# A ONE-WAY SEQUENCE FOR TRANSACTION VERIFICATION

Alan G. Konheim

Mathematical Sciences Department
IBM Thomas J. Watson Research Center
Yorktown Heights, New York 10598

**Abstract:** A protocol for transaction verification is defined and analyzed. *USER A* begins a *transaction* by sending *USER B* data concatenated with a number of *signatures*. The $i^{th}$-signature is an element of the $i^{th}$-*keyed-signature-sequence* of *USER A*. Its position in the sequence is determined by the protocol and data. A *keyed-signature-sequence*

$$KSS[k_A,i] = \{KSS_t[k_A,i] : 0 \le t < \infty\}$$

satisfies a recurrence of the form

$$KSS_t[k_A,i] = f_i(KSS_{t-1}[k_A,i])$$

where $f_i$ is a function whose inverse image(s) may not be effectively calculated and the initial element $KSS_0[k_A,i]$ is a function of the *USER A*'s (secret) key. The successors of $KSS_t[k_A,i]$ can be calculated without *USER A*'s key. *USER B* verifies that the transaction is *properly signed* by calculating from $KSS_{t_i}[k_A,i]$ the *reference signatures* $KSS_{r_i}[k_A,i]$ which are compared with supposed identical entries is a *contract* exchanged by the participants at the start of the protocol.