

CORRECTION

## Correction to: The replacement of irreducible polynomial and affine mapping for the construction of a strong S-box

Alamsyah  · Agus Bejo · Teguh Bharata Adji

Published online: 3 August 2018  
© Springer Nature B.V. 2018

**Correction to: Nonlinear Dyn**

<https://doi.org/10.1007/s11071-018-4310-2>

In the original publication of the article, Tables 4 and 7 were incorrectly published. The corrected tables are shown below (Tables 4, 7).

---

The original article can be found online at <https://doi.org/10.1007/s11071-018-4310-2>.

---

Alamsyah · A. Bejo · T. B. Adji (✉)  
Department of Electrical Engineering and Information  
Technology, Universitas Gadjah Mada, Yogyakarta,  
Indonesia  
e-mail: [adji@ugm.ac.id](mailto:adji@ugm.ac.id)

A. Bejo  
e-mail: [agusbj@ugm.ac.id](mailto:agusbj@ugm.ac.id)

Alamsyah  
Department of Computer Science, Universitas Negeri  
Semarang, Kota Semarang, Indonesia  
e-mail: [alamsyah.16@mail.ugm.ac.id](mailto:alamsyah.16@mail.ugm.ac.id);  
[alamsyah@mail.unnes.ac.id](mailto:alamsyah@mail.unnes.ac.id)

**Table 4** The proposed multiplicative inverse  $m_3$

0	1	177	222	233	74	111	140	197	165	37	193	134	84	70	231
211	93	227	133	163	52	209	237	67	166	42	99	35	158	194	119
216	45	159	28	192	10	243	171	224	181	26	98	217	33	199	189
144	86	83	234	21	162	128	121	160	91	79	229	97	73	138	205
108	154	167	24	254	124	14	230	96	61	5	232	200	130	228	58
112	106	235	50	13	135	49	145	221	246	161	57	210	17	239	191
72	60	43	27	152	213	117	151	187	184	81	113	64	155	141	6
80	107	156	142	150	102	195	31	129	55	149	178	69	255	215	136
54	120	77	201	226	19	12	85	127	214	62	204	7	110	115	157
48	87	175	248	179	122	116	103	100	212	65	109	114	143	29	34
56	90	53	20	196	9	25	66	183	172	242	39	169	182	249	146
223	2	123	148	225	41	173	168	105	186	185	104	198	47	238	95
36	11	30	118	164	8	188	46	76	131	219	253	139	63	250	245
236	22	92	16	153	101	137	126	32	44	252	202	247	88	3	176
40	180	132	18	78	59	71	15	75	4	51	82	208	23	190	94
241	240	170	38	251	207	89	220	147	174	206	244	218	203	68	125

**Table 7** The proposed S-box<sub>3</sub>

99	224	105	111	173	152	101	176	207	95	158	193	171	181	138	184
254	42	182	47	86	37	249	163	7	219	8	119	151	143	69	65
102	130	12	73	66	120	142	74	50	103	64	244	229	144	200	123
154	178	63	41	214	213	162	84	210	35	21	191	112	28	185	211
225	129	88	71	31	217	118	59	243	186	238	46	94	165	60	48
203	232	170	44	242	40	168	25	235	3	81	180	125	216	164	124
159	57	139	195	134	247	70	16	114	246	56	72	131	2	51	106
187	107	136	183	147	250	198	205	33	161	23	237	14	156	240	190
34	215	18	221	53	223	113	54	93	115	62	80	233	230	79	11
43	49	68	22	110	208	197	121	253	116	0	98	204	52	202	20
55	160	166	85	76	252	196	132	96	192	13	153	77	227	149	157
236	100	83	148	177	140	67	206	108	241	117	239	75	133	39	45
29	251	78	194	220	127	248	6	145	38	226	155	58	189	17	135
32	82	169	91	5	126	61	222	19	1	24	89	128	167	231	234
15	228	172	92	150	179	9	245	27	109	175	188	122	209	255	174
137	10	201	26	146	212	36	104	30	199	87	4	97	218	141	90