One-way Functions against a Quantum Computer

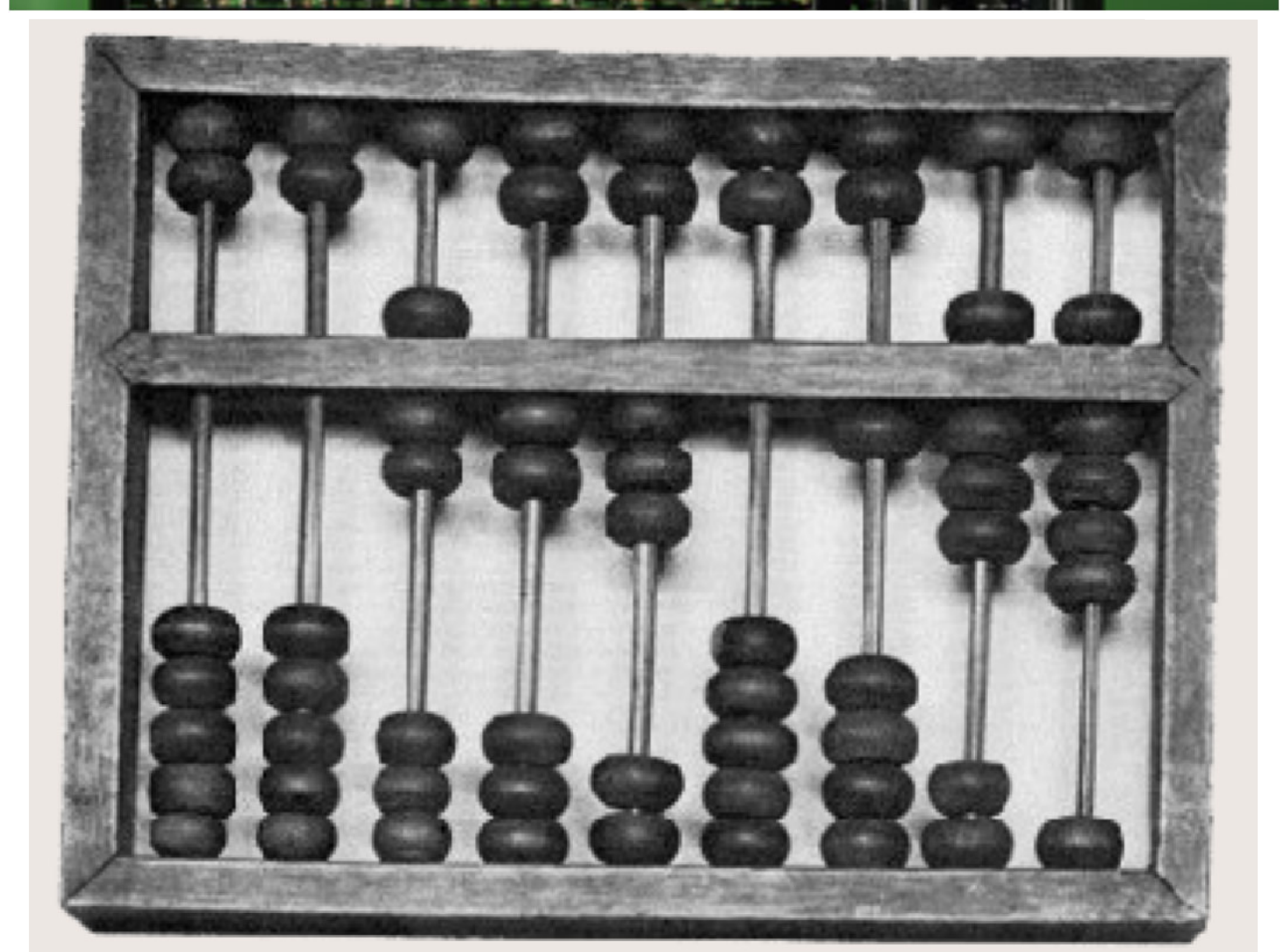
Claude Crépeau

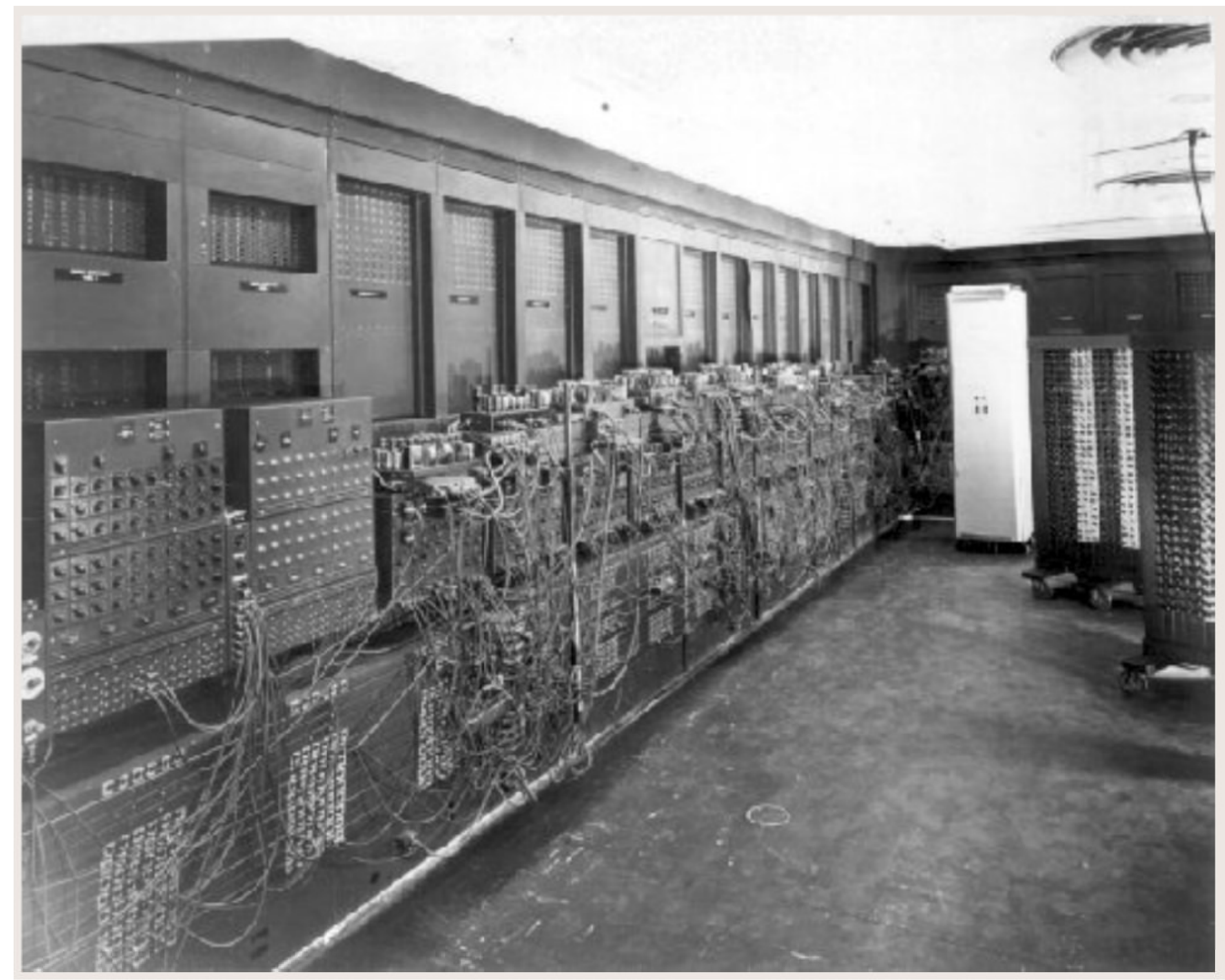
School of Computer Science
McGill University

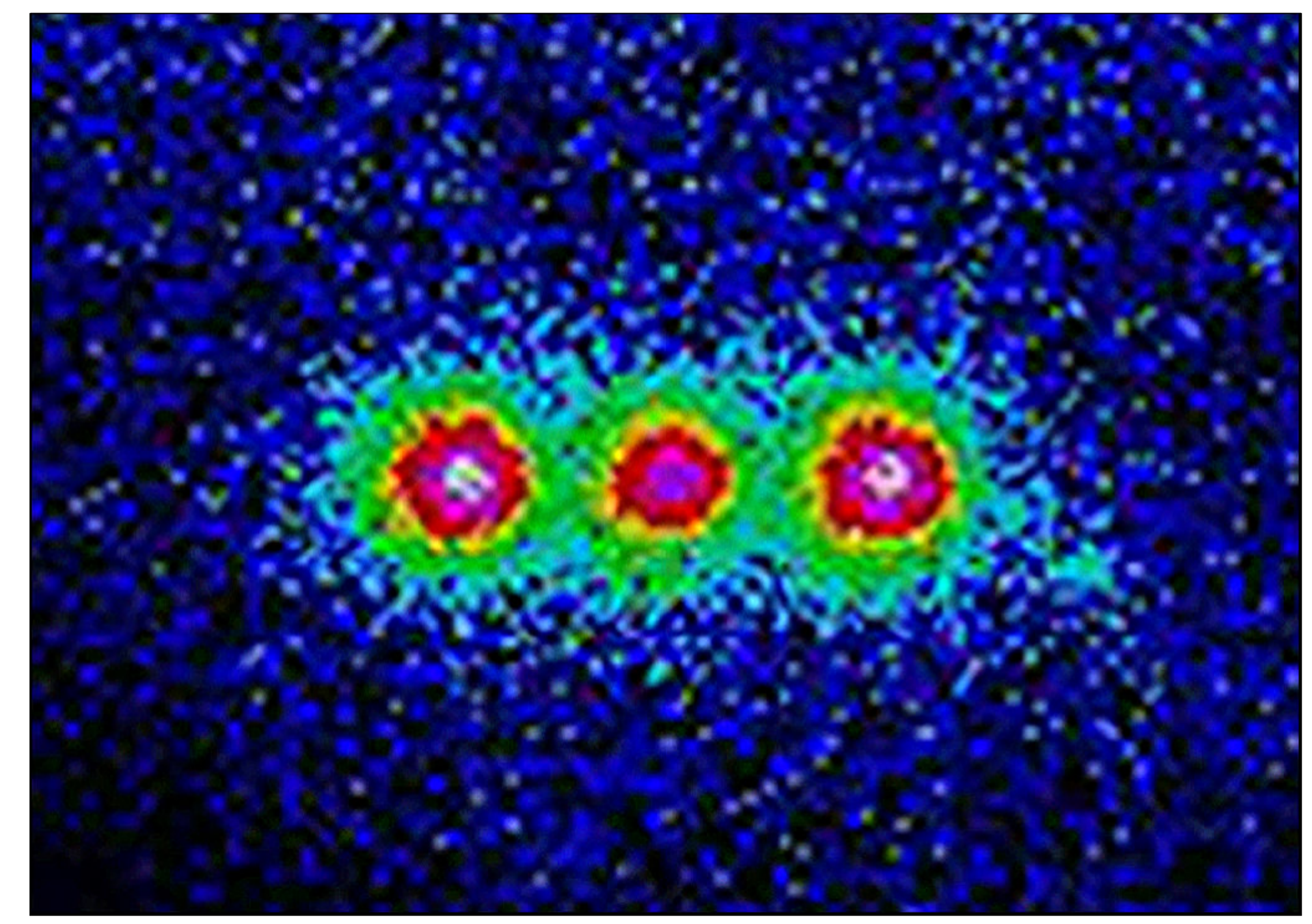
(0) Open Questions...

(1)
One-way Functions

Computational Security



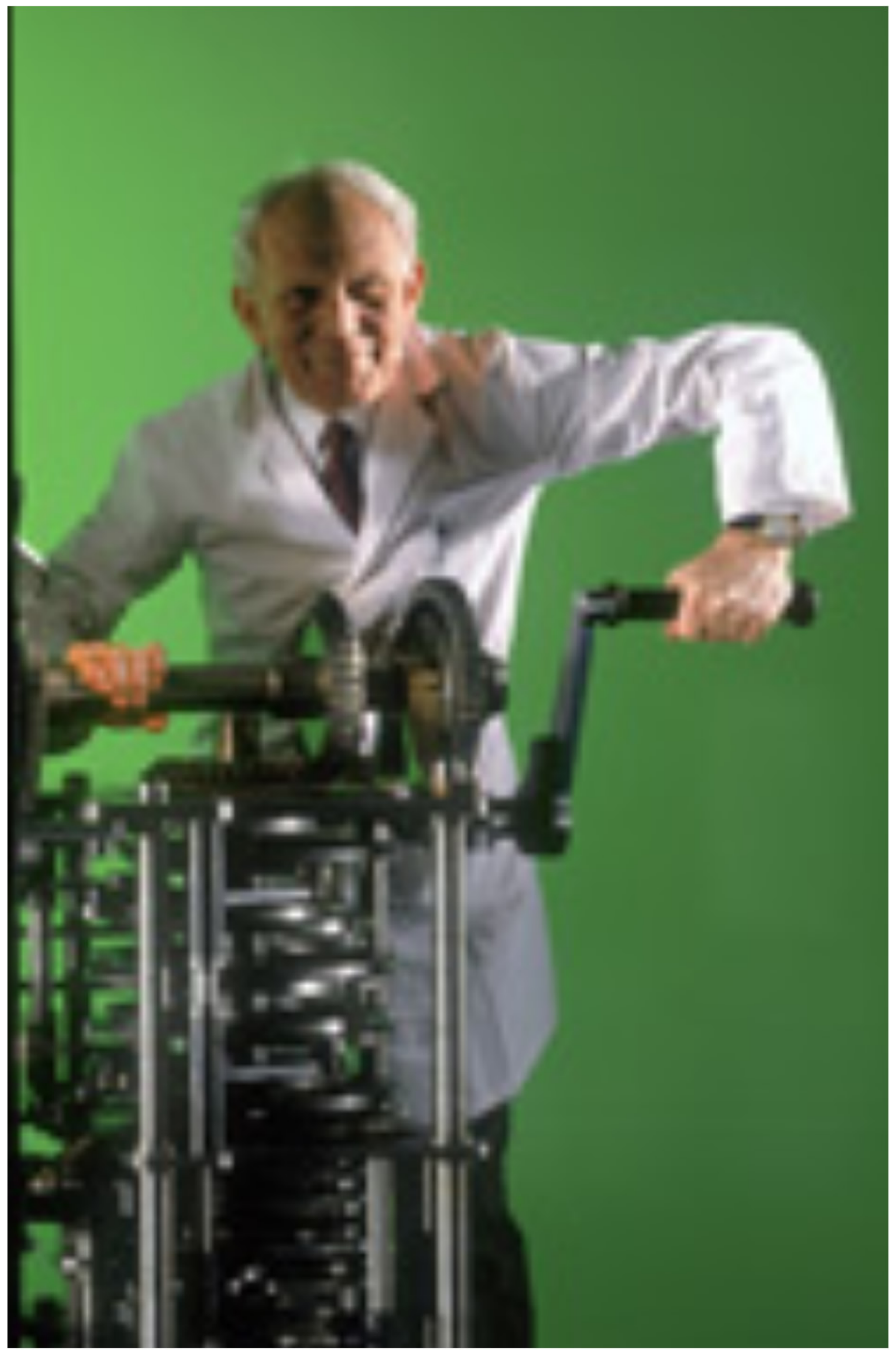




PAST **PRESENT** **FUTURE**

resists forseeable technology

Computational Security



PAST PRESENT FUTURE

resists arbitrary algorithms

Computational Assumption

Unfortunately
we have
no proof
of security...

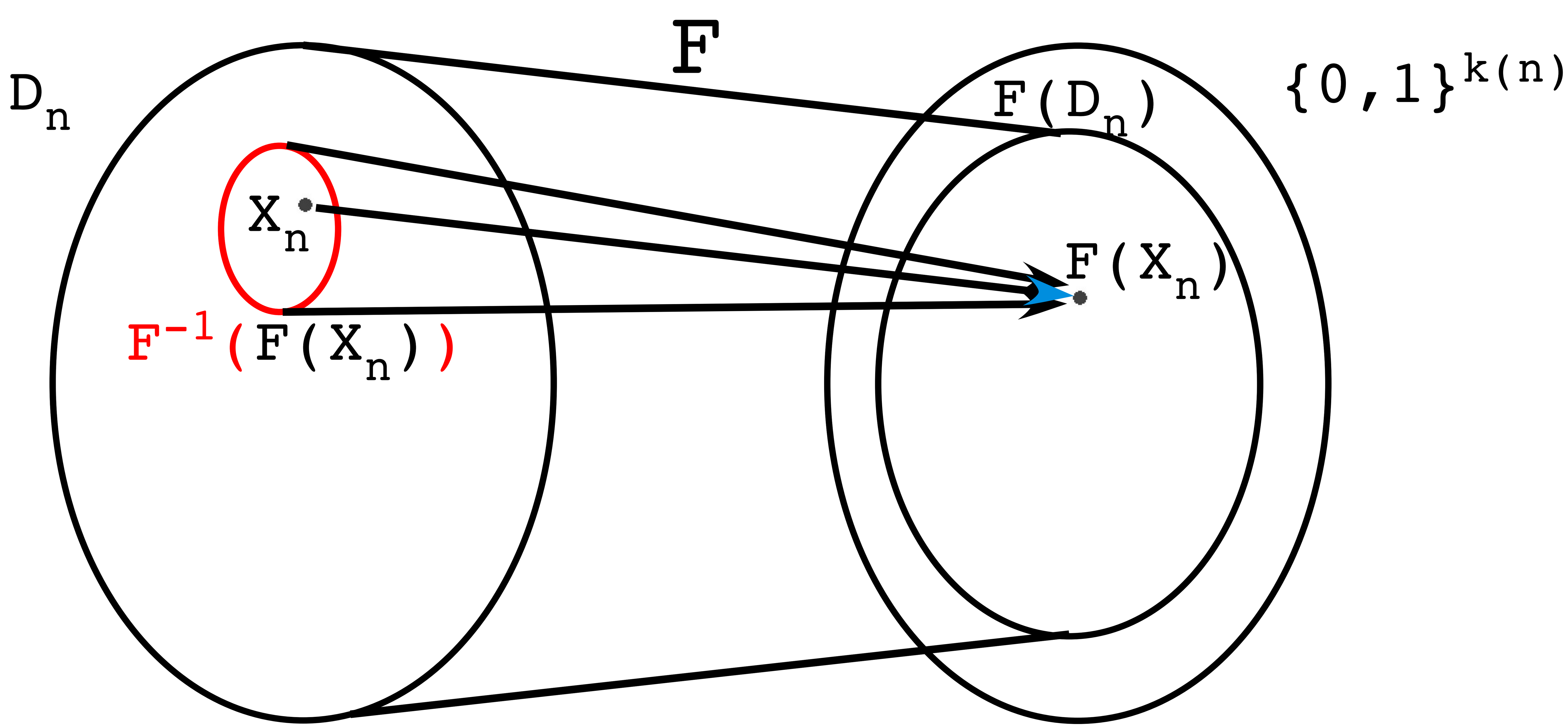
Definition: A collection of functions $\{f_n: D_n \dashrightarrow \{0,1\}^{k(n)}\}$ is called ***strongly one-way*** under the following two conditions

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

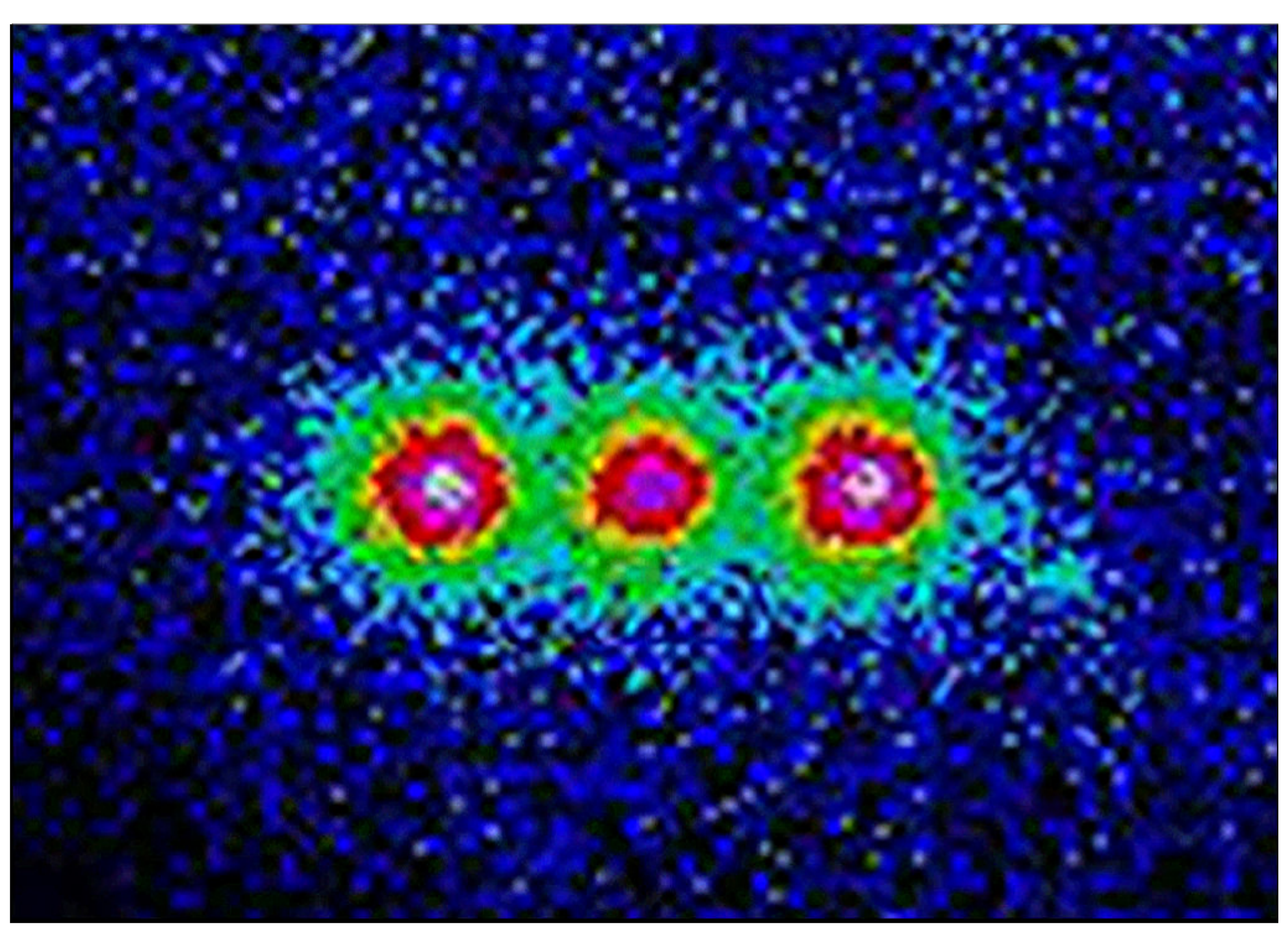
- for every probabilistic poly-time (Quantum) algorith A, every c>0 and all sufficiently large n

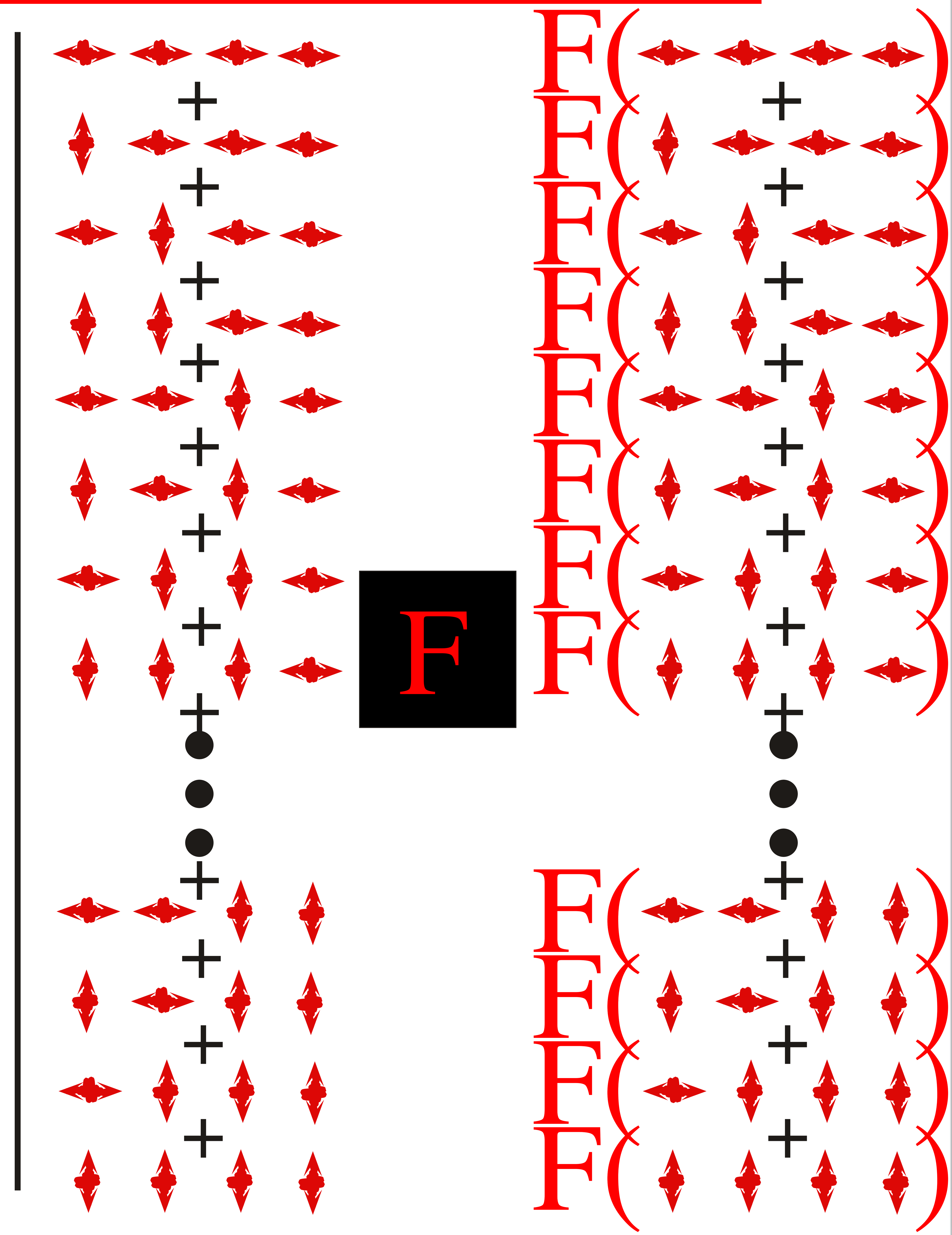
$$\mathbf{Pr}[\ A(F(X_n)) \in F^{-1}(F(X_n))\ ] < 1/n^c$$

where X_n is uniformely distributed over D_n.



Shor's factoring/DL algorithm



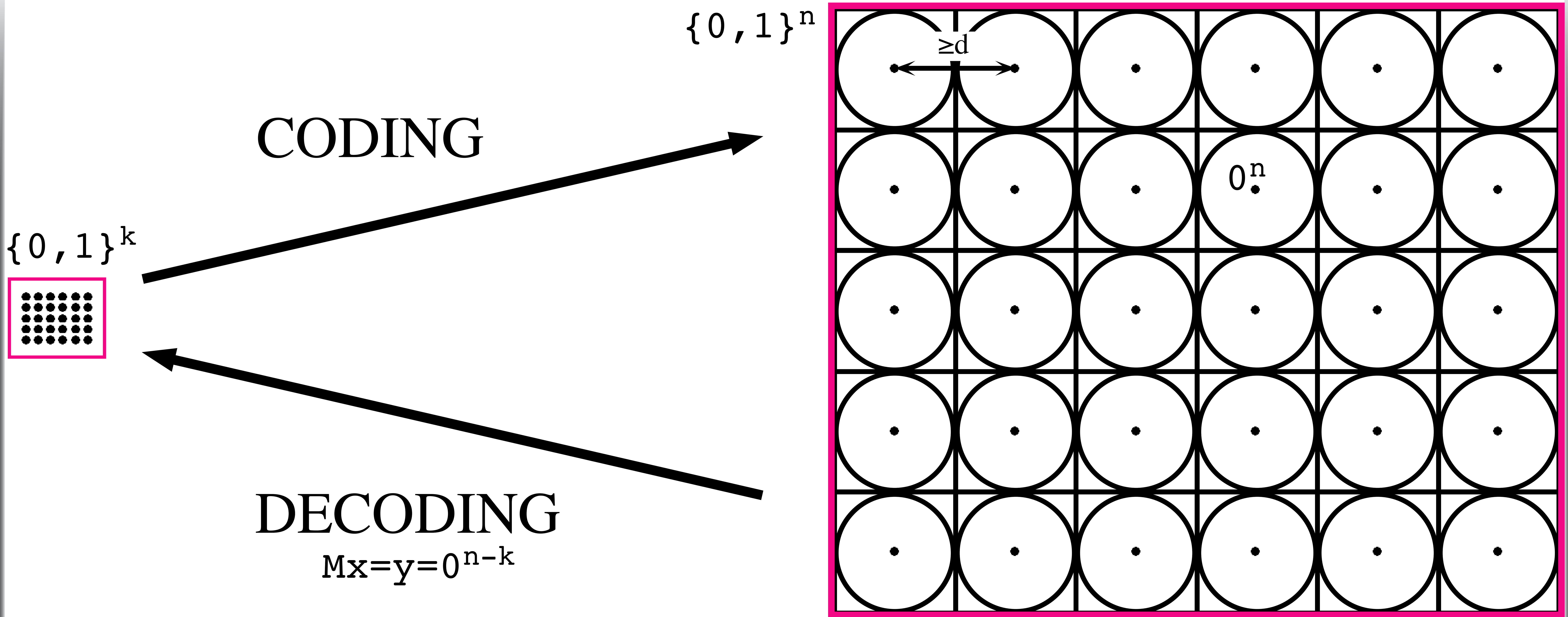


Shor's factoring/DL algorithm

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

. . .

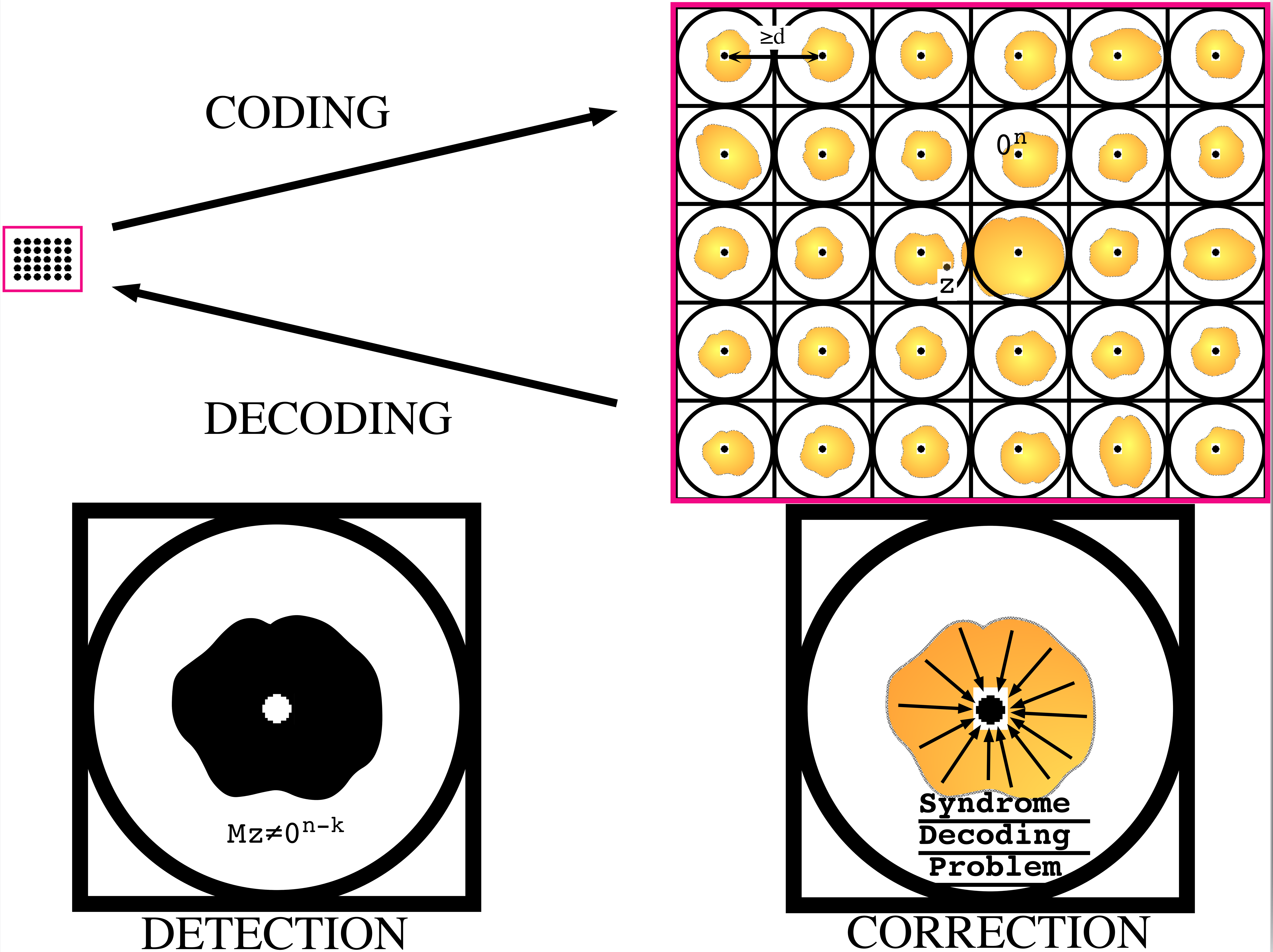
(2) Candidate One-way Function (Quantum Resistant)

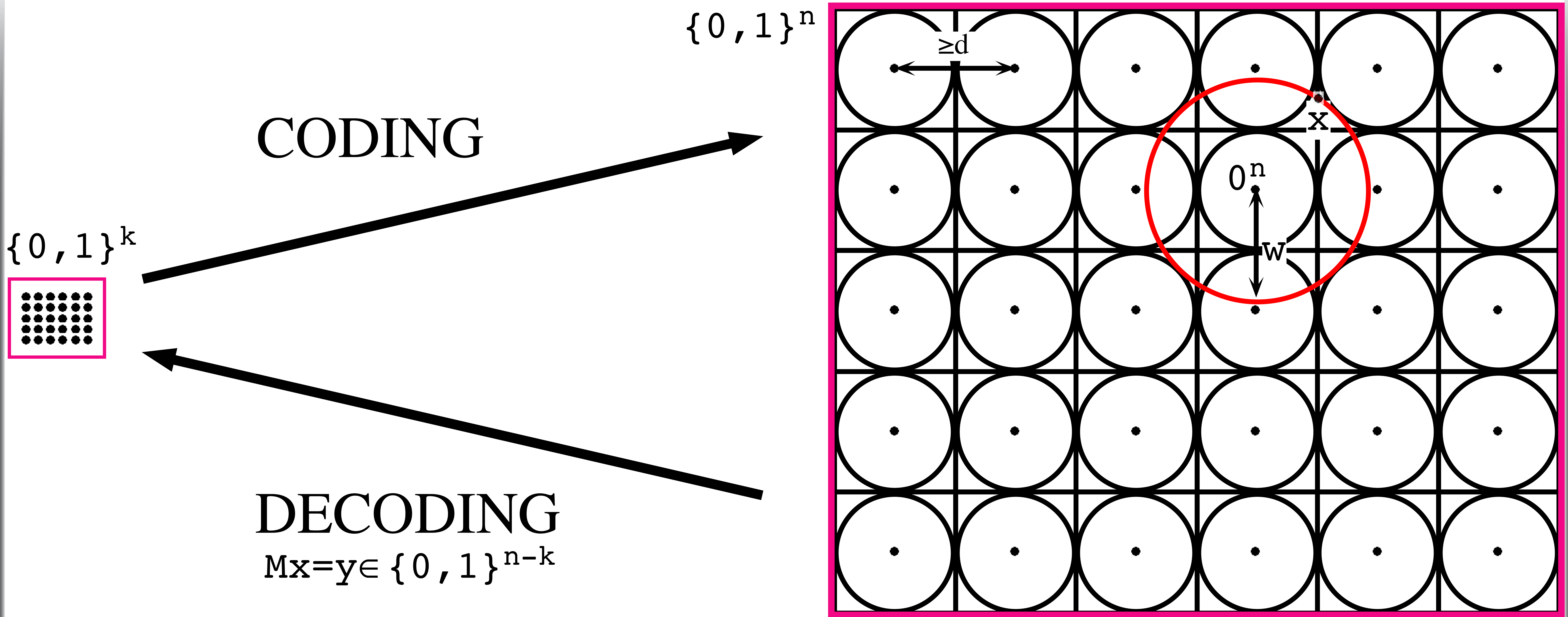


[n,k,d] linear code

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

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

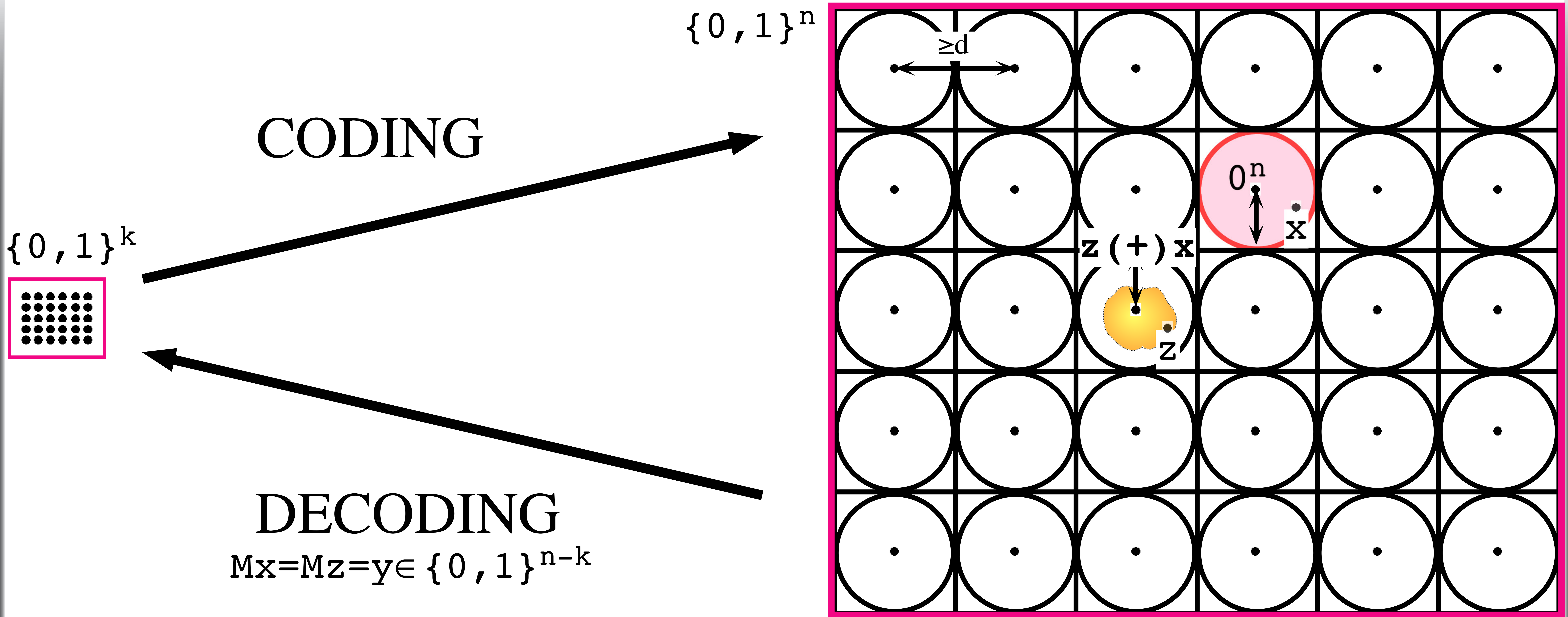

CODING
DECODING
≥d
0n
z
Mz≠0n-k
Syndrome
Decoding
Problem
DETECTION
CORRECTION



Syndrome Decoding Problem

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

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

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

CORRECTING(M,z) = z(+)x

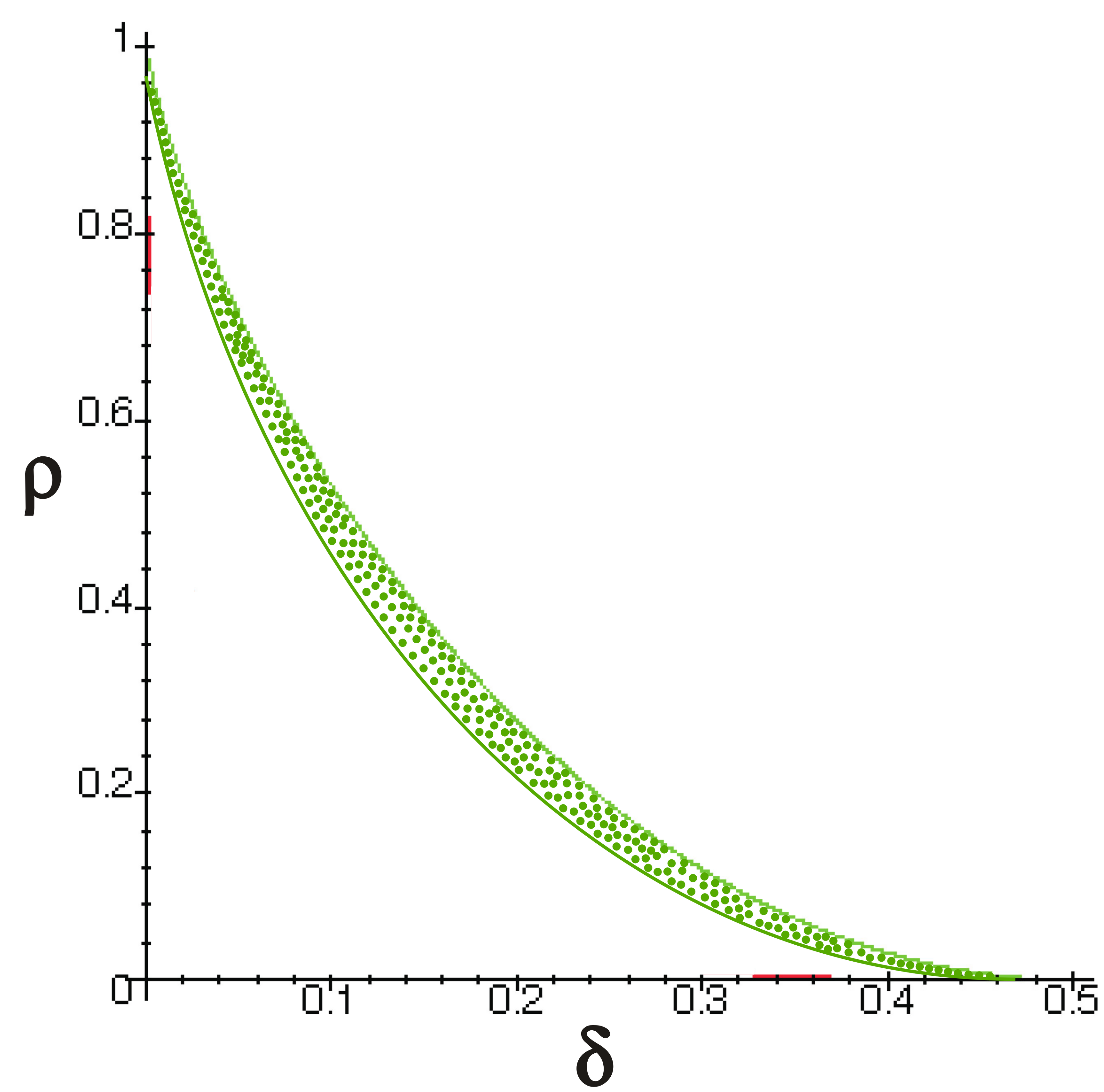
Definition: Let $\rho \in]0,1[$; let w and w' be integer functions such that $w(n) \leq w'(n) \leq n$. The SD(n,w,w') collection is the set of functions $\{f_n\}$ such that

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

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

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

Assumption 1: Let $\rho \in]0,1[$; let $\delta<1/2$ be such that $\rho=H_2(\delta)$. Then for any positive real ε, if we set $w(n)=[\delta n/(1+\varepsilon)]$ and $w'(n)=[\delta n]$, the SD(ρ,w,w') collection is strongly one-way.

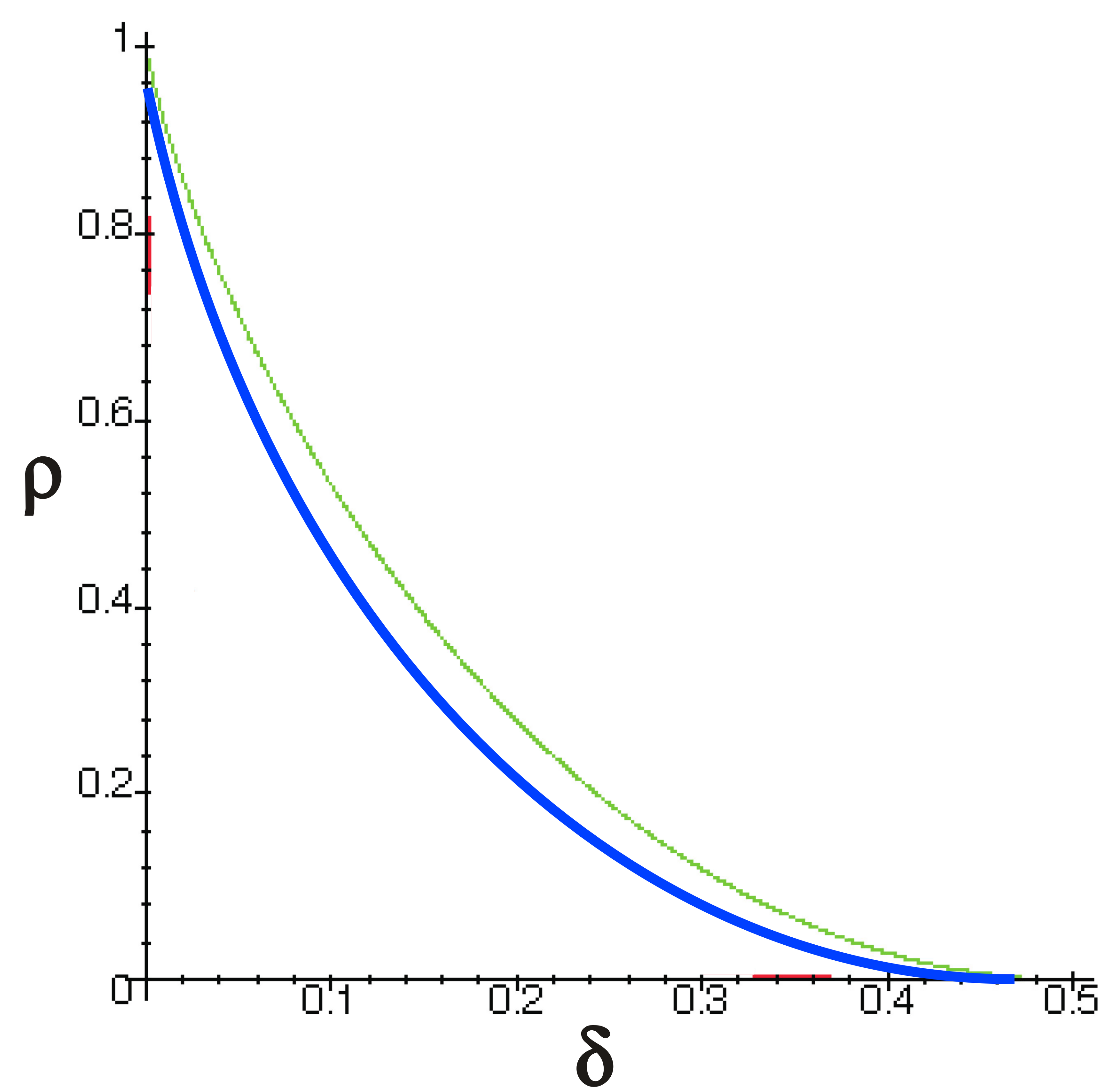


Definition: Let $\rho \in]0,1[$; let w and w' be integer functions such that $w(n) \leq w'(n) \leq n$. The SD(n,w,w') collection is the set of functions $\{f_n\}$ such that

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

$$f_n : D_n \longrightarrow \{0,1\}^{([\rho n]+1)\cdot n}$$
$$(M,x) \longrightarrow (M,Mx)$$

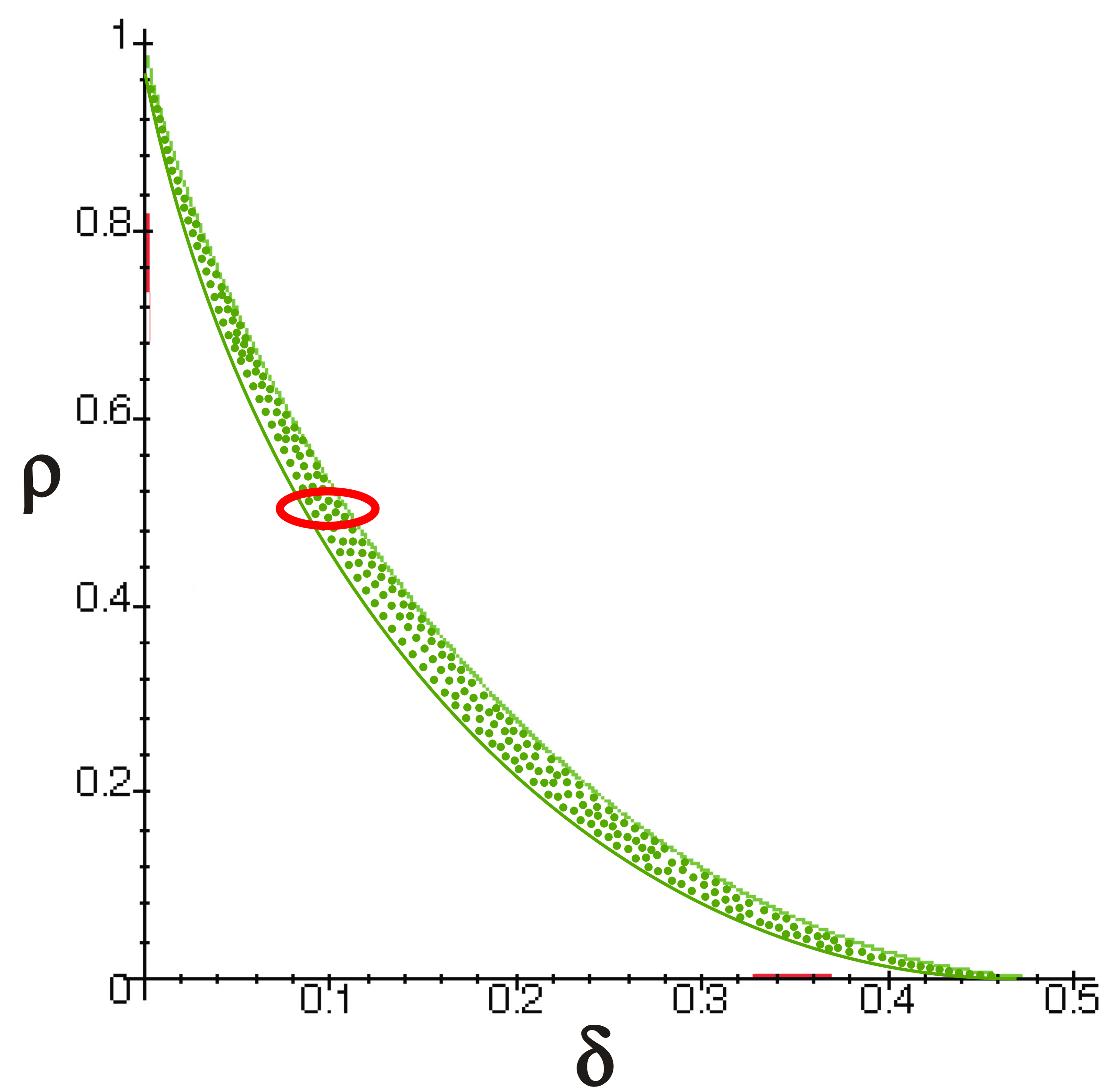
Assumption 2: Let $\rho \in]0,1[$; let $\delta < 1/2$ be such that $\rho > H_2(\delta)$. Then the SD(ρ,δn,δn) collection is strongly one-way.



$[n, \rho n, \delta n]$ linear code

For fixed
$\rho=1/2$

n	512	512	512	728	728	1024	1024
$\lfloor \delta n \rfloor$	56	55	50	78	71	110	100



(3) Applications of One-Way Functions

1991/1999

SIAM J. COMPUT.
Vol. 28, No. 4, pp. 1364–1396

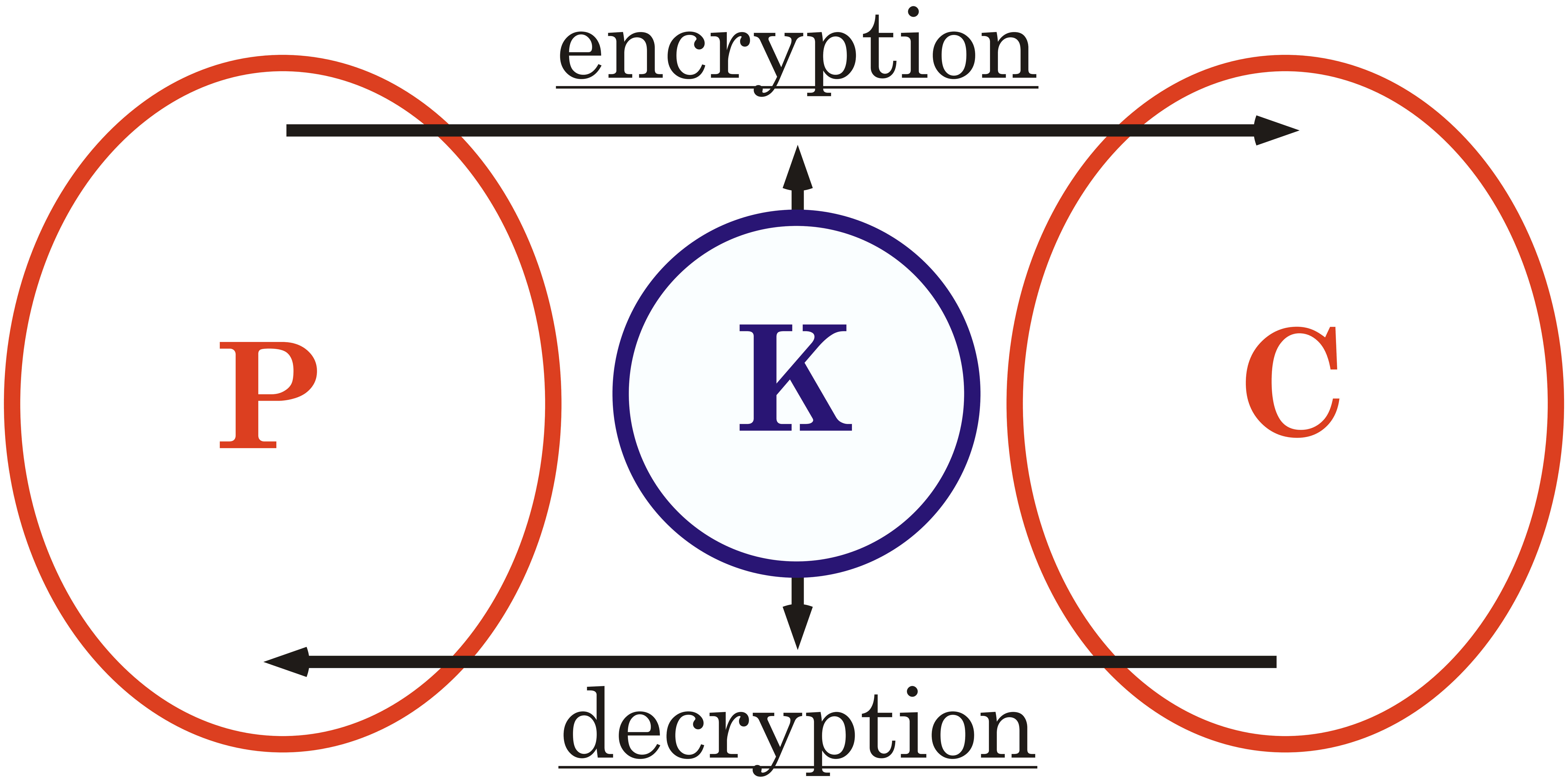
A PSEUDORANDOM GENERATOR FROM ANY ONE-WAY FUNCTION*

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.

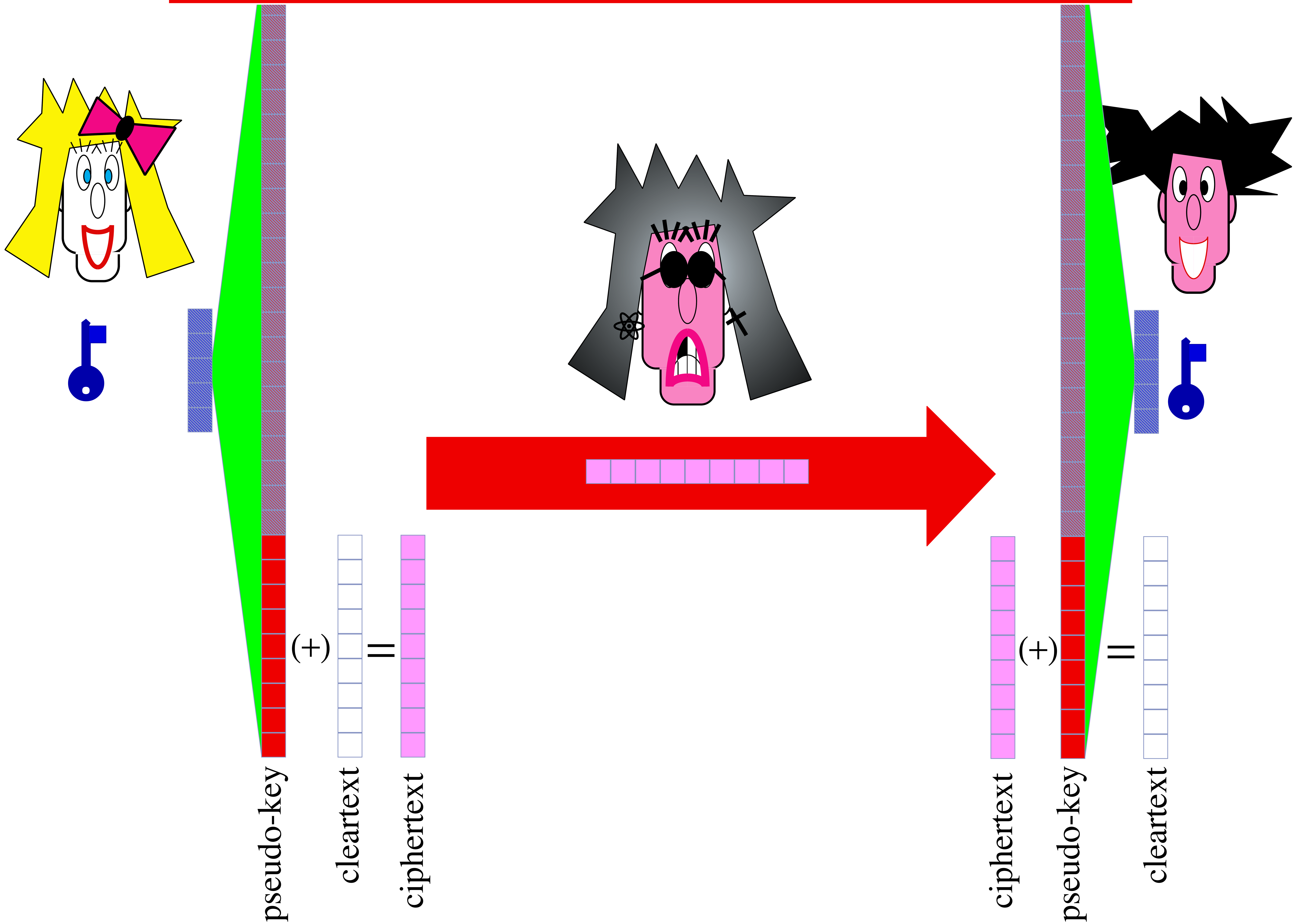
OWF--›PRBG

symmetric encryption

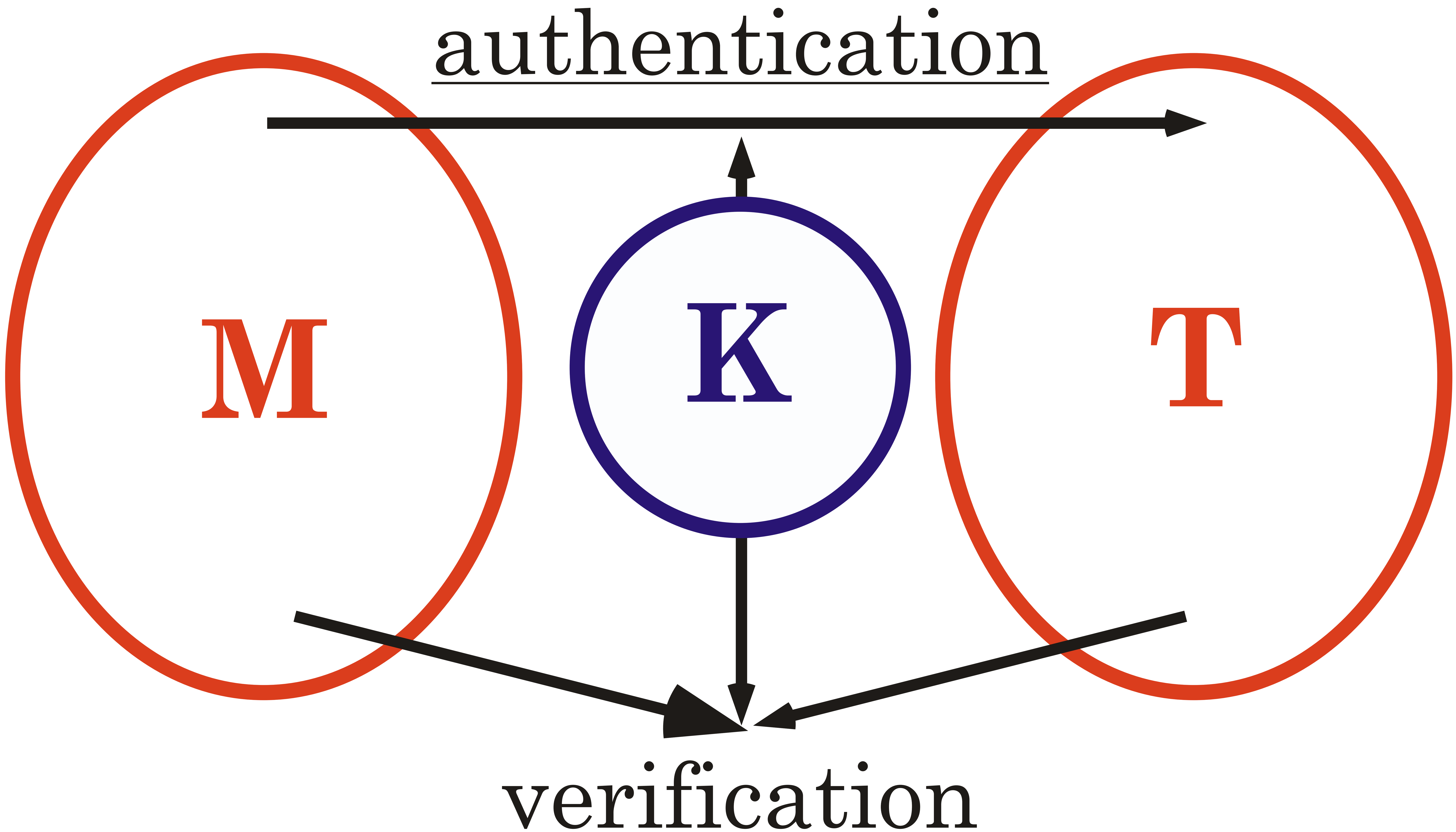


Information Theoretical Security

Stream-cipher from PRBG

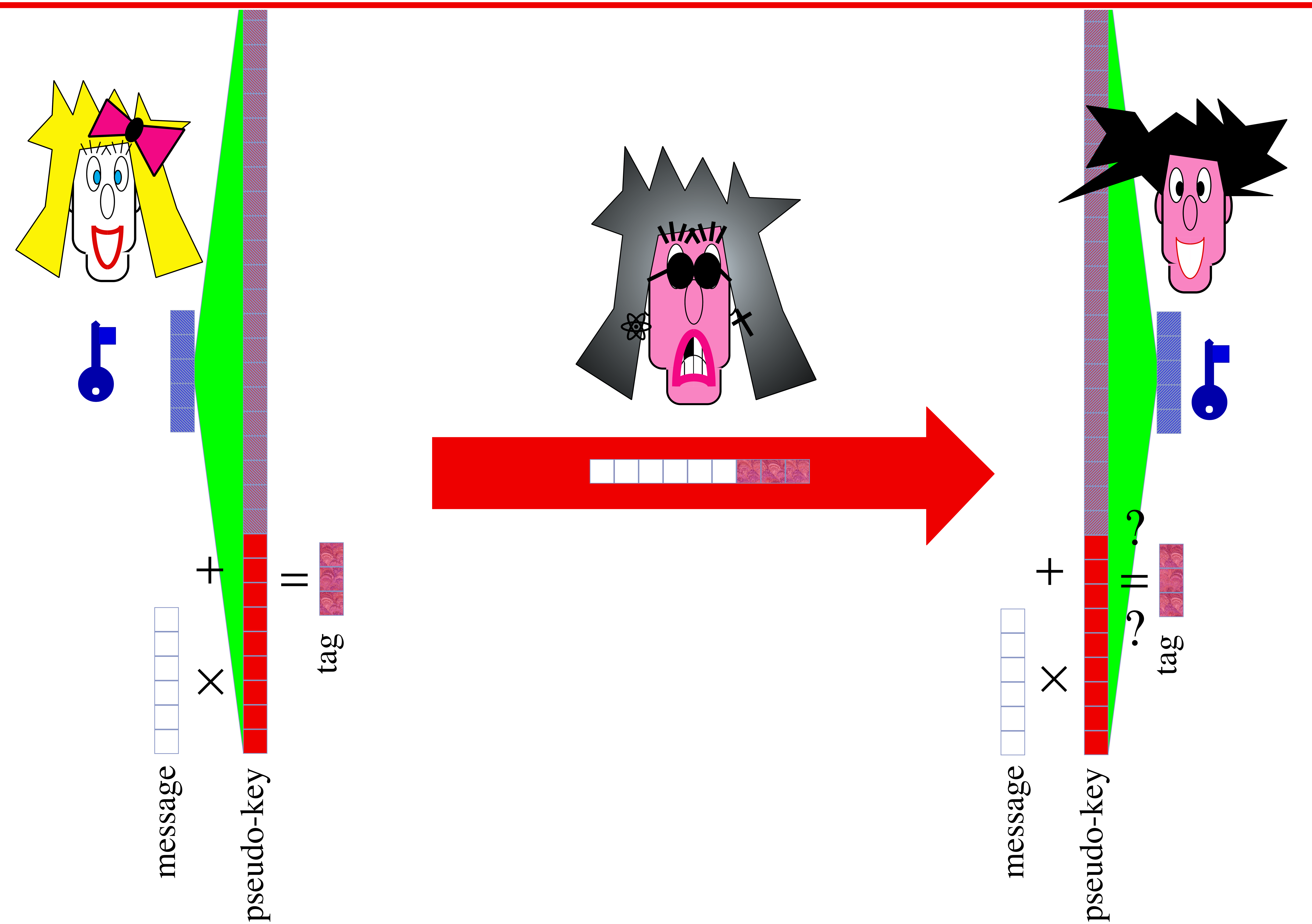


symmetric authentication



Information Theoretical Security

One-Time-Authentication from PRBG



1989/1995

Universal One-Way Hash Functions and their Cryptographic Applications *

Moni Naor[†] Moti Yung[‡]

Revised March 13, 1995

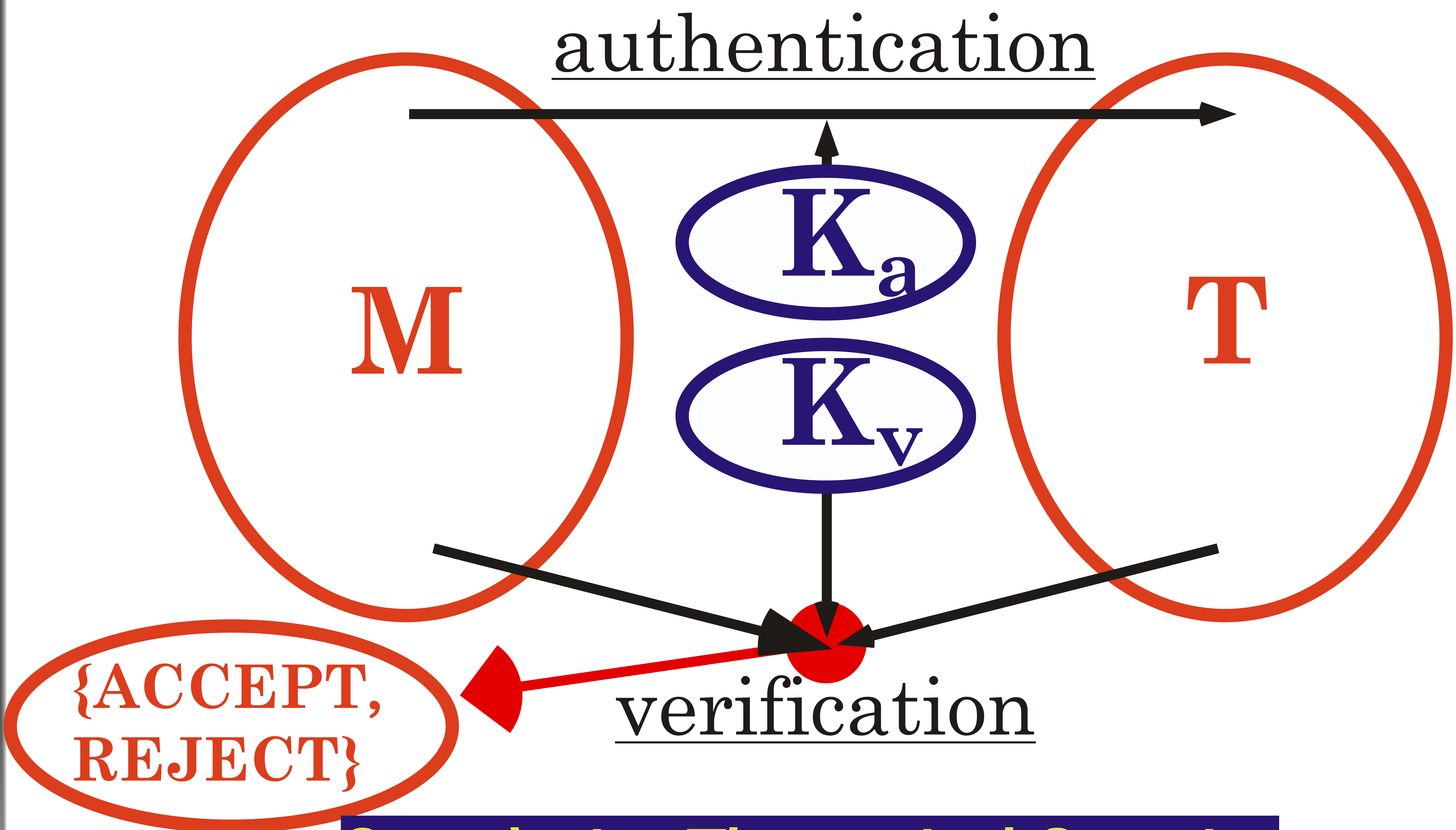
Abstract

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)



Complexity Theoretical Security

UOWHF

Let $\{n_{1_i}\}$ and $\{n_{0_i}\}$ be two increasing sequences such that for all i $n_{0_i} \leq n_{1_i}$, but $\exists q$, a polynomial, such that $q(n_{0_i}) \geq n_{1_i}$ (we say that these sequences are polynomially related). Let H_k be a collection of functions such that for all $h \in H_k$, $h : \{0,1\}^{n_{1_k}} \mapsto \{0,1\}^{n_{0_k}}$ and let $U = \bigcup_k H_k$. Let A be a probabilistic polynomial time algorithm (A is a *collision adversary*) that on input k outputs $x \in \{0,1\}^{n_{1_k}}$ which we call an *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 *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 $Prob[A(h,x) = y, h(x) = h(y), y \neq x] < 1/p(n_{1_k})$ 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

door permutation [BM1] and any one-way permutation [NY] have been constructed. In this paper, we present a method for constructing secure digital signatures given any one-way function. This is the best possible result, since a one-way function can be constructed from any secure signature scheme.

Our method follows [NY] in basing signatures on one-way hash functions: functions which compress their input, but have the property that even given one preimage, it is hard to find a different one. This in itself

OWF-->UOWHF*

2005

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

J. Cryptology (1991) 4: 151–158

Journal of Cryptology

Bit Commitment Using Pseudorandomness[1]

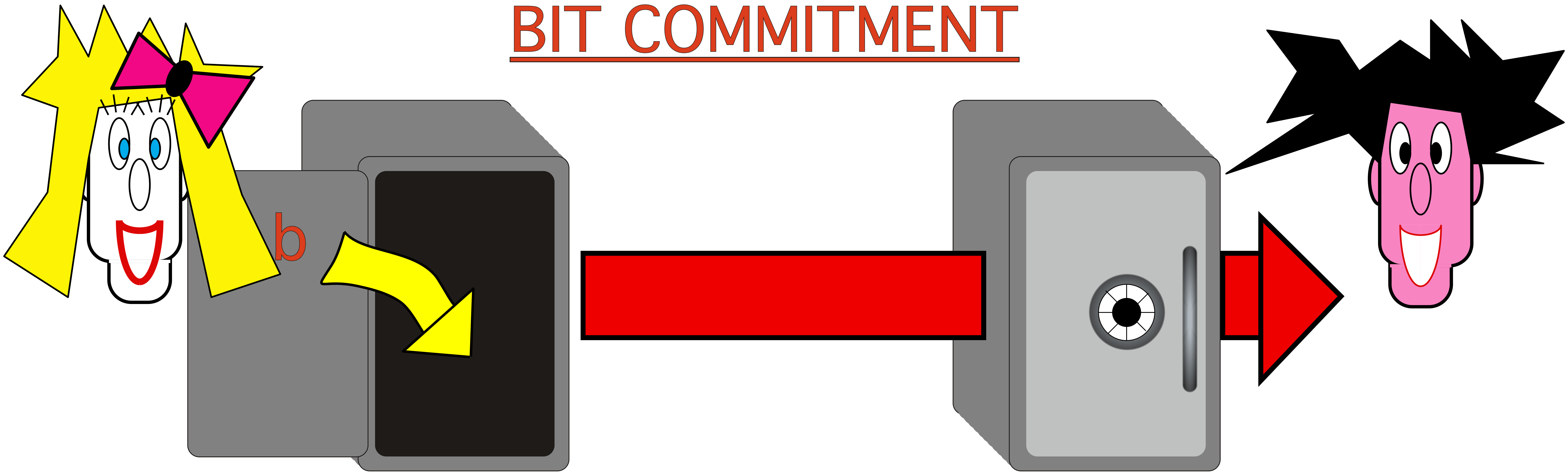
Moni Naor
IBM Almaden Research Center, 650 Harry Road,
San Jose, CA 95120, U.S.A.

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.

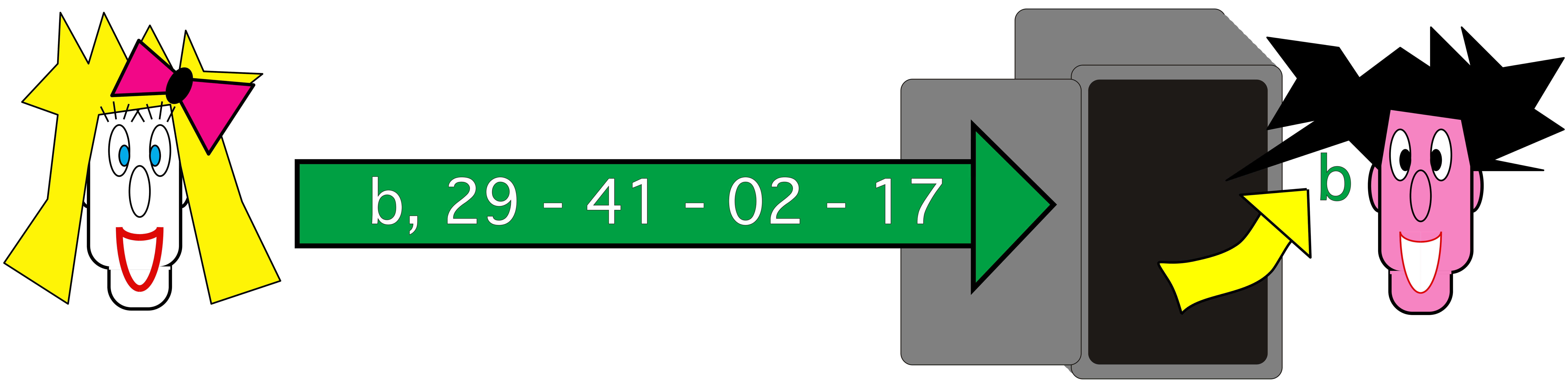
PRBG--›BC

BIT COMMITMENT

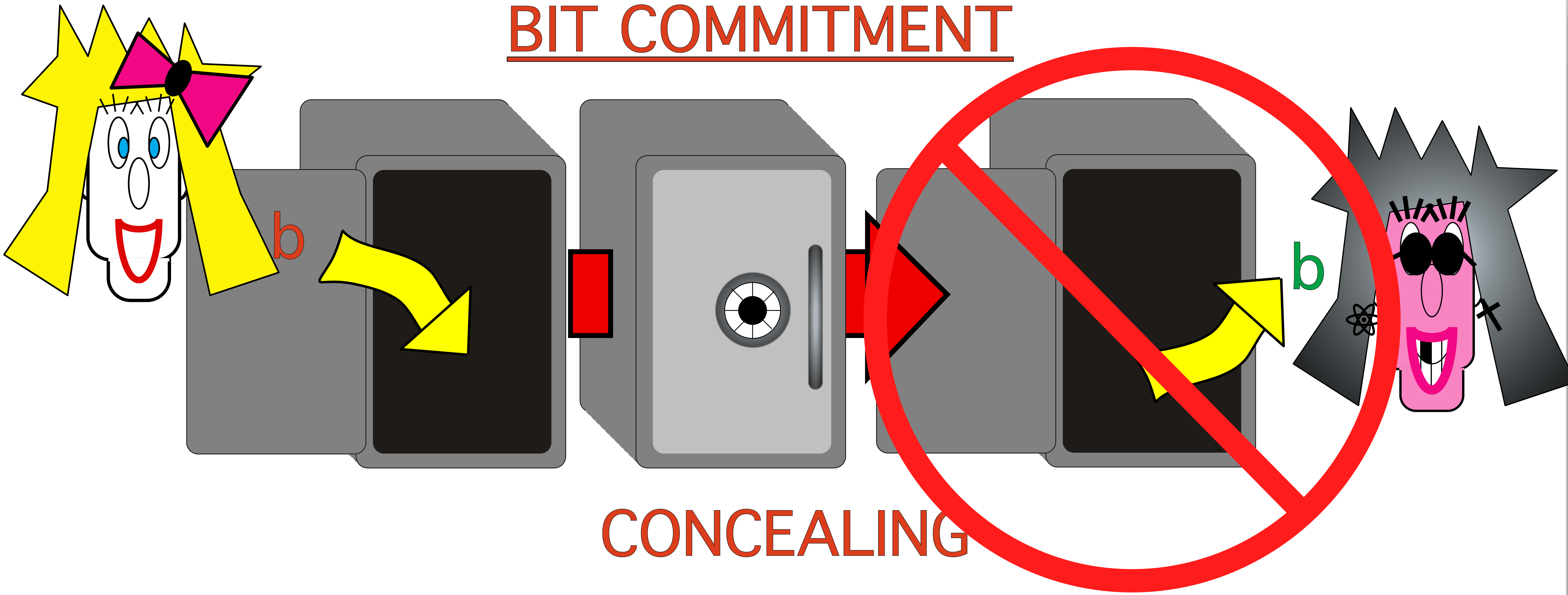


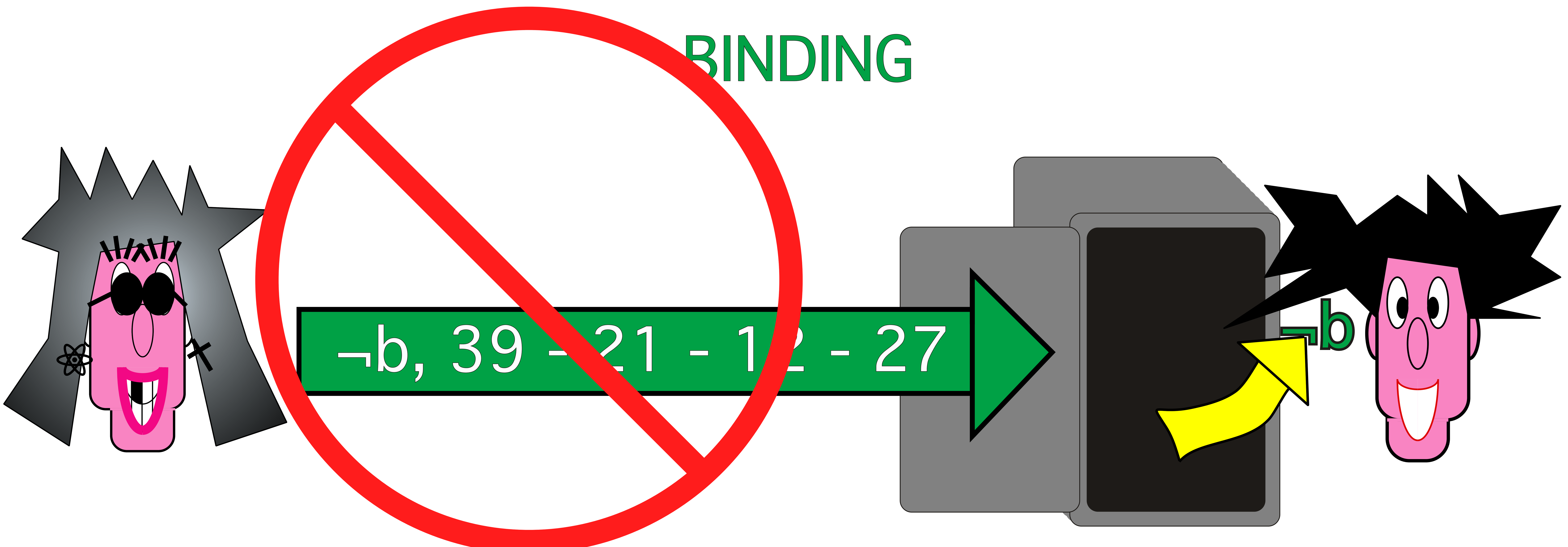
COMMIT

UNVEIL

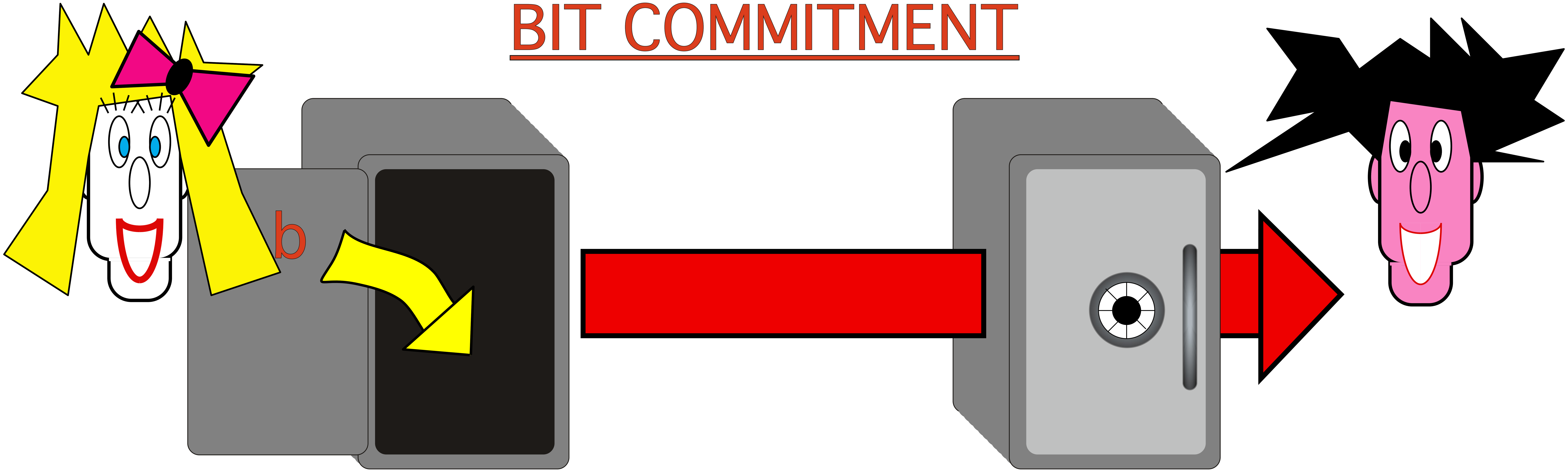


BIT COMMITMENT





BIT COMMITMENT

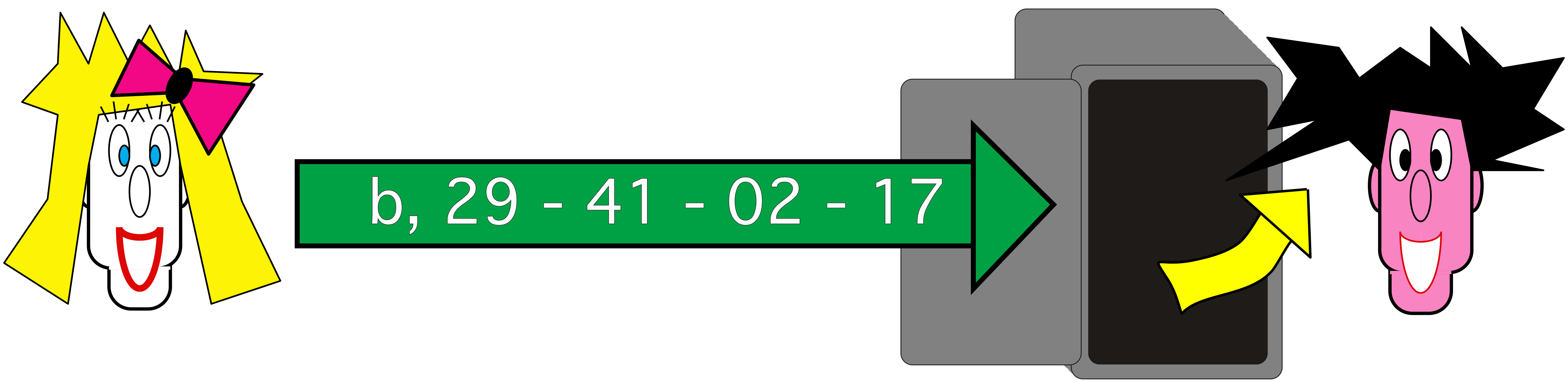


COMMIT

Computationally CONCEALING

Statistically BINDING

UNVEIL



2006

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 composability. 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].[1]

OWF --› 1/2-BC

1/2–BC

Definition 2.1. *A 2-phase commitment scheme (S, R) consists of four interactive protocols:*

- (S_c^1, R_c^1) *the first commitment phase*
- (S_r^1, R_r^1) *the first reveal phase*
- (S_c^2, R_c^2) *the second commitment phase*
- (S_r^2, R_r^2) *the second reveal phase*

1. *In the first commitment phase, S_c^1 receives a private input $\sigma^1 \in \{0,1\}$ and a sequence of coin tosses r_S* [5]. *S_c^1 and R_c^1 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_r^1 and R_r^1 receive as common input the commitment z^1 and a bit σ^1. S_r^1 receives as private input r_S. S_r^1 and R_r^1 receive a common output τ. (Without loss of generality, we can assume that τ is the transcript of the first commitment phase and the first reveal phase and includes R_r^1's decision to accept or reject).*

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

4. *In the second reveal phase, S_r^2 and R_r^2 receive as common input the commitment z^2 and a bit σ^2. S_r^2 receives as private input r_S. At the end of the protocol, R_r^2 accepts or rejects.*

5. *$S = (S^1, S^2) = ((S_c^1, S_r^1), (S_c^2, S_r^2))$ and $R = (R^1, R^2) = ((R_c^1, R_r^1), (R_c^2, R_r^2))$ are computable in probabilistic polynomial time* poly(n) *(where 1^n is the security parameter).*

2007

Statistically-Hiding Commitment from Any One-Way Function

Iftach Haitner* Omer Reingold†

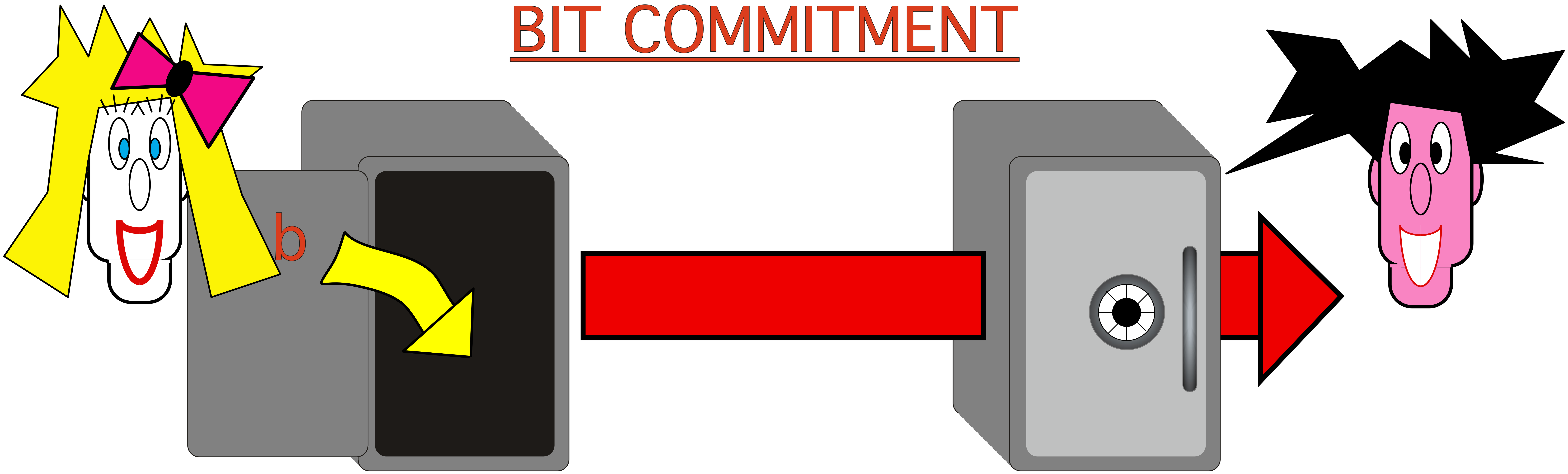
Abstract

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-BC +

UOWHF --› BC

BIT COMMITMENT

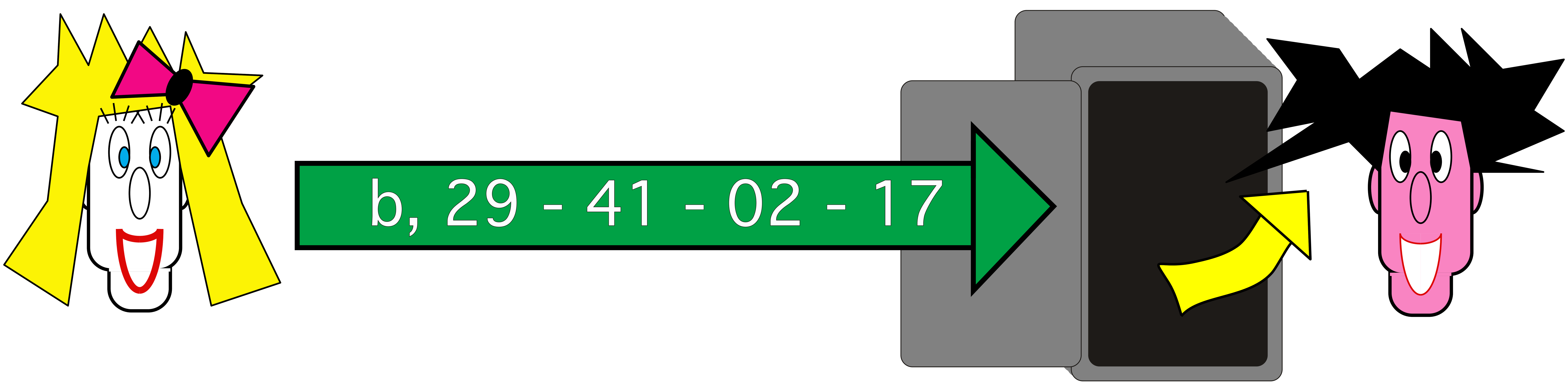


COMMIT

Perfectly CONCEALING

Computationally BINDING

UNVEIL




Universal One-Way Hash Functions and their Cryptographic Applications *
Moni Naor† Moti Yung‡
Revised March 13, 1995
UOWHF--›DS
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
OWF--›1/2-BC
OWF--›PRBG
A PSEUDORANDOM GENERATOR FROM ANY ONE-WAY FUNCTION*
JOHAN HÅSTAD†, RUSSELL IMPAGLIAZZO‡, LEONID A. LEVIN§, AND MICHAEL LUBY¶
J. Cryptology (1991) 4: 151–158
Journal of Cryptology
PRBG--›BC
Bit Commitment Using Pseudorandomness[1]
Moni Naor
IBM Almaden Research Center, 650 Harry Road, San Jose, CA 95120, U.S.A.
On Constructing Universal One-Way Hash Functions from Arbitrary One-Way Functions
Jonathan Katz*† Chiu-Yuen Koo*
OWF--›UOWHF
Statistically-Hiding Commitment from Any One-Way Function
Iftach Haitner* Omer Reingold†
1/2-BC + UOWHF --› BC
One-Way Functions are Necessary and Sufficient for Secure Signatures
John Rompel*
OWF--›UOWHF*
Proving all these results in a quantum setting is still open...

(4) 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