A Method for Obtaining Digital Signatures and More Citations

Christian Cachin, Ronald Rivest, Leonard Adleman, and Bart Preneel*

The authors are fake, so the employers can't be blamed

Abstract. While the world has seen many proposals for digital signatures in the decades since they were first proposed, some have proved to be more heavily cited than others. The RSA paper is an example of a paper that exhibits both positive and negative attributes in the search for a high H-factor.

Keywords: Mordell-Weil Groups · Machine Learning · Blockchain

1 Background

In the search for academic fame, authors have several options available to them. The primary currency of academic fame is of course citations to their papers. The more citations, the better. Some notably well-respected papers are listed in Table 1.

In the years since the original proposal of Rivest, Shamir and Adleman, the RSA algorithm has stood the test of time. This is in spite of the fact that there has never been a convincing argument for security that didn't depend on the utter ignorance of mathematicians. The scheme is now so well known that every undergraduate with an oscilliscope or an extra desktop computer has tried to attack it, so it must have done something right. This reinforces the fact that a paper with a good idea will gather many citations. At the same time, we believe that the RSA authors overlooked one factor in their search for academic fame.

A paper may gather citations for at least three reasons:

1. it's a truly great paper. OK it's possible but rare.
2. it impresses readers when they think you actually read the paper, because it's impossibly complicated. For this reason we often like to cite [W] and [TW] because it makes us look smart.
3. the paper has some *other* reason to attract attention.

We have no way to determine the reason why a paper gathers many citations, but we believe that the there is in fact a strong third reason that is unexploited.

* This paper was written under pseudonyms in order to enhance citations. The author pseudonyms were chosen in a way to describe this paper when it is cited.

Table 1. Citation counts for famous crypto papers

Authors	Year	Citations
Rivest, Shamir, Adleman	1978	22,918
Diffie-Hellman	1976	22,255
El Gamal	1984	10,821
Kocher, Jaffe, Jun	1999	8,814
Boneh-Franklin	2001	9799

2 A new approach to gather more citations

We hypothesize that a paper will gather more citations if doing so encourages people to pay attention. In the field of computer science, a paper is often cited by an acronym formed from the first initials of last names of authors. Thus when someone cites [RSA], the choice of a bibliography style will determine whether it appears with a numeric index into the bibliography, or possibly another string like `Rivest, et. al 78`.

In recent years we have noticed that many presentations use an acronym formed from the first initial of lastname of the authors. This leads us to hypothesize that a paper will gather more citations if it has a pronouncable acronym generated from the first letters of the last name of the authors. The appeal of the citation may in fact depend on the attractiveness or novelty of the acronym formed from the first letters of last name of authors. As an example, we believe that the RSA paper would have gathered more citations if the authors had appeared in alphabetical order. People would have enjoyed saying it and would have been anxious to cite it. The security community of the world wide web missed a similar opportunity when HTTP was being enhanced with encryption. At the time there were two competing proposals called HTTPS and S-HTTP. As it turns out, HTTPS was a better design for security, but the community would have been able to enjoy laughs for decades if URLs had been pronounced starting `shit-pee-colon-slash-slash-www...`.

There are a number of examples of papers that have fortuitous combinations of authors, but they sometimes miss the mark in various ways.

[FGMO] would have been more impressive if the authors were out of alphabetical order. We believe that Ostrovsky and Maurer should have held out for OMFG.

[MOM] should have more citations than expected. Who doesn't like their mom? Evidently Morita, Ohta, and Miyaguchi knew this when they became coauthors.

[STU] and [STU2] would have benefitted from having Amos Fiat or Matt Franklin as coauthors in appropriate priority, particularly if they had shifted the topic to denial of service attacks.

3 Choice of coauthors

The cases of the previous section indicate that authors should take care in their choice of coauthors if they want to benefit from a good acronym. It should also be obvious that nobody wants to be a coauthor with Aaron Aardvark, because they are destined not to be listed as a first author. We therefore advise that researchers should keep their eye out for convenient combinations of coauthor names, and adjust their collaborations to exploit this.

One classic case of a fortuitous combination is provided by section 1 of [WTF] This paper has received many more citations than it should have, because of the amusing part of section 1 where they cite another paper. We believe that upon meeting, the authors Cox and Zucker should have recognized that they should work together on a publication about a device.

While it might seem attractive to choose a large number of coauthors, and arrange the priority of authors in order to produce a good acronym. Unfortunately, there is a declining return on this approach, because authors who insist on a particular priority of authors may end up with something like [CDLLMMRAGGLMMMPPZ].

It is not only important to choose your coauthors carefully, but also to adhere to thematic consistency on the topic. Thus for example, the authors of the paper [SIFT] should have chosen to work on number field sieve instead of identity-based cryptosystems. Moreover, the authors of [POLLS] should have written their paper on elections. Similarly, [AES], [AES2], and [DES] should have been written about block ciphers. The paper [AMP] should have been written on the topic of differential power analysis.

Sometimes a paper can leave a bad impression from reading it, but it may also warn against reading the paper if the authors are not chosen carefully. We believe this may have affected [OOF], [DIM], and [FLOP]. One might expect the contribution of [NIT] to be a small one. The impact from [SHITY] might also be underestimated from the acronym.

Sometimes the choice of authors can result in an unfortunate suggestion that someone else wrote the paper. For example, it would be a fallacy to believe that Joppe Bos wrote the paper [BOS], but someone listening to a talk that cites the paper might naturally assume this is the case. The same goes for [ADI] and [CHOR].

Another example of a successful example is [HOT], because it sounds like it was written in a hot field, and you might be compelled to read it. Another example is [GLOW], because it sounds like it has an aura around it.

References

ADI. Jithra Adikari, Vassil Dimitrov, and Laurent Imbert. Hybrid binary-ternary joint sparse form and its application in elliptic curve cryptography, 2008. jithra.adikari@atips.ca 14063 received 25 Jun 2008, last revised 3 Jul 2008.

AES. Frederik Armknecht, Carsten Elsner, and Martin Schmidt. Using the inhomogeneous simultaneous approximation problem for cryptographic design, 2010. mschmidt@ifam.uni-hannover.de 14749 received 20 May 2010.

AES2. Gorka Irazoqui Apecechea, Thomas Eisenbarth, and Berk Sunar. Systematic reverse engineering of cache slice selection in intel processors. *IACR Cryptology ePrint Archive*, 2015:690, 2015.

AMP. Jean-Philippe Aumasson, Willi Meier, and Raphael C.-W. Phan. The hash function family lake. In *Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers*, volume 5086 of *Lecture Notes in Computer Science*, pages 36–53. Springer, 2008.

CHOR. Christina Boura, Virginie Lallemand, María Naya-Plasencia, and Valentin Suder. Making the impossible possible. *J. Cryptology*, 31:101–133, 2018.

BOS. Johannes Blömer, Martin Otto, and Jean-Pierre Seifert. Sign change fault attacks on elliptic curve cryptosystems, 2004. martinmo@upb.de 12672 received 8 Sep 2004, last revised 11 Sep 2004.

CDLLMMRAGGLMMMPPZ. Stefania Cavallar, Bruce Dodson, Arjen K. Lenstra, Walter M. Lioen, Peter L. Montgomery, Brian Murphy, Herman te Riele, Karen Aardal, Jeff Gilchrist, Gérard Guillerm, Paul C. Leyland, Joël Marchand, François Morain, Alec Muffett, Chris Putnam, Craig Putnam, and Paul Zimmermann. Factorization of a 512-bit rsa modulus. In *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, volume 1807 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2000.

DES. Paolo D'Arco, Navid Nasr Esfahani, and Douglas R. Stinson. All or nothing at all. *IACR Cryptology ePrint Archive*, 2015:998, 2015.

DIM. V. S. Dimitrov, L. Imbert, and P. K. Mishra. Fast elliptic curve point multiplication using double-base chains, 2005. Laurent.Imbert@lirmm.fr 12844 received 1 Mar 2005, last revised 2 Mar 2005.

FGMO. Matthias Fitzi, Juan A. Garay, Ueli Maurer, and Rafail Ostrovsky. Minimal complete primitives for secure multi-party computation. In *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*, pages 80–100. Springer, 2001.

FLOP. Tore Kasper Frederiksen, Yehuda Lindell, Valery Osheter, and Benny Pinkas. Fast distributed rsa key generation for semi-honest and malicious adversaries. In *Advances in Cryptology – CRYPTO 2018*, volume 10992 of *Lecture Notes in Computer Science*, pages 331–361. Springer, 2018.

GLOW. Michael Gerbush, Allison B. Lewko, Adam O'Neill, and Brent Waters. Dual form signatures: An approach for proving security from static assumptions. In *ASIACRYPT*, volume 7658, pages 25–42. Springer, 2012.

NIT. Juan A. Garay, Philip D. MacKenzie, and Ke Yang. Strengthening zero-knowledge protocols using signatures. *J. Cryptology*, 19:169–209, 2006.

HOT. Ryotaro Hayashi, Tatsuaki Okamoto, and Keisuke Tanaka. An rsa family of trap-door permutations with a common domain and its applications. In *Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 291–304. Springer, 2004.

MOM. Hikaru Morita, Kazuo Ohta, and Shoji Miyaguchi. A switching closure test to analyze cryptosystems. In *Advances in Cryptology - CRYPTO '91, 11th*

Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings, volume 576 of *Lecture Notes in Computer Science*, pages 183–193. Springer, 1991.

OOF. Kazuo Ohta, Tatsuaki Okamoto, and Atsushi Fujioka. Secure bit commitment function against divertibility. In *Advances in Cryptology - EUROCRYPT '92, Workshop on the Theory and Application of of Cryptographic Techniques, Balatonfüred, Hungary, May 24-28, 1992, Proceedings*, volume 658 of *Lecture Notes in Computer Science*, pages 324–340. Springer, 1992.

POLLS. Young-Ho Park, Sangho Oh, Sangjin Lee, Jongin Lim, and Maenghee Sung. An improved method of multiplication on certain elliptic curves. In *Public Key Cryptography - PKC 2003, 6th International Workshop on Theory and Practice in Public Key Cryptography, Miami, FL, USA, January 6-8, 2003, Proceedings*, volume 2274 of *Lecture Notes in Computer Science*, pages 310–322. Springer, 2002.

RSA. R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

WTF. Charles F. Schwartz. A mordell-weil group of rank 8, and a subgroup of finite index. *Nagoya Math Journal*, 93:19–26, 1984.

SHITY. Yumi Sakemi, Goichiro Hanaoka, Tetsuya Izu, Masahiko Takenaka, and Masaya Yasuda. Solving a discrete logarithm problem with auxiliary input on a 160-bit elliptic curve. In *Public Key Cryptography - PKC 2012*, volume 7293 of *Lecture Notes in Computer Science*, pages 595–608. Springer, 2012.

SIFT. S. Shinozaki, Toshiya Itoh, Atsushi Fujioka, and Shigeo Tsujii. Provably secure key-updating schemes in identity-based systems. In *Advances in Cryptology - EUROCRYPT '90, Workshop on the Theory and Application of of Cryptographic Techniques, Aarhus, Denmark, May 21-24, 1990, Proceedings*, volume 473 of *Lecture Notes in Computer Science*, pages 16–30. Springer, 1990.

STU2. Claudio Soriente, Gene Tsudik, and Ersin Uzun. Beda: Button-enabled device pairing, 2007. euzun@ics.uci.edu 13683 received 19 Jun 2007.

STU. Claudio Soriente, Gene Tsudik, and Ersin Uzun. Hapadep: Human asisted pure audio device pairing, 2007. euzun@ics.uci.edu 13584 received 12 Mar 2007.

TW. Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain hecke algebras. *Ann. of Math*, 141:553–572, 1995.

W. Andrew John Wiles. Modular elliptic curves and fermat's last theorem, 1995.