Oral S10

Advanced Baseband Communication and Cryptosystem Design

Date/Time 8/4 (四) 13:30-14:30

Chair(s) 施信毓教授 / 國立中山大學電機工程學系
吳志峰教授 / 長庚大學電子工程學系

S10.1 13:30 — 13:42

Reconfigurable Filtered-OFDM Baseband Processor for Mobile Communications

Huan-Lun Tso[1], Chun-Yu Chen[1], Ching Hsu[2], Pei-Yun Tsai[3], and Yuan-Hao Huang[1, 2]
[1]Institute of Communications Engineering, National Tsing Hua University
[2]Department of Electrical Engineering, National Tsing Hua University
[3]Department of Electrical Engineering, National Central Univerisity[1, 2]

Orthogonal Frequency Division Multiplex-ing (OFDM) has been widely used in wireless communi-cation systems. Filtered-OFDM is one of the potential improved modulation waveform for the 5G/B5G communication systems. Filtered-OFDM is a per-subband-filtering multi-carrier modulation, in which whole bandwidth is divided into several subband each carrying individual data information. The per-subband-filtering approach can reduce out-of-band emission and then avoid adjacent-channel interference (ACI). This work designed and implemented a reconfigurable filtered-OFDM baseband processor that supports 14 different frame structures in terms of bandwidth, FFT size and subcarrier spacing. The proposed processor was designed and synthesized by using TSMC 40 nm CMOS process technology. The proposed filtered-OFDM processor chip achieves maximum throughput of 840 Mb/s at clock speed of 140.9 MHz with chip area of 12 mm^2.

S10.2 13:42 — 13:54

Beam Tracking Based on Deep Reinforcement Learning for Hybrid Beamforming MIMO Communications Systems

Po-Chuan Huang and Pei-Yun Tsai
Department of Electrical Engineering, National Central University

In this paper, beam tracking based on deep reinforcement learning (DRL) in hybrid beamforming multiple-input multiple-output (MIMO) systems is designed and verified. With channel state information (CSI), the deep deterministic policy gradient (DDPG) of DRL is employed to compute the analog precoder, called aBFNet, which achieves good channel capacity. In the last layers of the actor network of the aBFNet, output normalization is performed and is considered during back propagation so that the generated outputs satisfying the magnitude constraint can be applied to the phase shifters directly. In addition, time-varying channels are taken into consideration and can be tracked by the aBFNet. Simulation results demonstrate the feasibility of aBFNet and its good performance compared to the conventional hybrid beamforming algorithm.

S10.3 13:54 — 14:06

High-Performance Radix-4 Montgomery Modular Multiplier with Carry-Propagation Free Format Conversion

Yen-Jui Chen, Chun-Yi Wang, and Shiann-Rong Kuang
Department of Computer Science and Engineering, National Sun Yat-sen University

Carry-save arithmetic and higher radix are frequently adopted to enhance the performance of Montgomery modular multiplication. In this paper, a carry-save radix-4 Montgomery modular multiplier is proposed to speed up the modular multiplication while maintaining a short critical path and low hardware complexity. The proposed multiplier takes binary numbers as the input/output operands and adopts Booth encoding in which a triple of modulus is replaced with a negative of modulus to reduce the register usage. Moreover, the carry-save adder (CSA) is used to not only perform the intermediate addition operations but also convert the result of modular multiplication from carry-save representation to binary representation to avoid the long carry propagation. The critical path of proposed multiplier is further shortened by simplifying quotient calculation, rapidly generating two's complement form of negative multiples, and pipelining the execution of Booth encoding and selection. In addition, an efficient detect circuit is developed to suspend the unnecessary carry-save addition operations so that the extra clock cycles for format conversion can be significant reduced. Experimental results show that the proposed multiplier can achieve considerable area-time product improvement when compared with previous designs.

S10.4 14:06 — 14:18

A new natural plant self-awareness Phytosensing sensor based on Electrophysiology circuit design

Yu-Hsien Yao and Chi-Chia Sun,
Department of Electrical Engineering, National Formosa University

In recent years, plant electrophysiology has become a feasible invasive tool for describing the thinking of plant properties of many systems. In this paper, we proposed a new electrophysiological sensor presented as an autonomous device, which can transfer plant electrical potential data into plant self-awareness information, it will explore how plants can end up in plant factories or smart warming and artificial intelligence technology to achieve the concept of making plants "think themselves". Plant sensing can measure certain aspects of the internal state of natural plants. The proposed sensor circuit design is based on ECG and EEG measurement methods in electrophysiology respectively. The major contribution of this paper is to use electrophysiological measure method to collect data that the plants themselves behavior can be further analyzed through machine learning. The experimental result shows that with each sensing condition with the external stimuli through the proposed plant electrophysiology sensor module (light, heat, humidity, CO2, etc.) the potential changes can be observed.

S10.5 🕓 **14:18 — 14:30**

VLSI Implementation of RSA cryptography

Chia-Yu Liu[1] and Yuan-Ho Chen[1, 2]
[1]Dept. of Electronics Engineering, Chang Gung University
[2]Dept. of Radiation Oncology, Chang Gung Memorial Hospital

RSA cryptosystem is a common asymmetric cryptography. Due to the complexity of the operation, it is hoped that the hardware can effectively improve its operation speed.The architecture proposed in this paper includes interleaved modular multiplication, modular exponentiation, Baillie-PSW primality test, and extended Euclidean algorithm. According to the architecture proposed in this paper, it is finally implemented on the chip of the TSMC 90nm CMOS technology. The operating frequency was 28.57 MHz, and the average operation time is about 0.34 ms. Finally, the architecture can be scaled directly to 1, 024 bits without further modification.