$z_1, z_2, \ldots$

$m_1, m_2, \ldots$ $c_1, c_2, \ldots$

$K$

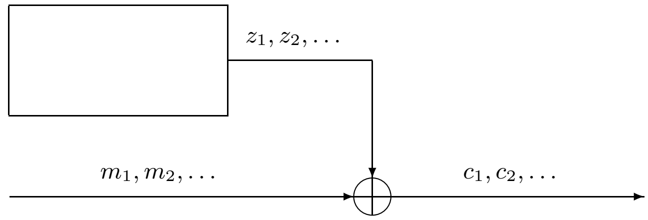
$K$

$K$ $z_1, z_2, \ldots, z_N$

$z_1, z_2, \ldots, z_N$

$K$

$K$




$u_1, u_2, \dots$

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

$f$

$f$

$z_n$

$l$ $g(x)$

$2^l$

$\mathbf{z} = z_1, z_2, \ldots, z_N$ $N$

$u_i$ $z_i$

$1/2 + \epsilon$ $1/2 + \epsilon = P(u_i = z_i)$ $0 < \epsilon < 1/2$

$(z_1, z_2, \ldots, z_N)$

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

$h(p)$

$N \gg N_0$

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

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

$g(x) = 1 + g_1 x + \dots g_l x^l$ $u_i$

$\mathbf{u}$

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

$w_{ij}, i \geq 1, 1 \leq j \leq l$

$g(x)$

$U(\mathbf{x})$

$$U(\mathbf{x}) = U(x_1, x_2, \dots, x_l) = u_1 x_1 + u_2 x_2 + \dots + u_l x_l.$$

$u_i$

$\mathbf{x}_i = (w_{i1}, w_{i2}, \dots, w_{ij})$

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

$u_i$ $z_i$

$$\mathbf{e} = (e_1, e_2, \dots, e_N),$$

$e_i \in \mathbb{F}_2$ $1 \leq i \leq N$ $P(e_i = 0) =$
$1/2 + \epsilon$ $\mathbf{z} = \mathbf{u} + \mathbf{e}$

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

$\mathbf{x}_i$ $l$ $1 \leq i \leq N$

$\mathbf{z}$

$U(\mathbf{x})$

$\{\mathbf{x}_1, \mathbf{x}_2, \dots \mathbf{x}_N\}$

$U(\mathbf{x})$

$f : F^l \to F$

$\mathcal{F}$ $\delta$

$g \in \mathcal{F}$ $f$

$\delta$

$\mathcal{F}$

$\mathcal{F}$ $l$
$d$
$F = \mathbb{F}_2$
$\epsilon > 0$ $f : F^l \to F$
$l/\epsilon$ $l$
$f$ $\delta = 1/2 + \epsilon$

$\mathbf{x}$
$p(\mathbf{x})$ $e$ $p(\mathbf{x}) + e$

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

$i$
$p(x_1, x_2, \ldots, x_i, 0, 0, \ldots, 0)$
$i$ $l$ $i$

$l$ $i$
$i$ $p(\mathbf{x})$ $i$
$(i-1)$
$x_i$
$(i-1)$
$i$

$(c_1, c_2, \ldots, c_i)$ $n =$ $(l/\epsilon)$ $\mathbb{F}_2^{l-i}$
$(s_{i+1}, \ldots, s_l)$ $\xi \in \mathbb{F}_2$

$$P(\xi) = Pr_{r_1,\ldots,r_i \in \mathbb{F}_2}\left[f(\mathbf{r},\mathbf{s}) = \sum_{j=1}^{i} c_j r_j + \xi\right].$$

$(\mathbf{r}, \mathbf{s})$ $(r_1, \ldots, r_i, s_{i+1}, \ldots, s_l)$
$(l/\epsilon)$

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

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

$$\mathbf{z} = (z_1, z_2, \ldots, z_N).$$

$$P(z_i = U(\mathbf{x}_i)) = 1/2 + \epsilon, \quad 1 \le i \le N,$$

$\mathbf{x}_i$ $l$ $1 \le i \le N$

$\mathbf{x}_i$

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

$\mathbf{x}_i + \mathbf{x}_j$

$$\begin{aligned} P(z_i + z_j = U(\mathbf{x}_i + \mathbf{x}_j)) &= P(z_i + z_j = U(\mathbf{x}_i) + U(\mathbf{x}_j)) \\ &= P(z_i = U(\mathbf{x}_i))P(z_j = U(\mathbf{x}_j)) \\ &\quad + P(z_i \ne U(\mathbf{x}_i))P(z_j \ne U(\mathbf{x}_j)) \\ &= (1/2 + \epsilon)^2 + (1/2 - \epsilon)^2 \\ &= 1/2 + 2\epsilon^2. \end{aligned}$$

$t$ $\sum_{j=1}^t z_{a_j}$

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

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

$\hat{\mathbf{x}} = \sum_{j=1}^t \mathbf{x}_{a_j}$ $\hat{z} = \sum_{j=1}^t z_{a_j}$

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

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

$\hat{\mathbf{x}}$

$\mathbf{x}_{a_j}$

$\hat{\mathbf{x}}$

$t$

$i$

$i$

$k$ $u_1, \dots, u_k$

$(u_1, \dots, u_k)$

$(\hat{u}_1, \dots, \hat{u}_k)$

$(l-k)$ $\mathbf{s}_i$

$t$ $\{\mathbf{x}_1, \mathbf{x}_2, \dots \mathbf{x}_N\}$

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

$$\hat{\mathbf{x}}(i) = (\hat{x}_1, \dots, \hat{x}_k, \mathbf{s}_i),$$

$\hat{x}_1, \dots, \hat{x}_k$

$t$

$O(N^{\lceil t/2 \rceil})$ $O(N^{\lfloor t/2 \rfloor})$

$\mathbf{z} = (z_1, \ldots, z_N)$ $[\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N]$ $t$ $k$ $n$
$n$ $(l-k)$ $\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_n$
$\mathbf{s}_i$ $\hat{\mathbf{x}}(i) = \sum_{j=1}^{t} \mathbf{x}_{a_j}$

$$\hat{\mathbf{x}}(i) = (\hat{x}_1, \ldots, \hat{x}_k, \mathbf{s}_i),$$

$\hat{x}_1, \ldots, \hat{x}_k$
$\hat{\mathbf{x}}(i)$ $\hat{z}(i) = \sum_{j=1}^{t} z_{a_j}$
$S_i$
$2^k$ $(u_1, \ldots, u_k)$ $=$
$(\hat{u}_1, \ldots, \hat{u}_k)$
$s_i$ $S_i$ $\{(\hat{\mathbf{x}}(i), \hat{z}(i))\}$

$$\sum_{j=1}^{k} \hat{u}_j \hat{x}_j = \hat{z}(i),$$

$num$

$$dist \leftarrow dist + (S_i - 2 \cdot num)^2.$$

$dist$ $(\hat{u}_1, \ldots, \hat{u}_k)$
$dist \leftarrow 0$
$(\hat{u}_1, \ldots, \hat{u}_k)$ $dist$

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

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

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

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

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

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

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

$S_i$

$num$

$\sum_{j=1}^{k}(u_j + \hat{u}_j)\hat{x}_j = 0$

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

$1/2 + 2^{t-1}\epsilon^t t$ $W = 0$ $W = 1$

$num$ $Bin(S_i, p)$ $p$

$\sum_{j=1}^{k}(u_j + \hat{u}_j)\hat{x}_j \neq 0$

$num$ $Bin(S_i, p)$

$p = 1/2$

$\sum_{j=1}^{k} \hat{u}_j\hat{x}_j = \hat{z}(i)$

$(S_i - 2 \cdot num)^2$

$\hat{\mathbf{x}}$ $t$ $\mathbf{x}_i$

$\mathbf{s}_i$

$\mathbf{s}_i$

$dist$

$i$

$(\hat{u}_1, \ldots, \hat{u}_k)$

$dist$

$k$

$(k + 1)$ $0$ $1$

$i$

$l$

$\Omega$

$\Omega$

$\mathbf{z} = (z_1, \ldots, z_N)$ $[\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N]$ $t$ $\hat{k}$ $n$
$threshold(k)$ $\Omega$ $\hat{k}$
$k$ $\hat{k} \leq k \leq l$

$n$ $(l-k)$ $\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_n$
$\mathbf{s}_i$ $\hat{\mathbf{x}}(i) = \sum_{j=1}^{t} \mathbf{x}_{a_j}$

$$\hat{\mathbf{x}}(i) = (\hat{x}_1, \ldots, \hat{x}_k, \mathbf{s}_i),$$

$\hat{x}_1, \ldots, \hat{x}_k$ $(\hat{\mathbf{x}}(i), \hat{z}(i) = \sum_{j=1}^{t} z_{a_j})$
$S_i$
$\Omega$ $(\hat{u}_1, \ldots, \hat{u}_k)$
$\mathbf{s}_i$ $S_i$ $\mathbf{s}_i$

$$\sum_{j=1}^{k} \hat{u}_j \hat{x}_j = \hat{z}(i),$$

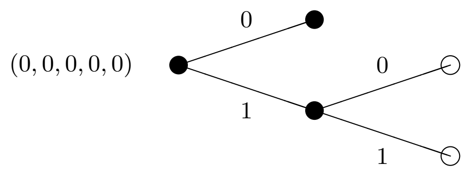
$num$

$$dist \leftarrow dist + (S_i - 2 \cdot num)^2.$$

$dist > threshold(k)$ $(\hat{u}_1, \ldots, \hat{u}_k, 0)$ $(\hat{u}_1, \ldots, \hat{u}_k, 1)$
$\Omega$ $dist \leftarrow 0$ $|\Omega| > 1$
$\Omega$ $l$

$\hat{k} = 5$
$(u_1, \ldots, u_5) = (0, 0, 0, 0, 0)$ $dist$
$threshold(5)$
$u_6$ $(0, 0, 0, 0, 0, 0)$ $(0, 0, 0, 0, 0, 1)$
$dist < threshold(6)$
$dist > threshold(6)$
$(0, 0, 0, 0, 0, 1, 0)$ $(0, 0, 0, 0, 0, 1, 1)$

$k$
$threshold(k)$




$\hat{\mathbf{x}}(i)$ $k$ $\hat{\mathbf{x}}(i)$
$k$ $\mathbf{s}_i$
$num$ $\hat{\mathbf{x}}(i)$
$num$ $\mathbf{s}_i$
$k$

$t = 2$ $t = 3$ $t$

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

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

$l = 60$

$N = 400000$

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

$p = 1/2 - \epsilon$ $t = 2$ $k = 13, \ldots, 16$
$n$ $N = 400000$

$l = 60$ $t = 2$

| $N$ | $k$ | $n$ | | $p$ |
|---|---|---|---|---|
| $40 \cdot 10^6$ | 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 | |

$l = 60$ $t = 3$

| $N$ | $k$ | $n$ | | $p$ |
|---|---|---|---|---|
| $1.5 \cdot 10^5$ | 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 | |

$l = 60$ $t = 2$ $t = 3$

$n = 1$

$n$ $p$
$l \geq 60$

$2^B$

$B$ $20 - 30$

$k$

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

$S_i$

$E[S]$

$t$ $N$ $\mathbf{x}_1, \ldots, \mathbf{x}_N$

$E[S]$

$$E[S] = \frac{\binom{N}{t}}{2^{l-k}}.$$

$\binom{N}{t.}$ $\mathbf{s}$ $1/2^{l-k}$.

$\binom{N}{t}/2^{l-k}$ $\mathbf{s}$.

■

$dist$

$\mathbf{s}$.

$\mathbf{s}$

$\mathbf{s}$ $S$

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

$(\hat{u}_1, \ldots, \hat{u}_k)$

$num$ $\sum_{j=1}^{k} \hat{u}_j \hat{x}_j = \hat{z}(i)$.

$H_0$, $H_1$. $H_1$

$H_0$

$W = \sum_{j=k+1}^{l} u_j s_j$ $p_0$ $p_0 = P(e = 0) = 1/2 + 2^{t-1}\epsilon^t$. $P(W = 0) = 1/2$.

$num$

$$num|H_0 \in Bin(S, 1/2),$$
$$num|H_1, W = 0 \in Bin(S, p_0),$$
$$num|H_1, W = 1 \in Bin(S, (1 - p_0)).$$

$num$

$Spq \gg 10$

$Y$ $Y = |2 \cdot num - S|$. $P((2 \cdot num - S) < 0|H_1, W = 0) = P((2 \cdot num - S) > 0|H_1, W = 1)$

$Y$

$$f_{Y|H_0}(y) = \frac{2}{\sqrt{\pi S}} e^{-y^2/S}$$

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

$(u_1, \ldots, u_k)$ $(\hat{u}_1, \ldots, \hat{u}_k)$ $P(H_1|Y)$
$P(H_1|Y)$
$(\hat{u}_1, \ldots, \hat{u}_k)$

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

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

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

$\lambda$
$y^2$
$S.$
$n$ $S_i$, $(S_1, S_2, \ldots, S_n)$ $Y = (Y_1, Y_2, \ldots, Y_n).$

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

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

$(\hat{u}_1, \ldots, \hat{u}_k).$

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

$(\hat{u}_1, \ldots, \hat{u}_k)$

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

$dist$

$$dist = \sum_{i=1}^{n}(2 \cdot num_i - S_i)^2 = \sum_{i=1}^{n}|2 \cdot num_i - S_i|^2.$$

$dist$ $n$
$dist$ $n$

$n$
$E(dist|H_1) > E(dist|H_0).$
$n \to \infty$ $\epsilon \to 0$

$P_F,$

$P_M,$

$dist$ $H_0$ $H_1$

$P_M$ $P_F$ $T.$

$P_M$

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

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

4 5