

Preface

This book is the result of a national project (ICTER) funded by the French National Research Agency (ANR) and involving four research centers (Montpellier, Paris, Lorient, Saint-Etienne) and a private company. When the project started in 2005, very few studies addressed the topic of digital security for reconfigurable architectures including FPGAs (Field Programmable Gate Arrays). But it was already clear that the sustained rate of integrating hardware and software resources in FPGAs would impact future embedded systems, especially in the field of digital security. The complexity of global systems has increased opportunities for designers and users but also resulted in an increase in vulnerabilities. We foresaw this problem and decided to combine efforts to identify the strengths and weaknesses of reconfigurable platforms from the point of view of security. We discovered a world of immense and unique opportunities for research. Our choice immediately focused on a holistic view, taking into account technological, logical, architectural and system levels, and hence, the security pyramid. This concept corresponds to a value chain structure in which the close links between each stage represent a significant gain, but also many potential security flaws.

Since 2005, we have not only been monitoring developments in the field but also been contributing to the state of the art. We have shown that by taking the target technology into account, it is possible to provide innovative techniques to build a system robust enough withstand a large number of attacks. We do not claim to have solved every problem, but we have established some rules and benchmarks that will undoubtedly be used in future applications on FPGAs. We would like to take this opportunity to thank all the contributors to this book, colleagues and PhD and Master students who shared and contributed to the same scientific objectives as we did. A warm thank to Dr. Reouven Elbaz, from Intel company, who friendly spent time to bring comments and remarks on our work. We all participated together in this very exciting project that involved many enthusiastic discussions and culminated in the significant contributions we are happy to share with you here. This project was generously supported by French Research Agency, ANR.¹ In fact, in 2005 ours was

¹<http://www.agence-nationale-recherche.fr/>.

among the very first projects to be approved by the ANR. We thank the ANR for having confidence in us and for supporting this work, without this support, this book would not exist.

“Security trends for FPGAs” is designed for all those who would like to upgrade their knowledge in the field of security and digital platforms including reconfigurable FPGAs. We believe you will find many useful technical references and solutions to your problems. We had a lot fun writing this book, we hope you will enjoy reading it just as much.

Montpellier, France
Paris, France
Saint-Etienne, France
Lorient, France
Montpellier, France

Benoit Badrignans
Jean Luc Danger
Viktor Fischer
Guy Gogniat
Lionel Torres

Security Trends for FPGAS

From Secured to Secure Reconfigurable Systems

Badrignans, B.; Danger, J.-L.; Fischer, V.; Gogniat, G.;

Torres, L. (Eds.)

2011, XV, 196 p., Hardcover

ISBN: 978-94-007-1337-6