Linkable and traceable anonymous authentication with fine-grained access control

April 19 2024

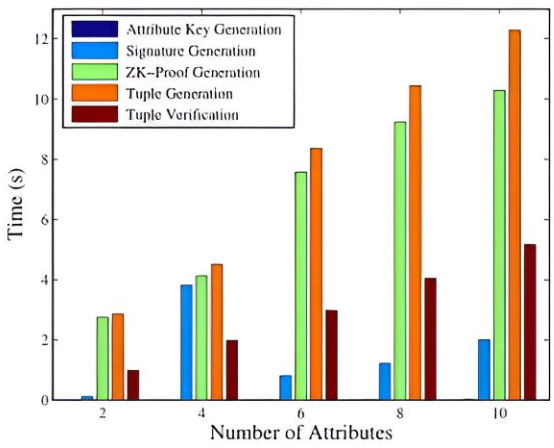

Fig. 1 Running time of algorithms.

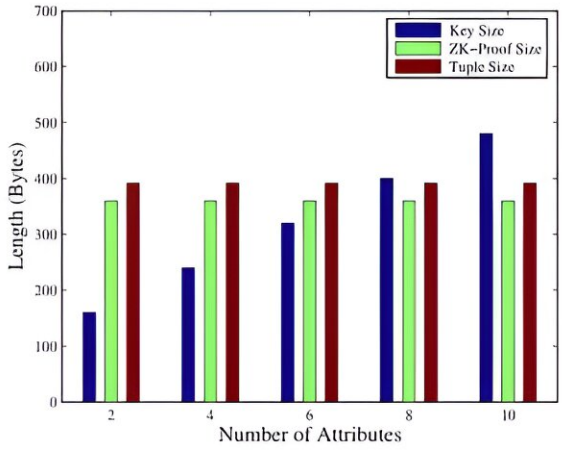

Fig. 2 Length of attribute key, zk-proof and Tuple.

Credit: Peng Li, Junzuo Lai, Dehua Zhou, Lianguan Huang, Meng Sun, Wei Wu, Ye Yang

Anonymous authentication plays a crucial role in privacy-focused applications, and it is used for authenticating a user's identity in a privacy-preserving way. If enough privacy is provided, malicious users may misuse privacy. Accountability is necessary to avoid abusing anonymity. Previous anonymous authentication schemes can not hold the basic requirements of public linking and tracing while further ensuring

access control simultaneously.

To address the problems, a research team led by Junzuo Lai published their research in *Frontiers of Computer Science*.

The team proposed a linkable and traceable anonymous authentication with fine-grained access control, supporting access control, anonymity, public linkability, and public traceability at the same time. The proposed scheme does not need a trusted authority to detect malicious behaviors. Anyone is able to judge whether a user authenticates multiple times or not, and further find its identity. A formal security proof and the experiment data show the efficiency and feasibility of the proposed scheme.

Future work can focus on expanding the scheme to a multi-authority scheme, allowing each authority to issue an attribute key corresponding to a certain attribute to a user.

More information: Linkable and traceable anonymous authentication with fine-grained access control, *Frontiers of Computer Science* (2024). DOI: 10.1007/s11704-023-3225-3

Provided by Higher Education Press