From: Paul, Souradyuti [souradyuti.paul@nist.gov]
Sent: Tuesday, June 16, 2009 3:18 PM
To: hash-function@nist.gov
Cc: hash-forum@nist.gov
Subject: OFFICIAL COMMENT: SHAvite-3

(This result does not attack the SHAvite-3-256 hash function. The results show a weakness of the underlying SHAvite-3-256 blockcipher.)

Dear all,

We have found 181 fixed points (two of which were earlier discovered by Peyrin) in the SHAvite-3-256 block cipher. The key of the block cipher for which the fixed points have been found is 0x00.....00(512 bits)||0x525252...5252(256 bits)||0x00..00(64 bits). This key was earlier detected by Peyrin who found two fixed points of the SHAvite-3-256 blockcipher. We henceforth call this key the Peyrin key. Our contribution in short: based on invariant properties of the AES round function (discovered by Le, Sparr, Wernsdorf and Desmedt in the paper "Complementation-like and Cyclic properties of AES Round Function" published in the AES conference 2004), we observe various plaintext patterns of SHAvite-3-256, where the plaintext and the ciphertext match under the Peyrin key. We ran a program over a search space of roughly 3 x 2^{32} to be able to discover those 181 fixed points. While the details of the results are forthcoming, below we write all the 181 plaintexts that give fixed points. The fixed points immediately constitute practical pseudo-multicollisions on the SHAvite-3-256 compression function, but they do not compromise the security of the hash function because the Peyrin key never appears in the hash mode.

With kind regards,

Mridul Nandi and Souradyuti Paul

Object under analysis: SHAvite3/256 Block Cipher.

Description: The following are the 256-bit plaintext words in hex, for each of which ciphertext=plaintext when used with the

key=0x00.....00(512 bits)||0x525252...5252(256 bits)||0x00..00(64 bits)

plaintext format:

pt[0]=xx; pt[1]=xx; pt[2]=xx; pt[3]=xx; pt[4]=yy; pt[5]=yy; pt[6]=yy; pt[7]=yy; |x| = |y| = 16

01. pt[0]=0x02020202; pt[1]=0x02020202; pt[2]=0x02020202; pt[3]=0x02020202; pt[4]=0x02020202; pt[5]=0x02020202; pt[6]=0x02020202; pt[7]=0x02020202;

02. pt[0]=0x02020202; pt[1]=0x02020202; pt[2]=0x02020202; pt[3]=0x02020202; pt[4]=0xe4e4e4e4; pt[5]=0xe4e4e4e4; pt[6]=0xe4e4e4e4; pt[7]=0xe4e4e4e4;

03. pt[0]=0x10161016; pt[1]=0x10161016; pt[2]=0x10161016; pt[3]=0x10161016; pt[4]=0x10161016; pt[5]=0x10161016; pt[6]=0x10161016; pt[7]=0x10161016;

04. pt[0]=0x10161016; pt[1]=0x10161016; pt[2]=0x10161016; pt[3]=0x10161016; pt[4]=0x8ed28ed2; pt[5]=0x8ed28ed2; pt[6]=0x8ed28ed2; pt[7]=0x8ed28ed2;

05. pt[0]=0x15e515e5; pt[1]=0x15e515e5; pt[2]=0x15e515e5; pt[3]=0x15e515e5; pt[4]=0x361e361e; pt[5]=0x361e361e; pt[6]=0x361e361e; pt[7]=0x361e361e;

06. pt[0]=0x15e515e5; pt[1]=0x15e515e5; pt[2]=0x15e515e5; pt[3]=0x15e515e5; pt[4]=0xd4d4d4d4; pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

07. pt[0]=0x16101610; pt[1]=0x16101610; pt[2]=0x16101610; pt[3]=0x16101610; pt[4]=0x16101610; pt[5]=0x16101610; pt[6]=0x16101610; pt[7]=0x16101610;

08. pt[0]=0x16101610; pt[1]=0x16101610; pt[2]=0x16101610; pt[3]=0x16101610; pt[4]=0xd28ed28e; pt[5]=0xd28ed28e; pt[6]=0xd28ed28e; pt[7]=0xd28ed28e;

09. pt[0]=0x1d1d1d1d; pt[1]=0x1d1d1d1d; pt[2]=0x1d1d1d1d; pt[3]=0x1d1d1d1d; pt[4]=0x98989898; pt[5]=0x98989898; pt[6]=0x98989898; pt[7]=0x98989898;

10. pt[0]=0x1d1d1d1d; pt[1]=0x1d1d1d1d; pt[2]=0x1d1d1d1d; pt[3]=0x1d1d1d1d; pt[4]=0xa3a3a3a3; pt[5]=0xa3a3a3a3; pt[6]=0xa3a3a3a3; pt[7]=0xa3a3a3a3;

11. pt[0]=0x1e361e36; pt[1]=0x1e361e36; pt[2]=0x1e361e36; pt[3]=0x1e361e36; pt[4]=0xe515e515; pt[5]=0xe515e515; pt[6]=0xe515e515; pt[7]=0xe515e515;

12. pt[0]=0x1e361e36; pt[1]=0x1e361e36; pt[2]=0x1e361e36; pt[3]=0x1e361e36; pt[4]=0xf9f9f9f9; pt[5]=0xf9f9f9f9; pt[6]=0xf9f9f9f9; pt[7]=0xf9f9f9f9;

13. pt[0]=0x292d292d; pt[1]=0x292d292d; pt[2]=0x292d292d; pt[3]=0x292d292d; pt[4]=0x292d292d; pt[5]=0x292d292d; pt[6]=0x292d292d; pt[7]=0x292d292d;

14. pt[0]=0x292d292d; pt[1]=0x292d292d; pt[2]=0x292d292d; pt[3]=0x292d292d; pt[4]=0xd4d4d4d4; pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

15. pt[0]=0x2d292d29; pt[1]=0x2d292d29; pt[2]=0x2d292d29; pt[3]=0x2d292d29; pt[4]=0x2d292d29; pt[5]=0x2d292d29; pt[6]=0x2d292d29; pt[7]=0x2d292d29;

16. pt[0]=0x2d292d29; pt[1]=0x2d292d29; pt[2]=0x2d292d29; pt[3]=0x2d292d29; pt[4]=0xd4d4d4d4; pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

17. pt[0]=0x361e361e; pt[1]=0x361e361e; pt[2]=0x361e361e; pt[3]=0x361e361e; pt[4]=0x15e515e5; pt[5]=0x15e515e5; pt[6]=0x15e515e5; pt[7]=0x15e515e5;

18. pt[0]=0x361e361e; pt[1]=0x361e361e; pt[2]=0x361e361e; pt[3]=0x361e361e; pt[4]=0xf9f9f9f9; pt[5]=0xf9f9f9f9; pt[6]=0xf9f9f9f9; pt[7]=0xf9f9f9f9;

19. pt[0]=0x3a3a3a3a; pt[1]=0x3a3a3a3a; pt[2]=0x3a3a3a3a; pt[3]=0x3a3a3a3a; pt[4]=0x69696969; pt[5]=0x69696969; pt[6]=0x69696969; pt[7]=0x69696969;

20. pt[0]=0x3a3a3a3a; pt[1]=0x3a3a3a3a; pt[2]=0x3a3a3a3a; pt[3]=0x3a3a3a3a; pt[4]=0xd4d4d4d4; pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

21. pt[0]=0x46b746b7; pt[1]=0x46b746b7; pt[2]=0x46b746b7; pt[3]=0x46b746b7; pt[4]=0x46b746b7; pt[5]=0x46b746b7; pt[6]=0x46b746b7; pt[7]=0x46b746b7;

22. pt[0]=0x46b746b7; pt[1]=0x46b746b7; pt[2]=0x46b746b7; pt[3]=0x46b746b7; pt[4]=0x5f865f86; pt[5]=0x5f865f86; pt[6]=0x5f865f86; pt[7]=0x5f865f86;

23. pt[0]=0x4eed4eed; pt[1]=0x4eed4eed; pt[2]=0x4eed4eed; pt[3]=0x4eed4eed; pt[4]=0x8bd08bd0; pt[5]=0x8bd08bd0; pt[6]=0x8bd08bd0; pt[7]=0x8bd08bd0;

24. pt[0]=0x4eed4eed; pt[1]=0x4eed4eed; pt[2]=0x4eed4eed; pt[3]=0x4eed4eed; pt[4]=0xed4eed4e; pt[5]=0xed4eed4e; pt[6]=0xed4eed4e; pt[7]=0xed4eed4e;

25. pt[0]=0x50b050b0; pt[1]=0x50b050b0; pt[2]=0x50b050b0; pt[3]=0x50b050b0; pt[4]=0x865f865f; pt[5]=0x865f865f; pt[6]=0x865f865f; pt[7]=0x865f865f;

26. pt[0]=0x50b050b0; pt[1]=0x50b050b0; pt[2]=0x50b050b0; pt[3]=0x50b050b0; pt[4]=0xb050b050; pt[5]=0xb050b050; pt[6]=0xb050b050; pt[7]=0xb050b050;

27. pt[0]=0x5f865f86; pt[1]=0x5f865f86; pt[2]=0x5f865f86; pt[3]=0x5f865f86; pt[4]=0x46b746b7; pt[5]=0x46b746b7; pt[6]=0x46b746b7; pt[7]=0x46b746b7;

28. pt[0]=0x5f865f86; pt[1]=0x5f865f86; pt[2]=0x5f865f86; pt[3]=0x5f865f86; pt[4]=0xb050b050; pt[5]=0xb050b050; pt[6]=0xb050b050; pt[7]=0xb050b050;

29. pt[0]=0x67806780; pt[1]=0x67806780; pt[2]=0x67806780; pt[3]=0x67806780; pt[4]=0x67806780; pt[5]=0x67806780; pt[6]=0x67806780; pt[7]=0x67806780;

30. pt[0]=0x67806780; pt[1]=0x67806780; pt[2]=0x67806780; pt[3]=0x67806780; pt[4]=0x8bd08bd0; pt[5]=0x8bd08bd0; pt[6]=0x8bd08bd0; pt[7]=0x8bd08bd0;

31. pt[0]=0x69696969; pt[1]=0x69696969; pt[2]=0x69696969; pt[3]=0x69696969; pt[4]=0x3a3a3a3a; pt[5]=0x3a3a3a3a; pt[6]=0x3a3a3a3a; pt[7]=0x3a3a3a3a;

32. pt[0]=0x69696969; pt[1]=0x69696969; pt[2]=0x69696969; pt[3]=0x69696969; pt[4]=0xd4d4d4d4; pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

33. pt[0]=0x80678067; pt[1]=0x80678067; pt[2]=0x80678067; pt[3]=0x80678067; pt[4]=0x80678067; pt[5]=0x80678067; pt[6]=0x80678067; pt[7]=0x80678067;

34. pt[0]=0x80678067; pt[1]=0x80678067; pt[2]=0x80678067; pt[3]=0x80678067; pt[4]=0xd08bd08b; pt[5]=0xd08bd08b; pt[6]=0xd08bd08b; pt[7]=0xd08bd08b;

35. pt[0]=0x82c182c1; pt[1]=0x82c182c1; pt[2]=0x82c182c1; pt[3]=0x82c182c1; pt[4]=0xc182c182; pt[5]=0xc182c182; pt[6]=0xc182c182; pt[7]=0xc182c182;

36. pt[0]=0x82c182c1; pt[1]=0x82c182c1; pt[2]=0x82c182c1; pt[3]=0x82c182c1; pt[4]=0xd4d4d4d4; pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

37. pt[0]=0x865f865f; pt[1]=0x865f865f; pt[2]=0x865f865f; pt[3]=0x865f865f; pt[4]=0x50b050b0; pt[5]=0x50b050b0; pt[6]=0x50b050b0; pt[7]=0x50b050b0;

38. pt[0]=0x865f865f; pt[1]=0x865f865f; pt[2]=0x865f865f; pt[3]=0x865f865f; pt[4]=0xb746b746; pt[5]=0xb746b746; pt[6]=0xb746b746; pt[7]=0xb746b746;

39. pt[0]=0x8bd08bd0; pt[1]=0x8bd08bd0; pt[2]=0x8bd08bd0; pt[3]=0x8bd08bd0; pt[4]=0x4eed4eed; pt[5]=0x4eed4eed; pt[6]=0x4eed4eed; pt[7]=0x4eed4eed;

40. pt[0]=0x8bd08bd0; pt[1]=0x8bd08bd0; pt[2]=0x8bd08bd0; pt[3]=0x8bd08bd0; pt[4]=0x67806780; pt[5]=0x67806780; pt[6]=0x67806780; pt[7]=0x67806780;

41. pt[0]=0x8ed28ed2; pt[1]=0x8ed28ed2; pt[2]=0x8ed28ed2; pt[3]=0x8ed28ed2; pt[4]=0x10161016; pt[5]=0x10161016; pt[6]=0x10161016; pt[7]=0x10161016;

42. pt[0]=0x8ed28ed2; pt[1]=0x8ed28ed2; pt[2]=0x8ed28ed2; pt[3]=0x8ed28ed2; pt[4]=0xa0d8a0d8; pt[5]=0xa0d8a0d8; pt[6]=0xa0d8a0d8; pt[7]=0xa0d8a0d8;

43. pt[0]=0x98989898; pt[1]=0x98989898; pt[2]=0x98989898; pt[3]=0x98989898; pt[4]=0x1d1d1d1d; pt[5]=0x1d1d1d1d; pt[6]=0x1d1d1d1d; pt[7]=0x1d1d1d1d;

44. pt[0]=0x98989898; pt[1]=0x98989898; pt[2]=0x98989898; pt[3]=0x98989898; pt[4]=0xa3a3a3a3; pt[5]=0xa3a3a3a3; pt[6]=0xa3a3a3a3; pt[7]=0xa3a3a3a3;

45. pt[0]=0x9b9b9b9b; pt[1]=0x9b9b9b9b; pt[2]=0x9b9b9b9b; pt[3]=0x9b9b9b9b; pt[4]=0xc9c9c9c9; pt[5]=0xc9c9c9c9; pt[6]=0xc9c9c9c9; pt[7]=0xc9c9c9c9;

46. pt[0]=0x9b9b9b9b; pt[1]=0x9b9b9b9b; pt[2]=0x9b9b9b9b; pt[3]=0x9b9b9b9b; pt[4]=0xe4e4e4e4; pt[5]=0xe4e4e4e4; pt[6]=0xe4e4e4e4; pt[7]=0xe4e4e4e4;

47. pt[0]=0xa0d8a0d8; pt[1]=0xa0d8a0d8; pt[2]=0xa0d8a0d8; pt[3]=0xa0d8a0d8; pt[4]=0x8ed28ed2; pt[5]=0x8ed28ed2; pt[6]=0x8ed28ed2; pt[7]=0x8ed28ed2;

48. pt[0]=0xa0d8a0d8; pt[1]=0xa0d8a0d8; pt[2]=0xa0d8a0d8; pt[3]=0xa0d8a0d8; pt[4]=0xa0d8a0d8; pt[5]=0xa0d8a0d8; pt[6]=0xa0d8a0d8; pt[7]=0xa0d8a0d8;

49. pt[0]=0xa3a3a3a3; pt[1]=0xa3a3a3a3; pt[2]=0xa3a3a3a3; pt[3]=0xa3a3a3a3; pt[4]=0x1d1d1d1d; pt[5]=0x1d1d1d1d; pt[6]=0x1d1d1d1d; pt[7]=0x1d1d1d1d;

50. pt[0]=0xa3a3a3a3; pt[1]=0xa3a3a3a3; pt[2]=0xa3a3a3a3; pt[3]=0xa3a3a3a3; pt[4]=0x98989898; pt[5]=0x98989898; pt[6]=0x98989898; pt[7]=0x98989898;

51. pt[0]=0xb050b050; pt[1]=0xb050b050; pt[2]=0xb050b050; pt[3]=0xb050b050; pt[4]=0x50b050b0; pt[5]=0x50b050b0; pt[6]=0x50b050b0; pt[7]=0x50b050b0;

52. pt[0]=0xb050b050; pt[1]=0xb050b050; pt[2]=0xb050b050; pt[3]=0xb050b050; pt[4]=0x5f865f86; pt[5]=0x5f865f86; pt[6]=0x5f865f86; pt[7]=0x5f865f86;

53. pt[0]=0xb746b746; pt[1]=0xb746b746; pt[2]=0xb746b746; pt[3]=0xb746b746; pt[4]=0x865f865f; pt[5]=0x865f865f; pt[6]=0x865f865f; pt[7]=0x865f865f;

54. pt[0]=0xb746b746; pt[1]=0xb746b746; pt[2]=0xb746b746; pt[3]=0xb746b746; pt[4]=0xb746b746; pt[5]=0xb746b746; pt[6]=0xb746b746; pt[7]=0xb746b746;

55. pt[0]=0xc182c182; pt[1]=0xc182c182; pt[2]=0xc182c182; pt[3]=0xc182c182; pt[4]=0x82c182c1; pt[5]=0x82c182c1; pt[6]=0x82c182c1; pt[7]=0x82c182c1;

56. pt[0]=0xc182c182; pt[1]=0xc182c182; pt[2]=0xc182c182; pt[3]=0xc182c182; pt[4]=0xd4d4d4d4; pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

57. pt[0]=0xc9c9c9c9; pt[1]=0xc9c9c9c9; pt[2]=0xc9c9c9c9; pt[3]=0xc9c9c9c9; pt[4]=0x9b9b9b9b; pt[5]=0x9b9b9b9b; pt[6]=0x9b9b9b9b; pt[7]=0x9b9b9b9b;

58. pt[0]=0xc9c9c9c9; pt[1]=0xc9c9c9c9; pt[2]=0xc9c9c9c9; pt[3]=0xc9c9c9c9; pt[4]=0xe3e3e3e3; pt[5]=0xe3e3e3e3; pt[6]=0xe3e3e3e3; pt[7]=0xe3e3e3e3;

59. pt[0]=0xd08bd08b; pt[1]=0xd08bd08b; pt[2]=0xd08bd08b; pt[3]=0xd08bd08b; pt[4]=0x80678067; pt[5]=0x80678067; pt[6]=0x80678067; pt[7]=0x80678067;

60. pt[0]=0xd08bd08b; pt[1]=0xd08bd08b; pt[2]=0xd08bd08b; pt[3]=0xd08bd08b; pt[4]=0xed4eed4e; pt[5]=0xed4eed4e; pt[6]=0xed4eed4e; pt[7]=0xed4eed4e;

61. pt[0]=0xd28ed28e; pt[1]=0xd28ed28e; pt[2]=0xd28ed28e; pt[3]=0xd28ed28e; pt[4]=0x16101610; pt[5]=0x16101610; pt[6]=0x16101610; pt[7]=0x16101610;

62. pt[0]=0xd28ed28e; pt[1]=0xd28ed28e; pt[2]=0xd28ed28e; pt[3]=0xd28ed28e; pt[4]=0xd8a0d8a0; pt[5]=0xd8a0d8a0; pt[6]=0xd8a0d8a0; pt[7]=0xd8a0d8a0;

63. pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]=0x15e515e5; pt[5]=0x15e515e5; pt[6]=0x15e515e5; pt[7]=0x15e515e5;

64. pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]=0x292d292d; pt[5]=0x292d292d; pt[6]=0x292d292d; pt[7]=0x292d292d;

65. pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]=0x2d292d29; pt[5]=0x2d292d29; pt[6]=0x2d292d29; pt[7]=0x2d292d29;

66. pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]=0x3a3a3a3a; pt[5]=0x3a3a3a3a; pt[6]=0x3a3a3a3a; pt[7]=0x3a3a3a3a;

67. pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]=0x69696969; pt[5]=0x69696969; pt[6]=0x69696969; pt[7]=0x69696969;

68. pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]=0x82c182c1; pt[5]=0x82c182c1; pt[6]=0x82c182c1; pt[7]=0x82c182c1;

69. pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]=0xc182c182; pt[5]=0xc182c182; pt[6]=0xc182c182; pt[7]=0xc182c182;

70. pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]=0xd4d4d4d4; pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

71. pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]=0xe515e515; pt[5]=0xe515e515; pt[6]=0xe515e515; pt[7]=0xe515e515;

72. pt[0]=0xd8a0d8a0; pt[1]=0xd8a0d8a0; pt[2]=0xd8a0d8a0; pt[3]=0xd8a0d8a0; pt[4]=0xd28ed28e; pt[5]=0xd28ed28e; pt[6]=0xd28ed28e; pt[7]=0xd28ed28e;

73. pt[0]=0xd8a0d8a0; pt[1]=0xd8a0d8a0; pt[2]=0xd8a0d8a0; pt[3]=0xd8a0d8a0; pt[4]=0xd8a0d8a0; pt[5]=0xd8a0d8a0; pt[6]=0xd8a0d8a0; pt[7]=0xd8a0d8a0;

74. pt[0]=0xdadadada; pt[1]=0xdadadada; pt[2]=0xdadadada; pt[3]=0xdadadada; pt[4]=0xdadadada; pt[5]=0xdadadada; pt[6]=0xdadadada; pt[7]=0xdadadada;

75. pt[0]=0xdadadada; pt[1]=0xdadadada; pt[2]=0xdadadada; pt[3]=0xdadadada; pt[4]=0xe3e3e3e3; pt[5]=0xe3e3e3e3; pt[6]=0xe3e3e3e3; pt[7]=0xe3e3e3e3;

76. pt[0]=0xe3e3e3e3; pt[1]=0xe3e3e3e3; pt[2]=0xe3e3e3e3; pt[3]=0xe3e3e3e3; pt[4]=0xc9c9c9c9; pt[5]=0xc9c9c9c9; pt[6]=0xc9c9c9c9; pt[7]=0xc9c9c9c9;

77. pt[0]=0xe3e3e3e3; pt[1]=0xe3e3e3e3; pt[2]=0xe3e3e3e3; pt[3]=0xe3e3e3e3; pt[4]=0xdadadada; pt[5]=0xdadadada; pt[6]=0xdadadada; pt[7]=0xdadadada;

78. pt[0]=0xe4e4e4e4; pt[1]=0xe4e4e4e4; pt[2]=0xe4e4e4e4; pt[3]=0xe4e4e4e4; pt[4]=0x02020202; pt[5]=0x02020202; pt[6]=0x02020202; pt[7]=0x02020202;

79. pt[0]=0xe4e4e4e4; pt[1]=0xe4e4e4e4; pt[2]=0xe4e4e4e4; pt[3]=0xe4e4e4e4; pt[4]=0x9b9b9b9b; pt[5]=0x9b9b9b9b; pt[6]=0x9b9b9b9b; pt[7]=0x9b9b9b9b;

80. pt[0]=0xe515e515; pt[1]=0xe515e515; pt[2]=0xe515e515; pt[3]=0xe515e515; pt[4]=0x1e361e36; pt[5]=0x1e361e36; pt[6]=0x1e361e36; pt[7]=0x1e361e36;

81. pt[0]=0xe515e515; pt[1]=0xe515e515; pt[2]=0xe515e515; pt[3]=0xe515e515; pt[4]=0xd4d4d4d4; pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

82. pt[0]=0xed4eed4e; pt[1]=0xed4eed4e; pt[2]=0xed4eed4e; pt[3]=0xed4eed4e; pt[4]=0x4eed4eed; pt[5]=0x4eed4eed; pt[6]=0x4eed4eed; pt[7]=0x4eed4eed;

83. pt[0]=0xed4eed4e; pt[1]=0xed4eed4e; pt[2]=0xed4eed4e; pt[3]=0xed4eed4e; pt[4]=0xd08bd08b; pt[5]=0xd08bd08b; pt[6]=0xd08bd08b; pt[7]=0xd08bd08b;

84. pt[0]=0xf9f9f9f9; pt[1]=0xf9f9f9f9; pt[2]=0xf9f9f9f9; pt[3]=0xf9f9f9f9; pt[4]=0x1e361e36; pt[5]=0x1e361e36; pt[6]=0x1e361e36; pt[7]=0x1e361e36;

85. pt[0]=0xf9f9f9f9; pt[1]=0xf9f9f9f9; pt[2]=0xf9f9f9f9; pt[3]=0xf9f9f9f9; pt[4]=0x361e361e; pt[5]=0x361e361e; pt[6]=0x361e361e; pt[7]=0x361e361e;

The number of fixed points = 85

Object under analysis: SHAvite3/256 Block Cipher.

Description: The following are the 256-bit plaintext words in hex, for each of which ciphertext=plaintext when used with the

key=0x00.....00(512 bits)||0x525252...5252(256 bits)||0x00..00(64 bits)

plaintext format:

pt[0]=xyxy; pt[1]=yxyx; pt[2]=xyxy; pt[3]=yxyx; pt[4]=zzzz; pt[5]=wwww; pt[6]=zzzz; pt[7]=wwww; |x| = |y| = |z| = |w| = 8

case 1: pt[0]=0x2c082c08; pt[1]=0x82c082c; pt[2]=0x2c082c08; pt[3]=0x82c082c; pt[4]=0x1d1d1d1d; pt[5]=0x71717171; pt[6]=0x1d1d1d1d; pt[7]=0x71717171;

break;

case 2: pt[0]=0x2c082c08; pt[1]=0x82c082c; pt[2]=0x2c082c08; pt[3]=0x82c082c; pt[4]=0x5f5f5f5f; pt[5]=0xa0a0a0a0; pt[6]=0x5f5f5f5f; pt[7]=0xa0a0a0a0;

break;

case 3: pt[0]=0xeb27eb27; pt[1]=0x27eb27eb; pt[2]=0xeb27eb27; pt[3]=0x27eb27eb; pt[4]=0x5f5f5f5f; pt[5]=0xa0a0a0a0; pt[6]=0x5f5f5f5f; pt[7]=0xa0a0a0a0;

break;

case 4: pt[0]=0xeb27eb27; pt[1]=0x27eb27eb; pt[2]=0xeb27eb27; pt[3]=0x27eb27eb; pt[4]=0xd2d2d2d2; pt[5]=0x58585858; pt[6]=0xd2d2d2d2; pt[7]=0x58585858;

break;

case 5: pt[0]=0x82c082c; pt[1]=0x2c082c08; pt[2]=0x82c082c; pt[3]=0x2c082c08; pt[4]=0x71717171; pt[5]=0x1d1d1d1d; pt[6]=0x71717171; pt[7]=0x1d1d1d1d;

break;

case 6: pt[0]=0x82c082c; pt[1]=0x2c082c08; pt[2]=0x82c082c; pt[3]=0x2c082c08; pt[4]=0xa0a0a0a0; pt[5]=0x5f5f5f5f; pt[6]=0xa0a0a0a0; pt[7]=0x5f5f5f5f;

break;

case 7: pt[0]=0xb64ab64a; pt[1]=0x4ab64ab6; pt[2]=0xb64ab64a; pt[3]=0x4ab64ab6; pt[4]=0x17171717; pt[5]=0x9c9c9c9c; pt[6]=0x17171717; pt[7]=0x9c9c9c9c;

break;

case 8: pt[0]=0xb64ab64a; pt[1]=0x4ab64ab6; pt[2]=0xb64ab64a; pt[3]=0x4ab64ab6; pt[4]

=0x53535353; pt[5]=0x53535353; pt[6]=0x53535353; pt[7]=0x53535353;

break;

case 9: pt[0]=0x8b4d8b4d; pt[1]=0x4d8b4d8b; pt[2]=0x8b4d8b4d; pt[3]=0x4d8b4d8b; pt[4]
=0x61616161; pt[5]=0xa7a7a7a7; pt[6]=0x61616161; pt[7]=0xa7a7a7a7;

break;

case 10: pt[0]=0x8b4d8b4d; pt[1]=0x4d8b4d8b; pt[2]=0x8b4d8b4d; pt[3]=0x4d8b4d8b; pt[4]
=0xd2d2d2d2; pt[5]=0x58585858; pt[6]=0xd2d2d2d2; pt[7]=0x58585858;

break;

case 11: pt[0]=0xc74ec74e; pt[1]=0x4ec74ec7; pt[2]=0xc74ec74e; pt[3]=0x4ec74ec7; pt[4]
=0x3b3b3b3b; pt[5]=0x2f2f2f2f; pt[6]=0x3b3b3b3b; pt[7]=0x2f2f2f2f;

break;

case 12: pt[0]=0xc74ec74e; pt[1]=0x4ec74ec7; pt[2]=0xc74ec74e; pt[3]=0x4ec74ec7; pt[4]
=0x6e6e6e6e; pt[5]=0x6060606; pt[6]=0x6e6e6e6e; pt[7]=0x6060606;

break;

case 13: pt[0]=0xd04fd04f; pt[1]=0x4fd04fd0; pt[2]=0xd04fd04f; pt[3]=0x4fd04fd0; pt[4]
=0x1d1d1d1d; pt[5]=0x71717171; pt[6]=0x1d1d1d1d; pt[7]=0x71717171;

break;

case 14: pt[0]=0xd04fd04f; pt[1]=0x4fd04fd0; pt[2]=0xd04fd04f; pt[3]=0x4fd04fd0; pt[4]=0xfefefefe;
pt[5]=0x6b6b6b6b; pt[6]=0xfefefefe; pt[7]=0x6b6b6b6b;

break;

case 15: pt[0]=0xa35ea35e; pt[1]=0x5ea35ea3; pt[2]=0xa35ea35e; pt[3]=0x5ea35ea3; pt[4]
=0x3b3b3b3b; pt[5]=0x2f2f2f2f; pt[6]=0x3b3b3b3b; pt[7]=0x2f2f2f2f;

break;

case 16: pt[0]=0xa35ea35e; pt[1]=0x5ea35ea3; pt[2]=0xa35ea35e; pt[3]=0x5ea35ea3; pt[4]
=0xc4c4c4c4; pt[5]=0x7e7e7e7e; pt[6]=0xc4c4c4c4; pt[7]=0x7e7e7e7e;

break;

case 17: pt[0]=0xc268c268; pt[1]=0x68c268c2; pt[2]=0xc268c268; pt[3]=0x68c268c2; pt[4]
=0x8a8a8a8a; pt[5]=0x9f9f9f9f; pt[6]=0x8a8a8a8a; pt[7]=0x9f9f9f9f;

break;

case 18: pt[0]=0xc268c268; pt[1]=0x68c268c2; pt[2]=0xc268c268; pt[3]=0x68c268c2; pt[4]
=0xd4d4d4d4; pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

break;

case 19: pt[0]=0x4d8b4d8b; pt[1]=0x8b4d8b4d; pt[2]=0x4d8b4d8b; pt[3]=0x8b4d8b4d; pt[4]
=0x58585858; pt[5]=0xd2d2d2d2; pt[6]=0x58585858; pt[7]=0xd2d2d2d2;

break;

case 20: pt[0]=0x4d8b4d8b; pt[1]=0x8b4d8b4d; pt[2]=0x4d8b4d8b; pt[3]=0x8b4d8b4d; pt[4]
=0xa7a7a7a7; pt[5]=0x61616161; pt[6]=0xa7a7a7a7; pt[7]=0x61616161;

break;

case 21: pt[0]=0xb4a2b4a2; pt[1]=0xa2b4a2b4; pt[2]=0xb4a2b4a2; pt[3]=0xa2b4a2b4; pt[4]
=0x61616161; pt[5]=0xa7a7a7a7; pt[6]=0x61616161; pt[7]=0xa7a7a7a7;

break;

case 22: pt[0]=0xb4a2b4a2; pt[1]=0xa2b4a2b4; pt[2]=0xb4a2b4a2; pt[3]=0xa2b4a2b4; pt[4]
=0xd1d1d1d1; pt[5]=0x5a5a5a5a; pt[6]=0xd1d1d1d1; pt[7]=0x5a5a5a5a;

break;

case 23: pt[0]=0x5ea35ea3; pt[1]=0xa35ea35e; pt[2]=0x5ea35ea3; pt[3]=0xa35ea35e; pt[4]=0x2f2f2f2f;
pt[5]=0x3b3b3b3b; pt[6]=0x2f2f2f2f; pt[7]=0x3b3b3b3b;

break;

case 24: pt[0]=0x5ea35ea3; pt[1]=0xa35ea35e; pt[2]=0x5ea35ea3; pt[3]=0xa35ea35e; pt[4]
=0x7e7e7e7e; pt[5]=0xc4c4c4c4; pt[6]=0x7e7e7e7e; pt[7]=0xc4c4c4c4;

break;

```
case 25: pt[0]=0xa2b4a2b4; pt[1]=0xb4a2b4a2; pt[2]=0xa2b4a2b4; pt[3]=0xb4a2b4a2; pt[4]
=0x5a5a5a5a; pt[5]=0xd1d1d1d1; pt[6]=0x5a5a5a5a; pt[7]=0xd1d1d1d1;

break;


case 26: pt[0]=0xa2b4a2b4; pt[1]=0xb4a2b4a2; pt[2]=0xa2b4a2b4; pt[3]=0xb4a2b4a2; pt[4]
=0xa7a7a7a7; pt[5]=0x61616161; pt[6]=0xa7a7a7a7; pt[7]=0x61616161;

break;


case 27: pt[0]=0x4ab64ab6; pt[1]=0xb64ab64a; pt[2]=0x4ab64ab6; pt[3]=0xb64ab64a; pt[4]
=0x53535353; pt[5]=0x53535353; pt[6]=0x53535353; pt[7]=0x53535353;

break;


case 28: pt[0]=0x4ab64ab6; pt[1]=0xb64ab64a; pt[2]=0x4ab64ab6; pt[3]=0xb64ab64a; pt[4]
=0x9c9c9c9c; pt[5]=0x17171717; pt[6]=0x9c9c9c9c; pt[7]=0x17171717;

break;


case 29: pt[0]=0x68c268c2; pt[1]=0xc268c268; pt[2]=0x68c268c2; pt[3]=0xc268c268; pt[4]
=0x9f9f9f9f; pt[5]=0x8a8a8a8a; pt[6]=0x9f9f9f9f; pt[7]=0x8a8a8a8a;

break;


case 30: pt[0]=0x68c268c2; pt[1]=0xc268c268; pt[2]=0x68c268c2; pt[3]=0xc268c268; pt[4]
=0xd4d4d4d4; pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

break;


case 31: pt[0]=0x4ec74ec7; pt[1]=0xc74ec74e; pt[2]=0x4ec74ec7; pt[3]=0xc74ec74e; pt[4]
=0x6060606; pt[5]=0x6e6e6e6e; pt[6]=0x6060606; pt[7]=0x6e6e6e6e;

break;
```

case 32: pt[0]=0x4ec74ec7; pt[1]=0xc74ec74e; pt[2]=0x4ec74ec7; pt[3]=0xc74ec74e; pt[4]=0x2f2f2f2f; pt[5]=0x3b3b3b3b; pt[6]=0x2f2f2f2f; pt[7]=0x3b3b3b3b;

break;

case 33: pt[0]=0x4fd04fd0; pt[1]=0xd04fd04f; pt[2]=0x4fd04fd0; pt[3]=0xd04fd04f; pt[4]=0x6b6b6b6b; pt[5]=0xfefefefe; pt[6]=0x6b6b6b6b; pt[7]=0xfefefefe;

break;

case 34: pt[0]=0x4fd04fd0; pt[1]=0xd04fd04f; pt[2]=0x4fd04fd0; pt[3]=0xd04fd04f; pt[4]=0x71717171; pt[5]=0x1d1d1d1d; pt[6]=0x71717171; pt[7]=0x1d1d1d1d;

break;

case 35: pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]=0x6060606; pt[5]=0x6e6e6e6e; pt[6]=0x6060606; pt[7]=0x6e6e6e6e;

break;

case 36: pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]=0x17171717; pt[5]=0x9c9c9c9c; pt[6]=0x17171717; pt[7]=0x9c9c9c9c;

break;

case 37: pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]=0x6e6e6e6e; pt[5]=0x6060606; pt[6]=0x6e6e6e6e; pt[7]=0x6060606;

break;

case 38: pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]=0x7e7e7e7e; pt[5]=0xc4c4c4c4; pt[6]=0x7e7e7e7e; pt[7]=0xc4c4c4c4;

break;

case 39: pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]=0x8a8a8a8a; pt[5]=0x9f9f9f9f; pt[6]=0x8a8a8a8a; pt[7]=0x9f9f9f9f;

break;

case 40: pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]=0x9c9c9c9c; pt[5]=0x17171717; pt[6]=0x9c9c9c9c; pt[7]=0x17171717;

break;

case 41: pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]=0x9f9f9f9f; pt[5]=0x8a8a8a8a; pt[6]=0x9f9f9f9f; pt[7]=0x8a8a8a8a;

break;

case 42: pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]=0xc4c4c4c4; pt[5]=0x7e7e7e7e; pt[6]=0xc4c4c4c4; pt[7]=0x7e7e7e7e;

break;

case 43: pt[0]=0x27eb27eb; pt[1]=0xeb27eb27; pt[2]=0x27eb27eb; pt[3]=0xeb27eb27; pt[4]=0x58585858; pt[5]=0xd2d2d2d2; pt[6]=0x58585858; pt[7]=0xd2d2d2d2;

break;

case 44: pt[0]=0x27eb27eb; pt[1]=0xeb27eb27; pt[2]=0x27eb27eb; pt[3]=0xeb27eb27; pt[4]=0xa0a0a0a0; pt[5]=0x5f5f5f5f; pt[6]=0xa0a0a0a0; pt[7]=0x5f5f5f5f;

break;

case 45: pt[0]=0xf9f5f9f5; pt[1]=0xf5f9f5f9; pt[2]=0xf9f5f9f5; pt[3]=0xf5f9f5f9; pt[4]=0x5a5a5a5a; pt[5]=0xd1d1d1d1; pt[6]=0x5a5a5a5a; pt[7]=0xd1d1d1d1;

break;

case 46: pt[0]=0xf9f5f9f5; pt[1]=0xf5f9f5f9; pt[2]=0xf9f5f9f5; pt[3]=0xf5f9f5f9; pt[4]=0x6b6b6b6b; pt[5]=0xfefefefe; pt[6]=0x6b6b6b6b; pt[7]=0xfefefefe;

break;

case 47: pt[0]=0xf5f9f5f9; pt[1]=0xf9f5f9f5; pt[2]=0xf5f9f5f9; pt[3]=0xf9f5f9f5; pt[4]=0xd1d1d1d1; pt[5]=0x5a5a5a5a; pt[6]=0xd1d1d1d1; pt[7]=0x5a5a5a5a;

break;

case 48: pt[0]=0xf5f9f5f9; pt[1]=0xf9f5f9f5; pt[2]=0xf5f9f5f9; pt[3]=0xf9f5f9f5; pt[4]=0xfefefefe; pt[5]=0x6b6b6b6b; pt[6]=0xfefefefe; pt[7]=0x6b6b6b6b;

break;

The number of fixed points =48

Object under analysis: SHAvite3/256 Block Cipher.

Description: The following are the 256-bit plaintext words in hex, for each of which ciphertext=plaintext when used with the

key=0x00.....00(512 bits)||0x525252...5252(256 bits)||0x00..00(64 bits)

plaintext format:

pt[0]=xxxx; pt[1]=yyyy; pt[2]=xxxx; pt[3]=yyyy; pt[4]=zwzw; pt[5]=wzwz; pt[6]=zwzw; pt[7]=wzwz; |x| = |y| = |z| = |w| = 8

case 1:pt[0]=0x1d1d1d1d; pt[1]=0x71717171; pt[2]=0x1d1d1d1d; pt[3]=0x71717171; pt[4]=0xd04fd04f; pt[5]=0x4fd04fd0; pt[6]=0xd04fd04f; pt[7]=0x4fd04fd0;

break;

case 2:pt[0]=0x5f5f5f5f; pt[1]=0xa0a0a0a0; pt[2]=0x5f5f5f5f; pt[3]=0xa0a0a0a0; pt[4]=0xeb27eb27; pt[5]=0x27eb27eb; pt[6]=0xeb27eb27; pt[7]=0x27eb27eb;

break;

```
case 3:pt[0]=0x5f5f5f5f; pt[1]=0xa0a0a0a0; pt[2]=0x5f5f5f5f; pt[3]=0xa0a0a0a0; pt[4]=0x2c082c08; pt
[5]=0x82c082c; pt[6]=0x2c082c08; pt[7]=0x82c082c;

break;

case 4:pt[0]=0xd2d2d2d2; pt[1]=0x58585858; pt[2]=0xd2d2d2d2; pt[3]=0x58585858; pt[4]
=0x8b4d8b4d; pt[5]=0x4d8b4d8b; pt[6]=0x8b4d8b4d; pt[7]=0x4d8b4d8b;

break;

case 5:pt[0]=0x71717171; pt[1]=0x1d1d1d1d; pt[2]=0x71717171; pt[3]=0x1d1d1d1d; pt[4]
=0x4fd04fd0; pt[5]=0xd04fd04f; pt[6]=0x4fd04fd0; pt[7]=0xd04fd04f;

break;

case 6:pt[0]=0xa0a0a0a0; pt[1]=0x5f5f5f5f; pt[2]=0xa0a0a0a0; pt[3]=0x5f5f5f5f; pt[4]=0x27eb27eb; pt
[5]=0xeb27eb27; pt[6]=0x27eb27eb; pt[7]=0xeb27eb27;

break;

case 7:pt[0]=0x17171717; pt[1]=0x9c9c9c9c; pt[2]=0x17171717; pt[3]=0x9c9c9c9c; pt[4]
=0xd4d4d4d4; pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

break;

case 8:pt[0]=0x53535353; pt[1]=0x53535353; pt[2]=0x53535353; pt[3]=0x53535353; pt[4]
=0x4ab64ab6; pt[5]=0xb64ab64a; pt[6]=0x4ab64ab6; pt[7]=0xb64ab64a;

break;

case 9:pt[0]=0x61616161; pt[1]=0xa7a7a7a7; pt[2]=0x61616161; pt[3]=0xa7a7a7a7; pt[4]
=0xb4a2b4a2; pt[5]=0xa2b4a2b4; pt[6]=0xb4a2b4a2; pt[7]=0xa2b4a2b4;

break;

case 10:pt[0]=0xd2d2d2d2; pt[1]=0x58585858; pt[2]=0xd2d2d2d2; pt[3]=0x58585858; pt[4]
=0xeb27eb27; pt[5]=0x27eb27eb; pt[6]=0xeb27eb27; pt[7]=0x27eb27eb;

break;

case 11:pt[0]=0x3b3b3b3b; pt[1]=0x2f2f2f2f; pt[2]=0x3b3b3b3b; pt[3]=0x2f2f2f2f; pt[4]=0xa35ea35e;
pt[5]=0x5ea35ea3; pt[6]=0xa35ea35e; pt[7]=0x5ea35ea3;

break;

case 12:pt[0]=0x6e6e6e6e; pt[1]=0x6060606; pt[2]=0x6e6e6e6e; pt[3]=0x6060606; pt[4]=0xd4d4d4d4;
pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

break;
```

```
case 13:pt[0]=0x1d1d1d1d; pt[1]=0x71717171; pt[2]=0x1d1d1d1d; pt[3]=0x71717171; pt[4]
=0x2c082c08; pt[5]=0x82c082c; pt[6]=0x2c082c08; pt[7]=0x82c082c;

break;

case 14:pt[0]=0xfefefefe; pt[1]=0x6b6b6b6b; pt[2]=0xfefefefe; pt[3]=0x6b6b6b6b; pt[4]=0xf5f9f5f9; pt
[5]=0xf9f5f9f5; pt[6]=0xf5f9f5f9; pt[7]=0xf9f5f9f5;

break;

case 15:pt[0]=0x3b3b3b3b; pt[1]=0x2f2f2f2f; pt[2]=0x3b3b3b3b; pt[3]=0x2f2f2f2f; pt[4]=0xc74ec74e;
pt[5]=0x4ec74ec7; pt[6]=0xc74ec74e; pt[7]=0x4ec74ec7;

break;

case 16:pt[0]=0xc4c4c4c4; pt[1]=0x7e7e7e7e; pt[2]=0xc4c4c4c4; pt[3]=0x7e7e7e7e; pt[4]
=0xd4d4d4d4; pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

break;

case 17:pt[0]=0x8a8a8a8a; pt[1]=0x9f9f9f9f; pt[2]=0x8a8a8a8a; pt[3]=0x9f9f9f9f; pt[4]=0xd4d4d4d4;
pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

break;

case 18:pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]
=0xc268c268; pt[5]=0x68c268c2; pt[6]=0xc268c268; pt[7]=0x68c268c2;

break;

case 19:pt[0]=0x58585858; pt[1]=0xd2d2d2d2; pt[2]=0x58585858; pt[3]=0xd2d2d2d2; pt[4]
=0x27eb27eb; pt[5]=0xeb27eb27; pt[6]=0x27eb27eb; pt[7]=0xeb27eb27;

break;

case 20:pt[0]=0xa7a7a7a7; pt[1]=0x61616161; pt[2]=0xa7a7a7a7; pt[3]=0x61616161; pt[4]
=0xa2b4a2b4; pt[5]=0xb4a2b4a2; pt[6]=0xa2b4a2b4; pt[7]=0xb4a2b4a2;

break;

case 21:pt[0]=0x61616161; pt[1]=0xa7a7a7a7; pt[2]=0x61616161; pt[3]=0xa7a7a7a7; pt[4]
=0x8b4d8b4d; pt[5]=0x4d8b4d8b; pt[6]=0x8b4d8b4d; pt[7]=0x4d8b4d8b;

break;

case 22:pt[0]=0xd1d1d1d1; pt[1]=0x5a5a5a5a; pt[2]=0xd1d1d1d1; pt[3]=0x5a5a5a5a; pt[4]
=0xf5f9f5f9; pt[5]=0xf9f5f9f5; pt[6]=0xf5f9f5f9; pt[7]=0xf9f5f9f5;

break;
```

```
case 23:pt[0]=0x2f2f2f2f; pt[1]=0x3b3b3b3b; pt[2]=0x2f2f2f2f; pt[3]=0x3b3b3b3b; pt[4]=0x4ec74ec7;
pt[5]=0xc74ec74e; pt[6]=0x4ec74ec7; pt[7]=0xc74ec74e;

break;

case 24:pt[0]=0x7e7e7e7e; pt[1]=0xc4c4c4c4; pt[2]=0x7e7e7e7e; pt[3]=0xc4c4c4c4; pt[4]
=0xd4d4d4d4; pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

break;

case 25:pt[0]=0x5a5a5a5a; pt[1]=0xd1d1d1d1; pt[2]=0x5a5a5a5a; pt[3]=0xd1d1d1d1; pt[4]
=0xf9f5f9f5; pt[5]=0xf5f9f5f9; pt[6]=0xf9f5f9f5; pt[7]=0xf5f9f5f9;

break;

case 26:pt[0]=0xa7a7a7a7; pt[1]=0x61616161; pt[2]=0xa7a7a7a7; pt[3]=0x61616161; pt[4]
=0x4d8b4d8b; pt[5]=0x8b4d8b4d; pt[6]=0x4d8b4d8b; pt[7]=0x8b4d8b4d;

break;

case 27:pt[0]=0x53535353; pt[1]=0x53535353; pt[2]=0x53535353; pt[3]=0x53535353; pt[4]
=0xb64ab64a; pt[5]=0x4ab64ab6; pt[6]=0xb64ab64a; pt[7]=0x4ab64ab6;

break;

case 28:pt[0]=0x9c9c9c9c; pt[1]=0x17171717; pt[2]=0x9c9c9c9c; pt[3]=0x17171717; pt[4]
=0xd4d4d4d4; pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

break;

case 29:pt[0]=0x9f9f9f9f; pt[1]=0x8a8a8a8a; pt[2]=0x9f9f9f9f; pt[3]=0x8a8a8a8a; pt[4]=0xd4d4d4d4;
pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

break;

case 30:pt[0]=0xd4d4d4d4; pt[1]=0xd4d4d4d4; pt[2]=0xd4d4d4d4; pt[3]=0xd4d4d4d4; pt[4]
=0x68c268c2; pt[5]=0xc268c268; pt[6]=0x68c268c2; pt[7]=0xc268c268;

break;

case 31:pt[0]=0x6060606; pt[1]=0x6e6e6e6e; pt[2]=0x6060606; pt[3]=0x6e6e6e6e; pt[4]=0xd4d4d4d4;
pt[5]=0xd4d4d4d4; pt[6]=0xd4d4d4d4; pt[7]=0xd4d4d4d4;

break;

case 32:pt[0]=0x2f2f2f2f; pt[1]=0x3b3b3b3b; pt[2]=0x2f2f2f2f; pt[3]=0x3b3b3b3b; pt[4]=0x5ea35ea3;
pt[5]=0xa35ea35e; pt[6]=0x5ea35ea3; pt[7]=0xa35ea35e;

break;
```

```
case 33:pt[0]=0x6b6b6b6b; pt[1]=0xfefefefe; pt[2]=0x6b6b6b6b; pt[3]=0xfefefefe; pt[4]=0xf9f5f9f5; pt
[5]=0xf5f9f5f9; pt[6]=0xf9f5f9f5; pt[7]=0xf5f9f5f9;

break;

case 34:pt[0]=0x71717171; pt[1]=0x1d1d1d1d; pt[2]=0x71717171; pt[3]=0x1d1d1d1d; pt[4]
=0x82c082c; pt[5]=0x2c082c08; pt[6]=0x82c082c; pt[7]=0x2c082c08;

break;

case 35:pt[0]=0x6060606; pt[1]=0x6e6e6e6e; pt[2]=0x6060606; pt[3]=0x6e6e6e6e; pt[4]=0x4ec74ec7;
pt[5]=0xc74ec74e; pt[6]=0x4ec74ec7; pt[7]=0xc74ec74e;

break;

case 36:pt[0]=0x17171717; pt[1]=0x9c9c9c9c; pt[2]=0x17171717; pt[3]=0x9c9c9c9c; pt[4]
=0xb64ab64a; pt[5]=0x4ab64ab6; pt[6]=0xb64ab64a; pt[7]=0x4ab64ab6;

break;

case 37:pt[0]=0x6e6e6e6e; pt[1]=0x6060606; pt[2]=0x6e6e6e6e; pt[3]=0x6060606; pt[4]=0xc74ec74e;
pt[5]=0x4ec74ec7; pt[6]=0xc74ec74e; pt[7]=0x4ec74ec7;

break;

case 38:pt[0]=0x7e7e7e7e; pt[1]=0xc4c4c4c4; pt[2]=0x7e7e7e7e; pt[3]=0xc4c4c4c4; pt[4]
=0x5ea35ea3; pt[5]=0xa35ea35e; pt[6]=0x5ea35ea3; pt[7]=0xa35ea35e;

break;

case 39:pt[0]=0x8a8a8a8a; pt[1]=0x9f9f9f9f; pt[2]=0x8a8a8a8a; pt[3]=0x9f9f9f9f; pt[4]=0xc268c268;
pt[5]=0x68c268c2; pt[6]=0xc268c268; pt[7]=0x68c268c2;

break;

case 40:pt[0]=0x9c9c9c9c; pt[1]=0x17171717; pt[2]=0x9c9c9c9c; pt[3]=0x17171717; pt[4]
=0x4ab64ab6; pt[5]=0xb64ab64a; pt[6]=0x4ab64ab6; pt[7]=0xb64ab64a;

break;

case 41:pt[0]=0x9f9f9f9f; pt[1]=0x8a8a8a8a; pt[2]=0x9f9f9f9f; pt[3]=0x8a8a8a8a; pt[4]=0x68c268c2;
pt[5]=0xc268c268; pt[6]=0x68c268c2; pt[7]=0xc268c268;

break;

case 42:pt[0]=0xc4c4c4c4; pt[1]=0x7e7e7e7e; pt[2]=0xc4c4c4c4; pt[3]=0x7e7e7e7e; pt[4]
=0xa35ea35e; pt[5]=0x5ea35ea3; pt[6]=0xa35ea35e; pt[7]=0x5ea35ea3;

break;
```

case 43:pt[0]=0x58585858; pt[1]=0xd2d2d2d2; pt[2]=0x58585858; pt[3]=0xd2d2d2d2; pt[4]
=0x4d8b4d8b; pt[5]=0x8b4d8b4d; pt[6]=0x4d8b4d8b; pt[7]=0x8b4d8b4d;

break;

case 44:pt[0]=0xa0a0a0a0; pt[1]=0x5f5f5f5f; pt[2]=0xa0a0a0a0; pt[3]=0x5f5f5f5f; pt[4]=0x82c082c; pt
[5]=0x2c082c08; pt[6]=0x82c082c; pt[7]=0x2c082c08;

break;

case 45:pt[0]=0x5a5a5a5a; pt[1]=0xd1d1d1d1; pt[2]=0x5a5a5a5a; pt[3]=0xd1d1d1d1; pt[4]
=0xa2b4a2b4; pt[5]=0xb4a2b4a2; pt[6]=0xa2b4a2b4; pt[7]=0xb4a2b4a2;

break;

case 46:pt[0]=0x6b6b6b6b; pt[1]=0xfefefefe; pt[2]=0x6b6b6b6b; pt[3]=0xfefefefe; pt[4]=0x4fd04fd0;
pt[5]=0xd04fd04f; pt[6]=0x4fd04fd0; pt[7]=0xd04fd04f;

break;

case 47:pt[0]=0xd1d1d1d1; pt[1]=0x5a5a5a5a; pt[2]=0xd1d1d1d1; pt[3]=0x5a5a5a5a; pt[4]
=0xb4a2b4a2; pt[5]=0xa2b4a2b4; pt[6]=0xb4a2b4a2; pt[7]=0xa2b4a2b4;

break;

case 48:pt[0]=0xfefefefe; pt[1]=0x6b6b6b6b; pt[2]=0xfefefefe; pt[3]=0x6b6b6b6b; pt[4]=0xd04fd04f;
pt[5]=0x4fd04fd0; pt[6]=0xd04fd04f; pt[7]=0x4fd04fd0;

break;

Total Number of Fixed points =48