■ 目　次

表 記法

記法	定義	記法	定義
$\mathbb{N}$	自然数集合	x	データ, 入力, 平文
$\mathbb{Z}$	整数集合	X	データの定義域
$\mathbb{R}$	実数値集合	n	データ数
$\emptyset$	空集合	d	データの属性数/次元数
$\mathbb{Z}/q\mathbb{Z}$	q を法とする剰余環	D	データ集合/データベース
$\{0,1\}^*$	任意長のビット列	$\mathcal{D}$	データ集合/データベースの定義域
poly	(任意の) 多項式	f	データ解析関数
negl	無視できる関数	q	クエリ
$\mathcal{A}$	確率的多項式アルゴリズム	y	出力
κ	セキュリティパラメータ	Y	出力の定義域
H	暗号学的ハッシュ関数	Ω	確率変数の定義域
k	秘密鍵暗号の鍵	S	確率変数の定義域の部分集合
pk	公開鍵暗号の公開鍵	Δ	大域敏感度
sk	公開鍵暗号の秘密鍵	m	メカニズム
Gen	鍵生成関数	$\lvert\cdot\rvert$	絶対値, 集合/ビット列のサイズ
Enc	暗号化関数	$\lVert\cdot\rVert$	ノルム
Dec	復号関数	$a \Vert b$	bit 例 a, b の連結
$\oplus$	加法準同型演算	$a \boxplus b$	bit 例 a, b の排他的論理和
$\otimes$	乗法準同型演算	$a \in_R A$	集合 A からのランダム要素選択