Security is a Major Concern

Diverse industries affected
• Credit cards, Set-top-boxes, ...
Security failure = Financial failure
Or even loss of business
Set Top Box division of ST had security concerns
• Needed a solution

Simplified (Security!) Problem Description

Design manipulating keys
• To decrypt data stream provided to consumers’ cable and satellite end point
Must check keys are not accidentally accessable from internal interfaces
• Security path is safe

Three major interfaces
• Only one interface can read keys back if rules allow that!
There are also System memory and RULES blocks
• Can be accessed by the design

Approach #1
Symbolic Approach for the Interface C: Idea

Approach #2
Miter Approach for the Interface C: Idea

Approach #3
X-Prop Approach for the Interface C: Idea

Approach #4
Symbolic Approach for the Interface C: PSL

Miter Approach for the Interface B: Idea

X-Prop Approach for the Interface B: Idea

Approach #5
Symbolic Approach for the Interface B: PSL

Miter Approach for the Interface A: Idea

X-Prop Approach for the Interface A: Idea

Simplified Design (Key Table) Diagram

Conclusion

Three security paths are verified
• Symbolic approach used as the most “confident” and “investigated”
Black boxing was used to conclude on assertions
• Proof real life time varying 5 mins – 30 mins
New IEV application is created
• Based on X propagation
• Automated set-up including covers, constraints and checks
• Provides witness waveform in case of security leakage