

# Réunion flash

Point hebdomadaire

Duzés Florian




# Sommaire

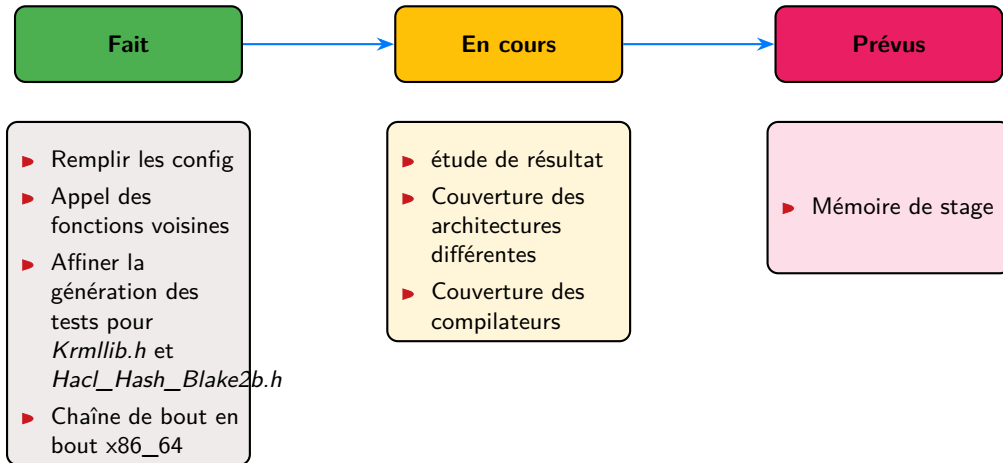
1. État des lieux
2. Érysichthon, travaille !
3. x86\_64, ARM, RiscV
4. Résultats - mémorisation et analyse
5. Mise en pratique
6. Conclusion

# 01

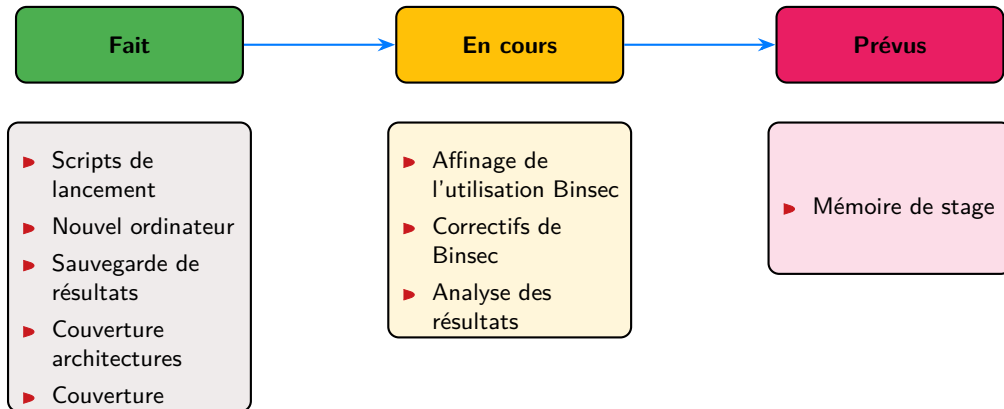
## État des lieux



## Point actuel



# Réalisation



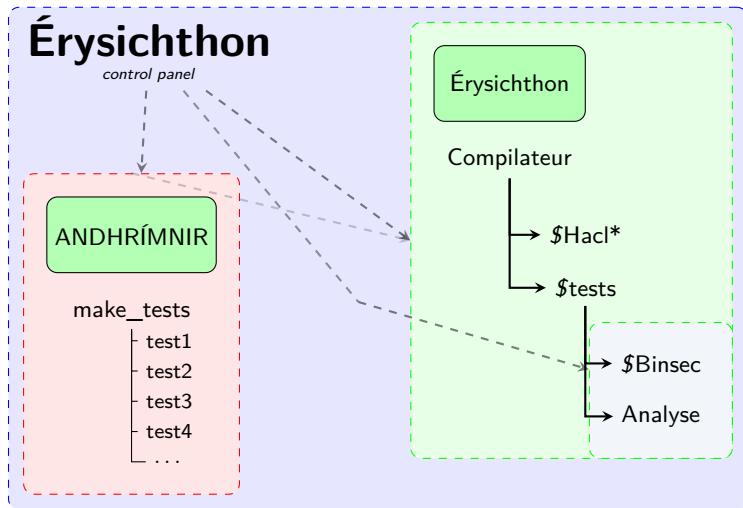
02

Érysichthon, travaille !



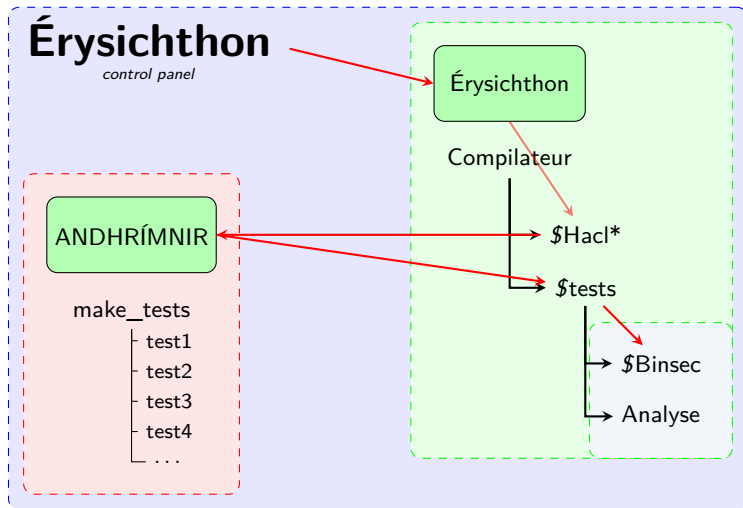


## Connexion des pièces détachés





## Connexion des pièces détachés







## Script de travail

```
$ ./erysichthon  
Usage: ./eryshicthon ARCHI PATH_Hacl [FORCE] [PATH_Compiler]  
- FORCE - default : 0s  
- PATH_Compiler - default : gcc
```

Code – ./erysichthon




## Lancement de l'analyse

```
for force in 01 02 03 0s 0z
do
  ./erysichthon x86_64 $HACL $force
done
```

Code – ./test.sh

# 03

## x86\_64, ARM, RiscV





# Le trio de tête

## Module x86\_64

- ▶ Compiler HACL\*
- ▶ Compilation des tests
- ▶ Script Binsec

# Le trio de tête

## Module x86\_64

- ▶ Compiler HACL\*
- ▶ Compilation des tests
- ▶ Script Binsec

## Module ARM

- ☐ Compiler HACL\*
- ☐ Compilation des tests
- ☐ Script Binsec

## Module RiscV

- ☐ Compiler HACL\*
- ☐ Compilation des tests
- ☐ Script Binsec

# Le trio de tête

## Module x86\_64

- ▶ Compiler HACL\*
- ▶ Compilation des tests
- ▶ Script Binsec

## Module ARM

- ☐ Compiler HACL\*
- ✓ Compilation des tests
- ✓ Script Binsec

## Module RiscV

- ☐ Compiler HACL\*
- ✓ Compilation des tests
- ✓ Script Binsec



## Compilation de HACL\*

```
Usage: configure -target <triple>
```

This script configures HACL/Evercrypt. You can specify the following options:

```
-target          Specify the target triple for the build. This follows the
                  Clang target triple convention.
                  Details: https://clang.llvm.org/docs/CrossCompilation.html
                  Currently supported triples are:
                  * aarch64-none-linux-android
                  * aarch64-none-linux-gnu
                  * aarch64-apple-darwin
                  * aarch64-apple-ios
                  * x86_64-apple-ios-simulator
--disable-bzero  Do not use explicit_bzero (binary will work with an old GL-
IBC)
--enable-power9  Enable Power ISA v3.0 instruction set for PowerPC architec-
ture
```

[Code](#) – ./configure



## Modification de HACL\*

```
Usage: configure -target <triple>
```

This script configures HACL/Evercrypt. You can specify the following options:

```
-target          Specify the target triple for the build. This follows the
                  Clang target triple convention.
                  Details: https://clang.llvm.org/docs/CrossCompilation.html
                  Currently supported triples are:
                  * aarch64-none-linux-android
                  * aarch64-none-linux-gnu
                  * aarch32-none-linux-gnu
                  * aarch64-apple-darwin
                  * aarch64-apple-ios
                  * x86_64-apple-ios-simulator
                  * x86_64-none-linux-gnu
                  * riscv64-unknown-linux-gnu
                  * riscv32-unknown-linux-gnu
--disable-bzero  Do not use explicit_bzero (binary will work with an old GL-
IBC)
```

Code – ./configure



# 04

## Résultats - mémorisation et analyse





## Des logs ...

### Conservations de traces

► *\$arch.log*

```
Binsec ... Hacl_Hash_SHA3_Simd256_shake128
[checkct:result] Program status is : secure (0.652)
Binsec ... Hacl_Hash_SHA3_Simd256_shake128_squeeze_nblocks
[sse:warning] Symbol state comes from the file /home/fduzes/projet_inria/erysichthon/x86_64-linux-gnu/libc.so.6
               Use "import <state> from FILE" to disambiguate
[sse:warning] Symbol state comes from the file /home/fduzes/projet_inria/erysichthon/x86_64-linux-gnu/libc.so.6
               Use "import <state> from FILE" to disambiguate
[checkct:result] Program status is : secure (0.263)
Binsec ... Hacl_Hash_SHA3_Simd256_shake256
[checkct:result] Program status is : secure (0.623)
Binsec ... Hacl_Hash_SHA3_Simd256_state_free
[sse:error] Cut path 1 (uninterpreted "Invalid replacement fallthrough") @ 0x00415970 (0.000)
[checkct:warning] Exploration is incomplete:
[sse:result] Value 0x64656262757473 : 0x64656262757473
[checkct:result] Program status is : unknown (0.075)
```

Code – x86\_64.log



## ... et des dictionnaires

### Mise en mémoire

- ▶ *results.json*
- ▶ *global\_results.json*

```
{ "$archi":  
    {"$option":  
        "fun": "secure|unknown|insecure"  
        ...  
        "date" : "mm_dd_yyyy_HH_MM"  
    }  
}
```

Code – global\_results.json

# 05

## Mise en pratique





## Matériel de calcul

### Ordinateur personnel

- ▶ Vivobook
- ▶ AMD Ryzen™ 5 3500U with Radeon™ Vega Mobile Gfx x 8
- ▶ Debian 12

*Récupéré auprès de proche au début du stage.*



## Matériel de calcul

### Ordinateur personnel

- ▶ Vivobook
- ▶ AMD Ryzen™ 5 3500U with Radeon™ Vega Mobile Gfx x 8
- ▶ Debian 12

*Récupéré auprès de proche au début du stage.*

### Colonne INRIA

- ▶ Dell Inc. Precision Tower 7910
- ▶ Intel® Xeon® E5-2620 v4 × 32
- ▶ Ubuntu 24.04.2 LTS

*Récupéré après le départ d'un thésard, ça traîné au bureau.*



## Premier lancement

```
(binsec: analyse
  @binsec -sse -sse-depth 1000000 -sse-timeout 20 -sse-script $(BINSEC_SCRIPT)
  -checkct $(DUMP)
```

[Code – x86\\_64/Makefile](#)



## Premier lancement

```
(binsec: analyse  
  @binsec -sse -sse-depth 1000000 -sse-timeout 20 -sse-script $(BINSEC_SCRIPT)  
  -checkct $(DUMP)
```

[Code](#) – x86\_64/Makefile

L'écran se gèle.  
Perte de contrôle...



```
fduzes@sta-02004063: ~/projec_inria/eryschthon
[checkct:result] Program status is : secure (0.157)
Binsec ... Hacl_EC_K256_felem_store
[checkct:result] Program status is : secure (0.131)
Binsec ... Hacl_EC_K256_felem_sub
[checkct:result] Program status is : secure (0.120)
Binsec ... Hacl_EC_K256_is_point_valid
[checkct:result] Program status is : secure (0.436)
Binsec ... Hacl_EC_K256_nk_base_point
[checkct:result] Program status is : secure (0.080)
Binsec ... Hacl_EC_K256_nk_felen_one
[checkct:result] Program status is : secure (0.102)
Binsec ... Hacl_EC_K256_nk_felen_zero
[checkct:result] Program status is : secure (0.101)
Binsec ... Hacl_EC_K256_nk_point_at_inf
[checkct:result] Program status is : secure (0.104)
Binsec ... Hacl_EC_K256_point_add
[checkct:result] Program status is : secure (0.477)
Binsec ... Hacl_EC_K256_point_double
[checkct:result] Program status is : secure (0.387)
Binsec ... Hacl_EC_K256_point_load
[checkct:result] Program status is : secure (0.202)
Binsec ... Hacl_EC_K256_point_mul
[checkct:result] Program status is : secure (3.243)
Binsec ... Hacl_EC_K256_point_negate
[checkct:result] Program status is : secure (0.110)
Binsec ... Hacl_EC_K256_point_store
[checkct:result] Program status is : secure (0.574)
Binsec ... Hacl_Ed25519_expand_keys
[sserror] Cut path 1 (uninterpreted "K0") @ 0x042042b
[checkct:warning] Exploration is incomplete:
[checkct:result] Program status is : unknown (2.106)
Binsec ... Hacl_Ed25519_secret_to_public
[sserror] Cut path 1 (uninterpreted "K0") @ 0x042042b
[checkct:warning] Exploration is incomplete:
[checkct:result] Program status is : unknown (2.136)
Binsec ... Hacl_Ed25519_sign
[sserror] Cut path 1 (uninterpreted "K0") @ 0x042042b
[checkct:warning] Exploration is incomplete:
[checkct:result] Program status is : unknown (2.416)
Binsec ... Hacl_Ed25519_sign_expanded
[sserror] Cut path 1 (uninterpreted "K0") @ 0x042042b
[checkct:warning] Exploration is incomplete:
[checkct:result] Program status is : unknown (2.821)
Binsec ... Hacl_Ed25519_verify
```

```
fduzes@sta-02004063: ~/projec_inria/eryschthon 94x45
[checkct:result] Program status is : secure (0.157)
Binsec ... Hacl_EC_K256_felem_store
[checkct:result] Program status is : secure (0.131)
Binsec ... Hacl_EC_K256_felem_sub
[checkct:result] Program status is : secure (0.120)
Binsec ... Hacl_EC_K256_is_point_valid
[checkct:result] Program status is : secure (0.436)
Binsec ... Hacl_EC_K256_nk_base_point
[checkct:result] Program status is : secure (0.080)
Binsec ... Hacl_EC_K256_nk_felen_one
[checkct:result] Program status is : secure (0.102)
Binsec ... Hacl_EC_K256_nk_felen_zero
[checkct:result] Program status is : secure (0.101)
Binsec ... Hacl_EC_K256_nk_point_at_inf
[checkct:result] Program status is : secure (0.104)
Binsec ... Hacl_EC_K256_point_add
[checkct:result] Program status is : secure (0.477)
Binsec ... Hacl_EC_K256_point_double
[checkct:result] Program status is : secure (0.387)
Binsec ... Hacl_EC_K256_point_load
[checkct:result] Program status is : secure (0.202)
Binsec ... Hacl_EC_K256_point_mul
[checkct:result] Program status is : secure (3.243)
Binsec ... Hacl_EC_K256_point_negate
[checkct:result] Program status is : secure (0.110)
Binsec ... Hacl_EC_K256_point_store
[checkct:result] Program status is : secure (0.574)
Binsec ... Hacl_Ed25519_expand_keys
[sserror] Cut path 1 (uninterpreted "K0") @ 0x042042b
[checkct:warning] Exploration is incomplete:
[checkct:result] Program status is : unknown (2.106)
Binsec ... Hacl_Ed25519_secret_to_public
[sserror] Cut path 1 (uninterpreted "K0") @ 0x042042b
[checkct:warning] Exploration is incomplete:
[checkct:result] Program status is : unknown (2.136)
Binsec ... Hacl_Ed25519_sign
[sserror] Cut path 1 (uninterpreted "K0") @ 0x042042b
[checkct:warning] Exploration is incomplete:
[checkct:result] Program status is : unknown (2.416)
Binsec ... Hacl_Ed25519_sign_expanded
[sserror] Cut path 1 (uninterpreted "K0") @ 0x042042b
[checkct:warning] Exploration is incomplete:
[checkct:result] Program status is : unknown (2.821)
Binsec ... Hacl_Ed25519_verify
```


# Script Binsec

```
starting from core  
halt at @[rsp, 8]  
explore all
```

Code – \*.ini

# 06

## Conclusion





# Conclusion

## Erreurs binsec

- ▶ Instructions non reconnu
- ▶ Syscall

## Étendre vers les autres architectures

- ▶ Inclure ARM et RiscV
- ▶ Tester sur Hacl\* public



# Conclusion

## Erreurs binsec

- ▶ Instructions non reconnu
- ▶ Syscall

## Étendre vers les autres architectures

- ▶ Inclure ARM et RiscV
- ▶ Tester sur Hacl\* public

## Modification de l'organisation du travail

- ▶ Objectif **Mémoire**
- ▶ 5 pages par jour
- ▶ *Continuité du projet au troisième plan*

*Merci.*

