Papers Published in Technical Journals and Conferences

An efficient quantum circuit for addition in GF(ρ) and Shor's algorithm

Y. Takahashi, N. Kunihiro, and K. Ohta

University of Science and Technology of China, Asian Conference on Quantum Information Science 06, Vol. 1, No. 1, pp. 109–110, Sept. 2006.

We decrease the number of qubits in Proos et al.'s quantum circuit for Shor's discrete logarithm algorithm for elliptic curves over the prime field GF(ρ). To decrease the number of qubits, we use the quantum circuit for addition with no ancillary qubits we have proposed. When we use the circuit for addition in place of the one in Proos et al.'s circuit, the number of qubits decreases from about $5n$ to $4n$ without increasing the depth and size, where n is the length of the binary representation for ρ. Moreover, we construct an efficient quantum circuit for addition in GF(ρ) that is useful for further decreasing the number of qubits.

GMPLS-based VPN service to realize end-to-end QoS and resilient paths

H. Matsuura and K. Takami

APNOMS 2006, Busan, Korea, Vol. LNCS 4238, pp. 302–311, Sept. 2006.

We propose a hierarchically distributed path computation element (HDPCE) architecture to improve existing PCE backup techniques. In this paper, we describe detailed path backup methods performed by HDPCEs to demonstrate the promising potential of HDPCE architecture.

Trusted-Link: Web-Link Enhancement for Integrity and Trustworthiness

S. Orihara, Y. Tsuruoka, and K. Takahashi

ACM, Workshop on Digital Identity Management (DIM2006), Vol. 1, No. 1, pp. 17–24, Nov. 2006.

We introduce Trusted-Link, a new framework that assures trust relationships between Web pages. With this framework, users can distinguish trustworthy pages from untrustworthy pages easily. This helps users avoid online fraud such as phishing. The ideas of Trusted-Link are as follows. (1) Add some attributes to a link (e.g. HTML anchor element), such as maximum number of traversable links or set of trusted domains. (2) Determine trust level of linked page based on trust level of current page and attributes of link. (3) Attach digital signature to the link to maintain its integrity. (4) A link has a signature verification key as its attribute to verify a signature in a linked page.

In this paper, we explain the trust model of Trusted-Link compared to TLS server authentication using a PKI, and algorithms of Trusted-Link, and then, we give some consideration about its effectiveness.

Asymmetric synthesis of amino acid precursors in interstellar complex organics by circularly polarized light

Y. Takano, J. Takahashi, T. Kaneko, K. Marumo, and K. Kobayashi

Earth and Planetary Science Letters, Elsevier, Vol. 254, pp. 106–114, Jan. 2007.

The asymmetric synthesis of amino acid precursors from complex organics have been performed. A gaseous mixture of carbon monoxide, ammonia and water (molecules which are among those identified in the interstellar medium) was irradiated with 3.0 MeV protons to obtain amino acid precursors within high-molecular-weight complex organics of up to 3000 Da. The amino acid precursor products synthesized were then irradiated with right (R-) or left (L-) ultraviolet circularly polarized light (UV–CPL) obtained from a synchrotron radiation (SR) source. Glycine was a predominant product, and number of chiral amino acids including alanine were identified following acid hydrolysis. R-UV–CPL preferentially produced D-alanine, while L-UV–CPL produced more L-alanine. Enantiomeric excesses (% D–% L) of +0.44% and -0.65% were obtained by R-UV–CPL and L-UV–CPL, respectively. These results imply that the origins of chirality in meteoritic amino acids could be accounted for by the formation of asymmetric amino acid precursors from extraterrestrial complex organics by CPL in space.

Analysing the penalty induced by PDλ of MZI in DQPSK receiver using novel measuring technique

H. Kawakami, E. Yoshida, Y. Miyamoto, and M. Oguma

IEE Electron. Lett., Vol. 43, No. 2, pp. 121–122, Jan. 2007.

The first demonstration is described of the quality degradation in a differential quadrature phase shift keying (DQPSK) receiver due to the polarisation dependent wavelength response (PDλ) of a Mach-Zehnder interferometer (MZI) and carrier frequency drifting. In the method, the value of PDλ and the corresponding penalty can be measured simultaneously at the receiver. Experimental data shows good agreement with the analysis.

The Quantum Fourier Transform on a Linear Nearest Neighbor Architecture

Y. Takahashi, N. Kunihiro, and K. Ohta

The University of Queensland, Quantum Information Processing Workshop, Vol. 1, No. 1, pp. 1–2, Jan. 2007.

We show how to construct an efficient quantum circuit for computing an approximation of the quantum Fourier transform modulo 2^n with precision $1/n^{O(1)}$ on a linear nearest neighbor architecture. The constructed circuit uses no ancillary qubits and its depth and size are $O(n)$ and $O(n\log n)$, respectively. The circuit is useful for constructing an efficient quantum circuit for Shor's algorithm on a linear nearest neighbor architecture. (Full version accepted for publication in Quantum Information and Computation)

Disjointed SRLG Routing for GMPLS Networks by Hierarchically Distributed PCE

H. Matsuura, N. Morita, T. Murakami, and K. Takami

IEICE Trans. Commun., Vol. E90-B, No. 1, pp. 51–62, Jan. 2007.

Multilayered network interaction among various networks such as IP/MPLS packet networks and optical fiber networks are now achieved using generalized multiprotocol label switching (GMPLS) technology. One unique feature of GMPLS networks is that GMPLS packet-layer label switching paths (LSPs), such as IP/MPLS LSPs, sometimes tunnel through GMPLS lower layer LSPs such as optical fiber/lambda LSPs. One problem that occurs in this situation is protecting an important primary packet LSP by using a protection LSP that is physically separated from the primary LSP. The packet router

has difficulty recognizing lower layer LSPs that are totally disjointed from the primary LSP. This is because, in a GMPLS's packet layer, a source router only differentiates one lower layer LSP from another, and does not check the disjointedness of segments through which the lower layer path passes. Sometimes, different lower LSPs pass through the same optical fiber, and a malfunction of one optical fiber sometimes causes many lower layer LSPs to malfunction at the same time. To solve this problem, a shared risk link group (SRLG) is introduced. Network links that belong to the same SRLG share a common physical resource. We apply this SRLG to the proposed hierarchically distributed path computation elements (HDPCEs) and achieve effective disjointed SRLG protection for important primary GMPLS packet paths.

UTC-PD-Based Optoelectronic Components for High-Frequency and High-Speed Applications

S. Kodama and H. Ito

IEICE Trans. Electron, Vol. E90-C, No. 2, pp. 429–435, Feb. 2007.

The uni-traveling-carrier photodiode (UTC-PD) is an innovative PD that has a unique operation mode in which only electrons act as the active carriers, resulting in ultrafast response and high electrical output power at the same time. This paper describes the features of the UTC-PD and its excellent performance. In addition, UTC-PD-based optoelectronic devices integrated with various elements, such as passive and active devices, are presented. These devices are promising for various applications, such as millimeter- and submillimeter-wave generation up to the terahertz range and ultrafast optical signal processing at data rates of up to 320 Gbit/s.
