

Análisis de un esquema de cifrado basado en cuasigrupos

TRABAJO DE FIN DE GRADO

ALEJANDRO GARCÍA CARRETERO

GRADO EN MATEMÁTICAS

DIRECTORA

MARÍA ISABEL GONZÁLEZ VASCO

- Introducción y Objetivos
- Fundamentos matemáticos
- Fundamentos criptográficos
- Esquema de cifrado presentado
- Criptoanálisis y alternativas propuestas
- Conclusiones y trabajos futuros

- Abordar temario no estudiado en la carrera
- Afianzar y aplicar conocimiento adquirido durante la carrera
- Hacer un estudio exhaustivo de un esquema de cifrado
 - “*A quasigroup-based public-key cryptosystem.*” – *C. Koscienly*
- Análisis constructivo del esquema: propuesta de mejoras

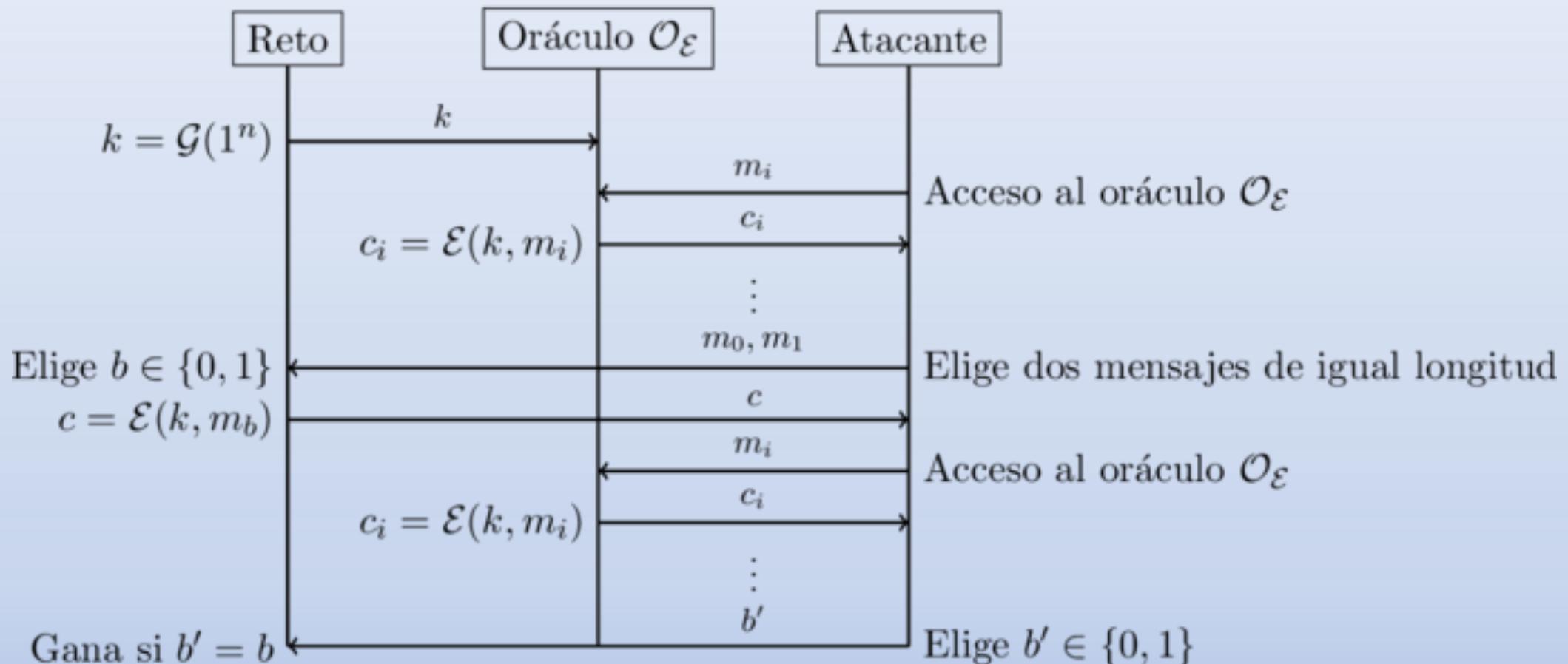
- Cuasigrupos: (Q, \oplus) que cumple $\forall a, b \in Q$:
 - $\exists! c \in Q$ t.q. $a \oplus c = b$
 - $\exists! d \in Q$ t.q. $d \oplus a = b$
- A esta operación no se le pide nada más, por lo que no tiene por qué existir elemento neutro ni opuestos, tampoco tiene por qué ser commutativa.
- Operaciones asociadas: \ominus y \oslash
 - $(x \oplus y) \ominus y = x$
 - $(x \ominus y) \oplus y = x$
 - $y \oslash (y \oplus x) = x$
 - $y \oplus (y \oslash x) = x$

Comparación de las estructuras algebraicas.

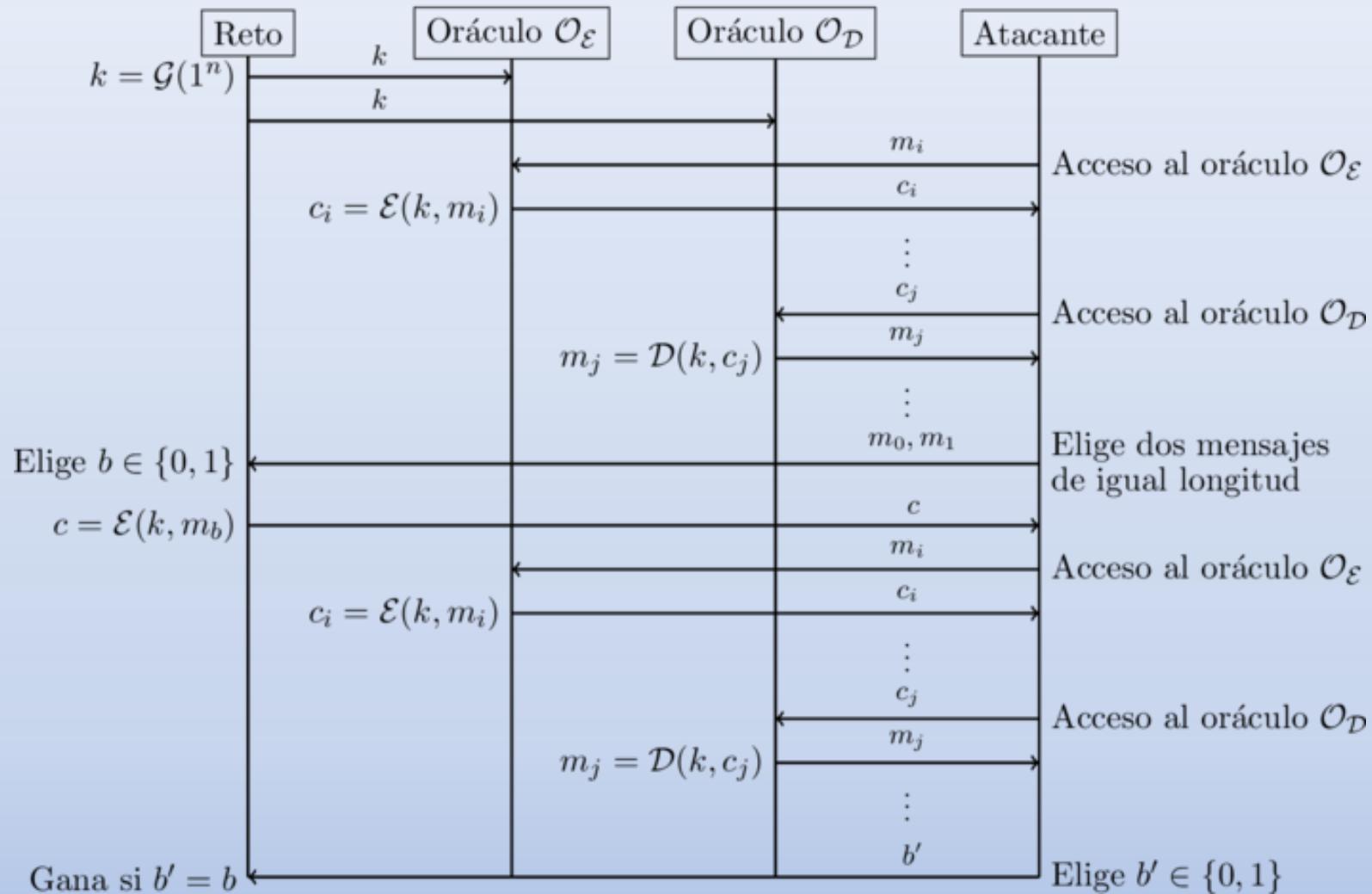
	Operación \oplus				Operación \otimes				
Propiedades	Commutativa	Elemento Neutro	Inversos	Asociativa	Commutativa	Elemento Neutro	Inversos	Asociativa	Distributiva
Cuasigrupo (Q, \oplus)					-	-	-	-	-
Grupo (G, \oplus)		X	X	X	-	-	-	-	-
Anillo (A, \oplus, \otimes)	X	X	X	X				X	X
Cuerpo (K, \oplus, \otimes)	X	X	X	X	X	X	X	X	X

- Principio de Kerckhoffs: algoritmos públicos.
- Sistemas de clave privada: una única clave.
- Sistemas de clave pública: dos claves, pública y privada.
- Seguridad en esquemas de cifrado
 - Indistinguibilidad
 - Maleabilidad

CPA-IND



CCA-IND



Esquema analizado



“A quasigroup-based public-key cryptosystem.” – C. Koscienly

ESQUEMA PRESENTADO

- Grupos de permutaciones
 - $\mathcal{S}_3 = \{id, f, g, h, i, j\}$
 - Las tres tablas son distintas

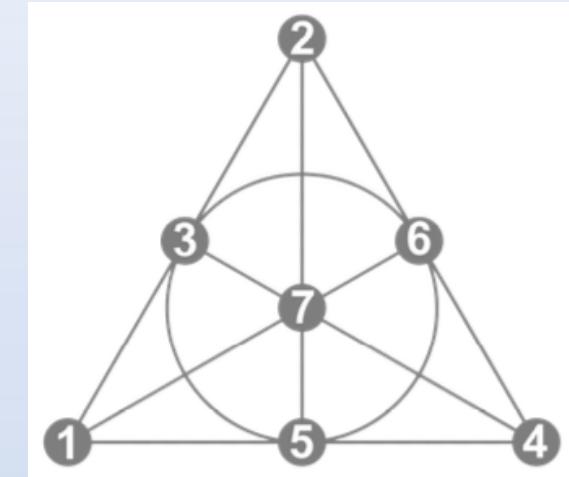
$id : \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$	$f : \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$
0 \mapsto 0	0 \mapsto 1
1 \mapsto 1	1 \mapsto 2
2 \mapsto 2	2 \mapsto 0
$g : \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$	$h : \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$
0 \mapsto 2	0 \mapsto 0
1 \mapsto 0	1 \mapsto 2
2 \mapsto 1	2 \mapsto 1
$i : \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$	$j : \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$
0 \mapsto 2	0 \mapsto 1
1 \mapsto 1	1 \mapsto 0
2 \mapsto 0	2 \mapsto 2.

\circ	id	f	g	h	i	j
id	id	f	g	h	i	j
f	f	g	id	j	h	i
g	g	id	f	i	j	h
h	h	i	j	id	f	g
i	i	j	h	g	id	f
j	j	h	i	f	g	id

- $k = fg(id)j, m = hihi$
- Ciframos con D, desciframos con S.
- $c = D(m, k) = D(hihi, fg(id)j) = ihhf$
- $m' = S(c, k) = S(ihhf, fg(id)j) = hihi$

D	id	f	g	h	i	j
id	id	g	f	h	i	j
f	f	id	g	j	h	i
g	g	f	id	i	j	h
h	h	j	i	id	f	g
i	i	h	j	g	id	f
j	j	i	h	f	g	id

- Triple sistema de Steiner (S, \mathcal{B})
 - $S = \{1, 2, 3, 4, 5, 6, 7\}$
 - $\mathcal{B} = \{246, 145, 347, 123, 257, 167, 356\}$
 - $x \oplus y = z \Leftrightarrow x = y = z \vee xyz \in \mathcal{B}$
- \oplus es idempotente y tiene simetría total
 - S, D y \hat{D} son iguales
- $k = 1234, m = 2461$
- Ciframos con S , desciframos con S .
- $c = S(m, k) = S(2461, 1234) = 3655$
- $m' = S(c, k) = S(3655, 1234) = 2461$



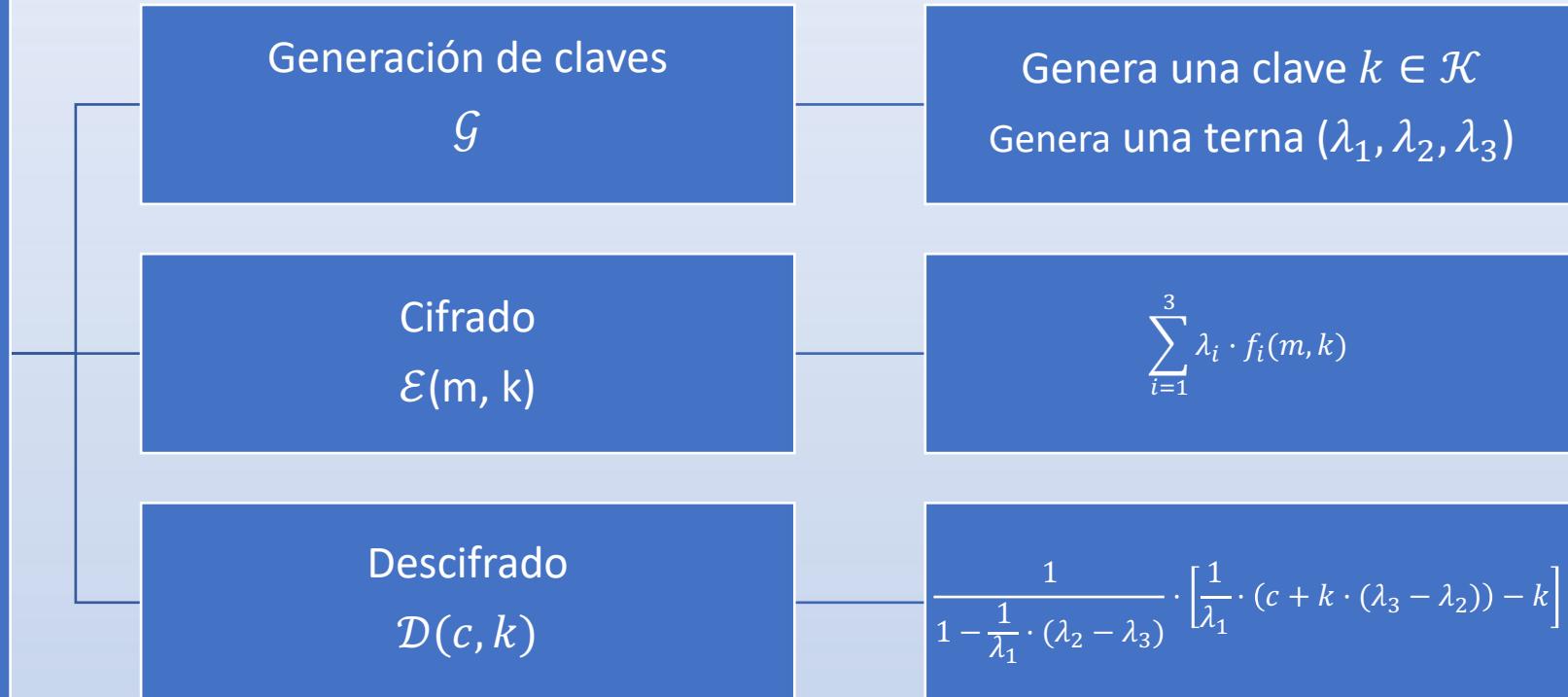
S	1	2	3	4	5	6	7
1	1	3	2	5	4	7	6
2	3	2	1	6	7	4	5
3	2	1	3	7	6	5	4
4	5	6	7	4	1	2	3
5	4	7	6	1	5	3	2
6	7	4	5	2	3	6	1
7	6	5	4	3	2	1	7



- Propuesta 1: Variante no determinista.
 - Aleatorización de las funciones de cifrado.
 - Cada vez que se intercambia un mensaje se utiliza un par de funciones distintas.
- Problemas de la propuesta 1:
 - Intercambio adicional de las funciones empleadas.
 - Hay determinados cuasigrupos donde no se puede hacer esto.
 - Ataque estadístico haciendo uso repetido del oráculo.
 - $P = 1 - \left[n \cdot \left(\frac{n-1}{n}\right)^m - n \cdot \left(\frac{1}{n}\right)^m \right]$
 - Las colisiones no son significativas.

	$S(m, k)$	$S(k, m)$	$\hat{D}(m, k)$	$\hat{D}(k, m)$
m_0	0311	2311	2131	2131
m_1	2311	0311	0131	0131

Segunda propuesta



- Un sistema no es más seguro por basarse en estructuras poco utilizadas o con poca complejidad.
- El diseño de los algoritmos es crucial. La estructura subyacente no lo es todo, por muy interesante que sea.
- La simple realeatorización de un sistema determinista no tiene por qué provocar una mejora significativa respecto al original.
- En trabajos futuros, puede ser interesante seguir investigando los cuasigrupos como base para un sistema criptográfico, ya que no es una estructura muy empleada.

Análisis de un esquema de cifrado basado en cuasigrupos

TRABAJO DE FIN DE GRADO

ALEJANDRO GARCIA CARRETERO

GRADO EN MATEMÁTICAS

DIRECTORA

MARÍA ISABEL GONZÁLEZ VASCO