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

Citations (according to Google Scholar): 1063

1.1 Summary

The paper "An O(ND) Difference Algorithm and Its Variations" by Eugene W. Myers is about solving the shortest edit script problem by first showing that the problem is equivalent to finding the longest common subsequence of two sequences. The paper then presents an algorithm that can solve this problem and refines it further to improve time and space complexity.

1.2 Discussion

Motivation/Significance The author of the paper motivates the importance of the algorithm by pointing out that there has been an extensive amount of research put into the field of edit script generation. He claims algorithms that solve this problem have applications in many various domains and that they could all benefit from a sped up version of already existing solutions.

The title of the paper is very informative and to the point. The main point of the paper is the above-said algorithm and the title reflects that. The abstract is short and sums up the findings in the paper very well. Every chapter has one or two corresponding short sentences in the abstract, so nothing is missing.

The introduction presents the research background and lists a few previous solutions to the given problem and motivates the need for a faster algorithm. The author shortly goes over the selected approach and under which circumstances it falls short and finally presents their final solution to the problem. Every step towards the final algorithm is clearly described in a way that builds on knowledge previously explained in the paper. The whole paper gets very complicated in the end and to understand it, a reader without a strong background in this field probably needs to read it several times because lots of information is often hidden in a single sentence. All the properties of the edit graph are presented in lemmas and proven before they are included in the algorithm. These proves can be followed rather easily and doing so verifies the lemmas' correctness. The author smartly uses a graphical representation in two different stages of the algorithm and refers to the same figure multiple times in the paper. The figure itself is black and white and big enough to be readable without any zoom applied and is therefore readable digitally or in a printed form. Related work is a big part of an algorithm that should improve previous ones and the author always presents both improvements and shortcomings of his algorithm compared to other ones, which is very scientific. The author likes to include small examples throughout the paper to exemplify some of the parts of the algorithm which improves understandability. Most of the examples are unfortunately in the beginning and therefore the complex refinements that are explained at the end of the paper do not have these small bits of help for the reader. Writing style overall is very clear and concise.

1.3 Methods

The research method used are mostly observations that lead to a more optimized algorithm and/or a better worst time complexity. These observations are always accompanied by a formal proof. There is also one Probabilistic Analysis that observes the performance of the algorithm under a stochastic model to show that the average case performs better than the worst case. All in all research methods are very clean and every claim that is made is also validated.

1.4 Results

Significant results are scattered all over the chapters, which are then taken into account in the "A Linear Space Refinement" chapter to formalize the final algorithm. More optimzations are explored in the last chapter but are discarded because of signifcant memory consumption. The way the pseudocode is scattered around in different chapters is very confusing for readers trying to recreate the code in an actual programming language. For a reader it is also very hard to just consume the results of the paper. I would suggest moving some proofs to the appendix to improve readability.

2 How to Leak a Secret

Ronald L Rivest, Adi Shamir, and Yael Tauman. 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" [2] 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 who 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 it 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 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 from a member of the goup while not giving away the identity of the person who actually leaked the document. This shows precisely 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 do not 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 I.e. 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 an ideal candidate for ring signatures and proves its significance.

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. It can stand on its own and motivates the reader to continue reading. 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. It would be even better for there to be an actual implementation in the appendix or similar. Finally the author makes some generalizations and proves the security of the suggested algorthm in 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 does not tell the reader exactly what the paper is about. A title that includes the core concept and purpose would fit a lot better, like: "Ring Signatures - an anonymous way to leak secrets" 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.

2.3 Methods

The research method used here is primarily observations of properties of other algorithms that can be combined to form this new ring signature algorithm. Most of the observations are proven to be correct or declared as trivially true. A very good way of keeping my interest while reading was the way the author made every small thought in between results explicit and clear in the text. This made it a lot easier to follow.

2.4 Results

The results of this paper are two versions of the ring signature algorithm, with the difference being the public-key cryptosystem used, as well as the proof of security. Algorithmic results are presented in a visually distinct look and each line of pseudocode is accompanied by a sentence explaining what the line does and sometimes also why. This makes recreation of the algorithm very straight forward versus just putting some pseudocode and a block of text together.

References

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

[2] Ronald L Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In Colin Boyd, editor, *Advances in Cryptology — ASIACRYPT 2001*, pages 552–565, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.