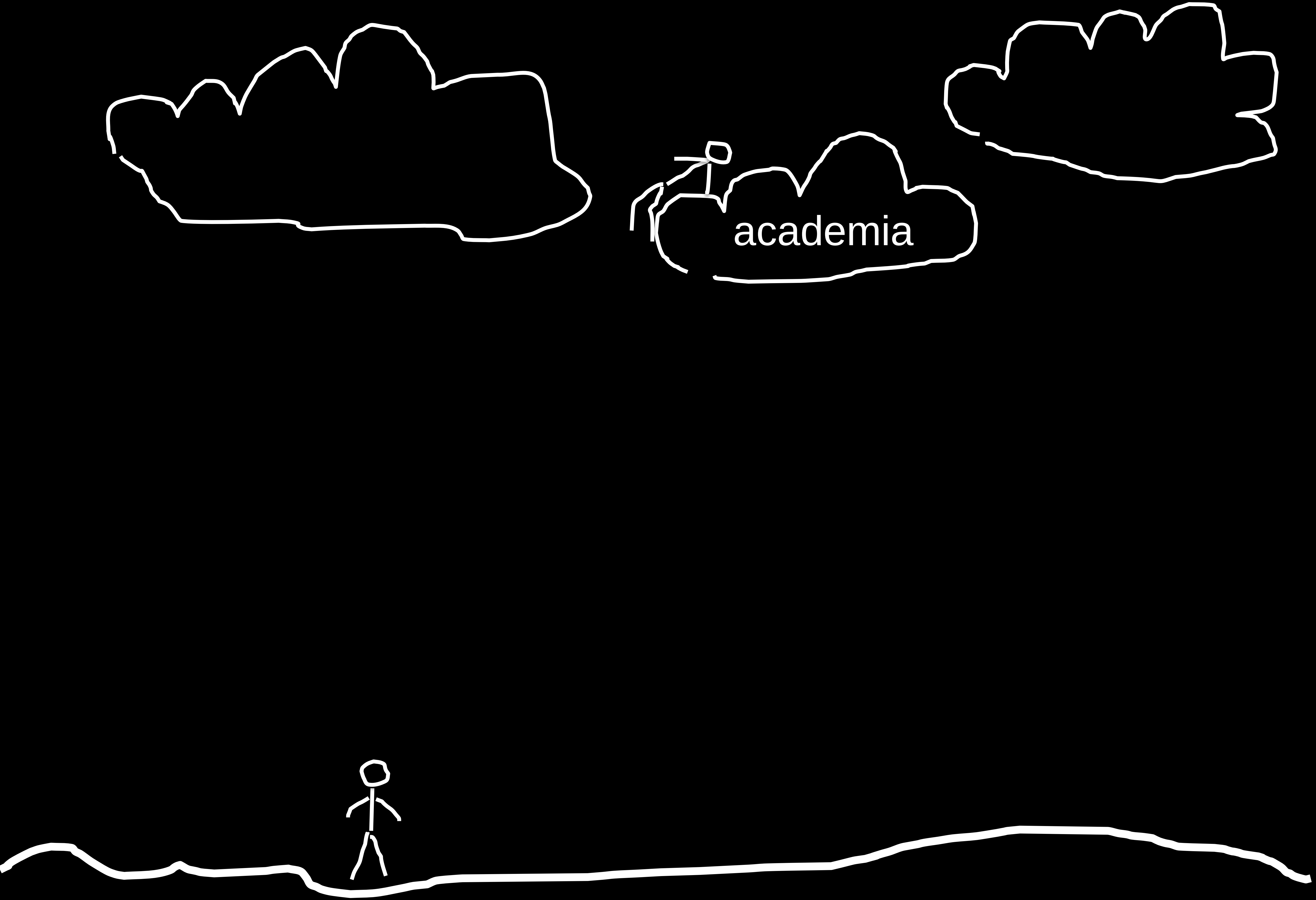
riscure

Academic vs. industrial perspective on SCA… …and an industrial innovation

Ilya Kizhvatov, Marc Witteman

COSADE 2013, Paris



academia

industry

disclaimer: this picture is the private opinion of the speaker

How many of you

have published a paper on SCA

in the recent year?

Do you think

your results

are practical?

Out of dozens of SCA papers

we as a test lab

find that few are practical.

Why?

1. Limited testing time

and SCA only part of it

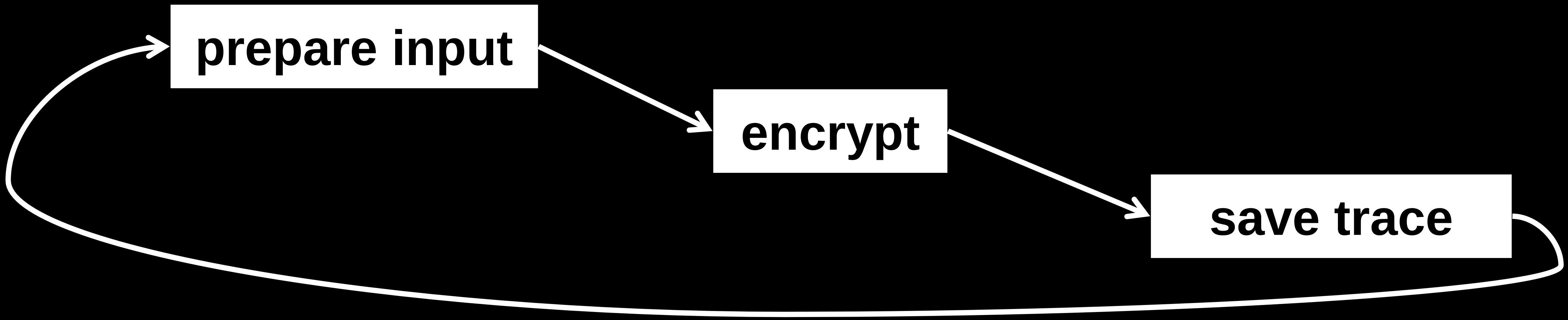
2. Large amounts of traces

Compute success rate, you say?

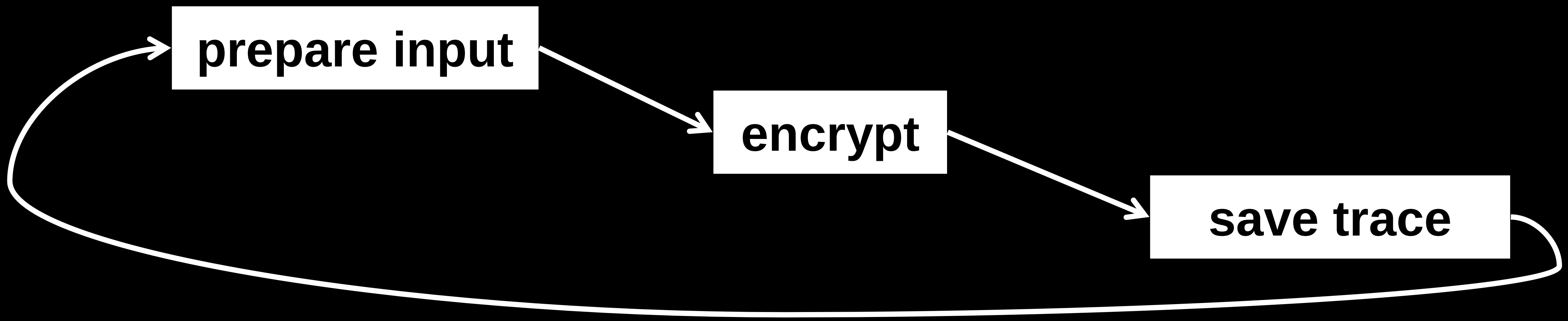
What do we do?

We use “fast acquisition” with averaging on the DSO.

Common acquisition flow



Common acquisition flow

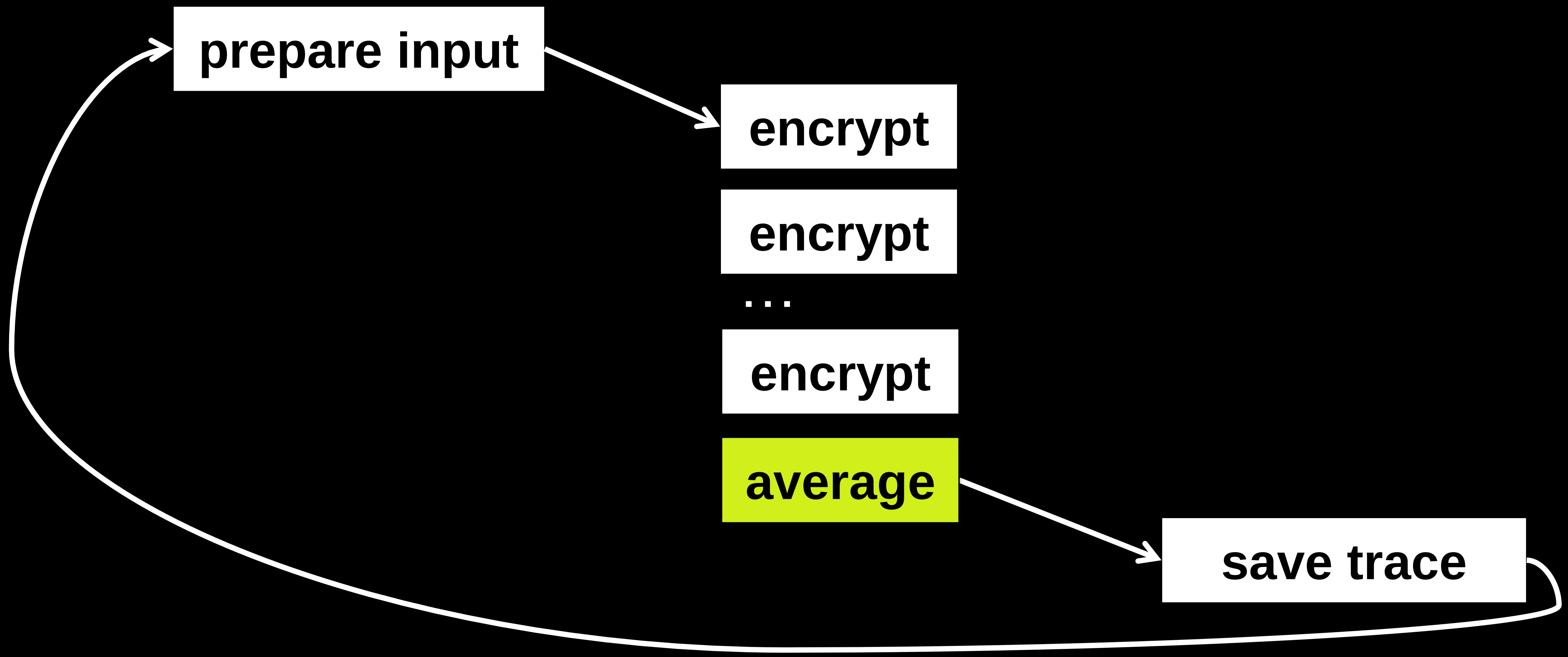


prepare input

encrypt

save trace

Fast acquisition flow with averaging



prepare input

encrypt

encrypt

…

encrypt

average

save trace

No slightest academic value.

Effect?

Up to 200 times speed up.

Requires great degree of control over the target → reject (-1)

Requires great degree of control

over the target → reject (-1)

Runtime control

is a standard prerequisite

in embedded scenarios

Will not work

with jitter → reject (-2)

Will not work

with jitter → reject (-2)

Well it works,

we align traces on the DSO

Will not work

against masking → reject (-2)

confidence 4!

Will not work

against masking → reject (-2)

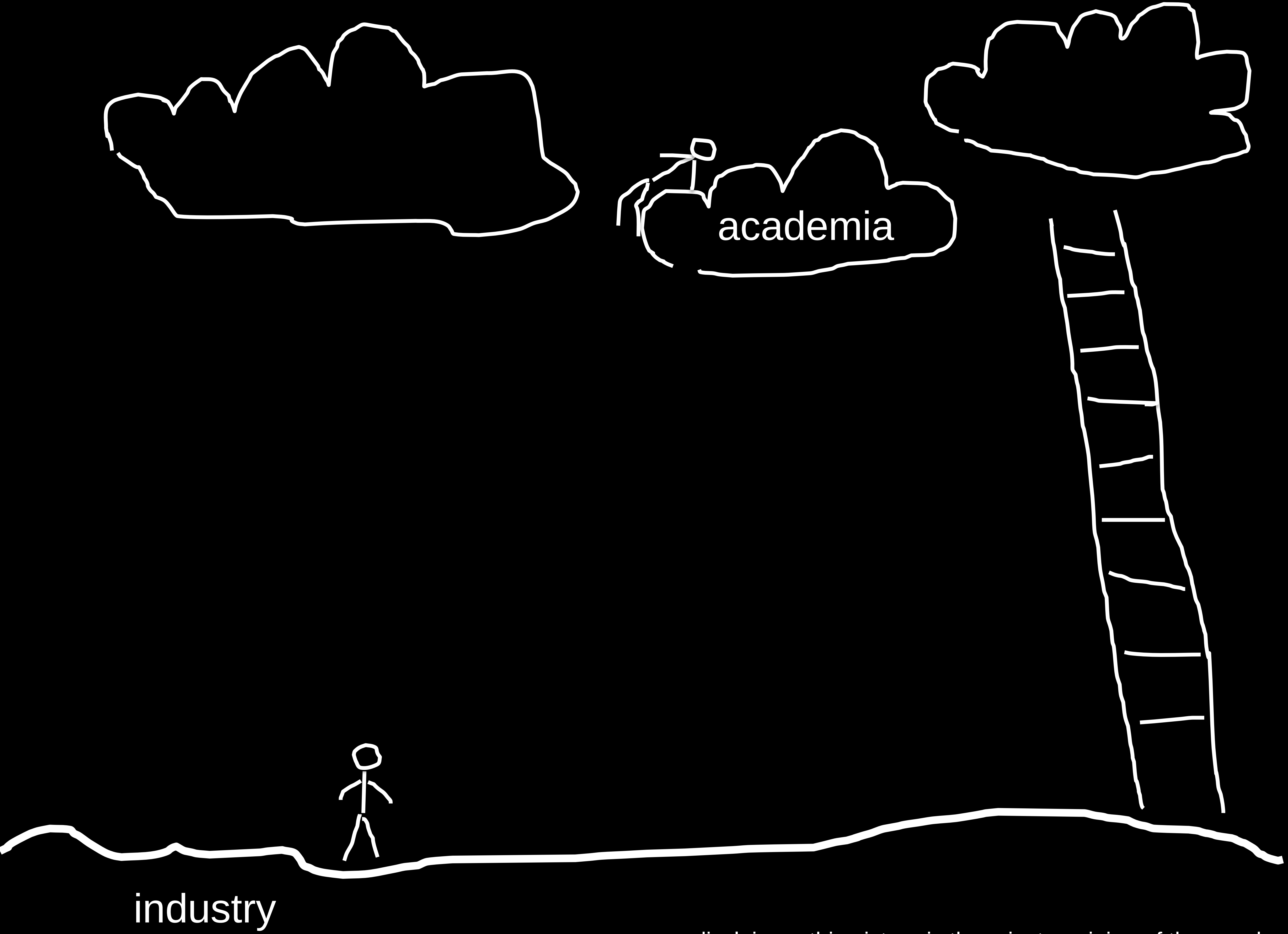
confidence 4!

Think of residual

first order leakage.

Full white paper on fast acquisition

www.riscure.com/news-events



disclaimer: this picture is the private opinion of the speaker riscure

Challenge your security

Contact: Ilya Kizhvatov
Security analyst
ilya@riscure.com

Riscure B.V.
Frontier Building, Delftechpark 49
2628 XJ Delft
The Netherlands
Phone: +31 15 251 40 90

www.riscure.com

Riscure North America
71 Stevenson Street, Suite 400
San Francisco, CA 94105
USA
Phone: +1 650 646 99 79

inforequest@riscure.com