US009083515B1

(12) **United States Patent**
**van Dijk et al.**

(10) **Patent No.: US 9,083,515 B1**
(45) **Date of Patent: Jul. 14, 2015**

(54) **FORWARD SECURE PSEUDORANDOM NUMBER GENERATION RESILIENT TO FORWARD CLOCK ATTACKS**

(71) Applicant: **EMC Corporation**, Hopkinton, MA (US)

(72) Inventors: **Marten van Dijk**, Somerville, MA (US); **Nikolaos Triandopoulos**, Arlington, MA (US); **Ari Juels**, Brookline, MA (US); **Ronald Rivest**, Arlington, MA (US)

(73) Assignee: **EMC Corporation**, Hopkinton, MA (US)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 235 days.

(21) Appl. No.: **13/728,271**

(22) Filed: **Dec. 27, 2012**

(51) **Int. Cl.**

| | |
|---|---|
| ***H04L 9/22*** | (2006.01) |
| ***H04L 9/08*** | (2006.01) |
| ***H04L 29/06*** | (2006.01) |
| ***H04L 9/00*** | (2006.01) |

(52) **U.S. Cl.**
CPC ..... ***H04L 9/0869*** (2013.01); ***H04L 9/005*** (2013.01); ***H04L 63/068*** (2013.01); *H04L 9/0891* (2013.01); *H04L 63/1441* (2013.01)

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 7,095,850 | B1 * | 8/2006 | McGrew | 380/42 |
| 7,810,147 | B2 * | 10/2010 | Duane et al. | 726/9 |
| 8,699,713 | B1 * | 4/2014 | Rivest et al. | 380/277 |
| 8,745,710 | B1 * | 6/2014 | Roth et al. | 726/6 |
| 2002/0199102 | A1 * | 12/2002 | Carman et al. | 713/168 |
| 2006/0184797 | A1 * | 8/2006 | Weis et al. | 713/178 |

OTHER PUBLICATIONS

Bowers et al., Drifting Keys: Impersonation Detection for Constrained Devices, Proceedings of the IEEE Infocom 2013, Turin, Italy, Apr. 14-19, 2013.

* cited by examiner

*Primary Examiner* — Jung Kim
*Assistant Examiner* — Tri Tran
(74) *Attorney, Agent, or Firm* — Ryan, Mason & Lewis, LLP

(57) **ABSTRACT**

Methods and apparatus are provided for generation of forward secure pseudorandom numbers that are resilient to such forward clock attacks. A forward secure pseudorandom number is generated by obtaining a first state $s_i$ corresponding to a current leaf node $v_i$ in a hierarchical tree, wherein the current leaf $v_i$ produces a first pseudorandom number $r_{i-1}$; updating the first state $s_i$ to a second state $s_{i+t}$ corresponding to a second leaf node $v_{i+t}$; and computing a second pseudorandom number $r_{i+t-1}$ corresponding to the second leaf node $v_{i+t}$, wherein the second pseudorandom number $r_{i+t-1}$ is based on a forward clock reset index that identifies an instance of the hierarchical tree, wherein the instance of the hierarchical tree is incremented when one or more criteria indicating a forward clock attack are detected. The forward clock reset index can be encoded in a forward secure manner in the hierarchical tree.

**31 Claims, 6 Drawing Sheets**