doi:10.1093/comjnl/bxr031

Capsule Reviews

FAIROUZ KAMAREDDINE

The Capsule Reviews are intended to provide a short succinct review of each paper in the issue in order to bring it to a wider readership. The Capsule Reviews were compiled by Fairouz Kamareddine. Professor Kamareddine is an Associate Editor of *The Computer Journal* and is based in the Department of Mathematical and Computer Sciences at Heriot-Watt University, Edinburgh, UK.

An Off-line Electronic Cash Scheme Based on Proxy Blind Signature. ZUOWEN TAN

This paper argues that off-line e-cash schemes are more efficient and practical than on-line e-cash schemes, however, they lead to double spending. Hence, the author advocates a secure off-line e-cash scheme which is unforgeable, anonymous and traceable and introduces an off-line electrical cash scheme based on a proxy blind scheme noting that a blind signature scheme for e-cash provides anonymity and has further advantages. After an introduction to the preliminaries and the assumed security notions, the author sets up his proxy blind signature scheme and shows that it satisfies the security properties of a proxy signature scheme. In particular, it is shown that the proposed proxy blind signature scheme satisfies correctness, unforgeability and unlinkability. Then, an off-line e-cash scheme based on the proxy blind signature scheme is constructed and it is shown that the e-cash scheme satisfies the security properties of unforgeability, anonymity and traceability.

Short Signatures with a Tighter Security Reduction Without Random Oracles. FUCHUN GUO, YI MU AND WILLY SUSILO

The authors state that proving security for short signatures in the standard model (without random oracles) is important for ensuring that these short signatures imply security in real-world applications. Recent work of Hofheinz and Kiltz (HK) in the literature gave a new short signature whose size is <320 bits with 80-bit security without random oracles and showed that the final signature length in the scheme can be as short as 230 bits in length. That earlier work leads to the question: 'how to construct a short signature scheme whose length is <320 bits with a tight security reduction without random oracles?'. This paper gives a 270-bit short signature scheme for 80-bit security with a much tighter security reduction (without using random oracles and with a loss of only log n bits) than that of HK, and shows how to shorten the signature length to 191 bits. The new short signature schemes are constructed using the HK signature scheme and a multi-generator hash function. First, the needed preliminaries and the new multi-generator hash function are introduced. This new hash function is shown to be provably collision resistant (like the hash function used in the HK signature scheme), but unlike that of the HK signature scheme, it can be used to program tight-reduction proofs. The new hash function is pairing based and the authors move to propose their pairing-based short signature scheme. On the basis of some assumptions, the authors show that the pairing-based short signature (of length 270 bits) is fully secure. Thereafter, the stateful short signature scheme is introduced and a short signature of length 191 bits is given and it is again shown to be fully secure in the presence of some assumptions. Furthermore, an RSA-based short signature scheme with a tight security reduction is given and a signature of size 1142 bits is shown to be fully secure under some assumptions. The various proposed short signature schemes are compared with the HK signature schemes and the so-called BB signature scheme.

Heterogeneous Signcryption with Key Privacy. QIONG HUANG, DUNCAN S. WONG AND GUOMIN YANG

Signcryption is a lower computational cost cryptographic operation than the traditional operations of signing and encrypting. However, existing signcryption are homogeneous in that they are either both public key based (where both the sender and receiver have public key pairs that are certified by a certification authority) or both identity based (where both the sender and the receiver use their identities which are issued by a key generation center as public keys). Homogeneous signcryption does not allow the sender and the receiver to use keys that are under different cryptographic settings. This paper proposes a heterogeneous signcryption where the sender can generate a ciphertext that the receiver can decrypt under a conventional private key and verify the recovered message and signature as if using an identity-based signature scheme. Three security models are given to capture confidentiality, unforgeability and key privacy. All these models are also shown to capture security. After introducing the related work, the authors introduce the heterogeneous signcryption scheme, which consists of six probabilistic polynomial time algorithms, define the three security models for capturing

confidentiality, unforgeability and key privacy (also called ciphertext anonymity), and explain how all these models support insider security. Two heterogeneous signcryption schemes are introduced and analyzed under the proposed security models. The second model is a modification of the first by replacing the bilinear pairing signature generation of the first model with a non-pairing-based identity-based signature generation algorithm. Performance studies are carried out from four points of view (key privacy, size, complexity and security) for both constructions as well as for other signcryption schemes in the literature providing good insight into the properties of these systems.

Information Security Risk Modeling Using Bayesian Index. CHIEN-LUNG CHAN

The paper starts by stating that not all enterprises can afford to implement International Organization for Standardization (ISO) or International Electrotechnical Commission (IEC) recommendations since not all information security (IS) personnel can master every aspect involved. This paper concentrates on the construction and evaluation of a Bayesian Index model for measuring the IS of an enterprise and giving a quantitative assessment of the IS risk of the enterprise. First, the Bayesian index is introduced and then the paper reports on its research method where an IS panel interviewed IS experts to identify IS risk factors/get consensus and then used the Bayesian index model to collect each expert's weighting for each risk factor. The IS risk assessment model is then constructed and evaluated with 41 companies. The results of this evaluation are given and discussed with respect to validity and reliability.

A Survey of Outlier Detection Methods in Network Anomaly Identification. PRASANTA GOGOI, D.K. BHATTACHARYYA, B. BORAH AND JUGAL K. KALITA

Outlier detection refers to finding patterns in data that are very different from the rest of the data. Anomaly detection is similar to finding outliers, specifically in network intrusion detection, and can detect new attacks that the system has never seen before as they cause deviation from normal behavior. This paper provides a comprehensive survey of outlier detection methods and approaches to network anomaly identification by using outlier detection methods. After an introduction to the needed preliminaries including distance-based outlier detection, density-based outlier detection and outlier detection based on soft computing approaches, and a brief comparison of outlier detection approaches, network anomaly detection is discussed. Thereafter, both the supervised and unsupervised approaches to outlier detection methodologies are introduced and existing outlier detection approaches for network anomaly detection are classified. Finally, research issues and challenges are presented.

Self-healing Key Distribution Schemes for Wireless Networks: A Survey. BIMING TIAN, SONG HAN, SAZIA PARVIN, JIANKUN HU AND SAJAL DAS

The target of key distribution is to establish and maintain secure channels between the group manager (GM) and multiple group users. Updating session keys is a necessity that has many complications. Self-healing key distribution for establishing keys over an unreliable network is an important technique for wireless security and efficiency. It enables group users to recover session keys by themselves, without requesting additional transmission from the GM even when they miss some broadcast messages. This reduces the network traffic, decreases the work load on the GM and lowers the risk of user exposure through traffic analysis. This paper highlights the features and performance/security attributes of self-healing key distribution schemes and discusses three ways to strengthen the robustness of self-healing key distribution schemes. After a review of the desirable features of self-healing key distribution schemes (forward and backward secrecy, collusion resistance, efficiency and scalability), a classification (unconditionally secure versus computationally secure) of self-healing key distribution schemes is given. Thereafter, the general model and the procedure of self-healing key distribution schemes are given. This is supplemented by an overview of typical self-healing key distribution schemes with an analysis and comparison on the performance of schemes in the same classification. Three considerations (sponsorization, mutual healing and authentication) are discussed which can be used to strengthen the robustness of the basic self-healing key distribution schemes. Finally, a compositive analysis on existing schemes is given and future directions are outlined.