View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Dagstuhl Research Online Publication Server

Engineering On-Chip Thermal Effects

Patrick Schaumont

ECE Department, Virginia Tech, Blacksburg, VA

Abstract. Temperature effects can be used to maliciously affect the behavior of digital crypto-circuits. For example, temperature effects can create covert communication channels, and they can affect the stability of physical unclonable functions (PUFs). This talk observes that these thermal effects can be engineered, and we describe two techniques. The first technique shows how to filter the information through a covert temperature channel. This leads to detectors for very specific events, for example, someone touching the chip package. The second technique shows how to mitigate the impact of temperature on a PUF design while avoiding costly post-processing. We discuss the design of a compact ring-oscillator PUF for FPGA which is tolerant to temperature variations.

1 Thermal Filtering of On-chip Events

The use of thermal effects as a covert channel was demonstrated by Brouchier et al. They modulated the fan speed of a personal computer with a secret sequence [1]. This method requires however relatively high signal-to-noise ratio, and it has a low communication bandwidth.

We present a method that relaxes the high signal-to-noise ratio requirement. Our objective is to increase the sensitivity of an on-chip digital thermal sensor [2]. In contrast to the existing mechanisms that characterize the overall temperature profile on a die, our solution is able to detect the submerged thermal variation caused by specific predefined events (SPE), under the precondition that the SPE's characteristic frequency component does not overlap with those of other thermal events. This is made possible by pre-filtering of the temperature value.

As illustrated in Figure 1, we use a digital temperature sensor based on periodically integrating and dumping the free-running frequency of a ring oscillator. The resulting value is then bandpass-filtered in order to detect the characteristic frequency of a specific heat source. We experimentally demonstrated that this filtering chain is sufficiently sensitive to detect a human touching an FPGA package, while at the same time remaining robust against other environmental effects.

2 Reducing the Thermal Sensitivity of PUF

The thermal sensitivity of digital circuits is of specific importance to Physical Unclonable Functions. For example, a change in temperature will affect the free

Dagstuhl Seminar Proceedings 09282
Foundations for Forgery-Resilient Cryptographic Hardware
http://drops.dagstuhl.de/opus/volltexte/2010/2403

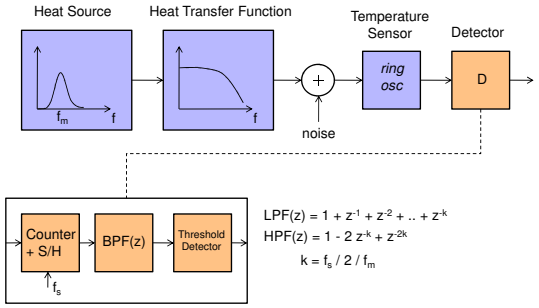

Fig. 1. Digital Filter Chain to Detect Thermal On-chip Events

running frequency of a ring-oscillator. This, in turn, may influence the challenge/response characteristic of a ring-oscillator based PUF. While the effects of temperature on the stability of a PUF can be addressed by proper helper data functions, it is also possible to compensate the effects of temperature at circuit-level, through redundancy [3]. We present an efficient FPGA implementation of such redundant ring-oscillators in [4]. The configurable ring oscillator, shown in Figure 2, increases PUF stability dramatically, yet it fits in the same amount of FPGA resources as a normal ring oscillator.

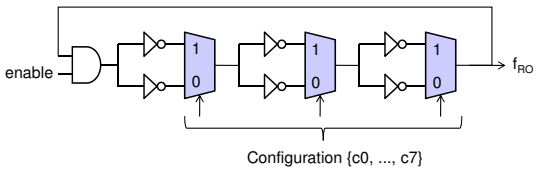

Fig. 2. Configurable Ring Oscillator for increased RO-PUF stability

References

1. Brouchier, J., Dabbous, N., Kean, T., Marsh, C., Naccache, D.: Thermocommunication, IACR ePrint publication 2009/002. `http://eprint.iacr.org/2009/002.pdf`.
2. Chen, Z., Nagesh, R., Reddy, A., Schaumont, P.: Increasing the Sensitivity of On-Chip Digital Thermal Sensors with Pre-filtering, IEEE Computer Society Annual Symposium on VLSI (ISVLSI 2009), May 2009.
3. G. E. Suh and S. Devadas. Physical Unclonable Functions for Device Authentication and Secret Key Generation. In Proceedings of Design Automation Conference, June 2007.
4. Maiti, A. Schaumont, P.: Improving the Quality of Physical Unclonable Functions Using Configurable Ring Oscillators, 19th International Conference on Field Programmable Logic and Applications, September 2009.