



## Secrets of the HDX6144 Encryption Algorithm

### Paper 4: The FUSION sub-routine

Dr William McMullen Hawthorne

Paper 2 in this series explained the relationship between the 24576-bit Master Key and the 6144-bit Session Key of the HDX6144 Encryption Algorithm. Paper 3 demonstrated that the 24576-bit Master Key has no redundancies. The aim of this Paper is to demonstrate the FUSION SUB-ROUTINE. This sub-routine, together with the Carousel Random Generator, which creates the Master Key in the first place, and the general method of divorcing encryption speed from key strength, are the three “inventions” which have made HDX6144 the strongest combination of strength and speed ever presented to the world market.

The use of a salt to refresh a session key is not new, but what distinguishes the FUSION SUB-ROUTINE is that it refreshes the Master Key. This means that the massive strength of the 24576-bit Master Key which, as it stands, is impossible to attack in real time by an exhaustive search, is, to all intents and purposes, a new key every time it is used.

In order to provide a numerical example, we return to the AliceBob Master Key, first introduced in Paper 2, which, when displayed in full, consists of 6144 Hex numbers and occupies two A4 pages! The following data displays the beginning and end of the AliceBob Master Key and the effect of “fusing” it with a salt:

Salt: D12C6E62A06668FE

Master Key:

B00C99AACEB04EDF314C5245F43AA9C1C1D321829A22AC855F14464A202B65CB2E980E35EB  
33A2B19892769BED8E06B4E53D63F22FD9149074C993AB0299.....

.....AC16D6E84CB0AB25FD12A87F8D82E932362867B0C625BAA1ABB13CEA635FC7D417117D8  
160FE9F74996E855026C961CAE9EC147DA79332B3F5B9C29EA10ADE3EED9D482F494CC

Fused Key:

101100BD7AB17C72644DB047CB99EDA7604E99E7DC878166D0223716C9674A9D2D03AA591B7  
A60D767E46CF7014F443DAB8E64FA0AA71AF6B40E2387A864.....

.....265D2A74E9B24DBF9BD726C5266A902456F1A532864B946A05B33CD26089CE7A5D34CFF  
B47F856531E98B4EF6C0F70B214EC004352B43A3FF412B3DBDE079F7EC856FCE694851

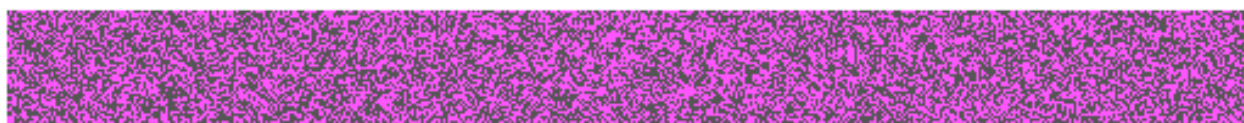
In order to show results more completely, we have adapted a “pseudo-electronic” method of display where “1” is shown in black and “0” is shown in contrasting magenta. The first nine binary characters,



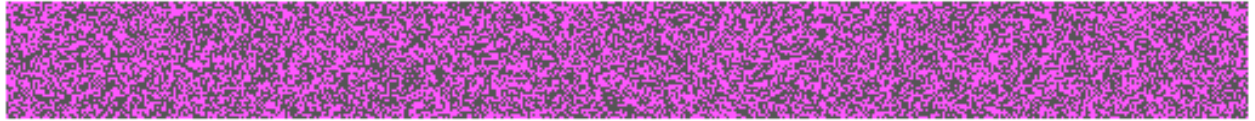
look like this:

The following is a selection of three of the 18 million, million, million variants of the AliceBob Master Key:

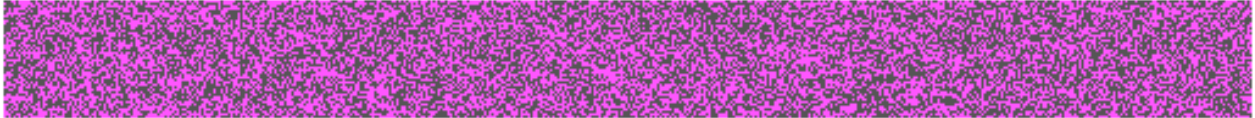
**Master Key:**



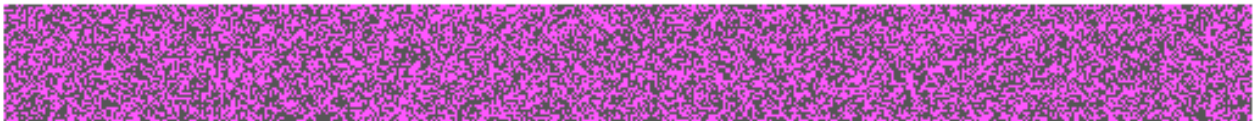
A53039A7E01DCBC6



6B4603D24A43C39D



C6BB2954CE0083A1



The FUSION SUB-ROUTINE is one of many “modules” devised by Hawthorne Davies to suit different technologies. The philosophy is guided by the general aim of being “future proof”. That is why we use a 24576-bit Master Key and a 6144-bit Session Key. But we could just as easily have used a 196608-bit Master Key and a 49152-bit Session Key without incurring any more serious a penalty than the sarcasm of Bruce Schneier, America’s leading cryptologist. This philosophy goes some way to explaining the design of the FUSION SUB-ROUTINE. In its current form, and for extra strength, it performs three “passes”. In the following examples the colour coding is as follows:

**salt** Master Key **passes** Fused Master Key

3-PASS FUSION SUB-ROUTINE:

152F

3A7C4ADADBCD8195E9A795E767DBF82CF7B0BC68DEAC1DE5C08E08C886339348  
 3B599B11E092E1FA359DD9439ADEC211EB46FC613892075C4BD792C7751BDDE4  
 8814BFEA689ED0A1D64719B457B1C50B025800389E1D26109FDA6DCF063C6CCD  
 8284C77F74B10ACDD1D3D1CD78017F3824E1008CB755A31BF394B6DEFA5EBAFC  
 8284C77F74B10ACDD1D3D1CD78017F3824E1008CB755A31BF394B6DEFA5EBAFC

15B7

669977B54110D7E1A6D080AC305D1F693DA612A7E140687F6368B3C7D471522F  
 0C72F913688B27A0DA48004E989245E56CF5856E3DD174F0C0B436D20757B52F  
 3E300D87F4C27AF17AE6733431F4D5861061450E469E96ED4A4422308DD3EEF2  
 2CEE83FE5643D9018922031962AAE85741D4C6D42774422519FF03A4EE180140  
 2CEE83FE5643D9018922031962AAE85741D4C6D42774422519FF03A4EE180140

6C7A

3C23F1ABD1D824799A4452DE2C10E3E520E9564CAEBFCC5A82D3909C07DF9C69  
 2FF137D295A7848D19E305D4AF7E558DC6A60F3979FD9B0E1D46095585ADFE885  
 F96343208205FC315B6A69BB78AE99907E3204BE7177B572157EC8135E475F9B  
 648EB7F552B46F8D53919A30CA9682D5528C5807610C4F913F7A89F01277F99B  
 648EB7F552B46F8D53919A30CA9682D5528C5807610C4F913F7A89F01277F99B

**FD8B**

02E805B1891E22427DDF2C8AE2E955A448A4FFC70576362AED2E07D388B97949  
 E0E55B643501683C18F5725E36132C46FFB8B33574FE226C3CFB424D03DED9E1  
 16415F06F26D249205782D183986B2474D4E352A38D4D0E6041216BECAC4F8BB  
 7C176B13971B9C31BBC6246A5FDF10202097571F6879F8C0A61226DC39E99189  
 7C176B13971B9C31BBC6246A5FDF10202097571F6879F8C0A61226DC39E99189

**D08E**

21702607E2DD6B193D73FBAAED56F5D700549710A85752F6273A55DC9722B9A  
 1C3FCE31803AEBBC1259B4E5250E04725562CB996C37F735528BA0DF04CC2818D  
 F7419C22FBCA61E1B1FB3D0601B70C444E8D6C7014CF932661B951AF098AD26Z  
 D251A152C27AFA2202D4F8597EDCC535BAE96E890DFA70B72C01C417717A481  
 D251A152C27AFA2202D4F8597EDCC535BAE96E890DFA70B72C01C417717A481

**1ABC**

EA7592586500AB1C0552B0477C04274466A37081BA6FDC657569758DD04B5740  
 AF000B8FBEBE0902B2907004BEC067F41156DC29D04D9F1FF9BDEED62357AE213  
 151A1D616EAF508BCFFEC07E5125A7E21F77A31A433FD17BA166C6CDBF24AC09  
 DA68EE61CE9E8BF0B12980547141D0BA70F125E32E51302A2B2B14767AECEB3C  
 DA68EE61CE9E8BF0B12980547141D0BA70F125E32E51302A2B2B14767AECEB3C

**7E6D**

D56B11DB8D051D1390522960BC9A4084D8BC0AFDC2873E9CE7613EFF46BF9AE3  
 D182EACDAEF98F31147598C9A7F2E1CA4D9B471DF2530B84C78DD91EC49F454  
 5E34E9CFC095B9D9A399AECFDB1BBC30F3925A168113D7D60CC0026C4ED6C2  
 DCC681B73D19B425C4F034C5C3C386D0CDB0519BDD2BAC92317AE9DE6A847C2B  
 DCC681B73D19B425C4F034C5C3C386D0CDB0519BDD2BAC92317AE9DE6A847C2B

**6280**

7006F1763A24803FB108E128397F354C472F6683E605E97C98C60787035E6ADB  
 CBA4B1C8290C1B9A749FBDDA5F3BA48C6A3746D19065F1A98F836591F45E3E9A  
 54F7F5AE96970BDB2B80ED550BDBF6BA6C943C5A6F429AA2DD767066E1A87273  
 BFD1A6B5A6879B75BD891D097770409B417D7953132FE658CB21F21B8F25CF88  
 BFD1A6B5A6879B75BD891D097770409B417D7953132FE658CB21F21B8F25CF88

**962C**

8E6D47457DC9B651078DECBA78DAC852C4B5311FA9D700D06BD8D8CBCDEA3CAD  
 E8F54FF71E4BBBEE887267CA1FE8C1D49587051F7893FE84995741E8C9EB41F6  
 F701BF5A2D690C2725388258A09F0A432A7027DB7F25AE7B6DA69BB76D9765CD  
 C0B32BAA1BFB74B1B9D3461B5026B0B989876629C9F5DAA238B4066EE0587937  
 C0B32BAA1BFB74B1B9D3461B5026B0B989876629C9F5DAA238B4066EE0587937

Should we ever deem it necessary, we could use a 20-pass FUSION SUB-ROUTINE without impeding the 60 Megabyte/second encryption speed of the HDX6144 Encryption Algorithm . . .

**20-PASS FUSION SUB-ROUTINE:****C730**

0514D59E7794D000DE4E64FEB56B893B14EBDB45CA9B0E1D22D295114C15F02F  
 63E8DC85AFF4FF636A960DC9F76CEE27C26B058245B9B4BB05AE7E05B06E6E3  
 B65FE2D6B95EA82F35FAA3C863ABFCD4ADA3159D94D15989BE32257B45F0BE0D  
 48C1439D1941AE886C67E9E4FE33AFEDC5662BE6A26EAAB9DDA1409E401DE94  
 9D7E72F7F5315CDEC4BF46BAF3D6A3E90857ED38C893DECFO98ED53D8A856CA1  
 BE705B7D4C1B2AF2218E9D577436898FC28CFBFB95AC6FBB49FC2296F092C14  
 BC808E4C5440AD31D8CFD053686AD8433DCB11B8857080ED201E917004F27A45  
 C1359F987B4350CE97FFE65A34321C0068EF6FFBA665AB9616CDE9666E07444A  
 DF6197E109E5B7B6CB007AF93D044F612E1091567ACA1DD54336D35EB31C68BA  
 2C2F78FC7F049B7B12FC15F90E0335C4913063BFC01975A483BD703C37C5D89  
 7CE81D145C8C03FAFDB447C29204880727A0B11ACF102D2ED5E91087D304EEE  
 2D4F89C4B82ECD991150FCA062709EA93FD45C027D02DA01C16B9E373BF63EB5  
 C26CF681CB5BAEF1281E1611ED4F5F750BEB0CB36C8052C494A4919480B40C2A  
 91F44FB0745106AEFA331C5ACEE6D5F7E82D117B21F74B32D52910A58ECCA9C2  
 A7F37F841316FF401CB4C06BCDAB69549C2D71383200D26B82909D6AA1FBB090  
 7D4207299DF5ABABA38593EFE64276CA97F116D11D44C907CCB423BAA2DBDBBE  
 B9CB7DA9C7CB4B5AC15600EDE9342E1680964AAA92230CE4ECE1C7CADF5CA01  
 8EBD83B37994E2D53B5BCB3B601F46DBC13C3DD689DEFA28C80369BB6BFC9E96  
 877F11EAF3EA7165707589C742AC5FDBA9C604D3AF795BDACCC27FDAB256ABD  
 DFC89EC08A285E6D5EBD53D46FC7D2A7F58A54C1BDCE749B0B7314990593BE45  
 DED4F6668A48A8160B70583AE3E9EDAF5C4E9E9E55FF4E4A375008EF1A594A85  
 DED4F6668A48A8160B70583AE3E9EDAF5C4E9E9E55FF4E4A375008EF1A594A85