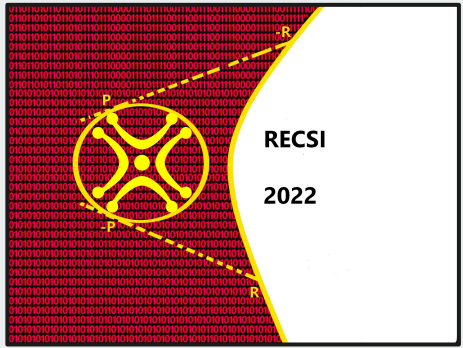
Diseño e implementación de un esquema criptobiométrico post-cuántico de protección de patrones. Aplicación en reconocimiento biométrico mediante mano

Diego José Abengózar Vilar
Carmen Sánchez Ávila



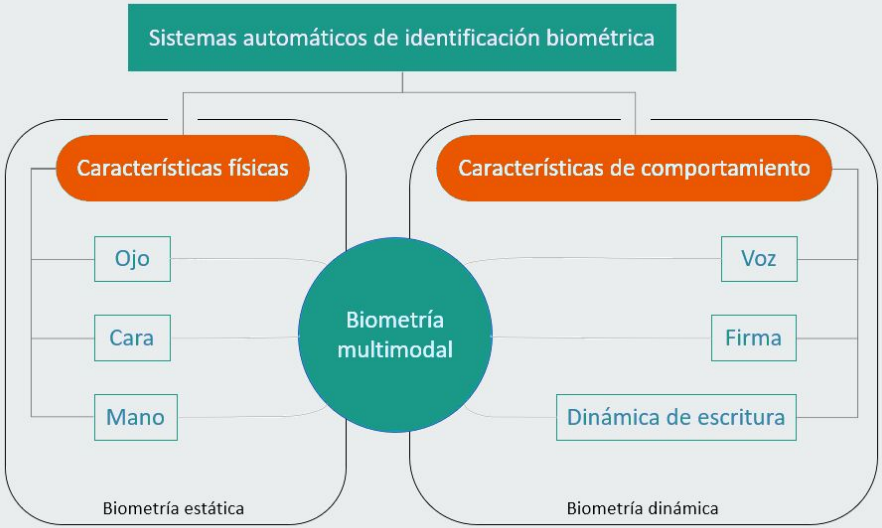
XVII Reunión Española sobre Criptología y Seguridad de la Información
Universidad Politécnica de Madrid

Índice

Introducción

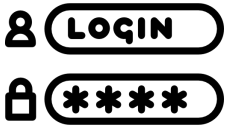
Biometría

Caracterización estadística de señales biológicas

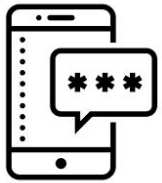


Sistemas de autenticación

- Algo que sabes



- Algo que tienes



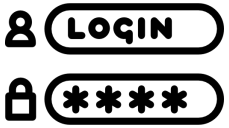
- Algo que eres

Biometría

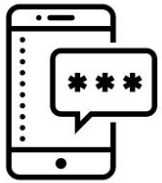
+

Sistemas de autenticación

- Algo que sabes

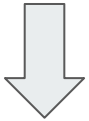


- Algo que tienes



- Algo que eres

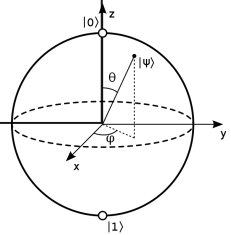
¿Seguridad?



Protección de patrón biométrico

Computación cuántica

- Irrupción de la computación cuántica
- Ej.: Algoritmo de Shor



¡NOVEDAD!

Esquema criptobiométrico post-cuántico de protección de patrones

Criptosistema de McEliece

Criptosistema de McEliece

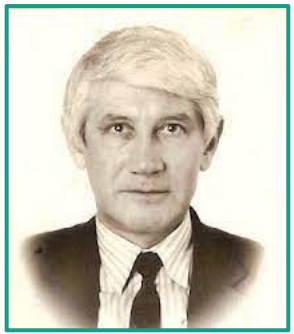
- Robert J. McEliece, 1978
- Criptosistema post-cuántico
- Candidato Fase 4 NIST (Albrecht, Bernstein et al.)

Criptosistema de McEliece

- Robert J. McEliece, 1978
- Criptosistema post-cuántico
- Candidato Fase 4 NIST (Albrecht, Bernstein et al.)

Códigos Goppa

- Valery Denisovich Goppa, 1970
- Familia de códigos lineales correctores de errores



Criptosistema de McEliece

$S_{k \times k}$

scrambler

$G_{k \times n}$

matriz generadora

$P_{n \times n}$

matriz de permutación

Criptosistema de McEliece

$$S_{k\times k} \qquad G_{k\times n} \qquad P_{n\times n}$$

Clave pública $(S \cdot G \cdot P, t)$

Clave privada (S, G, P)

Criptosistema de McEliece

Cifrado

$$\vec{c} = \vec{m} \cdot SGP + \vec{e}$$

Criptosistema de McEliece

Cifrado

$$\vec{c} = \vec{m} \cdot SGP + \vec{e}$$

Descifrado

$$\vec{c}P^{-1} = \vec{m} \cdot SGPP^{-1} + \vec{e}P^{-1}$$

Criptosistema de McEliece

Cifrado

$$\vec{c} = \vec{m} \cdot SGP + \vec{e}$$

Descifrado

peso t

$$\vec{c}P^{-1} = \vec{m} \cdot SGPP^{-1} + \vec{e}P^{-1}$$

algoritmo corrección errores

$$\vec{m} \cdot S$$

Criptosistema de McEliece

Cifrado

$$\vec{c} = \vec{m} \cdot SGP + \vec{e}$$

Descifrado

peso t

$$\vec{c}P^{-1} = \vec{m} \cdot SGPP^{-1} + \vec{e}P^{-1}$$

algoritmo corrección errores

$$\vec{m} \cdot S$$

$\cdot S^{-1}$

$$\vec{m}$$

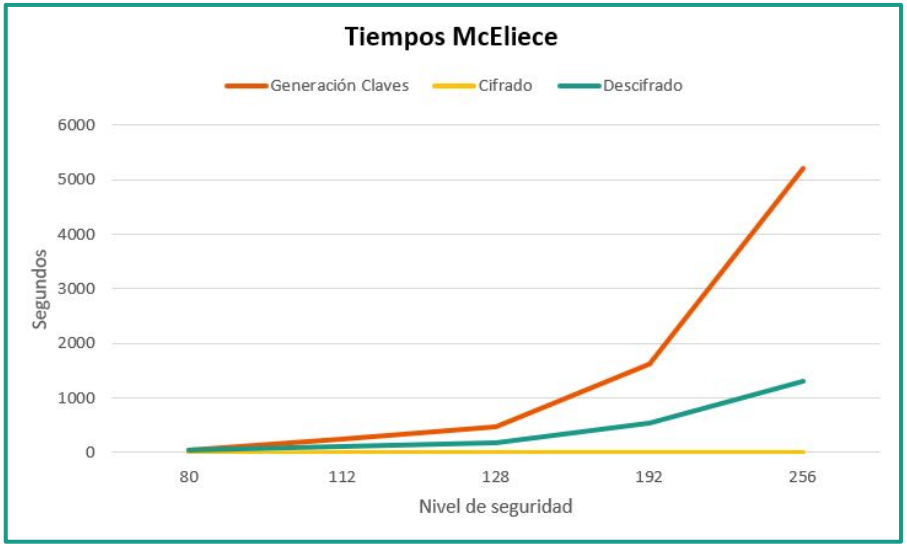
Implementación en Python

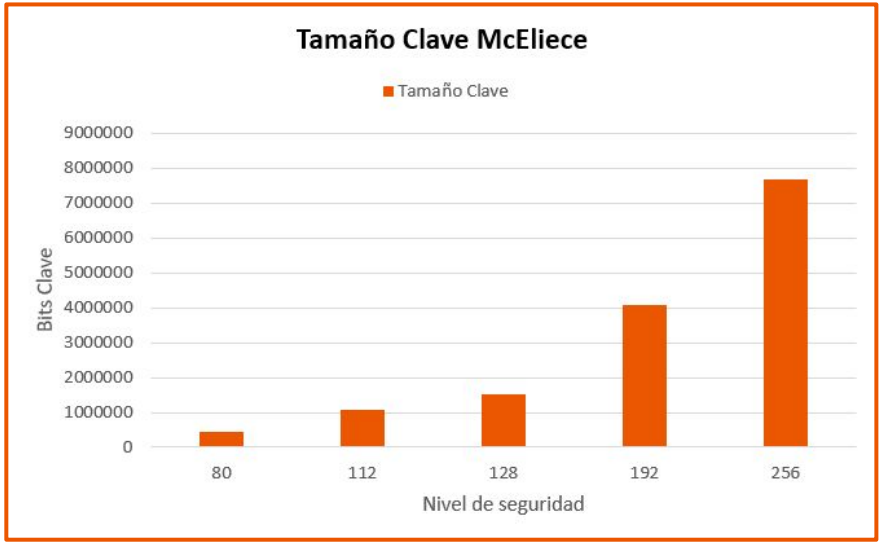
¡NOVEDAD!

```python
    def decrypt(self, ciphertext):
        if len(ciphertext) != self.n:
            print(f"McEliece.decrypt: El texto cifrado tiene que ser de longitud {self.n}")
            return

        # m * SGP * P^-1 + e * P^-1
        invP = np.linalg.inv(self.P)
        codeword = ciphertext.dot(invP)

        # m * S
        mS, errorVector = self.goppaCode.decode(codeword)

        # m * S * S^-1
        invS = np.linalg.inv(self.S)
        m = mS.dot(invS)
        return m, errorVector
```

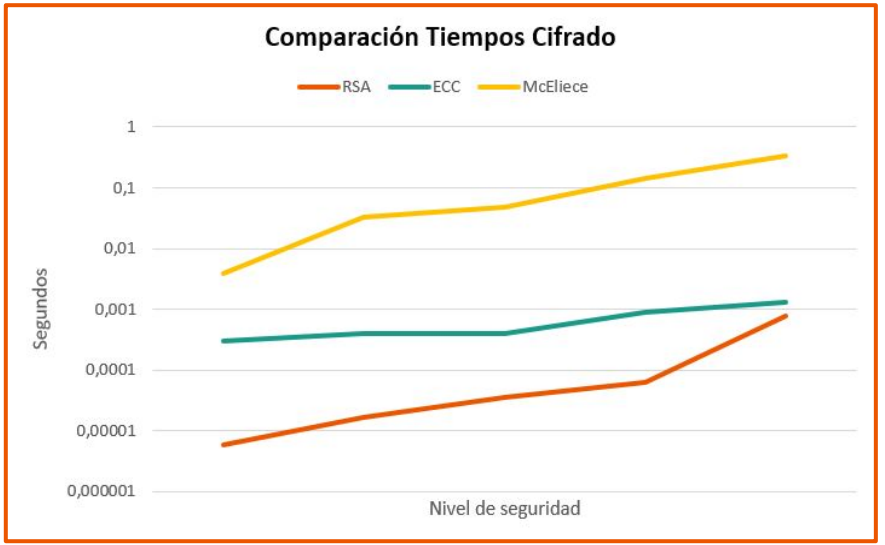
```python
class Goppa:

    def __init__(self, m, n, t):
        self.m = m
        self.n = n
        self.t = t
        self.q = 2
        self.k = None
        self.GF = None
        self.g = None
        self.L = None
        self.H = None
        self.binH = None
        self.G = None

    def generate(self):
        if (self.q**self.m < self.n):
            print(f"Goppa.generate: No se puede construir el código Goppa con estos parámetros: q={self.q}^m={self.m} < n={self.n}")
            return

        # Cuerpo GF(2^m)
        self.GF = galois.GF(self.q**self.m)

        # Generar g aleatorio, monico e irreducible (para evitar problemas) de grado t sobre GF
        self.g = galois.irreducible_poly(self.q**self.m, self.t, method="random")
```

Rendimiento

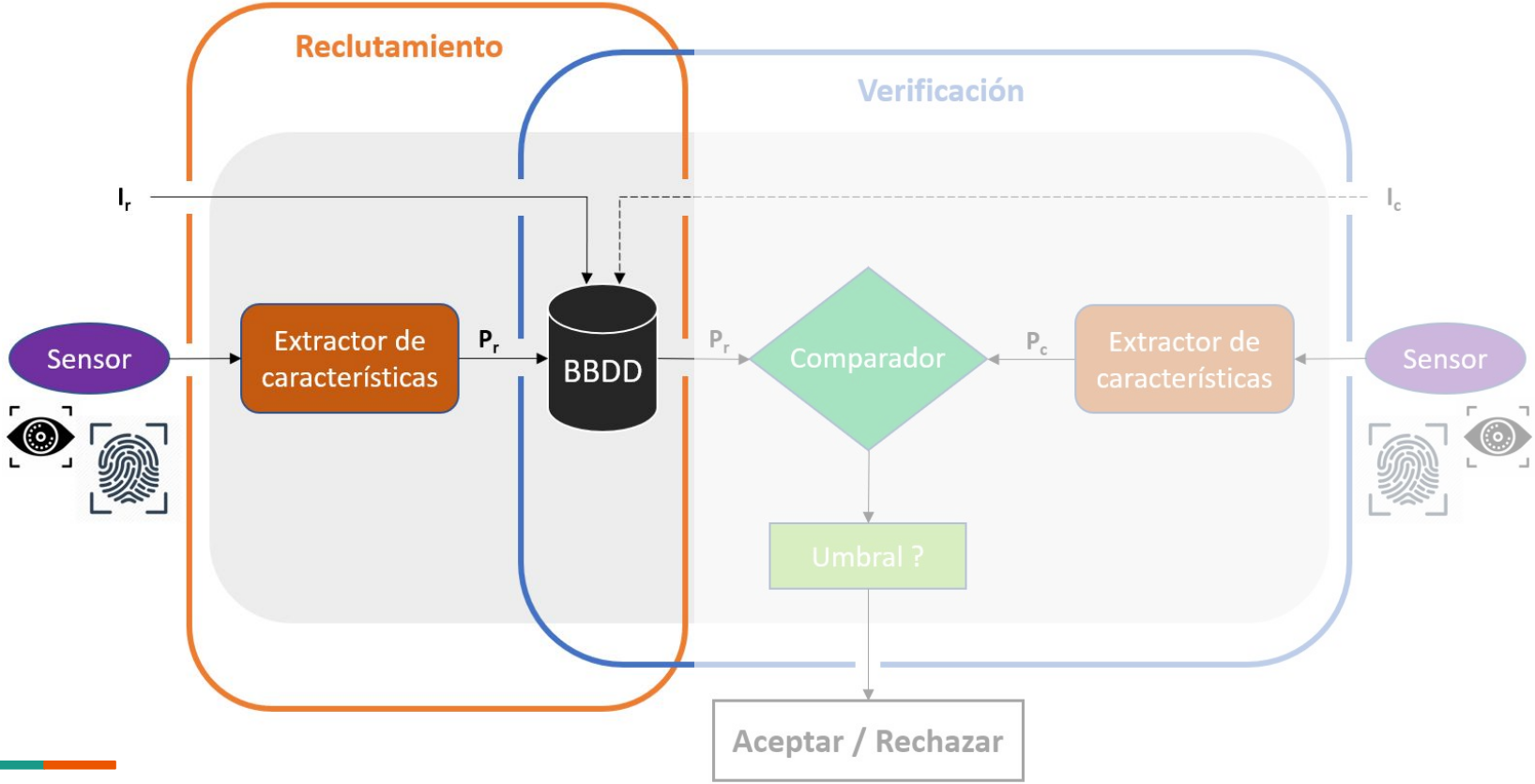


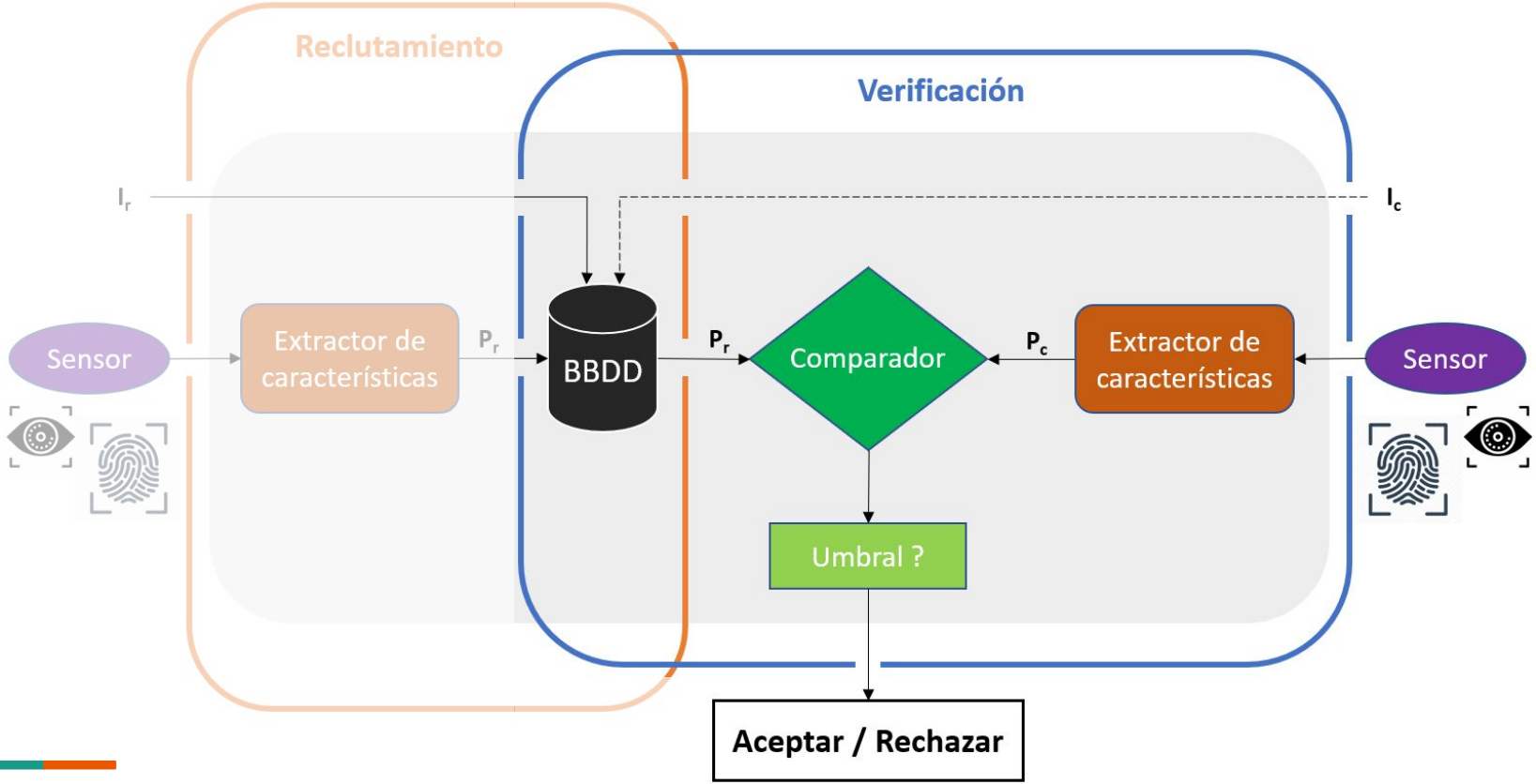


Rendimiento



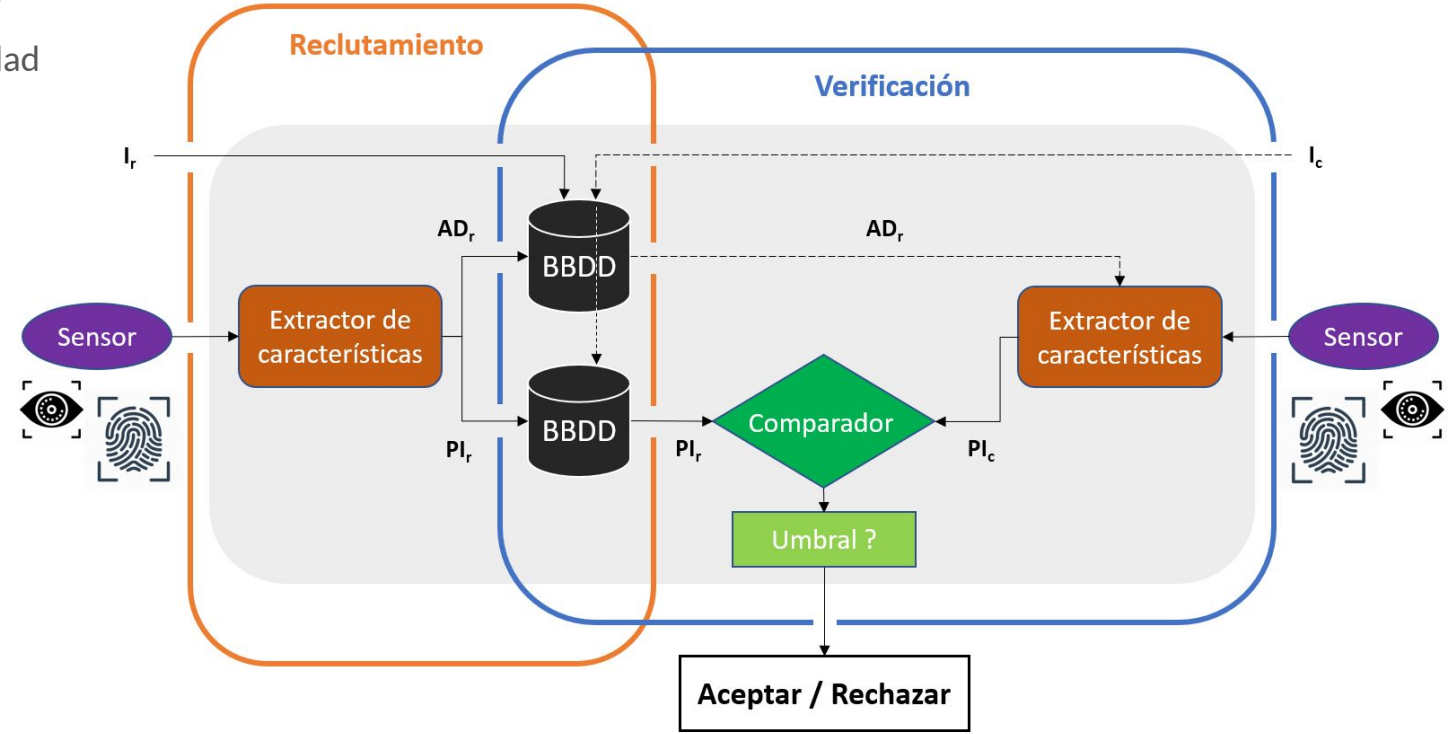
Esquema propuesto

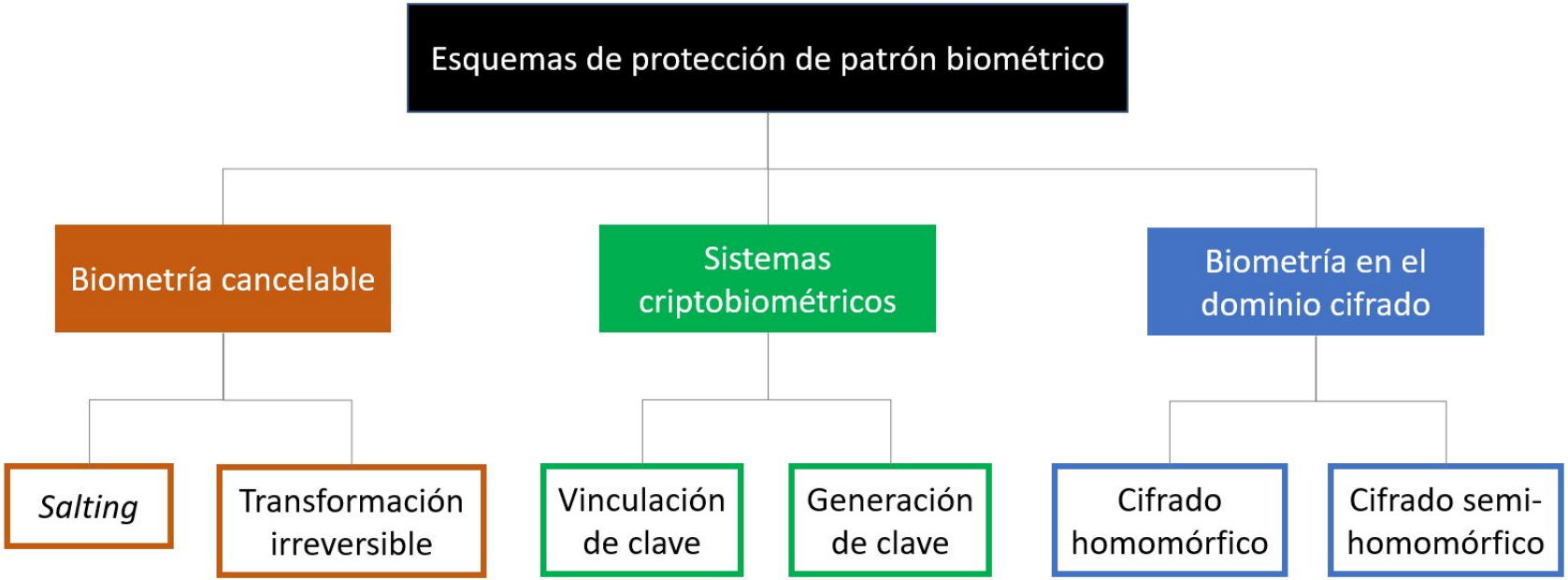

Reclutamiento
Verificación
I_r
I_c
Sensor
Extractor de características
P_r
BBDD
P_r
Comparador
P_c
Extractor de características
Sensor
Umbral ?
Aceptar / Rechazar


Reclutamiento
Verificación
I_r
I_c
Sensor
Extractor de características
P_r
BBDD
P_r
Comparador
P_c
Extractor de características
Sensor
Umbral ?
Aceptar / Rechazar

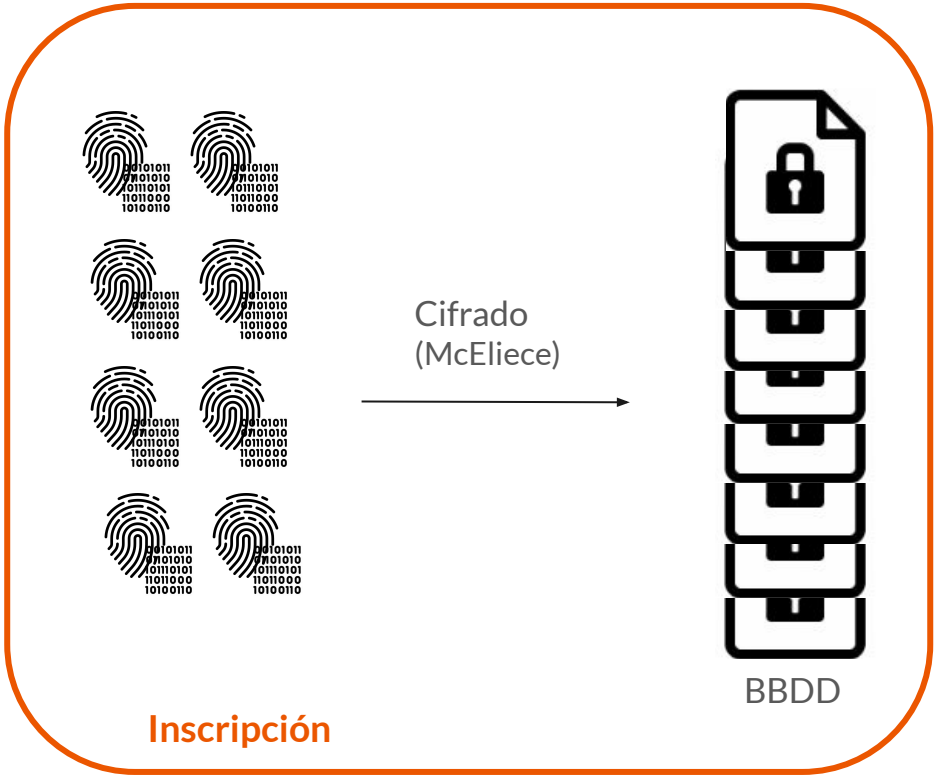
Estándar ISO 24745:2022

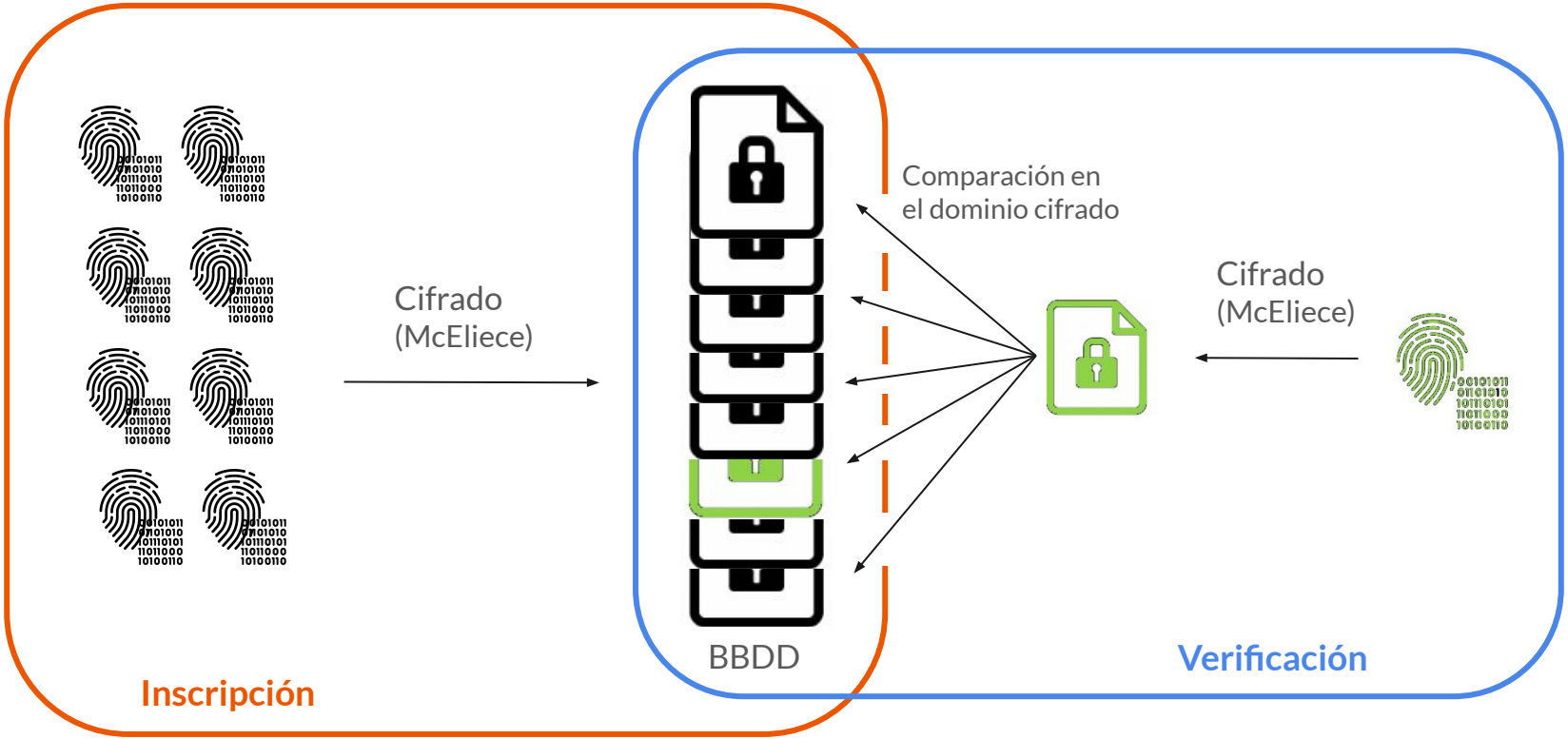
- Irreversibilidad
- Desvinculabilidad
- Revocabilidad




Esquemas de protección de patrón biométrico
Biometría cancelable
Sistemas criptobiométricos
Biometría en el dominio cifrado
Salting
Transformación irreversible
Vinculación de clave
Generación de clave
Cifrado homomórfico
Cifrado semi-homomórfico

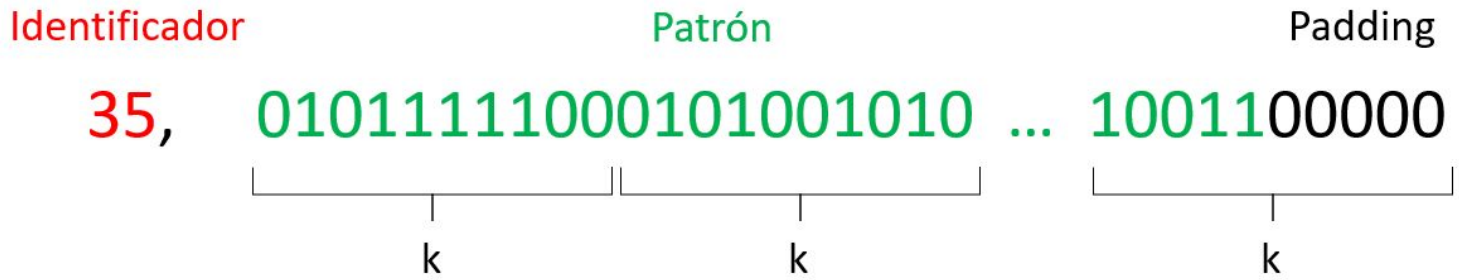
Esquema propuesto


Cifrado
(McEliece)
BBDD
Inscripción


Cifrado
(McEliece)
Comparación en
el dominio cifrado
Cifrado
(McEliece)
BBDD
Inscripción
Verificación

Inscripción

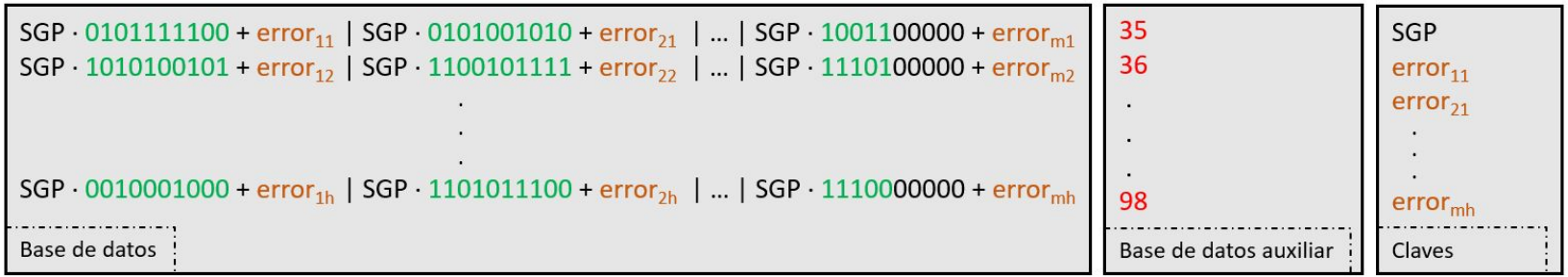
1. Se genera un par de claves, pública y privada, del criptosistema de McEliece.
2. Se separa cada patrón en bloques de la longitud correspondiente a las claves elegidas. En caso de que el último bloque no tenga la longitud suficiente, se añade un padding.



Inscripción

3. Cada bloque se cifra con la clave pública y se almacena en la base de datos del sistema biométrico. En la fase de cifrado se añade un vector de errores aleatorio, por lo que, además de la clave pública, se almacena también cada vector de errores utilizado.

4. En una base de datos auxiliar se almacena el identificador de usuario correspondiente a cada patrón.



Verificación

1. En la base de datos auxiliar se busca el identificador de usuario para determinar con qué patrón de referencia hay que comparar.
2. Se separa el patrón de consulta en bloques de la longitud correspondiente.
3. Se recupera la clave pública y el vector de errores correspondiente para cada bloque, y se cifra el patrón bloque a bloque.
4. Se realiza la comparación en el dominio cifrado de ambos patrones (distancia Euclídea).
5. Si la similitud de ambos patrones supera un cierto umbral, se acepta como válida la verificación.

Aplicación práctica

Base de datos *gb2s_ID*

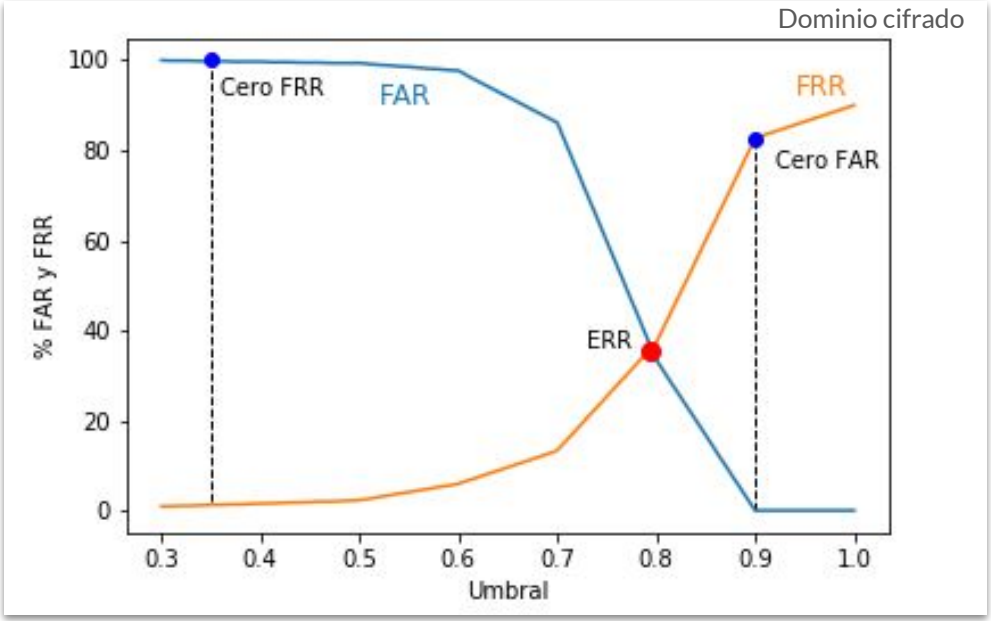
- 96 usuarios, y 10 patrones por cada usuario
- Gran variabilidad entre las distintas muestras
- Filtro de Gabor de extracción de características principales
- Especificaciones detalladas en la memoria

Evaluación de errores

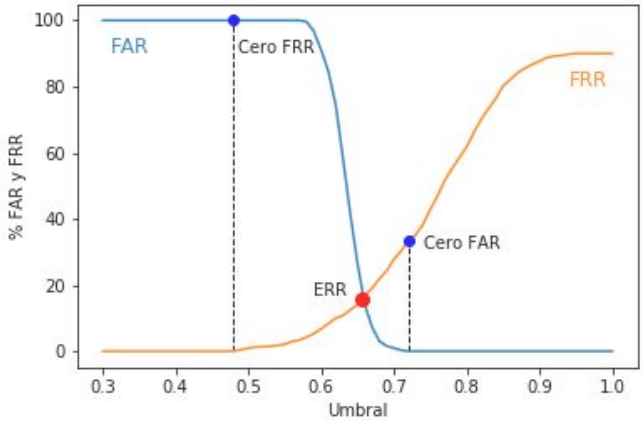
- **Tasa de falsos rechazos** (FRR): proporción de usuarios que siendo legítimos son rechazados por el sistema. Cuanto mayor es el umbral, más aumenta la tasa de falsos rechazos.
- **Tasa de falsas aceptaciones** (FAR): proporción de usuarios que siendo impostores son aceptados por el sistema. Cuanto menor es el umbral, más aumenta la tasa de falsas aceptaciones.
- **Tasa de igual error** (EER): momento en el que la tasa FAR es igual a la tasa FRR.
- **Cero FAR**: menor valor de la tasa FRR para el cual FAR = 0.
- **Cero FRR**: menor valor de la tasa FAR para el cual FRR = 0

Evaluación de errores

Dominio cifrado

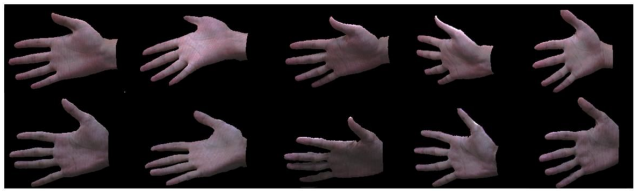


Dominio no cifrado



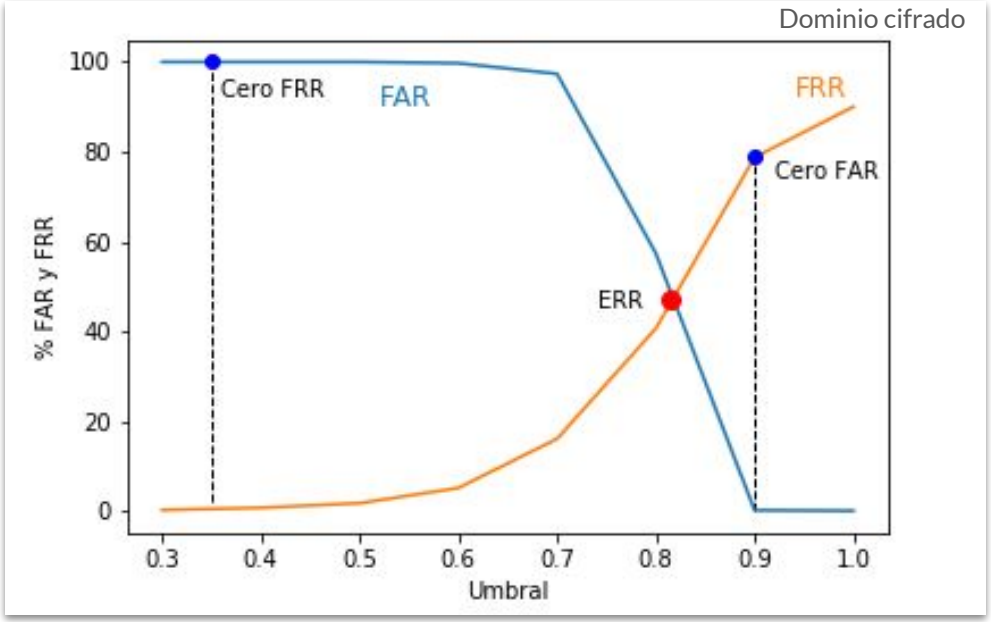
Base de datos *Hong Kong Polytechnic University Contact-free 3D/2D Hand Images Database*

- 177 usuarios, y 10 patrones por cada usuario
- Gran variabilidad entre las distintas muestras
- Filtro de Gabor de extracción de características principales
- Especificaciones detalladas en la memoria

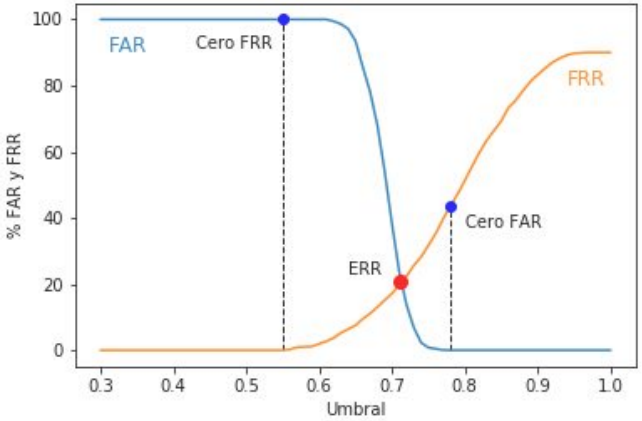


Evaluación de errores

Dominio cifrado



Dominio no cifrado



Evaluación de rendimiento y seguridad

Rendimiento

- Verificación
  - *gb2s_ID*: **1,4 segundos**
  - *Hong Kong DB*: **1,8 segundos**
- Identificación
  - *gb2s_ID* (96 usuarios): 90 segundos
  - *Hong Kong DB* (177 usuarios): 162 segundos

Hardware: Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz, 8 GB RAM.

Evaluación de rendimiento y seguridad

Rendimiento

- Verificación
  - *gb2s_ID*: **1,4 segundos**
  - *Hong Kong DB*: **1,8 segundos**
- Identificación
  - *gb2s_ID* (96 usuarios): 90 segundos
  - *Hong Kong DB* (177 usuarios): 162 segundos

Seguridad

- *Information Set Decoding*
  - Solución: cifrar vectores de errores
  - Recomendable almacenar dicha base de datos en un servidor diferente

Hardware: Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz, 8 GB RAM.

Conclusiones y líneas futuras

Conclusiones

Estudio del criptosistema de McEliece

↓

Implementación del criptosistema de McEliece

↓

Esquema post-cuántico de protección de patrones

↓

Caso práctico con patrones de mano

↓

Buenas tasas de fallos y rendimiento

↓

Buena primera aproximación, con posibilidad de mejoras

Conclusiones

Estudio del criptosistema de McEliece

↓

Implementación del criptosistema de McEliece

↓

Esquema post-cuántico de protección de patrones

↓

Caso práctico con patrones de mano

↓

Buenas tasas de fallos y rendimiento

↓

Buena primera aproximación, con posibilidad de mejoras

Conclusiones

Estudio del criptosistema de McEliece

↓

Implementación del criptosistema de McEliece

↓

Esquema post-cuántico de protección de patrones

↓

Caso práctico con patrones de mano

↓

Buenas tasas de fallos y rendimiento

↓

Buena primera aproximación, con posibilidad de mejoras

Conclusiones

Estudio del criptosistema de McEliece

↓

Implementación del criptosistema de McEliece

↓

Esquema post-cuántico de protección de patrones

↓

Caso práctico con patrones de mano

↓

Buenas tasas de fallos y rendimiento

↓

Buena primera aproximación, con posibilidad de mejoras

Conclusiones

Estudio del criptosistema de McEliece

↓

Implementación del criptosistema de McEliece

↓

Esquema post-cuántico de protección de patrones

↓

Caso práctico con patrones de mano

↓

Buenas tasas de fallos y rendimiento

↓

Buena primera aproximación, con posibilidad de mejoras

Conclusiones

Estudio del criptosistema de McEliece

↓

Implementación del criptosistema de McEliece

↓

Esquema post-cuántico de protección de patrones

↓

Caso práctico con patrones de mano

↓

Buenas tasas de fallos y rendimiento

↓

Buena primera aproximación, con posibilidad de mejoras

Líneas futuras

Líneas futuras

Otro mecanismo para solucionar los problemas de homomorfía de McEliece

Extracción de características diferente al filtro de Gabor

Modificaciones del criptosistema para evitar almacenar vectores de errores

Otras distancias en el módulo de comparación

Líneas futuras

Otro mecanismo para solucionar los problemas de homomorfía de McEliece

Extracción de características diferente al filtro de Gabor

Modificaciones del criptosistema para evitar almacenar vectores de errores

Otras distancias en el módulo de comparación

Líneas futuras

Otro mecanismo para solucionar los problemas de homomorfía de McEliece

Extracción de características diferente al filtro de Gabor

Modificaciones del criptosistema para evitar almacenar vectores de errores

Otras distancias en el módulo de comparación

Líneas futuras

Otro mecanismo para solucionar los problemas de homomorfía de McEliece

Extracción de características diferente al filtro de Gabor

Modificaciones del criptosistema para evitar almacenar vectores de errores

Otras distancias en el módulo de comparación

¡ Gracias !