Cryptography (SS2006) Prof. Michael Backes

Errata

Version: 07/16/2006 Saarland University

Chapter 1: Historical Ciphers

none.

Chapter 2: Stream Ciphers

none.

Chapter 3: Block Ciphers

- **Page 5, caption of Figure 3.5:**
  Old: For a binary string $x_0x_1x_2x_3x_4x_5x_6x_7$ the ...
  New: For a binary string $x_0x_1x_2x_3x_4x_5$ the ...
- **Page 5, caption of Figure 3.5:**
  Old: ...row x_0x_7 and column $x_1x_2x_3x_4x_5x_6$. This ...
  New: ...row x_0x_5 and column $x_1x_2x_3x_4$. This ...
- **Page 6, Figure 3.8:**
  Old: Input of PC-2 should be 56 bits instead of 28 bits (2 times)
  New: Output of PC-2 should be 48 bits instead of 28 bits (2 times)
- **Page 11, Line 2:**
  Old: ... thus computing $\mathsf{E}(K_1, \mathsf{E}(K_2, m))$. While ...
  New: ... thus computing $\mathsf{E}(K_2, \mathsf{E}(K_1, m))$. While ...
- **Page 11, Line 22:**
  Old: $\ldots := \mathsf{E}(K_1, \mathsf{D}(K_2, \mathsf{E}(K_3, m)))$.
  New: $\ldots := \mathsf{E}(K_3, \mathsf{D}(K_2, \mathsf{E}(K_1, m)))$.
- **Page 11, Line 24:**
  Old: $\mathsf{D}^{\mathsf{3DES}}((K_1, K_2, K_3), m) := \mathsf{D}(K_3, \mathsf{E}(K_2, \mathsf{D}(K_1, m)))$.
  New: $\mathsf{D}^{\mathsf{3DES}}((K_1, K_2, K_3), c) := \mathsf{D}(K_1, \mathsf{E}(K_2, \mathsf{D}(K_3, c)))$.

Chapter 4: PRPs, PRFs, Semantic Security

- **Page 2, Line 18:**
  Old: ... for all (sequences of) adversaries A.
  New: ... for all (sequences of) efficient adversaries A.
- **Page 4, Line 16:**
  Old: $|\mathsf{Pr}[Coll]| = \left|\frac{1}{|\mathcal{X}|} + \ldots + \frac{q-1}{|\mathcal{X}|}\right|$
  New: $|\mathsf{Pr}[Coll]| \leq \left|\frac{1}{|\mathcal{X}|} + \ldots + \frac{q-1}{|\mathcal{X}|}\right|$
- **Page 6, Line 7:**
  Old: ... Deterministic Counter Mode (detCTR
  New: ... Deterministic Counter Mode (detCTR)

- **Page 7, Figure 4.1, A's input:**
  Old: Cb'
  New: $c_{b'}$

- **Page 7, Line -5:**
  Old: ... equals $\frac{1}{2} + Adv^{\mathsf{CT-only}}[\mathsf{A}, \mathsf{E}]$, which ...
  New: ... equals $\frac{1}{2} + \frac{1}{2} \cdot Adv^{\mathsf{CT-only}}[\mathsf{A}, \mathsf{E}^{\mathsf{detCTR}}]$, which ...

- **Page 7, Line -1:**
  Old: $\ldots Adv^{\mathsf{CT-only}}[\mathsf{A}, \mathsf{E}]$
  New: $\ldots Adv^{\mathsf{CT-only}}[\mathsf{A}, \mathsf{E}^{\mathsf{detCTR}}]$.

- **Page 8, Line -6::**
  Old: $Adv^{\mathsf{CPA}}[\mathsf{A}, \mathsf{E}] := \left| \mathsf{Pr}\left[Exp_{\mathsf{A}}^{\mathsf{CPA}}(b) = 0\right] - \mathsf{Pr}\left[Exp_{\mathsf{A}}^{\mathsf{CPA}}(b) = 1\right] \right|.$
  New: $Adv^{\mathsf{CPA}}[\mathsf{A}, \mathsf{E}] := \left| \mathsf{Pr}\left[Exp_{\mathsf{A}}^{\mathsf{CPA}}(0) = 1\right] - \mathsf{Pr}\left[Exp_{\mathsf{A}}^{\mathsf{CPA}}(1) = 1\right] \right|.$

Chapter 5: MACs and Hash Functions

- **Page 9, Line 13:**
  Old: $\ldots H_{i+1} := \mathsf{F}(m_i, H_i)$ for $i = 2, \ldots, r$,
  New: $\ldots H_{i+1} := \mathsf{F}(m_i, H_i)$ for $i = 1, \ldots, r$,

Chapter 5*: Secure Channels and Key Management

none.

Chapter 6: Basic Number Theory Facts

- **Page 4, Line 4:**
  Old: $h_1 = g^{p+1}/4 \bmod p$ and $h_2 = -g^{p+1}/4 \bmod p$
  New: $h_1 = g^{p+1/4} \bmod p$ and $h_2 = -g^{p+1/4} \bmod p$

Chapter 7: Public-key Encryption, Diffie-Hellman, ElGamal

none.

Chapter 8: The Cramer-Shoup Encryption Scheme

- **Page 2, Line -7:**
  Old: ..., he would also know the ciphertext.
  New: ..., he would also know the plaintext.

- **In Figure 8.1:**
  Old: Adv. B
  New: Adv. $\mathsf{A}_{\mathsf{DDH}}$

- **In Figure 8.1:**
  Old: Adv. A
  New: Adv. A_{CS}

- **Page 6, Line 6:**
  Old: ... does not know r
  New: ... does not know y

- **In Figure 8.2:**
  Old: Adv. B
  New: Adv. $\mathsf{A}_{\mathsf{DDH}}$

- **Page 10, Line 9:**
  Old: ... and can therefore contain no new information ...
  New: ... and can therefore contain new information ...

Chapter 9: One-way Functions and the RSA Trapdoor Permutation

- **Page 3, Line 14:**
  Old: (DLog is an OWF)
  New: ($\mathsf{F}^{\mathsf{DLog}}$ is an OWF)

- **Page 5, Line 5:**
  Old: $\varphi(pq) = (p-1)(q-1)$
  New: $\varphi(pq) = \varphi(p)\varphi(q)$

Chapter 9: The RSA Trapdoor Permutation (cont'd)

- **Page 2, Line 3 and 4 (2 times):**
  Old: $\sqrt{n}$
  New: $\sqrt{N}$

- **Page 4, Line 15:**
  Old: $\mathsf{Gen}(k)$
  New: $\mathsf{Gen}(n)$

- **Page 4, Line 26:**
  Old: $\ldots \| R \| \ldots$
  New: $\ldots \| r \| \ldots$

Chapter 10: Digital Signature Schemes

- **Page 4, Line 5:**
  Old: $1 \leq j \leq 2$
  New: $0 \leq j \leq 1$

- **Page 4, Line -7:**
  Old: $r \leftarrow_{\mathcal{R}} \{1, \ldots, p-1\}$
  New: $r \leftarrow_{\mathcal{R}} \mathbb{Z}^*_{p-1}$

- **Page 5, Line 12:**
  Old: $t = \mathsf{DLog}_s g^a h^{-s}$
  New: $t = \mathsf{DLog}_s g^m h^{-s}$

- **Page 5, Line 13:**
  Old: $h^s s^t = g^a$
  New: $h^s s^t = g^m$

- **Page 5, Line 27:**
  Old: $\gcd(j, p-1)$
  New: $\gcd(j, p-1) = 1$

- **Page 9, Line -2:**
  Old: $\mathsf{Pr}[\mathsf{A} \text{ wins}] = \ldots$
  New: $\mathsf{Pr}[\mathsf{B} \text{ wins}] = \ldots$

Chapter 11: Certificates

none.

Chapter 12: Authentication Methods, SSL, and other Important Protocols

- **Page 1, Line -9:**
  Old: ... if an attackers gets ...
  New: ... if an attacker gets ...
- **Page 3, Line -2:**
  Old: $cert_S, g^y, \mathsf{E}(K, \mathsf{S}(sk_S, (g^x, g^y)))$
  New: $cert_B, g^y, \mathsf{E}(K, \mathsf{S}(sk_B, (g^x, g^y)))$
- **Page 6, Line 9:**
  Old: $z_2 = z_1^b \bmod p$
  New: $z_2 = g^b \bmod p$

Chapter 13: Commitment Schemes

none.

Chapter 14: Secret Sharing

none.

Chapter 15: Zero-Knowledge Proofs

none.