Privacy-Preserving Manner Using Homomorphic Encryption

Begüm TÜZÜN 2597821

What is Homomorphic Encryption

Homomorphic encryption allows you to analyze or manipulate encrypted data without disclosing it to anyone.

Selected Graph Algorithm:

All Paths From A Given Source to A Destination

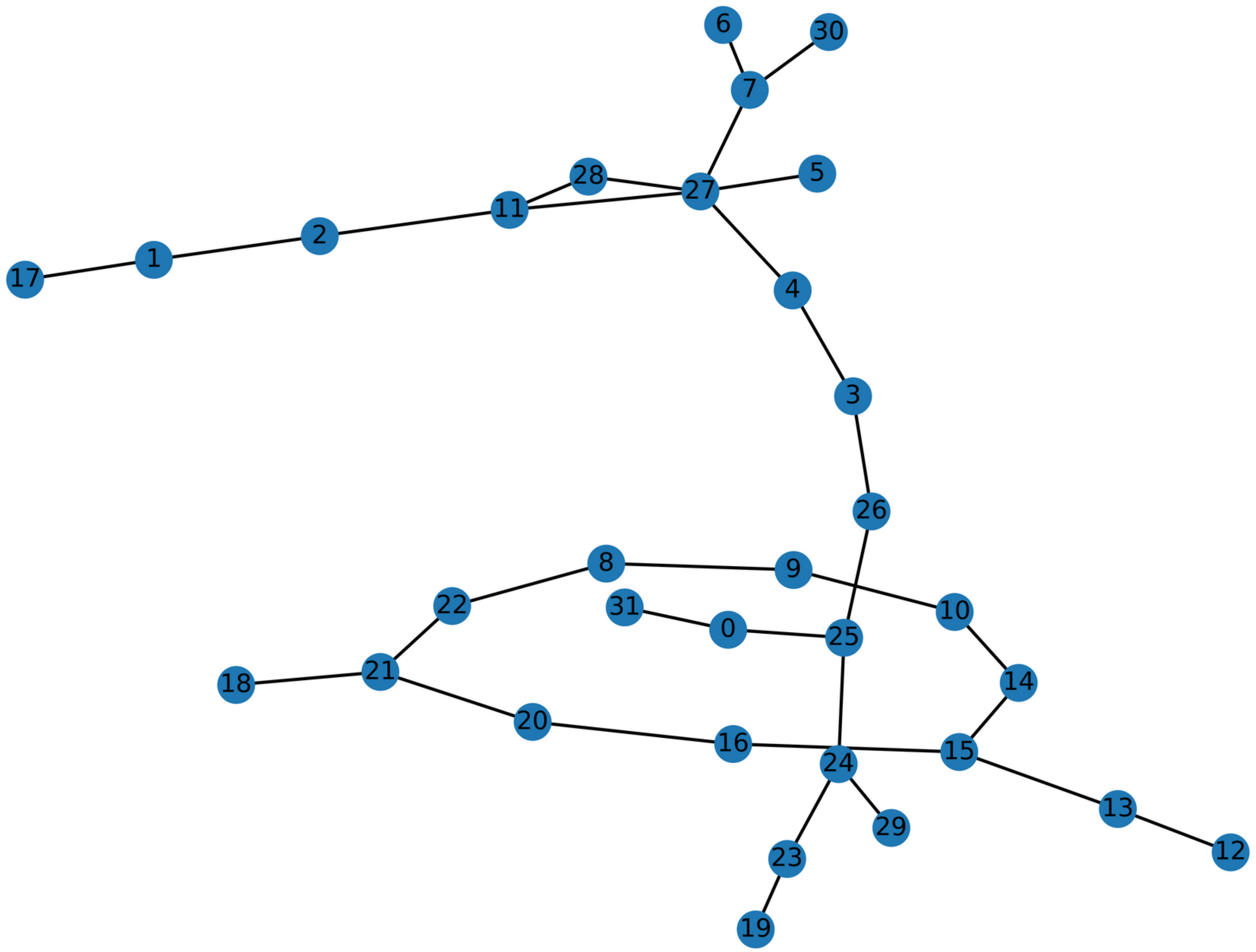
This algorithm finds all paths from the source node to the destination node by checking
every single connection with nodes.

Microsoft EVA

EVA is a homomorphic
encryption compiler that
automates the parts that require
cryptographic
expertise.

Implementation

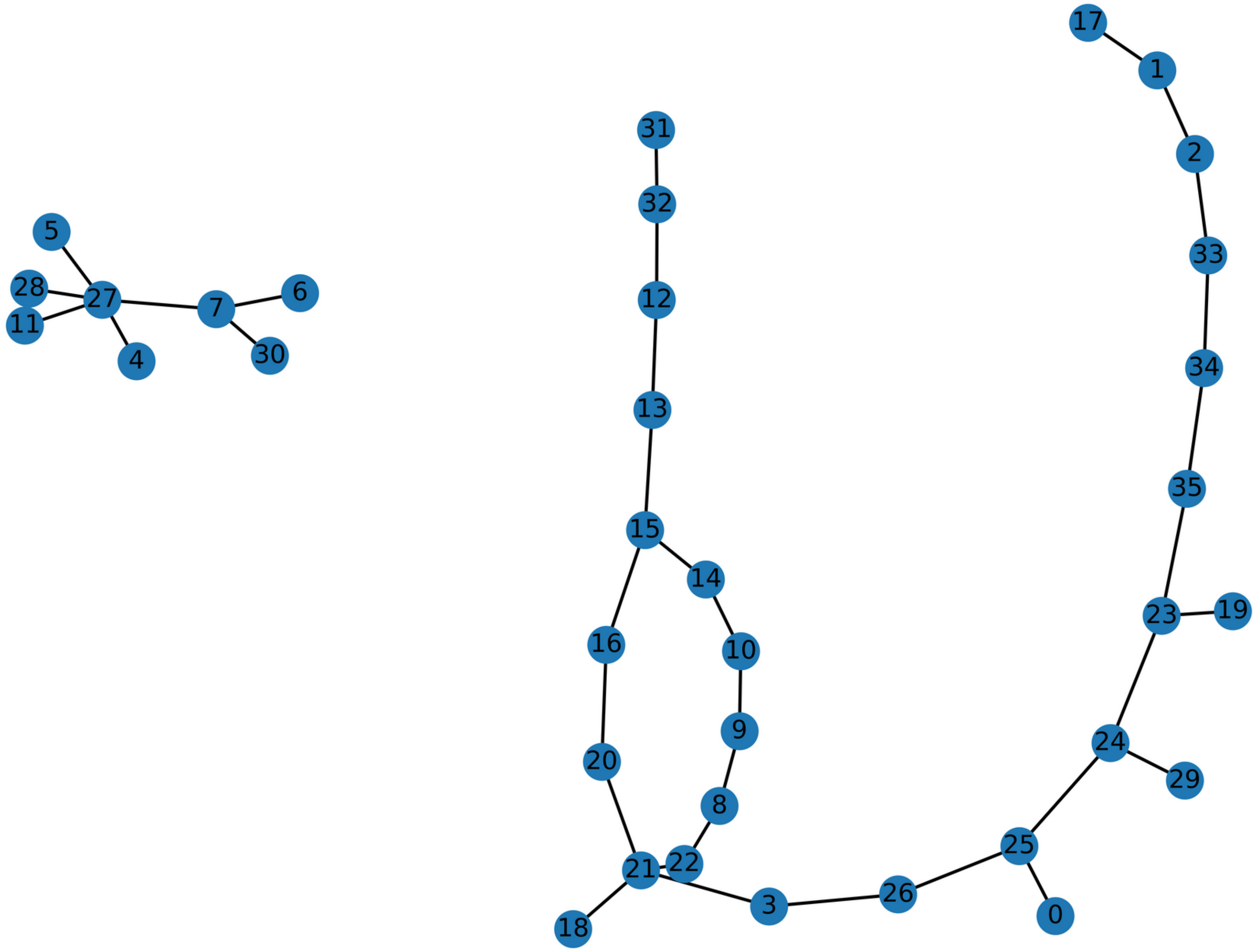
I printed all paths with a loop from source node value to destination node value by increasing 1 the source node value.



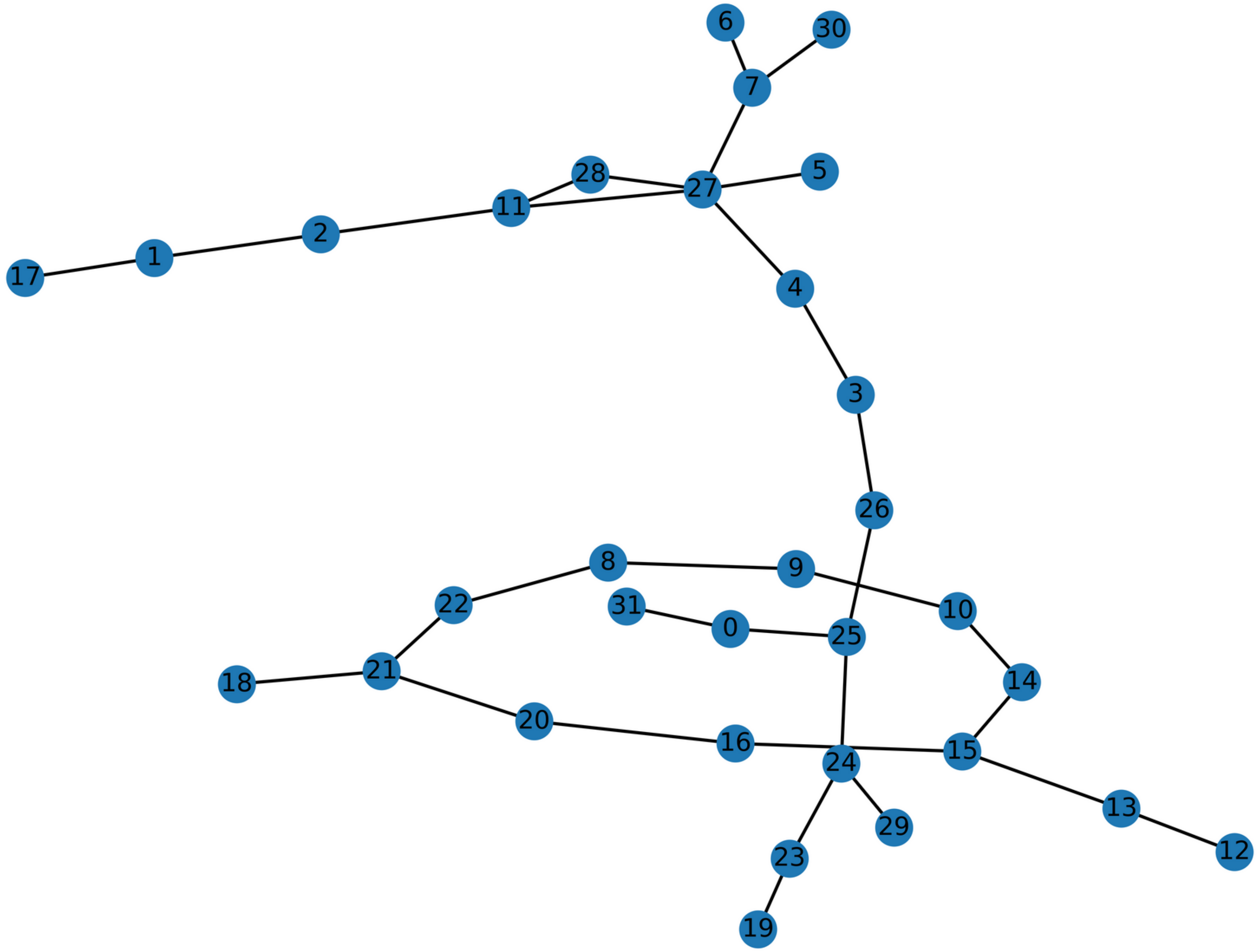
Creation of Nodes and Graphs

NetworkX was used to create a random graph.

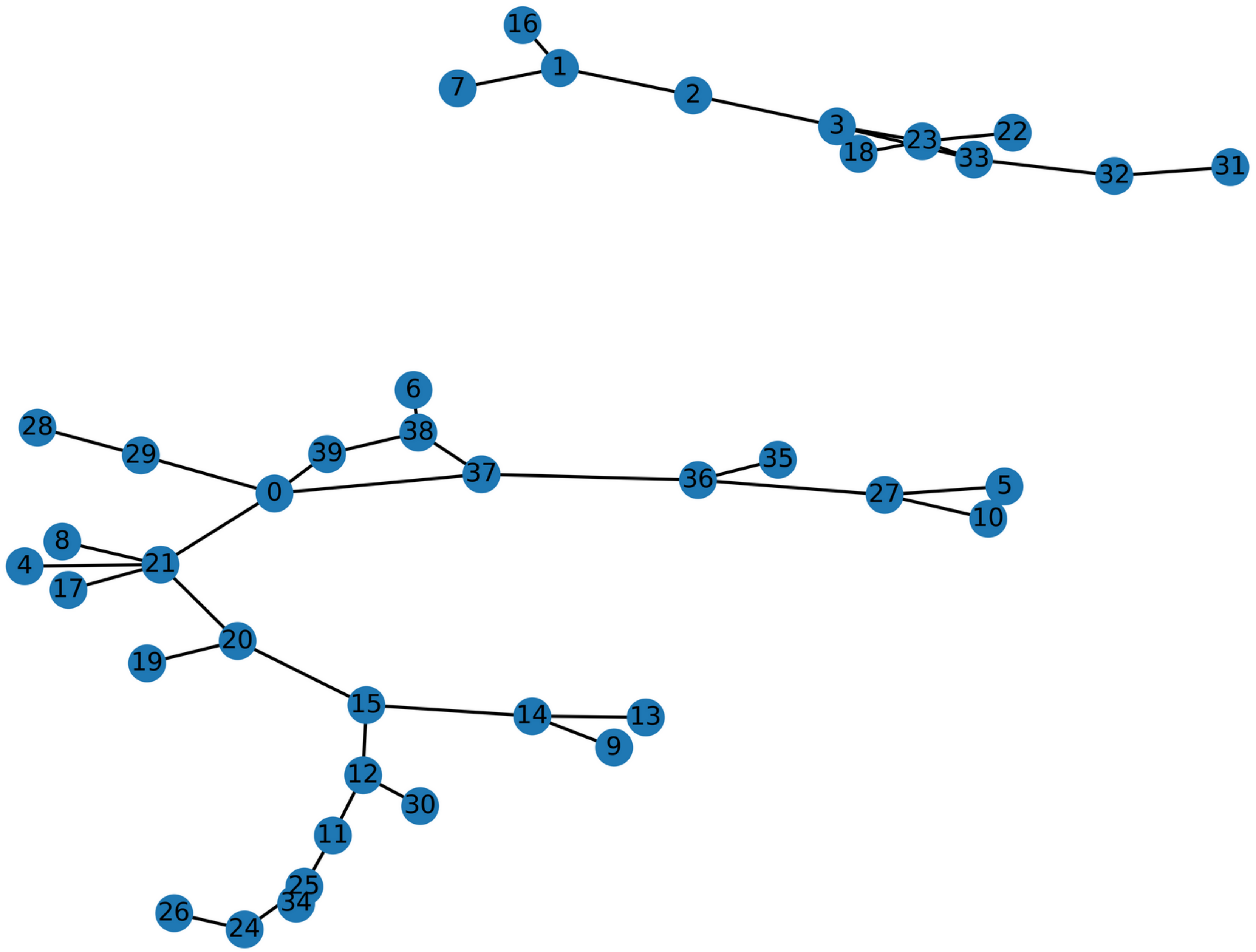
Diffferent graph structures



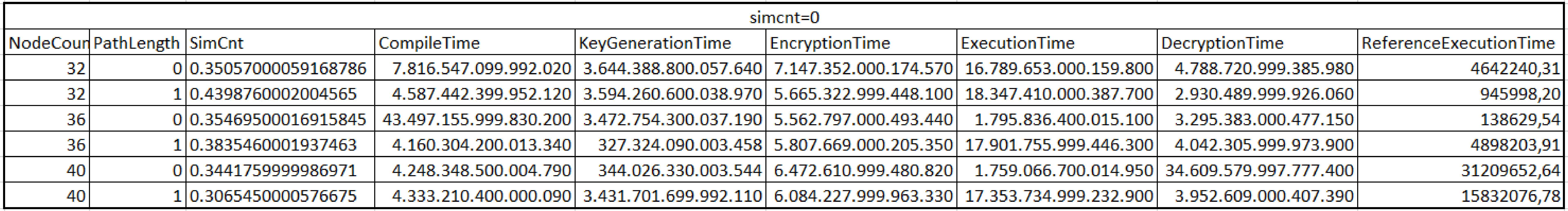
Diffferent graph structures



Diffferent graph structures

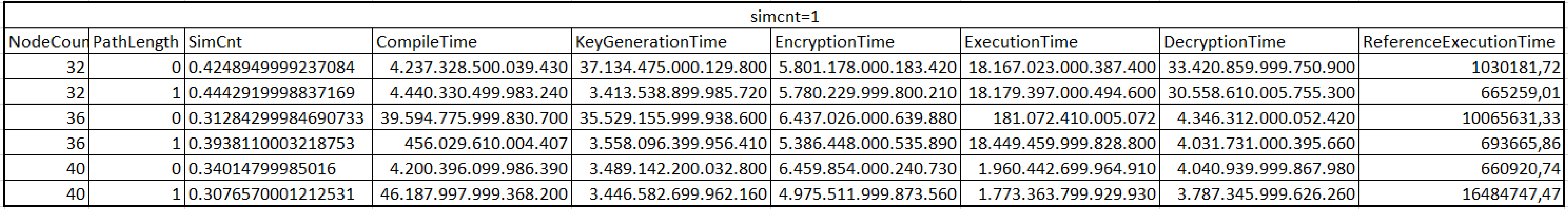


Implementation Findings



simcnt=0								
NodeCoun	PathLength	SimCnt	CompileTime	KeyGenerationTime	EncryptionTime	ExecutionTime	DecryptionTime	ReferenceExecutionTime
32	0	0.35057000059168786	7.816.547.099.992.020	3.644.388.800.057.640	7.147.352.000.174.570	16.789.653.000.159.800	4.788.720.999.385.980	4642240,31
32	1	0.4398760002004565	4.587.442.399.952.120	3.594.260.600.038.970	5.665.322.999.448.100	18.347.410.000.387.700	2.930.489.999.926.060	945998,20
36	0	0.35469500016915845	43.497.155.999.830.200	3.472.754.300.037.190	5.562.797.000.493.440	1.795.836.400.015.100	3.295.383.000.477.150	138629,54
36	1	0.3835460001937463	4.160.304.200.013.340	327.324.090.003.458	5.807.669.000.205.350	17.901.755.999.446.300	4.042.305.999.973.900	4898203,91
40	0	0.3441759999986971	4.248.348.500.004.790	344.026.330.003.544	6.472.610.999.480.820	1.759.066.700.014.950	34.609.579.997.777.400	31209652,64
40	1	0.3065450000576675	4.333.210.400.000.090	3.431.701.699.992.110	6.084.227.999.963.330	17.353.734.999.232.900	3.952.609.000.407.390	15832076,78

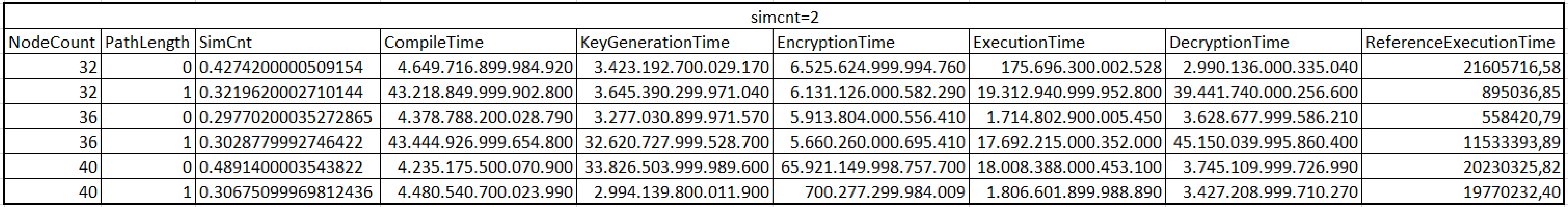
Implementation Findings



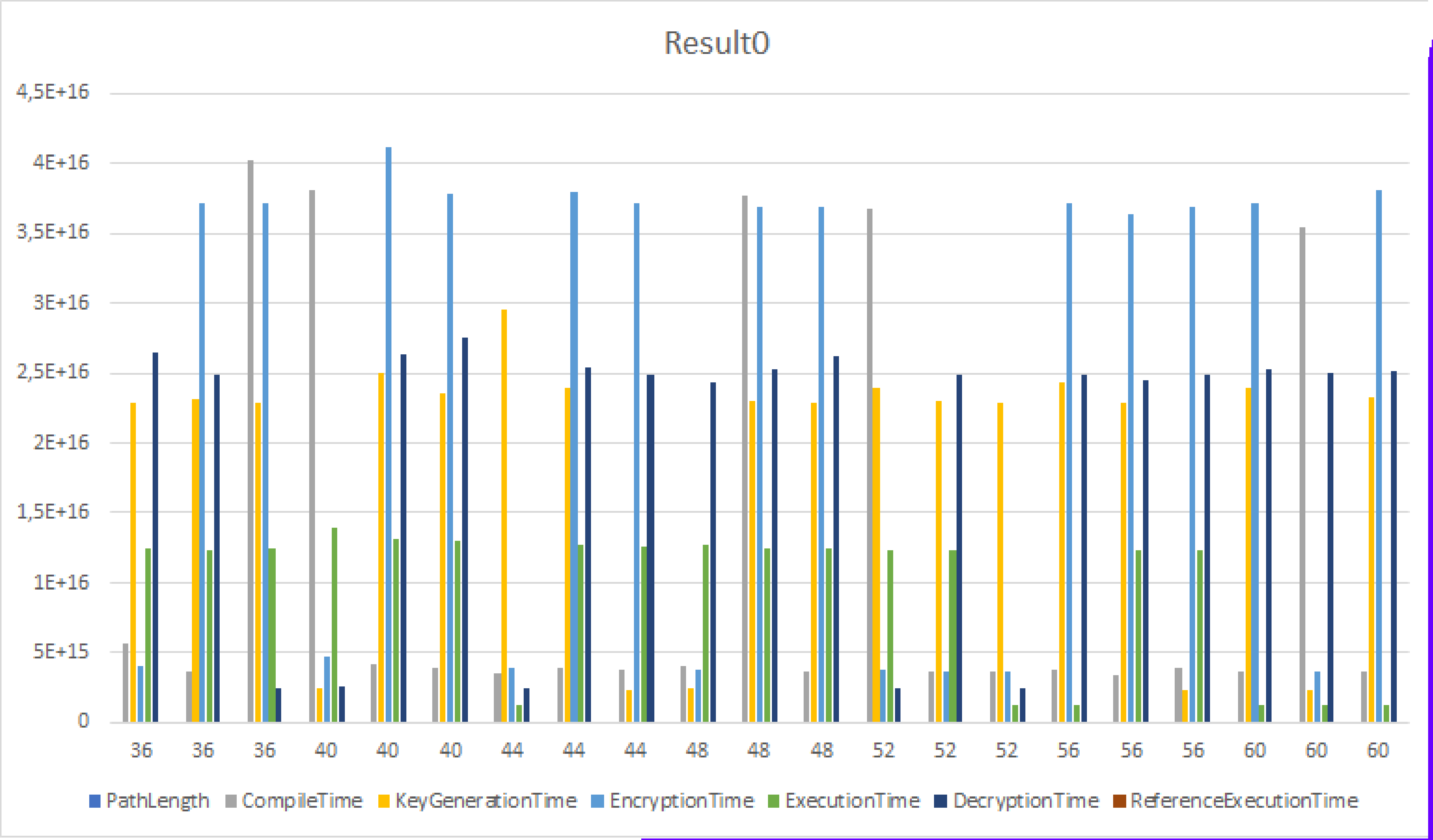
simcnt=1

NodeCoun	PathLength	SimCnt	CompileTime	KeyGenerationTime	EncryptionTime	ExecutionTime	DecryptionTime	ReferenceExecutionTime
32	0	0.4248949999237084	4.237.328.500.039.430	37.134.475.000.129.800	5.801.178.000.183.420	18.167.023.000.387.400	33.420.859.999.750.900	1030181,72
32	1	0.4442919998837169	4.440.330.499.983.240	3.413.538.899.985.720	5.780.229.999.800.210	18.179.397.000.494.600	30.558.610.005.755.300	665259,01
36	0	0.31284299984690733	39.594.775.999.830.700	35.529.155.999.938.600	6.437.026.000.639.880	181.072.410.005.072	4.346.312.000.052.420	10065631,33
36	1	0.3938110003218753	456.029.610.004.407	3.558.096.399.956.410	5.386.448.000.535.890	18.449.459.999.828.800	4.031.731.000.395.660	693665,86
40	0	0.34014799985016	4.200.396.099.986.390	3.489.142.200.032.800	6.459.854.000.240.730	1.960.442.699.964.910	4.040.939.999.867.980	660920,74
40	1	0.3076570001212531	46.187.997.999.368.200	3.446.582.699.962.160	4.975.511.999.873.560	1.773.363.799.929.930	3.787.345.999.626.260	16484747,47

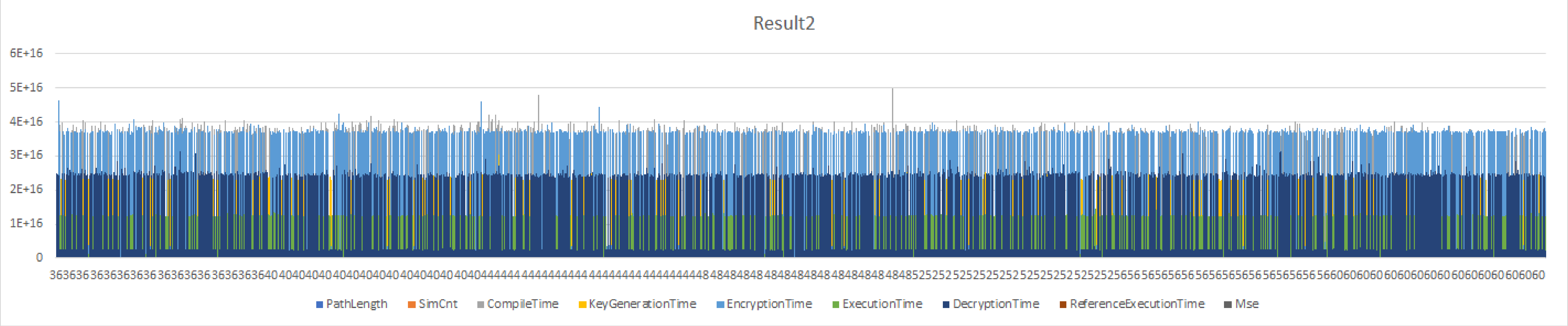
Implementation Findings



simcnt=2								
NodeCount	PathLength	SimCnt	CompileTime	KeyGenerationTime	EncryptionTime	ExecutionTime	DecryptionTime	ReferenceExecutionTime
32	0	0.4274200000509154	4.649.716.899.984.920	3.423.192.700.029.170	6.525.624.999.994.760	175.696.300.002.528	2.990.136.000.335.040	21605716,58
32	1	0.3219620002710144	43.218.849.999.902.800	3.645.390.299.971.040	6.131.126.000.582.290	19.312.940.999.952.800	39.441.740.000.256.600	895036,85
36	0	0.29770200035272865	4.378.788.200.028.790	3.277.030.899.971.570	5.913.804.000.556.410	1.714.802.900.005.450	3.628.677.999.586.210	558420,79
36	1	0.3028779992746422	43.444.926.999.654.800	32.620.727.999.528.700	5.660.260.000.695.410	17.692.215.000.352.000	45.150.039.995.860.400	11533393,89
40	0	0.4891400003543822	4.235.175.500.070.900	33.826.503.999.989.600	65.921.149.998.757.700	18.008.388.000.453.100	3.745.109.999.726.990	20230325,82
40	1	0.30675099969812436	4.480.540.700.023.990	2.994.139.800.011.900	700.277.299.984.009	1.806.601.899.988.890	3.427.208.999.710.270	19770232,40


Result0
4,5E+16
4E+16
3,5E+16
3E+16
2,5E+16
2E+16
1,5E+16
1E+16
5E+15
0
36
36
36
40
40
40
44
44
44
48
48
48
52
52
52
56
56
56
60
60
60
PathLength
CompileTime
KeyGenerationTime
EncryptionTime
ExecutionTime
DecryptionTime
ReferenceExecutionTime

Results


Result2
6E+16
5E+16
4E+16
3E+16
2E+16
1E+16
0
363636 363636363636 363636363636 3636363640 40404040 404040404040 404040404040 40404444444 4444444444 4444444444 44444444448484848 484848484848 484848484848 48485252 525252525252 525252525252 525252565656 565656565656 565656565656 566060606060 606060606060 606060606060 606060
■ PathLength
■ SimCnt
■ CompileTime
■ KeyGenerationTime
■ EncryptionTime
■ ExecutionTime
■ DecryptionTime
■ ReferenceExecutionTime
■ Mse

Results

Conclusion

Homomorphic Encryption is one of the most important types of encryption methods being researched in computational sciences today.

THANK YOU!