How to Write Papers

May 2020

Marc Fischlin

The Roadmap

Topic / Idea

Results

You are here!

Paper

But it‘s useful to first look at this!

Publication

Rule of Thumbs

„Persuade the lazy reader.“

Rule #1

Assume as little as possible from reader,
both in terms of knowledge and comprehension.

- also holds for reviewer, but the reviewer should also be a bit impressed / need not understand everything
- do not assume knowledge of all previous works
- avoid terms like „left as an easy exercise for reader“ for non-trivial statements

Example Implication from Rule #1

Our scheme works essentially as the one in [16].

vs.

Our solution is based on the scheme by Goldreich et al. [16]. There, the signing algorithm… Here, …

Rule #2

KISS: Keep it short and simple
(as long as semantically equivalent).

- short sentences, avoid redundancy
- but don‘t make it hardly readable, Cristina
- use active tense instead of passive tense
- formulate positively

Example Implications from Rule #2

…where A is a new variable, initially set to the value 1.

vs

…where A is a new variable, initialized to 1.

The program was run on a …

vs

We ran the program on a …

Our results do not allow to make any claim…

vs

Our results hold for…

Rule #3

Avoid ambuiguities
(especially for mathematical objects).

- what you mean when writing can be different from what reader thinks when parsing text

Example Implications from Rule #3

The compiler did not accept the program because it contained errors.

vs

The program did not compile because it contained errors.

Unforgeability means that no efficient algorithm can forge signatures.

vs

‹Description through Experiment›

Rule #4

Use self-explanatory notations.

- use common notation in the community, eg., KeyGen or Kgen for key generating algorithm
- only change notation from previous paper if really necessary
- use good names like isCorrupt$\in${0,1} instead of $\beta \in$ {0,1}
- use implicit reminder for common notation instead of explicit definition

Example Implications from Rule #4

Let ‹a,b› be the inner product of vectors a and b. …(3 pages)… Next compute ‹a,b›.

vs

Next compute the inner product ‹a,b› of the vectors a and b.

Rule #5

Claims are supported by arguments.

- as usual in science

Example Implications from Rule #5

According to the public opinion, politicians are overpaid.

vs

According to a recent study by BBC [15] among 1000 British citizens, the majority of the interviewees agreed that politicians are overpaid.

Rule #0 (Marketing)

Presentation is „positively sincere“.

- note that „positive“ is adverb here, „sincere“ is adjective
- focus still on honesty, do not claim more than there really is
- but present it in a positive way

Example Implications from Rule #0

Our result holds for a limited class of functions.

vs

Our result holds for a qualified class of functions.

Exaguration

Content:
costs money if
monthly income too low

Presentation:
... you profit…
…only…
…all advantages…

Examples of Positively Sincere Presentation

(assuming this ↓ is true)

Our solution is a combination of known results and the proof therefore straightforward.	vs	While our solution is based on common techniques, we give the first formal security proof in a profound attack model.
Our result does not work in the case that....	vs	Our result covers the most common scenarios like… but is not known to hold for the case where…
Our solution is inferior to the previous result by XY in most settings.	vs	Our solution is especially suited for … whereas for other cases the protocol by XY performs better.

Example

(1) too many adjectives (at security conference it's usually clear what a key is)

(2) assumes that reader knows „the" (exact) properties

(3) doesn't say anything about what it is!!!

(4) logical order: there's missing something… and, btw, it should matter to you

Abstract—Key exchange protocols allow two parties at remote locations to compute a shared secret cryptographic key. While the secrecy and authentication requirements for such protocols have been studied extensively the key confirmation property has been treated rather informally so far, despite many widely deployed protocols and standards naming key confirmation as a major design goal.

In this work, we pro

(1)

(2) reader may not know it, but understands that they're standard (and work goes beyond standard)

(3) informal explanation of main property/topic (must always be there!!!)

Abstract—**Key exchange protocols allow two parties at remote locations to compute a shared secret key. The common security notions for such protocols are secrecy and authenticity, but many widely deployed protocols and standards name another property, called key confirmation, as a major design goal. This property should guarantee that a party in the key exchange protocol is assured that another party also holds the shared key. Remarkably, while secrecy and authenticity definitions have been studied extensively, key confirmation has been treated rather informally so far.**

(4) reverse order: This is important…and disturbingly there's a gap

Quiz (I)

<some algorithm in which G_L,G_R, and G_K appear>

Figure 3.5: As building blocks we assume a PRG. For the meaning of the symbols G_L,G_R, G_K see Construction 5.

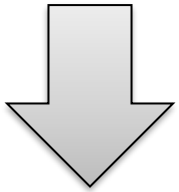
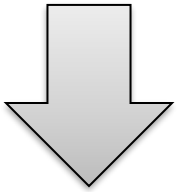


Figure 3.5: As a building block we use a PRG G where G_L,G_R, and G_K correspond to the output partition $G(x)= G_L(x) \| G_R(x) \| G_K(x)$ as in Construction 5.

Quiz (II)

Lemma 7 shows …. Lemma 8 establishes an important relation between the sets of sending actions that ‚eventually reach' a participant, and those that ‚directly reach' the participant. Finally, in Lemma 9…



…Lemma 8 establishes an important relation between the sets of sending actions that ‚eventually reach' a participant, and those that ‚directly reach' the participant. It proves that…

Structuring

Paper Structure

- Title + Abstract (+ Keywords)
- Section: Introduction
- Section: Preliminaries
- Section: Main Result #1
- Section: Main Result #2
- …

This is the (only) marketing section!

Seems clear doesn‘t it?

Feels strange if there‘s no Section 4, usually contains applications of main result

Introduction

- the most important part (after the results)
- reviewer‘s decision often made after introduction ?
- no general rule on how to write a good intro

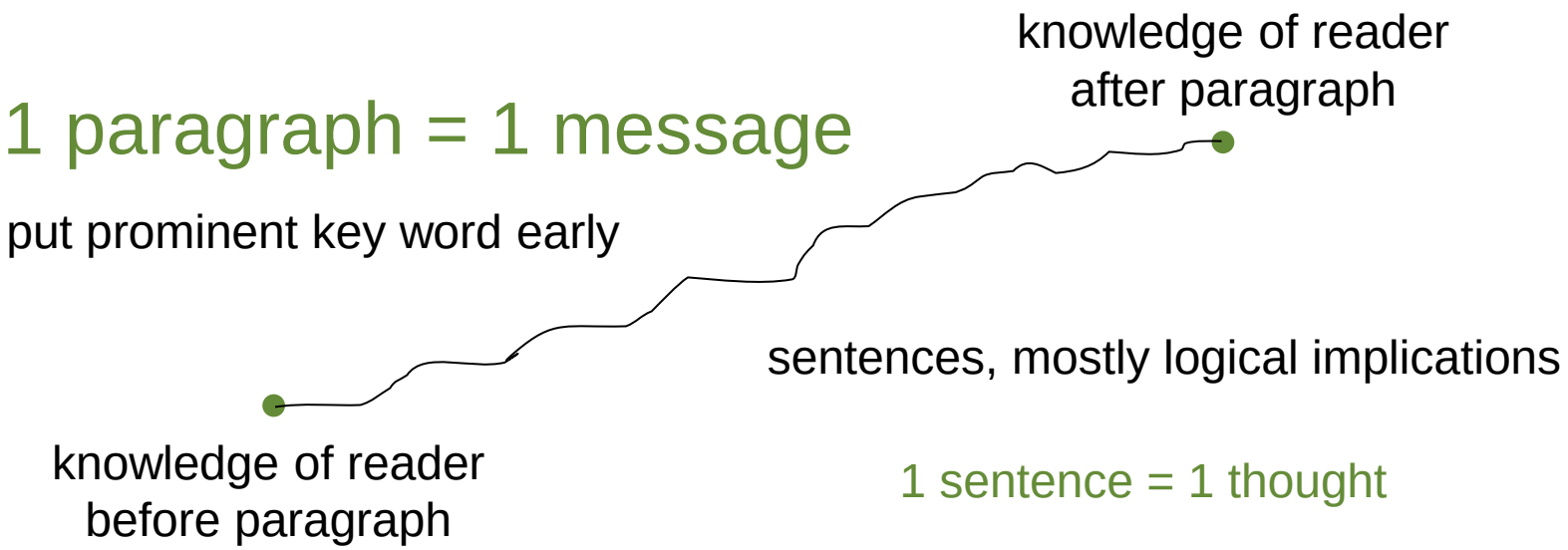
  first previous results (historic development) or „related work“ later?
- help reader to evaluate the importance of the paper

Introduction

- order depends on topic
  - context, our results, related work, or
  - previous work, our results
- should there be
  - details about the results?
  - an „organization“ part?
- It‘s more about getting the main thread and then…

Writing Paragraphs

New paragraph serves as mental break,
i.e., paragraph somewhat closed in itself



Example

knowledge before: reader superficially familiar with Dittmann definition
knowledge after: reader should understand that definition insufficient
(and that having “right” definition important)

“This definition of Dittmann et al. does not guarantee security in all possible scenarios. We show an attack against their scheme and their definition.”

cannot use demonstrative pronoun at beginning of paragraph

“A security definition per se cannot be wrong. However, a definition and in particular the underlying attack model may not capture all real-life threats. Consider for example [short example]. Then the model of Dittman et al. does not cover such attacks. In fact, we show that their scheme, while satisfying their definition, can be broken easily with such an advanced attack.”

What should go to the Preliminaries?

- Example: paper about blind signatures and
  new blind signature protocol using Encryption&Commitments

- Option #1:
  Define Enc+Com in Preliminaries 2.1, blind signatures in 2.2

- Option #2 (which I prefer):
  Define blind signatures in 2, and Enc+Com in Section 3.1
  when presenting protocol

define it close to where it‘s needed
(cf. Inner product example)

Technical Sections

- for very complicated results: think about first (or just) presenting a simpler version („vanilla model“)

inductive approach (often easier to grasp)
vs.
deductive approach (often easier to transfer)

more important during review phase

- don‘t move all proofs to appendix for submission, leave at least proof sketch

Separation of Duties

Algorithms, Constructions, Reductions,…

Intuition (explain)

„The idea of the reduction is …“

Description (define)

„The reduction receives pk and…“

(complicated definitions may contain further explanations)

$\mathsf{P}_{\text{par-OR}}(1^\lambda; (x_0, x_1), (b, w))$:

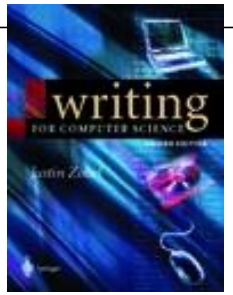
11: $\mathsf{com}_b \leftarrow_s \mathsf{P}_b(1^\lambda; x_b, w)$
12: $\mathsf{ch}_{1-b} \leftarrow_s \{0,1\}^{\ell(\lambda)}$
13: $(\mathsf{com}_{1-b}, \mathsf{resp}_{1-b}, \mathsf{ch}_{1-b}) \leftarrow_s \mathsf{S}_{1-b}(1^\lambda; x_{1-b}, \mathsf{ch}_{1-b})$
14: **return** $(\mathsf{com}_0, \mathsf{com}_1)$

Analysis (prove)

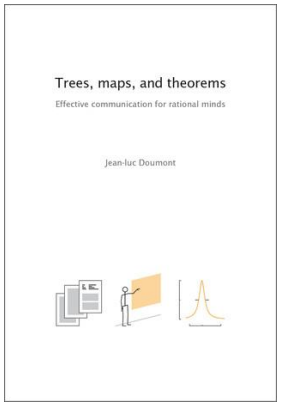
„The reduction succeeds with probability…“

Literature

- Writing for Computer Science
  Justin Zobel
  2nd Edition, Springer-Verlag, 2004



- Trees, maps, and theorems
  Jean-Luc Doumont
  Principiae, 2009



- Advice on Research and Writing
  Mark Leone
  Collection of Links to this topic
  www.cs.cmu.edu/afs/cs.cmu.edu/user/mleone/web/how-to.html