Основные достижения и тенденции развития теоретической криптологии в 2006 году

EUROCRYPT 2006

28.05-01.06

Санкт Петербург


The 25th International Cryptology Conference
EUROCRYPT 2006
28.05 - 01.06
ONGRESS HALL
КОНГРЕСС ЗАЛ
КОНГРЕСС ЗАЛ
CONGRESS HALL
CONGRESS-HALL "Pulkovskaya"
COSSACKS' SHOW
A. Mukienko


Vittel


• User
• User
• Mut


FBT


ВВЕДЕНИЕ
В КРИПТОСИСТЕМЫ
С ОТКРЫТЫМ КЛЮЧОМ

...URITY
...IN A NETWORKED WORLD

Bruce Schneier

...omputer Publishing
...Wiley & Sons, Inc.

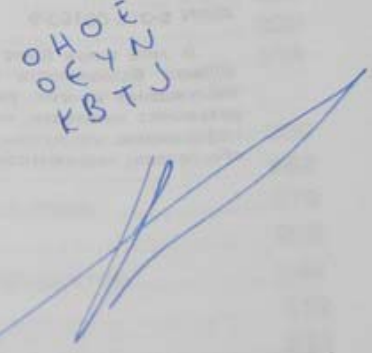
...einheim • Brisbane • Singapore • Toronto

КЛАССИКА COMPUTER SCIENCE

Б. ШНАЙЕР

СЕКРЕТЫ И ЛОЖЬ

БЕЗОПАСНОСТЬ ДАННЫХ В ЦИФРОВОМ МИРЕ



Москва · Санкт-Петербург · Нижний Новгород · Воронеж
Ростов-на-Дону · Екатеринбург · Самара
Киев · Харьков · Минск
2003


.05 - 01.06
Anatoly Lebedev
LAN Crypto
Russian Federation


VAIO


VAIO

CRYPTO 2006

21.08-24.08

SANTA BARBARA

SECOND CRYPTOGRAPHIC HASH WORKSHOP

AUGUST 24-25, 2006

UNIVERSITY OF CALIFORNIA, CORWIN PAVILION

SANTA BARBARA, CALIFORNIA

Proposed Timeline for the Development of New Hash Functions

Elaine Barker
NIST
ebarker@nist.gov
301-975-2911

Prior to a Competition

- **Aug. 2006 Second Hash Function Status and Research Workshop:**
  - Assess current status
  - Discuss hash function development strategy
  - Encourage further research.
- **2007 Third Hash Function Workshop 2007**
- **Decision**: NIST will decide whether or not to hold additional workshops on hash function research, especially on requirements and evaluation criteria, before initiating the competition.

Timeline for the Competition

Year 1 (2008?)

- 1Q: Draft and publish the minimum acceptability requirements, evaluation criteria, and submission requirements for public comments. Announce a public workshop to discuss these requirements.
- 2Q: Public comment period ends.
- 2Q: Host a workshop to discuss the requirements.
- 3Q: Finalize and publish the minimum acceptability requirements, evaluation criteria and submission requirements. Request submissions for new hash functions.

Year 2 (2009?)

- 2Q: Review submitted algorithms, and select candidates that meet basic submission requirements.
- 3Q: Host the First Hash Function Candidate Conference. Announce first round candidates.
- 3Q: Call for public comments on the first round candidates.

Year 3 (2010?)

- 1Q: Hold the Second Hash Function Candidate Conference. Discuss analysis results on the first round candidates.
- 2Q: Public comment period on the first round candidates ends.
- 3Q: Address public comments; select the second round finalists. Prepare a report to explain the selection.
- 3Q: Announce the second round finalists. Publish the selection report, and call for public comments on the second round candidates.

Year 4 (2011?)

- 2Q: Host the Third Hash Function Candidate Conference. Submitters of the second round finalists discuss comments on their algorithms.
- 2Q: Public comment period ends.
- 3Q: Address public comments, and select the finalist. Prepare a report to describe the final selection(s).
- 4Q: Announce the new hash function(s).

Year 5 (2012?)

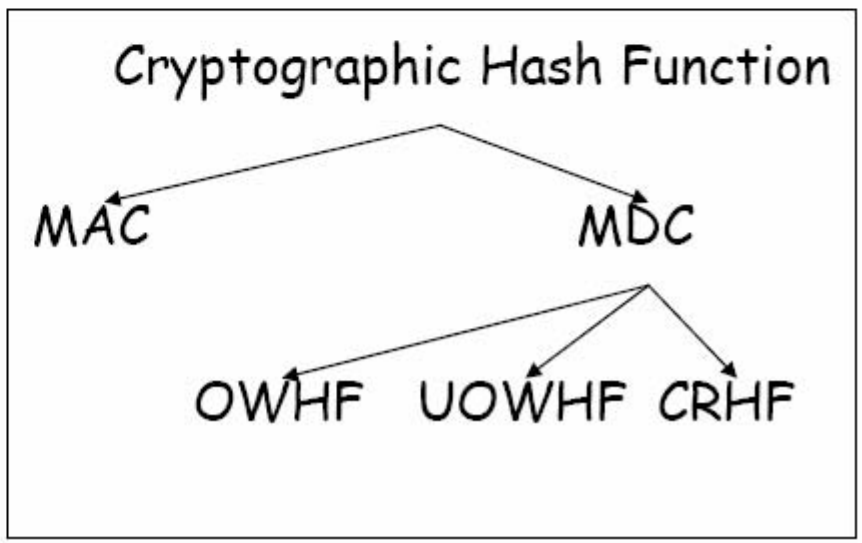
- 1Q: Publish a draft standard for public comments.
- 2Q: Public comment period ends.
- 3Q: Address public comments.
- 4Q: Publish the new hash function standard.

Classification of Hash Functions Suitable for Real-life Systems

Yasumasa Hirai (NTT DATA Corp.)
Takashi Kurokawa (NICT)
Shin'ichiro Matsuo (NTT DATA Corp.)
Hidema Tanaka (NICT)
Akihiro Yamamura (NICT)

Cryptographic Classification

- Cryptographic hash functions are classified into four categories
  - MAC (omit in this talk)
  - OWHF (omit in this talk)
  - CRHF
  - UOWHF



Collision Resistant Hash Function

- Hash function $h : \{0,1\}^* \rightarrow \{0,1\}^n$
- Computational cost to find x and x' s.t. $h(x) = h(x')$ is not smaller than $2^{n/2}$.
- There are efficient realizations:
  - Example: SHA-256/384/512, SHA-1(?)
- hard to prove their security
- widely used and hard to replace

Universal One-Way Hash Function

- Keyed hash function s.t.
  - Adversary choose x
  - For randomly chosen h_K , it is hard to find $y(\neq x)$ s.t. $h_K(x) = h_K(y)$.
- can construct provable secure signature scheme with UOWHF
- Few practical realizations.
  - Less efficient than CRHF (Performance, Key size)

Security of Hash in Real System

- Security requirements of real-system is decided by
  - Risk analysis method (ISMS, ISO15408)
  - Law, industrial standard.
  - Example:
    - Public key certificate must be valid from one to five years
    - Hash value in Cookie must be valid only in one session
    - Digital Signature must be valid for seven years (HIPPA)
- Requirements is represented as valid period.
- Standards for government use requests provable security for signature and encryption.

Quantitative Classification

Class	Period	Security Parameter(example)	Usages
Long-Term	Over 5 years	2^{128}	Certification Secure E-mail
Medium-Term	1 month - 5 years	2^{80}	PKI
Short-Term	Under 1 month	2^{64}	Secure Communication Authentication

Adding Rigorous Security

- Collision resistant is sufficient for most usages
- Some applications require rigorous security
  - Digital signatures for government PKI, time-stamping etc. must be provable secure scheme.
  - Hash functions for such signature scheme should aware provable security.

Hash standard should add provable secure hash class to conventional collision resistant hash class.

Qualitative classification

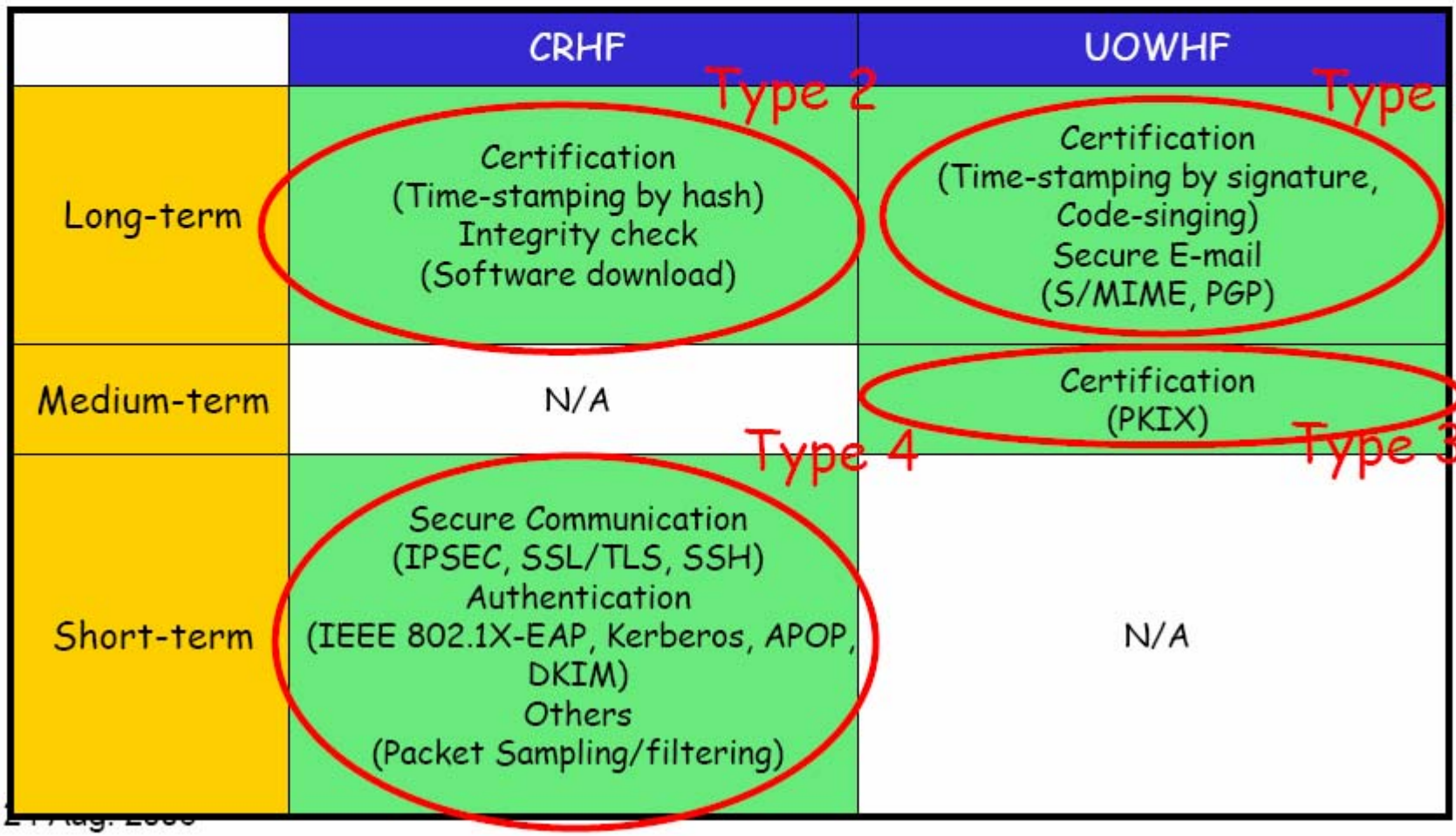
	CRHF	UOWHF
Key	No	Length grows with the message size
Adversary goal	Find $x, y \in D (x \neq y)$ s.t. $h(x) = h(y)$	Choose $x \in D$ Given $h_K \in H$ Find $y \in D (x \neq y)$ s.t. $h_K(x) = h_K(x')$
Compression function	Dedicated functions Block cipher based Arithmetic	Strongly universal functions
Construction methods	Markle-Damgaard Tree	XOR linear XOR tree Shoup (extended Markle-Damgaard)
Standard	ISO 10118-3	No

New classification

- To cover from cryptographic strong class to light weight and practically secure class…
  - New classification must contain quantitative index as well as qualitative index. (From short-term to long-term)
  - Qualitative index must cover strong class to light and practical security.
  - New classification will become 2 dimensional matrix.

4 types of hash functions

Future Standard for Hash function should consider…



eSTREAM - ECRYPT Stream Cipher project (2004 - 2008)

http://www.ecrypt.eu.org

eSTREAM

- ECRYPT Stream Cipher project

(2004 - 2008)

- 14-15.10.2004 – SASC - The State of the Art of Stream Ciphers (Bruges)
- 01.11.2004 – объявление о начале конкурса eSTREAM
- 29.04.2005 – Конец подачи документов на конкурс eSTREAM
- 26-27.05.2005 – SKEW - Symmetric Key Encryption Workshop
- 2-3.02.2006 – SASC 2006 (Leuven) – конец 1-й фазы конкурса
- 01.07.2006 – Начало 2-й фазы конкурса
- 31.01-1.02.2007 – SASC 2007 (Bochum)
- 01.2008 – Итоговый отчет ECRYPT Stream Cipher project

Call for Stream Cipher Primitives

- PROFILE 1. Stream ciphers for software applications with high throughput requirements. A key length of 128 bits must be accommodated. An IV length of at least one of 64 or 128 bits must be accommodated.

- PROFILE 2. Stream ciphers for hardware applications with restricted resources such as limited storage, gate count, or power consumption. A key length of 80 bits must be accommodated. An IV length of at least one of 32 or 64 bits must be accommodated.

Алгоритмы, представленные на конкурс eSTREAM

Профиль I

- ABC
- CryptMT/ Fubuki
- DICING
- DRAGON
- Frogbit A
- HC-256
- Mir-1
- Py
- Salsa20
- SOSEMANUK

Профиль I,II

- F-FCSR
- Hermes8
- LEX
- MAG
- NLS A
- Phelix A
- Polar Bear
- POMARANCH
- Rabbit
- SSS A
- TRBDK3 YAEA
- Yamb

Профиль II

- Achterbahn
- DECIM
- EDON-80
- Grain
- MICKEY
- MICKEY-128
- MOSQUITO
- SFINKS A
- Trivium
- TSC-3
- VEST A
- WG
- ZK-Crypt

Участники 2-й фазы конкурса eSTREAM по профилю I

Лидеры 2-й фазы по профилю I	Участники 2-й фазы по профилю I
DRAGON	ABC
HC-256	CryptMT
LEX	DICING
Phelix	NLS
Py	Polar Bear
Salsa20	Rabbit
SOSEMANUK	

Участники 2-й фазы конкурса eSTREAM по профилю II

Лидеры 2-й фазы по профилю II
Grain
MICKEY-128
Phelix
Trivium

Участники 2-й фазы конкурса eSTREAM по профилю II

Участники 2-й фазы по профилю II
Achterbahn
DECIM
Edon80
F-FCSR
Hermes8
LEX
MICKEY
MOUSTIQUE
NLS
Polar Bear
POMARANCH
Rabbit
Salsa20
TSC-4
VEST
WGZ
K-Crypt

Статистический анализ выходных последовательностей алгоритмов

- Выходные последовательности алгоритмов Decim, Frogbit, Polar Bear статистически отличимы от случайных.
- Выходные последовательности алгоритма Decim имеют корреляцию с ключом.
- Выходные последовательности алгоритмов Decim, F-FCRS-8, Frogbit, Mag, Zk-Crypt, полученные на одинаковых ключах и сходных IV коррелируют.
- Диффузионные слабости обнаружены у алгоритмов F-FCRS-8, Frogbit, Mag, Zk-Crypt.

Hongjun Wu and Bart Preneel

«*Distinguishing Attack on Stream Cipher Yamb*»

«It was shown in this paper that the keystream generated from Yamb can be distinguished from random with about $2^{57,8}$ outputs and with about $2^{54,8}$ simple operations.»

Исследование алгоритмов профиля I

- 2000MHz (one of two CPU cores) AMD Athlon 64 X2
- 533MHz (one of two CPUs) Motorola PowerPC G4 7410
- 1300MHz Intel Pentium M
- 900MHz AMD Athlon
- 440MHz (one of two CPUs) HP 9000/785 J5000
- 3000MHz Intel Pentium 4
- 1000MHz (one of two CPUs) Intel Pentium III
- 900MHz Sun UltraSPARC III
- 2800MHz (one of two CPUs) Intel Pentium 4
- 1900MHz Intel Pentium 4
- 400MHz DEC Alpha EV5.6 21164A
- 133MHz Intel Pentium

Скорость программной реализации поточных шифров профиля I с 256-битным ключом

Результаты приведены для Intel Pentium 4 3000MHz

Лидеры 2-й фазы

Участники 2-й фазы

AES

Шифрование большого объема данных

Алгоритм	Внутр. состояние (в битах)	Скорость (тактов на байт)
Py	4196	3.7
Py6	1124	3.8
HC-256	8396	5.0
Phelix	132	5.6
SOSEMANUK	452	5.7
Dragon	284	12.3
Salsa20	64	13.9
DICING	4396	14.7
Crypt MT	3020	16.1
YAMB	424	16.5
AES	260	33.1

Установка ключа и шифрование 40-байтного пакета

Алгоритм	Внутр. состояние (в битах)	Скорость (тактов на байт)
Phelix	132	33.5
Salsa20	64	44.9
AES	260	51.6
SOSEMANUK	452	64.2
Dragon	284	88.4
Py6	1124	117.3
Py	4196	320.6
DICING	4396	416.2
Crypt MT	3020	1066.9
YAMB	424	1227.6
HC-256	8396	2429.0

Скорость аппаратной реализации поточных шифров профиля II

Лидеры 2-й фазы

Участники 2-й фазы

AES

Аппаратная реализация AES-128 (технология ASIC)

Архитектура	8-bit	32-bit	64-bit	128-bit
Число S-блоков	1	4	8	20
Число тактов на 1 блок	1,032	54	32	11
Скорость [битов за такт]	0,12	2,37	4,00	11,64
Тактовая частота [MHz]	80	131	137	145
Скорость [Mbps]	9,9	311	548	1.691

Аппаратная реализация AES-128 (технология FPGA)

Архитектура	8-bit	32-bit
Число S-блоков	1	4
FPGA	Xilinx Spartan II XC2S15-6	Xilinx Spartan II XC2S30-6
Тактовая частота [MHz]	67	60
Скорость [Mbps]	2.2	69

Аппаратная реализация поточных шифров профиля 2

Алгоритм	Площ. (μm^2)	Тактовая частота [MHz]	Скорость [битов за такт]	Скорость [Gbit/s]	Эффект. (Gbit/ s_mm^2)	Эффект. в сравнении с AES
Trivium	144,128	312	64	18.57	128.83	68.30
ZK-Crypt	142,007	203	32	6.06	42.66	22.61
Grain	119,821	300	16	4.48	37.35	19.79
VEST	393,000	286	16	4.26	10.83	5.74
MICKEY	82,328	308	1	0.29	3.48	1.85
SFINKS+	361,643	167	8	1.24	3.43	1.82
MOSQUITO	306,907	265	3	0.74	2.41	1.27
Achterbahn	227,763	250	2	0.47	2.04	1.08
AES (OFB)	280.098	182	3.12	0.53	1.89	1.00