Security Analysis on NFC Applications

Xiaobo Guo
gxbbest@126.com
Master Candidate
Beijing University of Posts and Telecommunications
China

Security Analysis on NFC Applications

1	NFC Technology

2	Working Modes of NFC Devices

3	Security Problems of NFC Application

4	Countermeasures to Ensure NFC Security

NFC Technology

- **Protocol**
- **Coupling**
- **Channel**
- **Communicate**

NFC Application

Working Modes

Reader operating mode

Initiator

Target

Peer-to-Peer operating mode

Initiator

Target

Card emulation operating mode

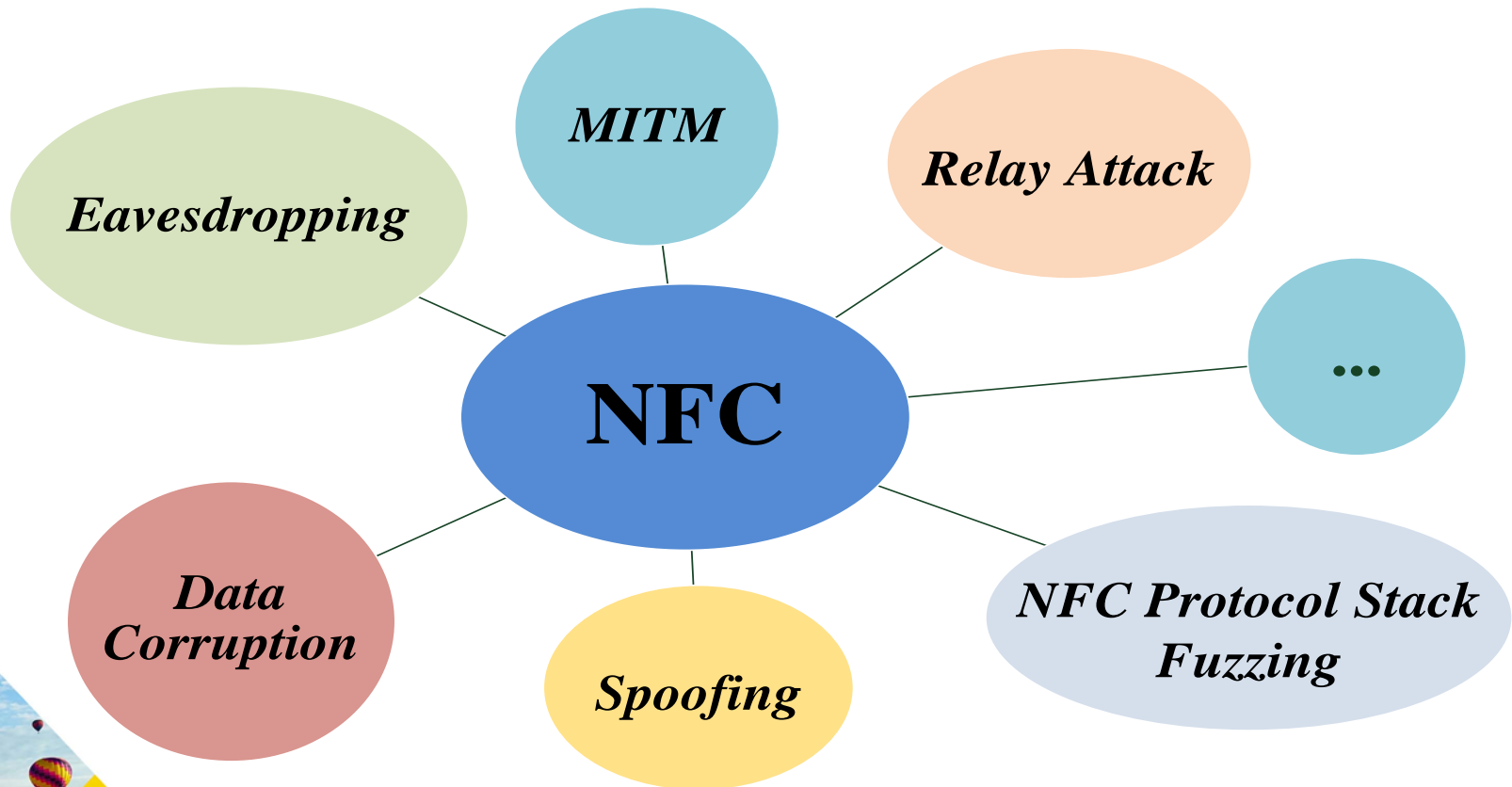Initiator
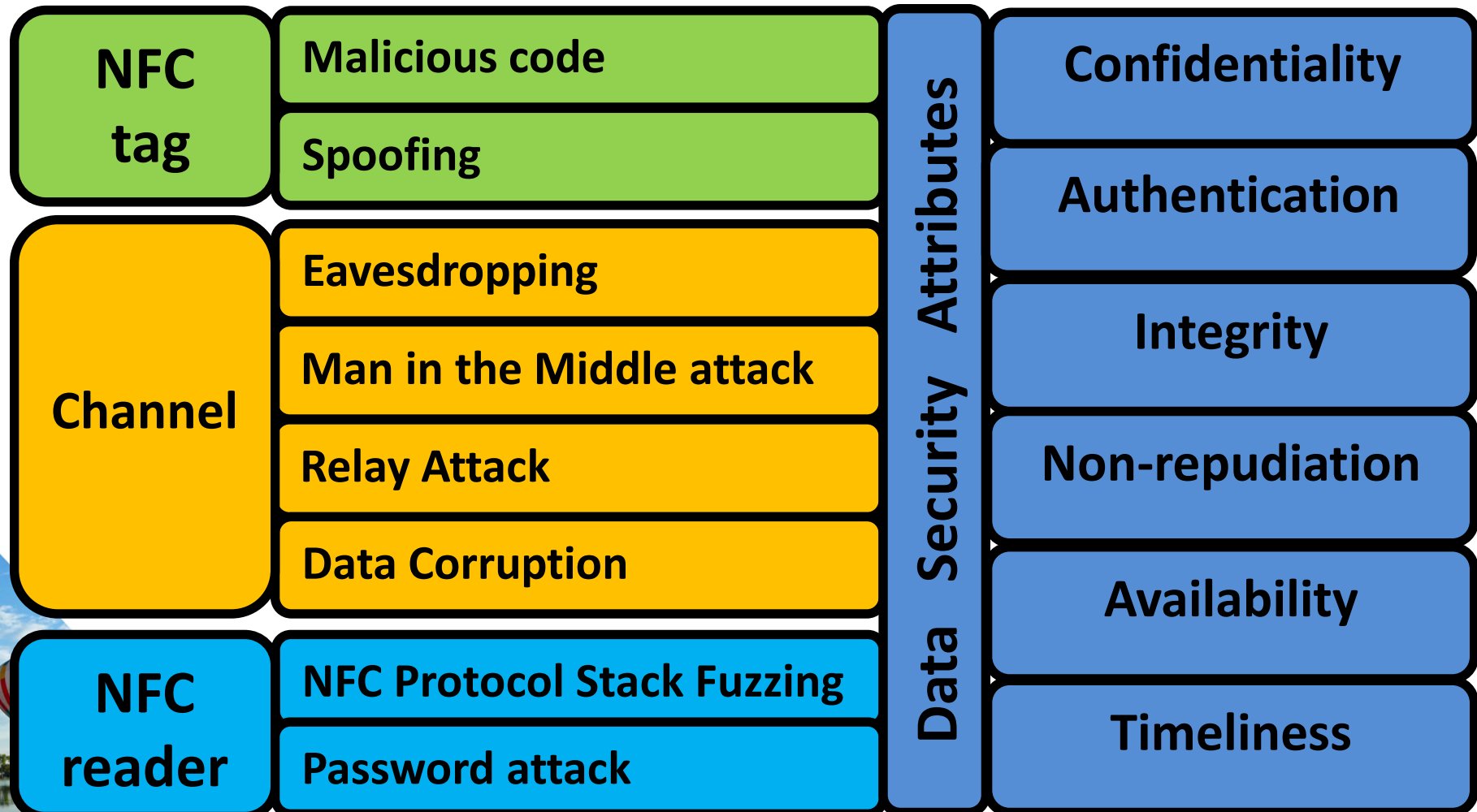
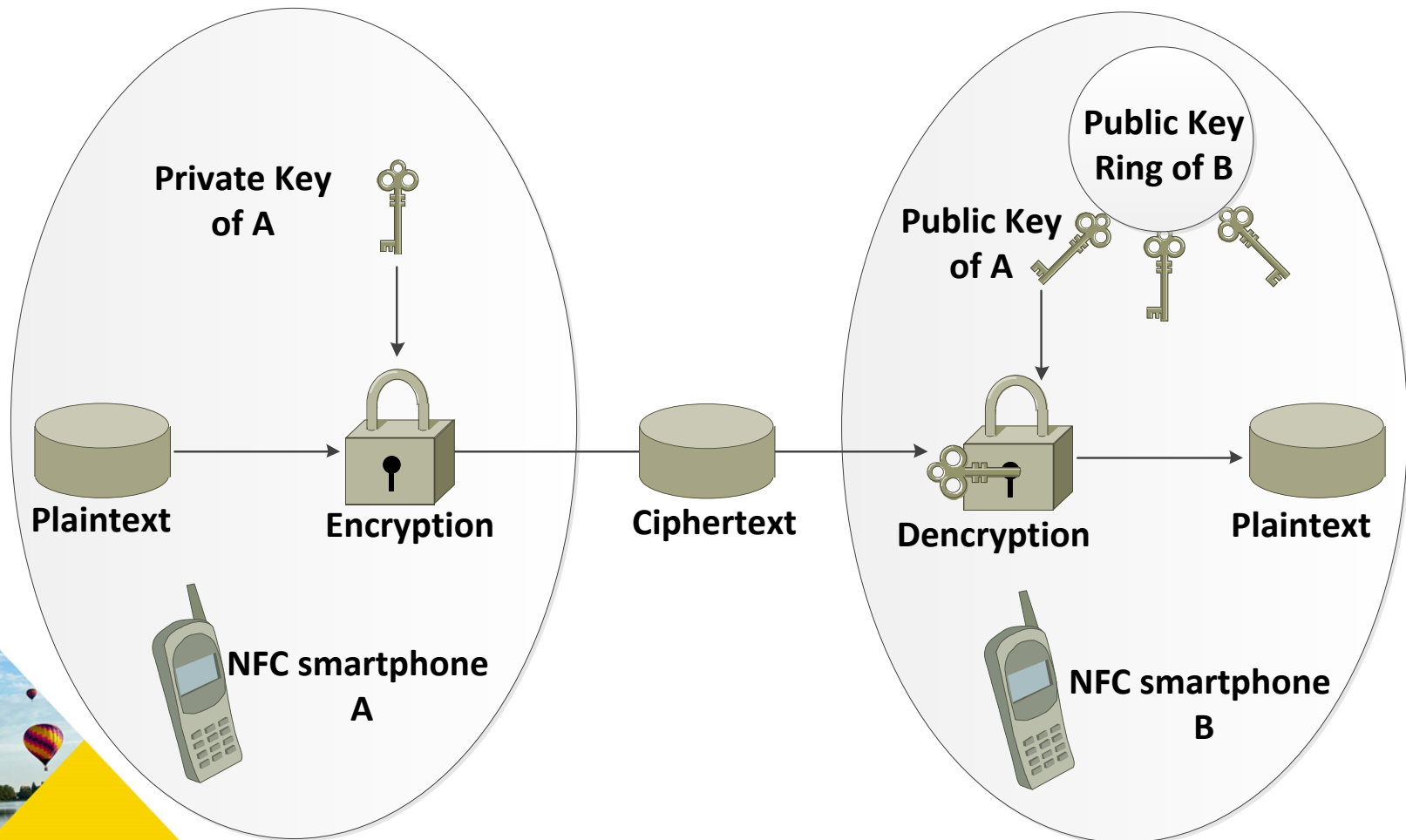Target

Security Problems

Security Problems

NFC tag	Malicious code		Confidentiality
	Spoofing		Authentication
Channel	Eavesdropping		
	Man in the Middle attack		Integrity
	Relay Attack	Data Security Attributes	Non-repudiation
	Data Corruption		Availability
NFC reader	NFC Protocol Stack Fuzzing		Timeliness
	Password attack		

Corresponding Measures

Data Security Attributes		
	Confidentiality	Data Encryption
	Authentication	Digital Signature
	Integrity	
	Non-repudiation	
	Availability	Malevolence Detection
	Timeliness	Monitoring of RF

Encryption Process
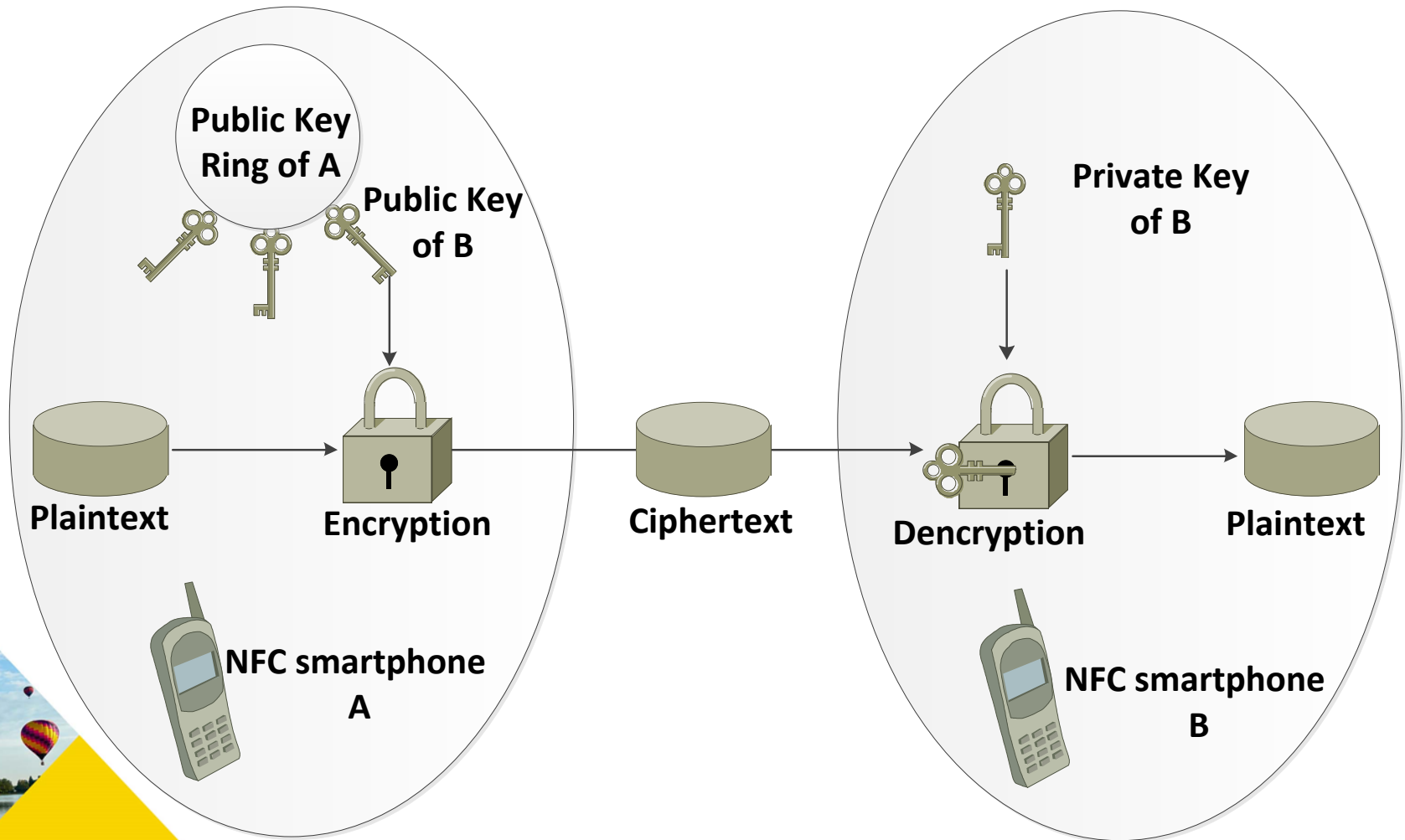
Digital Signature Process

THANK YOU!

gxbbest@126.com