Vladimir Trujillo-Olaya received his B.S, M.Sc and Ph.D. in Electronics Engineering from Universidad del Valle, Cali-Colombia, School of Electrical and Electronics Engineering in 2004, 2009 and 2014, respectively.

His research interests are in hardware implementation of finite fields, and cryptosystems, embedded system design, fault tolerant design and hardware implementation of bioinformatics applications. He is a student member of the IEEE.
Trujillo-Olaya has been a reviewer of IBERCHIP and LASCAS and some national publications and international conferences. Currently, he is an associate professor at Universidad de San Buenaventura-Cali and an assistant professor at Universidad del Valle-Colombia.

Vladimir Trujillo-Olaya

+57 3182763938
vlatruo@gmail.com
vtrujillo1@usbcali.edu.co
Vladimir.trujillo@correounivalle.edu.co

Research Interests:

FPGA-Based System Design
Digital VLSI System Design
Hardware Implementation of Cryptographic Algorithms on FPGAs
DNA Alignment Implementation on FPGAs
Fault Injection Techniques on VHDL designs

Education

PhD. Electric and Electronic Engineering, Universidad del Valle
Efficient Hardware Implementation of GF(2^m) and GF(3^m) Arithmetic for Curve-Based Cryptography 2014

M.sC. Electronic Engineering, Universidad del Valle 2009
Design of Elliptic Curve Cryptoprocessor using Polynomial and Gaussian Normal Basis

B.S. Electronic Engineering, Universidad del Valle 2004

Professional Experience

Academic Appointments

Visiting Research Fellow, ArchLab, University of California, Santa Barbara, USA. Ago 2011- Ene 2012
"Lightweight cryptography"

Visiting Research Fellow, TIMA Laboratory, Technical National Institute, Grenoble, France. Feb - Aug 2007
Project: ALFA-NICRON, "Design and Verification of Fault-Tolerance Advanced Integrated Systems for Critical Applications"

Assistant Professor, Electrical and Electronic Engineering School, Universidad del Valle Sep-Dec 2007
Assistant Professor, Electrical and Electronic Engineering School, Universidad del Valle 2005 – 2006
Assistant Professor, Electrical and Electronic Engineering School, Universidad del Valle 2012 – actual
Asociate Professor, Universidad de San Buenaventura-Cali, Colombia 2012 - actual
Asociate Professor, Universidad Autónoma de Occidente-Cali, Colombia 2013 - actual

Professional Activities

Researcher Bionanoelectronic Research Group, Universidad del Valle 2004– Present
Researcher Applied Electronic Lab (LEA) Group

Publications

2014

- "Design of elliptic curve cryptoprocessors over GF(2^163) using the Gaussian normal basis", Paulo Cesar Realpe Muñoz, Vladimir Trujillo-Olaya, Jaime Velasco-Medina. Revista Ingeniería E Investigación vol. 34, Num.2. **ISSN**: 0120-5609
- *"Implementación hardware del algoritmo keccak para hash-3 y comparación con blake, grøstl, jh y skein*", Melissa Ramírez, César Augusto Pino, Vladimir Trujillo Olaya, Jaime Velasco Medina;
  Revista Infromador Tecnico, VOL. 77, NÚM. 2 . **ISSN** 0122-056X • **ISSN** Virtual: 2256 – 5035
- "*Hardware implementation of the Smith-Waterman algorithm using a systolic architecture*", Marmolejo-Tejada, J.M.; Trujillo-Olaya, V. ; Renteria-Mejia, C.P. ; Velasco-Medina, J. Circuits and Systems (LASCAS), 2014 IEEE 5th Latin American Symposium on; 25-28 Feb. 2014, Santiago de Chile.

- "*Design of elliptic curve cryptoprocessors over GF(2163) on Koblitz curves*", Realpe-Munoz, Paulo ; Trujillo-Olaya, Vladimir ; Velasco-Medina, Jaime. Circuits and Systems (LASCAS), 2014 IEEE 5th Latin American Symposium on; 25-28 Feb. 2014, Santiago de Chile.

2013

- "*Design of an Elliptic Curve Cryptoprocessor using Optimal Normal Basis over GF(2^233)*", Urbano-Molano, F.A. Trujillo-Olaya, V. ; Velasco-Medina, J., Circuits and Systems (LASCAS), 2013 IEEE Fourth Latin American Symposium on. Feb. 27 2013-March 2013. Cusco-Peru.
- "*8912-bit Montgomery multipliers using radix-8 booth encoding and coded-digit*", Renteria-Mejia, C.P. ; Trujillo-Olaya, V. ; Velasco-Medina, J. ., Circuits and Systems (LASCAS), 2013 IEEE Fourth Latin American Symposium on. Feb. 27 2013-March 2013. Cusco-Peru.

2012

- *"Analysis of performance versus security in hardware realizations of small elliptic curves for lightweight applications", V. Trujillo-Olaya, T. Sherwood, and C. K. Koc. Journal of Cryptographic Engineering, 2(3):179-188, Volume 2, Issue 3, 2012,* **ISSN**: 2190-8508 (print version) **ISSN**: 2190-8516 (electronic version)
- "Design *of an 8192-bit RSA cryptoprocessor based on systolic architecture*" Claudia Patricia Renteria, Vladimir Trujillo-Olaya, Jaime Velasco-Medina, Programmable Logic (SPL), 2012 VIII Southern Conference on; Maezo 20-23 2012; Bento Goncalves Brasil.
- "Implementación Hardware de un Multiplicador Serial Basado en Bases Normales sobre GF(2^163)" FERNANDO APARICIO URBANO MOLANO, VLADIMIR TRUJILLO OLAYA, JAIME VELASCO MEDINA, Iberchip XVIII Workshop, 2012, Mexico

2011

- *"Design of an Elliptic Curve Cryptoprocessor over GF(p)", Abraham Farfan, Vladimir Trujillo, Jaime Velasco, Evento: XVII Iberchip 2011 Bogota, Colombia.*

2010

- *"Hardware Architectures for Elliptic Curve Cryptoprocessors Using Polynomial and Gaussian Normal Basis Over GF(2^{233})"*, Vladimir Trujillo-Olaya, Jaime Velasco-Medina, Special issue on Security in Computing Part II, Series Lecture Notes on in Computer Science **ISSN**:0302-9743. Vol 6480. Subseries: Transaction on Computational Science . Editor-in-chief: Gravilova, Marina L; Tan,C .J Keneth; First edition, 2010 softcover **ISBN**: 978-3-642-17696-8 p.79-103.
- *"Hardware Architectures for Inversion in GF(2^m) Using Polynomial and Gaussian Normal Basis"*, Vladimir Trujillo-Olaya, Jaime Velasco-Medina, IEEE ANDESCON 2010, Bogota – Colombia.
- *"Bit-Flip Injection Strategies for FSMs Modeled in VHDL Behavioral Style"*, John M. Espinosa, Vladimir Trujillo-Olaya, Jaime Velasco-Medina, Raoul Velazco, 11 LATW , Punta del Este, Uruguay.
- *"Dependability Validation of a Cryptoprocessor to SEU Effects"*, Vladimir Trujillo-Olaya, John M. Espinosa, Jaime Velasco-Medina, Raoul Velazco, 11 LATW , Punta del Este, Uruguay.
- *"Hardware Architectures for Inversion in GF(2^m)"*, Vladimir Trujillo-Olaya, Jaime Velasco-Medina, XVI Iberchip, Iguazu Falls, Brasil.
- *"Diseño en Hardware para los cifradores de flujo Grain-128, Mickey-128, Decim-128 y Trivium"*, Juan Manuel Marmolejo, Vladimir Trujillo-Olaya and Jaime Velasco-Medina, XVI Iberchip, Iguazu Falls , Brasil.
- *"Diseño de un Criptoprocesador RSA de 8192 bits usando un Multiplicador Sistólico"*, Claudia Patricia Renteria, Vladimir Trujillo-Olaya, Jaime Velasco-Medina, XVI Iberchip, , Iguazu Falls , Brasil

2009

- *"Implementacion Hardware de la funcion Hash SHA224"*, Vladimir Trujillo-Olaya, Jaime Velasco-Medina, XV Workshop Iberchip, Buenos Aires Argentina
- *"Diseño del Multiplicador de Montgomery basado en un Arreglo Sistolico Generico"*, Claudia Patricia Rentería-Mejía, Vladimir Trujillo-Olaya, John Michael Espinosa-Durán, Jaime Velasco-Medina, XV Iberchip, , Buenos Aires, Argentina
- *"Arquitectura Eficiente para un Criptoprocesador de Curvas Elípticas sobre GF(2163) usando Bases Normales Gaussianas"*, Paulo Realpe-Muñoz, Vladimir Trujillo-Olaya, Jaime Velasco-Medina, XV Iberchip, , Buenos Aires, Argentina

2008

- *"In-System Hardware Dependability Validation Of The SEUs Effects In A Cryptoprocessor"*, Vladimir Trujillo-Olaya, John Michael Espinosa-Duran, Jaime Velasco-Medina, 9 LATW, Puebla, Mexico

2007

- *"Diseño de un carné de identificación universitario mediante tarjetas inteligentes"*, Edwin Vargas – García, Vladimir Trujillo – Olaya, Jaime Velasco – Medina, Revista Ingeniería y Competitividad Volumen 9 : Número 2 : Artículo 7 **ISSN**: 0123-3033, 2007 vol:9 fasc: 2 págs: 93 – 104
- *"Simulation of SEUs in a Cryptoprocessor Using VHDL"*, Vladimir Trujillo, Jaime Velasco-Medina, Raoul Velazco, First International Congress on Dependable Integrated Circuits Design, DECIDE 2007, Buenos Aires, Argentina
- *"Design of polynomial basis multipliers over GF(2^{233})"*, Vladimir Trujillo, Jaime Velasco-Medina, XIII Workshop Iberchip, Lima, Peru
- *"Efficient Hardware Implementations for Gaussian Normal Basis Multiplication Over GF (2^{163})"*, Vladimir Trujillo, Jaime Velasco-Medina, Julio Cesar Lopez, III Southern Conference on Programmable Logic , Mar del Plata , Argentina SPL 2007
- *"Diseño de Aceleradores para el Alineamiento Global de Secuencias de ADN"*, Martin A. Lozano, Vladimir Trujillo-Olaya, Jaime Velasco-Medina, III Southern Conference on Programmable Logic , Mar del Plata , Argentina SPL 2007

2006

- *"Design of Gaussian Normal and Polynomial Basis Multipliers over GF(2^{163})"*, Vladimir Trujillo-Olaya , Jaime Velasco-Medina, Julio. C. López-Hernández, XII Iberchip, San Jose, Costa Rica

2005

- *"Design of an elliptic curve cryptoprocessor"*, Vladimir Trujillo-Olaya , Jaime Velasco-Medina, Julio. C. López-Hernández, XI Workshop Iberchip, Salvador de bahia, Brasil

2004

- *"Diseño de un procesador criptográfico para curvas elípticas sobre GF(2^{163})"*, Vladimir Trujillo-Olaya , Jaime Velasco-Medina, Julio. C. López-Hernández, X Workshop Iberchip, Cartagena

2003

- *"Multiplicador en el cuerpo finito GF(2^{163}) usando Bases Normales Gaussianas"*, Vladimir Trujillo-Olaya , Jaime Velasco-Medina, Julio. C. López-Hernández, IX Workshop Iberchip, Cuba