MSc thesis defense presentation

Yiannis Tselekounis defends his MSc thesis

Date:	Monday, 29 Sep 2014
Time:	12:00-13:00
Location:	Department of Informatics, University of Athens, A56
Thesis title:	Tamper Resilient Circuits
Committee:	• Aggelos Kiayias • Aristeidis T. Pagourtzis • Efstathios Zachos

---

Thesis abstract

This dissertation studies the effect of gate-tampering attacks against cryptographic circuits. The proposed adversarial model is motivated by the plausibility of tampering directly with circuit gates and by the increasing use of tamper resilient gates among the known constructions that are shown to be resilient against wire-tampering adversaries. We prove that gate-tampering is strictly stronger than wire-tampering. On the one hand, we show that there is a gate-tampering strategy that perfectly simulates any given wire-tampering strategy. On the other, we construct families of circuits over which it is impossible for any wire-tampering attacker to simulate a certain gate-tampering attack (that we explicitly construct). We also provide a tamper resilience impossibility result that applies to both gate and wire tampering adversaries and relates the amount of tampering to the depth of the circuit. Finally, we show that defending against gate-tampering attacks is feasible by appropriately abstracting and analyzing the circuit compiler of Ishai et al. in a manner which may be of independent interest. Specifically, we first introduce a class of compilers that, assuming certain well defined tamper resilience characteristics against a specific class of attackers, can be shown to produce tamper resilient circuits against that same class of attackers. Then, we describe a compiler in this class for which we prove that it possesses the necessary tamper-resilience characteristics against gate-tampering attackers.