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><td>Location</td><td>Original</td><td>Change</td></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>Á</td><td>11000001</td><td>C1</td></tr><tr><td>Ä</td><td>11000100</td><td>C4</td></tr><tr><td>Í</td><td>11001101</td><td>CD</td></tr><tr><td>×</td><td>11010111</td><td>D7</td></tr><tr><td>÷</td><td>11110111</td><td>F7</td></tr></table></td><td><table><tr><td>Á</td><td>1100001110000001</td><td>C381</td></tr><tr><td>Ä</td><td>1100001110000100</td><td>C384</td></tr><tr><td>Í</td><td>1100001110001101</td><td>C38D</td></tr><tr><td>×</td><td>1100001110010111</td><td>C397</td></tr><tr><td>÷</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 $\varphi_0(\mathtt{0}) = 0$.</td></tr>
<tr><td>Page 170, first paragraph</td><td>which is computationally infeasible according to property (c) of hash functions listed in Sect. 2.1.1.</td><td>which is computationally infeasible according to property (b) of hash functions listed in Sect. 2.1.1.</td></tr>
<tr><td>Page 177</td><td>$m = m_p y_q q + m_q y_p p \bmod n = 2 \times 2 \times 5 + 2 \times 2 \times 3 = 32 \bmod 15 = 2.$</td><td>$m = m_p y_q q + m_q y_p p \bmod n = 2 \times 2 \times 5 + 2 \times 2 \times 3 \bmod 15 = 32 \bmod 15 = 2.$</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>
<tr><td>Page 236, Example 4.2.15</td><td>$\mathrm{E}\left[\mathrm{wt}\left(\boldsymbol{v}\right)^2\right] = \frac{1}{\lvert\mathbb{F}_2^{\mathtt{S}}\rvert} \sum_{\boldsymbol{v} \in \mathbb{F}_2^{\mathtt{S}}} \mathrm{wt}\left(\boldsymbol{v}^2\right) = \dots$</td><td>$\mathrm{E}\left[\mathrm{wt}\left(\boldsymbol{v}\right)^2\right] = \frac{1}{\lvert\mathbb{F}_2^{\mathtt{S}}\rvert} \sum_{\boldsymbol{v} \in \mathbb{F}_2^{\mathtt{S}}} \mathrm{wt}\left(\boldsymbol{v}\right)^2 = \dots$</td></tr>
<tr><td>Page 248, Remark 4.3.1</td><td>For AES, the correlations between the first AddRoundKey outputs are higher than correlations between the first SubBytes operation outputs, that is why in...</td><td>For the PRESENT cipher, correlations among outputs from the initial <code>addRoundKey</code> operation are stronger than those between outputs of the initial <code>sBoxLayer</code>. Therefore, in...</td></tr>
<tr><td>Page 262, last sentence</td><td>With our profiling traces, we can compute M_{signal} templates.</td><td>With our profiling traces, we can compute M_{signal} templates, with each template correspond to one possible value of the target signal.</td></tr>
<tr><td>Page 263, first paragraph</td><td>For our illustrations, when the target signal is $\boldsymbol{v}$, we will have 16 templates. And when the target signal is $\mathrm{wt}\left(\boldsymbol{v}\right)$, we will have 5 templates.</td><td>For our illustrations, when the target signal is $\boldsymbol{v}$, we obtain 16 templates, each corresponding to a possible value of $\boldsymbol{v}$ from <code>0</code> to <code>F</code>. When the target signal is $\mathrm{wt}\left(\boldsymbol{v}\right)$, we derive 5 templates, each corresponding to a Hamming weight value from 0 to 4.</td></tr>
<tr><td>Page 263 Template Step c</td><td>For a fixed key hypothesis $\hat{k}_i$, we divide the M_p attack traces from P-DPA Step 10 into M_{signal} sets, $A_1, A_2, \dots, A_{M_{signal}}$, depending on the hypothetical target intermediate value $\hat{\boldsymbol{v}}_{ij}$ obtained in P-DPA Step 11. In particular, for an attack trace $\boldsymbol{\ell}_j$, let s_{ij} denote the index of the set that it belongs to. Namely
$$\boldsymbol{\ell}_j \in A_{s_{ij}} \quad \text{given key hypothesis } \hat{k}_i.$$
We are only interested in the leakages at the POIs for each attack trace $\boldsymbol{\ell}_j = (l_1^j, l_2^j, \dots, l_q^j)$. Define
$$\boldsymbol{\ell}_{j,\mathrm{POI}} := (l_{t_1}^j, l_{t_2}^j, \dots, l_{t_{q_{\mathrm{POI}}}}^j).$$
With the mean vector $\boldsymbol{\mu}_{s_{ij}}$ and the covariance matrix $Q_{s_{ij}}$ obtained in Template Step b, we can compute the probability of $\boldsymbol{\ell}_j$ given $\hat{k}_i$ using the PDF ...</td><td>We are only interested in the leakages at the POIs for each attack trace $\boldsymbol{\ell}_j = (l_1^j, l_2^j, \dots, l_q^j)$. Define
$$\boldsymbol{\ell}_{j,\mathrm{POI}} := (l_{t_1}^j, l_{t_2}^j, \dots, l_{t_{q_{\mathrm{POI}}}}^j).$$
For each key hypothesis $\hat{k}_i$ and attack trace $\boldsymbol{\ell}_j$, we compute the hypothetical target intermediate value given the knowledge of the associated plaintext. Let $\mu_{s_{ij}}$ and $Q_{s_{ij}}$ be the template for this hypothetical value, corresponding to $\hat{k}_i$ and $\boldsymbol{\ell}_j$, as obtained in Template Step b. The probability of $\boldsymbol{\ell}_j$ given $\hat{k}_i$ can then be computed using the PDF ...</td></tr>
</table>