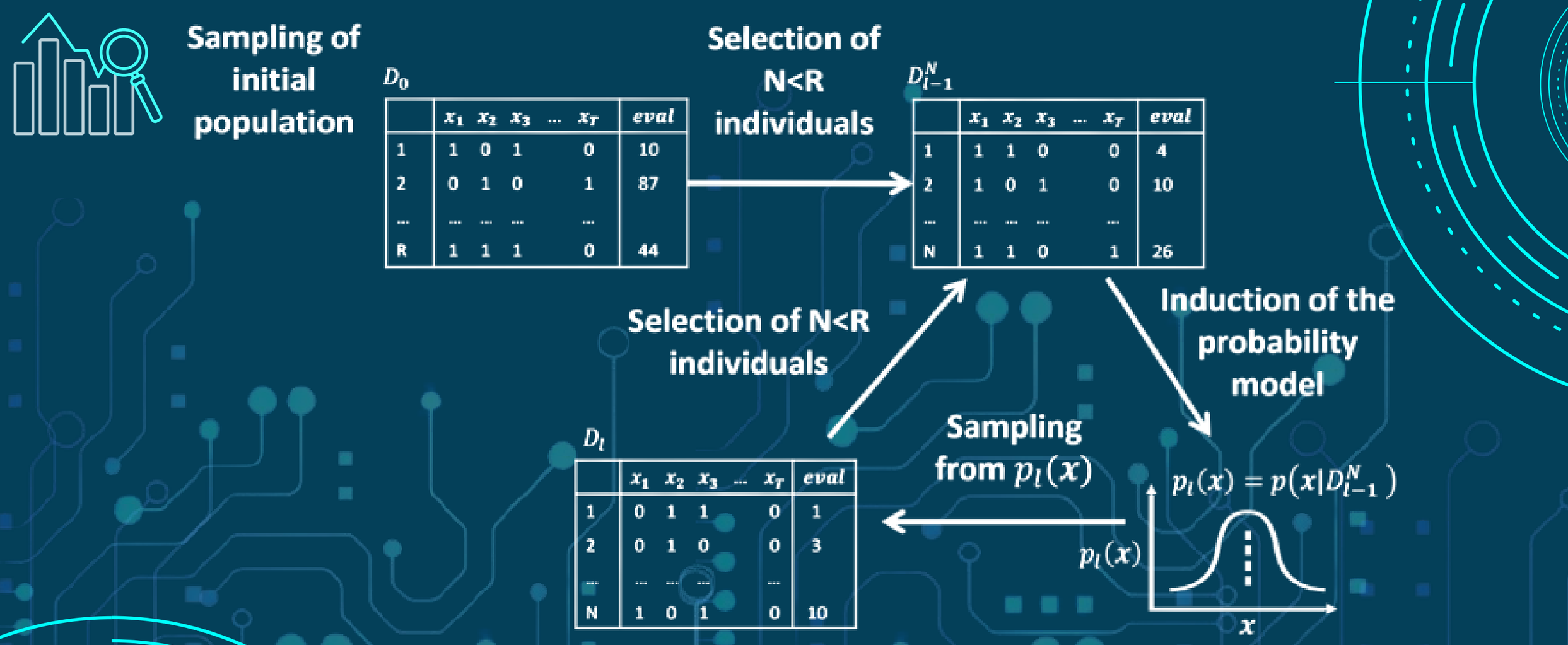
UTILIZACIÓN DE ALGORITMOS DE ESTIMACIÓN DE DISTRIBUCIONES PARA OPTIMIZAR ATAQUES DE CANAL LATERAL

Autor: Asier Insausti Carmona
Tutor: José Antonio Pascual

El Análisis de Canal Lateral es un conjunto de ataques que sirven para obtener las claves de cifrado de dispositivos embebidos. Dichos ataques son complejos de llevar a cabo, por lo que existe una gran posibilidad de cometer errores, además de necesitar la presencia humana para su correcto ajuste y funcionamiento. Una posible solución para minimizar esta dependencia es el uso de Algoritmos de Estimación de Distribuciones. En el presente proyecto, en colaboración con el centro tecnológico de Ikerlan, se propone crear una herramienta que implemente este tipo de algoritmo para realizar ataques de Canal Lateral, y con ello, evaluar dispositivos y comprobar su protección ante los ataques efectuados sin requerir de la presencia humana.



	x_1	x_2	x_3	...	x_T	*eval*
1	1	0	1		0	10
2	0	1	0		1	87
...	...	...	...		...	
R	1	1	1		0	44

	x_1	x_2	x_3	...	x_T	*eval*
1	1	1	0		0	4
2	1	0	1		0	10
...	...	...	...		...	
N	1	1	0		1	26

	x_1	x_2	x_3	...	x_T	*eval*
1	0	1	1		0	1
2	0	1	0		0	3
...	...	...	...		...	
N	1	0	1		0	10

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
ikerlan
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE
informatika fakultatea
facultad de informática