Welcome to the first issue of JRPIT for 2008. It is an interesting time in Australia with a new Federal Government which is planning to begin implementing its Digital Education Revolution mid-year. Providing senior high school students access to laptops is a good initiative. Where is the accompanying strategy to train teachers how to take advantage of this? Let us hope that Australia will not repeat the mistake it made when, decades ago, language laboratories were widely introduced but there was no adequate training of teachers to use them properly.

The first paper in this issue is "An Investigation into Business-to-Business Electronic Commerce Organizations" by Chad Lin, Graham Pervan, Hsiu-Yuan Tsao and Koong H.-C. Lin. "The issue of information technology (IT) investment evaluation in B2BEC (business-to-business electronic commerce) has generated a lot of interest and discussion among academics and researchers. This research was undertaken to investigate the relationships between the level of IT maturity, the use of IT investment evaluation (IEM) and benefits realization (BRM) methodologies, and the degree of satisfaction with the adoption of B2BEC in Taiwanese B2BEC organizations. The results indicated that the level of IT maturity was a strong predictor of the use of evaluation methodologies while the use of evaluation methodologies had a significant impact on the degree of satisfaction with the adoption of B2BEC."

The next paper, "A Model for Investigating Software Accidents", was written by Tom McBride. "A software accident is an unforeseen outcome that arises from a failure of a software project or software product. Death, severe injury or severe financial loss, could arise from such a failure. This paper asserts that there is not yet a good accident investigation model with which to investigate software accidents. Accident models from other fields are examined to determine their suitability for use in the field of software development. Although many existing models are very useful, all assume that the environment of the accident was operational. That is, there is a steady state of operations during which events or failures produce an accident. Software development and software operations are very different circumstances. Additionally, none of the existing models makes use of the considerable body of knowledge about software development. For these reasons a new system theoretic model is proposed."

Following that is "Fast XML Structural Join Algorithms by Partitioning" by Nan Tang, Jeffrey Xu Yu, Kam-Fai Wong and Jianxin Li. "An XML structural join evaluates structural relationships (parent-child or ancestor-descendant) between XML elements. It serves as an important computation unit in XML pattern matching. Several classical structural join algorithms have been proposed such as Stack-tree join and XRTree join. In this paper, we answer the problem of structural join by partitioning." "Extensive experiments show that the performance of our proposed algorithms outperform that of Stack-tree and XR-Tree algorithms."

And the final paper in this issue is "Identity-Based Parallel Key-Insulated Signature: Framework and Construction" by Jian Weng, Shengli Liu Kefei Chen and Xiangxue Li. "To minimize the damage caused by key-exposure in ID-based signatures, in ISPEC'06 Zhou *et al* (2006) proposed an ID-based key-insulated signature (IBKIS) scheme. However, their scheme is not strong key-insulated, i.e, if a user's helper is compromised, the adversary can derive all of this user's secret keys for any time period. Moreover, in practice, to alleviate the damage in case of key-exposure, secret keys in IBKIS schemes have to be updated at very short intervals, which will increase the risk of helper key-exposure. It is important to note that even for an IBKIS scheme with strong key-insulated security, once a user's helper and one of his secret keys are both compromised, the adversary can also derive all of this user's secret keys for any time period. Is it possible to allow frequent key-updates without increasing the risk of helper key-exposure in IBKIS systems? In this paper, we extend Hanaoka *et al* (2006) parallel key-insulated mechanism to IDbased signature

scenarios, and present an ID-based parallel key-insulated signature (IBPKIS) scheme. Compared with Zhou *et al* (2006) IBKIS scheme, our scheme enjoys three attractive features: (i) it is strong key-insulated; (ii) it can allow frequent key updates without increasing the risk of helper key-exposure, and over all, enhances the security of the system; (iii) even if one of a user's helpers and some of his secret keys are both exposed, it is impossible for an adversary to derive all of this user's secret keys."

Professor Sidney A. Morris
Editor-in-Chief
University of Ballarat
http://uob-community.ballarat.edu.au/~smorris/