INTRODUCTION

The term "*Near Field Communication*" refers to a wireless technology that facilitates data transfer between two devices that are relatively close to one another, usually just a few centimeters away. It belongs to the class of technologies known as Radio Frequency Identification (RFID), which uses electromagnetic induction to facilitate communication between devices.
Since its introduction in 2004, NFC has experienced rapid growth across several industries, including access control, mobile payments, and transportation. The ability to execute contactless transactions and share data with other NFC-enabled devices is now widely available in smartphones, credit cards, and other devices.
The simplicity and convenience of NFC are among its tremendous benefits. It may be used by just placing two devices near together and does not require pairing or configuration. NFC also offers high security because all communications between devices are encrypted, and only approved devices are allowed access to the data.

Mobile payments, access control, ticketing, and identification are just a few of the many uses for NFC technology. Users can tap an NFC-enabled device on a tag or banner to access information or promotions. NFC is also used in marketing and advertising. In conclusion, NFC technology has completely changed how we engage and communicate with the world around us.

NFC card is based on RFID (radio frequency identification) technology but has a much lower transmission range of about 4 cm or less. This makes NFC cards more secure and convenient than RFID cards, as it reduces the risk of unauthorized scanning or interception. NFC card also supports bidirectional communication, which means they can send and receive reader data.
NFC card is compatible with most smartphones and smartwatches with built-in NFC technology. This allows users to use their mobile devices as NFC cards for various purposes, such as accessing buildings, verifying their identity, making payments, or transferring data. NFC cards can also interact with other NFC-enabled devices, such as speakers, collectibles, and gaming consoles.

At the protocol level, reverse engineering analyzes the transmission between the smart card and the reader or host device. This can be done by using passive or active methods such as eavesdropping, intercepting, modifying, or injecting messages. These methods can reveal the format, content, and semantics of the smart card application protocol data unit (APDU), the standard way to exchange data between smart cards and readers. However, these methods depend on the protocol specifications, standards, and implementations and can be prevented by countermeasures such as authentication, encryption, and integrity checking.
The protocol level of smart card technology is how the smart card and the reader exchange data using the application protocol data unit (APDU) format. There are different types of contacted and contactless intelligent card protocols, such as T=0, T=1, Type A, Type B, etc. These protocols define the physical interface, transmission mode, error detection, and anti-collision methods. Standard protocols ensure interoperability and security, while proprietary protocols may have some advantages or disadvantages.

Reverse engineering of smart card technology is a challenging but feasible task that can pose serious threats to the security and privacy of smart card users and providers. Therefore, it is important to create and implement smart cards with security in mind, using appropriate techniques and countermeasures to protect them from reverse engineering attacks.

The protocol level of smart card technology is vital for ensuring interoperability, compatibility, and security between different intelligent cards and readers. Following standard protocols, smart cards can communicate with various devices without requiring specific drivers or software. However, some smart cards may also use proprietary protocols that are not compliant with the standards, limiting their functionality or exposing them to reverse engineering attacks. Therefore, using standard protocols whenever possible and implementing appropriate countermeasures to protect the communication from eavesdropping, interception, or modification is advisable.
In conclusion, the protocol level of smart card technology is a crucial aspect of brilliant card communication that affects its functionality, performance, and security. One can choose the most suitable protocol for a given application or device by understanding the different protocols and their characteristics. Moreover, by following standard protocols and implementing appropriate countermeasures, one can protect the intelligent card communication from reverse engineering attacks and ensure its reliability and integrity.