EAVESDROPPING ONE-TIME TOKENS OVER MAGNETIC SECURE TRANSMISSION IN SAMSUNG PAY

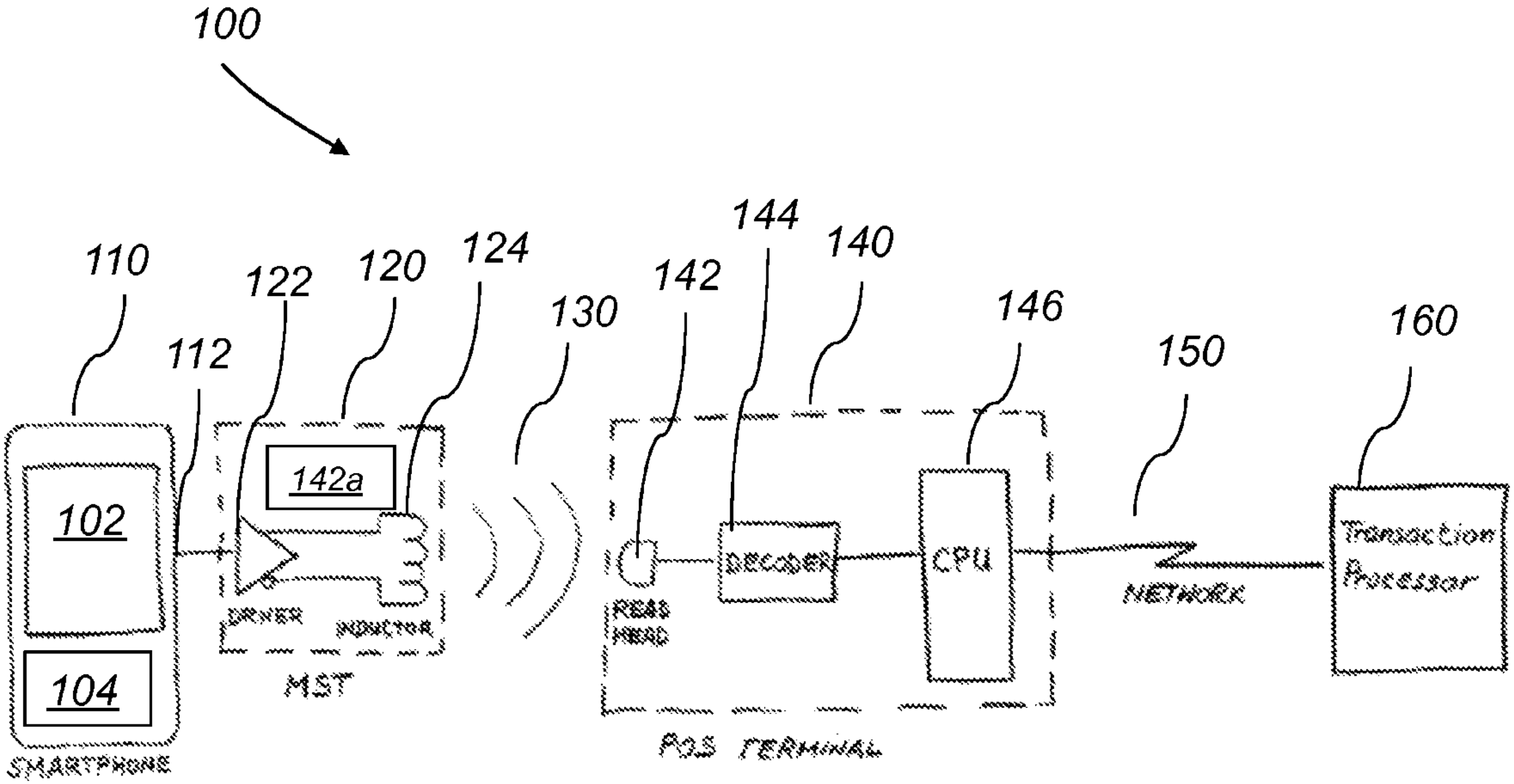
DAESEON CHOI, KONGJU NATIONAL UNIV.
YOUNHO LEE, SEOULTECH

국립공주대학교
KONGJU NATIONAL UNIVERSITY

서울과학기술대학교
1910
SEOUL NATIONAL UNIV. OF SCIENCE & TECHNOLOGY

MAGNETIC SECURE TRANSMITTION BY LOOPPAY

- US Patent 8628012



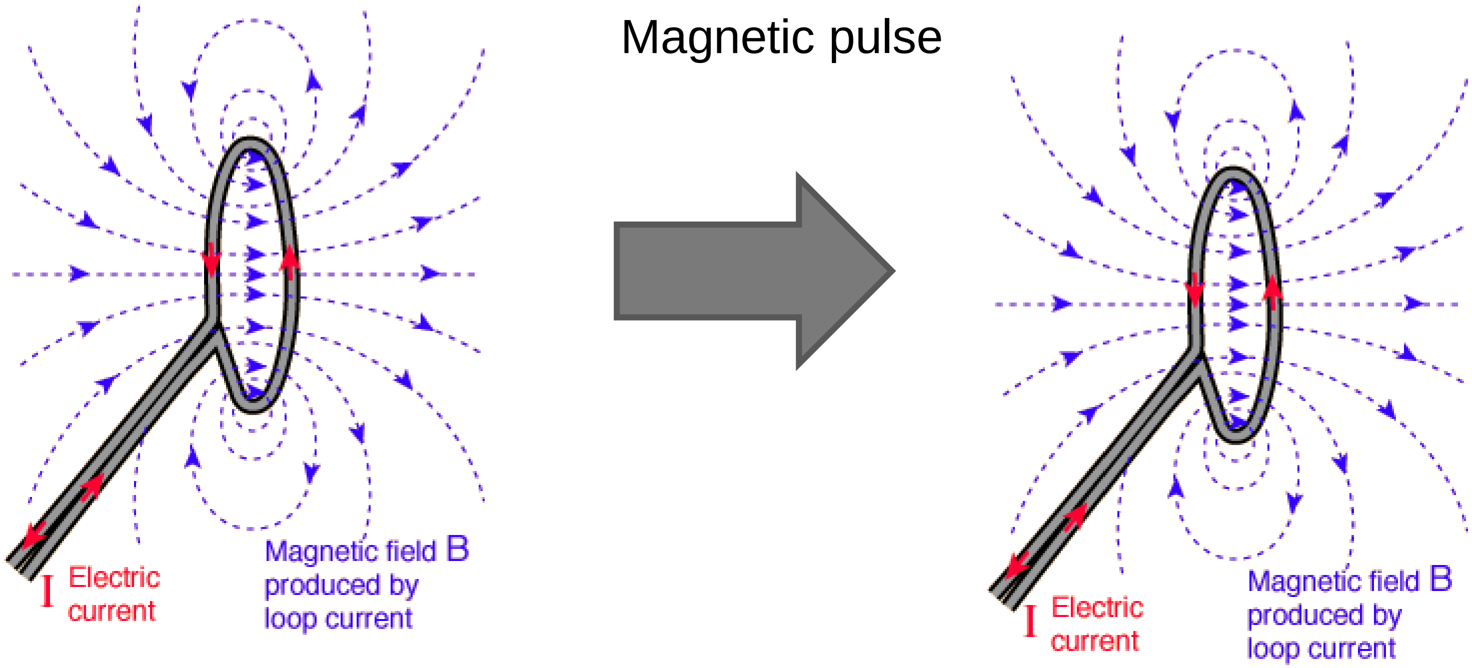
MST (CONT)

- Emitting magnetic pulse

Coil in the smartphone’s device

Coil in the card reader head

Magnetic pulse


I
Electric current
Magnetic field B produced by loop current
I
Electric current
Magnetic field B produced by loop current

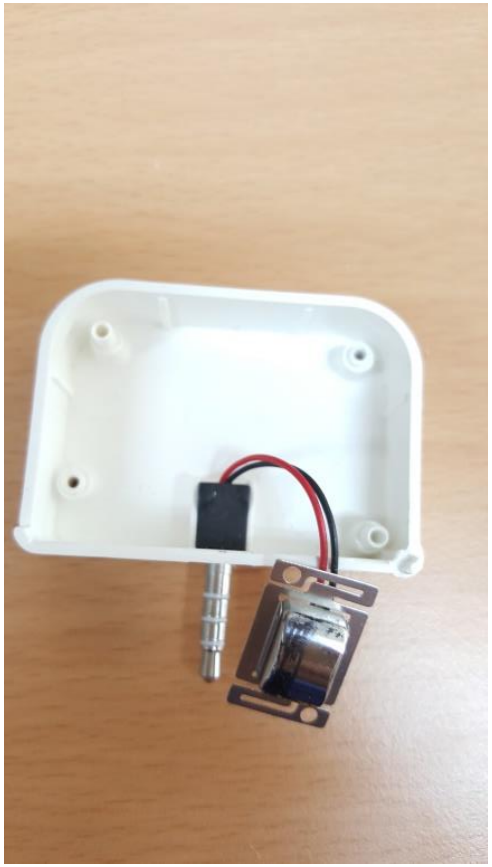
Source : http://hyperphysics.phy-astr.gsu.edu/hbase/magnetic/curloo.html

LOOPPAY CLAIMS

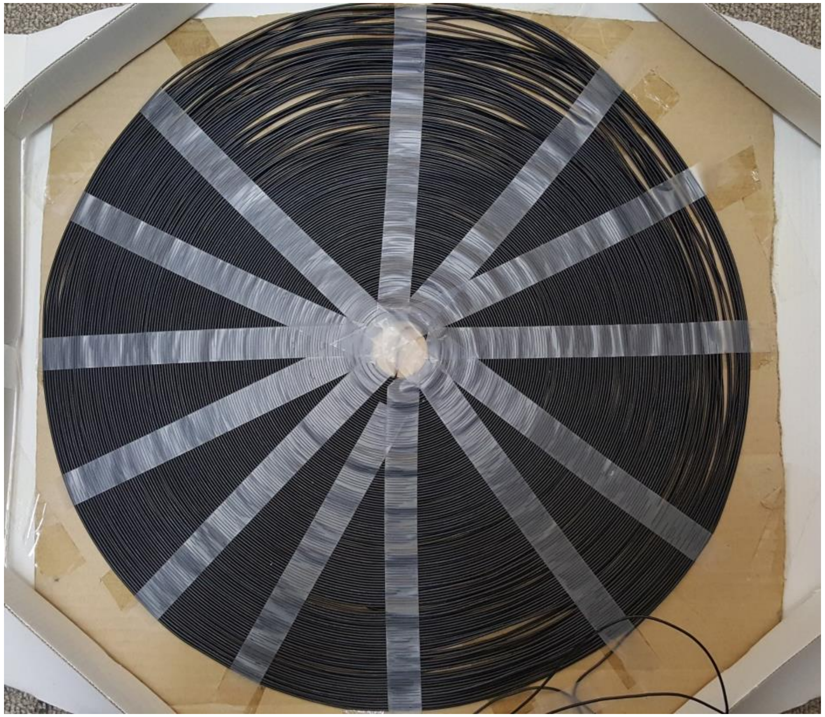
- The transmission between a LoopPay-enabled device and the POS reader must be activated by the user, it only lasts for a few milliseconds and can only be done over a very short distance (1 to 4 inches).
  - https://www.looppay.com/faqs/

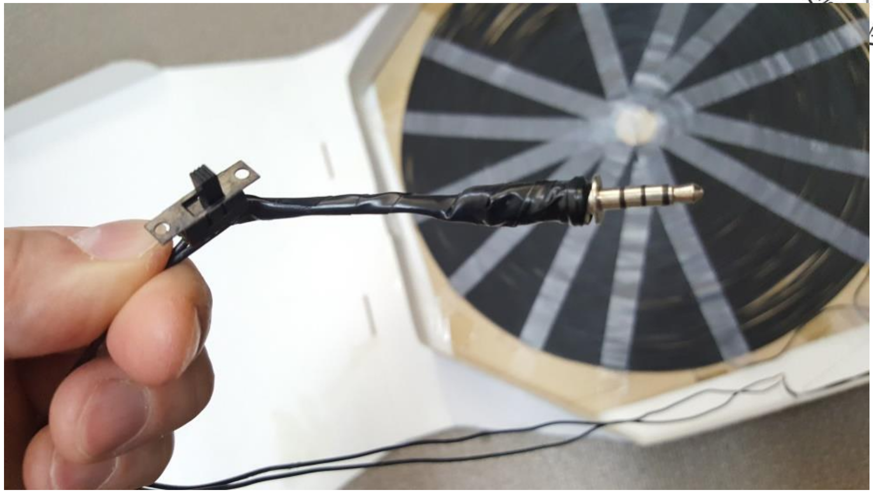
ARE THEY RIGHT?

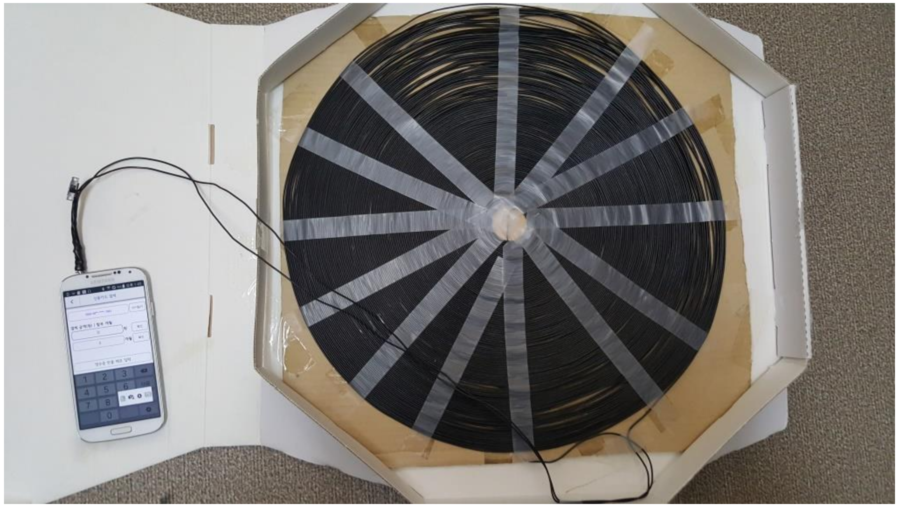
MOBILE CARD READER STRUCTURE



WHAT IF THE COIL IS BIG?

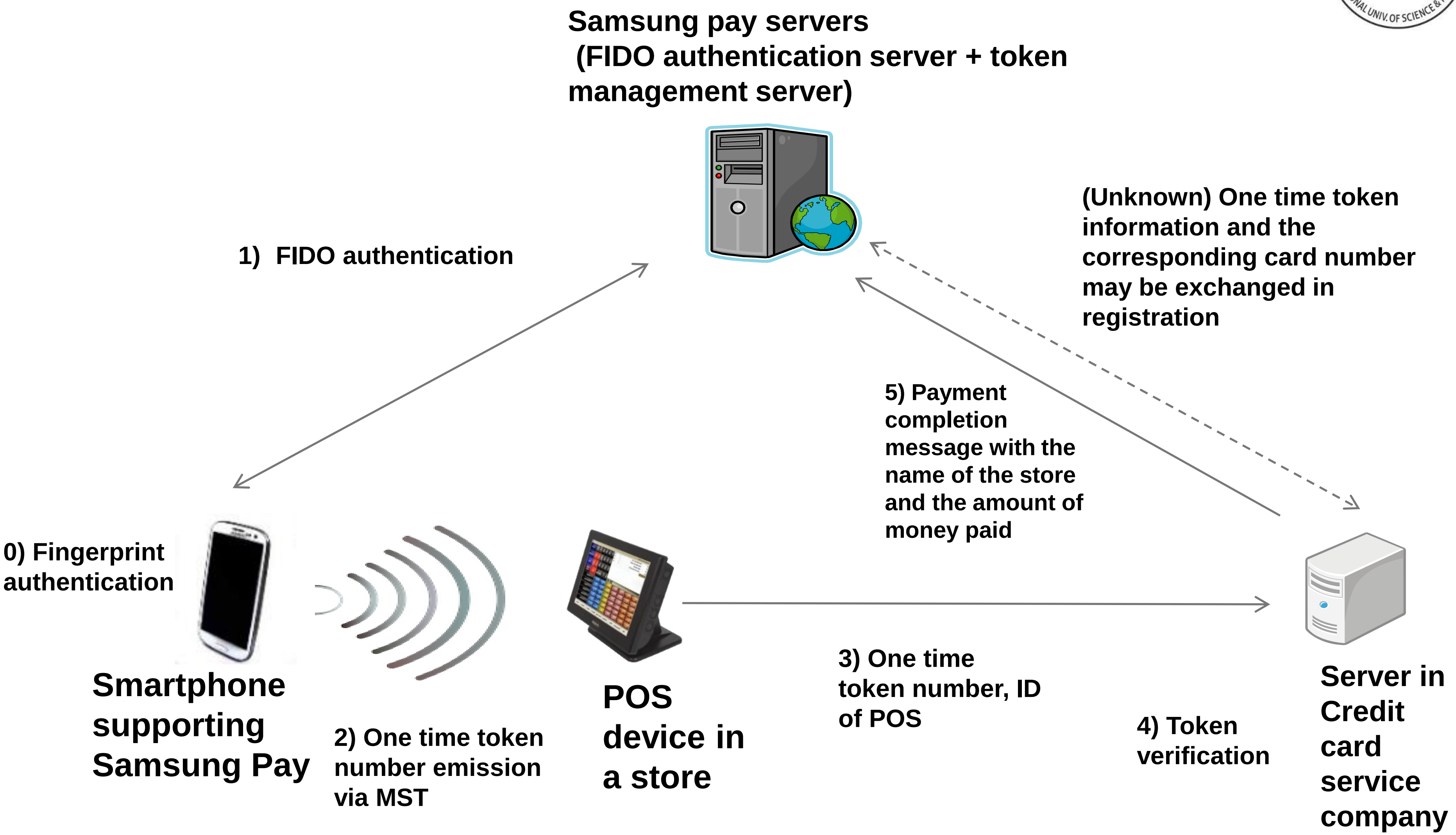






HOW FAR: 1.5M

SAMSUNG PAY SERVICE ARCHITECTURE



Samsung pay servers
(FIDO authentication server + token management server)

1) FIDO authentication

(Unknown) One time token information and the corresponding card number may be exchanged in registration

5) Payment completion message with the name of the store and the amount of money paid

0) Fingerprint authentication

Smartphone supporting Samsung Pay

2) One time token number emission via MST

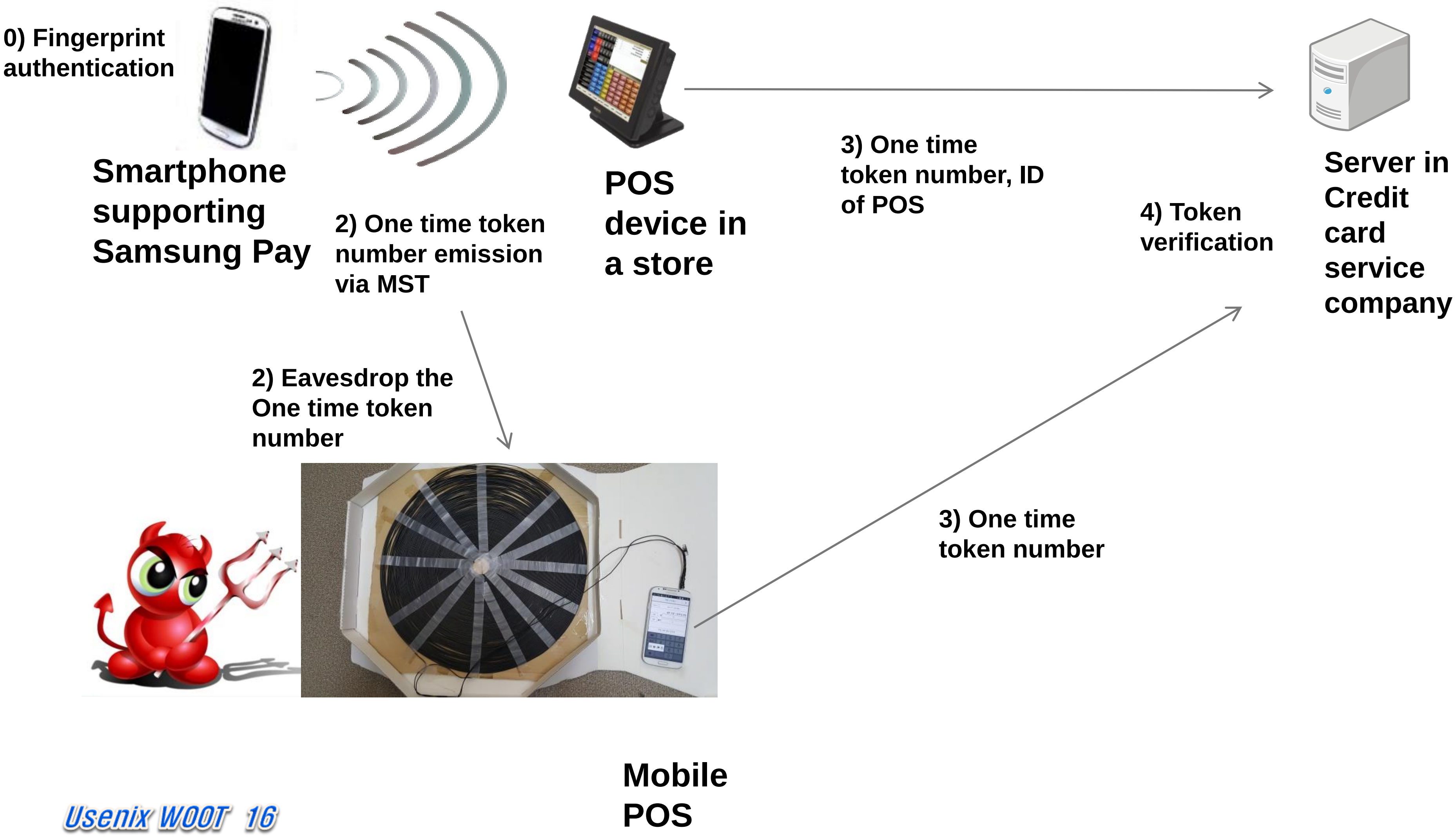
POS device in a store

3) One time token number, ID of POS

4) Token verification

Server in Credit card service company

PROPOSED ATTACK TYPE 1



0) Fingerprint authentication

Smartphone supporting Samsung Pay

2) One time token number emission via MST

POS device in a store

3) One time token number, ID of POS

4) Token verification

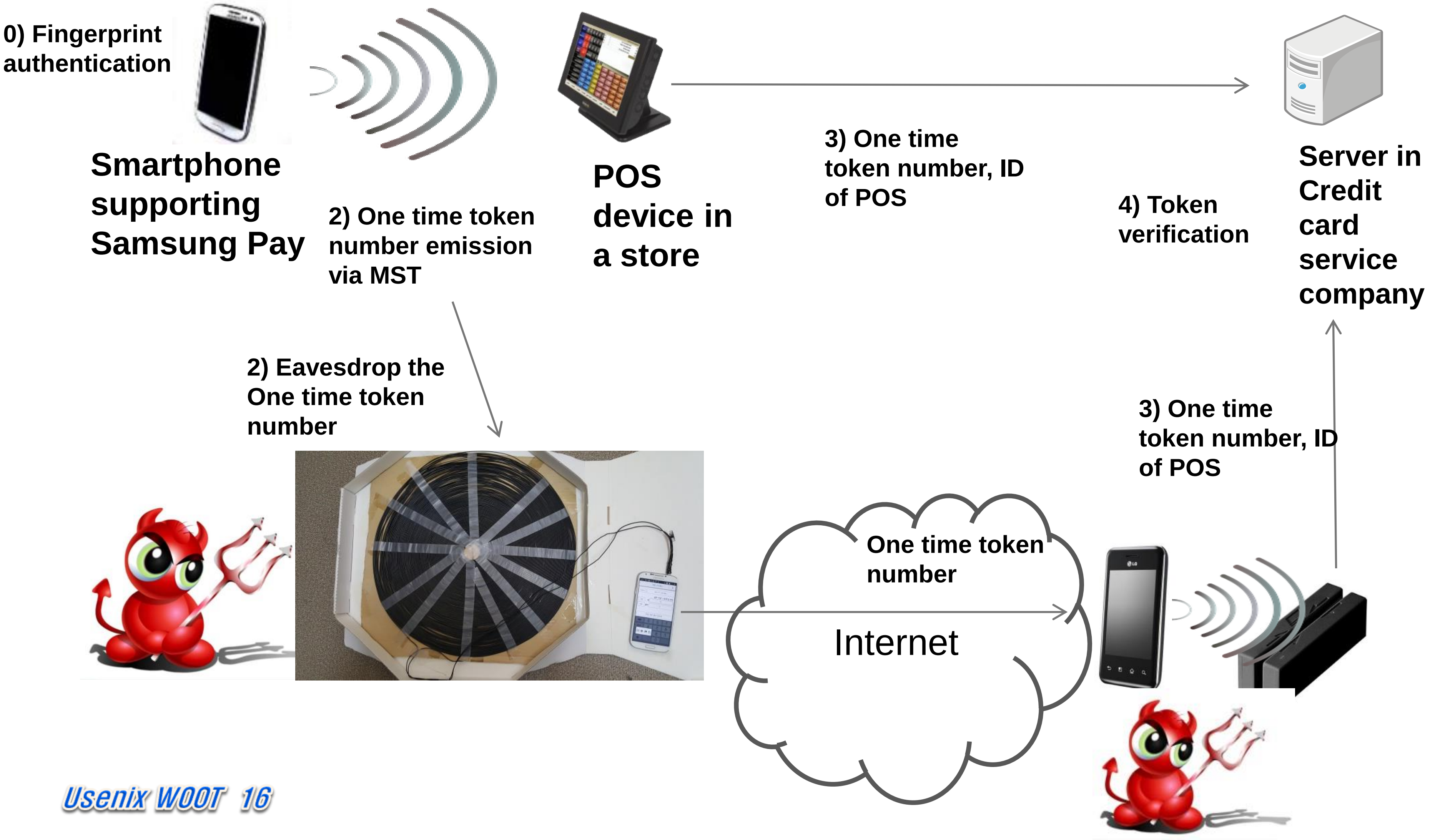
Server in Credit card service company

2) Eavesdrop the One time token number

3) One time token number

Mobile POS

PROPOSED ATTACK TYPE 2



0) Fingerprint authentication

Smartphone supporting Samsung Pay

2) One time token number emission via MST

POS device in a store

3) One time token number, ID of POS

4) Token verification

Server in Credit card service company

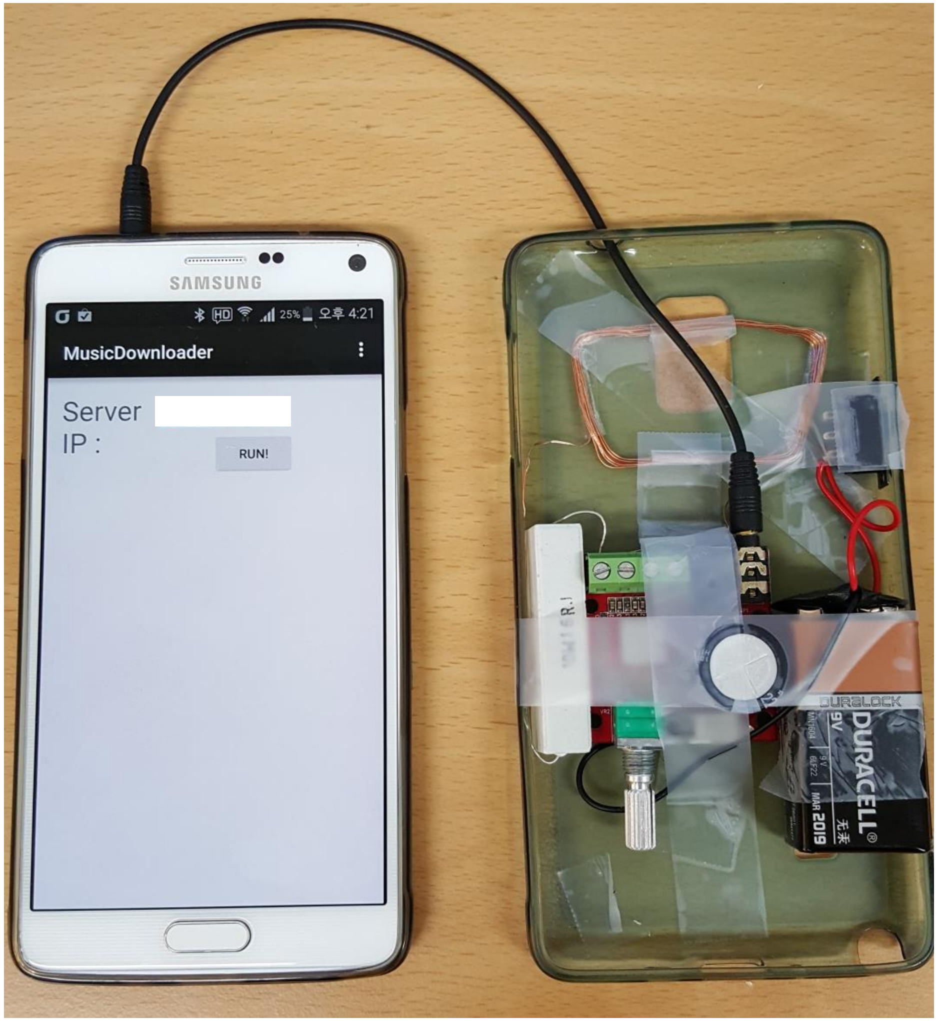
2) Eavesdrop the One time token number

One time token number

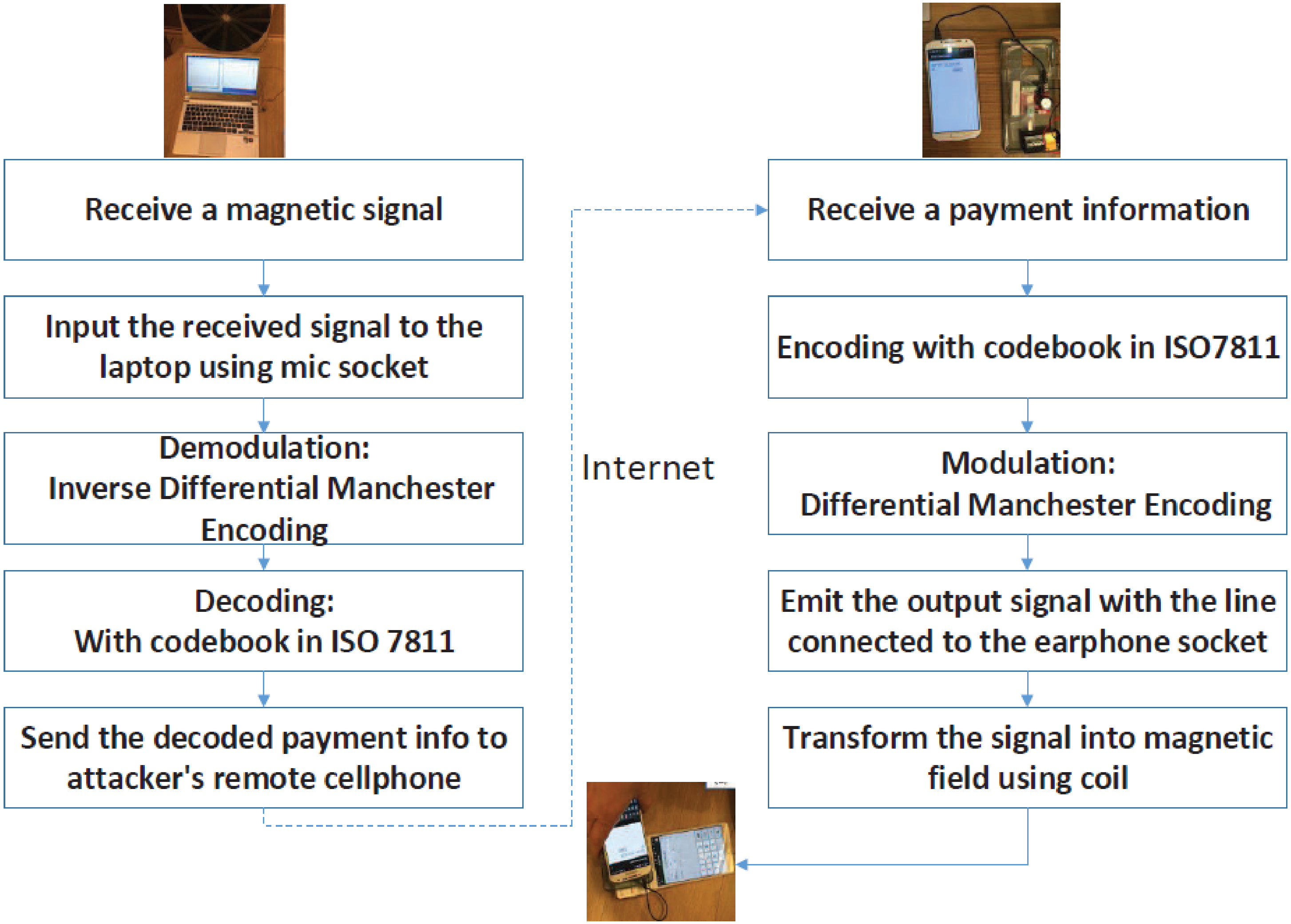
Internet

3) One time token number, ID of POS

FOR ATTACK PAYMENT



TYPE 2 ATTACK SYSTEM STRUCTURE



Receive a magnetic signal

Input the received signal to the laptop using mic socket

Demodulation:
Inverse Differential Manchester Encoding

Decoding:
With codebook in ISO 7811

Send the decoded payment info to attacker's remote cellphone

Internet

Receive a payment information

Encoding with codebook in ISO7811

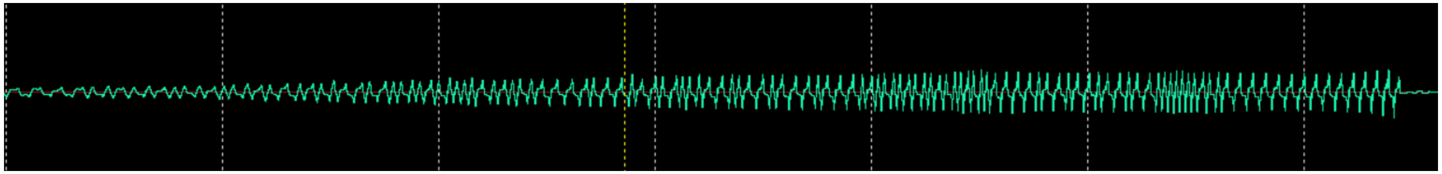
Modulation:
Differential Manchester Encoding

Emit the output signal with the line connected to the earphone socket

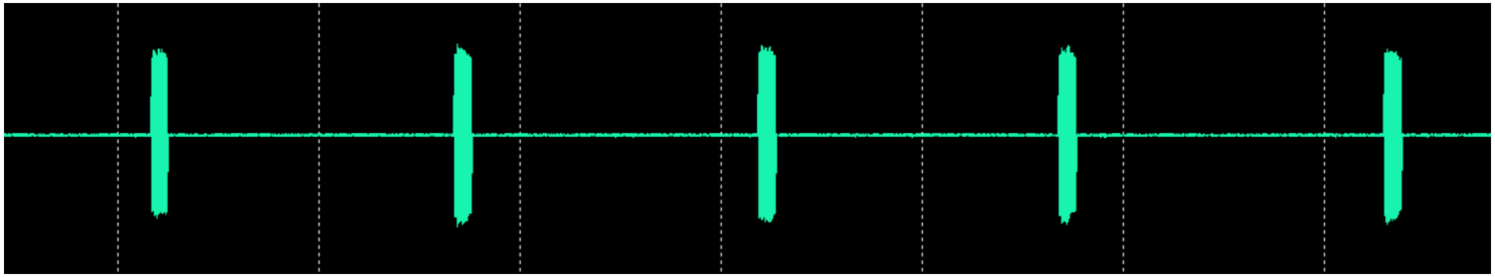
Transform the signal into magnetic field using coil

CAPTURED SIGNAL

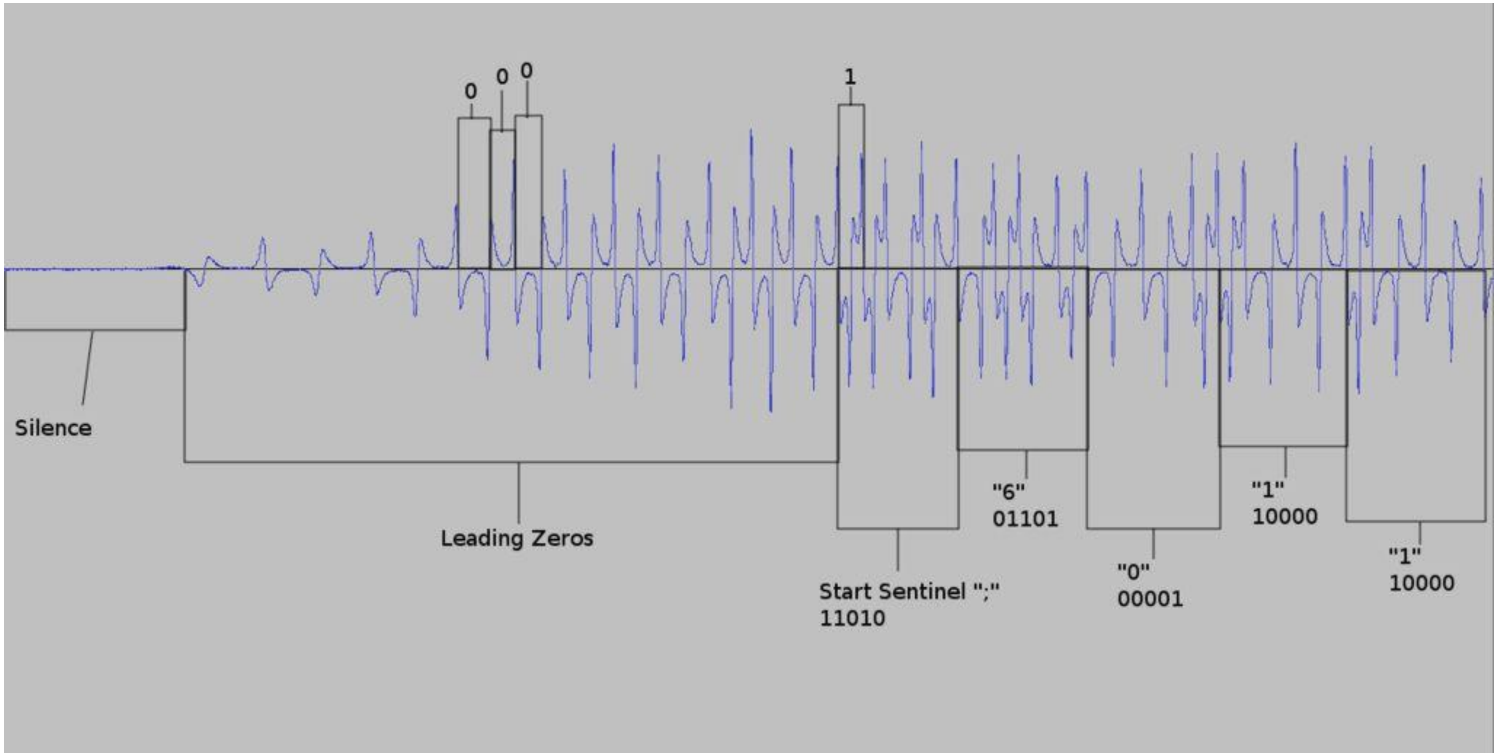
- Sound of magnetic strip card



- Sound of Samsung pay



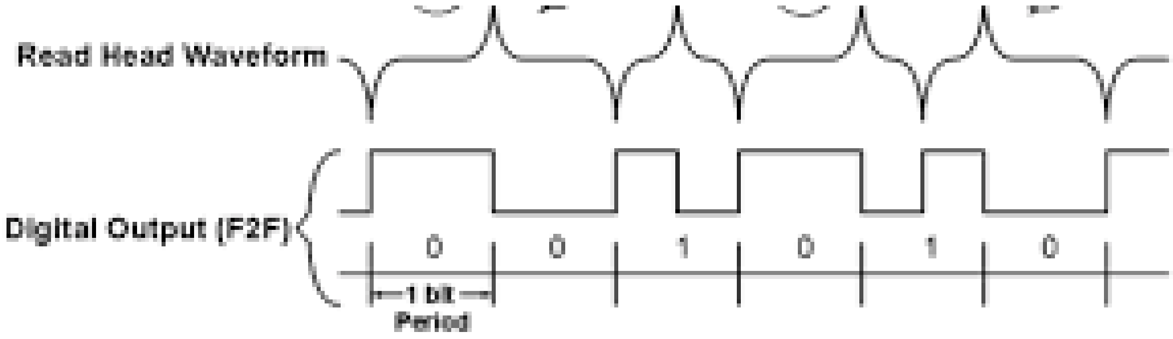
THE SOUND CONSISTS OF



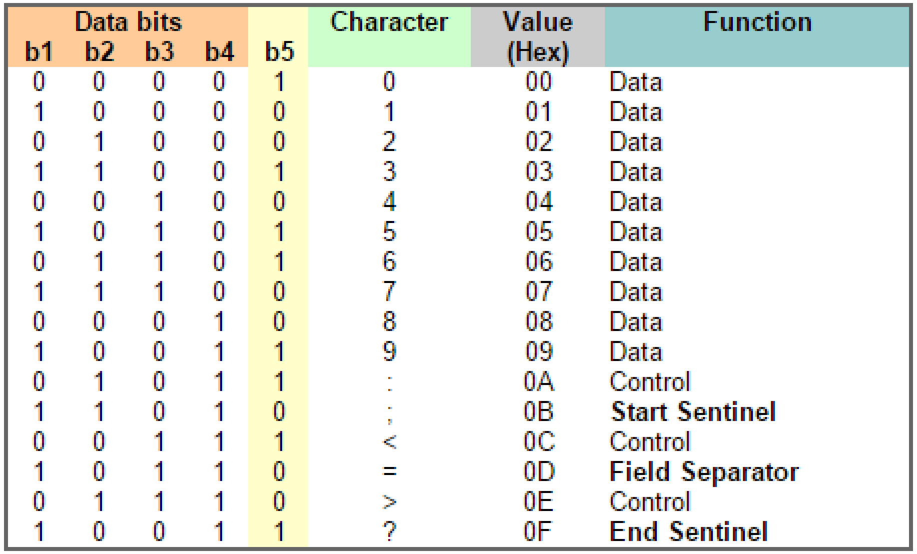
Source : http://jetruby.com/expertise/magnetic-stripe-reading/

DECODING RULE

- Binary

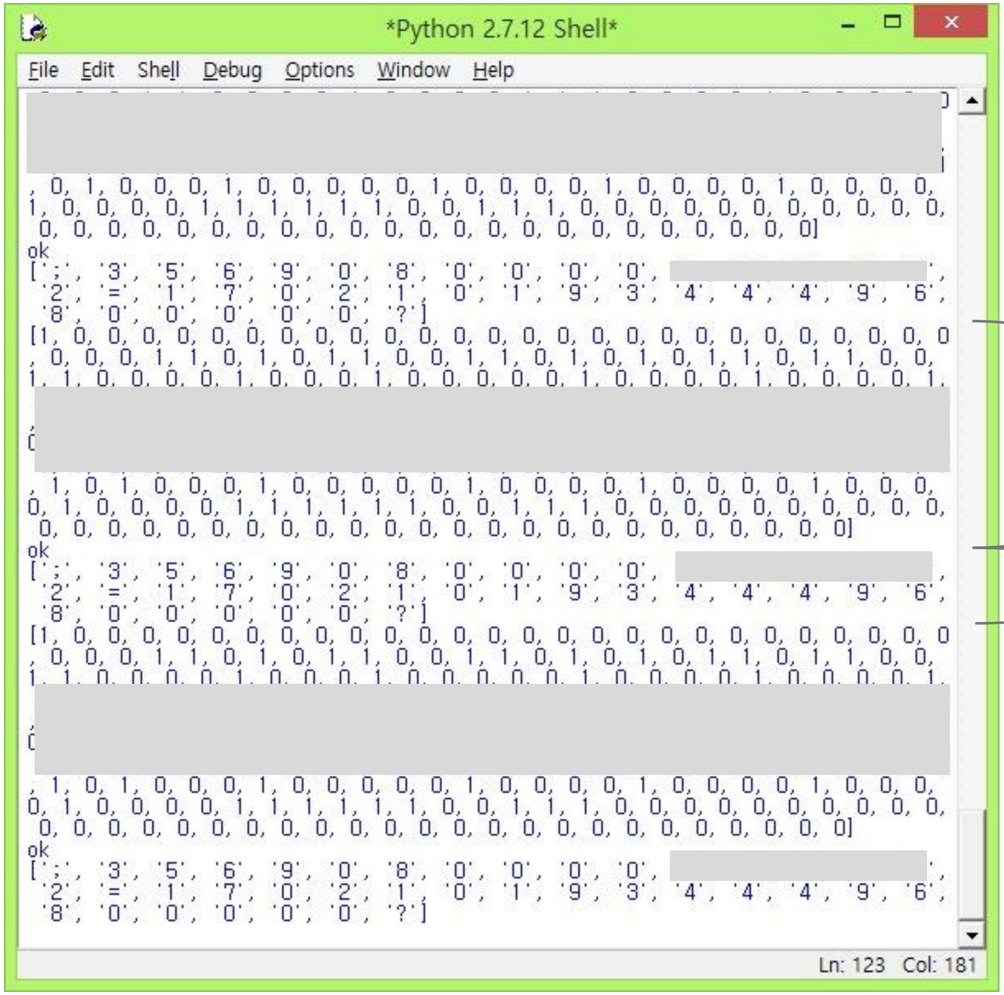


- Digits



Data bits					Character	Value	Function
b1	b2	b3	b4	b5		(Hex)	
0	0	0	0	1	0	00	Data
1	0	0	0	0	1	01	Data
0	1	0	0	0	2	02	Data
1	1	0	0	1	3	03	Data
0	0	1	0	0	4	04	Data
1	0	1	0	1	5	05	Data
0	1	1	0	1	6	06	Data
1	1	1	0	0	7	07	Data
0	0	0	1	0	8	08	Data
1	0	0	1	1	9	09	Data
0	1	0	1	1	:	0A	Control
1	1	0	1	0	;	0B	**Start Sentinel**
0	0	1	1	1	<	0C	Control
1	0	1	1	0	=	0D	**Field Separator**
0	1	1	1	0	>	0E	Control
1	0	0	1	1	?	0F	**End Sentinel**

DECODING RESULT

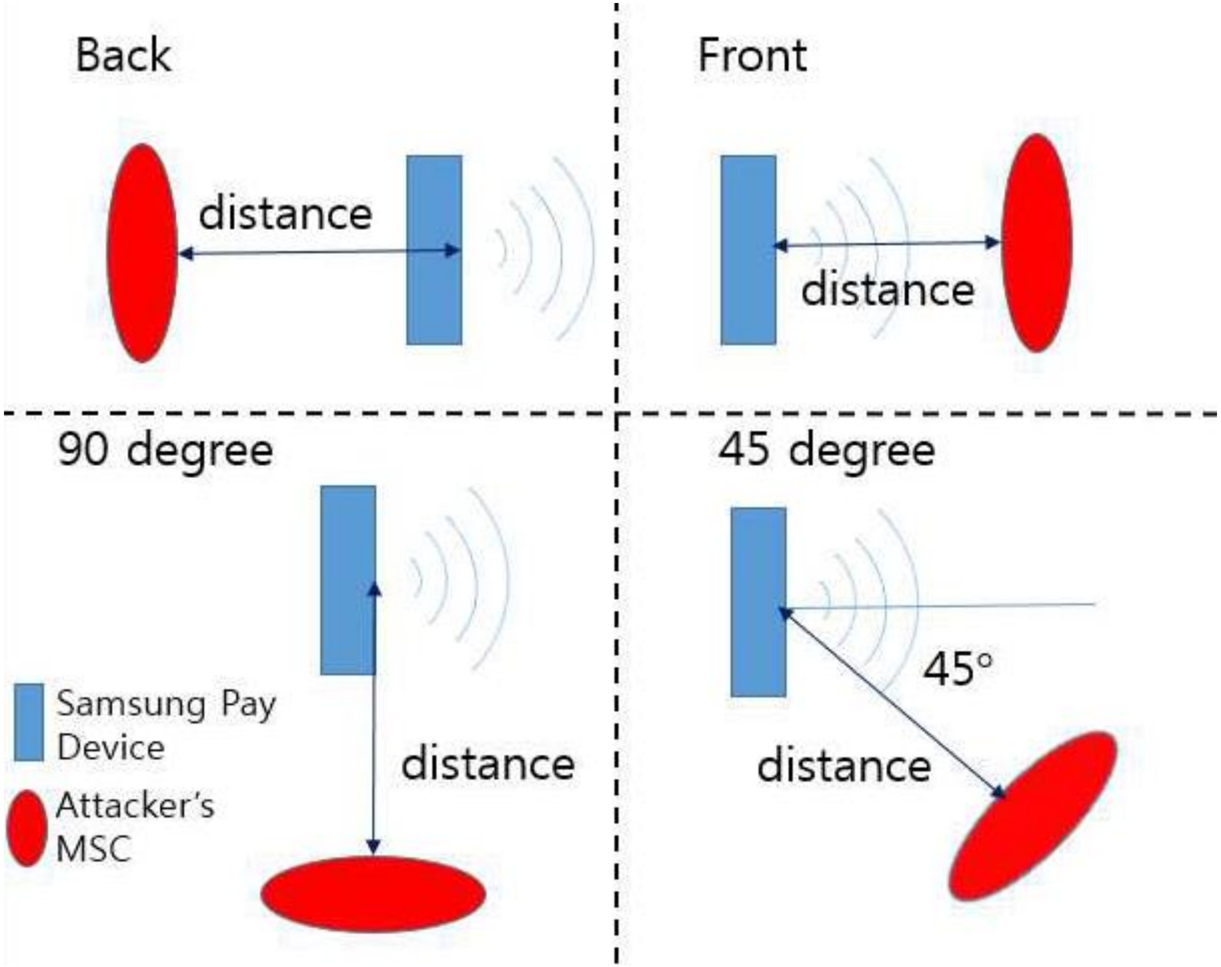


```
[redacted]
, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0,
1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
ok
[';', '3', '5', '6', '9', '0', '8', '0', '0', '0', '0', [redacted]',
 '2', '=', '1', '7', '0', '2', '1', '0', '1', '9', '3', '4', '4', '4', '9', '6',
 '8', '0', '0', '0', '0', '0', '?']
[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0,
1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1,
[redacted]
, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0,
0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
ok
[';', '3', '5', '6', '9', '0', '8', '0', '0', '0', '0', [redacted],
 '2', '=', '1', '7', '0', '2', '1', '0', '1', '9', '3', '4', '4', '4', '9', '6',
 '8', '0', '0', '0', '0', '0', '?']
[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0,
1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1,
[redacted]
, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0,
0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
ok
[';', '3', '5', '6', '9', '0', '8', '0', '0', '0', '0', [redacted]',
 '2', '=', '1', '7', '0', '2', '1', '0', '1', '9', '3', '4', '4', '4', '9', '6',
 '8', '0', '0', '0', '0', '0', '?']
```

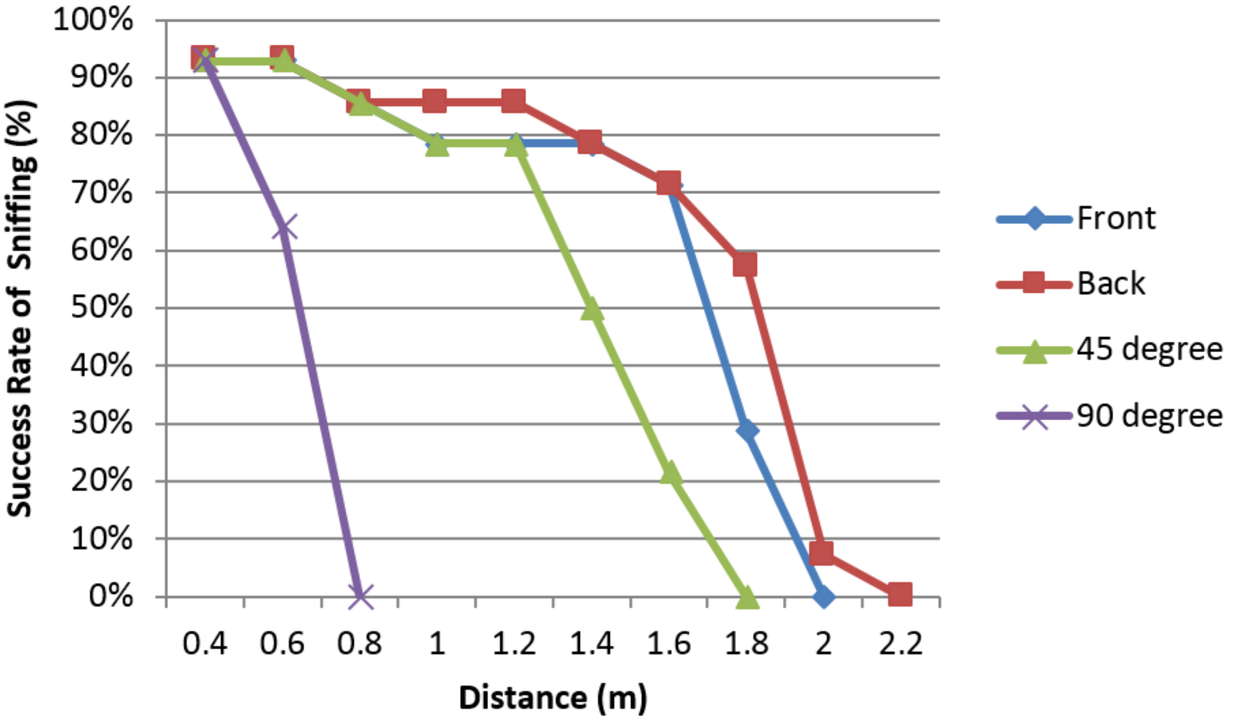
Demodulated binary

Decoded digits

IN VARIOUS SITUATIONS

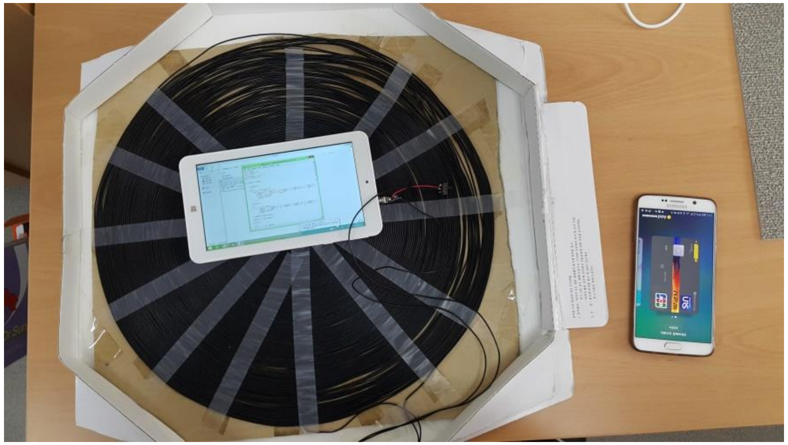


THE RESULTS ARE



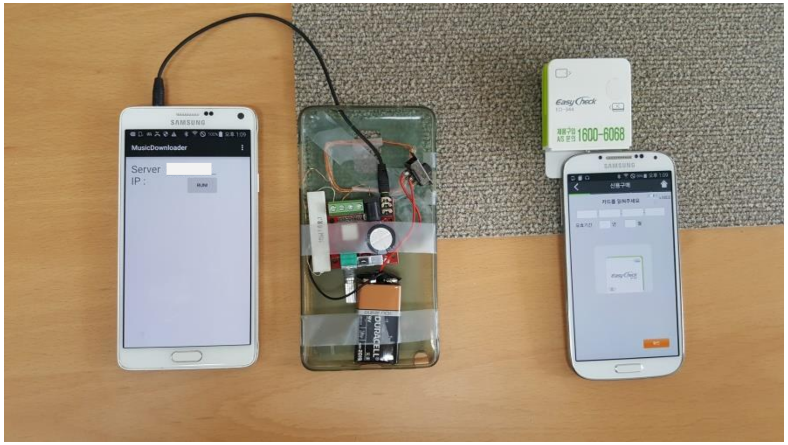
IN LAB : TYPE 1 ATTACK

Send
Sniffed token
Via Internet



<eavesdropper
Device
: sniff Samsung
Pay token>

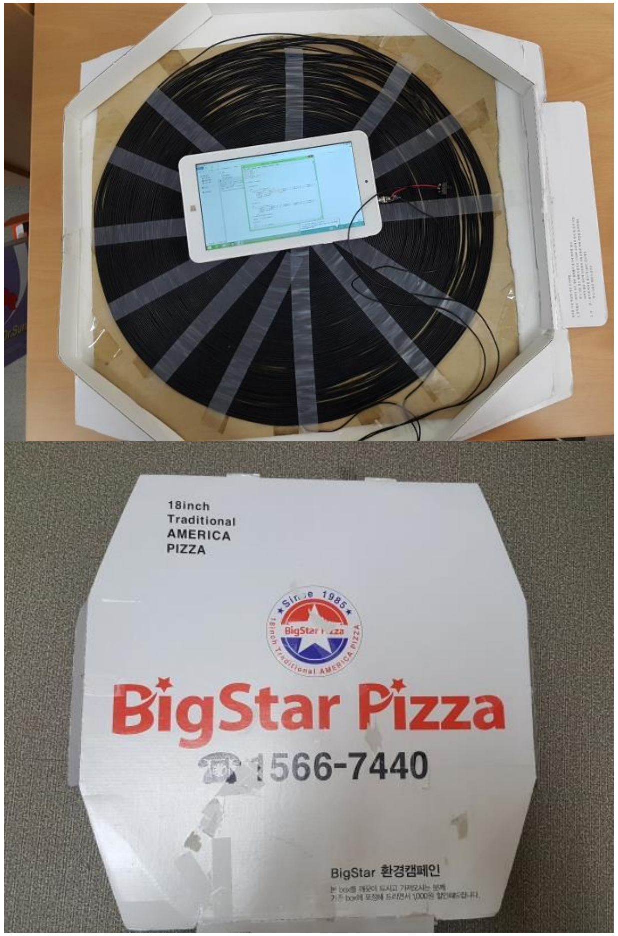
<victim's
smartphone>



<attack payer's
Device
: emit MST of
Sniffed token>

<mobile pos>

REAL WORLD : TYPE2 ATTACK



DEMO

- Sniffing Samsung pay token in 1.8m away

  https://youtu.be/6Nfyy92Go_M

- In lab, type1 attack

  https://youtu.be/NUvW_D4NA_s

- Real time wormhole attack of Samsung pay

  https://youtu.be/7VsHbrtPs0c