MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

Tagungsbericht 13/1992

Cryptographic Hash Functions

24.3. bis 27.3.1992

The workshop was organised by Thomas Beth (Karlsruhe) and covered the current research in the field of cryptographic hash functions that are an important tool e.g. when digitally signing electronic messages. The talks considered the use of hash functions in cryptography as well as requirements and principles for designing such functions. In a third group of talks results of hash function cryptanalysis were presented.

On Thursday evening a plenar discussion on the state of the art took place. Participants of the workshop suggested that 128 bit hash function output length might be insufficient for future use because of the expected advances in computing technology. Furthermore, the applicability of parallel calculations to cryptographic hash functions was discussed. In future, intermediate solutions between parallel and sequential calculation should be explored.

A list of the talks can be found in the appendix.

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Vortragsauszüge

G. BRASSARD:

Privacy Amplification by Hashing

Assume that Alice and Bob share a random n-bit string x, but that this string is somewhat compromised: Eve has obtained partial information about it. Perhaps she knows k physical bits of x, for $k < n$, or perhaps she knows the value of $e(x)$ for some function $e : \Sigma^n \rightarrow \Sigma^k$ that she cleverly chose ($\Sigma = \{0,1\}$), or perhaps she obtained x through a binary symmetric channel (BSC) with error probability 11% (in which case she has $k \approx n/2$ bits of Shannon information about x).

Even though they do not know exactly what Eve knows, Alice and Bob have an upper bound on the information in Eve' s hand (k) and they know what type of information it is (physical bits, value of a function, shannon information through BSC). Their goal is to publicly agree on a compression hash function $h : \Sigma^n \rightarrow \Sigma^{n-k-t}$ for some safety parameter $t \geq 0$ such that Eve' s information about $h(x)$ is arbitrarily small even though she learns all about the function h itself in addition to what she already knows about x. The value $h(x)$ can then be used as shared secret key between Alice and Bob.

It is proven that if Eve' s Renyi (or collision) information about x is no more than k bits, then both her Shannon and Renyi information about $h(x)$ is less than $2^{-t}/ln2$ in the expected sense. However her Shannon information could be very much smaller and much less severe compression could be sufficient to bring it down to roughly 2^{-t}.

E. BIHAM:

On the Applicability of Differential Cryptanalysis to Hash Functions

Differential cryptanalysis with respect to hash functions was presented, along with comparisons of the main requirements from cryptosystems and hash functions. The differential cryptanalysis of N-Hash and Snefru were shown, with conclusions about the design criteria for hash functions. Most of these criteria were already (independently) used in MD4, MD5 and NIST-SHS. It was advised to incorporate the initial value h_{i-1} into the w's entering directly into the various rounds of SHS. Notion of security zones in the design of hash functions was suggested.

F. DAMM:

Requirements for Cryptographic Hash Functions

Cryptographic hash functions are a widely used tool when digitally signing electronic messages. We try to discuss the quality requirements such functions should fulfill. Basically there are functional and security requirements. Functional requirements like e.g. contraction of the input and fast calculation are ordered by priority in the algorithm design and implementation process. Security requirements like collision resistance are seen with respect to known weaknesses of cryptographic hash functions and from an abstract point of view like 'calculation of collisions must be hard'. Requirements are analysed for logical interdependencies and thus a framework for the assessment of cryptographic hash functions is outlined that could be of help to designers, users and the cryptographic research community. (Joint work with Fritz Bauspieß.)

A. JUNG:

Random Numbers in Hash Functions

In his 1991 paper "Efficient Signature Generation by Smart Cards", C. P. Schnorr describes a signature scheme which uses the hash function in such a way that collisions or dependencies no longer pose a threat. This is achieved by including in the hashing process an intermediary value from the signature scheme. We show how such a property can be achieved for any signature scheme without compromising the hashing process. The solution that we propose and that we claim to introduce no new weaknesses is to choose a random number r (for every signature), to compute $h(h(r), m)$ and sign this value. The signature then consists of the pair $(s(h(h(r), m)), r)$. Since r can be of size about 2^{60}, neither performance nor storage requirements are affected much.

T. MATSUMOTO:

Constructing One-Way Hash Functions and Relatives

We reveal a duality between constructions of pseudo-random string generators and one-way hash functions. Applying the duality, we present a simple construction for universal hash functions assuming the existence of one-way permutations. Using ideas behind the construction, we propose a design principle of constructing building blocks (compressor) for one-way hash functions which can be useful for practical applications.

We also prove that universal one-way hash functions (UOHs) with respect to initial-strings chosen uniformly at random can be transformed into UOHs with respect

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

to initial-strings chosen arbitrarily, and mention the research history of constructing UOHs based on weaker assumptions. Furthermore, we investigate relationships among various versions of one-way hash functions classified by initial-string ensembles and by models of computation and by required security levels.

B. PRENEEL:

Hash Functions Based on Blockciphers

Collision resistant hash functions are an important tool for cryptographic applications such as pseudo-random generators and digital signature schemes. The talk reviews the hash functions that are based on block ciphers. A distinction is made between schemes where the size of the hashcode is equal to the blocklength of the block cipher and schemes where the hashcode is twice as long. For the first case it is possible to classify most existing proposals in a general framework. For the second type of functions an overview has been given of existing proposals. Finally a new scheme has been presented that allows a tradeoff between performance and security level.

M. GIRAULT:

FFT Hashing (first Version) is not Collision-Free

The FFT hash-function proposed by Schnorr at CRYPTO '91 hashes messages of arbitrary length into a 128-bit hash value. In this talk, we report a work by Baritaud, Gilbert and Girault, which shows that this function is not collision-free (Daemen et al. obtained independently the same result). We give the basic ideas of the attack, which allows to get two distinct 256-bit messages with the same hash value. Finding such a collision requires approximately 2^{23} practical computations of the hash function, and takes a few minutes on a SPARC workstation.

C.P. SCHNORR:

FFT-Hash II

We propose an efficient algorithm that hashes messages of arbitrary bit length into an 128-bit hash value. The algorithm is designed to make the production of a pair of colliding messages computationally infeasible. The algorithm performs a discrete Fourier transform and a polynomial recursion over a finite field. Each hash value in $\{0,1\}^{128}$ occurs with frequency at most 2^{-120}. This hash function is an improved

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

version of FFT-Hash I that was presented in the rump session of CRYPTO '91. It counters the attacks by Marc Girault and Daemen, Bosselaers that have generated collisions for FFT-Hash I.

P. CAMION:

A Probabilistic Algorithm that Breaks a Knapsack Hash Function

Let $a_1, \ldots, a_s$ be fixed integers of A binary digits randomly selected. If T is a plaintext of s binary symbols, $T = (x_1, \ldots, x_s)$, then

$$b = \sum_{i=1}^{s} x_i a_i$$

is the proposed hash value.

The values assigned are 256 for s and 120 for A. Thus b has at most $120 + 8 = 128$ binary digits.

Thus the probability that a random 256-bit string be a solution is 2^{-128}.

Here a probabilistic algorithm is however designed which solves the problem and thus breaks the knapsack.

The number of computations to come up with a solution is in the region of 2^{32}. (Joint work with Jacques Patarin.)

J.-J. QUISQUATER:

Collisions

Given a function h (DES, for instance), we first discuss about feasible computations in order to define the possible power of attacks. After that, we examine the complexity of finding a collision in different settings and the memory we need for it. The complexity result is based on the assumption that we are speaking about random mappings. It is possible to have problems otherwise. We then introduce the concept of trapdoor in hash functions in order to exemplify the problem. Finally we present a recent setting for hash functions (Zemor) and we show that there are many advantages.

Gefördert durch DFG Deutsche Forschungsgemeinschaft

M. YUNG:

Interactive Hashing

Combining Hash Functions and One-Way Functions has proven to be very effective in implementing cryptographic primitives (such as pseudo-random generators & digital signatures) based on reduced cryptographic assumptions. In this talk we present recent developments of using hash in reducing computational-complexity assumptions in interactive procedures (zero-knowledge proofs and protocols), via a generation of hash-functions (& hashing) by interacting parties.

Berichterstatter: Fritz Bauspieß, Frank Damm

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Tagungsteilnehmer

Fritz Bauspieß
Europäisches Institut für
Systemsicherheit E.I.S.S.
Universität Karlsruhe
Postfach 6980

W-7500 Karlsruhe 1
GERMANY

Prof.Dr. Thomas Beth
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Am Fasanengarten 5, Geb. 5034

W-7500 Karlsruhe 1
GERMANY

Dr. Eli Biham
Computer Science Department
TECHNION
Israel Institute of Technology

Haifa
ISRAEL

Prof.Dr. Gilles Brassard
Dept. of Computer Science
University of Montreal
C.P. 6128, Succ. A

Montreal , P.Q. H3C 3J7
CANADA

Prof.Dr. Paul Camion
INRIA Rocquencourt
Domaine de Voluceau
B. P. 105

F-78153 Le Chesnay Cedex

Frank Damm
Europäisches Institut für
Systemsicherheit E.I.S.S.
Universität Karlsruhe
Postfach 6980

W-7500 Karlsruhe 1
GERMANY

Dr. Markus Dichtl
Siemens AG
ZFE ST SN5
Otto-Hahn-Ring 5

W-8000 München 83
GERMANY

Prof.Dr. Whitfield Diffie
SUN Microsystems, MTV 01-40
2550 Garcia Avenue

Mountain View , CA 94043
USA

Dr. Marc Girault
SEPT
42 rue des Coutures
B.P. 6243

F-14066 Caen

Dr. Achim Jung
Fachbereich Mathematik
TH Darmstadt
Schloßgartenstr. 7

W-6100 Darmstadt
GERMANY

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Prof.Dr. Tsutomu Matsumoto
Division of Electrical and Computer
Engineering
Yokohama National University
156 Tokiwadai, Hodogaya

Yokohama 240
JAPAN

Dr. Bart Preneel
ESAT Lab,
K.U. Leuven
K. Mercierlaan 94

B-3001 Heverlee

Prof.Dr. Jean-Jacques Quisquater
3, Avenue des Canards

B-1640 Rhode-Saint-Genese

Prof.Dr. Claus-Peter Schnorr
Mathematisches Seminar
Fachbereich Mathematik
Universität Frankfurt
Postfach 11 19 32

W-6000 Frankfurt 1
GERMANY

Moti Yung
IBM, T.J. Watson Research Center
(h3 - c10)
P.O. Box 704

Yorktown Heights , NY 10598
USA

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

e-mail Adressen

Bauspieß, F.	bauspies@ira.uka.de
Beth, Th.	
Biham, E.	biham@cs.technion.ac.il
Brassard, G.	brassard@iro.umontreal.ca
Camion, P.	camion@seti.inria.fr
Damm, F.	damm@ira.uka.de
Dichtl, M.	
Diffie, W.	diffie@eng.sun.com
Girault, M.	girault@sept.fr
Jung, A.	XMATDB5R@ddathd21.bitnet
Matsumoto, T.	tsutomu@mlab.dnj.ynu.ac.jp
Preneel, B.	preneel@esat.kuleuven.ac.be
Quisquater, J.-J.	jjq@fai.ucl.ac.be
Schnorr, C.P.	schnorr@informatik.uni-frankfurt.de
Yung, M.	moti@watson.ibm.co