Cube attacks on Trivium

S. S. Bedi and N. Rajesh Pillai
Scientific Analysis Group, Metcalfe House Complex, Delhi, INDIA
ssbedi53@hotmail.com, nrpillai@yahoo.com

Abstract

This paper discusses the Cube attacks proposed in [1] applied to Trivium. Independent verification of the equations given in [1] were carried out. Experimentation showed that the precomputed equations were not general. They are correct when applied to the class of IVs for which they were computed - where IV bits at locations other than those corresponding to the cube are fixed at 0. When these IV bits are fixed at some other values, the relations do not hold. The probable cause for this is given and an extra step to the method for equation generation is suggested to take care of such cases.

1 Introduction

Cube Attacks [1] proposed by Dinur and Shamir are a powerful and generic class of attacks applicable to systems which can be described as tweakable polynomials. Here one tries to obtain linear equations in unknown key bits by combining outputs of cipher for certain chosen IVs.

The linear equations are computed by summing the outputs of the system for a set of chosen IVs for an unknown but fixed key K. The IVs in set are identical at all except k bit positions, which take all possible combination of values. In other words the inputs form coordinates of a k-dimensional hypercube.

By carefully choosing the cube, one can obtain linear equations involving only key bits and sum of output bits. One of the first attacks of this kind was described in [4] and applied on a Trivium variant. Linear equations for Trivium with reduced number of initialization rounds (576) were given. The equations were obtained by semi-exhaustive searching. A procedure for construction of linear equations was first given in [1]. Linear equations for variants of Trivium with 672,735 and 770 initial rounds were given in [1].

Independent verification of the equations in [1] was carried out. It was found that most of the equations hold for the special cases considered - IV bits assigned to zero at all places except for those defining the coordinates of the cube. The equations were not holding for the cubes when some random initial setting was used for the other bits in IV. The possible cause for this was investigated and an additional step to the method for generation of equations is suggested to tackle such cases.

In the next section a brief introduction to cube attacks is given. In section 3, verification (of the equations in [1]) performed and the results are given. In section 4, the causes for equations not holding when remaining bits of IV are fixed to other random values are investigated and modification suggested. This is followed by Discussions and Conclusions.

2 Cube Attacks

Cube attacks are applicable on systems which can be modelled as a polynomial $F(K, IV) = Y$, where K is the secret key (of say n bits $x_1, ...x_n$) and IV is publicly known initialization vector (of say m bits $v_1, ..., v_m$). For stream ciphers we have one algebraic expression for each output bit so we use the representation $F_i(K, IV) = Y_i$ to denote the polynomial representation for ith output bit. It is desirable for these polynomials to be complex and highly nonlinear to make them resistant to direct application of algebraic solvers. The main idea of cube attacks is to combine equations for same K but various chosen IV in such a way that low degree equations in the variables in K are obtained. In particular the IVs can be chosen such that linear relations (non-constant and of degree 1) for the unknown bits in K can be obtained. Given sufficient number of equations the key K can be recovered.

The set C of chosen IVs is taken such that $\sum_{IV \in C} F_i(K, IV)$ is a linear combination of bits in K. Let $IV = (v_1, .., v_m)$ and $K = (x_1, .., x_n)$. Suppose that for a particular group of variables $U = \{v_{i_1}, .., v_{i_k}\}$ from the IV part, the expression for the ith output bit can be rewritten as

$$F_i(x_1, .., x_n, v_1, .., v_m) = v_{i_1} v_{i_2} .. v_{i_k} P(x_1, .., x_n, V) + Q$$

Where $P(.)$ is a linear polynomial (over variables in $\{x_1, .., x_n\} \cup V$ with $V = \{v_1, .., v_m\} - U$) and the polynomial Q is such that none of the terms in Q have the monomial $v_{i_1} v_{i_2} .. v_{i_k}$ as a factor. Let C be the set of points where the variables in $\{x_1, .., x_n\} \cup V$ are fixed and the variables in U are allowed to take all possible combination of values. Consider the sum

$$\begin{aligned} \sum_C F_i(x_1, ..x_n, v_1, ..v_m) &= \sum_C v_{i_1} .. v_{i_k} P(x_1, .., x_n, V) + \sum_C Q \\ &= P(x_1, .., x_n, V) \end{aligned}$$

The first summation reduces to $P(x_1, .., x_n, V)$ as the coefficient of $P(x_1, .., x_n, V)$ in the summation is nonzero for only one case in C. The second summation evaluates to zero as each term in Q gets added an even number of times and hence cancels out. The bit locations i for which $P(.)$ are polynomials of degree 1 are identified and stored. In the online phase, the ith output bit of the system with the same unknown key K and for all the IVs in C are xored and the result is equated to $P(.)$ to obtain a linear relation. Each such equation gives one bit of information about the key. Once n linearly independent relations over key bits are obtained we can recover the key.

For precomputation of linear relations, the approach used in [1] was to randomly select $U = \{v_{i_1}, .., v_{i_k}\} \subset \{v_1, .., v_m\}$. The set of chosen IVs were formed by allowing variables in U to take all possible combination of values while keeping variables in $V = \{v_1, .., v_m\} - U$ fixed to 0. A linearity check was performed for the polynomial $p(x_1, .., x_n) = P(x_1, .., x_n, 0)$. If the check was satisfied, the polynomial p was saved for use in the online phase of attack.

3 Verification of Equations for Variants of Trivium

Equations for Trivium variants have been given in Tables 1, 2 and 3 of [1]. The variants considered differ from Trivium [3] only in the number of initialization rounds after which system generates outputs. The number of initialization rounds are 672 for Table 1, 735 for Table 2 and 770 for Table 3 (instead of 1152 rounds as in Trivium).

The equations have been given as triples $(p(K), U, i)$ where $p(K)$ is the linear combination of bits from K; U is the set of IV positions which define the cube and i is the output bit position. Let C denote the set of $2^{|U|}$ chosen IVs where bits at positions given in U are allowed to take all possible values and bits at remaining positions are kept fixed. Then equation denoted by the triple $(p(K), U, i)$ is

$$p(K) = \sum_{IV \in C} F_i(K, IV)$$

For computing the equations, the authors of [1] took C as the set of $2^{|U|}$ vectors where the bits in positions other than those given by U are fixed to 0.

For verification, we used the set U and the output bit number i as inputs and first checked if the sum of output bits at the given position with fixed key and IVs running over C is a linear function of key bits. This was done by taking 100 random pairs of keys (X, Y) and checking if

$$\sum_{IV \in C} F_i(X + Y, IV) = \sum_{IV \in C} F_i(X, IV) + \sum_{IV \in C} F_i(Y, IV) + \sum_{IV \in C} F_i(\mathbf{0}, IV)$$

If the above equation was satisfied for all the 100 random pairs, then the polynomial $p(.)$ was assumed to be linear in key bits. The linear combination of the key bits was then derived as given in [1]. Bit j of K is present in the linear combination if $\sum_{IV \in C} F_i(E_j, IV) \neq \sum_{IV \in C} F_i(\mathbf{0}, IV)$ where E_j is the unit vector with jth bit 1 and rest of the bits are 0.

The Tables 1 2, 3 give the results obtained by us when IV bits at locations in $V = \{1, 2, ..m\} - U$ are fixed to 0. The results for Trivium with 672 rounds show that all the equations listed in Table 1 of [1] hold except for one case (Cube No. 26, where relation was given as $x28$ instead of $1 + x28$).

For Trivium with 735 initial rounds, many of the cubes failed the linearity test. The values of the keys X and Y for which the test for linearity failed are given in Table 4. For cube no 48 the relation formed was $x63$ instead of $1 + x63$ as mentioned in [1]. For Trivium with 770 initial rounds, only one (first) of the four relations was holding. The rest of the relations were failing the test for linearity. The X and Y values for which failure occured are given in Table 5.

When IV bits at positions in V are fixed to some random value and the verification routine was executed, we observed that most of the relations do not hold. For this exercise a random 80-bit vector was generated and used as a template for IV for all the relations. The set C of chosen IVs for each equation was generated by varying the bits at the cube indices given by [1] through all possible combinations while keeping other positions unchanged. The test for linearity was applied with this set C of chosen IVs. Tables 6 and 7 give the results for the Trivium variants with 672 and 735 initialization rounds. None of the relations which were obtained by fixing locations in V to 0 were holding when random initialization was used for locations in V. This shows that the relations of Tables 1 and 2 (and 3) of [1] may not be as general as implied.

The equations of [4] were also computed with variables in V set to 0. Verification exercise for these equations have not been attempted by us.

4 Possible Cause and Modification Suggested

In this section the possible causes for the equations not holding for general case are discussed. The authors of [1] were aware of one - occurrence of a highly nonlinear term in the polynomial coefficient of the $v_{i_1}...v_{i_k}$. We show that nonlinear polynomials are detected as a linear polynomial for some other cases also.

Let $U = \{i_1, .., i_k\}$ and V denote the complement set $\{1..m\} - U$. The expression for ith output bit can be written as

$$F_i(x_i, .., x_n, v_1, ..v_m) = v_{i_1}v_{i_2}..v_{i_k}P(x_1, ..x_n, V) + q(x_1, ..x_n, v_1, ..v_m)$$

where $v_{i_1}v_{i_2}..v_{i_k}$ does not divide any of the terms of q.

For the cube attack we are interested in finding U and i such that we get equations of the form

$$F_i(x_1, .., x_n, v_1, .., v_m) = v_{i_1}v_{i_2}..v_{i_k}p(x_1, ..x_n) + q(x_1, ..x_n, v_1, ..v_m)$$

where $p(.)$ is linear. To identify such U, the method suggested in [1] (section 4.2) is to try for U of various sizes. For too large cases, the expression $\sum_{IV \in C} F_i(X, IV)$ evaluates to a constant irrespective of X. For small sizes, the expression will give a nonlinear polynomial in bits of X. The idea is to keep trying till we hit the size in between where the sum evaluates to a polynomial of degree 1. To check if $\sum_{IV \in C} F_i(X, IV)$ is a polynomial of degree 1, the method in [1] checks if

$$\sum_{IV \in C} F_i(X+Y, IV) = \sum_{IV \in C} F_i(X, IV) + \sum_{IV \in C} F_i(Y, IV) + \sum_{IV \in C} F_i(\mathbf{0}, IV)$$

for sufficient number of randomly selected keys X and Y. If the equation holds for all the random cases tried, the polynomial P was assumed to be of the required form viz. linear in x_js and then the individual coefficients for the linear combination are calculated.

The set C of IVs used were such that bits at locations in V were fixed to 0 and bits at locations in U were allowed to run over all possible choices (Second para of section 4.2 of [1]). Because of the this the polynomials of the kind $P() = x_1 + x_2 + v_k x_1 x_2$ for some $v_k \in V$ will also show up as linear. In fact both $x_1 + x_2 + v_{k_1} x_1 x_2$ and $x_1 + x_2 + v_{k_2} x_3$ will be detected as $x_1 + x_2$.

This shows that fixing the bits at positions in V to 0 will give us equations which need not hold for the general case. To detect such cases(with a high probability) verification exercise for sufficient cases with IV bits at locations in V fixed to some random values should also be carried out. This can be done by choosing a random key X and two random settings V_1 and V_2 for the variables at positions in set V. Check if the relation $P(X, V_1) = P(X, V_2)$ holds. If it holds for sufficient number(say 100) of Xs, then with a high probability $P(.)$ is independent of IV bits at positions in V. Once this is ensured, the other steps as given in [1] can be carried out.

This approach of making equations was attempted on Trivium with 672 initial rounds. Till the time of writing this paper, we were unable to obtain equations which hold for cubes of dimension up to 14. Work in this direction is still in progress.

4.1 Relaxation of the Maxterms

Observe that the equations computed in Tables 1,2 and 3 contain variables only from the secret key part. Where as in general case they can contain some linear terms from V, the fixed part of IV also. Using this observation, we tried to find polynomials $P(x_1, .., x_n, V)$ which were of degree 1 and having at least one variable from the secret key part. Set of 45 equations found for Trivium with 576 initialization rounds are given in Table 8. The precomputed equations in this case will be applicable to a large set of IVs. These equations will help in reducing the effective keyspace of Trivium with 576 rounds to 2^{35}.

5 Discussions

The method for finding equations given in [1] assumed that the bits in remaining positions of IV are set 0. The equations obtained though not general are applicable for some other sets of IVs. The usefulness of a relation depends on the proportion of IVs for which it holds. The methods of [2] can applied.

The fact that equations identified may not hold in general was mentioned in [1] also. The reasons given were that it might be due to some terms which are highly nonlinear and occur with a very low probability. We have given an example where terms which are not highly nonlinear can still lead to a situation where an incorrect linear equation is detected.

Finding cubes so that equations which hold in general may turn out to need more computation. In particular the cube dimensions may be larger than indicated in [1].

Larger cube dimension implies requirement of greater amount of crypts on same secret key setting. This may make the attack difficult to apply in practice.

Instead of precomputing equations holding in general, one can try to find equations for the particular class of IVs observed. One can look for cubes of lower dimension which give linear relations on key bits for the observed set of IVs.

Based on our experiments, we believe that using randomly chosen IVs with the additional constraint of a lower bound on Hamming weight will reduce the chances of finding useful equations.

6 Conclusions

Verification of the equations for cube attack in [1] for the reduced round of variants of Trivium was carried out. It was observed that the equations given in [1] are not general. The fact that equations may not hold in general was known to the authors of [1]. But the justification given was that it may occur due to highly nonlinear terms which will come into effect with a very low probability. We showed that there are cases besides occurrence of highly nonlinear terms which can lead to equations which do not hold in general. We showed that assigning bits of IV other than those on the cube to 0 makes some nonlinear functions appear as linear functions in the linearity test.

Modifications to the equation generation step of cube attack was proposed to include a probabilistic check to rule out such cases. Equation generation was attempted with this modification. It was observed that one has to try cubes of higher dimensions to get linear relations. Equations were generated for Trivium with 576 initial rounds. The 45 linearly independent equations obtained by us are given in Table 8.

Acknowledgements

The authors thank Dr P K Saxena, Director SAG, for his constant support and encouragement for the work.

References

[1] Itai Dinur and Adi Shamir. Cube Attacks on Tweakable Black Box Polynomials, Cryptology ePrint Archive, Report 2008/385, 2008. http://eprint.iacr.org/

[2] S. Fischer, S. Khazaei and W. Meier. Chosen IV Statistical Analysis for Key Recovery Attacks on Stream Ciphers, AFRICA CRYPT 2008.

[3] C. De Canniere and B. Preneel. TRIVIUM - stream cipher construction inspired by block cipher design principles. eStream: ECRYPT Stream Cipher Project, Report 2005/030, 2005. http://www.ecrypt-eu.org/stream/trivium.html

[4] M Vielhaber, Breaking ONE.FIVIUM by AIDA: An Algebraic IV Differential Attack, Cryptology ePrint Archive, Report 2007/413, 2007. http://eprint.iacr.org/

Table 1: Maxterms for Trivium for 672 initialization rounds

No.	Maxterm	Cube Indices	Output bit index
1	1+x0 +x9 +x50	2,13,20,24,37,42,43,46,53,55,57,67	675
2	1+x0 +x24	2,12,17,25,37,39,46,48,54,56,65,78	673
3	1+x1 +x10+x51	3,14,21,25,38,43,44,47,54,56,58,68	674
4	1+x1 +x25	3,13,18,26,38,40,47,49,55,57,66,79	672
5	1+x2 +x34+x62	0, 5, 7,18,21,32,38,43,59,67,73,78	678
6	1+x3 +x35+x63	1, 6, 8,19,22,33,39,44,60,68,74,79	677
7	x4	11,18,20,33,45,47,53,60,61,63,69,78	675
8	x5	5,14,16,18,27,31,37,43,48,55,63,78	677
9	x7	1, 3, 6, 7,12,18,22,38,47,58,67,74	675
10	1+x8 +x49+x68	1,12,19,23,36,41,42,45,52,54,56,66	676
11	x11	0, 4, 9,11,22,24,27,29,44,46,51,76	684
12	x12	0, 5, 8,11,13,21,22,26,36,38,53,79	673
13	x13	0, 5, 8,11,13,22,26,36,37,38,53,79	673
14	1+x14	2, 5, 7,10,14,24,27,39,49,56,57,61	672
15	x15	0, 2, 9,11,13,37,44,47,49,68,74,78	685
16	x16	1, 6, 7,12,18,21,29,33,34,45,49,70	675
17	x17	8,11,15,17,23,26,32,42,51,62,64,79	677
18	x18	0,10,16,19,28,31,43,50,53,66,69,79	676
19	x19	4, 9,10,15,21,24,32,36,37,48,52,73	672
20	x20	7,10,18,20,23,25,31,45,53,63,71,78	675
21	1+x20+x50	11,16,20,22,35,43,46,51,55,58,62,63	675
22	1+x21+x66	10,13,15,17,30,37,39,42,47,57,73,79	673
23	x22	2, 4,21,23,25,41,44,54,58,66,73,78	673
24	x23	3, 6,14,21,23,27,32,40,54,57,70,71	672
25	1+x24	3, 5,14,16,18,20,33,56,57,65,73,75	672
26	1+x28	6,11,14,19,33,39,44,52,58,60,74,79	676
27	x29	1, 7,12,18,21,25,29,45,46,61,68,70	675
28	x30	2, 8,13,19,22,26,30,46,47,62,69,71	674
29	x31	3, 9,14,20,23,27,31,47,48,63,70,72	673
30	x32	4,10,15,21,24,28,32,48,49,64,71,73	672
31	x33	2, 4, 6,12,23,29,32,37,46,49,52,76	680
32	1+x34+x62	0, 5, 7,13,18,21,32,38,43,59,73,78	678
33	1+x35+x63	1, 6, 8,14,19,22,33,39,44,60,74,79	677
34	x36	2, 4, 5, 8,15,19,27,32,35,57,71,78	677
35	x38+x56	0, 3, 4, 9,20,28,33,41,54,58,72,79	678
36	1+x39+x57+x66	8,11,13,17,23,25,35,45,47,54,70,79	674
37	x40+x58+x64	0, 6,10,16,19,31,43,50,66,69,77,79	676
38	1+x41	2,15,17,20,21,37,39,44,46,56,67,73	674
39	x42+x60	1,16,20,22,34,37,38,53,58,69,71,78	674
40	x43	2, 7,14,22,41,45,48,58,68,70,72,76	673
41	x44+x62	3,14,16,18,20,23,32,46,56,57,65,73	672
42	1+x45+x64	0, 6,10,16,18,28,31,43,53,69,77,79	676
43	x46+x55	2, 8,11,13,28,31,35,37,49,51,68,78	684
44	x47	5, 8,20,32,36,39,45,51,65,69,76,78	676
45	x48	2, 4,10,14,16,22,25,44,49,51,57,78	678
46	x49+x62	1,12,19,23,36,41,42,45,52,56,69,75	676
47	x51+x62	1, 7, 8,13,21,23,28,30,47,68,71,75	674
48	x52	5, 8, 9,12,16,18,23,40,44,63,66,70	674
49	x53	2,11,21,24,32,55,57,60,63,66,70,77	675
50	1+x54+x60	4, 7,10,18,20,25,50,53,61,63,71,78	675
51	x55+x64	5,12,16,19,22,36,47,55,63,71,77,79	674
52	1+x56	4, 9,18,21,23,27,32,38,43,58,67,69	677
53	x57	1, 7, 9,14,18,21,33,40,45,49,59,68	675
54	1+x58	2, 6,12,13,19,23,30,48,55,59,69,79	673
55	x60	5, 7,10,13,15,17,28,40,47,73,76,79	681
56	x61	13,21,24,39,42,46,48,51,55,61,72,78	673
57	1+x62	2, 4,10,11,19,34,47,55,56,58,69,77	674
58	x63	5, 7,10,15,17,35,40,47,52,57,76,79	674
59	x64	8,11,13,17,23,25,35,47,62,64,68,79	673
60	x65	2, 3,13,15,19,29,32,37,39,51,76,79	682
61	1+x66	5, 7,10,13,15,17,35,40,52,70,76,79	678
62	1+x67	5,20,24,29,33,35,37,39,63,65,74,78	677
63	1+x68	1,12,19,23,36,41,52,54,56,66,69,75	676

Table 2: Maxterms for Trivium for 735 initialization rounds

No.	Maxterm	Cube Indices	O/p bit index
1	1+x0	{ 1, 4, 8,11,12,13,18,27,35,37,39,46,48,50,51,52,54,56,62,63,65,72,78}	735
2	x1	{ 1, 8,13,14,16,19,21,24,29,32,37,41,44,48,50,52,60,68,70,72,74,77,79}	738
3	1+x2+x65+x67	{ 3, 7, 9,11,12,17,20,22,24,26,27,30,34,36,38,43,49,51,55,69,70,72,78}	736
4	x3	{ 1, 2, 4, 7,14,15,21,25,27,36,39,44,49,54,60,61,63,64,69,70,73,76,78}	736
5	x4	{ 2, 3, 5, 8,15,16,22,26,28,37,40,45,50,55,61,62,64,65,70,71,74,77,79}	735
6	Nonlinear	{ 1, 8,13,16,21,29,32,33,35,37,41,44,48,50,52,56,60,68,70,72,74,77,79}	739
7	1+x6+x57+x66	{ 2,14,16,19,22,24,26,27,30,37,44,47,52,53,56,60,61,63,70,72,75,76,79}	737
8	1+x7	{ 1, 3, 8,13,17,18,19,21,25,36,38,40,46,49,50,54,61,62,63,66,69,73,79}	736
9	x8	{ 4, 7,11,12,14,17,18,22,24,30,33,37,38,40,50,52,63,64,66,70,72,74,77}	735
10	x8+x21	{ 4,11,12,14,17,18,22,24,30,33,35,37,38,40,47,50,52,63,64,66,70,72,74}	735
11	Nonlinear	{ 1, 3, 5, 7, 9,12,14,17,18,25,30,31,43,45,49,52,54,61,62,70,73,75,79}	737
12	x10	{ 2, 4, 6, 8,10,13,19,23,31,32,34,39,44,46,53,55,62,69,71,73,74,76,79}	736
13	1+x12+x65	{ 2, 4, 6, 8,15,19,23,28,31,32,34,39,46,50,53,55,62,69,71,73,74,76,79}	736
14	x13	{ 3, 7, 9,11,12,17,20,22,24,25,27,30,38,43,49,51,52,62,69,70,72,75,78}	736
15	x14	{ 4, 8,10,12,13,18,21,23,25,26,28,31,39,44,50,52,53,63,70,71,73,76,79}	735
16	Nonlinear	{ 0, 2, 4, 6, 8,11,13,17,26,29,30,32,42,44,48,51,53,60,69,71,72,74,78}	739
17	x16+x18	{ 1, 3, 5, 7, 9,12,14,18,27,30,31,33,43,45,49,52,54,61,70,72,73,75,79}	738
18	1+x17	{ 2, 4, 8,13,15,19,23,28,31,34,39,44,46,50,53,55,62,69,71,73,74,76,79}	738
19	1+x18	{ 1, 3, 7, 8, 9,12,14,17,18,25,30,31,33,45,49,52,54,61,70,72,73,75,79}	738
20	1+x18+x52	{ 4, 8,11,13,15,18,21,26,31,33,35,42,48,49,50,53,57,58,59,60,67,69,78}	739
21	Nonlinear	{ 1,10,18,20,22,27,36,38,46,48,49,55,58,61,63,66,68,69,71,75,76,77,79}	737
22	x20	{ 4,11,12,14,18,20,22,24,30,33,35,37,38,40,47,50,52,63,64,66,70,72,74}	735
23	1+x22	{ 2, 3, 5, 9,15,16,22,26,28,37,40,50,61,62,63,64,69,70,71,74,76,77,79}	735
24	1+x22+x58+x68	{ 1, 3, 8,13,17,18,19,21,25,26,36,38,39,40,49,54,61,62,63,66,69,73,79}	735
25	x24	{ 0, 4, 7,11,12,17,18,22,24,33,35,37,38,40,47,50,52,63,64,66,70,72,77}	735
26	x28+x30	{ 4, 5, 8,11,13,15,18,21,26,33,35,47,48,50,53,57,58,59,60,67,69,76,78}	739
27	1+x29	{ 0, 3, 4, 8,13,14,17,19,21,22,25,37,40,41,44,46,56,59,70,72,73,75,78}	739
28	1+x30	{ 1, 4, 5, 9,14,15,18,20,22,23,26,38,41,42,45,47,57,60,71,73,74,76,79}	738
29	x31	{ 1, 4, 5, 9,14,15,18,20,22,23,33,38,42,45,47,52,57,60,67,71,73,74,79}	738
30	x32+x34	{ 4,11,12,14,17,18,20,24,30,33,35,37,38,40,47,53,63,64,66,68,70,72,74}	735
31	1+x33+x58+x64	{ 1, 2, 4, 8,14,15,21,25,27,36,39,44,49,60,61,62,63,64,69,70,73,75,78}	736
32	1+x34+x59+x65	{ 2, 3, 5, 9,15,16,22,26,28,37,40,45,50,61,62,63,64,65,70,71,74,76,79}	735
33	x35	{ 1, 3, 8,13,17,18,19,21,25,26,31,33,36,38,40,46,54,61,62,63,66,73,79}	735
34	x36	{ 0, 3, 5, 9,13,17,19,21,28,40,45,46,49,54,58,59,63,64,67,72,74,75,78}	735
35	1+x37+x61	{ 4,11,12,14,17,18,20,22,24,35,37,40,47,50,51,53,63,64,66,68,70,72,74}	735
36	1+x39	{ 0, 4,11,12,17,18,22,24,33,35,37,38,40,47,50,52,63,64,66,70,72,74,77}	735
37	Nonlinear	{ 3, 4, 6, 9,13,17,18,21,26,28,32,34,37,41,47,49,52,58,59,65,70,76,78}	748
38	Nonlinear	{ 4, 5, 7,10,14,18,19,22,27,29,33,35,38,42,48,50,53,59,60,66,71,77,79}	747
39	x54	{ 1, 4, 8,11,12,13,18,27,30,35,37,38,46,48,50,52,54,56,62,63,65,72,78}	735
40	x1+x55+x61+x64	{ 0, 2,14,23,26,27,29,33,36,38,41,45,51,58,60,62,64,65,67,68,71,75,79}	737
41	x56	{ 1, 4, 6, 8,10,13,16,17,19,21,24,26,27,29,38,41,45,50,55,60,69,72,78}	737
42	Nonlinear	{ 4,11,12,17,20,22,24,30,33,35,37,38,40,47,50,52,53,63,64,68,70,72,74}	735
43	x58	{ 2, 3, 4, 6,14,18,24,27,37,42,45,47,49,50,51,56,60,67,69,71,74,76,78}	739
44	x59	{ 1, 3, 9,10,11,17,25,32,34,36,39,45,47,59,65,66,67,68,70,72,74,75,78}	739
45	1+x60	{ 1, 4, 6, 8,10,16,17,18,21,24,26,27,33,38,41,45,50,52,60,69,71,72,78}	737
46	Nonlinear	{ 0, 2, 3, 7, 9,10,11,17,25,32,34,36,39,45,46,47,59,65,68,70,72,74,75,78}	739
47	x62	{ 1, 4, 5, 8, 9,15,20,23,26,32,38,42,45,47,52,57,60,67,71,73,74,76,79}	737
48	x63	{ 3, 5, 9,15,22,26,28,37,40,45,50,55,61,62,63,65,69,70,71,74,76,77,79}	735
49	1+x64	{ 1, 4, 8,12,13,18,27,35,37,38,39,46,48,50,52,54,56,62,63,65,72,78,79}	735
50	x65	{ 1, 4, 6, 8,16,17,18,21,24,26,27,29,33,38,41,45,50,52,60,69,71,72,78}	738
51	1+x66	{ 2, 5, 7, 9,17,18,19,22,25,27,28,30,34,39,42,46,51,53,61,70,72,73,79}	737
52	1+x67	{ 3, 5,13,15,18,20,23,28,32,33,37,40,44,50,53,56,60,62,63,65,72,75,78}	736

Table 3: Maxterms for Trivium for 770 initialization rounds

No.	Maxterm	Cube Indices	output index
1	x60	{2,4,10,13,15,19,23,25,27,31,33,34,37,40,41,45,48,50,51,54,56,60,61,62,67,69,71,73,76}	770
2	nonlinear	{2,4, 7,13,15,19,23,24,25,27,31,33,34,37,40,41,45,48,50,51,54,56,60,61,62,67,69,71,73}	771
3	nonlinear	{2,4, 7,10,13,15,19,23,24,25,27,31,33,34,36,37,40,45,48,50,54,56,60,61,62,67,69,71,73}	770
4	nonlinear	{1,3, 6,12,14,18,22,23,24,26,30,32,33,35,36,39,40,44,47,49,50,53,59,60,61,66,68,69,72,75}	771

Table 4: Key Pairs to show nonlinearity of equations for Trivium with 735 initial rounds

Cube No. 6. Indices={ 1 8 13 16 21 29 32 33 35 37 41 44 48 50 52 56 60 68 70 72 74 77 79 }
For output bit position 739, Key pair =
X = 00011111111110001011111111111110101100011001101110001001100110101011001101111 0001
Y = 01101101000011111000110100010101101000101101010010010001011000101100011000111001
Cube No. 11. Indices={ 1 3 5 7 9 12 14 17 18 25 30 31 43 45 49 52 54 61 62 70 73 75 79 }
For output bit position 737, Key pair =
X = 11001111101010111110000100111011001010000001100001001000111101001110010001011100
Y = 01000001010010001001011100001011001101001010110001010101111101110011011010101101
Cube No. 16. Indices={ 0 2 4 6 8 11 13 17 26 29 30 32 42 44 48 51 53 60 69 71 72 74 78 }
For output bit position 739, Key pair =
X = 00110010010100111001100110001000101110010110010010110001010010011011001011101001
Y = 00011100110001111001011110011010011110101111100001111110111010110011100100110000
Cube No. 21. Indices={ 1 10 18 20 22 27 36 38 46 48 49 55 58 61 63 66 68 69 71 75 76 77 79 }
For output bit position 737, Key pair =
X = 11011001111111100111000000010101001000011100100010110101000111101010100011001 01
Y = 01011110010111011111000011110001000010101110101101110111011010100000101011100011
Cube No. 37. Indices={ 3 4 6 9 13 17 18 21 26 28 32 34 37 41 47 49 52 58 59 65 70 76 78 }
For output bit position 748, Key pair =
X = 10000111011100010101101001001010010000101001100101011111100001001011000110100110
Y = 01110111111110111001011001101010101000101010110010111011101110100001101000111100 1
Cube No. 38. Indices={ 4 5 7 10 14 18 19 22 27 29 33 35 38 42 48 50 53 59 60 66 71 77 79 }
For output bit position 747, Key pair =
X = 01111101100110011101101111110000110000011000101001010101000000111100101000010000
Y = 10011001001000000100101101000000100111101010000001000000010010001000110110110111 01
Cube No. 42. Cube Indices={ 4 11 12 17 20 22 24 30 33 35 37 38 40 47 50 52 53 63 64 68 70 72 74 }
For output bit position 735, Key pair =
X = 10000100001101001001001111000111101111101111011110100010010000110011101010100011
Y = 00111011011010010111101110110001100001100010011000111000011001111110000101100000
Cube No. 46. Indices={ 0 2 3 7 9 10 11 17 25 32 34 36 39 45 46 47 59 65 68 70 72 74 75 78 }
For output bit position 739, Key pair =
X = 01010110100100001000001101010000101111101111101100100001100100110101010101001011
Y = 00000010001001110100001001011111110011011110001011010110101010011010111100110011

Table 5: Key Pairs to show nonlinearity of equations for Trivium with 770 initial rounds

Cube No. 2.
Indices = {2 4 7 13 15 19 23 24 25 27 31 33 34 37 40 41 45 48 50 51 54 56 60 61 62 67 69 71 73 }
For output bit position 771, Key Pair =
X = 11000111010100001101111101000111111100000110110001100010110101110000110101110010
Y = 10011110010101001100001011111010001110001011111001101000111010000110110011100011
Cube No. 3.
Indices = {2 4 7 10 13 15 19 23 24 25 27 31 33 34 36 37 40 45 48 50 54 56 60 61 62 67 69 71 73 }
For output bit position 770, Key Pair =
X = 00000100001101101111001111101101110100100001011111011101011000111111100010111000
Y = 11010001011010000101101000111000101101001110011001111101110010100001001100101001
Cube No. 4
Indices= {1 3 6 12 14 18 22 23 24 26 30 32 33 35 36 39 40 44 47 49 50 53 59 60 61 66 68 69 72 75}
For output bit position 771, Key Pair =
X= 11100111101001001101011111000011100111011011100010010111011010010001110010100101
Y= 00100010101001101010100001001011101100110000110011001001001111001110101111101110

Table 6: Verification of equations for Trivium with 672 initialization rounds
Chosen IVs were formed by using the IV given below as a fixed pattern and running bits at cube locations through all combinations. No linear relations were obtained for the cubes by combining bits. The check was done for all output bit positions in the range 672 to 735
The Fixed IV used for all the cases is
01000011010000001001010000111000110100111010010000110101101110010100100110100110 0

No.	Maxterm	Cube Indices	Output bit index
1	NonLinear	{ 2,13,20,24,37,42,43,46,53,55,57,67}	675
2	NonLinear	{ 2,12,17,25,37,39,46,48,54,56,65,78}	673
3	NonLinear	{ 3,14,21,25,38,43,44,47,54,56,58,68}	674
4	NonLinear	{ 3,13,18,26,38,40,47,49,55,57,66,79}	672
5	NonLinear	{ 0, 5, 7,18,21,32,38,43,59,67,73,78}	678
6	NonLinear	{ 1, 6, 8,19,22,33,39,44,60,68,74,79}	677
7	NonLinear	{11,18,20,33,45,47,53,60,61,63,69,78}	675
8	NonLinear	{ 5,14,16,18,27,31,37,43,48,55,63,78}	677
9	NonLinear	{ 1, 3, 6, 7,12,18,22,38,47,58,67,74}	675
10	NonLinear	{ 1,12,19,23,36,41,42,45,52,54,56,66}	676
11	NonLinear	{ 0, 4, 9,11,22,24,27,29,44,46,51,76}	684
12	NonLinear	{ 0, 5, 8,11,13,21,22,26,36,38,53,79}	673
13	NonLinear	{ 0, 5, 8,11,13,22,26,36,37,38,53,79}	673
14	NonLinear	{ 2, 5, 7,10,14,24,27,39,49,56,57,61}	672
15	NonLinear	{ 0, 2, 9,11,13,37,44,47,49,68,74,78}	685
16	NonLinear	{ 1, 6, 7,12,18,21,29,33,34,45,49,70}	675
17	NonLinear	{ 8,11,15,17,23,26,32,42,51,62,64,79}	677
18	NonLinear	{ 0,10,16,19,28,31,43,50,53,66,69,79}	676
19	NonLinear	{ 4, 9,10,15,21,24,32,36,37,48,52,73}	672
20	NonLinear	{ 7,10,18,20,23,25,31,45,53,63,71,78}	675
21	NonLinear	{11,16,20,22,35,43,46,51,55,58,62,63}	675
22	NonLinear	{10,13,15,17,30,37,39,42,47,57,73,79}	673
23	NonLinear	{ 2, 4,21,23,25,41,44,54,58,66,73,78}	673
24	NonLinear	{ 3, 6,14,21,23,27,32,40,54,57,70,71}	672
25	NonLinear	{ 3, 5,14,16,18,20,33,56,57,65,73,75}	672
26	NonLinear	{ 6,11,14,19,33,39,44,52,58,60,74,79}	676
27	NonLinear	{ 1, 7,12,18,21,25,29,45,46,61,68,70}	675
28	NonLinear	{ 2, 8,13,19,22,26,30,46,47,62,69,71}	674
29	NonLinear	{ 3, 9,14,20,23,27,31,47,48,63,70,72}	673
30	NonLinear	{ 4,10,15,21,24,28,32,48,49,64,71,73}	672
31	NonLinear	{ 2, 4, 6,12,23,29,32,37,46,49,52,76}	680
32	NonLinear	{ 0, 5, 7,13,18,21,32,38,43,59,73,78}	678
33	NonLinear	{ 1, 6, 8,14,19,22,33,39,44,60,74,79}	677
34	NonLinear	{ 2, 4, 5, 8,15,19,27,32,35,57,71,78}	677
35	NonLinear	{ 0, 3, 4, 9,20,28,33,41,54,58,72,79}	678
36	NonLinear	{ 8,11,13,17,23,25,35,45,47,54,70,79}	674
37	NonLinear	{ 0, 6,10,16,19,31,43,50,66,69,77,79}	676
38	NonLinear	{ 2,15,17,20,21,37,39,44,46,56,67,73}	674
39	NonLinear	{ 1,16,20,22,34,37,38,53,58,69,71,78}	674
40	NonLinear	{ 2, 7,14,22,41,45,48,58,68,70,72,76}	673
41	NonLinear	{ 3,14,16,18,20,23,32,46,56,57,65,73}	672
42	NonLinear	{ 0, 6,10,16,18,28,31,43,53,69,77,79}	676
43	NonLinear	{ 2, 8,11,13,28,31,35,37,49,51,68,78}	684
44	NonLinear	{ 5, 8,20,32,36,39,45,51,65,69,76,78}	676
45	NonLinear	{ 2, 4,10,14,16,22,25,44,49,51,57,78}	678
46	NonLinear	{ 1,12,19,23,36,41,42,45,52,56,69,75}	676
47	NonLinear	{ 1, 7, 8,13,21,23,28,30,47,68,71,75}	674
48	NonLinear	{ 5, 8, 9,12,16,18,23,40,44,63,66,70}	674
49	NonLinear	{ 2,11,21,24,32,55,57,60,63,66,70,77}	675
50	NonLinear	{ 4, 7,10,18,20,25,50,53,61,63,71,78}	675
51	NonLinear	{ 5,12,16,19,22,36,47,55,63,71,77,79}	674
52	NonLinear	{ 4, 9,18,21,23,27,32,38,43,58,67,69}	677
53	NonLinear	{ 1, 7, 9,14,18,21,33,40,45,49,59,68}	675
54	NonLinear	{ 2, 6,12,13,19,23,30,48,55,59,69,79}	673
55	NonLinear	{ 5, 7,10,13,15,17,28,40,47,73,76,79}	681
56	NonLinear	{13,21,24,39,42,46,48,51,55,61,72,78}	673
57	NonLinear	{ 2, 4,10,11,19,34,47,55,56,58,69,77}	674
58	NonLinear	{ 5, 7,10,15,17,35,40,47,52,57,76,79}	674
59	NonLinear	{ 8,11,13,17,23,25,35,47,62,64,68,79}	673
60	NonLinear	{ 2, 3,13,15,19,29,32,37,39,51,76,79}	682
61	NonLinear	{ 5, 7,10,13,15,17,35,40,52,70,76,79}	678
62	NonLinear	{ 5,20,24,29,33,35,37,39,63,65,74,78}	677
63	NonLinear	{ 1,12,19,23,36,41,52,54,56,66,69,75}	676

Table 7: Verification of equations for Trivium with 735 initialization rounds
Chosen IVs were formed by using the IV given below as a fixed pattern and running bits at cube locations through all combinations. No linear relations were obtained for the cubes by combining bits. The check was done for all output bit positions in the range 735 to 798
The Fixed IV used for all the cases is
01000011010000001001010000111000110100111010010000110101101110010100100110100110 0

No.	Maxterm	Cube Indices	O/p bit index
1	Nonlinear	{ 1, 4, 8,11,12,13,18,27,35,37,39,46,48,50,51,52,54,56,62,63,65,72,78}	735
2	Nonlinear	{ 1, 8,13,14,16,19,21,24,29,32,37,41,44,48,50,52,60,68,70,72,74,77,79}	738
3	Nonlinear	{ 3, 7, 9,11,12,17,20,22,24,26,27,30,34,36,38,43,49,51,55,69,70,72,78}	736
4	Nonlinear	{ 1, 2, 4, 7,14,15,21,25,27,36,39,44,49,54,60,61,63,64,69,70,73,76,78}	736
5	Nonlinear	{ 2, 3, 5, 8,15,16,22,26,28,37,40,45,50,55,61,62,64,65,70,71,74,77,79}	735
6	Nonlinear	{ 1, 8,13,16,21,29,32,33,35,37,41,44,48,50,52,56,60,68,70,72,74,77,79}	739
7	Nonlinear	{ 2,14,16,19,22,24,26,27,30,37,44,47,52,53,56,60,61,63,70,72,75,76,79}	737
8	Nonlinear	{ 1, 3, 8,13,17,18,19,21,25,36,38,40,46,49,50,54,61,62,63,66,69,73,79}	736
9	Nonlinear	{ 4, 7,11,12,14,17,18,22,24,30,33,37,38,40,50,52,63,64,66,70,72,74,77}	735
10	Nonlinear	{ 4,11,12,14,17,18,22,24,30,33,35,37,38,40,47,50,52,63,64,66,70,72,74}	735
11	Nonlinear	{ 1, 3, 5, 7, 9,12,14,17,18,25,30,31,43,45,49,52,54,61,62,70,73,75,79}	737
12	Nonlinear	{ 2, 4, 6, 8,10,13,19,23,31,32,34,39,44,46,53,55,62,69,71,73,74,76,79}	736
13	Nonlinear	{ 2, 4, 6, 8,15,19,23,28,31,32,34,39,46,50,53,55,62,69,71,73,74,76,79}	736
14	Nonlinear	{ 3, 7, 9,11,12,17,20,22,24,25,27,30,38,43,49,51,52,62,69,70,72,75,78}	736
15	Nonlinear	{ 4, 8,10,12,13,18,21,23,25,26,28,31,39,44,50,52,53,63,70,71,73,76,79}	735
16	Nonlinear	{ 0, 2, 4, 6, 8,11,13,17,26,29,30,32,42,44,48,51,53,60,69,71,72,74,78}	739
17	Nonlinear	{ 1, 3, 5, 7, 9,12,14,18,27,30,31,33,43,45,49,52,54,61,70,72,73,75,79}	738
18	Nonlinear	{ 2, 4, 8,13,15,19,23,28,31,34,39,44,46,50,53,55,62,69,71,73,74,76,79}	738
19	Nonlinear	{ 1, 3, 7, 8, 9,12,14,17,18,25,30,31,33,45,49,52,54,61,70,72,73,75,79}	738
20	Nonlinear	{ 4, 8,11,13,15,18,21,26,31,33,35,42,48,49,50,53,57,58,59,60,67,69,78}	739
21	Nonlinear	{ 1,10,18,20,22,27,36,38,46,48,49,55,58,61,63,66,68,69,71,75,76,77,79}	737
22	Nonlinear	{ 4,11,12,14,18,20,22,24,30,33,35,37,38,40,47,50,52,63,64,66,70,72,74}	735
23	Nonlinear	{ 2, 3, 5, 9,15,16,22,26,28,37,40,50,61,62,63,64,69,70,71,74,76,77,79}	735
24	Nonlinear	{ 1, 3, 8,13,17,18,19,21,25,26,36,38,39,40,49,54,61,62,63,66,69,73,79}	735
25	Nonlinear	{ 0, 4, 7,11,12,17,18,22,24,33,35,37,38,40,47,50,52,63,64,66,70,72,77}	735
26	Nonlinear	{ 4, 5, 8,11,13,15,18,21,26,33,35,47,48,50,53,57,58,59,60,67,69,76,78}	739
27	Nonlinear	{ 0, 3, 4, 8,13,14,17,19,21,22,25,37,40,41,44,46,56,59,70,72,73,75,78}	739
28	Nonlinear	{ 1, 4, 5, 9,14,15,18,20,22,23,26,38,41,42,45,47,57,60,71,73,74,76,79}	738
29	Nonlinear	{ 1, 4, 5, 9,14,15,18,20,22,23,33,38,42,45,47,52,57,60,67,71,73,74,79}	738
30	Nonlinear	{ 4,11,12,14,17,18,20,24,30,33,35,37,38,40,47,53,63,64,66,68,70,72,74}	735
31	Nonlinear	{ 1, 2, 4, 8,14,15,21,25,27,36,39,44,49,60,61,62,63,64,69,70,73,75,78}	736
32	Nonlinear	{ 2, 3, 5, 9,15,16,22,26,28,37,40,45,50,61,62,63,64,65,70,71,74,76,79}	735
33	Nonlinear	{ 1, 3, 8,13,17,18,19,21,25,26,31,33,36,38,40,46,54,61,62,63,66,73,79}	735
34	Nonlinear	{ 0, 3, 5, 9,13,17,19,21,28,40,45,46,49,54,58,59,63,64,67,72,74,75,78}	735
35	Nonlinear	{ 4,11,12,14,17,18,20,22,24,35,37,40,47,50,51,53,63,64,66,68,70,72,74}	735
36	Nonlinear	{ 0, 4,11,12,17,18,22,24,33,35,37,38,40,47,50,52,63,64,66,70,72,74,77}	735
37	Nonlinear	{ 3, 4, 6, 9,13,17,18,21,26,28,32,34,37,41,47,49,52,58,59,65,70,76,78}	748
38	Nonlinear	{ 4, 5, 7,10,14,18,19,22,27,29,33,35,38,42,48,50,53,59,60,66,71,77,79}	747
39	Nonlinear	{ 1, 4, 8,11,12,13,18,27,30,35,37,38,46,48,50,52,54,56,62,63,65,72,78}	735
40	Nonlinear	{ 0, 2,14,23,26,27,29,33,36,38,41,45,51,58,60,62,64,65,67,68,71,75,79}	737
41	Nonlinear	{ 1, 4, 6, 8,10,13,16,17,19,21,24,26,27,29,38,41,45,50,55,60,69,72,78}	737
42	Nonlinear	{ 4,11,12,17,20,22,24,30,33,35,37,38,40,47,50,52,53,63,64,68,70,72,74}	735
43	Nonlinear	{ 2, 3, 4, 6,14,18,24,27,37,42,45,47,49,50,51,56,60,67,69,71,74,76,78}	739
44	Nonlinear	{ 1, 3, 9,10,11,17,25,32,34,36,39,45,47,59,65,66,67,68,70,72,74,75,78}	739
45	Nonlinear	{ 1, 4, 6, 8,10,16,17,18,21,24,26,27,33,38,41,45,50,52,60,69,71,72,78}	737
46	Nonlinear	{ 0, 2, 3, 7, 9,10,11,17,25,32,34,36,39,45,46,47,59,65,68,70,72,74,75,78}	739
47	Nonlinear	{ 1, 4, 5, 8, 9,15,20,23,26,32,38,42,45,47,52,57,60,67,71,73,74,76,79}	737
48	Nonlinear	{ 3, 5, 9,15,22,26,28,37,40,45,50,55,61,62,63,65,69,70,71,74,76,77,79}	735
49	Nonlinear	{ 1, 4, 8,12,13,18,27,35,37,38,39,46,48,50,52,54,56,62,63,65,72,78,79}	735
50	Nonlinear	{ 1, 4, 6, 8,16,17,18,21,24,26,27,29,33,38,41,45,50,52,60,69,71,72,78}	738
51	Nonlinear	{ 2, 5, 7, 9,17,18,19,22,25,27,28,30,34,39,42,46,51,53,61,70,72,73,79}	737
52	Nonlinear	{ 3, 5,13,15,18,20,23,28,32,33,37,40,44,50,53,56,60,62,63,65,72,75,78}	736

Table 8: Equations for Trivium with 576 initialization rounds

No.	$p(x_1, ..x_{80}, v_1, ..v_{80})$	Cube Indices	O/p bit index
1	x68	{ 3,20,28,36,42,55,77,78}	579
2	v77+v64+x67	{18,26,36,45,61,73,78,79}	579
3	v78+x66	{11,18,34,37,45,51,70,79}	588
4	x65	{ 1, 3,28,34,51,61,67}	581
5	x64	{ 3,12,19,29,37,62,77}	578
6	x63	{ 8,13,21,39,53,73,74}	577
7	x62	{ 6, 7,12,13,15,16,36,73}	576
8	x61	{ 0,10,35,45,55,58,72,77}	584
9	v72+v09+v08+x60	{ 6, 7,10,27,35,36,67}	581
10	x59	{ 1,20,29,36,48,55,73}	587
11	x58	{ 8,16,19,28,52,62,69,72}	586
12	x57	{ 0,10,11,23,25,26,29,57,68,71}	593
13	x56	{ 5, 6,11,27,44,55,60,67}	578
14	x55	{ 0, 3, 7,20,21,31,66}	578
15	x54	{ 5, 6,11,44,60,65,67}	577
16	v65+v64+v50+x53	{17,25,27,35,54,62,63,79}	581
17	v64+v63+v49+v07+x52	{ 1, 2, 8,39,61,62,69,70}	579
18	x51	{15,23,32,47,49,58,76}	584
19	x50	{ 0, 5,14,23,38,48,67}	584
20	x49	{14,22,30,45,48,50,59,75}	585
21	x48	{ 4,29,38,43,46,47,57,66,73}	586
22	x47	{18,28,38,39,42,45,46,65,79}	587
23	v25+x46	{ 1,17,19,21,24,27,59,60,71}	614
24	x45	{ 9,18,25,28,43,45,55,69}	590
25	1+v20+x44	{ 2,21,29,40,57,66,73}	577
26	v40+x43	{ 1, 7, 8,32,39,42,67,74}	591
27	v39+x42	{ 7,15,29,38,41,42,50,75}	592
28	1+v51+v38+x41	{ 3, 9,12,22,30,49,52,53}	589
29	x40	{19,30,36,38,43,46,58,63,79}	595
30	v36+x39	{ 4, 5,21,22,37,38,39,72}	595
31	1+v48+v35+x38	{ 3, 7,11,23,44,49,50}	580
32	v49+v48+v34+x37	{ 1, 7, 9,15,46,47,59,68}	582
33	v48+v47+v33+x36	{ 7,21,23,45,46,58,74,76}	584
34	v47+v46+v32+x35	{22,25,41,44,45,51,55,58,67}	581
35	1+v44+v31+x34	{ 1,15,45,46,50,57,68,69}	583
36	1+v45+v44+v30+v27+x33	{ 5,22,28,31,42,43,51,75}	582
37	v44+v43+v29+x32	{ 0, 3,32,39,41,42,47,48,61}	585
38	1+v41+v28+x31	{ 4,20,37,42,43,54,64}	587
39	v42+v41+v27+x30	{10,11,25,26,39,40,47,56,70}	588
40	1+v39+v26+x29	{ 0, 2,11,30,40,41,53,54}	589
41	v40+v39+v25+x28	{18,28,37,38,42,45,46,65,79}	588
42	x03	{ 5, 9,10,11,12,42,68,77}	579
43	v68+v29+x02	{ 5, 8,12,28,31,67,74}	576
44	v67+x01	{ 9,10,19,33,41,68,77}	590
45	v66+x00	{ 3,12,37,63,65,71,74}	578