Underwriters Laboratories Inc.  
UL Transaction Security  
Basingstoke  
RG23 8BG  
United Kingdom

Kui Wang

Email: [kw5g11@gmail.com](mailto:kw5g11@gmail.com)

Mobile: +44 07759343908

**WORK EXPERIENCE AND INTERNSHIPS**

***2017.04-now*** **Underwriters Laboratories (UL) -- *UK Security Laboratory***

***Senior Security Hardware Evaluation Engineer***

***Implemented Data Encryption Algorithm (DES) on Spartan FPGA and performed Side Channel Attack on the device***

* Coded DES in **VHDL** and reused data receiving module implemented in previous project**.**
* Synthesised the design files and downloaded into Xilinx Spartan **FPGA**.
* Performed Correlation Attack on EM traces collected when FPGA performs DES operation.
* The DES implementation was successfully broken under side channel attack.

***2012.07-2017.3*** **Underwriters Laboratories (UL) -- *UK Security Laboratory***

***Security Hardware Evaluation Engineer***

**Implemented data acquisition and display system for smart card power analysis**

* Schematic and Layout **PCB** with Eagle (SMD 0402) for theADC circuit (ADC08100, 100MHz).Soldered components on PCB manually. LT-Spice and Tina 9-TI were involved in circuit simulation.
* Designed ADC data receiving module in **VHDL** and synthesised on Xilinx Spartan **FPGA**, including FIFO and UART module.
* Built WindowsUser Interface application in **C# programming language** to receive digital data (ADC result) from FPGA through an RS232-to-USB convertor.
* Implemented a LUA scripting language editor in User Interface application to enable script programming.

**Implemented a laser trigger system with FPGA for UL TS**

* Designed windows application in **C#** programming language for laser parameter control
* Coded modules for system logic control in **VHDL**
* Implemented **PCB** interface between **FPGA** board and laser driver device
* Tested the whole laser system and successfully implemented on every UL TS evaluation bench.

Familiar with side-channel attackson cryptographic device (smart card microcontroller or FPGA)

Have cryptographic background, familiar with DES, AES and RSA.

**EDUCATION AND TRAINING**

***2011.12-2012.5*** Studied MIPS microprocessor pipeline architecture, cache memory and virtual memory principle.

***2010.09-2011.12*** School of Electronics and Computer Science, University of Southampton, UK

MSc Microelectronics Systems Design

**Managed a group of five people designing a 16-bit Microprocessor** (0.35um CMOS technique)

* Layout for a cell library (CMOS035 process) with ***MAGIC*** in UNIX.
* Designed instruction set and the architecture of microprocessor.
* Coded the behavioural model of microprocessor using programming language – ***SystemVerilog***.
* Simulated and validated the functionality of microprocessor behavioural model with multiplication program written in assembly language. EDA tool, **Modelsim**, was used.
* Took part in the data path layout and synthesised the control unit with L-Edit.
* Performed cross-simulation between behavioural model and synthesised processor.
* Coded another two assembly programs, factorial and random number generator, for testing purpose.
* Wrote Programmer’s Guide for the microprocessor.
* Managed the project on schedule successfully and delivered final report ahead of schedule.
  + - 1. University of Central Lancashire, Preston, UK
* Studied **microcontroller AT89C51,** including the structure as well as **assembly language programming**.
* Familiar with **Keil 3**

**2007.08-2009.06** Beijing Institute of Technology

**A rectangular waveform frequency counter implemented on PCB.**

* Coded Altera **CPLD** EMP7128SLC84-15 with **VHDL**.
* Simulation and debugging with tool, **Max+plus II** (the previous version of **Quartus II**).
* Designed **PCB** (Printed Circuit Board) with **Protel 99SE**

**MAIN SKILLS**

Software **Cadence Encounter RTL Compiler (Genus), Incisive Enterprise Simulator (NCsim), SOC Encounter (Innovus)**, **Modelsim, Magic,** L-edit, **ISE design suit, Quartus II (MAX+PLUS II)**, **Eagle,** Matlab, Protel 99SE, LT-spice, Tina 9-TI, Microsoft Visual C# 2010 Express, PSpice, Keil 3.

Languages **VHDL, Verilog HDL,** C#, assembly language, lua script language, SystemVerilog, C,

Operation Systems Windows, UNIX

**Reference available on request**