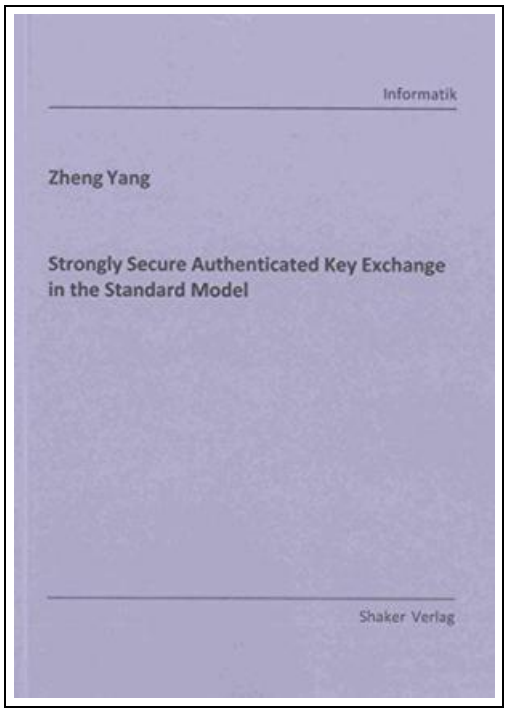
Strongly Secure Authenticated Key Exchange in the Standard Model



Filesize: 8.31 MB

Reviews

Complete guideline for publication lovers. it was writtern really properly and useful. Once you begin to read the book, it is extremely difficult to leave it before concluding.
(Treva Hamill)

STRONGLY SECURE AUTHENTICATED KEY EXCHANGE IN THE STANDARD MODEL

Shaker Verlag Sep 2013, 2013. Buch. Condition: Neu. Neuware - Nowadays many crucial network applications rely on the existence of a confidential channel established by authenticated key exchange (AKE) protocols over public networks. With the rapid development of cyber technology, novel attacks to cryptosystem emerge in an endless stream. This has also led to the development of AKE solutions to provide increasingly stronger security guarantees. In this thesis we focus on provision of practical constructions for AKE protocols which are provably secure in a strong sense without resorting to random oracles. We first we present three new efficient compilers to generically turn passively secure key exchange protocols (KE) into authenticated key exchange protocols (AKE) where security also holds in the presence of active adversaries. Our compilers are not only a useful tool for the design of new AKE systems with many additional security properties in a modular and less error-prone fashion, but they also help to relax the assumptions on existing, practical key exchange mechanisms which are not known to be provably secure AKE protocols. Security of our compilers is shown in a strong modified CK model where the adversary is allowed to reveal either long-term secret key or state information of the protocol participants. On the second, we study the open problem on constructing eCK secure two party AKE protocol without random oracles and NAXOS alike trick. A generic construction satisfying those requirements is given based on well-known cryptographic primitives following the guideline of efficiency. Then a concrete protocol is proposed which is the first eCK secure protocol in the standard model under both standard assumptions and post-specified peer setting (i.e. without knowing any cryptographic information about its communication peer). Both proposed schemes can be more efficiently implemented with secure device than previous works which are eCK secure in...

Other Books

31 Moralistic Motivational Bedtime Short Stories for Kids: 1 Story Daily on Bedtime for 30 Days Which Are Full of Morals, Motivations Inspirations

Createspace, United States, 2015. Paperback. Book Condition: New. 229 x 152 mm. Language: English . Brand New Book ***** Print on Demand *****.Reading to children is a wonderful activity and past time that both parents...

Read Book

»

Bringing Elizabeth Home: A Journey of Faith and Hope

BRILLIANCE AUDIO, United States, 2015. CD-Audio. Book Condition: New. Unabridged. 170 x 133 mm. Language: English . Brand New. At 3:58 in the morning of June 5, 2002, Ed and Lois Smart awoke to the...

Read Book

»

Walking

1st World Library, United States, 2004. Paperback. Book Condition: New. 208 x 134 mm. Language: English . Brand New Book ***** Print on Demand *****.Purchase one of 1st World Library s Classic Books and help...

Read Book

»

Oxford Reading Tree Read with Biff, Chip, and Kipper: Phonics: Level 5: Egg Fried Rice (Hardback)

Oxford University Press, United Kingdom, 2011. Hardback. Book Condition: New. 172 x 142 mm. Language: English . Brand New Book. Read With Biff, Chip and Kipper is the UK s best-selling home reading series. It...

Read Book

»

Oxford Reading Tree Read with Biff, Chip, and Kipper: Phonics: Level 5: Seasick (Hardback)

Oxford University Press, United Kingdom, 2011. Hardback. Book Condition: New. 174 x 142 mm. Language: English . Brand New Book. Read With Biff, Chip and Kipper is the UK s best-selling home reading series. It...

Read Book

»

Patent Ease: How to Write You Own Patent Application

Createspace, United States, 2014. Paperback. Book Condition: New. 229 x 152 mm. Language: English . Brand New Book ***** Print on Demand *****.Patent Ease! The new How to write your own Patent book for beginners!

Read ePub

»

DK Readers L2: Survivors: The Night the Titanic Sank

DK Publishing. Paperback / softback. Book Condition: new. BRAND NEW, DK Readers L2: Survivors: The Night the Titanic Sank, Caryn Jenner, Linda Martin, Will Tate and his family set sail for America. But they are

Read ePub

»

The Secret Life of Trees DK READERS

DK CHILDREN. Paperback. Book Condition: New. Paperback. 32 pages. Dimensions: 9.0in. x 6.0in. x 0.1in.This Level 2 book is perfect for children who are beginning to read alone. Why do trees lose their leaves in

Read ePub

»

The Tale of Jemima Puddle-Duck - Read it Yourself with Ladybird: Level 2

Penguin Books Ltd. Paperback. Book Condition: new. BRAND NEW, The Tale of Jemima Puddle-Duck - Read it Yourself with Ladybird: Level 2, This is a gentle adaptation of the classic tale by Beatrix Potter. Jemima

Read ePub

»

Damsels in Distress

Kensington Publishing, United States, 2016. Paperback. Book Condition: New. 170 x 104 mm. Language: English . Brand New Book. What happens when a fifteen-year-old secret between three best friends is exposed? Celeste Harper seems to

Read ePub

»