MTAT.07.006 Research Seminar in Cryptography
Comments on "Designated Verifier Signature Schemes"

Dan Bogdanov
db@math.ut.ee

October 9, 2005

1 Introduction

The aim of this document is to comment on the survey titled "Designated Verifier Signature Schemes"[4] by Liina Kamm. The survey describes some results on designated verifier signature schemes [DVS] published in [1], [2] and [3].

DVS schemes are used to construct proofs that can be validated by only these verifiers who are selected by the signer. The commented work is a survey meant to give and overview of the subject.

2 Structure and readibility

The survey is structured in a logical way, starting with the introduction and definitions for terms and continuing with covering topics from the articles. The articles are covered chronologically, starting with [1] and ending with [3].

The text is readable and doesn't contain any immediately visible errors. The text is overall a good reading.

3 Comments and questions

There is a number of terms which are referenced but not explained. Although some of these are standard cryptographic primitives and methods, they should be described in an entry-level survey.

The overview of DVS Security Notions (chapter 4) includes a description of *secure disavowability*. This description should be improved to explain the term of a simulated signature and the purpose of disavowability in general.

The non-delegatability definition contains the use of a *knowledge extractor*. A short description of a knowledge extractor would be very nice. Also, what are *proofs of knowledge* mentioned in the end of the definition for unforgeability?

In chapter 5 (The JSI Designated Verifier Signature Scheme) the formula $\Theta \bigvee \Phi_{Bob}$ should include some more information about the meaning of Θ and Φ_{Bob}. What is the letter ϑ in definition 5.1?

What are *confirmation schemes* mentioned in chapter 5.1 (Interactive Designated Verifier Proof of Undeniable Signatures).

Chapter 6 (The DVS Scheme with Tight Reduction to the Decisional Diffie-Hellman Problem in the Non-programmable Random Oracle) mentions the *Decisional Diffie-Hellman Problem* and *(Non-Programmable) Random Oracles*. An overview of these would improve understandability.

4 Conclusions

The presented material is a little hard to absorb for people with little background in cryptography. The math is readable, but not all of the used methods and primitives are fully explained. The missing explanations should be gathered in a separate chapter with a name like "Cryptographic Background".

Still, it is a good read if you are interested in the subject. With some more on explanations and definitions this work can be graded excellent.

References

[1] M. Jakobsson, K. Sako, R. Impagliazzo. Designated Verifier Proofs and Their Applications. Proc. Eurocrypt'96, p.143-154, Springer-Verlag, 1996.

[2] H. Lipmaa, G. Wang, F. Bao. Designate Verifier Signature Schemes: Attacks, New Security Notions and A New Construction. In Luis Caires, Guiseppe F. Italiano, Luis Monteiro, Catuscia Palamidessi and Moti Yung, editors, The 32nd International Colloquium on Automata, Languages and Programming, ICALP 2005, volume 3580 of Lecture Notes in Computer Science, p. 459-471, Lisboa, Portugal, July 11-15, 2005. Springer-Verlag.

[3] R. Zhang, J. Furukawa, H. Imai. Short Signature and Universal Designated Verifier Signature Without Random Oracles. Applied Cryptography and Network Security, Third International Conference, ANCS 2005, volume 3531 of Lecture Notes in Computer Science, p. 483-498, New York, June 7-10, 2005. Springer-Verlag.

[4] L. Kamm. MTAT.07.006 Research Seminar in Cryptography: Designated Verifier Signature Schemes. October 3, 2005