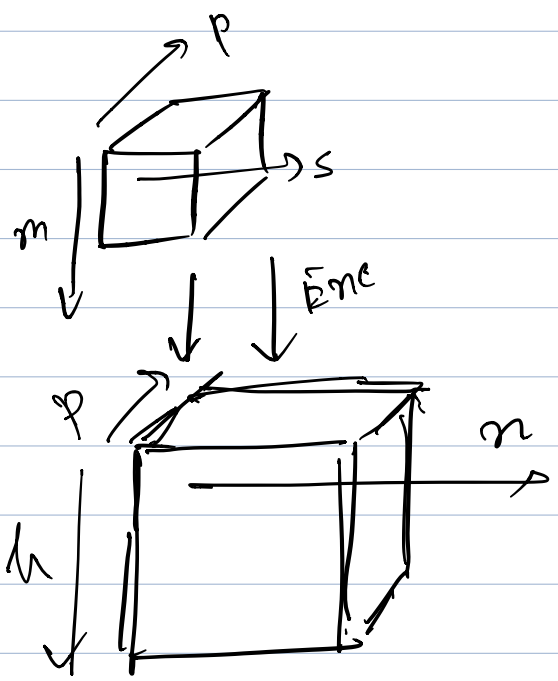
$N = pms$ – circuit size

Soundness – $2^{-\lambda}$

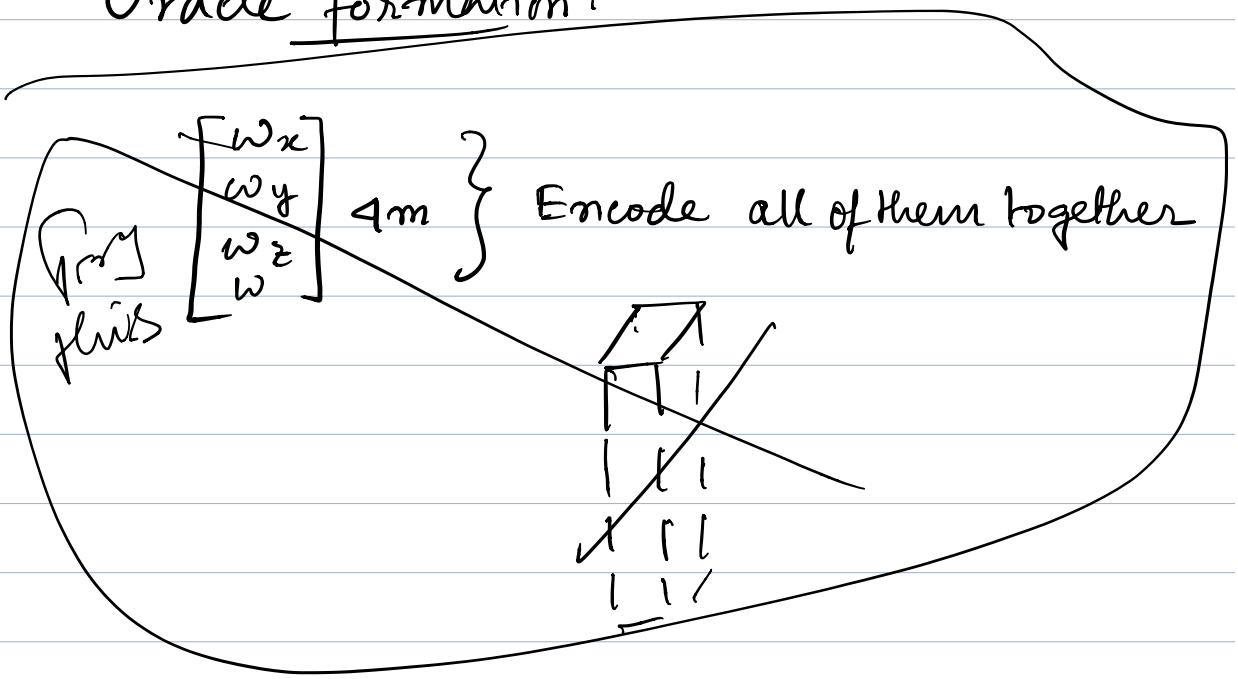
Proof size :



Verifier's time :

Prover's time :

Oracle formation :



Proof size: $4\ell + 3(s+\ell) + t \cdot 3p$

$+ t \cdot 3p$

$2\ell + t3p + 3pt$

Inner product: $8t(2\log m + 2)$

(Groth inner product)

Total = $16t \log m + 20t + 9\ell + 3s + 12tp$

Verifier's Time:

$O(N) + 8t$

$Aw = xw_x$

$\begin{bmatrix} A & -I \end{bmatrix} \begin{bmatrix} w \\ xw_x \end{bmatrix} = 0$

$Aw = b$

Check optimization of combining of Lincheck

$O(N) + 4t \cdot mult\text{-}exp(2m) + 4t \cdot mult\_exp(m)$

Prover's Complexity:

Encoding time: $4pm(FFT(\ell)+FFT(n)) + 4pn(FFT(m)+FFT(h))$

Commiting time: $p\ell \cdot mult\_exp(m) + p(n-\ell) \cdot mult\_exp(\min(\ell, m))$

Subprotocol: $8tm\ exp$

Soundness: $b\lambda$

$$(1-\frac{e}{n})^t + 2\left[\frac{2m}{h} + \left(1-\frac{2m}{h}\right)\left(\frac{2\ell+e}{n}\right)\right]^t$$

$n = 7\ell$, $h = 8m$,

$e \le \frac{n-\ell}{3} = 2\ell$

$$\frac{1}{4} + \frac{3}{4}\cdot\frac{4}{7} = \frac{19}{28}$$

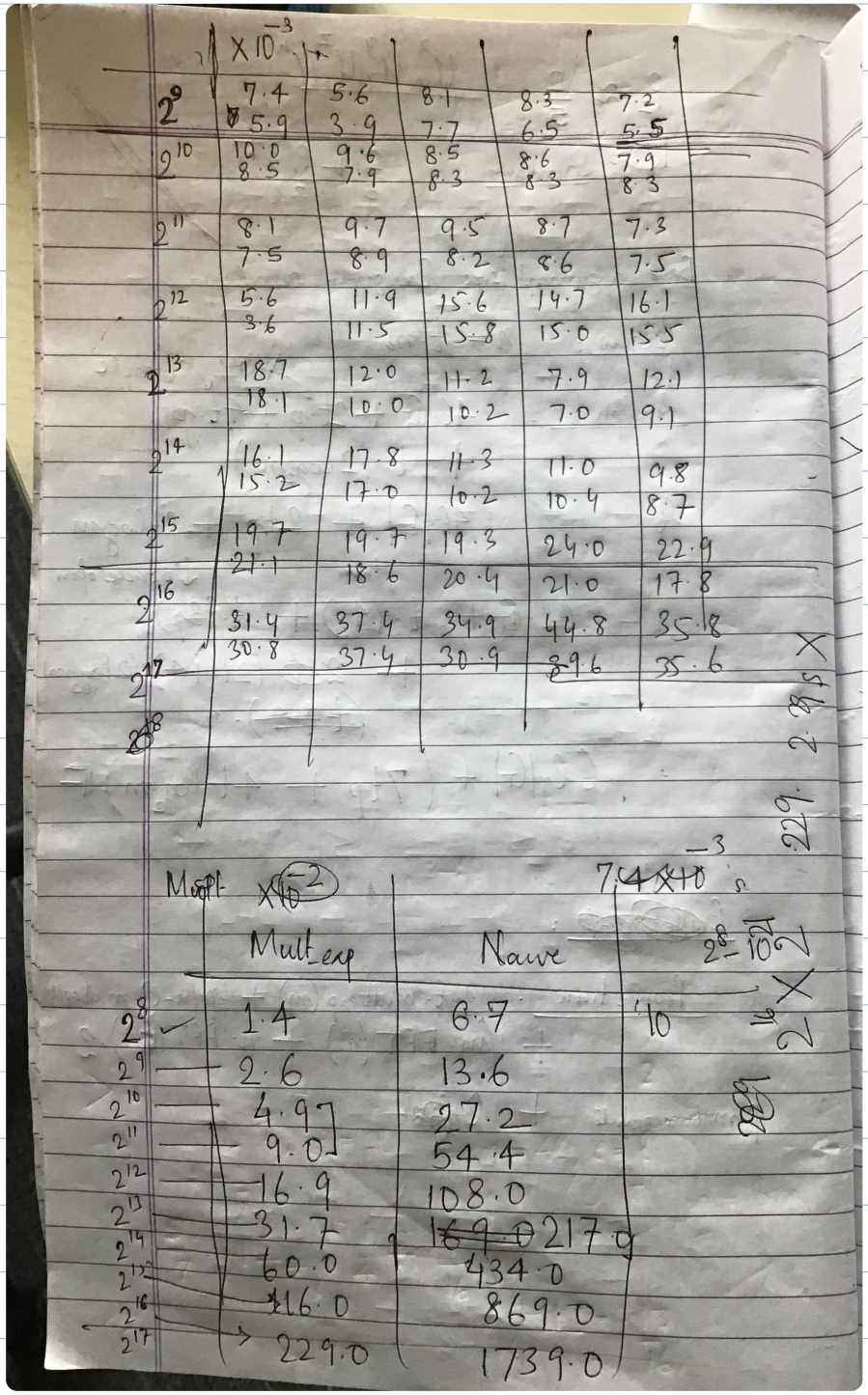
$t = 2\lambda$

$\ell = s+k$

$n = 7\ell$

$h = 8m$

$N = 10^6$



	$\times 10^{-3}$				
2^9	7.4	5.6	8.1	8.3	7.2
	5.9	3.9	7.7	6.5	5.5
2^{10}	10.0	9.6	8.5	8.6	7.9
	8.5	7.9	8.3	8.3	8.3
2^{11}	8.1	9.7	9.5	8.7	7.3
	7.5	8.9	8.2	8.6	7.5
2^{12}	5.6	11.9	15.6	14.7	16.1
	3.6	11.5	15.8	15.0	15.5
2^{13}	18.7	12.0	11.2	7.9	12.1
	18.1	10.0	10.2	7.0	9.1
2^{14}	16.1	17.8	11.3	11.0	9.8
	15.2	17.0	10.2	10.4	8.7
2^{15}	19.7	19.7	19.3	24.0	22.9
	21.1	18.6	20.4	21.0	17.8
2^{16}	31.4	37.4	34.9	44.8	35.8
	30.8	37.4	30.9	39.6	35.6
2^{17}					
2^{18}					

$229 \cdot 2 \cdot 8 \times$

7.4×10^{-3}

$2^8 = 10^2$

$\times 2$

	Mult $\times 10^{-2}$	
	Mult_exp	Naive
2^8	1.4	6.7
2^9	2.6	13.6
2^{10}	4.9	27.2
2^{11}	9.0	54.4
2^{12}	16.9	108.0
2^{13}	31.7	217.0
2^{14}	60.0	434.0
2^{15}	116.0	869.0
2^{16}	229.0	1739.0
2^{17}		

$N = 10^6$ $\quad\quad$ $\lambda = 80$

$t = 160$

$m = 400$
$p = 50$
$s = 50$
$\Rightarrow$ $h = 3200$, $\ell = 210$, $n = 1470$ — 20 bytes

$$\text{Total} = 16t \log m + 20t + 9\ell + 3s + 12tp$$

proof size:

$(16 \times 160 \times 9 + 20 \times 160 + 12 \times 160 \times 50) \times 20$ bytes

$= (25000 + 3200 + 96{,}000) = \frac{1{,}20{,}000 \times 20}{1000}$

$= 2.4$ mb.

Prover's time to commit:

$p\ell$.mult_exp(m) +
$p(n-\ell)$.mult_exp(min(ℓ, m))

3176230 $\longrightarrow$ .882 hours

$210 \times 50 \times 0.02 = 105 \times \frac{2}{100} = 210$

$50 \times 1260 \times 0.01 = 630$

$8 \times 160 \times 400 \times 0.1/256 = 200$

1040 sec.

$= 18\ m$

$= .28$ hrs.

Verifier's time:

$O(N) + 4t \cdot mult\text{-}exp(2m) + 4t \cdot mult\_exp(m)$

$4 \times 160 \times [0.045 + 0.02]$

$= 4 \times 160 \times 0.065$

$= 42$ sec

Around 60 sec for verification

$p = 50$ $m = 200$ $s = 100$	Proof size – 2.43 mb Prover time – 0.32 hrs Verifier time – 19 sec (Ex. field op)

$p = 50$ $m = 150$ $s = 200$	Proof Size – 2.4 mb Prover time – 0.4 hr Verifier time – 10 sec

$p = 10$ $m = 200$ $s = 500$	Proofsize – .99 mb Prover time – 641 sec Verifier – 19 sec (Ex. field)

$p = 2$ $m = 500$ $s = 1000$	Proof size - .87 mb Prover time - 477 sec Verifier time - 48 sec.

$p = 5$ $m = 200$ $s = 1000$	Proof size - .92 mb Prover time - 576 sec Verifier time - 19.2 sec.