Summary of changes – AITO paper

Anonymous

Dear Editor,

Enclosed please the summary of changes of the paper "AITO: Compact Authenticated Encryption for Private and Secret Messaging", previously submitted as "Tweety: Tweet Secrets Efficiently". The initial paper was submitted as a privacy mechanism for Twitter, and rejected from PETs 2016 Issue 2. The main comment by reviewers was the unrealistic Twitter scenario application, due to its broadcast objective and the hurdle of key management.

Summary of changes

Following the comments from the four reviewers we re-wrote the motivation, as well as the possible available applications. We switched the focus of the paper and provide now a compact authenticated encryption AITO which is not tight to a specific application as the main contribution, rather than an application to improve privacy on Twitter. In addition, we demonstrated how AITO can be used in several different applications, such as the mix message format Sphinx, secret messaging services, and microblogging privacy, to increase their efficiency and security while giving the flexibility to offer extra properties as filtering, re-randomization, and limited user-selected data utility to providers.

The paper has been fully restructured and re-written. The main changes are summarized as follows:

- Abstract and Introduction re-written.
- Threat model generalized.
- AITO constructions described as a general cipher and not as an application focused on Twitter. (Section 3, 4, and 5)
- Demonstrated the possible practical applications of AITO in different systems (Section 6), such as Sphinx and secret messaging, along with its security and privacy advantages.
- Practical Analysis remodeled with the proof-of-knowledge demonstrator used as a practical example of efficiency of the application.
- Discussion and conclusions section re-written and adapted to the now contribution of the paper.