Summary: Chameleon hash functions are collision resistant when only the hashing keys of the functions are known. In particular, without the knowledge of the secret information, the chameleon hash function is merely like a regular cryptographic hash function, where it is hard to find collisions. However, anyone who has trapdoor keys can efficiently generate pre-images for the chameleon hash function. In some applications, such as redactable blockchains, unfortunately the existing properties do not suffice and we need more features. Actually, it is required that without knowing the trapdoor keys, nobody can compute collisions, even if he can see collisions for arbitrary hash functions. In 2017, Ateniese et al. introduced the notion of chameleon hash functions in the enhanced collision resistant model and proposed a construction in the standard model satisfying the features. To date, efficient constructions of this kind of chameleon hash functions remain as an open research problem. In this paper, we answer this problem affirmatively by presenting efficient constructions of the chameleon hash function satisfying the enhanced collision resistance. The contributions of this work are twofold. First, we show the weakness of previous work. Then, we proceed with proposing new schemes with more efficiency. Technically, we present a new chameleon hash function in the basic model and based on simple assumptions. This chameleon hash function is well compatible with Groth-Sahai proof systems and the Cramer-Shoup encryption schemes, and can be used as a stepping stone to construct an efficient chameleon hash function in the enhanced collision resistant model. Moreover, we show our basic chameleon hash can be combined with optimal ZK-SNARKs of Groth and Maller that leads to shorter sizes for chameleon hash function in the enhanced collision resistant model.

MSC:
94A60 Cryptography

Keywords:
chameleon hash functions; enhanced collision resistant model; standard model; Groth-Sahai proofs; SNARKs

Full Text: DOI

References:


Gennaro, R.; Gentry, C.; Parno, B.; Raykova, M., Quadratic span programs and succinct NIZKs without PCPs, Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, 626-645 (2013), Springer - Zbl 1300.94056


Mohassel, P., One-time signatures and chameleon hashes, Proceedings of the International Workshop on Selected Areas in Cryptography, 302-319 (2010), Springer - Zbl 1285.94090


[39] Zhang, F.; Safavi-Naini, R.; Susilo, W., Id-Based Chameleon Hashes from Bilinear Pairings, 2003, 208 (2003), IACR Cryptology ePrint Archive


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.