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 FFFFFFF.

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).

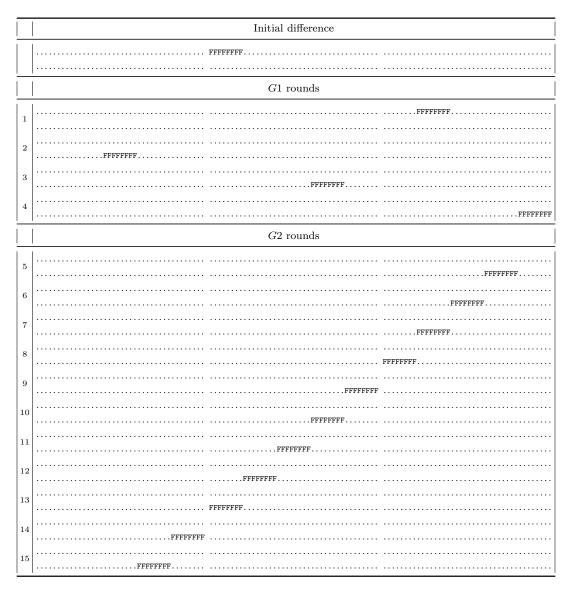


Fig. 1. Evolution of differences given an initial difference FFFFFFFF in S_5 , with 4 G1 rounds and 11 G2 rounds.

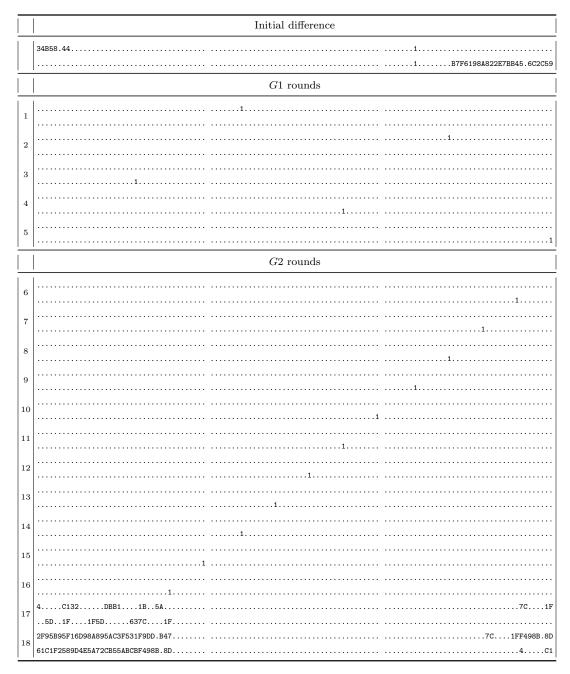


Fig. 2. Evolution of differences with a difference 00000001 in the 15 intermediate rounds, and a state S set to zero before the 17th round.

	G2 rounds (continued)
	2F95B95F16D98A895AC3F531F9DD.B47
18	61C1F2589D4E5A72CB55ABCBF498B.8D
	.C.765.A.CBC24976.7BC6FFE6A968A1
19	DC5139C5689E98EBB92F1FEC352B.A8D
	38.354D8D19CAD1ADD3C21C8E8623.1F
20	8FF6CD4DA2.B8.6DB6C.D8DDBCAFE2.2
	A6B5FF.87BE5E7.73219688B7FFC6C3A
21	7163.6E1BE669A322DA32653CAF8A797
	DAC69612873CEFA23.A839349B849765
22	AD64ED4681F9.BE7E5D181CB2ECBE532
	9F2848C91D1466FFD89A93E9AECC9C9D
23	B517.1EDF8E2E84.C937.923929EA61D
24	DF1D915133ED562FB15FFD41CB82D8F9
24	42A417718.2A2D.84E4479DB8.83AE13
25	5A1AB2BD39816966DD42511FDD7B8613
25	44.7DF3CAB9812A38E359E12.8C394B1
26	771D7EAFCE558D.1C3567BEC.F74A8 7C1FF498B.8D352B.A8DBCAFE2.2CAF8A797 2ECBE532929EA61D8.83AE13.8C394B154861.AD
26	7B6CC2ED714A24192B78B97.54861.AD
27	${\tt C77B181EE7F4993216D794954D1B27F47C1F\ F498B.8D352B.A8DBCAFE2.2CAF8A7972ECBE532\ 929EA61D8.83AE13.8C394B154861.ADD98FDF4D82B12B12B12B12B12B12B12B12B12B12B12B12B12$
21	${\tt C77.A9DB435.66B121.C9F.FD98FDF4D.} \\ 4 \\ {\tt C12F95B95F.C.765.A38.354D8A6B5FF.8} \\ {\tt DAC696129F2848C9DF1D91515A1AB2BD771D7EAF364B5B1296B129F2848C9DF1D91515A1AB2BD771D7EAF36B129F2848C9DF1D91515A1AB2BD771D7EAF36B129F2848C9DF1D91515A1AB2BD771D7EAF36B129F2848C9DF1D91515A1AB2BD771D7EAF36B129F2848C9DF1D91515A1AB2BD771D7EAF36B129F2848C9DF1D91515A1AB2BD771D7EAF36B129F2848C9DF1D91515A1AB2BD771D7EAF36B129F2848C9DF1D91515A1AB2BD771D7EAF36B129F2848C9DF1D91515A1AB2BD771D7EAF36B129F2848C9DF1D91515A1AB2BD771D7EAF36B129F2848C9DF1D91515A1AB2BD771D7EAF36B129F2848C9DF1D91515A1AB2BD771D7EAF36B129F2848C9DF1D91515A1AB2BD771D7EAF36B129F2848C9DF1D91515A1AB2BD771D7EAF36B129F2848C9DF1D91515A1AB2BD771D7EAF36B129F2848C9DF1D91515A1AB2BD771D7EAF36B129F2848C9DF1D91515A1AB2BD771D7EAF36B129F2848C9DF1D91515A1AB2BD771D7EAF36B129F284F284B129F284F284F284F284F284F284F284F284F284F284$
28	82CE.FDF196643374BBA5F1B35531D45F498B.8D 352B.A8DBCAFE2.2CAF8A7972ECBE532929EA61D 8.83AE13.8C394B154861.ADD98FDF4DD5278FF5
20	9AB3D4ACAAFABB5516.AAA.FD5278FF54C1 2F95B95F.C.765.A38.354D8A6B5FF.8DAC69612 9F2848C9DF1D91515A1AB2BD771D7EAFC77B181E
29	$3.8BF5E769A899578CFD54.B7B6B291.352B.A8D\ BCAFE2.2CAF8A7972ECBE532929EA61D8.83AE13\ .8C394B154861.ADD98FDF4DD5278FF562C2219.BF562C22219.BF562C2219.BF562$
29	$41B76EB77F6844A.4E646AF122C221512F95B95F .C.765.A38.354D8A6B5FF.8DAC696129F2848C9 \ DF1D91515A1AB2BD771D7EAFC77B181E82CE.FDF12B12B12B12B12B12B12B12B12B12B12B12B12B1$
30	A945EE54.498731E6ABB5E9B6655A7A9BCAFE2.2 CAF8A7972ECBE532929EA61D8.83AE13.8C394B1 54861.ADD98FDF4DD5278FF562C2219.9CE49.1E
	84D7A943BCA7F33BA62A84E2B3712941.C.765.A 38.354D8A6B5FF.8DAC696129F2848C9DF1D9151 5A1AB2BD771D7EAFC77B181E82CE.FDF3.8BF5E7

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.