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):251–266, Nov 1986

1.1 Summary

2 How to Leak a Secret

How to leak a secret. In Colin Boyd, editor, *Advances in Cryptology — ASIACRYPT 2001*, pages 552–565, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg

Citations (according to Google Scholar): 1465

2.1 Summary

The paper "How to leak a secret" [1] 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. The authors also show that it can replace a Message Authentication Code when two entities communicate and don't want the signature to act as proof. Using their algorithm insted removes the need to exchange keys by just signing with a ring signature with both keys from entity A and entity B.

Significance The authors motivate the significance of the presented algorithm by making and proving various claims about its properties: The algorithm runs in linear time in relation to the number of keys used which is feasable for most small to mid sized groups. It is therefore more efficient than various other previous attempts at ring signatures. The algorithm is also proven to be secure as long as the underlying key generation is ie. it does not contain vulnverabilities that could lead to an attacker finding the original signer of a ring signature without knowing their private key or having the signer himself expose this fact. These properties make this algorithm a ideal candiate for ring signatures.

Presentation, Reproducability and Correctness Even though I am no security expert, most of the paper is easy to follow. The author always argues with logic and adds mathematical proves when needed. The abstract is very well written and includes the most important bits of information in the paper without going into too much detail. The structure of the paper is very logical as well, after first explaining the concept, terminology and motivation, the paper shows how efficient the algorithm is and then follows up with a step by step guide on how to generate and validate a ring signature. This also makes it relatively easy to replicate as this pseudocode only needs to be translated in any programming language. Even better would be a an implementation in the appendix or similar. Finally it goes on to prove the security of the suggested algorthm and some special cases. This part is very detailed and formal and therefore makes the results a lot more trustworthy. The only thing i found lacking was the title, as it is a bit too general and doesn't tell enough about what the paper is about. The authors also included a paragraph about a fictional world as a usecase scenario where they stop using scientific lingo all together which feels a bit unprofessional. The references in the paper are from previous attempts at similar algorithms and cryptographic/mathematical building blocks that are used by this specific algorithm and its proofs. Some of them are also very famous papers in computer science which increases the reputability of this paper.

References

[1] How to leak a secret. In Colin Boyd, editor, *Advances in Cryptology — ASIACRYPT 2001*, pages 552–565, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

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