Adnan Vaseem Alam

Disk Encryption
Scrutinizing IEEE Standard 1619\XTS-AES

Trondheim, June 2009

Master's thesis

benchmark **XTS-AES**
CTS Transparent
Software-based FreeOFTE AES encryption Narrow-block
Cut-and-paste Exhaustive-key-search DTD
Dictonary attack Base64 TrueCrypt
Coldboot XML NIST Performance Security
P1619 IEEE Non-malleability
Birthday-paradox Hardware-based
Plaintext Tweakable TCB FIPS-140 decryption
XEX XTS-AES-256 dm-crypt Ciphertext XTS-AES-128

NTNU
Norwegian University of
Science and Technology