P

Probing Model

Gaëtan Cassiers
UCLouvain, Louvain-la-Neuve, Belgium

Synonyms

Threshold probing model

Definitions

The probing model, also known as threshold probing model, is a leakage model used to analyze the security of implementations against side-channel attacks. More precisely, this model has been introduced in Ishai et al. (2003) to prove the security of the masking countermeasure in the finite field $\mathbb{F}_2$ and then extended to any finite field by Rivain and Prouff (2010). A masked arithmetic circuit is *t-probing secure* if the values carried by any set of t wires in the circuit are jointly independent of any secret. The security parameter t is known as the *security order*.

Background

The probing model was introduced fairly quickly after the first proposal of a masking countermeasure (Chari et al. 1999; Messerges 2000) to protect against side-channel attacks. Some of these early schemes have been shown to be broken (Coron and Goubin 2000), highlighting the need for a formalization of a security notion for these schemes. The probing model comprises both a simple and abstract model for the side-channel leakage that can be observed by an adversary and a simple definition of adversary's goal.

Theory

In the probing model, computations are modeled as randomized arithmetic circuits over a finite field (i.e., arithmetic circuits extended with "random gates" whose output is a uniformly distributed element). The most common examples of fields are $\mathbb{F}_2$ (for bit-level masking) and $\mathbb{F}_{256}$ (for implementations of the AES).

A masked circuit is modeled in three parts: (i) randomized encoder sub-circuits I that generate sharings (so-called input sharings) from sensitive input variables, (ii) the actual masked circuit C that performs secure computations on input sharing to generate output sharings, and (iii) the decoders O that unmask the output sharings. The parts I and O are assumed to not leak (they should manipulate only public values such as ciphertext or be executed when the leakage cannot be observed).

In the probing model, the adversary can place t probes (t is the security parameter), where a probe is the selection of a wire in C. When the circuit is executed, the adversary observes the value carried by each probed wire. A circuit

S. Jajodia et al. (eds.), *Encyclopedia of Cryptography, Security and Privacy*,
https://doi.org/10.1007/978-3-642-27739-9_1699-1

is t-probing secure if, for any choice of probes by the adversary, the observations are jointly independent of the sensitive input variables.

Composition

A major limitation of the t-probing model is its lack of composability. For example, let us consider two t-probing secure circuits C and C', and let us build C'' by connecting the output shares of C to the input shares of C'; then C'' may not be t-probing secure. To solve this limitation, stronger definitions have been introduced such as (strong) non-interference (Barthe et al. 2016) or probe-isolating non-interference (Cassiers and Standaert 2020) for which some generic composition properties hold. These properties therefore enable design by composition: large secure circuits can be built by composing multiple small ones.

Real-World Leakage

Despite being fairly abstract, t-probing security has been shown to imply (Prouff and Rivain 2013; Duc et al. 2019) security in more realistic leakage models such as the *random probing model* (where, for some parameter p, the adversary gets the value of each wire in the circuit with independent probability p) or the *noisy leakage model* (where a noisy version of every wire is observed by the adversary). The provable security level in these models scales however very poorly with the size of the circuit, which has led to the introduction of the region probing model (Duc et al. 2019) in which the circuit is split in multiple regions, and the adversary can place t probes in every region. As a result, if the size of the regions is kept constant, the random probing and noisy leakage security bounds become linear in the size of the circuit.

Another limitation of the t-probing model is its failure to model physical leakage phenomena in which the leakage depends jointly on multiple values. This has been solved with the *robust probing model* of Faust et al. (2018) that takes into account so-called glitches, transitions, and couplings by considering *extended probes*. A glitch-, transition-, or coupling-extended probe on a wire gives more information to the adversary than just the value of the wire: it also leaks the value of other wires (the set of wires leaking depend on the structure of the circuit and the type of extended probe).

Open Problems and Future Directions

The t-probing model and its robust extensions are well-established for analyzing the security of small circuits and their composition, thanks to their simplicity and practical relevance to real-world security. However, the current reductions to more realistic leakage models give bounds much worse that the observed practical security level. Improving these bounds is an active research topic with multiple approaches, such as improving the tightness of the reductions between models (Prest et al. 2019), directly analyzing the security of circuits in the more realistic models (Belaïd et al. 2021; Cassiers et al. 2021), and introducing improved variants of the models (Dziembowski et al. 2015).

References

Barthe G, Belaïd S, Dupressoir F, Fouque P, Grégoire B, Strub P, Zucchini R (2016) Strong non-interference and type-directed higher-order masking. In: CCS. ACM, pp 116–129

Belaïd S, Rivain M, Taleb AR (2021) On the power of expansion: more efficient constructions in the random probing model. In: EUROCRYPT (2). Lecture notes in computer science, vol 12697. Springer, pp 313–343

Cassiers G, Standaert F (2020) Trivially and efficiently composing masked gadgets with probe isolating non-interference. IEEE Trans Inf Foren Secur 15:2542–2555

Cassiers G, Faust S, Orlt M, Standaert F (2021) Towards tight random probing security. In: CRYPTO (3). Lecture notes in computer science, vol 12827. Springer, pp 185–214

Chari S, Jutla CS, Rao JR, Rohatgi P (1999) Towards sound approaches to counteract power-analysis attacks. In: CRYPTO. Lecture notes in computer science, vol 1666. Springer, pp 398–412

Coron J, Goubin L (2000) On boolean and arithmetic masking against differential power analysis. In: CHES. Lecture notes in computer science, vol 1965. Springer, pp 231–237

Duc A, Dziembowski S, Faust S (2019) Unifying leakage models: from probing attacks to noisy leakage. J Cryptol 32(1):151–177

Dziembowski S, Faust S, Skorski M (2015) Noisy leakage revisited. In: EUROCRYPT (2). Lecture notes in computer science, vol 9057. Springer, pp 159–188

Faust S, Grosso V, Pozo SMD, Paglialonga C, Standaert F (2018) Composable masking schemes in the presence of physical defaults & the robust probing model. IACR Trans Cryptogr Hardw Embed Syst 2018(3):89–120

Ishai Y, Sahai A, Wagner DA (2003) Private circuits: securing hardware against probing attacks. In: CRYPTO. Lecture notes in computer science, vol 2729. Springer, pp 463–481

Messerges TS (2000) Securing the AES finalists against power analysis attacks. In: FSE. Lecture notes in computer science, vol 1978. Springer, pp 150–164

Prest T, Goudarzi D, Martinelli A, Passelègue A (2019) Unifying leakage models on a rényi day. In: CRYPTO (1). Lecture notes in computer science, vol 11692. Springer, pp 683–712

Prouff E, Rivain M (2013) Masking against side-channel attacks: a formal security proof. In: EUROCRYPT. Lecture notes in computer science, vol 7881. Springer, pp 142–159

Rivain M, Prouff E (2010) Provably secure higher-order masking of AES. In: CHES. Lecture notes in computer science, vol 6225. Springer, pp 413–427