Scientific Writing

Nilanjan Datta

Institute for Advancing Intelligence

tcg crest

Inventing Harmonious Future

Necessity of Good Writing

Necessity of Good Writing

- Wider dissemination of the results.
- Helps in the review process.
- Creates a Good reputation in the community.
- Depicts your thinking capability.

Necessity of Good Writing

Strong Result

Bad Writing

Steps of Good Writing

Macro-Level Discussions

- Organisation of the paper.
- General Issues of presentability.

Steps of Good Writing

Macro-Level Discussions

- Organisation of the paper.
- General Issues of presentability.

Micro-Level Discussions

- Stylistic Issues.
- Examples of Good and Bad Writing,

Steps of Good Writing

Macro-Level Discussions (Today's class)

- Organisation of the paper.
- General Issues of presentability.

Micro-Level Discussions

- Stylistic Issues.
- Examples of Good and Bad Writing,

Organisation of a Paper

1. Title
2. Authors
3. Abstract
4. Key words
5. Introduction
6. Preliminaries / Definition / Notation
7. Technical Content
8. Conclusion
9. Acknowledgements
10. References
11. Appendices

Order of Preparation

1. Title and Authors (Initial)
2. Preliminaries / Definition / Notation
3. Technical Contents including Appendices
4. Conclusion

Order of Preparation

1. Title and Authors (Initial)
2. Preliminaries / Definition / Notation
3. Technical Contents including Appendices
4. Conclusion
5. Introduction
6. Abstract, Key words

Order of Preparation

1. Title and Authors (Initial)
2. Preliminaries / Definition / Notation
3. Technical Contents including Appendices
4. Conclusion
5. Introduction
6. Abstract, Key words
7. References
8. Title and Authors (Final)
9. Acknowledgements

Title

Avik Chakraborti, **Nilanjan Datta**, Ashwin Jha, Cuauhtemoc Mancillas-López, Mridul Nandi, Yu Sasaki:
Elastic-Tweak: A Framework for Short Tweak Tweakable Block Cipher. INDOCRYPT 2021: 114-137

Nilanjan Datta, Avijit Dutta, Kushankur Dutta:
Improved Security Bound of (E/D)WCDM. IACR Trans. Symmetric Cryptol. 2021(4): **138-176** (2021)

Avijit Dutta, Ashwin Jha, Mridul Nandi:
A New Look at Counters: Don't Run Like Marathon in a Hundred Meter Race. IEEE Trans. Computers 66(11): 1851-1864 (2017)

Sayandeep Saha, Arnab Bag, Dirmanto Jap, **Debdeep Mukhopadhyay**, Shivam Bhasin:
Divided We Stand, United We Fall: Security Analysis of Some SCA+SIFA Countermeasures Against SCA-Enhanced Fault Template Attacks. ASIACRYPT (2) 2021: 62-94

Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, **Axel Poschmann**, Matthew J. B. Robshaw, Yannick Seurin, C. Vikkelsoe:
PRESENT: An Ultra-Lightweight Block Cipher. CHES 2007: 450-466

Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, Yosuke Todo:
GIFT: A Small Present - Towards Reaching the Limit of Lightweight Encryption. CHES 2017: 321-345

Avik Chakraborti, Tetsu Iwata, Kazuhiko Minematsu, Mridul Nandi:
Blockcipher-Based Authenticated Encryption: How Small Can We Go? CHES 2017: **277-298**

Avik Chakraborti, **Nilanjan Datta**, Ashwin Jha, Snehal Mitragotri, Mridul Nandi:
From Combined to Hybrid: Making Feedback-based AE even Smaller. IACR Trans. Symmetric Cryptol. 2020(S1): **417-445 (2020)**

Title

- Summarizes the main idea of your work.
- Part of your paper that is read first and read the most.
- Fewest possible words that adequately describe the purpose.
- Consider it as the abstract of your abstract.
- Start with an working title, finalize carefully at the end.

Choosing the Title

Do's (✓)

- Indicate accurately the subject and scope of the study.
- Make it attractive (may be framed as question).
- Limited to 8-12 substantive words.

Choosing the Title

Do's (✓)

- Indicate accurately the subject and scope of the study.
- Make it attractive (may be framed as question).
- Limited to 8-12 substantive words.

Don'ts (×)

- Make it too generalized.
- Suggest things not covered.
- Use abbreviation.

Authors

Nilanjan Datta[1], Avijit Dutta[2(✉)], Mridul Nandi[2], and Kan Yasuda[3]

[1] Indian Institute of Technology, Kharagpur, Kharagpur, India
nilanjan_isi_jrf@yahoo.com
[2] Indian Statistical Institute, Kolkata, India
avirocks.dutta13@gmail.com, mridul.nandi@gmail.com
[3] NTT Secure Platform Laboratories, NTT Corporation, Tokyo, Japan
yasuda.kan@lab.ntt.co.jp

Who are the Authors?

- At a broad level, authorship is linked to intellectual contribution:
  - Experimental design.
  - Analysis of the data.
  - Suggesting the idea.
  - Obtaining funding. (Is it really an intellectual contribution..??)

Who are the Authors?

- At a broad level, authorship is linked to intellectual contribution:
  - Experimental design.
  - Analysis of the data.
  - Suggesting the idea.
  - Obtaining funding. (Is it really an intellectual contribution..??)
- Ideally, Authorship implies non-trivial technical contribution.
- Not necessarily true everywhere
  - Guest Author: official supervisor may become a default author.
  - Ghost Author: Person with substantial contribution but not listed as an author.

Ordering of Authors

- Ordering is typically done in one of the two following ways:
  - Hardy-Littlewood principle (alphabetic according to surname).
  - Contribution-based ordering.
- Might vary depending on subjects:
  - Biologists tend to place a supervisor or lab head last in an author list.
  - Organic chemists might put them first.

Acknowledgement

Acknowledgments

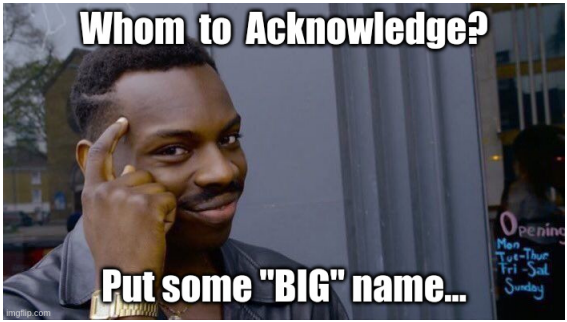
The authors would like to thank Dr. Nicky Mouha for his insightful comments and suggestions in preparing the final draft. We would also like to thank all the anonymous reviewers of ToSC 2019 for their valuable comments. Nilanjan Datta, Ashwin Jha and Mridul Nandi are supported by the project "Study and Analysis of IoT Security" under Government of India at R.C.Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata.

Acknowledgement

Way of giving credits to someone who has helped in preparing the paper.

- Anonymous reviewer(s) whose comments/suggestions might have helped you.
- May include projects and/or funding agencies.
- Not a mandatory field and may be added after acceptance (maintain anonymity).

Acknowledgement



Not a good idea..!!

Key Words

Keywords: authenticated encryption · release of unverified plaintext · AERUP · generalization · SUNDAE · ANYDAE · MONDAE · TUESDAE

Key Words

Main Purpose

- Helps in assigning the paper to the proper reviewer(s).
- Searches on the key word will return the paper.

Two Parts

- First part may have to be chosen from one or more lists provided by the journal or the conference.
- The second part will be specific to the paper.

Preliminaries

2 Preliminaries

SYMBOLS AND NOTATIONS. For a set $\mathcal{X}$, $X \leftarrow_{\$} \mathcal{X}$ denotes that X is sampled uniformly at random from $\mathcal{X}$ and independent to all random variables defined so far. $\{0,1\}^n$ denotes the set of all binary strings of length n. The set of all functions from $\mathcal{X}$ to $\mathcal{Y}$ is denoted as $\mathsf{Func}(\mathcal{X}, \mathcal{Y})$ and the set of all permutations over $\mathcal{X}$ is denoted as $\mathsf{Perm}(\mathcal{X})$. $\mathsf{Func}_{\mathcal{X}}$ denotes the set of all functions from $\mathcal{X}$ to

Preliminaries

- Start with the basic definitions and terminologies required to express the results.
- It is useful to draw up a list of notation before starting the technical description.
- If there is a new notion involved, precisely write down the formal/precise/rigorous definition of that notion before using it anywhere else.

Preliminaries: Do's and Don'ts

Do's (✓)

- Follow standard notations.
- Explain any new notion in plain English and illustrate by examples.
- Write in your own words.

Preliminaries: Do's and Don'ts

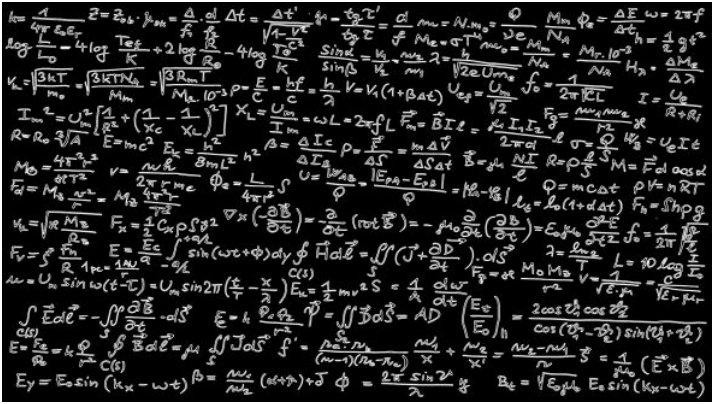
Do's (✓)

- Follow standard notations.
- Explain any new notion in plain English and illustrate by examples.
- Write in your own words.

Don'ts (×)

- Use the same symbol to denote two different things.
- Use two different symbols to denote the same thing.
- Keep unnecessary definitions and/or notations.
- Use too many symbols and over explain standard definitions.

Technical Content



Technical Contents (Mathematical Paper)

Contains one or more of the following

- Mathematical Results (Theorems).
- Algorithms.
- Comparison to previous work.

Natural Division of the paper into sections

- Subsections help in further structuring of the description.
- If a section becomes too long, divide it into multiple sections.

Naming Mathematical Results

Theorem

The main important results in the context of the work.

Lemma

Small results which lead up to a theorem: key step in the proof of several theorems.

Proposition

A stand-alone result which is perhaps not important enough to be called a theorem. The Nomenclature of proposition is not always very clear.

Naming Mathematical Results

Corollary

A direct consequence of a theorem (and sometimes also of a lemma).

- May be of more specific interest.
- Sometimes a corollary arises out of a side-effect of the technique used to prove the theorem.
- Sometimes corollaries are used in the subsequent work.

Presentation of Theorems

- Explain the motivation for the result before stating the result.
- If the theorem statement is complicated, then explain the different components before getting into the proof.
- If the theorem has interesting consequences, then mention some of them before getting into the proof.
- This will convince a reader that the theorem and its proof is worth reading.

Presentation of Theorems: Proof Structure

- Breaks into smaller results (lemmas).
- This helps in verifying and maintaining the proof.
- The lemmas could come earlier or later.
- Provide an overall description (intuition) of the proof strategy before getting into the details of the proof.

Algorithms

- Description.
- Correctness.
- Complexity (time, space, randomness).
- Results of running the algorithm (if applicable).
- Comparison with other algorithms (Theoretical and/or Practical).

Algorithm Description (Formal)

- Clearly state the data structures before the algorithm description.
- Divide into sub-routines.
- Provide concrete formal description of each sub-routine.

Algorithm Description (Informal)

- Provide a matching textual description, and aim for clarity.
- Explain the role played by each data structure.
- Describe in plain language the non-trivial core of the algorithm.
- You can mention optimisation tricks in the text.

Correctness of the Algorithm

- Proof of Termination.
- Proof that the algorithm perfroms the intended task.
- If non-trivial, state these as theorems.

Complexity

- Depending on your algorithm, these may need rigourous proofs.
- Asymptotics may be used depending on the context.
- However, for some applications, the constants do matter.

Results

- Depicts that the algorithm is implementable.
- Use tables and/or graphs as required.
- Highlight the novel features of your algorithm: efficient on larger inputs etc.

Comparison to Previous Algorithms

- Use tables and/or graphical comparison.
- The comparison could be theoretical (like counting multiplications) or experimental (like reporting time in seconds).
- Mention the hardware and software platform used for comparison.

Comparison to Previous Works

An Improved Algorithm

- Faster/ smaller memory / smaller code size / lesser randomness, ...
- Comparison may be theoretical and/or experimental.

Comparison to Previous Works

An Improved Algorithm

- Faster/ smaller memory / smaller code size / lesser randomness, ...
- Comparison may be theoretical and/or experimental.

An Improved Theorem

- Previous results follow as special cases.
- Previous results with weaker assumptions, and hence wider applicability.

Comparison to Previous Works

An Improved Proof

- A new technique is used.
- The technique applies to other situations.
- The proof is simpler.
- The proof is more elegant.

Comparison to Previous Works

An Improved Proof

- A new technique is used.
- The technique applies to other situations.
- The proof is simpler.
- The proof is more elegant.

Increased Practicability

- Provide a real-life scenario which your work covers but is not covered by previous work.

Comparison to Previous Works

Technical Contents (General Scientific Paper)

Contents

- Methods.
- Results.
- Discussions.

Methods

- Describe all experimental procedures, including controls concretely.
- Provide complete description to enable someone else to re-create the work.
- Explain why each procedure was done.
- Use proper citations, if required.

Results

- All results should be presented (including those that do not support the hypothesis).
- Tables, figures and graphs should be used effectively.
- Statements made in the text must be supported by the results contained in figures and tables.

Discussions

- The relationship between the results and the original hypothesis.
- An integration of the results with those of previous studies in order to arrive at explanations for the observed phenomena.
- Possible explanations for unexpected results and observations.
- Comparison with previous works.
- Propose specific further study.

Appendices

A Advantages of the distinguishers based on parity sets

In order to estimate the advantages of the distinguishers exhibited in this paper, we need to evaluate the probability that, given an input set X, a randomly chosen permutation π is such that $\pi(X)$ does not satisfy the division property of order 2. For the weaker distinguisher, we similarly need to evaluate the probability that a given u does not belong to $\mathcal{U}(\pi(X))$. Clearly, the probability that $\pi(X)$ satisfies the division property of order 2 (i.e., is balanced) is close to 2^{-n}, while the probability that a given u does not belong $\mathcal{U}(\pi(X))$ is close to $1/2$. However,

Appendices

- Results which chronologically belong somewhere in the text, but, placing it there will interrupt the smooth reading of the paper.
- An alternate proof illustrating some other aspects.
- A simpler but less efficient algorithm.
- Quick review of basic background material which may not be familiar to the readers in the area.

Introduction

1 Introduction

Authenticated encryption schemes, which target both data confidentiality and integrity simultaneously, have received considerable attention over the last years. The increased interest is in part due to the ongoing CAESAR competition [CAE14], which aims to deliver a portfolio of state-of-the-art authenticated encryption schemes covering a spectrum of security and efficiency trade-offs.

Whereas the security of conventional authenticated encryption schemes, such as OCB1-3 [RBBK01, Rog04, KR11] and GCM [MV04], breaks down if a nonce is used twice, new schemes offer varying degrees of robustness when nonces are reused [FFL12, ABL+13, RS06, HRRV15]. Albeit different levels of confidentiality in the nonce misuse setting may be

Introduction

- Start broadly and then narrow down to set the context.
- Provide proper motivation.
- State all the relevant related results with proper citations.
- State your contributions convincingly:
  - Do not be shy
  - Do not oversell
- Show, don't tell and keep it short.

Introduction: Challenges

Notational Challenge

- Without some notation you cannot proceed.
- Using too much notation will make the description dense at the beginning itself.

Introduction: Challenges

Notational Challenge

- Without some notation you cannot proceed.
- Using too much notation will make the description dense at the beginning itself.

Defining New Terminologies

- You need to define a few terms to get started.
- Putting a formal and precise definition at the start will scare readers.

Introduction: Challenges

Your Contribution

- Try to state your contributions as soon as possible (remember reviewers may not be patient souls..!!)
- Without stating some necessary background work you cannot place the results in the proper context.

Introduction: Challenges

Your Contribution

- Try to state your contributions as soon as possible (remember reviewers may not be patient souls..!!)
- Without stating some necessary background work you cannot place the results in the proper context.

Details of Experimental Results

- You should be providing tabular/graphical comparison.
- You cannot provide too much details.

Introduction: Challenges

Introduction: Meeting the Challenges

- There is no definite prescription for achieving the above balance.
- Requires time, patience, effort (in thinking and writing and re-writing) and experience.
- This could vary depending on the submission venue.
- Consciously read papers written by others watching for both flaws and good features.

Abstract

- The abstract is the first thing that a reader will read.
- In many cases searches also return the abstract along with the title.
- Abstracts are short and sometimes have word limits.
- It is a place to state your contributions and explicitly mention the significance of the work.
- Avoid trying to motivate the problem in the abstract.
- In a condensed form, the challenges in writing the introduction are also present for writing the abstract.

Conclusion

- A casual reader will often move to the conclusion right after the abstract.
- State limitations of the work and possible ways of overcoming them.
- State possible open problems, future research directions.
- Conclusion should not be a re-statement of the abstract.

Conclusion

Without a conclusion the ending of the paper becomes abrupt.

References

References

1. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404 (2013). http://eprint.iacr.org/2013/404
2. Beierle, C., et al.: The `SKINNY` family of block ciphers and its low-latency variant `MANTIS`. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part II. LNCS, vol. 9815, pp. 123–153. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53008-5_5
3. Bellare, M., Impagliazzo, R.: A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion. Cryptology ePrint Archive, Report 1999/024 (1999). http://eprint.iacr.org/

References

- BibTeX allows one to generate and format a bibliography automatically in a LaTeX document.
- One should carefully cite all the necessary references (specially the recent ones).
- Unnecessary self-citation should be avoided.
- Do not cite unpublished works, personal communications, .

Preparation of A Paper

- May take quite some time (goes through several revisions).
- The addition of new material may be accumulative.
- Be critical of your own writing.
- Provide reasonable time gaps between successive readings.
- Obtain feedback from colleagues.

Conference Papers

- A conference is a competition: can accept only a certain number of papers.
- Something new on a topic of current interest is likely to attract attention.
- Reviewers may be less concerned about the long term value of the idea.
- A generalisation, even if non-trivial, may not be of interest to a conference.
- A topic/result that will appeal to a larger group will be preferred.

Conference Papers: Things to Remember

Limited space

- Do not cut down on the abstract and the references.
- Do not cut down on the motivation and your contributions.
- You have to clearly explain the ideas behind a proof or an algorithm.
- Detailed technical material may be put in an appendix (if allowed), or may have to be omitted.

Conference Papers: Things to Remember

Limited Time

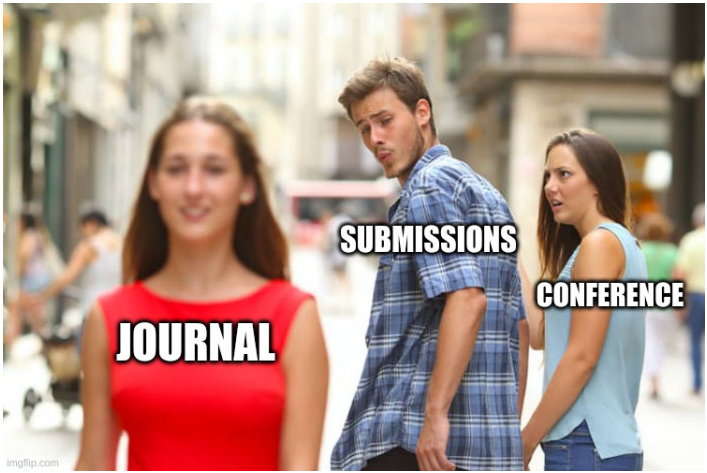
- Have a definite submission deadline.
- Unless you start early, it will be difficult to write properly.

Limited Reviewer Time

- A reviewer has a deadline within which to give decisions on several papers.
- A reviewer has to quickly decide whether the paper is interesting enough.

Journal Papers: Things to Remember

- Free of Submission deadline.
- Reviewers have sufficient time.


SUBMISSIONS
CONFERENCE
JOURNAL
imgflip.com


Waiting for my Journal review
imgflip.com

Journal Papers: Things to Remember

- Free of Submission deadline.
- Reviewers have sufficient time.
- Review turnaround time may be long.
- A rejection after a long delay may adversely affect thesis.

Summary

- Importance of Good Writing.
- Paper Organisation.
- General Guidelines to Follow.
- Conference and Journal Papers.

References

- P. Sarkar, *A Course on Research Methodology*, 2011. https://www.isical.ac.in/~palash/research-methodology.html

Thank You..!!!