Tanish Kumar

Dr. Oas

Introduction to Quantum Computing

18 December 2022

An Overview of Quantum Digital Signatures

In this paper, I will be explaining the purpose and structure of digital signatures, both in the quantum and classical realms. I will begin by giving a quick overview of the basic types of cryptography as well as explaining the nature of hash functions. Then, I will outline the procedure of sending a digital signature classically and in which situations a digital signature is useful. Finally, I will illustrate a quantum digital signature scheme (authored by Gottesman and Chuang) and contrast it with classical digital signature schemes.

There are two primary types of cryptography that are relevant to digital signatures: symmetric (secret key) and asymmetric cryptography. [1] In symmetric cryptography, the same key that is used to encrypt the message/data is also used to decrypt the message. Essentially, if we imagine that the key is a function, wherein the message is the input and the encrypted message is the output, the key is an easily invertible function such that we can input the encrypted message into the inverted to obtain the original message again. An example of symmetric cryptography would be the Caesar cipher, which substitutes each letter in a message with a letter that comes a specified number of positions later in the alphabet (and letters near the end of the alphabet would wrap-around to the beginning). It is quite simple to encrypt a message using a Caesar cipher simply by substituting each letter one by one according to the specific Caesar cipher chosen. However, simply by inverting the Caesar cipher (such that each letter is substituted by the letter that comes a specified number of positions before in the alphabet, where the number is the same one as in the original Caesar cipher), one can obtain the original message from the encrypted message. In this way, the Caesar cipher can be used both to encrypt and decrypt the same data.

In asymmetric cryptography, there are two keys, named the private and public keys, where one is used for encryption and the other for decryption. It is vital that the public key be derived from the private key through a one-way function. A one-way function is a function where obtaining the output from an input is a computationally inexpensive process, but where the reverse (obtaining an input from a specific output), is computationally impossible. There is a current debate over whether one-way functions actually exist. As is obvious from the naming scheme, public keys are meant to be announced/released to the public whereas the private key is meant to be kept strictly a secret. There are two different schemes within asymmetric cryptography: 1) the public key is used for encryption and the private key is used for decryption, 2) the public key is used for decryption and the private key is used for encryption. Digital signatures fall under the latter scheme, whereas traditional cryptography (as we think of it as sending secret messages), falls under the former scheme.

Hash functions are also another vital part of digital signatures. Essentially, hash functions relate data (in our case, a message) of any size to fixed-length alphanumeric strings (called hashes or digests) through some deterministic calculations. [2] There are a few features of good hash functions: 1) irreversibility and 2) collision-minimizing. [3] In terms of irreversibility, good hash functions should be irreversible, in that no individual should be able to obtain the original message given the hash. Furthermore, hash functions should be such that no two, distinct inputs can lead to the same hash (a collision). As a side note, good digital signatures should appear to act chaotically. Despite the deterministic calculations, small changes in the original message should lead to a vastly different hash. For example, the Secure Hash Algorithm – 256 (SHA-256), maps about a 1 MB large Bitcoin transaction block to a fixed-length 256-bit (32 byte) string.

Digital signatures function a lot like physical signatures, except that digital signatures are tailored to the message associated with them. [4] Digital signatures are not to be confused with electronic signatures, a category that can include digital signatures, but can also refer to digital versions of one's physical signature, as is done through web services like DocuSign. Classical digital signatures are a string of alphanumeric characters that only take on meaning when associated with a message. There are three main algorithms required for digital signatures: a key generating, signing, and verifying algorithm. Digital signatures are applicable in virtually all forms of online communication, from cryptocurrency to online purchases.

There are three main properties associated with a digital signature: authenticity, integrity, and nonrepudiation. A digital signature ensures that the message is authentic and has actually been sent by the expected sending party (in other words, the message signer). A digital signature also ensures that the contents of the message have not been tampered with during transit. Finally, a digital signature makes it such that the sending party cannot deny having signed/interacted with the message being sent. This might be particularly helpful in legal contexts.

The procedure for sending a message with a digital signature is as follows. First, the sending/signing party uses a key generating algorithm (like a one-way function), to generate a public and private key. The sending party then announces the public key to the public. In addition, the sending party selects an appropriate hash function and announces the function as well. After doing so, the sending party inputs the message into the hash function, obtaining a message digest, or hash, and encrypts this hash using the private key. This encrypted hash is the digital signature. The sending party then sends the encrypted hash along with the original, unencrypted message to the receiving party. Using the public key, the receiving party decrypts the encrypted hash. Using the announced hash function, the receiving party also inputs the unencrypted message into the hash function, to obtain a new hash. If the unencrypted hash and the new hash match, the digital signature is verified, and all the three properties of digital signatures hold. This process is summarized in the figure below.

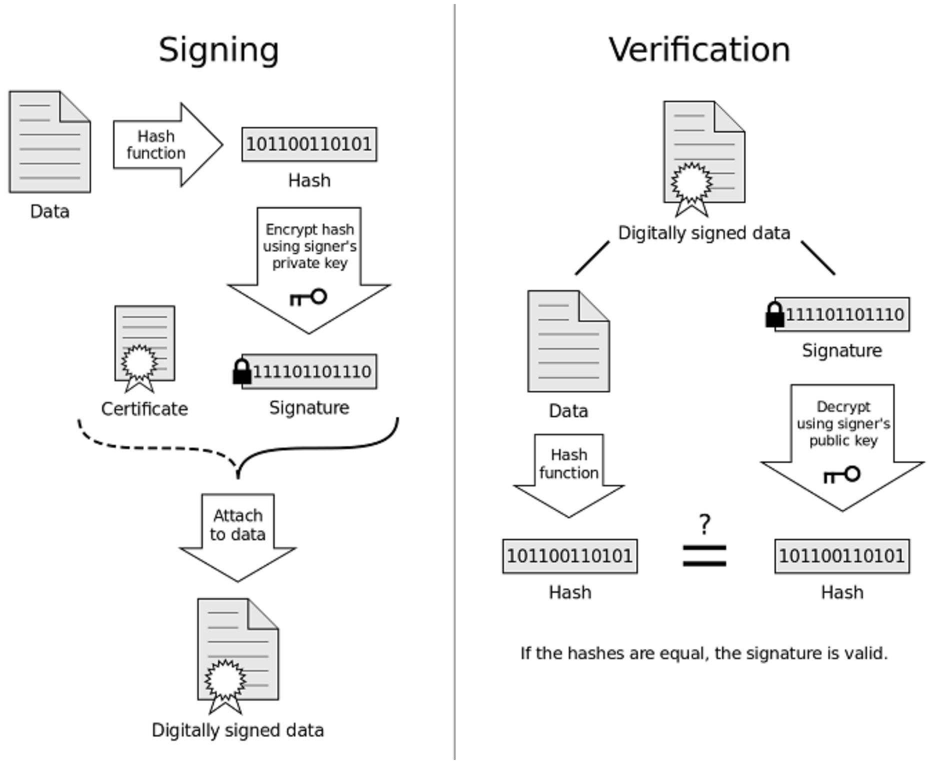


Figure 1: Diagram of classical digital signature procedure [5]

A real-world example where digital signatures would be useful is in downloading software. When downloading software from the internet, individuals would like to ensure the integrity of the software (no injected malware, no bugs, etc.), as well as ensure that the software comes from a reputable source. By adding a digital signature to the software, the source can give its customers a guarantee of the authenticity of the software. In the case that the software is altered in transit, the individual downloading the software would not see identical hashes and would know that the received software should be deleted as soon as possible. More specific schemes of digital signatures include Lamport signatures, Merkle signatures, and Rabin signatures.

Quantum digital signatures work in a similar way to classical digital signatures with some notable differences. While quantum digital signatures also employ asymmetric cryptography, public keys can be generated a few different ways. In this case, quantum public keys are derived from private keys, but the private keys can either be a classical bit string or quantum state(s). Quantum one-ways functions (deriving a *single* quantum public key from a quantum private key), is through to be almost complete irreversible due to fundamental uncertainties. Due to the no cloning theorem, a single quantum public key cannot be duplicated and distributed, meaning that multiple slightly different quantum public keys must be used. Furthermore, by the nature of how these public keys are constructed, if an unfriendly party obtains many public keys, they could determine the private key (through various computational means), compromising the cryptosystem. Note this does not conflict with the discussion of quantum one-way functions above, as the quantum one-way function is thought to be irreversible given only a single output.

The basis of a quantum digital signature scheme was developed by Gottesman and Chuang, and a simplified version of the scheme is described below. [6][7] Assume the sending party has a message in binary bit form. Using this quantum scheme, the sending party must digitally sign each bit. Let us say the sending party has chosen a single bit to sign and send. The sending party generates 2N bit strings (where N is a positive integer), N bit strings for the case where the bit is 0 and another N bit strings for the case where the bit is 1. The sending party then chooses and announces an appropriate quantum one-way function and sends the outputs of this quantum one-way function for all 2N bit strings to the public. The sending party then sends the set of classical bit strings corresponding to the message bit, along with the bit itself, to the receiving party. Depending on the message bit, the receiving party chooses the corresponding set of N bit strings to put through the quantum one-way function, to obtain a set of N new quantum states. The receiving party compares the new quantum states to those that the sending party had announced (using a SWAP test). If the number of matches exceeds a certain pre-defined threshold, the signature is verified. Note, increasing N increases the security of the cryptosystem. The following two figures display this procedure in diagram-form.

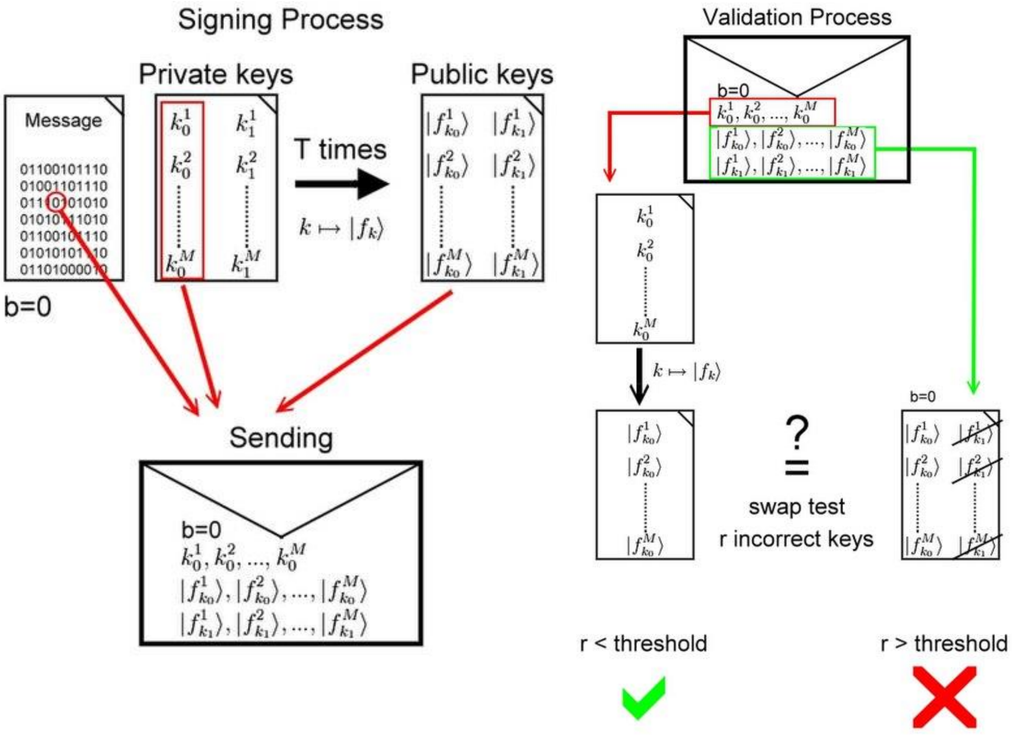


Figure 2 and 3: Diagram of quantum digital signature procedure [7]

The quantum circuit for the SWAP test used in this scheme is displayed below.

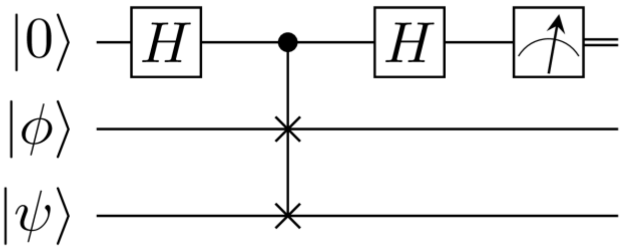
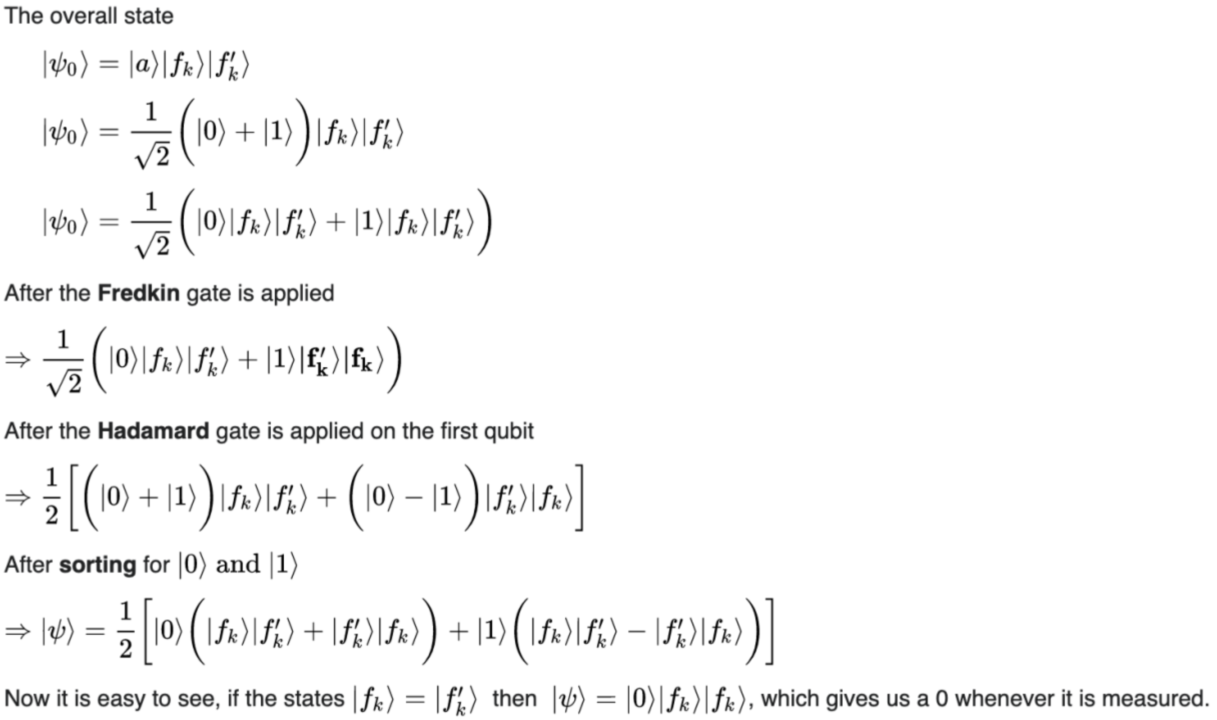


Figure 3: Quantum circuit for a SWAP test [7]

To see how this quantum circuit works, refer to the calculations below.



The overall state

$$|\psi_0\rangle = |a\rangle|f_k\rangle|f'_k\rangle$$

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big)|f_k\rangle|f'_k\rangle$$

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle|f_k\rangle|f'_k\rangle + |1\rangle|f_k\rangle|f'_k\rangle\Big)$$

After the **Fredkin** gate is applied

$$\Rightarrow \frac{1}{\sqrt{2}}\Big(|0\rangle|f_k\rangle|f'_k\rangle + |1\rangle|\mathbf{f'_k}\rangle|\mathbf{f_k}\rangle\Big)$$

After the **Hadamard** gate is applied on the first qubit

$$\Rightarrow \frac{1}{2}\Big[\Big(|0\rangle + |1\rangle\Big)|f_k\rangle|f'_k\rangle + \Big(|0\rangle - |1\rangle\Big)|f'_k\rangle|f_k\rangle\Big]$$

After **sorting** for $|0\rangle$ and $|1\rangle$

$$\Rightarrow |\psi\rangle = \frac{1}{2}\Big[|0\rangle\Big(|f_k\rangle|f'_k\rangle + |f'_k\rangle|f_k\rangle\Big) + |1\rangle\Big(|f_k\rangle|f'_k\rangle - |f'_k\rangle|f_k\rangle\Big)\Big]$$

Now it is easy to see, if the states $|f_k\rangle = |f'_k\rangle$ then $|\psi\rangle = |0\rangle|f_k\rangle|f_k\rangle$, which gives us a 0 whenever it is measured.

Figure 4: Quantum state throughout the quantum circuit for a SWAP test [7]

In the theoretical formula of this quantum digital signature scheme, the tools used to obtain quantum states are assumed to be perfect. In addition, we know that by the nature of the quantum public keys, the keys may differ slightly leading to the possibility of the SWAP test coming up false. This is why a threshold is built-in – that exceeding the threshold gives some breathing room for false test results, but also gives reasonable certainty that the message integrity remains.

In conclusion, quantum digital signatures offer a more secure way of signing data and offer some security advantages to classical digital signatures. Notably, quantum one-way functions are thought to be more secure (more “one-way”) than classical schemes due to fundamental uncertainties, but that quantum key distribution needs to be more carefully done due to the no cloning theorem and the nature of how quantum keys are produced. In addition, due to the infancy of the field, as we saw in the Gottesman and Chuang scheme, a lot of resources and energy is required to send messages, especially bit by bit. In the future, with the rise of quantum networks, quantum digital signatures will play a large role in online communication and may eventually form the basis for secure and authentic message transit.

References

[1]: Goel, Shorya. “What Is Cryptography in Security? What Are the Different Types of Cryptography?” *Encryption Consulting*, 13 Oct. 2022, https://www.encryptionconsulting.com/education-center/what-is-cryptography/.

[2]: *Hash Functions*. https://cryptobook.nakov.com/cryptographic-hash-functions. Accessed 19 Dec. 2022.

[3]: Crane, Casey. “What Is a Hash Function in Cryptography? A Beginner's Guide.” *Hashed Out by The SSL Store™*, 25 Jan. 2021, https://www.thesslstore.com/blog/what-is-a-hash-function-in-cryptography-a-beginners-guide/.

[4]: “Digital Signature Overview.” *IBM*, https://www.ibm.com/docs/en/b2badv-communication/1.0.0?topic=overview-digital-signature.

[5]: Nadeem, M Salman. “Digitally Signed Emails. What Is It and How Do Digital Signatures Work?” *Mailfence Blog*, 16 Aug. 2022, https://blog.mailfence.com/how-do-digital-signatures-work/.

[6]: Gottesman, Daniel, and Isaac Chuang. *Quantum Digital Signatures*. arXiv, 14 Nov. 2001. *arXiv.org*, https://doi.org/10.48550/arXiv.quant-ph/0105032.

[7]: “Quantum Digital Signature.” *Wikipedia*, Wikimedia Foundation, 19 June 2021, https://en.wikipedia.org/wiki/Quantum_digital_signature.