Obfuscation : expressions mixtes arithmético-booléennes (MBA)

Alexandre “0poss” Brenner 0poss.github.io

A propos

Alexandre “0poss” Brenner

- Fan de rétro-ingénierie et de logique
- Evangéliste NixOS, Gentoo & Emacs

Shamless plug : `0poss.github.io/Rapport1.pdf`

Au menu

“MBA”, was ist das ?

Expressions linéaires

Expressions polynomiales

Exemple overkill

Attaques

Conclusion

“MBA”, was ist das ?

Expressions mixtes arithmético-booléennes (MBA)

- Mélange d'opérations arithmétiques ($+$, $-$, $\times$, ...) avec des expressions booléennes ($\wedge$, $\vee$, $\neg$, $\oplus$, ...)

Expressions mixtes arithmético-booléennes (MBA)

- Mélange d'opérations arithmétiques ($+$, $-$, $\times$, ...) avec des expressions booléennes ($\wedge$, $\vee$, $\neg$, $\oplus$, ...)

$$x + (y \oplus z)$$

Expressions mixtes arithmético-booléennes (MBA)

- Mélange d'opérations arithmétiques ($+$, $-$, $\times$, ...) avec des expressions booléennes ($\wedge$, $\vee$, $\neg$, $\oplus$, ...)

$$x + (y \oplus z)$$

$$5 \times (x \oplus y)^2 - 3 \times (\neg x \wedge y)$$

Expressions mixtes arithmético-booléennes (MBA)

- Mélange d'opérations arithmétiques ($+$, $-$, $\times$, ...) avec des expressions booléennes ($\wedge$, $\vee$, $\neg$, $\oplus$, ...)

$$x + (y \oplus z)$$

$$5 \times (x \oplus y)^2 - 3 \times (\neg x \wedge y)$$

- Monstre de Frankenstein
  - Croisement entre deux mondes
  - Pas de règle de réduction simple

Expressions mixtes arithmético-booléennes (MBA)

- Objectifs :

Expressions mixtes arithmético-booléennes (MBA)

- Objectifs :
  - Obfuscation de fonctions :

Expressions mixtes arithmético-booléennes (MBA)

- Objectifs :
  - Obfuscation de fonctions :

$$x + y = 2 \times (x \wedge y) - (\neg x \oplus y) - 1$$

Expressions mixtes arithmético-booléennes (MBA)

- Objectifs :
  - Obfuscation de fonctions :

$$x + y = 2 \times (x \wedge y) - (\neg x \oplus y) - 1$$

  - Dissimulation de constantes :

Expressions mixtes arithmético-booléennes (MBA)

- Objectifs :
  - Obfuscation de fonctions :

$$x + y = 2 \times (x \wedge y) - (\neg x \oplus y) - 1$$

  - Dissimulation de constantes : `'ESN'HACK '`

Expressions mixtes arithmético-booléennes (MBA)

- Objectifs :
  - Obfuscation de fonctions :

$$x + y = 2 \times (x \wedge y) - (\neg x \oplus y) - 1$$

  - Dissimulation de constantes : 'ESN'HACK '=

$$121403544221068433 + (7666712018297851300 + (12911658816994541568 + 5423371770071613440 \times \neg(a \oplus b) + 7553537285300420608 \times \neg(\neg a \vee b) + 5423371770071613440 \times (a \vee b) + 5423371770071613440 \times (\neg a \vee \neg b) + 7553537285300420608 \times (\neg a \vee b)) \times (13023493913971338385 + 1088535238210896644 \times \neg(a \oplus b) + 5423173283112440644 \times \neg(\neg a \vee b) + 1088535238210896644 \times (a \vee b) + 1088535238210896644 \times (\neg a \vee \neg b) + 5423173283112440644 \times (\neg a \vee b)) + 12644207112491633356 \times \neg(a \oplus b) + 16780032669580679052 \times \neg(\neg a \vee b) + 12644207112491633356 \times (a \vee b) + 12644207112491633356 \times (\neg a \vee \neg b) + 16780032669580679052 \times (\neg a \vee b)) \times (12308927618052259840 + 1250411442545360896 \times (12911658816994541568 + 5423371770071613440 \times \neg(a \oplus b) + 7553537285300420608 \times \neg(\neg a \vee b) + 5423371770071613440 \times (a \vee b) + 5423371770071613440 \times (\neg a \vee \neg b) + 7553537285300420608 \times (\neg a \vee b)) \times (13023493913971338385 + 1088535238210896644 \times \neg(a \oplus b) + 5423173283112440644 \times \neg(\neg a \vee b) + 1088535238210896644 \times (a \vee b) + 1088535238210896644 \times (\neg a \vee \neg b) + 5423173283112440644 \times (\neg a \vee b)) + 15038082913197359104 \times \neg(a \oplus b) + 6275814991828353024 \times \neg(\neg a \vee b) + 15038082913197359104 \times (a \vee b) + 15038082913197359104 \times (\neg a \vee \neg b) + 6275814991828353024 \times (\neg a \vee b)) + 4115925354337667259 \times (12911658816994541568 + 5423371770071613440 \times \neg(a \oplus b) + 7553537285300420608 \times \neg(\neg a \vee b) + 5423371770071613440 \times (a \vee b) + 5423371770071613440 \times (\neg a \vee \neg b) + 7553537285300420608 \times (\neg a \vee b)) \times (13023493913971338385 + 1088535238210896644 \times \neg(a \oplus b) + 5423173283112440644 \times \neg(\neg a \vee b) + 1088535238210896644 \times (a \vee b) + 1088535238210896644 \times (\neg a \vee \neg b) + 5423173283112440644 \times (\neg a \vee b)) + 552504112576348932 \times \neg(a \oplus b) + 14780961750334198596 \times \neg(\neg a \vee b) + 552504112576348932 \times (a \vee b) + 552504112576348932 \times (\neg a \vee \neg b) + 14780961750334198596 \times (\neg a \vee b)$$

Expressions mixtes arithmético-booléennes (MBA)

- Objectifs :
  - Obfuscation de fonctions :

$$x + y = 2 \times (x \wedge y) - (\neg x \oplus y) - 1$$

  - Dissimulation de constantes : `'ESN'HACK '`$=$
$$121403544221068433 + (7666712018297851300 + (12911658816994541568 + 5423371770071613440 \times \neg(a \oplus b) + 7553537285300420608 \times \neg(\neg a \vee b) + 5423371770071613440 \times (a \vee b) + 5423371770071613440 \times (\neg a \vee \neg b) + 7553537285300420608 \times (\neg a \vee b)) \times (13023493913971338385 + 1088535238210896644 \times \neg(a \oplus b) + 5423173283112440644 \times \neg(\neg a \vee b) + 1088535238210896644 \times (a \vee b) + 1088535238210896644 \times (\neg a \vee \neg b) + 5423173283112440644 \times (\neg a \vee b)) + 12644207112491633356 \times \neg(a \oplus b) + 16780032669580679052 \times \neg(\neg a \vee b) + 12644207112491633356 \times (a \vee b) + 12644207112491633356 \times (\neg a \vee \neg b) + 16780032669580679052 \times (\neg a \vee b)) \times (12308927618052259840 + 1250411442545360896 \times (12911658816994541568 + 5423371770071613440 \times \neg(a \oplus b) + 7553537285300420608 \times \neg(\neg a \vee b) + 5423371770071613440 \times (a \vee b) + 5423371770071613440 \times (\neg a \vee \neg b) + 7553537285300420608 \times (\neg a \vee b)) \times (13023493913971338385 + 1088535238210896644 \times \neg(a \oplus b) + 5423173283112440644 \times \neg(\neg a \vee b) + 1088535238210896644 \times (a \vee b) + 1088535238210896644 \times (\neg a \vee \neg b) + 5423173283112440644 \times (\neg a \vee b)) + 15038082913197359104 \times \neg(a \oplus b) + 6275814991828353024 \times \neg(\neg a \vee b) + 15038082913197359104 \times (a \vee b) + 15038082913197359104 \times (\neg a \vee \neg b) + 6275814991828353024 \times (\neg a \vee b)) + 4115925354337667259 \times (12911658816994541568 + 5423371770071613440 \times \neg(a \oplus b) + 7553537285300420608 \times \neg(\neg a \vee b) + 5423371770071613440 \times (a \vee b) + 5423371770071613440 \times (\neg a \vee \neg b) + 7553537285300420608 \times (\neg a \vee b)) \times (13023493913971338385 + 1088535238210896644 \times \neg(a \oplus b) + 5423173283112440644 \times \neg(\neg a \vee b) + 1088535238210896644 \times (a \vee b) + 1088535238210896644 \times (\neg a \vee \neg b) + 5423173283112440644 \times (\neg a \vee b)) + 552504112576348932 \times \neg(a \oplus b) + 14780961750334198596 \times \neg(\neg a \vee b) + 552504112576348932 \times (a \vee b) + 552504112576348932 \times (\neg a \vee \neg b) + 14780961750334198596 \times (\neg a \vee b)$$

  - Anti-tamper

Expressions mixtes arithmético-booléennes (MBA)

- Objectifs :
  - Obfuscation de fonctions :

$$x + y = 2 \times (x \wedge y) - (\neg x \oplus y) - 1$$

  - Dissimulation de constantes : `'ESN'HACK '`$=$
$$121403544221068433 + (7666712018297851300 + (12911658816994541568 + 5423371770071613440 \times \neg(a \oplus b) + 7553537285300420608 \times \neg(\neg a \vee b) + 5423371770071613440 \times (a \vee b) + 5423371770071613440 \times (\neg a \vee \neg b) + 7553537285300420608 \times (\neg a \vee b)) \times (13023493913971338385 + 1088535238210896644 \times \neg(a \oplus b) + 5423173283112440644 \times \neg(\neg a \vee b) + 1088535238210896644 \times (a \vee b) + 1088535238210896644 \times (\neg a \vee \neg b) + 5423173283112440644 \times (\neg a \vee b)) + 12644207112491633356 \times \neg(a \oplus b) + 16780032669580679052 \times \neg(\neg a \vee b) + 12644207112491633356 \times (a \vee b) + 12644207112491633356 \times (\neg a \vee \neg b) + 16780032669580679052 \times (\neg a \vee b)) \times (12308927618052259840 + 1250411442545360896 \times (12911658816994541568 + 5423371770071613440 \times \neg(a \oplus b) + 7553537285300420608 \times \neg(\neg a \vee b) + 5423371770071613440 \times (a \vee b) + 5423371770071613440 \times (\neg a \vee \neg b) + 7553537285300420608 \times (\neg a \vee b)) \times (13023493913971338385 + 1088535238210896644 \times \neg(a \oplus b) + 5423173283112440644 \times \neg(\neg a \vee b) + 1088535238210896644 \times (a \vee b) + 1088535238210896644 \times (\neg a \vee \neg b) + 5423173283112440644 \times (\neg a \vee b)) + 15038082913197359104 \times \neg(a \oplus b) + 6275814991828353024 \times \neg(\neg a \vee b) + 15038082913197359104 \times (a \vee b) + 15038082913197359104 \times (\neg a \vee \neg b) + 6275814991828353024 \times (\neg a \vee b)) + 4115925354337667259 \times (12911658816994541568 + 5423371770071613440 \times \neg(a \oplus b) + 7553537285300420608 \times \neg(\neg a \vee b) + 5423371770071613440 \times (a \vee b) + 5423371770071613440 \times (\neg a \vee \neg b) + 7553537285300420608 \times (\neg a \vee b)) \times (13023493913971338385 + 1088535238210896644 \times \neg(a \oplus b) + 5423173283112440644 \times \neg(\neg a \vee b) + 1088535238210896644 \times (a \vee b) + 1088535238210896644 \times (\neg a \vee \neg b) + 5423173283112440644 \times (\neg a \vee b)) + 552504112576348932 \times \neg(a \oplus b) + 14780961750334198596 \times \neg(\neg a \vee b) + 552504112576348932 \times (a \vee b) + 552504112576348932 \times (\neg a \vee \neg b) + 14780961750334198596 \times (\neg a \vee b)$$

  - Anti-tamper
  - Watermarking

Expressions linéaires

MBA “linéaires”

- MBA “linéaires” : additionner des expressions booléennes et les multiplier par des constantes.

$$x \times y \qquad x^2 \qquad 11^x$$

$$x \qquad 5 \times (x \oplus y) + z \qquad 9^{14}$$

Génération d'expressions linéaires

MBA linéaires : génération

1. Choix (100% arbitraire) de fonctions booléennes et dressage la table de vérité correspondante dans une matrice :

MBA linéaires : génération

1. Choix (100% arbitraire) de fonctions booléennes et dressage la table de vérité correspondante dans une matrice :

$$x \quad y \quad x \oplus y \quad x \vee y \quad x \wedge y$$

MBA linéaires : génération

1. Choix (100% arbitraire) de fonctions booléennes et dressage la table de vérité correspondante dans une matrice :

$$\begin{array}{cccccc} x & y & x \oplus y & x \vee y & x \wedge y \\ \left[\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{array}\right] \end{array}$$

MBA linéaires : génération

1. Choix (100% arbitraire) de fonctions booléennes et dressage la table de vérité correspondante dans une matrice :

$$\begin{matrix} x & y & x \oplus y & x \vee y & x \wedge y \end{matrix}$$
$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

MBA linéaires : génération

1. Choix (100% arbitraire) de fonctions booléennes et dressage la table de vérité correspondante dans une matrice :

$$\begin{matrix} x & y & x \oplus y & x \vee y & x \wedge y \end{matrix}$$
$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

2. $\Leftrightarrow$ Résoudre le système :

MBA linéaires : génération

1. Choix (100% arbitraire) de fonctions booléennes et dressage la table de vérité correspondante dans une matrice :

$$\begin{array}{cccccc} x & y & x \oplus y & x \vee y & x \wedge y & \\ \left[\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{array}\right. & & & & & \left.\begin{array}{c} \\ \\ \\ \\ \end{array}\right] \end{array} \begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

2. $\Leftrightarrow$ Résoudre le système :

$$\begin{cases} 0a + 0b + 0c + 0d + 0e = 0 \\ 0a + 1b + 1c + 1d + 0e = 0 \\ 1a + 0b + 1c + 1d + 0e = 0 \\ 1a + 1b + 0c + 1d + 1e = 0 \end{cases}$$

MBA linéaires : génération

1. Choix (100% arbitraire) de fonctions booléennes et dressage la table de vérité correspondante dans une matrice :

$$\begin{array}{cccccc} x & y & x \oplus y & x \vee y & x \wedge y & \\ \left[\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{array}\right. & & & & & \left.\begin{array}{c} \\ \\ \\ \\ \end{array}\right] \end{array} \begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

2. $\Leftrightarrow$ Résoudre le système :

$$\begin{cases} 0a + 0b + 0c + 0d + 0e = 0 \\ 0a + 1b + 1c + 1d + 0e = 0 \\ 1a + 0b + 1c + 1d + 0e = 0 \\ 1a + 1b + 0c + 1d + 1e = 0 \end{cases} \Leftrightarrow \begin{cases} a = c - e \\ b = c - e \\ c = c \\ d = -2 \times c + e \\ e = e \end{cases}$$

MBA linéaires : génération

$$\begin{cases} a = c - e \\ b = c - e \\ d = -2 \times c + e \end{cases}$$

MBA linéaires : génération

$$\begin{cases} a = c - e \\ b = c - e \\ d = -2 \times c + e \end{cases}$$

3. Profit ! L'ensemble des solutions génère $E_{c,e}$:

$$(c-e)\times x + (c-e)\times y + c\times(x \oplus y) + (-2c+e)\times(x \vee y) + e\times(x \wedge y) = 0$$

Théorème 1 [zhou2007]

MBA linéaires : génération

A partir de $E_{c,e}$

$$(c-e)\times x+(c-e)\times y+c\times(x\oplus y)+(-2c+e)\times(x\vee y)+e\times(x\wedge y)=0$$

MBA linéaires : génération

A partir de $E_{c,e}$

$$(c-e)\times x+(c-e)\times y+c\times(x\oplus y)+(-2c+e)\times(x\vee y)+e\times(x\wedge y)=0$$

on a $E_{3,1}$:

MBA linéaires : génération

A partir de $E_{c,e}$

$$(c-e)\times x+(c-e)\times y+c\times(x\oplus y)+(-2c+e)\times(x\vee y)+e\times(x\wedge y)=0$$

on a $E_{3,1}$:

$$2x+2y=-3\times(x\oplus y)+5\times(x\vee y)-(x\wedge y)$$

MBA linéaires : génération

A partir de $E_{c,e}$

$$(c-e)\times x+(c-e)\times y+c\times(x\oplus y)+(-2c+e)\times(x\vee y)+e\times(x\wedge y)=0$$

on a $E_{3,1}$:

$$2x+2y=-3\times(x\oplus y)+5\times(x\vee y)-(x\wedge y)$$

avec $E_{3,2}$:

MBA linéaires : génération

A partir de $E_{c,e}$

$$(c-e)\times x+(c-e)\times y+c\times(x\oplus y)+(-2c+e)\times(x\vee y)+e\times(x\wedge y)=0$$

on a $E_{3,1}$:

$$2x+2y=-3\times(x\oplus y)+5\times(x\vee y)-(x\wedge y)$$

avec $E_{3,2}$:

$$y=-x-3\times(x\oplus y)+4\times(x\vee y)-2\times(x\wedge y)$$

MBA linéaires : génération

A partir de $E_{c,e}$

$$(c-e)\times x+(c-e)\times y+c\times(x\oplus y)+(-2c+e)\times(x\vee y)+e\times(x\wedge y)=0$$

on a $E_{3,1}$:

$$2x+2y=-3\times(x\oplus y)+5\times(x\vee y)-(x\wedge y)$$

avec $E_{3,2}$:

$$y=-x-3\times(x\oplus y)+4\times(x\vee y)-2\times(x\wedge y)$$

en réécrivant les y de $E_{-3,1}$ avec $E_{3,2}$:

MBA linéaires : génération

A partir de $E_{c,e}$

$$(c-e)\times x+(c-e)\times y+c\times(x\oplus y)+(-2c+e)\times(x\vee y)+e\times(x\wedge y)=0$$

on a $E_{3,1}$:

$$2x+2y=-3\times(x\oplus y)+5\times(x\vee y)-(x\wedge y)$$

avec $E_{3,2}$:

$$y=-x-3\times(x\oplus y)+4\times(x\vee y)-2\times(x\wedge y)$$

en réécrivant les y de $E_{-3,1}$ avec $E_{3,2}$:

$$2x+2y=-3\times(x\oplus -1\times x+-3\times(x\oplus y)+4\times(x\vee y)+-2\times\neg(\neg x\vee\neg y))+5\times(x\vee -1\times x+-3\times(x\oplus y)+4\times(x\vee y)+-2\times\neg(\neg x\vee\neg y))+-1\times\neg(\neg x\vee\neg(-1\times x+-3\times(x\oplus y)+4\times(x\vee y)+-2\times\neg(\neg x\vee\neg y)))$$

Implémentation

MBA linéaires : LLVM

MBA linéaires : LLVM

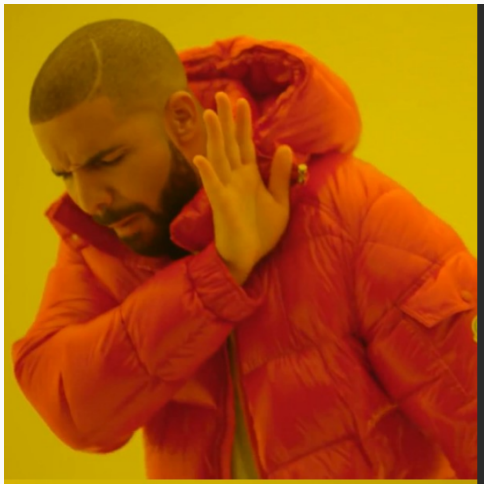
- Pass LLVM : Gauss-Jordan dans $\mathbb{Z}/2^n\mathbb{Z}$

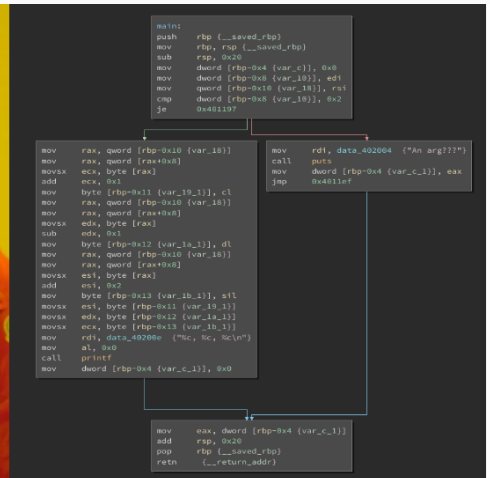
MBA linéaires : LLVM

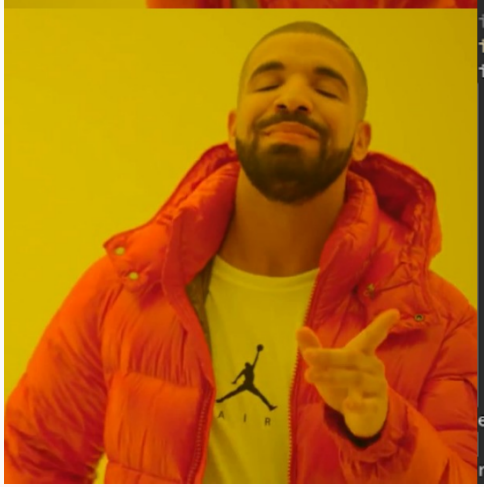
- Pass LLVM : Gauss-Jordan dans $\mathbb{Z}/2^n\mathbb{Z}$
- Introduit gratuitement du polymorphisme au programme (équivalences aléatoires)

MBA linéaires : LLVM

- Pass LLVM : Gauss-Jordan dans $\mathbb{Z}/2^n\mathbb{Z}$
- Introduit gratuitement du polymorphisme au programme (équivalences aléatoires)







```
int32_t var_c = 0
int32_t var_c_1
if (arg1 == 2)
    char rcx_1 = **(arg2 + 8)
    char rdx_7 = (rcx_1 | 1) * 2 + 1 + (((rcx_1 ^ 0xff) | 1) ^ 0xff) * -0x40 + ((rcx_1 ^ 0xff) | 0xfe) * 0 + (rcx_
    int32_t rcx_5 = sx.d(**(arg2 + 8))
    char rsi_25 = (rcx_5 << 1).b + 0xfc + ((rcx_5.b | 0xfe) ^ 0xff) * -0x1e + (((rcx_5.b ^ 0xff) | 1) ^ 0xff) * -0
    char rsi_29 = rsi_25 + ((rcx_5.b | 1) ^ 0xff) * 0 + ((rcx_5.b ^ 0xff) | 0xfe) * 0 + (rcx_5.b ^ 0xfe) * 0 + (rc
    char rsi_33 = rsi_29 + (rcx_5.b | 0xfe) * -0xc + (rcx_5.b ^ 0xff ^ 1) * 0 + (rcx_5.b | 1) * 0x2c + (((rcx_5.b
    int32_t rcx_10 = sx.d(**(arg2 + 8))
    uint64_t r8_14 = zx.q((rcx_10 | 2) * 0xe0413d50)
    char rdi_43 = (rcx_10.b | 0xfd) + 0x4f + (rcx_10.b ^ 2) * 0 + (((rcx_10.b ^ 0xff) | 0xfd) ^ 0xff) * -0x4e + (r
    char* rax_6
    rax_6.b = 0
    printf(format: "%c, %c, %c\n", zx.q(sx.d(rdx_7 + (rcx_1 ^ 0xff ^ 1) * 0 + (rcx_1 ^ 1 ^ 0xff) * -0x50)), zx.q(s
    var_c_1 = 0
else
    var_c_1 = puts(str: "An arg???")
return var_c_1
```

Expressions polynomiales

Expressions polynomiales

- Tous les polynômes - mais seulement les polynômes - sont autorisés.

Expressions polynomiales

- Tous les polynômes - mais seulement les polynômes - sont autorisés.

$$11^x$$

$$x \times (y \oplus z) \qquad x^2 \qquad 9^{14}$$

Polynômes de permutation

Polynômes de permutation

- Propriétés :

Polynômes de permutation

- Propriétés :
  - Bijectifs

Polynômes de permutation

- Propriétés :
  - Bijectifs , donc :

Polynômes de permutation

- Propriétés :
  - Bijectifs , donc :
  - Tous inversibles : il existe un (unique) Q tq. $Q(P(x)) = x$

Polynômes de permutation

- Propriétés :
  - Bijectifs , donc :
  - Tous inversibles : il existe un (unique) Q tq. $Q(P(x)) = x$
- Utilité :

Polynômes de permutation

- Propriétés :
  - Bijectifs , donc :
  - Tous inversibles : il existe un (unique) Q tq. $Q(P(x)) = x$
- Utilité :
  - Runtime : écrire en mémoire avec $P(x)$ au lieu de x et utiliser Q pour la lecture

Polynômes de permutation

- Propriétés :
  - Bijectifs , donc :
  - Tous inversibles : il existe un (unique) Q tq. $Q(P(x)) = x$
- Utilité :
  - Runtime : écrire en mémoire avec $P(x)$ au lieu de x et utiliser Q pour la lecture
  - Transformer une MBA seulement linéaire en MBA polynomiale

Polynômes de permutation

- Propriétés :
  - Bijectifs , donc :
  - Tous inversibles : il existe un (unique) Q tq. $Q(P(x)) = x$
- Utilité :
  - Runtime : écrire en mémoire avec $P(x)$ au lieu de x et utiliser Q pour la lecture
  - Transformer une MBA seulement linéaire en MBA polynomiale
  - Cacher n'importe quel autre polynôme f : développer $Q(K + P(f))$, avec $K = 0$ une MBA

Exemple overkill

Exemple

- $c = 1337$

Constante à cacher

Exemple

- $c = 1337$

  Constante à cacher

- $P(x) = 9543x^{16} + 31922x^{15} + 49485x^{14} + 3577x^{13} + 7115x^{12} + 50138x^{11} + 45503x^{10} + 25130x^{9} + 37449x^{8} + 47827x^{7} + 58867x^{6} + 13758x^{5} + 12731x^{4} + 61184x^{3} + 39973x^{2} + 6235x^{1} + 42377$

  $Q(x) = 65524x^{15} + 5x^{14} + 65481x^{13} + 54x^{12} + 65506x^{11} + 128x^{10} + 65201x^{9} + 203x^{8} + 65533x^{7} + 1193x^{6} + 2028x^{5} + 6888x^{4} + 35087x^{3} + 7345x^{2} + 52609x^{1} + 1175$

  Génération d'un PP et de son inverse

Exemple

- $c = 1337$

  Constante à cacher

- $P(x) = 9543x^{16} + 31922x^{15} + 49485x^{14} + 3577x^{13} + 7115x^{12} + 50138x^{11} + 45503x^{10} + 25130x^{9} + 37449x^{8} + 47827x^{7} + 58867x^{6} + 13758x^{5} + 12731x^{4} + 61184x^{3} + 39973x^{2} + 6235x^{1} + 42377$

  $Q(x) = 65524x^{15} + 5x^{14} + 65481x^{13} + 54x^{12} + 65506x^{11} + 128x^{10} + 65201x^{9} + 203x^{8} + 65533x^{7} + 1193x^{6} + 2028x^{5} + 6888x^{4} + 35087x^{3} + 7345x^{2} + 52609x^{1} + 1175$

  Génération d'un PP et de son inverse

- $P(1337) = 56662$

  Encodage de c

Exemple

- $c = 1337$

  Constante à cacher

- $P(x) = 9543x^{16} + 31922x^{15} + 49485x^{14} + 3577x^{13} + 7115x^{12} + 50138x^{11} + 45503x^{10} + 25130x^{9} + 37449x^{8} + 47827x^{7} + 58867x^{6} + 13758x^{5} + 12731x^{4} + 61184x^{3} + 39973x^{2} + 6235x^{1} + 42377$

  $Q(x) = 65524x^{15} + 5x^{14} + 65481x^{13} + 54x^{12} + 65506x^{11} + 128x^{10} + 65201x^{9} + 203x^{8} + 65533x^{7} + 1193x^{6} + 2028x^{5} + 6888x^{4} + 35087x^{3} + 7345x^{2} + 52609x^{1} + 1175$

  Génération d'un PP et de son inverse

- $P(1337) = 56662$

  Encodage de c

- $K(x, y, z) = P(1337) =$

Exemple

- $c = 1337$

  Constante à cacher

- $P(x) = 9543x^{16} + 31922x^{15} + 49485x^{14} + 3577x^{13} + 7115x^{12} + 50138x^{11} + 45503x^{10} + 25130x^{9} + 37449x^{8} + 47827x^{7} + 58867x^{6} + 13758x^{5} + 12731x^{4} + 61184x^{3} + 39973x^{2} + 6235x^{1} + 42377$

  $Q(x) = 65524x^{15} + 5x^{14} + 65481x^{13} + 54x^{12} + 65506x^{11} + 128x^{10} + 65201x^{9} + 203x^{8} + 65533x^{7} + 1193x^{6} + 2028x^{5} + 6888x^{4} + 35087x^{3} + 7345x^{2} + 52609x^{1} + 1175$

  Génération d'un PP et de son inverse

- $P(1337) = 56662$

  Encodage de c

- $K(x, y, z) = P(1337) = 8965 \times (x \oplus y) + 11115 \times (x \wedge y) + 6815 \times (\neg(x \vee y)) + 8104 \times (\neg x) + 2150 \times (\neg y) + -18406 \times (z) + 18406 \times (y \wedge z) + 5954 \times (x \vee z) + -5954 \times ((\neg x) \wedge z) + -18406 \times (y \vee (\neg z))$

  MBA linéaire constante

Exemple

- $c = 1337$

  Constante à cacher

- $P(x) = 9543x^{16} + 31922x^{15} + 49485x^{14} + 3577x^{13} + 7115x^{12} + 50138x^{11} + 45503x^{10} + 25130x^{9} + 37449x^{8} + 47827x^{7} + 58867x^{6} + 13758x^{5} + 12731x^{4} + 61184x^{3} + 39973x^{2} + 6235x^{1} + 42377$

  $Q(x) = 65524x^{15} + 5x^{14} + 65481x^{13} + 54x^{12} + 65506x^{11} + 128x^{10} + 65201x^{9} + 203x^{8} + 65533x^{7} + 1193x^{6} + 2028x^{5} + 6888x^{4} + 35087x^{3} + 7345x^{2} + 52609x^{1} + 1175$

  Génération d'un PP et de son inverse

- $P(1337) = 56662$

  Encodage de c

- $K(x, y, z) = P(1337) = 8965 \times (x \oplus y) + 11115 \times (x \wedge y) + 6815 \times (\neg(x \vee y)) + 8104 \times (\neg x) + 2150 \times (\neg y) + -18406 \times (z) + 18406 \times (y \wedge z) + 5954 \times (x \vee z) + -5954 \times ((\neg x) \wedge z) + -18406 \times (y \vee (\neg z))$

  MBA linéaire constante

- $K'(x, y, z) = P(1337) =$

Exemple

- $c = 1337$

  Constante à cacher

- $P(x) = 9543x^{16} + 31922x^{15} + 49485x^{14} + 3577x^{13} + 7115x^{12} + 50138x^{11} + 45503x^{10} + 25130x^{9} + 37449x^{8} + 47827x^{7} + 58867x^{6} + 13758x^{5} + 12731x^{4} + 61184x^{3} + 39973x^{2} + 6235x^{1} + 42377$

  $Q(x) = 65524x^{15} + 5x^{14} + 65481x^{13} + 54x^{12} + 65506x^{11} + 128x^{10} + 65201x^{9} + 203x^{8} + 65533x^{7} + 1193x^{6} + 2028x^{5} + 6888x^{4} + 35087x^{3} + 7345x^{2} + 52609x^{1} + 1175$

  Génération d'un PP et de son inverse

- $P(1337) = 56662$

  Encodage de c

- $K(x, y, z) = P(1337) = 8965 \times (x \oplus y) + 11115 \times (x \wedge y) + 6815 \times (\neg(x \vee y)) + 8104 \times (\neg x) + 2150 \times (\neg y) + -18406 \times (z) + 18406 \times (y \wedge z) + 5954 \times (x \vee z) + -5954 \times ((\neg x) \wedge z) + -18406 \times (y \vee (\neg z))$

  MBA linéaire constante

- $K'(x, y, z) = P(1337) =$
  $35091 \times (x \wedge y) \times (x \oplus y) + 5572 \times (x \oplus y) \times \neg(x \vee y) + 56500 \times (x \oplus y) \times \neg x + 57113 \times (x \oplus y) \times \neg y + 38767 \times z \times (x \oplus y) + 47844 \times (y \wedge z) \times (x \oplus y) + 6609 \times (x \vee z) \times (x \oplus y) + 37206 \times (\neg x \wedge z) \times (x \oplus y) + 38575 \times (y \vee \neg z) \times (x \oplus y) + 15790 \times (x \wedge y) \times \neg(x \vee y) + 21002 \times (x \wedge y) \times \neg x + 22022 \times (x \wedge y) \times \neg y + 6712 \times z \times (x \wedge y) + 50091 \times (x \wedge y) \times (y \wedge z) + 19401 \times (x \wedge y) \times (x \vee z) + 50194 \times (x \wedge y) \times (\neg x \wedge z) + 33677 \times (x \wedge y) \times (y \vee \neg z) + 52861 \times \neg x \times \neg(x \vee y) + 62685 \times \neg y \times \neg(x \vee y) + 3760 \times z \times \neg(x \vee y) + 47123 \times (y \wedge z) \times \neg(x \vee y) + 49735 \times (x \vee z) \times \neg(x \vee y) + 33836 \times (\neg x \wedge z) \times \neg(x \vee y) + 41947 \times (y \vee \neg z) \times \neg(x \vee y) + 34397 \times \neg x \times \neg y + 37142 \times z \times \neg x + 7319 \times (y \wedge z) \times \neg x + 13199 \times (x \vee z) \times \neg x + 12581 \times (\neg x \wedge z) \times \neg x + 37334 \times (y \vee \neg z) \times \neg x + 7100 \times z \times \neg y + 28628 \times (y \wedge z) \times \neg y + 47596 \times (x \vee z) \times \neg y + 43720 \times (\neg x \wedge z) \times \neg y + 34257 \times (y \vee \neg z) \times \neg y + 40760 \times z \times (x \vee z) + 20717 \times z \times (\neg x \wedge z) + 33509 \times (y \wedge z) \times (x \vee z) + 36086 \times (y \wedge z) \times (\neg x \wedge z) + 13795 \times (x \vee z) \times (y \vee \neg z) + 47682 \times (\neg x \wedge z) \times (y \vee \neg z)$

  Obf. des coefficients de K avec d'autres MBA constantes

Exemple

- $c = 1337$

  Constante à cacher

- $P(x) = 9543x^{16} + 31922x^{15} + 49485x^{14} + 3577x^{13} + 7115x^{12} + 50138x^{11} + 45503x^{10} + 25130x^{9} + 37449x^{8} + 47827x^{7} + 58867x^{6} + 13758x^{5} + 12731x^{4} + 61184x^{3} + 39973x^{2} + 6235x^{1} + 42377$

  $Q(x) = 65524x^{15} + 5x^{14} + 65481x^{13} + 54x^{12} + 65506x^{11} + 128x^{10} + 65201x^{9} + 203x^{8} + 65533x^{7} + 1193x^{6} + 2028x^{5} + 6888x^{4} + 35087x^{3} + 7345x^{2} + 52609x^{1} + 1175$

  Génération d'un PP et de son inverse

- $P(1337) = 56662$

  Encodage de c

- $K(x, y, z) = P(1337) = 8965 \times (x \oplus y) + 11115 \times (x \wedge y) + 6815 \times (\neg(x \vee y)) + 8104 \times (\neg x) + 2150 \times (\neg y) + -18406 \times (z) + 18406 \times (y \wedge z) + 5954 \times (x \vee z) + -5954 \times ((\neg x) \wedge z) + -18406 \times (y \vee (\neg z))$

  MBA linéaire constante

- $K'(x, y, z) = P(1337) =$
  $35091 \times (x \wedge y) \times (x \oplus y) + 5572 \times (x \oplus y) \times \neg(x \vee y) + 56500 \times (x \oplus y) \times \neg x + 57113 \times (x \oplus y) \times \neg y + 38767 \times z \times (x \oplus y) + 47844 \times (y \wedge z) \times (x \oplus y) + 6609 \times (x \vee z) \times (x \oplus y) + 37206 \times (\neg x \wedge z) \times (x \oplus y) + 38575 \times (y \vee \neg z) \times (x \oplus y) + 15790 \times (x \wedge y) \times \neg(x \vee y) + 21002 \times (x \wedge y) \times \neg x + 22022 \times (x \wedge y) \times \neg y + 6712 \times z \times (x \wedge y) + 50091 \times (x \wedge y) \times (y \wedge z) + 19401 \times (x \wedge y) \times (x \vee z) + 50194 \times (x \wedge y) \times (\neg x \wedge z) + 33677 \times (x \wedge y) \times (y \vee \neg z) + 52861 \times \neg x \times \neg(x \vee y) + 62685 \times \neg y \times \neg(x \vee y) + 3760 \times z \times \neg(x \vee y) + 47123 \times (y \wedge z) \times \neg(x \vee y) + 49735 \times (x \vee z) \times \neg(x \vee y) + 33836 \times (\neg x \wedge z) \times \neg(x \vee y) + 41947 \times (y \vee \neg z) \times \neg(x \vee y) + 34397 \times \neg x \times \neg y + 37142 \times z \times \neg x + 7319 \times (y \wedge z) \times \neg x + 13199 \times (x \vee z) \times \neg x + 12581 \times (\neg x \wedge z) \times \neg x + 37334 \times (y \vee \neg z) \times \neg x + 7100 \times z \times \neg y + 28628 \times (y \wedge z) \times \neg y + 47596 \times (x \vee z) \times \neg y + 43720 \times (\neg x \wedge z) \times \neg y + 34257 \times (y \vee \neg z) \times \neg y + 40760 \times z \times (x \vee z) + 20717 \times z \times (\neg x \wedge z) + 33509 \times (y \wedge z) \times (x \vee z) + 36086 \times (y \wedge z) \times (\neg x \wedge z) + 13795 \times (x \vee z) \times (y \vee \neg z) + 47682 \times (\neg x \wedge z) \times (y \vee \neg z)$

  Obf. des coefficients de K avec d'autres MBA constantes

- $Q(K') = 1337 =$

  Décodage

$$1175+35091\times(x\wedge y)\times(x\oplus y)+5572\times(x\oplus y)\times\neg(x\vee y)+56500\times(x\oplus y)\times\neg x+57113\times(x\oplus y)\times\neg y+38767\times z\times(x\oplus y)+47844\times(y\wedge z)\times(x\oplus y)+6609\times(x\vee z)\times(x\oplus y)+37206\times(\neg x\wedge z)\times(x\oplus y)+38575\times(y\vee\neg z)\times(x\oplus y)+15790\times(x\wedge y)\times\neg(x\vee y)+21002\times(x\wedge y)\times\neg x+22022\times(x\wedge y)\times\neg y+6712\times z\times(x\wedge y)+50091\times(x\wedge y)\times(y\wedge z)+19401\times(x\wedge y)\times(x\vee z)+50194\times(x\wedge y)\times(\neg x\wedge z)+33677\times(x\wedge y)\times(y\vee\neg z)+52861\times\neg x\times\neg(x\vee y)+62685\times\neg y\times\neg(x\vee y)+3760\times z\times\neg(x\vee y)+47123\times(y\wedge z)\times\neg(x\vee y)+49735\times(x\vee z)\times\neg(x\vee y)+33836\times(\neg x\wedge z)\times\neg(x\vee y)+41947\times(y\vee\neg z)\times\neg(x\vee y)+34397\times\neg x\times\neg y+37142\times z\times\neg x+7319\times(y\wedge z)\times\neg x+13199\times(x\vee z)\times\neg x+12581\times(\neg x\wedge z)\times\neg x+37334\times(y\vee\neg z)\times\neg x+7100\times z\times\neg y+28628\times(y\wedge z)\times\neg y+47596\times(x\vee z)\times\neg y+43720\times(\neg x\wedge z)\times\neg y+34257\times(y\vee\neg z)\times\neg y+40760\times z\times(x\vee z)+20717\times z\times(\neg x\wedge z)+33509\times(y\wedge z)\times(x\vee z)+36086\times(y\wedge z)\times(\neg x\wedge z)+13795\times(x\vee z)\times(y\vee\neg z)+47682\times(\neg x\wedge z)\times(y\vee\neg z)\times(52609+35091\times(x\wedge y)\times(x\oplus y)+5572\times(x\oplus y)\times\neg(x\vee y)+56500\times(x\oplus y)\times\neg x+57113\times(x\oplus y)\times\neg y+38767\times z\times(x\oplus y)+47844\times(y\wedge z)\times(x\oplus y)+6609\times(x\vee z)\times(x\oplus y)+37206\times(\neg x\wedge z)\times(x\oplus y)+38575\times(y\vee\neg z)\times(x\oplus y)+15790\times(x\wedge y)\times\neg(x\vee y)+21002\times(x\wedge y)\times\neg x+22022\times(x\wedge y)\times\neg y+6712\times z\times(x\wedge y)+50091\times(x\wedge y)\times(y\wedge z)+19401\times(x\wedge y)\times(x\vee z)+50194\times(x\wedge y)\times(\neg x\wedge z)+33677\times(x\wedge y)\times(y\vee\neg z)+52861\times\neg x\times\neg(x\vee y)+62685\times\neg y\times\neg(x\vee y)+3760\times z\times\neg(x\vee y)+47123\times(y\wedge z)\times\neg(x\vee y)+49735\times(x\vee z)\times\neg(x\vee y)+33836\times(\neg x\wedge z)\times\neg(x\vee y)+41947\times(y\vee\neg z)\times\neg(x\vee y)+34397\times\neg x\times\neg y+37142\times z\times\neg x+7319\times(y\wedge z)\times\neg x+13199\times(x\vee z)\times\neg x+12581\times(\neg x\wedge z)\times\neg x+37334\times(y\vee\neg z)\times\neg x+7100\times z\times\neg y+28628\times(y\wedge z)\times\neg y+47596\times(x\vee z)\times\neg y+43720\times(\neg x\wedge z)\times\neg y+34257\times(y\vee\neg z)\times\neg y+40760\times z\times(x\vee z)+20717\times z\times(\neg x\wedge z)+33509\times(y\wedge z)\times(x\vee z)+36086\times(y\wedge z)\times(\neg x\wedge z)+13795\times(x\vee z)\times(y\vee\neg z)+47682\times(\neg x\wedge z)\times(y\vee\neg z)\times(7345+35091\times(x\wedge y)\times(x\oplus y)+5572\times(x\oplus y)\times\neg(x\vee y)+56500\times(x\oplus y)\times\neg x+57113\times(x\oplus y)\times\neg y+38767\times z\times(x\oplus y)+47844\times(y\wedge z)\times(x\oplus y)+6609\times(x\vee z)\times(x\oplus y)+37206\times(\neg x\wedge z)\times(x\oplus y)+38575\times(y\vee\neg z)\times(x\oplus y)+15790\times(x\wedge y)\times\neg(x\vee y)+21002\times(x\wedge y)\times\neg x+22022\times(x\wedge y)\times\neg y+6712\times z\times(x\wedge y)+50091\times(x\wedge y)\times(y\wedge z)+19401\times(x\wedge y)\times(x\vee z)+50194\times(x\wedge y)\times(\neg x\wedge z)+33677\times(x\wedge y)\times(y\vee\neg z)+52861\times\neg x\times\neg(x\vee y)+62685\times\neg y\times\neg(x\vee y)+3760\times z\times\neg(x\vee y)+47123\times(y\wedge z)\times\neg(x\vee y)+49735\times(x\vee z)\times\neg(x\vee y)+33836\times(\neg x\wedge z)\times\neg(x\vee y)+41947\times(y\vee\neg z)\times\neg(x\vee y)+34397\times\neg x\times\neg y+37142\times z\times\neg x+7319\times(y\wedge z)\times\neg x+13199\times(x\vee z)\times\neg x+12581\times(\neg x\wedge z)\times\neg x+37334\times(y\vee\neg z)\times\neg x+7100\times z\times\neg y+28628\times(y\wedge z)\times\neg y+47596\times(x\vee z)\times\neg y+43720\times(\neg x\wedge z)\times\neg y+34257\times(y\vee\neg z)\times\neg y+40760\times z\times(x\vee z)+20717\times z\times(\neg x\wedge z)+33509\times(y\wedge z)\times(x\vee z)+36086\times(y\wedge z)\times(\neg x\wedge z)+13795\times(x\vee z)\times(y\vee\neg z)+47682\times(\neg x\wedge z)\times(y\vee\neg z)\times(6888+35091\times(x\wedge y)\times(x\oplus y)+5572\times(x\oplus y)\times\neg(x\vee y)+56500\times(x\oplus y)\times\neg x+57113\times(x\oplus y)\times\neg y+38767\times z\times(x\oplus y)+47844\times(y\wedge z)\times(x\oplus y)+6609\times(x\vee z)\times(x\oplus y)+37206\times(\neg x\wedge z)\times(x\oplus y)+38575\times(y\vee\neg z)\times(x\oplus y)+15790\times(x\wedge y)\times\neg(x\vee y)+21002\times(x\wedge y)\times\neg x+22022\times(x\wedge y)\times\neg y+6712\times z\times(x\wedge y)+50091\times(x\wedge y)\times(y\wedge z)+19401\times(x\wedge y)\times(x\vee z)+50194\times(x\wedge y)\times(\neg x\wedge z)+33677\times(x\wedge y)\times(y\vee\neg z)+52861\times\neg x\times\neg(x\vee y)+62685\times\neg y\times\neg(x\vee y)+3760\times z\times\neg(x\vee y)+47123\times(y\wedge z)\times\neg(x\vee y)+49735\times(x\vee z)\times\neg(x\vee y)+33836\times(\neg x\wedge z)\times\neg(x\vee y)+41947\times(y\vee\neg z)\times\neg(x\vee y)+34397\times\neg x\times\neg y+37142\times z\times\neg x+7319\times(y\wedge z)\times\neg x+13199\times(x\vee z)\times\neg x+12581\times(\neg x\wedge z)\times\neg x+37334\times(y\vee\neg z)\times\neg x+7100\times z\times\neg y+28628\times(y\wedge z)\times\neg y+47596\times(x\vee z)\times\neg y+43720\times(\neg x\wedge z)\times\neg y+34257\times(y\vee\neg z)\times\neg y+40760\times z\times(x\vee z)+20717\times z\times(\neg x\wedge z)+33509\times(y\wedge z)\times(x\vee z)+36086\times(y\wedge z)\times(\neg x\wedge z)+13795\times(x\vee z)\times(y\vee\neg z)+47682\times(\neg x\wedge z)\times(y\vee\neg z)\times(2028+35091\times(x\wedge y)\times(x\oplus y)+5572\times(x\oplus y)\times\neg(x\vee y)+56500\times(x\oplus y)\times\neg x+57113\times(x\oplus y)\times\neg y+38767\times z\times(x\oplus y)+47844\times(y\wedge z)\times(x\oplus y)+6609\times(x\vee z)\times(x\oplus y)+37206\times(\neg x\wedge z)\times(x\oplus y)+38575\times(y\vee\neg z)\times(x\oplus y)+15790\times(x\wedge y)\times\neg(x\vee y)+21002\times(x\wedge y)\times\neg x+22022\times(x\wedge y)\times\neg y+6712\times z\times(x\wedge y)+50091\times(x\wedge y)\times(y\wedge z)+19401\times(x\wedge y)\times(x\vee z)+50194\times(x\wedge y)\times(\neg x\wedge z)+33677\times(x\wedge y)\times(y\vee\neg z)+52861\times\neg x\times\neg(x\vee y)+62685\times\neg y\times\neg(x\vee y)+3760\times z\times\neg(x\vee y)+47123\times(y\wedge z)\times\neg(x\vee y)+49735\times(x\vee z)\times\neg(x\vee y)+33836\times(\neg x\wedge z)\times\neg(x\vee y)+41947\times(y\vee\neg z)\times\neg(x\vee y)+34397\times\neg x\times\neg y+37142\times z\times\neg x+7319\times(y\wedge z)\times\neg x+13199\times(x\vee z)\times\neg x+12581\times(\neg x\wedge z)\times\neg x+37334\times(y\vee\neg z)\times\neg x+7100\times z\times\neg y+28628\times(y\wedge z)\times\neg y+47596\times(x\vee z)\times\neg y+43720\times(\neg x\wedge z)\times\neg y+34257\times(y\vee\neg z)\times\neg y+40760\times z\times(x\vee z)+20717\times z\times(\neg x\wedge z)+33509\times(y\wedge z)\times(x\vee z)+36086\times(y\wedge z)\times(\neg x\wedge z)+13795\times(x\vee z)\times(y\vee\neg z)+47682\times(\neg x\wedge z)\times(y\vee\neg z)\times(1193+35091\times(x\wedge y)\times(x\oplus y)+5572\times(x\oplus y)\times\neg(x\vee y)+56500\times(x\oplus y)\times\neg x+57113\times(x\oplus y)\times\neg y+38767\times z\times(x\oplus y)+47844\times(y\wedge z)\times(x\oplus y)+6609\times(x\vee z)\times(x\oplus y)+37206\times(\neg x\wedge z)\times(x\oplus y)+38575\times(y\vee\neg z)\times(x\oplus y)+15790\times(x\wedge y)\times\neg(x\vee y)+21002\times(x\wedge y)\times\neg x+22022\times(x\wedge y)\times\neg y+6712\times z\times(x\wedge y)+50091\times(x\wedge y)\times(y\wedge z)+19401\times(x\wedge y)\times(x\vee z)+50194\times(x\wedge y)\times(\neg x\wedge z)+33677\times(x\wedge y)\times(y\vee\neg z)+52861\times\neg x\times\neg(x\vee y)+62685\times\neg y\times\neg(x\vee y)+3760\times z\times\neg(x\vee y)+47123\times(y\wedge z)\times\neg(x\vee y)+49735\times(x\vee z)\times\neg(x\vee y)+33836\times(\neg x\wedge z)\times\neg(x\vee y)+41947\times(y\vee\neg z)\times\neg(x\vee y)+34397\times\neg x\times\neg y+37142\times z\times\neg x+7319\times(y\wedge z)\times\neg x+13199\times(x\vee z)\times\neg x+12581\times(\neg x\wedge z)\times\neg x+37334\times(y\vee\neg z)\times\neg x+7100\times z\times\neg y+28628\times(y\wedge z)\times\neg y+47596\times(x\vee z)\times\neg y+43720\times(\neg x\wedge z)\times\neg y+34257\times(y\vee\neg z)\times\neg y+40760\times z\times(x\vee z)+20717\times z\times(\neg x\wedge z)+33509\times(y\wedge z)\times(x\vee z)+36086\times(y\wedge z)\times(\neg x\wedge z)+13795\times(x\vee z)\times(y\vee\neg z)+47682\times(\neg x\wedge z)\times(y\vee\neg z)\times(65533+35091\times(x\wedge y)\times(x\oplus y)+5572\times(x\oplus y)\times\neg(x\vee y)+56500\times(x\oplus y)\times\neg x+57113\times(x\oplus y)\times\neg y+38767\times z\times(x\oplus y)+47844\times(y\wedge z)\times(x\oplus y)+6609\times(x\vee z)\times(x\oplus y)+37206\times(\neg x\wedge z)\times(x\oplus y)+38575\times(y\vee\neg z)\times(x\oplus y)+15790\times(x\wedge y)\times\neg(x\vee y)+21002\times(x\wedge y)\times\neg x+22022\times(x\wedge y)\times\neg y+6712\times z\times(x\wedge y)+50091\times(x\wedge y)\times(y\wedge z)+19401\times(x\wedge y)\times(x\vee z)+50194\times(x\wedge y)\times(\neg x\wedge z)+33677\times(x\wedge y)\times(y\vee\neg z)+52861\times\neg x\times\neg(x\vee y)+62685\times\neg y\times\neg(x\vee y)+3760\times z\times\neg(x\vee y)+47123\times(y\wedge z)\times\neg(x\vee y)+49735\times(x\vee z)\times\neg(x\vee y)+33836\times(\neg x\wedge z)\times\neg(x\vee y)+41947\times(y\vee\neg z)\times\neg(x\vee y)+34397\times\neg x\times\neg y+37142\times z\times\neg x+7319\times(y\wedge z)\times\neg x+13199\times(x\vee z)\times\neg x+12581\times(\neg x\wedge z)\times\neg x+37334\times(y\vee\neg z)\times\neg x+7100\times z\times\neg y+28628\times(y\wedge z)\times\neg y+47596\times(x\vee z)\times\neg y+43720\times(\neg x\wedge z)\times\neg y+34257\times(y\vee\neg z)\times\neg y+40760\times z\times(x\vee z)+20717\times z\times(\neg x\wedge z)+33509\times(y\wedge z)\times(x\vee z)+36086\times(y\wedge z)\times(\neg x\wedge z)+13795\times(x\vee z)\times(y\vee\neg z)+47682\times(\neg x\wedge z)\times(y\vee\neg z)\times(203+35091\times(x\wedge y)\times(x\oplus y)+5572\times(x\oplus y)\times\neg(x\vee y)+56500\times(x\oplus y)\times\neg x+57113\times(x\oplus y)\times\neg y+38767\times z\times(x\oplus y)+47844\times(y\wedge z)\times(x\oplus y)+6609\times(x\vee z)\times(x\oplus y)+37206\times(\neg x\wedge z)\times(x\oplus y)+38575\times(y\vee\neg z)\times(x\oplus y)+15790\times(x\wedge y)\times\neg(x\vee y)+21002\times(x\wedge y)\times\neg x+22022\times(x\wedge y)\times\neg y+6712\times z\times(x\wedge y)+50091\times(x\wedge y)\times(y\wedge z)+19401\times(x\wedge y)\times(x\vee z)+50194\times(x\wedge y)\times(\neg x\wedge z)+33677\times(x\wedge y)\times(y\vee\neg z)+52861\times\neg x\times\neg(x\vee y)+62685\times\neg y\times\neg(x\vee y)+3760\times z\times\neg(x\vee y)+47123\times(y\wedge z)\times\neg(x\vee y)+49735\times(x\vee z)\times\neg(x\vee y)+33836\times(\neg x\wedge z)\times\neg(x\vee y)+41947\times(y\vee\neg z)\times\neg(x\vee y)+34397\times\neg x\times\neg y+37142\times z\times\neg x+7319\times(y\wedge z)\times\neg x+13199\times(x\vee z)\times\neg x+12581\times(\neg x\wedge z)\times\neg x+37334\times(y\vee\neg z)\times\neg x+7100\times z\times\neg y+28628\times(y\wedge z)\times\neg y+47596\times(x\vee z)\times\neg y+43720\times(\neg x\wedge z)\times\neg y+34257\times(y\vee\neg z)\times\neg y+40760\times z\times(x\vee z)+20717\times z\times(\neg x\wedge z)+33509\times(y\wedge z)\times(x\vee z)+36086\times(y\wedge z)\times(\neg x\wedge z)+13795\times(x\vee z)\times(y\vee\neg z)+47682\times(\neg x\wedge z)\times(y\vee\neg z)\times(65205+35091\times(x\wedge y)\times(x\oplus y)+5572\times(x\oplus y)\times\neg(x\vee y)+56500\times(x\oplus y)\times\neg x+57113\times(x\oplus y)\times\neg y+38767\times z\times(x\oplus y)+47844\times(y\wedge z)\times(x\oplus y)+6609\times(x\vee z)\times(x\oplus y)+37206\times(\neg x\wedge z)\times(x\oplus y)+38575\times(y\vee\neg z)\times(x\oplus y)+15790\times(x\wedge y)\times\neg(x\vee y)+21002\times(x\wedge y)\times\neg x+22022\times(x\wedge y)\times\neg y+6712\times z\times(x\wedge y)+50091\times(x\wedge y)\times(y\wedge z)+19401\times(x\wedge y)\times(x\vee z)+50194\times(x\wedge y)\times(\neg x\wedge z)+33677\times(x\wedge y)\times(y\vee\neg z)+52861\times\neg x\times\neg(x\vee y)+62685\times\neg y\times\neg(x\vee y)+3760\times z\times\neg(x\vee y)+47123\times(y\wedge z)\times\neg(x\vee y)+49735\times(x\vee z)\times\neg(x\vee y)+33836\times(\neg x\wedge z)\times\neg(x\vee y)+41947\times(y\vee\neg z)\times\neg(x\vee y)+34397\times\neg x\times\neg y+37142\times z\times\neg x+7319\times(y\wedge z)\times\neg x+13199\times(x\vee z)\times\neg x+12581\times(\neg x\wedge z)\times\neg x+37334\times(y\vee\neg z)\times\neg x+7100\times z\times\neg y+28628\times(y\wedge z)\times\neg y+47596\times(x\vee z)\times\neg y+43720\times(\neg x\wedge z)\times\neg y+34257\times(y\vee\neg z)\times\neg y+40760\times z\times(x\vee z)+20717\times z\times(\neg x\wedge z)+33509\times(y\wedge z)\times(x\vee z)+36086\times(y\wedge z)\times(\neg x\wedge z)+13795\times(x\vee z)\times(y\vee\neg z)+47682\times(\neg x\wedge z)\times(y\vee\neg z)\times(54+35091\times(x\wedge y)\times(x\oplus y)+5572\times(x\oplus y)\times\neg(x\vee y)+56500\times(x\oplus y)\times\neg x+57113\times(x\oplus y)\times\neg y+38767\times z\times(x\oplus y)+47844\times(y\wedge z)\times(x\oplus y)+6609\times(x\vee z)\times(x\oplus y)+37206\times(\neg x\wedge z)\times(x\oplus y)+38575\times(y\vee\neg z)\times(x\oplus y)+15790\times(x\wedge y)\times\neg(x\vee y)+21002\times(x\wedge y)\times\neg x+22022\times(x\wedge y)\times\neg y+6712\times z\times(x\wedge y)+50091\times(x\wedge y)\times(y\wedge z)+19401\times(x\wedge y)\times(x\vee z)+50194\times(x\wedge y)\times(\neg x\wedge z)+33677\times(x\wedge y)\times(y\vee\neg z)+52861\times\neg x\times\neg(x\vee y)+62685\times\neg y\times\neg(x\vee y)+3760\times z\times\neg(x\vee y)+47123\times(y\wedge z)\times\neg(x\vee y)+49735\times(x\vee z)\times\neg(x\vee y)+33836\times(\neg x\wedge z)\times\neg(x\vee y)+41947\times(y\vee\neg z)\times\neg(x\vee y)+34397\times\neg x\times\neg y+37142\times z\times\neg x+7319\times(y\wedge z)\times\neg x+13199\times(x\vee z)\times\neg x+12581\times(\neg x\wedge z)\times\neg x+37334\times(y\vee\neg z)\times\neg x+7100\times z\times\neg y+28628\times(y\wedge z)\times\neg y+47596\times(x\vee z)\times\neg y+43720\times(\neg x\wedge z)\times\neg y+34257\times(y\vee\neg z)\times\neg y+40760\times z\times(x\vee z)+20717\times z\times(\neg x\wedge z)+33509\times(y\wedge z)\times(x\vee z)+36086\times(y\wedge z)\times(\neg x\wedge z)+13795\times(x\vee z)\times(y\vee\neg z)+47682\times(\neg x\wedge z)\times(y\vee\neg z)\times(61481+35091\times(x\wedge y)\times(x\oplus y)+5572\times(x\oplus y)\times\neg(x\vee y)+56500\times(x\oplus y)\times\neg x+57113\times(x\oplus y)\times\neg y+38767\times z\times(x\oplus y)+47844\times(y\wedge z)\times(x\oplus y)+6609\times(x\vee z)\times(x\oplus y)+37206\times(\neg x\wedge z)\times(x\oplus y)+38575\times(y\vee\neg z)\times(x\oplus y)+15790\times(x\wedge y)\times\neg(x\vee y)+21002\times(x\wedge y)\times\neg x+22022\times(x\wedge y)\times\neg y+6712\times z\times(x\wedge y)+50091\times(x\wedge y)\times(y\wedge z)+19401\times(x\wedge y)\times(x\vee z)+50194\times(x\wedge y)\times(\neg x\wedge z)+33677\times(x\wedge y)\times(y\vee\neg z)+52861\times\neg x\times\neg(x\vee y)+62685\times\neg y\times\neg(x\vee y)+3760\times z\times\neg(x\vee y)+47123\times(y\wedge z)\times\neg(x\vee y)+49735\times(x\vee z)\times\neg(x\vee y)+33836\times(\neg x\wedge z)\times\neg(x\vee y)+41947\times(y\vee\neg z)\times\neg(x\vee y)+34397\times\neg x\times\neg y+37142\times z\times\neg x+7319\times(y\wedge z)\times\neg x+13199\times(x\vee z)\times\neg x+12581\times(\neg x\wedge z)\times\neg x+37334\times(y\vee\neg z)\times\neg x+7100\times z\times\neg y+28628\times(y\wedge z)\times\neg y+47596\times(x\vee z)\times\neg y+43720\times(\neg x\wedge z)\times\neg y+34257\times(y\vee\neg z)\times\neg y+40760\times z\times(x\vee z)+20717\times z\times(\neg x\wedge z)+33509\times(y\wedge z)\times(x\vee z)+36086\times(y\wedge z)\times(\neg x\wedge z)+13795\times(x\vee z)\times(y\vee\neg z)+47682\times(\neg x\wedge z)\times(y\vee\neg z)\times65524)))))))))))))$$

Attaques

Déobfuscation/simplification de MBA

Déobfuscation/simplification de MBA

- Inversion pour les polynômes de permutation.

Déobfuscation/simplification de MBA

- Inversion pour les polynômes de permutation.
- Bit-blasting avec **Arybo**

Déobfuscation/simplification de MBA

- Inversion pour les polynômes de permutation.
- Bit-blasting avec **Arybo** trop lent avec les expressions trop grandes (souvent une grosse multiplication suffi à casser le tool)

Déobfuscation/simplification de MBA

- Inversion pour les polynômes de permutation.
- Bit-blasting avec **Arybo** trop lent avec les expressions trop grandes (souvent une grosse multiplication suffi à casser le tool)
- Synthèse de programme stochastique I/O-based avec **Xyntia**

Déobfuscation/simplification de MBA

- Inversion pour les polynômes de permutation.
- Bit-blasting avec **Arybo** trop lent avec les expressions trop grandes (souvent une grosse multiplication suffi à casser le tool)
- Synthèse de programme stochastique I/O-based avec **Xyntia** a du mal avec les expressions trop complexes

Déobfuscation/simplification de MBA

- Inversion pour les polynômes de permutation.
- Bit-blasting avec **Arybo** trop lent avec les expressions trop grandes (souvent une grosse multiplication suffi à casser le tool)
- Synthèse de programme stochastique I/O-based avec **Xyntia** a du mal avec les expressions trop complexes
- Simplification d'AST par synthèse de programme avec oracle avec **QSynthesis**

Déobfuscation/simplification de MBA

- Inversion pour les polynômes de permutation.
- Bit-blasting avec **Arybo** trop lent avec les expressions trop grandes (souvent une grosse multiplication suffi à casser le tool)
- Synthèse de programme stochastique I/O-based avec **Xyntia** a du mal avec les expressions trop complexes
- Simplification d'AST par synthèse de programme avec oracle avec **QSynthesis** good

Déobfuscation/simplification de MBA

- Inversion pour les polynômes de permutation.
- Bit-blasting avec **Arybo** trop lent avec les expressions trop grandes (souvent une grosse multiplication suffi à casser le tool)
- Synthèse de programme stochastique I/O-based avec **Xyntia** a du mal avec les expressions trop complexes
- Simplification d'AST par synthèse de programme avec oracle avec **QSynthesis** good mais sensible aux opérateurs commutatifs et associatifs

Déobfuscation/simplification de MBA

- Inversion pour les polynômes de permutation.
- Bit-blasting avec **Arybo** trop lent avec les expressions trop grandes (souvent une grosse multiplication suffi à casser le tool)
- Synthèse de programme stochastique I/O-based avec **Xyntia** a du mal avec les expressions trop complexes
- Simplification d'AST par synthèse de programme avec oracle avec **QSynthesis** good mais sensible aux opérateurs commutatifs et associatifs
- Projection de N-bit vers 1-bit avec **MBA-solver**

Déobfuscation/simplification de MBA

- Inversion pour les polynômes de permutation.
- Bit-blasting avec **Arybo** trop lent avec les expressions trop grandes (souvent une grosse multiplication suffi à casser le tool)
- Synthèse de programme stochastique I/O-based avec **Xyntia** a du mal avec les expressions trop complexes
- Simplification d'AST par synthèse de programme avec oracle avec **QSynthesis** good mais sensible aux opérateurs commutatifs et associatifs
- Projection de N-bit vers 1-bit avec **MBA-solver** très prometteur

Déobfuscation/simplification de MBA

- Inversion pour les polynômes de permutation.
- Bit-blasting avec **Arybo** trop lent avec les expressions trop grandes (souvent une grosse multiplication suffi à casser le tool)
- Synthèse de programme stochastique I/O-based avec **Xyntia** a du mal avec les expressions trop complexes
- Simplification d'AST par synthèse de programme avec oracle avec **QSynthesis** good mais sensible aux opérateurs commutatifs et associatifs
- Projection de N-bit vers 1-bit avec **MBA-solver** très prometteur mais que pour les expressions linéaires

Déobfuscation/simplification de MBA

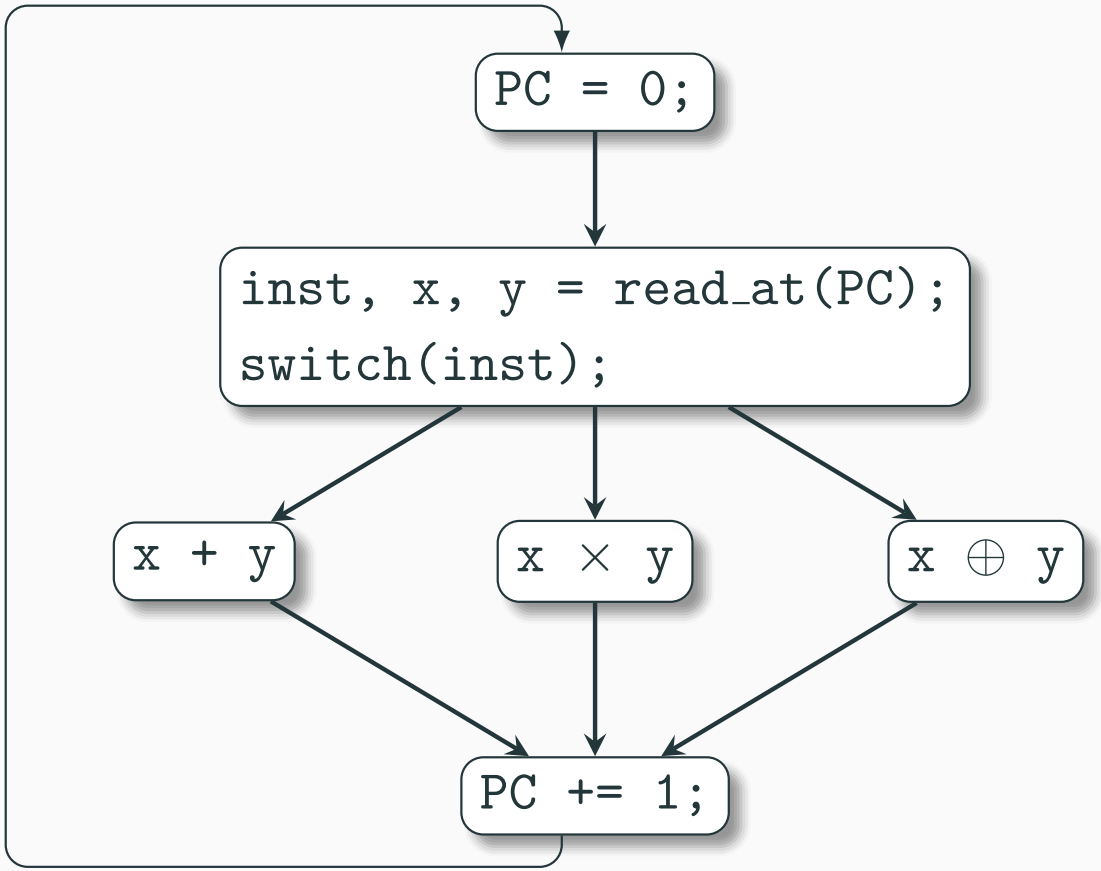
- Inversion pour les polynômes de permutation.
- Bit-blasting avec **Arybo** trop lent avec les expressions trop grandes (souvent une grosse multiplication suffi à casser le tool)
- Synthèse de programme stochastique I/O-based avec **Xyntia** a du mal avec les expressions trop complexes
- Simplification d'AST par synthèse de programme avec oracle avec **QSynthesis** good mais sensible aux opérateurs commutatifs et associatifs
- Projection de N-bit vers 1-bit avec **MBA-solver** très prometteur mais que pour les expressions linéaires
- Réseau de neurones sur les chaînes de caractères avec **NeuReduce**

Déobfuscation/simplification de MBA

- Inversion pour les polynômes de permutation.
- Bit-blasting avec **Arybo** trop lent avec les expressions trop grandes (souvent une grosse multiplication suffi à casser le tool)
- Synthèse de programme stochastique I/O-based avec **Xyntia** a du mal avec les expressions trop complexes
- Simplification d'AST par synthèse de programme avec oracle avec **QSynthesis** good mais sensible aux opérateurs commutatifs et associatifs
- Projection de N-bit vers 1-bit avec **MBA-solver** très prometteur mais que pour les expressions linéaires
- Réseau de neurones sur les chaînes de caractères avec **NeuReduce** "sur les chaînes de caractères", **sérieux ?**

Merci !

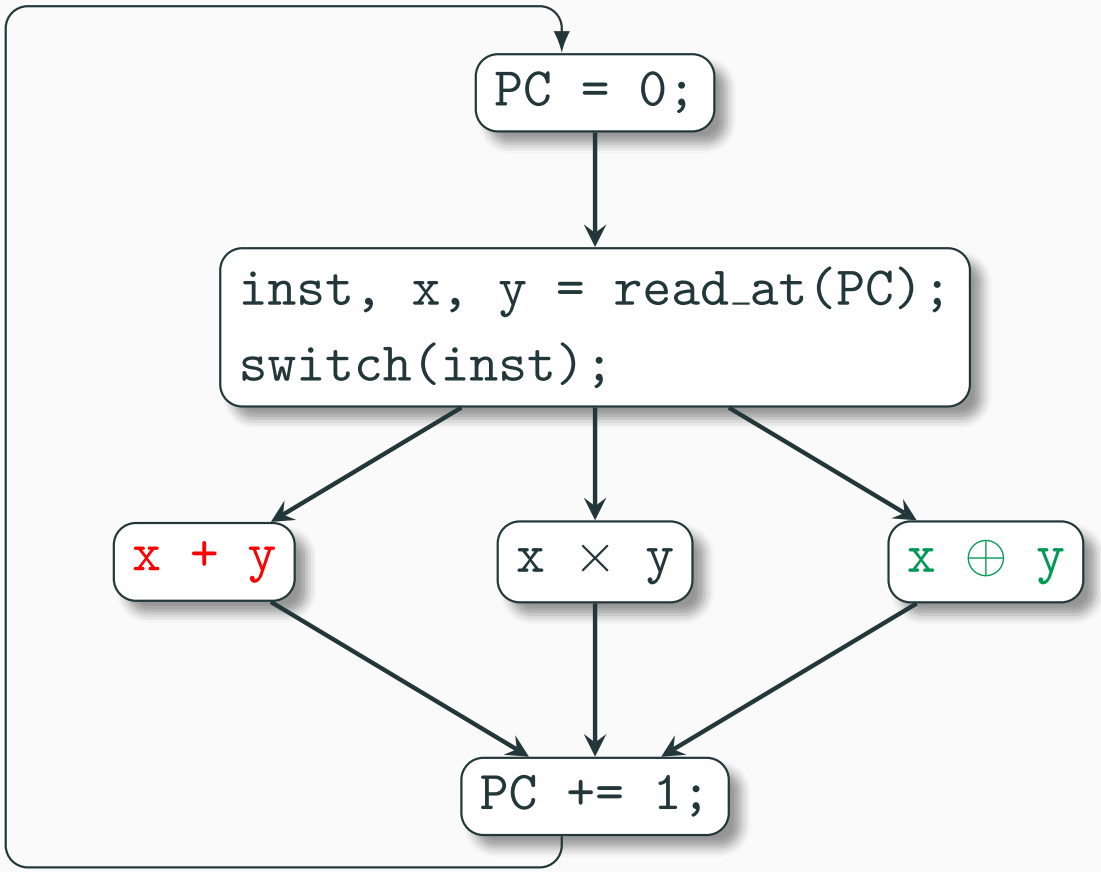
Complexifier la virtualisation



Complexifier la virtualisation : entrelacement de handlers

$$E_{3,2} : x + y = -3 \times (x \oplus y) + 4 \times (x \vee y) - 2 \times (x \wedge y)$$

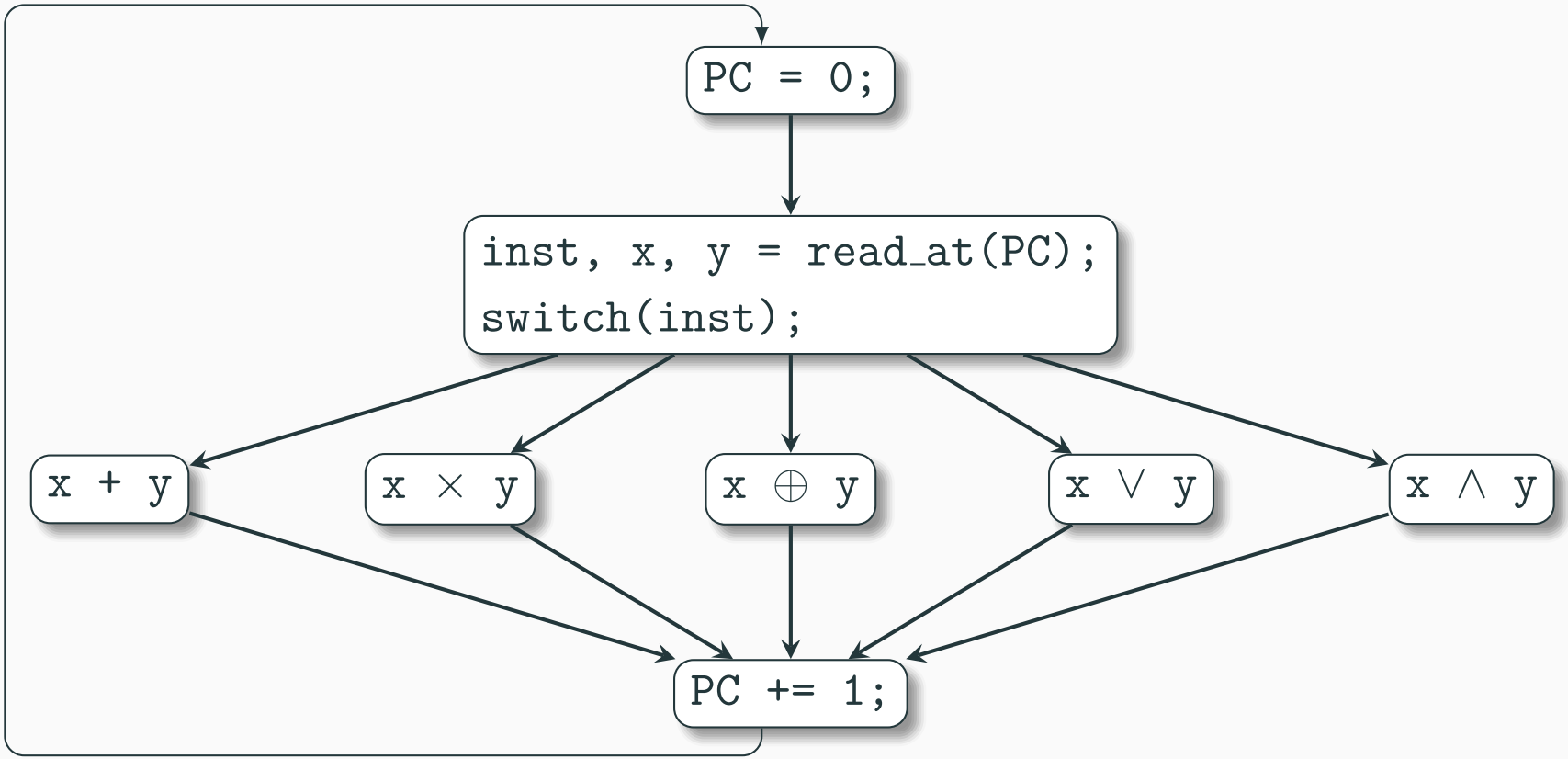
$$E_{1,7} : x \oplus y = 6 \times x + 6 \times y - 5 \times (x \vee y) - 7 \times (x \wedge y)$$



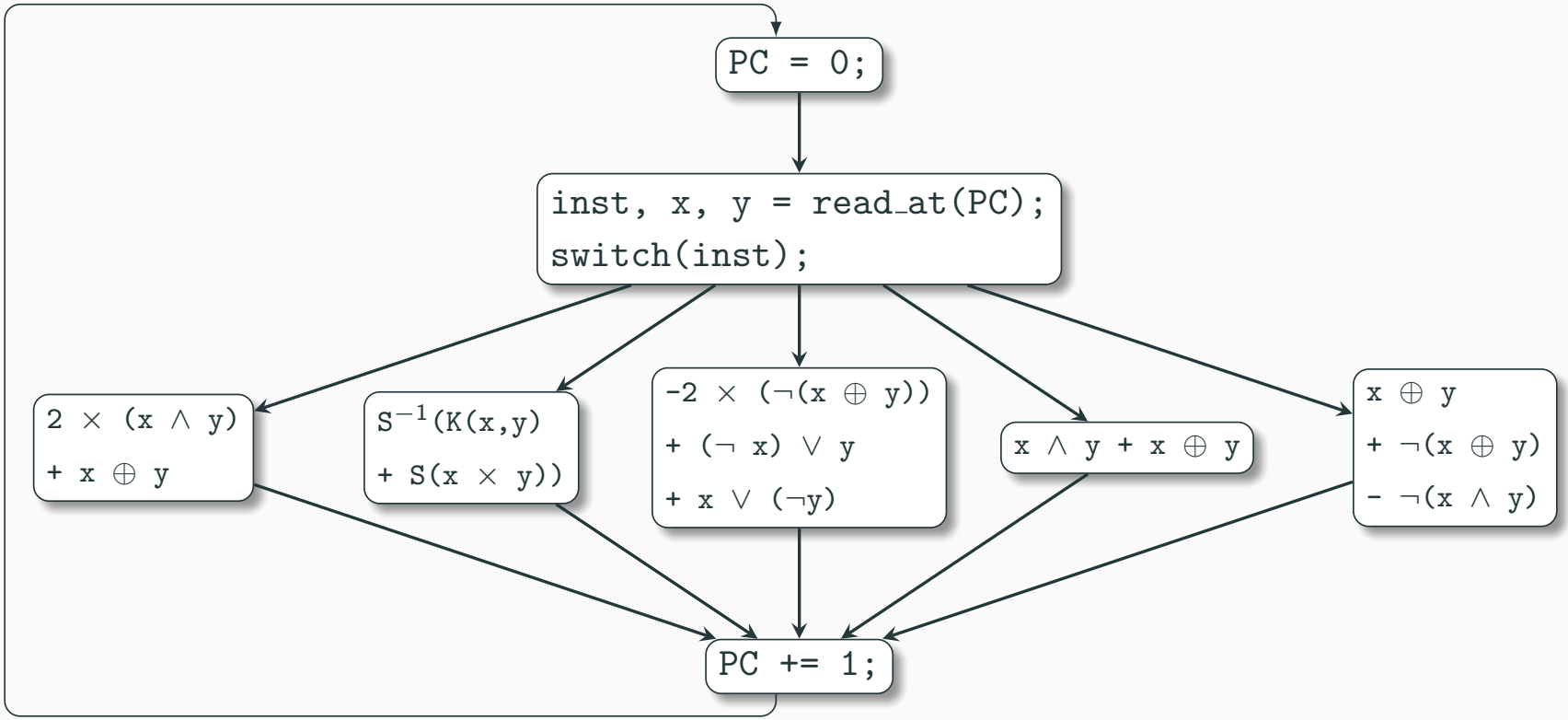
Complexifier la virtualisation : entrelacement de handlers

$$E_{3,2} : x + y = -3 \times (x \oplus y) + 4 \times (x \vee y) - 2 \times (x \wedge y)$$

$$E_{1,7} : x \oplus y = 6 \times x + 6 \times y - 5 \times (x \vee y) - 7 \times (x \wedge y)$$



Complexifier la virtualisation : obfuscation des handlers



Complexifier la virtualisation : dispatching polynomial