Random Reference-Switching Functions

Chung-Chih Li

School of Information Technology
Illinois State University
Normal, IL 61790, USA

This idea of RRS (Random Reference-Switching) functions emerged from our previous effort in developing VPF (Virtual Password Functions) to avoid some common password thief attacks. After some speculation, I learned that, if properly defined, some RRS functions were much stronger than we originally expected in the context of light-weighted cryptosystem in which the computational power was limited. What I have proven is the reverse functions of such RRS are NP-complete. However, a probabilistic algorithm can resolve the hidden random key in a polynomial time. Here I give the definitions and a theorem.

Let $\mathbb{Z}_m = \{0, 1, \ldots m-1\}$, and let $X, R, V \in \mathbb{Z}_m^n$ be vectors as follows:

$$X = (x_0, x_1, x_2, \ldots, x_{n-1}), R = (r_0, r_1, r_2, \ldots, r_{n-1}), V = (v_0, v_1, v_2, \ldots, v_{n-1})$$

Definitions:

- An RRS function, f, is a function of type $\mathbb{Z}_m^n \times \mathbb{Z}_m^n \to \mathbb{Z}_m^n$ such that, it is intractable to find X from any **given** R and V such that $f(X, R) = V$.
- An *strong* RRS function, f, is an RRS function such that, it is intractable to find X from any **chosen** R and V such that $f(X, R) = V$.

An RRS function is said to be weak if it is not strong.

Theorem 1 *Given any nonzero $n, m \in \mathbf{N}$ and $V \in \mathbb{Z}_m^n$, to decide whether there exists $X \in \mathbb{Z}_m^n$ such that* (1) *hold is an NP-complete problem.*

$$\begin{array}{ccccc} v_0 & \equiv & x_0 x_{(x_0 \mod n)} & & \mod m \\ v_1 & \equiv & x_1 x_{(x_1 \mod n)} & & \mod m \\ \vdots & \equiv & \vdots & & \\ v_{n-1} & \equiv & x_{n-1} x_{(x_{n-1} \mod n)} & & \mod m \end{array} \quad (1)$$

In this informal presentation, I would like to expose the concept of RRS and use the theorem to define strong RRS functions.