

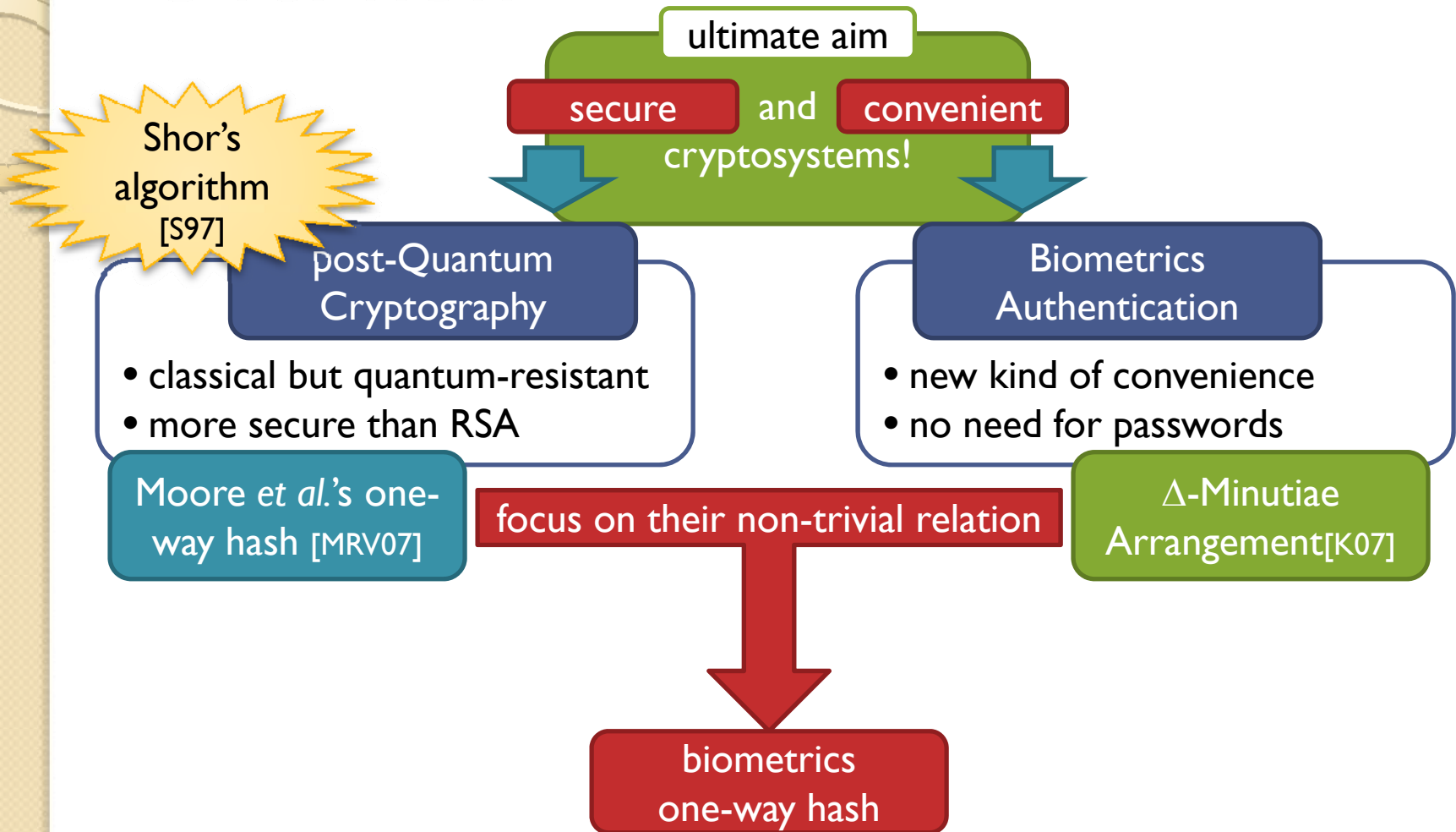


# **Biometrics Hash Functions against Quantum Adversaries**

**Koji Kojima**

Graduate School of Information Science and Technology, The University of Tokyo  
Quantum Computation and Information Project, ERATO-SORST, JST

# Overview



[S97] Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer"

[MRV07] Moore, Russell, Vazirani, "A classical one-way function to confound quantum adversaries"

[K07] Kojima, "Zero-Knowledge Proofs Considering Error for Secure Fingerprint Authentication"



# **BACKGROUND**

# post-Quantum Cryptography

solved by Shor's algorithm[S97]

randomly selected instances are difficult?

	Worst-case hardness	Average-case hardness	Simple structure
Factorization, Logarithm	×	×	⊙
Graph isomorphism	○	×	△
Inversion of Moore et al.'s hash[MRV07]	○	○	○

interesting!

[S97] Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer"

[MRV07] Moore, Russell, Vazirani, "A classical one-way function to confound quantum adversaries"

[K07] Kojima, "Zero-Knowledge Proofs Considering Error for Secure Fingerprint Authentication"

# Biometrics Authentications

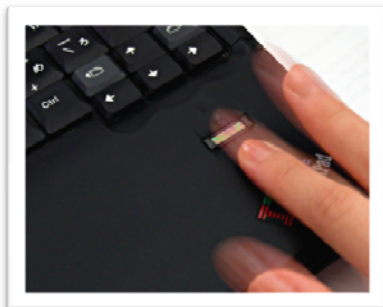
Use fingerprints, irises, and so on as keys

⊙ **Convenient for users**

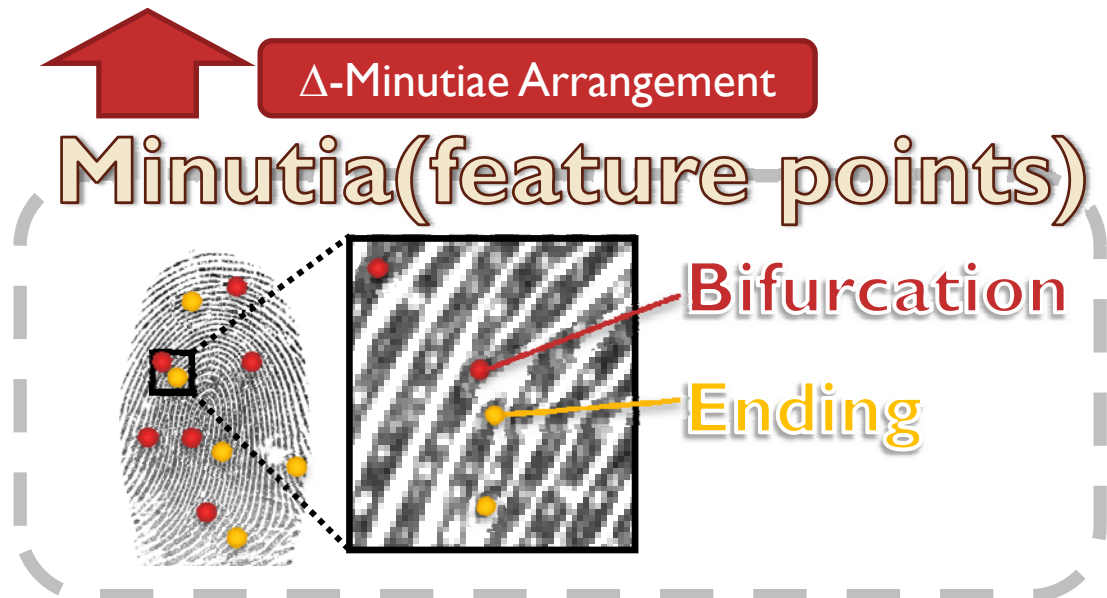
- no need to memorize complicated phrases

✓ **Noisy secret data**

- technical difficulties arise



fingerprint authentication





# **RESEARCHES**

# Our research

requirements for our biometrics hash

1. Quantum tolerant
2. Similarity-preserving

want to make hash functions useful for biometrics data

Quantum tolerant

Moore et al.'s one-way hash[MRV07]

$$f_V(M) = \{Mv \mid v \in V\},$$

where  $v \in \mathbb{F}_q^n$

Quantum tolerant and Similarity-preserving

biometrics one-way hash function

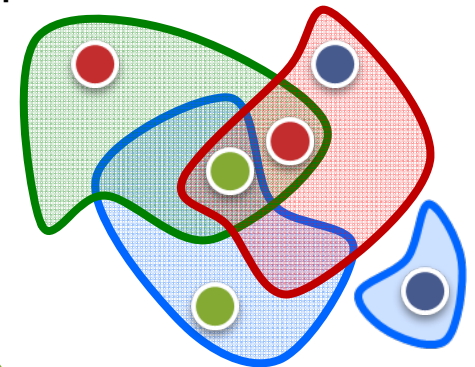
$$f_V(M) = \{Mv \mid v \in V\},$$

where  $v \in \{0,1\}^n$

Similarity-preserving

$\Delta$ -Minutiae Arrangement[K07]

Arrange 3 kinds of points under restrictions



[MRV07] Moore,Russell,Vazirani, "A classical one-way function to confound quantum adversaries"

[K07]Kojima, "Zero-Knowledge Proofs Considering Error for Secure Fingerprint Authentication"

# What is biometrics hash?

## Requirements

### 1. Quantum Tolerant

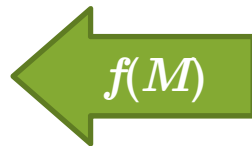
Getting  $N$  so that  $f(N) \approx f(M)$  from  $f(M)$

is difficult even by using quantum algorithm

### 2. Similarity Preserving

$$M' \approx M \Leftrightarrow f(M') \approx f(M)$$

## Registration



## Authentication

$f(M') \approx f(M)?$



# Moore *et al.*'s one-way hash<sub>[MRV07]</sub>

$$f_V(M) = \{Mv \mid v \in V\} \text{ (on finite field } \mathbb{F}_q)$$

e.g.)  $V := \left\{ \begin{pmatrix} 3 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 1 \end{pmatrix}, \begin{pmatrix} 5 \\ 2 \end{pmatrix} \right\}$  all operations are performed on finite field  $\mathbb{F}_7$

$$\begin{aligned} & \left\{ M \begin{pmatrix} 3 \\ 1 \end{pmatrix}, M \begin{pmatrix} 4 \\ 1 \end{pmatrix}, M \begin{pmatrix} 5 \\ 2 \end{pmatrix} \right\} \quad \Rightarrow \quad M := \begin{pmatrix} 2 & 5 \\ 6 & 3 \end{pmatrix} \\ = & \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 0 \end{pmatrix}, \begin{pmatrix} 6 \\ 6 \end{pmatrix} \right\} \end{aligned}$$

there are **3!** possible correspondences

More difficult than Graph Isomorphism

Moore *et al.*'s hash is Quantum Tolerant

[MRV07] Moore, Russell, Vazirani, "A classical one-way function to confound quantum adversaries"

●●● correspond to minutia in fingerprint authentication

# $\Delta$ -Minutiae Arrangement<sub>[K07]</sub>

Similar to Moore et al.'s hash

hidden correspondences

Similar point configurations satisfy Similar restrictions

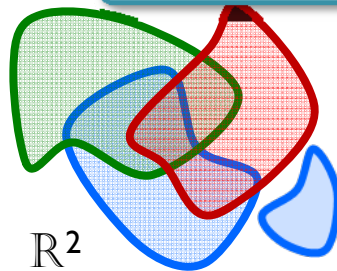
restriction about the points in region

e.g.)

- {2,2,0} ●●● s are in red region
- {2,1,1} ●●● s are in green region
- {2,1,1} ●●● s are in blue region

Q.

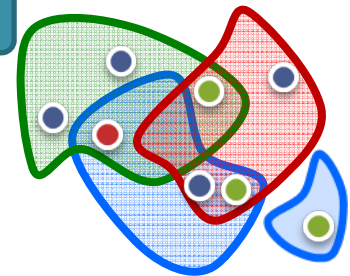
Arrange 8 ●●● s, where...



$\mathbb{R}^2$

??

A.



$\Delta$ -Minutiae Arrangement is Similarity-Preserving

[K07]Kojima, "Zero-Knowledge Proofs Considering Error for Secure Fingerprint Authentication"

# From Moore *et al.*'s hash to biometrics hash (overview)

Moore *et al.*'s hash

$$f_V(M) = \{Mv \mid v \in V\} \text{ (on finite field } \mathbb{F}_q)$$

All the elements of  $v$  are 0 to  $q-1$

insight from  $\Delta$ -MA

generalized to the form of Moore *et al.*'s hash by using **binary representation of regions**

our hash

$$f_V(M) = \{Mv \mid v \in V\} \text{ (on finite field } \mathbb{F}_q)$$

All the elements of  $v$  are 0 or 1

Our hash function is  
Quantum Tolerant **and** Similarity-Preserving

# Analyses

$$f_V(M) \approx f_V(N) \Leftrightarrow \min_{\pi} \max_i \|M\mathbf{v}_i - N\mathbf{v}_{\pi(i)}\| \leq \Delta$$

## 1. Quantum Tolerant

Getting  $N$  so that  $f_V(N) \approx f_V(M)$

from  $f_V(M)$  is difficult?

➤ **More Difficult than Graph Isomorphism**

under the condition  $\Delta < \frac{q-2}{9}$

## 2. Similarity-preserving

similarities of original biometrics data are preserved? i.e,

$$M' \approx M \Leftrightarrow f_V(M') \approx f_V(M) \quad ?$$

➤ **Similarities are preserved to some extent**

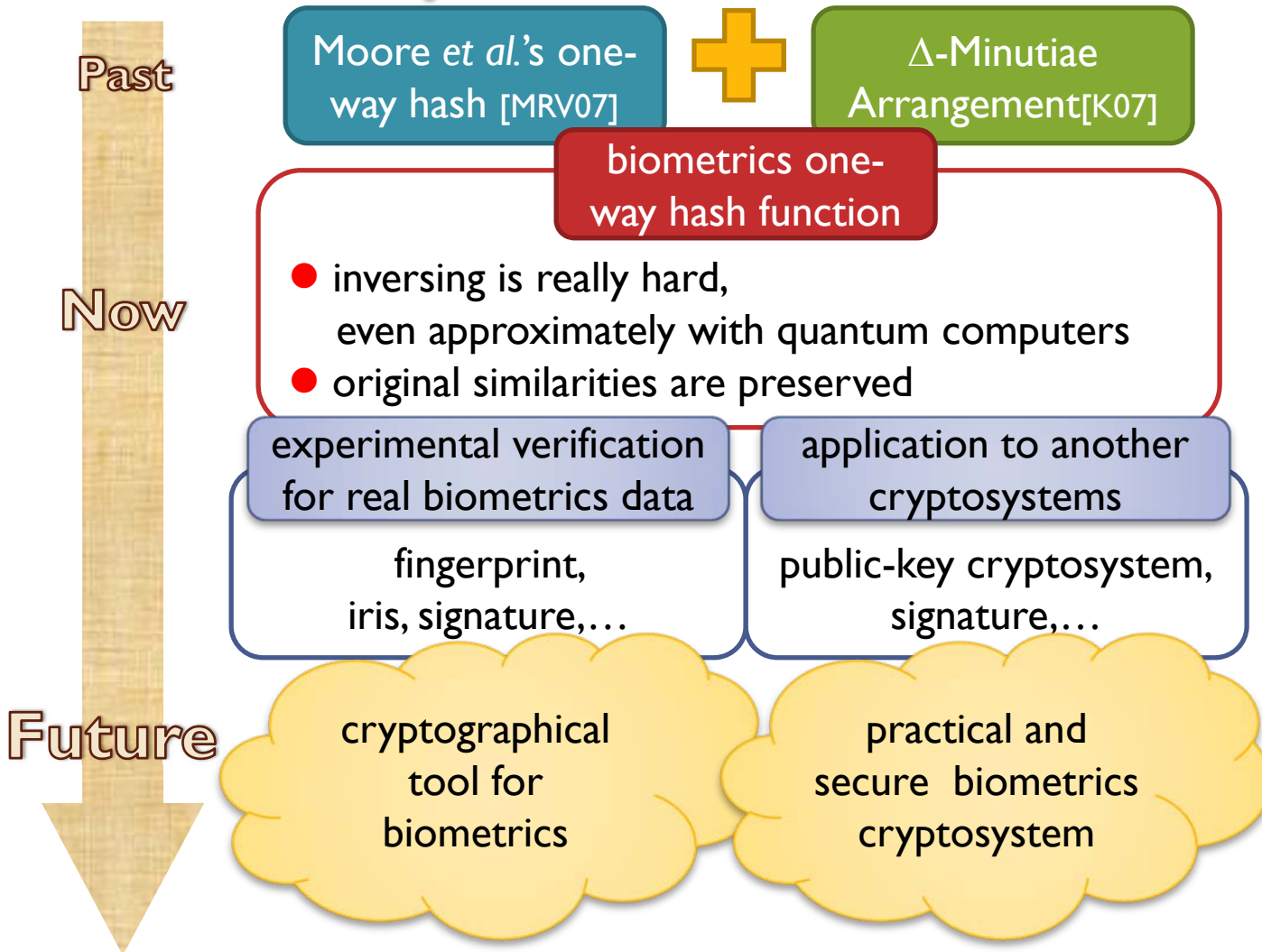
$$\sqrt[d]{\sum_i \|M'e_i - Me_i\|_1^d} \leq \Delta \Rightarrow f_V(M') \approx f_V(M)$$

$$\lim_{n \rightarrow \infty} \Pr_X[f_V(M) \approx f_V(X)] = 0$$



# **SUMMARY**

# Summary



[MRV07] Moore,Russell,Vazirani, "A classical one-way function to confound quantum adversaries"

[K07]Kojima, "Zero-Knowledge Proofs Considering Error for Secure Fingerprint Authentication"



# End

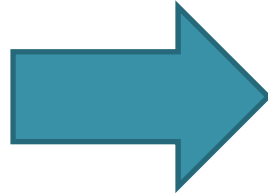
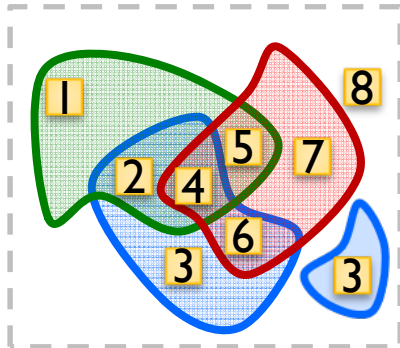
Thank you for listening

[S97] Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM J. Comput.*

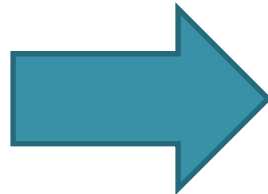
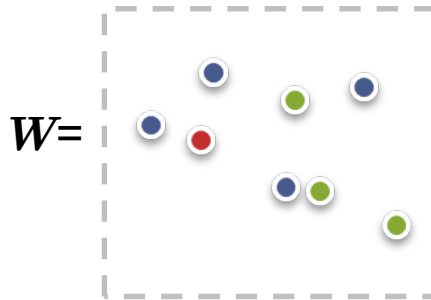
[MRV07] Moore, Russell, Vazirani, "A classical one-way function to confound quantum adversaries", *arXiv:quant-ph/0701115v2*

[K07] Kojima, "Zero-Knowledge Proofs Considering Error for Secure Fingerprint Authentication", *IPSJ SIG Notes*

# Generalization of $\Delta$ -MA



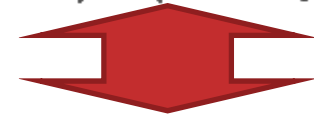
$$\begin{array}{l}
 R = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \\
 G = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \\
 B = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}
 \end{array}$$



$$\begin{array}{l}
 r = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \\
 g = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix} \\
 b = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}
 \end{array}$$



$$f_{\{R,G,B\}} \begin{pmatrix} r \\ g \\ b \end{pmatrix} = \left( \left\{ \begin{array}{l} r \cdot R \\ g \cdot R \\ b \cdot R \end{array} \right\}, \left\{ \begin{array}{l} r \cdot G \\ g \cdot G \\ b \cdot G \end{array} \right\}, \left\{ \begin{array}{l} r \cdot B \\ g \cdot B \\ b \cdot B \end{array} \right\} \right)$$



$$\begin{aligned}
 f_Y(M) &= \{Mv \mid v \in V\} \\
 &= \left\{ \begin{pmatrix} m_1 \cdot v_1 \\ m_2 \cdot v_1 \\ m_3 \cdot v_1 \end{pmatrix}, \begin{pmatrix} m_1 \cdot v_2 \\ m_2 \cdot v_2 \\ m_3 \cdot v_2 \end{pmatrix}, \begin{pmatrix} m_1 \cdot v_3 \\ m_2 \cdot v_3 \\ m_3 \cdot v_3 \end{pmatrix} \right\}
 \end{aligned}$$

all elements of  $R, G, B$  are  $\{0, 1\}$

all elements of  $V$  are  $\mathbb{F}_q$

critical difference!