Kryptographie im 21. Jahrhundert

Willi Meier Simon Fischer Jean-Philippe Aumasson

Institut IAST

University of Applied Sciences Northwestern Switzerland
School of Engineering

Einsatz von Kryptographie

- Absicherung von Computernetzwerken
- Sicherer elektronischer Geldtransfer
- Abhörsichere Handy's
- Embedded Systems
- Biometrische Pässe
- Sicherheit von RFID's



Einsatz von Kryptographie

Verschiedene praktische Verfahren sind unsicher:

- Bluetooth Protokoll
- Digitale Signaturen (Hashfunktionen)

Ziel:

- Entwicklung sicherer und effizienter Verfahren, je nach industriellem Anwendungszweck

Projekte

Internationale Projekte:

- eSTREAM
- NIST Plan

Eigene Forschungsprojekte:

- Design und Analyse von neuen Systemen
- Analyse vor praktischem Einsatz wesentlich

Gewonnene Resultate nutzbar für:

- Industrie (KTI-Projekt)
- Beiträge an internationale Bestrebungen
- Design von sicheren Systemen

Externe Finanzierung:

- MICS, SNF
- Gebert Rüf Stiftung, Hasler Stiftung

Überblick

1. Stream Ciphers
2. Hashfunktionen

Neue Zürcher Zeitung MEDIEN UND

Mit Hash auf Kollisionskurs

Hashfunktion SHA-1 möglicherweise geknackt

Seit vergangener Woche steht die Behauptung im Raum, die Hashfunktion SHA-1 sei geknackt worden. Diese Funktion wird verwendet, um die Authentizität und Integrität von Dokumenten sicherzustellen, und spielt in der Kryptologie insbesondere im Zusammenhang mit der digitalen Signatur eine grosse Rolle.

Die kryptographische Hashfunktion SHA-1 soll geknackt worden sein. Dies behauptet zumindest der amerikanische Sicherheitsexperte Bruce Schneier auf seiner Website.[1] Schneier bezieht sich auf ein bisher unveröffentlichtes Papier einer chinesischen Forschergruppe um Xiaoyun Wang, Yiqun Lisa Yin und Hongbo Yu von der Shandong University. Diese Forschergruppe hat sich in der Zwischenzeit zu Wort gemeldet und die Veröffentlichung eines Berichtes in Aussicht gestellt.

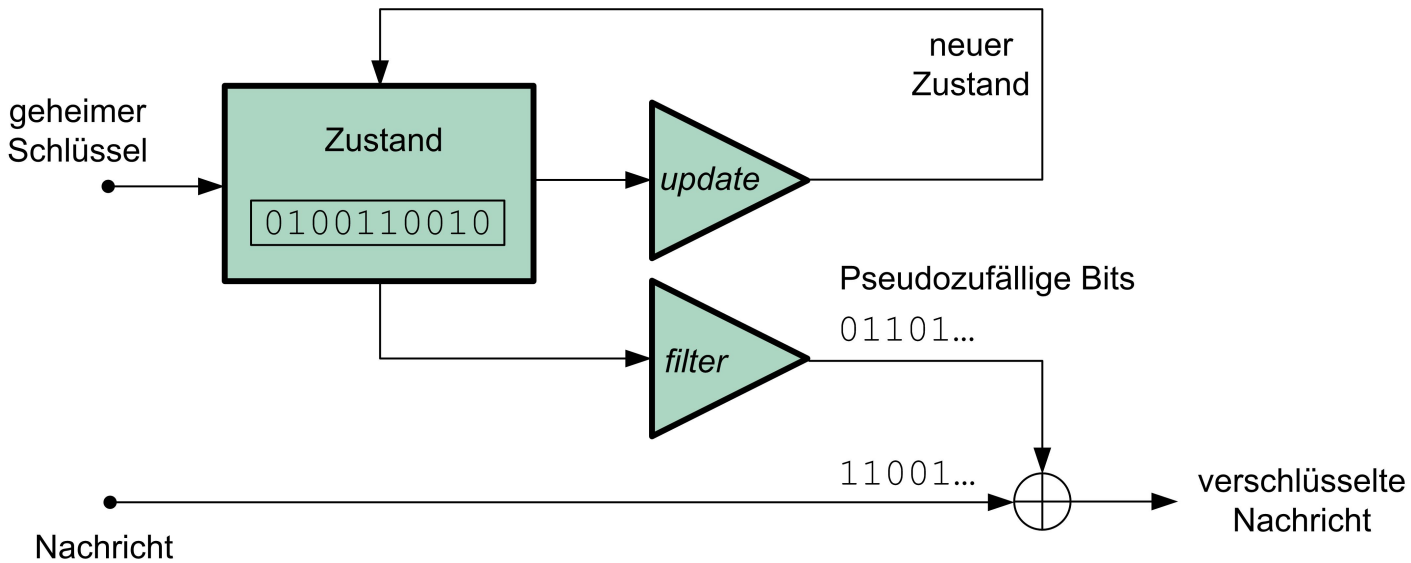
Hashfunktionen

S. B. Das englische Wort «to hash» heisst zermalmen, zerhacken. In der Informatik werden mit Hilfe von sogenannten Hashfunktionen Daten zu einem Konzentrat verdichtet. Dank der geringeren Grösse lässt sich dieses Konzentrat – der Hashwert – einfacher handhaben. Der Hashwert kann verwendet werden, um gespeicherte Daten wiederzufinden oder um die Authentizität und Integrität von Dokumenten zu überprüfen.

STREAM CIPHERS

Was ist ein Stream Cipher?

Ziel ist Geheimhaltung von Nachrichten. Stream Cipher sind sehr klein und schnell.



Profil 1: Optimiert für Software (hoher Durchsatz).
Profil 2: Optimiert für Hardware mit wenig Ressourcen.

Anwendungen

Stream Ciphers vom Profil 2 (HW) können in mobilen Geräten verwendet werden:

- Mobiltelefone
- RFID's
- Wifi-Netzwerke

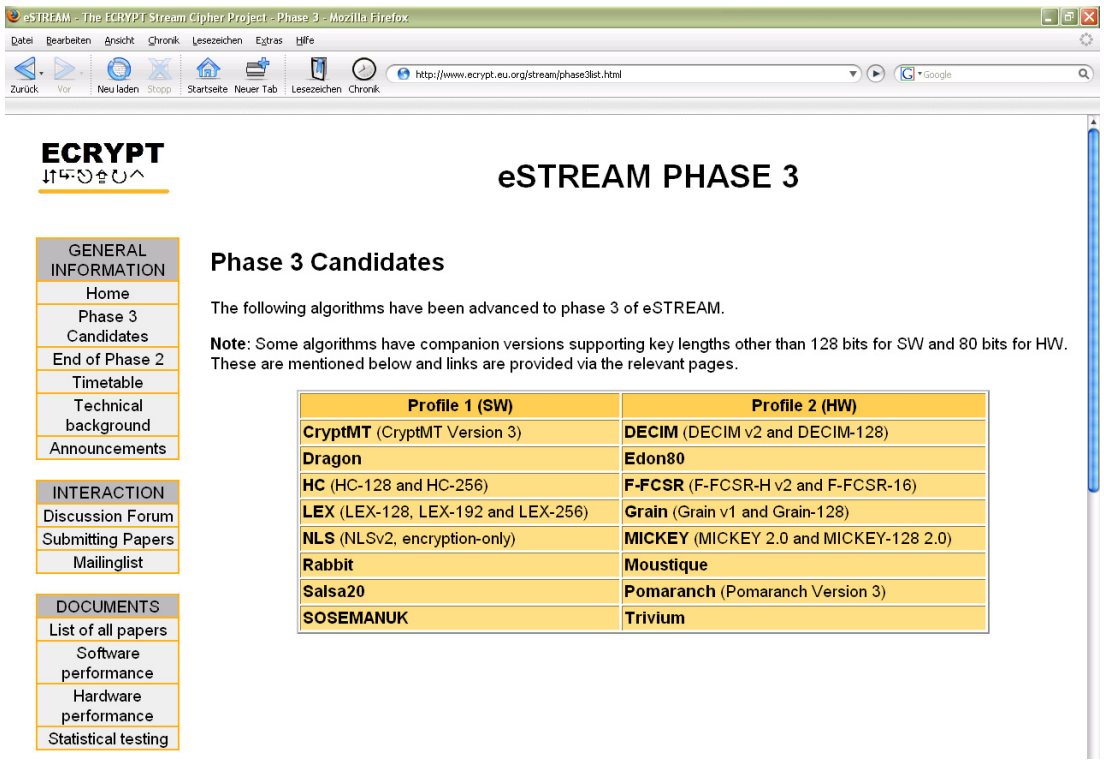


Bekannte Beispiele: Stream Cipher von GSM und Bluetooth. Beide Designs sind aber unsicher (kann geheimen Schlüssel finden)!

eSTREAM

Europäisches Projekt eSTREAM läuft seit 2004.
Entwickler von Algorithmen wurden aufgefordert, neue Vorschläge von Stream Cipher einzureichen.

- 34 Vorschläge sind weltweit eingereicht worden
- Grosser Wettbewerb durch öffentliche Analyse
- Gewinner werden im Mai 2008 bestimmt



Beiträge

Wir haben einen eigenen Stream Cipher eingereicht (mit Uni Lund): Grain.
Einer der besten Kandidaten im Profil 2 (HW).

Wir haben die Sicherheit anderer Stream Cipher untersucht:

- Vollständiger Angriff gegen einen schwachen Kandidaten
- Bestätigung der Sicherheit eines angesehenen Kandidaten
- Verbesserung bisheriger Angriffe
- Beobachtung von teilweisen Schwächen

Beispiel einer Analyse

Bekannte Angriffe auf Stream Cipher: *Algebraische Angriffe* - finde und löse ein Gleichungssystem mit tiefem algebraischen Grad.

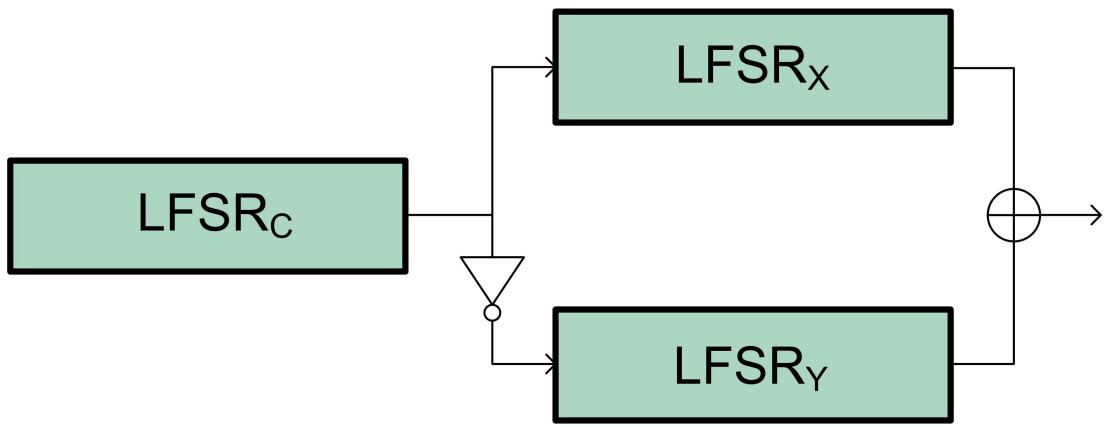
Wir haben ein neues Tool entwickelt (inspiriert durch algebraische Angriffe), um die Sicherheit von gewissen Stream Cipher zu beurteilen.

- Überraschender Angriff auf den "Alternating Step Generator".
- Bestätige Sicherheit eines eSTREAM Kandidaten.

ASG

Der Stream Cipher ASG ist sehr einfach und elegant. Er wurde vor 20 Jahren in der Schweiz entwickelt.

Konstruktion: 3 lineare Schieberegister, wovon 2 irregulär getaktet werden.



Unser Angriff ist etwa 7000 mal schneller als die bisherigen Angriffe!

HASH FUNCTIONS

What is this?

Hash functions =  of cryptography.

Cryptographic component used for secret communication, identification, etc., in







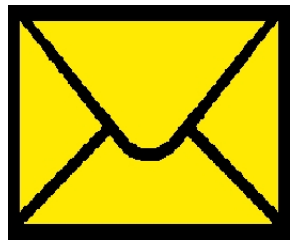


Applications

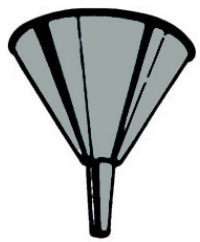
- digital signatures
- micropayment systems
- modification detection
- protection of passwords
- pseudo-random generators
- construction of encryption schemes
- etc.

Principle

Message



Can be of any length



Hash function

Hash value

Has fixed length

Principle

Hash functions map a message of arbitrary length to a bit-string of fixed length:

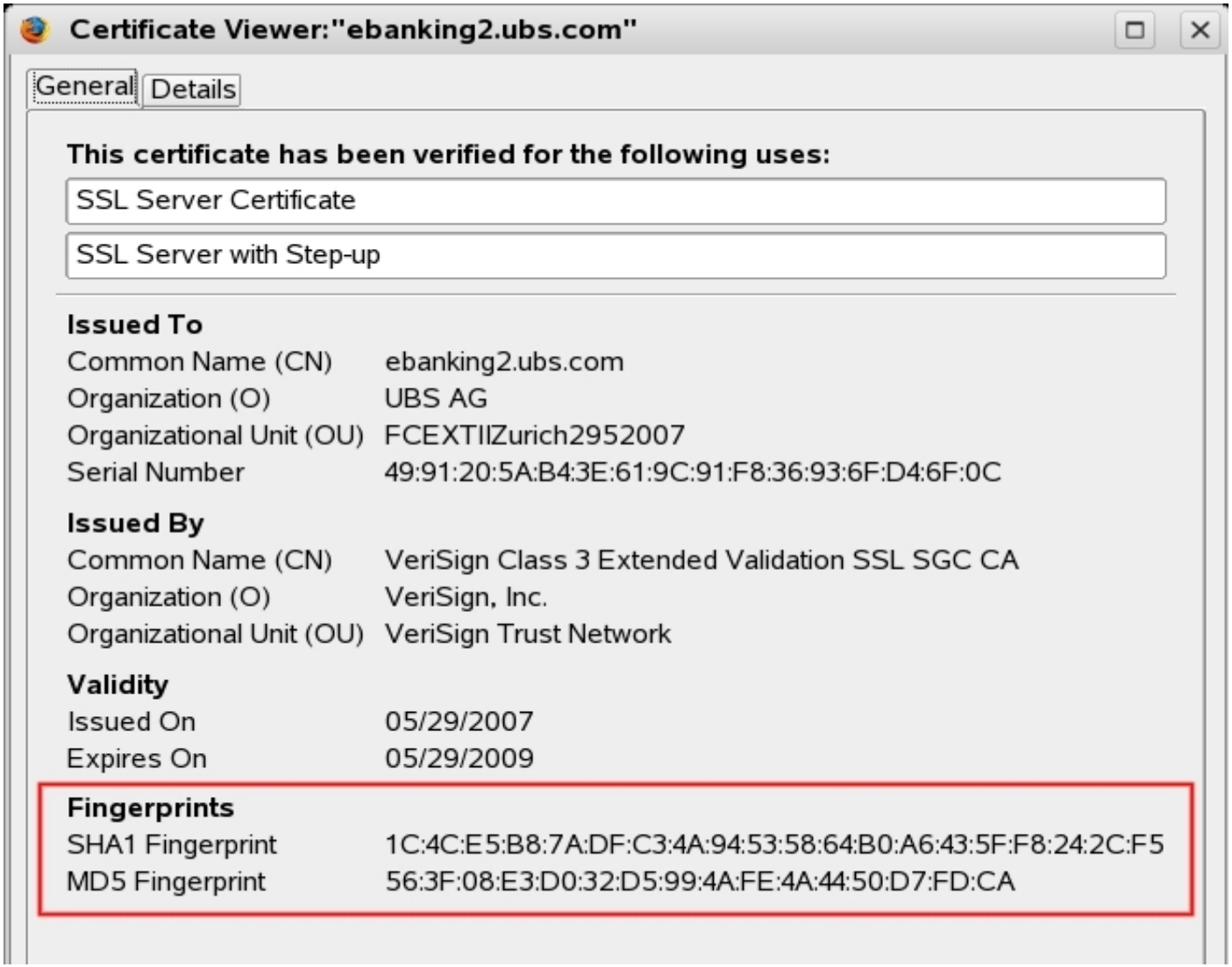
$$H : \text{message} \mapsto \text{hash value}$$

Typical hash function have a hash value of 160 bits, 256 bits, or 512 bits.

Important: a small change in the message should result in a big change in the hash value, e.g. with the function MD5

$$\begin{aligned} H(\text{“H}\mathbf{e}\text{llo”}) &= \texttt{09f7e02f1290be211da707a266f153b3} \\ H(\text{“H}\mathbf{a}\text{llo”}) &= \texttt{3290ec3c19a8a39362f7d70043f15627} \end{aligned}$$

Example: UBS Certificate



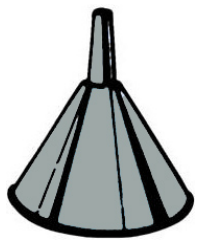
Security Requirement

It should be impossible to find a **preimage**:

Hash value

↓

Inversion



↓

Message

Many preimages exist

Password Protection

Login with `ID` and `Password`

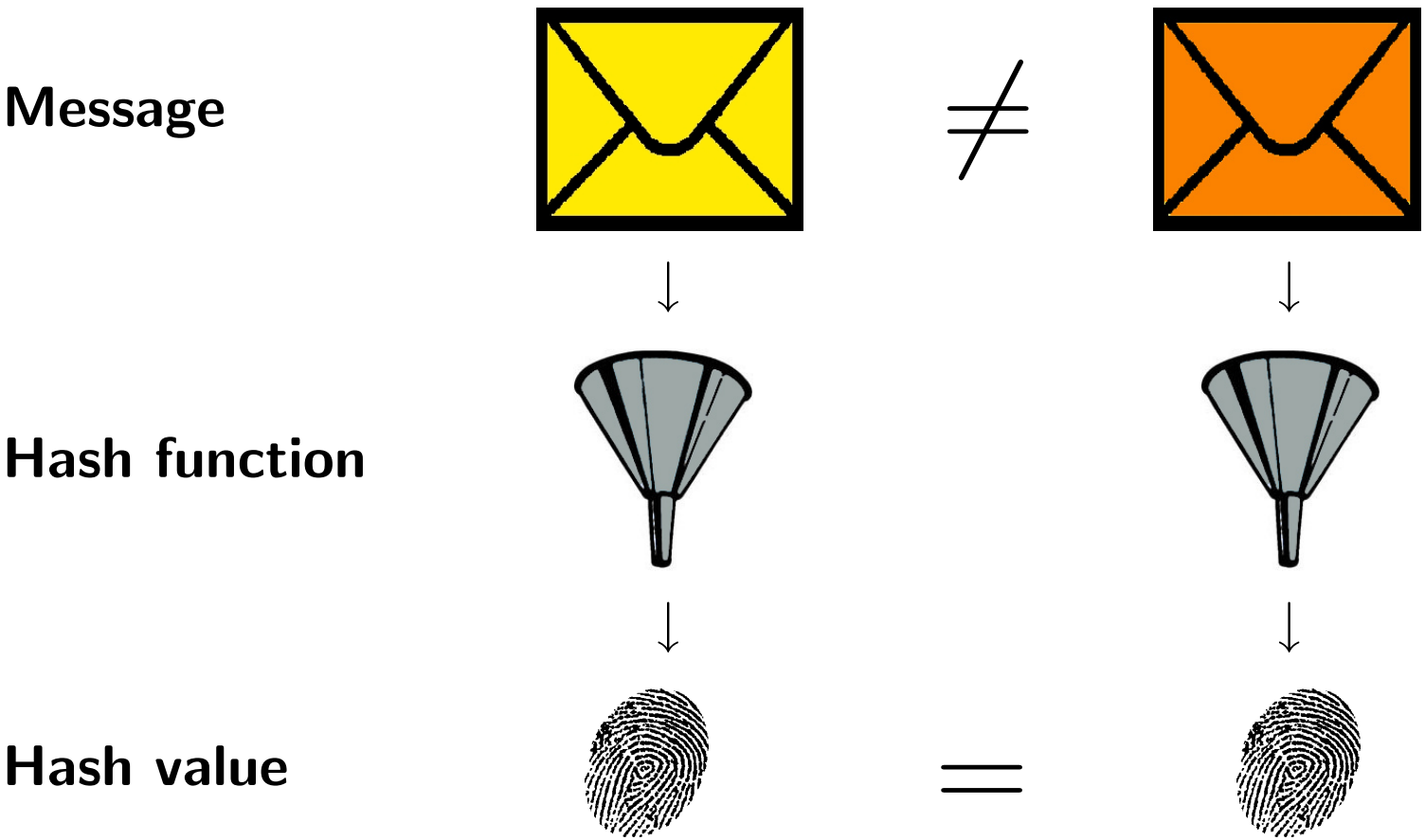
Computer **stores fingerprints** of passwords, and checks if the password entered has the correct fingerprint.

$\Rightarrow$ if the computer is stolen, the robber won't find the password.

If **preimages** can be found, passwords can be recovered!

Security Requirement

It should be impossible to find a **collision**:



Digital Signatures

Handwritten signature

Digital signature

`011101...001101`

In **digital signatures** schemes, one does not sign the message, but its **fingerprint** (for efficiency).

$\Rightarrow$ given a message, if one is able to find a distinct one with same fingerprint, then he can claim that you signed it.

Example of **critical collision**:

$$H(\text{“I agree to pay 100 CHF”}) = H(\text{“I agree to pay 100000 CHF”})$$

Current Status

NIST standards (for U.S. and *de facto* worldwide industry, academia, government usage):

- functions SHA-1, SHA-224, SHA-256, etc.
- not broken yet, but. . .
- too few security guarantees.

Current Status

NIST standards (for U.S. and *de facto* worldwide industry, academia, government usage):

- functions SHA-1, SHA-224, SHA-256, etc.
- not broken yet, but. . .
- too few security guarantees.

Reaction:

= international **competition for new hash functions** (2007-2012)

Our Work

Objectives

- Break hash functions (i.e. find collisions or preimages)
- Study new constructions (security, efficiency)

Current achievements

- Discovered methods for finding collisions efficiently in two recent proposals
- Discovered security flaws in another proposal

Conclusion

We make daily use of cryptography (cellphones, Wifi, etc.)

- **Stream ciphers** for encryption in wireless networks.
- **Hash functions** for digital signatures, authentication, etc.

Through local and international projects, we contribute to the analysis and design of new algorithms.