Review of the book

"Practical Signcryption"

by Alexander W. Dent and Yuliang Zheng

Springer, 2010

ISBN: 978-3-540-89409-4

Amit K Awasthi
Gautam Buddha University, Gr Noida, India

1 Summary of the review

As the title says this book is about the signcryption. It begins from the root of the signcryption and covers the latest developments including details of security analysis. This book includes the story of the combination of the two primitives into one 'signcryption'. It covers various development phases of this primitive, which motivates researchers.

2 Summary of the book

The book is organized into thirteen chapters. It begins with historical developments of signcryption and describes how two of the most important functions of modern cryptography, data confidentiality and data integrity, were achieved by combining the two basic primitives encryption and digital signature simultaneously. This first introductory chapter covers the basic signcryption scheme, which was the first attempt to achieve this cost effective solution by Zhang, one of the editors of this book. This chapter also covers the initial attempts made towards security of signcryption.

After the introductory chapter, the rest of the book is divided into four parts: The first part deals with security models for signcryption and consists of two chapters. Chapter 2 provides a formal definition for the security of signcryption in two user setting and analysis of the security of signcryption schemes that are constructed by composing signature schemes in a public-key setting. Due to the asymmetry of the public-key setting, two types of security settings arise: insider and outsider security. This chapter covers both security settings in terms of both privacy and authenticity. Then this chapter discusses the security of signcryption in all the three possible cases: Encrypt-then-sign, encrypt-and-sign, sign-then-encrypt. The next chapter discusses the security settings in multi user settings.

Part II contains three chapters. This part is devoted to a few schemes, which are the turning points towards the extension of signcryption. Chapter 4 starts with the definitions of Diffie-Hellman Problems, and covers schemes that, similarly to the first signcryption scheme by Zhang, are based on it. This chapter also discusses the important modification that added the future of non-repudiation to signcryption. Further, a feature of publicly verifiability was added. This type of work opens the opportunity for new researchers to learn how they can think in directions of incremental research. This chapter covers schemes based on DSA and Schnorr's Scheme.

Chapter 5 covers some schemes based on bilinear maps. Here, some of the advantages of signcryption, such as cipher text anonymity and detachable signatures, are discussed, and a few examples of schemes that enjoy these properties are given. This chapter has a rigorous discussion over security of such schemes.

Chapter 6 reviews early attempts to construct a signcryption scheme based on RSA moduli and certain padding schemes.

The next part III is devoted to construction issues. Chapter 7 is on Hybrid signcryption and starts with a gentle introduction of hybrid cryptography. Following this, the adaption of hybrid encryption KEMs to outsider-secure signcryption is discussed and finally the use of tag-KEM is discussed to cover insider-secure hybrid signcryption. Various security analyses are very interesting and useful for researchers.

Chapter 8 discusses two main application of concealment to the area of authentication encryption.

Chapter 9 covers a very interesting work of parallel signcryption. Previously the two cryptographic operations signing and encrypting were taking place sequentially, now they are carried out in parallel, and this results into further gain in efficiency. This chapter closes with security analysis of the proposed technique.

Part IV, the last part, is devoted to the extension of signcryption and is comprised of three chapters. Chapter 10 describes identity-based signcryption, which takes advantage of identity-based cryptography, and a selection of ID based constructions is covered.

Chapter 11 is focusing on key agreement and key transportation protocols by using signcryption.

Chapter 12 finally discusses the issues regarding various applications of signcryption and shows a few examples of practical signcryption. It motivates to think further in new directions and to find the areas where signcryption may be useful.

3 What is the book like (style)?

The book covers many aspects around the primitive 'signcryption', which is a combination of two natural primitives 'signature' and 'encryption' to gain more efficiency. This includes achieving efficient constructions, assessing the security level, listing efficient schemes, applications and practical implementation issues. The book is comprised of chapters written by world-renowned cryptographers. It is able to serve as a handbook on signcryption and also motivates researchers, for it covers the historical events of how this primitive was born.

4 Would you recommend this book?

I would certainly recommend this book for an audience that is interested in secure communication where the cost of communication should be optimized. This book provides a good starting point for signcryption, regardless of the background of the reader: omputer science, mathematics, or any other discipline in which signcryption knowledge is required. This title is very useful for understanding signcryption, hence, it is not only a valuable source for researchers but also for practitioners who can benefit from this book as a reference.

The reviewer is an assistant professor of Mathematics at Department of Applied Science, Gautam Buddha University.