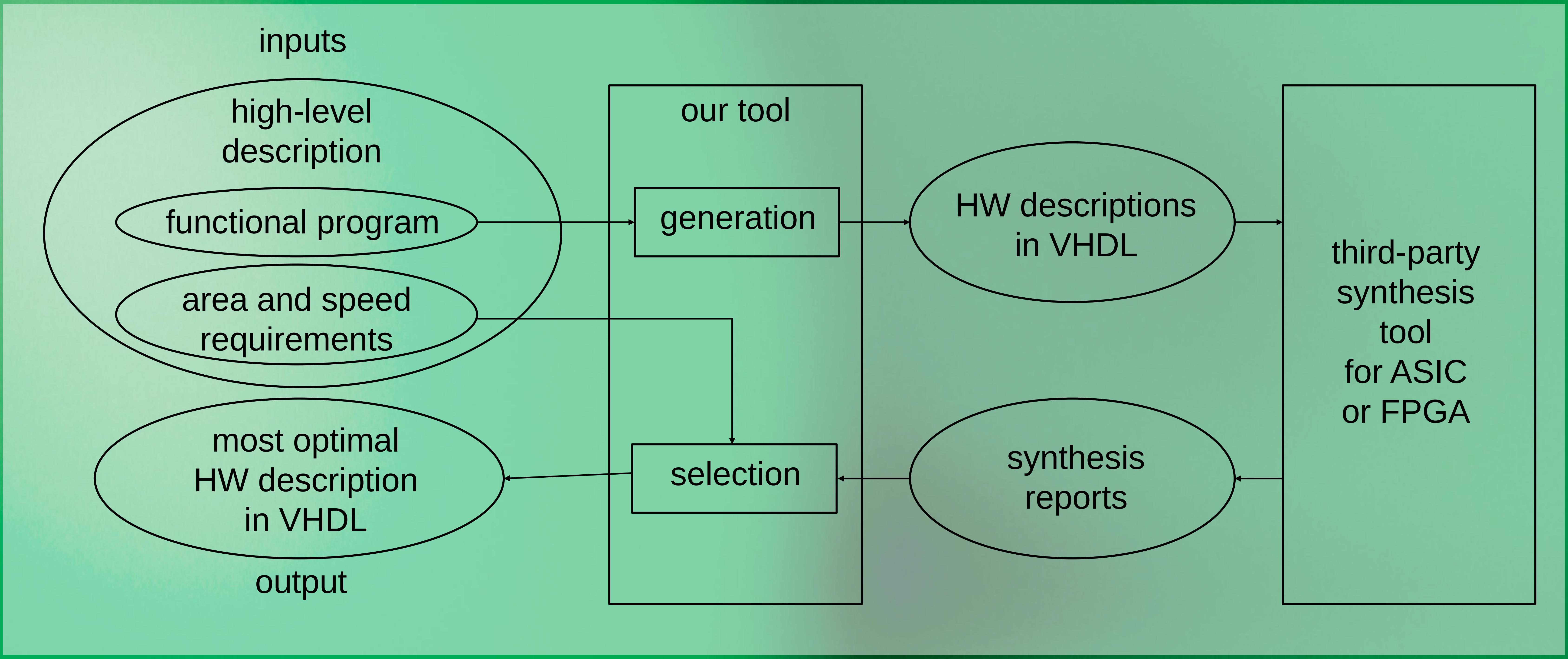
DESIGN SPACE EXPLORATION FOR AUTOMATICALLY GENERATED CRYPTOGRAPHIC HARDWARE USING FUNCTIONAL LANGUAGES

D. Wolfs[1,3], K. Aerts[2,3], N. Mentens[1,3]

[1] KU Leuven, ESAT-SCD/COSIC, Kasteelpark Arenberg 10, 3001 Leuven, Belgium
[2] KU Leuven, CS-Informatica/DTAI, 3001 Leuven, Belgium
[3] KHLim, ACRO-ES&S, Agoralaan Gebouw B bus 3, 3590 Diepenbeek, Belgium
email: {davy.wolfs,kris.aerts,nele.mentens}@khlim.be

Goals:

- EDA tool for the automatic generation of cryptographic hardware in VHDL
- taking into account user requirements by design space exploration



Results:

- listing features for design space exploration
  - exploration in the generation phase
  - exploration in the synthesis phase (by exploring options of synthesis tool)
- data path example: 192-bit adder → 32 automatically generated architectures
- control logic example: AES controller → 18 automatically generated architectures

This research was funded by BOF project CREA/09/016 of the Katholieke Universiteit Leuven.