



**Hawthorne Davies Limited**

Tel: 0845 519 0154

+44(0)1276 510724

[info@hdencrypt.com](mailto:info@hdencrypt.com)

## **A SIMPLE ALTERNATIVE TO QUANTUM KEY MANAGEMENT**

Dr Bill Hawthorne  
Research Director  
Hawthorne Davies Ltd

Toshiba Research Europe Ltd at Cambridge Research Laboratory recently made the following announcement:

*Toshiba's Quantum Key Distribution System delivers digital keys for cryptographic applications on fibre optic based computer networks. Based on quantum cryptography it provides a failsafe method of distributing verifiably secret digital keys, with significant cost and key management advantages.*

*The system provides world-leading performance. In particular, it allows key distribution over standard telecom fibre links exceeding 100 km in length and bit rates sufficient to generate 1 Megabit per second of key material over a distance of 50 km — sufficiently long for metropolitan coverage.*

*Toshiba's system uses a simple 'one-way' architecture, in which the photons travel from sender to receiver. This design has been rigorously proven as secure from all types of eavesdropping attack. This ensures that the Toshiba design will be secure not only today, but also in the future.*

*Toshiba has pioneered active stabilisation technology that allows the system to distribute key material continuously, in even the most challenging operating conditions, without any user intervention. This avoids the need for recalibration of the system due to temperature-induced changes in the fibre lengths. Initiation of the system is also managed automatically, allowing simple turn-key operation.*

*It has been shown to work successfully in several network field trials. The system can be used for a wide range of cryptographic applications, e.g., encryption or authentication of sensitive documents, messages or transactions. A programming interface gives the user access to the key material.*

Inevitably Toshiba has faced criticism. That is the penalty for publishing information on the web. But I am prepared to accept that the claims are true if only for the reason that it is a prestigious organisation staffed by highly skilled researchers.

Several important inferences can be made from the announcement:

1. The system only works between stations linked by fibre optics and has a limited working range. It has been tested at 50 kilometres and "allows" a distance of over 100 kilometres. It is therefore, on Toshiba's own admission, only useful within a metropolitan area.
2. The system can be used by, say, the London Metropolitan Police, provided they do not need to communicate with Interpol. The system can also be used



Tel: 0845 519 0154

+44(0)1276 510724

[info@hdencrypt.com](mailto:info@hdencrypt.com)

## Hawthorne Davies Limited

between London hospitals or within Government Departments, again provided they do not need to send messages to other parts of the UK.

3. In general terms, Quantum Key Distribution sets out to achieve what Public Private Key sets out to achieve, namely, the ability to send a Session Key (a key used for one message only) without the sender and recipient having to share pre-agreed secret information. But in the short range situations in which QKM operates the advantages of not having to share pre-agreed secret information are largely irrelevant.

We in Hawthorne Davies Ltd believe that there is a very simple alternative to QKD. To make a direct comparison with the research in Cambridge and in the interests of clarity, we will assume that there are Government Departments in London who wish to communicate at the very highest level of secrecy. The main features of our CRYPTETO ENCRYPTION SYSTEM are as follows.

1. We abandon entirely the need to transfer a Session Key. So, at one stroke, Quantum Key Distribution is irrelevant. In place of a Session Key we create a massive non-deterministic MASTER KEY, which can be as strong as 196608 bits. Provided it is stored safely, it will never be broken by brute force in real time, or, to put in more succinctly, it will last forever.
2. When it comes to generating a Session Key, we then use our specially developed FUSION KEY MANAGEMENT algorithm to refresh the Master Key using a "salt" consisting of a 16-character hex string. (See Appendix)
3. The salt is placed as a header to the encrypted message. This header allows the recipient to re-create the Session Key, and hence to decrypt the message. The key itself is not transferred.
4. The system is entirely portable. It can be carried on USB Flash Drive..

The obvious question is how we transfer the Master Key in order to establish the link between two correspondents.

Unlike QKD, the CRYPTETO system does not need the transfer of a key every time a message is sent. Transferring a new Master Key is a rare event, so the obvious method of transfer is by courier. At the risk of sounding facetious it is much cheaper to take a taxi across London once in a blue moon than to maintain a fibre optic link for 365 days a year. Hacking into a key without the recipient knowing is one thing. Hacking down a courier is another. He is sure to be missed! And if a new government office opens up in Manchester, then a First Class ticket plus a taxi takes a courier far beyond the reach of QKD. Even the occasional Air Ticket to Sydney is more cost efficient than QKD to London.

Within our own company we send all messages as emails using a 24576-bit Master Key which we distributed in the first instance by surface mail. As an extra precaution the original keys were sent on CDs, each wrapped and sealed with signatures over each seam and then inserted into inconspicuous plain envelopes. (As an elaboration we actually included four different 24576-bit keys on each disc.)



**Hawthorne Davies Limited**

Tel: 0845 519 0154

+44(0)1276 510724

[info@hdencrypt.com](mailto:info@hdencrypt.com)

The software is our own CRYPTETO<sup>®</sup>safe and CRYPTETO<sup>®</sup>mail, both of which use the HDX6144 Encryption Algorithm with a 6144-bit Session Key. Net encryption speed is in excess of 60 Mbytes per second. The product allows the user to test that the Master Key has no redundancies. (See Appendix)

To compete with Quantum Key Distribution we have developed a Key Management algorithm based on a 196608-bit Master Key. It can generate a Session Key of any required length. (See Appendix). We should be delighted to send to any expert a sample Master Key to test its non-deterministic qualities.

APPENDIX: Redundancy tests carried out on an authentic Master Key:

TEST 1 Session Key strength: 256

Salt sent as a header to the encrypted message: F893AC0925711BB3

Session Key (calculated by both sender and recipient):

75A09B9DDFDC167E804A3ECC32B86EBB0B  
467344E1FC03A7272FF95EC1854D8B

TEST 2 Session Key strength: 256

Salt sent as a header to the encrypted message: F893AC0925711BB2

Session Key (calculated by both sender and recipient):

F2AAFEA10E7290AD3F9E0967519F1EE86F4  
1D75392AEED2B17A6F6045B52921C

TEST 3 Session Key strength: 256

Salt sent as a header to the encrypted message: F893AC0925711BB3

Session Key (calculated by both sender and recipient):

AFCC6C7DB51EFC89683D5DC91EDC692513  
C324C5B35FBEE8E27DF42E4DEECCE5

Test 1 and Test 2 demonstrate that a minimal alteration in the salt total alters the Session Key. In Test 3 the salt has been restored but the penultimate character in the Master Key has been altered from "0" to "1". This proves conclusively that there are no redundancies in the 196608-bit Master Key

TEST 4: Session Key strength: 3072

Salt sent as a header to the encrypted message: 03491B81D4367451

Session Key (calculated by both sender and recipient):

36CA178FDB830A2073E327D1C1EBF3EE6826BCAD8C3DE7C258E5F61C  
7A5BDFD821FF82262DC7E5D5E86A455FAA12BC4DEA6A76C4439C5872  
2B2D2EFA50124A54A13B1FC3EEABBA63FA6675BDE86D025B38DA4051  
303BF6D3B98BED711263A8ECEAD08827F9002EA2975A72F17CD23072B  
591409587D571CB5F974EC84C7F4AD65A7600E554DAFE2612CEE4A875  
40243F8A88EFD943277B91D10D40C4F7D0145F5AAEE3B3839778AB7EB  
3ACFBD49C1D7318D99DDAF105634A29F160AE939FF1CC8796A61D59F  
AC3B21F43BAAC9EB762D229EB39E1135943F70DC9C0EB99B718481249  
04B01BE0B94B153A277E2A9EA37EF8E14C23DDA4C6604A3DDB8F1C53  
F0D704C6B07DE9F1BA96F070C904576897F422402BCD9673023AD7A380  
1188A80D0DBCEA0EDB7C437A6172F4A223AA0D6DDAE91FF1AFFAA518  
B9716B218109DEE0987B5D66F180EA1B6BF4714397390F46BE0977DD4D  
06B02BA89776CFCAAFC81C7D2D9CF487EB1AC693B04E84499140B086F  
CFEF1ECDE42B769DCA39EF0F0F4AAACE