



Hawthorne Davies Limited

Tel: 0845 519 0154

+44(0)1276 510724

info@hdencrypt.com

Secrets of the HDX6144 Encryption Algorithm Paper 1

Dr. William McMullen Hawthorne

It comes as no surprise to us that the public is rather skeptical about our claim that the Session Key of the HDX6144 Encryption Algorithm is 6144 bits, managed by a "MASTER KEY" of 24576-bits. The question most often asked is why we believe it is necessary to use such strong keys.

The real answer is that we wish to exploit the unique design of the HDX6144, which differs from all other algorithms in that the speed of encryption and decryption is independent of strength. It all started with the HFX40 algorithm designed by the present writer at the request of the British Facsimile Consultative Committee for submission to the International Telecommunications Union. The algorithm was limited to 40-bits (1 million, million in decimal notation) and followed the principles of a Vernam type cipher. It was evident from the start that an 80-bit version and even an 800-bit version would run at the same speed.

The first HDX was 720-bit. As PCs became more sophisticated we began to achieve higher and higher encryptions speeds and realized that the Session Key could be increased by multiples of 24-bit to any strength we wished to achieve.

The sticking point was the method of generating Master Keys of appropriate strength which we set at (Session Key strength)⁴, but once we had developed the Carousel Random Number Generator then it became possible to create a family of algorithms in multiples of 3072 bits. HDX6144 is currently the engine in CRYPTETOsafe[®] and CRYPTETOMail[®], but we could just as easily have introduced HDX49152, which, like all other versions, encrypts at 60 Mbytes per second. So the short answer to the question "Why such strong keys?" is "Why not?" Our mission is to create an algorithm that is future-proof.

In order to show how the Master Key and the Session Key inter-relate, we start with a 24576-bit Master Key named "AliceBob". It consists of a string of 6144 hex numbers:

```
B00C99AACEB04EDF314C5245F43AA9C1C1D321829A22AC855F14464A202B65CB2
E980E35EB33A2B19892769BED8E06B4E53D63F22FD9149074C993AB0299E1BBAC
D79659BD54201B7A701247CFB488B783EF566C5B8188B818FFCCA7971D330553B
B20719C428D8768534E083ADFB4382EFF50E272BEFF794FEEFA223EC59F5D6F24
CC963A54A2AC9F4A98D4B7B430E7228078A109F4CF19E2333DA1AE2095665113A
FE8F7FD2EB59D3C3A5AA80EFBC7EB90B6332CA970D3635E7F1D901263D944DAA8
EAF5C3BD74DC291E0379D9CF735000C665C68C95B800DE1C4978F7B164116A71F
737596BEAFC0E1B8D46C227608B91125C98714496ED829BB2103112DC6F474814
CACFA16F5B929A21F489D725344FA4659B9EAB30AC0D1740F4AD84D0F4373A453
F1732F3B57BA77A97F70A28D5B0905E4BA244319CF356F6C2C3BE0B3C0F697024
2044D31FD1A97752AAF08CDD4FA9B48526AB6E57B2F9FB8CA589454028409A085
C4231056CB61FDE83DE22750DB9444DD10629F0D11F7133735107E4D86BAEA3C2
2C6C27CED444EEED3C30B089538D5DB3CF3E818827482A04378A0BE86321EDF08
C37F721AEE14BAB7CACAB399576E2D8321247C7DD7A223590D97E4C399D074FC9
6772AD9F7FAD846094F7EC85512FABAA58849C1D29F5A83BDB38CBC6C8123AF19
62E1669302496A0D127D3645B1C30745097BE61F3A900F9D6B936EF1AEB3CAC1C
91E250DE40ADD7067F0EBC134C36BA635807F7AA3FDF6B2E20EFF8EA14F3B7A99
AB26728251684715C7C1D80E46C2D83DAD6133290ED25CC8A919214E369FEA190
150FE6F26417474FC2E756CE80A4738405347272B5A40BEC550C024651D8490DE
17E5E4262418427F4F456C31C3391BB2F40060B543B7066946AEB531EF09D5CBE
8BC939521A760A94AAC0A504C285C1DE39F9E350AC02C519246210A822844F1A5
FBA336A1FEF5B4F1C7C7D5766322834CA2208329C3A1F2AB12FFA81E9E9F254DC
```



Tel: 0845 519 0154

+44(0)1276 510724

info@hdencrypt.com

Hawthorne Davies Limited

57D15B61F6E9114F0F30F888CB28C45E4B55E79037C0197C5829A5DB2337A6EA3
D21C913D12806F5FECE1A69FC1BD6E87ECDDAB0F021F1EC20AB7331DF6DC5E649
C309D1069B6B3B9F31AC51FBFFF34EACA4B110305DF08E26BC57E8B24CAF2D967
8EB0FC84013BD624AFBB81E7BF5767FB8F9888DAFEDF36F2C6D6A186937438B7E
CBB4DCE7F30E9415A198869F9691072119E2FC09064FA0EB30F79CA95AA9D7E0C
056B928B543863E67B8BDBB1C5D53D50C439A95CE26699F757B627F36C63CE69E
A9C909A7532991CDF8CE299FF6C31B11A879DCA085A5E29188369AE9CF9B3FD82
D7C97995C417E53493DC604DD6520C99EF13DFD58BCE1A71DCD4447734646419A
7651622A26540426AF865738DE0C43DA927F060E5DD07E85C95FACB90BB22A567
C7AB68A598F4C7F22015920797DE06371457DA6DABEC95FDE5F0803E023746C8F
5F9E31090AB1B57CAD87F719398EA211559F11ACE407AF9FD59CE8896E5B0C68F
15F45FEB9567C43488BEEDA7C93519C4D57C0FAD9BD8A06B3279D99F006B308FA
09569140F4EA62190F0CC07C02AFE93A33C53DD0C4D728FD02A08ACA40C0BA8A0
B5CED107D34B3B10B2BEFB4CEA3E9005BA1AB04B630A2A9D129213B4C0EB5BA8B
336FDC81779EA09AC52D2E88B3B006DE5C79948C70C27B8A89083FBC1C8C9B3AE
13ADA19BB31216617894D9F5CB16B196B1B6EC0DBAB0CD386E7EED6B0B36D2F24
EBEBBD7465636DC3AE7ADC55B40D60B84DB02120A3A7C4E388AACD8CD640E051A
68D00D59C7E8230B64B032C63D12AB0AD8E30576DE3D9B9C5A5458BA1775D7587
35B10C0F830066045BE81220C0F39AEA13B0780C3CC85D8A5A5E49DF41F5532FF
33AC68C655BD3F5114BACA761FF943ECF3F3789E07F420CEA0FB02BE69DED0915
DA726F0C4D9370595543153ABA7856165E0B864BE4A34B6E7B9C87B0C3B2798CF
491CB2775D05A7EB1A93DDA19A1230B8445F75C3DDEA43FBA5430C32E7230E16F
B359F0B60313B5987A01462478CF0DA5E79E81AE71F538A9CAD42268D7AA0AE84
EBDCADDEC03EDB98F0104265ABA40396D914A8FB1EDC1CEF77FEED2003643F395
A6DEE099801EF0746ED7F3950B423D9BAB2C967E9C9A9D7A70B681F87D82583B4
031D845A9E958F3DCF651FCA90760722171CCDF5501D06237844F7F7D6EC02699
972E618CBD13E91074ED4867DC59F8875E89F1793E68B76DE6C97D2996C72A19A
F72A0F1045D2A73D75FD33B2918D7BCC013A864B9B800C81031F74FB674FE9837
B8FEB0C938711C6FF5DC1A0EE5F83883C4513CB435FE2D627D3CB6A298DDD02D5
43D68445A66D70B645CE59DE3C04D9657600D7EA9591EADFF6D1793DA4CBB8A23
B773998D0B6EB7F66EB72004C667671EA3DD2193313B1F7D5B3883EE709F2D4F7
DD2C4239CF54DB67BB9FE410E773B443F582EDDACE243E549BD32F33B6DF66F6D
EF20D4110278935FAE9811C03B1587740058B0C5F9079DF0D3403DABABDEC1213
385142F102B54AD0A79E138323B27BC3E35027DC1BB21FDB06B362FA61D5432BD
70CE99AB877EC75D8C49D2EA5EC43185698578C6879D20DECAEE4B817164E2DA1
7ED68AB21FA86FE49BC0E91CCCE99889A88E6A59B06C6E4B8A0718B94FE0098AA
78F280B84B73399C6DE32F093116A280AF442E66A01315E3599AF1F87E1E7F65E
49032805C034BF121E4878C3361F9FE85B9BAB7F6F61A0EAD765430C53720413B
5E07D59598BE2D5C3C695479B72EF4F7CB8ACEEEDB08DC51D2E9970B2260650F9
88DA9F32A1659CB0C93FB569D1ADE4523E251A11501440D2D4AFC9978F1A080E2
5AE8AE142111142E620DCF3AB1F817C9D742AD5F0C8E8B18685D689C04BADE16
DFB074152EB8E1541BF93D05A2CE88B3B8EF5D75C3858788F532F336CF6C003E4
878560146396081F604C2C97CFC038AE699D2C867F2472F19D637CBA446F2BAE
45F77A6091EC043F5D3ADD443243D4C7BD003F9E997CBE1993560D2E617C1AB40
B7A003B22A05A24E41CAD79B6FF9493B2919BCEC87882AF1C49BC8FED6DE501D8
4CDDF16543E597FE4A30A11D2D85E664D9CC06D1BDE0CC36DF2E3ADE085322ED8
0C3498AADBDEF531ACF671F596903131B742330F1061211578A9C91F77C4CFC53
F7E2C9A33A6FD2470F214E9A4F80E7A0B94AD86CE06F856442DFFC17EB7444940
C83CEED23112811249943A53BAEA6D662D62CE824C991BC749D0D2F554CA6CCC9
D1A4876F6B03F1BE9443D449BD7725B01687C1165700DD912FDA8DAB2A52216F4
FE7C016618AB26135A0A948E56D6B48CC14BFC3085E6927DDFA0586C09B40F2C4
75814B83DE6089BF116FBF2F2DA3E03ECC2E6D34EA2765057174DF9A89CD5F378
3C51156F0A650EC32FA2976248C689DB803E8BB634736C85E94CAFBCB60D4551F



Tel: 0845 519 0154

+44(0)1276 510724

info@hdencrypt.com

Hawthorne Davies Limited

F6BB27A505B74E88920F0ECC02D89F3062FA94441AE5B57092A019DFE24C593D7
4A50D729090EFAB8EB88162843127B7582DAC399D1A5A2A588FEBA0BA277657A6
5FFBCE6431B5B557DB43F28DDC2AFDD35169CBD0D64CB26C0BAAFCB0E9FA8F10B
A2E212CEA965827858E08CA80F1AEDA21E69499D46FE9965C03DD07BA6D458E5E
3BEFB5C91ED157F834664BBE26D623599B561DA8B3C6E60F51BF658762E1A2EC1
FDD668FED2D8C429987C951AC0B9AA6E5689A22D86EE3661DCFBAF486B8B12EEA
14383A8260BE1DF25DB5EB989089CF03DBA19F1C1711858F4E3A9422FA8E1FDE1
81B086B766BF191D861250B621EA748036EE2779F60F18C8FD2F6B2CF2161E2FF
925CFD6E78C672B5B1B9455291B41EF530DC1FBD8F33A48B613F601777DA893F8
FD191EB542C545B468AAE5866E8002EEE07EEB40751E1446D2723A17426E32724
3F98A796E53D885C48D4773F84E6A3C739D2EAF28AEE5EB388DFA350F657A1CEA
4BF716D0B12189174330FA4F7FAA240708E6EE48AB1EE453BA09BC74423310DFE
84E7E8FC596B7D1264BA6282ACBF25D0AD7F1B4D70B5A1FD5ED2F1731012DC2BB
F639771E64CBE97C8F2395772476B314E6E0446D1B897099608CD1C31A53CD1A6
B50FD0C1D66EDB4182CAB9095CD6922CA2692195CF321477B96158BE6889575C5
6FD2B0502DC5D28857F45BCF9346DBA44B9213343EFD6D068D8D68D04EC1293A6
832089FD9413B8DA0383DB382EB4F3DE647511DFC4627B6C32D33FA605A6DF3BE
7803E8A46B81034AE5E76C4AC16D6E84CB0AB25FD12A87F8D82E932362867B0C6
25BAA1ABB13CEA635FC7D417117D8160FE9F74996E855026C961CAE9EC147DA79
332B3F5B9C29EA10ADE3EED9D482F494CC

Every time the HDX6144 encryption algorithm is run, a new random header is generated. This header acts as a “salt”, and, using the powerful FUSION one-way function, generates a unique Session Key in the form of 512 x 12-bit primitives. The decryption algorithm reads the header and constructs an identical set of primitives.

Authentic Session Keys developed from “AliceBob”, each using a distinct “salt”:

SALT: DEEF1F99EBFEA7F2

9B749981F5C7786B9CBB9CD AFF132852E384FCE2D1FE4FD19113B9E657C992E2946F861CD1B65D
198B69C24EFE22FA0050DE16AE5592DA27F0769A8F36391D44CBF64B3B46F9DE364A36B0EFD291
5E4D66C32C5C57489A263464EE8151813B9BC1DA47242D01A6EAB9F8773638B59315B2769022B5
9ABABC58F35EA5CAD677BDD80267B6A72CE43BB1E73FB47410DBDE73D0F5FB7FF13D9ECFD5993D
1ACF74CF51B57B11E8C3877E953DC23E903624A5E859E4683E7B542D68F6CE4E02903236244733
579BD2AA572B359826D445E7AD616BD9C21578944548400D08E9A41313F7ED564B0BA3ECE38248
229A4F2E229DDFD083063AD36975956EEC2148A898FDE50AB9D499D8778B1D2BCEC598AB4465F
20EBCD2F5E1711363BE9398BE3C2116D3ABC637F6FF69B59CAB360D5DD5703C34E21489B747D2B
05E6AFAFF8CE55DCB3AE423430809733A07D751763D894406E66B8CD601502C09D80B2A8F5B81
96754B92846BD6E6C7A74FBD8B6BC003E9B03A7DEFD7B099B4A399DE3330B2DC2AZB3D26A588A
23731DD924C10278067203D93D81D6428E71036F6B66807783DCEA1EEBA25325D8C23ED1B9DAE
3D7C24B70AF08C0EBDE0806021605EE53BFCED6B7DAA853CEZF63C650017C6042162A3223D7FD9
8750D4684EFC2BC360E5BC21CBB092E3400FC0A4959EA488A95F60BD6DF5EB0CF9DD03E4DA9C21
F1CBBFC20B63A3708D6EE30C91BF5D9E1C74B956FADDEE2CF33240AED2467BB3819AD355C4E
BB08C7C98A78CEC85FFD5D5ED57002CF0BAD239908A6F1BC29060BCF4AD3A367749E908FF1757
EAE55477D2EF14F9071F64BE8B141780034E12623AFA042F6A69C6EDDA9F0FE00A253FB9C69C0
344D531C767187F0BE4DA467F8D8CBDF9D133862FF219EEC15EA741E56A9AB5E0D68804E003C3E
C2F8DC05BB88C6F8680812844A4560D45D21D0B49A788BC3362B6851880354C45BDABAE3C435ED
0566431C8A5072DC4B0FAAAABCAC31AC0DE039922D111324F1E96A819CBAE96FD049208DEED4CF
9060AA171B52D6F89E4E29BB7F676F3745D801D0D3C55EA2E72D3B



Tel: 0845 519 0154

+44(0)1276 510724

info@hdencrypt.com

Hawthorne Davies Limited

SALT: 43596586577CEAE1E

C997915D17CA0DAE6214B7DE5B27D788C6C08D016A33A63D35BE0C6F268DB3F345C056BF21EE73
1960F792D630C872588E65997256EE8C558A071DBF46849D435D51D0DFDE3C963D6C56FE10D98
6302EBEE13DDCB56BF045EECA5A41F1E552552E8609704DAE786AB55264F85AFAD4B87A9B416
3069ECC016BEF7A283B54805FE331204B9CA4B5885263BE47605D42C40982244FF3C18587ABED
2CA776E61519057D7F160940ADA6B47208217885ABF7757A4EAB3613CEB4058AB594F7B6E4C5EC
CBF8CF695F175E5215EC0C477C816AF2F78433F6FBBD78F662C6D7BDC91C72E6E432A36DE243D0
A9E7F125296FCBF241447A4756957626DA9E048E226F519A79310BB112EC977808F9A788BBF4
C6DFC38F57983C26800D82261C6ABDE83C759AECBEC78299F7012BCBAC12139E4F03FBA11E21C6
3F1BAC92B8F18E5CEFEF95BAA039AC50004381B8A0217C13F1806C5C0398160E1E73D1B1D547A
5E39334B49F65603576F0EE150A454DB4D3B3405B521572ACBBD0CCCEAD6F20EF2A4E0B0A2BCA
A056EE7AA351E028018561354E68F86FE05AB84ECF6A105312AF06F17418884CDECC7F7A3C4932
513F46031819ED9F7E8B39152BF8508BCDF49CCE7E0610F72F3961124B1530A191ECD2A0800307
424B335F021EFB21FEDC6F761D800E813E08E4F1A8A524BDCA61F902BDDBCA9A479415A561941B
0A87D38AD4A791C3F8BB763D44C84285E0C99DC82BE6684DCD0CF9716CA6CEC291DB49AE2C290A
E636BB41A30D52A974EA6CAA8BF1486753A08E7C6060541034148660E5529F57D8430115C8C24
082B7E10F3F294B66A1E0F36F24841511A19FCE621D39A4BC207B31E6223D15D7C1F1B76783B31
8B93F08907E6888A972729C207FDF0114927072EAB7B1A34A938C07C111548A227E98F48FB02
0849BB42B54A6F7B7F03391FECC934843751CD276D3A7D57BD5CBA42EF8D9784A4284C7CAF925
52DC4C0E8CE1685171A889630E175AF692332C48ECC4F49A094E483FC9D7C01A56086E6E1AAAF
C2ADF7CB103A74908BBE13E839D3B3A2F6E9B40D32172A9FEDB00F

SALT: 7F5DFFE6901112C2

A306240A9C69FDA235D3772E492B222A6B0AB4F5492F528D90A3747FAFA45EA916AF65B7849051
BD56B7ABF73ECB048A34AB107AE0AB83E3D586A98831BA7A6E5FB5365583AD2725FEA2930AA94
8EF72A6663E071830490E84D998A8C2AF8BE0C1B84037A934B683319766B5301CE8A5C60D609E
0839EB76F72750BF2EE1ED7B4B24B9DD14B0DD780E05D85E4D21B2EB3BB758D142E6ECT81329E
4117EF88EBC3FE24AD5DE2F246C056627B20BF5CABB2E75E4C09BAD81BF90D471B198E3A53F11
2036E91CEAFFA3E042166AB86C1EBDEDAE9D2C9B83B47BE9680F434F8AB06DB5FB6C37C7D9236C
5C6E15145A47A56953F059148726915CA23BDBA03499FCC38D7EEADA95ED9A5760526F2FBA7B96
7DE5A665582C649BFB8BD667968F6C729FE1F7045350732AC8E8C6F5B3597871281BEBFA260
D14B2F749D5CFE4C76B6BED0C42F4B2A4E70E1A7962E474B45DD57D7647643D66BA16F7389A1ED4
BFE72567455C78349750B2D38C7414640EE1DF392D86567EC2CA186B9F4281D0E1AFFDA44B9CD
AC7E662159CF018E821CE607954CE16FE01A835ECC90F27C758EECF0445DCDC380CFD0AB7ABD
199FF84CDFD5D768C49FE4BC779C4E215BEF05DF80773454049CCAC193594E038D89E61ABFBFE
90FD5C8AF2724BE17C90A039FB46ECCB192671D07EC45A6D11A728BAD73101A2E752271B57A1EA
2C62FC588F71FD9FF5F088E8CFFA0A0C9FCBE9841AFEA9F45530D9949DF124366623DFCFC1D
D2F7E0AC5E5E63C1B8D2B9F66D9CA88C1F1CB811C1D6B51EBB9FC2758578D1DFF83164A21DC0
7D7D543BEB03DF44D7070AB71DBC84AFA08C38FAC0F5496E6B857BF7939A6891C83880C05D4B8
2E06CD99DEC02D0BA3CE59F9F163951AE86B7A719AEA21A53DC4B76FCAB3FE40A57CEB442A4702
BB4A2E100E45C9D8A0DC43E82DE2F64452BC25720FABBE91D9251FF0AE26A6C933CE9C52C553
C6E699DE71A3CB4EBF76A846CC178D08F748072FFD7BE3CB91B59E8A26360217446E269B29E5BA
6531C2A7932DB26AC63C2990A67385C52550F44EBDFDE1994F15A

SALT: AA7C7BECBEB733D2

38D5565488EFD2E67E43E2442E38D50F39BEBA3A3FFE3BE6DF11E3BCDED92E5857BDC5C2733
07B20B5A5C229AB8149B0126E032F8209F64AD4F9509E18F400DEEDF5C8B511B28055D7E2156B
FF6A27EBB243EC92D3D3624AC4746E88BEF642A2A358E029385B5A4BCD94734D37E961CA7731D8
F4BDDC0A850B21EF12FD6BE0205F7D6674F01CA56BA44CFB5032B4D90E0DD17090CBE30B5F058
840A9CAF2F394559C34C435CCDE9A32D965ED116A15103A4465DB5AC474B40F1F9B7DED697741
9F39FC8E3F7B6FFD547C6D5584C452B86FA4542C7E485CD07A0F2651DB84B0A72CF78BE0FD514E
6E05BDEBABC5B5425041B6E38FDF60B3F60DE9F37C35BF86B30615043E399797956548146B4
4D659D26B55078FA5808C0A677E6092421057355AC00255743AAEE77F888106EB8DE8229B674AE
F1EE7C62B8C2992BEF653D8A203520DCFCAF3CD0C502574CF30CCA9BB35ED8066867617326263
57C4DA5A906354955670394FF3F181D2A84F5D9158965EB719F5C817E3E93045A8908A2F4607
58CD89002B7472E2DE02AB2D073062DC168984D2C57C416F385E3A15C740131DB7BF3FAC6F18D5
E3A80B576B9864B9223B7F688E0EAA34908BD8EF1384C01F8CCF301052322187EC5D40EED1FE35
D1F2B21D6113063401E98E0E96719A4AC7CE2ACADEC09AF9578D6C26775F66D98625BDE3A0C49F
962F82C77950722047DD7311D58200D865B50331A6AD16CC293BBF1B1D70A150E2B8B84B5B3426
DD3AB641D6AF331620BD65DBCC350FA936C7862303EDA9D0463D278C9B052F53D4412472EDDC95
D63D9FAFC62732B39E36A3F1BE01A6C78B0258AC985D8A513EAB590EA86448BB39180665B52CC
C1181BCC5A0F0A0ED60F8DBFA4B300741DDBDDF154DBFD8BE5D6E132E262395233578DBC2CE52F
86B88E64EE2EC402ABCCB2B7A6383FE5BB99907D82ECA9AC3A9DB80F2631C5CA3E45BDA86871
643CDDA16E29825FCF858CF95389CE802DA16B9A4D22449B9D9EC2D3781E1A2A887462CD1E306B
CF025428A9CBB7ED01C29D0537AE3C8627C6D8C1A4D3BEE65F01C5

By contrast: A typical 256-bit key . . .

BB944C0CDB06DC5FD0F58C09749A44DD9FE3BF381FA0911C40464FF6422A66B5