## **mQRCode**: Secure QR Code Using Nonlinearity of Spatial Frequency in Light

Hao Pan<sup>\*</sup>, Yi-Chao Chen<sup>\*</sup>, Lanqing Yang<sup>\*</sup>, Guangtao Xue<sup>\*</sup>, Chuang-Wen You<sup>^</sup>, Xiaoyu Ji<sup>†</sup>

\*Shanghai Jiao Tong University, ^National Taiwan University, †Zhejiang University



## Outline

#### Motivation

Basic Idea Spatial Frequency Encryption Scheme Against Attacks Evaluation Conclusion

## **QR** Code

#### Quick Response Code: a near-field comm method.

- Rapid readability for any handheld device with a camera.
- Applications: retail, transportation, advertisement, social contact, gaming, access controlling, and etc.



#### **Social E-cards**



#### **Mobile Payment**



#### **Electronic Tickets**



#### **Access Control**



### Motivation

#### **QR** Code is Popular



# > 3100 Brillion USD viaQR Code Payment in 2016.



it consultis

### Motivation

#### QR Code is **INSECURE**

**[USENIX Security'17]** Picking Up My Tab: Understanding and Mitigating Synchronized Token Lifting and Spending in Mobile Payment.



**[NEWs'19]** QR code scams rise in China, putting e-payment security in spotlight. https://www.jianshu.com/p/b9657161933a



**Replay Attack** in a Mobile Payment Scenario



#### **Replay Attack** in a Mobile Payment Scenario



#### Replay Attack in a Mobile Payment Scenario



|                              | 4 (B (B))      |   |
|------------------------------|----------------|---|
| 流水                           | 050            |   |
| - 1124-1-199<br>R<br>U) 181= | 10.0 × 2011共   |   |
| 29 M-                        | 井(変 × 900.00   | - |
| 被信用户<br>2010:51 网络科          | ¥ 900.00       |   |
| 1-23 同二                      | #1 1% × 900.00 |   |
| 微信用户<br>180227 段信            | ¥ 900.00       |   |

#### QR Code is insecure - why?





## Outline

#### Motivation

#### **Basic Idea**

Spatial Frequency Encryption Scheme Against Attacks Evaluation Conclusion

#### Can we reduce the range of attacks?





**Can we reduce the range of attacks?** 



#### **Design Principle:**

#### Impose the least cost to users (e.g., additional hardware or communication channels)



## Nonlinearity of Spatial Frequency



## Outline

#### Motivation Basic Idea **Spatial Frequency Encryption Scheme Against Attacks Evaluation Conclusion**

## **Spatial Frequency**

**†**2

#### What is Nonlinearity of Spatial Frequency?



- $= (a_1 + b_1 \cos 2\pi f_1 t) \times (a_2 + b_2 \cos 2\pi f_2 t)$
- $= a_1 a_2 + a_2 b_1 \cos 2\pi f_1 t + a_1 b_2 \cos 2\pi f_2 t +$

 $b_1 b_2 \cos 2\pi (f_1 + f_2)t + b_1 b_2 \cos 2\pi (f_1 - f_2)t$ 

### Observation

#### Spatial frequency is everywhere!



## mQRCode



## mQRCode



Color Filter Array



Pixel Array





Random pattern to human eyes.





Nonlinear interaction results in QR Code.

## Outline

#### Motivation Basic Idea Spatial Frequency Encryption Scheme Against Attacks Evaluation Conclusion

## **Encryption Scheme**



## **Encryption Scheme**



## **Encryption Scheme**



## Outline

Motivation Basic Idea Spatial Frequency Encryption Scheme Against Attacks Evaluation Conclusion





 $|f_1| \cong |f_2|$  $f_1 - f_2$  is evident



 $b_1 b_2 \cos 2\pi (f_1 - f_2) t$ 





| $\langle 0 \rangle$ |
|---------------------|
|                     |
|                     |

 $b_1 b_2 \cos 2\pi (f_1 - f_2) t$ 





## Example of mQRCode



QR Code

mQR Code

Photographs taken at the designated position Photographs taken at other positions

## Outline

Motivation Basic Idea Spatial Frequency Encryption Scheme Against Attacks Evaluation Conclusion

## **Evaluation: Cameras and Displays**

| Displays           | Cameras             |   |
|--------------------|---------------------|---|
| D0: iPhone 6       | C0: iPhone 6        |   |
| D1: iPhone 7Plus   | C1: iPhone 7Plus    | °€ 100 L  |
| D2: iPhone X       | C2: iPhone X        |   |
| D3: iPhone XS      | C3: iPhone XS       |   |
| D4: Huawei P20Pro  | C4: Huawei P20Pro   | ·탈 94   |
| D5: Samsung S7     | C5: Samsung S7      | <sup>6</sup> 92   |
| D6: Nexus 6P       | C6: Nexus 6P        |   |
| D7: Google Pixel 2 | C7: Google Pixel 2  | D <sub>3</sub> D <sub>5</sub>                                   |
| D8: DELL S2340M    | C8: Pi Camera (5MP) | $D_7 D_9 C C_4 C_5 C_4 C_5 C_5 C_5 C_5 C_5 C_5 C_5 C_5 C_5 C_5$ |
| D9: MacBookPro     | P9: Pi Camera (8MP) | 0012  |
| 2016               |                     |   |
|                    |                     |   |

### **Evaluation: Multi-Frame Decryption**



## Outline

Motivation Basic Idea Spatial Frequency Encryption Scheme Against Attacks Evaluation Conclusion

### Conclusion

**mQRCode** enables secure QR Code applications:

Novel visual encryption method using nonlinear interaction between camera and display.

No additional hardware.

No additional communication channel.

The same using behavior.



## **Demo of mQRCode**



## Backup

#### **Alipay System and STLS Attack**

System Overview Pinhole Imaging Model Decryption Scheme Evaluation (Supplement) Can mQRCode work with printed QR Code?

### **Alipay System and STLS Attack**



## Backup

### Alipay System and STLS Attack System Overview Pinhole Imaging Model Decryption Scheme Evaluation (Supplement) Can mQRCode work with printed QR Code?

### **System Overview**



## Backup

#### Alipay System and STLS Attack System Overview Pinhole Imaging Model Decryption Scheme Evaluation (Supplement) Can mQRCode work with printed QR Code?

## **Pinhole Imaging Model**



## Backup

## Alipay System and STLS Attack System Overview Pinhole Imaging Model Decryption Scheme

Evaluation (Supplement) Can mQRCode work with printed QR Code?

## **Decryption: Why not Black and White?**



## **Decryption: Why not Black and White?**



## **Decryption: Simulation-based Analysis**



1. Projecting display onto camera with distortion.



3. Image sensor values with Bayer CFA.



2. Distorted image overlap with Bayer CFA pattern.



## **Decryption: Challenges**



## **Decryption: Challenges**



## **Decryption: Multi-Frame Decryption Scheme**



## **Fast Decryption: Idea**









Original White Image Nonlinearity between camera and display

Original White/Blac k Image Nonlinearity between camera and display

## **Fast Decryption: Method**



## Backup

## Alipay System and STLS Attack System Overview Pinhole Imaging Model Decryption Scheme

#### **Evaluation (Supplement)**

Can mQRCode work with printed QR Code?

#### Evaluation: Number of Frames for Decryption



### **Evaluation: Fast Decryption**



## **Evaluation: Lighting Conditions**

#### Environments

LA: Outdoor at 8 A.M. LB: Outdoor at 12 P.M. LC: Outdoor at 11 P.M. LD: Outdoor in a cloudy day LE: Office LF: Office with all

light off





#### (a) Multi-frame decryption.

(b) Fast decryption.

### **Evaluation: Cameras and Displays**

| Displays  | Cameras  |
|---|--|
| D0: iPhone 6  | C0: iPhone 6   |
| D1: iPhone 7Plus  | C1: iPhone 7Plus   |
| D2: iPhone X  | C2: iPhone X   |
| D3: iPhone XS   | C3: iPhone XS  |
| D4: Huawei P20Pro   | C4: Huawei P20Pro  |
| D5: Samsung S7  | C5: Samsung S7   |
| D6: Nexus 6P  | C6: Nexus 6P   |
| D7: Google Pixel 2  | C7: Google Pixel 2   |
| D8: DELL S2340M   | C8: Pi Camera (5MP)  |
| D9: MacBookPro  | P9: Pi Camera (8MP)  |
| 2016  |  |
| <ul> <li>1: iPhone 7Plus</li> <li>2: iPhone X</li> <li>3: iPhone XS</li> <li>4: Huawei P20Pro</li> <li>5: Samsung S7</li> <li>6: Nexus 6P</li> <li>7: Google Pixel 2</li> <li>8: DELL S2340M</li> <li>9: MacBookPro<br/>2016</li> </ul> | C1: iPhone 7Plus<br>C2: iPhone X<br>C3: iPhone XS<br>C4: Huawei P20Pro<br>C5: Samsung S7<br>C6: Nexus 6P<br>C7: Google Pixel 2<br>C8: Pi Camera (5MP)<br>P9: Pi Camera (8MP) |



Multiastabeenpeticyption

## Backup

Alipay System and STLS Attack System Overview Pinhole Imaging Model Decryption Scheme Evaluation (Supplement) Can mQRCode work on printed QR Code?

## Can mQRCode work on printed QR Code?



Display







