REPRODUCING SPECTRE ATTACK WITH GEM5

PIERRE AYOUB - EURECOM

PIERRE.AYOUB@EURECOM.FR

CLÉMENTINE MAURICE - UNIV LILLE, CNRS, INRIA CLEMENTINE.MAURICE@INRIA.FR

ICHSA'21

01 JUNE, 2021

PROCESSOR'S MICROARCHITECTURE IS A **BLACK BOX**

Consequence: Micro-architectural security is **hard**

Transient Instruction

⇒ Affects the processor **micro-architectural state** – leaving its architectural state as prior the execution

Spectre

⇒ Execute malicious transient instructions exploiting the **branch predictor**

SIMULATION CAN BREAK THIS BLACK BOX

How: Allowing the user to view the micro-architecture's behavior

GEM5

Cycle-accurate simulator

⇒ Simulate very precisely hardware entirely in software
Build a system

⇒ Instantiate and parameterize **Python objects**

Run a system

⇒ Launch the Python script, then **view and inspect** the running system!

OBSERVING SPECTRE WITH KONATA

SUCCESS SCENARIO

Cycles (Time)

12807: s182738 (t0: r3384): 0x004006b4:

orr x0, xzr, x26

12769: s182700 (t0: r3392): 0x0041b430:	b.ne 0x41b500																						
12770: s182701 (t0: r3393): 0x0041b500:	subs x2, #16																						
12771: s182702 (t0: r3394): 0x0041b504:	b.cs 0x41b528																						
12772: s182703 (t0: r3349): 0x0040095c:	ret	F DC Rn 1 I	s Cm 1																				
12773: \$182704 (to: \$3350). Av00400054:	dsb	F DC Rn 1	Ds 1	23	4 Is	Cm 1]																
12774:	ldr x1, [sp, #28]	F DC Rn 1	23	45	67	89	10 11	12 Is	Cm 1	23	4	56	78	3 9	10 1	.1 12	13 1	4 15	16 17	18 1	19 20	21 22	2 23
12775: Attacked	ldr x0, [sp, #40]	F DC Rn 1	23	45	67	89	10 11	12 Is	Cm 1	23	4	56	78	3 9	10 1	.1 12	13 1	4 15	16 17	18 :	19 20	21 22	2 23
12776:	scvtf f0, f1	F DC Rn 1	23	45	67	89	10 11	12 Ds	1 2	34	5	67	8 9) 10	11 1	.2 13	14 1	5 16	17 18	19 2	20 21	22 23	8 24
12777: Branch	ucvtf f1, f0	F DC Rn 1	23	45	67	89	10 11	12 Ds	1 2	34	5	67	8 9) 10	11 1	.2 13	14 1	5 16	17 18	19 2	20 21	22 23	8 24
12778:	fdiv f0, f0, f1	F DC Rn 1	23	45	67	89	10 11	12 Ds	1 2	34	5	67	8 9) 10	11 1	.2 13	14 1	5 16	17 18	19 3	20 21	22 23	3 24
12779: Condition	fmov f1, #1065353216	F DC Rn 1	23	45	67	89	10 11	12 Is	1 2	Cm 1	2	3 4	56		8 9	9 10	11 1	2 13	14 15	16 :	17 18	19 20) 21
12780	fcmpe f0, f1	F DC Rn 1					10 11	12 Ds					8 9) 10	11 1	.2 13	14 1	5 16	17 18	19 1	20 21	22 23	3 24
12781: 3102/12 (10. 13330). 0x00400674:	b.pl 0x400e88	F DC R						11 Ds							11 1	.2 13					20 21		
L2782: s182713 (t0: r3359): 0x00400e78:	adrp x0, #548864	F DC R	n 1 2	34	56	78	9 10	11 12	Is														
12783: s182714 (t0: r3360): 0x00400e7c:	ldr x0, [x0, #3992]	F DC R																					
12784: s182715 (t0: r3361): 0x00400e80:	ldrb w0, [w0, w1, SXTW]	F 1	23	45	67	89	10 11	12 Dc		Ds 1													
12785: s182716 (t0: r3362): 0x00400e84:	bl 0x400bdc	F 1	23	4 5	67	89	10 11	12 Dc															
12786: s182717 (t0: r3363): 0x00400bdc:	adrp x1, #557056	F	: 1 2	3 4	56	7 8	9 10	11 Dc	Rn 1	Is													
12787: s182718 (t0: r3364): 0x00400be0:	and x0, x0, #255	F	: 1 2	3 4	56	7 8	9 10	11 Dc		Ds 1													
12788: s182719 (t0: r3365): 0x00400be4:	ldr x2, [x1, #2656]	F		3 4	56		9 10	11 Dc															
12789: s182720 (t0: r3366): 0x00400be8:	adrp x1, #548864	F	: 1 2	3 4	56	78	9 10	11 Dc															
12790: s182721 (t0: r3367): 0x00400bec:	ldr x1, [x1, #3968]	F					9 10	11 Dc															
12791. \$182722 (to. r3368). @x00400bf0:	ldr x1, [x1]	F	: 1 2	3 4	56	7 8	9 10	11 Dc		Ds 1													
127	madd x0, x1, x0, x2	F	: 1 2	3 4	56	7 8	9 10	11 12	DC Rn														
127 Malicious 18	b 0x400960	F					9 10	11 12	Dc Rn														
127	sub sp, sp, #16		F 1	23	4 5	6 7	89	10 11	. 12 13	DC Rn	1	Is											
127 transient load 14:	ldr x0, [x0]		F 1	23	4 5	6 7	89	10 11	. 12 13	DC Rn	1	Ds 1	2 3	3 4	5 (6 7	8 9	10	11 12	13	14 15	16 17	18
127 58:	str x0, [sp, #12]		F 1	23	45	67	89	10 11	. 12 13	DC Rn	1												
127 Instruction C	dsb		F 1	23	4 5	67	89	10 11	. 12 13	DC Rn													
127 7	isb		F 1	23	4 5	6 7	89	10 11	. 12 13	DC													
127	add sp, sp, #16		F 1	23	4 5	6 7	89	10 11	. 12 13	DC													
12800: s182731 (t0: r3377): 0x00400978:	ret		F 1	23	4 5	6 7	89	10 11	. 12 13	DC													
12801: s182732 (t0: r3378): 0x00400e88:	ldp_uop x29, x30, [sp]		F	1 2	3 4	56	78	9 10	11 12	DC													
12802: s182733 (t0: r3379): 0x00400e88:	addxi_uop sp, sp, #48							9 10		13 Dc													
12803: s182734 (t0: r3380): 0x00400e8c:	ret							9 10		13 Dc													
12804: s182735 (t0: r3381): 0x00400698:	subs x3, #4			F 1	23	4 5	67	89	10 11	12 Dc													
12805: s182736 (t0: r3382): 0x0040069c:	b.ls 0x4006b0			F 1	2 3	4 5	6 7	89	10 11	12 Dc													
12806: s182737 (t0: r3383): 0x004006b0:	orr x1, xzr, x24			F				7 8	9 10	11 Dc													

Allows to understand how the attack works

Instructions



DEFEATED BY THE BRANCH PREDICTOR

Cycles (Time)

Instructions

176001: s345932 (t0: r45933): 0x0040095c:		F DC Rn 1 IS Cm 1
1760-22	dsb	F DC Rn 1 DS 1 2 3 4 Is Cm 1
1766	ldr x1, [sp, #28]	F DC Rn 1 2 3 4 5 6 7 8 9 10 11 12 Is Cm 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
1766 ALLA AL D. A ALL'	ldr x0, [sp, #40]	F DC Rn 1 2 3 4 5 6 7 8 9 10 11 12 Is Cm 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44
1766 Attacked Branch	scvtf f0, f1	F DC Rn 1 2 3 4 5 6 7 8 9 10 11 12 Ds 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 Is 1 Cm 1
	ucvtf f1, f0	F DC Rn 1 2 3 4 5 6 7 8 9 10 11 12 Ds 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 Is 1 Cm 1
	fdiv f0, f0, f1	F DC Rn 1 2 3 4 5 6 7 8 9 10 11 12 Ds 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 Is 1 2 3 4 5 6 7 8 9 10 11 Cm 1
1766 ::	fmov f1, #1065353216	F DC Rn 1 2 3 4 5 6 7 8 9 10 11 12 Is 1 2 Cm 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56
1766):	fcmpe f0, f1	F DC Rn 1 2 3 4 5 6 7 8 9 10 11 12 Ds 1 2 3 4 5 6 7 8 9 10 11 12 Ds 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 43 53 63 73 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 Is 1 Cm 1
176010. 5345941 (LU. 145942). UXUU400014:	b.pl 0x400e88	F Dc Rn 1 2 3 4 5 6 7 8 9 10 11 Ds 1 2 3 4 5 6 7 8 9 10 11 Ds 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 Is Cm 1
1766 ::	ldp_uop x29, x30, [sp]	F 1 2 3 4 5 6 7 8 9 10 11 DC Rn 1 Is Cm 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59
¹⁷⁶⁶ Malicious Part of	addxi_uop sp, sp, #48	F 1 2 3 4 5 6 7 8 9 10 11 Dc Rn 1 Is Cm 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59
1766 Widneroud I dit of	ret	F 1 2 3 4 5 6 7 8 9 10 11 Dc Rn 1 Ds 1 Is Cm 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57
¹⁷⁶⁶ the Branch Not	subs x3, #4	F 1 2 3 4 5 6 7 8 9 10 Dc Rn 1 Is Cm 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 32 4 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59
1766 the Branch tot ::	b.ls 0x4006b0	F 1 2 3 4 5 6 7 8 9 10 Dc Rn 1 Ds Is Cm 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 33 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58
Taken	dsb	F 1 2 3 4 5 6 7 8 9 10 Dc Rn 1 Ds 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 33 24 25 26 27 28 29 30 31 32 33 43 53 63 73 83 9 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 Is cm 1
1760	orr w1, wzr, w3	F 1 2 3 4 5 6 7 8 9 10 Dc Rn 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 44 55 65 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 Is Cm 1
1766	orr x0, xzr, x23	F 1 2 3 4 5 6 7 8 9 10 Dc Rn 1 2 3 4 5 6 7 8 9 10 Dt Rn 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 Is cm 1
176019: s345950 (t0: r45951): 0x004006ac:	DL 0x400bfc	F 1 2 3 4 5 6 7 8 9 10 11 DC Rn 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 9 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 Is Cm 1
176020: \$345951 (t0: r45952): 0x00400bTc:	addx1_uop ureg0, sp, #-96	F 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 4 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 DC Rn 1 18 Cm 1
176021: \$345952 (t0: r45953): 0x00400bfc:	strx1_uop x29, [ureg0]	F 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 4 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 51 52 53 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 DC RN 1 DS 15 Cm 1
170022: \$345953 (L0: F45954): 0x004000FC:	strxt_uop x3a, [urega, #8]	F 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 45 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 51 52 55 54 50 57 58 59 60 51 52 55 54 55 56 57 58 59 60 51 52 55 54 55 56 57 58 50 50 50 50 50 50 50 50 50 50 50 50 50
176023: S345954 (L0: F45955): 0x004000DC:	addx1_uop sp, urege, #e	
176024. 5345955 (to. 145956). 0x00400000.	adu x29, 5µ, #0	
176026, $c245057$ (to, $r45957$), $0x00400c04$.	strvi uon v21 [uren0]	
176027: s345958 (to: r45959): 0x00400c04.	strxi uop x22, [ureg0]	
176028: s345959 (t0: r45960): 0x00400c08:	adrp x22, #548864	
176029: s345960 (t0: r45961): 0x00400c0c:	sbfm x21, x1, #0, #31	
176030: s345961 (t0: r45962): 0x00400c10:	addxi_uop ureg0, sp, #48	F 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 <u>68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 Dc Rm 1 25</u>
176031: s345962 (t0: r45963): 0x00400c10:	strxi_uop x23, [ureg0]	F 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 Dc Rn 1 Ds 15 Cm 1
176032: s345963 (t0: r45964): 0x00400c10:	strxi_uop x24, [ureg0, #8]	F 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 Dc Rn 1 Ds 1s 0m 1
176033: s345964 (t0: r45965): 0x00400c14:		F 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 Dc Rn 1 15 Cm 1 2
176034: s345965 (t0: r45966): 0x00400c18:		F 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 Dc Rn 1 Ds Is Cm 1 2
176035: s345966 (t0: r45967): 0x00400c1c:	ldr x22, [x22, #3968]	F 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 Dc Rn 1 Ds 1 Is Cm 1 2
176036: s345967 (t0: r45968): 0x00400c20:		F 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 Dc Rn 1 Ds 1s Cm 1 2
176037: s345968 (t0: r45969): 0x00400c24:		F 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 Dc Rn 1 Ds Is Cm 1 2 3
176038: s345969 (t0: r45970): 0x00400c28:		F 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 Dc Rn 1 Is Cm 1 2 3 4
176039: s345970 (t0: r45971): 0x00400c28:		F 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 Dc Rn 1 Ds Is Cm 1 2 3

Allows to visualize the root cause of a failed attack!

TRAINING SCENARIO

Instructions

Cycles (Time)



We can even identify more scenarios...

31	32	33	34	35	36 3	7 38	39	40	41	42	43																														
31	32	33	34	35	36 3	7 38	39	40	41	42	43	44																													
32	33	34	35	36	37 3	B 39	40	41	42	Is	1	Cm :																													
32	33	34	35	36	37 3	B 39	40	41	42	43	Is	1 0	m 1	1																											
32	33	34	35	36	37 3	B 39	40	41	42	43	44	45 I	s 1	1 2	3	4	5	6 7	7 8	9	10	11 Cm	1																		
29	30	31	32	33	34 3	5 36	37	38	39	40	41	42 4	3 4	4 4	5 46	47	48	19 5	0 51	52	53	54 55	56																		
32	33	34	35	36	37 3	B 39	40	41	42	43	44	45 4	64	7 41	3 49	50	51	52 5	3 54	55	56	57 Is	1	Cm	1																
32	33	34	35	36	37 3	B 39	40	41	42	43	44	45 4	6 4	7 41	3 49	50	51	52 5	3 54	55	56	57 58	59	Is	Cm	1															
30	31	32	33	34	35 3	6 37	38	39	40	41	42	43 4	4 4	5 40	5 47	48	49	50 5	1 52	53	54	55 56	57	58	59	60															
29	30	31	32	33	34 3	5 36	37	38	39	40	41	42 4	3 4	4 4	5 46	47	48	49 5	0 51	52	53	54 55	56	57	58	59															
29	30	31	32	33	34 3	5 36	37	38	39	Is	Cm	1	2 3	3 4	5	6	7	8 9) 10	11	12	13 14	15	16	17	18															
28	29	30	31	32	33 3	4 35	36	37	38	39	40	41 4	24	3 4	4 45	46	47	18 4	9 50	51	52	53 54	55	56	57	58															
28	29	30	31	32	33 3	4 35	36	37	38	39	40	41 4	2 4	3 4	4 45	46	47	48 4	9 50	51	52	53 54	55	56	57	58															
29	30	31	32	33	34 3	5 36	37	38	39	40	41	IsC	m 1	1 2	3	4	5	6 7	7 8	9	10	11 12	13	14	15 :	16															
27	28	29	30	31	32 3	3 34	35	36	37	38	39	40 4	14	2 4:	3 44	45	46	47 4	8 49	50	51	52 53	54	55	56	57															
28	29	30	31	32	33 3	4 35	36	37	38	39	40	41 4	24	3 44	4 45	46	47	48 4	9 50	51	52	53 54	55	56	57	58 5	59														
27	28	29	30	31	32 3	3 34	35	36	37	38	39	40 4	14	2 4:	3 44	45	46	47 4	8 49	50	51	52 53	54	55	56	57 5	58														
24	25	26	27	28	29 3	Ð 31	32	33	34	35	36	37 3	83	9 40	9 41	42	43 4	14 4	5 46	47	48	49 50	51	52	53	54 5	55														
28	29	30	31	32	33 3	4 35	36	37	38	39	40	41 I	s 1	12	Cm	1	2	3 4	15	6	7	89	10	11	12	13 1	L4														
27	28	29	30	31	32 3	3 34	35	36	37	38	39	40 4	14	2 43	3 44	45	46	47 4	8 49	50	51	52 53	54	55	56	57 5	58														
25	26	27	20								27	20 2	~ 4	0 4	1 42	43	44	45 4	6 47	48	49	50 51	52	53	54	55 E	56														
26	27	20	28		30 3					36		30 3	9 4	0 4.																											
26	0.7.		28	29 30	30 3 31 3	1 32 2 33	33 34	34 35	35 36	36 37	38	38 3 39 4	94 04	1 4	2 IS	Cm	1	2 3	3 4	5	6	78	9	10	11	12 1	L3														
~~		28	29 29 29	29 30 30	30 3 31 3 31 3	1 32 2 33 2 33	33 34 34	34 35 35	35 36 36	36 37 37	37 38 38	30 3 39 4 39 4	94 04 04	1 4 1 4	2 Is 2 43	Cm 44	1 Is (2 3 Cm 1	3 4 L 2	5	6 4	78 56	9 7	10 8	11 : 9 :	12 1 10 1	13 11														
	27 27	28 28 28	29 29 29 29	29 30 30 30	30 3 31 3 31 3 31 3	1 32 2 33 2 33 2 33	33 34 34 34	34 35 35 35	35 36 36 36	36 37 37 37	37 38 38 38	39 4 39 4 39 4 39 4	94 04 04 04	1 4: 1 4: 1 4: 1 4:	2 Is 2 43 2 43	Cm 44 44	1 Is 0 45	2 3 Cm 1 46 4	3 4 1 2 7 48	5 3 49	6 4 50	78 56 5152	9 7 53	10 8 54	11 : 9 : 55 :	12 1 10 1 56 5	13 11 57 5	58 5	96	06	16	2 I	s Cr	n 1							
26 28	27 27 29	28 28 28 30	28 29 29 29 29 31	29 30 30 30 32	30 3 31 3 31 3 31 3 31 3 33 3	1 32 2 33 2 33 2 33 2 33 4 35	33 34 34 34 36	34 35 35 35 35 37	35 36 36 36 38	36 37 37 37 39	38 38 38 38 40	38 3 39 4 39 4 39 4 39 4 41 4	9 4 0 4 0 4 0 4 2 4	1 4: 1 4: 1 4: 1 4: 1 4:	2 Is 2 43 2 43 4 45	Cm 44 44 46	1 Is 45 4	2 3 Cm 1 46 4 48 4	8 4 1 2 7 48 9 50	5 3 49 51	6 4 50 52	7 8 5 6 51 52 53 54	9 7 53 55	10 8 54 56	11 : 9 : 55 : 57 :	12 1 10 1 56 5 58 5	13 57 59 (58 5 50 6	9 6 1 6	06 26	16 36	2 I 4 6	s Cr 5 60	n 1 5 67	68	69	70	Is	Cm	12	3
26 28 28	27 27 29 29	28 28 30 30	28 29 29 29 31 31	29 30 30 30 30 32 32	30 3 31 3 31 3 31 3 33 3 33 3	1 32 2 33 2 33 2 33 4 35 4 35	33 34 34 34 36 36	34 35 35 35 37 37	35 36 36 36 38 38	36 37 37 37 39 39	37 38 38 38 40 40	38 3 39 4 39 4 39 4 41 4 41 4	9 4 0 4 0 4 0 4 2 4 2 4	1 4: 1 4: 1 4: 1 4: 1 4: 1 4: 1 4: 1 4:	2 Is 2 43 2 43 4 45 4 45	Cm 44 44 46 46	1 1s (45 4 47 4	2 3 0m 1 46 4 48 4 48 4	8 4 1 2 7 48 9 50 9 50	5 3 49 51 51	6 4 50 52	7 8 5 6 51 52 53 54 53 54	9 7 53 55 55	10 8 54 56	11 : 9 : 55 : 57 :	12 1 10 1 56 5 58 5	13 57 59 69	58 5 50 6	9 6 1 6	06 26 26	16 36 36	2 I 4 6 4 6	s Cr 5 60	n 1 5 67 6 67	68	69 69	70	Is Is	Cm	12	3
26 28 28 28	27 27 29 29 29	28 28 30 30 30	29 29 29 31 31 31	29 30 30 30 32 32 32	30 3 31 3 31 3 31 3 33 3 33 3 33 3	1 32 2 33 2 33 2 33 4 35 4 35	33 34 34 36 36 36	34 35 35 35 37 37 37	35 36 36 38 38 38	36 37 37 37 39 39 39	37 38 38 38 40 40 40	38 3 39 4 39 4 39 4 41 4 41 4 41 4	9 4 0 4 0 4 0 4 2 4 2 4 2 4	11 42 11 42 11 42 11 42 13 44 13 44 13 44	42 1s 2 43 2 43 2 43 4 45 4 45	Cm 44 44 46 46	1 Is 1 45 4 47 4 47 4	2 3 Cm 1 46 4 48 4 48 4	8 4 2 2 7 48 9 50 9 50 9 50	5 3 49 51 51 51	6 4 50 52 52	7 8 5 6 51 52 53 54 53 54	9 7 53 55 55 55	10 8 54 56 56	11 9 55 57 57 57 57	12 1 10 1 56 5 58 5 58 5 58 5	13 11 57 5 59 (59 (59 (5 8 5 60 6 60 6	9 6 1 6 1 6	0 6 2 6 2 6 2 6	16 36 36	2 I 4 6 4 6	s Cr 5 60 5 60	n 1 6 67 6 67	68 68	69 69	70 70 70	Is Is	Cm	12	3
26 28 28 28 28	27 27 29 29 29 29	28 28 30 30 30	29 29 29 31 31 31 31	29 30 30 30 32 32 32 32	30 3 31 3 31 3 31 3 33 3 33 3 33 3 33 3 33 3 33 3 33 3	1 32 2 33 2 33 2 33 4 35 4 35 4 35 4 35 4 35 4 35	33 34 34 34 36 36 36 36	34 35 35 35 37 37 37 37	35 36 36 38 38 38 38 38	36 37 37 37 39 39 39 39	38 38 38 40 40 40 40	38 3 39 4 39 4 39 4 41 4 41 4 41 4 41 4	9 4 0 4 0 4 2 4 2 4 2 4 2 4	11 42 11 42 11 42 11 42 13 44 13 44 13 44	2 Is 2 43 2 43 4 45 4 45 4 45 4 45 4 45	Cm 44 44 46 46 46 46	1 IS 45 47 47 47 47	2 3 Cm 1 46 4 48 4 48 4 48 4	3 4 1 2 7 48 9 50 9 50 9 50 9 50 9 50 9 50	5 3 49 51 51 51	6 4 50 52 52 52 52	7 8 5 6 51 52 53 54 53 54 53 54 53 54 53 54	9 7 53 55 55 55 55	10 8 54 56 56 56	11 9 55 57 57 57 57 57	12 1 10 1 56 5 58 5 58 5 58 5 58 5 58 5	13 11 57 5 59 (59 (59 (58 5 60 6 60 6	9 6 1 6 1 6 1 6	0 6 2 6 2 6 2 6 2 6	1 6 3 6 3 6 3 6	2 1 4 6 4 6 4 6	s Cr 5 60 5 60 5 60	n 1 667 667 667 667	68 68 68	69 69 69	70 70 70 70	Is Is Ds	Cm Is	12	3
28 28 28 28 28 28 27	27 27 29 29 29 29 29 28	28 28 30 30 30 30 29	28 29 29 31 31 31 31 31 31	29 30 30 30 32 32 32 32 32 32	30 3 31 3 31 3 31 3 33 3 33 3 33 3 33 3 33 3 33 3 33 3 33 3 32 3	1 32 2 33 2 33 2 33 4 35 4 35 4 35 4 35 4 35 3 34	33 34 34 36 36 36 36 35	34 35 35 37 37 37 37 37 36	35 36 36 38 38 38 38 38 38 38	36 37 37 37 39 39 39 39 39 39	38 38 38 38 40 40 40 40 39	38 3 39 4 39 4 39 4 41 4 41 4 41 4 41 4 41 4 41 4 41 4 41 4 41 4	9 4 0 4 0 4 2 4 2 4 2 4 1 4	1 4.1 1 4.2 1 4.2 1 4.2 1 4.2 1.3 4.4 4.3 4.4 4.3 4.4 4.3 4.4 4.3 4.4 4.3 4.4 4.3 4.4	42 15 2 43 2 43 4 45 4 45 4 45 4 45 3 44	Cm 44 44 46 46 46 45	1 IS 45 47 47 47 47 47 47 47 47 47 47	2 3 Cm 1 46 4 48 4 48 4 48 4 48 4 48 4	3 4 1 2 7 48 9 50 9 50 9 50 9 50 9 50 9 50 9 50 9 50 9 50 9 50 9 50	5 3 49 51 51 51 51 51 51 51	6 4 50 52 52 52 52 52	7 8 5 6 51 52 53 54 53 54 53 54 53 54 53 54 53 54 53 54 53 54 53 54 53 54 52 53	9 7 53 55 55 55 55 55	10 8 54 56 56 56 56 55	11 9 55 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57	12 1 10 1 56 5 58 5 58 5 58 5 58 5 58 5 58 5 58 5 58 5 58 5	13 57 59 6 59 6 59 6 59 6 59 6 59 6 59 6 5	58 5 60 6 60 6 60 6	9 6 1 6 1 6 1 6 1 6	9 6 2 6 2 6 2 6 1 6	1 6 3 6 3 6 3 6 3 6 2 6	2 I 4 6 4 6 4 6 3 6	s Cr 5 60 5 60 5 60	n 1 5 67 5 67 5 67 5 67 5 66	68 68 68 68 68	69 69 69 69	70 70 70 70 69	IS IS DS DS	Cm Is Is	12	3
28 28 28 28 28 28 27 27	27 27 29 29 29 29 29 28 28	28 28 30 30 30 30 29 29	28 29 29 31 31 31 31 31 30 30	29 30 30 30 32 32 32 32 31 31	30 3 31 3 31 3 33 3 33 3 33 3 33 3 33 3 33 3 33 3 32 3 32 3 32 3	1 32 2 33 2 33 2 33 2 33 4 35 4 35 4 35 4 35 3 34 3 34	33 34 34 36 36 36 36 35 35	34 35 35 37 37 37 37 37 36 36	35 36 36 38 38 38 38 38 38 38 37 37	36 37 37 37 39 39 39 39 39 38 38	38 38 38 40 40 40 39 39	38 3 39 4 39 4 39 4 41 4 41 4 41 4 41 4 41 4 41 4 41 4 41 4 41 4 41 4 41 4 40 4	9 4 0 4 0 4 2 4 2 4 2 4 1 4 1 4	I I <thi< th=""> <thi< th=""> <thi< th=""> <thi< th=""></thi<></thi<></thi<></thi<>	42 1 2 3 4	Cm 44 46 46 46 46 45 45	1 IS 45 47 47 47 47 47 46 46	2 3 Cm 1 46 4 48 4 48 4 48 4 48 4 48 4 47 4	3 4 2 2 7 48 9 50 9 50 9 50 9 50 9 50 9 50 9 50 9 50 8 49 8 49	5 3 49 51 51 51 51 51 50 50	6 4 50 52 52 52 52 51 51	7 8 5 6 51 52 53 54 53 54 53 54 53 54 53 54 53 54 53 54 53 54 52 53 52 53	9 7 53 55 55 55 55 55 54	10 8 54 56 56 56 55 55	11 9 55 57 57 57 57 57 57 56 56	12 1 10 1 56 5 58 5 58 5 58 5 58 5 58 5 57 5 57 5	13 1 57 59 69 69 69 69 69 69 69 69 69 69 639 639 639 639 639 639 639 639 639 638 538	58 5 60 6 60 6 60 6 60 6 59 6	9 6 1 6 1 6 1 6 1 6 1 6	0 6 2 6 2 6 2 6 1 6 1 6	1 6 3 6 3 6 3 6 2 6 2 6	2 I 4 6 4 6 4 6 3 6	s Cr 5 60 5 60 5 60 4 65	n 1 5 67 5 67 5 67 5 66	68 68 68 68 67 67	69 69 69 69 68 68	70 70 70 70 69	Is Is Ds Ds	Cm Is Is	1 2 2 Is	3
28 28 28 28 27 27 27	27 27 29 29 29 29 29 28 28 28 28	28 28 30 30 30 29 29 29	28 29 29 31 31 31 31 31 30 30 30	29 30 30 32 32 32 32 32 31 31 31	30 3 31 3 31 3 31 3 33 3 33 3 33 3 33 3 33 3 33 3 33 3 32 3 32 3 32 3 32 3 32 3 32 3 32 3 32 3	1 32 2 33 2 33 2 33 4 35 4 35 4 35 4 35 4 35 3 34 3 34 3 34 3 34	33 34 34 36 36 36 36 35 35 35 35	34 35 35 37 37 37 37 37 36 36 36	35 36 36 38 38 38 38 38 38 38 37 37	36 37 37 39 39 39 39 39 39 38 38 38	38 38 38 40 40 40 39 39	38 3 39 4 39 4 39 4 39 4 41 4 41 4 41 4 41 4 41 4 41 4 41 4 41 4 41 4 41 4 40 4 40 4	9 4 0 4 0 4 2 4 2 4 2 4 1 4 1 4 1 4	I I <thi< th=""> <thi< th=""> <thi< th=""> <thi< th=""></thi<></thi<></thi<></thi<>	42 1s 2 1s 2 43 2 43 4 45 4 45 4 45 3 44 3 44 3 44	Cm 44 46 46 46 46 45 45 45	1 IS 45 47 47 47 46 46 46	2 3 Cm 1 16 4 18 4 18 4 18 4 18 4 18 4 17 4 17 4 147 4	3 4 2 2 7 48 9 50 9 50 9 50 9 50 9 50 9 50 9 50 9 50 8 49 8 49 8 49	5 3 49 51 51 51 51 50 50 50 50	6 4 50 52 52 52 52 51 51 51	7 8 5 6 51 52 53 54 53 54 53 54 53 54 53 54 53 54 53 54 53 54 52 53 52 53 52 53	9 7 53 55 55 55 55 54 54 54	10 8 54 56 56 56 55 55 55	11 9 55 57 57 57 57 57 57 56 56	12 1 10 1 56 5 58 5 58 5 58 5 58 5 57 5 57 5 57 5	13 57 59 59 59 59 59 59 58 58 58 58	58 5 60 6 60 6 60 6 59 6 59 6	9 6 1	0 6 2 6 2 6 2 6 1 6 1 6 1 6	1 6 3 6 3 6 3 6 2 6 2 6 2 6	2 1 4 6 4 6 4 6 3 6 3 6 3 6	s Cr 5 60 5 60 5 60 4 65 4 65	n 1 67 667 667 667 667 666 566 566	68 68 68 68 67 67 67	69 69 69 68 68 68	70 70 70 69 69	IS IS DS DS IS IS	Cm Is Is	1 2 2 Is	3
28 28 28 28 28 27 27 27 27	27 27 29 29 29 29 28 28 28 28 28 28	28 28 30 30 30 29 29 29 29	28 29 29 31 31 31 31 30 30 30 30 30	29 30 30 30 32 32 32 32 31 31 31 31	30 3 31 3 31 3 31 3 33 3 33 3 33 3 33 3 33 3 33 3 33 3 32 3 32 3 32 3 32 3 32 3 32 3 32 3 32 3	1 32 2 33 2 33 2 33 2 33 4 35 4 35 4 35 4 35 3 34 3 34 3 34 3 34 3 34 3 34	33 34 34 36 36 36 36 35 35 35 35	34 35 35 37 37 37 37 37 36 36 36 36	35 36 36 38 38 38 38 38 38 38 37 37 37	36 37 37 39 39 39 39 39 38 38 38 38	38 38 38 40 40 40 39 39 39	38 3 39 4 39 4 39 4 41 4 41 4 41 4 41 4 41 4 40 4 40 4 40 4 40 4	9 4 0 4 0 4 2 4 2 4 2 4 1 4 1 4 1 4	I I <thi< th=""> <thi< th=""> <thi< th=""> <thi< th=""></thi<></thi<></thi<></thi<>	42 1s 2 1s 2 43 2 43 4 45 4 45 4 45 4 45 3 44 3 44 3 44 3 44	Cm 44 46 46 46 46 45 45 45 45	1 15 45 47 47 47 47 46 46 46 46 46	2 3 100m 1 146 4 148 4 148 4 148 4 148 4 148 4 148 4 147 4 147 4 147 4 147 4 147 4	3 4 2 7 48 9 50 8 49 10 <th10< th=""> <</th10<>	5 3 49 51 51 51 51 50 50 50 50 50	6 4 50 52 52 52 51 51 51 51	7 8 5 6 51 52 53 54 53 54 53 54 53 54 53 54 53 54 53 54 52 53 52 53 52 53 52 53	9 7 53 55 55 55 55 54 54 54 54	10 8 54 56 56 56 55 55 55	11 9 55 57 57 57 57 56 56 56 56	12 1 10 1 56 5 58 5 58 5 58 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5	13 13 157 157 159 159 159 159 159 159 159 159 159 159 159 159 159 159 159 159 159 159 159 158 158 158	58 5 60 6 60 6 60 6 59 6 59 6 59 6	9 6 1	0 6 2 6 2 6 2 6 1 6 1 6 1 6 1 6	1 6 3 6 3 6 3 6 2 6 2 6 2 6 2 6	2 1 4 6 4 6 4 6 3 6 3 6 3 6 3 6	s Cr 5 60 5 60 5 60 5 60 4 65 4 65 4 65	n 1 5 67 5 67 5 67 5 66 5 66 5 66 5 66	68 68 68 67 67 67 67	69 69 69 68 68 68 68 68	70 70 70 69 69 69 69	Is Is Ds Ds Ds Is Is Ds	Cm Is I Is	1 2 2 Is	3
28 28 28 28 27 27 27 27 27 27	27 27 29 29 29 29 28 28 28 28 28 28 28	28 28 30 30 30 29 29 29 29 29 29	28 29 29 31 31 31 31 30 30 30 30 30	29 30 30 30 32 32 32 31 31 31 31 31	30 3 31 3 31 3 33 3 33 3 33 3 33 3 33 3 33 3 32 3 33 3 3	1 32 2 33 2 33 2 33 2 33 2 33 4 35 4 35 4 35 3 34 3 34 3 34 3 34 3 34 3 34 3 34 3 34	33 34 34 36 36 36 35 35 35 35 35 35	34 35 35 37 37 37 37 37 36 36 36 36 36 36	35 36 36 38 38 38 38 38 38 37 37 37 37 37	36 37 37 39 39 39 39 39 39 38 38 38 38 38	37 38 38 38 38 40 40 40 40 40 39 39 39 39 39 39	38 3 39 4 39 4 39 4 41 4 41 4 41 4 41 4 40 4 40 4 40 4 40 4 40 4 40 4	9 4 0 4 0 4 0 4 0 4 2 4 2 4 2 4 2 4 2 4 1 4 1 4 1 4 1 4	I I <thi< th=""> <thi< th=""> <thi< th=""> <thi< th=""></thi<></thi<></thi<></thi<>	2 1s 2 43 2 43 4 45 4 45 4 45 3 44 3 44 3 44 3 44 3 44 3 44	Cm 44 46 46 46 46 46 45 45 45 45 45 45	1 15 45 47 47 47 47 46 46 46 46 46 46 46 46 46 46	2 3 Cm 1 46 4 48 4 48 4 48 4 48 4 47 4 47 4 47 4 47 4	3 4 2 7 48 9 50 9 50 9 50 9 50 9 50 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49	5 3 49 51 51 51 51 50 50 50 50 50 50	6 50 52 52 52 51 51 51 51 51	7 8 5 6 51 52 53 54 53 54 53 54 53 54 53 54 53 54 53 54 52 53 52 53 52 53 52 53 52 53 52 53 52 53	9 7 53 55 55 55 55 54 54 54 54 54 54	10 8 54 56 56 56 55 55 55 55 55	11 9 55 57 57 57 57 56 56 56 56 56 56 56 56 56	12 1 10 1 56 5 58 5 58 5 58 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5	13 11 11 15 17 18 19 19 10 11 11 11 11 11 11 11 11 11 12 13 14 15 15 16 17 18 19 10 10 11 11 11 11 17 18 18 19 10 10 11 11 11 11 11 10 11 11 12 13 14 15 15	58 5 60 6 60 6 60 6 60 6 59 6 59 6 59 6 59 6	9 6 1 6	0 6 2 6 2 6 2 6 1 6 1 6 1 6 1 6 1 6	1 6 3 6 3 6 3 6 2 6 2 6 2 6 2 6 2 6	2 I 4 6 4 6 4 6 3 6 3 6 3 6 3 6 3 6	s Cr 5 60 5 60 5 60 4 65 4 65 4 65 4 65	n 1 5 67 5 67 5 66 5 66 5 66 5 66 5 66	68 68 68 67 67 67 67 67	69 69 69 68 68 68 68 68 68	70 70 70 69 69 69 69 69	Is Is Ds Ds Is Is Ds 70	Cm Is Is Is Is Is	1 2 2 Is	3
28 28 28 28 28 27 27 27 27 27 27 27	27 29 29 29 28 28 28 28 28 28 28 28 28 28	28 28 30 30 30 29 29 29 29 29 29 29	28 29 29 31 31 31 30 30 30 30 30 30 30	29 30 30 30 32 32 32 32 31 31 31 31 31 31 31	30 3 31 3 31 3 31 3 33 3 33 3 33 3 33 3 33 3 33 3 34 3 35 3 32 3 32 3 32 3 32 3 32 3 32 3 32 3 32 3	1 32 33 33 2 33 2 33 2 33 2 33 4 35 4 35 4 35 3 34 3 34 3 34 3 34 3 34	33 34 34 36 36 36 35 35 35 35 35 35 35	34 35 35 37 37 37 37 36 36 36 36 36 36	35 36 36 38 38 38 37 37 37 37 37 37 37 37 37 37 37 37 37	36 37 37 37 39 39 39 39 39 39 39 39 38 38 38 38 38 38 38 38	37 38 38 38 40 40 40 40 40 39 39 39 39 39 39	38 3 39 4 39 4 39 4 41 4 41 4 41 4 40 4 40 4 40 4 40 4 40 4 40 4 40 4 40 4 40 4 40 4 40 4 40 4 40 4 40 4	9 4 0 4 0 4 0 4 0 4 0 4 2 4 2 4 2 4 2 4 1 4 1 4 1 4 1 4 1 4	I I <thi< th=""> <thi< th=""> <thi< th=""> <thi< th=""></thi<></thi<></thi<></thi<>	42 15 2 43 2 43 2 43 4 45 4 45 4 45 3 44 3 44 3 44 3 44 3 44 3 44 3 44 3 44 3 44 3 44 3 44	Cm 44 46 46 46 46 45 45 45 45 45 45	1 45 47 47 47 47 46 46 46 46 46 46 46 46 46 46	2 3 Cm 1 46 4 48 4 48 4 48 4 48 4 48 4 47 4 47 4 47 4 47 4 47 4 47 4	3 4 2 7 48 9 50 9 50 9 50 9 50 9 50 9 50 9 50 9 50 9 50 9 50 9 50 9 50 9 50 9 50 9 50 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49	5 3 49 51 51 51 51 50 50 50 50 50 50 50 50	6 50 52 52 52 51 51 51 51 51 51 51	7 8 5 6 51 52 53 54 53 54 53 54 52 53 52 53 52 53 52 53 52 53 52 53 52 53 52 53 52 53 52 53 52 53 52 53	9 7 53 55 55 55 54 54 54 54 54 54	10 8 54 56 56 55 55 55 55 55 55	11 9 55 57 57 57 57 56 56 56 56 56 56 56 56 56 56 56 56 56 56 56 56 56 56	12 1 10 1 56 5 58 5 58 5 58 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5	13 11 57 58 59	58 5 60 6 60 6 60 6 60 6 60 6 60 6 60 6 60	9 6 11 6 11 6 11 6 11 6 10 6 10 6 10 6 10	0 6 2 6 2 6 2 6 2 6 1 6 1 6 1 6 1 6 1 6 1 6	1 6 3 6 3 6 3 6 3 6 2 6 2 6 2 6 2 6 2 6 2 6 2 6 2 6	2 I 4 6 4 6 4 6 3 6 3 6 3 6 3 6 3 6 3 6	S Cr 5 60 5 60 5 60 6 60 4 65 4 65 4 65 4 65 4 65 4 65 4 65	n 1 5 67 5 67 5 66 5 66 5 66 5 66 5 66	68 68 68 67 67 67 67 67 67 67	69 69 69 68 68 68 68 68 68 68	70 70 70 69 69 69 69 69 69	Is Is Ds Ds Is Ss Is 70	Cm Is Is Is Is Is Is	1 2 2 Is	3
28 28 28 28 28 28 27 27 27 27 27 27 27 27 27	27 27 29 29 29 29 28 28 28 28 28 28 28 28 28 28 28	28 28 30 30 30 29 29 29 29 29 29 29	29 29 29 31 31 31 30 30 30 30 30 30 30	29 30 30 30 32 32 32 32 31 31 31 31 31 31 31 31	30 3 31 3 31 3 31 3 33 3 33 3 33 3 33 3 33 3 33 3 32 3 33 3 3 33 3 <	1 32 33 2 33 32 33 2 33 34 35 4 35 34 35 3 344 35 34 3 34 34 34 3 34 34 34 3 34 34 34 3 34 34 34 3 34 34 34 3 34 34 34	33 34 34 36 36 36 36 35 35 35 35 35 35 35 35 35 35 35 35	34 35 35 37 37 37 37 36 36 36 36 36 36 36 36	35 36 36 38 38 38 38 38 38 37 37 37 37 37 37 37 37	36 37 37 39 39 39 39 39 38 38 38 38 38 38 38 38	37 38 38 38 38 40 40 40 40 39 39 39 39 39 39 39 39	38 3 39 4 39 4 39 4 39 4 41 4 41 4 41 4 41 4 41 4 40 4 40 4 40 4 40 4 40 4 40 4 40 4 40 4 40 4 40 4 40 4	9 4 0 4 0 4 2 4 2 4 2 4 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1 4	4. 4. 11 4. 11 4. 11 4. 13 4. 13 4. 13 4. 13 4. 13 4. 13 4. 13 4. 13 4. 13 4. 13 4. 13 4. 13 4. 14 4. 15 4. 16 4. 17 4. 18 4. 19 4. 10 4. 11 4. 12 4. 12 4. 12 4. 12 4.	1 12 2 Is 2 43 2 43 4 45 4 45 4 45 3 44 3 44 3 44 3 44 3 44 3 44 3 44 3 44 3 44 3 44 3 44 3 44	Cm 44 46 46 46 46 45 45 45 45 45 45 45 45	1 IS 45 47 47 47 47 47 47 46 46 46 46 46 46 46 46 46	2 3 Cm 1 446 4 48 4 488 4 488 4 488 4 418 4 418 4 417 4 417 4 417 4 417 4 417 4 417 4 417 4 417 4 417 4	a 4 2 7 48 9 50 9 50 9 50 9 50 9 50 9 50 9 50 9 50 9 50 9 50 9 50 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49	5 3 49 51 51 51 51 50 50 50 50 50 50 50 50	6 4 50 52 52 52 51 51 51 51 51 51 51 51	7 8 5 6 53 54 53 54 53 54 53 54 52 53 52 53 52 53 52 53 52 53 52 53 52 53 52 53 52 53 52 53 52 53 52 53 52 53	9 7 55 55 55 55 55 54 54 54 54 54 54 54 54	10 8 54 56 56 56 55 55 55 55 55 55 55 55 55 55 55	11 9 555 57 57 57 56 56 56 56 56 56 56 56 56 56 56 56 56 56	12 1 10 1 10 1 56 5 58 5 58 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5	13 11 11 1577 15577 1559 1559 1559 1559 1559 1559 1559 1559 1558 1558 1558 1558 1558 1558 1558	58 5 60 6	9 6 1 6 1 6 1 6 1 6 0 6 0 6 0 6 0 6	0 6 2 6 2 6 2 6 1 6 1 6 1 6 1 6 1 6 1 6 1 6 1 6	1 6 3 6 3 6 3 6 3 6 3 6 2 6 2 6 2 6 2 6 2 6 2 6 2 6 2 6 2 6	2 I 4 6 4 6 4 6 4 6 3 6 3 6 3 6 3 6 3 6 3 6 3 6 3 6 3 6 3 6 3 6 3 6	S Cf 5 6 (5 6 (4 6) 4 6)	n 1 6 67 5 67 5 67 5 66 5 66 5 66 5 66 5 66 5 66 5 66	68 68 68 67 67 67 67 67 67 67 67	69 69 69 68 68 68 68 68 68 68 68 68	70 70 70 69 69 69 69 69 69 69	Is Is Is Ds Ds Is 70 70 70	Cm IS IS IS IS IS IS	1 2 2 Is	3
28 28 28 28 28 28 27 27 27 27 27 27 27 27 27 27	27 27 29 29 29 29 28 28 28 28 28 28 28 28 28 28 28	28 28 30 30 30 29 29 29 29 29 29 29 29	29 29 29 31 31 31 31 30 30 30 30 30 30 30 30 30 30 30 30 30	29 30 30 30 32 32 32 32 31 31 31 31 31 31 31 31 31	30 3 31 3 31 3 33 3 33 3 33 3 33 3 33 3 32 3 33 3 3 32 3 <	1 32 2 33 2 33 2 33 2 33 4 35 4 35 3 34 3 34 3 34 3 34 3 34 3 34 3 34 3 34 3 34 3 34 3 34 3 34 3 34	33 34 34 36 36 36 36 36 36 35 35 35 35 35 35 35 35	34 35 35 37 37 37 37 37 36 36 36 36 36 36 36 36 36 36	35 36 36 38 38 38 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37	36 37 37 39 39 39 39 39 39 39 38 38 38 38 38 38 38 38 38 38 38 38 38	37 38 38 38 38 40 40 40 40 40 39 39 39 39 39 39 39 39 39 39	33 33 4 339 4 339 4 339 4 4 4 4 41 4 4 4 4 41 4 4 4 4 40 4 4 4 4 40 4 <	9 4 0 4 0 4 2 4 2 4 2 4 1	4.0 4.0 1 4.1 4.1 4.1 11 4.1 13 4.4 13 4.4 13 4.4 13 4.4 13 4.4 13 4.4 13 4.4 13 4.4 13 4.4 13 4.4 13 4.4 13 4.4 13 4.4 13 4.4 13 4.4 13 4.4 14 4.1 15 4.1 16 4.1 17 4.1 18 4.1 19 4.1 10 4.1 11 4.1 12 4.1 13 4.1 14 4.1	1 1 2 Is 2 43 4 45 4 45 4 45 3 44 3 44 3 44 3 44 3 44 3 44 3 44 3 44	Cm 44 44 46 46 46 45 45 45 45 45 45 45 45 45 45 45 45 45	1 IS 1 45 4 47 4 47 4 47 4 47 4 47 4 46 4 46 4 46 4 46 4 46 4 46 4 46 4 46 4 46 4 46 4 46 4 46 4 46 4 46 4	2 3 Cm 1 46 4 48 4 48 4 48 4 48 4 48 4 47 4 477 4 477 4 477 4 477 4 477 4 417 4 417 4 417 4 417 4 417 4 417 4	a 4 2 2 7 48 9 50 9 50 9 50 9 50 9 50 9 50 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49 8 49	5 3 49 51 51 51 51 51 50 50 50 50 50 50 50 50 50	6 4 50 52 52 52 51 51 51 51 51 51 51 51 51 51	7 8 5 6 51 52 53 54 53 54 53 54 53 54 53 54 53 54 53 54 52 53 52 53 52 53 52 53 52 53 52 53 52 53 52 53 52 53 52 53 52 53 52 53	9 7 53 55 55 55 55 54 54 54 54 54 54 54 54	10 8 54 56 56 55 55 55 55 55 55 55 55 55 55 55 55 55 55	11 9 55 57 57 57 57 57 56 56 556 566 556 556 556 556 556 556 556 556 556	12 1 10 1 56 5 58 5 58 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5 57 5	13 11 11 157 559 6 559 6 558 558 558 558 558 558 558 558 558 558 558 558	58 5 60 6 60 6 60 6 60 6 53 6 53 6 53 6 53 6 53 6 53 6 53 6 53 6 53 6 53 6 53 6 53 6	9 6 1 6	0 6 2 6 2 6 2 6 1 6 1 6 1 6 1 6 1 6 1 6 1 6 1 6 1 6 1 6	1 6 3 6 3 6 3 6 2 6 2 6 2 6 2 6 2 6 2 6 2 6 2 6 2 6 2 6 2 6	2 1 4 6 4 6 4 6 4 6 3 6 3 6 3 6 3 6 3 6 3 6 3 6 3 6 3 6 3 6 3 6 3 6 3 6	S Cr 5 60 5 60 5 60 5 60 4 65 4 65 4 65 4 65 4 65 4 65 4 65 4 65 4 65 4 65	1 3 67 5 67 5 67 5 66 5 66 5 66 5 66 5 66 5 66 5 66 5 66 5 66 5 66 5 66 5 66 5 66	68 68 68 67 67 67 67 67 67 67 67 67	69 69 69 68 68 68 68 68 68 68 68 68	70 70 70 69 69 69 69 69 69 69	IS IS DS DS IS TS 70 70 70 70	Cm Is Is Is Is Ds Ds	1 2 2 Is 1	3

FAITHFULNESS OF THE SIMULATION

Comparing a real system and a simulation

⇒ Very similar result of number of mispredicted branches

⇒ Helped to implement the attack on a real system

Limitations

⇒ **Slow** simulation, possibly **inaccurate** models

CONCLUSION



PAPER

Reproducing Spectre Attack with gem5

How To Do It Right?

Pierre Ayoub pierre.ayoub@eurecom.fr EURECOM Sophia Antipolis, France

Pierre Ayoub and Clémentine Maurice. *Reproducing Spectre Attack with gem5: How To Do It Right?* (EuroSec '21), April 26, 2021

- GitHub: https://pierreay.github.io/reproduce-spectre-gem5/
- Contact: pierre.ayoub@eurecom.fr

Clémentine Maurice clementine.maurice@inria.fr Univ Lille, CNRS, Inria Lille, France