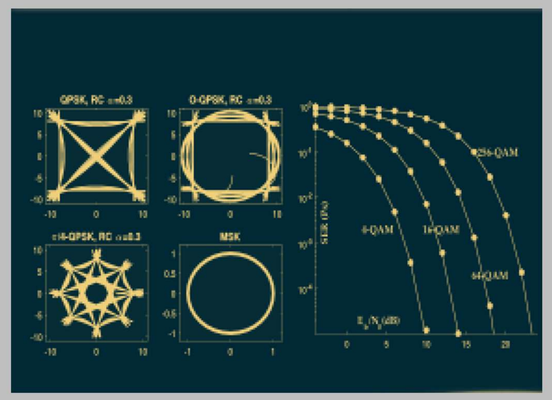
CASP

CIRCUIT AND SIGNAL PROCESSING GROUP

casp@bahria.edu.pk

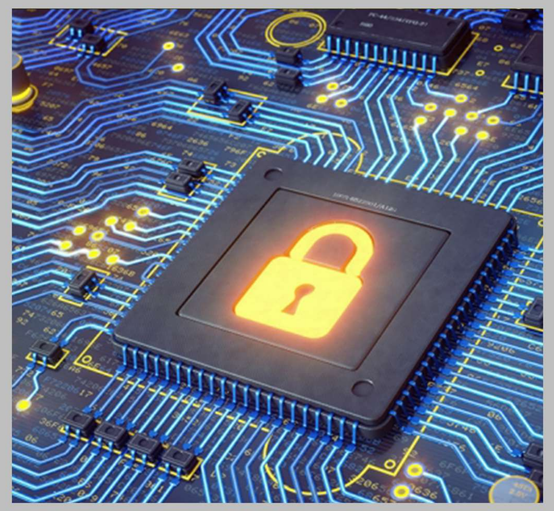
Circuit design covers systems ranging from complex electronic systems to the individual transistors within an integrated circuit. Moore's law has driven the worldwide semiconductor industry; as such, the expectation of continued device scaling drove fundamental research on physics, materials, devices, interconnect, leading to an enormous and diverse range of commercial electronics. As we move into the era of nanoscale devices, however, scaling-as-usual is under significant duress. The devices are smaller, but many aspects of their performance deteriorate: for example, leakage increases, gain decreases, and sensitivity to unavoidable small fluctuations in the manufacturing process rises dramatically. The Circuit and Signal Processing (CASP) Group in the Department of Electrical Engineering, Bahria University, Islamabad Campus focusses on scientific theory, analysis, design and implementation of circuits, and the application of circuit to systems and signal processing. The key research directions in circuit domain include but not limited to; hardware implementation of baseband wireless communication, cryptographic algorithms, FPGA-based cyber security solutions, EMI issues in high-speed serial links and visible light communication system. The work of CASP research group in signal processing domain includes information processing as well as the theory and application of filtering, coding, transmitting, estimating, detecting, analyzing, recognizing, synthesizing, recording, and reproducing signals to solve real world problems. One of the salient features of this group is its capacity to undertake and deliver product oriented projects. In this regard, projects have been delivered to Military and Industrial Partners such as Pakistan Air Force, NESCOM, Maritime Technologies Complex.

RESEARCH & SERVICES PORTFOLIO



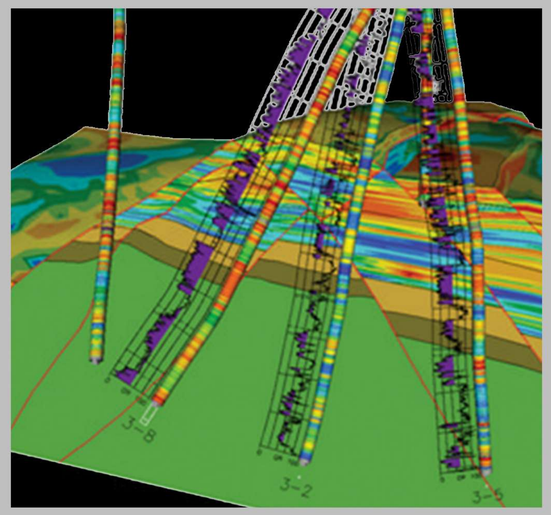
Flexible and Scalable Turbo Receiver

Additive White Gaussian Noise (AWGN) and fading are the key factors affecting the quality of wireless communication. Iterative receivers using the concept of feedback remove the effect of AWGN and fading during multiple iterations through the concept of Turbo Decoding, Turbo Demodulation and Turbo Equalization. This project focuses on development of a Turbo Receiver implementing three turbo processes on a single hardware architecture. To address the flexibility related to different wireless standards, the architecture is based on Application Specific Instruction Processor (ASIP) whereas the communication is handled through the use of Network on Chip (NoC). Three different ASIPs have been developed for decoding, demapping and MIMO Equalization. In each ASIP, data path is designed in such a way that algorithm level parallelism is implemented to get the best compromise between flexibility and throughput. Data level parallelism is achieved through adding multiple instances of each ASIP which makes the architecture scalable. Additionally, NoC are used which ensure reliable communication between multiple ASIPs.



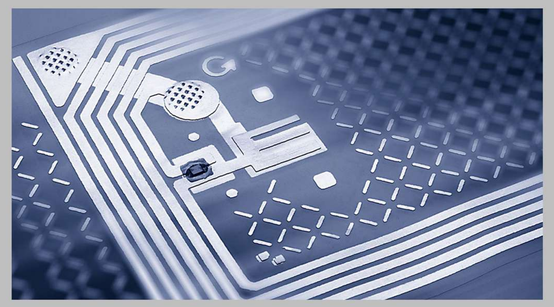
ACryp-Proc: Flexible Asymmetric Crypto Processor for Point Multiplication

Flexibility is one of the driving agents for 5G architecture development to incorporate Enhanced Mobile Broad Band (eMBB), Machine Type Communication (MTC) and ultra-reliable MTC. While considering flexibility in the domain of security/reliability, we present a unified and flexible hardware architecture, implementing point multiplication algorithm for both Elliptic Curve Cryptography (ECC) and Binary Huff Curves (BHC). The proposed architecture can be used in the scenarios where the users can tradeoff between the algorithmic execution time and different reliability/security levels. To establish an area overhead for the unified design, dedicated architectures for ECC and BHC over the GF(2m) field are implemented. Then, a unified architecture for ECC and BHC is implemented. The performance results of proposed unified architecture promise a good trade-off between execution time and security level.



Advanced Petrophysical Analysis Framework

Well log curve records the physical, electrical or other properties of the rock/ fluid mixtures penetrated by drilling a borehole into the subsurface. These logs are then converted into raster images which are further digitized for geological interpretation. Researchers are developing advanced petrophysical analysis and interpretation framework which aids geoscientists and petroleum engineers in efficiently finding highly probable hydrocarbon formations. The proposed framework first extracts the petrophysical parameters and utilizes the extracted information for an in-depth analysis and 3D visualization of subsurface geology for oil and gas exploration.

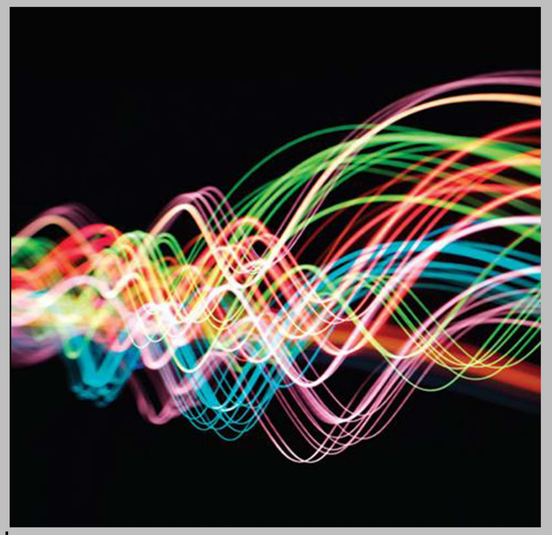


Ultralightweight RFID Authentication Protocol

RFID is one of the most promising identification schemes in the field of pervasive systems. Due to wireless channel incorporation, security issues arise and to make the system reliable and secure, numerous Ultralightweight Mutual Authentication Protocol (UMAPs) have been proposed which involve only simple bitwise logical operations in their designs. However, almost all of the previously proposed UMAPs are reported to be vulnerable against various security attacks. We propose a new pseudo-Kasami code based Mutual Authentication Protocol (KMAP) which avoids unbalanced logical operations and introduces a new Ultra lightweight primitive: pseudo-Kasami code. This enhances the diffusion properties of the protocol messages and makes hamming weight of the secrets unpredictable and irreversible. The performance evaluation shows that the KMAP requires fewer resources on the tag in terms of on-chip memory, communication cost and computational operations which makes it a more feasible protocol.

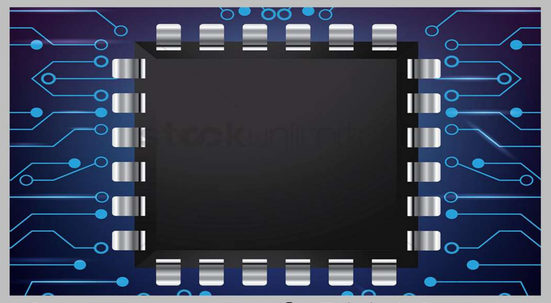
Cryptanalysis of Ultralightweight Mutual Authentication Protocol for Radio Frequency Identification Enabled IOT Networks

The main aim of this product is to eradicate all security issues that were present in existing implementations (at a lower resource cost). Without a doubt, IOT is the center of modern technology. It helps to interconnect devices with each other and also with the rest of the world. The RFID system is used as a node/linkage point in IOT systems. Due to its relative openness, IOT systems are quite vulnerable against malware. To reduce this and also the cost that goes into it, researchers only use XOR and rotation functions as a proposed ultralightweight authentication protocol. This helps to fend off all sorts of attacks.



Waveforms for Future Wireless Communication

A number of issues are experienced with the wireless communication. In order to rectify some of these issues, an architecture has been developed which is an advanced alternative to OFDM. The hardware is built specifically to implement UFMC transmitter. The reduced complexity schemes for IFFT, filtering and spectrum shifting help to achieve a minimalist cost. The whole design uses far less resources than previous implementations in terms of registers, LUTs and MUXs. Throughput and frequency amount up to 773.5 Msamples/s and 364 MHz respectively. The presented architecture provides only 2% latency. This can be further modified due to the scalable nature of 10MHz LTE architecture.

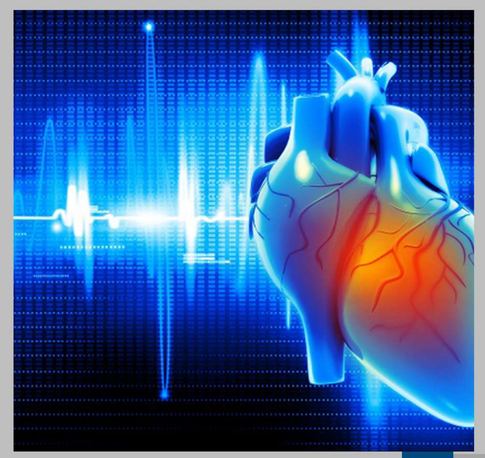


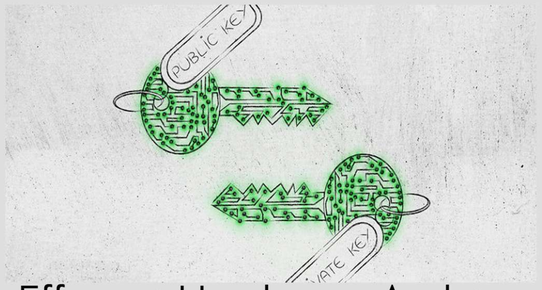
Suppression of CM Noise in High-Speed SERDES Links

EMI is becoming a serious issue as the data rate per lane and the number of parallel lines continue to grow rapidly. It is therefore essential for system-on-package (SOP) integrating multiple drivers to have smaller electromagnetic radiation and to minimize EMI inside active devices. Regulatory limits prescribed by FCC and CISPR are in place to control maximum radiation. The distorted differential signal in a communication link generates an unwanted common-mode (CM) component more severely at the backplane connector at double the Nyquist frequency and harmonics. The generated spectrum components are later radiated by PCB parasitic antennas and causes EMC failure. Therefore, it is essential to counter the EMI issue during the product design phase instead of handling it at the end of product development. The prosposed arhcituecture calibrates the pull-up and pull-down path reisstance, conserving the RC constant over the PVT variations and results in 20% increase in symmetry of rising and falling edge and reduce the peak CM noise by 80% whilst achieving better signal quality.

Analysis of PCG Signals for the Diagnosis of Cardiovascular Abnormalities

Cardiac disorders are spreading rapidly all over the world . As per World Health Organization (WHO), 17.5 million people die each year due to cardiovascular diseases (CVD). This implies that, there is a dire need to develop cost effective, time efficient and fully automated solutions to diagnose cardiovascular abnormalities. Many researchers have worked on detecting CVD from electrocardiogram (ECG) signals. where, ECG signals gives reliable information about cardiac pathology however phonocardiogram (PCG) signal provides an easy, cost effective, objective and comprehensive information about cardiovascular abnormalities by measuring heart beats. Accordingly, we are working on developing a fully automated robust clinical decision support system that can identify cardiovascular abnormalities by analyzing heart sounds from PCG signals.





Efficient Hardware Architectures for Scalar Multiplication on Elliptic Curves

Suitable cryptographic protocols are required to meet the growing demands of data security in many different systems, ranging from large servers to small hand-held devices. Many constraints such as computation time, silicon area, power consumption, and security level must be considered by the designers. Elliptic curve cryptography (ECC) based crypto-systems are better in terms of the bandwidth utilization, power consumption, implementation cost and are considered as an excellent choice in future hand-held and IoT devices. However, underlying computational intensive mathematical operations in ECC restrict its deployment in many applications. This work proposes many interesting and novel high-speed flexible ECC hardware architectures. The proposed designs provides excellent tradeoffs between throughput and hardware resource consumption. In addition, these designs also have resistance to many side channel attacks and can be deployed where there is a threat of physical security.

FPGA and RSD ECC Point Multiplication Accelerators

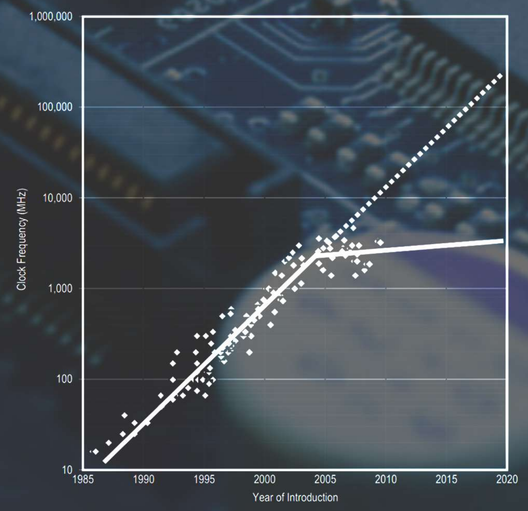
Finite Field arithmetic (FFA) primitives are the bottleneck in Point Multiplication (PM) operation in ECC. This project explores both circuit and system levels to optimize different FFA operations. At the circuit level to reduce the long carry propagation delay, a Redundant-Signed-Digit (RSD) based approach is adopted which somehow facilitates the carry free operations. At the system level, different coordinates systems and PM algorithms were deeply examined and modified according to the project requirements. The designs are proposed for different category of elliptic curves and different security levels. The targeted curves are general, NIST and more recent famous Curve448 and Curve255. These novel designs are synthesized and implemented on different Field programmable Gate Array (FPGA) platforms. The implementation results reveal that the proposed designs outperform almost all of the existing state of the art designs.

Apple Harvester Robot

This research project aims to improve picking efficiency of apple harvester using advanced computer vision. It focuses on rapid picking methods like SLAM, visual obstacle and occlusion avoidance. The goal of this research is to deepen our understanding of apple picking using modern robots. The research work is closely connected to Machine Vision and visual Servo Design. This project has also been provisionally approved by the Ministry of Science and Technology China and currently being reviewed in Ministry of Science and Technology Pakistan under protocol 18 and 19 of Intergovernmental research collaborations.

MOORE'S LAW ENDING?

"Scaling silicon is not the only way to get lower power and better performance. It was just the easiest way until 10 years ago."



KEY RESEARCHERS

Dr. M. Najam ul Islam

Dr. Najam ul Islam is currently serving as a Professor and the Dean with the Faculty of Engineering and Sciences, Bahria University, Islamabad. He received his bachelor's degree in electrical engineering from UET, Lahore, Pakistan, and a Master's degree in computer sciences from LUMS. He further completed his Ph.D. degree in electrical engineering from Telecom ParisTech, France. During his doctoral studies, he was with EURECOM, Sophia Antipolis on the research theme of Flexible Radios for Multi-Standard Wireless Communication Devices. He was also engaged with the Government of Pakistan in Research and Development projects from 1998 to 2004. Moreover, he has authored over 40 papers in reputed international journals and conferences. His current research interests include Information Security, Flexible Radios, and Renewable Energy.

Dr. Atif Raza Jafri

Dr. Jafri is serving as Head of Department, Electrical Engineering at Bahria University Islambad. He received his B.Sc. degree in electrical engineering from UET Lahore, Pakistan, in 1999, the M.S. degree from the University of Nice Sophia Antipolis, France, in 2007, and a Ph.D. degree from Telecom Bretagne, Brest, France, in 2011. He has served in the Research and Development sector for over ten years. His research interests include hardware architectures implementation for wireless communication and cryptographic applications using both HDL and HLS. He is also involved in research related to architectures of physical layer of future wireless communications and ultra-light weight and asymmetric cryptography.

Dr. Khawaja Qasim Maqbool

Khawaja Qasim Maqbool received his Ph.D. in Electronic and Computer Engineering from The Hong Kong University of Science and Technology. He is currently serving as a Sr. Asst. Professor in EE Department, BUIC. His research focuses on signal integrity and high-speed wireline and optical communication IC design. Qasim has also published several research papers in highly reputed journals and conference proceedings as part of his Ph.D. research. He is a reviewer for IEEE ISCAS and BioCAS. He was awarded a national fellowship for M.Sc. & Ph.D. studies, he is a co-recipient of the best paper award finalist at DesignCon 2017, and his ISCAS 2017 paper has been invited for the TCAS-I special issue. He was awarded a student travel grant for ISSCC 2018 and received HKUST research travel grant twice. He is a member of IEEE CASS and SSCS, Professional Engineer, PEC. He has been awarded HEC research start-up grant on suppression of common-mode noise in high-speed serial links. He is also a HEC approved supervisor.

Dr. Taimur Hassan

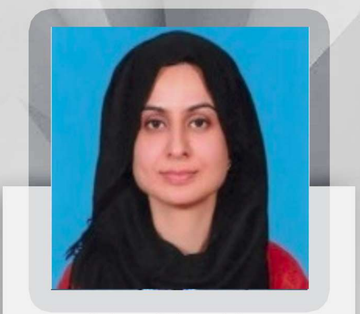
Dr. Taimur Hassan is one of the top young researchers and academicians of Pakistan who is actively involved in cutting edge research in the areas of medical image analysis, biomedical signal processing, artificial intelligence, embedded computing and Internet of Things. He received his Ph.D from NUST, Pakistan and his dissertation is in the field of Ophthalmic Image Processing. Taimur has 6 years of industrial and teaching experience. Currently, he is working as a Lecturer in the EE Department, BUIC. He has been a part of many local and foreign research projects. Currently, he is leading one project as a Principal Investigator. He is a recipient of various national and international awards. He is also serving as a reviewer in IEEE Journal of Biomedical Health Informatics [Quartile Score: Q1, Impact Factor: 3.85], IEEE Access [Quartile Score: Q1, Impact Factor: 3.557] and Springer Journal of Digital Imaging [Quartile Score: Q2, Impact Factor: 1.536]. His Ph.D. research won Gold Award in Research & Development category at (P@SHA) 2016 and Asia Pacific ICT Alliance (APICTA) 2016. Recently he and his team won Gold Award in the Artificial Intelligence category at P@SHA 2018. Mr. Taimur Hassan has 30+ research publications in last 3 years having 100+ research citations with the cumulative impact factor of 24.399.

Dr. Khalid Javeed

Dr. Khalid received Ph.D. from School of Electronics Engineering, Dublin City University. His PhD study was funded by Telecommunication Graduate Initiative (TGI). He is currently senior Asst. Professor and Head of Computer Engineering Department His research focuses on cryptographic engineering, hardware software co-design and hardware acceleration of signal processing & machine learning algorithms. He has published several research papers in journals and conferences of international repute. He is a reviewer of IEEE Trans. on Circuit and Systems II, IEEE Trans. on VLSI and Elsevier Microprocessor & Microsystems.

Dr. Imran Fareed

Dr. Imran Fareed Nizami is currently serving as a Senior Assistant Professor in the Department of Electrical Engineering, Bahria University, Islamabad Campus. He received his B.S. degree in Computer Engineering from UET Taxila, Pakistan, and M.S. degree in Electrical and Electronic engineering from Yonsei University, South Korea. He recieved his Ph.D. in Electrical Engineering from National University of Science and Technology (NUST), Pakistan. Furthermore, his research interests include image quality assessment and machine learning.



Ms. Madiha Khalid

Madiha Khalid received her B.S. degree in Electrical Engineering from University of Engineering and Technology, Lahore in 2010, and M.S degree in Electrical Engineering from CASE affiliated with University of Engineering and Technology, Taxila in 2012. She is currently doing Ph.D. in Electrical Engineering from Department of Electrical Engineering, Bahria University, Islamabad Campus. She is also working as a Senior Lecturer and Women in Engineering (WIE) coordinator in the Department of Electrical Engineering, Bahria University Islamabad Campus. Her research focuses on cryptanalysis of ultra-light weight mutual authentication protocol for radio frequency identification enabled Internet of Things networks. She is a member of IEEE and advisor of IEEE student branch Bahria University.