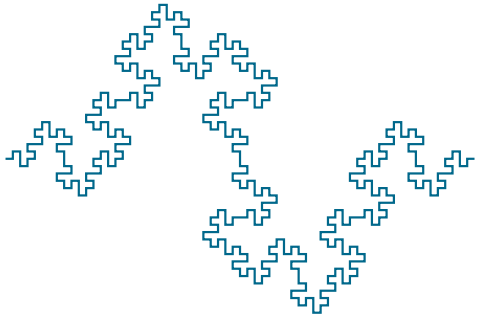
Secure Hash Algorithm

SHA-256

Chi Trung Nguyen
T-Systems



18. Juni 2012

Inhalt

- Einführung
  - Was ist ein Hash?
- Geschichte
  - SHA
  - SHA-0
  - SHA-1
  - SHA-2
  - eig
- Implementierung
  - Algorithmus
  - Pseudocode
- Anwendung
  - Verwendungszweck
  - Sicherheitslücken
- Ausblick
  - SHA-3

WAS IST EIN HASH?

- deutsch: *„zerhacken“* , *„verstreuen“*

WAS IST EIN HASH?

- deutsch: *„zerhacken“* , *„verstreuen“*
- Hashfunktion oder Streuwertfunktion erstellt aus beliebiger großer Quellmenge eine immer gleich große Zielmenge
  - $f(x) = f(x')$

WAS IST EIN HASH?

- deutsch: „*zerhacken*“ , „*verstreuen*“
- Hashfunktion oder Streuwertfunktion erstellt aus beliebiger großer Quellmenge eine immer gleich große Zielmenge
  - $f(x) = f(x')$
- Item C

SHA ALLGEMEIN

- 1993 vom **National Institute of Standards(NIST)** als ein **U.S. Federal Information Processing Standard (FIPS)** veröffentlicht

SHA ALLGEMEIN

- 1993 vom **National Institute of Standards(NIST)** als ein **U.S. Federal Information Processing Standard (FIPS)** veröffentlicht
- Gruppe von kryptologischer Hashfunktionen
  - SHA-0
  - SHA-1
  - SHA-2
  - SHA-3

SHA-0

- Item A

SHA-0

- Item A
- Item B
  - Subitem 1
  - Subtem 2
- Item C

SHA-1

SHA-2

EIG

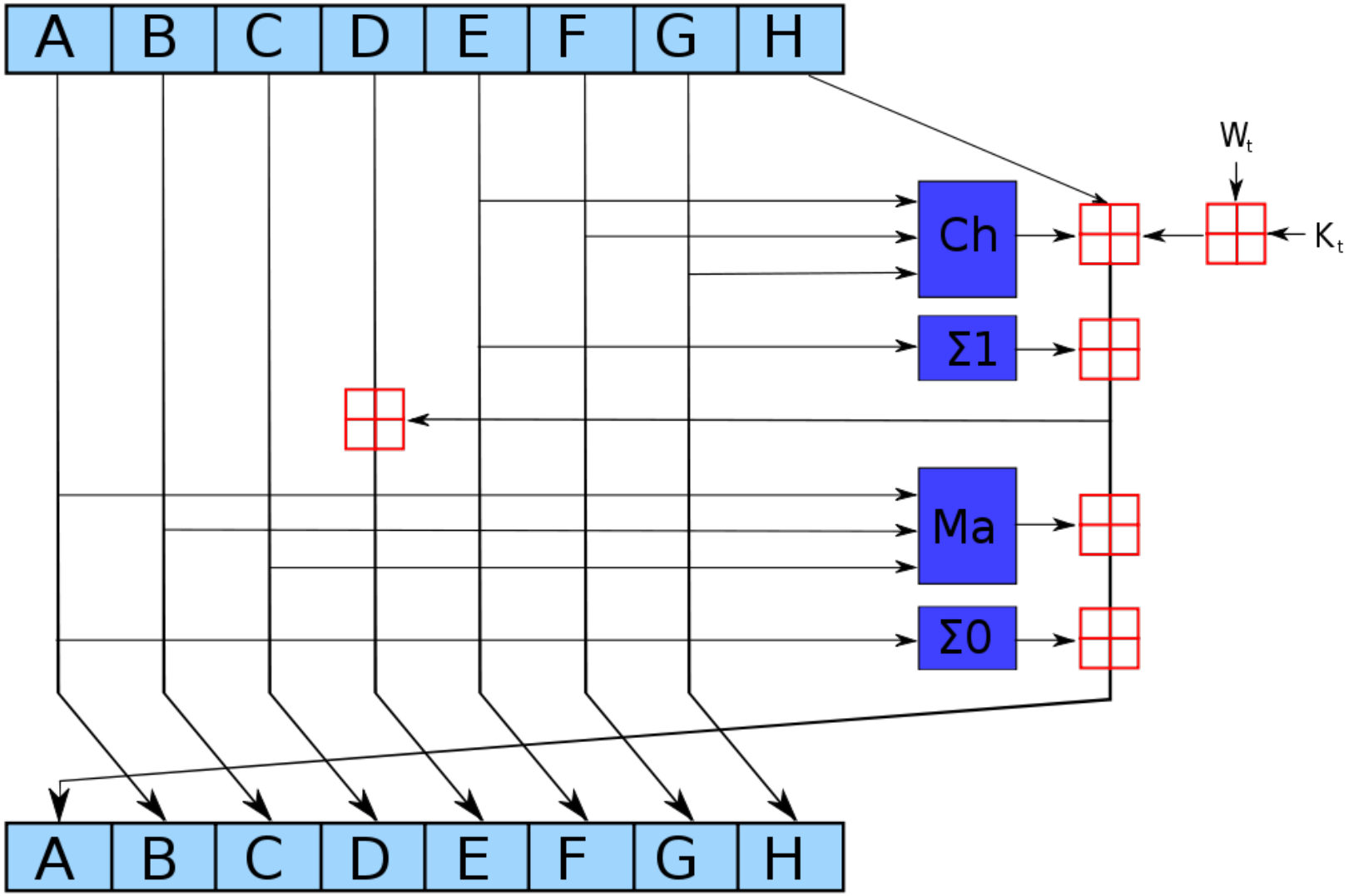
Tabelle : Secure Hash Algorithmus Eigenschaften

Algorithmus	Message Size(bits)	Block Size(bits)	Word Size(bits)	Message Digest Size(bits)
SHA-1	$< 2^{64}$	512	32	160
SHA-224	$< 2^{64}$	512	32	224
SHA-256	$< 2^{64}$	512	32	256
SHA-384	$< 2^{128}$	1024	64	384
SHA-512	$< 2^{128}$	1024	64	512

FUNKTIONEN

$$Ch(E,F,G) = (E \wedge F) \oplus (\neg E \wedge G)$$
$$Ma(A,B,C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C)$$
$$\Sigma_0 = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$$
$$\Sigma_1 = (A \ggg 6) \oplus (A \ggg 11) \oplus (A \ggg 25)$$

DARSTELLUNG DES ALGORITHMUS



PSEUDOCODE

VERWENDUNGSZWECK

- Digitale Zertifikate und Signaturen

VERWENDUNGSZWECK

- Digitale Zertifikate und Signaturen
- Passwortverschlüsselung
  - pam_unix: sha2, md5
  - htpasswd(Apache): sha1, md5
  - MySQL: sha1

VERWENDUNGSZWECK

- Digitale Zertifikate und Signaturen
- Passwortverschlüsselung
  - pam_unix: sha2, md5
  - htpasswd(Apache): sha1, md5
  - MySQL: sha1
- Prüfsummen bei Downloads

SICHERHEITSLÜCKEN & ANGRIFFSVEKTOREN

SHA-3