Sichere Authentifizierung mit einer Klasse von Einwegfunktionen

Fachgebiet
- Kryptographie

Schlüsselwörter
- Einwegfunktion
- Authentifizierung
- Sicherheit
- Hash
- Verschlüsselung

Schutzrecht
- EP 14 176 198.1
  angemeldet 07/2014

Entwicklungsstand
- Prototyp
  (Softwareumsetzung zu Testzwecken)

Angebote
- Verkauf
- Lizenzierung
- Option
- FuE-Kooperation

Ansprechpartner
Gelfa Grünbacher
gruenbacher@brainshell.de
Tel. +49 331 977 6173
www.brainshell.de

ZAB ZukunftsAgentur
Brandenburg GmbH
Brainshell
Steinstraße 104-106
14480 Potsdam
Deutschland

Referenz
Angebot Nr. 14-09
Juni 2015

Beschreibung

Bei der vorliegenden Erfindung handelt es sich um die Konstruktion und Erzeugung unendlich vieler echter Einwegfunktionen, die man zur Verschlüsselung von Passworten, zur „universal hashing“ und zur Konstruktion von digitalen Signaturverfahren und Public-Key-Systemen verwenden kann.

Ablauf

Die Einwegfunktionen kann man sehr einfach konstruieren. Die Inputwerte für die Funktionen sind Vektoren von Zahlen. Jeder Vektor hat die Dimension $k \geq 2$, wobei k vom Benutzer frei gewählt wird. Je größer k, desto mehr Sicherheit erreicht man.

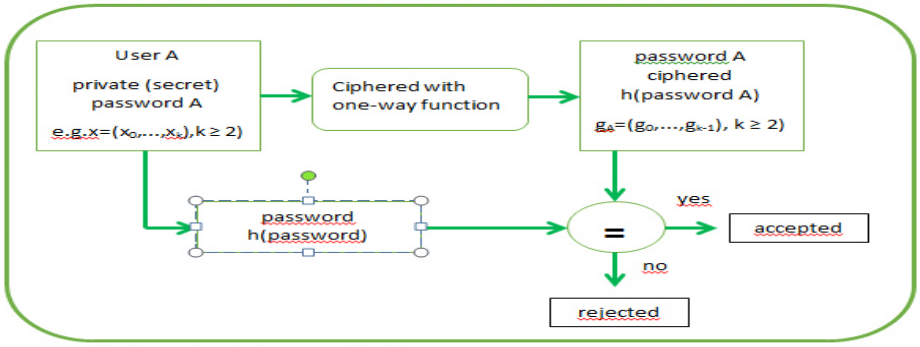

Fig.: One-way function for password-checking

Gibt der Benutzer im System, in dem die Einwegfunktion liegt, ein privates (geheimes) Passwort A ein, berechnet sie den Vektor h(Passwort A) und nur dieser Vektor wird in der Datenbank gespeichert, nicht das Passwort. Gibt ein Benutzer sein Passwort ein, berechnet die Einwegfunktion den Vektor h(Passwort). Nur wenn der Vektor h(Passwort) gleich dem gespeicherten Vektor h(Passwort A) ist, ist die Authentifizierung erfolgreich. Da nur die Vektoren gespeichert werden, ist das Passwort absolut sicher, selbst wenn die Datenbank geknackt wird, ist es unmöglich aus dem Vektor das Passwort zurück zu bilden. Auch können die Passwörter nicht manipuliert werden, nicht einmal durch den Administrator des Systems.

Details

In Tests haben die Einwegfunktionen sehr gut funktioniert. Sie könnten z.B. beim Online-Shopping eingesetzt werden. Man könnte sie auf Handys implementieren, um via cloud-computing Personen zu authentifizieren. Würde die Einwegfunktion auf einem Chip (z.B. EC-Karte) implementiert werden, würde der Verlust der Karte keine Rolle mehr spielen.

Neben der Anwendung zur Authentifizierung ist die Implementierung von Einwegfunktionen in Zugangsberechtigungs- und Bezahlsystemen möglich. Bei Internet-Anwendungen können die Einwegfunktionen zum Erzeugen von Session-IDs genutzt werden. Dabei sind die Sessions-IDs Hashwerte, die von wechselnden Zustandswerten abhängen (z.B. Zeit, IP-Adresse). Zu klären ist noch, ob die Einwegfunktionen in einem ASIC- oder RFID-System denkbar wären.

Gesucht wird ein Partner für die Entwicklung konkreter Anwendungen oder Käufer / Lizenznehmer für die Erfindung.