A hardware evaluation of π-Cipher

FPGA Results (by Mohamed El Haddedy)

Table 1: FPGA results for all variants of π-Cipher (Spartan-6 (xc6slx16csg324-3))

	Area(Slices)	Max. Freq (MHz)	Number of Cycles	Throughput (Mbps)	Throughput/Area (Kbps/slices)
16-bit Encryption	1298	125	1753	9.13	7.20
16-bit Decryption	1259	126	1782	9.05	7.36
16-bit Encrypt/Decrypt	1345	170	1782	12.21	9.30
32-bit Encryption	2036	155	1753	22.64	11.38
32-bit Decryption	2120	150	1782	21.56	10.41
32-bit Encrypt/Decrypt	2138	145	1782	20.83	9.98
64-bit Encryption	Oversize of the platform		1753	NA	
64-bit Decryption			1782		
64-bit Encrypt/Decrypt			1782		

From Number of slices (we can get the following number of used LUT, FF, and unused (FF, LUT)

	LUT Flip-flop pairs used	Number of unused LUT-FF pairs	Number of unused LUT	Number of fully used LUT-FF pairs
16-bit Encryption	4449	1721 out of 4449	399 out of 4449	2329 out of 4449
16-bit Decryption	4383	1700 out of 4383	430 out of 4383	2253 out of 4383
16-bit Encrypt/Decrypt	4527	1793 out of 4527	405 out of 4527	2329 out of 4527
32-bit Encryption	7523	2302 out of 7523	461 out of 7523	4760 out of 7523
32-bit Decryption	7643	2399 out of 7643	650 out of 7643	4594 out of 7643
32-bit Encrypt/Decrypt	7642	2,416 out of 7642	537 out of 7642	4689 out of 7642
64-bit Encryption	NA			
64-bit Decryption				
64-bit Encrypt/Decrypt				

Table 2: FPGA results of π-function on (Spartan-6 (xc6slx16csg324-3))

	Area(slices)	Max.Freq (MHz)	Number of Cycles	Throughput (Mbps)	Throughput/Area (Kbps/slices)
16-bit	685	130	192	173.33	259.11
32-bit	856	185	192	246.67	295.08
64-bit	Number of IOB are limited compare to the design		192	Number of IOB are limited compare to the design	

From Number of Slices (we can get the following number of used LUT, FF, and unused (FF, LUT)

	LUT Flip-Flop pairs used	Number of unused LUT-FF pairs	Number of unused LUT	Number of fully used LUT-FF pairs
16-bit	2449	808 out of 2449	127 out of 2449	1514 out of 2449
32-bit	4787	1542 out of 4787	288 out of 4787	2957 out of 4787
64-bit	Number of IOB are limited compare to the design			

Table 3: FPGA results of ARX operation on (Spartan-6 (xc6slx16csg324-3))

	Area(slices)	Max.Freq (MHz)	Number of Cycles	Throughput (Mbps)	Throughput/Area (Kbps/slices)
16-bit	220	190	5	4864	22638
32-bit	Number of IOB are limited compare to the design		5	Number of IOB are limited compare to the design	
64-bit			5		

From Number of Slices (we can get the following number of used LUT, FF, and unused (FF, LUT)

	LUT Flip-Flop pairs used	Number of unused LUT-FF pairs	Number of unused LUT	Number of fully used LUT-FF pairs
16-bit	771	245 out of 771	84 out of 771	442 out of 771
32-bit	Number of IOB are limited compare to the design			
64-bit				

Table 4: FPGA results for all variants of π-Cipher (VC707 (XC7VX485t-2FFG1761) and ISE14.7)

	Area(Slices)	Max. Freq (MHz)	Number of Cycles	Throughput (Mbps)	Throughput/Area (Kbps/slices)
16-bit Encryption	1307	362	1753	26.43	20.71
16-bit Decryption	1399	278	1782	20.00	14.64
16-bit Encrypt/Decrypt	1192	308	1782	22.12	19.00
32-bit Encryption	2307	227	1753	33.15	14.71
32-bit Decryption	2308	245	1782	35.20	15.62
32-bit Encrypt/Decrypt	2352	231	1782	33.19	14.45
64-bit Encryption	4204	201	1753	58.71	14.30
64-bit Decryption	4039	187	1782	53.73	13.62
64-bit Encrypt/Decrypt	4221	201	1782	57.75	14.01

From Number of slices (we can get the following number of used LUT, FF, and unused (FF, LUT)

	LUT Flip-flop pairs used	Number of unused LUT-FF pairs	Number of unused LUT	Number of fully used LUT-FF pairs
16-bit Encryption	4460	1753 out of 4460	511 out of 4460	2196 out of 4460
16-bit Decryption	4449	1763 out of 4449	507 out of 4449	2179 out of 4449
16-bit Encrypt/Decrypt	4295	1664 out of 4295	281 out of 4295	2350 out of 4295
32-bit Encryption	7984	2696 out of 7984	1103 out of 7984	4185 out of 7984
32-bit Decryption	7979	2711 out of 7979	1087 out of 7979	4181 out of 7979
32-bit Encrypt/Decrypt	7994	2733 out of 7994	1096 out of 7994	4165 out of 7994
64-bit Encryption	14983	4675 out of 14983	1971 out of 14983	8337 out of 14983
64-bit Decryption	14727	4357 out of 14727	1782 out of 14727	8588 out of 14727
64-bit Encrypt/Decrypt	15015	4652 out of 15015	2137 out of 15015	8226 out of 15015

Table 5: FPGA results of π-function (VC707 (XC7VX485t-2FFG1761) and ISE14.7)

	Area(Slices)	Max. Freq (MHz)	Number of Cycles	Throughput (Mbps)	Throughput/Area (Kbps/slices)
16-bit	646	395	192	527	835.37
32-bit	1246	332	192	885	727.32
64-bit	2411	298	192	1589	675.30

From Number of slices (we can get the following number of used LUT, FF, and unused (FF, LUT)

	LUT Flip-flop pairs used	Number of unused LUT-FF pairs	Number of unused LUT	Number of fully used LUT-FF pairs
16-bit	2356	725 out of 2356	121 out of 2356	1510 out of 2356
32-bit	4657	1396 out of 4657	237 out of 4657	3024 out of 4657
64-bit	9049	2625 out of 9049	387 out of 9049	6037 out of 9049

Table 6: FPGA results of ARX operation (VC707 (XC7VX485t-2FFG1761) and ISE14.7)

	Area(Slices)	Max. Freq (MHz)	Number of Cycles	Throughput (Mbps)	Throughput/Area (Kbps/slices)
16-bit	357	417	5	10675.2	30620.18
32-bit	754	338	5	17305.6	23502.57
64-bit	1300	324	5	33177.6	26133.74

From Number of slices (we can get the following number of used LUT, FF, and unused (FF, LUT)

	LUT Flip-flop pairs used	Number of unused LUT-FF pairs	Number of unused LUT	Number of fully used LUT-FF pairs
16-bit	981	446 Out of 981	2 out of 981	533 out of 981
32-bit	1969	896 Out of 1969	2 out of 1969	1071 out of 1969
64-bit	3759	1791 Out of 3759	2 out of 3759	1966 out of 3759

Throughput = no.bits * Max.Freq /no.cycles

Picipher 16-bit version: key length is 96 bits, message block length is 128 bits
Picipher 32-bit version: key length is 128 bits, message block length is 256 bits
Picipher 64-bit version: key length is 256 bits, message block length is 512 bit

Notes: these processors are small, they occupied around 1% of the total capacity of the FPGA. If we are targeting high speed we can repeat these processor as many as we want and the throughput will be increased by the factor of number of processors (n)

Throughput = n * one processor throughput
Area = n * one processor area
The ratio between them is fixed.

ASIC Results (by Mohamed El Haddedy and Xinfei Guo)

Table 7: ASIC results for all variants of π-Cipher (28/32nm technology)

	Area (um^2)	Estimated Gate Count (K)	Max. Freq. (GHz)	# of cycles	Power (mW)	Throughput (Mbps)	Throughput/Area ($Kbps/um^2$)
16-bit Encryption	61790.639056	22.1	1.35	1753	13.2	98.57387336	1.595288135
16-bit Decryption	61415.602764	21.97	1.33	1782	13.2	95.53310887	1.555518542
16-bit Encryption/ Decryption	61416.317661	21.97	1.33	1782	13.0	95.53310887	1.555500435
32-bit Encryption	118240.263083	42.3	1.35	1753	26.3	197.1477467	1.667348681
32-bit Decryption	117617.137101	42.07	1.33	1782	25.7	191.0662177	1.624476011
32-bit Encryption/ Decryption	117617.851997	42.07	1.33	1782	25.7	191.0662177	1.624466137
64-bit Encryption	233609.105908	83.56	1.30	1753	50.0	379.6919566	1.625330293
64-bit Decryption	235077.497797	84.09	1.30	1782	49.5	373.5129068	1.588892643
64-bit Encryption/ Decryption	235078.212694	84.09	1.30	1782	49.5	373.5129068	1.588887811

Table 8: ASIC results of π-function (28/32nm technology)

	Area (um^2)	Estimated Gate Count (K)	Max. Frequency (GHz)	# of cycles	Power (mW)	Throughput (Mbps)	Throughput/Area ($Kbps/um^2$)
16-bit	70670.269512	25.28	0.9	192	7.836	1200	16.98026636
32-bit	149886.289943	53.62	0.83	192	14.6	2213.333333	14.76674974
64-bit	302800.943439	108.31	0.74	192	26.5	3946.666667	13.03386516

Table 9: ASIC results of ARX operation (28/32nm technology)

	Area (um^2)	Estimated Gate Count	Max. Frequency (GHz)	# of cycles	Power (mW)	Throughput (Mbps)	Throughput/Area ($Kbps/um^2$)
16-bit	27284.780654	9.76	1.0	5	0.693	25600	938.2519993
32-bit	54209.047626	19.39	0.77	5	1.095	39424	727.2586722
64-bit	111306.972957	39.81	0.74	5	2.11	75776	680.7839436