T-79.515 Cryptography: Special Topics / Pairing-based Crypthography: Comments on "Some ID-PKC signcryption schemes"

Sven Laur

April 6, 2003

1 Introduction

In this notes, we comment Lauri Tarkkala's survey [4] which examines ID-based signcryption schemes. Briefly, the signcryption schemes guarantee integrity and secrecy of a message with single operation which makes them more efficient compared with traditional techniques.

First the survey introduces Zheng protocol that is not an ID-based signcryption scheme. This example gives a nice intuitive understanding how the security goals are achieved. Next security model is formally defined. It is followed by description of Malone-Lee, Nalla-Reddy and Libert-Quisquater signcryption schemes. The last section contains discussion about security of the Libert-Quisquater scheme which clears the vagueness of the assumptions of Theorem 6.1.

The survey is well written and contains enough details. However, we correct some minor slips and suggest some additional changes.

2 More detailed comments

Section 2 (A simple example) The security requirements for the trusted party are a vague. Generally there is no need for secure party, since A and B can generate p, q and g according to DSA signature scheme. Moreover, according to [3, p. 454] the common public of parameter p, q and g do not compromise the security of A and B.

In the description of **Signcrypt** scheme A should choose x instead of r. The difference between signcryption and ordinary solutions would be more clear if some comparison data like tables from the original article [5] or other more up to date comparison would have been included.

Section 3 (Security model) As a minor detail that **Unsigncrypt**(φ, d_B, A) should return $\perp$ if φ is invalid cryptogram is missing, otherwise an adversary can be more powerful. Namely, the additional constraint prohibits chosen ciphertext attack with invalid messages.

I must agree with Lauri that the original definition of existential forgery is faulty in [1]. Note that in the second article [2] the error does not occur. The triple (φ', A, B) is ordered unnaturally, since it suggest that A sends a message to B which opposite to the actual meaning.

Section 4, 5 and 6 (pairing based signcryption schemes) As all three schemes have very similar structure it is worth considering describing them together. For example the **Setup** algorithm is almost identical and therefore is should have been described only once. And afterwards describe additional details depending on the scheme separately. And maybe even summarize the different aspects of the signcryption schemes in a table.

For consistency with general framework given in section 3 the **Keygen** algorithm should return only a private key.

It is worth mentioning that the Libert-Quisquater scheme has separated verification. Namely, every third party is able to check whether the message was sent by A or not. One possible application is identity based rooting where rooters can let through only authentic packages from fixed set of identities.

Also, a slight hint why these schemes are more efficient than sign-and-encrypt technique would have been enlightening.

Discussion of security assumptions Although it is true that a weak block-cipher E allows to bypass the DBDH problem, it does not compromise the security of secret keys, since the whole session key k can be revealed. In article [1] is even suggested that if the B wants to convince third party that the message m was signed by A, he should reveal the decryption-key k_2.

References

[1] Benoît Libert and Jean-Jacques Quisquater. New identity based signcryption schemes from pairings. Cryptology ePrint Archive, Report 2003/023, 2003. `http://eprint.iacr.org/`.

[2] John Malone-Lee. Identity-based signcryption. Cryptology ePrint Archive, Report 2002/098, 2002. `http://eprint.iacr.org/`.

[3] A. J. (Alfred J.) Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. The CRC Press series on discrete mathematics and its applications. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, 1997.

[4] Lauri Tarkkala. Some ID-PKC signcryption schemes. Survey for the seminar T-79.515 Cryptography: Special Topics / Pairing-based Crypthography at HUT, 25 March 2003.

[5] Yuliang Zheng. Digital signcryption or how to achieve cost (signature & encryption) << cost(signature) + cost(encryption). *Lecture Notes in Computer Science*, 1294:165–179, 1997.