Scientific Writing

Review

Christoph Wedenig (01560073)

May 2019

1 An O(ND) Difference Algorithm and Its Variations

Eugene W. Myers. An O(ND) difference algorithm and its variations. *Algorithmica*, 1(1-4):251–266, November 1986

2 How to Leak a Secret

Ronald L Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 552–565. Springer, 2001 Citations (according to Google Scholar): 1465

2.1 Summary

The paper "How to leak a secret" [RST01] indroduces the concept of a ring signature. This type of signature makes it possible to create a signature from a set of possible signers without their permission or coordination. Ring signatures do not give away which of the signers is the original author. This implies that if someone was to check the signature, the original author of the signature would stay anonymous while still proving that they had to be someone among the used signers.

2.2 Discussion

Motivation The authors motivate the importance of this algorithm by giving a usecase example that would not be possible without ring signatures: Leaking a secret from inside a specific group to a journalist while wishing to stay anonymous. With ring signatures, this is easy to accomplish, as using your private key as well as all the other group members public keys to sign the document proves that it came from inside the group while not giving away the identity of the person who actually leaked the document. This shows precicely where the results of the papers could be applied in the real world to improve whistleblower anonymity.

References

[Mye86] Eugene W. Myers. An O(ND) difference algorithm and its variations. *Algorithmica*, 1(1-4):251–266, November 1986.

[RST01] Ronald L Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 552–565. Springer, 2001.