Confusing Information

Éloi de Chérisey, Sylvain Guilley, Olivier Rioul

Abstract

In this presentation, we will recall the notions of *confusion* and show that, in the case of a monobit leakage, MIA and CPA are similar.

To do so, we recall the link between CPA and the confusion coefficient, and then, explore by Taylor expansions how we can link this confusion coefficient to MIA. We show that the distinguishers corresponding to both CPA and MIA are proportional when the sensitive variable is binary.

We apply these results to the case of a monobit leakage with AES substitution box and without substitution box to show the impact of this confusion coefficient, and how this impact can be measured.

Finally, we open the discussion to extend these results to non-binary distributions.