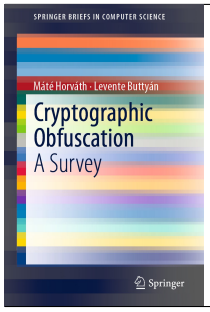

Errata of "*Cryptographic Obfuscation - A Survey*"

Máté Horváth and Levente Buttyán

If You find further errors, please let us know by sending an e-mail to

mhorvath@crysys.hu

Last updated: July 20, 2022

page xix, line 14:

✗ common reference string (see Glossary)

✓ common reference string (see the Glossary)

page xxi, line 14:

✗ Turing machine (Glossary)

✓ Turing machine (see the Glossary)

page 9: Sub-subsection titles of §1.5.1–1.5.3 contain unnecessary full stop.

page 13, line 1 and 3 of footnote 4:

✗ a publicly known circuit $C(.,.)$ with two inputs ... (i.e. $\mathcal{O}[C_K](.)$ is published)

✓ a publicly known circuit $C(\cdot,\cdot)$ with two inputs ... (i.e. $\mathcal{O}[C_K](\cdot)$ is published)

page 17, last line:

✗ degree$-\kappa$ polynomials on encodings

✓ degree-κ polynomials on encodings

page 18, column 6, row 3 of Table2.1:

✗ $S_k \cap S_l$

✓ $S_k \cap S_l = \varnothing$

page 19, line 17:

✗ These are addition, multiplication, and zero-testing.[9]. The first two

✓ These are addition, multiplication, and zero-testing.[9] The first two

page 45, line last but 11:

✗ of Tok.Enc(.,.) must be independent of C

✓ of Tok.Enc$(\cdot,\cdot)$ must be independent of C

page 45, line last but 10:

✗ ... not useful for the the goals usual type of obfuscation...

✓ ... not useful for the goals of the usual type of obfuscation...

page 57, line 13:

✗ the matrices $A_{i,b}$ of the ith step of the MBP to form $B_{i,b} = R_{i-1}^{-1} A_{i,b} R_i$ for $b = \{0,1\}$

✓ the matrices $A_{i,b}$ of the ith step of the MBP to form $B_{i,b} = R_{i-1}^{-1} A_{i,b} R_i$ for $b \in \{0,1\}$

page 31, footnote 1:

✗ In the case of Turing machine (Glossary)s, even this assumption is unnecessary.

✓ In the case of Turing machines, even this assumption is unnecessary.

page 59: The paragraph "Avoiding algebraic attacks" is duplicated. The first occurrence, starting on page 58, is the correct one, its copy (just below it) contains typos and should be omitted.

page 67, line 24:

✗ (denoted by ◊in Table...

✓ (denoted by ◊ in Table...