Secure and Effective Methods for Increasing Citation Count

Alptekin Küpçü
Koç University, İstanbul, Turkey
akupcu@ku.edu.tr

Abstract

Academic research is mostly judged based on the citation count. This metric is defined to measure quality of research outputs, rather than quantity. The motivation is that the more citations an article receives, the more people regard it highly, and thus the higher its quality is.

Recent research uncovered that it is possible to game this system using self-citations. In this paper, we first present secure and effective methods to increase citation counts, and then provide performance evaluation of these methods based on Google Scholar citation numbers. We provide a comparative analysis of cryptography research citations, computer science citations, and zoology citations. We show that the best (most secure) method for increasing citations is being a self-citer in a prestigious and refereed journal, such as the Journal of Craptology. We demonstrate our findings in this paper.

Keywords: research quality metrics, citation count, self-citations, useless keywords.

1 Lorem Ipsum Dolor

Every successful research publication starts with an existing paper format. Nowadays, no researcher starts writing a LaTeX document from scratch. This encourages double- or multiple-publication of research results in various venues. University deans, presidents, and board members have realized this tendency, and hence replaced the quantity-based metric of "the number of publications" with a quality-based metric of "the number of citations".

Researchers, being the smartest guys on the planet, quickly learned how to game this new metric. Various strategies have been proposed in the literature. In this paper, we present both existing and novel techniques, and provide performance evaluation. In addition to providing evaluation of the effectiveness of these techniques, we also give a comparative analysis of current usage of these techniques in different disciplines such as cryptography, computer science, and zoology. We also pick the best (most secure) method and demonstrate it live in this paper.

Our contributions can be summarized as follows:

1. To the best of our knowledge, this is the first paper that demonstrates its best finding.
2. We provide a framework for analyzing security and effectiveness of methods for increasing citation count.
3. We provide a comparative analysis clearly showing differences between cryptography, and other areas of science.

The organization of this paper is as follows: It follows regular organization of millions of other research papers (cf. [14]). Starts with an introduction containing motivation, presents the methods, provides security proof which must exist in cryptography papers, and concludes after presenting evaluation results. As all real papers do, finishes with an acknowledgement and a comprehensive bibliography.

2 Methods

In this section we present secure and effective methods to increase citation count. This section only describes the methods. The next section provides their security proofs. The last section details performance evaluations and compares effectiveness of the methods.

2.1 Self-Citations

This is a very widely-known method among researchers. The goal of becoming a self-citer is the same as any other option for increasing citation count: getting promoted, obtaining increased salary, having tenure, having a nice big house and a happy family. The technique itself is complicated, and is worth explaining, though.

In this method, an author Alice[1] provides as many citations as possible to her previous papers. But, since many submissions are anonymous, there are multiple ways of achieving this, with different levels of security as explained in the next section.

In a non-anonymous submission, Alice can freely cite all her existing papers [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 16, 15, 17, 18, 19]. But, for anonymous submissions, the following strategies must be employed:

- It must be the case that not all previous papers of Alice has her as the first author. If that is the case, Alice can only cite as many of her own previous work as she cites someone else's previous work.
- If previous papers of Alice have different first authors, then she can freely cite more of those, as long as she abides by the above rule for the papers that have Alice as the first author. Since LaTeX sorts the references by the first author, a careless referee will not be able to de-anonymize Alice.
- In some cases, sorted bibliography reveals the author. A reviewer (who remains anonymous due to the laziness of the author) suggests that the Bibtex sorting method can be tweaked to make sure self citations are not apparent in anonymous submissions. Since Google Scholar citations can be manually fixed, it is even possible to *add randomly-generated fake authors* to some papers.
- If Alice wants to cite even more papers of her, going beyond the limits above, she must *wait patiently until her anonymous submission is accepted*, and then add many more self-citations before the camera-ready deadline. Since the peer review process has ended at that point, nothing can stop Alice from reaching her goal.

2.2 Citation Cliques

This is a more sophisticated version of self-citations. Here, the attacker author Alice colludes with other authors Charlie, David, and Eve. The larger the clique is, the better. Ideally, the clique should have about 26 authors, each of whose names starting with a different letter of the alphabet. As long as they are the first authors, it does not matter if they are the sole authors or not.

The idea is to form a clique, as in graphs. The authors are the vertices, and the edges between them represent citations. This is a directed graph where an edge from author A to author B denotes that a paper of A referred to a paper of B. The weight on such an edge represents the number of papers of B that are referred by various papers of A.

[1] For multi-author papers, any author can do this.

The reason that the large cliques are better is that finding large cliques is NP-Hard. As in everything in cryptology, our goal is to make the job of the good guys easy, and the bad guys hard. The bad guys here as possibly referees, deans, etc. To prevent authors from forming citation cliques, they need to find such large cliques in a graph where there is a vertex for each author in the world. Since this is an NP-Hard task, this will guarantee anonymity except with negligible probability of guessing.

2.3 Bribing

This is the most expensive attack of all. In this method, one needs a very talented personal financial advisor, a lot of luck, and a very good salary. Indeed, we prove in this paper that if this attack is to be successful at a large scale, no polynomial amount of salary will be enough. Therefore, we can classify this attack as requiring exponential resources.

The idea is to bribe a referee, or even better a dean, or maybe a university president. A referee may be bribed to accept your paper, and also reject papers who do not cite your paper. Even better, especially journal referees may force other papers to cite your paper. Therefore, they are a valuable resource, deserving a valuable payment.

Bribing deans and university presidents have more direct effects on your promotion and salary. Unfortunately, as we explained above, if you have enough resources to bribe them, then with high probability you do not need to bribe them. This is proven in detail in the next section.

3 Security Analysis

Theorem 3.1. *Self-Citation is secure under non-anonymous submission setting.*

Proof. The proof is *obvious*, and is thus skipped for the sake of space. □

Theorem 3.2. *Self-Citation is secure under anonymous submission setting.*

Proof. Using the rules provided, the proof is *obvious*, and is thus skipped for the sake of space. □

Theorem 3.3. *Citation-Cliques are secure assuming P != NP.*

Proof. If an attacker can recover a citation clique in polynomial time with only polynomially-many queries to the citation oracle, then we can construct a reduction that can solve the largest clique problem in polynomial time. This means that finding the largest clique is in P. Since this problem is known to be NP-Hard, then such a reduction would imply P = NP, contradicting our assumption. Note that this assumption is known to hold in the *generic group model*. □

Theorem 3.4. *Bribing is insecure assuming honest users exist.*

Proof. The proof is obvious based on the assumption. The issue is to prove that it is insecure with non-negligible probability. The proof is as follows: There are only polynomially-many persons in the World. By our assumption, at least one honest person exists. Each time a referee (or a dean, etc.) is assigned, there is a 1/poly chance that the honest person becomes your referee (or dean, etc.), in which case the attack succeeds. Therefore, with non-negligible probability bribing fails. □

4 Evaluation

The first subsection will provide a comparative analysis of the usage of the above methods in various disciplines, including cryptography [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16, 15, 17, 18, 19], computer science [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16, 15, 17, 18, 19], and zoology [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16, 15, 17, 18, 19]. The second subsection shows performance measurements, letting us conclude that the most secure and effective method of increasing citation counts is becoming a self-citer.

Comparative Analysis: Table 1 summarizes our results.

	Cryptography	**CS**	**Zoology**
avg num of citations	37	337	3.7
self-citer percentage	100	101	1
largest clique size	12	26	2
largest bribe amount $	11413	27534	24054

Table 1: Completely Real Statistics.

Effectiveness of Methods: Table 2 summarizes our results.

	Self-Citation	**Citation Cliques**	**Bribing**
security ($2^?$)	1024	780	-80
avg % increase in citations	500	160	-20
max % increase in citations	2^{32}	1600	-2^{64}
min % increase in citations	0	1	-20

Table 2: Completely Real Statistics.

Discussion: In cryptography, and computer theory in general, the author names in multi-author papers are ordered alphabetically according to the last names (with some exceptions, e.g. [18]). This led to a tendency of changing last names to ones that are lexicographically smaller. These mostly happen via marriages (e.g. [3]), but sometimes via using courts to change one's own last name.

Some reviewer feels that there is no treatment of the distribution of names on the probability of success, and its effects on Yuliang Zheng's career, the only author in IACR database whose family name starts with Z. We choose to let the reviewer enjoy that feeling, and leave it as future work. But we emphasize our deduction from the above example: **IACR needs more authors with last names starting with Z!**

5 Conclusion and Future Work

Our evaluation results prove that the most secure and effective method of increasing citation counts is becoming a self-citer. We have demonstrated this fact in our paper [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16, 15, 17, 18, 19].

As future work, we are planning to extend our findings with a novel method that **enables Alice to cite not only her previous work, but also her future work**.

ACKNOWLEDGEMENTS

This work is supported by Alptekin Küpçü. We thank Nigel Smart for his encouragement for the submission of this paper to the Journal of Craptology. We also thank anonymous reviewers who chose not to increase their citation count using this valuable resource. Everything written in this document is total crap.

References

[1] T. Acar, M. Belenkiy, and A. Küpçü. Single password authentication. *Computer Networks*, 2013.

[2] M. Belenkiy, T. Acar, H. N. J. Morales, and A. Kupcu. Securing passwords against dictionary attacks, Apr. 7 2010. US Patent App. 12/755,426.

[3] M. Belenkiy, M. Chase, C. C. Erway, J. Jannotti, A. Küpçü, and A. Lysyanskaya. Incentivizing outsourced computation. In *NetEcon*, 2008.

[4] M. Belenkiy, M. Chase, C. C. Erway, J. Jannotti, A. Küpçü, A. Lysyanskaya, and E. Rachlin. Making p2p accountable without losing privacy. In *ACM WPES*, 2007.

[5] D. Cash, A. Küpçü, and D. Wichs. Dynamic proofs of retrievability via oblivious ram. *EUROCRYPT*, 2013.

[6] S. E. Cebeci, A. Küpçü, and Ö. Özkasap. Secure peer-to-peer health-sharing. In *National Medical Informatics Conference*, 2011.

[7] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia. Dynamic provable data possession. In *ACM CCS*, pages 213–222. ACM, 2009.

[8] M. Etemad and A. Küpçü. Transparent, distributed, and replicated dynamic provable data possession. In *ACNS*, 2013.

[9] A. Kachkeev, E. Esiner, A. Küpçü, and Ö. Özkasap. Energy efficiency in secure and dynamic cloud storage. In *EE-LSDS*, 2013.

[10] A. Küpçü. Secmece: optimizing lifetime of federated sensor networks by exploiting data and model redundancy. 2007.

[11] A. Kupcu. *Efficient Cryptography for the Next Generation Secure Cloud*. PhD thesis, BROWN UNIVERSITY, 2010.

[12] A. Küpçü. *Efficient Cryptography for the Next Generation Secure Cloud: Protocols, Proofs, and Implementation*. Lambert Academic Publishing, 2010.

[13] A. Küpçü. Official arbitration and its application to secure cloud storage. *Cryptology ePrint Archive, report*, 2012/276.

[14] A. Küpçü. Secure and effective methods for increasing citation count. *Journal of Craptology*, to appear.

[15] A. Küpçü and A. Lysyanskaya. Optimistic fair exchange with multiple arbiters. In *ESORICS*, 2010.

[16] A. Küpçü and A. Lysyanskaya. Usable optimistic fair exchange. In *CT-RSA*, 2010.

[17] A. Küpçü and A. Lysyanskaya. Usable optimistic fair exchange. *Computer Networks*, 56(1):50–63, 2012.

[18] S. Meiklejohn, C. C. Erway, A. Küpçü, T. Hinkle, and A. Lysyanskaya. Zkpdl: a language-based system for efficient zero-knowledge proofs and electronic cash. In *USENIX Security*, 2010.

[19] R. TAMASSIA, C. PAPAMANTHOU, C. ERWAY, and A. KUPCU. Apparatus, methods, and computer program products providing dynamic provable data possession, Jan. 29 2010. WO Patent 2,010,011,342.