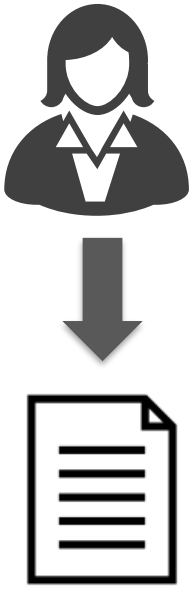
How to Review Papers

WESP Seminar WS 20/21

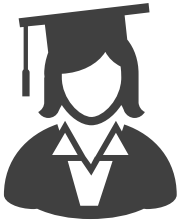
Marc Fischlin

Responsibility of Reviewer

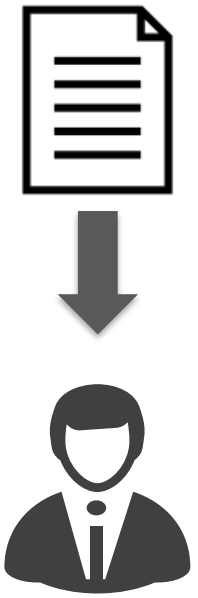
towards authors



towards editor/program chair



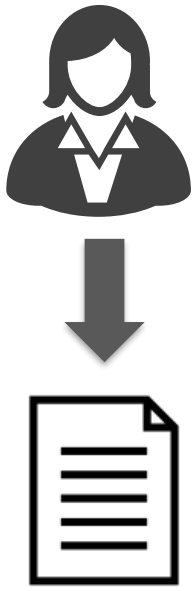
towards readers



based on Council of Science Editors, Reviewer Roles and Responsibilities

Responsibility of Reviewer

towards authors



provide unbiased and constructive feedback

indicate clarity, accuracy, originality, interest

avoid personal comments or criticsm

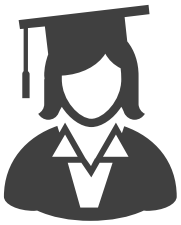
maintain confidentiality

Responsibility of Reviewer

provide thoughtful, fair, constructive critique

determine merit, originality, improvements

notify about ethical concerns



towards editor/program chair

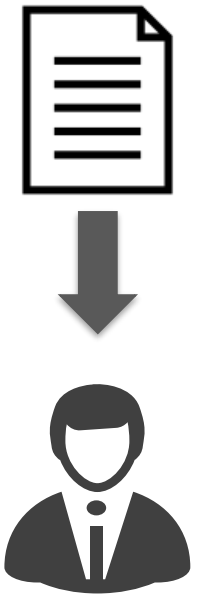
Responsibility of Reviewer

ensure readability

support replication

allow to judge merits and originality

towards readers



Content

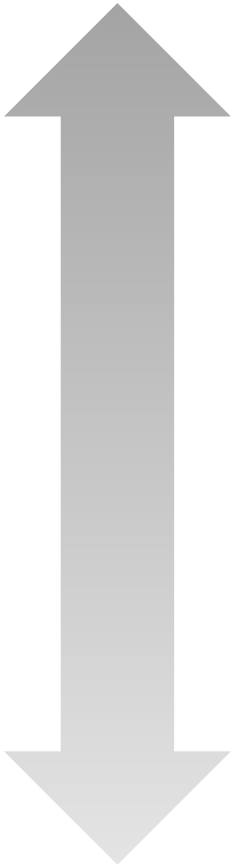
Content of Reviews

„objective“ criteria

Originality and Correctness

Editorial Quality

Scientific Quality
(impact & contribution)



„subjective“ criteria

Example

Structure: Summary – Good – Bad – Other Comments

AUTHOR-COMMENTS:
The paper proposes an authenticated key exchange protocol based on KEMs, with small communication costs and a tight security reduction to multi-receiver non-committing encryption schemes. The paper discusses that the latter can be based on hash proofs systems and the DDH assumption in the random oracle model.

***What's good about the paper:**
Provides a tightly secure key exchange protocol with session state reveals, improving over the efficiency of previous constructions. At first glance, it also seems to have a nice idea how to deal with session state reveal, basically encrypting the state with ephemeral randomness and a key put into the long-term secret. At first I was a bit worried that they would only do a single TEST query in the security model but they actually achieve security against multiple queries. The construction of the non-committing key encapsulation may be useful elsewhere.
…

Example

Structure: Summary – Good – Bad – Other Comments

…

***What's less good:**

If one thinks about the solution a bit longer, the conceptually novelty in deriving tightly secure schemes is not a big leap step: The NCKE seems to follow the idea in [GJ14] of using a random oracle commitment over the DH part to be able to adapt the value later, and generalizes this idea. But this is still a decent contribution. The state encryption has appeared in previous works, but usually less explicitly and in different forms. The construction resolves some issues by 'delegating' them to the random oracle model.

***Soundness and presentation:**

Proofs look sound to me, except for the small issues below and the fact that I didn't get the table work and couldn't verify the final steps in the proofs (because of this I cannot say that the model and proof are perfectly sound and really capture the desired level of forward secrecy). Besides this presentation is quite good, except for the inappropriate reference work, mentioned also below.

…

Example

Structure: Summary – Good – Bad – Other Comments

…

***References:**

The paper doesn’t do a good job of giving appropriate references. For example:

It refers to [23] for attacks against forward secrecy against two round protocol with state reveal. I guess this should be [Boyd and Gonzales Nieto, Cryptography and Coding, 2011], instead. In the intro, surprisingly [24] is also cited for this.

The idea of distributing ephemeral and long-term secrets by placing some ephemeral material in the long-term key, such that a reveal of either one doesn't hurt the other one, has been implicitly used already in the NAXOS [LaMaccia et al, ProvSec 2007] and KEA [Lauter et al, PKC 2006 and Kudla et al. Asiacrypt 2005] protocols, and has been used elsewhere, eg, One Round Key exchange... [Bergsma et al., PKC 2015]. It appears explicitly for example in the work by [Yoneyama, IWSEC 2012].

…

Example

Structure: Summary – Good – Bad – Other Comments

…

***Minor comments:**

'how to construct a tight AKE scheme without pairings in the random oracle model.' (page 2)- ambiguous: without (pairings in the ROM) or without pairings, in the ROM.

Smooth projective hashing (page 7) is defined as a function \Lambda:Y->Z but then refers to entropies.

Partial matching session (page 12, in bold) should be partially matching sessions, I think.

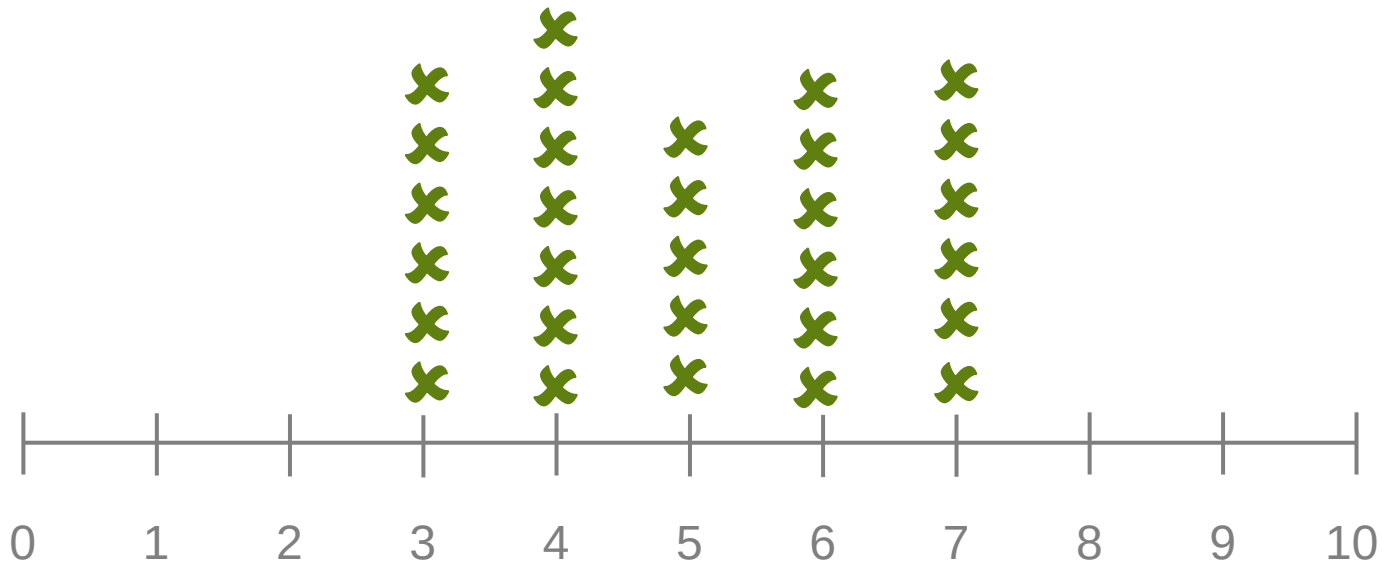
I didn't get the comment on page 16, in the proof, about state decryption being omitted and that this 'is only conceptual'.

'to obtain secret key sk_n and outputs both sk_n and k_n' on page 19. One of the sk keys should be sk_n′.

…

Things to Consider

Center Tendency Bias



use full range of scale

Critique, not Criticism

taken from Cambridge Dictionary

critique

noun

a report that discusses a situation or the writings or ideas of someone and offers a judgment about them

criticism

noun

the act of saying that something or someone is bad

How much to invest?