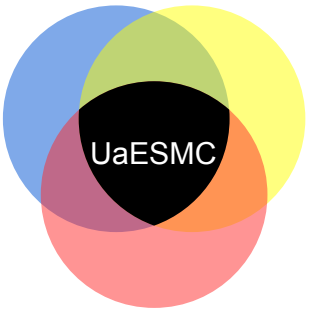


Project N°: **FP7-284731**

Project Acronym: **UaESMC**

Project Title: **Usable and Efficient Secure Multiparty Computation**

Instrument: **Specific Targeted Research Project**

Scheme: **Information & Communication Technologies**

Future and Emerging Technologies (FET-Open)

Deliverable D3.3
Quantification of the Effects of Partially Revealing Private Data

Due date of deliverable: 31st January 2014

Actual submission date: 31st January 2014

Start date of the project: **1st February 2012** Duration: **36 months**

Organisation name of lead contractor for this deliverable: **UoA**

Specific Targeted Research Project supported by the 7th Framework Programme of the EC		
Dissemination level		
PU	Public	✓
PP	Restricted to other programme participants (including Commission Services)	
RE	Restricted to a group specified by the consortium (including Commission Services)	
CO	Confidential, only for members of the consortium (including Commission Services)	

Executive Summary:
Quantification of the Effects of Partially Revealing Private Data

This document summarizes deliverable D3.3 of project FP7-284731 (UaESMC), a Specific Targeted Research Project supported by the 7th Framework Programme of the EC within the FET-Open (Future and Emerging Technologies) scheme. Full information on this project, including the contents of this deliverable, is available online at `http://www.usable-security.eu`.

This report contains a high-level discussion and overview of the work done by the research team from the University of Athens during the 2nd year of the project. This work is included in our two attached papers [12, 9]. The underlying theme of the deliverable is that of studying the effect that partial revelation of private information can have to the reliability and the performance of multi-party protocols. Of course this is a very general idea, and we tried to approach it from two directions, a fundamental cryptographic one as well as from an auction-theoretic one.

List of Authors

Yiannis Giannakopoulos (UoA)
Yiannis Tselekounis (UoA)

Contents

1 Introduction **4**

2 Quantifying tampering attacks as a means for achieving private information disclosure **5**
2.1 Tampering attacks against cryptographic implementations and private information disclosure 5
2.2 Quantifying tampering effects 6
2.3 A qualitative comparison between adversarial models 7
2.4 A secure construction based on secret sharing 7

3 Quantifying the performance of truthful and simple auctions **8**
3.1 Auctions 8
3.2 The effect of partially revealing private data - truthfulness 8
3.3 The need for simple and truthful auctions 9
3.4 Main results: approximation ratios of our auctions 9

Bibliography **11**

Chapter 1

Introduction

In any protocol that can potentially be used as a component of an SMC framework, there is some private information that each participating party owns. Partial revelation of this data, either in the form of a leak, an interception, or just a voluntary, sometimes payed-for disclosure, can change dramatically the status of the protocol and its performance. This is the underlying idea of the current deliverable, and given its abstract character and generality, we chose to approach it in two ways, in order to capture two different, but very relevant to the question in place, application.

Our first approach is a fundamental, cryptographic one. The goal is to protect cryptographic implementations against *physical* (*tampering*) *attacks* that aim to extract the implementation's private data. According to the model, the cryptographic functionality is implemented by a boolean circuit equipped with *private memory*, and the attacker is allowed to alter the circuit's computation and use the output of the faulty computation so as to infer information about the circuit's private data. The main objective is to build *efficient compilers* that transform any circuit into a tamper resilient one. Towards that direction, and being both theoretically and practically motivated, we propose a new adversarial model, we give feasibility results on tamper resilience with respect to the new attack model, and finally, we give an impossibility result on tamper resilience that applies to the new model, as well as to previous ones.

The second approach is from a game-theoretic perspective, which is also the main ingredient of WP3 anyways. In particular, we utilize one of the most challenging problems in modern Auction Theory, that of designing *multi-item auctions* that maximize the sellers revenue, in a bayesian setting where the seller has some prior (incomplete) information about the potential bids, in the form of a joint probability distribution. The fact that the participating players won't share their private, true valuations for the items unless we monetarily motivate them to, has a critical effect on the auction design process and the structure of revenue-maximizing auctions. These make apparent the need to study and quantify the performance of, possibly suboptimal, auctions which are however simple, natural and easy to describe, implement and run. We do that by providing exact, closed-form formula bounds for the *approximation ratios* of such auctions. Furthermore, as a side result we get an important optimality result for the case of i.i.d. exponential valuation priors which is essentially the first of its kind in the Economics and Algorithmic Game Theory literature.

Chapter 2

Quantifying tampering attacks as a means for achieving private information disclosure

In this chapter we provide a high-level presentation of our results in [12].

2.1 Tampering attacks against cryptographic implementations and private information disclosure

The traditional cryptographic context considers attackers having *black box* access to cryptographic functionalities, meaning the attacker is allowed to supply the functionality with input of it's choice, receive the corresponding output, and it is not allowed to interact with the functionality during execution. The functionality is implemented by a circuit equipped with private memory containing some sort of secret data, e.g., the decryption key of the decryption algorithm of a symmetric cipher, and the security of the implementation relies on the aforementioned *black box* assumption. However, real world attackers are much more powerful since besides observing the input-output behaviour of the functionality, they may also land physical attacks against the implementation, e.g., by inducing faults to the computation ([1, 2, 13]). Such attacks lead to private information disclosure in the following way: assume the cryptographic implementation computes $\mathcal{F}_{\mathbf{s}}(\mathbf{x})$, where $\mathbf{s}$ denotes the circuit's private memory and $\mathbf{x}$ is the circuit's input. $\mathcal{F}_{\mathbf{s}}$, as any non-trivial cryptographic functionality, ensures that any efficient (polynomial-time) black box adversary against the functionality cannot infer any valuable information about $\mathbf{s}$, with all but negligible probability in the security parameter of the cryptographic primitive employed by $\mathcal{F}_{\mathbf{s}}$. However, a tampering attacker who induces faults to the circuit that computes $\mathcal{F}_{\mathbf{s}}(\mathbf{x})$, it receives $\mathcal{F}'_{\mathbf{s}}(\mathbf{x})$, and uses $\mathcal{F}'_{\mathbf{s}}$ to infer information about $\mathbf{s}$, while in some cases, such as in [1] the attacker my extract the entire $\mathbf{s}$ by adaptively querying and tampering with the cryptographic device.

Physical attacks against cryptographic circuits have proven to be a significant threat to practical security, since any successful attack renders the device that carries the circuit redundant, by extracting the circuits' private key and instantiating the device from scratch. For instance, consider identification smart cards which enable the owner to have access to some sort of sensitive information. A malicious reader that queries and tampers with such a smart card, may extract its private key, and eventually replicate it, allowing access to unauthorized users.

Defending against tampering attacks may be achieved by employing tamper-resilient hardware, i.e., hardware that cannot be affected by specific types of physical attacks. However, this solution might be expensive, and moreover, it usually protects only against known types of attacks. Another approach, which is the one followed by [11, 6, 3, 12], is to protect circuits by employing algorithmic techniques, i.e., by appropriately modifying the original circuit to a tamper resilient one. Although the existing theoretical

models may not completely capture real world attacks, the algorithmic approach provides tamper-resilience even against unknown types of attacks.

The works of [11, 6, 3] undertook the difficult task of modeling and defending against tampering attackers that directly attack the cryptographic implementation. In this setting the adversary is given access to a circuit equipped with secret data stored in private memory; it is allowed to modify a bounded number of circuit wires and/or memory gates in each circuit invocation, by setting the value of each component to 0 or 1, or toggling its value. The objective is to contruct an efficient compiler that receives the original circuit, say $C_{\mathbf{s}}$,[1] an upper bound on the number of circuit components the attacker is allowed to tamper with, say t, and the security parameter k, and produces a circuit $C'_{\mathbf{s}'}$, such that for any tampering adversary $\mathcal{A}$ who tampers with up to t circuit components of $C'_{\mathbf{s}'}$, there exists an efficient simulator $\mathcal{S}$ who produces output indistinguishable from the output of $\mathcal{A}$ with all but negligible probability in k, while having *black box* access to $C_{\mathbf{s}}$. Hence tampering with $C'_{\mathbf{s}'}$ gives no advantage to the adversary, since it cannot learn anything more about the circuit's private memory than an adversary having black box access to $C_{\mathbf{s}}$.

The main observation here is that the works of [11, 6, 3] do not consider attacks against circuit gates, while some of them ([6, 3]) even employ tamper-proof gates. This fact suggests a fundamental issue since an attacker may effectively land physical attacks against circuit gates ([18]). In [12] we introduce the *gate* tampering attacker, that in each circuit invocation chooses a bounded number of circuit gates,[2] and for each gate it is allowed to alter its functionality by substituting it with another gate, with the restriction that both gates receive the same number of inputs bits. We investigate the relation between *gate* tampering and *wire* tampering attacks and we prove that gate attackers are strictly stronger than wire ones.

2.2 Quantifying tampering effects

In section 3 of [12] we quantify the tampering effects of *wire* and *gate* attackers by providing the minimum number of circuit components (wires or gates), that each attacker needs to tamper with so as to break the security of any cryptographic implementation. Our impossibility result relates the amount of tampering with the depth of the circuit: we prove that for any boolean circuit C of depth d, security cannot be achieved if we allow an adversary to tamper with $d(k-1)$ circuit wires, or d circuit gates, where k denotes the circuit's fan-in. Notice that as the circuit's fan-in increases, the required amount of wire tampering instructions should also increase. On the other hand, *gate* tampering is independent of the circuit's fan-in.

Informally, the impossibility result proceeds as follows: first we define the notion of *non-triviality* of a cryptographic circuit which attempts to capture the essence of a meaningful cryptographic implementation. Non-triviality states that for every circuit C with private memory $\mathbf{s}$, which implements some sort of cryptographic functionality, and for any efficient adversary $\mathcal{A}$, $\mathcal{A}$ should not be able to learn $\mathbf{s}$ with probability very close to 1, while having black box access to C. Non-triviality constitutes a weak assumption that should be achieved by any cryptographic implementation, since any attacker who learns $\mathbf{s}$ renders the implementation obsolete and simulates it from scratch. Then we prove that any *non-trivial* circuit C possesses a *weakly unpredictable bit*, i.e., there exists a private memory bit s_i, such that for every efficient adversary $\mathcal{A}$, $\mathcal{A}$ should not be able to extract s_i with probability very close to 1, while having black box access to C. Now, let C be a circuit of depth d and assume C consists of gates with fan-in at most 2. If we allow the adversary to tamper with up to d circuit components (we prove our result for either wires or gates), there exists a strategy that extracts the weakly unpredictable bit with probability equal to 1. The impossibility result follows from this, since any simulator with black-box access to C has no capability to predict the unpredictable bit as good as the tampering adversary. Hence, for any $d, k \in \mathbf{N}$, and every compiler T that receives a circuit C and produces a circuit C' of depth at most d, with fan-in k, T cannot be secure against an adversary who tampers with d circuit gates or $d(k-1)$ wires, *regardless of the size of* C'.

[1] $\mathbf{s}$ denotes the circuit's private memory.

[2] As in previous works, we also consider boolean gates.

2.3 A qualitative comparison between adversarial models

The impossibility result of [12] on tamper resilience highlights the relation between the circuit's depth and fan-in, with the minimum number of tampering instructions and provides us with a quantitative separation between gate and wire attackers. But how do wire and gate attackers fair against each other in general? In section 4 of [12] we first prove that any tampering attack on up to t circuit wires can be simulated by an adversary who tampers with up to t circuit gates, i.e., for every circuit $C_{\mathbf{s}}$ and any efficient adversary $\mathcal{A}$ who tampers with up to t wires of $C_{\mathbf{s}}$, there exists an efficient adversary $\mathcal{A}'$ who tampers with up to t gates of $C_{\mathbf{s}}$, such that the outputs of $\mathcal{A}$ and $\mathcal{A}'$ are exactly the same. Then we prove that gate adversaries are strictly stronger than wire adversaries, independently of the number of tampering instructions allowed to the attackers. Specifically, we show that there exist a family of circuits $\tilde{C}_{\tilde{\mathbf{s}}}$ parameterized by n, t and an efficient adversary $\mathcal{A}$ who tampers with up to n circuit gates, such that for all efficient adversaries $\mathcal{A}'$ who tamper with up to t circuit wires, where t can be arbitrarily larger than n, $\mathcal{A}'$ fails to produce output indistinguishable from the output of $\mathcal{A}$. In this way, we receive a qualitative separation between the two adversarial models, which demonstrates the effectiveness of gate tampering attacks against cryptographic implementations.

Our separation theorem relies on the following idea: consider a single boolean AND-gate g, with two input wires and one output wire. As it was mentioned above, any tampering strategy against the wires that are adjacent to g can be simulated by the gate attacker by substituting g with another boolean gate. Now, in order to see that the other direction does not hold, suppose the gate attacker substitutes g with an XOR-gate g'. One can easily verify that there is no tampering strategy against the adjacent wires of g, that sets the value of each wire to 0 or 1, or toggles its value, and produces the XOR tampering effect. Based on this observation, we construct a circuit that has a "critical area" comprised of AND-gates, and we define a gate-adversary that transforms all AND-gates of the critical area into XOR-gates. The primitives employed by the circuit (PRF,digital signatures, counters) enables the gate-attacker to produce a circuit output with a certain specific distribution that is verifiable in polynomial-time, and we show that there exists no efficient wire-tampering strategy that simulates the gate-tampering strategy. The separation between the two models follows.

2.4 A secure construction based on secret sharing

The last section of [12] gives feasibility results for defending against gate attackers by appropriately analysing the construction of [11], which is provably secure against wire tampering attacks. The compiler employs a randomized secret sharing scheme which shares the bit-value of a wire in the original circuit among k wires, and then introduces redundancy by making $2kt$ copies of each wire, where k denotes the security parameter. Moreover, each gate on the original circuit is substituted by a subcircuit that performs computations over encoded values. The randomization of the encoding guarantees that any tampering with the resulting circuit will produce an invalid encoding with high probability, triggering the circuit's self-destruction mechanism that erases the circuit's secret memory. Since this mechanism is also prone to tampering, the adversary could try to deactivate it so as to tamper with the rest of the circuit while keeping the secret state intact. In order to prevent such a scenario, the construction employs an error-propagation mechanism which propagates errors induced by tampering attacks.

Chapter 3

Quantifying the performance of truthful and simple auctions

In this chapter we discuss and give a brief overview of our results from paper [9].

3.1 Auctions

We gave a formal treatment of introducing auctions within the general framework of Mechanism Design and Game Theory in last year's deliverable D3.2 [7]. The interested reader is referred to that document for details. The basic idea behind any auction setting is that a certain "authority" (seller) wants to allocate different services/products (items) to different participating parties (buyers) and receive back some form of payment from them as a compensation for this transaction. We consider sellers that have as their goal to maximize their own total revenue at the end of the auction. In order to do that, they try to design the best possible auction for them based on some prior knowledge/expectation that they may have about the buyers' potential bids. The standard way to model this, is by assuming that the players' valuations for each item come from some probability distribution (bayesian setting).

3.2 The effect of partially revealing private data - truthfulness

At the same time, a fundamental game-theoretic assumption is that each participating agent is completely rational and selfish, so she will try to optimize her own "happiness", which is captured by how much the item is worth to her minus the payment she had to pay to the seller to acquire it. We refer to this quantity as the player's *utility*. That means that a buyer will not hesitate to lie and misreport a *false* bid which will probably be below her true value for the item if this is to result in her being asked to submit a lower payment. That is why we want to design auctions that are *truthful*, i.e. they don't give any incentives to the buyers to lie. There is a very elegant characterization of truthfulness in terms of the properties of the players' utility functions that readily transforms the problem to a concrete optimization problem of mathematical analysis, due to Rochet [16]. In particular, an auction is truthful if and only if it induces *convex* utility functions the *derivatives* of which with respect to an item equals the probability that this item is sold to the player.

This important requirement has a critical effect to the characteristics of feasible auctions, and it imposes beautiful but also very challenging features in the task of analyzing and designing *optimal* (i.e. revenue-maximizing) auctions. It has been common knowledge in the Economics community that characterizing optimality in settings of more than a single item[1] is an extremely involved problem, see e.g. [17, 14, 10]. Up until very recently our understanding of the structure of optimality was very unclear, and only partial results where known for the case of two items. Very recently Giannakopoulos and Koutsoupias [8] where able

[1]The single item case was completely resolved by Myerson in his celebrated 1981 paper [15], who also received the 2007 Nobel Memorial Prize in Economic Sciences for these contributions in Mechanism Design.

to utilize a duality-theory inspired framework for the problem, that was able to characterize some elegant geometric properties of optimal auctions for many items. In this deliverable we use their technique to get approximation ratios for the revenue of specific "simple" and natural auctions.

3.3 The need for simple and truthful auctions

In addition to the significance of truthfulness as a property that the auctions we design must possess, there is another important aspect that we should not forget, and which is critical especially in SMC settings: our protocols muse be "easy" to describe and implement, straightforward for the participants to understand and commit to it and also it should not have unrealistic computational demands. This last issue becomed even more important in the view of the recent #P-hardness result of Daskalakis, Deckelbaum and Tzamos [4]. Therefore, we would ideally want to know how well specific *natural and easy to describe* auctions perform. In other words, what is the cost that truthfulness imposes to our auction design setting? An auction designer might be happy, for example, to trade-off a provable performance guarantee of 95% of the optimal revenue for the benefit of having an efficiently implementable algorithm that is also easy to explain to the participating parties.

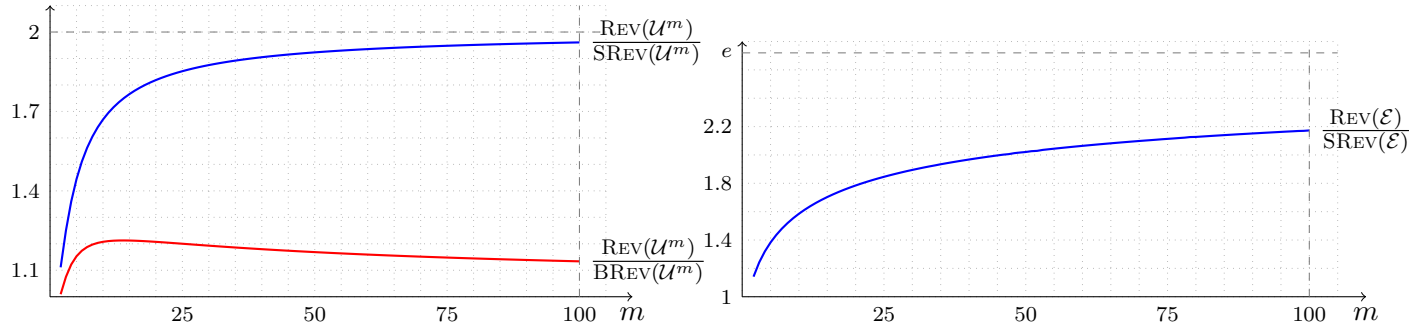
Such auctions were studied particularly by Hart and Nisan [10] who focused on two simple auctions, both deterministic: the one that treats every item on its own and sells them independently and the one that sells all items in a full bundle. They were able to prove some general approximation-ratio bounds for the class of all possible valuations' distributions, however these were asymptotic, and logarithmic in the number of items. We focus on two special cases, which seem to be the most natural ones, and we give exact, numerical approximation ratios for any number of items. In particular, we consider a setting where valuations come i.i.d. from the uniform distribution over the unit interval and another one where they come from independent (but not necessarily identical) exponential distribution over the nonnegative reals. Especially for this last settings, Daskalakis et al. had provided exact optimality results for the case of up to two items, in [5]. We choose these two models due to the fact that these two distributions are essentially the maximum entropy distributions over an interval and over the nonnegative reals, respectively, thus they are the "natural" choice if we want to enforce as few assumptions over our setting as possible.

3.4 Main results: approximation ratios of our auctions

The most essential step into computing a bound on the performance of a specific auction, is to have access to a "useable" expression for the best possible revenue, in order to compare it with. Practically, this means that we would like to have a *closed form formula* for bounding the optimal revenue in each of our models. As we discussed before, there has been no useful characterization for optimality in order to provide such closed form descriptions, and also it is widely believed that such descriptions probably not even exist. But, driven by traditional LP-duality for approximation algorithms, we could use closed form *upper bounds* of the optimal revenue if we had access to any. And that is exactly what the duality-theory framework for auctions of [8] provides us with. They transform the optimal auctions problem under the truthfulness constraint, i.e. the problem of maximizing revenue (see (3.1) below) over the set of all feasible convex utility functions with derivatives in $[0, 1]$ (remember that these correspond to probabilities of allocation), to a relaxed dual problem of minimizing the volume under the graph of some functions (see (3.1)) that have to satisfy certain boundary conditions (see (3.4)–(3.5)) and also cannot increase to "steeply" (see (3.3)).

More formally, consider a single-buyer m-items setting where the buyer has valuations $\mathbf{x} = (x_1, \ldots, x_m)$ for the items, drawn from some (joint) probability distribution F with density f, over a domain $D = [L_1, H_1] \times \cdots \times [L_m, H_m]$. Let $u(\mathbf{x})$ denote the player's utility when he reports bid-vector $\mathbf{x}$. Then the optimal revenue problem is

$$\sup_{u} \mathop{\mathbb{E}}_{\mathbf{x}\sim F}[p(\mathbf{x})] = \int_D \left(\nabla u(\mathbf{x}) \cdot \mathbf{x} - u(\mathbf{x})\right) dF(\mathbf{x}) \tag{3.1}$$



(a) Uniform i.i.d. valuations

(b) Independent exponential valuations.

Figure 3.1: Approximation ratios for the auction that sells every item separately (blue line) and for the one that sells all items in a full bundle (red line)

where u ranges over the space of nonnegative convex functions on D having the property $\nabla u(\mathbf{x}) \in [0,1]^m$ almost everywhere in D. The dual "program" is

$$\inf_{z_1,\ldots,z_m} \int_D \sum_{j=1}^{m} z_j(\mathbf{x})\, d\mathbf{x} \tag{3.2}$$

where $z_1, \ldots, z_m$ are absolutely continuous functions over D that satisfy the following properties:

$$z_j(L_j, \mathbf{x}_{-j}) \leq L_j f(L_j, \mathbf{x}_{-j}) \quad \text{for all } \; j \in [m] \tag{3.3}$$

$$z_j(H_j, \mathbf{x}_{-j}) \geq H_j f(H_j, \mathbf{x}_{-j}) \quad \text{for all } \; j \in [m] \tag{3.4}$$

$$\sum_{j=1}^{m} \frac{\partial z_j(\mathbf{x})}{\partial x_j} \leq (m+1) f(\mathbf{x}) + \mathbf{x} \cdot \nabla f(\mathbf{x}). \tag{3.5}$$

The challenging part is to come up with appropriate "dual variables" $z_1, \ldots, z_m$ that are able to give a good upper bound on the optimal revenue. By constructing such dual variables and analyzing their properties, we are able to exactly compute the performance of selling items separately or in a full bundle, in our two models of valuations' priors. The results can be summarized in the graphs in Figures 3.1a and 3.1b.

In addition to these approximations ratios, and given the fact that analyzing the performance of the full-bundle auction for the case of exponential distributions is very difficult (there is no red line at the graph of Figure 3.1b), we propose a simple, randomized modification of this auction, that essentially sells the items with probability proportional to their exponential distribution parameters. We call this auction Proportional and, if $f_j(x) = \lambda_j e^{-\lambda_j x}$ is the density function of the j-th item valuation, with λ_j's w.l.o.g. ordered in decreasing order, then we can prove that Proportional is $\frac{\lambda_1}{\lambda_m}$ approximate. A very important consequence of this is that, for identical exponential settings this ratio becomes 1, meaning that Proportional is optimal. In fact, in such a case Proportional is essentially reduced to the deterministic full-bundling auction, thus proving its optimality. We must point out that such optimality results for *any number of items* did not exist in the Auction Theory literature before, and it has been one of the most challenging research directions within this area during the last decade.

Bibliography

[1] Eli Biham and Adi Shamir. Differential fault analysis of secret key cryptosystems. In *Advances in Cryptology-CRYPTO'97*, pages 513–525. Springer, 1997.

[2] Dan Boneh, Richard A DeMillo, and Richard J Lipton. On the importance of checking cryptographic protocols for faults. In *Advances in Cryptology-EUROCRYPT'97*, pages 37–51. Springer, 1997.

[3] Dana Dachman-Soled and Yael Tauman Kalai. Securing circuits against constant-rate tampering. In *Advances in Cryptology–CRYPTO 2012*, pages 533–551. Springer, 2012.

[4] Constantinos Daskalakis, Alan Deckelbaum, and Christos Tzamos. The complexity of optimal mechanism design. *CoRR*, abs/1211.1703, 2013.

[5] Constantinos Daskalakis, Alan Deckelbaum, and Christos Tzamos. Mechanism design via optimal transport. In *Proceedings of the fourteenth ACM conference on Electronic commerce*, EC '13, pages 269–286, New York, NY, USA, 2013. ACM.

[6] Sebastian Faust, Krzysztof Pietrzak, and Daniele Venturi. Tamper-proof circuits: How to trade leakage for tamper-resilience. In *Automata, Languages and Programming*, pages 391–402. Springer, 2011.

[7] Yiannis Giannakopoulos. Strongly Truthful and Composable Mechanism Design, January 2013. UaESMC Deliverable 3.2.

[8] Yiannis Giannakopoulos and Elias Koutsoupias. Duality and optimality for uniform auctions. Manuscript, 11 2013.

[9] Yiannis Giannakopoulos and Elias Koutsoupias. Bounding optimal revenue in multiple-items auctions. Manuscript, 2014.

[10] Sergiu Hart and Noam Nisan. Approximate revenue maximization with multiple items. In *Proceedings of the 13th ACM Conference on Electronic Commerce*, EC '12, pages 656–656, New York, NY, USA, 2012. ACM.

[11] Yuval Ishai, Manoj Prabhakaran, Amit Sahai, and David Wagner. Private circuits ii: Keeping secrets in tamperable circuits. In *Advances in Cryptology-EUROCRYPT 2006*, pages 308–327. Springer, 2006.

[12] Aggelos Kiayias and Yiannis Tselekounis. Tamper resilient circuits: The adversary at the gates. In *Advances in Cryptology-ASIACRYPT 2013*, pages 161–180. Springer, 2013.

[13] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Advances in Cryptology-CRYPTO'99*, pages 388–397. Springer, 1999.

[14] Alejandro M. Manelli and Daniel R. Vincent. Bundling as an optimal selling mechanism for a multiple-good monopolist. *Journal of Economic Theory*, 127(1):1 – 35, 2006.

[15] R.B. Myerson. Optimal auction design. *Mathematics of Operations Research*, 6(1):58–73, 1981.

[16] J.C. Rochet. The taxation principle and multi-time hamilton-jacobi equations. *Journal of Mathematical Economics*, 14(2):113 – 128, 1985.

[17] J.C. Rochet and L.A. Stole. The economics of multidimensional screening. In *Advances in Economics and Econometrics: Theory and Applications. Eighth World Congress*, page 150. Cambridge University Press, 2003.

[18] Sergei P Skorobogatov and Ross J Anderson. Optical fault induction attacks. In *Cryptographic Hardware and Embedded Systems-CHES 2002*, pages 2–12. Springer, 2003.