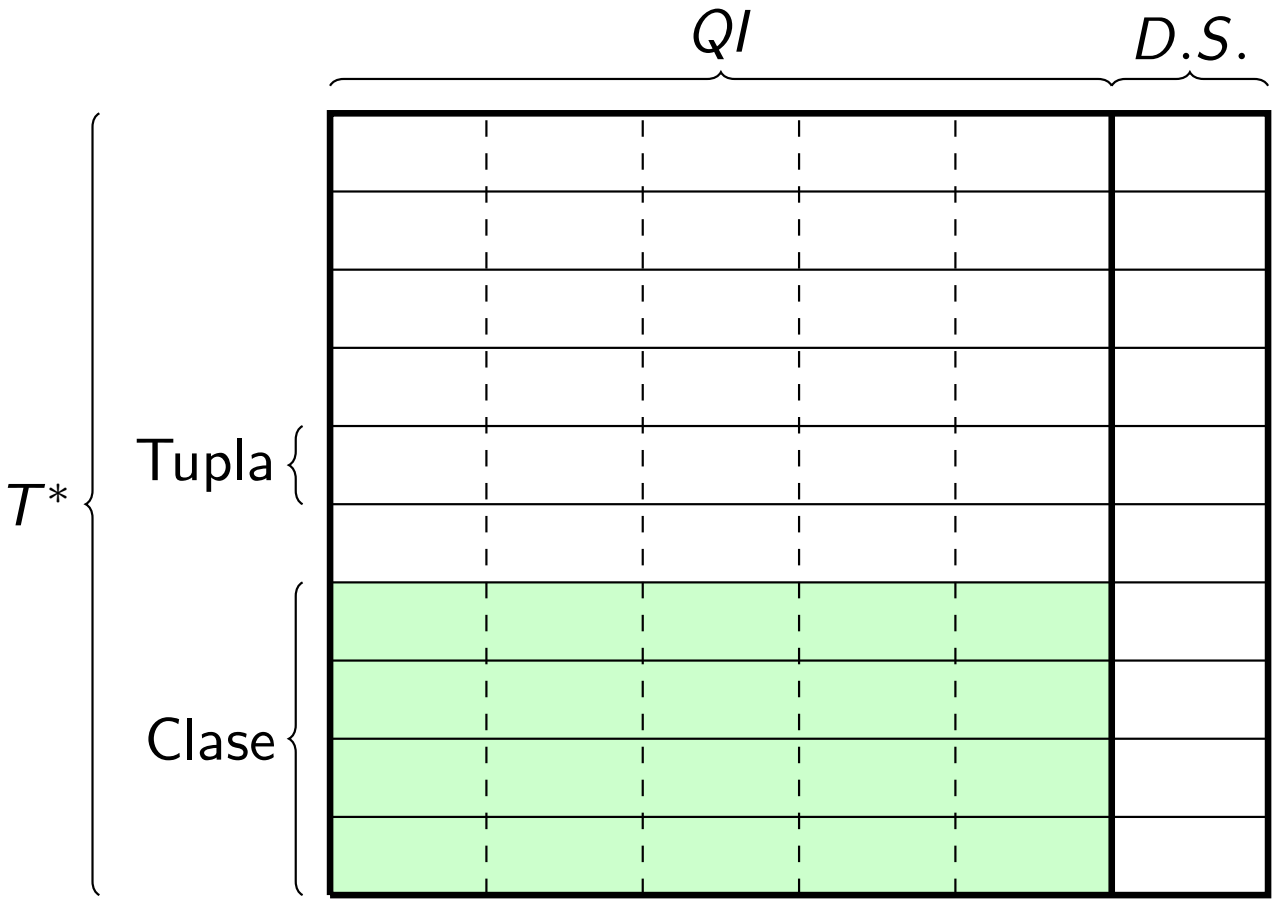
Análisis de ataques a bases de datos de publicación continua en privacidad sintáctica

Adrián Tobar Nicolau[12]
Javier Parra-Arnau[12]
Jordi Forné[12]

[1]Universidad Politécnica de Catalunya,Barcelona, Spain
[2]{adrian.tobar,javier.parra,jordi.forne}@upc.edu

Contenidos

Estructura de la base de datos



- T^*: anonymized release.
- QI: datos no sensibles (sexo, edad, peso, altura,...).
- D.S.: dato sensible que se quiere proteger (enfermedad, sueldo,...).
- Tuplas: cada tupla corresponde a algún usuario.
- Clase: conjunto de tuplas con QI iguales.

Publicación continua

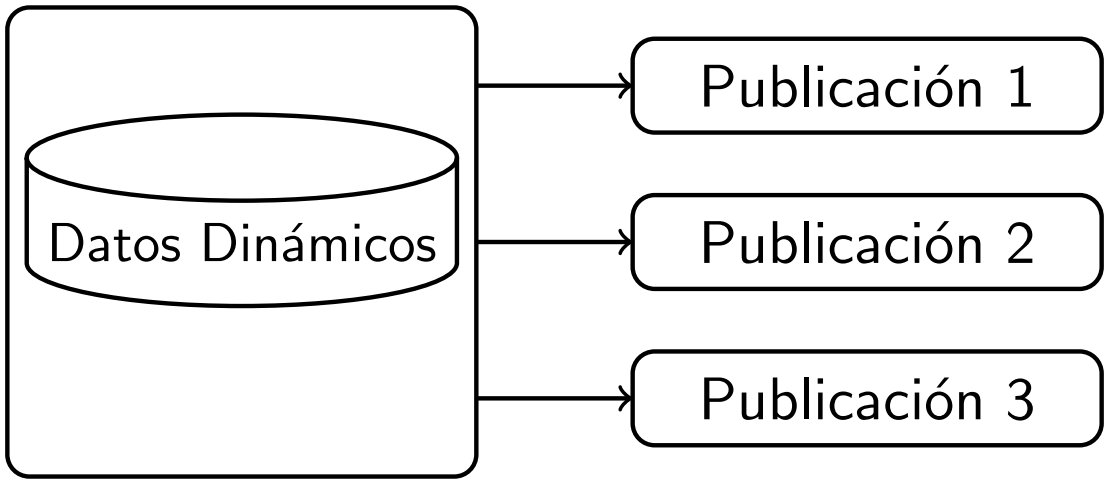


Figura: Publicación continua. La información va cambiando entre publicaciones.

Tres posibles niveles de dinamicidad:

- Incremental: Sólo se añaden tuplas nuevas.
- Dinámica: Se añaden tuplas nuevas y se pueden eliminar las existentes.
- Completamente Dinámica: Inserciones, eliminaciones, reinserciones de tuplas previamente eliminadas y actualización de la información de cualquier tupla.

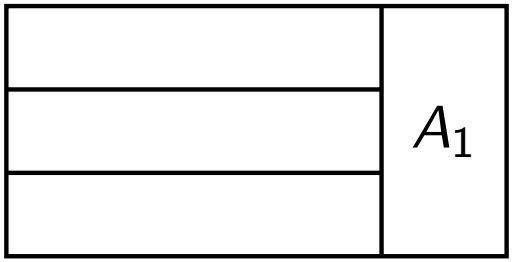
Tipos de atacante

ATACANTE	PARTICIPACIÓN[1]	QI[2]	T.K[3].	S.D.K.[4]	S.B.K.[5]	C.B.K.[6]
TRIVIAL	No	No	No	No	No	No
MÍNIMO	SINGULAR	SINGULAR	No	No	No	No
INCOMPLETO	Si	ACOTADO	No	No	No	No
OBJETIVO	Si	SINGULAR	Si	No	No	No
LIMITADO	Si	Si	ACOTADO	No	No	No
COMPLETO	Si	Si	Si	No	No	No
INTERIOR	Si	Si	Si	ACOTADO	No	No
PROBABILÍSTICO	Si	Si	Si	P. ACOTADO	Si	Si

[1] Participantes: Usuarios que pueden aparecer en la base de datos.
[2] QI: Información no sensible (Quasi identifiers).
[3] Temporal Knowledge: Cuando se insertan y/o eliminan las tuplas.
[4] Sensitive Data Knowledge : Información sensible de un subcojunto de tuplas.
[5] Sensitive Background Knowledge: Correlación de los QI con los datos sensibles.
[6] Correlation Background Knowledge: Correlación entre datos sensibles y sus posibles actualizaciones.

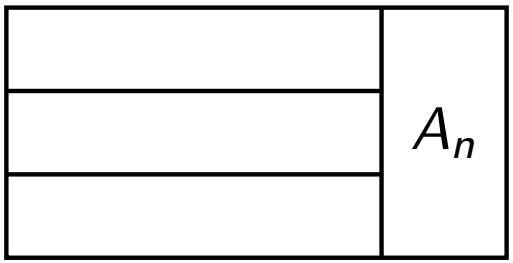
Contenidos

Ataque de intersección



Clase de p en T_1^*

$\vdots$ $\Longrightarrow$ p tiene el dato sensible en $\bigcap_{i=1}^{n} A_i$



Clase de p en T_n^*

Ataque intersección: ejemplo

Id	SEXO	EDAD	D.S.
1	-	$[20-22]$	VIH
2	-	$[20-22]$	FIEBRE

(a) T_1^*

Id	SEXO	EDAD	D.S.
1	VARÓN	[19-20]	VIH
3	VARÓN	[19-20]	ACNÉ
2	MUJER	22	FIEBRE
4	MUJER	22	COUGH

(b) T_2^*

Figura: Ataque de intersección al usuario 1.

Ataque de intersección

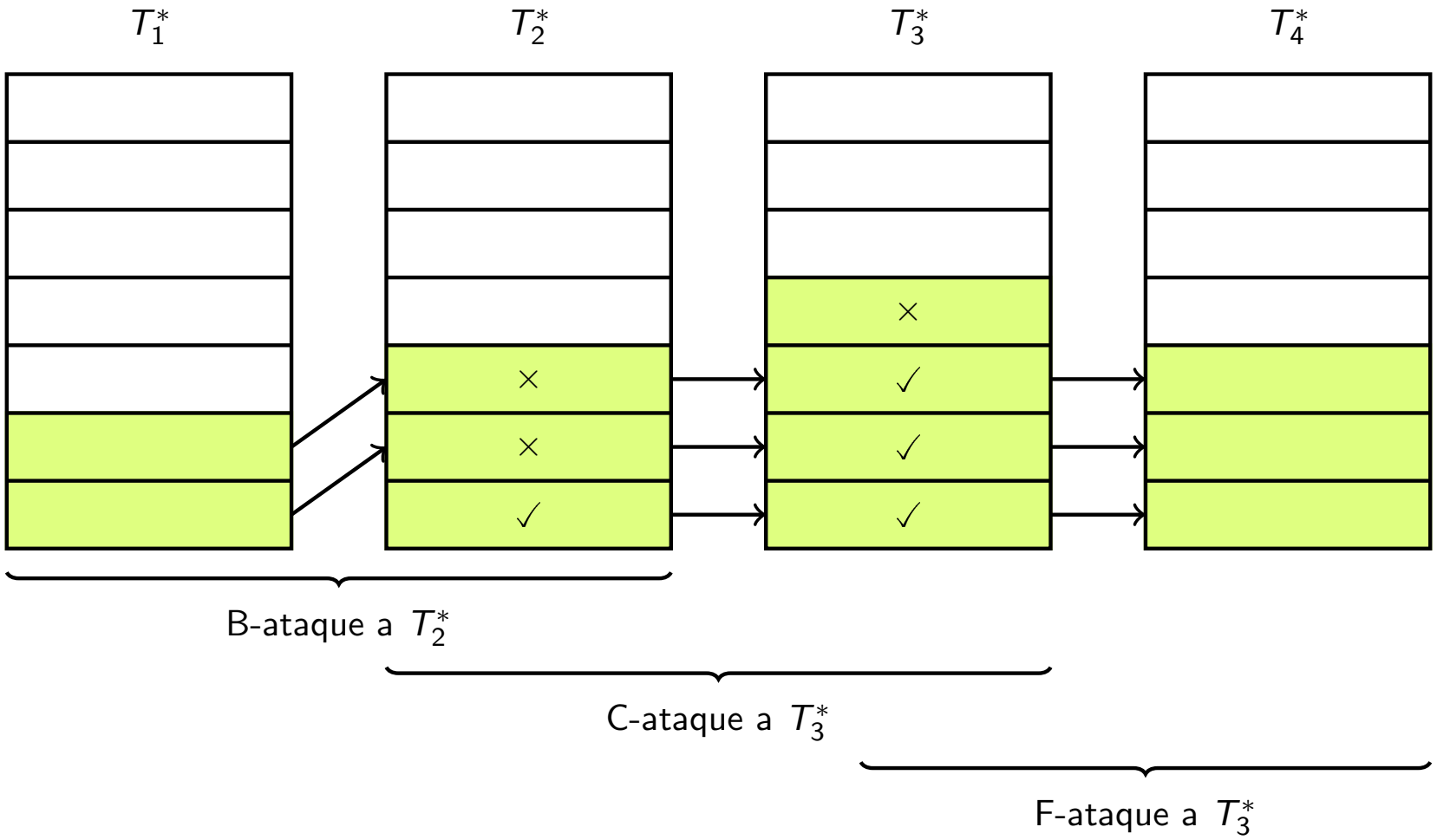
- Solo necesita conocimiento de los QI y participación.
- Puede aplicarse en cualquier base de datos no estática.
- Si no son prevenidos, pueden revelar el dato sensible inequívocamente.
- Se pueden evitar manteniendo la "firma" de cada tupla constante entre publicaciones.

	I	D	C.D.
MÍNIMO	×		
INCOMPLETO	×		
OBJETIVO	×	×	×
LIMITADO	×	×	×
COMPLETO	×	×	×
INTERIOR	×	×	×
PROB.	×	×	×

Cuadro: Combinaciones donde puede aplicarse un ataque de intersección.

Firma de una tupla: conjunto de datos sensibles de su clase.

Ataque de correspondencia



B: $p \in T_2^*$.

C: $p \in T_2^*, T_3^*$.

F: $p \in T_3^*, T_4^*$.

Ataque de correspondencia: ejemplo

Sea p un usuario con $p[QI] = [FRANCIA, ABOGADO]$ y $p \in T_1^*, T_2^*$.

Id	ORIGEN	JOB	D.S.
1	EU	ABG.	FIEBRE
2	EU	ABG.	FIEBRE
3	EU	ABG.	FIEBRE
4	EU	ABG.	VIH
5	EU	ABG.	VIH

(a) T_1^*

Id	ORIGEN	JOB	D.S.
1	UK	PROF.	FIEBRE
2	UK	PROF.	FIEBRE
3	UK	PROF.	FIEBRE
9	UK	PROF.	VIH
10	UK	PROF.	VIH
4	FRANCIA	PROF.	VIH
5	FRANCIA	PROF.	VIH
6	FRANCIA	PROF.	VIH
7	FRANCIA	PROF.	FIEBRE
8	FRANCIA	PROF.	FIEBRE

(b) T_2^*

Figura: Ejemplo de F-ataque en una base de datos incremental (buscar p en T_1^*).

- No todos los registros en T_1^* (en verde/rojo) pueden ser de la forma $[FRANCIA, ABOGADO, FIEBRE]$ porque solo hay 2 tuplas de esa forma en T_2^*.

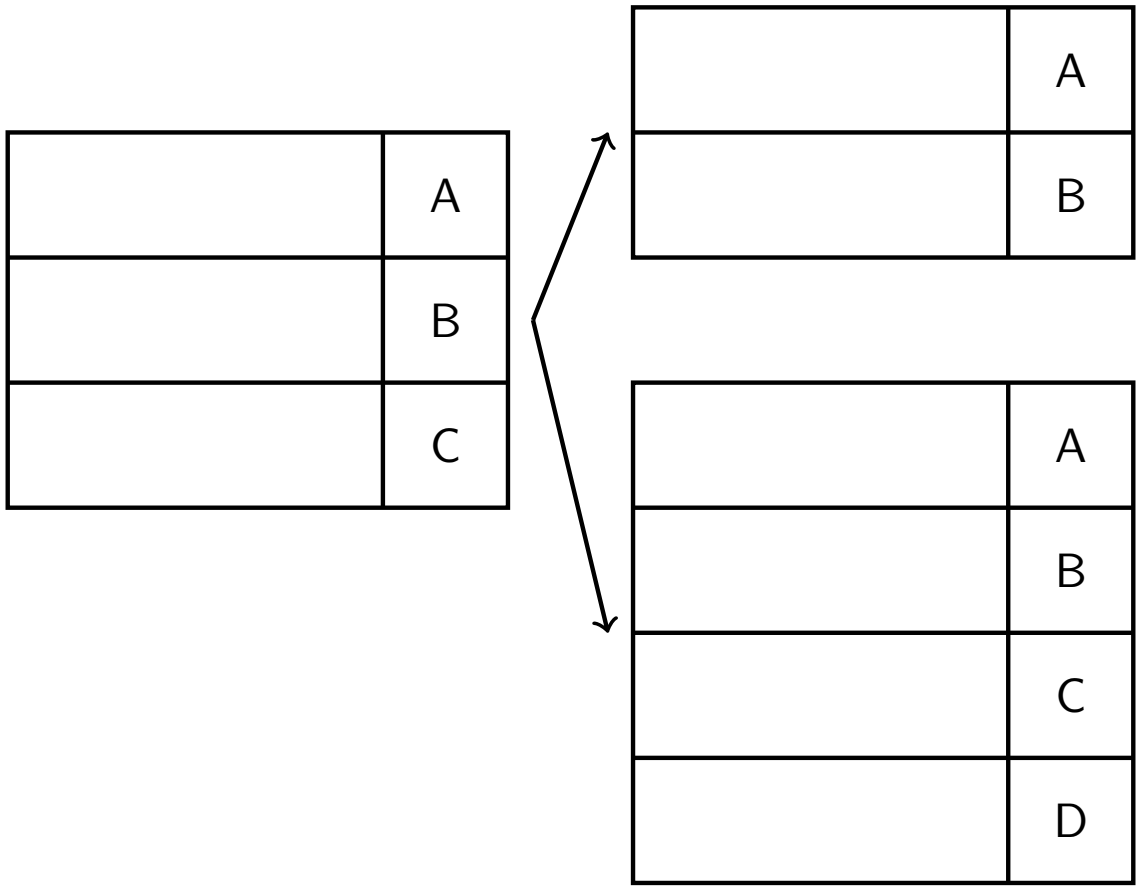
Ataque de correspondencia

- Reduce el número de tuplas candidato de un usuario.
- Abusa de la multiplicidad de tuplas con la misma información.
- Se pueden evitar manteniendo la multiplicidad constante en cada clase.

	I	D	C.D.
MÍNIMO			
INCOMPLETO			
OBJETIVO	x	x	x
LIMITADO	x	x	x
COMPLETO	x	x	x
INTERIOR	x	x	x
PROB.	x	x	x

Cuadro: Combinaciones donde puede aplicarse un ataques de correspondencia.

Ausencia/Presencia crítica



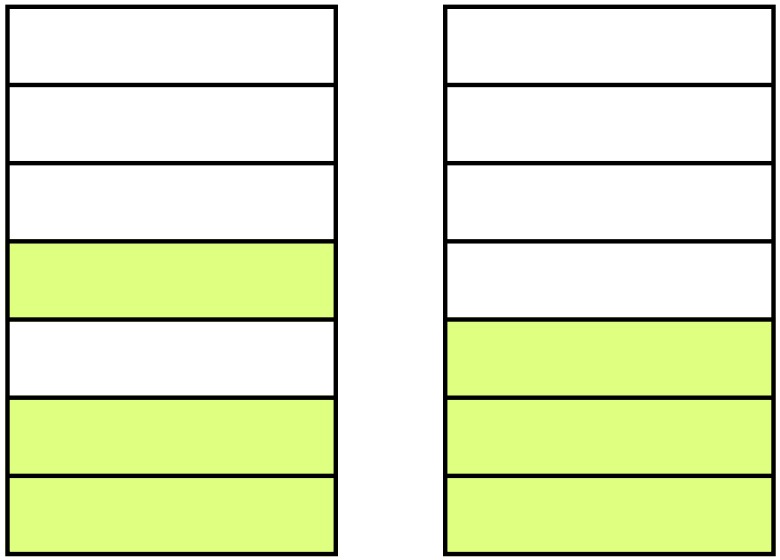
Ausencia/Presencia crítica

- Ataca a las tuplas insertadas y/o eliminadas.
- Se puede evitar asegurando el tamaño de tuplas insertadas/eliminadas.
- Se puede evitar con tuplas falsas o reteniendo información.

	I	D	C.D.
MÍNIMO			
INCOMPLETO			
OBJETIVO	×	⊗	⊗
LIMITADO	×	⊗	⊗
COMPLETO	×	⊗	⊗
INTERIOR	×	⊗	⊗
PROB.	×	⊗	⊗

Cuadro: Combinaciones donde puede aplicarse ausencia crítica (◯) y presencia crítica (×).

Ataque de equivalencia



Ataque de equivalencia: ejemplo

Sabemos los QI y participación en cada publicación. En particular del usuario 3.

ID	EDAD	SEXO	D.S.
1	[18-20]	VARÓN	FIEBRE
3	[18-20]	VARÓN	ACNÉ
2	[21-22]	MUJER	FIEBRE
4	[21-22]	MUJER	VIH

(a) T_1^*

ID	EDAD	SEXO	D.S.
1	[20-22]	-	FIEBRE
4	[20-22]	-	VIH
3	[18-19]	VARÓN	ACNÉ
5	[18-19]	VARÓN	FIEBRE

(b) T_2^*

Figura: Ejemplo de ataque de equivalencia.

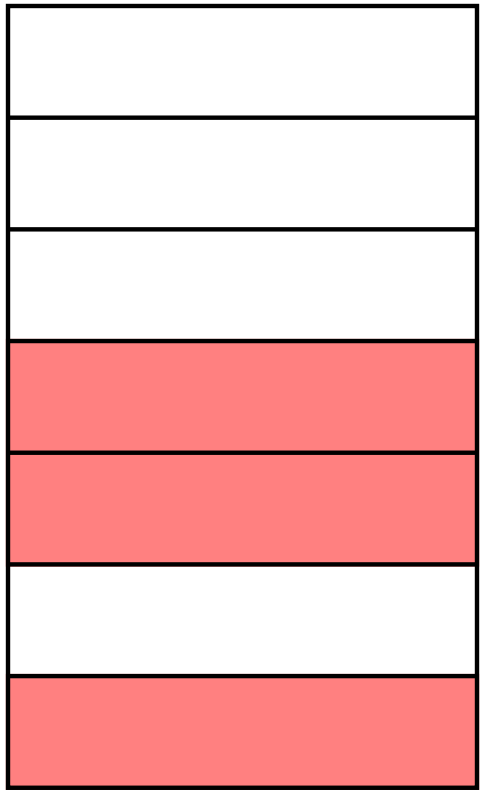
Ataque de equivalencia

- Relaciona conjuntos de tuplas con el mismo multiconjunto de datos sensibles.
- No causa revela información por si mismo.
- Combinado con información interior puede causar un efecto cascada.

	I	D	C.D.
MÍNIMO			
INCOMPLETO			
OBJETIVO			
LIMITADO	x	x	x
COMPLETO	x	x	x
INTERIOR	x	x	x
PROB.	x	x	x

Cuadro: Combinaciones donde puede aplicarse un ataque de equivalencia.

Ataque interior



Ataque interior: ejemplo

Asumimos el conocimiento de los cuasi identificadores, participantes, publicaciones y dato sensible del usuario 3.

ID	EDAD	SEXO	D.S.
1	[18-20]	VARÓN	FIEBRE
3	[18-20]	VARÓN	ACNÉ
2	[21-22]	MUJER	FIEBRE
4	[21-22]	MUJER	VIH

(a) T_1^*

ID	EDAD	SEXO	D.S.
1	[20-22]	-	FIEBRE
4	[20-22]	-	VIH
3	[18-19]	VARÓN	ACNÉ
5	[18-19]	VARÓN	FIEBRE

(b) T_2^*

Figura: Ejemplo de ataque interior $(3 \rightarrow 5, 1 \rightarrow 4 \rightarrow 2)$.

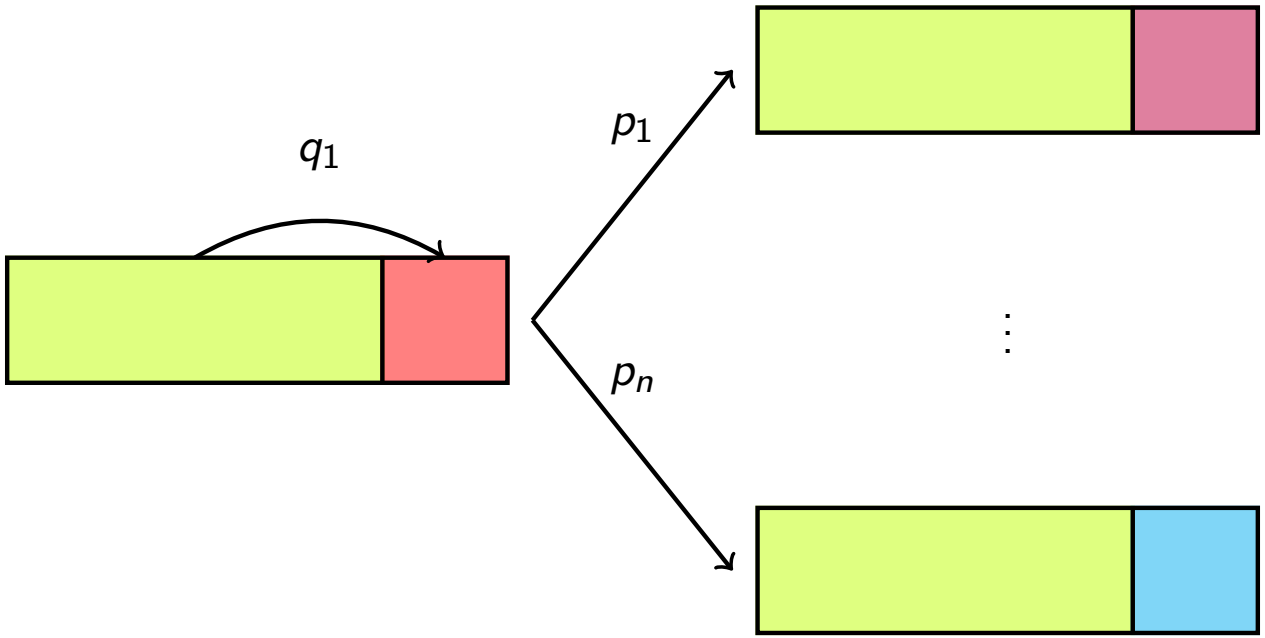
Ataque interior

- Usa el conocimiento de un subconjunto para comprometer el resto de tuplas.
- No puede ser prevenido en general. Se puede acotar la probabilidad de éxito asumiendo una cota constante a la información del atacante.
- Se puede ejecutar con información probabilística.

	I	D	C.D.
MÍNIMO			
INCOMPLETO			
OBJETIVO			
LIMITADO			
COMPLETO			
INTERIOR	x	x	x
PROB.	p	p	p

Cuadro: Combinaciones donde puede aplicarse un ataque interior (p probabilístico).

Ataque probabilístico



Ataque probabilístico: ejemplo

ID	EDAD	D.S.
1	[20-60]	ANSIEDAD
4	[20-60]	DIABETES II

(a) T_1^*

ID	EDAD	D.S.
1	[20-60]	DEPRESIÓN
4	[20-60]	PANCREATITIS

(b) T_2^*

Figura: Ejemplo de ataque probabilístico.

Ataque probabilístico

- Busca los atributos sensibles más probables y sus posibles actualizaciones.
- Se asume un atacante informado o que la distribución de la base de datos es conocida para el público.
- Abarca el caso particular de los datos sensibles permanentes.
- No se tiene una solución en su caso más general.

	I	D	C.D.
MÍNIMO			
INCOMPLETO			
OBJETIVO			
LIMITADO			
COMPLETO			
INTERIOR			
PROB.	x	x	x

Cuadro: Combinaciones donde puede aplicarse un ataque probabilístico.

Contenidos

Nociones Sintácticas

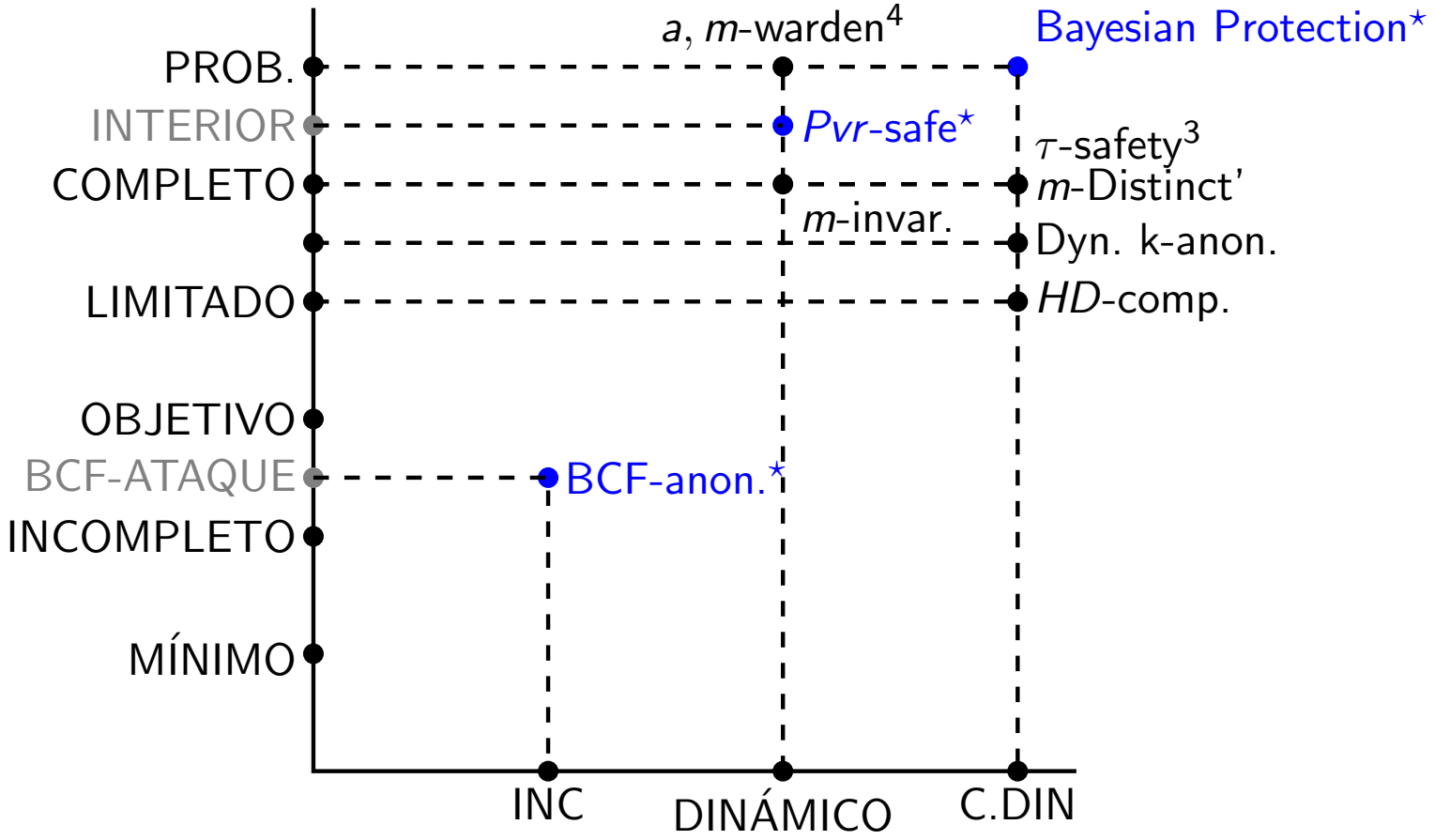


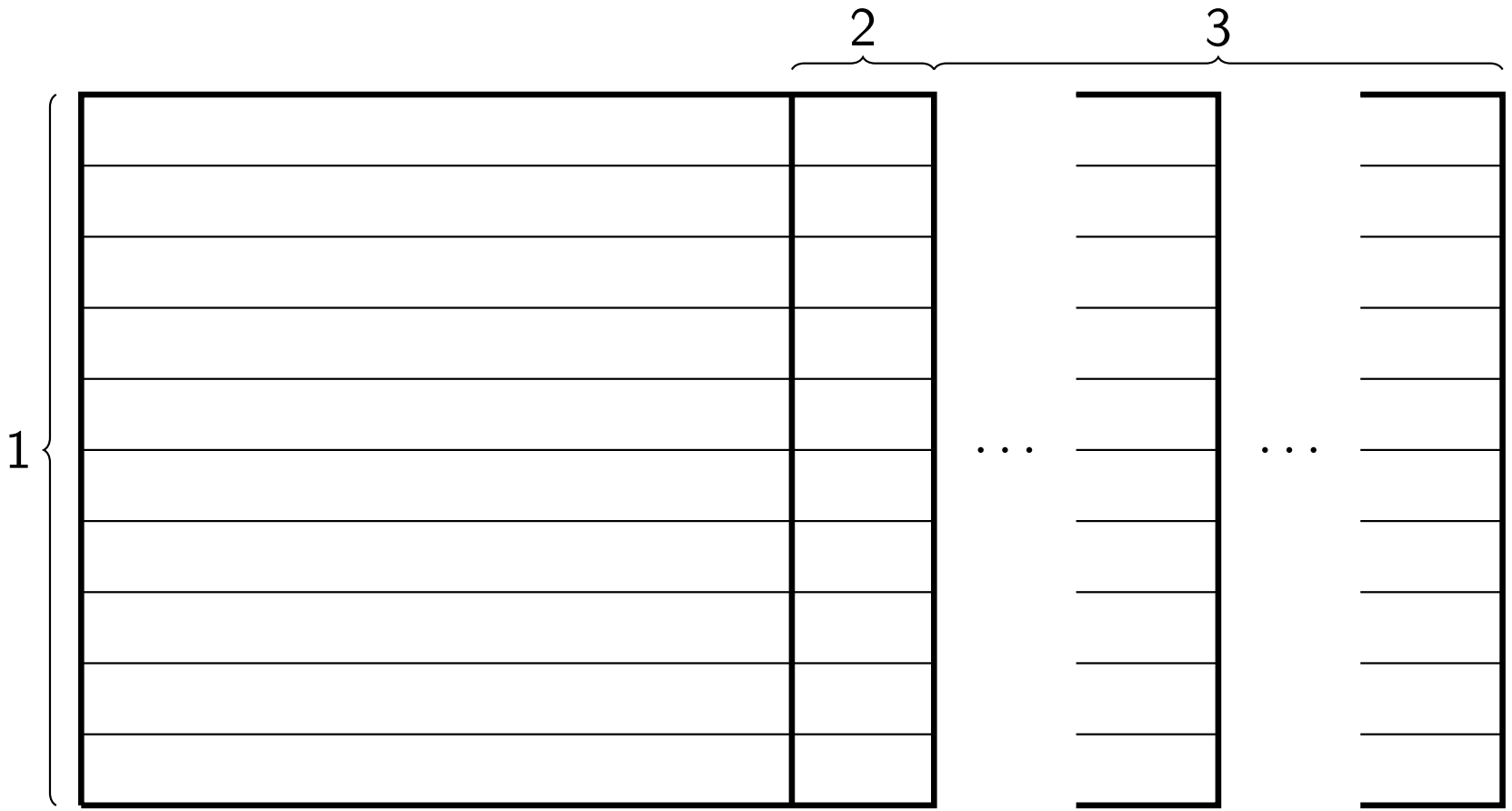
Figura: Nociones sintácticas para publicación continua.

[3]Y sus variaciones: (τ, m)-slicedBucket y τ-safe (l, k)-diversity.

[4]Nuestro trabajo actual.

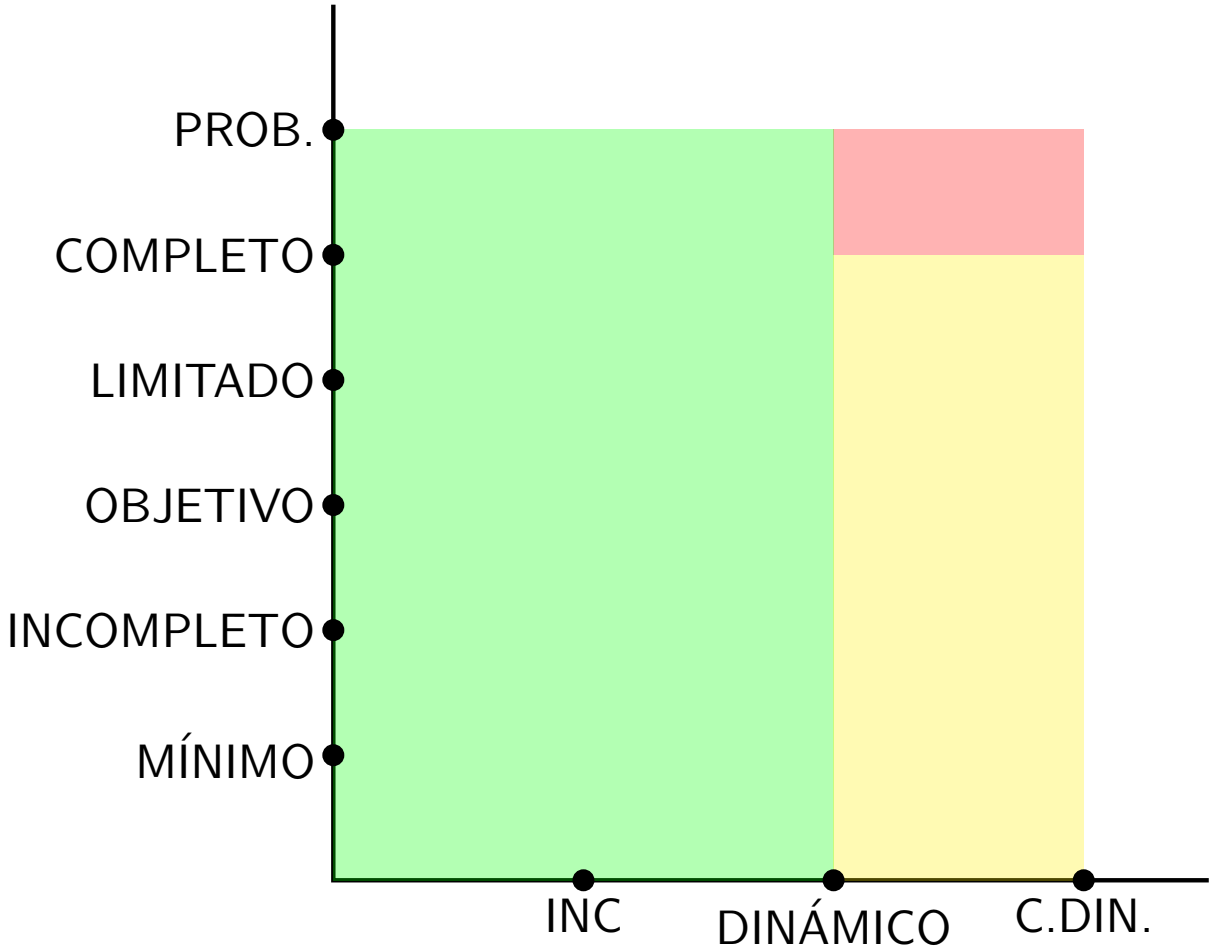
$\star$: Dan privacidad solo ante ataques concretos.

Idea detrás de las principales nociones



1 Mantenemos una noción de privacidad sintáctica estática p.e. l-diversidad.
2 Las clases no tienen repeticiones del mismo dato sensible (m-unicidad).
3 Para cada tupla, su clase mantiene la misma firma entre publicaciones.

Estado del arte: garantías de privacidad



- Verde: noción incondicional con garantía de privacidad.
- Amarillo: noción condicional con noción de privacidad (se asumen propiedades extra).
- Rojo: no hay noción y/o garantía de privacidad adecuada.

Contenidos

Conclusiones

- Hemos visto y ejemplificado los ataques clásicos de la literatura en publicación continua.
- Ponemos en contexto los mecanismos de protección más relevantes.
- Presentamos el estado de la cuestión en relación a en qué casos se puede dar una garantía de privacidad para diferentes atacantes y bases de datos.

Fin de la presentación[5]

[5]El proyecto del que se obtuvieron estos resultados fue financiado por el Gobierno de España bajo el proyecto de investigación "Enhancing Communication Protocols with Machine Learning while Protecting Sensitive Data (COMPROMISE)" (PID2020-113795RB-C31/AEI/10.13039/501100011033). Este trabajo también ha sido apoyado por una beca de Fundación "la Caixa" (ID 100010434) y por el programa de investigación e innovación European Union's Horizon 2020 bajo el acuerdo Marie Skłodowska-Curie No 847648. Con código de beca LCF/BQ/PR20/11770009.