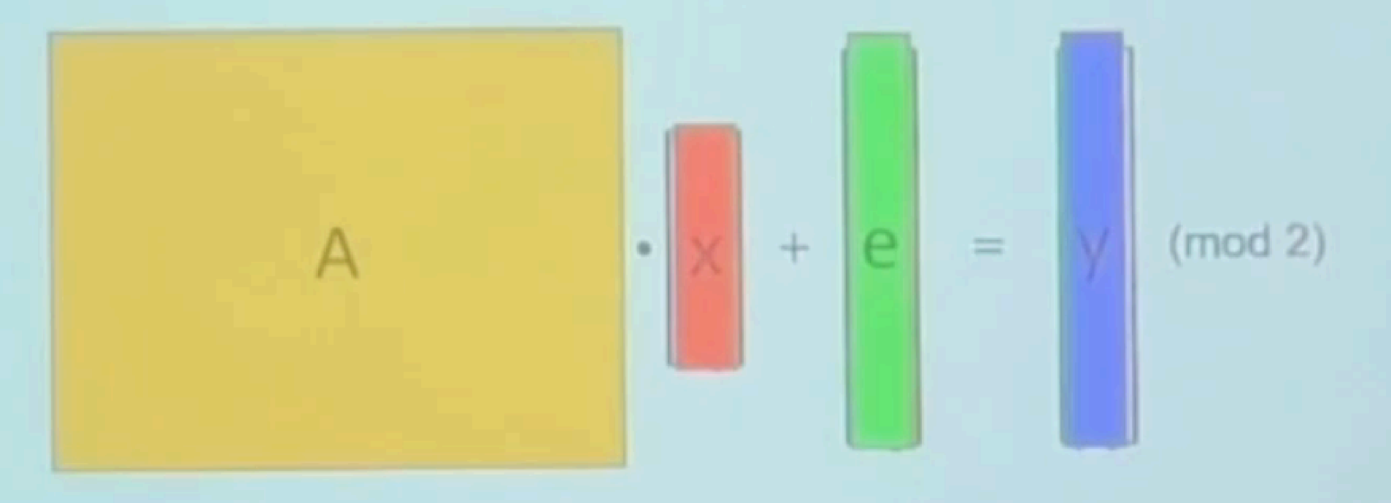
Learning Party with Noise (LPN)

Problem Discription

For $A \xleftarrow{\$} \mathbb{Z}_2^{m\times n}$, $x \xleftarrow{\$} \mathbb{Z}_2^{n}$, $e \sim Bern_\mu^m$, $\hat{y} =_{mod\,2} Ax + e$;



$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \\ a_{61} & a_{62} & a_{63} & a_{64} & a_{65} \\ a_{71} & a_{72} & a_{73} & a_{74} & a_{75} \\ a_{81} & a_{82} & a_{83} & a_{84} & a_{85} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \\ e_7 \\ e_8 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \end{bmatrix} \pmod 2$$

Given A, x, find out x; $\Leftrightarrow_{poly}$ Distinguish between $(A, y)\&(A, z \xleftarrow{\$} \mathbb{Z}_2^n)$

noise rate: $Pr(e_i = 1) = \mu$��

Evaluation

However, this is a very hard question. The complexity of this problem is based on different noise rates and assumptions:

Noise rate μ	**Assumption**		**Attack**
0<O(1)<0.5	Standard LPN	Sub-exp LPN	BKW attack
	$\geq n^{\omega(1)}$	$\geq 2^{\Omega(n^{0.5})}$	$\leq 2^{O(\frac{n}{logn})}$
$\frac{1}{\sqrt{n}}$	Low-noise LPN	Sub-exp low-noise LPN	best attack
	$\geq n^{\omega(1)}$	$\leq 2^{\Omega(\frac{\sqrt{n}}{logn})}$	$\leq 2^{O(\sqrt{n})}$
$\frac{(logn)^2}{n}$	Extremely low-noise LPN		best attack
	$\geq n^{\omega(1)}$		$\leq 2^{O(logn)}$