UCLouvain

UCL Crypto Group
Place du Levant, 3
1348 Louvain-la-Neuve
+32 10 47 2565
fstandae@uclouvain.be

To whom it may concern

Małgorzata Gałązka's PhD dissertation delves into the increasingly critical issue of securing (e.g., cryptographic) implementations against Hardware Trojan Horses (HTHs), which are malicious modifications inserted during the manufacturing of the implementations.

These modifications can cause devices to deviate from their intended functionality which, as shown by previous work, poses significant security risks. The thesis aims at developing countermeasures against HTHs that are provably secure in theoretically sound models.

The introduction sets the scene by highlighting the growing importance of security in our increasingly interconnected world. It explains what HTHs are, categorizes them, and describes how they can be introduced during the manufacturing process. The introduction also further motivates the thesis by showing that, as the production of computational devices is often outsourced globally, ensuring their security becomes paramount.

The thesis then explores existing solutions to counter HTHs, primarily focusing on "circuit compilers" and "testing procedures". Circuit compilers transform a given circuit into one that is resilient against HTHs, while testing procedures involve dividing the lifecycle of a circuit into so-called lab (i.e., test) and wild (i.e., use) phases to detect tampering.

A bit more in detail, the second section provides detailed modeling of HTHs and the countermeasures against them while the next two sections describe the main contributions. The third section focuses on "efficiently testable circuits", discussing the tampering model, wire- and gate-covering sets, and the notion of information loss used to capture security. And the fourth section explores "very simple schemes", which aim to simplify the master module of a device and minimize the overheads (in size) of the compiled circuits.

Both sections are based on a sound (cryptographic) methodology, where a threat model is formally defined and the security of the countermeasures is reduced to clear assumptions, with discussions of what can/cannot be achieved with models and of the optimality of the proposals. Compared to previously published solutions relying on cryptographic constructions leading to significant overheads (e.g., multiparty or verifiable computations), the very simple schemes come with enhanced practicality. Indeed, they essentially leverage the circuit to protect against HTHs without additional (cryptographic) functionalities. Efforts are also made in order to minimize the assumptions required for security. Of particular interest in this direction, the candidate discusses how to get rid of a "conductivity" assumption, which conveniently (but unrealistically) restricts the tampering of wires with multiple destinations (i.e., large fan-out) so that they cannot be targeted individually.

The dissertation relies on published material in recognized venues in cryptography and information security research (TCC and ITCS). This is remarkable in the sense that HTHs are in general a difficult topic on which to publish (mostly because the threat is hard to capture). Overall, the technical contribution and editorial quality of the manuscript are excellent. Despite the theoretical nature of her work, the candidate spent useful efforts in illustrating the formal models with more concrete examples, so that the thesis becomes accessible to a more practical audience. Discussions also make the practical limitations that should still be addressed as further research explicit. Doing so, I believe the thesis provides a solid foundation for future research, with both theoretical and more practical directions.

As a result of the above, I deem the thesis sufficient to grant the PhD degree.

Don't hesitate to contact me in case of further questions.

Pr. François-Xavier Standaert
UCL Crypto Group, Belgium
November 14, 2024