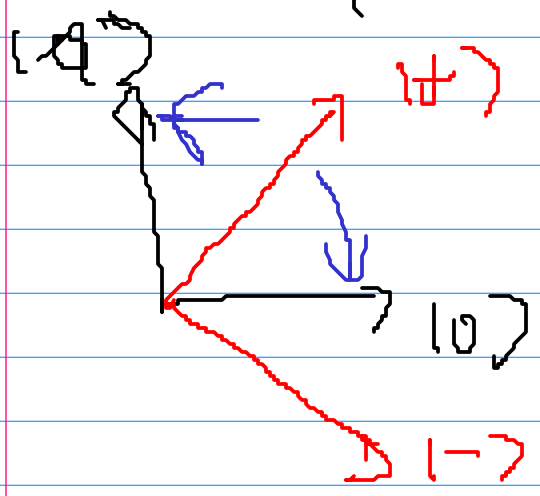


|||

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

b_0, b_1, \dots, b_{i-1}



$|+\rangle$

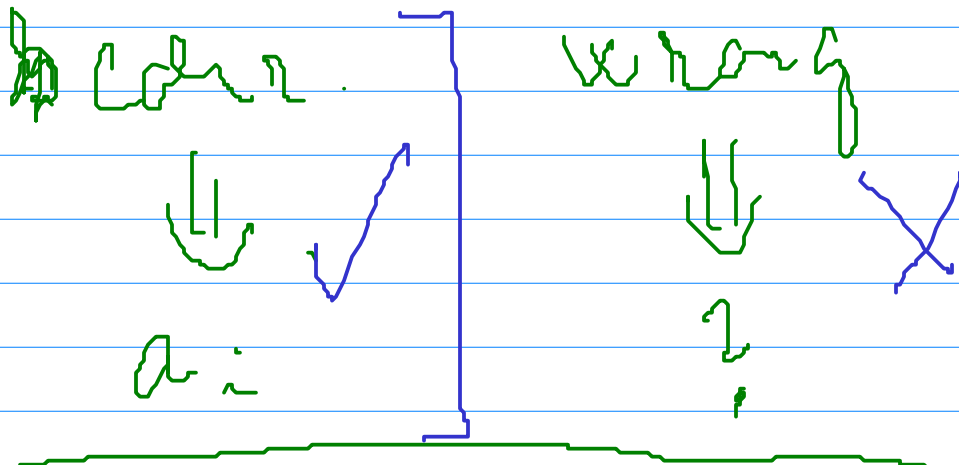
$M \sim |0\rangle, |1\rangle$

partou hilt
destroyed

guess of b_i

$$c_0, c_1, \dots, c_n = a$$

measure in binary c_i



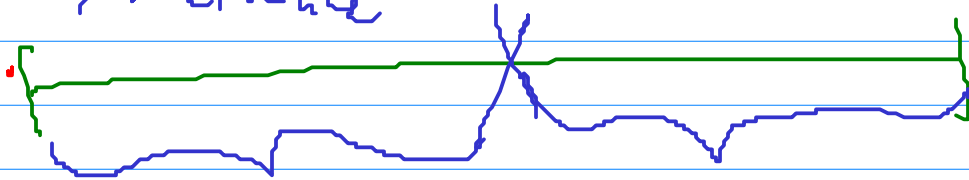
b_i PUBLISH a_i

a_i

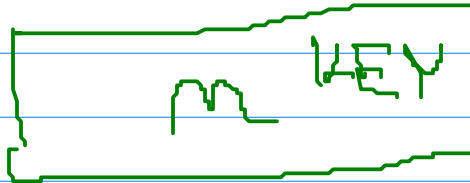
~ 1/2 of bits correct
(47%) more 2M correct

$$\underbrace{e_i}_{a_i} \left\{ \begin{array}{l} b_i \neq \underbrace{c_i} \\ || \\ c_i \end{array} \right.$$

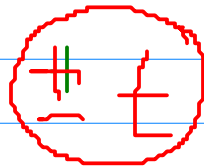
signature estimate 2m



TEST



$a_i = \hat{a}_i$



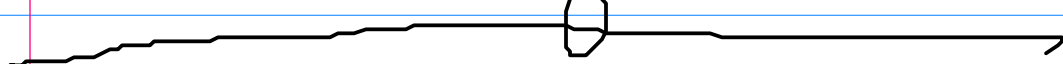
$A = B$

55 - Eve's body

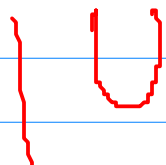
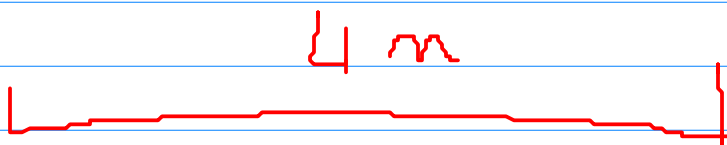
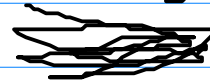
$b_i = c_i$ - Alice's body

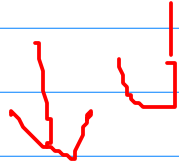
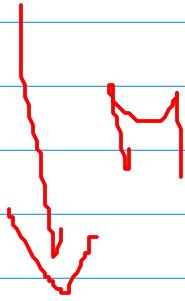
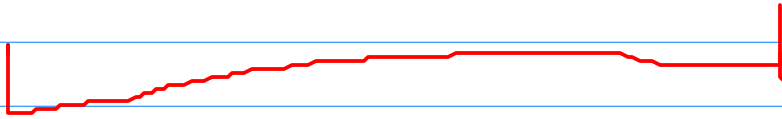
- error correction

- hashing



SECURITY PROOF





BLDCM

