

# Scoping the NIST Masked Circuits Project

Luís Brandão<sup>1</sup> and René Peralta<sup>2</sup>

January 24, 2022

In the year 2022, the NIST [Masked Circuits](#) project will aim to collect concrete masked circuits specified at the logical level. Of particular interest are unrolled Boolean circuits useful as components of cryptographic primitives. At this stage the project is not aiming at new standards, nor at a competition, but intends to establish a public basis for subsequent analysis.

**Masked circuits.** Masking schemes for Boolean circuits apply secret sharing to the secret bits of the original circuit. At a logical level, masking can be specified using *netlists* that represent the circuit flow as a directed acyclic graph. After a  $d$ -th order masking, the probing of up to  $d$  wires in a masked circuit should not reveal information about the logical values of the bits in the original circuit. However, not all masking schemes and attack models correspond well to one another. Masked circuits can attain various properties of interest, and can span diverse tradeoffs between masking order, number of gates, circuit depth, and amount of randomness. One important consideration is composability, which relates to how some properties of interest are maintained or not once various masked circuit-components (a.k.a. gadgets, e.g., an S-Box) are composed to form a larger circuit.

**Utility.** There is a large body of research, still active, on circuit masking. The goal of masking an unrolled circuit (say, to print on a chip) is to enhance resistance against certain side-channel attacks. In particular, masking can affect the signal-to-noise ratio available to an attacker during an evaluation with noisy leakage. However, the effect on side-channel leakage may vary across implementation settings, and a masking produced from generic principles may not be as efficient and/or cheap as a tailored masking. The tailoring makes sense when considering a particular application setting: circuit, adversary and cost metric. Given the tension of performance-and-cost vs. security models-and-properties, different settings justify using different types of masking schemes. For example, during the evaluation of a hardware circuit, a *glitch* may enable a wire probing to obtain more information than what would be expected in a simplified model, so this may also affect what masking scheme to use.

**Action.** The Masked Circuits project will issue a public call for contributions in the form of concrete masked circuits. These will be organized, in collaboration with the Circuit Complexity project, in the Cryptographic Technology Group, into a *masked circuits library* (MCL). There is an initial focus on circuits for the advanced encryption standard (AES), but with time this will be extended to other primitives represented in the form of vectorial Boolean functions. The MCL will be an open reference of masked circuits for analysis by the community, to foster a better understanding of various tradeoffs, as well as of tools for verification of properties.

**Complementary aspects out of scope.** In the future, the MCL can serve as a basis for comparative analyses of side-channel leakage and resistance for certain physical implementations. However, said testing and evaluation is currently out of scope for this project.

---

<sup>1,2</sup>NIST [Cryptographic Technology Group](#). <sup>1</sup>Foreign guest researcher at NIST, contractor from Strativia.