Two New Examples of TTM

T. Moh*

Abstract

We will review the past history of the attacks and defenses of TTM. The main tool of the past attacks is linear algebra, while the defenses rely on algebraic geometry and commutative algebra. It is hard for attackers to completely succeed against the formidable castle of modern mathematics. It is out of the common sense that problems of algebraic geometry can always be solved by linear algebra. It repeatly happens that the attackers find some points which could be exploited by linear algebra using complicated computations, usually the attackers overexaggerate the power of linear algebra and illusional believe that they succeed totally, then the points are disappearing by a simple twist in algebraic geometry and commutative algebra. All attacks in the past simply strengthen the structures of TTM. For these facts we are very grateful to the attackers.

Last year there is a paper entitled "*Breaking a New Instance of TTM Cryptosystem*" by Xuyun Nie, Lei Hu, Jianyu Li, Crystal Updegrove and Jintai Ding [11] claiming a successive attack on the scheme of TTM presented in [7]. In our previous article [8], we show that their claim is a **misunderstanding**.

The discussions of [11] and [8] center on if in [11] the authors really just use the *public keys*. Right after we post [8], to settle the discrepancy of [11] and [8], we have sent the public keys of a new example (which is attached as the **Appendix I** of this article) to the authors of [11] to test their claim in the *abstract* of [11], i.e., they will be able to crack TTM using only the public keys (in 20 minutes as stated in the abstract of [11]). After two weeks, Mr Nie asks the private keys of the new example for his *theoretical analysis* and we will consider his request only if he concedes that he is unable to crack the new example by the method of [11]. Since there is no definite answer from them after 4 months, we will publish the example in this article to give other people chances to attack. Furthermore, we publish a second example as **Appendix II**.

1 Introduction

The TTM cryptosystem (cf [5],[7]) is a truly higher dimensional method. It is given by the composition of *tame* mappings $\pi(=\prod_i \phi_i)$ from K^n to K^m where K is a finite field and $n \leq m$. **The public key is the composition** π (which can be written as a sequence of quadratic polynomials) **while the private key is the set of mappings** $\{\phi_i\}$. The *tame* mappings, which are commonly known in mathematics, are defined as

Definition: We define a *tame* mapping $\phi_i = (\phi_{i,1}, \cdots, \phi_{i,m})$ as either a linear transformation, or of the following form in any *order* of variables $x_1, \cdots, x_m$ with polynomials $h_{i,j}$,

$$\begin{aligned}
&(1): \phi_{i,1}(x_1, \cdots, x_m) = x_1 = y_1 \\
&(2): \phi_{i,2}(x_1, \cdots, x_m) = x_2 + h_{i,2}(x_1) = y_2 \\
&\cdots\cdots\cdots \\
&(j): \phi_{i,j}(x_1, \cdots, x_m) = x_j + h_{i,j}(x_1, \cdots, x_{j-1}) = y_j \qquad (1)
\end{aligned}$$

*Math Department, Purdue University, West Lafayette, Indiana 47907-1395. tel: (765) -494-1930, e-mail ttm@math.purdue.edu

....

$$(m): \phi_{i,m}(x_1, \cdots, x_m) = x_m + h_{i,m}(x_1, \cdots, x_{m-1}) = y_m$$

In papers [5],[6], [7], implementations of TTM are given. The public key is the composition of $\phi_4\phi_3\phi_2\phi_1$ which will be written as a sequence of quadratic polynomials. An attacker shall focus on them. The private keys $\phi_4, \phi_3, \phi_2, \phi_1$ are written as polynomials of degrees $1, 8, 2, 1$ respectively.

For the users (not the attackers) we provide the decoding process consisting of the private keys which are mainly the inverse linear transformations ϕ_1^{-1}, ϕ_2^{-1}, the *lock polynomials* (which gives ϕ_3^{-1}) and ϕ_2^{-1}.

2 Past History of Attacks and Defenses

The crytposystem TTM is a method of algebraic geometry and commutative algebra for encryption purpose. It goes through stages of attacks and defenses. We should list some important ones as follows,

(1) Sathaye-Montgomery's attack (private correspondences, 1998): Using linear algebra to analyze the dimension of the vector space generated by the degree 2 forms. As we consider only one *non-linear tame map* at the middle at that time. This method shows that the dimension is $m-1$, and the whole system can solved successively.

The defense is to increase the number of middle non-linear tame maps to two and invent a lock polynomial for these purpose ([5] 1999). Then the dimension of the vector space generated by the degree 2 forms will be m, and their analysis fails.

(2) Kipnis-Shamir's *relinearization* ([4]) and Courtois-Shamir-Patarin-Klimorv's *XL* methods ([1] 2000). The main object of the attacks is Patarin's HFE (*hidden field equation*) which is a 0-dimensional encryption system disguised as multivariante cryptosystem in the tradition of Matsumoto-Imai. The main point of HFE is hidding a field equation (it is 0-dimensional in the sense of algebraic geometry). We show that the said methods applying to TTM, a genuine n-dimensional cryptosystem, are inefficient in [9] (1999) and [10] (2001).

(3) Minrank attack of L.Goubin and N.Courtois ([3], 2000): There they show that we not only have to consider the dimension, but also have to consider the rank to have a secure system. They obtain a formula for complexity, $q^{(rank)\lceil m/n \rceil} \times m^3$ where q is the number of elements in the gound field (which we take to be 2^8). They mistakely believe that the minrank(as indicated by $(rank)$ in the preceding formula) of TTM is always 2 (otherwise their attack will fail).

The defense is to increase the number of lock polynomials to at least four, and the minrank to 4 or more, thus the minrank attack fail ([6] 2001).

(4) The generalized Patarin attack of Ding-Schmidt([2] 2003): Their attack is using the linear equations produced by the generalized Patarin attack as finding coefficients $a, \{b_i\}, \{c_j\}, \{d_{ij}\}$ in the following formula,

$$a + \sum_i b_i x_i + \sum_j c_j y_j + \sum_{i,j} d_{ij} x_i y_j = 0$$

As long as the number of free variables is tolerably small (say,< 9), then all free varibles may be assigned to all possible values in the finite field (say, GL(2^8)) to find the right system of linear equations, thus the whole system can be solved.

The defense is to slightly modify the system so that the number of free variables is intolerably high (say, > 10) ([7] 2004) and the attack of Ding-Schmidt fails.

(5) Rely on the knowledge of the private key and the process of constructing the private key (i.e., knowing the compact forms of the lock polynomials), Xuyun Nie-Lei Hu-Jianyu Li-Crystal Updegrove-Jintai Ding ([11] 2006) show that they may use the following criterion to find the values of $\{b_{kj}\}, \{c_i\}$

satisfying the following inequality and solve the system step by step,

$$degree(\sum b_{jk}y_jy_k + \sum c_iy_i) \leq 1 \ or \ 2$$

The defense is to make the above equations simply producing constant or *parasite* (i.e., useless) polynomials (**Appendix I** of this article, they are sent to the authors of [11] in 2006). The reader is referred to the next two sections to see the details

3 Legitimate Attack

The strength of a public key system is solely on the public key, i.e., with the public key known to the general public, the attacker tries to find the private key or its equivalences. Note that the attacker has no information about the private key nor how it is constructed. By the constructions of the private keys, we mean the **compact** expressions of the lock polynomials.

The attacker on TTM shall only use the public key which is a sequence of quadratic polynomials. The so called *lock polynomials* are parts of ϕ_3, hence are parts of the *private keys.* In the *abstract* of article [11], the authors claim that they only use the public key, while in the *content* of article [11], they use the private keys and their constructions (i.e., their compact forms) freely. It will be unfair to them to ask them to completely forget the *lock polynomials* and the *constructions (i.e., their compact forms) of the lock polynomials* of the example in [7]. The only fair way is to provide them with another example so they may test their skill.

Right after we post our article [8], we have sent Mr Nie and Dr Ding the public keys of our example in the **Appendix I** of this article for Mr Nie to fulfill his claim that he will crack our examples in two weeks. BTW, they claim that the complexity of our system is 2^{38} which can be translated to less than 20 minutes on a PC of 256 Hz. How does he explain that he needs two weeks? After two weeks, he has sent us a surprising email: "$\cdots$. *Hence, for theoretical analysis, one should assume that the adversary (attacker) know the explicit forms of central map (lock polynomials).*"(on 5 Jan 2007). This is absurd! The central polynomials (lock polynomials) are part of the private key. Apparently, they are confused about what are public keys and what are private keys. We feel that to provide the *lock polynomials* will not help the *theoretical analysis* of our system. The hard parts are the constructions (i.e., their compact forms) of the *lock polynomials.* It is easy to see that there are vast number of ways to construct the *lock polynomials.* It is impossible to guess right the construction (i.e., their compact forms). The constructions (i.e., their compact forms) are even routinely hidden from the legitimate users. He has to request both the *lock polynomials* and the *constructions* (i.e., their compact forms) of them. However, to keep the contest pure and to test their claim in the *abstract* of [11], we refuse to give him the parts of the private keys unconditionally.

4 On the Appendix

Instead of publishing the composition of $\phi_4\phi_3\phi_2\phi_1$ which will be written as a sequence of long quadratic polynomials, we publish the explicit forms of $\phi_3\phi_2$. The polynomials $\{fi\}$ in **Appendix I** are general quadratic polynomials in $x_0, \cdots, x_{i-1}$. The honest attacker should assign explicit forms to $\{fi\}$ and add general linear transformations ϕ_4, ϕ_1 on both sides of $\phi_3\phi_2$.

We will be refrained from comment on **Appendix I**. As for **Appendix II**, we have

- (1) Knowning the lock polynomials, the method of [11] will produce

  a security of 2^{138}.

- (2) Knowning the lock polynomials and the constructing process (i.e., their compact forms), the method of [11] will produce a security of 2^{109}.

The above shows that the example of **Appendix II** is even secured from the inventor using the method of [11].

References

[1] Courtois, N., Shanir, A., Patarin, J., and Klimov, A., *Efficient Algorithm for Solving Overdefined System of Multivariante Polynomial Equations.* Eurocrypt 2000.

[2] Ding, J., Schmidt, D., *A Defect of The Implementation Schemes of The TTM Cryptosystem* http://eprint.iacr.org/2003/086.

[3] Goubin, L., Courtois, N., *Cryptanalysis of TTM.* ASIACRYPT 200, LNCS v1976 pp44-57.

[4] Kipnis, A., Shamir, A., *Cryptanalysis of the HFE Public Key Cryptosystem.* Crypto 1999.

[5] Moh, T. *A Public Key System with Signature and Master Key Functions.* Communications in Algebra, 27(5), 2207-2222 (1999).

[6] Moh, T., Chen, J.M., *On the Goubin-Courtois Attack on TTM.* http://eprint.iacr.org/2001/072.

[7] Moh, T., Chen, J.M., and Yang, B.Y., *Building Instances of TTM Immune to the Goubin-Courtois Attack and the Ding-Schmidt Attack.* http://eprint.iacr.org/2004/168.

[8] Moh, T., *The Recent Attack of Nie et al On TTM is Faulty.* http://eprint.iacr.org/2006/417.

[9] Moh, T., *Relinearization and TTM.* http://www.usdsi.com/ttm.html/ .

[10] Moh, T., *The Mothed of XL and Its inefficient to TTM.* http://eprint/iacr.org/2001/047

[11] Nie, Xuyun., Hu, lei., Li, Jianyu., Updegrove, Crystal., and Ding, Jintai *Breaking a New Instance of TTM Cryptosystems.* ACNS 2006, LNCS 3989, pp. 210-225, 2006.

Appendix I

y0 := x4 x3 + x1 x2 + x0
y1 := x55 x60 + x51 x61 + x50 x62 + x54 x63 + x1
y2 := x71 x76 + x67 x77 + x66 x78 + x70 x79 + x2
y3 := x87 x92 + x83 x93 + x82 x94 + x86 x95 + x3
y4 := x39 x44 + x35 x45 + x34 x46 + x38 x47 + x4
y5 := f5 + x5
y6 := f6 + x6
y7 := f7 + x7
y8 := f8 + x8
y9 := f9 + x9
y10 := f10 + x10
y11 := x4 x5 + x1 x0 + x8 + x11
y12 := f12 + x12
y13 := f13 + x13
y14 := f14 + x14
y15 := f15 + x15
y16 := f16 + x5
y17 := f17 + x6
y18 := f18 + x7
y19 := x4 x17 + x2 x15 + x19
y20 := x1 x17 + x2 x16 + x20
y21 := x14 x5 + x13 x7 + x21
y22 := x14 x0 + x12 x7 + x22
y23 := f23 + x23
y24 := x12 x5 + x13 x0 + x24 + x11
y25 := f25 + x25
y26 := f26 + x26
y27 := x12 x16 + x13 x15 + x24 + x27
y28 := x12 x17 + x18 x15 + x28
y29 := x13 x17 + x18 x16 + x29
y30 := x14 x16 + x13 x23 + x30
y31 := x14 x15 + x12 x23 + x31
y32 := f32 + x32
y33 := f33 + x33
y34 := f34 + x34
y35 := f35 + x35
y36 := f36 + x36
y37 := f37 + x37
y38 := f38 + x38
y39 := f39 + x39
y40 := f40 + x40
y41 := f41 + x41
y42 := f42 + x42
y43 := x32 x37 + x33 x36 + x40 + x43
y44 := x32 x38 + x34 x36 + x44
y45 := x33 x38 + x34 x37 + x45
y46 := x35 x37 + x33 x39 + x46
y47 := x35 x36 + x32 x39 + x47
y48 := f48 + x48
y49 := f49 + x49
y50 := f50 + x50
y51 := f51 + x51
y52 := f52 + x52
y53 := f53 + x53
y54 := f54 + x54
y55 := f55 + x55
y56 := f56 + x56
y57 := f57 + x57
y58 := f58 + x58
y59 := x48 x53 + x49 x52 + x56 + x59
y60 := x48 x54 + x50 x52 + x60
y61 := x49 x54 + x50 x53 + x61
y62 := x51 x53 + x49 x55 + x62
y63 := x51 x52 + x48 x55 + x63
y64 := f64 + x64
y65 := f65 + x65
y66 := f66 + x66
y67 := f67 + x67
y68 := f68 + x68
y69 := f69 + x69
y70 := f70 + x70
y71 := f71 + x71
y72 := f72 + x72
y73 := f73 + x73
y74 := f74 + x74
y75 := x64 x69 + x65 x68 + x72 + x75
y76 := x64 x70 + x66 x68 + x76
y77 := x65 x70 + x66 x69 + x77
y78 := x67 x69 + x65 x71 + x78
y79 := x67 x68 + x64 x71 + x79
y80 := f80 + x80
y81 := f81 + x81
y82 := f82 + x82
y83 := f83 + x83
y84 := f84 + x84
y85 := f85 + x85
y86 := f86 + x86
y87 := f87 + x87
y88 := f88 + x88
y89 := f89 + x89
y90 := f90 + x90
y91 := x80 x85 + x81 x84 + x88 + x91
y92 := x80 x86 + x82 x84 + x92
y93 := x81 x86 + x82 x85 + x93
y94 := x83 x85 + x81 x87 + x94
y95 := x83 x84 + x80 x87 + x95
y96 := f96 + x96
y97 := f97 + x97
y98 := f98 + x98
y99 := f99 + x99
y100 := f100 + x100
y101 := f101 + x101
y102 := f102 + x102
y103 := x4 x6 + x0 x30 + x14
y104 := x1 x6 + x30 x5 + x10
y105 := x23 x5 + x1 x7 + x21
y106 := x0 x23 + x4 x7 + x22
y107 := x4 x16 + x1 x15 + x8 + x27
y108 := x3 x16 + x1 x23 + x30
y109 := x3 x15 + x23 x4 + x31
y110 := x12 x6 + x18 x0 + x28
y111 := x13 x6 + x18 x5 + x29
y112 := x20 x17 + x19 x18 + x2 + x29
y113 := x20 x23 + x8 x18 + x1
y114 := x19 x23 + x8 x17 + x4
y115 := x10 x17 + x19 x14 + x30
y116 := x10 x18 + x20 x14 + x31
y117 := x4 x20 + x1 x19 + x2 x8 + x3 x10
y118 := x0 x21 + x5 x22 + x6 x9 + x7 x11
y119 := x10 x0 + x14 x5 + x6 x8 + x7 x31
y120 := x4 x21 + x1 x22 + x30 x9 + x23 x11
y121 := x10 x22 + x14 x21
y122 := x10 x9 + x8 x21 + x7
y123 := x14 x9 + x8 x22 + x23
y124 := x31 x22 + x14 x11 + x30
y125 := x31 x9 + x8 x11 + x1 + x0
y126 := x23 x6 + x30 x7
y127 := x31 x21 + x10 x11 + x6
y128 := x15 x29 + x16 x28 + x17 x24 + x23 x26
y129 := x12 x30 + x13 x31 + x18 x25 + x14 x27
y130 := x29 x31 + x28 x30

y131 := x29 x25 + x24 x30 + x23
y132 := x28 x25 + x24 x31 + x14
y133 := x26 x31 + x28 x27 + x18
y134 := x26 x25 + x24 x27 + x13 + x15
y135 := x14 x17 + x18 x23
y136 := x26 x30 + x29 x27 + x17
y137 := x15 x20 + x16 x19 + x8 x17 + x23 x10
y138 := x30 x4 + x1 x31 + x2 x25 + x3 x27
y139 := x20 x31 + x19 x30
y140 := x20 x25 + x8 x30 + x23
y141 := x19 x25 + x8 x31 + x3
y142 := x10 x31 + x19 x27 + x2
y143 := x10 x25 + x8 x27 + x1 + x15
y144 := x3 x17 + x2 x23
y145 := x10 x30 + x20 x27 + x17
y146 := x19 x23 + x3 x20 + x2 x30 + x17 x31
y147 := x28 x7 + x14 x29 + x18 x21 + x6 x22
y148 := x0 x29 + x5 x28 + x6 x24 + x7 x26
y149 := x12 x21 + x13 x22 + x18 x9 + x14 x11
y150 := x29 x22 + x28 x21
y151 := x29 x9 + x24 x21 + x7
y152 := x28 x9 + x24 x22 + x14
y153 := x26 x22 + x28 x11 + x18
y154 := x26 x9 + x24 x11 + x13 + x0
y155 := x14 x6 + x18 x7
y156 := x26 x21 + x29 x11 + x6
y157 := x18 x4 + x1 x17 + x2 x23 + x14 x3
y158 := x20 x30 + x19 x31 + x8 x28 + x10 x29
y159 := x4 x31 + x1 x30
y160 := x4 x28 + x2 x30 + x14
y161 := x1 x28 + x2 x31 + x10
y162 := x3 x31 + x1 x29 + x8
y163 := x3 x28 + x2 x29 + x19 + x18
y164 := x23 x10 + x8 x14
y165 := x3 x30 + x4 x29 + x23
y166 := x14 x7 + x23 x10 + x30 x21 + x6 x22
+ x32 x45 + x33 x44 + x34 x40 + x35 x42
y167 := x14 x7 + x23 x10 + x30 x21 + x6 x22
+ x36 x46 + x37 x47 + x38 x41 + x39 x43
y168 := x36 x45 + x37 x44 + x38 x40 + x39 x42
y169 := x32 x46 + x33 x47 + x34 x41 + x35 x43
y170 := x45 x47 + x44 x46
y171 := x45 x41 + x40 x46 + x39
y172 := x44 x41 + x40 x47 + x35
y173 := x42 x47 + x44 x43 + x34
y174 := x42 x41 + x40 x43 + x33 + x36
y175 := x35 x38 + x34 x39
y176 := x42 x46 + x45 x43 + x38
y177 := x14 x7 + x23 x10 + x30 x21 + x6 x22
+ x48 x61 + x49 x60 + x50 x56 + x51 x58
y178 := x14 x7 + x23 x10 + x30 x21 + x6 x22
+ x52 x62 + x53 x63 + x54 x57 + x55 x59
y179 := x52 x61 + x53 x60 + x54 x56 + x55 x58
y180 := x48 x62 + x49 x63 + x50 x57 + x51 x59
y181 := x61 x63 + x60 x62
y182 := x61 x57 + x56 x62 + x55
y183 := x60 x57 + x56 x63 + x51
y184 := x58 x63 + x60 x59 + x50
y185 := x58 x57 + x56 x59 + x49 + x52
y186 := x51 x54 + x50 x55
y187 := x58 x62 + x61 x59 + x54
y188 := x14 x7 + x23 x10 + x30 x21 + x6 x22
+ x64 x77 + x65 x76 + x66 x72 + x67 x74
y189 := x14 x7 + x23 x10 + x30 x21 + x6 x22
+ x68 x78 + x69 x79 + x70 x73 + x71 x75
y190 := x68 x77 + x69 x76 + x70 x72 + x71 x74
y191 := x64 x78 + x65 x79 + x66 x73 + x67 x75
y192 := x77 x79 + x76 x78
y193 := x77 x73 + x72 x78 + x71
y194 := x76 x73 + x72 x79 + x67
y195 := x74 x79 + x76 x75 + x66
y196 := x74 x73 + x72 x75 + x65 + x68
y197 := x67 x70 + x66 x71
y198 := x74 x78 + x77 x75 + x70
y199 := x14 x7 + x23 x10 + x30 x21 + x6 x22
+ x80 x93 + x81 x92 + x82 x88 + x83 x90
y200 := x14 x7 + x23 x10 + x30 x21 + x6 x22
+ x84 x94 + x85 x95 + x86 x89 + x87 x91
y201 := x84 x93 + x85 x92 + x86 x88 + x87 x90
y202 := x80 x94 + x81 x95 + x82 x89 + x83 x91
y203 := x93 x95 + x92 x94
y204 := x93 x89 + x88 x94 + x87
y205 := x92 x89 + x88 x95 + x83
y206 := x90 x95 + x92 x91 + x82
y207 := x90 x89 + x88 x91 + x81 + x84
y208 := x83 x86 + x82 x87
y209 := x90 x94 + x93 x91 + x86

Appendix II

y0 := x1 x4 + x2 x3 + x0
y1 := x96 x100 + x92 x102 + x91 x103 + x95 x104 + x1
y2 := x80 x85 + x76 x86 + x75 x87 + x79 x88 + x2
y3 := x64 x69 + x60 x70 + x59 x71 + x63 x72 + x1 x2 + x3
y4 := x48 x53 + x44 x54 + x43 x55 + x47 x56 + x1 x3 + x2 x3 + x4
y5 := x0 x4 + x1 x2 + x3 x4 + x2 x4 + x2 x3 + x1 x3 + x5
y6 := x5 x0 + x1 x4 + x2 x3 + x5 x1 + x2 x4 + x6
y7 := x6 x0 + x5 x1 + x3 x4 + x2 x6 + x5 x4 + x7
y8 := x7 x1 + x2 x6 + x5 x3 + x4 x7 + x3 x6 + x8
y9 := x8 x0 + x7 x2 + x6 x4 + x5 x1 + x4 x7 + x9
y10 := x9 x0 + x8 x1 + x7 x2 + x3 x6 + x5 x4 + x10
y11 := x6 x10 + x7 x9 + x6 + x9 + x10 + x11
y12 := x5 x10 + x7 x8 + x5 + x8 + x10 + x12
y13 := x5 x9 + x8 x6 + x8 + x9 + x13
y14 := x13 x8 + x12 x9 + x11 x10 + x13 x11 + x12 x7 + x14
y15 := x14 x4 + x13 x5 + x12 x6 + x11 x7 + x10 x8 + x15
y16 := x15 x14 + x13 x12 + x11 x10 + x9 x8 + x7 x6 + x16
y17 := x16 x15 + x14 x5 + x13 x6 + x12 x7 + x11 x8 + x17
y18 := x17 x5 + x16 x10 + x15 x11 + x14 x12 + x13 x6 + x18
y19 := x18 x4 + x17 x6 + x16 x8 + x15 x10 + x14 x12 + x19
y20 := x19 x7 + x18 x9 + x17 x11 + x16 x13 + x15 x8 + x20
y21 := x20 x16 + x19 x14 x18 x12 + x17 x10 + x16 x8 + x21
y22 := x21 x8 + x20 x9 + x19 x10 + x18 x11 + x17 x12 + x22
y23 := x18 x22 + x19 x21 + x18 + x21 + x22 + x23
y24 := x17 x22 + x19 x20 + x17 + x20 + x22 + x24
y25 := x17 x21 + x20 x18 + x20 + x21 + x25
y26 := x25 x11 + x24 x12 + x23 x13 + x22 x14 + x26
y27 := x26 x5 + x25 x7 + x24 x9 + x23 x11 + x22 x13 + x27
y28 := x27 x6 + x26 x8 + x25 x10 + x24 x12 + x23 x14 + x28 + x27 + x26
y29 := x28 x5 + x27 x7 + x26 x9 + x25 x11 + x24 x13 + x29 + x21 + x22
y30 := x29 x15 + x28 x16 + x27 x17 + x26 x18 + x25 x19 + x24 x18 + x30
y31 := x30 x17 + x28 x18 + x26 x19 + x24 x20 + x22 x21 + x23 x6 + x31 + x30 + x29
y32 := x31 x7 + x30 x8 + x29 x9 + x28 x10 + x27 x11 + x26 x12 + x25 x13 + x32 + x27 + x23
y33 := x32 x5 + x31 x6 + x30 x7 + x29 x14 + x28 x15 + x27 x16 + x26 x17 + x33 + x5 + x6
y34 := x33 x20 + x32 x19 + x31 x18 + x30 x17 + x29 x16 + x28 x15 + x34 + x4 + x10 + x11
y35 := x30 x22 + x31 x21 + x30 + x21 + x22 + x35
y36 := x29 x22 + x31 x20 + x29 + x20 + x22 + x36
y37 := x29 x21 + x20 x30 + x20 + x21 + x37
y38 := x33 x7 + x34 x6 + x6 + x33 + x34 + x38
y39 := x32 x7 + x34 x5 + x5 + x32 + x34 + x39
y40 := x32 x6 + x5 x33 + x32 + x33 + x40
y41 := x40 x1 + x39 x3 + x38 x5 + x37 x7 + x36 x9 + x35 x11 + x41 + x40 + x39
y42 := x41 x2 + x40 x4 + x39 x6 + x38 x8 + x37 x10 + x36 x12 + x42 + x38 + x37
y43 := x42 x13 x41 x15 + x40 x17 + x39 x19 + x38 x21 + x37 x23 + x43
y44 := x43 x14 + x42 x26 + x41 x18 + x40 x20 + x39 x22 + x38 x24 + x44 + x43 + x3
y45 := x44 x25 + x43 x27 + x42 x29 + x41 x31 + x40 x33 + x39 x35 + x45 + x8 + x6
y46 := x45 x26 + x44 x28 + x43 x30 + x42 x32 + x41 x34 + x40 x36 + x46 + x40 + x39
y47 := x46 x1 x45 x4 + x44 x7 + x43 x10 + x42 x13 + x41 x16 + x40 x19 + x47 + x3 + x7
y48 := x47 x2 + x46 x5 + x45 x8 + x44 x11 + x43 x14 + x42 x17 + x41 x20 + x48 + x47 + x38
y49 := x48 x3 + x47 x6 + x46 x9 + x45 x12 + x44 x15 + x43 x18 + x42 x21 + x49
y50 := x49 x22 + x48 x25 + x47 x28 + x46 x31 + x45 x34 + x44 x37 + x43 x40 + x50 + x10 + x17
y51 := x50 x23 + x49 x26 + x48 x29 + x47 x32 + x46 x35 + x45 x38 + x44 x41 + x51 + x8 + x22
y52 := x41 x46 + x42 x45 + x49 + x52
y53 := x41 x47 + x43 x45 + x53
y54 := x42 x47 + x43 x46 + x54
y55 := x44 x46 + x42 x48 + x55
y56 := x44 x45 + x41 x48 + x56
y57 := x56 x0 + x55 x5 + x54 x10 + x53 x15 + x52 x20 + x51 x25 + x50 x30 + x57 + x56
y58 := x57 x1 + x56 x6 + x55 x11 + x54 x16 + x53 x21 + x52 x26 + x51 x31 + x58 + x52 + x47
y59 := x55 x2 + x54 x7 + x53 x12 + x52 x17 + x51 x22 + x50 x27 + x49 x32 + x59 + x20 + x15
y60 := x59 x3 + x58 x8 + x57 x13 + x56 x18 + x55 x23 + x54 x28 + x53 x13 + x60 + x2 + x8
y61 := x56 x7 + x44 x8 + x33 x17 + x35 x20 + x40 x22 + x48 x25 + x23 x24 + x60 + x7 + x15
y62 := x61 x20 + x37 x38 + x44 x34 + x57 x9 + x59 x15 + x40 x39 + x60 x2 + x62 + x9 + x35
y63 := x62 x15 + x58 x7 + x37 x13 + x48 x16 + x36 x38 + x27 x44 + x55 x3 + x63 + x44
y64 := x61 x19 + x60 x9 + x54 x17 + x41 x52 + x56 x28 + x3 x6 + x16 x8 + x64 + x23 + x17
y65 := x64 x63 + x34 x56 + x29 x41 + x31 x61 + x55 x37 + x59 x62 + x1 x56 + x65 + x6
y66 := x65 x64 + x1 x27 + x47 x59 + x38 x39 + x48 x50 + x27 x62 + x36 x57 + x66 + x56 + x46
y67 := x65 x63 + x38 x58 + x27 x39 + x37 x59 + x40 x65 + x4 x34 + x15 x46 + x67 + x4 + x16
y68 := x57 x62 + x58 x61 + x65 + x68
y69 := x57 x63 + x59 x61 + x69
y70 := x58 x63 + x59 x62 + x70
y71 := x60 x62 + x58 x64 + x71
y72 := x60 x61 + x57 x64 + x72
y73 := x72 x71 + x70 x69 + x68 x67 + x1 x19 + x25 x70 + x36 x68 + x57 x66 + x73 + x72 + x9
y74 := x73 x5 + x72 x9 + x71 x15 + x68 x3 + x69 x27 + x38 x49 + x40 x70 + x74 + x11 + x21
y75 := x74 x4 + x72 x67 + x36 x68 + x49 x51 + x27 x67 + x39 x44 + x48 x66 + x75 + x12 + x22
y76 := x74 x75 + x49 x27 + x36 x1 + x46 x65 + x70 x6 + x71 x18 + x72 x7 + x76 + x13 + x34
y77 := x76 x0 + x75 x16 + x68 x24 + x74 x69 + x73 x57 + x70 x27 + x69 x17 + x77 + x18 + x29
y78 := x77 x9 + x76 x30 + x75 x73 + x74 x41 + x73 x45 + x68 x53 + x69 x62 + x78 + x12 + x37
y79 := x78 x41 + x77 x31 + x76 x7 + x67 x75 + x39 x51 + x45 x63 + x29 x28 + x79 + x0 + x27 + x49

y80 := x79 x71 + x74 x75 + x76 x77 + x38 x47
+ x45 x62 + x37 x71 + x25 x53 + x80 + x71 + x47
y81 := x80 x72 + x79 x78 + x48 x64 + x78 x5
+ x77 x9 + x71 x36 + x68 x59 + x81 + x80 + x35
y82 := x81 x49 + x79 x26 + x77 x10 + x75 x47
+ x73 x64 + x71 x70 + x79 x3 + x82 + x56 + x49
y83 := x82 x8 + x73 x74 + x81 x69 + x79 x78
+ x35 x61 + x74 x75 + x80 x72 + x83 + x1 + x48
y84 := x73 x78 + x74 x77 + x81 + x84
y85 := x73 x79 + x75 x77 + x85
y86 := x74 x79 + x75 x78 + x86
y87 := x76 x78 + x74 x80 + x87
y88 := x76 x77 + x73 x80 + x88
y89 := x88 x84 + x87 x10 + x86 x29 + x85 x21
+ x83 x19 + x79 x14 + x78 x65 + x89 + x84 + x11
y90 := x89 x11 + x35 x77 + x83 x87 + x84 x27
+ x85 x37 + x86 x47 + x88 x57 + x90 + x85 + x4
y91 := x90 x6 + x88 x15 + x87 x23 + x86 x35
+ x85 x84 + x83 x17 + x79 x34 + x91 + x88 + x43
y92 := x91 x12 + x89 x13 + x90 x14 + x88 x21
+ x87 x31 + x86 x41 + x67 x65 + x92 + x87 + x21
y93 := x92 x24 + x90 x56 + x88 x63 + x86 x54
+ x84 x44 + x79 x56 + x78 x91 + x93 + x89 + x42
y94 := x93 x17 + x86 x26 + x92 x35 + x91 x90
+ x89 x44 + x88 x51 + x87 x66 + x94 + x78 + x3
+ x17
y95 := x94 x11 + x93 x1 + x92 x41 + x91 x55
+ x89 x33 + x88 x71 + x87 x22 + x95 + x1 + x17
+ x29
y96 := x95 x4 + x94 x17 + x93 x29 + x92 x77
+ x91 x76 + x90 x53 + x89 x65 + x96 + x94 + x19
y97 := x96 x5 + x94 x53 + x94 x16 + x92 x88
+ x91 x75 + x90 x62 + x89 x77 + x97 + x7 + x18
y98 := x97 x8 + x96 x17 + x95 x89 + x92 x73
+ x81 x82 + x90 x82 + x89 x84 + x98 + x9 + x27
y99 := x98 x7 + x96 x97 + x95 x23 + x92 x71
+ x81 x90 + x82 x89 + x85 x86 + x99 + x89 + x12
y100 := x95 x89 + x91 x93 + x100
y101 := x89 x94 + x90 x93 + x97 + x101
y102 := x90 x95 + x91 x94 + x102
y103 := x92 x94 + x90 x96 + x103
y104 := x92 x93 + x89 x96 + x104
y105 := x1 x34 + x2 x33 + x1 + x33 + x34 + x105
y106 := x0 x34 + x2 x32 + x0 + x32 + x34 + x106
y107 := x0 x33 + x32 x1 + x32 + x33 + x107
y109 := x4 x19 + x108 x18 + x4 + x108 + x18
+ 1 + x19 + x109
y110 := x3 x19 + x108 x17 + x3 + x108 + x17
+ 1 + x19 + x110
y111 := x3 x18 + x17 x4 + x3 + x4 + x17 + x18
+ x111
y112 := x18 x10 + x19 x9 + x18 + x9 + x10 + x23
y113 := x17 x10 + x19 x8 + x17 + x8 + x10 + x24
y114 := x17 x9 + x8 x18 + x8 + x9 + x25
y115 := x4 x31 + x108 x30 + x4 + x108 + x30
+ 1 + x31 + x109
y116 := x3 x31 + x108 x29 + x3 + x108 + x29
+ 1 + x31 + x110
y117 := x3 x30 + x29 x4 + x3 + x4 + x29 + x30
+ x111
y118 := x1 x22 + x2 x21 + x1 + x21 + x22 + x105
y119 := x0 x22 + x2 x20 + x0 + x20 + x22 + x106
y120 := x0 x21 + x20 x1 + x20 + x21 + x107
y121 := x5 x11 + x12 x6 + x7 x13 + x11 + x12 + x13
+ x0 x105 + x1 x106 + x2 x107 + x105 + x106
+ x107
y122 := x3 x109 + x4 x110 + x108 x111 + x109
+ x110 + x111 + x0 x105 + x1 x106 + x2 x107
+ x105 + x106 + x107
y123 := x29 x35 + x30 x36 + x31 x37 + x35
+ x36 + x37
y124 := x32 x38 + x33 x39 + x34 x40 + x40
y125 := x0 x38 + x1 x39 + x2 x40 + x38 + x39 + x40
y126 := x32 x105 + x33 x106 + x34 x107 + x107
y127 := x105 x39 + x38 x106 + x2 + x34
y128 := x105 x40 + x107 x38 + x1 + x33
y129 := x106 x40 + x107 x39 + x0 + x32
y130 := x17 x23 + x24 x18 + x25 x19 + x23
+ x24 + x25
y131 := x26 x17 + x18 x27 + x19 x28 + x26
+ x27 + x28
y132 := x20 x23 + x21 x24 + x22 x25 + x25
y133 := x23 x27 + x26 x24 + x19 + x22
y134 := x23 x28 + x25 x26 + x18 + x21
y135 := x24 x28 + x25 x27 + x17 + x20
y136 := x14 x5 + x6 x15 + x7 x16 + x14 + x15 + x16
y137 := x11 x8 + x12 x9 + x10 x13 + x13
y138 := x15 x11 + x14 x12 + x7 + x10
y139 := x11 x16 + x13 x14 + x6 + x9
y140 := x12 x16 + x13 x15 + x5 + x8
y141 := x0 x26 + x1 x27 + x2 x28 + x26 + x27 + x28
y142 := x20 x105 + x21 x106 + x22 x107 + x107
y143 := x105 x27 + x26 x106 + x2 + x22
y144 := x105 x28 + x107 x26 + x1 + x21
y145 := x106 x28 + x107 x27 + x0 + x20
y146 := x3 x23 + x4 x24 + x108 x25 + x23
+ x24 + x25
y147 := x17 x109 + x18 x110 + x19 x111 + x109
+ x110 + x111
y148 := x109 x24 + x23 x110 + x108 + x19
y149 := x109 x25 + x111 x23 + x4 + x18 + 1
y150 := x110 x25 + x111 x24 + x3 + x17 + 1
y151 := x3 x35 + x4 x36 + x108 x37 + x35
+ x36 + x37
y152 := x29 x109 + x30 x110 + x31 x111 + x109
+ x110 + x111
y153 := x109 x36 + x35 x110 + x108 + x31
y154 := x109 x37 + x111 x35 + x4 + x30 + 1
y155 := x110 x37 + x111 x36 + x3 + x29 + 1
y156 := x29 x26 + x30 x27 + x31 x28 + x26
+ x27 + x28
y157 := x35 x20 + x21 x36 + x22 x37 + x37
y158 := x35 x27 + x26 x36 + x31 + x22
y159 := x35 x28 + x37 x26 + x30 + x21
y160 := x36 x28 + x37 x27 + x29 + x20
y161 := x32 x11 + x33 x12 + x34 x13 + x13
y162 := x38 x5 + x39 x6 + x7 x40 + x38 + x39 + x40
y163 := x38 x12 + x11 x39 + x34 + x7
y164 := x38 x13 + x40 x11 + x33 + x6
y165 := x39 x13 + x40 x12 + x32 + x5
y166 := x17 x14 + x18 x15 + x19 x16 + x14 + x15
+ x16
y167 := x8 x23 + x24 x9 + x25 x10 + x25
y168 := x23 x15 + x14 x24 + x19 + x10
y169 := x23 x16 + x25 x14 + x18 + x9
y170 := x24 x16 + x25 x15 + x17 + x8
y171 := x41 x54 + x42 x53 + x43 x49 + x44 x51
+ x111 + x110 + x109 + x4 x110 + x108 x111
+ x3 x109
y172 := x45 x55 + x46 x56 + x47 x50 + x48 x52
y173 := x45 x54 + x46 x53 + x47 x49 + x48 x51
y174 := x41 x55 + x42 x56 + x43 x50 + x44 x52

y175 := x54 x56 + x53 x55
y176 := x54 x50 + x49 x55 + x48
y177 := x53 x50 + x49 x56 + x44
y178 := x51 x56 + x53 x52 + x43
y179 := x51 x50 + x49 x52 + x42 + x45
y180 := x44 x47 + x43 x48
y181 := x51 x55 + x54 x52 + x47
y182 := x57 x70 + x58 x69 + x59 x65 + x60 x67
+ x111 + x110 + x109 + x4 x110 + x108 x111
+ x3 x109
y183 := x61 x71 + x62 x72 + x63 x66 + x64 x68
y184 := x61 x70 + x69 x62 + x65 x63 + x64 x67
y185 := x57 x71 + x58 x72 + x59 x66 + x60 x68
y186 := x70 x72 + x69 x71
y187 := x70 x66 + x65 x71 + x64
y188 := x69 x66 + x65 x72 + x60
y189 := x72 x67 + x69 x68 + x59
y190 := x67 x66 + x65 x68 + x58 + x61
y191 := x60 x63 + x59 x64
y192 := x67 x71 + x70 x68 + x63
y193 := x73 x86 + x74 x85 + x75 x81 + x76 x83
+ x111 + x110 + x109 + x4 x110 + x108 x111
+ x3 x109
y194 := x77 x87 + x78 x88 + x79 x82 + x80 x84
y195 := x77 x86 + x78 x85 + x79 x81 + x80 x83
y196 := x73 x87 + x74 x88 + x75 x82 + x76 x84
y197 := x86 x88 + x85 x87
y198 := x86 x82 + x81 x87 + x80
y199 := x85 x82 + x81 x88 + x76
y200 := x83 x88 + x85 x84 + x75
y201 := x83 x82 + x81 x84 + x74 + x77
y202 := x76 x79 + x75 x80
y203 := x83 x87 + x86 x84 + x79
y204 := x89 x102 + x90 x100 + x91 x97 + x92 x99
+ x111 + x110 + x109 + x4 x110 + x108 x111
+ x3 x109
y205 := x93 x103 + x94 x104 + x95 x98 + x96 x101
y206 := x93 x102 + x94 x100 + x95 x97 + x96 x99
y207 := x89 x103 + x90 x104 + x91 x98 + x92 x101
y208 := x102 x104 + x100 x103
y209 := x102 x98 + x97 x103 + x96
y210 := x100 x98 + x97 x104 + x92
y211 := x99 x104 + x100 x101 + x91
y212 := x99 x98 + x97 x101 + x90 + x93
y213 := x92 x95 + x91 x96
y214 := x99 x103 + x102 x101 + x95