DRAM の構造及び Rowhammer に関する調査

演習III

Liu Luhao

0612

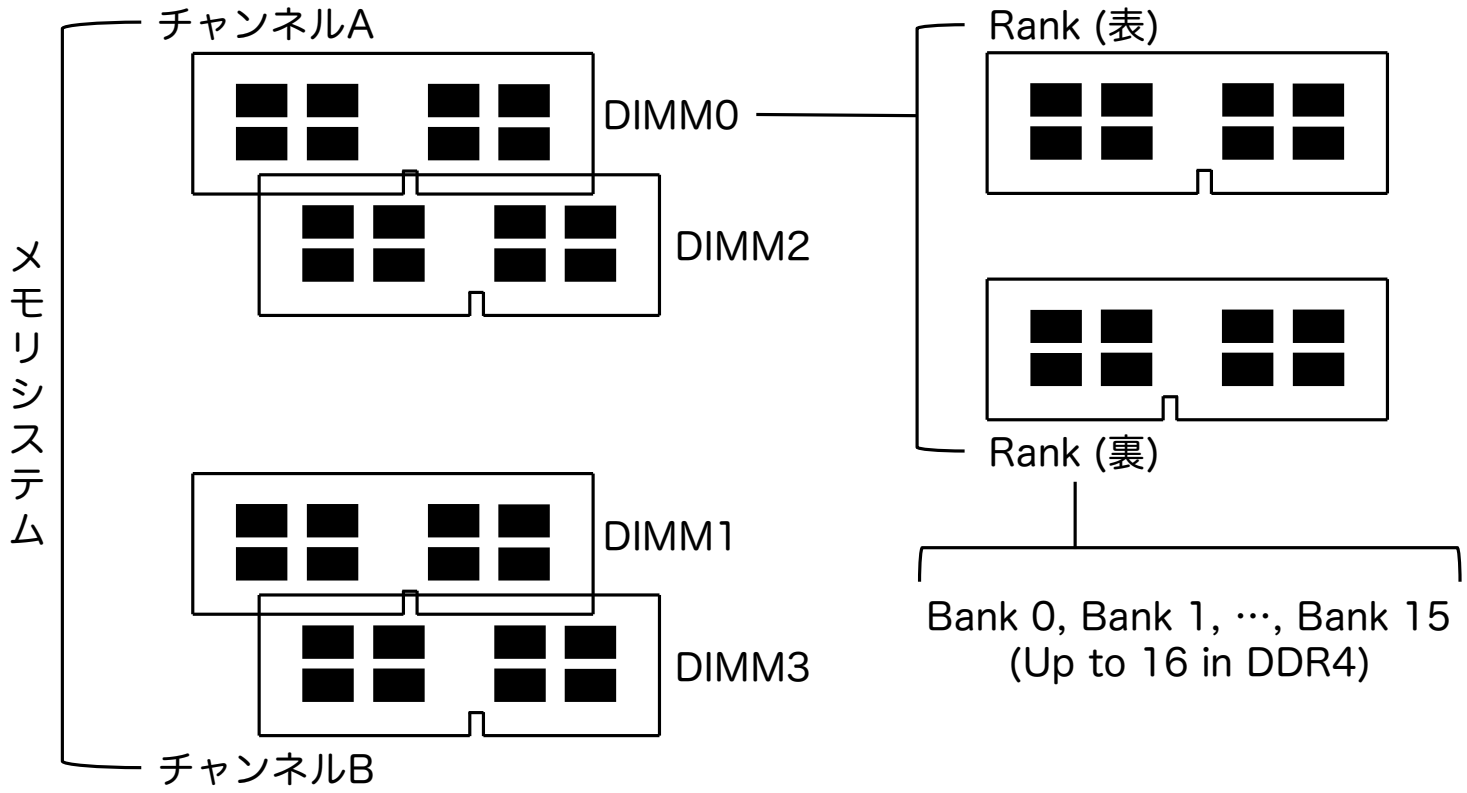
Rowhammer

あるメモリラインにアクセスし続けると，物理的に近いメモリラインでビット反転が起きてしまうハードウェアのバグ

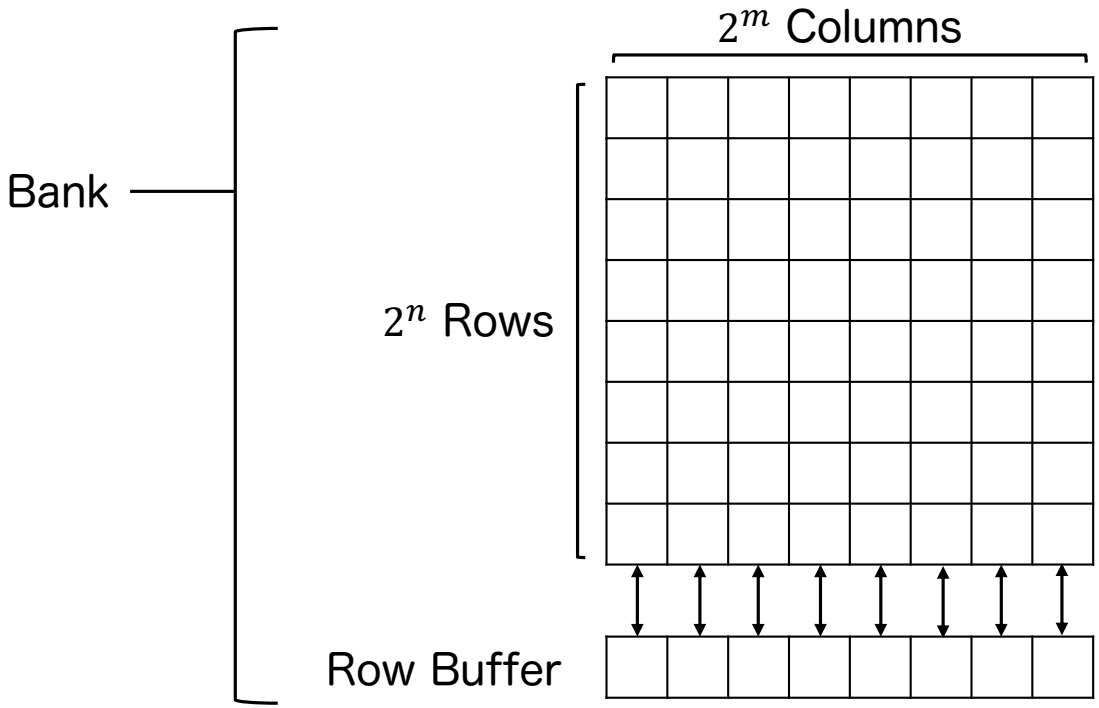
しかし，物理アドレスの近さ ≠ 物理的に近い

関連研究をするためにはまず DRAM の構造を調査し，物理アドレスとの対応関係を調べる必要がある

メモリシステムの構成


チャンネルA
DIMM0
DIMM2
メモリシステム
DIMM1
DIMM3
チャンネルB
Rank (表)
Rank (裏)
Bank 0, Bank 1, ⋯, Bank 15
(Up to 16 in DDR4)

メモリシステムの構成



適切にドライバをロードしていれば decode-dimms 命令で具体的な数値を確認できる

一般的には行数が $2^{14} - 2^{17}$ で列数が 2^{10} で各セルが 64bits であることが多い

バンクレベル並列性とタイミング

各バンクはそれぞれ独立した Rowbuffer を持っている
そのため異なるバンクへのアクセスは同時に行える

言い換えれば，同じバンクで異なる Row への交互アクセスは，
必ず Rowbuffer にヒットしないので比較的に遅くなる

これをうまく使えば，物理アドレスがどのように行・バンク・列
に対応しているのかを調べることができる

Pessl, P., Gruss, D., Maurice, C., Schwarz, M., & Mangard, S. (2016). {DRAMA}: Exploiting {DRAM} addressing for {Cross-CPU} attacks. In *25th USENIX security symposium (USENIX security 16)* (pp. 565-581).

物理アドレスの先へ

AMDはこの変換方法を BIOS and Kernel Developer’s Guide で公開しているが，Intel は調べた限り公開していない様子

バンクレベルの並列性を利用したいので，よくあるメモリアクセスパターン(e.g. 配列)を考慮すると，高位ビットから

[Row Index, Bank Index, Column Index]

とおおよそなるのではないかと予想できる

アクセス時間を測ってみる

大きなメモリ領域を確保して /proc/self/pagemap でページテーブルのエントリを見て対応する物理アドレスを取得する

1bit だけ異なるような二つのアドレスを持ってきて交互にアクセスし，アクセス時間が長いものは選択した bit が Row のみを決める bit であることがわかる

Row のみを決める bit に加えてさらに 1bit 異なるような二つのアドレスを持ってきて交互にアクセスし，アクセス時間が長いものは Column のみを決める bit であることがわかる

Wang, M., Zhang, Z., Cheng, Y., & Nepal, S. (2020, July). Dramdig: A knowledge-assisted tool to uncover dram address mapping. In 2020 57th ACM/IEEE Design Automation Conference (DAC) (pp. 1-6). IEEE.

アクセス時間を測ってみる

時間計測に必要なプリミティブ

1. サイクルレベルのカウンタ
   rdtsc/rdtscp 命令
2. 特定のキャッシュラインを無効化する命令
   clflush 命令

アクセス時間を測ってみる

しかし，同一の bit が複数の役割を持つこともあるので，残りの bit が全て Bank のみに関連する bit であるとは限らない

さらに精査する必要があるが，時間の都合上そこまでやることはできなかった

論文の結果をそのまま載せると

アクセス時間を測ってみる

Machine No.	Microarch.	DRAM		Bank Address Functions	Row Bits	Column Bits
		Type, Size	Config.			
No.1	Sandy Bridge i5-2400	DDR3, 8GiB	2, 1, 1, 8	(6), (14, 17), (15, 18), (16, 19)	17∼32	0∼5, 7∼13
No.2	Ivy Bridge i5-3230M	DDR3, 8GiB	2, 1, 2, 8	(14, 18), (15, 19), (16, 20), (17, 21), (7, 8, 9, 12, 13, 18, 19)	18∼32	0∼6, 8∼13
No.3	Ivy Bridge i5-3230M	DDR3, 4GiB	1, 1, 2, 8	(13, 17), (14, 18), (15, 19), (16, 20)	17∼31	0∼12
No.4	Haswell i5-4210U	DDR3, 4GiB	1, 1, 1, 8	(13, 16), (14, 17), (15, 18)	16∼31	0∼12
No.5	Haswell i7-4790	DDR3, 16GiB	2, 1, 2, 8	(14, 18), (15, 19), (16, 20), (17, 21), (7, 8, 9, 12, 13, 18, 19)	18∼32	0∼6, 8∼13
No.6	Skylake i5-6600	DDR4, 16GiB	2, 1, 2, 16	(7, 14), (15, 19), (16, 20), (17, 21), (18, 22), (8, 9, 12, 13, 18, 19)	19∼33	0∼7, 9∼13
No.7	Skylake i5-6200U	DDR4, 4GiB	1, 1, 1, 8	(6, 13), (14, 16), (15, 17)	16∼31	0∼12
No.8	Coffee Lake i5-9400	DDR4, 8GiB	1, 1, 1, 16	(6 13), (14 17), (15 18), (16, 19)	17∼32	0∼12
No.9	Coffe Lake i5-9400	DDR4, 16GiB	2, 1, 2, 16	(7, 14), (15, 19), (16, 20), (17, 21), (18, 22), (8, 9, 12, 13, 18, 19)	19∼33	0∼7, 9∼13

TABLE II: Reverse-Engineered DRAM Mappings on 9 different machine settings. (The **Config.** column presents a specific DRAM configuration in a quadruple: (channel (#), DIMMs (#) per channel, ranks (#) per DIMM, banks (#) per rank).)

Wang, M., Zhang, Z., Cheng, Y., & Nepal, S. (2020, July). Dramdig: A knowledge-assisted tool to uncover dram address mapping. In 2020 57th ACM/IEEE Design Automation Conference (DAC) (pp. 1-6). IEEE.

Rowhammer してみる

結果を元に推測するとおそらく
0x102000000
0x102088100 [19, 15, 8 ビット目が1]
0x102110000 [20, 16 ビット目が1]
が同じバンクの連続する 3 Rows の物理アドレス

1番目と3番目に連続アクセスして2番目の値を観測する

Rowhammer してみる

残念ながらビット反転は観測できなかった

```
Before hammer: f0f0f0f0:f0f0f0f0:f0f0f0f0:f0f0f0f0
After hammer: f0f0f0f0:f0f0f0f0:f0f0f0f0:f0f0f0f0
```

考えられる原因

1. Rowhammer のやり方が間違っている
   https://github.com/google/rowhammer-test を参考にした
2. 前記した3つのアドレスが連続した Row ではない
3. 何らかの対策がすでにシステムに入っている
4. 同じ Subarray ではない