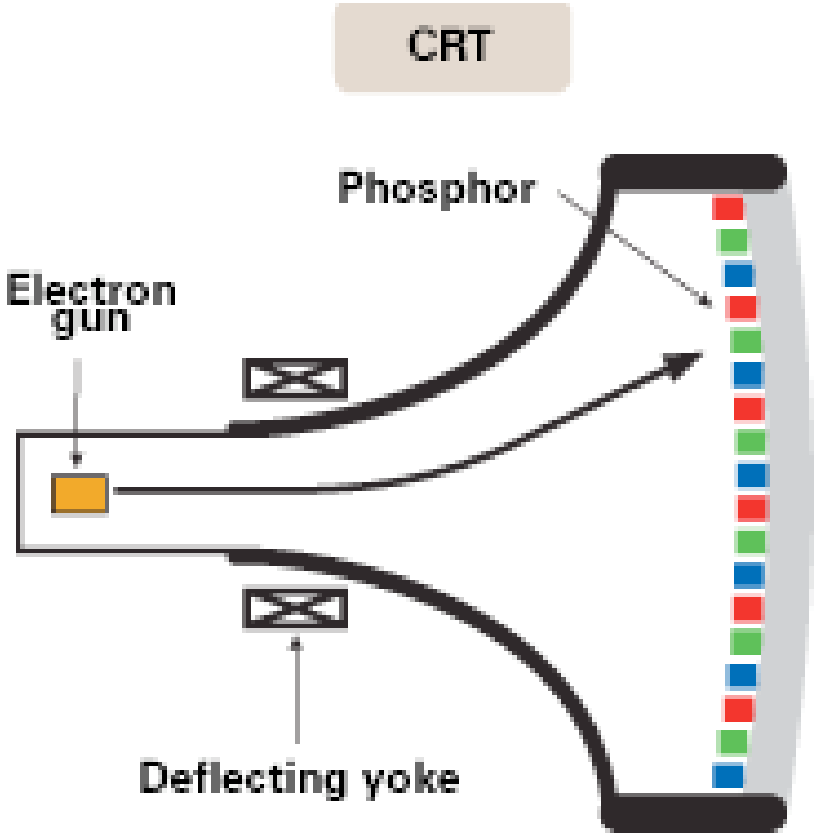
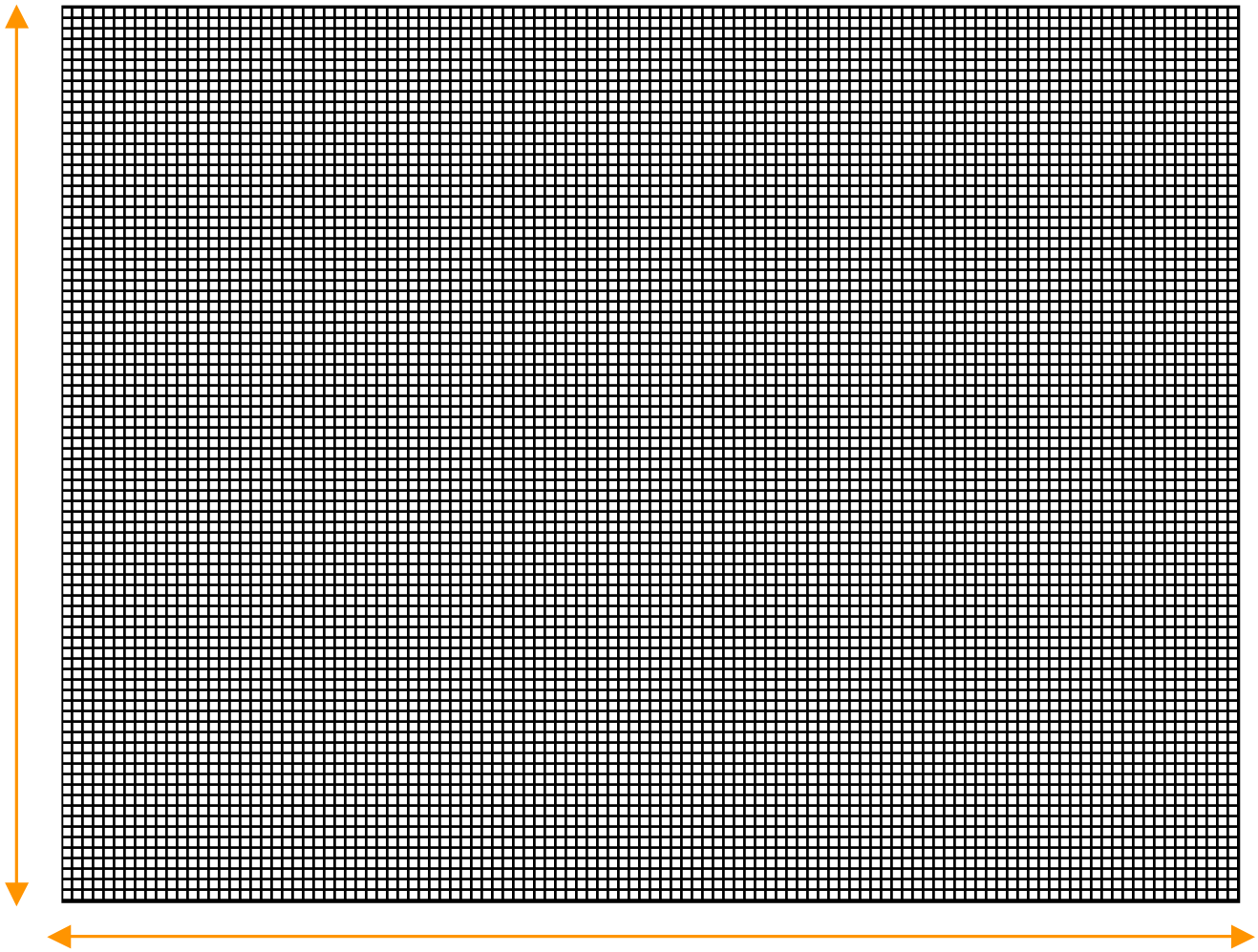
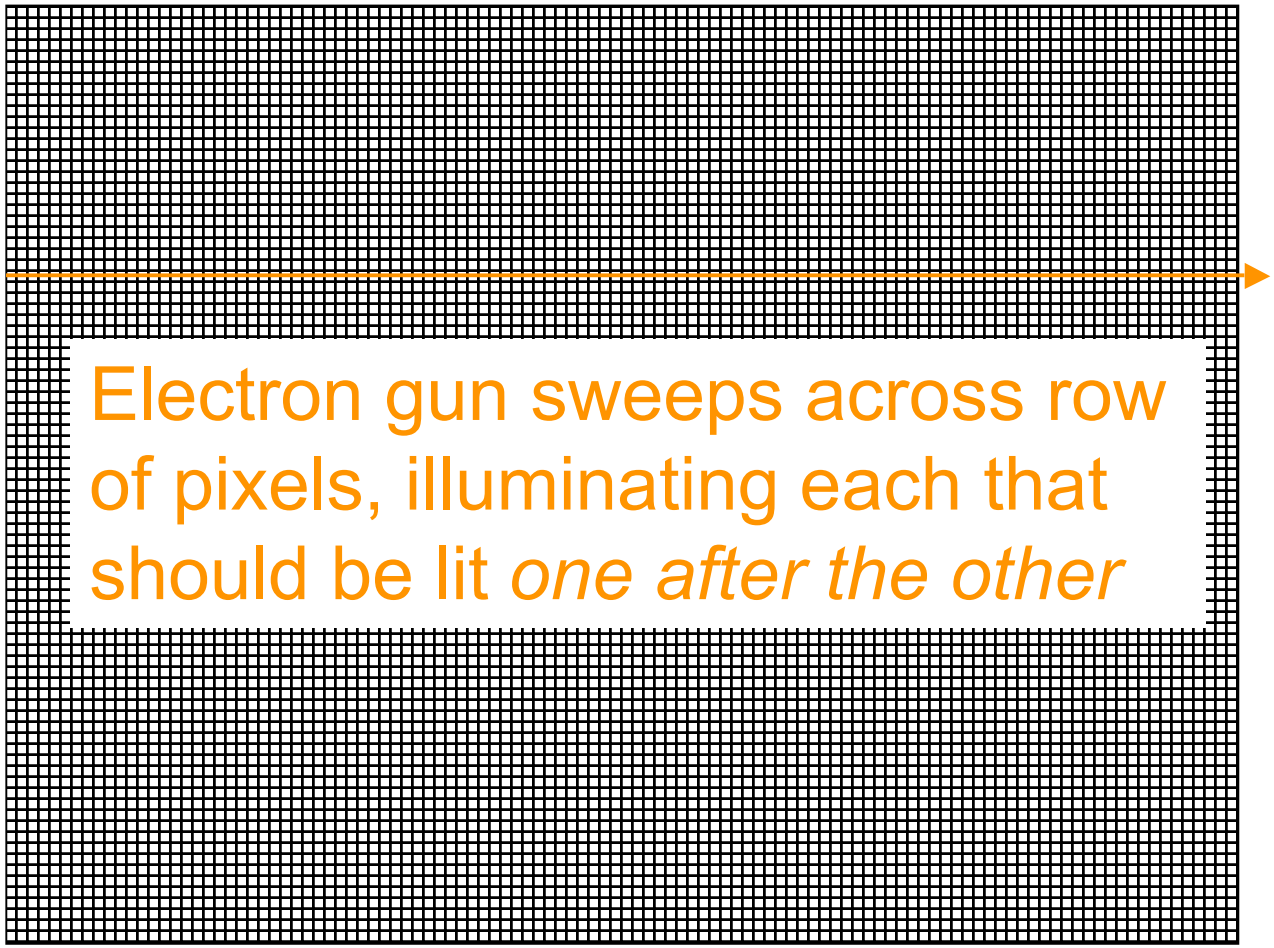
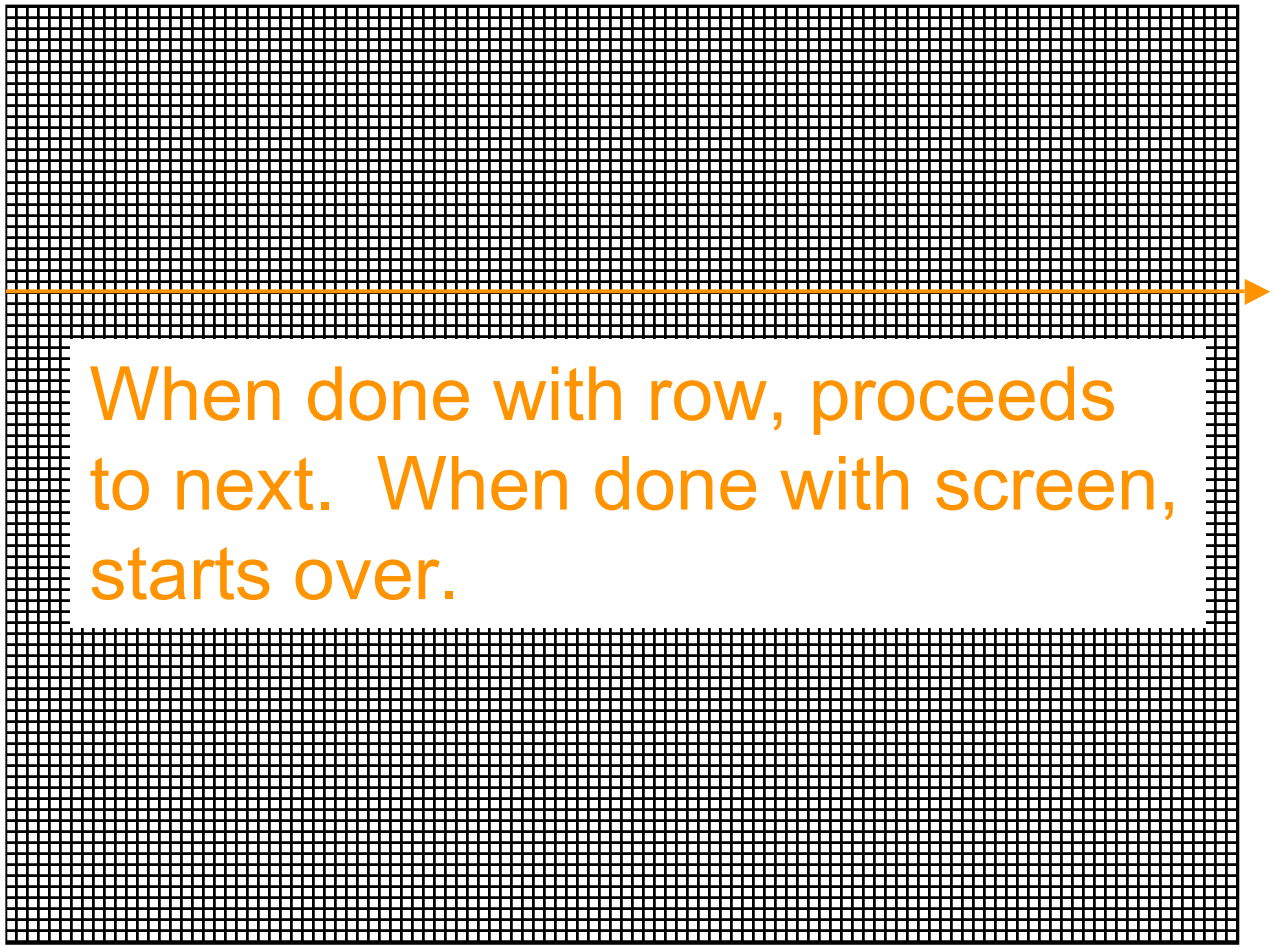

CRT
Phosphor
Electron gun
Deflecting yoke

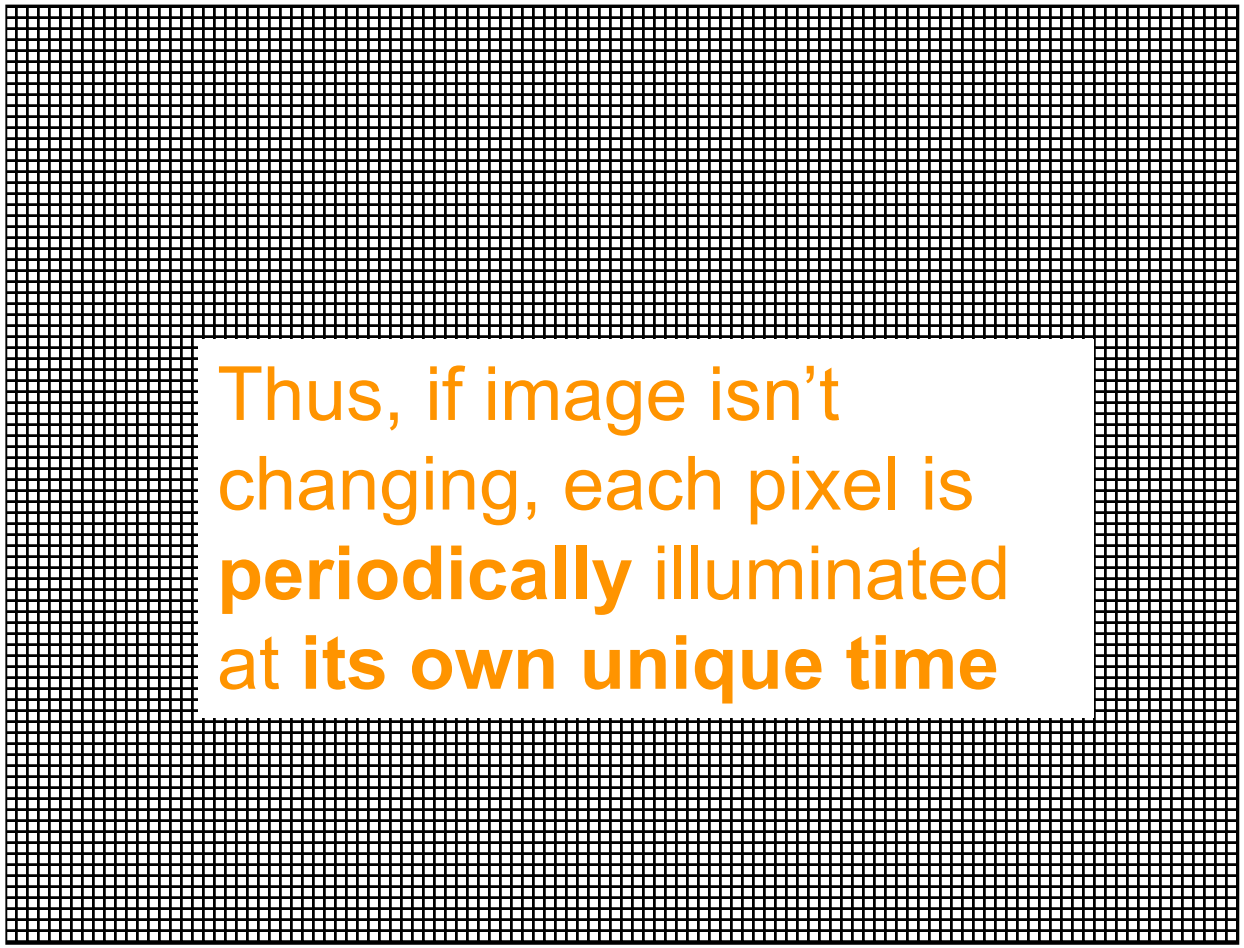
CRT display is made up of an array of phosphor pixels



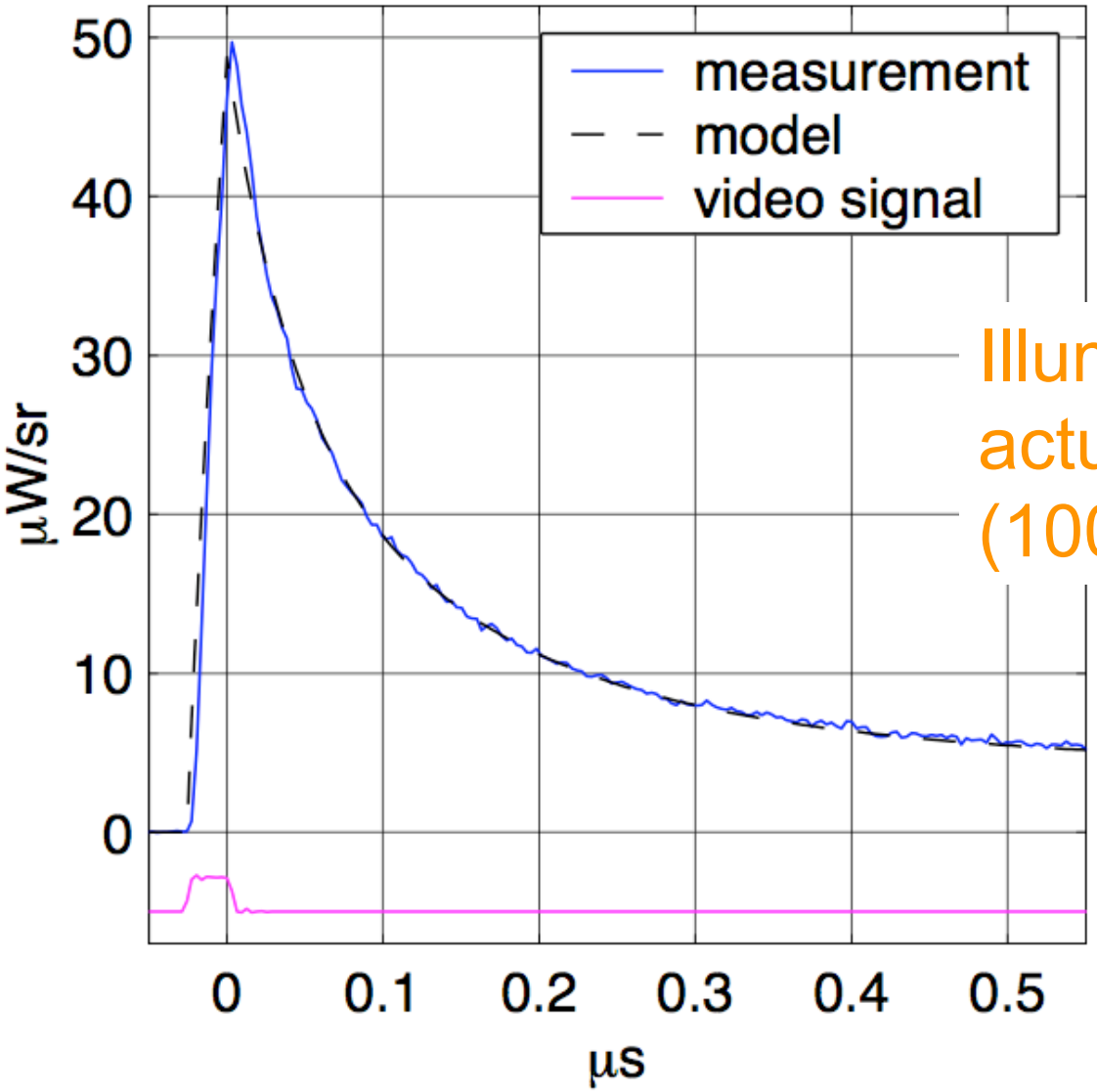
640x480 (say)


Electron gun sweeps across row of pixels, illuminating each that should be lit *one after the other*

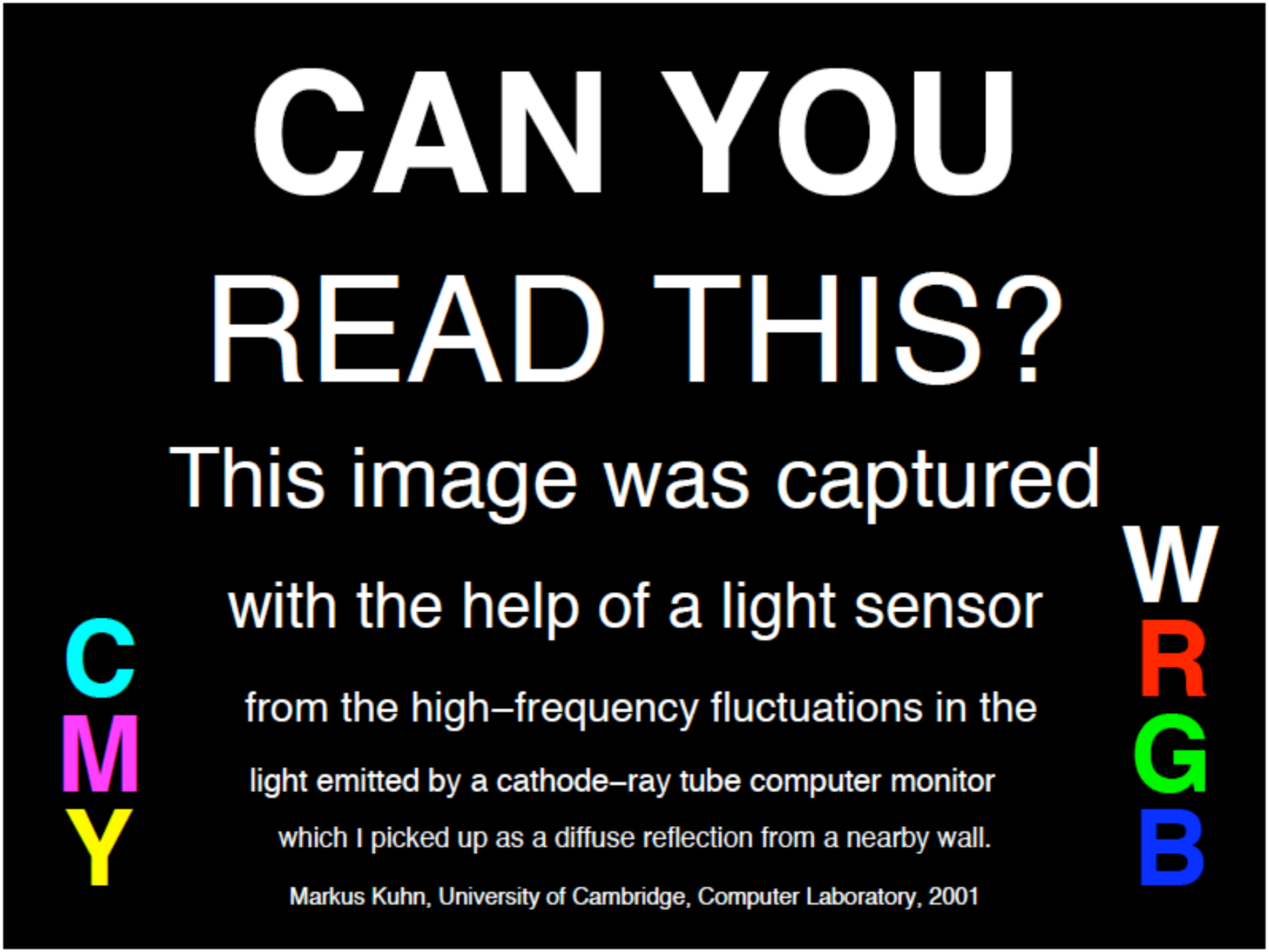

When done with row, proceeds to next. When done with screen, starts over.


Thus, if image isn’t changing, each pixel is **periodically** illuminated at **its own unique time**

(a) Emission decay of a single pixel (f_p = 36 MHz)



Illumination is actually short-lived (100s of nsec).


CAN YOU
READ THIS?
This image was captured
with the help of a light sensor
from the high–frequency fluctuations in the
light emitted by a cathode–ray tube computer monitor
which I picked up as a diffuse reflection from a nearby wall.
Markus Kuhn, University of Cambridge, Computer Laboratory, 2001
C
M
Y
W
R
G
B

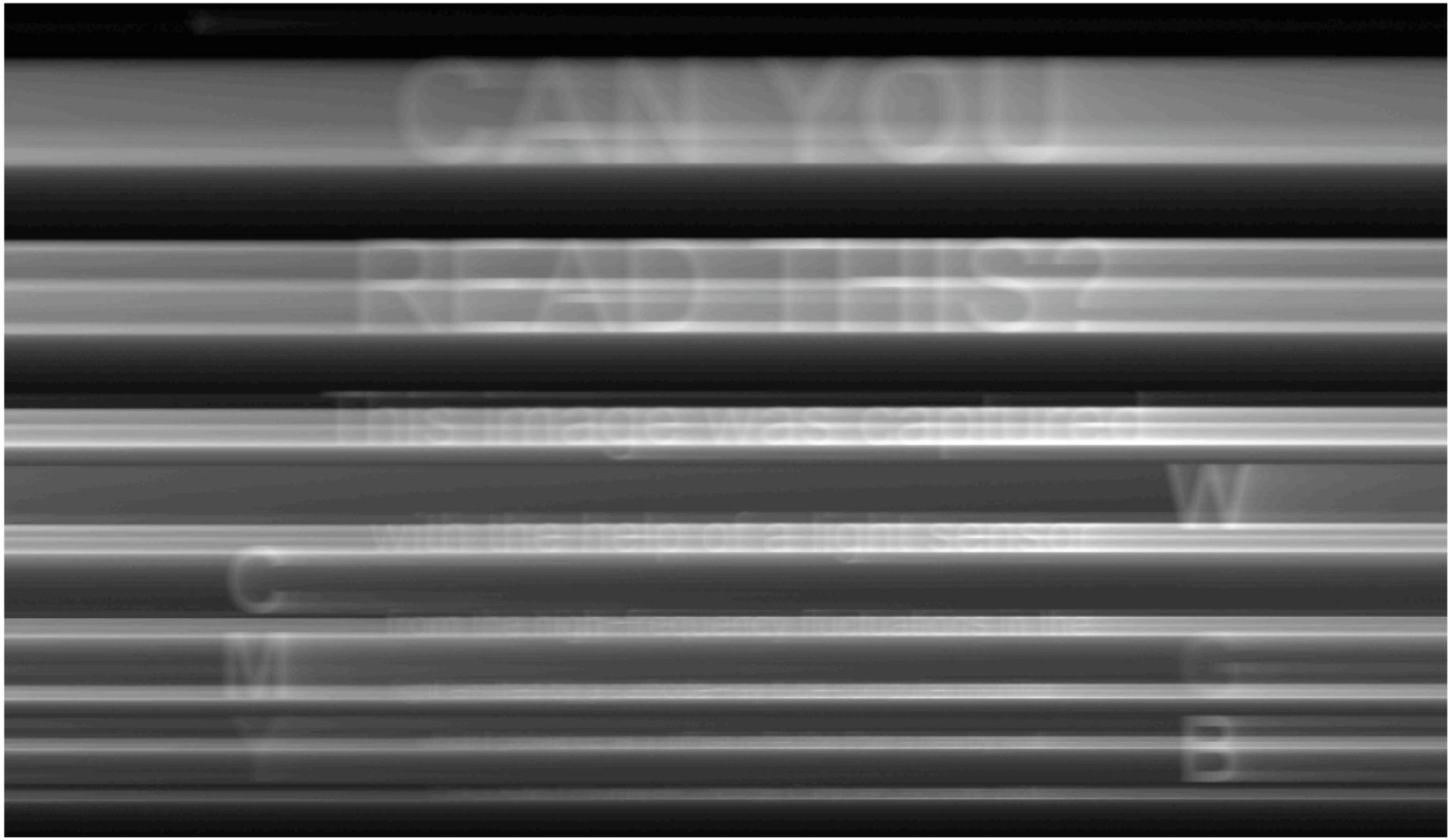


Figure 6.9: Unprocessed photomultiplier output after diffuse reflection from a wall

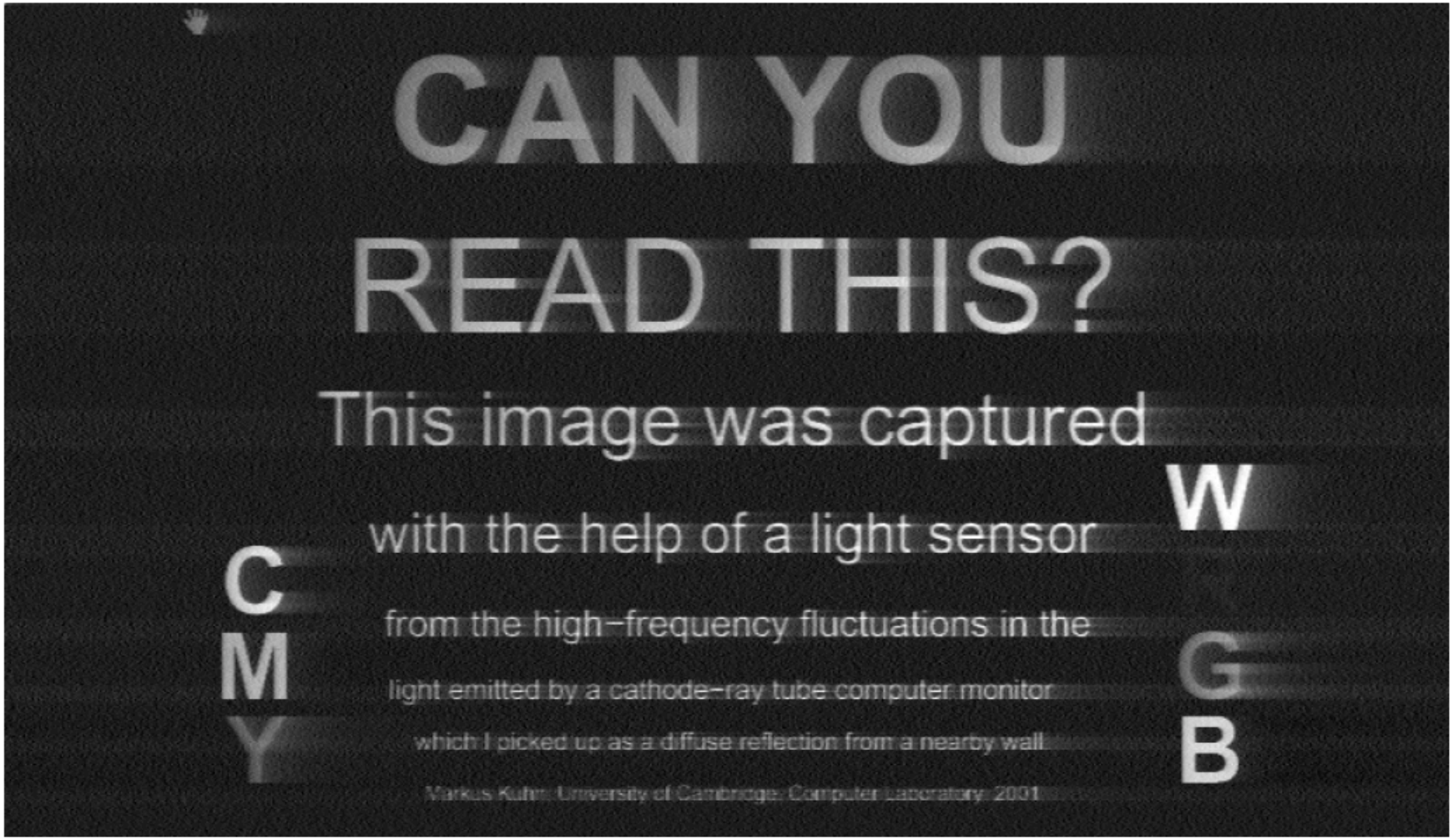


Figure 6.11: A much better image quality can be achieved by applying a matched filter with a frequency characteristic that is inverse to that of white shown in Fig. 6.7.

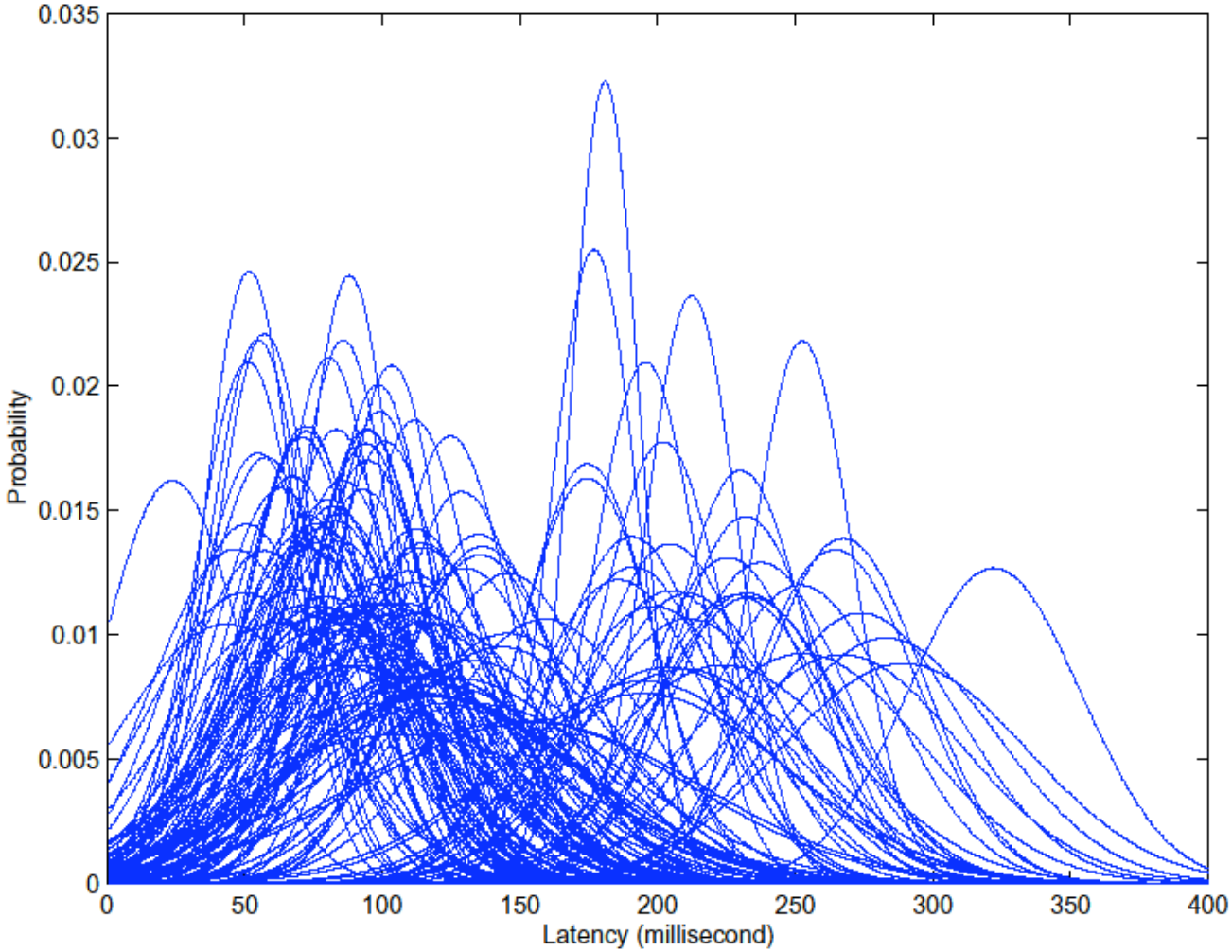
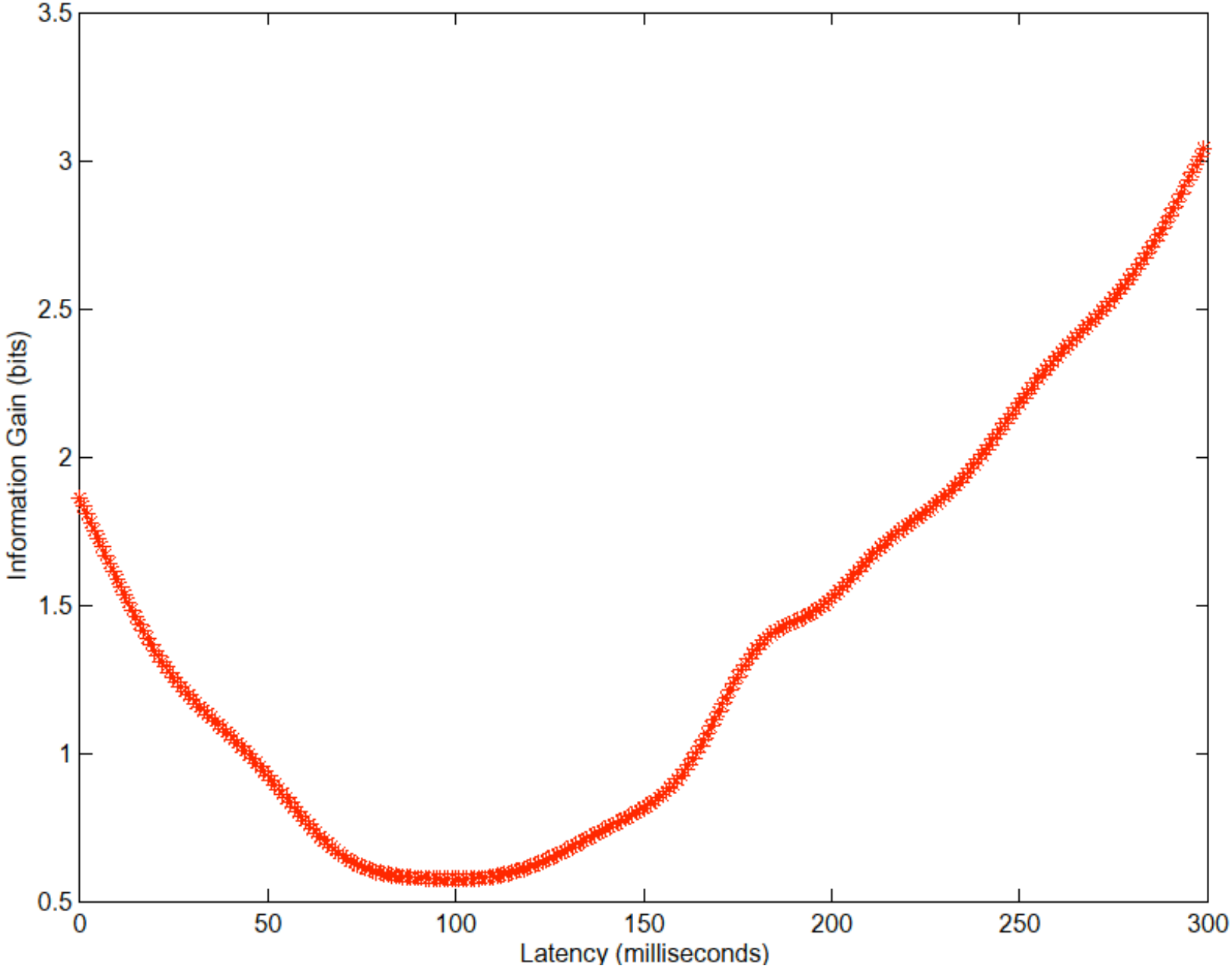
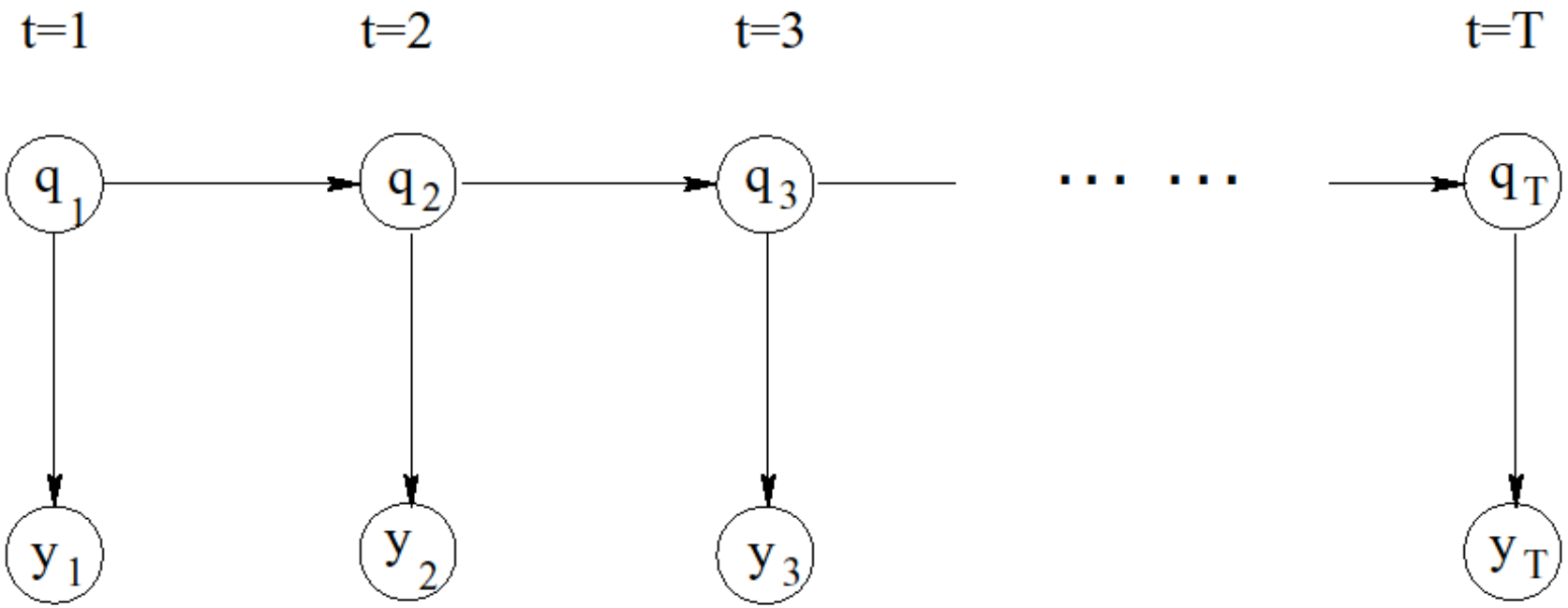


Figure 5: Estimated Gaussian distributions of all 142 character pairs collected from a user.


3.5
3
2.5
2
1.5
1
0.5
Information Gain (bits)
0
50
100
150
200
250
300
Latency (milliseconds)


t=1
t=2
t=3
t=T
q 1
q 2
q 3
q T
y 1
y 2
y 3
y T

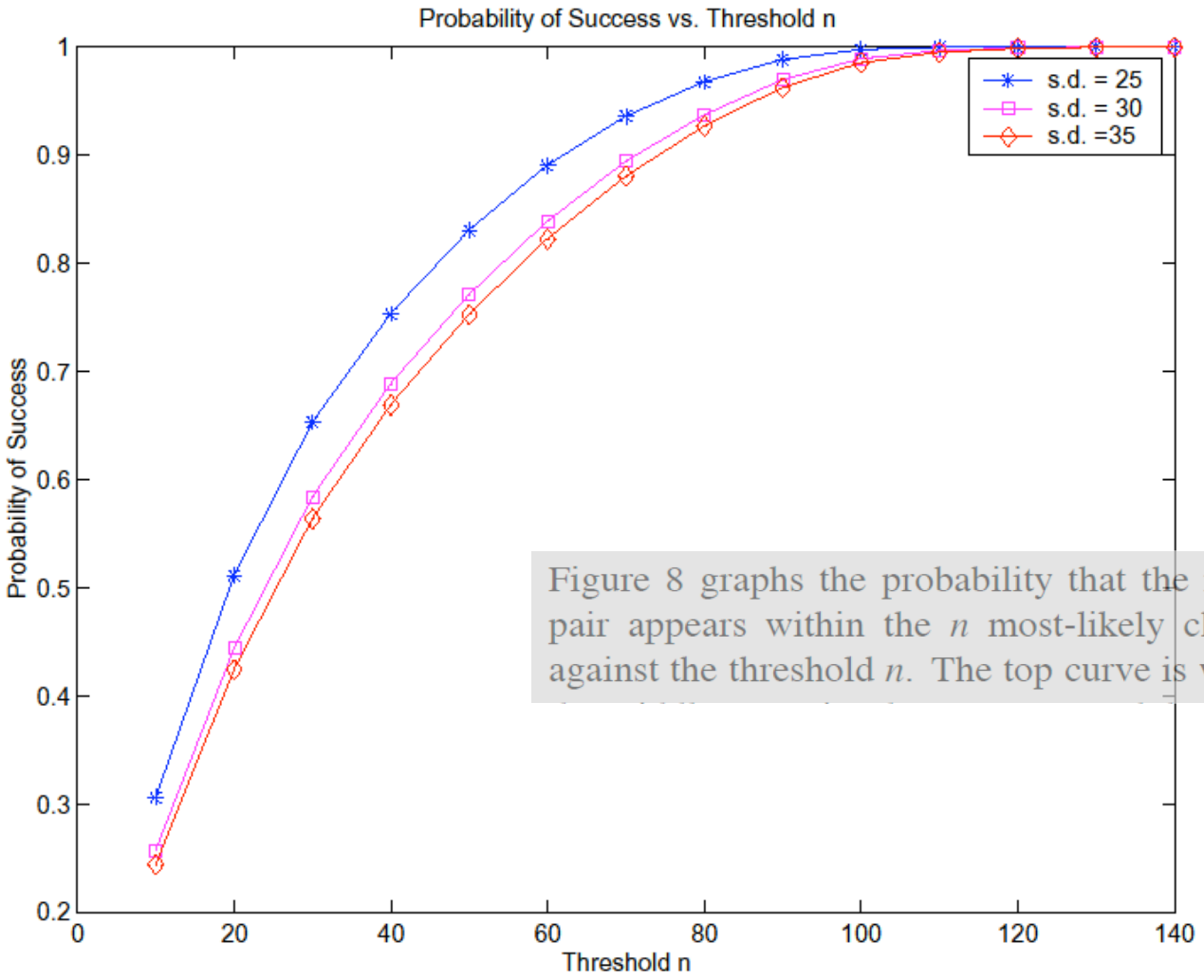


Figure 8 graphs the probability that the real character pair appears within the n most-likely character pairs against the threshold n. The top curve is when $\sigma = 25$,

Figure 8: The probability that the n-Viterbi algorithm outputs the correct password before the first n guesses, graphed as a function of n.

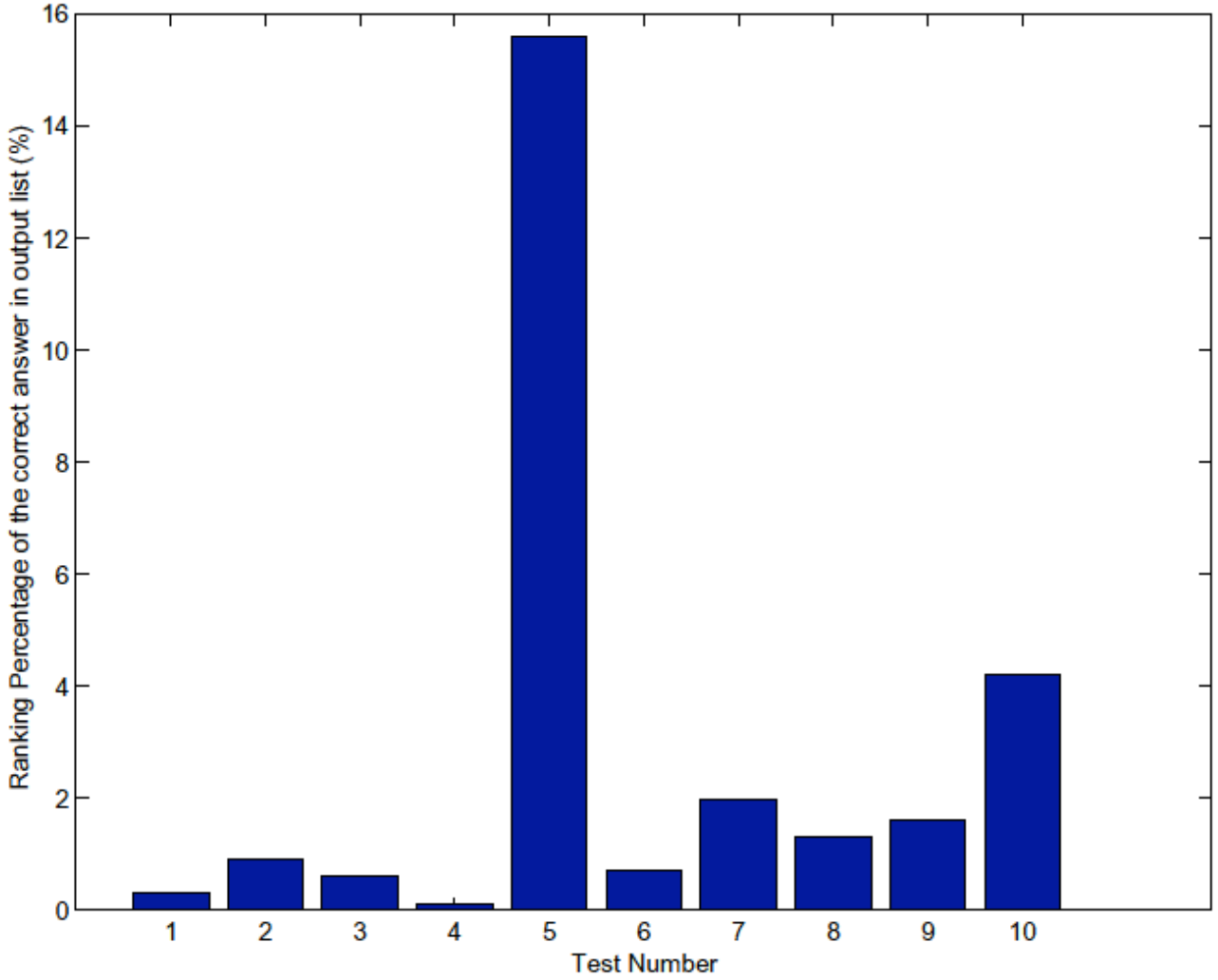
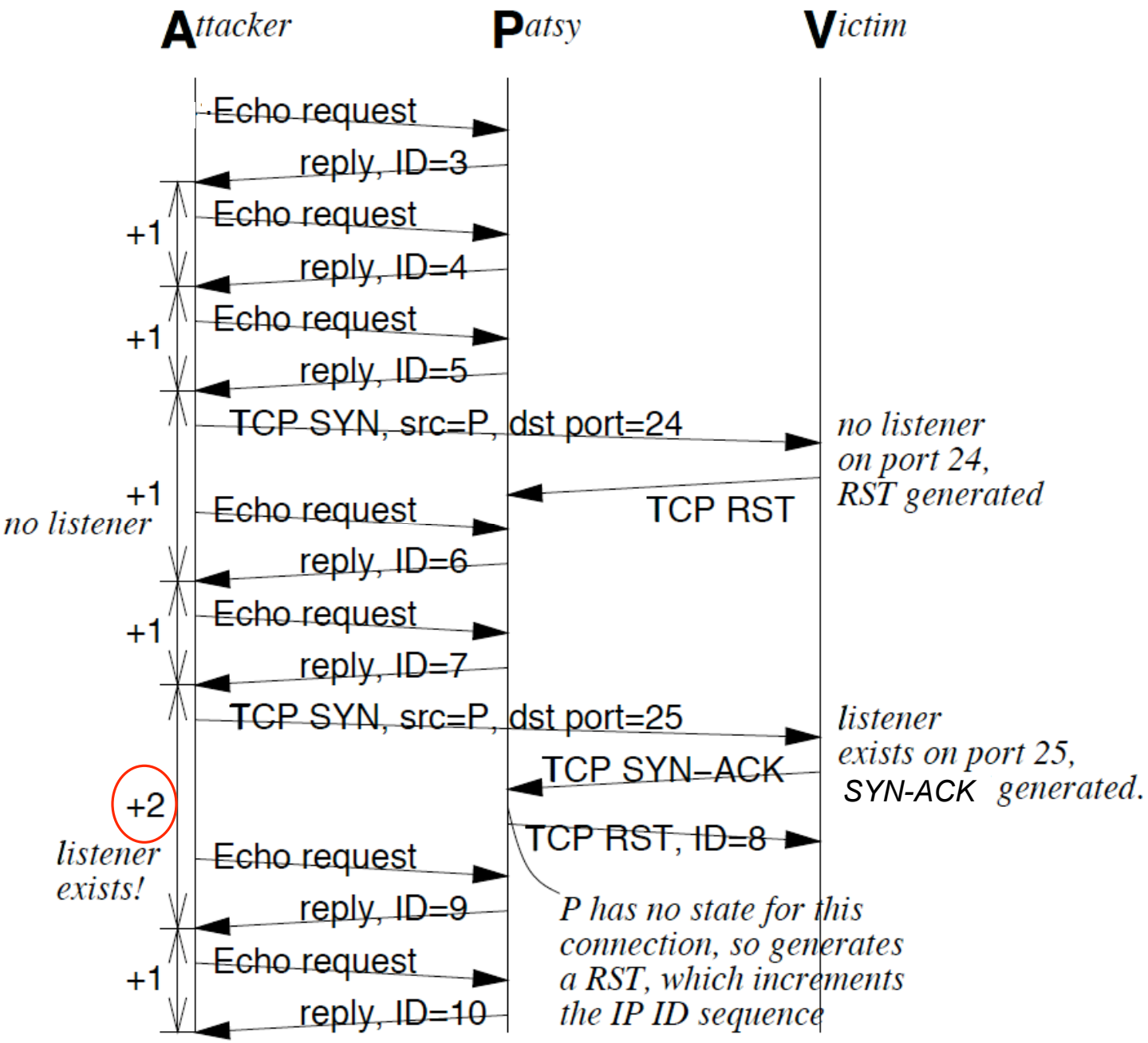
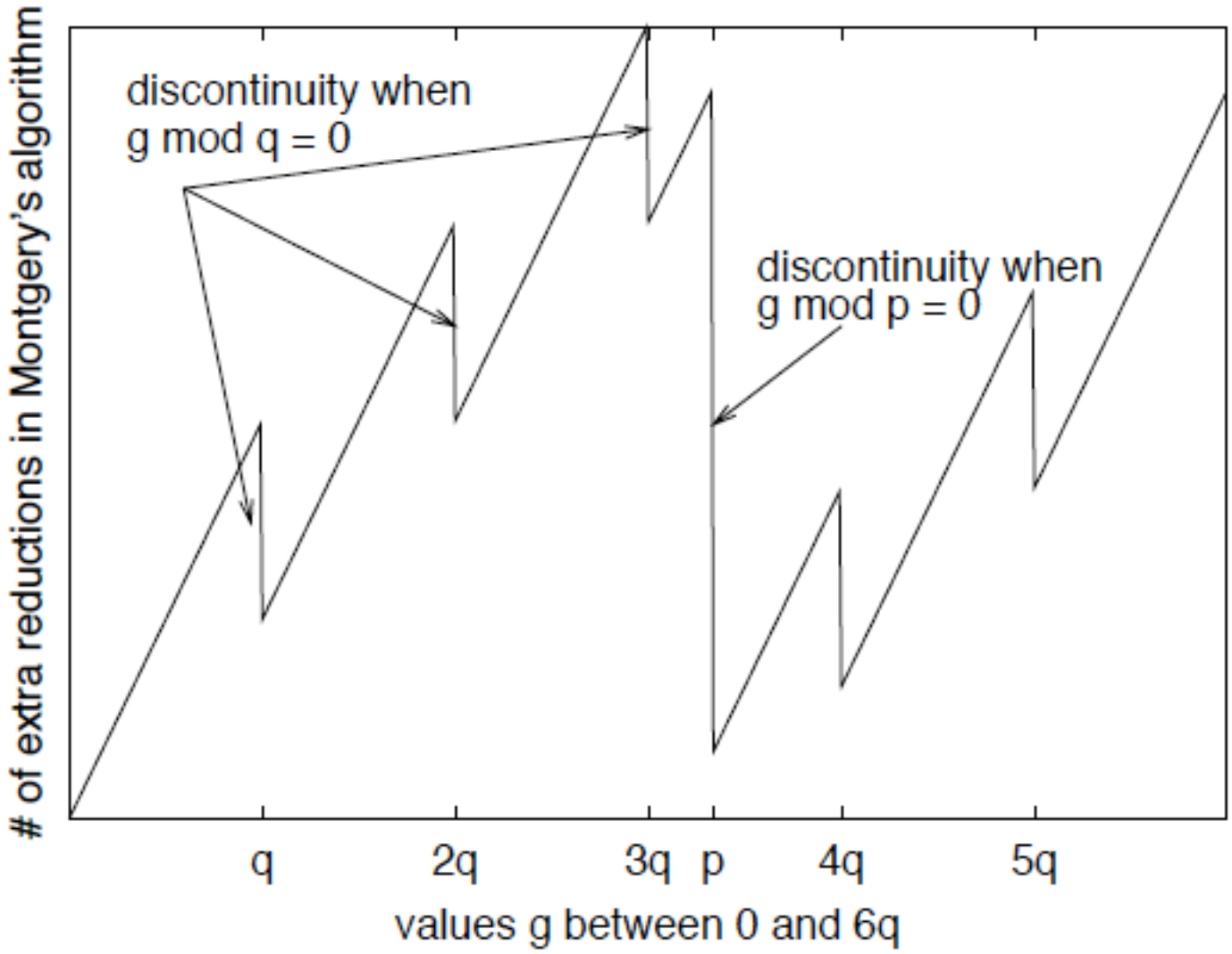


Figure 10: The percentage of the password space tried by Herbivore in 10 tests before finding the right password.

Training Set	Test Set	Test Cases				
		Password 1	Password 2	Password 3	Password 4	Password 5
User 1	User 1	15.6%	0.7%	2.0%	1.3%	1.6%
User 1	User 2	62.3%	15.2%	7.0%	14.8%	0.3%
User 1	User 3	6.4%	N/A	1.8%	3.1%	4.2%
User 1	User 4	1.9%	31.4%	1.1%	0.1%	28.8%
User 2	User 1	4.9%	1.3%	1.6%	12.3%	3.1%
User 2	User 2	30.8%	15.0%	2.8%	3.7%	2.9%
User 2	User 3	4.7%	N/A	5.3%	6.7%	38.4%
User 2	User 4	0.7%	16.8%	3.9%	0.6%	5.4%

Table 1: Success rates for password inference with multiple users. The numbers are the percentage of the search space the attacker has to search before he finds the right password.


Attacker
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
TCP SYN, src=P, dst port=24
no listener on port 24, RST generated
TCP RST
+1
no listener
Echo request
reply, ID=6
+1
Echo request
reply, ID=7
TCP SYN, src=P, dst port=25
listener exists on port 25, SYN-ACK generated.
TCP SYN–ACK
+2
TCP RST, ID=8
listener exists!
Echo request
reply, ID=9
+1
Echo request
reply, ID=10
P has no state for this connection, so generates a RST, which increments the IP ID sequence


discontinuity when
g mod q = 0
discontinuity when
g mod p = 0
# of extra reductions in Montgery's algorithm
q
2q
3q
p
4q
5q
values g between 0 and 6q