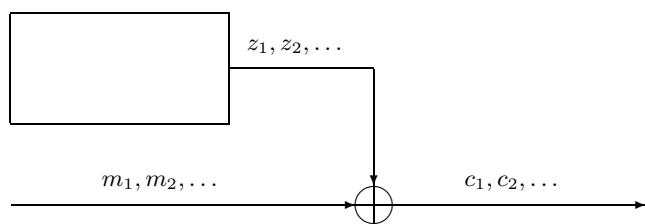


$$\begin{matrix}z_1,z_2,\dots\\m_1,m_2,\dots\\K\end{matrix}\qquad\qquad\qquad\begin{matrix}c_1,c_2,\dots\\K\end{matrix}$$

$$\begin{matrix}K&&&z_1,z_2,\dots,z_N\\&&&z_1,z_2,\dots,z_N\\&&&K\end{matrix}$$

$$K$$



$$u_1,u_2,\ldots$$

$$P(u_i=z_i)\neq 1/2,\quad i\geq 1.$$

$$\mathop{f}\limits^f$$

$${z}_n$$

$$\begin{array}{ccc} l & & g(x) \\ 2^l & & \\ \mathbf{z} = z_1, z_2, \dots, z_N & & N \\ u_i & z_i & \\ 1/2 + \epsilon & 1/2 + \epsilon = P(u_i = z_i) & 0 < \epsilon < 1/2 \\ & & (z_1, z_2, \dots, z_N) \end{array}$$

$$N \gg N_0 = l/(1 - h(p))$$

$$\mathbf{u} = (u_1, u_2, \dots, u_l).$$

$$u_i=\sum_{j=1}^lg_ju_{i-j},\quad i>l,$$

$$\begin{matrix}g(x)=1+g_1x+\ldots g_lx^l\\ \mathbf u\end{matrix}\qquad\qquad\qquad u_i$$

$$u_i = \sum_{j=1}^l w_{ij} u_j, \quad \forall i \geq 1,$$

$$\begin{matrix}w_{ij}, i\geq 1, 1\leq j\leq l\\ g(x)\end{matrix}$$

$$U(\mathbf{x})$$

$$U(\mathbf{x})=U(x_1,x_2,\dots,x_l)=u_1x_1+u_2x_2+\cdots+u_lx_l.$$

$$\begin{matrix}\mathbf x_i \\ u_i\end{matrix}=(w_{i1},w_{i2},\ldots,w_{ij})$$

$$u_i=U(\mathbf{x}_i),\quad i\geq 1.$$

$$\begin{matrix}u_i\\z_i\end{matrix}$$

$$\mathbf e=(e_1,e_2,\ldots,e_N),$$

$$\begin{matrix}e_i\in\mathbb F_2\\1/2+\epsilon\end{matrix}\qquad\qquad\qquad\begin{matrix}1\leq i\leq N\\\mathbf z=\mathbf u+\mathbf e\end{matrix}\qquad\qquad\qquad P(e_i=0)=$$

$$\mathbf z=(U(\mathbf{x}_1)+e_1,U(\mathbf{x}_2)+e_2,\ldots,U(\mathbf{x}_N)+e_N),$$

$$\begin{matrix}\mathbf x_i\\l\end{matrix}\qquad\qquad\qquad\begin{matrix}1\leq i\leq N\end{matrix}$$

$$\begin{matrix}\mathbf z\\ \{\mathbf x_1,\mathbf x_2,\ldots\mathbf x_N\}\\ U(\mathbf x)\end{matrix}$$

$$\begin{matrix}\mathcal F\\ \delta\\ \delta\end{matrix}\qquad\qquad\qquad\begin{matrix}f:F^l\rightarrow F\\ g\in\mathcal F\\ f\end{matrix}$$

F

$$\begin{array}{ccccccc}
& \mathcal{F} & & & l & & \\
& d & & F = \mathbb{F}_2 & & & \\
\epsilon > 0 & & l/\epsilon & & & f : F^l \rightarrow F & \\
& f & & \delta = 1/2 + \epsilon & & l & \\
& & & & & & \\
& & & \mathbf{x} & & & \\
p(\mathbf{x}) & & e & & & p(\mathbf{x}) + e &
\end{array}$$

$$p(\mathbf{x}) = \sum_{i=1}^l c_i x_i.$$

$$\begin{array}{lll} (c_1, c_2, \dots, c_i) & n = \begin{array}{c} (l/\epsilon) \\ (s_{i+1}, \dots, s_l) \end{array} & \mathbb{F}_2^{l-i} \\ & & \xi \in \mathbb{F}_2 \\ P(\xi) = Pr_{r_1, \dots, r_i \in \mathbb{F}_2} \left[f(\mathbf{r}, \mathbf{s}) = \sum_{j=1}^i c_j r_j + \xi \right]. & \\ (\mathbf{r}, \mathbf{s}) & (r_1, \dots, r_i, s_{i+1}, \dots, s_l) & (l/\epsilon) \end{array}$$

$$\begin{array}{cccc} (r_1,\ldots,r_i) \\ (s_{i+1},\ldots,s_l) \end{array} \qquad \qquad \xi \qquad \qquad P(\xi) \qquad \qquad 1/2+\epsilon/3$$

$$N \qquad \qquad U({\bf x}) \quad l \\ {\bf z} = (z_1,z_2,\ldots,z_N).$$

$$P(z_i=U({\bf x}_i))=1/2+\epsilon, \quad 1\leq i\leq N,\\ {\bf x}_i \qquad \qquad \qquad l \qquad \qquad \qquad 1\leq i\leq N$$

$$U({\bf x}_j))=1/2+\epsilon \qquad {\bf x}_i \qquad {\bf x}_j \qquad U({\bf x}) \qquad \qquad \qquad P(z_i=U({\bf x}_i))=1/2+\epsilon \qquad z_i \qquad z_j \qquad U({\bf x}) \\ P(z_j= {\bf x}_i+{\bf x}_j)$$

$$P(z_i+z_j=U({\bf x}_i+{\bf x}_j))=P(z_i+z_j=U({\bf x}_i)+U({\bf x}_j))\\ =P(z_i=U({\bf x}_i))P(z_j=U({\bf x}_j))\\ +P(z_i\neq U({\bf x}_i))P(z_j\neq U({\bf x}_j))\\ =(1/2+\epsilon)^2+(1/2-\epsilon)^2\\ =1/2+2\epsilon^2.$$

$$a_1,\dots a_t \in \{1,2,\dots,N\} \qquad \qquad \begin{matrix} t & \sum_{j=1}^t z_{a_j} \\ U(\sum_{j=1}^t \mathbf{x}_{a_j}) \end{matrix}$$

$$P(\sum_{j=1}^tz_{a_j}=U(\sum_{j=1}^t\mathbf{x}_{a_j}))=1/2+2^{t-1}\epsilon^t.$$

$$\hat{\mathbf{x}}\,=\,\textstyle\sum_{j=1}^t\mathbf{x}_{a_j}\qquad\hat{z}\,=\,\textstyle\sum_{j=1}^tz_{a_j}$$

$$U(\hat{\mathbf{x}})=\hat{z}+e,$$

$$e \qquad \qquad P(e\,=\,0)\,=\,1/2+2^{t-1}\epsilon^t$$

$$\hat{\mathbf{x}}$$

$$\mathbf{x}_{a_j}$$

$$\begin{matrix} \dot{\mathbf{x}} \\ t \end{matrix}$$

$$\begin{matrix} i \\ i \end{matrix}$$

$$k \qquad \qquad u_1,\ldots,u_k$$

$$\begin{matrix} (u_1,\ldots,u_k) \\ (\hat{u}_1,\ldots,\hat{u}_k) \\ \mathbf{s}_i \\ (l-k) \\ \{ \mathbf{x}_1,\mathbf{x}_2,\ldots \mathbf{x}_N \} \end{matrix} \qquad t$$

$$\hat{\mathbf{x}}(i)=\sum_{j=1}^t\mathbf{x}_{a_j},$$

$$\begin{matrix} \hat{\mathbf{x}}(i)=(\hat{x}_1,\ldots,\hat{x}_k,\mathbf{s}_i), \\ \hat{x}_1,\ldots,\hat{x}_k \\ t \\ O(N^{\lceil t/2\rceil}) \qquad \qquad O(N^{\lfloor t/2\rfloor}) \end{matrix}$$

$$\boxed{\begin{array}{ccccccccc} \mathbf{z} = (z_1,\ldots,z_N) & [\mathbf{x}_1,\mathbf{x}_2,\ldots,\mathbf{x}_N] & & t & k & n \\ & n & & (l-k) & & \\ & \mathbf{s}_i & & & \mathbf{s}_1,\mathbf{s}_2,\ldots,\mathbf{s}_n & \\ & & & & \hat{\mathbf{x}}(i) = \sum_{j=1}^t \mathbf{x}_{a_j} & \\ \\ \hat{\mathbf{x}}(i) = (\hat{x}_1,\ldots,\hat{x}_k,\mathbf{s}_i), & & & & & & \\ \\ \hat{x}_1,\ldots,\hat{x}_k & \hat{z}(i) = \sum_{j=1}^t z_{a_j} & & & & & \\ \hat{\mathbf{x}}(i) & S_i & & & & & \\ & 2^k & & & & & (u_1,\ldots,u_k) & = \\ & s_i & & & & & \{(\hat{\mathbf{x}}(i),\hat{z}(i))\} & \\ \\ (\hat{u}_1,\ldots,\hat{u}_k) & & & & & & & \\ & & & & & & & \\ num & & & & & & & \\ dist \leftarrow dist + (S_i - 2 \cdot num)^2. & & & & & & & \\ \\ dist & & & & & & & \\ dist \leftarrow 0 & & & & & & & \\ & (\hat{u}_1,\ldots,\hat{u}_k) & & & & & & \\ & & & & & & & dist \\ & & & & & & & \\ \end{array}}$$

$$U(\hat{\mathbf{x}}(i)) \qquad \hat{z}(i)$$

$$U(\hat{\mathbf{x}}(i))=\hat{z}(i)+e,$$

$$e \hspace{10cm} P(e\,=\,0)\,=\,1/2+2^{t-1}\epsilon^t$$

$$\sum_{j=1}^k u_j \hat{x}_j + \sum_{j=k+1}^l u_j s_j = \hat{z}(i) + e,$$

$$\sum_{j=1}^k (u_j+\dot{u}_j)\hat{x}_j + \sum_{j=k+1}^l u_j s_j + e = \sum_{j=1}^k \dot{u}_j \hat{x}_j + \hat{z}(i).$$

$$W = \textstyle{\sum_{j=k+1}^l u_j s_j}$$

$$W=0 \hspace{1.5cm} \hat{\mathbf{x}}(i) \hspace{1.5cm} W=1$$

$$S_i$$

$$\begin{array}{c} num \\ \sum_{j=1}^k(u_j+\hat u_j)\hat x_j\,=\,0 \\ P(W+e=0) \\ 1/2+2^{t-1}\epsilon^t t \\ num \\ Bin(S_i,p) \\ p=1/2 \end{array} \qquad \qquad \begin{array}{c} 1/2-2^{t-1}\epsilon^t \\ W=0 \qquad W=1 \\ p \\ \sum_{j=1}^k(u_j+\hat u_j)\hat x_j\neq 0 \\ Bin(S_i,p) \end{array}$$

$$\begin{array}{c} \sum_{j=1}^k\hat u_j\hat x_j=\hat z(i) \\ (S_i-2\cdot num)^2 \\ \hat{\bf x} \\ t\; {\bf x}_i \end{array}$$

$$\begin{array}{c} {\bf s}_i \\ {\bf s}_i \\ dist \end{array}$$

$$i\,$$

$$\begin{array}{c} (\hat u_1,\ldots,\hat u_k) \\ dist \\ k \end{array}$$

$$(k+1) \qquad \qquad 0 \qquad 1$$

$$i\,$$

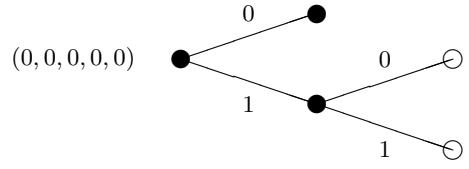
$$l\,$$

$${\varOmega}$$

$$\varOmega$$

$$\boxed{\begin{array}{llll} \mathbf{z} & = & (z_1,\ldots,z_N) & [\mathbf{x}_1,\mathbf{x}_2,\ldots,\mathbf{x}_N] \\ & & threshold(k) & \Omega \\ & & & \hat{k} \\ & & k & \hat{k} \leq k \leq l \\ \\ \mathbf{s}_i & n & (l-k) & \mathbf{s}_1,\mathbf{s}_2,\ldots,\mathbf{s}_n \\ & S_i & \Omega & \hat{\mathbf{x}}(i) = \sum_{j=1}^t \mathbf{x}_{a_j} \\ \\ & & \hat{x}_1,\ldots,\hat{x}_k & (\hat{\mathbf{x}}(i),\hat{z}(i) \;=\; \sum_{j=1}^t z_{a_j}) \\ & & S_i & \mathbf{s}_i \\ & & \Omega & (\hat{u}_1,\ldots,\hat{u}_k) \\ \\ & & \sum_{j=1}^k \hat{u}_j \hat{x}_j & = \hat{z}(i), \\ & & num & \\ & & dist \leftarrow dist + (S_i - 2 \cdot num)^2. & \\ \\ dist > threshold(k) & & (\hat{u}_1,\ldots,\hat{u}_k,0) & (\hat{u}_1,\ldots,\hat{u}_k,1) \\ \Omega & dist \leftarrow 0 & |\Omega| > 1 & l \\ \\ u_6 & (u_1,\ldots,u_5) = (0,0,0,0,0) & dist < threshold(6) & dist > threshold(6) \\ & threshold(5) & & \\ & (0,0,0,0,0,0) & (0,0,0,0,0,1) & \\ & & dist < threshold(6) & \\ & & (0,0,0,0,0,1,0) & (0,0,0,0,0,1,1) \\ & & & \end{array}}$$

$$k\\threshold(k)$$



$$\begin{array}{ccccc} \hat{\mathbf{x}}(i) & & k & & \hat{\mathbf{x}}(i) \\ k & & & & \mathbf{s}_i \\ num & \hat{\mathbf{x}}(i) & & & \\ & num & & & \mathbf{s}_i \\ & k & & & \end{array}$$

$$t = 2 \qquad t = 3 \qquad \qquad t$$

$$\begin{array}{llll}
 p = 1/2 - \epsilon & & & \\
 N = 400000 & k & 13-16 & n \\
 n \in \{1, 2, 4, 8, \dots, 512\} & & k = 16, n = 256 \\
 p = 0.45 & 400000 & & \\
 3 & & &
 \end{array}$$

$$n = 1 \quad k = 15 \quad n = 4 \quad k = 14 \quad n = 16 \quad k = 13 \quad n = 64 \quad k = 16$$

l = 60

$$N = 400000$$

n	$k = 13$	$k = 14$	$k = 15$	$k = 16$
1				
2				
4				
8				
16				
32				
64				
128				
256				
512				

$$\begin{array}{ll} p = 1/2 - \epsilon & t = 2 \quad k = 13, \dots, 16 \\ n \quad N = 400000 & \end{array}$$

$$l = 60 \quad t = 2$$

N	k	n		p
$40 \cdot 10^6$	23	1	96	
$40 \cdot 10^6$	22	2	48	
$40 \cdot 10^6$	21	4	25	
$40 \cdot 10^6$	25	1	26	
$40 \cdot 10^6$	24	2	13	
$40 \cdot 10^6$	23	4	6.5	
$40 \cdot 10^6$	22	8	3.3	
$40 \cdot 10^6$	25	4	106	

$$l = 60 \quad t = 3$$

N	k	n		p
$1.5 \cdot 10^5$	24	1	4.5	
$1.5 \cdot 10^5$	23	2	2.3	
$1.5 \cdot 10^5$	22	4	69	
$1.5 \cdot 10^5$	25	1	18	
$1.5 \cdot 10^5$	24	2	9.2	
$1.5 \cdot 10^5$	23	4	4.6	

$$l = 60 \quad t = 2 \quad t = 3$$

$$n = 1$$

$$\begin{array}{ccccc} n & & & p \\ & & & l \geq 60 & \end{array}$$

$$\begin{array}{ccccc} B & & & 2^B \\ & & 20-30 & & \end{array}$$

$$k$$

$$N = 400000 \quad p = 0.40 \quad t = 2 \quad n = 64$$

$$\begin{array}{lllll}E[S] & t & N & \mathbf{x}_1,\ldots,\mathbf{x}_N \\ E[S] & & E[S]=\frac{\binom{N}{t}}{2^{l-k}}. & & \\ \left(\begin{matrix} N \\ t \end{matrix}\right) & & & \mathbf{s} & 1/2^{l-k}. \\ \left(\begin{matrix} N \\ t \end{matrix}\right)/2^{l-k} & & & \mathbf{s.} & \\ \blacksquare & & & & \\ dist & & & & \\ \mathbf{s} & & & \mathbf{s} & \\ U(\mathbf{x}) & & S & & (\hat{u}_1,\ldots,\hat{u}_k) \\ num & & & & \sum_{j=1}^k \hat{u}_j \hat{x}_j = \hat{z}(i). \\ H_0, & H_1. & H_1 & & \\ p_0 & & & W=\sum_{j=k+1}^l u_j s_j & p_0 \quad p_0=P(e= \\ 0)=1/2+2^{t-1}\epsilon^t. & & & P(W=0)=1/2. & \\ & & num & & \\ num|H_0 \in Bin(S,1/2), & & & & \\ num|H_1,W=0 \in Bin(S,p_0), & & & & \\ num|H_1,W=1 \in Bin(S,(1-p_0)). & & & & \\ & & & & num \\ Spq \gg 10 & Y & Y=|2\cdot num-S|. & & P((2\cdot num-S) < \\ 0|H_1,W=0)=P((2\cdot num-S)>0|H_1,W=1) & & & & \\ & Y & & & & & & & \\ f_{Y|H_0}(y)=\frac{2}{\sqrt{\pi S}}e^{-y^2/S} & & & & & & & & \end{array}$$

$$f_{Y|H_1}(y) = \frac{1}{\sqrt{4\pi S p_0(1-p_0)}} e^{-\frac{(y-Sp_0)^2}{4Sp_0(1-p_0)}}$$

$$\begin{array}{ccc} (u_1,\ldots,u_k) & (\hat u_1,\ldots,\hat u_k) & P(H_1|Y) \\ & P(H_1|Y) & \\ & (\hat u_1,\ldots,\hat u_k) & \end{array}$$

$$\varLambda=\frac{P(H_1|Y)}{1-P(H_1|Y)}=\frac{P(H_1|Y)}{P(H_0|Y)}=\frac{P(Y|H_1)P(H_1)}{P(Y|H_0)P(H_0)},$$

$$\lambda=\ln(\varLambda).$$

$$\arg\max_{(\hat{u}_1,\dots,\hat{u}_k)}\left[\ln P(Y|H_1)+\ln P(H_1)-\ln P(Y|H_0)-\ln P(H_0)\right].$$

$$\begin{array}{ccccc} & & \lambda & & \\ & & y^2 & & \\ n & S_i,\,(S_1,S_2,\ldots,S_n) & & S. & \\ & & & & Y=(Y_1,Y_2,\ldots,Y_n). \end{array}$$

$$P(Y|H_0)=P(Y_1|H_0)P(Y_2|H_0)\cdots P(Y_n|H_0)$$

$$dist=dist_1+dist_2+\ldots+dist_n,\\ dist_i=y_i^2.$$

$$(\hat u_1,\ldots,\hat u_k).$$

$$|2\cdot num_i - S_i|\in N(S_i(2p_0-1),2S_ip_0(1-p_0)).$$

$$(\hat u_1,\ldots,\hat u_k)$$

$$(2\cdot num_i - S_i)\in N(0,S/2).$$

$$\begin{array}{cccc} dist & & & \\ dist = \sum\limits_{i=1}^n (2\cdot num_i - S_i)^2 = \sum\limits_{i=1}^n |2\cdot num_i - S_i|^2. & & & \\ dist & & n & \\ & & & n \\ E(dist|H_1) > E(dist|H_0). & & & \\ n \rightarrow \infty & & \epsilon \rightarrow 0 & \\ & & & n \end{array}$$

$$P_F,$$

$$\begin{array}{ccccc} P_M, & & dist & & H_0 \qquad H_1 \\ P_M & \qquad P_F & & & T. \\ P_M & & & & \end{array}$$

$$P_M=P(dist < T|H_1),$$

$$P_F=P(dist > T|H_0).$$

$$\begin{array}{cc} 4 & 5 \end{array}$$

