Notes on a family of collision-free functions

János Folláth

January 22, 2010

In [1] the authors proposed a new collision-free function for application in cryptography. This construction was also implemented by Crypto Ltd.. Later in [2] a weakness of this cryptographic primitive was found. In [3] a similar but stronger new construction was studied. In this talk some new results will be presented about this latter construction.

References

[1] Béreces, A.; Ködmön, J. and Pethő, A. 2004. "A one-way function based on norm form equations." Periodica Mathematica Hungarica, 49, 1-13.

[2] Aumasson, J.-P. 2009. "Cryptanalysis of a hash function based on norm form equations." Cryptologia, 33, 1-4.

[3] Béreces, A.; Folláth, J. and Pethő, A. 2010. "On a family of collision-free functions." to appear.