Errata Version 6 Dec 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`

Location	Original	Change
Page 9, Algorithm 1.1, lines 2-4	**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	**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
Page 18, first paragraph below Definition 1.2.12	By definition, for any $a \in F$, there exists $b \in F$ such that ...	By definition, for any $a \in F$, $a \neq 0$, there exists $b \in F$ such that ...
Page 20, Example 1.2.24	$f(1 \oplus 0) = f(1) = a,\ f(1) + f(0) = a + b = a$	$f(1 \oplus 0) = f(1) = b,\ f(1) + f(0) = b + a = b$
Page 49, Theorem 1.5.1	of $\deg(f(x)) \geq 1$	if $\deg(f(x)) \geq 1$
Page 51, Example 1.5.6	$\mathbb{F}_2[x]/(f(x)) = \{1, x, x+1\}$ ... $\mathbb{F}_2[x]/(g(x)) = \{1, x, x+1\}$	$\mathbb{F}_2[x]/(f(x)) = \{0, 1, x, x+1\}$ ... $\mathbb{F}_2[x]/(g(x)) = \{0, 1, x, x+1\}$
Page 59, Definition 1.6.6	A binary code C is said to be $k-$*error correcting* if the minimum distance decoding outputs the correct codeword...	A binary code C is said to be $k-$*error correcting* if with the incomplete decoding rule, minimum distance decoding outputs the correct codeword...
Page 106 Table 2.2 (b)	Á 11000001 `C1` Ä 11000100 `C4` Í 11001101 `CD` × 11010111 `D7` ÷ 11110111 `F7`	Á 1100001110000001 `C381` Ä 1100001110000100 `C384` Í 1100001110001101 `C38D` × 1100001110010111 `C397` ÷ 1100001110110111 `C3B7`
Page 133	When $\omega_1 = \omega_2$...the Sbox is a ω_1-bit Sbox	When $\omega_1 = \omega_2$...the Sbox is an ω_1-bit Sbox
Page 139, RSA security	Nevertheless, post-quantum public key cryptosystems are being proposed (see e.g. [HPS98, BS08]) to protect communications after a quantum computer is built.	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.
Page 160, Example 3.2.4 last sentence	Then $\varphi_0(\boldsymbol{x}) = 0$.	Then $\varphi_0(\mathtt{0}) = 0$.
Page 170, first paragraph	which is computationally infeasible according to property (c) of hash functions listed in Sect. 2.1.1.	which is computationally infeasible according to property (b) of hash functions listed in Sect. 2.1.1.
Page 177	$m = m_p y_q q + m_q y_p p \bmod n = 2 \times 2 \times 5 + 2 \times 2 \times 3 = 32 \bmod 15 = 2$.	$m = m_p y_q q + m_q y_p p \bmod n = 2 \times 2 \times 5 + 2 \times 2 \times 3 \bmod 15 = 32 \bmod 15 = 2$.
Page 209, last paragraph of Section 4.1.1	Similar to SPA, the attack does not require statistical analysis of the traces, only visual inspection is enough.	The sentence should be removed
Page 236, Example 4.2.15	$\mathrm{E}\left[\mathrm{wt}\left(\boldsymbol{v}\right)^2\right] = \frac{1}{\lvert\mathbb{F}_2^8\rvert}\sum_{\boldsymbol{v}\in\mathbb{F}_2^8} \mathrm{wt}\left(\boldsymbol{v}^2\right) = \ldots$	$\mathrm{E}\left[\mathrm{wt}\left(\boldsymbol{v}\right)^2\right] = \frac{1}{\lvert\mathbb{F}_2^8\rvert}\sum_{\boldsymbol{v}\in\mathbb{F}_2^8} \mathrm{wt}\left(\boldsymbol{v}\right)^2 = \ldots$
Page 248, Remark 4.3.1	For AES, the correlations between the first AddRoundKey outputs are higher than correlations between the first SubBytes operation outputs, that is why in...	For the PRESENT cipher, correlations among outputs from the initial `addRoundKey` operation are stronger than those between outputs of the initial `sBoxLayer`. Therefore, in...
Page 262, last sentence	With our profiling traces, we can compute M_{signal} templates.	With our profiling traces, we can compute M_{signal} templates, with each template correspond to one possible value of the target signal.
Page 263, first paragraph	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.	For our illustrations, when the target signal is $\boldsymbol{v}$, we obtain 16 templates, each corresponding to a possible value of $\boldsymbol{v}$ from `0` to `F`. 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.
Page 263 Template Step c	For a fixed key hypothesis $\hat{k}_i$, we divide the M_p attack traces from P-DPA Step 10 into M_{signal} sets, $A_1, A_2, \ldots, A_{M_{signal}}$, 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 $\boldsymbol{\ell}_j = (l_1^j, l_2^j, \ldots, l_q^j)$. Define $$\boldsymbol{\ell}_{j,\mathrm{POI}} := (l_{t_1}^j, l_{t_2}^j, \ldots, l_{t_{q_{\mathrm{POI}}}}^j).$$ 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 ...	We are only interested in the leakages at the POIs for each attack trace $\boldsymbol{\ell}_j = (l_1^j, l_2^j, \ldots, l_q^j)$. Define $$\boldsymbol{\ell}_{j,\mathrm{POI}} := (l_{t_1}^j, l_{t_2}^j, \ldots, l_{t_{q_{\mathrm{POI}}}}^j).$$ 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 ...
Page 334, below Equation (4.83)	The size of T1 is 8×4, and the storage required is $2^8 \times 2^4 = 2^{12}$ bits, or 2^9 bytes. The table T2 requires 16 bits of memory.	The size of T1 is 8×4, and the storage required is $2^8 \times 4 = 2^{10}$ bits, or 2^7 bytes. The table T2 requires $2^4 \times 4 = 64$ bits of memory.
Page 395, the last equation	$q = \gcd(s'^e - m, n) = \gcd(7^{11} - 2143) = \gcd(1977326741, 143)$.	$q = \gcd(s'^e - m, n) = \gcd(7^{11} - 2, 143) = \gcd(1977326741, 143)$.