Appendix A

Tests results

Avalanche property for 128-bit hash functions after 5000 ρ-iterations

hash function	average	variance	min	max
MD5	63.999195	4127.919100	36	96
EdonC 128-bit	63.998888	4127.829649	36	92
EdonR 128-bit	63.994578	4127.342406	33	92

Avalanche property for 160-bit hash functions after 5000 ρ-iterations

hash function	average	variance	min	max
SHA-1	80.000848	6440.133338	50	110
EdonC 160-bit	80.000309	6440.066016	49	110
EdonR 160-bit	79.992679	6438.845868	51	111

Number of iterations before reaching partial collisions for 128-bit hash functions

bits	90	91	92	93	94	95	96
MD5	181921		274830	45 101 984	79 514 544		81 343 278
EdonC 128-bit		262813	1570617			4 883 355	
EdonR 128-bit	465883		677348			7 515 481	

Number of iterations before reaching partial collisions for 128-bit hash functions

bits	107	109	110	111	112	113	118
SHA-1		82432	383354	1 449 009	2 259 464	13 135 456	14 044 770
EdonC 160-bit		105209	204901	1 391 314		2 143 924	
EdonR 160-bit	62171			372542		3 432 190	

Maurer's uniformity test

MD5	15.167458
EdonC 128-bit	15.167506
EdonR 128-bit	15.167343
SHA-1	15.167256
EdonC 160-bit	15.167243
EdonR 160-bit	15.167153
expectation for uniform distribution	15.167379

Möbius statistical analysis of 128-bit hash functions

hash function	$T_1^1D^2$	$T_1^2D^2$	$T_1^3D^2$	$T_2^1D^2$	$T_2^2D^2$	$T_2^3D^2$
MD5	62.601563	68.744053	67.498870	1.654167	2.466667	0.554167
EdonC 128-bit	60.093750	53.710632	73.149739	3.000000	2.154167	4.554167
EdonR 128-bit	55.128906	67.455051	55.935845	2.616667	2.887500	3.320833
0.05	154.301516			5.991465		
0.01	166.987390			9.210340		
0.001	181.993045			13.815511		
significance α	χ^2_{127} distribution			χ^2_2 distribution		

Möbius statistical analysis of 128-bit hash functions

hash function	$T_1^1D^2$	$T_1^2D^2$	$T_1^3D^2$	$T_2^1D^2$	$T_2^2D^2$	$T_2^3D^2$
SHA1	76.878906	70.897581	89.457610	0.256667	0.426667	2.016667
EdonC 160-bit	85.480469	75.221685	81.467442	0.443333	1.560000	3.693333
EdonR 160-bit	102.281250	77.200511	90.228846	2.016667	3.266667	4.843333
0.05	189.424220			5.991465		
0.01	203.399752			9.210340		
0.001	219.846046			13.815511		
confidence α	χ^2_{159} distribution			χ^2_2 distribution		