Corrections and additions to “CryptoSchool”, Springer Verlag, October 2016

Joachim von zur Gathen

October 27, 2016

Section 2.2, page 32: in the matrix at the top, the bottom right entry `01` should be `02`:

$$\begin{pmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{pmatrix} = \begin{pmatrix} \texttt{02} & \texttt{01} & \texttt{01} & \texttt{03} \\ \texttt{03} & \texttt{02} & \texttt{01} & \texttt{01} \\ \texttt{01} & \texttt{03} & \texttt{02} & \texttt{01} \\ \texttt{01} & \texttt{01} & \texttt{03} & \texttt{02} \end{pmatrix} \cdot \begin{pmatrix} a_3 \\ a_2 \\ a_1 \\ a_0 \end{pmatrix}.$$

(Alfredo Viola, 22.08.2016).

Section 2.2, page 32: in the centered line below the middle, the value of b_3 is `DC`, not `FC`:

$$b_3 = t^7 + t^6 + t^4 + t^3 + t^2 = (11011100) = \texttt{DC} \quad in \mathbb{F}_{256}.$$

(Alfredo Viola, 22.08.2016).

Section 3.8, page 129. In the centered equation in the lower half, replace the second p by q:

$$x - z \equiv \begin{cases} \neq 0 \text{ in } \mathbb{Z}_p, \\ 0 \text{ in } \mathbb{Z}_q. \end{cases}$$

(Alfredo Viola, 06.09.2016).

Exercise 3.16, page 148, reference “Shamir 1993” missing in Bibliography: A. Shamir, *On the Generation of Polynomials which are Hard to Factor*, Proceedings STOC 1993, ACM, pages 796–804 (30.11.2015).

Section 5.1, page 208, equation (5.4): v is not quantified, and (5.4) should read:

$$L \cap E = \{(u, v) \in F^2 \colon v = ru + s \text{ and } (ru + s)^2 = u^3 + au + b\}. \quad (1)$$

(Christian Berghoff, 07.10.2016).

Section 5.1, page 210, second line below Figure 5.3: replace $(P+Q)+S = 0$ by $(P+Q)+S = \mathcal{O}$. (Christian Berghoff, 07.10.2016).

Section 5.2, page 214, line -3: missing space, should be “polynomial of”. (Christian Berghoff, 07.10.2016).

Section 5.7, page 227, first line of Section 5.7: replace “cyptographic” by “cryptographic” (30.11.2015).

Section 5.7, page 229: replace on line 8 “For a prime ℓ” by “For a prime ℓ not dividing the characteristic p of $\mathbb{F}_q$”. Equation (5.22): correct to

$$u = \prod l > 4\sqrt{q}, \tag{2}$$

and correspondingly six lines below: $B \approx \ln(4\sqrt{q}) = \bigl(2 + \frac{1}{2}\log_2 q\bigr)\ln 2$. (Christian Berghoff, 07.10.2016).

Notes to Section 6.3, page 296, last but one paragraph: replace “round round” by “round” (Ralph Wernsdorf, 21.03.2016).

Notes to Section 6.3, page 296, last line of last but one paragraph: replace “(Daemen & Rijmen 1999, Section 9.1.1)” by “(Daemen & Rijmen 2002b, Section 9.1.1)” (Ralph Wernsdorf, 21.03.2016).

Section 13.13, page 625: replace “Cyptography” by “Cryptography” (Oded Regev, 07.11.2015).

Section 13.13, page 628: on the last line, replace the exponent r by r^n:

$$\begin{aligned} \delta_r^{(n)}\colon \mathbb{R}^n &\to \mathbb{R}, \\ x &\mapsto r^{-n} \cdot e^{-\pi(||x||/r^n)^2}. \end{aligned}$$

(Yara Elias, 18.10.2016).

Section 13.13, pages 637 and 651: replace “unifom” by “uniform”, twice (Oded Regev, 07.11.2015).

Section 13.13, page 637, paragraph after Definition 13.123: replace L^* by L, twice (Oded Regev, 07.11.2015).

Section 13.13, page 647: replace “Zuckermann” by “Zuckerman”; also on pages 839 and 907 (Oded Regev, 07.11.2015).

Section 15.3, page 748: the term x^3 occurs in the product of a and b, but not modulo m:

$$\begin{aligned} a \cdot b &= x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^3 + x^2 + x + 1 \\ &= (x^6 + x^5 + x^3) \cdot m + x^4 + x^2 + x + 1 \text{ in } \mathbb{Z}_2[x], \end{aligned}$$

$$a \cdot b = x^4 + x^2 + x + 1 \text{ in } \mathbb{Z}_2[x]/(m).$$

(Alfredo Viola, 22.08.2016).

Sources of quotations for Chapter 11, pages 812–813: Albert Einstein, letter to Max Born dated 4 December 1926. The Albert Einstein Archives of the Hebrew University of Jerusalem hold a copy as their document AEA 8-180 (30.11.2015).

Sources of quotations for Chapter 11, page 813: John Edensor Littlewood, *A Mathematicians Miscellany*, Methuen & Co. Ltd., London, 1953, page 23. © 1953 Methuen & Co. Ltd. *The Mathematician's Art of Work*, © 1967 Rockefeller University Press. Revised edition first published in 1986 by Cambridge University Press, © 1986 B. Bollobás, reproduced with permission (30.11.2015).

Bibliography, page 822: replace the URL "http://www.ibbergmann.de/" by "http://www.ibbergmann.org/" (Ralph Wernsdorf, 21.03.2016).

Outside back cover: the color photograph is © 2015 Martin Apsel-von zur Gathen and reproduced with kind permission (30.11.2015).