Μετρήσεις

Kintex-7 (xc7k70tfbv676-2)

Αρχιτεκτονική basic

Sbox (d1)

	U=1	U=2	U=3	U=6
Period	2.85 ns	5.15 ns	7.55 ns	14.8 ns
Frequency	350.877 MHz	194.174 MHz	132.450 MHz	67.568 MHz
slices	468	629	768	1298
LUTs	1239	1611	2063	3403
FFs	1145	1462	1784	2743
TP	3742.68	4142.37	4238.4	4324.352
TP(hash)	362.196	400.875	410.168	418.486
TP/A(slice)	3.49	2.571	2.054	1.271
TP/A(sliceh)	0.77392	0.63732	0.534073	0.32241

Alt_Sbox (d2)

	U=1	U=2	U=3	U=6
Period	2.1 ns	3.45 ns	5.38 ns	10.5 ns
Frequency	476.19 MHz	289.855 MHz	185.874 MHz	95.238 MHz
slices	366	513	642	1093
LUTs	1252	1834	2341	3883
FFs	827	824	826	825
TP	4637.65	6183.57	5947.96	6095.23
TP(hash)	469.208	598.410	575.609	589.861
TP/A(slice)	3.70	3.37	2.54	1.569
TP/A(slice)h	1.28990	1.16649	0.89659	0.53967

Αρχιτεκτονική pipeline

Sbox (d1)

	U=1	U=2	U=3	U=6
Period	4.1 ns	6.7 ns	9.3 ns	16.5 ns
Frequency	243.902 MHz	149.254 MHz	107.527 MHz	60.606 MHz
slices	1459	2039	2698	4455
LUTs	4518	6173	8042	13392
FFs	3610	4908	6167	10009
TP	2601.62	1592.043	1720.432	1939.392
TP(hash)	325.203	398.011	430.108	484.848
TP/A(slice)	0.575	0.78079	0.63767	0.43533
TP/A(slice)h	0.22289	0.19520	0.15942	0.10883

Alt_sbox (d2)

	U=1	U=2	U=3	U=6
Period	3.3 ns	5.1 ns	6.5 ns	13.5 ns
Frequency	303.030 MHz	196.078 MHz	153.846 MHz	74.074 MHz
slices	1338	1731	2460	3323
LUTs	4518	6104	9145	12346
FFs	2324	2333	2336	2339
TP	1616.16	2091.499	2461.536	2370.368
TP(hash)	404.04	522.875	615.384	592.592
TP/A(slice)	1.20789	1.20826	1.00062	0.71332
TP/A(slice)h	0.30197	0.30206	0.25016	0.17833

Artix-7 (xc7a75tftg256-2)

Αρχιτεκτονική basic

Sbox (d1)

	U=1	U=2	U=3	U=6
Period	4.2 ns	7.2 ns	10.5 ns	21.3 ns
Frequency	238.095 MHz	138.889 MHz	95.238 MHz	46.948 MHz
slices	477	630	796	1216
LUTs	1194	1602	2059	3349
FFs	1144	1462	1784	2743
TP	2539.68	2962.96	3047.616	3004.672
TP(hash)	245.775	286.739	294.931	290.775
TP/A(slice)	2.127	1.85	1.48	0.9
TP/A(slice)h	0.51525	0.45514	0.37052	0.23912

Alt_Sbox (d2)

	U=1	U=2	U=3	U=6
Period	3.2 ns	5.5 ns	8.8 ns	17 ns
Frequency	312.5 MHz	181.818 MHz	113.636 MHz	58.824 MHz
slices	396	504	611	913
LUTs	1252	1711	1911	3073
FFs	826	824	826	825
TP	3333.33	3878.784	3636.352	3764.736
TP(hash)	322.581	375.366	351.905	364.329
TP/A(slice)	2.67	2.27	1.90	1.22
TP/A(slice)h	0.81460	0.74477	0.57595	0.39905

Αρχιτεκτονική pipeline

Sbox (d1)

	U=1	U=2	U=3	U=6
Period	5.5 ns	9.5 ns	14 ns	24.2 ns
Frequency	181.818 MHz	105.263 MHz	71.423 MHz	41.322 MHz
slices	1482	2081	2684	4460
LUTs	4530	6181	7977	13366
FFs	3610	4884	6167	10009
TP	969.696	1122.805	1142.768	1322.304
TP(hash)	242.424	280.701	285.692	330.576
TP/A(slice)	0.65432	0.53955	0.42577	0.29648
TP/A(slice)h	0.16301	0.13489	0.10644	0.07412

Alt_sbox (d2)

	U=1	U=2	U=3	U=6
Period	5 ns	7.6 ns	10.5 ns	19.35 ns
Frequency	200 MHz	131.579 MHz	95.238 MHz	51.680 MHz
slices	1339	1783	2112	3399
LUTs	4228	5871	7481	12361
FFs	2324	2333	2336	2339
TP	1066.667	1403.509	1523.808	1653.76
TP(hash)	266.667	350.877	380.952	413.44
TP/A(slice)	0.79661	0.78716	0.72150	0.48654
TP/A(slice)h	0.19915	0.19679	0.18037	0.12164

Spartan-7 (xc7s75fgga676-2)

Αρχιτεκτονική basic

Sbox (d1)

	U=1	U=2	U=3	U=6
Period	4.3 ns	7.3 ns	10.85	21.5 ns
Frequency	232.558 MHz	136.986 MHz	92.166 MHz	46.512 MHz
slices	468	593	769	1264
LUTs	1179	1611	2060	3351
FFs	1144	1462	1784	2743
TP	2480.619	2922.368	2949.312	2976.768
TP(hash)	240.060	282.810	285.418	288.074
TP/A(slice)	2.1	1.81	1.43	0.89
TP/A(slice)h	0.51295	0.47691	0.37115	0.22791

Alt_Sbox (d2)

	U=1	U=2	U=3	U=6
Period	3.1 ns	5.4 ns	7.5 ns	17.1 ns
Frequency	322.581 MHz	185.185 MHz	133.333 MHz	58.480 MHz
slices	374	508	659	936
LUTs	1254	1747	2328	3072
FFs	826	824	826	825
TP	3440.864	3950.61	4266.656	3742.72
TP(hash)	332.987	382.317	412.902	362.199
TP/A(slice)	2.74	2.26	1.83	1.22
TP/A(slice)h	0.89034	0.75259	0.62656	0.38696

Αρχιτεκτονική pipeline

Sbox (d1)

	U=1	U=2	U=3	U=6
Period	5.6 ns	9.4 ns	13 ns	24 ns
Frequency	178.571 MHz	106.383 MHz	76.923 MHz	41.667 MHz
slices	1479	2033	2787	4498
LUTs	4529	6169	8015	13370
FFs	3632	4884	6167	10009
TP	952.379	1134.752	1230.768	1333.344
TP(hash)	238.095	283.688	307.692	333.336
TP/A(slice)	0.64393	0.55817	0.44161	0.29643
TP/A(slice)h	0.16098	0.13954	0.11040	0.07411

Alt_sbox (d2)

	U=1	U=2	U=3	U=6
Period	5.2 ns	8 ns	10.8 ns	19.8 ns
Frequency	192.308 MHz	125 MHz	92.593 MHz	50.505 MHz
slices	1355	1725	2135	3368
LUTs	4228	5802	7447	12358
FFs	2324	2333	2336	2339
TP	1025.643	1333.333	1481.488	1616.16
TP(hash)	256.411	333.333	370.372	404.04
TP/A(slice)	0.75693	0.77295	0.69390	0.47986
TP/A(slice)h	0.18923	0.19324	0.17348	0.11996

Συγκριση

Ascon-128 on Spartan				
Έκδοση	**Μέγιστη Συχνότητα (MHz)**	**Επιφάνεια (LUT)**	**Throughput (Mbps)**	**T/A (Mbps/LUT)**
U=1	322.58 vs 206.26	1254 vs 2060	645.16 vs 315.2	0.51 vs 0.15
U=2	185.18 vs 147.23	1747 vs 2720	740.74 vs 392.61	0.42 vs 0.14
U=3	133.33 vs 126.08	2328 vs 3630	800 vs 448.25	0.34 vs 0.13
U=6	58.48 vs -	3353 vs 22630	701.76 vs 688.83	0.21 vs 0.03