Iyokan 入門

2021/09/11

L-III 松本 直樹

対象とする lyokan のバージョン情報

- 9/11 現在の master HEAD(f167d43)

アップデート手順

- seccamp2021-l3 の update_toolchain.sh を実行
- エラーが出る場合は Iyokan ディレクトリを削除して install_toolchain.sh を実行

```
naoki@LAPTOP-SMJ75B8R:~/seccamp2021-ex$ ./update_toolchain.sh
From https://github.com/virtualsecureplatform/Iyokan
 * branch            master     -> FETCH_HEAD
Already up to date.
-- The CXX compiler identification is Clang 10.0.0
-- Check for working CXX compiler: /usr/bin/clang++
-- Check for working CXX compiler: /usr/bin/clang++ -- works
-- Detecting CXX compiler ABI info
-- Detecting CXX compiler ABI info - done
-- Detecting CXX compile features
-- Detecting CXX compile features - done
-- Looking for C++ include pthread.h
-- Looking for C++ include pthread.h - found
```

新機能

- 以下の機能を追加・修正
  - yosys で合成した回路ファイルを直接 lyokan で読めるようになった
  - lyokan が出力した結果をそのまま入力できるようになった
  - 定数が直接ポートから出力される回路を処理できない問題を修正
  - 30万ゲートを超える回路でGPUを利用した処理が遅くなる問題を修正
  - --show-combinational-progress オプションを追加

yosys で合成した回路ファイルを直接 lyokan で読めるようになった

- ビルド手順とlyokan-L1 のメンテコストを削減する目的で対応
- 回路を定義する toml ファイルで指定すれば利用可能
  type = “yosys-json” を指定

```
[[file]]
type = "yosys-json"
path = "../yosys-json/addr-4bit-yosys.json"
name = "addr"

[connect]
"addr/io_inA[0:3]" = "@A[0:3]"
"addr/io_inB[0:3]" = "@B[0:3]"
"@out[0:3]" = "addr/io_out[0:3]"
```

Iyokan が出力した結果をそのまま入力できるようになった

- 複数回路を順番に実行するための機能追加
  - 回路 A を Iyokan で実行 → 結果を得る
  - 回路 A の結果を 回路 B に入力し Iyokan で実行 → 結果を得る
  - 回路 B の結果を 回路 C に入力し Iyokan で実行 → 結果を得る

- 使い方は Wiki を参照(https://bit.ly/3C0l7bV)

--show-combinational-progress オプションを追加

- 巨大な組み合わせ回路の実行状況を確認するために追加
- Iyokan の実行時に --show-combinational-progress を指定する

```
naoki@LAPTOP-SMJ75B8R:~/Iyokan$ build/bin/iyokan tfhe --blueprint test/config-toml/cahp-ruby-mux-1KiB.
toml --bkey bkey -i _test_req_packet --out _test_res_packet -c 5 --show-combinational-progress
[2021-09-11 14:47:57.881] [iyokan] [info] Build config
[2021-09-11 14:47:57.881] [iyokan] [info]       Type: Debug
[2021-09-11 14:47:57.881] [iyokan] [info]       Git revision: 05584be
[2021-09-11 14:47:57.881] [iyokan] [info]       TFHE security parameter: 128bit
[2021-09-11 14:47:57.881] [iyokan] [info]       GPU support: disabled
[2021-09-11 14:47:57.932] [iyokan] [info] Options
[2021-09-11 14:47:57.932] [iyokan] [info]       Blueprint: test/config-toml/cahp-ruby-mux-1KiB.toml
[2021-09-11 14:47:57.932] [iyokan] [info]       # of cycles: 5
[2021-09-11 14:47:57.932] [iyokan] [info]       BKey file: bkey
[2021-09-11 14:47:57.932] [iyokan] [info]       Input file (request packet): _test_req_packet
[2021-09-11 14:47:57.933] [iyokan] [info]       Output file (result packet): _test_res_packet
[2021-09-11 14:47:57.933] [iyokan] [info]       --verbose: false
[2021-09-11 14:47:57.933] [iyokan] [info]       --quiet: false
[2021-09-11 14:47:57.933] [iyokan] [info]       --show-combinational-progess: true
[2021-09-11 14:48:02.487] [iyokan] [info] Run Parameters
[2021-09-11 14:48:02.487] [iyokan] [info]       Mode: TFHEpp
[2021-09-11 14:48:02.487] [iyokan] [info]       Blueprint: test/config-toml/cahp-ruby-mux-1KiB.toml
[2021-09-11 14:48:02.487] [iyokan] [info]       # of CPU workers: 8
[2021-09-11 14:48:02.487] [iyokan] [info]       # of cycles: 5
[2021-09-11 14:48:02.487] [iyokan] [info]       BKey file: bkey
[2021-09-11 14:48:02.487] [iyokan] [info]       Input file (request packet): _test_req_packet
[2021-09-11 14:48:02.487] [iyokan] [info]       Output file (result packet): _test_res_packet
[2021-09-11 14:48:08.912] [iyokan] [info] Circuit Executing... 1002/63140
[2021-09-11 14:48:12.856] [iyokan] [info] Circuit Executing... 2003/63140
[2021-09-11 14:48:15.001] [iyokan] [info] Circuit Executing... 3005/63140
```

Iyokan の使い方(最新版)

- Iyokan は以下の手順で利用する
  1. Chisel で回路を記述する
  2. sbt run を実行し生成された Verilog ファイルを yosys で変換する
  3. 回路の定義 TOML ファイルを書く
  4. 入力 TOML ファイルを書く
  5. 秘密鍵を生成する
  6. 入力 TOML ファイルを iyokan-packet で専用フォーマットに変換
  7. 変換された入力を iyokan-packet で暗号化
  8. Iyokan で実行
  9. 結果を iyokan-packet で復号
  10. 復号した結果を iyokan-packet で TOML形式に変換

1. Chisel で回路を記述する

- これまでと同様に記述すればよい

```
class Counter8bit extends Module {
    val io = IO(new Bundle{
        val out    = Output(UInt(8.W))
    })

    val cnt = RegInit(0.U(8.W))

    io.out := cnt

    when(cnt === 7.U){
        cnt := cnt
    }.otherwise{
        cnt := cnt + 1.U
    }
}
```

2. 生成された Verilog ファイルを yosys で変換する

- build_circuit.sh が利用できる
- ./build_circuit.sh Counter4bit.v

```
naoki@LAPTOP-SMJ75B8R:~/seccamp2021-ex$ ./build_circuit.sh Counter4bit.v

 /-----------------------------------------------------------------------------\
 |                                                                             |
 |  yosys -- Yosys Open SYnthesis Suite                                        |
 |                                                                             |
 |  Copyright (C) 2012 - 2020  Claire Xenia Wolf <claire@yosyshq.com>          |
 |                                                                             |
 |  Permission to use, copy, modify, and/or distribute this software for any   |
 |  purpose with or without fee is hereby granted, provided that the above     |
 |  copyright notice and this permission notice appear in all copies.          |
 |                                                                             |
 |  THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES   |
```

```
naoki@LAPTOP-SMJ75B8R:~/seccamp2021-ex$ ls -l Counter4bit.json
-rw-rw-r-- 1 naoki naoki 6292 Sep 11 15:51 Counter4bit.json
```

3. 回路の定義 TOML ファイルを書く

- type は “yosys-json” を指定
- connect の仕様は Wiki を参照(https://bit.ly/3le2Kte)

```
naoki@LAPTOP-SMJ75B8R:~/seccamp2021-ex$ cat counter-4bit.toml
[[file]]
type = "yosys-json"
path = "Counter4bit.json"
name = "counter"

[connect]
"counter/reset" = "@reset"
"@out[0:3]" = "counter/io_out[0:3]"
```

4. 入力 TOML ファイルを書く

- これまでと同様
  (ここでは addr に対する入力)
- size は bit 単位、 bytes はリトルエンディアン

```
naoki@LAPTOP-SMJ75B8R:~/seccamp2021-ex/Iyokan$ cat test/in/test04.in
[[bits]]
name = "A"
size = 4
bytes = [0xc]

[[bits]]
name = "B"
size = 4
bytes = [0xa]
```

5. 秘密鍵を生成する

- ./iyokan-packet genkey で秘密鍵を生成
- ./iyokan-packet genbkey でブートストラッピング鍵を生成

```
naoki@LAPTOP-SMJ75B8R:~/Iyokan/build/bin$ ./iyokan-packet genkey --type tfhepp --out skey
[2021-09-11 18:22:05.146] [iyokan-packet] [info] Starting genkey...
[2021-09-11 18:22:05.147] [iyokan-packet] [info] genkey done. (0 seconds)
```

```
naoki@LAPTOP-SMJ75B8R:~/Iyokan/build/bin$ ./iyokan-packet genbkey --in skey --out bkey
[2021-09-11 18:22:28.583] [iyokan-packet] [info] Starting genbkey...
[2021-09-11 18:23:11.667] [iyokan-packet] [info] genbkey done. (43 seconds)
```

6. 入力 TOML ファイルを変換する

- ./iyokan-packet toml2packet で専用フォーマットに変換

```
naoki@LAPTOP-SMJ75B8R:~/Iyokan/build/bin$ ./iyokan-packet toml2packet --in test04.in --out test04_packet.in
[2021-09-11 18:25:49.123] [iyokan-packet] [info] Starting toml2packet...
[2021-09-11 18:25:49.124] [iyokan-packet] [info] toml2packet done. (0 seconds)
```

7. 暗号化する

- ./iyokan-packet enc で暗号化する

```
naoki@LAPTOP-SMJ75B8R:~/Iyokan/build/bin$ ./iyokan-packet enc --in test04_packet.in --key skey --out test04_packet.enc
[2021-09-11 18:26:57.498] [iyokan-packet] [info] Starting enc...
[2021-09-11 18:26:57.499] [iyokan-packet] [info] enc done. (0 seconds)
```

8. Iyokan で実行する

- 平文モードで実行するときは ./iyokan plain で回路や入力等を指定する

```
naoki@LAPTOP-SMJ75B8R:~/Iyokan/build/bin$ ./iyokan plain --blueprint addr-4bit.toml --in test04_packet.in --out res_plain.out -c 1
[2021-09-11 18:29:30.344] [iyokan] [info] Build config
[2021-09-11 18:29:30.344] [iyokan] [info]       Type: Debug
[2021-09-11 18:29:30.344] [iyokan] [info]       Git revision: 05584be
[2021-09-11 18:29:30.344] [iyokan] [info]       TFHE security parameter: 128bit
[2021-09-11 18:29:30.344] [iyokan] [info]       GPU support: disabled
[2021-09-11 18:29:30.355] [iyokan] [info] Options
[2021-09-11 18:29:30.355] [iyokan] [info]       Blueprint: addr-4bit.toml
[2021-09-11 18:29:30.355] [iyokan] [info]       # of cycles: 1
[2021-09-11 18:29:30.355] [iyokan] [info]       Input file (request packet): test04_packet.in
[2021-09-11 18:29:30.355] [iyokan] [info]       Output file (result packet): res_plain.out
[2021-09-11 18:29:30.355] [iyokan] [info]       --verbose: false
[2021-09-11 18:29:30.355] [iyokan] [info]       --quiet: false
[2021-09-11 18:29:30.369] [iyokan] [info] Run Parameters
[2021-09-11 18:29:30.369] [iyokan] [info]       Mode: Plain
[2021-09-11 18:29:30.369] [iyokan] [info]       Blueprint: addr-4bit.toml
[2021-09-11 18:29:30.369] [iyokan] [info]       # of CPU workers: 8
[2021-09-11 18:29:30.369] [iyokan] [info]       # of cycles: 1
[2021-09-11 18:29:30.369] [iyokan] [info]       Input file (request packet): test04_packet.in
[2021-09-11 18:29:30.369] [iyokan] [info]       Output file (result packet): res_plain.out
[2021-09-11 18:29:30.369] [iyokan] [info] #1
[2021-09-11 18:29:30.369] [iyokan] [info]       done. (193 us)
```

8. Iyokan で実行する

- 暗号モードで実行するときは ./iyokan tfhe で回路や入力、ブートストラッピング鍵を指定する
- GPU を利用する場合は --enable-gpu オプションを付ける
  (ビルド時に GPU オプションを付ける必要がある)

```
naoki@LAPTOP-SMJ75B8R:~/Iyokan/build/bin$ ./iyokan tfhe --blueprint addr-4bit.toml --bkey bkey --in test04_pac
ket.enc --out res.enc -c 1
[2021-09-11 18:36:24.883] [iyokan] [info] Build config
[2021-09-11 18:36:24.883] [iyokan] [info]       Type: Debug
[2021-09-11 18:36:24.883] [iyokan] [info]       Git revision: 05584be
[2021-09-11 18:36:24.883] [iyokan] [info]       TFHE security parameter: 128bit
[2021-09-11 18:36:24.883] [iyokan] [info]       GPU support: disabled
[2021-09-11 18:36:24.895] [iyokan] [info] Options
[2021-09-11 18:36:24.895] [iyokan] [info]       Blueprint: addr-4bit.toml
[2021-09-11 18:36:24.895] [iyokan] [info]       # of cycles: 1
[2021-09-11 18:36:24.895] [iyokan] [info]       BKey file: bkey
[2021-09-11 18:36:24.895] [iyokan] [info]       Input file (request packet): test04_packet.enc
[2021-09-11 18:36:24.895] [iyokan] [info]       Output file (result packet): res.enc
[2021-09-11 18:36:24.895] [iyokan] [info]       --verbose: false
[2021-09-11 18:36:24.895] [iyokan] [info]       --quiet: false
[2021-09-11 18:36:24.901] [iyokan] [info] Run Parameters
[2021-09-11 18:36:24.901] [iyokan] [info]       Mode: TFHEpp
[2021-09-11 18:36:24.901] [iyokan] [info]       Blueprint: addr-4bit.toml
[2021-09-11 18:36:24.901] [iyokan] [info]       # of CPU workers: 8
[2021-09-11 18:36:24.901] [iyokan] [info]       # of cycles: 1
[2021-09-11 18:36:24.901] [iyokan] [info]       BKey file: bkey
[2021-09-11 18:36:24.901] [iyokan] [info]       Input file (request packet): test04_packet.enc
[2021-09-11 18:36:24.901] [iyokan] [info]       Output file (result packet): res.enc
[2021-09-11 18:36:27.504] [iyokan] [info] #1
[2021-09-11 18:36:27.761] [iyokan] [info]       done. (256317 us)
```

9. 結果を復号する

- ./iyokan-packet dec で結果を復号

```
naoki@LAPTOP-SMJ75B8R:~/Iyokan/build/bin$ ./iyokan-packet dec --key skey --in res.enc --out res.out
[2021-09-11 18:37:20.538] [iyokan-packet] [info] Starting dec...
[2021-09-11 18:37:20.539] [iyokan-packet] [info] dec done. (0 seconds)
```

10. 復号した結果をTOML形式に変換する

- ./iyokan-packet packet2toml で変換

```
naoki@LAPTOP-SMJ75B8R:~/Iyokan/build/bin$ ./iyokan-packet packet2toml --in res.out
[2021-09-11 18:38:56.574] [iyokan-packet] [info] Starting packet2toml...
rom = []
ram = []
cycles = 1
bits = [
{bytes=[6],size=4,name="out"},
]
[2021-09-11 18:38:56.575] [iyokan-packet] [info] packet2toml done. (0 seconds)
```