公開鍵暗号の数理 （共立出版） 正誤表

*

最終更新日: October 6, 2017

- 3 章 基礎理論, p40 下から 4 行目

  誤： $f(z) = y$

  正： $f_i(z) = y$

- 4 章 共通鍵暗号, p67 9 行目

  誤： アルゴリズム D

  正： アルゴリズム $\mathcal{D}$

- 5 章 公開鍵暗号の安全性, p82 16 行目

  誤： Bleichenbach の攻撃法

  正： Bleichenbacher の攻撃法

- 5 章 公開鍵暗号の安全性, p90 2 行目と p91 5 行目

  誤： 安全性である場合

  正： 安全である場合

- 5 章 公開鍵暗号の安全性, p90 下から 7 行目

  誤： 「上記の定式化において, もし攻撃者 $\mathcal{A}_2$ が出力した暗号文が c^* と一致している場合は復号せずに特別な記号 $\perp'$ を出力するものとする.」

  正： 削除. 代わりに p91 6 行目の文直後に「ただし, 攻撃者 $\mathcal{A}_2$ が出力した暗号文が c^* と一致している場合は復号せずに特別な記号 $\perp'$ を出力するものとする.」を追加.

- 5 章 公開鍵暗号の安全性, p97 下から 2 行目と 3 行目

  誤： c_1

  正： c_2

- 5 章 公開鍵暗号の安全性, p101 15 行目

  誤： (m_0, m_1, s) を出力

---

*

正： s' を出力

- 6 章 OAEP, p129 最終行

  誤： $(s_i, H(s_i)) \notin \mathsf{G\text{-}List}$

  正： $(s_i, H(s_i)) \notin \mathsf{H\text{-}List}$

- 6 章 Cramer-Shoup, p133 6 行目と p137 下から 11 行目

  誤： $\mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}_{\Pi,\mathcal{A}}$

  正： $\frac{1}{2}\mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}_{\Pi,\mathcal{A}}$

- 6 章 Cramer-Shoup, p133 13 行目

  誤： c_i

  正： C_i

- 6 章 Cramer-Shoup, p136 7 行目

  誤： $\Pr[F_5] - \Pr[F_4]|$

  正： $|\Pr[F_5] - \Pr[F_4]|$

- 6 章 ハイブリッド暗号の構成, p150 下から 5 行目

  誤： SKE

  正： DEM

- 6 章 ハイブリッド暗号の構成, p152 1 行目

  誤： $\Pr[r \leftarrow \mathcal{R}_{pk} | y = \mathsf{Enc}(pk, m; r)]$

  正： $\Pr[y = \mathsf{Enc}(pk, m; r) | r \leftarrow \mathcal{R}_{pk}]$

- 6 章 ハイブリッド暗号の構成, p152 6 行目

  誤： γ 一様性を持つ

  正： γ が negligible であるような γ 一様性を持つ

- 6 章 ハイブリッド暗号の構成， p154 5 行目

  誤： $(K'_{sym}, K'_{mac}) := \mathsf{KDF}(v')$ とする．

  正： $d' := a^{x_1 + v' y_1} \hat{a}^{x_2 + v' y_2}$ を計算し $(K'_{sym}, K'_{mac}) := \mathsf{KDF}(d')$ とする．

- 7 章 ディジタル署名, p160 1 行目

  誤： σ

  正： σ^*

- 7 章 ディジタル署名, p172 最終行

誤：「が得られる.」

正：削除.

- 8 章 IBE, p189 下から 9 行目

  誤：$c_1 \coloneqq H_2(v_0^r)$

  正：$c_1 \coloneqq s \oplus H_2(v_0^r)$

- 8 章 IBE, p190 最終行

  誤：$t := s \oplus H_3(v_0^s, c_0, c_1)$

  正：$t := s \oplus H_3(v_0^s, c, c_0, c_1)$

- 8 章 IBE, p191 5 行目

  誤：$s' := t \oplus H_3(k', c_0, c_1)$

  正：$s' := t \oplus H_3(k', c, c_0, c_1)$