CS 577: Project Report

On

Compiler optimization for Constant time

Guided By-:
Prof. Chandan Karfa
(Assistant professor IIT Guwahati)

Mentor:
Priyanka Panigrahi
(PhD Computer Science, IIT Guwahati)

Group - 4

Group Members -

1. Ajay Gahlot 204101004
2. Anil Singh 204101007
3. Sarthak Agarwal 204101049
4. Mukesh Gandharva 204101034
5. Vivek Singh 204101061

Initially we started by observing the **x^k mod p** algorithm

```
r = 1;
for(int i=base-1;i>=0;i--)
{
        r = (r*r)%p;

        if ( (k>>i) & 1) r = (r*x)%p;
}
```

We get the following HLS results for above algo

Performance Estimates

Timing (ns)

Summary

Clock	Target	Estimated	Uncertainty
ap_clk	10.00	8.510	1.25

Latency (clock cycles)

Summary

Latency		Interval		
min	max	min	max	Type
381	741	381	741	none

Detail

Instance

Loop

Utilization Estimates

Summary

Name	BRAM_18K	DSP48E	FF	LUT	URAM
DSP	-	-	-	-	-
Expression	-	6	0	156	-
FIFO	-	-	-	-	-
Instance	-	-	788	476	-
Memory	-	-	-	-	-
Multiplexer	-	-	-	373	-
Register	-	-	209	-	-
Total	0	6	997	1005	0
Available	280	220	106400	53200	0
Utilization (%)	0	2	~0	1	0

In this above algorithm line with red color there is leakage
At each iteration r contains the value of x^(k/(2^i)) , each loop iteration squares r and if the bit at i is 1 then r is multiplied by x. If an attacker can measure the time taken by each iteration of the loop, it can distinguish between the iteration where the tested bit of k is 0 or 1.

We fix this leakage as given below

```
r = 1
for(int i = base - 1; 0 <= i; --i) {
        r = (r * r) % p;
        r1 = (r * x) % p;
        r = ((k >> i) & 1) ? r1 : r;
}
```

Performance Estimates

Timing (ns)

Summary

Clock	Target	Estimated	Uncertainty
ap_clk	10.00	8.555	1.25

Latency (clock cycles)

Summary

Latency		Interval		
min	max	min	max	Type
741	741	741	741	none

Detail

Instance

Loop

Utilization Estimates

Summary

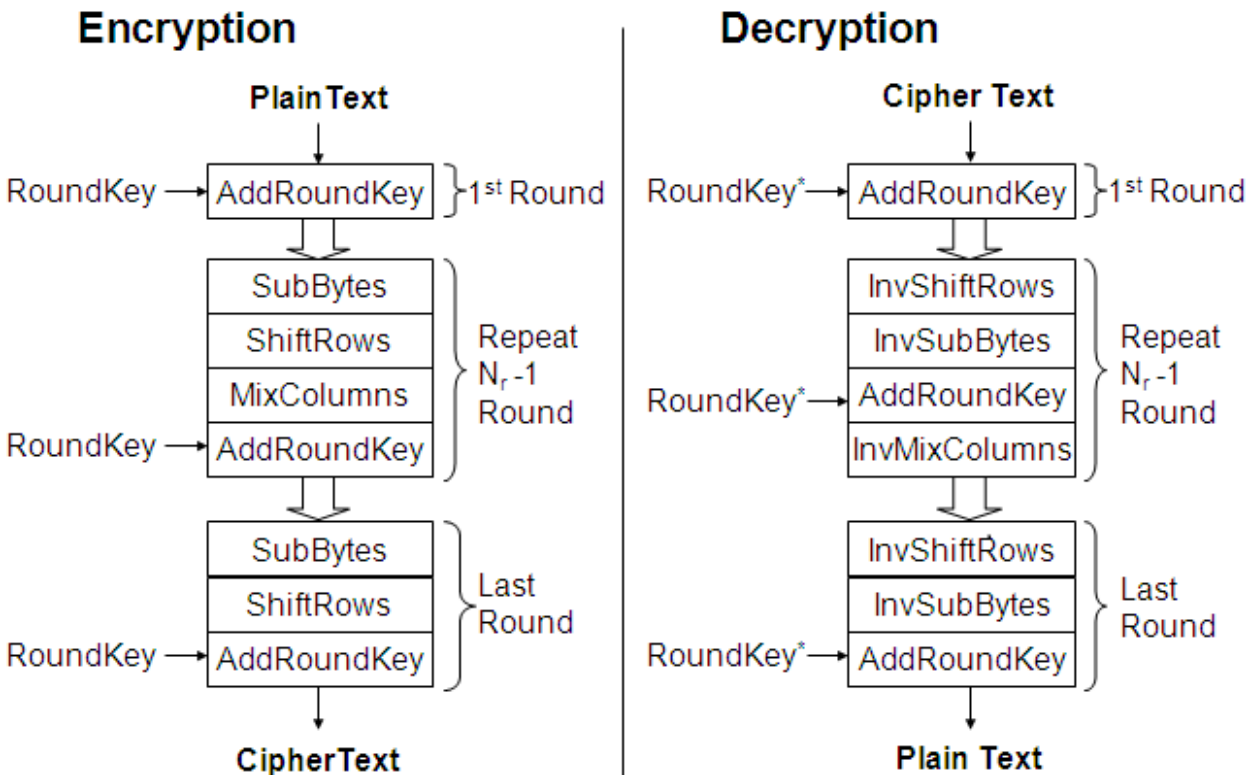
Name	BRAM_18K	DSP48E	FF	LUT	URAM
DSP	-	-	-	-	-
Expression	-	6	0	188	-
FIFO	-	-	-	-	-
Instance	-	-	788	476	-
Memory	-	-	-	-	-
Multiplexer	-	-	-	355	-
Register	-	-	213	-	-
Total	0	6	1001	1019	0
Available	280	220	106400	53200	0
Utilization (%)	0	2	~0	1	0

We have fixed the leakage now latency is the same for min and max which is required.

In in terms of resource requirement there is increase in constant time as compared to to without constant time.

Advanced Encryption standard (AES)

Flowchart for AES is as follows -



We have taken the benchmark of AES without applying any change we get following results -

Performance Estimates

Timing (ns)

Summary

Clock	Target	Estimated	Uncertainty
ap_clk	10.00	8.706	1.25

Latency (clock cycles)

Summary

Latency		Interval		
min	max	min	max	Type
2990	3150	2990	3150	none

Detail

- Instance
- Loop

Utilization Estimates

Summary

Name	BRAM_18K	DSP48E	FF	LUT	URAM
DSP	-	-	-	-	-
Expression	-	-	-	-	-
FIFO	-	-	-	-	-
Instance	9	-	2232	8485	0
Memory	4	-	0	0	0
Multiplexer	-	-	-	276	-
Register	-	-	38	-	-
Total	13	0	2270	8761	0
Available	280	220	106400	53200	0
Utilization (%)	4	0	2	16	0

There were many statements in code where there can be leakage we make change in those statements so that it become constant time

Constant time

After making AES constant time we get the following results -

Performance Estimates

Timing (ns)

Summary

Clock	Target	Estimated	Uncertainty
ap_clk	10.00	8.706	1.25

Latency (clock cycles)

Summary

Latency		Interval		
min	max	min	max	Type
3070	3070	3070	3070	none

Detail

Instance

Loop

Utilization Estimates

Summary

Name	BRAM_18K	DSP48E	FF	LUT	URAM
DSP	-	-	-	-	-
Expression	-	-	-	-	-
FIFO	-	-	-	-	-
Instance	9	-	2190	8585	0
Memory	4	-	0	0	0
Multiplexer	-	-	-	276	-
Register	-	-	38	-	-
Total	13	0	2228	8861	0
Available	280	220	106400	53200	0
Utilization (%)	4	0	2	16	0

C/RTL Cosimulation

Cosimulation Report for 'aes_main'

Result

		Latency			Interval		
RTL	Status	min	avg	max	min	avg	max
VHDL	NA	NA	NA	NA	NA	NA	NA
Verilog	Pass	3070	3070	3070	3071	3071	3071

Export the report(.html) using the Export Wizard

After applying constant time we were able to achieve constant latency (i.e min and max latency is equal to 3070)
For all the test cases we were getting correct results.
As we can see in the figure there is an increase in resources(area) when we make the program constant time which is expected since we need more operators and variables.
.

Optimization

we have apply optimization on constant time code of AES

We started by using **loop unrolling**

Partial Loop Unrolling (factor = 2)

Performance Estimates

Timing (ns)

Summary

Clock	Target	Estimated	Uncertainty
ap_clk	10.00	8.706	1.25

Latency (clock cycles)

Summary

Latency		Interval		
min	max	min	max	Type
2372	2372	2372	2372	none

Detail

Instance

Loop

Utilization Estimates

Summary

Name	BRAM_18K	DSP48E	FF	LUT	URAM
DSP	-	-	-	-	-
Expression	-	-	-	-	-
FIFO	-	-	-	-	-
Instance	9	-	2898	12280	0
Memory	4	-	0	0	0
Multiplexer	-	-	-	306	-
Register	-	-	38	-	-
Total	13	0	2936	12586	0
Available	280	220	106400	53200	0
Utilization (%)	4	0	2	23	0

Complete Loop Unrolling

Performance Estimates

Timing (ns)

Summary

Clock	Target	Estimated	Uncertainty
ap_clk	10.00	8.706	1.25

Latency (clock cycles)

Summary

Latency		Interval		
min	max	min	max	Type
1809	1809	1809	1809	none

Detail

- Instance
- Loop

Utilization Estimates

Summary

Name	BRAM_18K	DSP48E	FF	LUT	URAM
DSP	-	-	-	-	-
Expression	-	-	-	-	-
FIFO	-	-	-	-	-
Instance	9	-	3124	13414	0
Memory	4	-	0	0	0
Multiplexer				306	
Register	-	-	38	-	-
Total	13	0	3162	13720	0
Available	280	220	106400	53200	0
Utilization (%)	4	0	2	25	0

Array Partition + Loop Unrolling

We have used cyclic array partition with factor = 2

Performance Estimates

Timing (ns)

Summary

Clock	Target	Estimated	Uncertainty
ap_clk	10.00	8.706	1.25

Latency (clock cycles)

Summary

Latency		Interval		
min	max	min	max	Type
1501	1501	1501	1501	none

Detail

Instance

Loop

Utilization Estimates

Summary

Name	BRAM_18K	DSP48E	FF	LUT	URAM
DSP	-	-	-	-	-
Expression	-	-	-	-	-
FIFO	-	-	-	-	-
Instance	10	-	3003	13720	0
Memory	6	-	0	0	0
Multiplexer	-	-	-	426	-
Register	-	-	38	-	-
Total	16	0	3041	14146	0
Available	280	220	106400	53200	0
Utilization (%)	5	0	2	26	0

Array Partition + Loop Unrolling + Pipelining

Performance Estimates

Timing (ns)

Summary

Clock	Target	Estimated	Uncertainty
ap_clk	10.00	9.279	1.25

Latency (clock cycles)

Summary

Latency		Interval		
min	max	min	max	Type
1252	1252	1252	1252	none

Detail

- Instance
- Loop

Utilization Estimates

Summary

Name	BRAM_18K	DSP48E	FF	LUT	URAM
DSP	-	-	-	-	-
Expression	-	-	-	-	-
FIFO	-	-	-	-	-
Instance	13	-	6920	22791	0
Memory	6	-	0	0	0
Multiplexer	-	-	-	435	-
Register	-	-	38	-	-
Total	19	0	6958	23226	0
Available	280	220	106400	53200	0
Utilization (%)	6	0	6	43	0

As we can see as we decrease the latency the area increases since there is tradeoff b/w area and latency.
And here latency is constant after applying the optimizations.