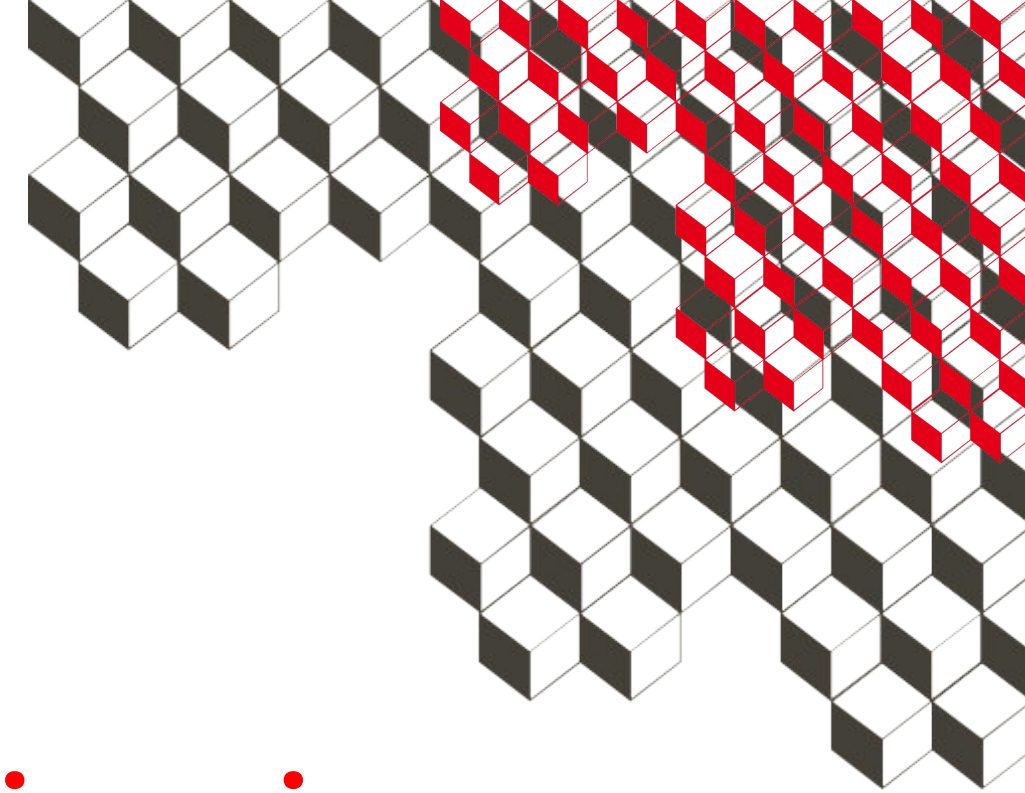
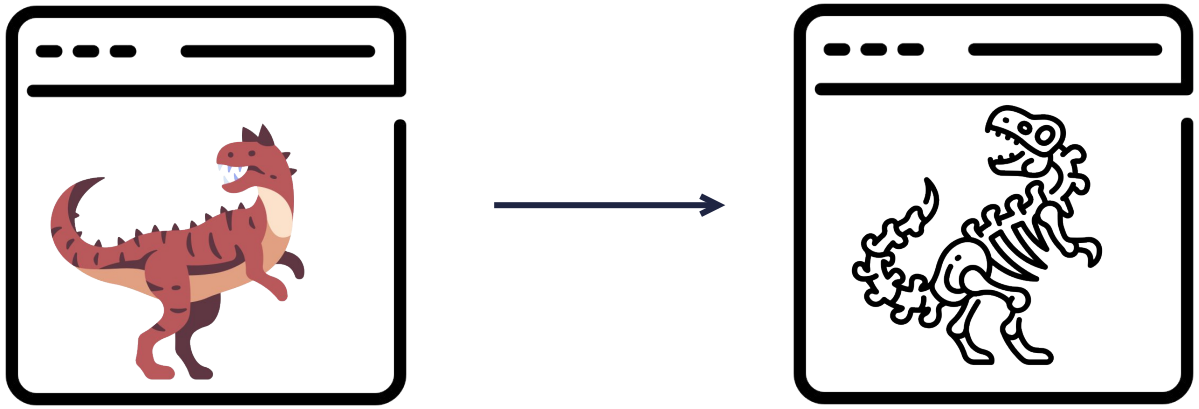


Program Synthesis for Binary Code Reverse Engineering

Grégoire Menguy (CEA LIST)

What is Reverse Engineering?



Understand how a software works internally

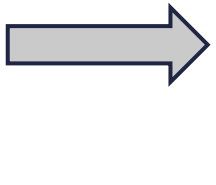
for Malware analysis

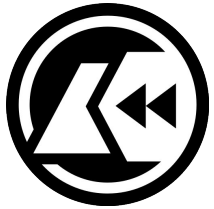
for Code refactoring

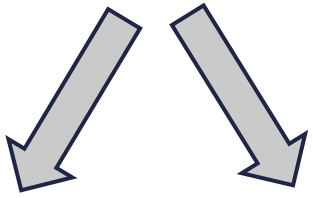
for Code documentation

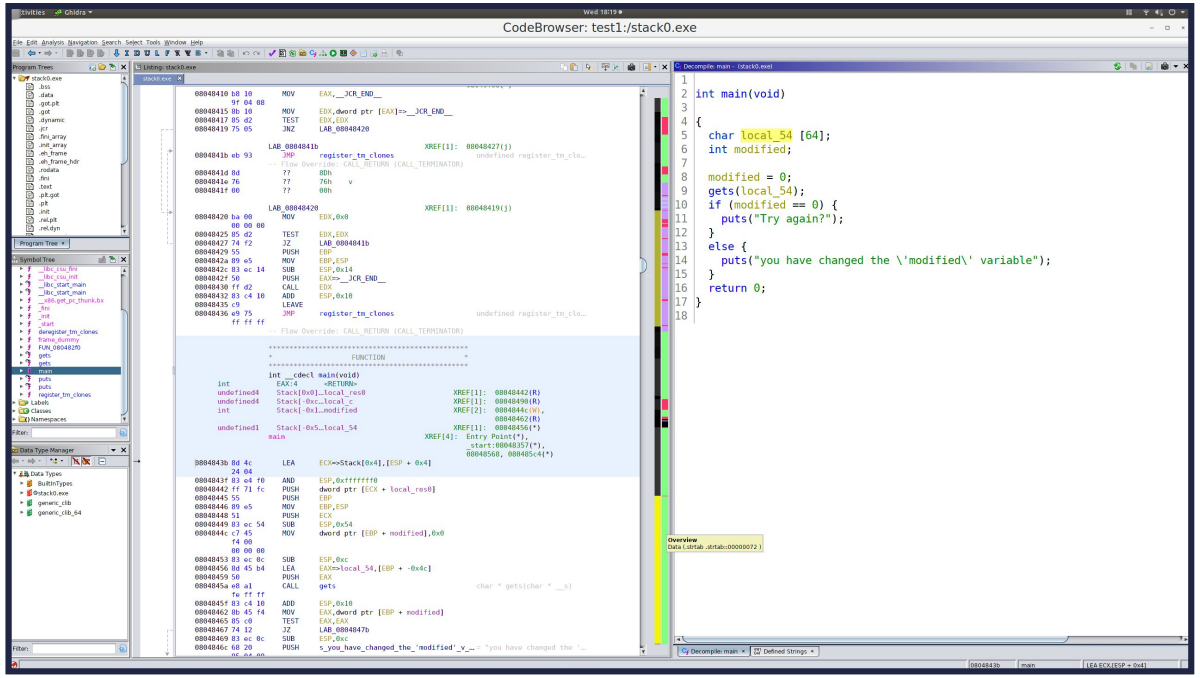
How to Do Reverse Engineering ?

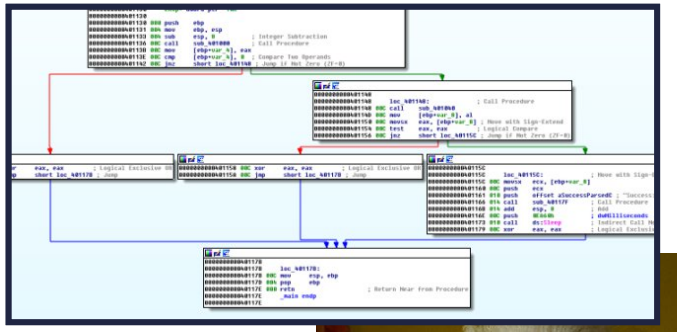
Already interresting questions :
- How to desassemble ?
- How to decompile ?
- How to unstrip ?

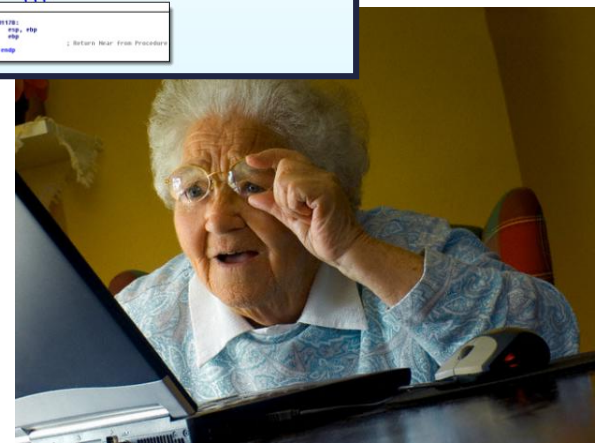








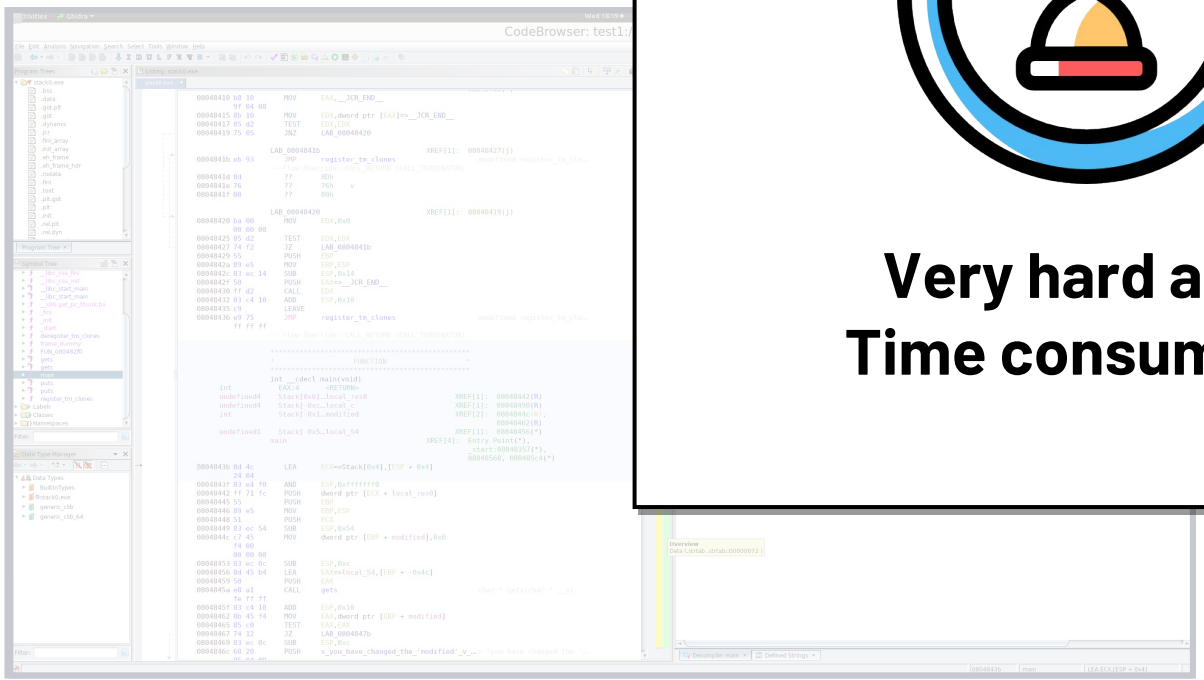


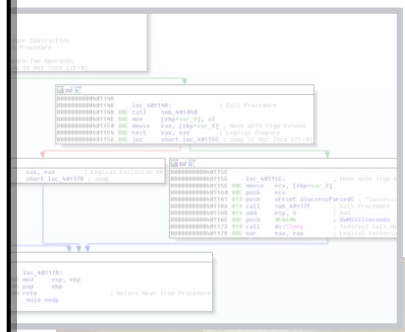


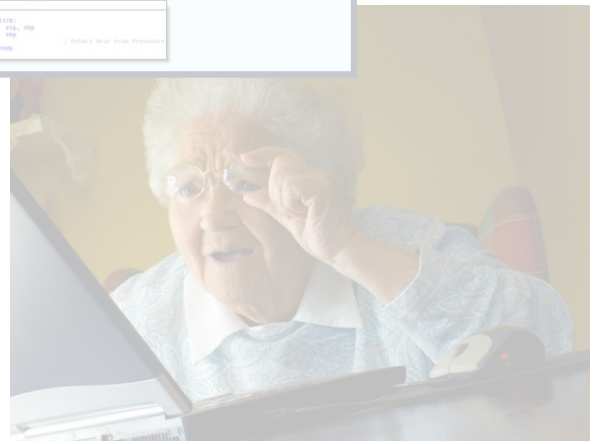
How to Do Reverse Engineering ?

Already interresting questions :
- How to desassemble ?
- How to decompile ?
- How to unstrip ?

Very hard and
Time consuming







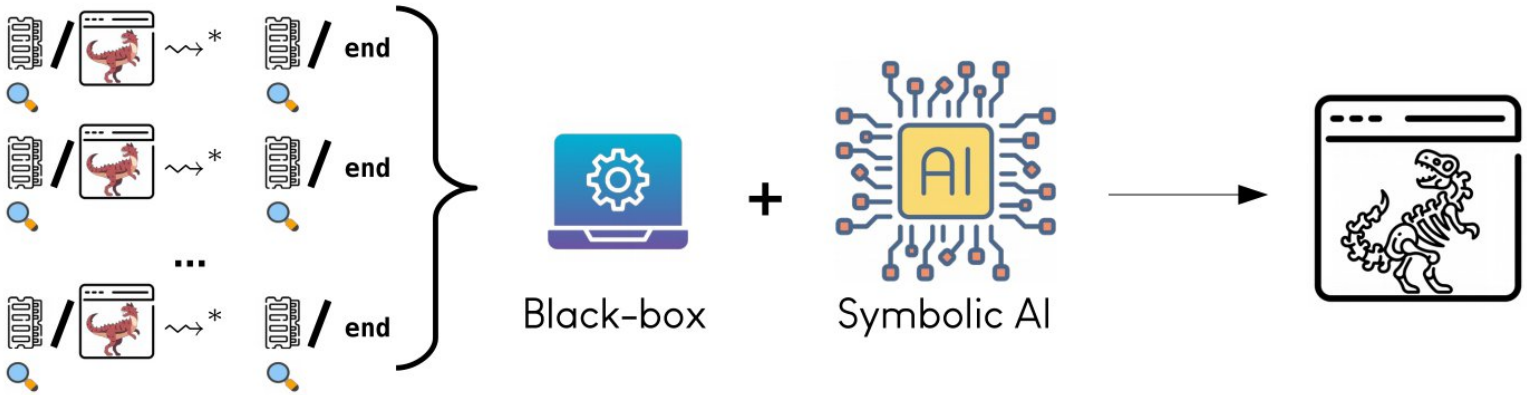
How to Help Reverse Engineering ?

From white-box analysis ...

- Taint analysis
- Backward Slicing
- Symbolic execution
- Algebraic simplifications

Deduction

To black-box analysis



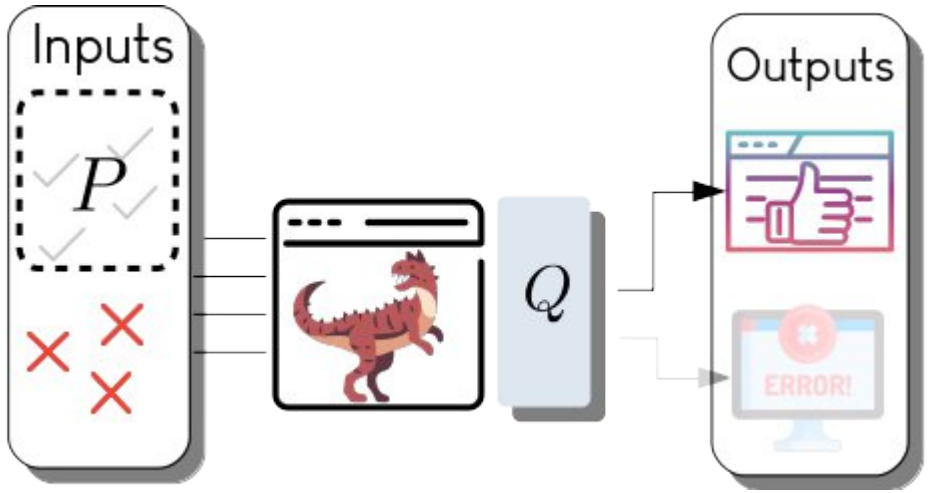
Not impacted by obfuscation

Inference

My Current Usecases

PreCA : Contract inference for reverse

(IJCAI 2022 / KR 2023 / JAIR 24)

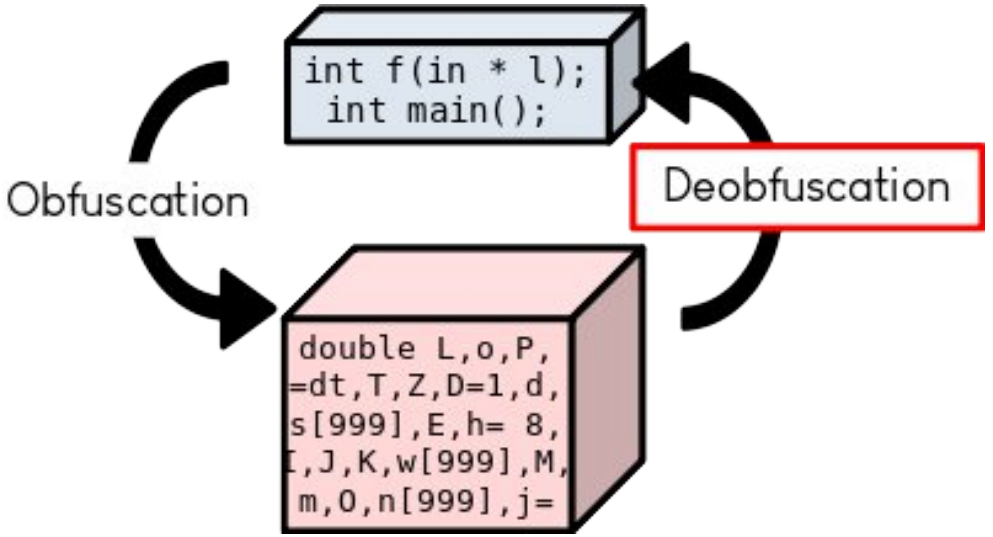


Constraint Acquisition based inference

- Good guarantees : Correctness / Termination
- Grammar : Finite set of constraints

Xyntia : Code inference for deobfuscation

(CCS 2021, CCS 2025)



Local-search-based synthesis :

- Flexible grammar
- Fast
- Returns simple results

My Current Usecases

PreCA : Contract inference for reverse

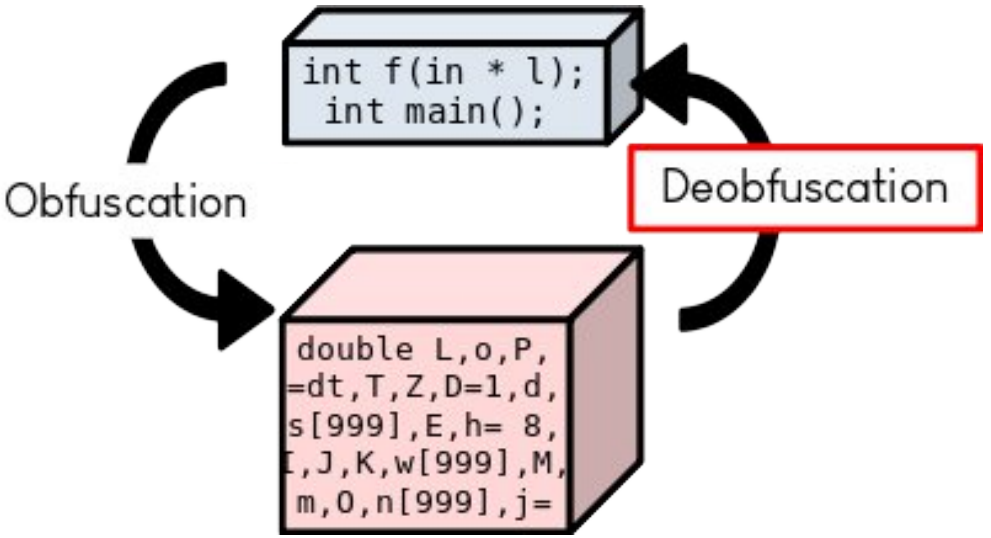
(IJCAI 2022 / KR 2023 / JAIR 24)

Constraint Acquisition based inference

- Good guarantees : Correctness / Termination
- Grammar : Finite set of constraints

Xyntia : Code inference for deobfuscation

(CCS 2021, CCS 2025)



Local-search-based synthesis :

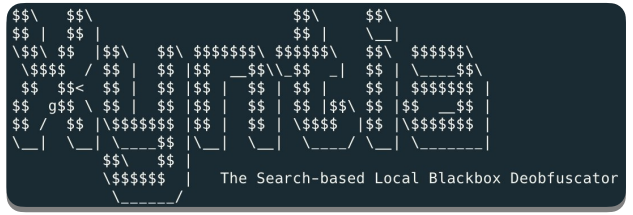
- Flexible grammar
- Fast
- Returns simple results

Goal of this Presentation

A Glimpse of the Black-box Deobfuscation Journey

1. **Xyntia: A Synthesizer for deobfuscation**
   - Synthesis as an optimization problem
   - Powerful for VM-handler deobfuscation

2. **Beyond the VM-handler case with XSMIR**
   - Search Modulo Inference Rules (SMIR)

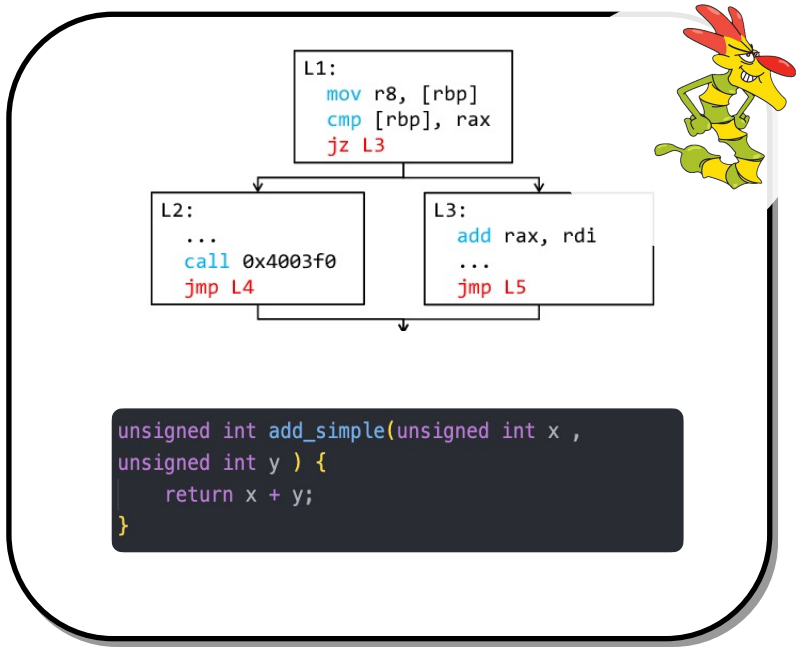


binsec / xyntia Public

77 stars

- Synthesizer
- Sampler

Obfuscation and Deobfuscation

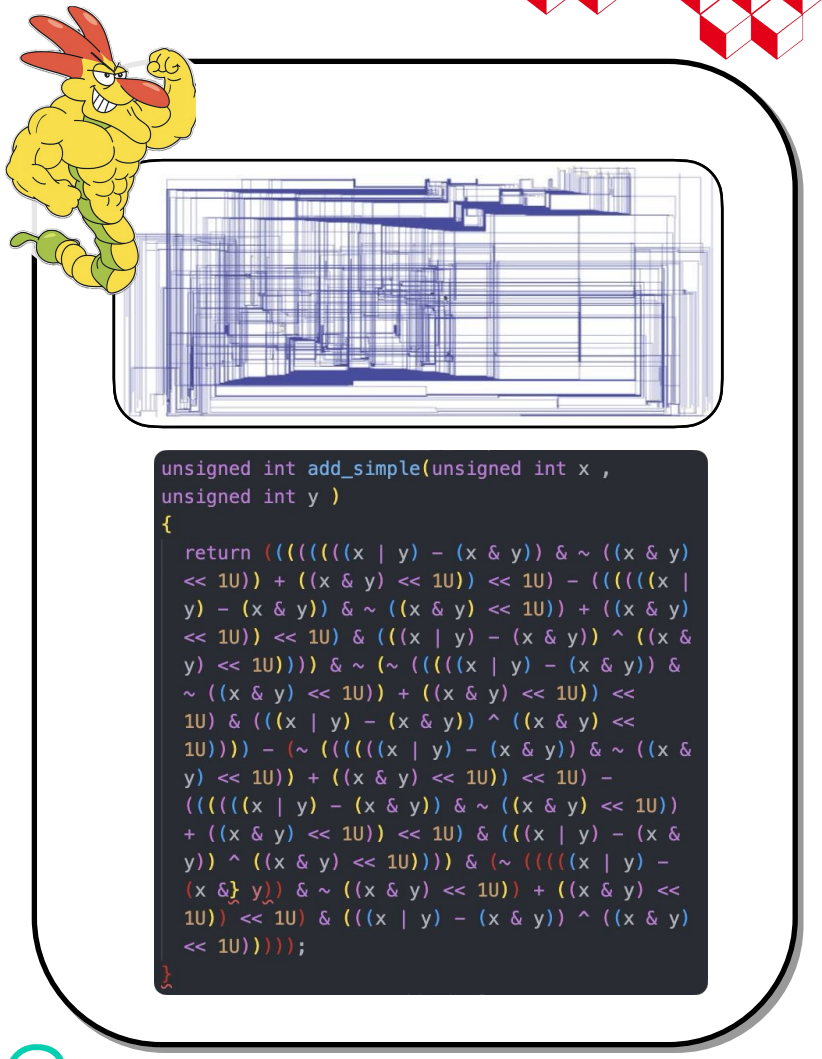


Obfuscation

☣ Thwart analysis and detection

Deobfuscation

☣ Help malware analysis



All You Ever Wanted to Know About
Dynamic Taint Analysis and Forward Symbolic Execution
(but might have been afraid to ask)

Edward J. Schwartz,
Carn

Symbolic Execution and Program Testing

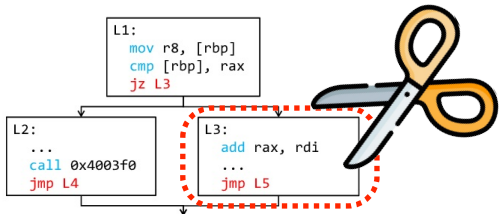
James C. King
IBM Thomas J. Watson Research Center

BINSEC

Problem: anti-white-box deobfuscation

Breakthrough 2017: Black-Box Deobfuscation

1 Defining a reverse window



Obfuscated binary

```
L3:
  add rax, rdi
  ...
  jmp L5
```

Region of interest

2 Sampling I/O

x = 0xD142
x = 0x7A0C
x = 0x0ABE
x = 0xE8B3

Obfuscated code

f(x) = 0xD144
f(x) = 0x7A0E
f(x) = 0x0AC0
f(x) = 0xE8B5

3 Synthesizing simpler expression

x	f(x)
0xD142	0xD144
0x7A0C	0x7A0E
0x0ABE	0x0AC0
0xE8B3	0xE8B5

SyGuS
Syntax-Guided Synthesis

Synthesizer

f(x) = x + 2

Main Applications:

VM-handler deobfuscation

Themida®
ADVANCED WINDOWS SOFTWARE PROTECTION

NEW

All binary-level code blocks

Augmenting Search-based Program Synthesis with Local Inference Rules to Improve Black-box Deobfuscation

Vidal Attias
Université Paris-Saclay, CEA, List
Palaiseau, France
vidal.attias@cea.fr

Nicolas Bellec
Université Paris-Saclay, CEA, List
Palaiseau, France
nicolas.bellec@cea.fr

Grégoire Menguy
Université Paris-Saclay, CEA, List
Palaiseau, France
gregoire.menguy@cea.fr

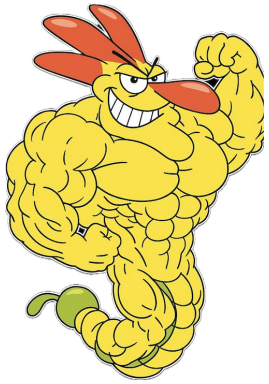
Sébastien Bardin
Université Paris-Saclay, CEA, List
Palaiseau, France
sebastien.bardin@cea.fr

Jean-Yves Marion
Université de Lorraine, CNRS, LORIA
Nancy, France
jean-yves.marion@loria.fr

Black-Box is Immune to Syntactic Complexity

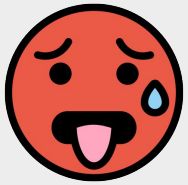
```
int add(int x , int y )
{
  return ((x ^ y) +
   ((x & y) << 1));
}
```

```
int add(int x , int y )
{
  return (((((x | y) - (x & y)) |
  ((x & y) << 1))
   << 1) - (((x | y) - (x & y))
   ^ ((x & y) << 1)));
}
```



```
int add(int x , int y )
{
  return ((((((((x | y) - (x & y)) & ~
  ((x & y) << 1)) + ((x & y) << 1)) <<
  1) & ~ (((x | y) - (x & y)) ^ ((x &
  y) << 1))) - (~ (((((x | y) - (x &
  y)) & ~ ((x & y) << 1)) + ((x & y) <<
  1)) << 1) & (((x | y) - (x & y)) ^
  ((x & y) << 1))));
}
```

White Box



Black Box

Under the Hood: Program Synthesis

Syntactic specification

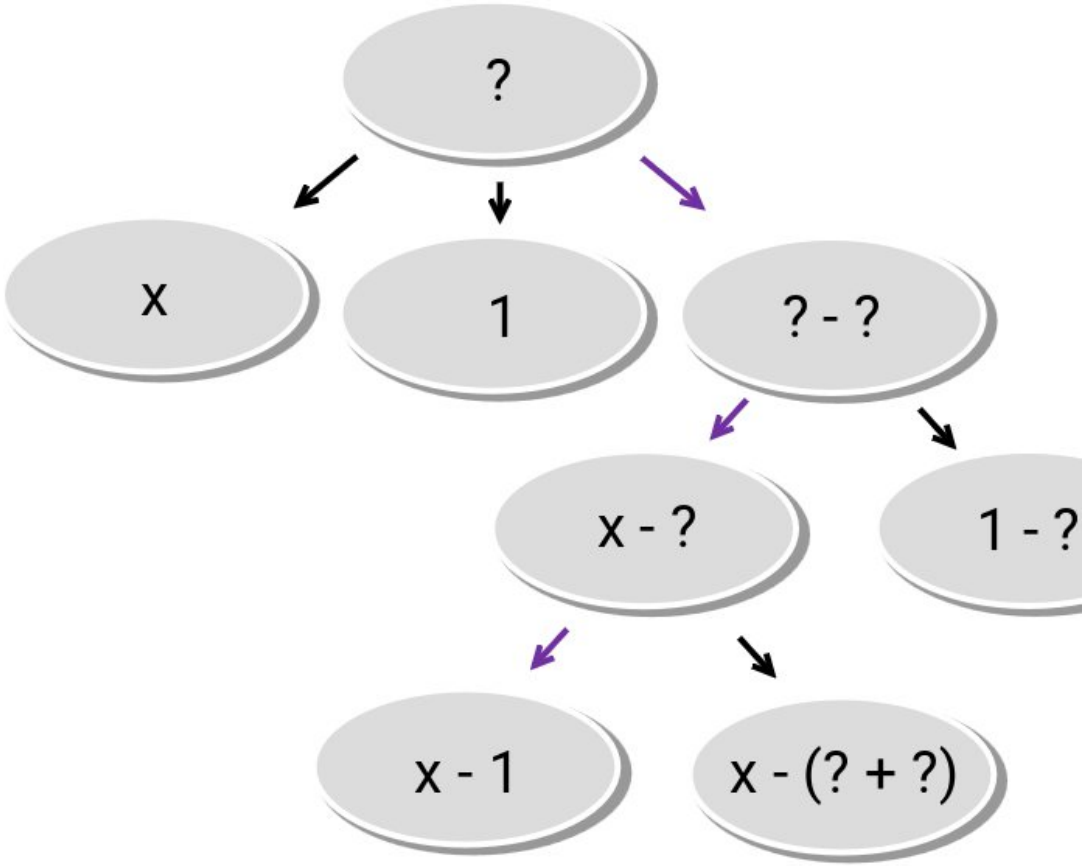
E := E + E | E - E | ...
E := V | C
V := x
C := 1

Semantic specification

0xD142	→	0xD144
0x7A0C	→	0x7A0E
0x0ABE	→	0x0AC0
0xE8B3	→	0xE8B5

x f(x)

SyGuS
Syntax-Guided Synthesis



Xyntia: Program Synthesis on Steroids

Challenge of Black-box deobfuscation

↳ Get powerful enough synthesis to handle real obfuscated code

↳ **Problem**: SOTA is not enough

usenix SYNTIA

(and (or (and (= x0 y0) (= y0 x1)) (z0 x y1 (y2)) (a z1 x (= y2 x3)) (and (= x2 z2) (z2 x3))) (not (= x0 x3)))

CVC4

CVC5

Session 10A: Crypto, Symbols and Obfuscation CCS '21, November 15–19, 2021, Virtual Event, Republic of Korea

Search-Based Local Black-Box Deobfuscation: Understand, Improve and Mitigate

Grégoire Menguy
gregoire.menguy@cea.fr
Université Paris-Saclay, CEA, List
France

Sébastien Bardin
sebastien.bardin@cea.fr
Université Paris-Saclay, CEA, List
France

Richard Bonichon
richard.bonichon@nomadic-labs.com
Nomadic Labs
France

Cauim de Souza Lima
cauimsouza@gmail.com
Université Paris-Saclay, CEA, List
France

ABSTRACT

Code obfuscation aims at protecting Intellectual Property and other secrets embedded into software from being retrieved. Recent works leverage advances in artificial intelligence (AI) with the hope of getting blackbox deobfuscators completely immune to standard (whitebox) protection mechanisms. While promising, this new field of *AI-based*, and more specifically *search-based blackbox deobfuscation*, is still in its infancy. In this article we deepen the state of search-based blackbox deobfuscation in three key directions: *understand* the current state-of-the-art, *improve* over it and design dedicated *protection mechanisms*. In particular, we define a novel generic framework for search-based blackbox deobfuscation encompassing prior work and highlighting key components; we are the first to point out that the search space underlying code deobfuscation is too unstable for simulation-based methods (e.g., Monte Carlo Tree Search used in prior work) and advocate the use of robust methods such as S-metaheuristics; we propose the new optimized search-based blackbox deobfuscator Xyntia which significantly outperforms prior work in terms of success rate (especially with small time budget) while being completely immune to the most recent anti-analysis code obfuscation methods; and finally we propose two novel protections against search-based blackbox deobfuscation, allowing to counter Xyntia powerful attacks.

CCS CONCEPTS

• **Security and privacy** → **Software reverse engineering**; • **Computing methodologies** → **Randomized search**; **Game tree search**.

KEYWORDS

Binary-level code analysis; deobfuscation; artificial intelligence; S-metaheuristics

CCS '21, November 15–19, 2021, Virtual Event, Republic of Korea

ACM ISBN 978-1-4503-8454-4/21/11…$15.00
https://doi.org/10.1145/3460120.3485250

ACM Reference Format:
Grégoire Menguy, Sébastien Bardin, Richard Bonichon, and Cauim de Souza Lima. 2021. Search-Based Local Black-Box Deobfuscation: Understand, Improve and Mitigate. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21), November 15–19, 2021, Virtual Event, Republic of Korea.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3460120.3485250

1 INTRODUCTION

Context. Software contain valuable assets, such as secret algorithms, business logic or cryptographic keys, that attackers may try to retrieve. The so-called Man-At-The-End-Attacks scenario (MATE) considers the case where software users themselves are adversarial and try to extract such information from the code. *Code obfuscation* [12, 13] aims at protecting codes against such attacks, by transforming a sensitive program P into a functionally equivalent program P' that is more "difficult" (more expensive, for example, in money or time) to understand or modify. On the flip side, *code deobfuscation* aims to extract information from obfuscated codes.

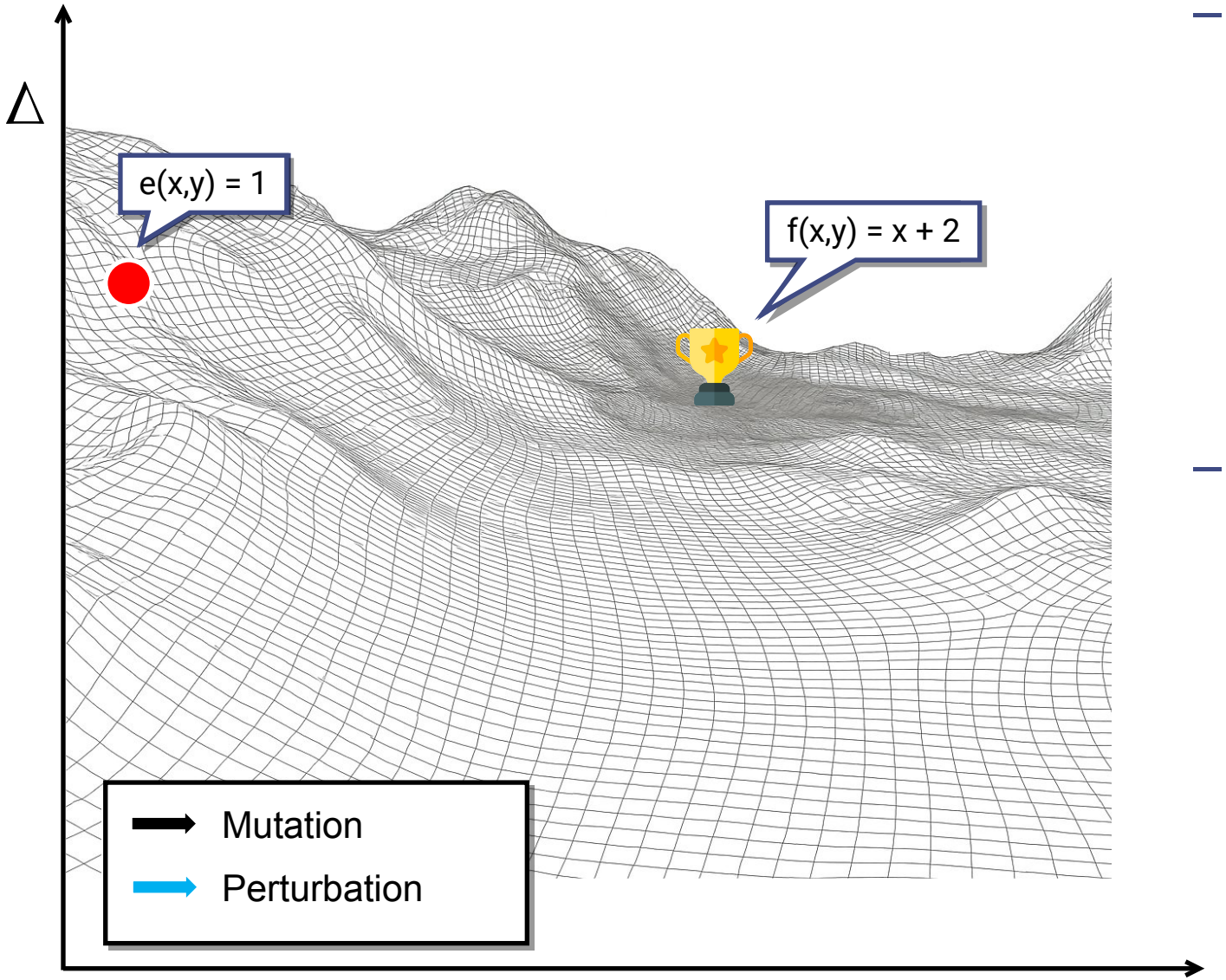
Whitebox deobfuscation techniques, based on advanced symbolic program analysis, have proven extremely powerful against standard obfuscation schemes [3, 5, 10, 22, 28, 30, 36] – especially in local attack scenarios where the attacker analyses pre-identified parts of the code (e.g., trigger conditions). But they are inherently sensitive to the *syntactic complexity* of the code under analysis, leading to recent and effective countermeasures [12, 25, 26, 37].

Search-based blackbox deobfuscation. Despite being rarely complete or sound, *artificial intelligence* (AI) techniques are flexible and often provide good enough solutions to hard problems in reasonable time. They have been therefore recently applied to binary-level code deobfuscation. The pioneering work by Blazytko et al. [7] shows how *Monte Carlo Tree Search* (MCTS) [9] can be leveraged to solve local deobfuscation tasks by *learning* the semantics of pieces of protected codes in a *blackbox manner*, in principle *immune to the syntactic complexity* of these codes. Their method and prototype, Syntia, have been successfully used to reverse state-of-the-art protectors like VMProtect [34], Themida [27] and Tigress [11], drawing attention from the software security community [8].

Problem. While promising, search-based blackbox (code) deobfuscation techniques are still not well understood. Several key questions of practical relevance (e.g., deobfuscation correctness and quality, sensitivity to time budget) are not addressed in Blazytko et

Xyntia synthesizer for BV theory
> Synthesis as an optimization problem

The Xyntia Synthesizer



– Guidance w.r.t., objective function

Target expr. output

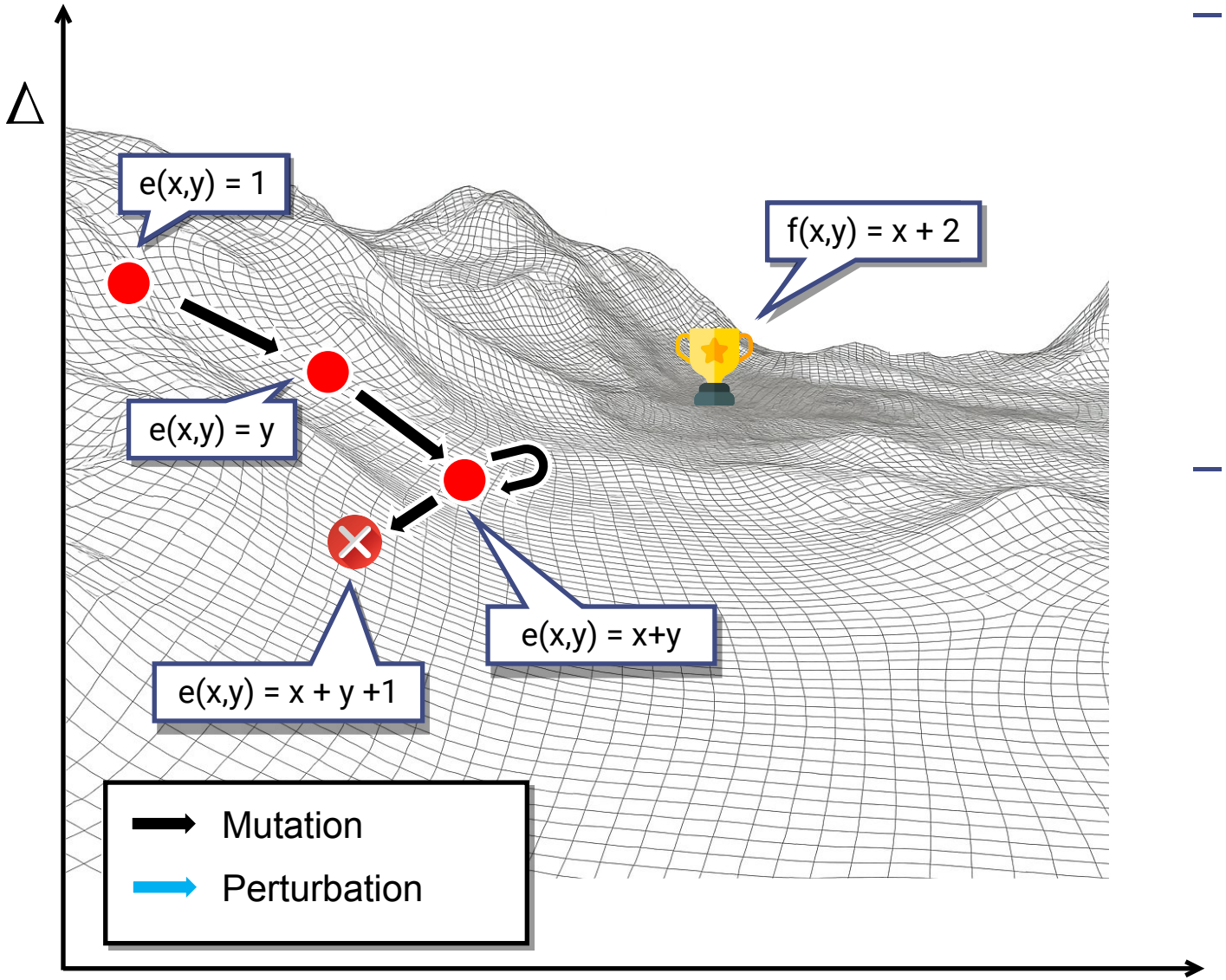
$$\Delta(f, e) = \sum_{i \in Samples} |f(i) - e(i)|$$

Candidate expr. output

– Main search steps:

1. **Mutations:** keep candidate only if Δ decreases
2. **Perturbations:** keep candidate even if Δ increases
3. **Ending condition:** if Δ = 0 we found the solution

The Xyntia Synthesizer



- **Guidance w.r.t., objective function**

Target expr. output

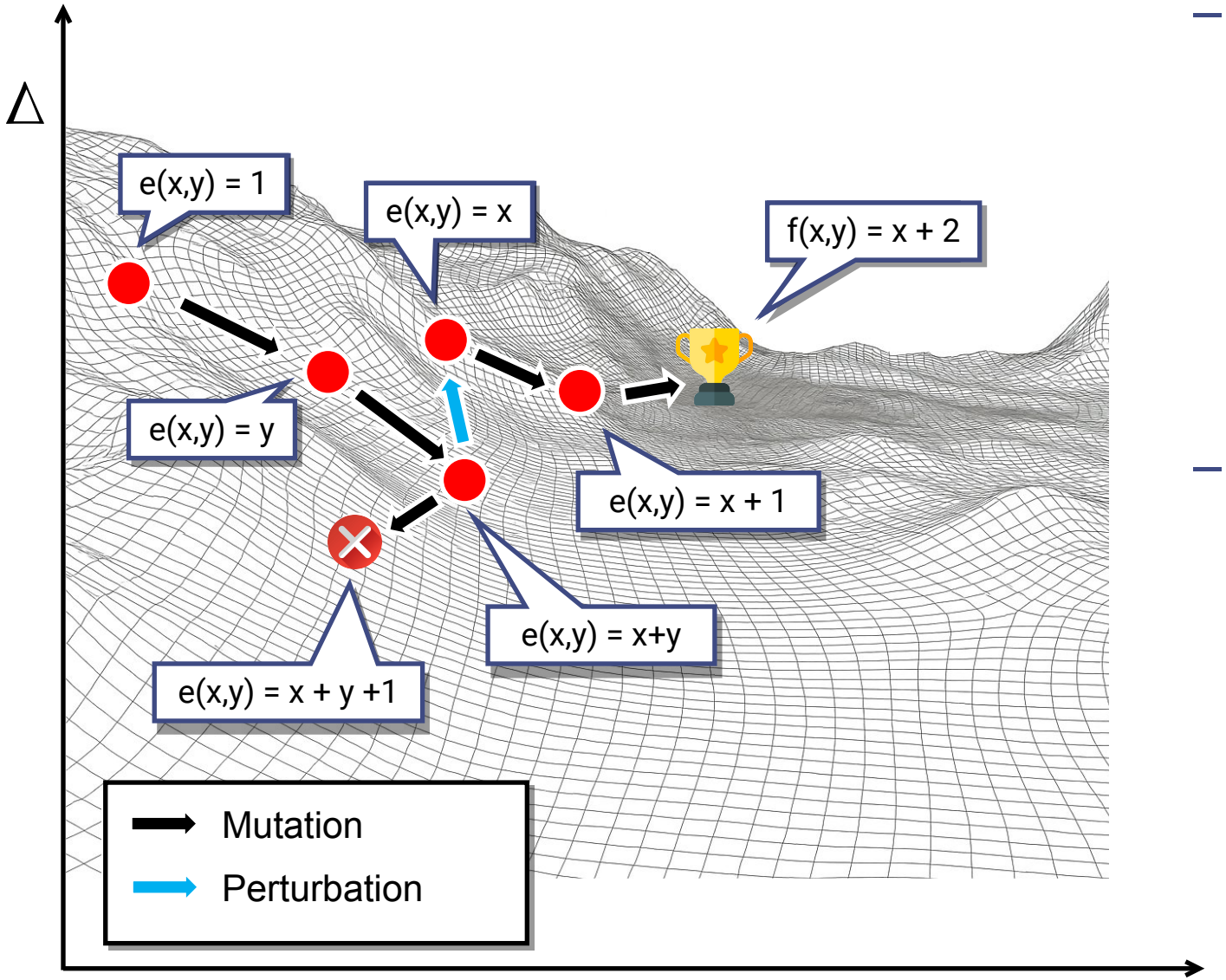
$$\Delta(f, e) = \sum_{i \in Samples} |\overbrace{f(i)}^{} - \underbrace{e(i)}_{}|$$

Candidate expr. output

- **Main search steps:**

1. **Mutations:** keep candidate only if Δ decreases
2. **Perturbations:** keep candidate even if Δ increases
3. **Ending condition:** if Δ = 0 we found the solution

The Xyntia Synthesizer



– Guidance w.r.t., objective function

Target expr. output

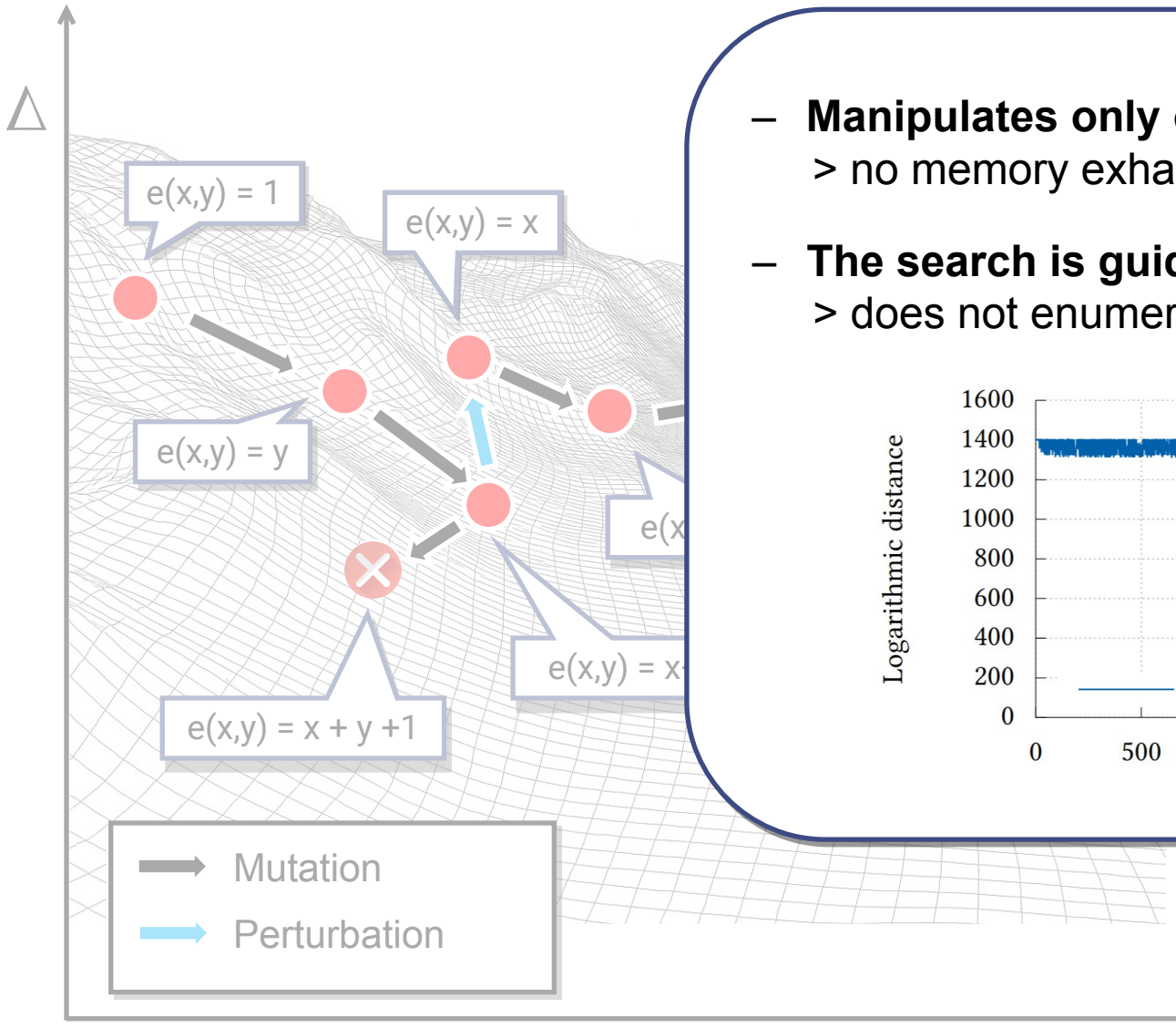
$$\Delta(f, e) = \sum_{i \in Samples} |\overbrace{f(i)}^{} - \underbrace{e(i)}_{}|$$

Candidate expr. output

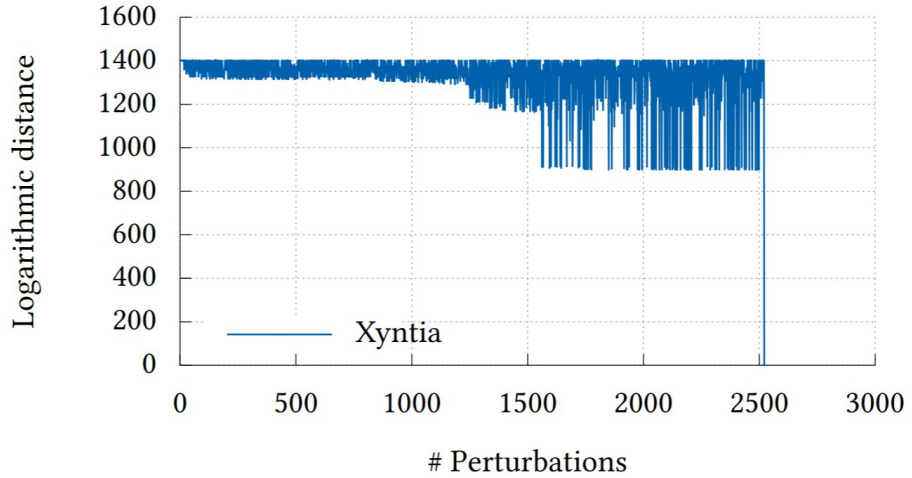
– Main search steps:

1. **Mutations:** keep candidate only if Δ decreases
2. **Perturbations:** keep candidate even if Δ increases
3. **Ending condition:** if Δ = 0 we found the solution

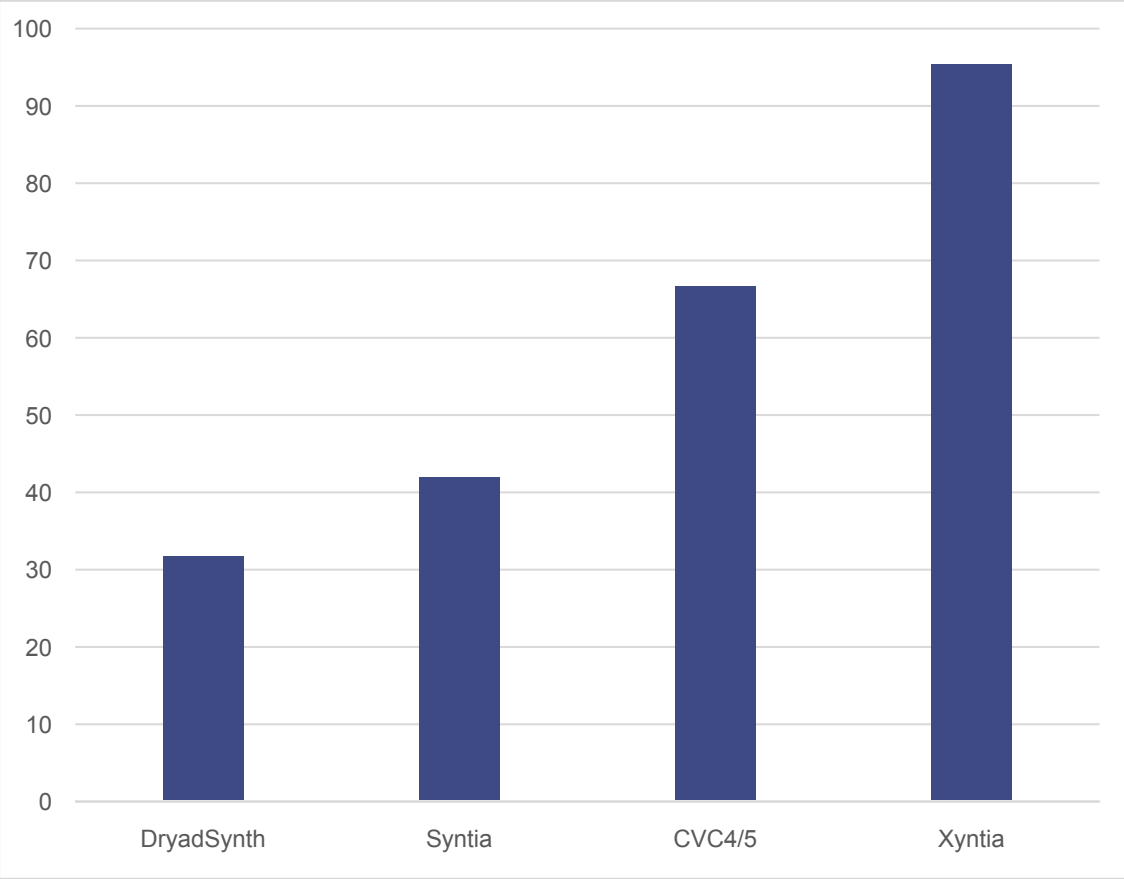
The Xyntia Synthesizer



- **Manipulates only one expression**
  > no memory exhaustion
- **The search is guided w.r.t., the objective function**
  > does not enumerate all the search space



Some Results

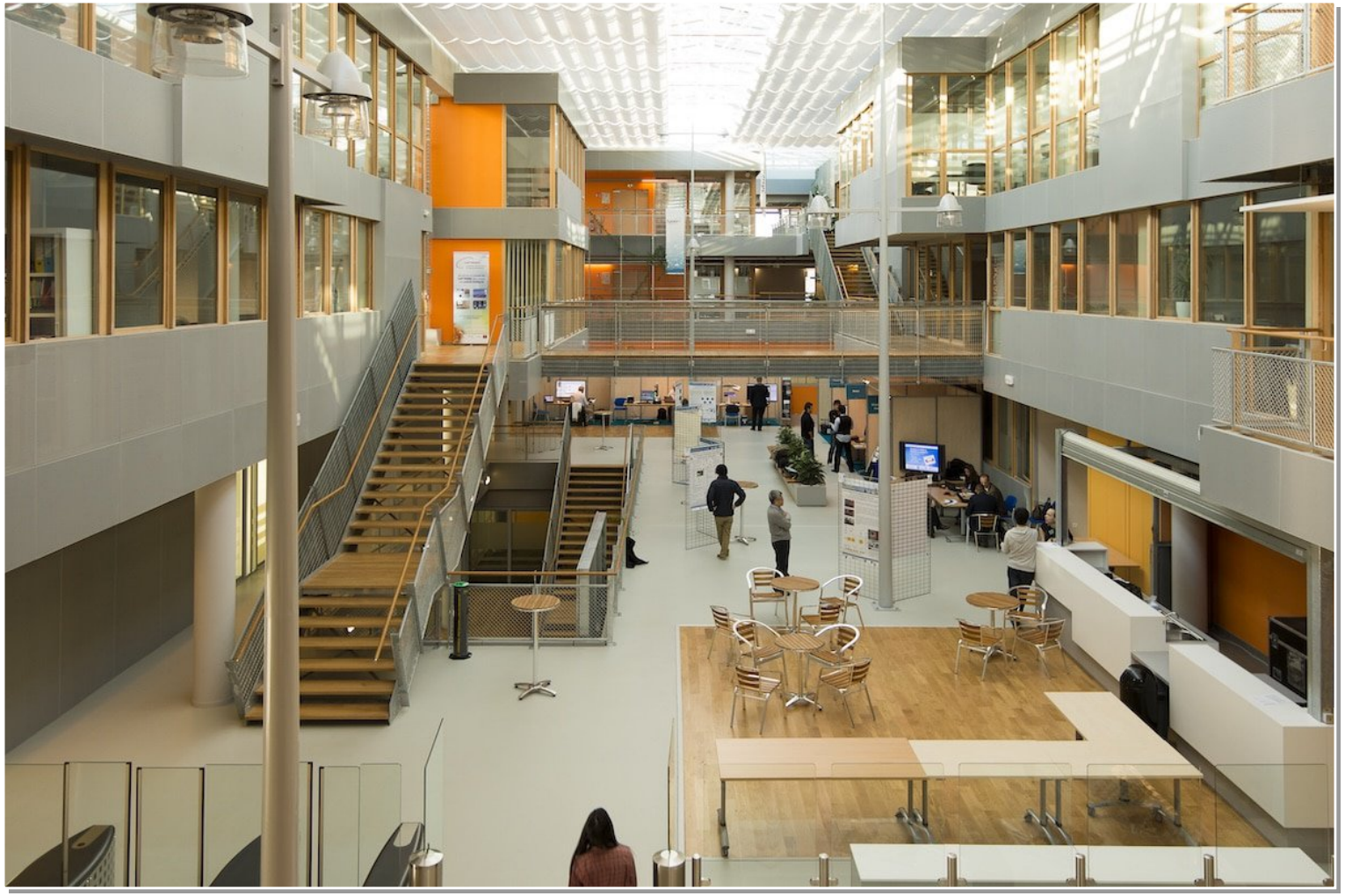


Xyntia outperforms the SOTA
(95% vs 65% vs 42% vs 32%)

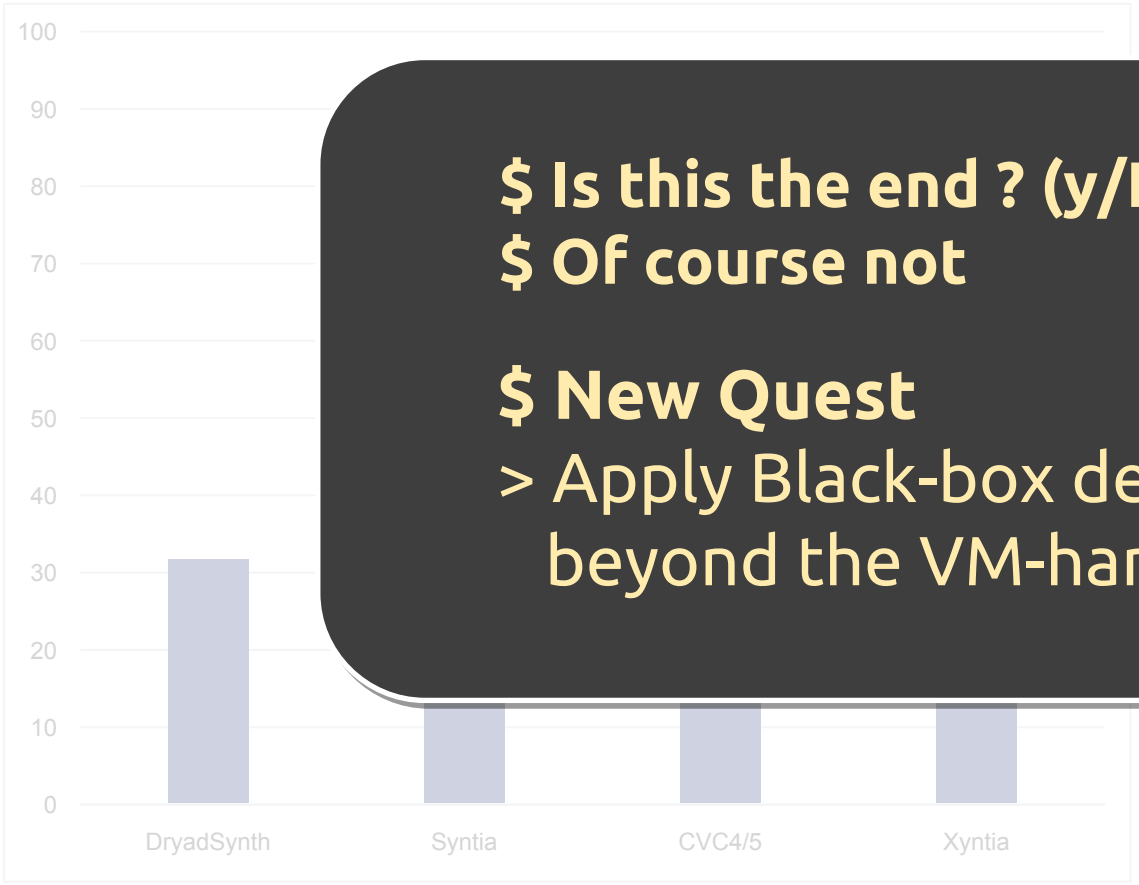
Xyntia is immune to standard obfuscations
(opaque predicates, covert channels)

Xyntia efficiently deobfuscates VM-Handlers

A Bit of Rest: Do You Have Questions ?



Some Results



$ Is this the end ? (y/N)
$ Of course not

$ New Quest
> Apply Black-box deobfuscation beyond the VM-handler case ?

bfuscations
els)

tes VM-Handlers

Wait There is a Problem

Real example from Snapchat iOS app

```
add x0,sp,#0x1b8 ;struct timeval *tva
mov x1,#0x0 ;struct timezonze *tzone
adrp x8,0x109499000
ldr x8,[x8, #0x1d0]
blr x8 ;gettimeofday(tval,tzone)
ldr x8,[sp, #0x1b8] ;tval->tv_sec
mov w9,#0x3e8
mul x8,x8,x9
ldrsw x9,[sp, #0x1c0] ;tval->tv_usec
lsr x9,x9,#0x3
mov x10,#0xf7cf
movk x10,#0xe353, LSL #16
movk x10,#0x9ba5, LSL #32
movk x10,#0x20c4, LSL #48
umulh x9,x9,x10
mov x10,#0xe6b3
movk x10,#0x7dba, LSL #16
movk x10,#0xecfa, LSL #32
movk x10,#0xd0e1, LSL #48
add x9,x10,x9, LSR #0x4
orr x11,x9,x8
lsl x11,x11,#0x1
eor x8,x9,x8
sub x8,x11,x8
eor x9,x8,x10
mov x10,#0xe6b3
movk x10,#0x7dba, LSL #16
movk x10,#0xecfa, LSL #32
movk x10,#0x50e1, LSL #48
bic x8,x10,x8
sub x8,x9,x8, LSL #0x1 ;tv_sec *= 1000
```

Timeout: 1h

- cvc5
- DryadSynth
- Syntia
- Xyntia

Expression:

$y = x * 1000$

Tigress example

```
push   %rbp
mov    %rsp,%rbp
mov    %edi,-0x14(%rbp)
mov    %esi,-0x18(%rbp)
mov    -0x14(%rbp),%eax
imul   $0x6aa7671b,%eax,%eax
add    $0x52f20197,%eax
mov    %eax,-0x4(%rbp)
mov    -0x18(%rbp),%eax
imul   $0x6aa7671b,%eax,%eax
add    $0x52f20197,%eax
mov    %eax,-0x8(%rbp)
mov    -0x4(%rbp),%eax
imul   -0x8(%rbp),%eax
imul   $0xd2d29b13,%eax,%edx
mov    -0x4(%rbp),%eax
imul   $0x253574cb,%eax,%eax
add    %eax,%edx
mov    -0x8(%rbp),%eax
imul   $0x253574cb,%eax,%eax
add    %edx,%eax
sub    $0x42f0ad26,%eax
mov    %eax,-0xc(%rbp)
mov    -0xc(%rbp),%eax
pop    %rbp
ret
```

Timeout: 1h

- cvc5
- DryadSynth
- Syntia
- Xyntia

Expression:

$z = x * y * 0x6aa7671b + 0x52f20197$

Common limitations in SyGUS

1. **Dedicated deobfuscation synthesizers**
   - Syntia
   - Xyntia
2. **General purpose synthesizers**
   - CVC4 / cvc5
   - DryadSynth

But there are limitations

- Constant values
- Large expressions

Search Modulo Inference Rules

1 Search Modulo Inference Rules (SMIR)

Combine **search-based synthesis** with **symbolic reasoning**

- Automatically *elevate* candidate solutions
- Guide the search

2 Implementation of SMIR on top of Xyntia

https://github.com/binsec/xyntia

3 First evaluation of black-box deobfuscation at scale on binary-level code blocks

Augmenting Search-based Program Synthesis with Local Inference Rules to Improve Black-box Deobfuscation

Vidal Attias
Université Paris-Saclay, CEA, List
Palaiseau, France
vidal.attias@cea.fr

Nicolas Bellec
Université Paris-Saclay, CEA, List
Palaiseau, France
nicolas.bellec@cea.fr

Grégoire Menguy
Université Paris-Saclay, CEA, List
Palaiseau, France
gregoire.menguy@cea.fr

Sébastien Bardin
Université Paris-Saclay, CEA, List
Palaiseau, France
sebastien.bardin@cea.fr

Jean-Yves Marion
Université de Lorraine, CNRS, LORIA
Nancy, France
jean-yves.marion@loria.fr

Abstract

Code obfuscation aims to protect programs from reverse engineering, with applications ranging from intellectual property protection to malware hardening. Recent works on black-box analyses propose to leverage program synthesis in order to infer the semantics of highly obfuscated code blocks. Being fully *black-box*, these approaches are immune to *syntactic* complexity and can thus bypass standard obfuscation mechanisms. Yet, they are restricted by their synthesis capabilities and can only be applied to *semantically* simple code blocks. It explains why they have mainly been used on virtual machine handlers, where behaviors are usually simple enough. Applying black-box deobfuscation at scale beyond virtualization is still an open problem, notably because black-box methods cannot synthesize complex behaviors involving, for example, arbitrary constant values or affine or polynomial relations over mixed-boolean-arithmetic expressions. In this article, we show how to combine *search-based program synthesis* with *local inference rules*, resulting in a new method named *Search Modulo Inference Rules* (SMIR) that boosts search-based program synthesis while keeping its generality and flexibility. We instantiate SMIR with inference rules for hard synthesis problems like arbitrary constant values and affine or polynomial relations over mixed boolean expressions, yielding the new black-box deobfuscation tool: XSMIR. Experiments demonstrate that XSMIR significantly outperforms prior black-box deobfuscators, synthesizing overall 76% and 84% of the expressions from our real-world obfuscated and non-obfuscated benchmarks where prior works recover 63% and 55%, together with 2 to 3 times less false positive and slightly improved compression rate.

CCS Concepts

• **Security and privacy → Software reverse engineering**; • **Computing methodologies → Randomized search**.

Keywords

Deobfuscation, reverse engineering, program synthesis

CCS '25, Taipei, Taiwan

ACM ISBN 979-8-4007-1525-9/2025/10
https://doi.org/10.1145/3719027.3765134

ACM Reference Format:
Vidal Attias, Nicolas Bellec, Grégoire Menguy, Sébastien Bardin, and Jean-Yves Marion. 2025. Augmenting Search-based Program Synthesis with Local Inference Rules to Improve Black-box Deobfuscation. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25), October 13–17, 2025, Taipei, Taiwan.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3719027.3765134

1 Introduction

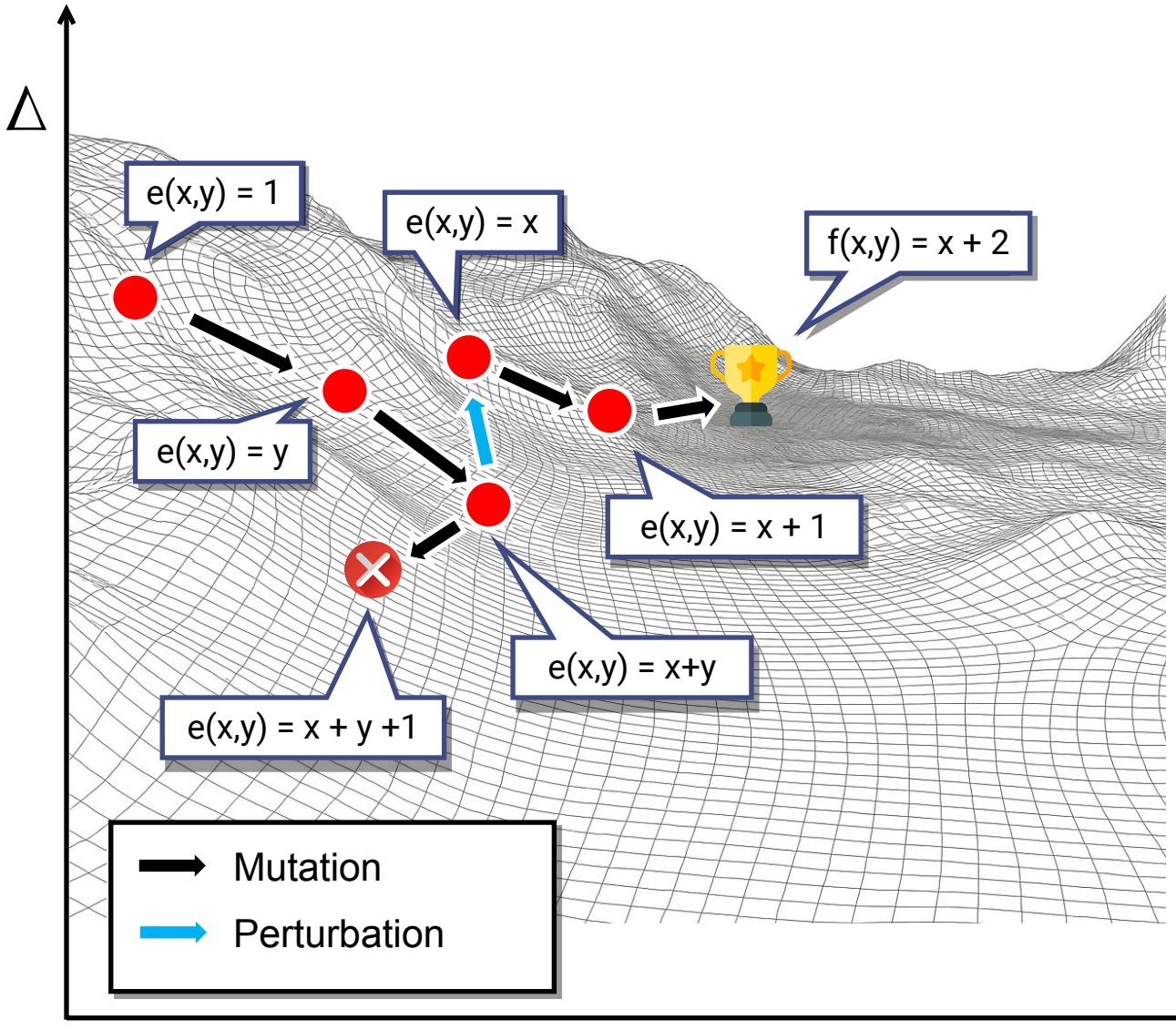
Obfuscation [18, 19] aims to protect software from reverse engineering. It translates a program P into a functionally equivalent program P_o, harder to analyze. As cryptography has not yet provided a bullet-proof solution for this problem, the obfuscation community mainly focuses on program-analysis-based techniques [19], leading to a cat-and-mouse game between defenders and attackers.

While obfuscation is used to protect *Intellectual Property* and other valuable software assets, it is also used to protect malware. Thus, automated *deobfuscation* methods [12, 21, 39, 50, 51] have been proposed to cope with the quick advances in obfuscation. Given an obfuscated program P_o, the goal here is to simplify it into a simpler yet functionally equivalent program P^* – ideally P^* should be as simple as the original unprotected code P.

In the last decade, *white-box deobfuscation* techniques, lifting the latest methods of static program analysis, have proved highly effective against many standard obfuscation schemes like opaque predicates [7, 54, 60] or virtualization [32, 51, 54]. However, several obfuscation methods significantly impair white-box analysis. Dedicated protections, including Mixed Boolean Arithmetic (MBA) expressions [63], covert channels [55] or path-oriented protections [3, 44, 45, 59], have emerged, many of which increase the syntactic complexity of the original code to break white-box approaches.

The promises of black-box deobfuscation. New deobfuscation methods, based on program synthesis, have emerged to simplify heavily obfuscated local code snippets [12, 39]. These methods rely only on *input-output* (I/O) *observations* to infer the code snippet behavior. Through synthesis, they explore a *space of candidate expressions* generated by an *inference grammar*, seeking an expression that mimics the I/O observations. Unlike white-box approaches, black-box ones are immune to syntactic complexity, but the analyzed code must be semantically simple to synthesize it. This explains why black-box methods primarily focused on virtualized code: handlers

Search-based Synthesis



– **Guidance w.r.t., objective function**

Target expr. output

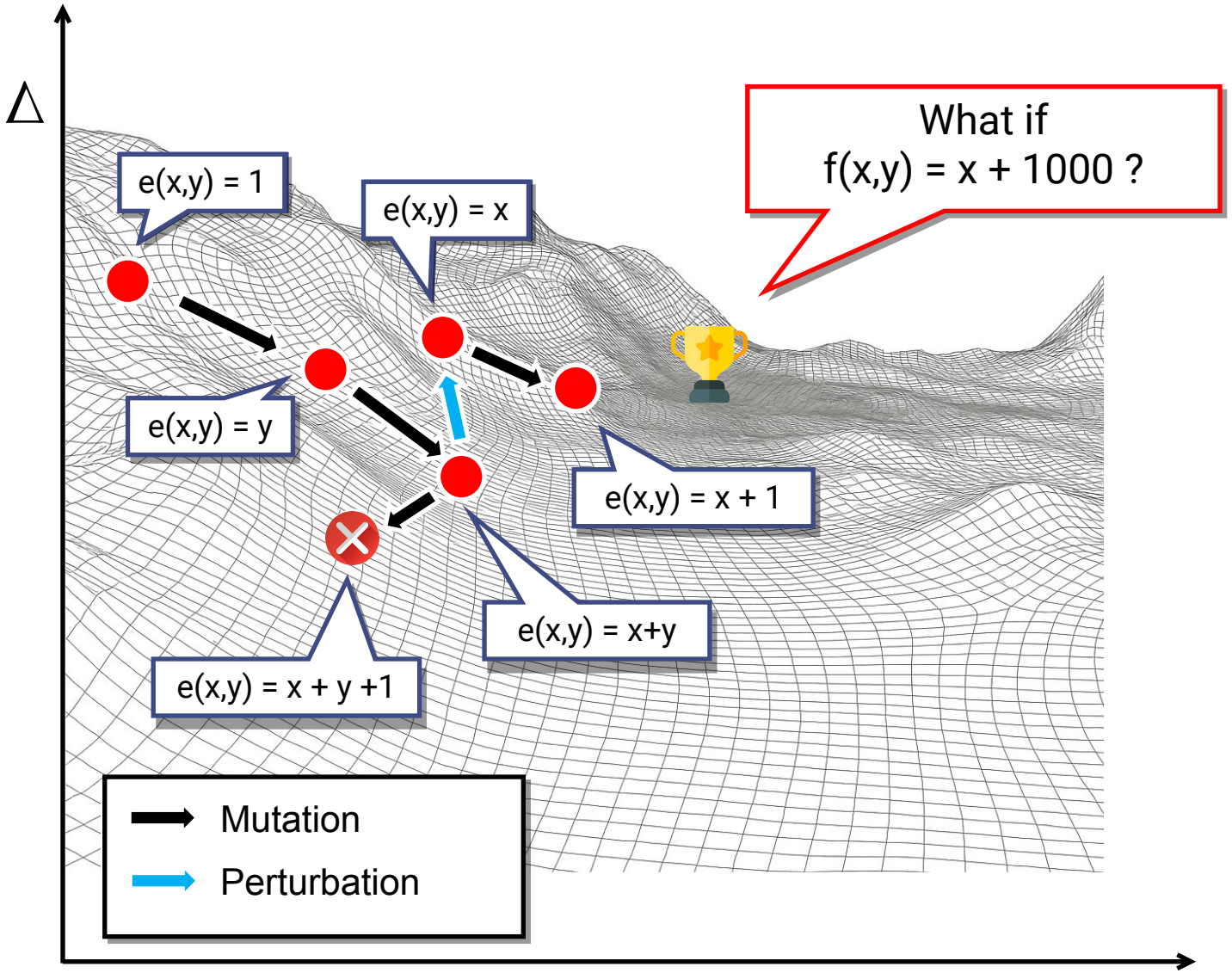
$$\Delta(f, e) = \sum_{i \in Samples} |\overbrace{f(i)}^{} - \underbrace{e(i)}_{}|$$

Candidate expr. output

– **Main search steps:**

1. **Mutations:** keep candidate only if Δ decreases
2. **Perturbations:** keep candidate even if Δ increases
3. **Ending condition:** if Δ = 0 we found the solution

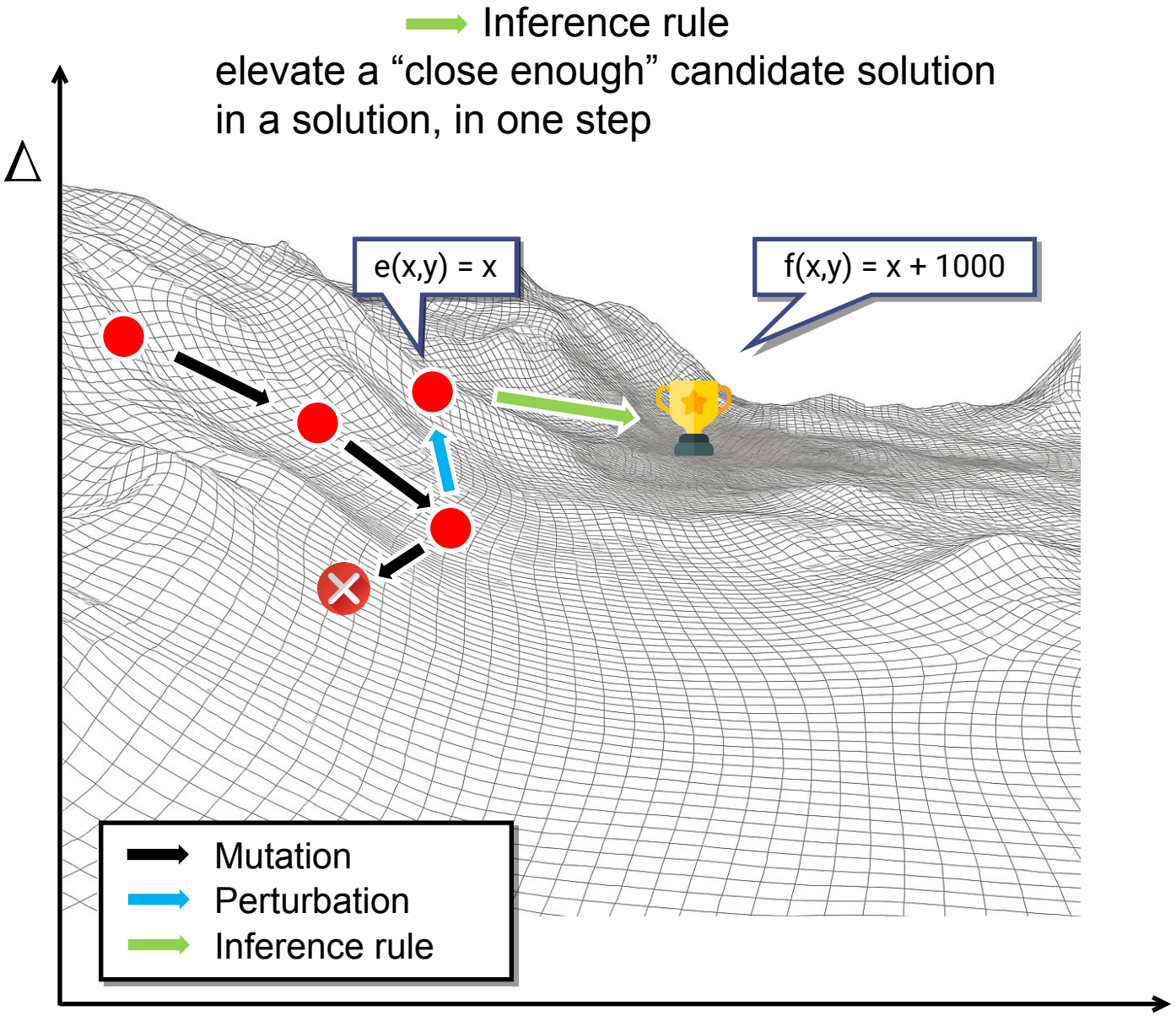
Search-based Synthesis



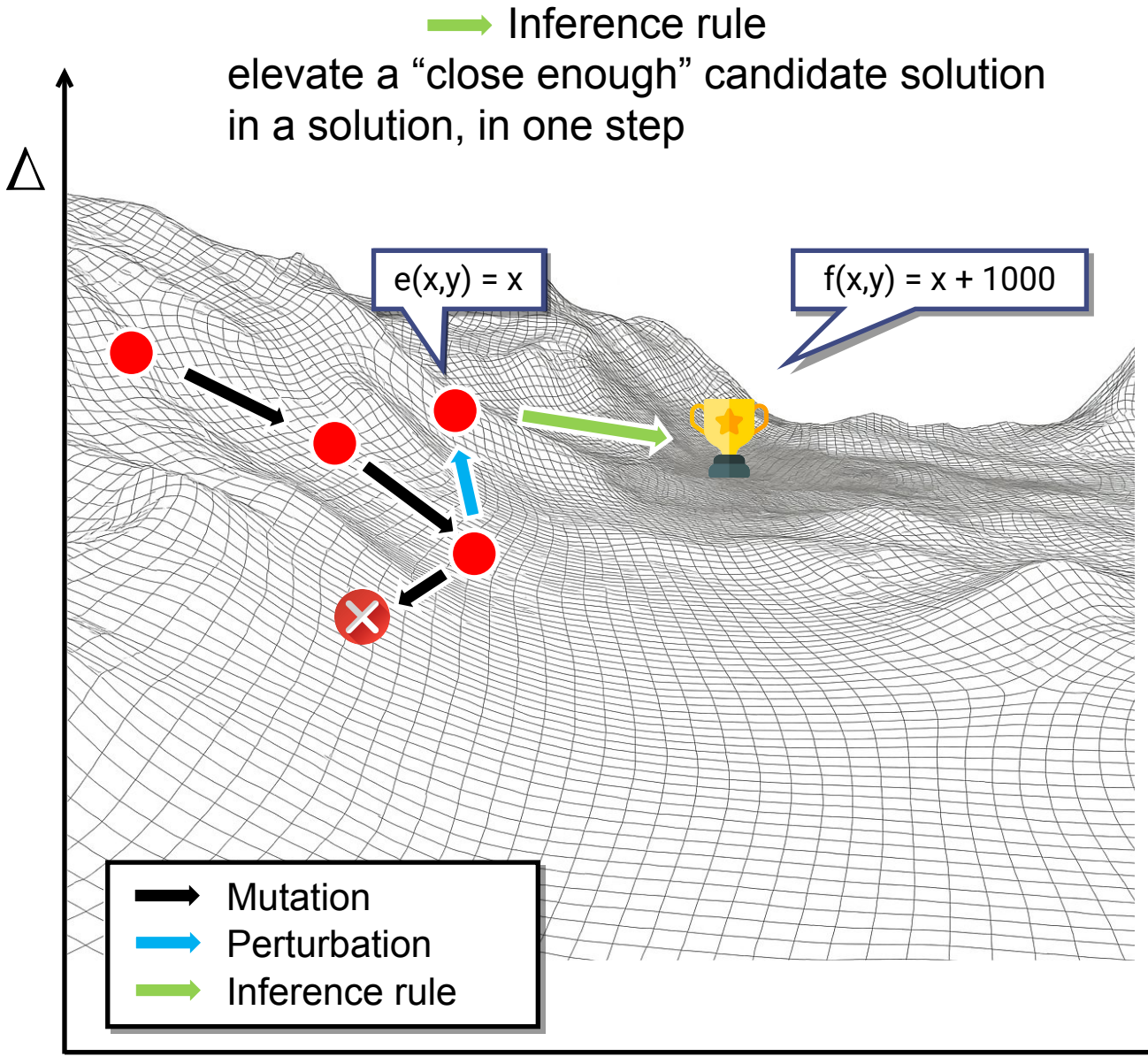
Problem:

- Very unlikely to generate
  x + 1 + ... + 1
  (times 1000)
- Search is too heuristic

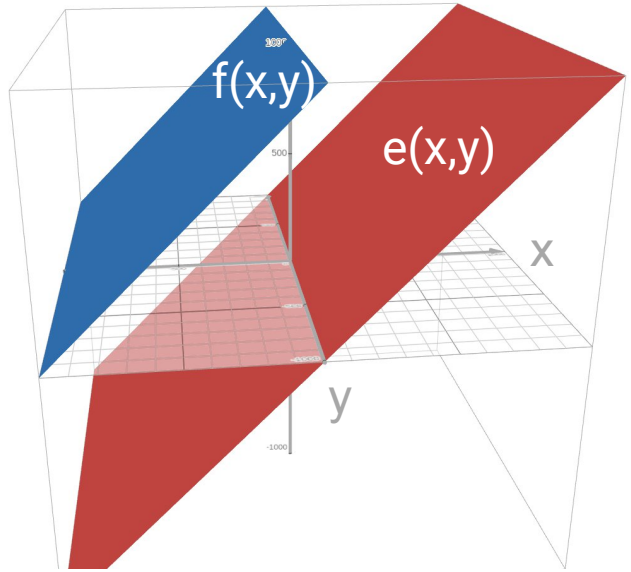
Search Modulo Inference Rules (SMIR)



Search Modulo Inference Rules (SMIR)



Inference rule for +



The variance of f(x,y) - e(x,y) equals 0

⇒ The solution equals e(x,y) up to an offset

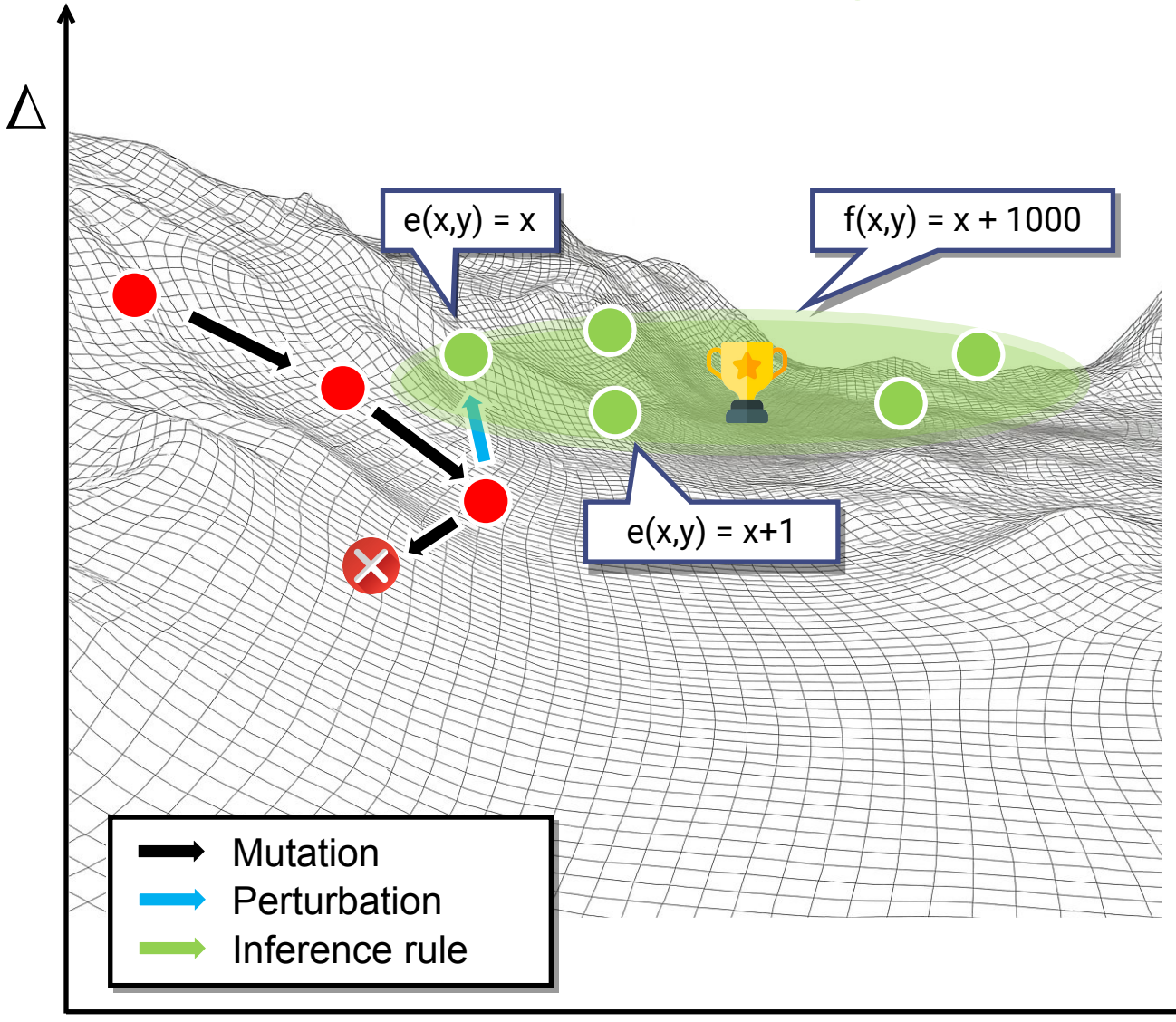
⇒ **Solution** = e(x,y) + f(0, 0) - e(0, 0)

= e(x, y) + 1000

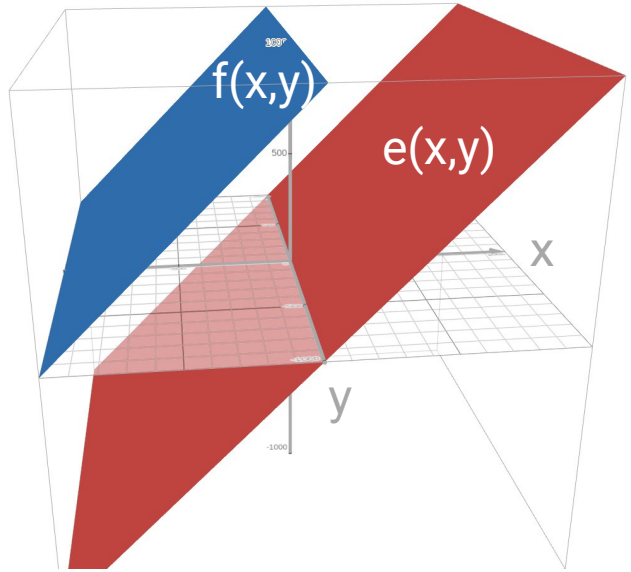
Search Modulo Inference Rules (SMIR)

Search: find the exact right expression

SMIR: find any close-enough expression



Inference rule for +



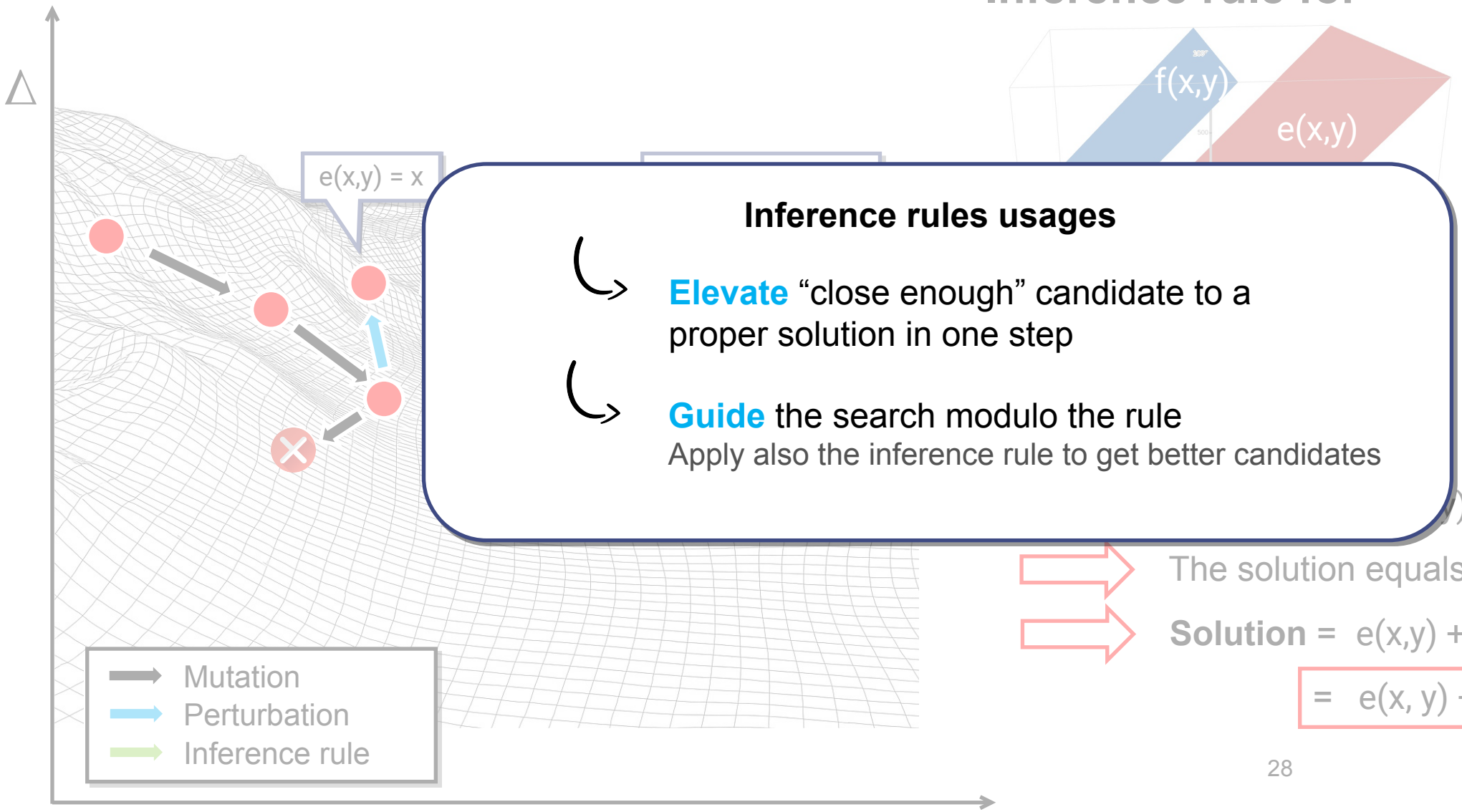
The variance of f(x,y) - e(x,y) equals 0

⇒ The solution equals e(x,y) up to an offset

⇒ **Solution** = e(x,y) + f(0, 0) - e(0, 0)

= e(x, y) + 1000

Search Modulo Inference Rules (SMIR)



Inference rules usages

Elevate “close enough” candidate to a proper solution in one step

Guide the search modulo the rule
Apply also the inference rule to get better candidates

Inference rule for +

) equals 0

The solution equals e(x,y) up to an offset

Solution = e(x,y) + f(0, 0) - e(0, 0)

= e(x, y) + 1000

Our Current Inference Rules

1. **Addition** $e + c$
2. **Multiplication** $e \times c$
3. **XOR mask** $e \oplus c$
4. **AND/OR mask** $(e \wedge c_1) \vee c_2$
5. **Rotation** $rotate(e,c)$
6. **Log. left shift** $e \ll c$
7. **Log. right shift** $e \gg c$
8. **Affine** $c_1 \cdot e + c_2$
9. **Polynomial** $\sum_{i=0}^{k} c_i \cdot e^i$

In the paper:

- Recipes for creating rules
  > Inversion vs Enumeration
- Explain how to handle multiple rules

Back to our Examples

Real example from Snapchat iOS app

```
add x0,sp,#0x1b8 ;struct timeval *tv
mov x1,#0x0 ;struct timezonze *tzor
adrp x8,0x109499000
ldr x8,[x8, #0x1d0]
blr x8 ;gettimeofday(tval,tzone)
ldr x8,[sp, #0x1b8] ;tval->tv_sec
mov w9,#0x3e8
mul x8,x8,x9
ldrsw x9,[sp, #0x1c0] ;tval->tv_u
lsr x9,x9,#0x3
mov x10,#0xf7cf
movk x10,#0xe353, LSL #16
movk x10,#0x9ba5, LSL #32
movk x10,#0x20c4, LSL #48
umulh x9,x9,x10
mov x10,#0xe6b3
movk x10,#0x7dba, LSL #16
movk x10,#0xecfa, LSL #32
movk x10,#0xd0e1, LSL #48
add x9,x10,x9, LSR #0x4
orr x11,x9,x8
lsl x11,x11,#0x1
eor x8,x9,x8
sub x8,x11,x8
eor x9,x8,x10
mov x10,#0xe6b3
movk x10,#0x7dba, LSL #16
movk x10,#0xecfa, LSL #32
movk x10,#0x50e1, LSL #48
bic x8,x10,x8
sub x8,x9,x8, LSL #0x1 ;tv_sec *= 1000
```

Timeout: 1h

- cvc5
- DryadSynth
- Syntia
- Xyntia

XSmir

2ms

Expression: y = x * 1000

Tigress example

```
push   %rbp
mov    %rsp,%rbp
mov    %edi,-0x14(%rbp)
mov    %esi,-0x18(%rbp)
mov    -0x14(%rbp),%eax
imul   $0x6aa7671b,%eax,%eax
add    $0x52f20197,%eax
mov    %eax,-0x4(%rbp)
mov    -0x18(%rbp),%eax
imul   $0x6aa7671b,%eax,%eax
add    $0x52f20197,%eax
mov    %eax,-0x8(%rbp)
mov    -0x4(%rbp),%eax
imul   -0x8(%rbp),%eax
imul   $0xd2d29b13,%eax,%edx
mov    -0x4(%rbp),%eax
imul   $0x253574cb,%eax,%eax
add    %eax,%edx
mov    -0x8(%rbp),%eax
imul   $0x253574cb,%eax,%eax
add    %edx,%eax
sub    $0x42f0ad26,%eax
mov    %eax,-0xc(%rbp)
mov    -0xc(%rbp),%eax
pop    %rbp
ret
```

Timeout: 1h

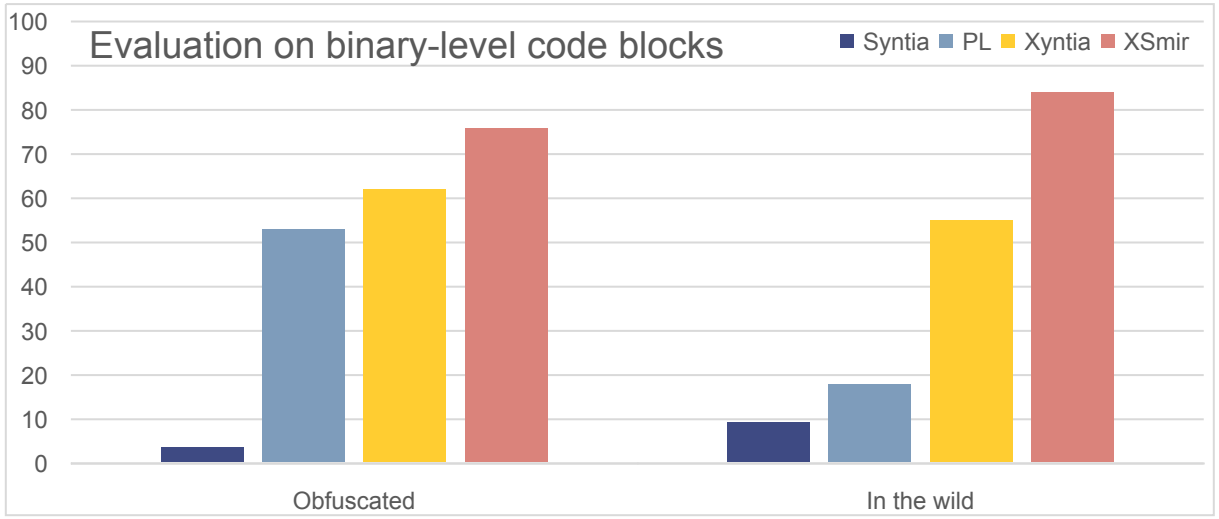
- cvc5
- DryadSynth
- Syntia
- Xyntia

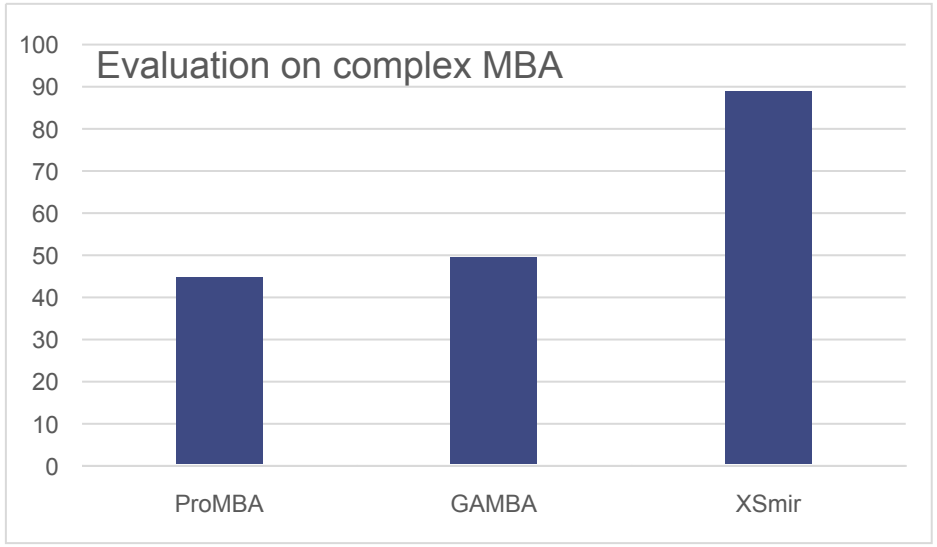
XSmir

500ms

Expression: z = x * y * 0x6aa7671b + 0x52f20197

Experimental Results Summary





↳ Obfuscated binaries : **76%** vs. **63%** vs **53%** vs **4%**

VMProtect software

RUHR UNIVERSITÄT BOCHUM RUB

APT28 FANCY BEAR

↳ In-the-wild binaries: **84%** vs **55%** vs **18%** vs **9%**

curl://

OpenSSL Cryptography and SSL/TLS Toolkit

FFmpeg

↳ Complex MBA: **90%** vs. **50%**

⊕ XSmir is black-box and general purpose

Also: Divides by 2 the number of false positives

Using Xyntia in Practice

```
0000000000001129 <obfuscated>:
  1129:  f3 0f 1e fa      endbr64
  112d:  55               push   rbp
  112e:  48 89 e5         mov    rbp,rsp
  1131:  89 7d fc         mov    DWORD PTR [rbp-0x4],edi
  1134:  89 75 f8         mov    DWORD PTR [rbp-0x8],esi
  1137:  8b 45 f8         mov    eax,DWORD PTR [rbp-0x8]
  113a:  f7 d0            not    eax
  113c:  23 45 fc         and    eax,DWORD PTR [rbp-0x4]
  113f:  89 c2            mov    edx,eax
  1141:  8b 45 f8         mov    eax,DWORD PTR [rbp-0x8]
  1144:  f7 d0            not    eax
  1146:  29 c2            sub    edx,eax
   ...
  1447:  29 d0            sub    eax,edx
  1449:  01 c0            add    eax,eax
  144b:  01 c8            add    eax,ecx
  144d:  5d               pop    rbp
  144e:  c3               ret
```

Xyntia Script

starting from 0x1129

explore all

hook 0x144e with
  sample 100 eax
  halt
end

```
→ xyntia git:(main) xyntia -bin binary.exe -config script

expression: (mem_1<32> + mem_0<32>)
simplified: (mem_1<32> + mem_0<32>)
smtlib: (bvadd mem_1 mem_0)
output: eax<32>
success: yes
synthesis time: 0.000251
equiv: yes
```

eax.json / eax.sl / formula

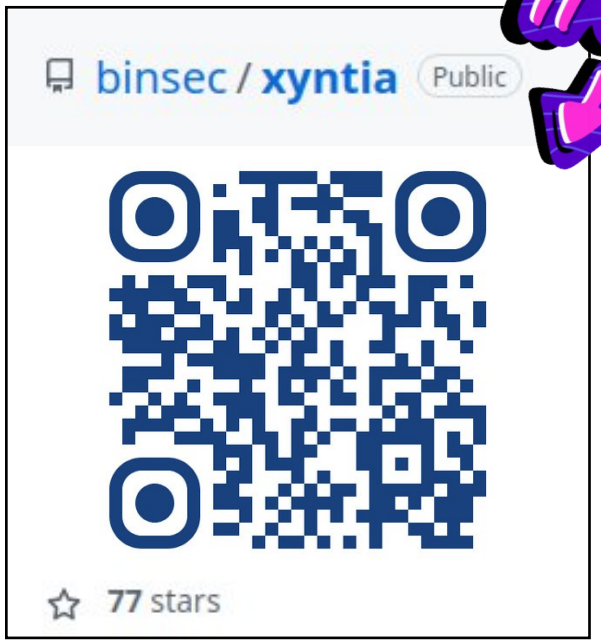
```
→ cvc5 ./cvc5 eax.sl

(define-fun f ((mem_1 (_ BitVec 32)) (mem_0 (_ BitVec 32)))
      (_ BitVec 32) (bvadd mem_1 mem_0))
```

Conclusion

– **Xyntia black-box deobfuscation framework**

↳ **Efficient synthesizer on the BV theory**
> Synthesis as an optimization problem
> Additional features: CEGIS, SyGUS2 output

↳ **Search Modulo Inference Rules (SMIR)**
> Inference rules to guide the search & elevate expressions to the solution
> Allow to apply Black-box deobf. beyond VM-handlers



BINSEC

https://binsec.github.io/

Internships
(apply quickly)