☆「暗号技術　実践活用ガイド」用語の統一

「発生器」→「生成器」

頁	行
6	15
9	8
13	12
54	11
66	11
67	4
315	下から4
362	12
366	下から6

「暗号文単独攻撃者」→「単独暗号文攻撃者」

頁	行
11	18
36	7
363	12

「決定論的乱数生成器」→「決定論的ランダムビット生成器」

頁	行
11	下から5
39	15
55	8
122	14
364	5

「完全準同型暗号化」→「完全準同型暗号」

頁	行
12	3
14	下から6
43	下から8, 7
44	8
364	13

「フォーマット保持暗号化」「形式保持暗号化」→「フォーマット保持暗号」

頁	行
12	5
14	下から7
43	9, 15, 19
364	3

「多変量二次方程式」→「多変数多項式」

頁	行
12	下から7
356	15
365	21

「転置」→「置換」

頁	行
13	19
14	16
16	17
27	15, 16, 18, 19, 20, 25
28	5, 7, 8, 10, 12, 13, 15, 16, 17, 19, 21, 22, 26, 28, 29
29	2, 4, 12, 15, 16, 24
30	6, 8, 9, 10, 14, 17, 20, 21, 22, 23, 24, 26
83	20, 23, 30, 32
90	4
94	18
96	7, 12, 下から6
97	14
100	下から3, 2
106	3
144	5, 10, 下から6
153	下から4
175	下から9
205	14, 19, 24
224	（ページ左上）
363	下から3
365	下から4

「調整値付き暗号」「調整可能暗号化」→「調整可能暗号」

頁	行
13	下から8
14	下から4
44	14, 15, 下から5
120	下から9
365	下から9

「演算モード」→「暗号利用モード」

頁	行
14	17
16	下から7
27	15, 17
28	最終行
29	1, 12,
91	下から3
106	5, 下から3
107	1, 2, 4, 5, 10
108	（ページ左上）
110	（ページ左上）
112	（ページ左上）
114	（ページ左上）
175	下から3

195	4
223	3
363	22

「暗号化の安全性」→「暗号の安全性」

頁	行
14	23
33	1
259	下から4

「（非）対称暗号化」「（非）対称鍵暗号」「対称鍵暗号化」→「（非）対称暗号」

頁	行
14	下から10
24	2, 3
41	11, 12, 21, 23, 25
42	10
229	下から5
253	5, 6
365	3
366	21

「認証付き暗号化」「認証暗号」「認証された暗号」→「認証付き暗号」

頁	行
14	下から8
42	8, 9
43	1, 8
120	下から9
310	10
その他	カバー折り返し（表紙側）、裏表紙

「検索可能暗号化」→「検索可能暗号」

頁	行
14	下から5
44	5
364	7

「（第一/第二）原像困難性」→「（第一/第二）原像計算困難性」

頁	行
17	15
156	下から10
158	12, 13
159	1, 3, 4, 6, 下から5
160	7, 9, 下から2
161	6
167	13
174	下から8
183	18
364	8

365	2, 6

「衝突困難性」→「衝突計算困難性」

頁	行
17	16
156	下から10
158	12
160	14, 下から6, 2
161	6, 7
166	1, 2, 5, 6
172	下から4
174	下から7
183	18
365	4

「平方乗算」「平方乗算法」→「繰り返し自乗法」

頁	行
20	13
267	2, 18,
268	3, 24, 29
269	下から6
272	3
305	6

「決定論的ディフィー・ヘルマン」→「決定的ディフィー・ヘルマン」

頁	行
20	24
281	下から4
282	7, 11
364	4

「ランダムさ」→「ランダム性」

頁	行
21	19
315	11
345	下から6

「コード」→「符号」※全て統一ではない。訂正箇所のみ示す

頁	行
22	10
351	最終行
352	1
353	12, 16, 17, 19, 20
361	1

「多変量」→「多変数」

頁	行
22	下から8

252	6
353	12
356	1, 2
357	9, 11, 13
365	20

「公開鍵暗号化」「公開暗号化」→「公開鍵暗号」

頁	行
24	3
98	最終行
253	2, 6
262	14
364	11

「暗号家」→「暗号学者」

頁	行
27	11
34	下から4
35	8
37	下から3
42	4
43	下から7
46	下から4
59	下から3
107	下から8
124	7
164	7
282	20
347	3
359	10

「整合性」→「完全性」

頁	行
37	15
155	5
157	5
181	4
186	1, 10, 17, 21
206	下から4
213	15

「無作為暗号化」→「ランダム化暗号」

頁	行
38	19, 26
39	11
44	下から2
365	7

「疑似乱数ビット」→「疑似ランダムビット」

頁	行
54	19
86	9
122	16

「(非)暗号PRNG」→「(非)暗号的PRNG」

頁	行
60	下から3
61	8
70	6, 13, 下から4, 2
71	2
86	下から4
102	22

「複雑性理論(家)」「複雑性の理論(家)→「計算複雑性理論(家)」

頁	行
72	3
82	14, 下から3
232	4
234	4
235	下から9, 6
237	2, 4, 9
239	6
241	14, 下から4
252	8
347	3
348	13

「携帯電話○○」→「モバイル○○」

頁	行
79	下から4
137	4
141	下から2

「鍵合意プロトコル」→「鍵共有プロトコル」

頁	行
86	15
155	6

「チャンク」→「ブロック」

頁	行
96	15
109	10
121	4, 6
123	下から2
135	下から2
164	3

165	10
196	3, 8
201	下から3
206	17
215	2
325	最終行
326	2
354	2, 3

「（非）暗号学的（な）ハッシュ」→「（非）暗号的（な）ハッシュ」

頁	行
156	下から5, 4, 2
197	下から3
201	14
294	下から4

「Rhoメソッド」→「ρ法」

頁	行
162	12, 13
163	下から6
363	10

「安全性の目標」「安全性の目的」「安全性目標」→「安全性のゴール」

頁	行
197	最終行
285	7
286	1, 3
320	下から4

「固定時間」→「定数時間」

頁	行
204	下から5, 3
205	1
234	下から7