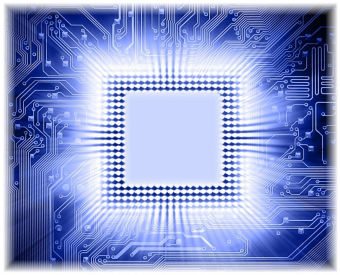
Advanced Logic Synthesis for Electronics
www.ALSE-FR.com

A.L.S.E.

CPLD-based Anti-Copy solution

Bertrand CUZEAU – CTO
www.ALSE-FR.com or www.FPGA.fr
info@alse-fr.com
8 passage Barrault - 75013– PARIS France
Tel +33 1 84 16 32 32



Anti-copy

Advanced Logic Synthesis for Electronics
www.ALSE-FR.com

Facts :

- Copying a design using an FPGA is often trivial !
- Production usually occurs in far countries where control is difficult to exercise (over-building).
- Controlling the number of FPGA devices using a given IP is nearly impossible (even when fingerprinting is available).

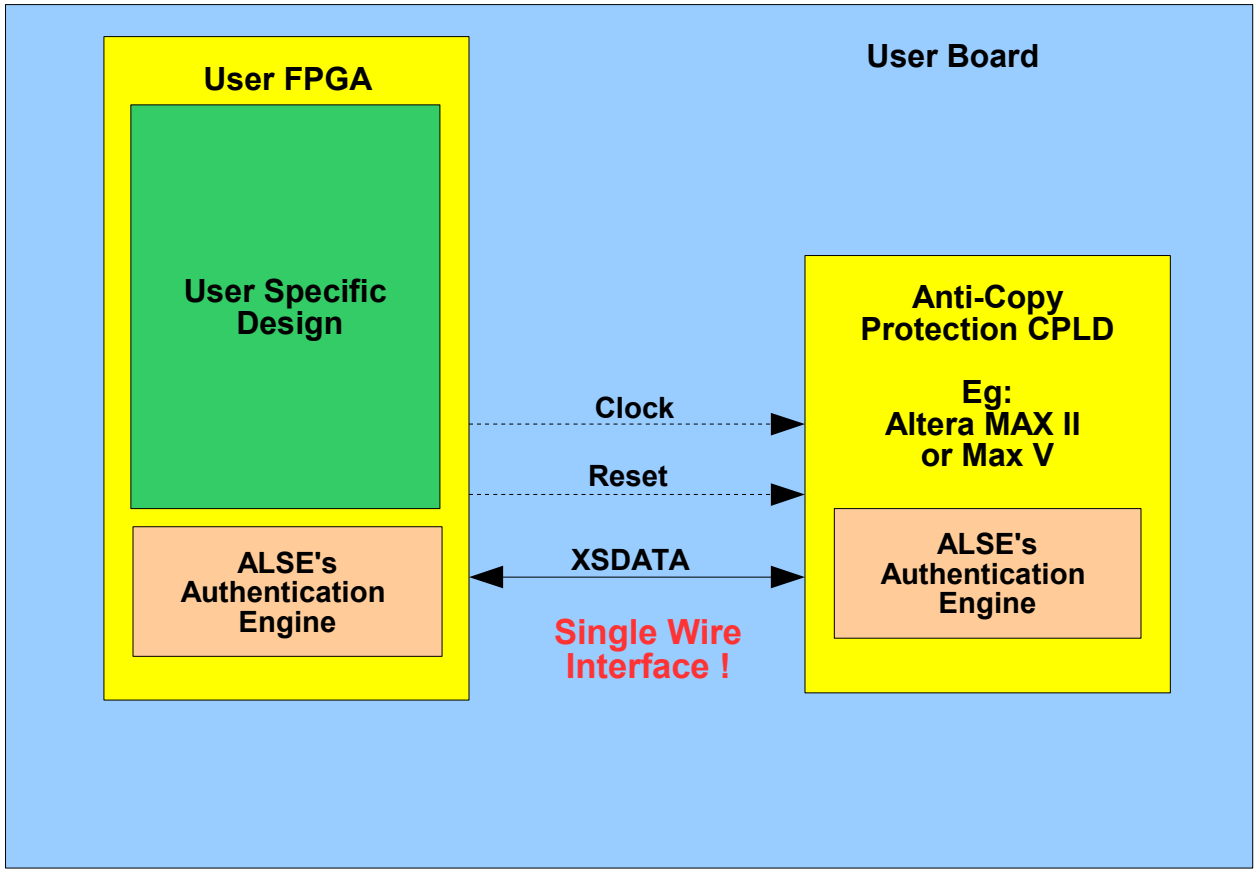
Solution : the **ALSE Anti-Copy kit**

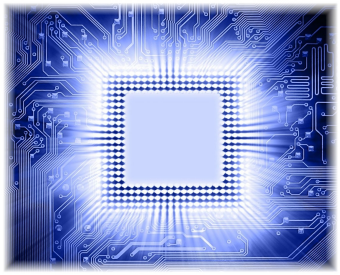
- Low cost, easy to fit in any project at any stage (even late), makes copying really difficult.
- Not strong enough for extreme protection (like monetary grade protection) but hard enough to require high efforts for cracking that are not worth it in most applications.

Anti-copy Principle

Advanced Logic Synthesis for Electronics
www.ALSE-FR.com

Block diagram

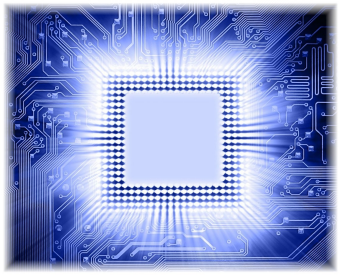




Simplified Theory of operation

Advanced Logic Synthesis for Electronics
www.ALSE-FR.com

- The unsecured user device (SRam-based FPGA) generates a long random challenge code at random times, in a random sequence, and sends this code to the authentication device over **a single wire**. This challenge code is also used by the internal FPGA encryption engine to produce the smaller expected authentication response inside the FPGA.
- The authentication device receives the challenge code, and starts the exact same computation as the FPGA.
  At the end of the calculation, the device sends back the response code to the User device (FPGA) over the (same) single-wire link.
- The FPGA receives the response code, and can compare with the code computed internally. If codes do not match, the FPGA knows that the authentication failed and can take appropriate actions.



Anti-copy Summary

Advanced Logic Synthesis for Electronics
www.ALSE-FR.com

- Extremely easy to integrate in a project (even at a late stage).
- CPLD cost can be < 2 $ in qty !
- Altera Max version fits in ~240 LCs.
- Very small FPGA overhead (less than 400 Logic Elements) !
- One-wire communication (uses only one FPGA pin).
- Several features complicate cracking attempts.
- The FPGA source code is not available to customers, and has been obfuscated before encryption.
- The anti-copy kit is protected by an Altera license
- Not strong enough for extreme protection (monetary systems)
- Data Sheets available on request