Errata Version 4 Oct 2024

This is the errata for the book

Cryptography and Embedded Systems Security, Xiaolu Hou, Jakub Breier, ISBN: 978-3-031-62205-2, Springer Nature, 2024.

published version

`https://link.springer.com/book/10.1007/978-3-031-62205-2`

The author's copy with errors corrected can be found in the following link:

`https://xiaoluhou.github.io/Textbook.pdf`

<table>
<tr><th>Location</th><th>Original</th><th>Change</th></tr>
<tr><td>Page 9, Algorithm 1.1, lines 2-4</td><td>
Input: $m,\ n$// $m,n \in \mathbb{Z},\ m \neq 0$
Output: $\gcd(m,n)$
1 while $m \neq 0$ do
2 $r = n\%m$// remainder of n divided by m
3 $n = m$
4 $m = r$
5 return r
</td><td>
Input: $m,\ n$// $m,n \in \mathbb{Z},\ m \neq 0$
Output: $\gcd(m,n)$
1 while $m \neq 0$ do
2 $r = m$
3 $m = n\%m$// remainder of n divided by m
4 $n = r$
5 return n
</td></tr>
<tr><td>Page 18, first paragraph below Definition 1.2.12</td><td>By definition, for any $a \in F$, there exists $b \in F$ such that ...</td><td>By definition, for any $a \in F$, $a \neq 0$, there exists $b \in F$ such that ...</td></tr>
<tr><td>Page 20, Example 1.2.24</td><td>$f(1 \oplus 0) = f(1) = a,\ f(1) + f(0) = a + b = a$</td><td>$f(1 \oplus 0) = f(1) = b,\ f(1) + f(0) = b + a = b$</td></tr>
<tr><td>Page 49, Theorem 1.5.1</td><td>of $\deg(f(x)) \geq 1$</td><td>if $\deg(f(x)) \geq 1$</td></tr>
<tr><td>Page 51, Example 1.5.6</td><td>$\mathbb{F}_2[x]/(f(x)) = \{1, x, x+1\}$
...
$\mathbb{F}_2[x]/(g(x)) = \{1, x, x+1\}$</td><td>$\mathbb{F}_2[x]/(f(x)) = \{0, 1, x, x+1\}$
...
$\mathbb{F}_2[x]/(g(x)) = \{0, 1, x, x+1\}$</td></tr>
<tr><td>Page 106 Table 2.2 (b)</td><td>
<table>
<tr><td>$\acute{A}$</td><td>11000001</td><td>C1</td></tr>
<tr><td>$\ddot{A}$</td><td>11000100</td><td>C4</td></tr>
<tr><td>$\acute{I}$</td><td>11001101</td><td>CD</td></tr>
<tr><td>$\times$</td><td>11010111</td><td>D7</td></tr>
<tr><td>$\div$</td><td>11110111</td><td>F7</td></tr>
</table>
</td><td>
<table>
<tr><td>$\acute{A}$</td><td>1100001110000001</td><td>C381</td></tr>
<tr><td>$\ddot{A}$</td><td>1100001110000100</td><td>C384</td></tr>
<tr><td>$\acute{I}$</td><td>1100001110001101</td><td>C38D</td></tr>
<tr><td>$\times$</td><td>1100001110010111</td><td>C397</td></tr>
<tr><td>$\div$</td><td>1100001110110111</td><td>C3B7</td></tr>
</table>
</td></tr>
<tr><td>Page 133</td><td>When $\omega_1 = \omega_2$...the Sbox is a ω_1-bit Sbox</td><td>When $\omega_1 = \omega_2$...the Sbox is an ω_1-bit Sbox</td></tr>
<tr><td>Page 139, RSA security</td><td>Nevertheless, post-quantum public key cryptosystems are being proposed (see e.g. [HPS98, BS08]) to protect communications after a quantum computer is built.</td><td>Nevertheless, post-quantum public key cryptosystems are being proposed (see e.g. [HPS98, BS08]) to protect communications after a sufficiently strong quantum computer is built.</td></tr>
<tr><td>Page 160, Example 3.2.4 last sentence</td><td>Then $\varphi_0(\boldsymbol{x}) = 0$.</td><td>Then $\varphi_0(0) = 0$.</td></tr>
<tr><td>Page 209, last paragraph of Section 4.1.1</td><td>Similar to SPA, the attack does not require statistical analysis of the traces, only visual inspection is enough.</td><td>The sentence should be removed</td></tr>
</table>