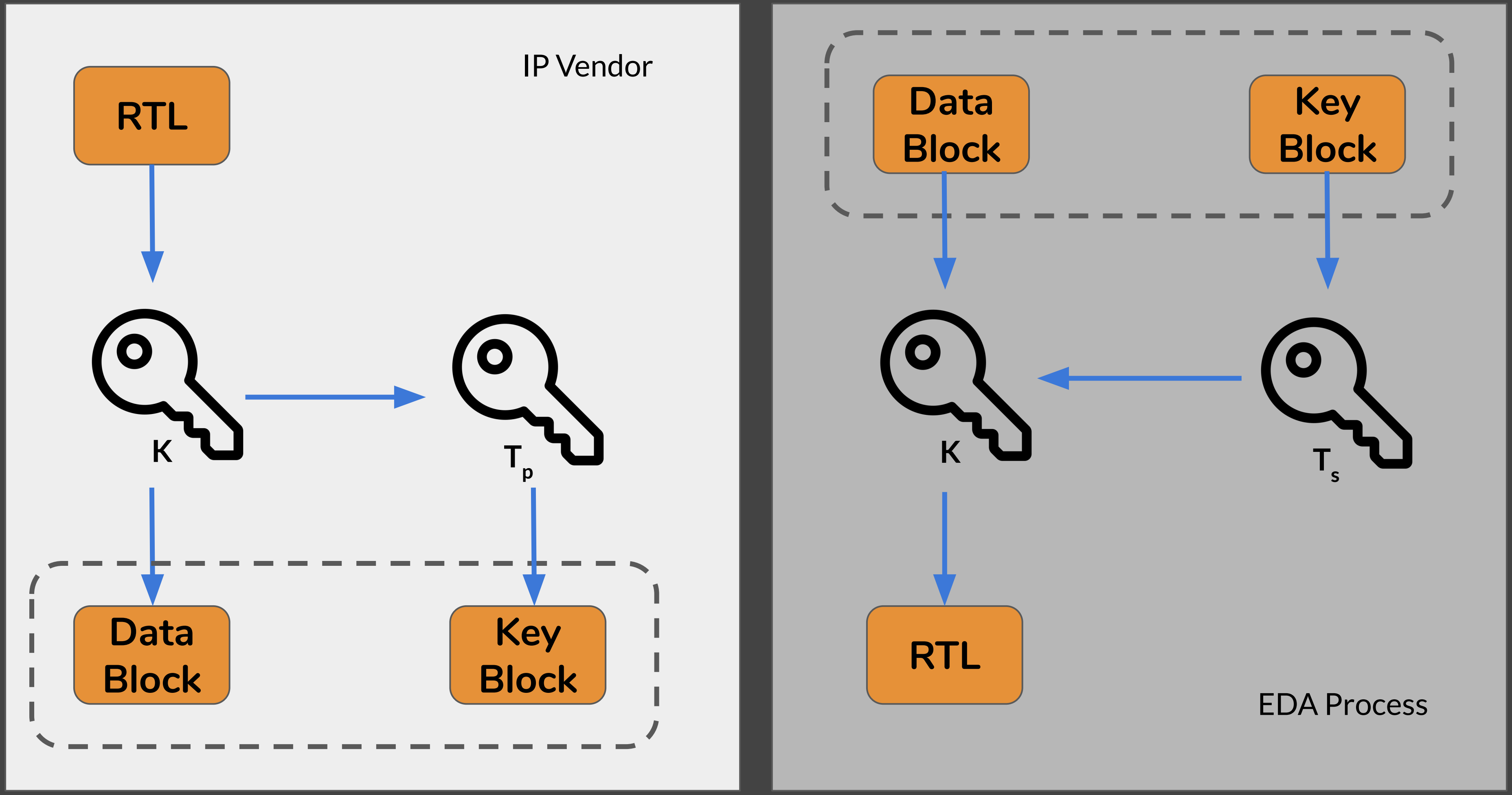
DPI Protected Verilog Instead of Encryption

A non-broken and open source friendly alternative to IEEE 1735

Todd Strader
@ ORConf 2019

IP is everywhere

- Modular hardware components
- Licensed by a third party
- Term clearly coined by lawyers
- IEEE P1735 standardizes RTL encryption


IP Vendor
RTL
K
T_p
Data Block
Key Block
Data Block
Key Block
K
T_s
RTL
EDA Process

Open source tools can’t play

Possible solutions:

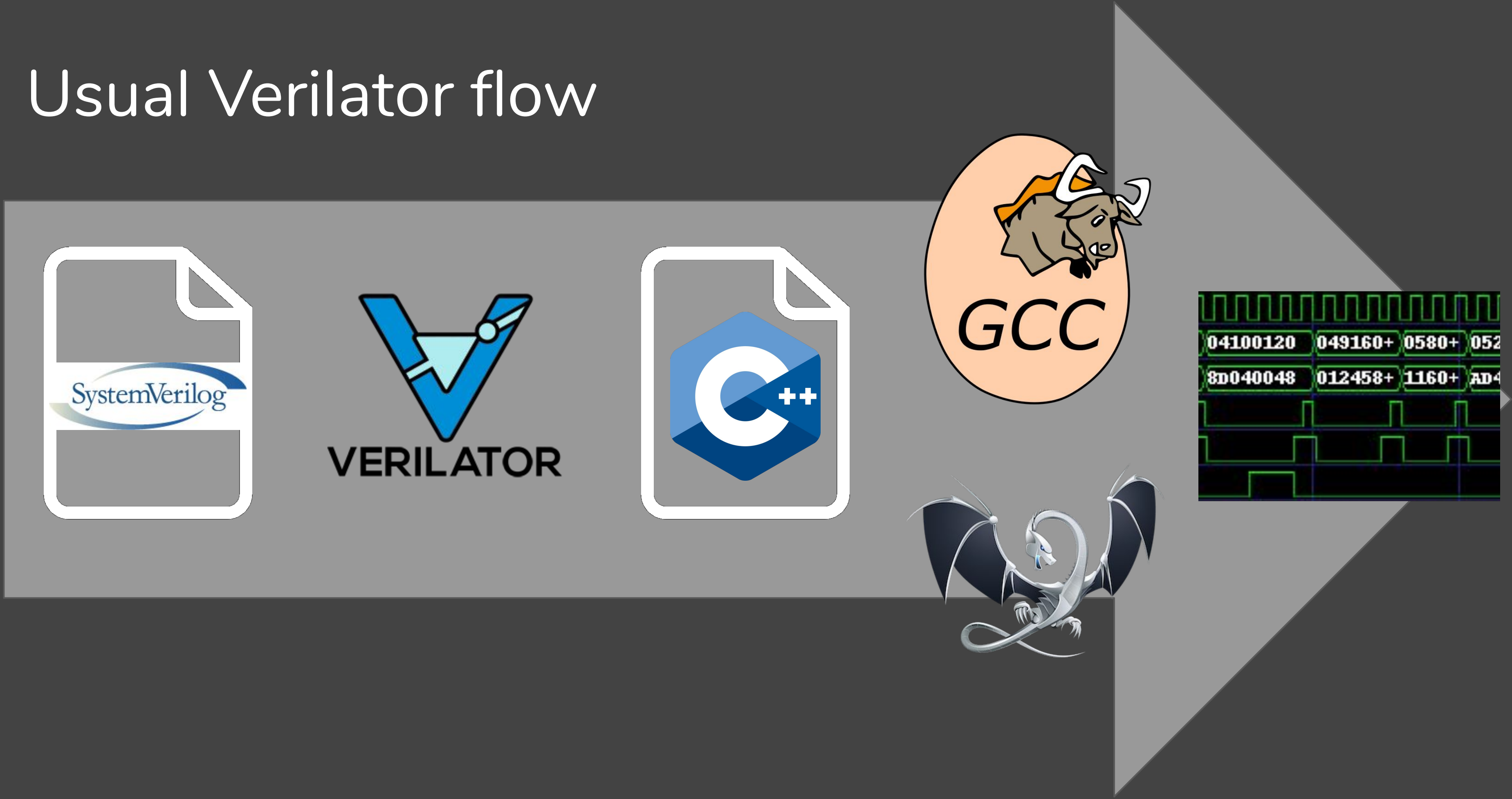
- Use closed source simulator $€
- Emulate functionality
- Gate-level sim
- Negotiate for source
- Give up

VERILATOR

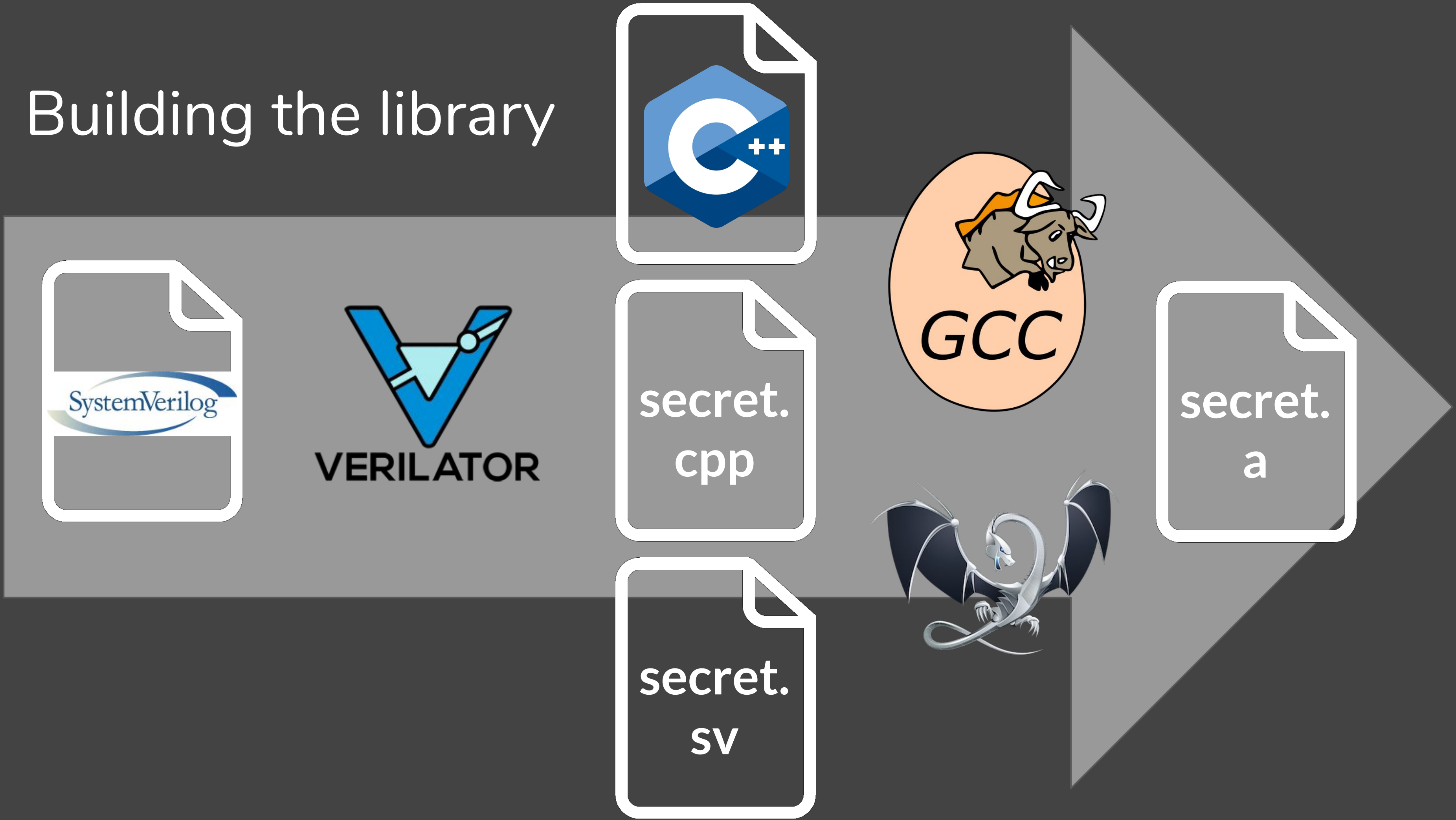
What if we could compile the secret Verilog and use it via a standardized interface?

DPI

Usual Verilator flow



Building the library

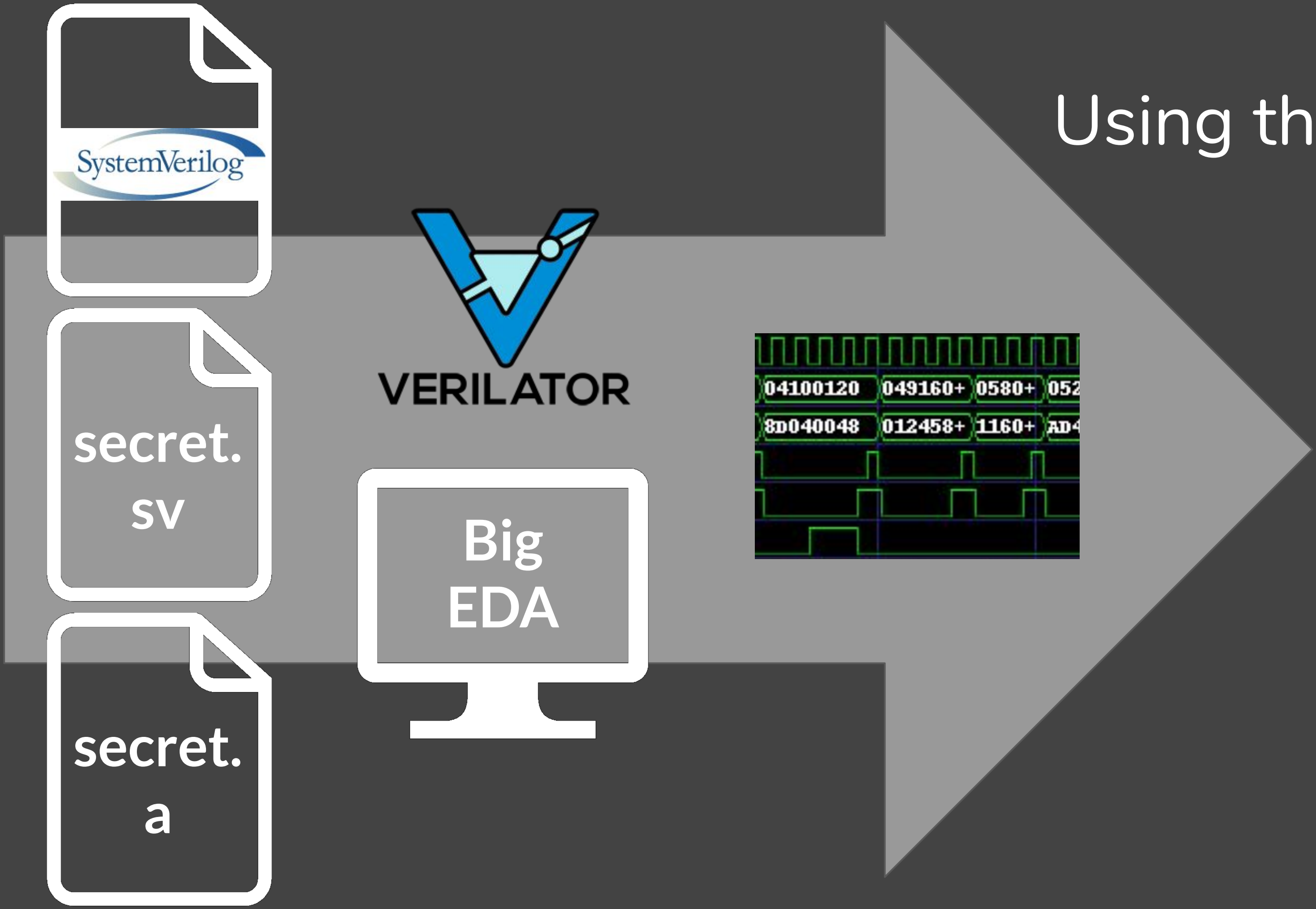


secret.cpp

secret.sv

secret.a

Using the library



Let’s add it all up

- Portable across DPI-capable simulators
- Including open source simulators
- Compiled library is pretty indecipherable
- No possibility of leaked RTL
- Stable API via the DPI
- Could lead to fewer trusted keys

Is everything fine?

- Everything is not fine

Top-level parameters

- Verilator requires fixed top-level parameters
- Possible solutions:
  - Don’t do that
  - Build libraries on-demand
  - Convert parameters to wires?
  - Dynamically construct hierarchy?

Build matrix

- OS
- Machine architecture
- C++ ABI
- Static or shared library

Try it out

```
$ git clone -b protect-lib
https://github.com/toddstrader/verilator-dev.git

$ # build Verilator

$ make -C examples/dpi_protect_lib/

$ test_regress/t/t_prot_lib.pl

$ test_regress/t/t_prot_lib.pl --xsim
```

Next steps

- Land upstream
- Larger tests
  - verilator_ext_tests
  - Benchmarking
- Test more commercial simulators
- Support x’s and z’s
- Isolate Verilator runtime
- Performance optimizations
- Better obfuscation
- VCD replay
- Support top-level parameters

Thanks

```
$ verilator --cc --protect-lib secret
```

Further reading

- https://acmccs.github.io/papers/p1533-chhotarayA.pdf
- https://thehackernews.com/2017/11/ieee-p1735-ip-encryption.html
- https://standards.ieee.org/content/ieee-standards/en/standard/1735-2014.html