Cryptology ePrint Archive: Report 2011/227

Robust parent-identifying codes and combinatorial arrays

Alexander Barg and Grigory Kabatiansky

Abstract: An n-word y over a finite alphabet of cardinality q is called a descendant of a set of t words $x^1,\dots,x^t$ if $y_i\in\{x^1_i,\dots,x^t_i\}$ for all $i=1,\dots,n.$ A code $\cC=\{x^1,\dots,x^M\}$ is said to have the t-IPP property if for any n-word y that is a descendant of at most t parents belonging to the code it is possible to identify at least one of them. From earlier works it is known that t-IPP codes of positive rate exist if and only if $t\le q-1$.

We introduce a robust version of IPP codes which allows {unconditional} identification of parents even if some of the coordinates in y can break away from the descent rule, i.e., can take arbitrary values from the alphabet, or become completely unreadable. We show existence of robust t-IPP codes for all $t\le q-1$ and some positive proportion of such coordinates. The proofs involve relations between IPP codes and combinatorial arrays with separating properties such as perfect hash functions and hash codes, partially hashing families and separating codes.

For $t=2$ we find the exact proportion of mutant coordinates (for several error scenarios) that permits unconditional identification of parents.

Category / Keywords: Combinatorial cryptography; fingerprinting; traitor tracing

Date: received 9 May 2011

Contact author: abarg at umd edu

Available formats: PDF | BibTeX Citation

Version: 20110512:034957 (All versions of this report)

Discussion forum: Show discussion | Start new discussion
