One-way Functions against a Quantum Computer

Claude Crépeau

School of Computer Science
McGill University
(0)
Open Questions...
One-way Functions
Computational Security

PAST | PRESENT | FUTURE

resists foreseeable technology

© Claude Crépeau 2002-2008
Computational Security

PAST  PRESENT  FUTURE

resists arbitrary algorithms
Computational Assumption

Unfortunately we have no proof of security...
**Definition:** A collection of functions \( \{f_n : D_n \to \{0,1\}^{k(n)}\} \) is called **strongly one-way** under the following two conditions

- there exists a poly-time algorithm \( F \) that, on input \( x \in D_n \), always outputs \( f_n(x) \).

- for every probabilistic poly-time (Quantum) algorithm \( A \), every \( c>0 \) and all sufficiently large \( n \)

\[
\Pr[ A(F(X_n)) \in F^{-1}(F(X_n)) ] < \frac{1}{n^c}
\]

where \( X_n \) is uniformly distributed over \( D_n \).
Shor’s factoring/DL algorithm

F F(→→→→→→→)

© Claude Crépeau 2002-2008
Shor’s factoring/DL algorithm

- **RSA**: discret root extraction
- **ElGamal**: discret log
- **Menezes-Vanstone**: elliptic curves
- **Blum-Goldwasser**: factoring
- **Paillier**: DL + DR

...
(2) Candidate One-way Function (Quantum Resistant)
CODING

\{0,1\}^k \rightarrow \{0,1\}^n

DECODING

\text{M}x = y = 0^{n-k}

\text{[n,k,d] linear code}

M \in \{0,1\}^{(n-k) \cdot n} \text{ is a Parity Check matrix}

C = \{ x \mid Mx = 0^{n-k} \}
CODING

DETECTION

Mz \neq 0^{n-k}

DECODING

CORRECTION

Syndrome Decoding Problem

\ge d
 Syndrome Decoding Problem

**Instance:** PC matrix $M \in \{0,1\}^{(n-k) \times n}$, syndrome $y \in \{0,1\}^{n-k}$, weight $w \leq n$

**Problem:** is there a word $x \in \{0,1\}^n$, $|x| \leq w$ s.t. $Mx = y$? 
CORRECTING$(M,z) \leq\text{ Syndrome Decoding Problem } (M, w=(d-1)/2, y=Mz)$

Instance: PC matrix $M \in \{0,1\}^{(n-k) \times n}$, $y=Mz \in \{0,1\}^{n-k}$, $w=(d-1)/2$

Problem: is there a word $x \in \{0,1\}^n$, $|x| \leq w$ s.t. $Mx = y$?

CORRECTING$(M,z) = z(+)x$
**Definition:** Let $\rho \in ]0,1[; \text{ let } w \text{ and } w' \text{ be integer functions such that } w(n) \leq w'(n) \leq n$. The $SD(n, w, w')$ collection is the set of functions $\{f_n\}$ such that

$$D_n = \{(M, x) : M \in \{0,1\}^{\lfloor \rho n \rfloor \cdot n}, x \in \{0,1\}^n \text{ s.t. } w(n) \leq |x| \leq w'(n)\}$$

$$f_n : D_n \rightarrow \{0,1\}^{\lfloor \rho n \rfloor \cdot (n+1)}$$

$$(M, x) \rightarrow (M, Mx)$$

**Assumption 1:** Let $\rho \in ]0,1[; \text{ let } \delta < 1/2 \text{ be such that } \rho = H_2(\delta)$. Then for any positive real $\varepsilon$, if we set $w(n) = \lfloor \delta n/(1+\varepsilon) \rfloor$ and $w'(n) = \lfloor \delta n \rfloor$, the $SD(\rho, w, w')$ collection is strongly one-way.
**Definition:** Let \( \rho \in ]0,1[; \) let \( w \) and \( w' \) be integer functions such that \( w(n) \leq w'(n) \leq n \). The \( SD(n,w,w') \) collection is the set of functions \( \{f_n\} \) such that

\[
D_n = \{(M,x) : M \in \{0,1\}^{[\rho n] \cdot n}, \ x \in \{0,1\}^n \ \text{s.t.} \ w(n) \leq |x| \leq w'(n)\}
\]

\[
f_n : D_n \to \{0,1\}^{([\rho n]+1) \cdot n}
\]

\[
(M,x) \to (M,Mx)
\]

**Assumption 2:** Let \( \rho \in ]0,1[; \) let \( \delta < 1/2 \) be such that \( \rho > H_2(\delta) \). Then the \( SD(\rho,\delta n,\delta n) \) collection is strongly one-way.
\[ [n, \rho n, \delta n] \text{ linear code} \]

For fixed \( \rho = 1/2 \)

<table>
<thead>
<tr>
<th>( n )</th>
<th>512</th>
<th>512</th>
<th>512</th>
<th>728</th>
<th>728</th>
<th>1024</th>
<th>1024</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \delta n )</td>
<td>56</td>
<td>55</td>
<td>50</td>
<td>78</td>
<td>71</td>
<td>110</td>
<td>100</td>
</tr>
</tbody>
</table>
(3) Applications of One-Way Functions
A PSEUDORANDOM GENERATOR FROM ANY ONE-WAY FUNCTION

JOHAN HÅSTAD†, RUSSELL IMPAGLIAZZO‡, LEONID A. LEVIN§,
AND MICHAEL LUBY¶

Abstract. Pseudorandom generators are fundamental to many theoretical and applied aspects of computing. We show how to construct a pseudorandom generator from any one-way function. Since it is easy to construct a one-way function from a pseudorandom generator, this result shows that there is a pseudorandom generator if and only if there is a one-way function.

OWF –> PRBG
symmetric encryption

Information Theoretical Security

encryption

decryption

P

K

C
Stream-cipher from PRBG

pseudo-key \oplus \text{cleartext} = \text{ciphertext}

ciphertext \oplus \text{pseudo-key} = \text{cleartext}
symmetric authentication

M  K  T

authentication

verification

Information Theoretical Security
One-Time-Authentication from PRBG

pseudo-key \times \text{message} \oplus \text{tag} = \text{tag} \oplus \text{message} \times \text{pseudo-key}

© Claude Crépeau 2002-2008
Universal One-Way Hash Functions and their Cryptographic Applications *

Momi Naor† Moti Yung‡

Revised March 13, 1995

Abstract

We define a *Universal One-Way Hash Function* family, a new primitive which enables the compression of elements in the function domain. The main property of this primitive is that given an element $x$ in the domain, it is computationally hard to find a different domain element which collides with $x$. We prove constructively that universal one-way hash functions exist if any 1-1 one-way functions exist.

Among the various applications of the primitive is a *One-Way based Secure Digital Signature* Scheme which is existentially secure against adoptive attacks. Previously, all provably secure signature schemes were based on the stronger mathematical assumption that *trapdoor* one-way functions exist.

**UOWHF--→DS**
asymmetric authentication
(digital signature schemes)

authentication

\[ K_a \quad K_v \]

M \quad T

\{ACCEPT, REJECT\}

verification

Complexity Theoretical Security
Let \( \{n_1,\} \) and \( \{n_0,\} \) be two increasing sequences such that for all \( i \) \( n_0, \leq n_1, \), but \( \exists q, \) a polynomial, such that \( q(n_0,) \geq n_1, \) (we say that these sequences are polynomially related). Let \( H_k, \) be a collection of functions such that for all \( h \in H_k, \) \( h : \{0,1\}^{n_1,k} \rightarrow \{0,1\}^{n_0,k} \) and let \( U = \bigcup H_k. \) Let \( A, \) be a probabilistic polynomial time algorithm (\( A \) is a \textit{collision adversary}) that on input \( k \) outputs \( x \in \{0,1\}^{n_1,k} \) which we call an \textit{initial value}, then given a random \( h \in H_k, \) attempts to find \( y \in \{0,1\}^{n_1,k} \) such that \( h(x) = h(y) \) but \( x \neq y. \) In other words, after getting a hash function it tries to find a collision with the initial value.

**Definition:** Such a \( U \) is called a \textit{family of universal one-way hash functions} if for all polynomials \( p \) and for all polynomial time probabilistic algorithms \( A \) the following holds for sufficiently large \( k. \)

1. If \( x \in \{0,1\}^{n_1,k} \) is \( A \)'s initial value, then \( \text{Prob}[A(h,x) = y, h(x) = h(y), y \neq x] < 1/p(n_1,k) \) where the probability is taken over all \( h \in H_k \) and the random choices of \( A. \)

2. \( \forall h \in H_k \) there is a description of \( h, \) of length polynomial in \( n_1,k, \) such that given \( h \)'s description and \( x, \) \( h(x) \) is computable in polynomial time.

3. \( H_k \) is accessible: there exists an algorithm \( G \) such that \( G \) on input \( k \) generates uniformly at random a description of \( h \in H_k. \)
1990

One-Way Functions are Necessary and Sufficient for Secure Signatures

John Rompel*

Laboratory for Computer Science
Massachusetts Institute of Technology
Cambridge, MA 02139

1 Introduction

Much research in theoretical cryptography has been centered around finding the weakest possible cryptographic assumptions required to implement major primitives. Ever since Diffie and Hellman first suggested that modern cryptography be based on one-way functions (which are easy to compute, but hard to invert) and trapdoor functions (one-way functions which are, however, easy to invert given an associated secret), researchers have

OWF $\rightarrow$ UOWHF*
On Constructing Universal One-Way Hash Functions from Arbitrary One-Way Functions

Jonathan Katz*  Chiu-Yuen Koo*

Abstract

A fundamental result in cryptography is that a digital signature scheme can be constructed from an arbitrary one-way function. A proof of this somewhat surprising statement follows from two results: first, Naor and Yung defined the notion of universal one-way hash functions and showed that the existence of such hash functions implies the existence of secure digital signature schemes. Subsequently, Rompel showed that universal one-way hash functions could be constructed from arbitrary one-way functions. Unfortunately, despite the importance of the result, a complete proof of the latter claim has never been published. In fact, a careful reading of Rompel's original conference publication reveals a number of errors in many of his arguments which have (seemingly) never been addressed.

We provide here what is — as far as we know — the first complete write-up of Rompel's proof that universal one-way hash functions can be constructed from arbitrary one-way functions.

OWF→UOWHF
1988/1991


Journal of Cryptology
© 1991 International Association for Cryptologic Research

Bit Commitment Using Pseudorandomness

Moni Naor
IBM Almaden Research Center, 650 Harry Road,
San Jose, CA 95120, U.S.A.

Abstract. We show how a pseudorandom generator can provide a bit-commitment protocol. We also analyze the number of bits communicated when parties commit to many bits simultaneously, and show that the assumption of the existence of pseudorandom generators suffices to assure amortized $O(1)$ bits of communication per bit commitment.

Key words. Cryptographic protocols, Pseudorandomness, Zero-knowledge proof systems.

PRBG $\rightarrow$ BC
BIT COMMITMENT

COMMIT

UNVEIL

b, 29 - 41 - 02 - 17
BIT COMMITMENT

CONCEALING

BINDING

−b, 39 - 21 - 12 - 27
BIT COMMITMENT

COMMIT Computationally CONCEALING

UNVEIL Statistically BINDING

b, 29 - 41 - 02 - 17
Zero Knowledge with Efficient Provers

Minh-Huyen Nguyen
Harvard University
Division of Engineering and Applied Sciences
Cambridge, MA 02138, USA
mnguyen@eecs.harvard.edu

Salil Vadhan
Harvard University
Division of Engineering and Applied Sciences
Cambridge, MA 02138, USA
salil@eecs.harvard.edu

ABSTRACT
We prove that every problem in NP that has a zero-knowledge proof also has a zero-knowledge proof where the prover can be implemented in probabilistic polynomial time given an NP witness. Moreover, if the original proof system is statistical zero knowledge, so is the resulting efficient-prover proof system. An equivalence of zero knowledge and efficient-prover zero knowledge was previously known only under the assumption that one-way functions exist (whereas our result is unconditional), and no such equivalence was known for statistical zero knowledge. Our results allow us to translate the many general results and characterizations known for zero knowledge with inefficient provers to zero knowledge with efficient provers.

Categories and Subject Descriptors
F.1.2 [Modes of Computation]: Interactive and reactive computation

General Terms

1. INTRODUCTION
Zero-knowledge proofs [18] have been one of the most fertile sources of interaction between cryptography and complexity theory. From the perspective of cryptography, zero-knowledge proofs provide a powerful building block for secure protocols and serve as a good testbed for understanding new security concerns such as concurrency and compositability. From a complexity point of view, zero knowledge enriches the classical study of NP proofs with randomness, interaction, and secrecy, and provides an interesting classification of computational problems.

In the past decade, this interaction has yielded a number of very general results about zero-knowledge proofs. These include natural complete problems (or similar characterizations), closure properties, equivalence of private coins and public coins, equivalence of honest-verifier and malicious-verifier zero knowledge, and more. Results of this form were first obtained for the class SZK of problems having "statistical" zero-knowledge proofs [28, 31, 15, 17, 32], and were recently extended to the class ZK of problems having general, "computational" zero-knowledge proofs [34].

OWF \rightarrow 1/2-BC
DEFINITION 2.1. A 2-phase commitment scheme $(S, R)$ consists of four interactive protocols:

- $(S_1^L, R_1^L)$ the first commitment phase
- $(S_1^R, R_1^R)$ the first reveal phase
- $(S_2^L, R_2^L)$ the second commitment phase
- $(S_2^R, R_2^R)$ the second reveal phase

1. In the first commitment phase, $S_1^L$ receives a private input $\sigma^1 \in \{0, 1\}$ and a sequence of coin tosses $rs^5$. $S_1^L$ and $R_1^L$ receive as common output a commitment $z^1$ (without loss of generality, we can assume that $z^1$ is the transcript of the first commitment phase).

2. In the first reveal phase, $S_1^R$ and $R_1^R$ receive as common input the commitment $z^1$ and a bit $\sigma^1$. $S_1^R$ receives as private input $rs$. $S_1^R$ and $R_1^R$ receive a common output $\tau$. (Without loss of generality, we can assume that $\tau$ is the transcript of the first commitment phase and the first reveal phase and includes $R_1^R$'s decision to accept or reject).

3. In the second commitment phase, $S_2^L$ and $R_2^L$ receive the common input $\tau \in \{0, 1\}^*$ (where $\tau$ denotes the common output of the first reveal phase). $S_2^L$ receives a private input $\sigma^2 \in \{0, 1\}$ and the coin tosses $rs$. $S_2^L$ and $R_2^L$ receive as common output a commitment $z^2$ (without loss of generality, we can assume that $z^2$ is the concatenation of $\tau$ and the transcript of the second commitment phase).

4. In the second reveal phase, $S_2^R$ and $R_2^R$ receive as common input the commitment $z^2$ and a bit $\sigma^2$. $S_2^R$ receives as private input $rs$. At the end of the protocol, $R_2^R$ accepts or rejects.

5. $S = (S_1^L, S_1^R, S_2^L, S_2^R)$ and $R = (R_1^L, R_1^R, R_2^L, R_2^R)$ are computable in probabilistic polynomial time $\text{poly}(n)$ (where $1^n$ is the security parameter).
Statistically-Hiding Commitment from Any One-Way Function

Iftach Haitner*  Omer Reingold†

Abstract

We give a construction of statistically-hiding commitment schemes (ones where the hiding property holds information theoretically), based on the minimal cryptographic assumption that one-way functions exist. Our construction employs two-phase commitment schemes, recently constructed by Nguyen, Ong and Vadhan (FOCS '06), and universal one-way hash functions introduced and constructed by Naor and Yung (STOC '89) and Rompel (STOC '90).

\[
1/2 - \text{BC} + \text{UOWHF} \rightarrow \text{BC}
\]
BIT COMMITMENT

COMMIT

Perfectly CONCEALING

UNVEIL

Computationally BENDING

b, 29 - 41 - 02 - 17
Proving all these results in a quantum setting is still open...
Conclusions
• One-way functions theory has to be reconsidered in the context of quantum computers.

• Get to a blackboard and do it!
One-way Functions against a Quantum Computer

Claude Crépeau

School of Computer Science
McGill University