Developing Cost-Effective Combinations of Static Analysis Techniques

Minseok Jeon

DGIST

October 16, 2025
@ Dagstuhl, Germany

Analysis techniques are usually developed and evaluated **independently**

An **Issue** in the Current Trend of Developing Static Analysis Techniques

Minseok Jeon

DGIST

October 16, 2025
@ Dagstuhl, Germany

Program

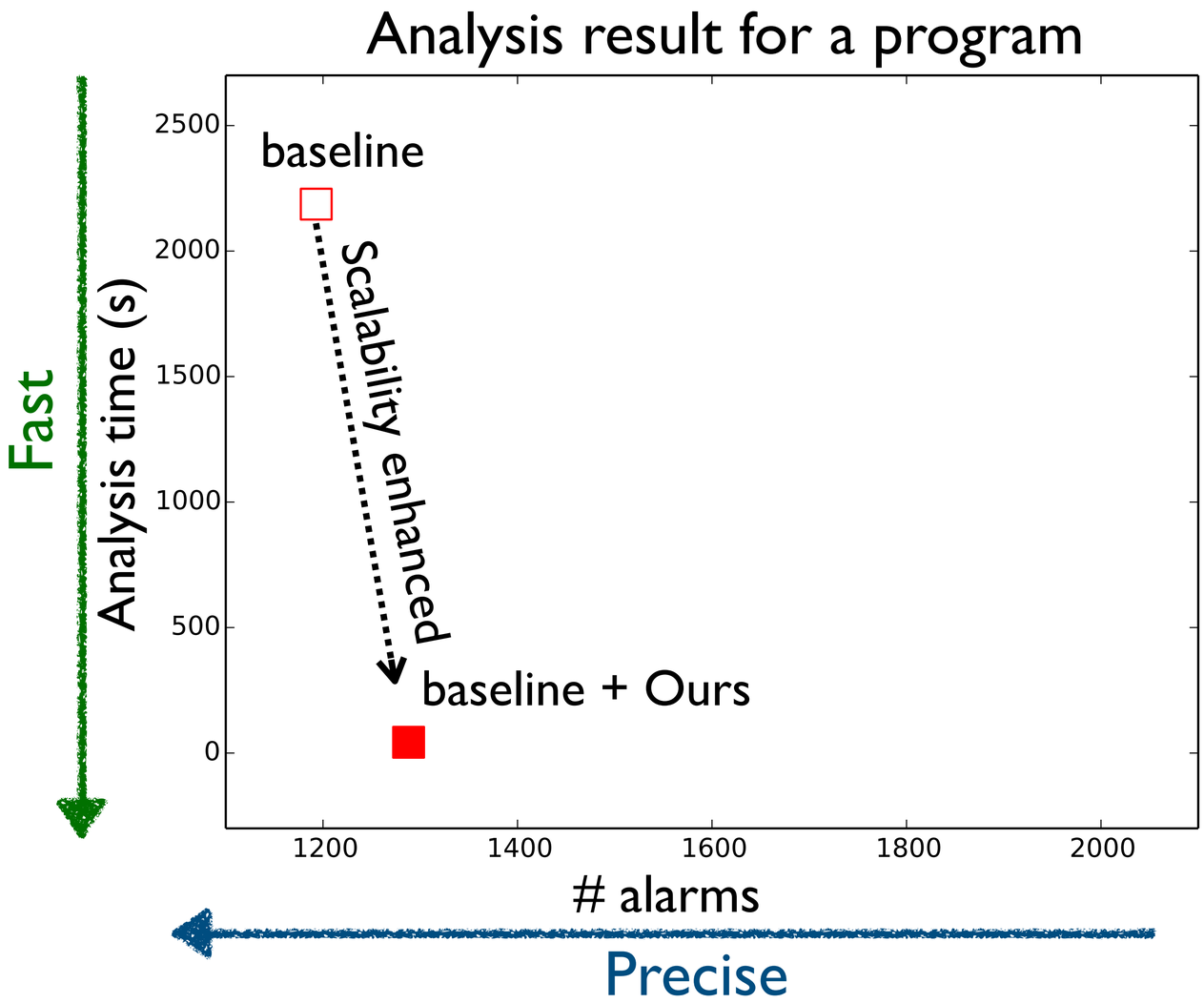
Sound Static Program Analyzer

Precise & Scalable Analysis Results

- Effective static program analyzers require various techniques
  - Partial flow sensitivity techniques [Jeon et al. 2019]
  - Selective context sensitivity techniques [Jeon et al. 2017, 2020]
  - Context tunneling techniques [Jeon et al. 2018, 2022]
  - …

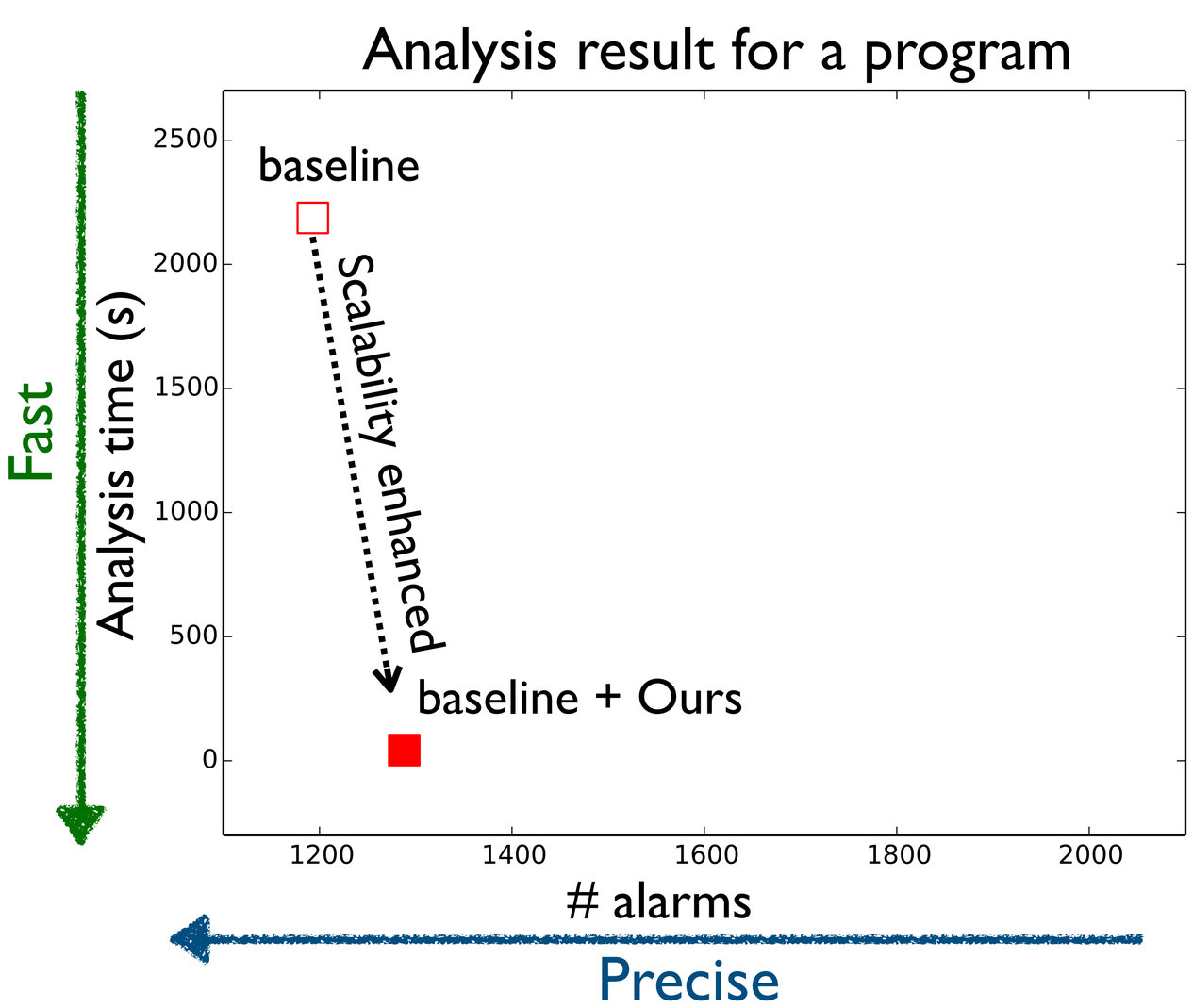
Research Scenario

(1) Develop an analysis technique that enhances the performance of a baseline analysis



Research Scenario

(2) Write a paper showing the effectiveness of our technique when applied to the baseline



Paper Scenario

We present a new static analysis technique

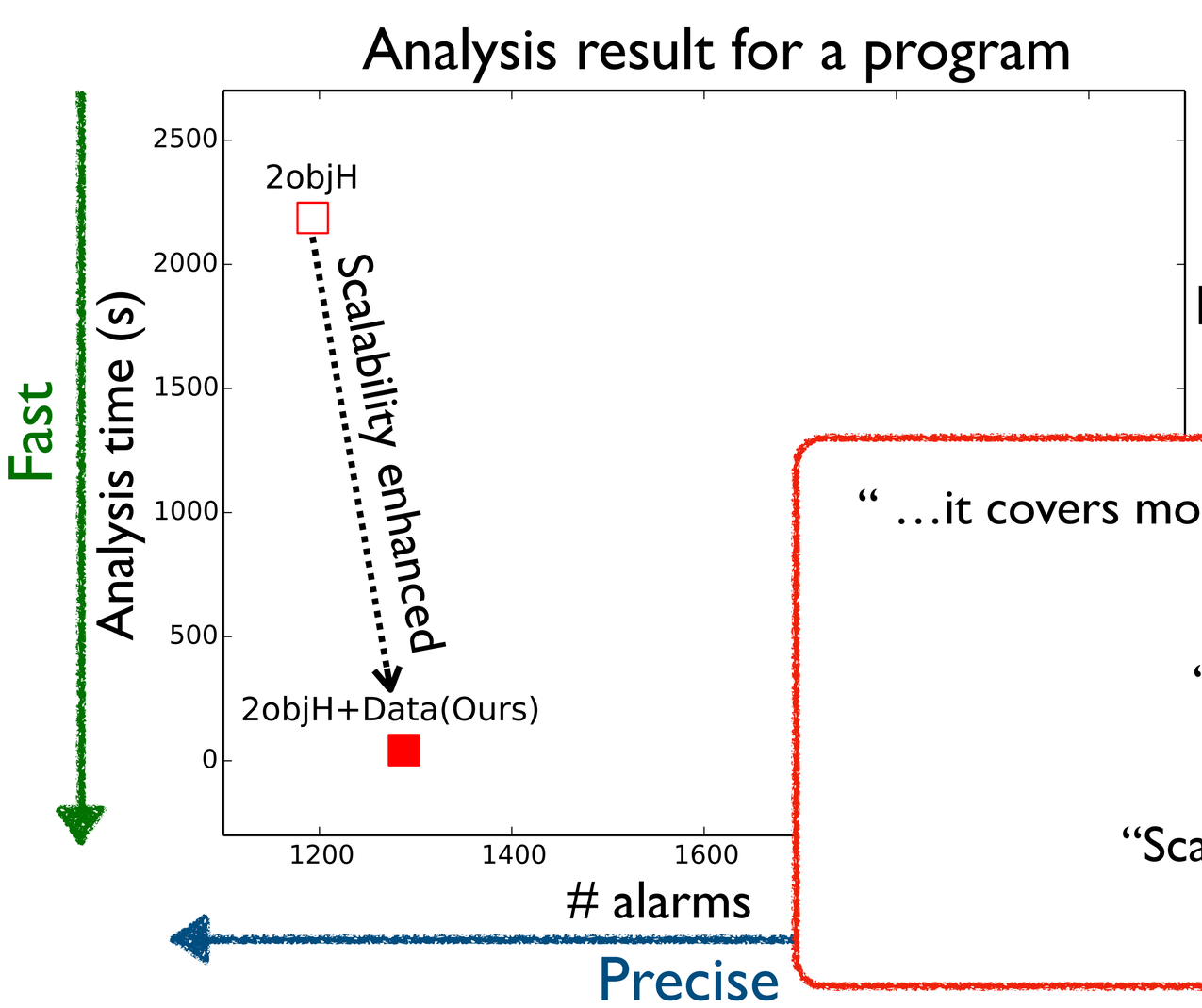
↓

Our technique enhanced scalability of the **baseline**

Vanilla analysis

Research Scenario

(2) Write a paper showing the effectiveness of our technique when applied to the baseline



Paper Scenario

We present a new static analysis technique

↓

Our technique enhanced scalability of the **baseline**

Vanilla analysis

" …it covers more than two-thirds of the precision advantage of 2objH"

-Smaragdakis et al. [PLDI' 14]

"… 98.8% of the precision of 2obj can be preserved…"

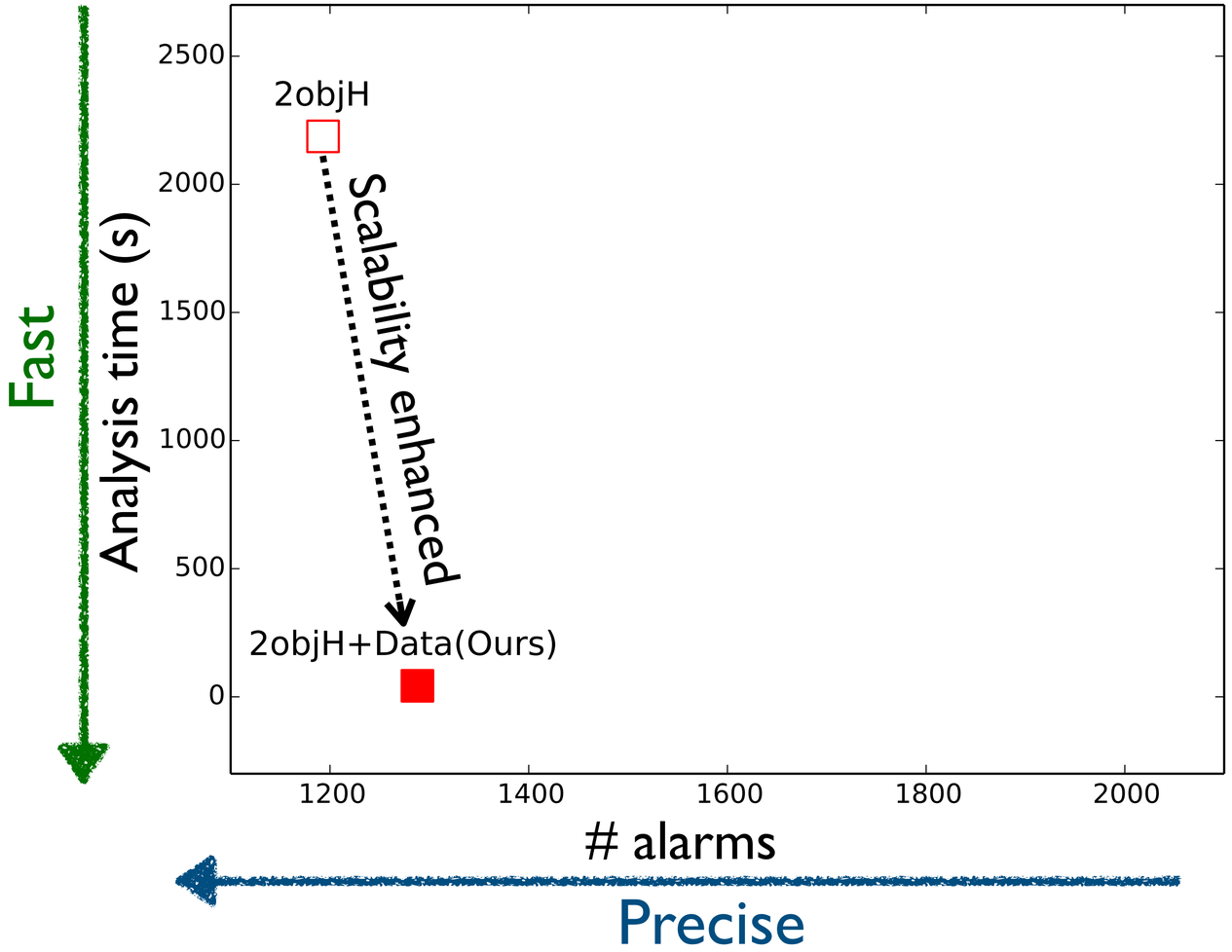
-Li et al. [OOPSLA' 18]

"Scaler still attains most of the precision gains of 2obj …"

-Li et al. [FSE' 18]

Research Scenario

(3) Get review comments and incorporate them into the revision



Paper Scenario

We present a new static analysis technique

↓

Our technique enhanced scalability of the **baseline**

Vanilla analysis

Review comments

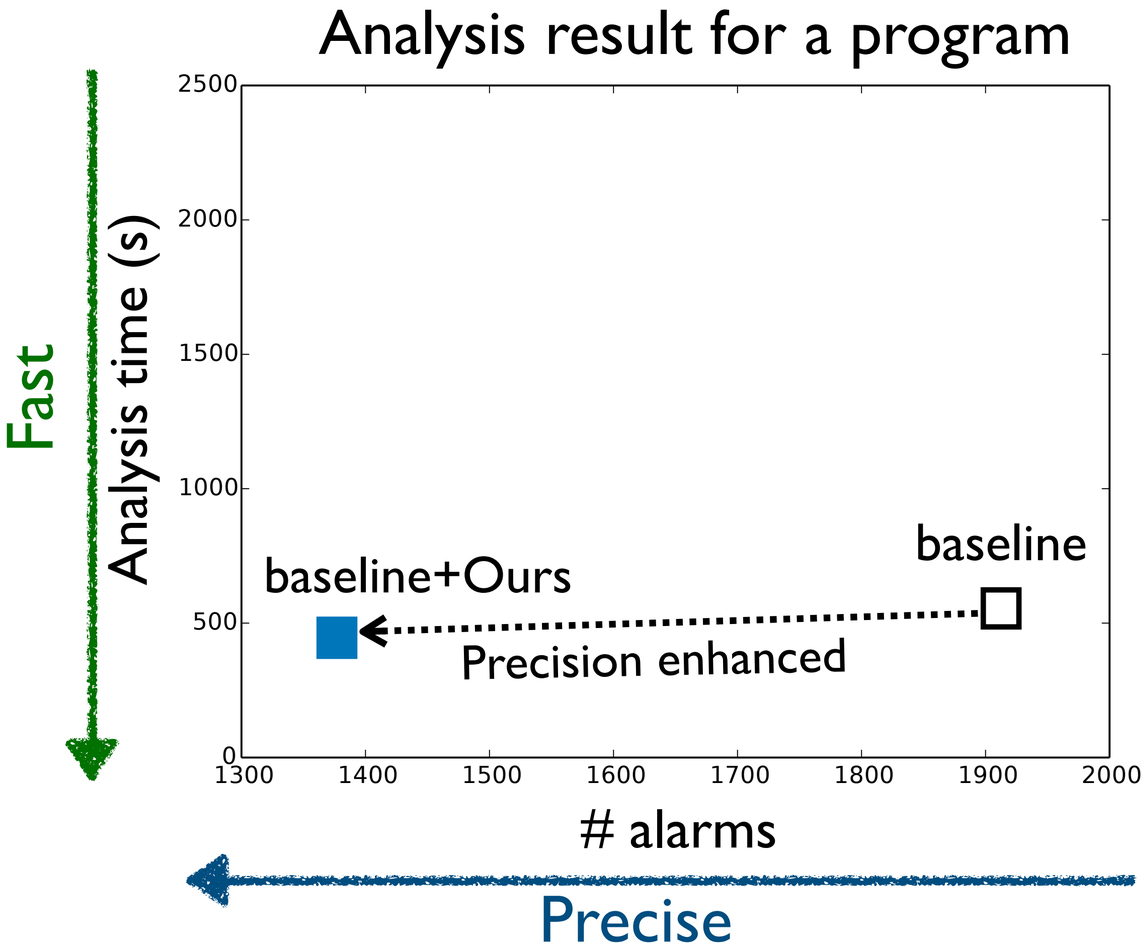
Check whether the idea is interesting

↓

Check whether the technique sufficiently enhances **baseline**

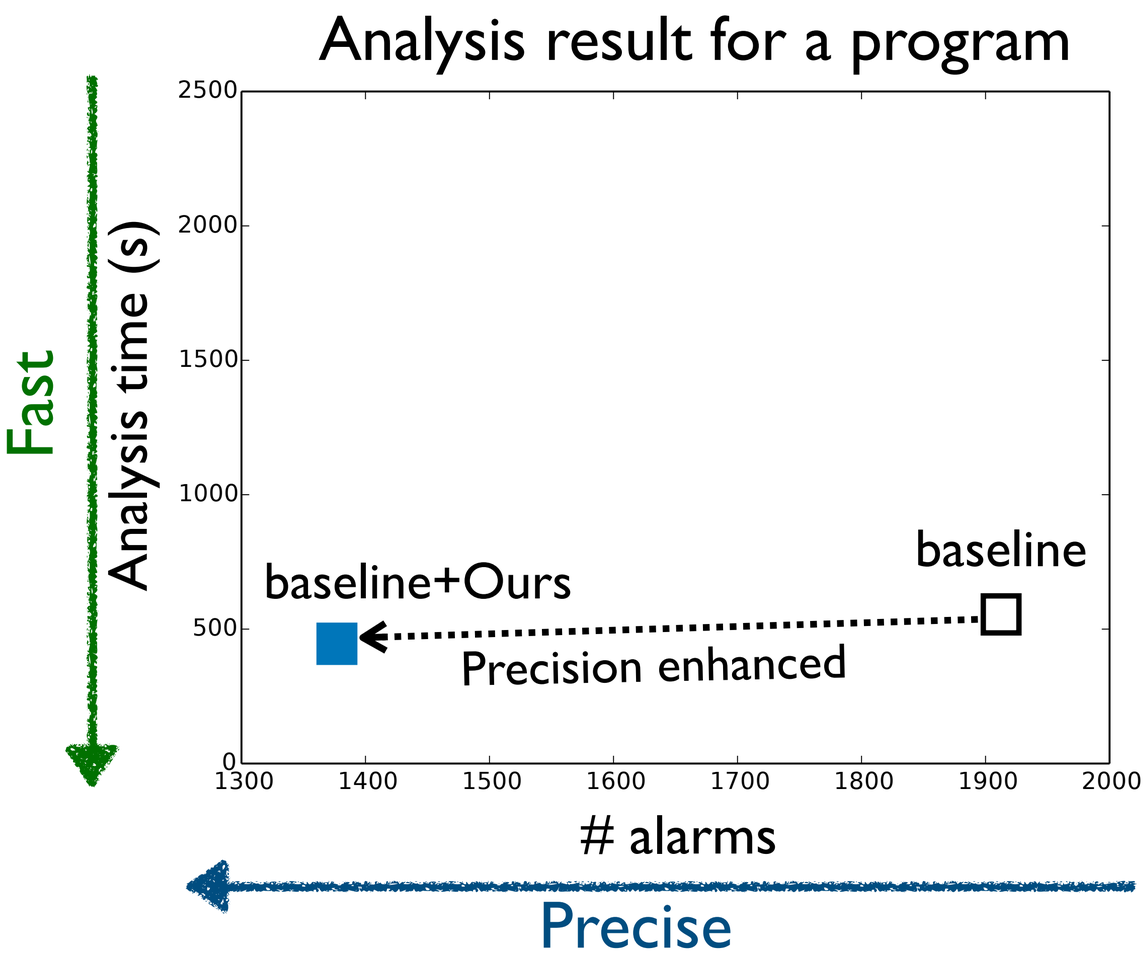
Research Scenario

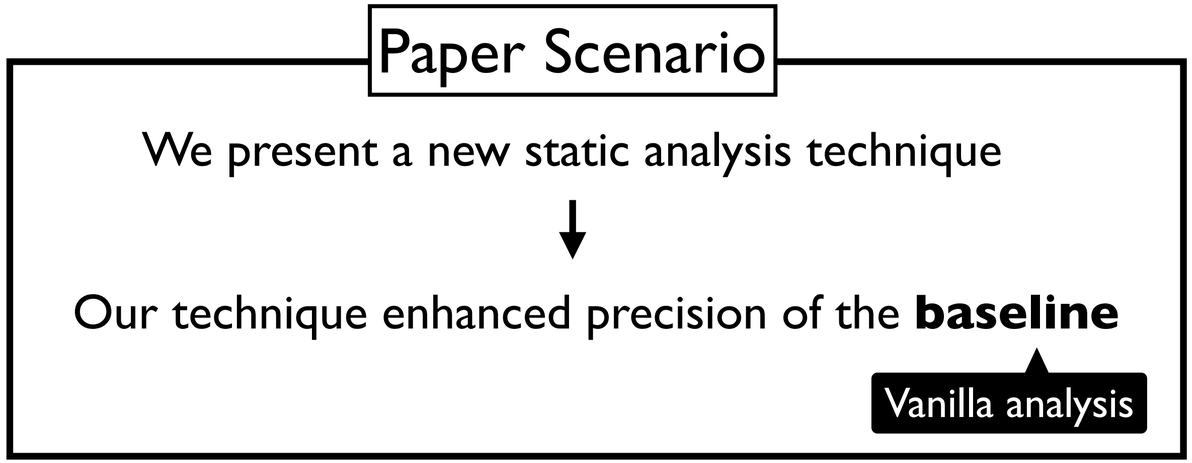
(1) Develop an analysis technique that enhances the performance of a baseline analysis



Research Scenario

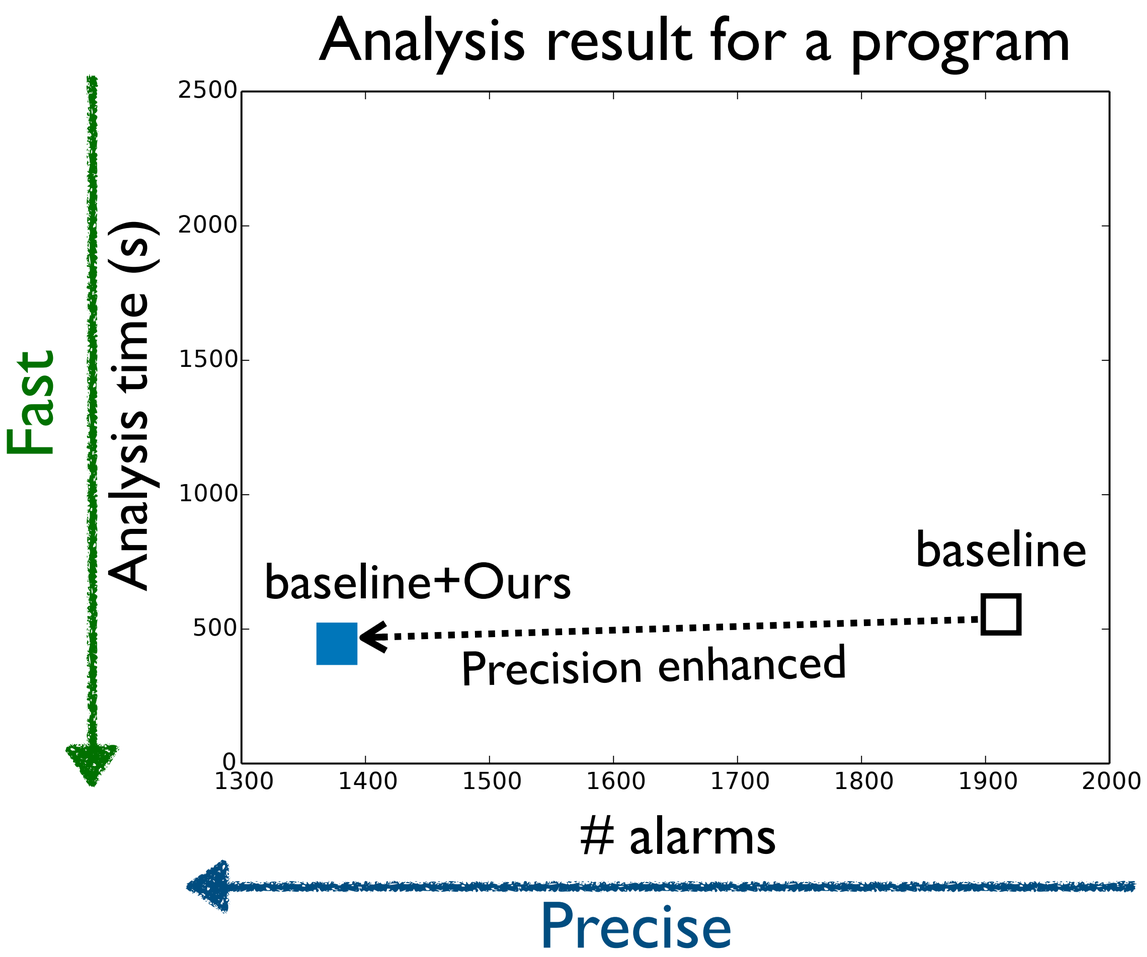
(2) Write a paper showing the effectiveness of our technique when applied to the baseline





Research Scenario

(3) Get review comments and incorporate them into the revision



Paper Scenario

We present a new static analysis technique

↓

Our technique enhanced precision of the **baseline**

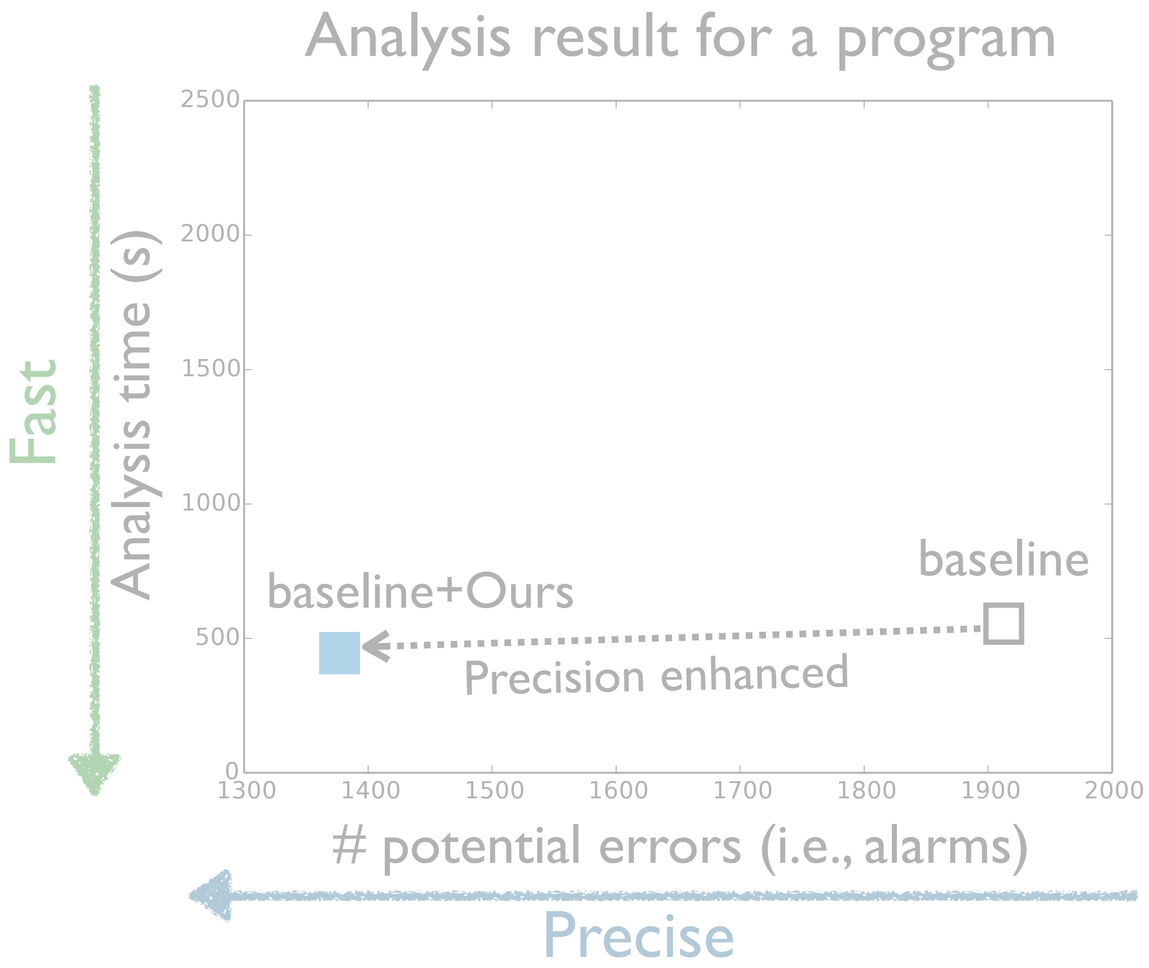
Vanilla analysis

Review comments

Check whether the idea is interesting

↓

Check whether the technique sufficiently enhances **baseline**



Paper Scenario

We present a new static analysis technique

↓

Our technique enhanced precision of the **baseline**

Vanilla analysis

Review comments

This paper presents a new technique

↓

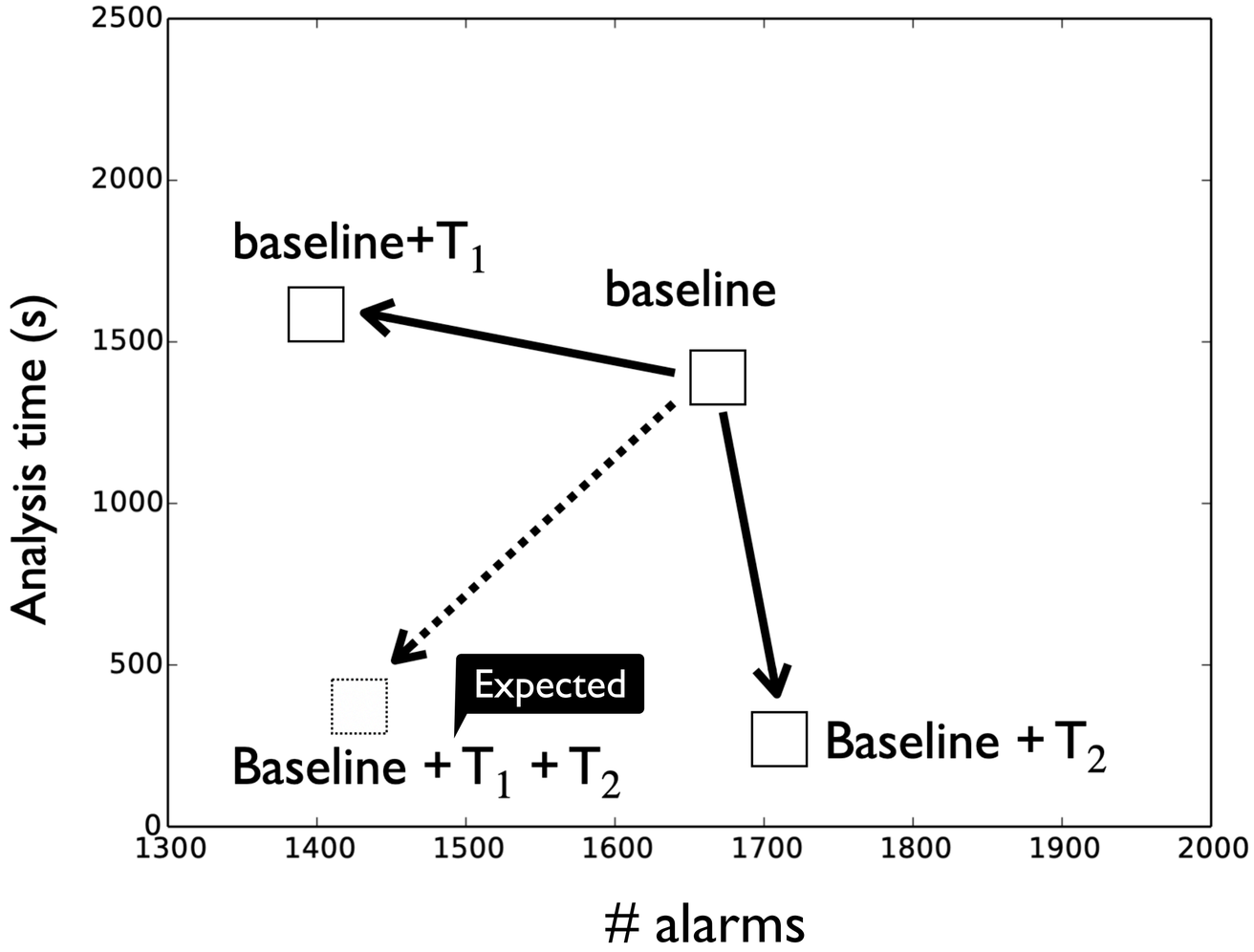
Excellent improvements in precision

Underlying assumption

Individually optimized techniques will also perform effective when combined.

Research Question

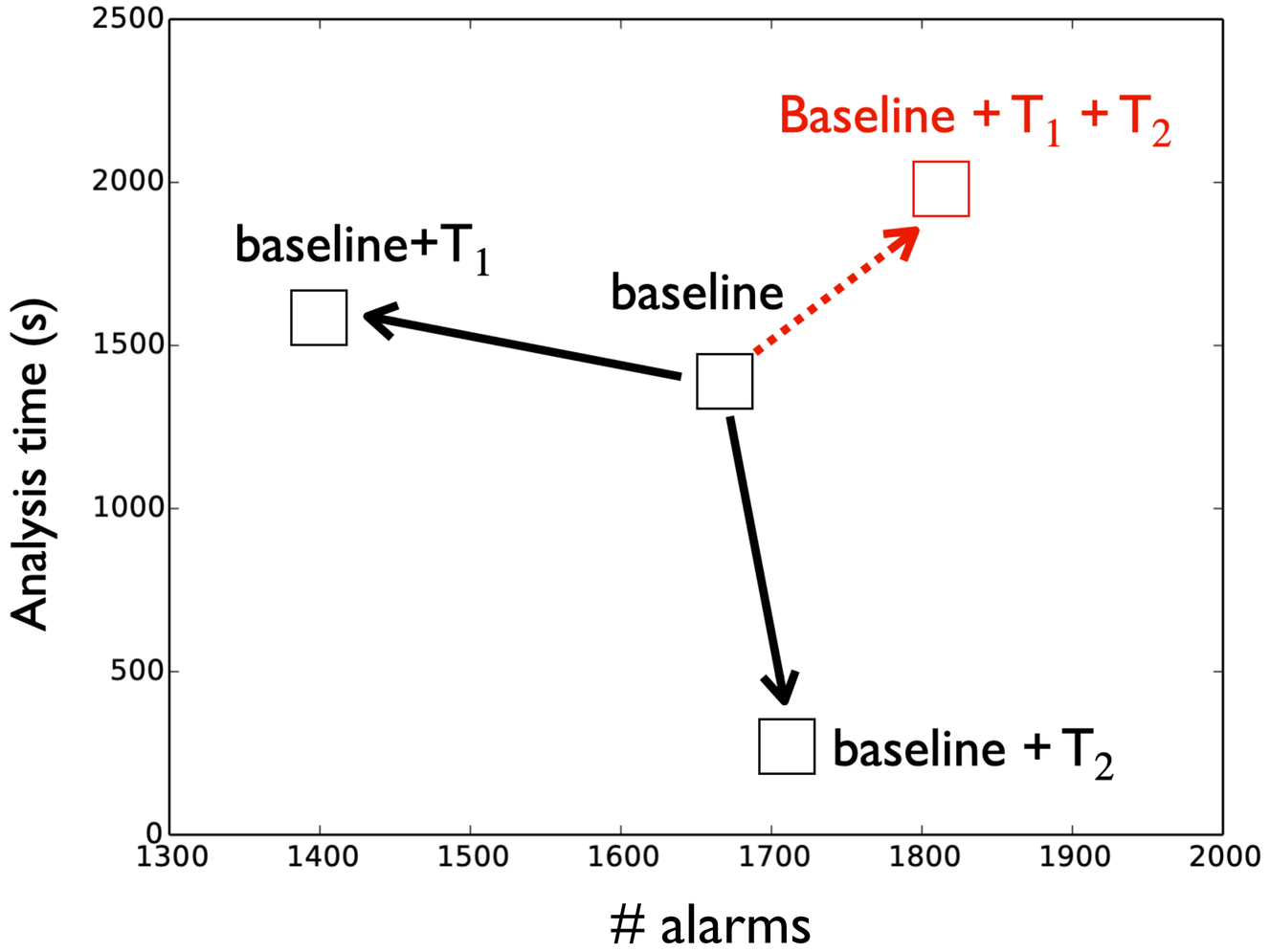
- Does a combination of individually effective techniques achieve effective performance?



Research Question

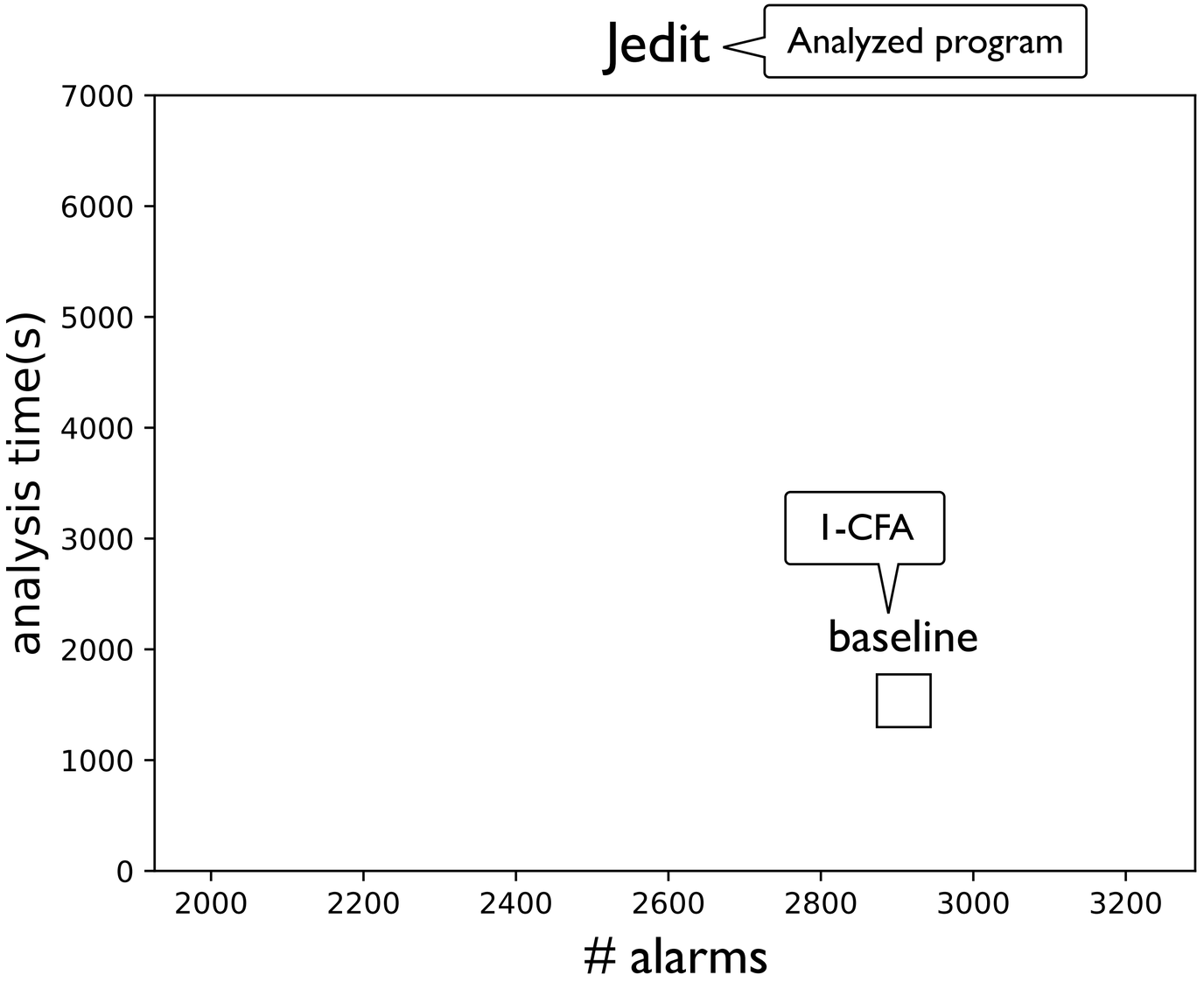
- Does a combination of individually effective techniques achieve effective performance?

No



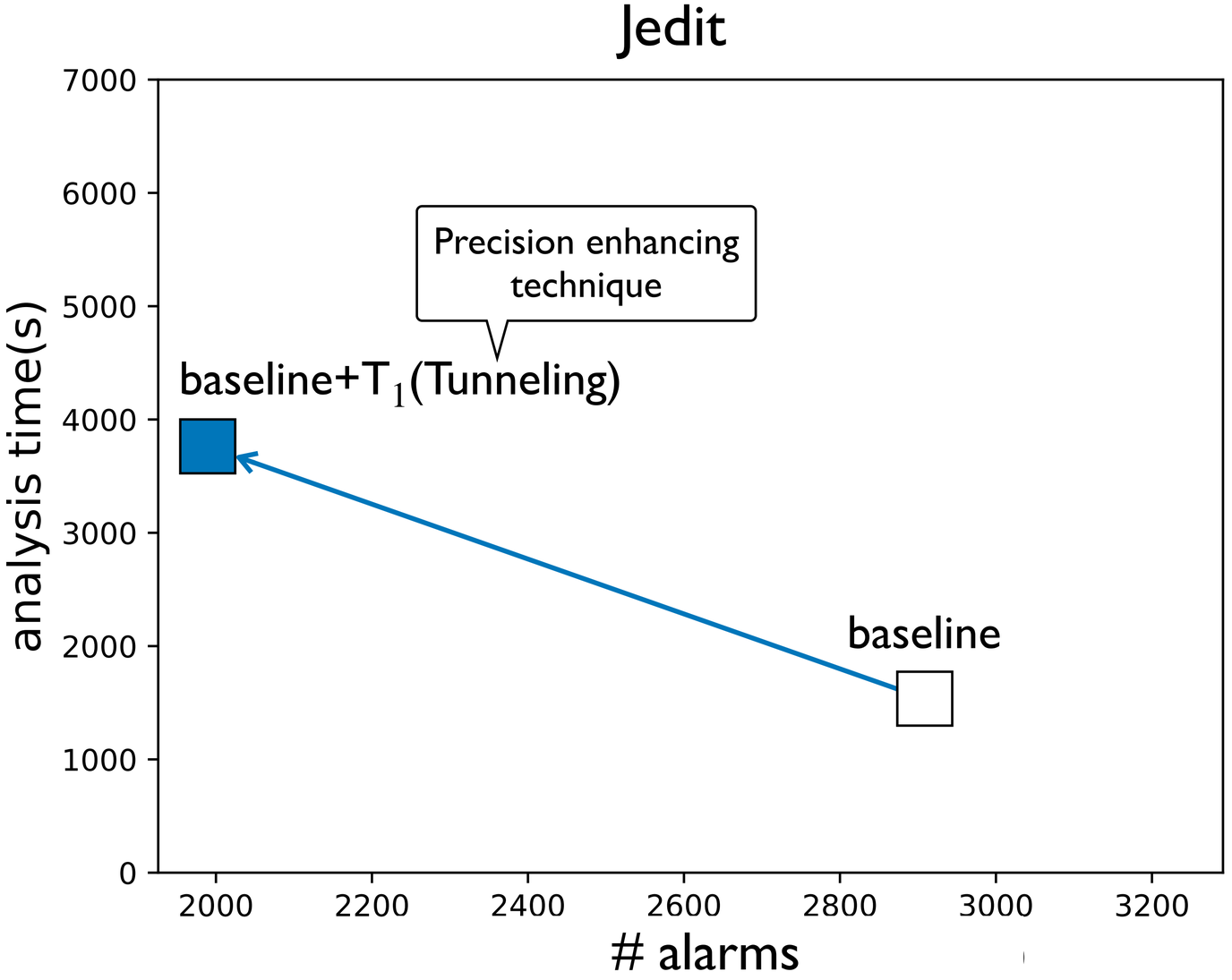
Experimental Results

- Combination of existing SOTA techniques achieve suboptimal performance



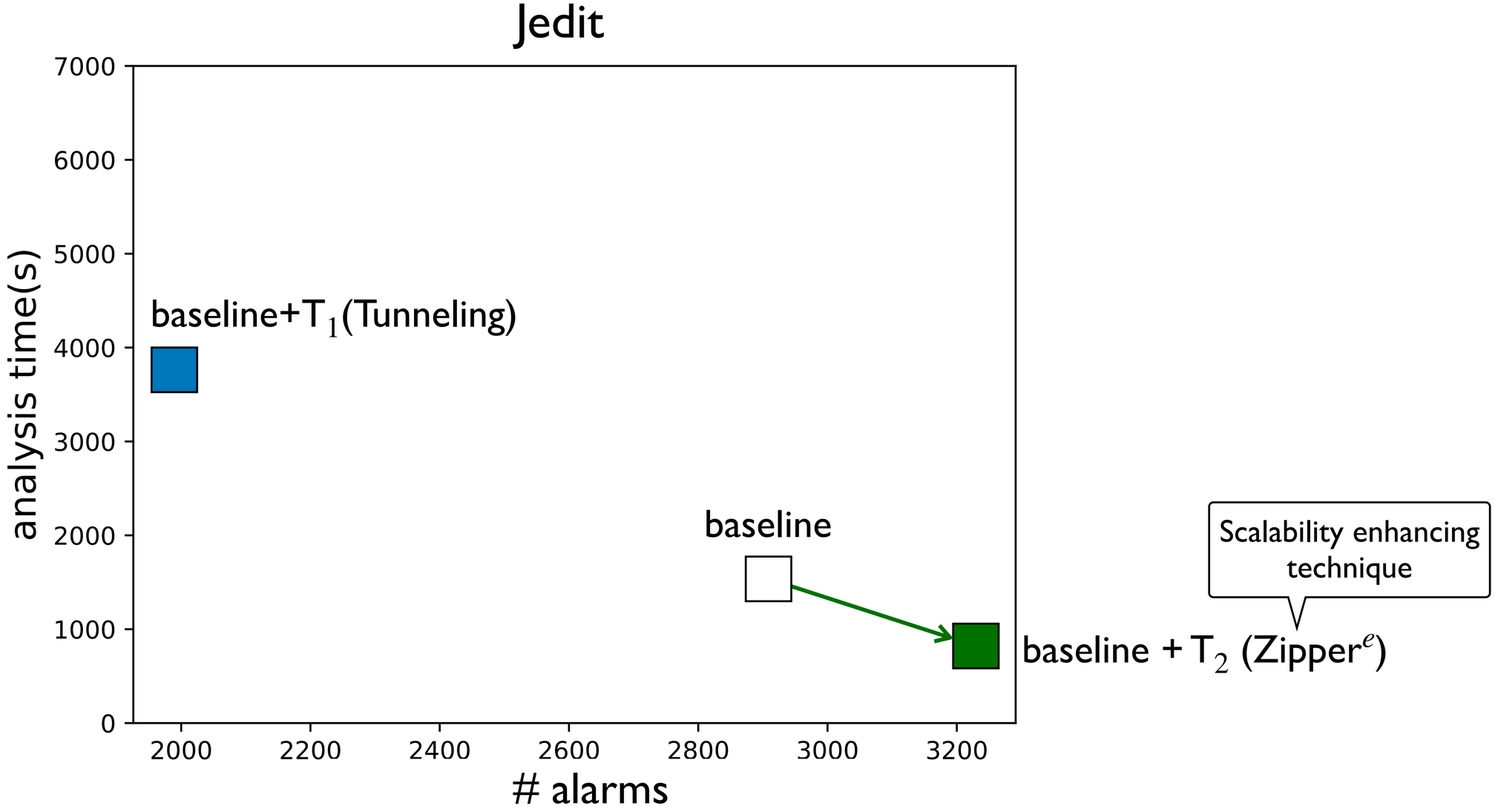
Experimental Results

- Combination of existing SOTA techniques achieve suboptimal performance



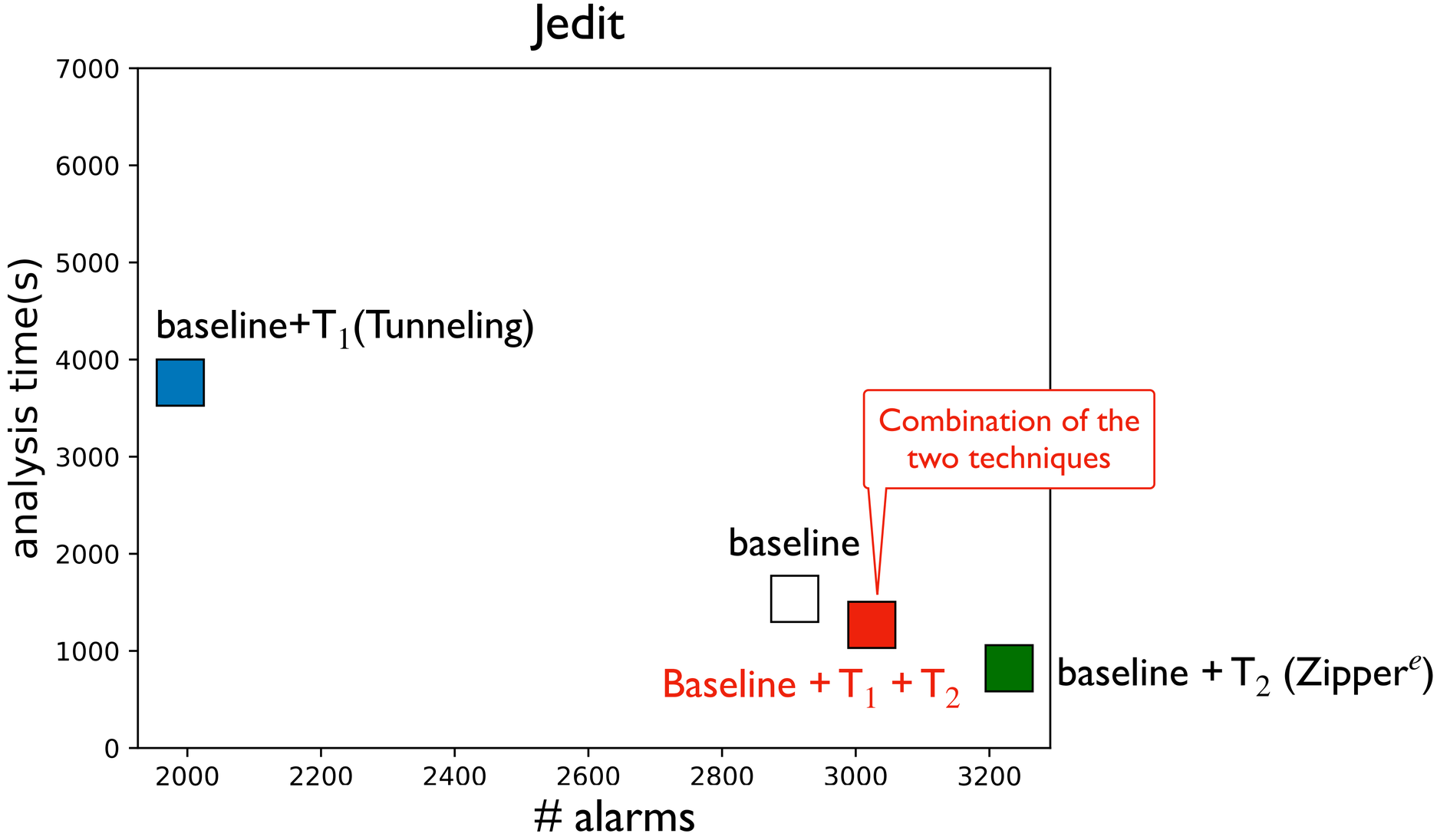
Experimental Results

- Combination of existing SOTA techniques achieve suboptimal performance



Experimental Results

- Combination of existing SOTA techniques achieve suboptimal performance

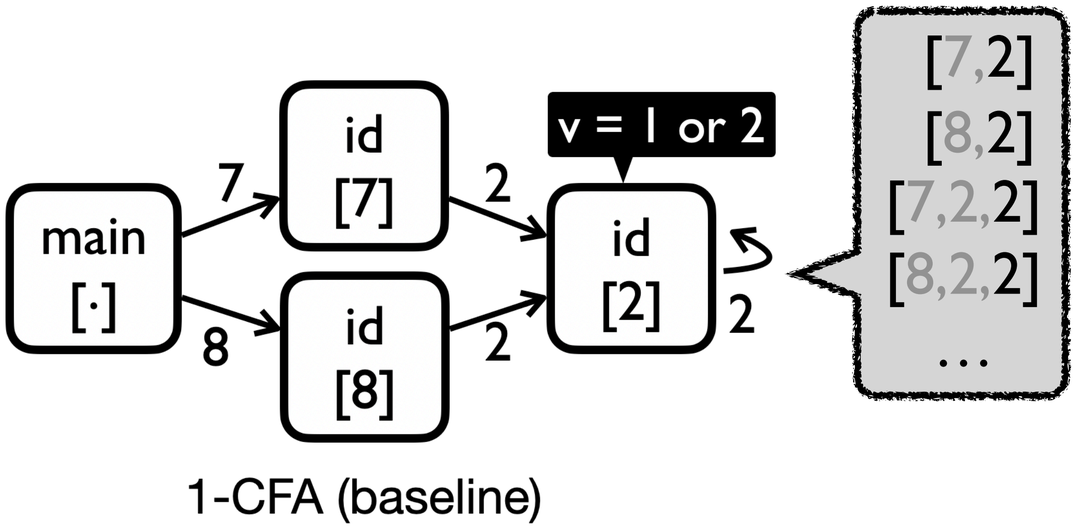


Counterexample

- Combining individually ideal techniques does not result in ideal performance

```
0:  id(v, i){
1:    if (i > 0){
2:      return id(v, i-1);}
3:    return v;}
4:
5:  main(){
6:    i = input();
7:    v1 = id(1, i);
8:    v2 = id(2, i);
9:    assert (v1 != v2);//query
10: }
```

Example program



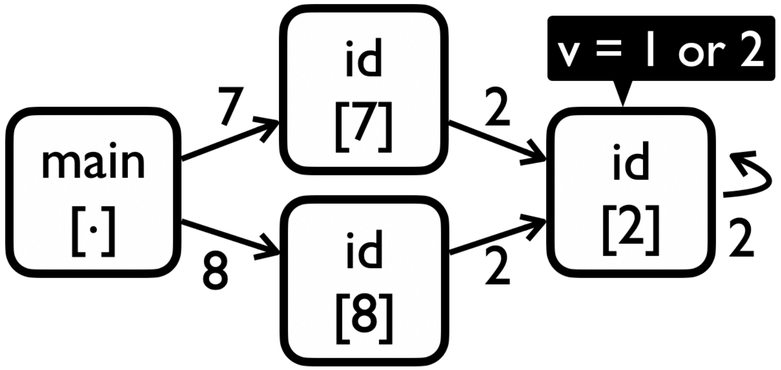
1-CFA (baseline)

Counterexample

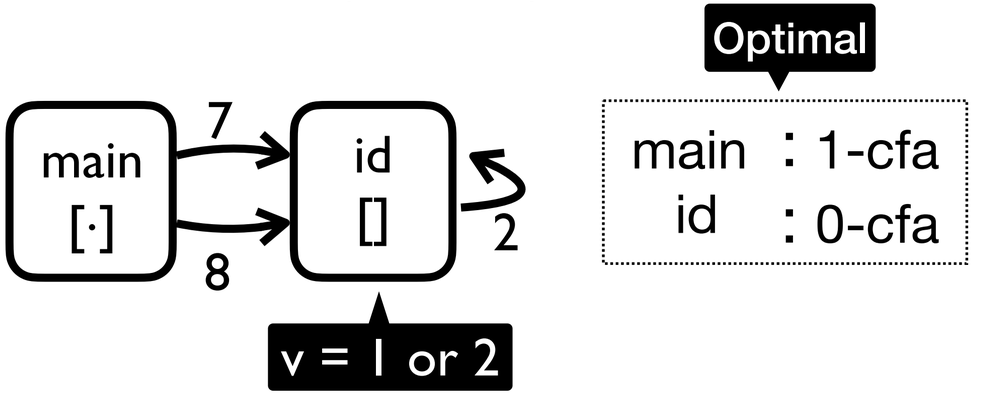
- Selective ctx sensitivity improves scalability by selectively analyzing methods coarsely

```
0:  id(v, i){
1:    if (i > 0){
2:      return id(v, i-1);}
3:    return v;}
4:
5:  main(){
6:    i = input();
7:    v1 = id(1, i);
8:    v2 = id(2, i);
9:    assert (v1 != v2);//query
10: }
```

Example program



1-CFA (baseline)



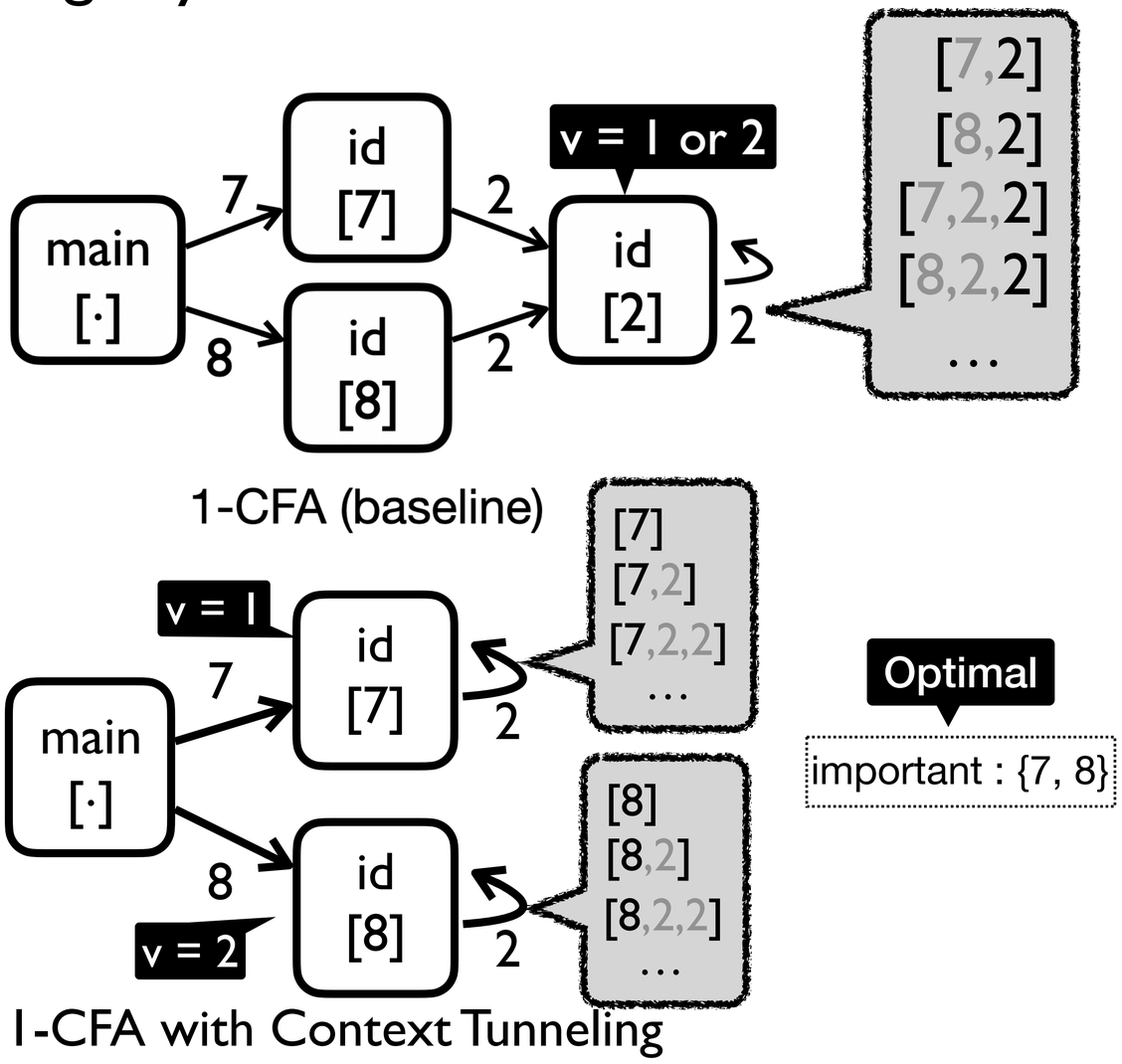
1-CFA with Selective Ctx Sensitivity

Counterexample

- Context tunneling improves precision by keeping key context elements

```
0:  id(v, i){
1:    if (i > 0){
2:      return id(v, i-1);}
3:    return v;}
4:
5:  main(){
6:    i = input();
7:    v1 = id(1, i);
8:    v2 = id(2, i);
9:    assert (v1 != v2);//query
10: }
```

Example program

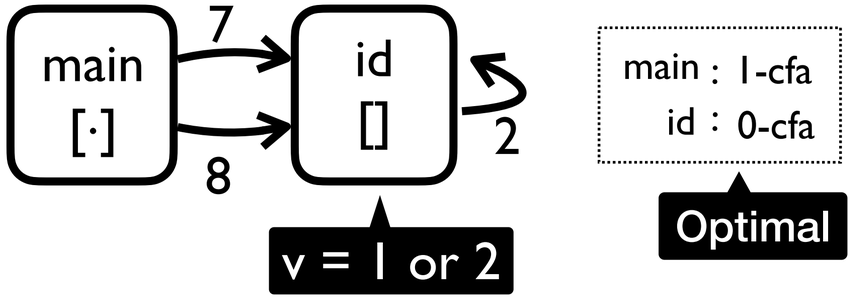


Counterexample

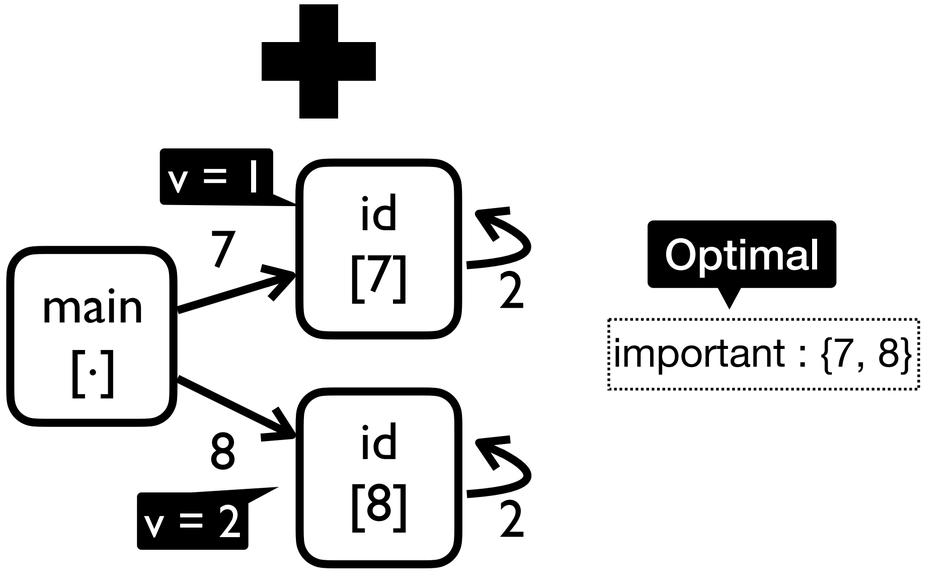
- Does combining individually ideal techniques also result in ideal performance?

```
0:  id(v, i){
1:    if (i > 0){
2:      return id(v, i-1);}
3:    return v;}
4:
5:  main(){
6:    i = input();
7:    v1 = id(1, i);
8:    v2 = id(2, i);
9:    assert (v1 != v2);//query
10: }
```

Example program



1-CFA with Selective Ctx Sensitivity



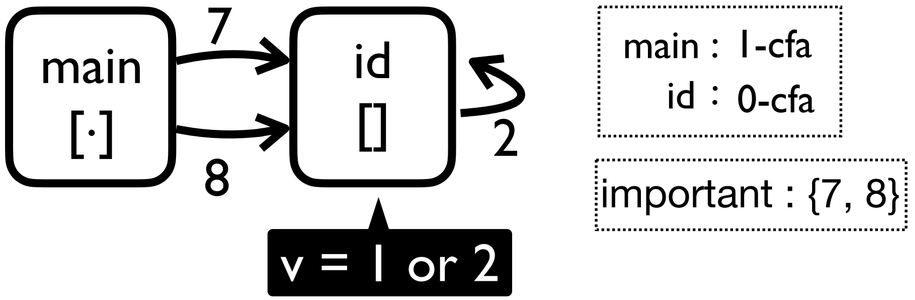
1-CFA with Context Tunneling

Counterexample

- Combining individually ideal techniques does not result in ideal performance

```
0:  id(v, i){
1:    if (i > 0){
2:      return id(v, i-1);}
3:    return v;}
4:
5:  main(){
6:    i = input();
7:    v1 = id(1, i);
8:    v2 = id(2, i);
9:    assert (v1 != v2);//query
10: }
```

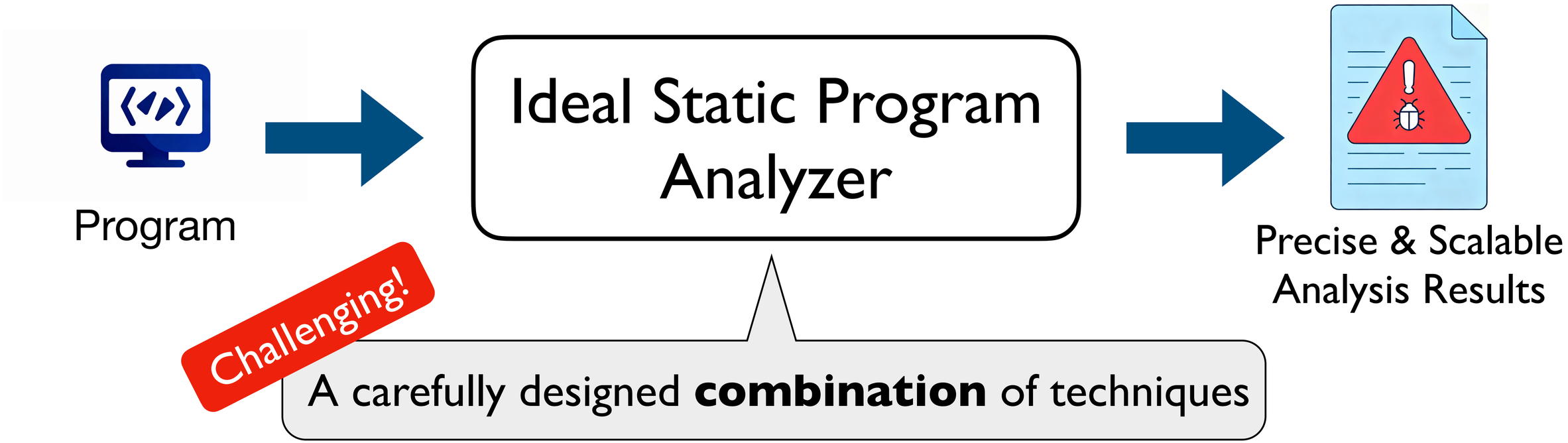
Example program



1-CFA with Selective + Tunneling

Problem

- Analysis techniques should be designed together with considering all their interactions



Our Solution

- We present a framework that safely reduces the burden of developing a combination of techniques

Enables sequential development

Our Solution

- We present a framework that safely reduces the burden of developing a combination of techniques
- Suppose we design a pair of precision improving and scalability improving techniques

e.g., context tunneling

e.g., selective ctx sensitivity

Our Solution

- We present a framework that safely reduces the burden of developing a combination of techniques
- Suppose we design a pair of precision improving and scalability improving techniques

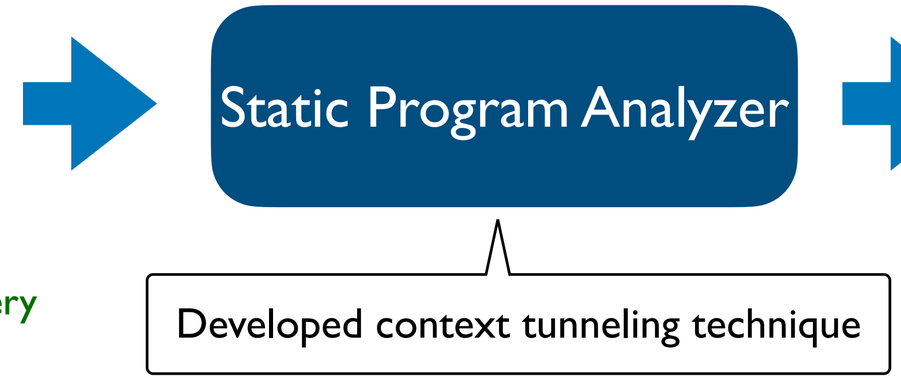
e.g., context tunneling

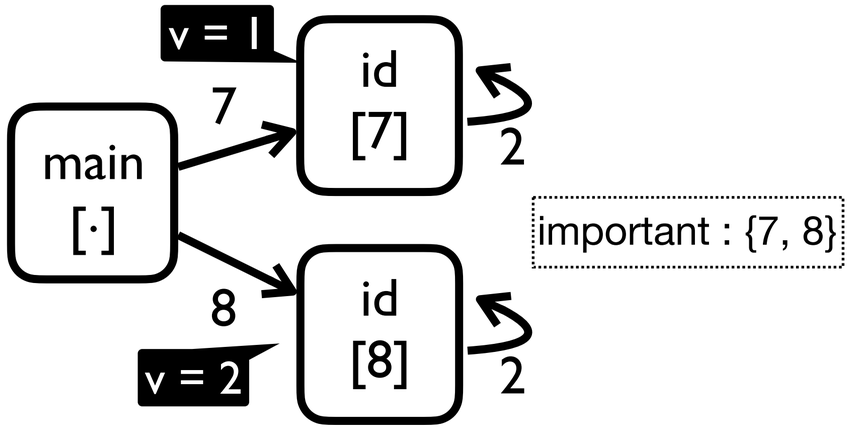
e.g., selective ctx sensitivity

(1) Develop a precision improving technique without considering the other technique

```
0:  id(v, i){
1:    if (i > 0){
2:      return id(v, i-1);}
3:    return v;}
4:
5:  main(){
6:    i = input();
7:    v1 = id(1, i);
8:    v2 = id(2, i);
9:    assert (v1 != v2);//query
10: }
```

Example program





1-CFA with Tunneling

Our Solution

- We present a framework that safely reduces the burden of developing a combination of techniques
- Suppose we design a pair of precision improving and scalability improving techniques

e.g., context tunneling

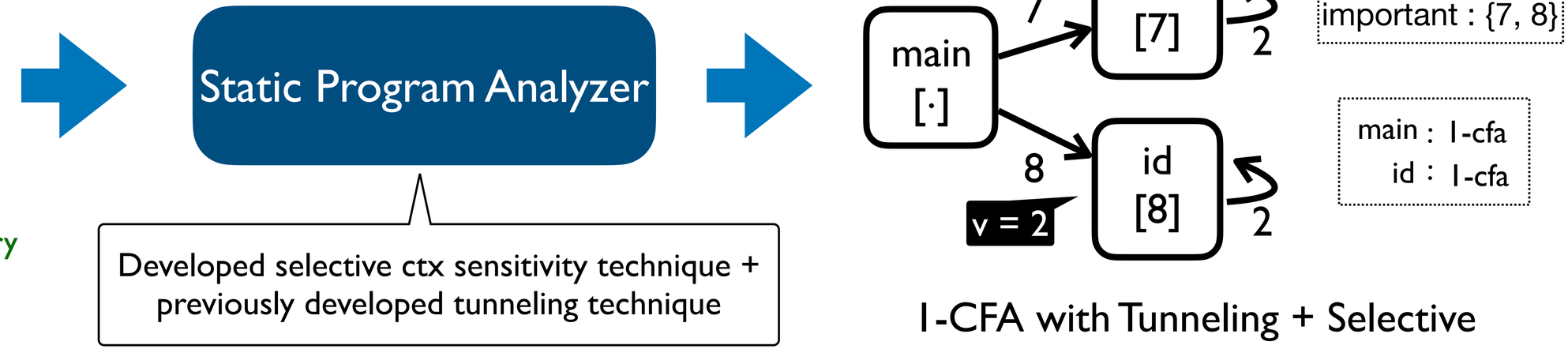
e.g., selective ctx sensitivity

(1) Develop a precision improving technique without considering the other technique

(2) Develop a scalability improving technique based-on the previously developed precision improving technique

```
0:  id(v, i){
1:    if (i > 0){
2:      return id(v, i-1);}
3:    return v;}
4:
5:  main(){
6:    i = input();
7:    v1 = id(1, i);
8:    v2 = id(2, i);
9:    assert (v1 != v2);//query
10: }
```

Example program



1-CFA with Tunneling + Selective

Our Solution

- We present a framework that safely reduces the burden of developing a combination of techniques
- Suppose we design a pair of precision improving and scalability improving techniques

e.g., context tunneling

e.g., selective ctx sensitivity

(1) Develop a precision improving technique without considering the other technique

(2) Develop a scalability improving technique based-on the previously developed precision improving technique

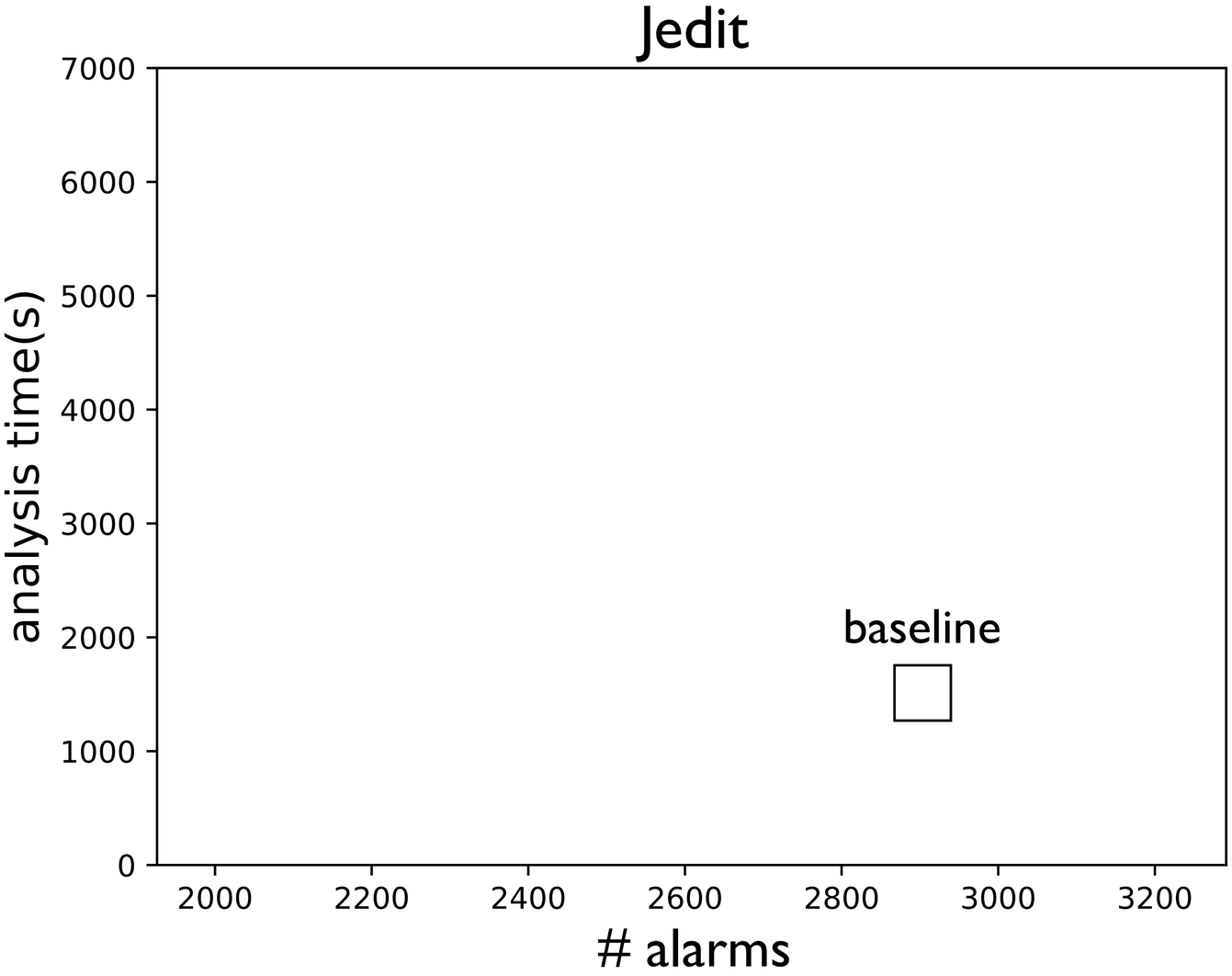
(3) Combine the two techniques

Theorem

Let T_1 be a tunneling technique which is ideal when used alone and T_2 be a selective context sensitivity technique which is ideal when used along with T_1, the the combination of the two techniques (T_1,T_2) is an ideal combination.

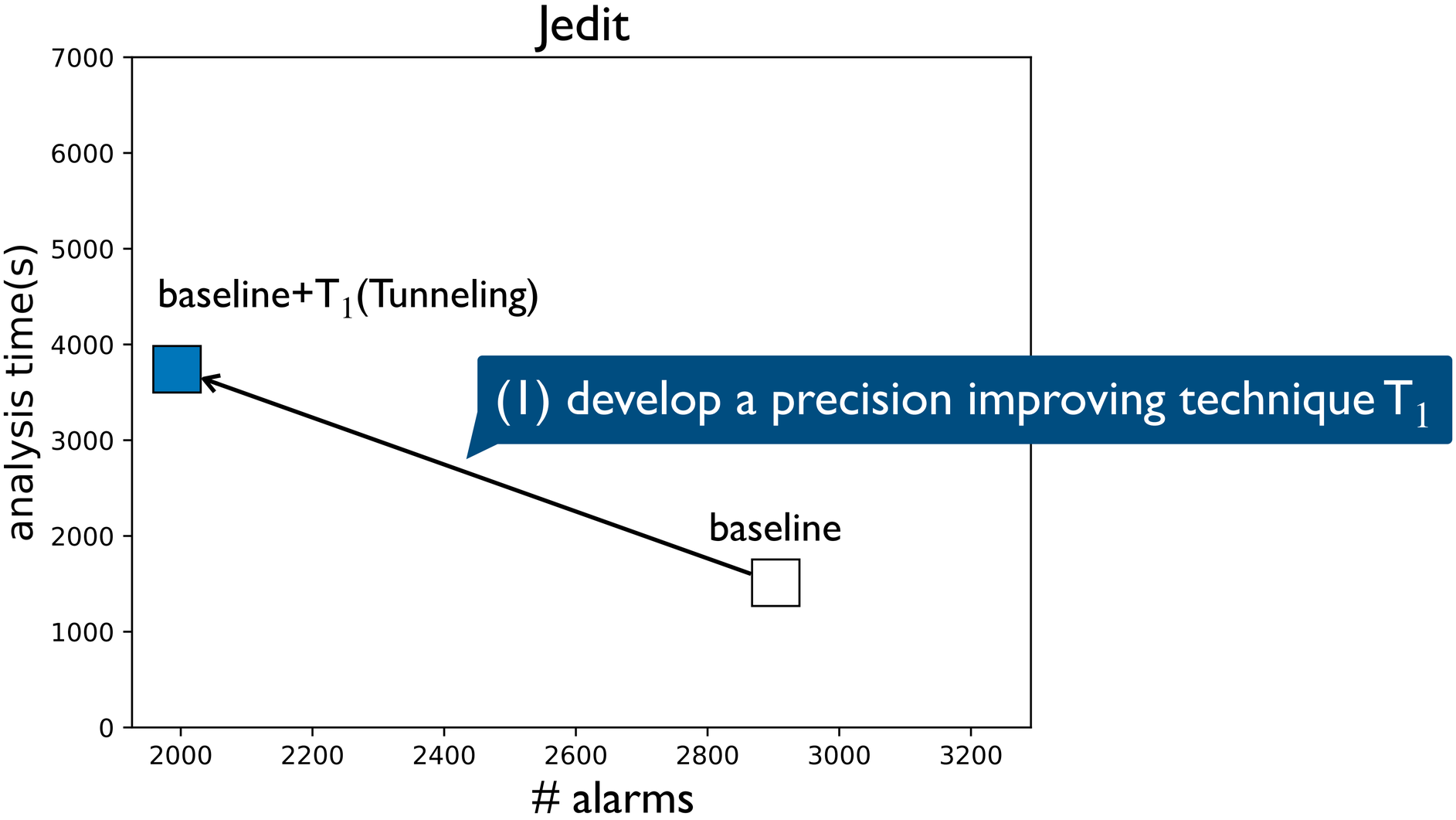
Experimental Results

- Following our framework enables developing an effective combination of the two techniques



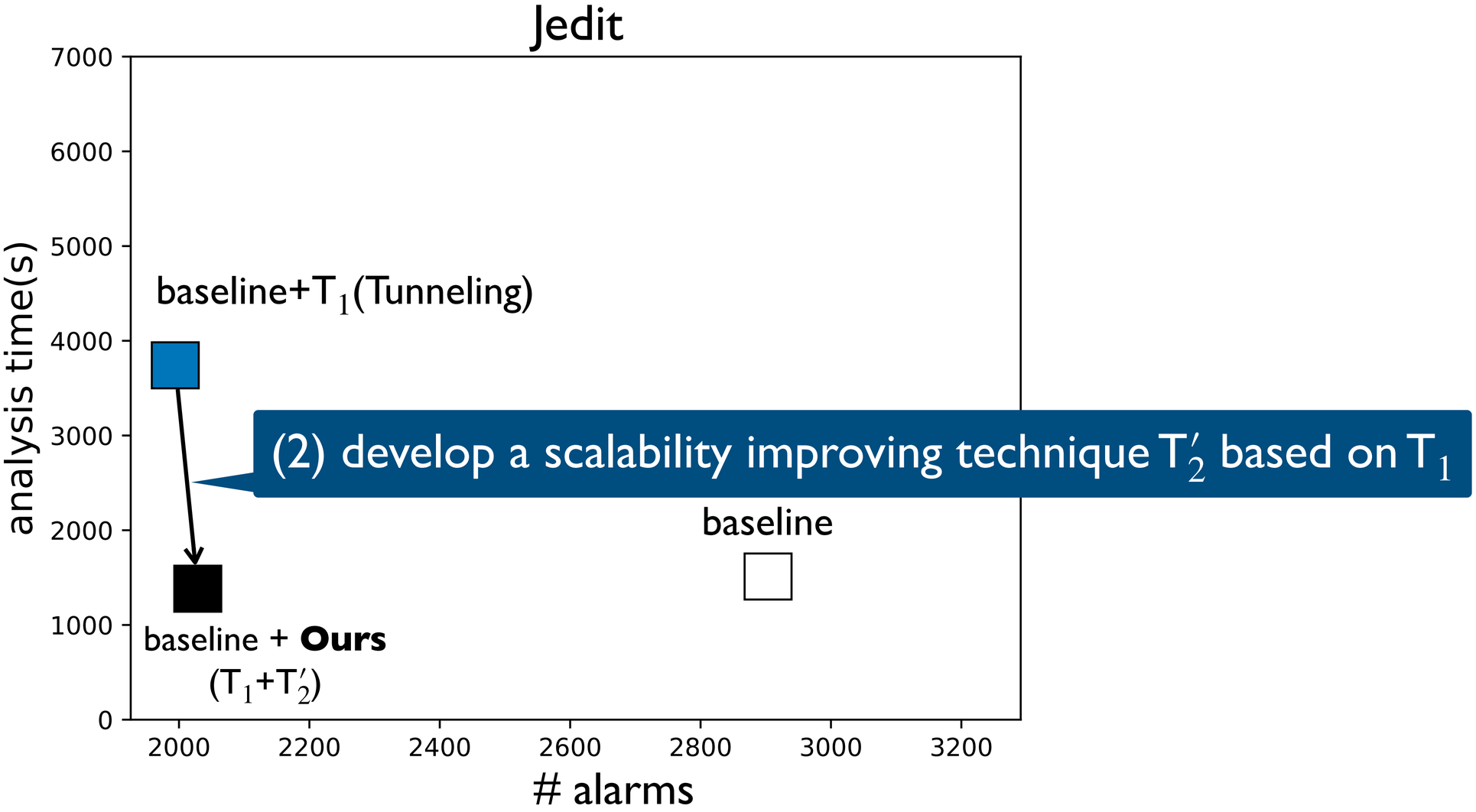
Experimental Results

- Following our framework enables developing an effective combination of the two techniques



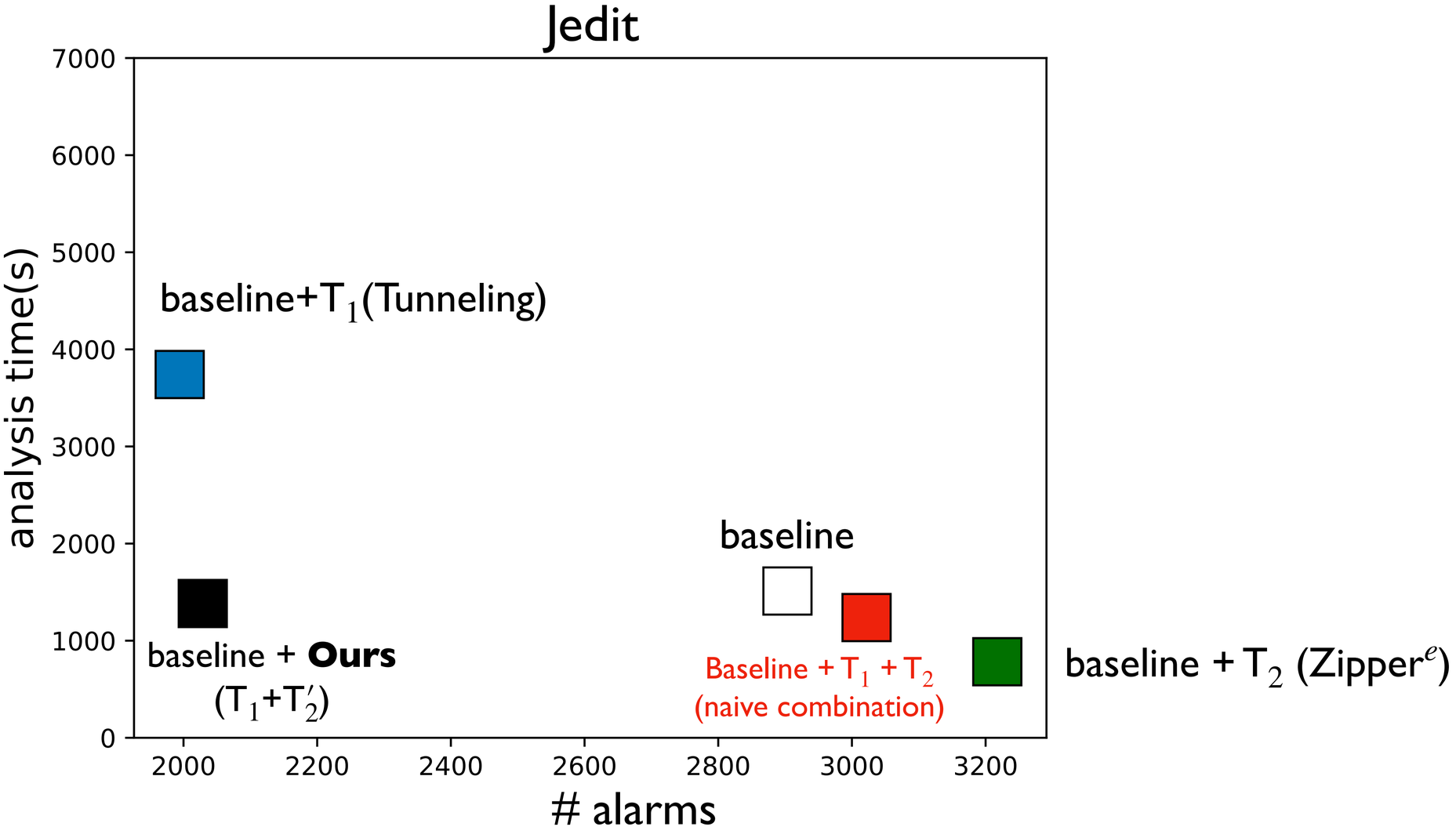
Experimental Results

- Following our framework enables developing an effective combination of the two techniques



Experimental Results

- Following our framework enables developing an effective combination of the two techniques



Conclusion

Independently developing analysis techniques will result in suboptimal analysis