_2, r_2), \text{COM}(v_2, s_2)], \quad (4) \\ \text{COM}(Z) &= [\text{COM}(u_3, r_3), \text{COM}(v_3, s_3)] \end{aligned}$$

The EP posts the commitments (4) or sends them to the Verifier VER and claims that the hidden vectors X, Y, Z satisfy (3).

When challenged by VER to prove this claim, the EP posts or sends to Verifier the above value w. The Verifier now presents to EP a randomly chosen challenge $c \leftarrow \{1, 2\}$.

Assume that $c = 1$. The EP decommits/reveals to Verifier $u_j, r_j, j = 1, 2, 3$. The Verifier checks the commitments, that is, computes COM(u_j, r_j), $j = 1, 2, 3$, and compares to the posted first coordinates of COM(X), COM(Y), COM(Z).

The Verifier next checks that $u_1 + u_2 = u_3 + w$. If $c = 2$ was chosen, then the Verifier asks for the second coordinates of X, Y, Z, and checks that $u_1 + u_2 = u_3 - w$. The following two theorems are immediately obvious.

Theorem 1. *If (3) is not true for the vectors committed in* COM*(X),* COM*(Y),* COM*(Z), then Verifier will accept with probability at most 1/2 the claim that (3) holds.*

Proof. Under our assumption about the COM function being computationally binding, the EP can open the commitments for u_j, v_j, $j = 1, 2, 3$, in only one way. Now, if (3) does not hold, then at least one of the equations $u_1 + u_2 = u_3 + w$, or $v_1 + v_2 = v_3 - w$ is not true. So the probability that a random challenge $c \leftarrow \{1, 2\}$ will not uncover the falsity of the claim (3) is less than 1/2.

Theorem 2. *The above interactive proof between EP and Verifier reveals nothing about the values val(X), val(Y), val(Z) beyond, if successful, that the claim that (3) is true (subject to probability at most 1/2 of Verifier accepting a false claim).*

Proof. We note that the interactive proof involves only the revelation of either all the first coordinates or all the second coordinates of X, Y, Z. Assume that Verifier's challenge was $c = 1$. The only revealed values were random u_1, u_2, u_3, w which satisfy $u_1 + u_2 = u_3 + w$. Because the commitment function $C(\ ,\ )$ is information-theoretically hiding, the un opened second coordinates in the commitments (3) of COM(X), COM(Y), COM(Z) are consistent with any three values $v_{1,1}$, $v_{2,2}$, $v_{3,3}$, satisfying $v_{1,1} + v_{2,2} = v_{3,3} - w$. Thus, the interactive proof is consistent with any three vectors X_1, Y_1, Z_1 satisfying the sum equality (3).

A probability of 1/2 of the Verifier being cheated is of course not acceptable. The probability of being cheated is exponentially reduced by simultaneously employing k repetitions of the process.

Simultaneous verification of several additions. Consider the GSLC (2) which involves n inputs $x_1, \ldots, x_n$, and has as output their sum $x_1 + \cdots + x_n$. The EP will present to Verifier $2n - 1$ commitments COM(X_j), $1 \le j \le 2n - 1$, for random representation for the values x_j, $1 \le j \le 2n - 1$. The interactive proofs for correctness of all $n - 1$ claimed equalities val(X_{n+1}) = val(X_1) + val(X_2), val(X_{n+2}) = val(X_{n+1}) + val(X_3), etc., will be done simultaneously for all equations. The EP will present to Verifier $n - 1$ values $w_1, \ldots, w_{n-1}$. The Verifier will then randomly choose a challenge $c \leftarrow \{1, 2\}$. The same challenge c will be used by EP and Verifier to check all the $n - 1$ equalities. It is clear that if not all $n - 1$ claimed equations are true, then the probability that Verifier will accept is at most 1/2. Also, the argument of Theorem 2 that the interactive proof is information-theoretic value-hiding holds without change.

Proving claimed correctness of multiplications. For proving correctness of the operations of multiplication $x_m = x_i \times x_j$ in the SLC (1), the EP will have posted on the SBB for the Verifier commitments COM(X_m), COM(X_i), COM(X_j) for random representations of the values x_m, x_i, x_j. The EP has to prove to Verifier that

$$\text{val}(X_i) \times \text{val}(X_j) = \text{val}(X_m) \qquad (5)$$

Let $X_i = (u_1, v_1)$, $X_j = (u_2, v_2)$, and $X_m = (u_3, v_3)$. The EP prepares auxiliary vectors $Z_0 = (u_1u_2, v_1v_2)$, $Z_1 = (u_1v_2 + w_1, p - w_1)$, $Z_2 = (u_2v_1 + w_2, p - w_2)$, where w_1, w_2 are randomly chosen values. The EP augments the commitments presented to Verifier into:

$$\begin{gathered} \text{COM}(X_m), \text{COM}(X_i), \text{COM}(X_j), \\ \text{COM}(Z_0), \text{COM}(Z_1), \text{COM}(Z_2) \quad (6) \end{gathered}$$

Clearly (5) holds if the following Aspects 0–4 hold true for the vectors committed in (6):

Aspect 0: $Z_0 = (u_1u_2, v_1v_2)$.
Aspect 1: $\text{val}(Z_1) = u_1v_2$.
Aspect 2: $\text{val}(Z_2) = u_2v_1$.
Aspect 4: $\text{val}(X_m) = \text{val}(Z_0) + \text{val}(Z_1) + \text{val}(Z_2)$.

In the interactive proof/verification, either Aspects 0 and 4 are checked together, or Aspect 1 or Aspect 2 is separately checked. The Veifier randomly chooses with probability 1/2 to verify Aspect 0 and the addition in Aspect 4. He randomly chooses $c \leftarrow \{1, 2\}$. Say $c = 1$. The EP reveals the first coordinates of X_m, X_i, X_j and Z_0. Aspect 0 is verified. Aspect 4 is verified in the manner of verification of additions. If the EP's claim is false with respect to Aspect 0 or Aspect 4, then the probability of Verifier accepting is at most $3/4 = 1 - (1/2) \times (1/2)$.

The Verifier chooses to check either Aspect 1 or Aspect 2, each with probability 1/4. Say Aspect 1 was chosen by Verifier. The EP reveals the first coordinate u_1 of X_i and the second coordinate v_2 *of* X_j and both coordinates of Z_1 and checks the equality of Aspect 1. Note that if Aspect 1 is false and is chosen for verification, then Verifier will never accept. Similarly for Aspect 2. Consequently, if (5) is false and the proof of correctness (6) presented by EP to Verifier is false in Aspect 1, or Aspect 2, then the probability that Verifier will accept is at most 3/4. Altogether we have:

Theorem 3. *If the product claim (5) is false then the probability that the Verifier will accept EP's proof of correctness is at most 3/4.*

Remark. To achieve the information-theoretic value hiding property of the above interactive proof of correctness, we require an additional step in EP's construction of the posted proof (6). We note that the same x_i can appear in the GSLC (1) as left factor and as right factor. One example arises if the GSLC has an operation $x_m = x_i \times x_i$. In this case, verifying Aspect 1 will reveal both coordinates of X_i and hence reveal the value $x_i = \text{val}(X_i)$. When preparing a proof of correctness of the GSLC (1), the EP creates for every x_i involved in multiplications two random vector representations X_i^L and X_i^R.

The proof of correctness of the multiplication $x_m = x_i \times x_j$ will be:

$$\text{COM}(X_m), \text{COM}(X_i^L), \text{COM}(X_j^R),$$
$$\text{COM}(Z_0), \text{COM}(Z_1), \text{COM}(Z_2),$$

where now $X_i^L = (u_1, v_1)$, $X_i^R = (u_2, v_2)$. It is clear that even if $i = j$, and Aspect 1 is checked, u_1 and v_2 are independent random values from F_p. Similarly if SLC contains another multiplication $x_k = x_s \times x_i$, it, as well as $x_m = x_i \times x_j$, is verified with respect to Aspect 1. For the first multiplication, X_i^R will be employed, and for the second multiplication, X_i^L will be used. Thus again independent random first coordinate of X_i^R and second coordinate of X_i^L are revealed.

Proving claimed inequalities $\mathbf{x_m}$ = TruthValue($\mathbf{x_i \leq x_j}$). Such inequalities $x \leq y$ are proved for cases $x, y < p/2$. It is clear that for such x, y, we have $x \leq y$ iff $y - x < p/2$. Example: Let $p = 17$, $x = 7$, $y = 5$. Then $x \leq y$ is false and $y - x = 15 > 17/2$.

So the EP can prove correctness of inequalities if he can, when true, prove for a commitment COM(X) *that* val(X) < p/2.

In Rabin et al.,[10, 11] Lagrange's theorem that every integer x is the sum of four squares of integers: $x = w_1^2 + w_2^2 + w_3^2 + w_4^2$ is employed to enable the EP to create a Value Hiding Proof of the GSLC (1) by use of which he can achieve [Rabin et al.,[10,11] Theorem 1]:

Theorem 4. *Let commitments COM*(X_1), …, *COM*(X_n) *to input values* $x_1, \ldots, x_n$ *be posted and let the EP perform the GSLC (1) and post the K output values* $x_{(L+1)}, \ldots, x_{(L+k)}$. *The claimed correctness of the output values can be interactively proven by the EP and a Verifier while keeping all inputs and intermediate values information-theoretically secret. If the Prover's claim is true then the Verifier will always accept the claim. If the Prover's claim is false then the probability that Verifier will accept the claim is at most 3/4.*

Amplification of Verifier's Confidence

In the previous section, we saw how the EP has expanded the GSLC (1) into a sequence of commitments to be called a Value Hiding Proof (VHP-GSLC). The *Value Hiding Proof* is employed by EP and VER in an input and intermediate value-hiding interactive proof of correctness of the output values of the GSLC as claimed by the EP. We have shown that the probability of the VER to accept a false claim is at most 3/4. In applications, a 3/4 probability of being cheated is of course unacceptable. The solution is of course duplication of the interactive proof in k translations of the GSLC (1). A successful verification of correctness of all k translations by VER will assure him that the probability of him having been cheated by the EP is smaller than $(3/4)^k$.

In practice, the EP may be called upon to interactively prove correctness of announced results to different Verifiers upon K different occasions. So, what is needed is for the EP to prepare and post $K \times k$ Value Hiding Proofs of the GSLC. Next we give an algorithm for doing that.

Making multiple copies of a sequence of hidden values. The reader who is mainly interested in the overall structure of our results may skip the details of this section and just take for granted its conclusion that many copies of posted hidden values can be made and their value consistency can be proved without revelation of actual values.

In the general case, as well as in the application to securing Vickrey auctions, the EP will have a sequence of m hidden input values $y_1, \ldots, y_m$. Some of these inputs were supplied by players $P_1, \ldots, P_n$ (in the case of auctions by bidders) and some of these inputs are created by the EP as part of the GSLC computation and proofs that he will conduct.

To begin with, the AU posts on the Secure Bulletin Board $3k$ rows:

$$\text{COM}(Y_1^{(j)}), \ldots, \text{COM}(Y_m^{(j)}), \quad 1 \leq j \leq 3k. \quad (7)$$

Each of these $3k$ rows consists of m commitments to vector representations of the m values $\text{val}(Y_i^{(j)}) = y_i$, $1 \leq i \leq m$. For some column indices i, the $3k$ commitments $\text{COM}(Y_i^{(j)})$, $1 \leq j \leq 3k$, to vector representations of the value y_i were provided by one of the players $P_1, \ldots, P_n$. For the other column indices i, the $3k$ commitments were supplied by the EP. For a proof of correctness of announced output results, the question arises: How can the EP prove to a Verifier that for each column index i the posted commitments $\text{COM}(Y_i^{(j)})$, $1 \leq j \leq 3k$, all contain vector representations of the same value. That is, how can the EP prove that the rows in (7) are *pairwise value consistent* in the following sense.

Definition 4: *Two rows of commitments*

$$\begin{matrix} \text{COM}(X_1), \ldots, \text{COM}(X_m) \\ \text{COM}(Y_1), \ldots, \text{COM}(Y_m) \end{matrix} \quad (8)$$

are called *value consistent* if $\text{val}(X_i) = \text{val}(Y_i)$, $1 \leq i \leq m$.

Assume that the EP wants to prove for two posted commitments COM(X) and COM(Y), where $X = (u_1, v_1)$ and $Y = (u_2, v_2)$, a claim that val(X) = val(Y). He reveals to VER the pair $(w, -w)$ such that $X = Y + (w, -w)$. As in the verification of addition, the Verifier now presents to EP a randomly chosen challenge $c \leftarrow \{1, 2\}$. If $c = 1$, then the EP reveals to VER the first coordinates u_1 and u_2. The VER checks that $u_1 = u_2 + w$. Similarly if $c = 2$. Clearly, if the EP's claim is false, then the probability that

VER will accept the claim is at most 1/2.

The same procedure will apply to proving/verifying a claim that the two rows (8) are value consistent. Here, EP posts m vectors $(w_i, -w_i)$, $1 \le i \le m$. The VER uses one random challenge $c \leftarrow \{1, 2\}$ to require from the EP to either reveal/open all first coordinates in all commitments or to reveal/open all second coordinates.

We now come to the procedure whereby the EP proves to a VER the value consistency of the initially posted $3k$ rows of commitments (7) and creates additional N rows of commitments to be used in multiple proofs of correctness of announced results of the GSLC.

Theorem 5. *(Rabin et al.,[10,11] Theorem 8) Let the EP choose an L (say $L = 10$) and prepare and post $M = 10 \times k \times L$ new rows (9):*

$$\mathrm{COM}(X_1^{(j)}), \ldots, \mathrm{COM}(X_m^{(j)}), \quad 1 \le j \le M, \quad (9)$$

so that each row of (9) is pairwise value consistent with every one of the $3k$ rows (7). That is, for every input index i, $\mathrm{val}(X_i^{(j)}) = y_i$, $1 \le j \le M$.

Upon demand, EP can conduct an information-theoretic value-hiding interactive proof convincing a Verifier that:

1. Among the initially posted $3k$ rows (7) at least a majority of $2k$ rows are pairwise value consistent. By definition, the m values $y_1, \ldots, y_m$ of the vectors committed to in that $2k$ majority are the input values to the process.
2. In the additional M rows (9) posted by EP, at least $(1 - 1/L)M$ rows are pairwise value consistent with at least $2k$ pairwise value consistent rows of (7).
3. The probability that the Verifier will accept claims 1–2 when not both are true is at most $(1/2 + 1/e^2)^k + (1/2 + 1/e^2)^{3k} < 2(1/2 + 1/e^2)^k$. □

The interactive proof involves EP opening one coordinate in every one of the 3 km pairs (7) and opening one coordinate in each commitment in 6 kL rows of (9). Thus this interactive proof leaves 4 kL untouched rows of (9) with the assurance that at least $(1 - 1/L)4\ kl$ of these rows are pairwise value consistent with the m values initially committed to in (7). The untouched rows can be employed in $N = 4L = 40$ proofs of correctness of outputs, where each proof uses k rows extended to Value Hiding Proofs. Every such interactive proof employing k rows reduces probability of Verifier being cheated to $(1/10 + 3/4)^k$.

In the following treatment of Vickrey auctions, we shall assume the availability of any needed number of value-consistent rows of commitments to input values without repeating the details as to how these rows were obtained from the initial input rows.

In practice, the EP may be called upon to interactively prove correctness of announced results to different Verifiers upon *K* different occasions.

Deniable Revelation of a Value

We want to show that the EP can post commitments $\mathrm{COM}(X)$ to vector presentations of a value x and reveal the value x to a player P in a manner that P can subsequently deny knowledge of the value x. Furthermore, even though the commitments are publicly posted on the SBB and viewable by other players, P cannot open any of these commitments. Consequently, the value x remains information-theoretically hidden from everybody except for the EP and P.

Our algorithm requires a step where P *privately* meets with the EP in a manner unobserved by anybody else and that P does not carry away from the meeting a record of the value x. The question whether this private meeting can be replaced by exchanges of encrypted messages is a topic for further research.

Theorem 6. *Assume that the EP has posted on the SBB 20k commitments:*

$$(P, \mathrm{COM}(X^{(j)})), \quad 1 \le j \le 20k, \quad (10)$$

where P is a name of a player, to random representations of a value x, that is, $\mathrm{val}(X^{(j)}) = x$, $1 \le j \le 20k$. Note that these posted commitments are publicly associated with the player P.

The EP reveals the value x to P and claims to him that the posted commitments (10) are to vector representations of this x. The EP can prove to P that the commitments are to random representations of the value x in a manner that (a) If more than $2k$ of the above $20k$ commitments are *not* to vector representations of x, then the probability that P will accept the false claim is at most d^k; (b) P cannot be compelled to reveal that value x to another party or prove to another party that the commitments are to the value x.

Proof. Player P meets privately with the EP. The EP claims to P that the hidden value is x. Player P randomly chooses $10k$ commitments out of the $20k$ commitments $(P, \mathrm{COM}(X^{(i)}))$.

For each of the $10k$ commitment $(P, \mathrm{COM}(X^{(i)}))$ chosen by P, the EP privately claims to P that $X^{(i)} = (u^{(i)}, v^{(i)})$. Note that this is what EP claims, without opening the commitment $\mathrm{COM}(X^{(i)})$.

Player P checks that for every claimed value of a vector $X^{(i)}$, $(u^{(i)} + v^{(i)}) \bmod p = x$.

Next, P chooses, for each of the $10k$ selected $\mathrm{COM}(X^{(i)})$, independently a random challenge $c_i \in \{1, 2\}$ and presents c_i to EP. If $c_i = 1$, then EP opens/reveals to P the first commitment of the chosen pair $\mathrm{COM}(X^{(i)})$. Player P checks that for $\mathrm{COM}(X^{(i)})$, the revealed coordinate value matches the above value $u^{(i)}$ as claimed by EP. Similarly for the case $c_i = 2$. Player P accepts that (10) are $20k$ commitments to representations of the value x only if all the above $10k$ checks are true.

The opening of the commitment to the coordinate c_i is done by EP on the *SBB* so that the identity of the opened commitment is publicly known.

Why is knowledge of the value x deniable by P? Player P was privately shown both coordinates, $u^{(i)}$ and $v^{(i)}$, of $10k$ vectors $X^{(i)}$. Thus he has deniability of what he saw. For each of these vectors, the EP publicly opened just one of the two posted commitments $\mathrm{COM}(u^{(i)})$, $\mathrm{COM}(v^{(i)})$), where $\mathrm{COM}(X^{(i)})) = (\mathrm{COM}(u^{(i)}), \mathrm{COM}(v^{(i)}))$. Hence, nobody except for the EP can open the other coordinate and the value x remains information-theoretically hidden.

We turn to the probability that the player P will accept a false claim. For brevity of discussion, we present a heuristic argument that if, say, $k > 30$ then the value d in the above bound d^k on the probability of P being cheated is close to $\sqrt{(1/e)}$, e being the natural log base $2.71 \ldots$. Namely, if more than $2k$ of the $20k$ vectors $X^{(i)}$ have $\mathrm{val}(X^{(i)}) \neq x$, then the probability for a randomly chosen $X^{(i)}$ to lead P to find that EP is cheating is $>(1/10) \times 1/2$. Consequently, the probability of accepting EP's claim for a randomly chosen $X^{(i)}$ that $\mathrm{val}(X^{(i)}) = x$ is $< 11/20$. For $10k$ choices, the probability of accepting is smaller than $(11/20)^{10k}$. But $(11/20)^{10}$ approximates $\sqrt{(1/e)}$. □

Uncontrollable, Deniable Bidding

We turn to describe the method implementing uncontrollable, deniable bidding by use of deniable revelation of a value. In the following sections, the auctioneer AU will play the role of an evaluator prover EP vis-à-vis the bidders in the auction. The terms AU and EP will be used interchangeably.

Step 6.1 Assume a one-time single-item Vickrey auction. The auctioneer AU, who will later also act as a prover, announces the auction and a reserve price r below which the item will not be sold. AU announces a time T for closing of the auction participation phase. AU also announces a time $T_1 > T$ for completion of submission of bids.

Step 6.2 Assume that bidders $B_1, \ldots, B_n$ have decided to participate in the auction. As each bidder B_i declares to AU prior to time T his intention to participate in the auction, the AU assigns to B_i a randomly chosen identification number $id_i \in F_p$ and a randomly chosen value $x_i \in F_p$. The value x_i will be subsequently used to enable B_i to submit his bid in an uncontrollable, deniable way.

The EP posts for every B_i $20k$ pairs $(B_i, \mathrm{COM}(X_i^{(j)}))$, $1 \leq j \leq 20k$, to random vector representations of the value x_i, that is, $\mathrm{val}(X_i^{(j)}) = x_i$, $1 \leq j \leq 20k$.

In a private meeting, EP reveals to B_i the value x_i in a deniable way as discussed earlier.

Step 6.3 To bid the value b_i bidder B_i computes, while still privately meeting with EP, the $z_i \in F_p$ such that $x_i + z_i = b_i \bmod p$.

Bidder B_i prepares $3k$ commitments $\mathrm{COM}(Z_i^{(j)})$, $1 \leq j \leq 3k$, to random vector representations of the value z_i, that is, $\mathrm{val}(Z_i^{(j)}) = z_i$, $1 \leq j \leq 3k$. He digitally signs these commitments and hands them over to EP who posts them on the SBB.

Now B_i erases from his device the values x_i and b_i but retains the value z_i and the data required for opening/decommitting $\mathrm{COM}(Z_i^{(j)})$, $1 \leq j \leq 3k$.

Note that at this point in time, before the closing of the auction, B_i has made his chosen bid b_i, but the EP does not know what that bid value is because he does not know the value z_i.

Theorem 7. *The above process implements a sealed-bid uncontrollable and deniable submission of a bid by bidder B_i.*

Proof. The bid value b_i equals the sum $x_i + z_i$. While EP knows the value x_i, he will know the value z_i only after bidder B_i will reveal it to the EP at the closing of the auction at time T_1. Thus we have a sealed-bid auction.

Bidder B_i cannot be compelled to make a specified bid because until his private meeting with the EP he does not know the value x_i. After he made his bid he can perhaps be made, or volunteer, to reveal the value z_i. But the value x_i was revealed to B_i in a deniable way. As shown earlier and in Theorem 6, B_i can claim anything about that value but can prove nothing about it. Thus this deniability extends to his bid value $x_i + z_i = b_i$.

Conducting the Second Price Auction

The purpose of the following procedure is to enable the EP to prove to bidders who won and what price the winner should pay by referring only to id numbers assigned by the EP to bidders. The procedure keeps bid values information-theoretically secret as well as the correlation between id numbers and actual bidders.

Step 7.1 The EP chooses for every bidder B_i a random identifier id_i. The identifiers are known only to the EP. At time T, the announced end of auction participation phase, the AU will post on the Secure Bulletin Board (SBB) the following data:

$$\begin{aligned} &\langle B1, \mathrm{COM}(ID_1^{(j)}), \mathrm{COM}(Y_1^{(j)}), \\ &\quad \mathrm{COM}\,(Z_1{}^{(j)})\rangle, \ldots, \\ &\langle B_n, \mathrm{COM}\,(ID_n^{(j)}, \mathrm{COM}(Y_n{}^{(j)}, \\ &\quad \mathrm{COM}(Z_n^{(j)}))\rangle, \quad 1 \leq j \leq 3k \end{aligned} \tag{11}$$

where $ID_1{}^{(j)}$ is the jth random vector representation of the identifier id_1; $\mathrm{COM}(Y_1{}^{(j)})$ is the jth random vector representation of the value x_1 chosen as explained at the end of of the section "Deniable Revelation of a Value"; and $Z_1^{(j)}$ is the jth random vector representation of the value z_1. Similarly for the other subscripts $2, \ldots, n$.

Step 7.2 After time T of closing the submission of sealed-bid auction and posting of the $3k$ rows (11), every bidder B_i opens his $3k$ commitments $\mathrm{COM}(Z_i^{(j)})$, for the EP.

The EP chooses $M = 10\,kL$, $L = 10$, and randomly chooses M permutations π

of the indexes $\{1, \ldots, n\}$. The EP creates for every bidder B_i M commitments COM(VB_i) to random vector representations VB_i of the value B_i (the names of the bidders are ASCII code words reduced to numbers).

The EP now creates and posts M *new rows* R_{3k+h}, $1 \leq h \leq M$ each row R_{3k+h}, a random permutation π_h of the n quadruples:

$$\begin{aligned}&\langle \mathrm{COM}(VB_1^{(3k+h)}), \mathrm{COM}(ID_1^{(3k+h)}),\\&\quad \mathrm{COM}(Y_1^{(3k+h)}), \mathrm{COM}(Z_1^{(3k+h)})\rangle, \ldots,\\&\langle \mathrm{COM}\,(VB_n^{(3k+h)}), \mathrm{COM}(ID_n^{(3k+h)}),\\&\quad \mathrm{COM}(Y_n^{(3k+h)}, \mathrm{COM}(Z_n^{(3k+h)})\rangle,\\&\quad 1 \leq h \leq M.\end{aligned} \tag{12}$$

Each of the rows (12) contains $m = 4n$ commitments and, before being permuted, is pairwise value consistent with each of the rows (11) viewed as a sequence of $m = 4n$ commitments to vector representations of values.

Step 7.3 The EP acting as Prover and all bidders $B_1, \ldots, B_n$ jointly acting as Verifier, now conduct the secrecy preserving proof noted earlier confirming that out of the $3k$ rows (11) at least $2k$ are pairwise value consistent and out of the new M rows (12) no more than M/L are not value consistent with at least $2k$ majority of the rows (11).

The only new point in this interactive proof is that whenever a row R_{3k+h} is chosen by the Verifier, the EP/Prover opens all the n commitments COM($VB_i^{(3k+h)}$) revealing the names $B_1, \ldots, B_n$ and ordering the quadruples according to the names.

As mentioned, 4 kL of the rows R_{3k+h} remain untouched at the end of this Step 7.3.

Step 7.4 Now the EP proves which identifier number id_w had highest bid and which identifier number id_s had the second highest bid. Without revealing bid values and without revealing names of the bidders associated with these identifier numbers, this is done as follows:

The Verifiers $B_1, \ldots, B_n$ randomly choose k rows R_{3k+h} out of the 4 kL remaining untouched rows in Step 7.3. Slightly abusing notations, call these rows $R_1, \ldots, R_k$.

The EP orders the identifier numbers $id_1, \ldots, id_n$ he has assigned to the bidders $B_1, \ldots, B_n$ according to size. This induces a permutation π on the indices $\{1, \ldots, n\}$ so that

$$id_{\pi(1)} < id_{\pi(2)} <, \ldots, < id_{\pi(n)} \tag{13}$$

The EP opens in each of the rows $R_1, \ldots, R_k$ the n commitments COM(ID). Thus the rearranged row R_j will look to the Verifiers as:

$$\begin{aligned}&\langle \mathrm{COM}(VB_{\pi(1)}^{(j)}), id_{\pi(1)}, \mathrm{COM}(Y_{\pi(1)}^{(j)}),\\&\quad \mathrm{COM}(Z_{\pi(1)}^{(j)})\rangle, \ldots,\\&\langle \mathrm{COM}\,(VB_{\pi(\mathrm{n})}^{(j)}), id_{\pi(n)},\\&\quad \mathrm{COM}(Y_\pi(n)^{(j)}, \mathrm{COM}(Z_\pi(n)^{(j)})\rangle,\\&\quad 1 \leq j \leq k\end{aligned} \tag{14}$$

Recall that for every quadruple $\langle \mathrm{COM}(VB), id, \mathrm{COM}(Y), \mathrm{COM}(Z)\rangle$, the bid value b of the bidder B to whom the EP secretly attached the identifier number id is $b = \mathrm{val}(Y) + \mathrm{val}(Z)$.

Using the k rows (14) as inputs and noting that the pairwise value consistency for these rows has already been established for the Verifiers, the EP can interactively prove to the Verifiers that for identifier numbers id_w and id_s the bid value represented in the quadruple containing id_w is the highest and the bid value represented in the quadruple containing id_s is the second highest. The interactive proofs are as in Rabin et al.[10,11] and as detailed in the section discussing previous results.

Step 7.5 Informing the winner, the second highest bidder and the other bidders. The EP now privately proves to the winning bidder that his associated identifier number is the id_w of step 7.4, thereby proving to him that he is the Winner. The EP reveals to the winner in a deniable way that the bid value associated with the identifier number id_s is b_s and collects that payment from the Winner.

In preparation for the kick back promised by the EP/AU to the second highest bidder, the EP privately and deniably proves to the second highest bidder that his identifier number is id_s.

The EP also privately proves to every other bidder that his identifier number is neither id_s nor id_w. These interactive proofs are conducted without revealing to the bidder in question his identifier number.

In the interest of brevity, we omit the detailed constructions of the above proofs. They follow the patterns and employ the tools developed in Rabin et al.[10,11] and in previous sections of this article.

Countering Collusion

The construction of a bidding process having Properties 1–8 is now complete.

Formation of the cartel. By way of example we assume that seven bidders, $B_1, \ldots, B_7$, out of the n bidders get together before the closing of the auction and, following a discussion, agree that:

a. Bidder B_i will bid according to strategy s_i, $1 \leq i \leq 7$.
b. If a cartel bidder B_i is the winner, he will make side payments $p_j^{(i)}$ to each player $B_j, j \neq i$, in the cartel.

Remark. Clauses (a)–(b) enable, for example, an agreement that B_1 will be the highest bidder among $B_1, \ldots, B_7$, and that if he wins he will make promised side payments to $B_2, \ldots, B_7$. On the other hand, if one of $B_2, \ldots, B_7$ wins by deviating from the agreement then he will make punitively high side payments to the other cartel members.

Theorem 8. *If the auction mechanism satisfies conditions 1–9 then collusion is avoidable.*

Proof. We assume that the bidders $B_1, \ldots, B_7$ are independent self-interested entities and that the auction for the item IT with reserve price r is a one-time event.

When announcing the auction, the AU promises in a binding way that the second price bidder B_j among all bidders $B_1, \ldots, B_n$, whoever he will turn out to be, will get a kick back payment of $(b_j - r)/k$, where b_j is his bid and r is the announced reserve price. Say $k = 10$.

Now, every cartel member B_i argues for himself as follows. In the proof of correctness of the auction result, all bid values will remain information-theoretically secret. Each of the cartel members can arrange it so that if he wins, the fact that he won will remain unknown to me (bidder B_i). Because that winner is self-interested, he will not make the side payment to me without any danger of reprisal. Also if I win, this fact will remain unknown to everyone except to me and to the AU, hence I shall not need to make any side payments. On the other hand, if I bid b_i = my true private value for IT, then if I win I shall get the IT at the second highest bid value. If I am the second highest bidder, then I shall get a kick back payment of $(b_i - r)/k$, where b_i = my private true value for the IT. The fact that I got the kick back payment will remain secret and be deniable by me.

The above argument can be strengthened to cover certain instances where the identity of the winner does not remain secret. Namely, the winner B_w has to pay the AU the second highest bid value b_s. But the identity of the second highest bidder B_s is secret from everyone except for the AU and B_s himself. The bidder B_s is informed that he is the second highest in a deniable way. The winner B_w learns from the AU in a deniable way of the payment b_s he has to make. Thus he can claim to other cartel members anything about that payment and consequently cheat them about the level of side payments he has to make.

The only concern that a cartel member B_i planning to deviate from the cartel agreement may have is that if another cartel member was designated as winner and that if he (B_i) bids his true value, he may turn out to be the winner and be subject to a fine payment. If B_i, based on his estimate of bids by other bidders, concludes that this is a likely outcome, then he will deviate only if he knows that his becoming the winner can be concealed. Possible concealment strategies are described following this Theorem.

Conclusion. Cartels are useless and the best strategy for every bidder is to bid his private true value. □

Keeping the winner's identity secret. The possibility of doing so depends on laws governing auctions and on special circumstances of a bidder, auctioneer, and the nature of the item IT up for auction.

For example: If the Auctioneer is a government agency, then there are often transparency requirements with respect to who gets the IT. Similarly, if a bidder is a government agency. The same restrictions may apply to publicly held corporations. In the latter case, the corporation may circumvent restrictions by use of an entity registered in another jurisdiction.

If the IT is a financial instrument, then transfer to the winner may be secretly done and subsequently known only to tax authorities.

Consider an auction of a large plot of land. If a bidder is a developer intending to build on it, then if he wins the fact is not concealable. If the bidder is an investor who intends to later on resell for a profit, then if he wins he can ask the AU to transfer right to sell to a confidentiality protecting trust. That trust will arrange the transfer of title to a subsequent buyer while keeping the winner's identity concealed.

All in all the possibility of keeping the winner's identity concealed depends on a myriad of legal and practical factors governing the auction in question. It gives rise to creative solutions. It is in the interest of the auctioneer and a winning bidder to cooperate in implementing a solution when legal and possible.

Verification of Stable Matching Solutions

In 1962, Gale and Shapley[2] formulated the stable matching problem and provided an efficient algorithm for its solution. A number of players $H_1, \ldots, H_m$ are looking at a pool of candidates $G_1, \ldots, G_k$.

In one example, the players are women, the candidates are men, and $m = k$. Every woman has her ordering of preference of men as spouses, and similarly for every man. A matching is a permutation $\mu: [1, n] \rightarrow [1, n]$ assigning to H_i the spouse $G_\mu(i)$. The matching is *stable* if there is no pair of indexes i, j such that H_i prefers $G_\mu(j)$ to $G_\mu(i)$ and $G_\mu(j)$ prefers H_i to H_j. If the latter happens, then H_i can drop $G_\mu(i)$ and $G_\mu(j)$ will move to H_i.

In another important example, the players are hospital departments (say surgery departments) and the candidates are graduating medical interns looking to become residents. In this case, $k > m$ and every department may induct several residents. Again every department has its ordering of preference of candidates and every candidate has his ordering of preference of departments. These orderings are submitted to an agency that computes a stable matching and announces the assignments while keeping the preferences secret.

Assume that a resident G_i assigned to hospital department H_j suspects that the agency could have assigned him to another department preferred by him because such a department got assigned a resident less desirable to it than G_i. Upon demand, G_i can get a proof that that is not the case. The proof of correctness does not reveal any preferences, only that G_i was not cheated. Similarly a department can obtain a secrecy preserving proof that no more desirable candidate is willing to move over to it.

Acknowledgments

Michael O. Rabin thanks Eric Maskin for very useful conversations and comments on the topic of Vickrey auctions, and Hal Varian for suggesting the application to matching problems.

References

1. Ben-David, A., Nisan, N., Pinkas, B. Fairplaymp a system for secure multi-party computations. In *CCS* (2008), ACM.
2. Gale, D., Shapley, L.S. College admissions and the stability of marriage. *Am. Math. Mon. 69* (1962), 9–14.
3. Goldreich, O., Micali, S., Wigderson, A. Proofs that yield nothing but their own validity, or all languages in np have zkp systems. *J. ACM 38* (1991), 692–729.
4. Goldwasser, S., Micali, S., Racoff, C. The knowledge complexity of interactive proof systems. *SIAM J. Comput. 18* (1989), 186–208.
5. Graham, D., Marshall, R. Collusive bidder behavior in single-object second-price and English auctions. *J. Polit. Econ. 95*, 6 (1987).
6. Marshall, R., Marx, L. Bidder collusion. *J. Econ. Theor. 133* (2007), 374–402.
7. Paillier, P. Public-key encryptions based on composite residuosity classes. In *Proceedings of EUROCRYPT 99* (1999), 223–239.
8. Parkes, D., Rabin, M.O., Shieber, S., Thorpe, C. Practical secrecy-preserving verifiably correct and trust worthy auctions. In *Proceedings of 8th International Conference on Electronic Commerce (ICEC)* (2006), 71–81.
9. Pedersen, T. Non-interactive and information-theoretic secure verifiable secret sharing. In *Proceedings of CRYPTO 91* (1991), Springer Verlag, 129–140.
10. Rabin, M., Mansour, Y., Muthukrishnan, S., Yung, M. Strictly black-box zero-knowledge and efficient validation of financial transactions. In *Proceedings of ICALP* (2012), Springer Verlag, 738–749.
11. Rabin, M., Servedio, R., Thorpe, C. Practical secrecy-preserving, verifiably correct and trustworthy auctions. In *Proceedings of IEEE Symposium on Logic in Computer Science* (Wroclaw, 2007).
12. Sandhholm, T. Limitations of the Vickrey auction in computational multi-agent systems. Research Paper. Department of Computer Science, Washington University, St. Louis, MO.
13. Ungern-Sternberg, T.V. Cartel stability in sealed bid second price auctions. *J. Ind. Econ. 36* (Mar. 1988), 351–358.
14. Vickrey, W. Counterspeculation, auctions, and competitive sealed tenders. *J. Finance 16* (1961), 8–37.

Silvio Micali (silvio@csail.mit.edu) is the Ford Professor of Engineering in the Electrical Engineering and Computer Science Department at the Massachusetts Institute of Technology, Cambridge, MA. He is co-recipient of the 2012 ACM A.M. Turing Award.

Michael O. Rabin (morabin@gmail.com) is The Thomas J. Watson Professor of Computer Science at Harvard University, Cambridge, MA, and professor of computer science at Columbia University, New York, NY. He is co-recipient of the 1976 ACM A.M. Turing Award.