Commitment Schemes

Leonhard Applis

***Abstract*—This Paper introduces to and summarizes the topic of Commitment-Schemes, a two party kryptographic protocoll.**

The aim of commitment schemes is to provide a mechanism for Party A to commit to a hidden value and reveal it if necessary. Party B can confirm that the revealed value and the hidden value match.

This Paper first introduces to the topic itself, a hash-based implementation and the *pedersen-commitments* which are based on the discrete logarithm. In Conclusion a Case-study of commitments for one-time authorization in a distributed web-application is provided.

I. Introduction

ToDo: IntroText // Motivation

A. Protocoll

B. Attributes

ToDo: Copy from Presentation but with sources

C. Additional Security-Measures

ToDo: Copy from Presentation (After Hash) but elaborate

II. Implementation

A. Hash-Based Commitments

ToDo: Hash-Based Commitments with sources

B. Pedersen Commitments

ToDo: Pedersen Commitments with sources

C. Quadratic-Residues

Iff i need more content

III. Case-Study: Migrating user privileges in web-applications

ToDo: Describe Web-Application, Requirements and the Solution

References

Please number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use "Ref. [3]" or "reference [3]" except at the beginning of a sentence: "Reference [3] was the first ..."

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors' names; do not use "et al.". Papers that have not been published, even if they have been submitted for publication, should be cited as "unpublished" [4]. Papers that have been accepted for publication should be cited as "in press" [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

References

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.