Secure Auctions without Cryptography

Jannik Dreier, Hugo Jonker, Pascal Lafourcade

Secure Auctions Without Cryptography*

Jannik Dreier[1], Hugo Jonker[2], and Pascal Lafourcade[3,4]

[1] Institute of Information Security, Department of Computer Science, ETH Zurich, Switzerland
[2] University of Luxembourg, Luxembourg
[3] Clermont Université, Université d'Auvergne, LIMOS, Clermont-Ferrand, France
[4] CNRS, UMR 6158, LIMOS, Aubière, France

Abstract. An auction is a simple way of selling and buying goods. Modern auction protocols often rely on complex cryptographic operations to ensure manifold security properties such as bidder-anonymity or bid-privacy, non-repudiation, fairness or public verifiability of the result. This makes them difficult to understand for users who are not experts in cryptography. We propose two physical auction protocols inspired by Sako's cryptographic auction protocol. In contrast to Sako's protocol, they do not rely on cryptographic operations, but on physical properties of the manipulated mechanical objects to ensure the desired security properties. The first protocol only uses standard office material, whereas the second uses a special wooden box. We validate the security of our solutions using ProVerif.

1 Introduction

Auctions provide sellers and buyers with a way to exchange goods for a mutually acceptable price. Unlike a marketplace, where the *sellers* compete with each other, auctions are a seller's market where *buyers* bid against each other over the goods for sale. Because of the competitive nature of the process, often an *auctioneer* serves as a trusted third party to mediate the process. However, in many cases (for example on eBay) the auctioneer charges a percentage of the selling price as his fee. Hence he has a financial interest in the auction, which may compromise his neutrality.

Auction protocols typically rely on assorted cryptographic primitives and/or trusted parties to simultaneously achieve seemingly contrary security goals like privacy and verifiability. Examples include signatures of knowledge and zero-knowledge proofs [1], coin-extractability, range proofs and proofs of knowledge [2], hash chains [3], and proxy-oblivious transfers and secure evaluation functions [4]. Sako's protocol [5], explained in detail in Section 2, applies public-key encryption in a clever way to implement a verifiable sealed-bid auction. Although it is fully verifiable, the bidders need to trust the auctioneers for privacy of the losing bids. Brandt's protocol [6] goes even further: with the help of an ad hoc cryptographic primitive, Brandt claims to achieve full privacy for *all* bidders, i.e. only the winner and the seller learn who the winner is. However, the reliance on cryptographic primitives has its downside: cryptographic primitives are complex, and their use requires great care not to introduce subtle weaknesses, as recent analysis of Brandt's protocol shows [7].

* The original publication is available on www.springerlink.com

Moreover, as these protocols rely on complex cryptography, they are difficult to understand for a non-expert. This is particularly intriguing when it comes to verifiability – anyone lacking cryptographic expertise cannot ascertain for themselves that the verification procedure is indeed correct, and is thus forced to trust the judgment of cryptographic experts. This view underlies the German Constitutional Court's decision on electronic voting machines: "the use of electronic voting machines requires that the essential steps of the voting and of the determination of the result can be examined by the citizen reliably and *without any specialist knowledge of the subject*" [8]. Chaum [9] argued along the same line in 2004 that all the ingeniously designed verifiable voting protocols that had been put forward in literature did little to empower actual voters to verify elections. To address this issue, he proposed a voting protocol using visual cryptography: the ballot was distributed over two layers, that on top of each other showed the voter's choice. One layer was destroyed, leaving the voter with a layer full of random dots from which no choice can be inferred. However, anyone can verify that the system accurately recorded this layer – *without* any cryptographic expertise. In the same spirit, we propose in this paper two auction protocols that only rely on physical manipulations to enable non-experts to understand the protocol and its verification procedure.

Apart from Chaum's "true voter-verifiable" voting protocol [9], the power of (partly) physical protocols have also been studied for other applications. Stajano and Anderson [10] proposed a partly physical auction protocol using anonymous broadcast (e.g. small radio transmitters), which however still uses some cryptography (e.g. one-way functions and a Diffie-Hellman key exchange). More generally, Moran and Naor showed that many cryptographic protocols can be implemented using tamper-evident seals [11]. They also analyzed a polling protocol based on physical envelopes [12]. Moreover, in the context of game theory, Izmalkov, Lepinski and Micali [13] showed that a class of games (normal-form mechanisms) can be implemented using envelopes, ballot boxes, and a verifiable mediator in a privacy-preserving way. Fagin, Naor and Winkler [14] described various physical methods of comparing two secret values. Finally, Schneier [15] proposed a cypher based on a pack of cards.

Contributions. We start by recalling Sako's auction protocol [5] in §2. Inspired by this protocol, we propose a first physical implementation called *Envelopako*[5] in §3. This variant does not require cryptography nor trusted parties, yet retains the verifiability, privacy, authentication and fairness properties of Sako's protocol. Based on the definitions by Dreier et al. [16, 17] we also provide a formal analysis of these security properties in ProVerif [18], modeling their physical properties using a special equational theory. Although ensuring privacy for the losing bidders, both the Sako protocol and the Envelopako variant publicly reveal the winner. Our final contribution, *Woodako*[6], is described in §4: a physical auction protocol that offers stronger privacy *i.e.*, the winner is not publicly revealed, yet the result remains verifiable for losing bidders (similar to the protocol by Brandt [6]). In this protocol, physical properties take the place of cryptography and the trusted auctioneer. We build a concrete prototype, and formally verify the security properties with the help of ProVerif. Finally, we conclude in §5.

[5] **Envelop**e version of S**ako**'s protocol.

[6] **Wood**en box based implementation of S**ako**'s protocol.

2 Protocol by Sako

Sako [5] proposed a protocol for sealed-bid first-price auctions which hides the bids of losing bidders and ensures verifiability. The paper provides a high-level description using a generic cryptographic primitive that ensures certain properties (e.g. ciphertext indistinguishability). Sako also proposes two instantiations using specific cryptographic primitives: the first one uses Elgamal [19] encryption, and the second one employs a probabilistic version of RSA [20].

2.1 Informal Description

Informally, the protocol works as follows:

1. The authorities select a list of allowed bids $p_1, \ldots, p_m$ and a public constant c.
2. For each allowed bid p_i, the authorities set up encryption and decryption algorithms E_{p_i} and D_{p_i} (in both implementations simply a public-private key pair). The encryption scheme must provide an indistinguishability property. The authorities publish the encryption algorithms (or public keys in the implementation) and the list of allowed bids on a bulletin board (a public append-only broadcast channel).
3. To bid for price p_i, a bidder encrypts the public constant c using E_{p_i}, signs it and publishes the bid $C_j = E_{p_i}(c)$ together with the signature on the bulletin board.
4. After the bidding phase is over, the authorities check the signatures and start decrypting all bids with the highest possible price $t = p_m$. If $D_t(C_j) = c$, then bid j was a bid for price t. If all decryptions fail, the authorities decrease t and try again. Each time a decryption is done, they publish a proof of correct decryption to enable verifiability. This can be a zero-knowledge proof, or it might be achieved by simply publishing the secret key.
5. To verify the outcome, anybody can verify the signatures, and check the proofs of correct decryption.

In the rest of the this section we consider the implementation based on public and private key pairs as a concretization of the general encryption/decryption algorithms, however we abstract away of the precise encryption scheme. Note that dishonest authorities can break privacy since they have access to all secret keys, but because of verifiability a manipulation of the auction outcome can be detected.

2.2 Security Properties

We now argue informally that the protocol ensures *Fairness*, *Non-Repudiation*, *Non-Cancellation* and *Verifiability* (as defined in [17, 16]). Moreover it ensures *Privacy* of the losing bidders ("Strong Bidding-Price Secrecy" in terms of [17]) if the authorities are trusted. To formally verify these properties we use ProVerif [18], which allows us to prove that all the properties hold. Due to the space limitations we only give the informal analysis here, the formal analysis is available in the extended version of the paper [21].

Non-Cancellation and Non-Repudiation [17]. The bids are signed and published on the append-only bulletin board. Hence a bidder cannot deny that he made his bid, and the submitted bids cannot be altered or otherwise canceled.

Fairness. We consider the two aspects defined in [17]:

(a) Envelopako biding form for price p_i. (b) Envelopako bidding envelope for price p_i.

Fig. 1: The Envelopako protocol

– *Highest-Price-Wins:* This property is to ensure that an attacker cannot win the auction at a price below the actual highest bid. In this protocol, the authorities start by decrypting using the decryption algorithm corresponding to the highest possible price (if not, this can be detected, see Verifiability), hence they will identify the highest bid. Similarly, because of the signatures on the bids and the properties of the bulletin board, the bids cannot be modified, deleted or replaced.
– *Weak-Non-Interference:* This property is to ensure that no information about the bidders' bids is leaked before the bidding phase ends – otherwise they might employ unfair strategies based on that information. In this protocol the bids leak no other information apart from the identity of the bidders (revealed by the signature) because of the indistinguishability property of the encryption scheme.

Verifiability. Everybody can check the signatures of the bids on the bulletin board, ensuring that all bids originated from eligible bidders and were not modified. Similarly, all participants can use the proofs of correct decryption to check whether the authorities opened the bids correctly, hence ensuring the correctness of the outcome computation.

Privacy. The authorities have all private keys and can hence open all bids, breaking privacy. If the authorities are trusted, they will discard all unused keys, thereby preventing anyone from opening the losing bids and breaking the privacy of losing bidders. Given the indistinguishability property of the encryption scheme, this ensures secrecy of the losing bids.

3 The "Envelopako" Protocol

This protocol is a practical implementation of Sako's protocol using office material.

3.1 Description

In the Envelopako protocol each bidder has one sheet of paper per price (the *bidding form*) and as many envelopes with a transparent window (see Fig. 1). To bid for his chosen price, the bidder marks "Yes" on the bidding form corresponding to his price, and "No" on all other forms. All forms are inserted into the envelopes, and signed on the outside by the bidder. The envelopes are sealed and shown to all other bidders so that they can check the signatures. For m possible prices $p_m > p_{m-1} > \ldots > p_1$, the bid thus consists of m envelopes. The window allows to see the price without opening the envelope, yet the envelope hides whether the bidder chose "Yes" or "No".

Once all bidders have finished creating bids and shown their signatures, the bidders randomly exchange their bids (i.e. the sets of m envelopes) and jointly open the envelopes, starting with the highest possible price. If one of the envelopes contains a

"Yes", the bidders identified a bid for this (highest) price, and hence a winner. The signature on the outside then allows for the identification of the winner. If all envelopes contain "No", the bidders open the envelopes for the second price, and so on. Note also that the opening happens in presence of all bidders and the seller to ensure that protocol is followed. To fully ensure verifiability, the protocol must also ensure that only eligible bidders can bid. This is achieved through the verification of the signatures on the envelopes by the seller and bidders when bids are submitted.

3.2 Security Properties

The Envelopako protocol relies on the physical properties of the envelopes: Nobody can see from the outside the contents of a envelope, in particular whether the bidder marked "Yes" or "No" for a given price, and opening the envelopes breaks the seal. Hence the bids are private, and by opening the envelopes one by one in decreasing order only the winning bid(s) is/are revealed. The protocol offers verifiability similar to Sako's protocol as well as non-cancellation and non-repudiation due to the signatures and the mixing of the envelopes: All participants are in the same room, can check the signatures, and whether an envelope contained a "Yes" or "No". It ensures fairness since no premature information is leaked (*Weak Non-Interference*) and due to the joint bid opening no cheating is possible (*Highest Price Wins*).

Obviously a malicious bidder can open an envelope of his choice to read its contents – but this is actually similar to Sako's protocol, where dishonest authorities can break privacy. The difference is that in Envelopako such a behavior will be detected by the other bidders, since they are in the same room and the envelope is damaged. An extension to improve privacy could be to put the signed envelopes into slightly bigger and indistinguishable envelopes after the signature has been verified by the other parties. These envelopes can be posted into a ballot box (one per possible price) to break the link between a bidder and his bid. Hence a malicious bidder can only break the privacy of a random bid, but not necessary of the one he is interested in. A detailed discussion of other possible (side-channel) attacks is available in the extended version [21].

In our formal analysis [21] we model the physical properties of the envelopes using a special equational theory in ProVerif, which allows to employ the same verification steps as for Sako's protocol. ProVerif concludes that the protocol ensures *Non-Repudiation*, *Non-Cancellation*, *Weak Non-Interference*, *Highest Price Wins* and *Verifiability*. When verifying *Privacy*, ProVerif finds the obvious attacks of opening the envelopes discussed above, but if we assume honest bidders, Privacy can also be proven.

3.3 A distributed variant

The Envelopako protocol requires all participants to be in the same room during the bid opening, yet we can build a distributed protocol with a few minor modifications, and assuming a semi-trusted seller. Firstly each bidder also signs on the bidding form. To prevent issues resulting from multiple instances run in parallel, the bidders should also add an auction identifier to the form to link their bid to a specific auction. After preparing the envelopes, each bidder then sends (e.g. by postal mail) his envelopes to the seller, who collects all envelopes. The seller then determines the winner using the

same technique as above.[7] To prove to the bidders that his result is correct, he sends them photocopies of all bidding forms from the envelopes he opened. Moreover, he returns the unopened envelopes to the bidders, in order to prove that he did not violate privacy. This allows all bidders to verify the correctness of the outcome, and even their privacy. In this variant the seller is semi-trusted in the sense that he can misbehave and violate some properties of the protocol, e.g. privacy by opening all envelopes. However his behavior is completely verifiable, i.e. any misbehavior is detectable.

4 The "Woodako" Protocol

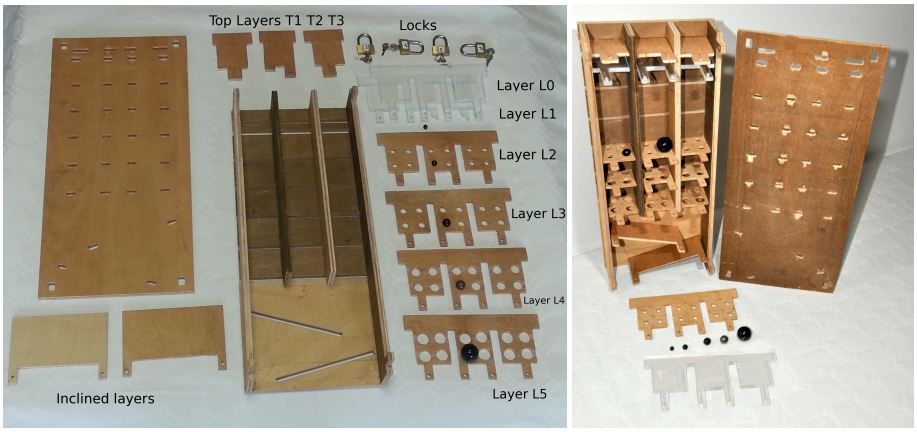
To improve the privacy of the Envelopako protocol, we developed *Woodako*, which relies on a special wooden box. Our prototype is designed for 3 bidders and 5 possible prices, but such a box can be built for other numbers n, m of bidders and prices. Fig. 2a shows all components of the box. The Woodako auction system uses: (1) five black marbles per bidder, each size represents one price; (2) six layers ($L0$ – $L5$): layers $L0$ and $L1$ are made of transparent plexiglass and have no holes. The other layers are made of wood and contain four holes per column[8], which correspond to the size of the marbles: the holes in $L2$ are only big enough for the smallest marbles, the holes in $L3$ for the second-smallest etc.; (3) three top layers $T1$, $T2$, $T3$ – each layer is associated with a bidder; (4) two inclined layers: these are placed below the layers, near the bottom of the box; (5) locks and keys: each bidder and the seller has a set of locks and keys; (6) one front side made of wood that closes the box and contains holes to insert the extremities of the layers. These extremities will stick out and so constitute a place where the parties can put locks. The locks are used to ensure security properties regarding that layer, for example that it cannot be removed unless everybody agrees.

4.1 Description

The wooden box carries out the important steps of the auction in a secure way through its physical properties. The box (see Fig. 2b) is composed of three columns and seven horizontal plus two inclined layers. Each column (the left, middle and right part of the box) corresponds to one bidder. The top layers $T1$, $T2$ and $T3$ are used to achieve confidentiality of the bid of each bidder, as the marbles (corresponding to the bids) are inserted underneath. The transparent layer $L0$ is used to lock the bids, once they are made, to achieve non-repudiation and non-cancellation. The five lower horizontal layers $L1$ – $L5$ are used to determine the winning price in a private way. Finally, the two inclined layers are intended to make it impossible to know from which column a marble fell by guiding all of them to the same spot in the bottom left part of the box.

[7] There is a potential attack when a bidder and the seller collude: the seller can open all bids from the other bidders until he identifies the highest bid, and then inform the colluding bidder to submit a bid for the same price in order to provoke a tie. Note that this can only be used to provoke a tie, as submitting a higher bid afterwards results in two envelopes for different prices containing "Yes" with broken seals, which can be detected. Moreover, it can be addressed by opening the envelopes for the same price one after the other, and declaring the first "Yes" as the winner. No other envelope is opened, and hence any situation with two envelopes containing "Yes" with broken seals (even for the same price, as in the above attack) identifies a misbehavior of the seller.

[8] The choice of four holes per column is arbitrary, we simply used multiple holes to improve practicality.



(a) The Woodako prototype.

(b) Inside our Woodako prototype, where layers $L1$ and $L2$ are removed.

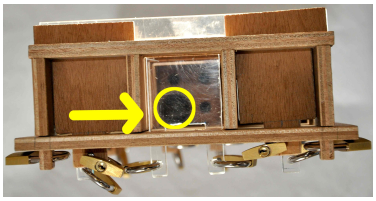
Fig. 2: Our prototype

The main idea is the following: Each bidder places his bid, represented by a marble of a certain size, in the top part of the box. We use five different sizes, the smallest one representing the highest possible price, and the biggest one representing the lowest possible price. In the bidding phase, all marbles are inserted into the box onto solid layer $L1$. In the opening phase, layer $L1$ is removed. Below there is layer $L2$ with holes big enough to only let the smallest marbles pass through. Below $L2$, there is $L3$ with bigger holes (the size of the next biggest marble), etc. If a bidder inputs the smallest marble (the highest possible price), it will fall through all layers once the solid layer is removed, hence revealing the winning price – but not the winning bidder, thanks to the inclined layers. If nobody inserted the smallest marble, no marble will fall through and the participants can remove the next layer to check for the second highest price, etc.

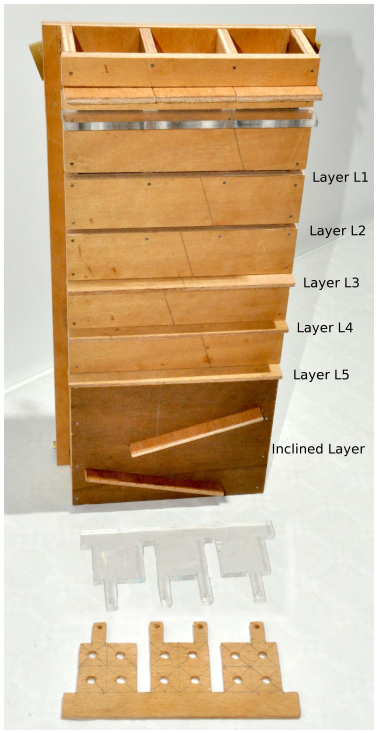
All layers $L0$ – $L5$ are equipped with four locks, one for each of the three bidders, plus one for the seller. This ensures that a layer can only be removed if all parties agree to do so. Similarly, the removable front side of the box is attached using four locks in the four corners (cf. Fig. 3a), one for each bidder plus one for the seller. This allows the parties to inspect the interior of the box before starting the protocol.

The topmost layer consists of three independent parts $T1$, $T2$ and $T3$ that each bidder can use to secure his bid (i.e. his marble inside the box, cf. Fig. 3a). Once all bids are inserted, the transparent layer $L0$ is inserted just below and locked by all parties to ensure non-cancellation (cf. Fig. 2b). Once the winning price is determined, the bidders can open their column by removing their lock on Ti and check through the transparent layer if their part of the box is empty or not, i.e. if they won or not (cf. Fig. 3b). Similarly the seller can remove the two inclined layers at the bottom to check if a marble is present inside a column or not (cf. Fig. 3d). The first solid layer $L1$ of the price determination part is transparent to allow the participants to check at the start of the protocol if each

(a) The Woodako box after the bid of bidder number two.



(b) Bidder verifiability (i.e. view from top).



(c) The Woodako box after two prices have been tested.

(d) Seller verifiability (i.e. view from bottom).

Fig. 3: The Woodako box: bidding, determining the winner, and verification

bidder inserted exactly one marble. Note also that all participants are always in presence of the box to be able to detect misbehavior.

The protocol is divided into 4 phases:

1) Initialization: Each participant can check the material and look the inside of the box as in Fig. 2b to convince himself of the correct design of the machine. The seller gives black marbles of different sizes to each bidder. The smallest marble corresponds to the biggest price, the biggest marble represents the lowest price. Moreover the seller and each bidder have a set of padlocks and keys (as in Fig. 3a). Once all bidders have

checked the box and received their material, the seller closes the box with the front side. The seller and each bidder put a padlock on the box (on each corner of Fig. 3c, marked with 1, 2, 3, and S). The seller places the layers $L1$ – $L5$ in the box, but neither the individual top layers $T1$, $T2$ and $T3$ nor the transparent layer $L0$. The seller also places the two inclined layers in the bottom of the box. Finally, he puts one lock on each layer on the middle column, all four locks on the inclined layers, and assigns a column to each bidder.

2) Bidding Phase: Each bidder selects a marble corresponding to the price he wants to bid and puts it in his column without showing the marble to the other parties. He then closes his column using his top layer Ti and secures it using one of his locks. He also puts locks on the five layers $L1$ – $L5$ below. In Fig. 3a you can see the box after bidder number 2 assigned to the middle column has made his bid. Once all bids are made and all locks in place, the seller introduces the transparent plexiglass layer $L0$, i.e. in the hole between the individual top layers and the first full layer $L1$. Finally each participant puts a lock on plexiglass layer $L0$.

3) Opening Phase: The seller and all bidders verify that each bidder inserted exactly one marble by removing the inclined layers (to which the seller has the keys) and looking through the holes of layers $L2$ – $L5$ and the plexiglass layer $L1$ from below[9]. After the inclined layers have been reinstalled and locked by the seller, all participants remove their lock on the layer $L1$, and the seller removes it. If somebody chose to bid the highest possible price, i.e. inserted the smallest possible marble, it will now fall down through all the holes (since all lower layers have bigger holes) and all participants know the winning price, yet not the winner. If no marble falls down, they repeat this process with the next layer below corresponding to the next price. In Fig. 3c, we see the back of the box once the two first prices have been tested. The inclined layers are there to hide from which column the marble fell, as all marbles will end up in the bottom left part independently of where they came from (cf. Fig. 2b).

4) Verification Phase: Once a marble has fallen down, each bidder can open his lock on his top layer Ti and check if his marble is still inside. In Fig, 3b, bidder number two notes that his marble is still inside the box, so he did not win. Similarly the seller can remove the two inclined layers and check for each column, whether there is still a marble inside, hence determining the winner – the column with no marble. An example is given in Fig. 3d: the left bidder won since his column is empty, and the two others lost, as their marbles are still there (highlighted by the yellow circles).

Resolving ties: Note that in the case of a tie two or more marbles fall down at the same time. Thus everybody knows that there is a tie, the seller can also identify the tied parties, and the bidders know if they are tied or not. Moreover a tied party can prove to anybody that he is tied by opening his top and showing that his compartment is empty. To resolve the situation either an external tie-breaking mechanism can be used (e.g. rolling a die), or the auction can simply be restarted. Using an external mechanism implies revealing the identity of the tied parties or trusting the seller, since he is the only one who knows who is tied. If privacy is the main concern and the seller is not to be

[9] In our experiments it was sometimes necessary to incline the box slightly so that the marbles stay in the same corner, similar to Fig. 3d

trusted, the auction can simply be restarted and giving the bidders the chance to modify their bids. Sako's protocol (our inspiration) also reveals the identity of the tied parties.

4.2 Security Properties

We now argue how the properties defined in [16, 17] are achieved, as long as there is at least one honest party following the protocol (i.e. one bidder or the seller). Note that we also successfully verified all the properties using ProVerif. The box and its properties are again modeled using a special equational theory, described in our extended version [21].

Non-cancellation and non-repudiation. Everybody can see in which column a bidder inserted his marble. Due to the fact that the layer $L0$ is locked by all the participants, nobody can change his price during the execution of the protocol. Hence nobody can cancel his bid. Similarly nobody can deny that it was his marble that fell down as the seller and the concerned bidder can verify in which column a marble is still present. Moreover the check at the beginning of the opening phase ensures due to the transparent layer $L1$ that there is exactly one marble per bidder.

Fairness. We consider the two aspects defined in [17]: *1) Highest-Price-Wins:* By the design of the box and the holes of different size in layers $L2 - L5$, the highest price offered by a bidder which is represented by the smallest marble is the first marble to fall down. No bidder can make a larger marble drop before a smaller one. *2) Weak-Non-Interference:* For a given set of bidders no information about the bids is leaked until the end of the bidding phase, since each bidder can choose his marble privately and drop it into the box in such a way that nobody can identify its size.

Privacy. The winner is only known to the seller and himself, but everybody knows the winning price. The inclined layers prevent anybody else from determining the winner by observing from which column the marble fell[10]. Once a marble has dropped, the winner can check if his column is empty by unlocking his top layer Ti and looking inside. The seller can also determine the winner by removing the inclined layers and checking which column is empty as shown in Fig. 3d. Since the remaining marbles are too big to fall through the holes, the seller can only see if there is a marble, but will be unable to determine its size, as all marbles have the same color. This preserves the secrecy of the losing bids. The losing bidders can also open their top layers Ti and verify if their marbles are still inside as shown in Fig. 3b. This leaks no information about the winner, yet they know the price from the moment when the marble falls as each layer corresponds to a price. Hence we have two cases: If the seller is honest, the winner stays anonymous, and only the winning price is revealed. If however the seller is corrupted, he can reveal the winner, and we only have secrecy of the losing bids.

Verifiability. The registration is done at the beginning of the protocol by the seller, and all participants can check if only the registered bidders participate by inserting

[10] Note that with two layers as shown in Fig. 2b there is a side-channel attack: If the marble falls down in the rightmost column, one can hear the sound of a falling marble only once, whereas in the case of the other two columns the marble falls down twice. However there are simple solutions: one can extend both layers further to the right so that the marbles fall down twice independently of their original column, or one can use something similar to a "bean machine", i.e. several rows of pins, arranged so that the falling marble hits a pin in each row. The idea is that the marble has a 50% chance of falling down on either side of the pin, hence arrives at a random location on the bottom.

a marble into the box. Hence the protocol ensures registration verifiability. Outcome verifiability is achieved by the fact that each participant can check the box and the mechanism at the beginning of the protocol, and that each bidder can check at the end whether he lost or won by opening his top layer Ti. The seller can also verify the outcome by opening the bottom of the box.

5 Conclusion

Current auction protocols rely on complex cryptographic operations. However, we argued that the verifiability of an auction should not depend on cryptographic expertise – without understanding, there is no meaningful verifiability. With that in mind, we adapted a suitable cryptographic auction protocol to achieve its security properties *without* cryptography. We began by analyzing Sako's protocol for *Non-Cancellation*, *Non-Repudiation*, *Fairness*, *Verifiability* and *Privacy* informally, and formally using the ProVerif tool. As the protocol mostly passed our automated scrutiny (for privacy, the auctioneers have to be trusted), we took this protocol as a base for the development of our two protocols.

We then proposed the Envelopako protocol, an auction protocol inspired by Sako's protocol where each bidder marks on a separate piece of paper for each possible price if they want to bid this price or not. These bidding forms are then inserted into signed envelopes, which are opened in descending order to determine the winner in a private way. We modeled the physical properties of the envelopes using an equational theory in ProVerif, which allows to apply the exact same analysis as for the cryptographic protocol. The analysis successfully proved *Non-Repudiation*, *Non-Cancellation*, *Weak Non-Interference*, *Verifiability*, and *Highest Price Wins*. For privacy, an issue was automatically found: dishonest participants may open an envelope to see the corresponding bidding form. A mitigation is that such actions are readily detectable by all, as any handling of the envelopes occurs in public view. We also discussed a distributed variant of this protocol with a semi-trusted seller, i.e. the protocol does not prevent him from misbehaving, but any misbehavior can be detected.

To improve privacy, we introduced the Woodako protocol. This protocol is again inspired by Sako's protocol, and again replaces cryptography and trusted parties by physical properties. Bids are represented by marbles, where smaller marbles denote higher bids. Bidders place the marble corresponding to their bid in their designated column in a (mechanical) contraption. Then, the first layer below all columns is removed, leaving a new layer with holes the size of the smallest marble. If at least one marble falls through, there is a winner, otherwise this layer is removed and the next layer with larger holes is now the base layer. We argued that Woodako achieves *Non-Repudiation*, *Non-Cancellation*, *Weak Non-Interference*, *Verifiability*, and *Highest Price Wins*. Moreover, this argumentation did not require any expert knowledge to understand, nor did it hinge on correct behavior by trusted parties. As the seller knows the winning bidder, a dishonest seller can reveal the winner. As such, the protocol ensures *Privacy* for all bidders including anonymity of the winner in case of an honest seller, and simple privacy for losing bidders in case of a dishonest seller. This was again confirmed by a formal analysis in ProVerif. As future work we look to improve the practicality of our protocols, as they do not scale well for higher numbers of bidders or possible prices. Moreover, we would like to examine whether our protocols can be adapted for second-

price auctions, and how we can improve the handling of ties. For this we are looking into other cryptographic protocols as sources of inspiration.

Acknowledgments. This research was conducted with the support of the "Digital trust" Chair from the University of Auvergne Foundation, and partly supported by the ANR project ProSe (decision ANR 2010-VERS-004). We also want to thank our carpenter Sylvain Thouvarecq for helping us building the Woodako prototype.

References

1. Omote, K., Miyaji, A.: A practical english auction with one-time registration. In: Proc. ACISP'01. Volume 2119 of LNCS. (2001) 221–234
2. Lipmaa, H., Asokan, N., Niemi, V.: Secure vickrey auctions without threshold trust. In: Proc. 6th Conference on Financial Cryptography. Volume 2357 of LNCS. (2003) 87–101
3. Stubblebine, S.G., Syverson, P.F.: Fair on-line auctions without special trusted parties. In: 3rd Conference on Financial Cryptography. Volume 1648 of LNCS. (1999) 230–240
4. Naor, M., Pinkas, B., Sumner, R.: Privacy preserving auctions and mechanism design. In: Proc. 1st ACM Conference on Electronic Commerce. (1999) 129–139
5. Sako, K.: An auction protocol which hides bids of losers. In: Proc. 3rd Workshop on Practice and Theory in Public Key Cryptosystems. Volume 1751 of LNCS. (2000) 422–432
6. Brandt, F.: How to obtain full privacy in auctions. International Journal of Information Security **5** (2006) 201–216
7. Dreier, J., Dumas, J.G., Lafourcade, P.: Brandt's fully private auction protocol revisited. In: Proc. AFRICACRYPT'13. Volume 7918 of LNCS. (2013) 88–106
8. Bundesverfassungsgericht (Germany's Federal Constitutional Court): Use of voting computers in 2005 bundestag election unconstitutional. Press release 19/2009 `http://www.bundesverfassungsgericht.de/en/press/bvg09-019en.html` (2009)
9. Chaum, D.: Secret-ballot receipts: True voter-verifiable elections. IEEE Security & Privacy **2**(1) (2004) 38–47
10. Stajano, F., Anderson, R.J.: The cocaine auction protocol: On the power of anonymous broadcast. In: Proc. Information Hiding'00. Volume 1768 of LNCS. (1999) 434–447
11. Moran, T., Naor, M.: Basing cryptographic protocols on tamper-evident seals. Theor. Comput. Sci. **411**(10) (2010) 1283–1310
12. Moran, T., Naor, M.: Polling with physical envelopes: A rigorous analysis of a human-centric protocol. In: Proc. EUROCRYPT 2006. Volume 4004 of LNCS. (2006) 88–108
13. Izmalkov, S., Lepinski, M., Micali, S.: Perfect implementation. Games and Economic Behavior **71**(1) (2011) 121–140
14. Fagin, R., Naor, M., Winkler, P.: Comparing information without leaking it. Commun. ACM **39**(5) (May 1996) 77–85
15. Schneier, B.: The solitaire encryption algorithm. `http://www.schneier.com/solitaire.html` (1999)
16. Dreier, J., Jonker, H.L., Lafourcade, P.: Defining verifiability in e-auction protocols. In: Proc. ASIACCS 2013, ACM (2013) 547–552
17. Dreier, J., Lafourcade, P., Lakhnech, Y.: Formal verification of e-auction protocols. In: Proc. 2nd Conference on Principles of Security and Trust (POST'13). LNCS (2013)
18. Blanchet, B.: An Efficient Cryptographic Protocol Verifier Based on Prolog Rules. In: Proc. 14th Computer Security Foundations Workshop (CSFW'14), IEEE (June 2001) 82–96
19. El Gamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. In: Proc. Advances in cryptology - CRYPTO'84, Springer (1985) 10–18

20. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2) (February 1978) 120–126
21. Dreier, J., Jonker, H., Lafourcade, P.: Secure auctions without cryptography (extended version). Available at `http://dx.doi.org/10.3929/ethz-a-010127116` (2014)