HYPERSPHERE®

Never Lost, Always Revived

Fundamentals

CONTENTS

IDENTIFYING THE PROBLEM 3
LEXICOGRAPHY 4
N-DIMENSIONAL MATH 5
HIGHER DIMENSIONS 6
EXAMPLE ARCHITECTURE: 8
KEY SHADOWING AND BLOCKCHAINS 10
BENEFITS 12
PATENTS 12
REFERENCES 13

IDENTIFYING THE PROBLEM:

Modern data security has serious problems. According to IBM research, approximately 4 billion data records were compromised in 2016 with an average cost of $158 each. That is a total loss of $632 billion.

Attempts to address this problem generally rely on data encryption. However, this approach has a major problem. Namely, a key used to encrypt the data and/or a copy of the encrypted data still has to be stored. That stored information is subject to attack.

A solution that addresses the above described issues now exists: Key Shadowing Technology. The keys and/or data are never stored anywhere, but rather are regenerated from Shadows at the time of an authorized usage. After use, the keys and/or data are simply destroyed. Thus, that information is never at risk of being hacked, stolen, lost, or corrupted. Further details are provided below.

LEXICOGRAPHY:

Cryptography: The process of transforming information for transmission ("in-flight") or storage ("at rest") into coded information and then accessing the information using a Master Key (see below).

Encryption: The part of cryptography used to transform the information.

Decryption: The part of cryptography used to access the transformed information.

Asymmetric Cryptography: Cryptography involving encryption of information with one key and decryption of the information with another key, for example the one deployed by RSA (RSA, 2017). The security of Asymmetric Cryptography is predicated on the difficulty of factoring large composite numbers that are the product of two prime numbers.

Public Key: A key used for encryption in asymmetric cryptography.

Private Key: A key used for decryption in asymmetric cryptography.

Symmetric Cryptography: Cryptography involving encryption of information with a key and decryption of the information with that same key. Examples include:

- IDEA (Khovratovich, Leurent, & Rechberger, 2017)
- AES (National Institute of Standards and Technology, 2001)
- DES (Diffie & Hellman) -- generally considered to be no longer secure).

Symmetric Key: A key used in symmetric cryptography.

Master Key: A Public Key, Private Key, or Symmetric Key. Typically, a 128, 160, 256, or 512 bit long number.

Enterprise Key Management: Storing Master Keys in a database.

Key Shadows: Mathematical constructs that can be used to regenerate a Master Key.

N-Spheres: The surface of all points in any dimension spaced equidistant from a defined center in that space. In a two-dimensional space, an N-Sphere is a circle. In a three-dimensional space, an N-Sphere is the surface of a sphere (i.e., ball). In a four-dimensional space, an N- Sphere a set of spheres that lie on the surface of the hypersphere (Harley, 1989) and (Frankel).

True Random Number Generator (TRNG): A device that provably creates truly random numbers for example via quantum mechanics (Symul, Assad, & Lam, 2011).

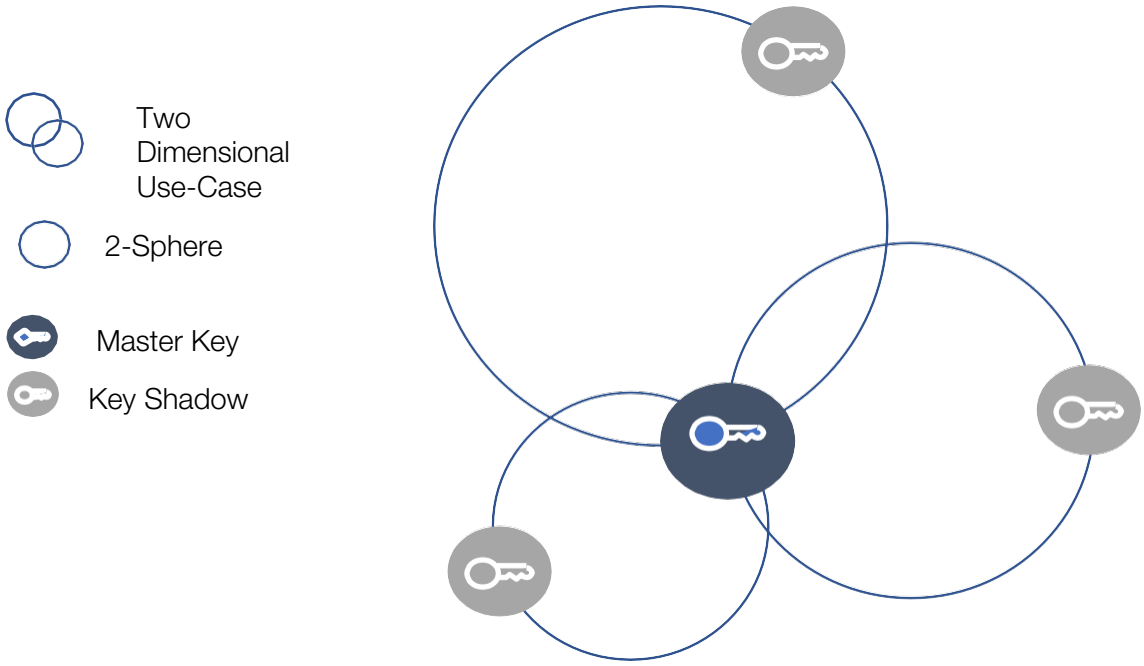
Pseudo Random Number Generator (PRNG): A device or algorithm that creates an approximation of truly random numbers (Pseudorandom number generator, n.d.).

Quantum Computing: A form of computing that does not use variables defined as ones and zeros, but instead uses "q-bits" defined as both a one and a zero at the same time (DWave, n.d.). Quantum Computing has the potential to factor large composite numbers in a short period of time rendering most if not all existing asymmetric cryptography obsolete.

N-DIMENSIONAL MATH:

A Master Key is just a number albeit a very large one. A point representing the number can be generated in an abstract space. The point preferably is generated using a TRNG or cryptographically secure PRNG and some additional math.

A simple explanation of Key Shadowing technology starts with a two-dimensional case involving generated random positions and distances defining N-Spheres of order 2 (i.e., circles) that intersect at the point representing the Master Key. An illustration of a possible result follows:



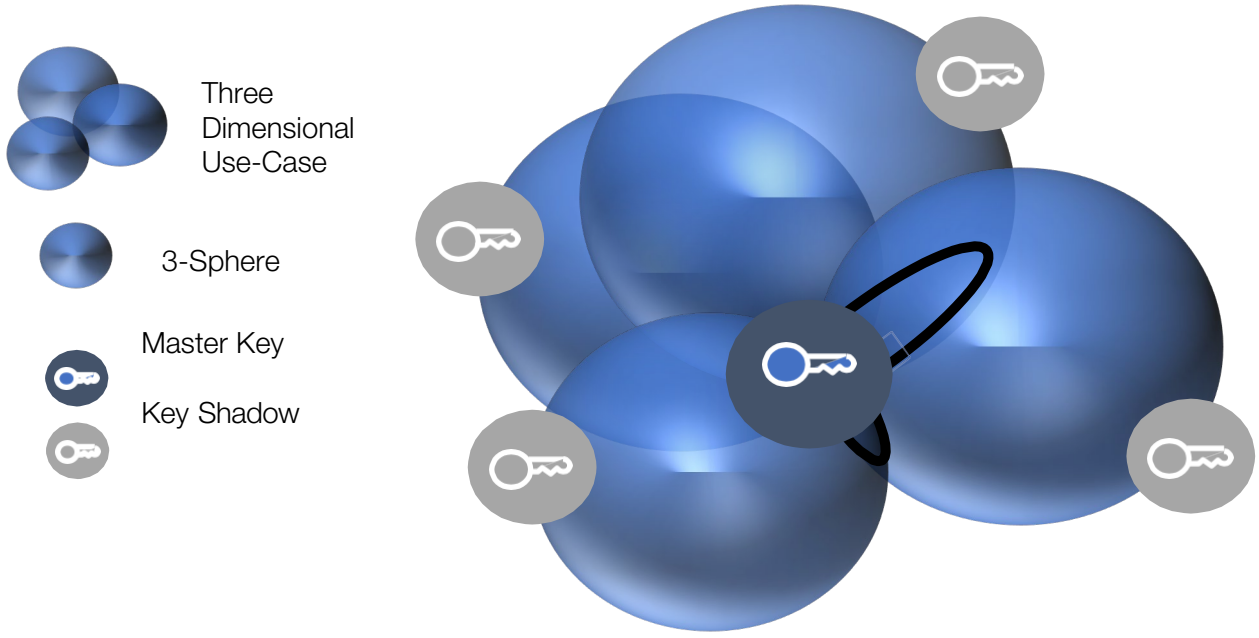
The above figures illustrate generation of three Key Shadows for a Master Key. Any two of the Key Shadows intersect and therefore permit regeneration of the Master Key.

This illustration shows three generated Key Shadows with two required to regenerate a Master Key. Any number of Key Shadows can be generated.

Certain constraints are placed on the random positions and distances that comprise Key Shadows of the Master Key. Each Key Shadow passes through every possible Master Key. In other words, no single Key Shadow by itself contains any information about the Master Key. Thus, without two Key Shadows, no information about the Master Key can be determined even using Quantum Computing.

HIGHER DIMENSIONS:

The following figure illustrates expansion of Key Shadowing Technology to three dimensions:

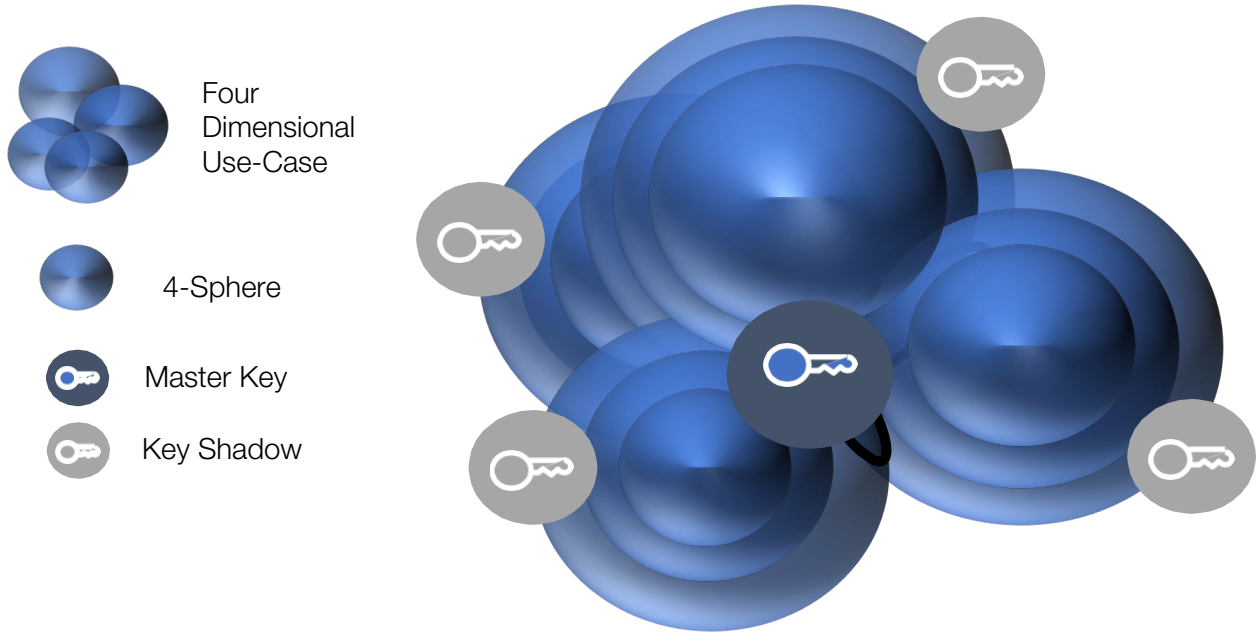


Each Key Shadow is an N-Sphere of order 3 (i.e., a surface of a sphere or ball). Any two 3-spheres intersect in a circle as shown. A third 3-shpere intersects that circle at two points, one of which represents the Master Key. Thus, three Key Shadows are sufficient to regenerate the Master Key.

Again, each N-sphere passes through all possible Master Keys. The circile that is the interestection of two N-sphere also passes through all possible Master Keys. Thus, two Key Shadows provide no information about the Master Key in this three dimensional case.

While only four Key Shadows are illustrated, any number of Key Shadows may be generated with any three sufficient to regenerate the Master Key.

Key Shadowing has also been implemented in four dimensions (i.e., four Key Shadows are required to regenerate a Master Key.)



Almost twenty years were spent ensuring (1) less than the required number of Key Shadows provides no information about the Master Key, and (2) the Master Key can be regenerated every time a sufficient number of Key Shadows are provided. These aspects have been extensively tested.

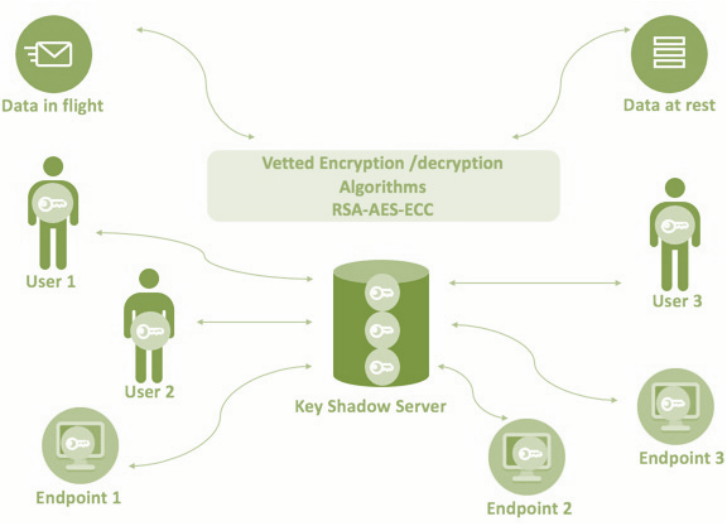
The math behind Key Shadowing Technology has been successfully implemented for the two, three, and four dimensional cases. Higher dimensional cases are possible and in fact have been derived but not yet fully coded.

EXAMPLE ARCHITECTURE:

The following figures illustrate the superiority of Key Shadowing Technology:

Note that each Key Shadow is not half of the Master Key. Rather, each Key Shadow is a mathematical construct that shadows the Master Key. As noted above, any number of Key Shadows may be issued with a defined number required to regenerate the Master Key.

One example of an architecture for implementing Key Shadowing Technology is illustrated below:



The Key Shadow Server is not a key server in the traditional sense. While the Key Shadow Server may retain a Key Shadow (useless by itself to regenerate a Master Key), the Key Shadow Server does not retain any Master Keys. Traditional key servers retain Master Keys and therefore represent a single point of failure for protected information.

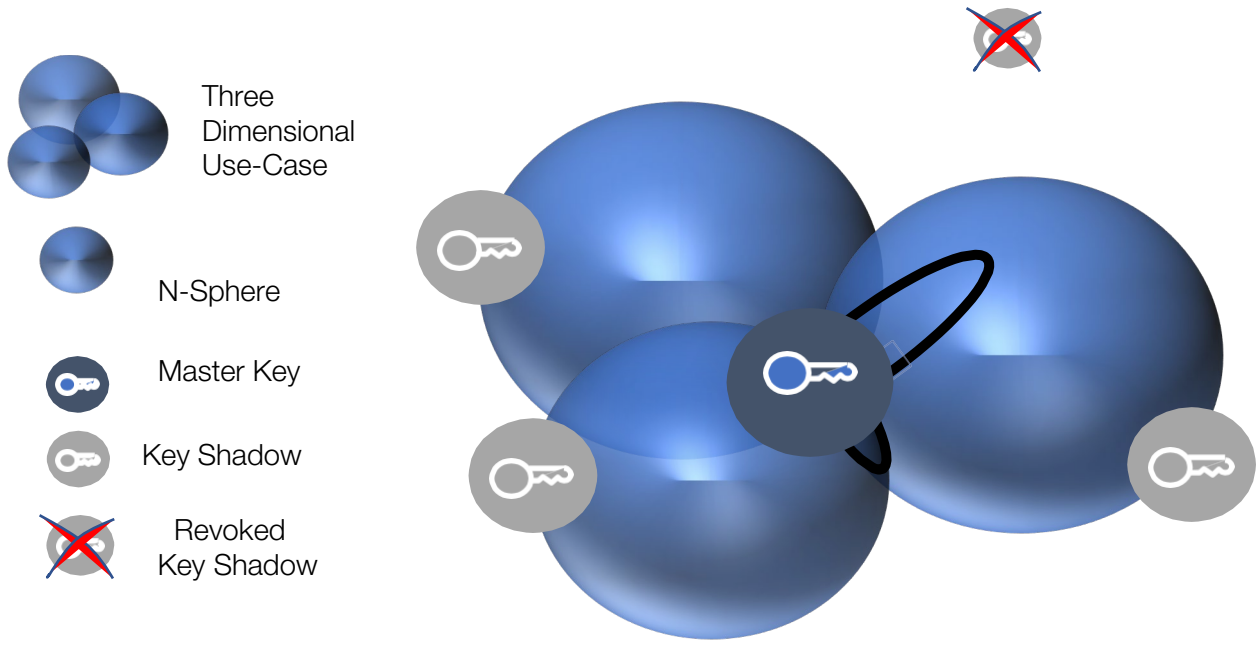
Instead, information in flight (i.e., being transmitted) and/or information at rest (i.e., stored) is encrypted using a Master Key generated by the Key Shadow Server. The Master Key is then destroyed in memory, preferably by application of techniques at least compliant with the DoD 5220.22-M standard (United States Department of Defense). Other techniques may be used. For example, several commercial information destructions programs employ techniques far superior to those set forth in the 5220.22-M standard.

Key Shadows of the Master Key are issued to various users and/or computing devices. When needed, the Master Key is regenerated if a sufficient number of those users and/or computing devices participate in a transaction. The Master Key is used and then again destroyed.

Key Shadowing Technology therefore actually enables far more than “The Ideal World” Solution posited by Dyadic. Neither Dyadic nor Proticor’s technology comes close to doing so.

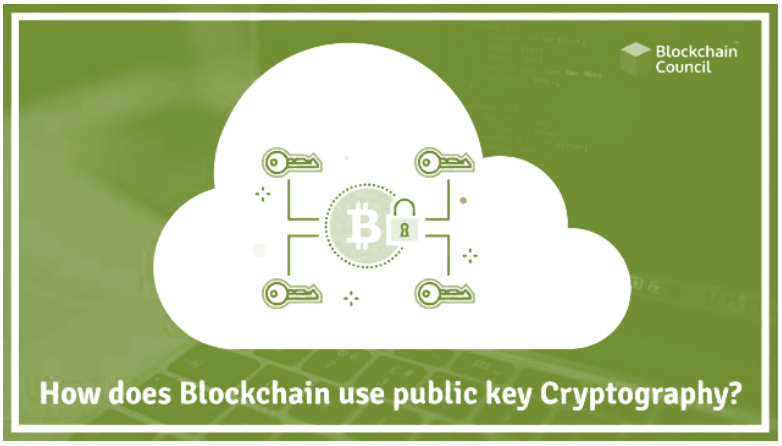
Additional options for implementation of Key Shadowing Technology have been contemplated and architected.

Key Shadowing Technology has a further capability not enabled by the competing technologies: Key Shadow revocation. A user's or device's Key Shadow can be revoked as illustrated below:



A revoked Key Shadow is no longer capable of participating in regeneration of a Master Key. Two different techniques can be used to revoke a Key Shadow from a user or device. At least one of the techniques permits revocation without the device or user participating or even knowing about the revocation. Revoking a Key Shadow does not change the Master Key and thus can be performed without having to re-encrypt the information protected by the Master Key.

KEY SHADOWING AND BLOCKCHAINS:



Asymmetric cryptography or public cryptography is an essential component of blockchains:

Note: The example above is with respect to Bitcoin blockchains but applies to any blockchain.
Public key cryptography is used in several places in any blockchain protocol.
Public key cryptography relies on a pair of keys: (1) a private key that is kept secret, and (2) a public key which is broadcasted out to the network.

Blockchain Vulnerabilities:

- If you lose your private key, you cannot authorize new transactions. For example, you cannot spend or redeem your Bitcoins. This has happened without any bad actors involved.
- If someone hacks your private key, the hacker can pretend to be you.
- If someone derives your private key from the public key, the hacker can pretend to be you. This vulnerability has become more acute due to the surprisingly rapid advances in quantum computing. See, e.g., MIT Technology Review, “Quantum Computers Pose Imminent Threat to Bitcoin Security,” November 8, 2017.
- Bitcoin is an example of a blockchain implementation. Bitcoin wallets include private key(s). “Wallets can be compromised, manipulated, stolen and transferred, just like any other store of value on a computer.” The same applies to keys involved in any other blockchain.

HOW KEY SHADOWING WILL HELP

- Create shadows of your private key, share those shadows with a Circle of Trust, and then destroy the private key. As long as enough people and/or devices in the Circle of Trust come together, you will be able to recreate your private key.
- A private key that is never persistently stored is much harder if not impossible to be “compromised, manipulated, stolen and transferred.”
- Create shadows of the public key, share only those shadows with the world or defined group, and then destroy the public key. At least some number of people and/or devices would have to come together to recreate the public key just as a first step to try deriving your private key from the public key.
- A public key that is never persistently stored is much harder if not impossible to be

“compromised, manipulated, stolen and transferred.” Also, deriving a private key from a public key that is never persistently stored is also much harder if not impossible.

BENEFITS:

Key Shadowing provides a significant change for the cryptography market. Exemplary use cases include:

- Securing payment systems,
- Enterprise Key Management,
- Securing electronic medical records,
- Securing device communications,
- FIngerprint electronic hardware,
- Tracking document custody,
- Multi-factor authentication,
- Financial transaction fingerprinting,
- And, e-discovery protection, to name a few

Enterprise Key Management involves storing, managing, and controlling access to Master Keys. This represents a single point of failure. Namely, if the Enterprise Key Management system is compromised, the Master Keys are exposed. If the Enterprise Key Management system fails, all data protected by the previously stored Master Keys is lost.

With Key Shadowing Technology, only Key Shadows have to be managed. No choice has to be made about who has to perform Enterprise Key Management and accept the associated business and financial risks because no Master Keys are ever persistently stored.

Key rotation strategies are impacted because Key Shadowing allows for the implementation to revoke a shadow and add new shadows to a Master Key without the need to decrypt and re-encrypt the data. Since the Master Key exists only at time of use, the Key Shadows can be treated and handled under a completely difference set of policies. Key Shadows have the ability to implement military type two-person or multiple person integrity before the Master Key is temporarily recreated for access.

Furthermore, we believe that Key Shadowing Technology is the only key management system immune to Quantum Computing.

PATENTS:

Key Shadowing Technology is patented. See U.S. Patent No. 9,634,836 issued on April 25, 2017. Additional patents are pending.

REFERENCES:

https://www.research.ibm.com/5-in-5/lattice-cryptography

Diffie, W., & Hellman, M. E. (n.d.). *Exhaustive Cryptanalysis of the NBS Data Encryption Standard.* Retrieved 2017, from https://web.archive.org/web/20140226205104/http://origin-www.computer.org/csdl/mags/co/1977/06/01646525.pdf

DWave. (n.d.). *The Quantum Computing Company*. Retrieved 2017, from

https://www.dwavesys.com/ Dyadic. (2015). *Dyadic Technology*. (Dyadic, Producer) Retrieved

2017, from https://www.dyadicsec.com/technology_mpc/

Frankel, R. (n.d.). *The HyperSphere, from an Artistic point of View.* Retrieved 2017, from http://groups.csail.mit.edu/mac/users/rfrankel/fourd/FourDArt.html

Harley, F. (1989). *Differential forms with applications to the physical sciences.* Dover Publications.

Intuit, Inc. (2016). *Intuit Data Protection Services*. Retrieved 2017, from https://security.intuit.com/index.php/idps

Khovratovich, D., Leurent, G., & Rechberger, C. (2017). *Narrow-Bicliques: Cryptanalysis of Full IDEA.* Retrieved from http://www.cs.bris.ac.uk/eurocrypt2012/Program/Tues/Rechberger.pdf

National Institute of Standards and Technology. (2001, November 26). ADVANCED ENCRYPTION STANDARD (AES) .

Pseudorandom number generator. (n.d.). Retrieved 2017, from https://en.wikipedia.org/wiki/Pseudorandom_number_generator

RSA. (2017). Retrieved from https://www.rsa.com/en-us

Symul, T., Assad, S. M., & Lam, P. K. (2011, May). Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Applied Physics Letters*.

United States Department of Defense. (n.d.). *US Department of Defense 5220.22-M Clearing and Sanitization Matrix.* Retrieved 2017, from https://it.ouhsc.edu/policies/documents/infosecurity/DoD_5220.pdf

https://news.bitcoin.com/guy-lost-bitcoin-computer-upgrade/ (Note: This is just one example. The current value of the lost Bitcoins in this single example is now over $1M.)

https://www.technologyreview.com/s/609408/quantum-computers-pose-imminent-threat-to-bitcoin-security/

https://www.csoonline.com/article/3241121/cyber-attacks-espionage/hacking-bitcoin-and-blockchain.html