SPRINGER LINK Log in

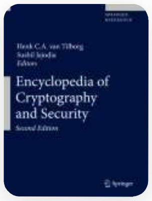
Menu Search Cart

Home > Encyclopedia of Cryptography and Security > Reference work entry

Chaum Blind Signature Scheme

| Reference work entry

| pp 199–200 | Cite this reference work entry



Encyclopedia of Cryptography and Security

Gerrit Bleumer

341 Accesses

Related Concepts

Blind Signature

Definition

The Chaum Blind Signature Scheme [3, 4], invented by David Chaum, was the first blind signature scheme proposed in the public literature.

Theory

The Chaum Blind Signature Scheme [3, 4] is based on the RSA signature scheme using the fact that RSA is an *automorphism* on $\mathbb{Z}_n{}^*$, the multiplicative group of units modulo an RSA integer $n = pq$, where *n* is the public modulus and *p*,*q* are safe RSA prime numbers. The tuple (n, e) is the public verifying key, where *e* is a prime between 2^{16} and $\phi(n) = (p-1)(q-1)$, and the tuple (p, q, d) is the corresponding private key of the signer, where $d = \mathrm{e}^{-1}\mathrm{mod}\phi(n)$ is the signing exponent. The signer computes signatures by raising the hash value $H(m)$ of a given message *m* to the *d*th power modulo *n*, where $H(\cdot)$ is a publicly known collision resistant hash function. A recipient verifies a signature *s* for message *m*with respect...

Recommended Reading

1. Bellare M, Namprempre C, Pointcheval D, Semanko M (2001) The one-more-RSA inversion problems and the security of Chaum's blind signature scheme. In: Syverson PF (ed) Financial cryptography 2001. Lecture notes in computer science, vol 2339. Springer, Berlin, pp 319–338

Chapter Google Scholar

2. Camenisch J, Piveteau J-M, Stadler M (1995) Blind signatures based on the discrete logarithm problem. In: De Santis A (ed) Advances in cryptology: EUROCRYPT'94. Lecture notes in computer science, vol 950. Springer, Berlin, pp 428–432

Google Scholar

3. Chaum D (1993) Blind signatures for untraceable payments. In: Chaum D, Rivest RL, Sherman AT (eds) Advances in cryptology: CRYPTO'82. Plenum, New York, pp 199–203

Google Scholar

4. Chaum D (1990) Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms. In: Seberry J, Pieprzyk J (eds)

Advances in cryptology: AUSCRYPT'90. Lecture notes in computer science, vol 453. Springer, Berlin, pp 246–264

Google Scholar

5. Chaum D, Pedersen TP (1993) Wallet databases with observers. In: Brickell EF (ed) Advances in cryptology: CRYPTO'92. Lecture notes in computer science, vol 740. Springer, Berlin, pp 89–105

Google Scholar

6. ElGamal T (1985) A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Info Theory 31(4):469–472. http://www.emis.de/MATH-item?0571.94014 http://www.ams.org/mathscinet-getitem?mr$=$798552

7. Horster P, Michels M, Petersen H (1994) Meta-message recovery and meta-blind signature schemes based on the discrete logarithm problem and their applications. In: Pieprzyk J, Safari-Naini R (eds) Advances in cryptography: ASIACRYPT'94. Lecture notes in computer science, vol 917. Springer, Berlin, pp 224–237

Google Scholar

8. National Institute of Standards and Technology (NIST) (1993) Digital signature standard. Federal Information Processing Standards Publication (FIPS PUB 186)

Google Scholar

9. Nyberg K, Rueppel R (1993) A new signature scheme based on the DSA giving message recovery. In: 1st ACM conference on computer and communications security, proceedings, Fairfax, November 1993. ACM, New York, pp 58–61

Chapter Google Scholar

10. Pointcheval D (1998) Strengthened security for blind signatures. In: Nyberg K (ed) Advances in cryptology: EUROCRYPT'98. Lecture notes in computer science, vol 1403. Springer, Berlin, pp 391–405

Google Scholar

11. Pointcheval D, Stern J (1996) Provably secure blind signature schemes. In: Kim K, Matsumoto T (eds) Advances in cryptography: ASIACRYPT'96. Lecture notes in computer science, vol 1163. Springer, Berlin, pp 252–265

Google Scholar

12. Schnorr C-P (1988) Efficient signature generation by smart cards. J Cryptol 4(3):161–174

MathSciNet Google Scholar

Author information

Authors and Affiliations

Research and Development, Francotyp Group, Triftweg 21-26, 16547, Birkenwerder bei Berlin, Germany

Gerrit Bleumer

Editor information

Editors and Affiliations

Department of Mathematics and Computing Science, Eindhoven University of Technology, 5600 MB, Eindhoven, The Netherlands

Henk C. A. van Tilborg

Center for Secure Information Systems, George Mason University, Fairfax, VA, 22030-4422, USA

Sushil Jajodia

Rights and permissions

Reprints and permissions

Copyright information

About this entry

Cite this entry

Bleumer, G. (2011). Chaum Blind Signature Scheme. In: van Tilborg, H.C.A., Jajodia, S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-5906-5_185

.RIS⤓ .ENW⤓ .BIB⤓

DOI
https://doi.org/10.1007/978-1-4419-5906-5_185

Publisher Name
Springer, Boston, MA

Print ISBN
978-1-4419-5905-8

Online ISBN
978-1-4419-5906-5

eBook Packages
Computer Science Reference Module
Computer Science and Engineering