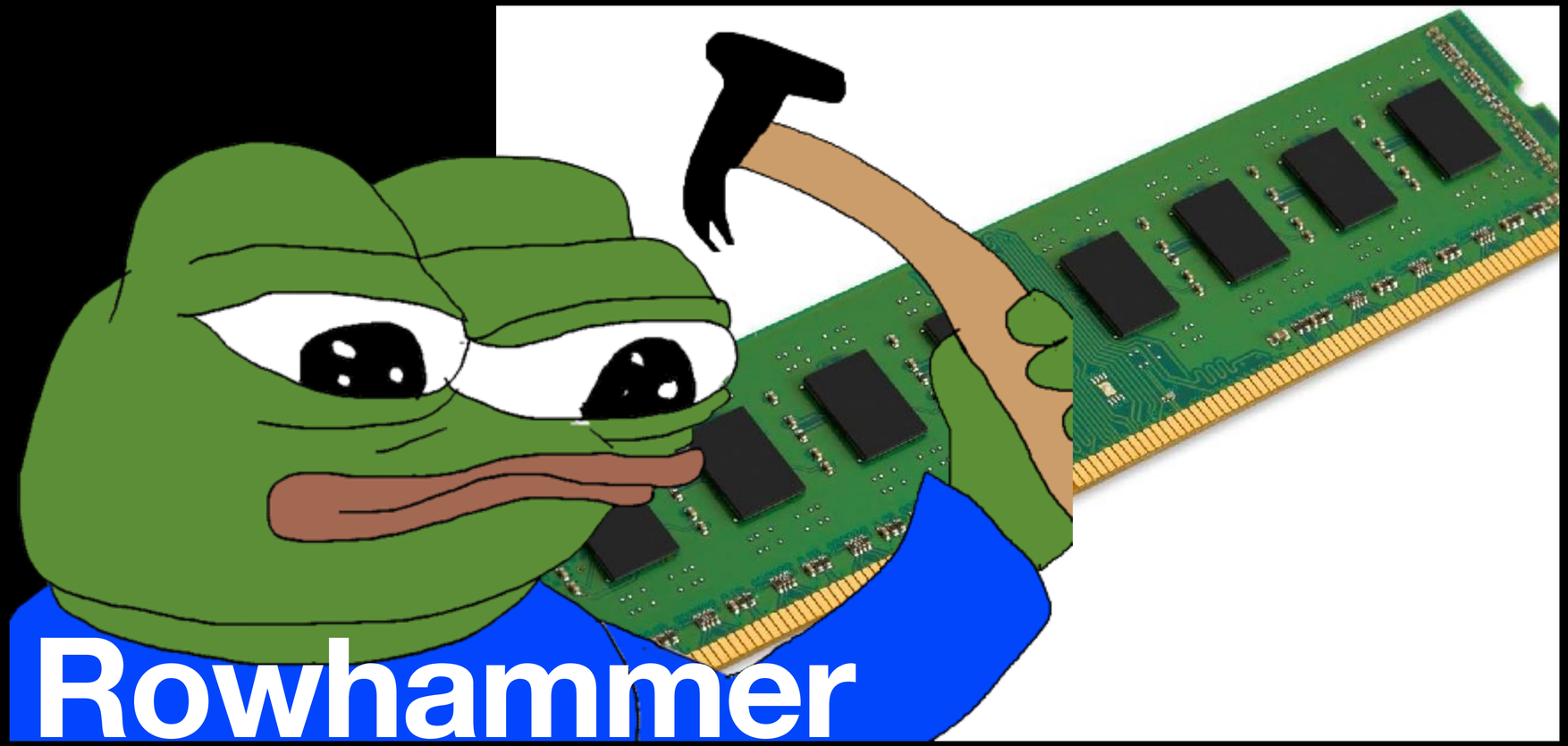
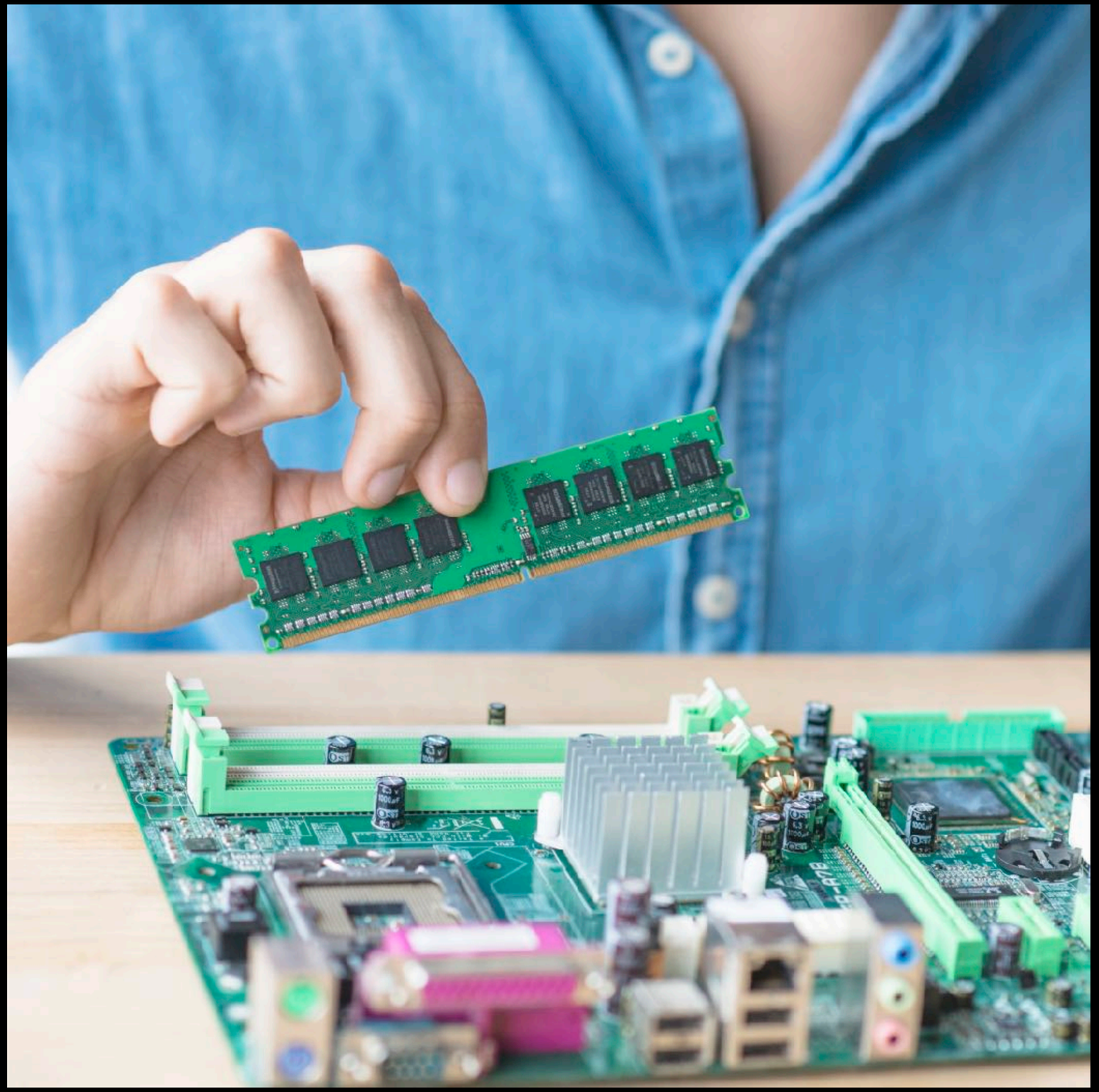
jboy — 2024-11-08



Rowhammer

Grundlagen und aktuelle Entwicklungen

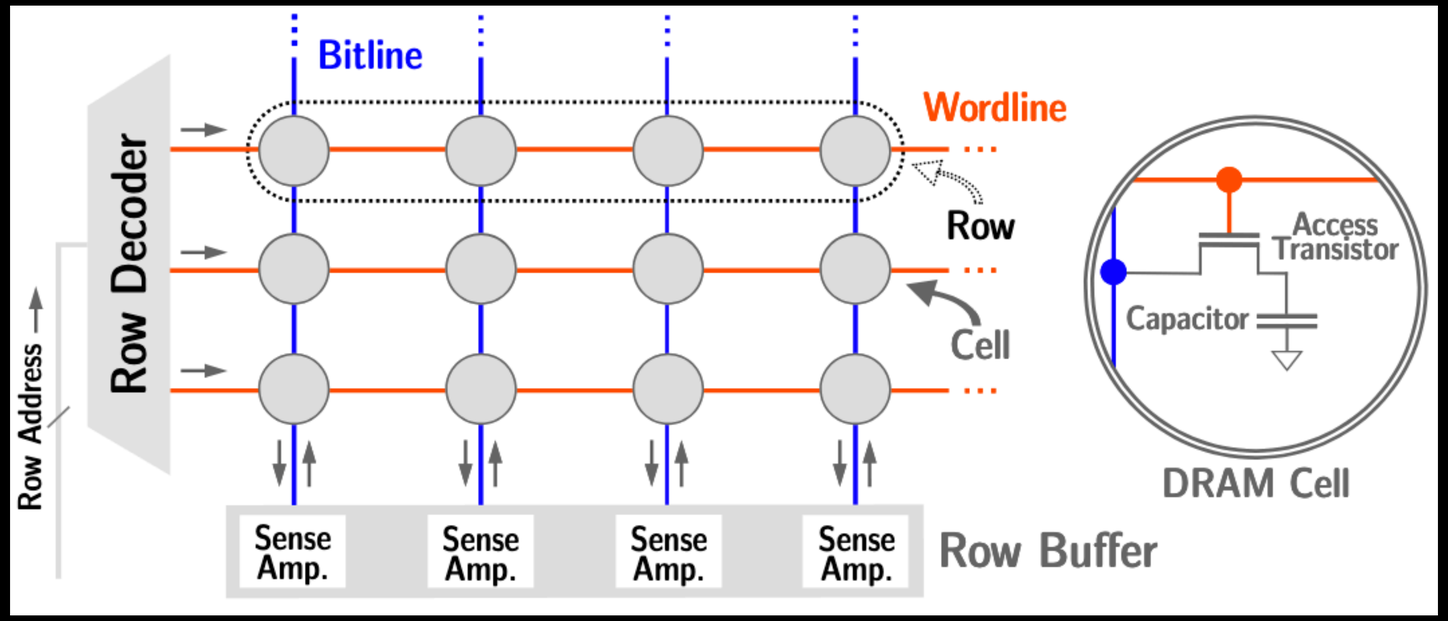


DDR

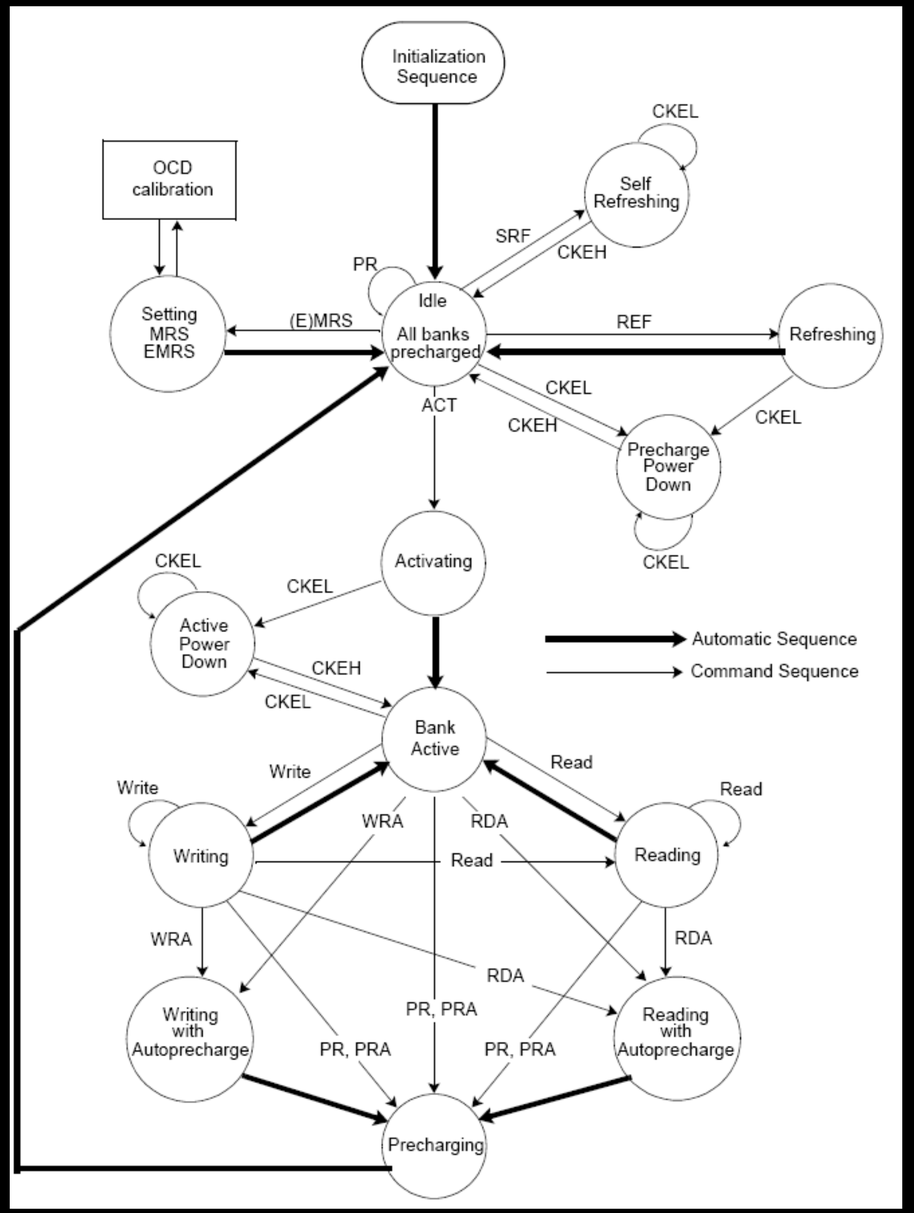
DDR2

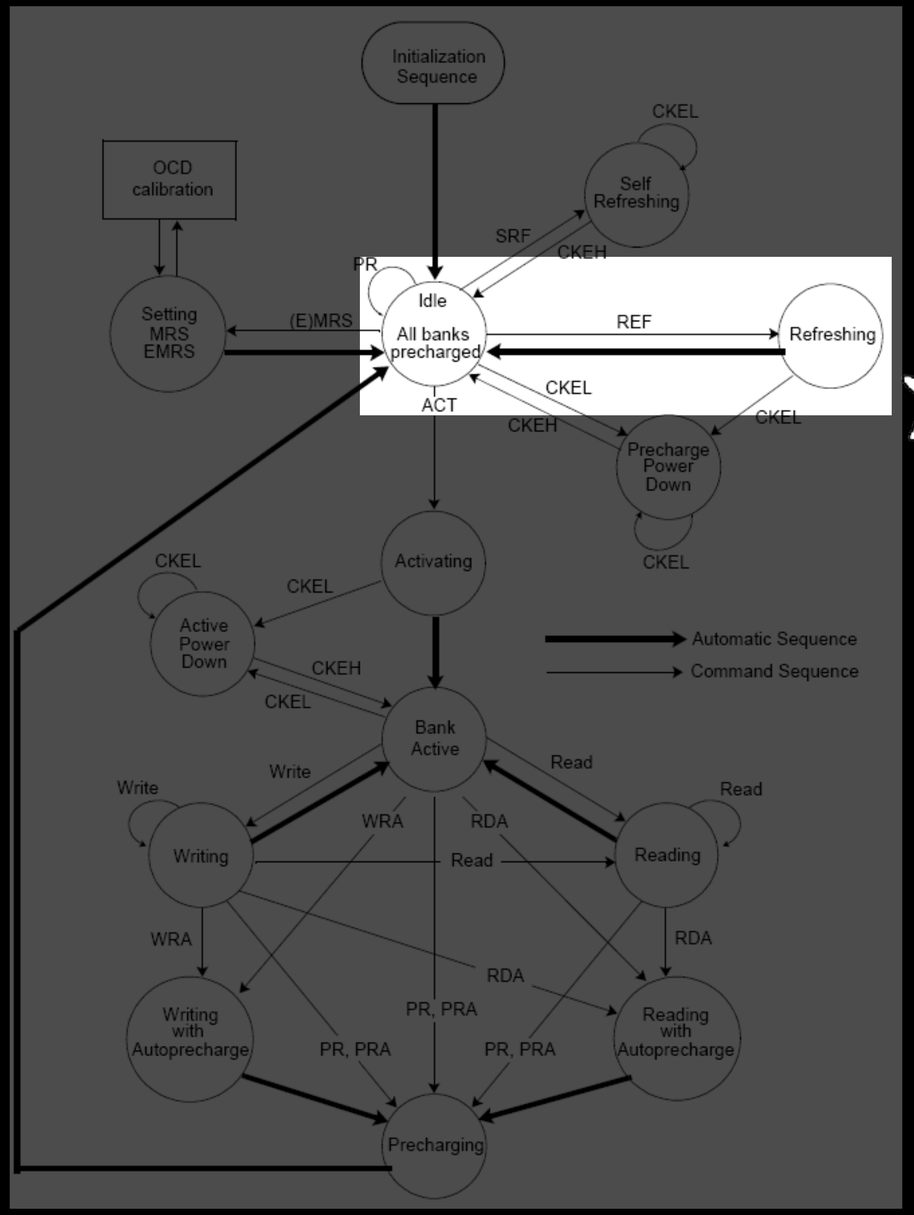
DDR3

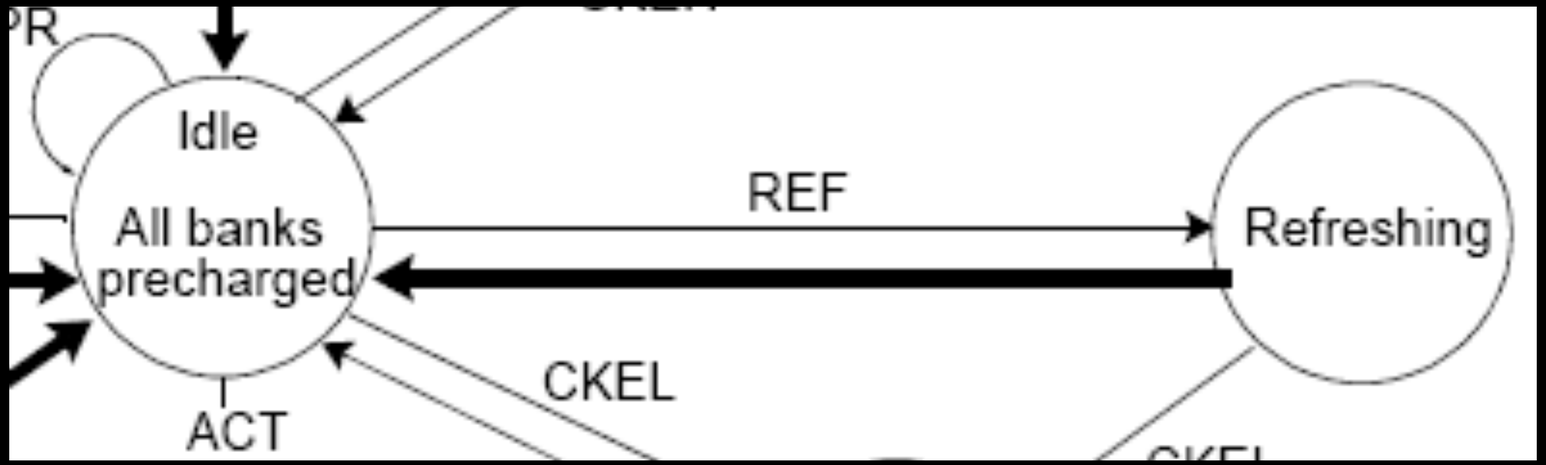
DDR4

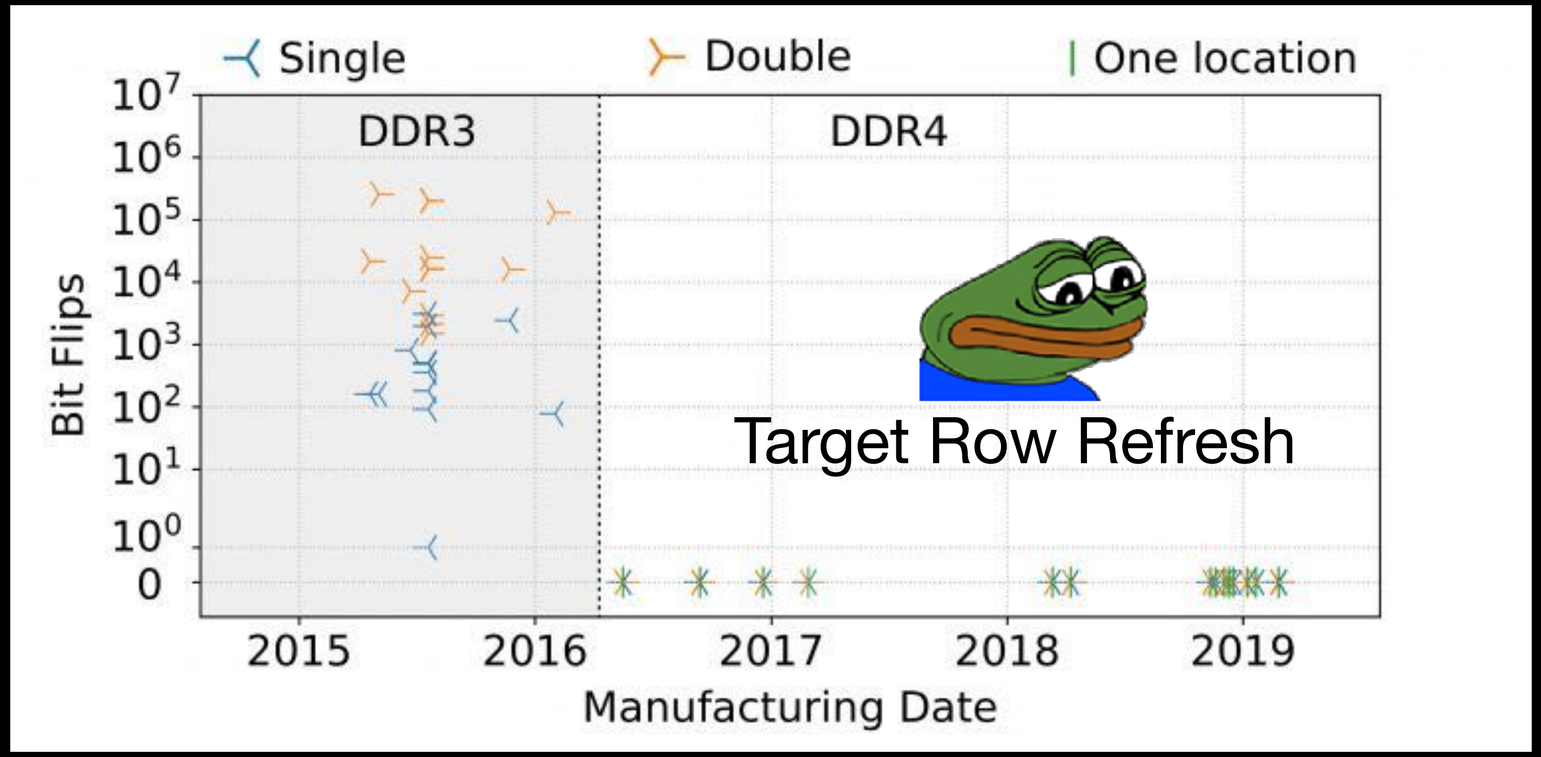

Bitline
Wordline
Row Decoder
Row
Cell
Row Address
Sense Amp.
Sense Amp.
Sense Amp.
Sense Amp.
Row Buffer
Access Transistor
Capacitor
DRAM Cell


wow
many bitflip
much cryptography
c = m^e mod n
s_p = m^{d_p} mod p
broken computer
if (authenticated) { return true; }
made with dogetizer


Initialization Sequence
OCD calibration
Self Refreshing
CKEL
SRF
CKEH
PR
Idle
All banks precharged
Setting MRS EMRS
(E)MRS
REF
Refreshing
CKEL
ACT
CKEH
Precharge Power Down
CKEL
CKEL
Activating
CKEL
Active Power Down
CKEH
CKEL
Automatic Sequence
Command Sequence
Bank Active
Write
Read
Write
Read
WRA
RDA
Writing
Read
Reading
WRA
RDA
RDA
Writing with Autoprecharge
PR, PRA
PR, PRA
PR, PRA
Reading with Autoprecharge
Precharging


Initialization Sequence
CKEL
OCD calibration
Self Refreshing
SRF
CKEH
PR
Idle
All banks precharged
(E)MRS
Setting MRS EMRS
REF
Refreshing
CKEL
ACT
CKEH
CKEL
Precharge Power Down
CKEL
Activating
CKEL
CKEL
Active Power Down
CKEH
CKEL
Automatic Sequence
Command Sequence
Bank Active
Write
Read
Write
Read
WRA
RDA
Writing
Read
Reading
WRA
RDA
RDA
Writing with Autoprecharge
PR, PRA
PR, PRA
PR, PRA
Reading with Autoprecharge
Precharging


Idle
All banks
precharged
REF
Refreshing
CKEL
ACT


Single
Double
One location
DDR3
DDR4
Bit Flips
10^7
10^6
10^5
10^4
10^3
10^2
10^1
10^0
0
2015
2016
2017
2018
2019
Manufacturing Date
Target Row Refresh

Und nu?

Fuzzing!

DIMM	Blacksmith				TRRespass [12]			
	$\lvert\mathbb{P}^{+}\rvert$	$\lvert\mathbb{F}^{\text{total}}_{\text{fuzz}}\rvert$	$\lvert\mathbb{F}^{\text{total}}_{\text{swp}}\rvert$	$\lvert\mathbb{F}^{0\to1}_{\text{swp}}\rvert$	$\lvert\mathbb{P}^{+}\rvert$	$\lvert\mathbb{F}^{\text{total}}_{\text{fuzz}}\rvert$	$\lvert\mathbb{F}^{\text{total}}_{\text{swp}}\rvert$	$\lvert\mathbb{F}^{0\to1}_{\text{swp}}\rvert$
$\mathcal{A}_0$	47	1,061	82,183	41,471	0	–	–	–
$\mathcal{A}_1$	116	2,125	12,134	6,095	12	12	5	5
$\mathcal{A}_2$	462	106,815	134,702	68,801	715	16,054	7,404	4,563
$\mathcal{A}_3$	82	239	1,746	890	326	852	114	58
$\mathcal{A}_4$	460	1,604	5,132	2,602	78	105	22	9
$\mathcal{A}_5$	42	7,771	113,190	57,655	0	–	–	–
$\mathcal{A}_6$	102	17,790	98,425	49,296	4	11	4	4
$\mathcal{A}_7$	66	3,415	32,090	15,988	0	–	–	–
$\mathcal{A}_8$	83	11,105	92,660	46,914	0	–	–	–
$\mathcal{A}_9$	349	1,176	4,889	2,461	14	844	1	1
$\mathcal{A}_{10}$	350	1,282	3,051	1,532	367	961	505	280
$\mathcal{A}_{11}$	202	632	3,171	1,630	261	479	38	25
$\mathcal{A}_{12}$	74	13,641	43,581	22,149	0	–	–	–
$\mathcal{A}_{13}$	72	9,889	59,721	30,320	0	–	–	–
$\mathcal{A}_{14}$	51	9,729	64,083	32,543	1	1	4	0
$\mathcal{A}_{15}$	67	8,333	52,580	26,483	0	–	–	–
$\mathcal{A}_{16}$	372	61,493	99,552	51,029	688	5,499	1,450	983
$\mathcal{A}_{17}$	425	57,245	138,601	70,902	711	12,196	3,871	2,690
$\mathcal{A}_{18}$	126	12,689	80,601	40,876	14	14	1	1
$\mathcal{A}_{19}$	107	2,543	11,599	5,736	0	–	–	–
$\mathcal{B}_0$	9	11	63	22	0	–	–	–
$\mathcal{B}_1$	7	14	506	256	0	–	–	–
$\mathcal{B}_2$†	9	41	15	7	7	8	5	3
$\mathcal{B}_3$	1	2	111	58	0	–	–	–
$\mathcal{B}_4$	101	177	1,107	577	0	–	–	–
$\mathcal{B}_5$	19	24	14	6	0	–	–	–
$\mathcal{B}_6$	18	41	78	46	0	–	–	–
$\mathcal{B}_7$	4	4	70	34	0	–	–	–
$\mathcal{B}_8$†	4	6	258	131	0	–	–	–
$\mathcal{B}_9$†	40	86	1,223	625	0	–	–	–
$\mathcal{C}_0$	1	3	26	16	0	–	–	–
$\mathcal{C}_1$	16	29	28	8	0	–	–	–
$\mathcal{C}_2$	82	282	2,551	1,242	0	–	–	–
$\mathcal{C}_3$	6	7	636	296	0	–	–	–
$\mathcal{C}_4$	31	57	769	385	0	–	–	–
$\mathcal{C}_5$	23	58	1,028	516	0	–	–	–
$\mathcal{D}_0$	26	250	10,646	5,329	0	–	–	–
$\mathcal{D}_1$	37	458	6,655	3,406	3	3	0	–
$\mathcal{D}_2$	3	16	2,030	1,008	0	–	–	–
$\mathcal{D}_3$	41	463	6,797	3,475	8	8	1	1
$\sum$	**4,133**		**1.168 M**		**3,209**		**13,425**	

References

- P. Jattke, V. Van Der Veen, P. Frigo, S. Gunter and K. Razavi, "BLACKSMITH: Scalable Rowhammering in the Frequency Domain," *2022 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2022, pp. 716-734, doi: 10.1109/SP46214.2022.9833772.

- Frigo, Pietro, et al. "TRRespass: Exploiting the many sides of target row refresh." *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020.

- Ji, Jinsong & Wang, Chao & Zhou, Xuehai. (2008). System-Level Early Power Estimation for Memory Subsystem in Embedded Systems. 370 - 375. 10.1109/SEC.2008.48.