卧村密碼学報
Journal of WoCrypt
www.uow.edu.au/~fuchun/jow
办好卧报 龙场悟道

Volume: 2023 (51)

How to Understand “Research Gap” [*]

Fuchun Guo, Willy Susilo

University of Wollongong, Australia
{*fuchun, wsusilo*}@*uow.edu.au*

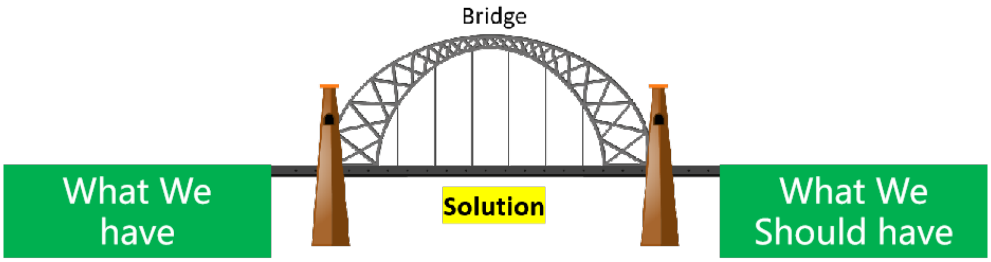
Abstract

If you have proposed a new scheme (protocol) but have no idea how to sell it, you should read this article.

1 Introduction

When doing cryptography research, you might come out with a new but strange scheme (protocol) for an old or new cryptographic notion like what Fuchun often did during his PhD study. If you have no idea how to sell this kind of research outcome, it means that you don’t really understand what the research gap is.

We are not to give a formal definition for this notion but explain it using the following picture, which matches the contributions for proposing novel schemes (protocols). This picture first time appeared in Fuchun’s little head when he prepared the lecture slides for “CSCI368/968: Advanced Network Security” delivered at CCNU and SIM in July of 2023. This picture was given to explain the reasons for having many different protocols, such as SSH, TLS, and IPSec.



The research gap, in the above picture, can be seen as the gap between “What We Have” and “What We Should Have”. Due to the existence of this gap, we aim to build a solution called *bridge*, such that we can eventually achieve “What We Should Have” from “What We Have”.

[*] We came out this topic when supervising our postdoc during a regular meeting.

2 Research Gap

“What We Have” and “What We Should Have” are further explained as follows.

- *What We Have:* Something we have already in the literature, such as proposed foundations (e.g. groups, lattice, hardness assumption) and proposed schemes (e.g. BLS signature scheme, RSA scheme).
- *What We Should Have:* Something we don’t have yet, including foundations and schemes with specific properties.

Therefore, a specific research gap is decided by the specific “What We Should Have”. Now, it is time to introduce how to sell a proposed scheme (protocol). This is what we are going to share with you.

■ **First, we should clearly state What We Should Have in the paper.** This is to clarify what we are researching. Otherwise, reviewers don’t know what we have contributed. For example,

- We need a scheme with X property for the cryptographic notion N, or
- We need a new cryptographic notion N (and also a scheme instantiation).

■ **Second, we should clearly state why What We Should Have is important in the paper.** This is to clarify the importance of our research. In the literature, the most interesting way is providing a reasonably imaginable application scenario that could happen in the future. The first actress and first actor are always our superstars Alice and Bob. Of cause, there are some other non-personal entities like cloud servers.

■ **Third, we should clearly state our contributions related to What We Should Have.** This is to clarify the specific results that we have produced. For example,

- We need a scheme with a very short signature size, but how short are the signatures in our proposed scheme? We must introduce this in the contribution part.
- We need a new cryptographic notion N, but how the notion is defined? We must introduce the composed algorithms and security definition in this notion.

■ **Lastly, if possible, we must explain why achieving What We Should Have is not easy.** This is to clarify the novelty of our research outcome because we have filled a research gap that is difficult to fill. We can do any research including crap research as long as we are happy, but top conferences only accept papers with high quality due to the contributions of novelty. Here, we would like to highlight something.

- Some research gap looks interesting and important but are easy to fill. Taking the BLS signature scheme as an example. It is important to have signatures as short as possible (What We Should We). The BLS signatures have 160 bits for 80-bit security (What We Have). Let $H(m)^{\alpha} = \sigma_m = b_1 b_2 \cdots b_{150} b_{151} b_{151} \cdots b_{160}$ be the signature represented with

160 number of bits b_i. We can create a new signature scheme by cutting the last 10 bits off and setting the new signature to be $\sigma'_m = b_1 b_2 \cdots b_{150}$, which has 150 bits and is shorter than the BLS signature. The new signature can still pass verification by doing as follows.

  - Set B=0000000000
  - Verify whether $\sigma'_m || B$ is a valid signature of m.
  - If yes, return true. Othewise, set B:= B+1 and go to the second step until B=1111111111.
  - Return false if B=1111111111.

- It will be great if we can have this, but explaining difficulty is optional because pointing out the reason may be rather challenging. If we cannot do this, we should be able to somehow convince reviewers that the new scheme is not trivially modified from **What We Have**. We can show those new tricks that have been invented in our scheme construction or security proof. It is worth noting that some solutions could be surprisingly simple, but the naughty alien is stopping us from finding them.

3 Conclusion

People understand the contributions (or benefits) inside a new scheme with the help of the research gap, which should be illustrated in the paper by the authors who proposed the new scheme. All the above related to **What We Should Have** must be organized in very nice logical storytelling. If this part cannot pleasure reviewers, they will displeasure us and decide to give us some blood-red color to see see.

Early Reject

================================END================================