

This note presents example differential characteristics for the final round **G** of Fugue-256 (details of our analysis will appear in a subsequent paper). A state is displayed on two lines left-to-right from S_0 to S_{14} , and from S_{15} to S_{29} , in hexadecimal basis, replacing zeroes by dots for readability.

Figure 1 depicts a probability-1 differential characteristic for 4 $G1$ rounds followed by 11 $G2$ rounds, with the example difference **FFFFFFFF**.

Fig. 2 shows the characteristic when exploited for a distinguisher on the full 18-round **G**, with 00000001 as difference.

Fig. 3 shows how differences propagate on more than 18 rounds of **G** (adding $G2$ rounds).

Initial difference	
	FFFFFFFF
G1 rounds	
1	FFFFFFFF
2	FFFFFFFF
3	FFFFFFFF
4	FFFFFFFF
G2 rounds	
5	FFFFFFFF
6	FFFFFFFF
7	FFFFFFFF
8	FFFFFFFF
9	FFFFFFFF
10	FFFFFFFF
11	FFFFFFFF
12	FFFFFFFF
13	FFFFFFFF
14	FFFFFFFF
15	FFFFFFFF

Fig. 1. Evolution of differences given an initial difference **FFFFFFFF** in S_5 , with 4 $G1$ rounds and 11 $G2$ rounds.

Initial difference	
34B58.44.....1.....1.....B7F6198A822E7BB45.6C2C59
G1 rounds	
11.....
21.....
31.....
41.....
51.....
G2 rounds	
61.....
71.....
81.....
91.....
101.....
111.....
121.....
131.....
141.....
151.....
161.....
17	4.....C132.....DBB1.....1B..5A.....7C....1F ..5D..1F....1F5D.....637C....1F.....
18	2F95B95F16D98A895AC3F531F9DD.B47.....7C....1FF498B.8D 61C1F2589D4E5A72CB55ABCBF498B.8D.....4.....C1

Fig. 2. Evolution of differences with a difference 00000001 in the 15 intermediate rounds, and a state S set to zero before the 17th round.

G2 rounds (continued)	
18	2F95B95F16D98A895AC3F531F9DD.B47.....7C....1FF498B.8D 61C1F2589D4E5A72CB55ABCBF498B.8D.....4.....C1 .C.765.A.CBC24976.7BC6FFFE6A968A1.....7C....1FF498B.8D352B.A8D
19	DC5139C5689E98EBB92F1FEC352B.A8D.....4.....C12F95B95F 38.354D8D19CAD1ADD3C21C8E8623.1F.....7C....1FF498B.8D352B.A8DBCAFE2.2 8FF6CD4DA2.B8.6DB6C.D8DDBCAFE2.2.....4.....C12F95B95F.C.765.A A6B5FF.87BE5E7.73219688B7FFC6C3A.....7C....1FF498B.8D352B.A8DBCAFE2.2CAF8A797
20	7163.6E1BE669A322DA32653CAF8A797.....4.....C12F95B95F.C.765.A38.354D8 DAC69612873CEFA23.A839349B849765.....7C....1F F498B.8D352B.A8DBCAFE2.2CAF8A7972ECBE532
21	AD64ED4681F9.BE7E5D181CB2ECBE532.....4.....C12F95B95F.C.765.A38.354D8A6B5FF.8 9F2848C91D1466FFD89A93E9AECC9C9D.....7C....1FF498B.8D 352B.A8DBCAFE2.2CAF8A7972ECBE532929EA61D
22	B517.1EDF8E2E84.C937.923929EA61D.....4.....C1 2F95B95F.C.765.A38.354D8A6B5FF.8DAC69612 DF1D915133ED562FB15FFD41CB82D8F9.....7C....1FF498B.8D352B.A8D BCAFE2.2CAF8A7972ECBE532929EA61D8.83AE13
23	42A417718.2A2D.84E4479DB8.83AE13.....4.....C12F95B95F .C.765.A38.354D8A6B5FF.8DAC696129F2848C9 5A1AB2BD3981696DD42511FDD7B8613.....7C....1FF498B.8D352B.A8DBCAFE2.2 CAF8A7972ECBE532929EA61D8.83AE13.8C394B1
24	44.7DF3CAB9812A38E359E12.8C394B1.....4.....C12F95B95F.C.765.A 38.354D8A6B5FF.8DAC696129F2848C9DF1D9151 771D7EAFCE558D.1C3567BEC.F.74A8.....7C....1FF498B.8D352B.A8DBCAFE2.2CAF8A797 2ECBE532929EA61D8.83AE13.8C394B154861.AD
25	7B6CC2ED714A24192B78B97.54861.AD.....4.....C12F95B95F.C.765.A38.354D8 A6B5FF.8DAC696129F2848C9DF1D91515A1AB2BD C77B181EE7F4993216D794954D1B27F47C....1F F498B.8D352B.A8DBCAFE2.2CAF8A7972ECBE532 929EA61D8.83AE13.8C394B154861.ADD98FDF4D
26	C77.A9DB435.66B121.C9F.FD98FDF4D.....4.....C12F95B95F.C.765.A38.354D8A6B5FF.8 DAC696129F2848C9DF1D91515A1AB2BD771D7EAF 82CE.FDF196643374BBA5F1B35531D45F498B.8D 352B.A8DBCAFE2.2CAF8A7972ECBE532929EA61D 8.83AE13.8C394B154861.ADD98FDF4D5278FF5
27	9AB3D4ACAFAAB5516.AAA.FD5278FF54.....C1 2F95B95F.C.765.A38.354D8A6B5FF.8DAC69612 9F2848C9DF1D91515A1AB2BD771D7EAF77B181E 3.8BF5E769A899578CFD54.B7B6B291.352B.A8D BCAFE2.2CAF8A7972ECBE532929EA61D8.83AE13 .8C394B154861.ADD98FDF4D5278FF562C2219.
28	41B76EB77F6844A.4E646AF122C221512F95B95F .C.765.A38.354D8A6B5FF.8DAC696129F2848C9 DF1D91515A1AB2BD771D7EAF77B181E82CE.FDF A945EE54.498731E6ABB5E9B6655A7A9BCAFE2.2 CAF8A7972ECBE532929EA61D8.83AE13.8C394B1 54861.ADD98FDF4D5278FF562C2219.9CE49.1E
29	84D7A943BCA7F33BA62A84E2B3712941.C.765.A 38.354D8A6B5FF.8DAC696129F2848C9DF1D9151 5A1AB2BD771D7EAF77B181E82CE.FDF3.8BF5E7
30	

Fig. 3. Evolution of differences with a difference 00000001 in the 15 intermediate rounds, and a state S set to zero before the 17th round (continued from Fig. 2). The final differences in S_4 and in S_{19} are unaffected by modification in the state entering the 17th rounds that map backwards to sparse differences.