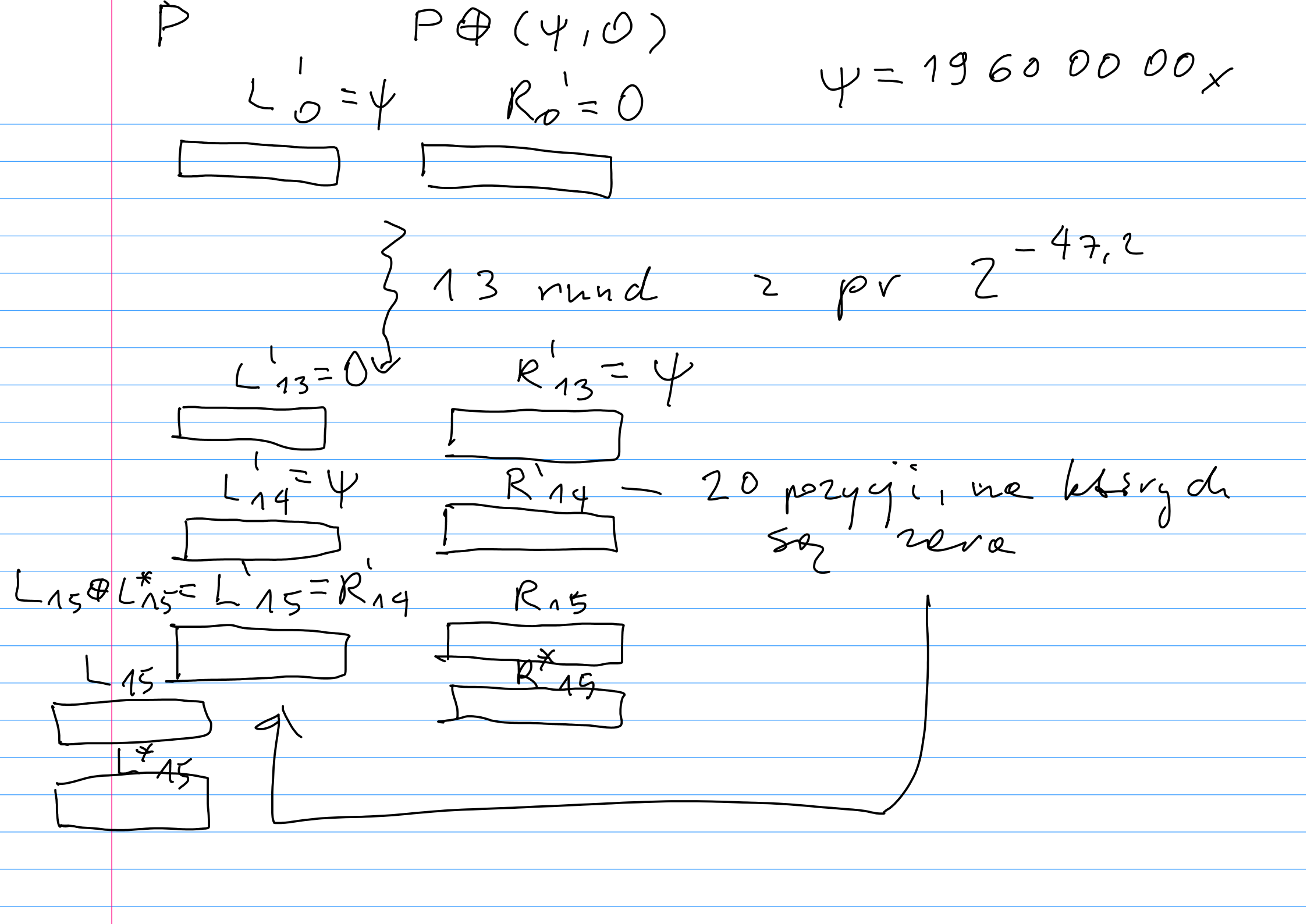
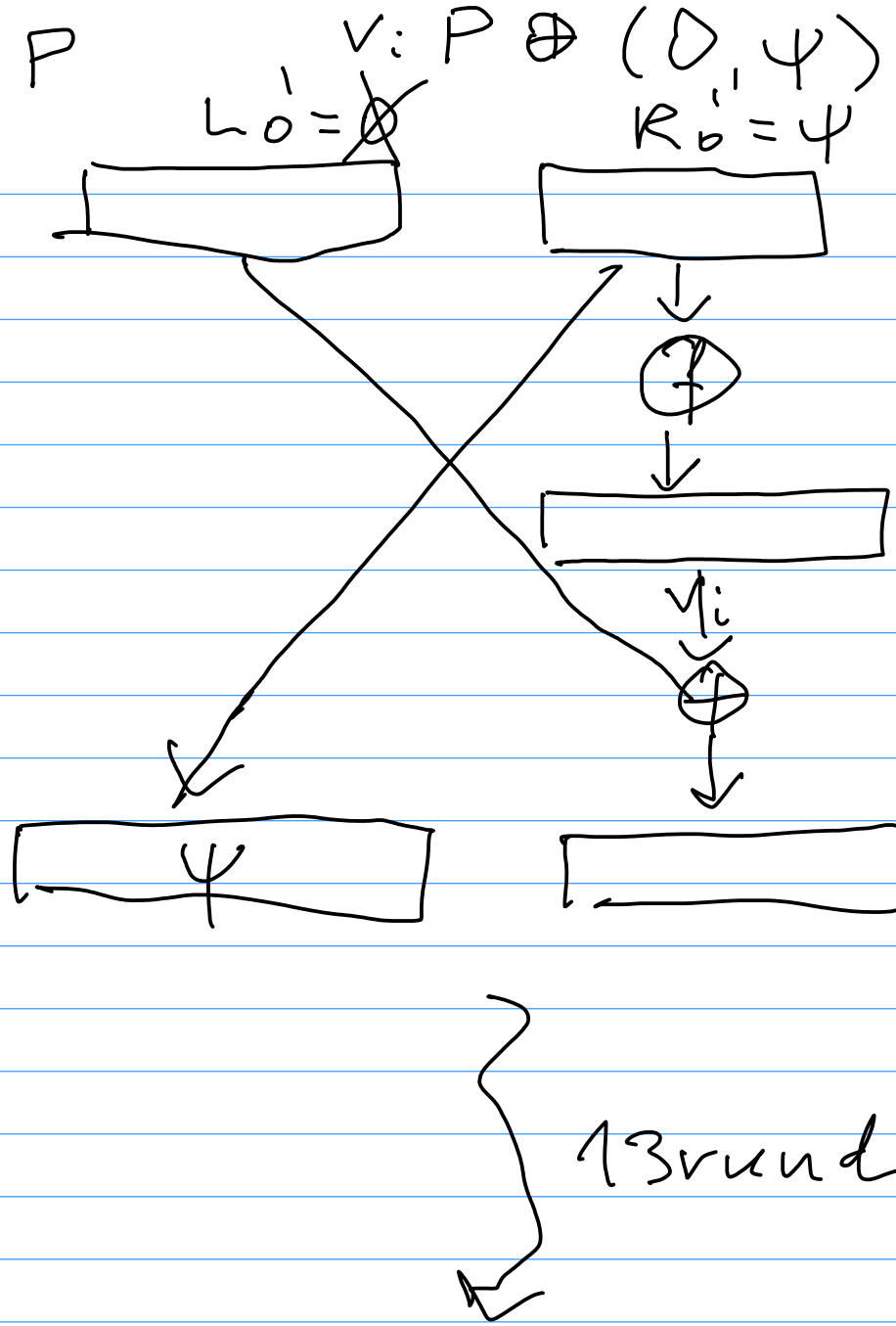

P
P⊕(Ψ,0)
$L'_0 = \Psi$
$R'_0 = 0$
$\Psi = 19600000_x$
13 rund
z pr $2^{-47,2}$
$L'_{13} = 0$
$R'_{13} = \Psi$
$L'_{14} = \Psi$
R'_{14} — 20 pozycji, na których są zera
$L_{15} \oplus L^*_{15} = L'_{15} = R'_{14}$
R_{15}
L_{15}
R^*_{15}
L^*_{15}



V_i – jeden z 2^{12} ciągów 32 bitowych

0 * 0 * 0 * 0 * 0 * 0

$0 = V_i \oplus V_i$

13 rund

dla danego P wyznaczamy szyfrogramy wszystkich $P_i = P \oplus v_i$ i $P_i^* = P \oplus v_i \oplus \psi$ w ten sposób jako pary L_1^1, R_1^1 wyznaczamy $(\psi, 0)$ na 2^{12} sposobów 2 par P_i, P_j^*. Chcemy teraz zidentyfikować pary P_i, P_j^*, które powstały w pierwszej rundzie dają różnice $(\psi, 0)$ i pochodzą przez wejście 2 godnie z charakterystyką 13 rund stylu.

2^{24} par (p_i, p_j^*)

prawdop $\frac{1}{2^{20}}$, że na bitach

L_{16} odp sekwencja $S_4 - S_8$ są zera

średnio $2^4 = 16$ par spełnia

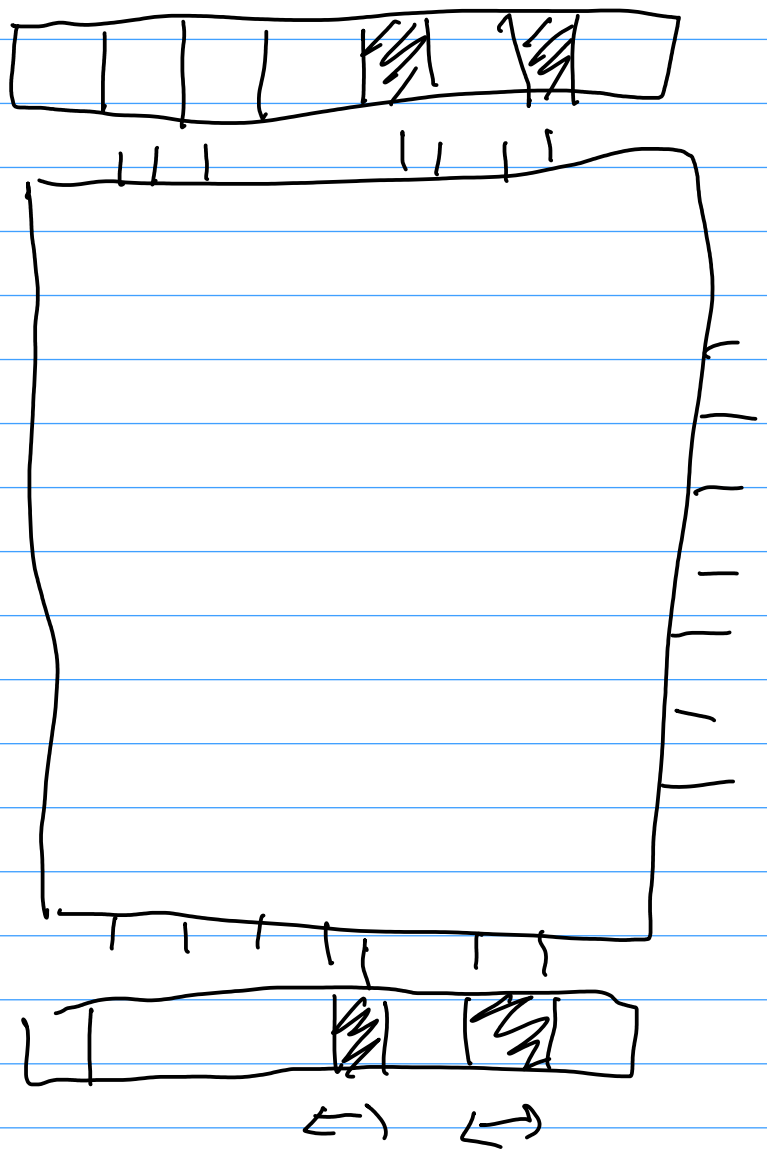
warunek oczekiwania

Testowanie różnic symetrycznych

w ostatniej rundzie eliminuje

92% tych par. Czyli średnio

pozostaje 1,5 pary z 2^{24}



przesunięcie wyjściowe K_1

przesunięcie wyjściowe K_{16}

Znajdowanie (generowanie) dużych losowych liczb pierwszych
(np liczb pierwszych k-cyfrowych)
np $k \geq 1024$

$\pi(n)$ – ilość liczb pierwszych w $[0, n]$

$$\pi(n) \sim \frac{n}{\ln n}$$

Test Millera - Rabina (n)

1° Jeżeli $2 \mid n$ to n - złożona

2° $n - 1 = 2^k m$ (m - nieparzyste)

3° Losujemy $a < n$

4° Obliczamy $a^m, a^{2m}, a^{2^2 m}, \ldots, a^{2^k m} \mod n$

5° Jeżeli $a^{2^k m} \neq 1$ to n - złożona

6° Jeżeli $a^{2^k m} = 1$ i $a^{2^{k-1} m} \neq \pm 1$ to n - złożona

$a^m, a^{2m}, \ldots, a^{2^k m}$

$-1, 1, 1, 1$

n - pierwsze

$x \quad x^2 \equiv_n 1$ mody

Tw 1: Liczba pierwsza $\Leftrightarrow$

n wtedy i tylko wtedy $x = \pm 1$

okazuje się 2 tylko w teście M-R

Dowód

1° jeżeli n - pierwsza, to $2 \nmid n$

2° jeżeli n - pierwsza, to $a^{n-1} \equiv_n 1$

3° jeżeli n-pierwsza, to $x^2 \equiv_n 1 \Rightarrow x = \pm 1$

Tw 2: Jeżeli n - złożona, to
Test M-R wykrywa to z pr. $\geq \frac{1}{2}$

2 przypadki

1° $n = p^\alpha$

2° $n = n_1 \cdot n_2$
gdzie $n_1 \perp n_2$

1° G - grupa i H - podgrupa G

Fakt: Jeżeli istnieje $g \in G \setminus H$,
to $|H| \leq \frac{|G|}{2}$

$\Rightarrow$ przypadkowy el G należy do H z
pr $\leq \frac{1}{2}$

$G = \mathbb{Z}_{p^\alpha}^*$ $\quad H = \{a \in G : a^{p^{\alpha-1}} \equiv 1\}$

G jest cykliczna rzędu $p^\alpha - p^{\alpha-1}$

Generator g ma rząd $p^\alpha - p^{\alpha-1}$, więc $g^{p^{\alpha-1}} \equiv g^{p^{\alpha-1}-1} \not\equiv 1$