0272-5428/82/0000/0160$00.75 © 1982 IEEE

此文档通过<https://www.dogetranslator.com/> 将原pdf文档转换为此word文档，原始转换后的文档

1

power and limitation of one-way functions. For example,

The protocol proceeds as follows:

work is essential if we are ever to understand the intrinsic

choosing a random element from Q

N

.

security of protocols. More fundamentally, such a frame-

M to M. Let E

a

be the public key of Alice, generated by

mon proof techniques can be developed for proving the

gers, and Q

N

be the set of all 1-1 onto functions from

all these applications can be related, and where com-

values). Let M be the set of all N-bit nonnegative inte-

would be desirable to have a uniﬁed framework where

the only thing they know in the end (aside from their own

suspecting parties are to generate an unbiased bit. It

for them to decide whether i < j, such that this is also

line, and “coin ﬂipping” (Blum [6]), in which two mutually

has j millions, where 1< i, j <10. We need a protocol

players deal cards by communicating over a telephone

For deﬁniteness, suppose Alice has i millions and Bob

includes “mental poker” (Shamir, et.al. [5]), in which two

three solutions we have.

saboteurs [1, 2, 3, 4]. The second kind of applications

In this abstract, we will describe in detail only one of the

them unreadable and unalterable for eavesdroppers and

3.1 Solutions to the Millionaires’ Problem

the encryption and transmission of messages to make

kinds of applications. The ﬁrst kind is concerned with

3 Deterministic Computations

(Difﬁe and Hellman [1]), they have been used in two

Since one-way functions were ﬁrst proposed in 1976

Results on the other case will be reported elsewhere.

computation-intense case with no outside saboteurs.

2 A Uniﬁed View of Secure Computation

will report here only the results corresponding to the

view of secure computation in the next section.

together. However, due to length considertion, we

this work in perspective by ﬁrst considering a uniﬁed

It would be natural to discuss these two special cases

Before describing these results, we would like to put

the case of m parties communicating.

be accomplished with one-way functions”.

above description, all discussions can be extended to

cheating. Finally, we study the question “What cannot

Note that, although we have used Alice and Bob in the

tion”, and describe methods to prevent participants from

version of this problem which will also be discussed.)

“How many bits need to be exchanged for the computa-

(Mental poker and coin ﬂipping represent a stochastic

poker, etc. We will also discuss the complexity question

we get the problem which is to be studied in this paper.

ing of database, oblivious negotiation, playing mental

nored, but the computation of f and g is nontrivial, then

results have applications to secret voting, private query-

the other extreme, when such external threats can be ig-

which are easy to evaluate but hard to invert). These

the basic concern is eavesdropping and sabotage. In

of solving it by use of one-way functions (i.e., functions

the ﬁrst kind of applications mentioned before, in which

lation of this general problem and describe three ways

trivial, e.g. if f = constant and g(i, j) = i, then we get

0 otherwise. In this paper, we will give precise formu-

In one extreme, when the computation component is

1

2

1

2

case when m = 2 and f(x

, x

) = 1 if x

< x

, and

ﬁed.

variables? The millionaires’ problem corresponds to the

may not wish to reveal the exact value of i) can be satis-

giving away any information about the values of their own

*straints* (against saboteur) and *privacy constraints*  (Alice

f, by communicating among themselves, without unduly

Alice and Bob to follow, such that certain  *security con-*

other x’s. Is it possible for them to compute the value of

pose of a protocol would be to design an algorithm for

i

i

sume initially person P

knows the value of x

and no

pers or saboteurs on the communication line. The pur-

i

function of m integer variables x

of bounded range. As-

Bob a function g(i, j). There may be some eavesdrop-

1

2

3

m

function f(x

, x

, x

, . . . , x

), which is an integer-valued

nicate so that Alice can evaluate a function f(i, j), and

lem. Suppose m people wish to compute the value of a

of private variables i and j respectively, wish to commu-

This is a special case of the following general prob-

lowing view. Two parties Alice and Bob, in possession

carry out such a conversation?

In response to this need, we propose to adopt the fol-

information about each other’s wealth. How can they

1/e ?”

they do not want to ﬁnd out inadvertently any additional

pecting parties to interactively generate a bit with bias

Two millionaires wish to know who is richer; however,

question such as “Is it possible for three mutually sus-

1 Introduction

without a precise model it would be hard to answer a

University of California Berkeley, California 94720

Andrew C. Yao

(extended abstract)

Protocols for Secure Computations

2

may cheat in the process, by deviating from the agreed

end of the execution of the protocol. By that time, the

One may have noticed the possibility that some party

there is a special symbol whose appearance means the

be given in Section 3.2, we will deﬁne this precisely.

send a string according to the protocol. We agree that

of time to gain this information. In the formal deﬁnition to

bilistically. Now it is Bob’s turn to compute strings and

cannot perform calculation within a reasonable amount

send a string to Bob, again the string is chosen proba-

of the exchange speciﬁed by the protocol, but also they

tosses. After she has ﬁnished this computation, she will

2

8

only the participants do not gain information as a result

compute α

+ 3α

based on the outcomes of some coin

one also has to include in the formal deﬁnition that not

probabilistic, i.e. she will decide to evaluate E(4), or to

b

a

has been the outcome of the previous conclusion. Thus,

to apply or whether to evaluate E

or D

is in general

information that Bob is not supposed to ﬁnd out, if i≥j

a string already obtained. The choice of which function

a

b

a

ﬁnd out whether i≥9. That would be an extra piece of

strings, or of the form E

(y), E

(y) or D

(y) where y is

9

u

to be t, and knows the value of z

, which enables him to

where each new string α

is a function of the earlier

9

t+1

t+2

s

k−j+ 9; if he succeeds, he then knows the value y

she should compute in private strings α

, α

, . . . , α

a

to randomly choose a number t and check if E

(t) =

ted between her and Bob, the protocol speciﬁes how

making more calculations. For example, Bob might try

1’s); based on the bits that have so far been transmit-

b

3

9

8

Bob might try to ﬁgure out the other person’s value by

strings (e.g. E

(α

) = α

, α

has an odd number of

1

2

t

This has not ﬁnished the argument yet, as Alice or

of strings α

, α

, . . . , α

, and some relations among the

u

u

far in her possession, which consists of some sequence

him, he cannot tell if they are z

or z

+ 1.

u

ﬁnished transmission, Alice examines the information so

ues of other z

, and by looking at the numbers Alice sent

j

strings to each other alternately. Each time after Bob has

hence z

. However, he has no information about the val-

j

Bob should communicate as follows. Alice and Bob send

What does Bob know? He knows y

(which is x) and

puting a function f(i, j) speciﬁes exactly how Alice and

a

E

is random all the 10 possibilities are equally likely.

some s between k−j+ 1 to k−j+ 10. As the function

onto functions on N-bit integers. A protocol A for com-

N

domly drawn from Q

, the set of all the possible 1-1

a

coming from Bob is that Bob knows the vaue ofD

(s) for

b

a

b

D

. Assume that E

and E

are independently and ran-

sult that Bob told her, because the only other information

b

j, except for the constraint on j implied by the ﬁnal re-

ice; similarly Bob has a public E

, and a private inverse

a

a

Firstly Alice will not know anything about Bob’s wealth

tion E

, whose inverse function D

is known only to Al-

**Protocol**. Assume Alice has a public one-way func-

met.

Here we will informally argue why the requirement is

“collusions” that are absent in the 2-person case.

ﬁne a precise model which will be done in Section 3.2.

there are extra security considerations such as possible

tion about the wealth of the other party, we need to de-

eral case involve additional technical complications, and

the requirement that they cannot get any more informa-

be brieﬂy discussed in Section 5. The proofs for the gen-

correctly who is the richer person. To show that it meets

and Bob). Generalization of the results to general m will

This protocol clearly enables Alice and Bob to decide

sults for the case when f is 0−1 valued and m= 2 (Alice

7. Bob tells Alice what the conclusion is.

For simplicity, we will only give the deﬁnitions and re-

the model that corresponds to the ﬁrst solution.

modp, and i < j otherwise.

tail for each solution. In this abstract, we will only give

from Alice, and decides that i≥j if it is equal to x

assumptions, a precise model has to be speciﬁed in de-

6. Bob looks at the j-th number (not counting p) sent

As these three solutions base their security on different

preted in the modp sense.

3.2 Model for the General Problem

10

1, . . . , z

+ 1; the above numbers should be inter-

by Goldwasser and Micali [2].

1

2

i

i

i+1

bers to B: z

, z

, . . . , z

followed by z

+ 1, z

+

makes use of a probabilistic encryption method invented

5. Alice sends the prime p and the following 10 num-

a

b

b

a

ity property, i.e. E

E

(x) =E

E

(x). The other solution

u

p, z

denote this ﬁnal set of numbers;

function, where these functions satisfy the commutativ-

u

peat the process until all z

differ by at least 2; let

sumes that Alice and Bob each owns a private one-way

otherwise generates another random prime and re-

lem based on different principles. The ﬁrst of them as-

u

all z

differ by at least 2 in the modp sense, stop;

We have two other solutions to the millionaires’ prob-

u

u

computes the values z

= y

(modp) for all u; if

mental poker protocol in Shamir et. al. [5].)

4. Alice generates a random prime p of N/2 bits, and

quirement than the veriﬁability requirement used in the

j+u) for u= 1,2, . . . ,10.

possible in Section 3.3. (Note that this is a stronger re-

u

a

3. Alice computes privately the values of y

=D

(k−

revealing the values of i and j? We will show that this is

successful cheating becomes vanishingly small, without

2. Bob sends Alice the number k−j+ 1;

way of designing a protocol such that the chance of a

a

privately the value of E

(x); call the result k.

nal step and tell Alice the wrong conclusion. Is there a

1. Bob picks a random N-bit integer, and computes

protocol. For example, Bob may lie to Alice in the ﬁ-

3

time S, then the protocol can be implemented such that

other member’s. Furthermore, the protocol makes the

In fact, if f can be computed by a Turing machine in

ﬁnal action f, without anyone knowing the opinion of any

in this paper means that it is possible to agree on the

δ

1

2

3

m

O

C(f) log

*.*

as a function f(x

, x

, x

, . . . , x

). The results obtained

1

i

“

”

write an opinion x

, and the ﬁnal action can be regarded

*isfying the* (, δ)*-privacy constraint such that:* T(A) =

wish to decide on a yes-no action. Each member is to

*size* C(f)*, then there is a protocol* A *computing* f *sat-*

**Secret Voting**. Suppose a committee of m members

*tion. If* f *can be computed by a boolean circuit of*

**Theorem 2** *Let* 1 > , δ > 0 *and* f(i, j)  *be a 0-1 func-*

3.4 Applications

changed between Alice and Bob when A is used.

*pant is at most* γ*.*

tocol, let T(A) denote the maximum number of bits ex-

*ability of a successful cheating by the other partici-*

we can prove that this is not the case. Let A be a pro-

*2. if one participant behaves according to* A*, the prob-*

infeasible with the extra privacy constraint. Fortunately,

δγ

computable without the privacy requirement, but become

γ

*1.* T(A) =O

C(f) log

log

*, and*

1

1

straint. Conceivably, there are functions that are easily

“

”

protocol to compute f that satisﬁes the (, δ)-privacy con-

*such that*

to determine the minimum number of bits needed by any

*of Theorem 2, there exists a protocol* A  *for computing f*

ted is proportional to n. An interesting question is then,

**Theorem 4** *Let* 1> γ >0*. Under the same assumption*

of i, j become large, since the number of bits transmit-

lionaires’ problem will become impractical if the range n

*ful cheating by Bob is deﬁned similarly.*

**(A) Complexity**. The solution given earlier for the mil-

*any value of* i  *and yet Bob does not detect it. A success-*

***ing***  *by Alice, if Alice does not behave consistently with*

3.3 Additional Requirements

*protocol. We will consider it to be a*  ***successful cheat-***

case of probabilistic computations.

**Deﬁnition 1** *Consider an instance in the execution of a*

go into that here. In Section 4, that becomes a special

the initial distribution of (i, j) is nonuniform. We will not

is the only cheating that Alice (or Bob) can do.

It is possible to consider the more general case when

most that a protocol can achieve is to make sure that this

behaving as if she had a different variable value i0, the

*privacy constraint.*

Since a protocol can never prohibit Alice (or Bob) from

*exists a protocol for computing* f *that satisﬁes the* (, δ)*-*

cheating, without asking either to reveal the variable.

**Theorem 1** *For any* , δ > 0 *and any function* f*, there*

back. The following results will show that one can thwart

to be given later, this sometimes can be a serious draw-

3. the above requirement is also true for Bob.

their variables. As will become clear in the applications

putation. However, that will force both parties to reveal

still get the above distribution on j, and

both parties are required to reveal all their private com-

and D’s, then with probability at least 1−δ she will

covered if there is a veriﬁcation stage afterwards where

tions with no more than O(Nk) evaluations of E’s

It is true that with our protocol, any cheating will be dis-

2. if Alice tries afterwards to perform more calcula-

or to mislead the other party to receive a wrong answer?

i

them might cheat in order to gain additional information

where G

is the set of j for which f(i, j) =v,

i

rules speciﬁed by an agreed protocol. What if either of

|G

|

for j∈G

, and 0 otherwise,

i

1. p

(j) =

1 +O()

i

1

cussions have assumed that Bob and Alice observe the

`

´

**(B) Mutually-Suspecting Participants**. So far the dis-

*constraint*  if the following conditions are satisﬁed:

i

this p

(j). A protocol is said to *satisfy the* (, δ)*-privacy*

*large* n*.*

compute a probability distribution of the values of j; call

(, δ)*-privacy constraint must have* T(A) > 2n/2  *for all*

value v of the function and the strings in her possesion,

n

*element of* F

*, then any protocol* A *that computes* f  *with*

5

At the end, Alice can in principle, from her computed

**Theorem 3** *Let*  1

> , δ >0 *be ﬁxed. Let* f  *be a random*

out the computation faithfully according to the protocol.

values are equally likely. Suppose Bob and Alice carry

further discussions).

valued function. Assume that initially all pairs of (i, j)

in the absence of the privacy constraint (See Yao [7] for

**Privacy Constraint**. Let , δ > 0, and f(i, j) be a 0-1

at most n bits of transmitted information can compute f,

function f(i, j) with i and j being n-bit integers. Clearly,

n

k is an integer chosen in advance.

privacy constraint. Let F

be the family of 0-1 valued

and D’s by Bob and Alice be bounded by O(Nk), where

many bits transmitted between Bob and Alice with the

that, in a protocol, the total number of evaluations of E’s

However, there exist functions that need exponentially

pute the function value f in private. Finally, we require

execute the protocol with a time bound O

Slog(1/δ)

.

`

´

protocol has an instruction for each participant to com-

both Alice and Bob have Turing machine algorithms to



4

W is the set of all 5-element subsets of {1,2, . . . , 52},

being detected by all the participants of K.

following situation: I = J = {0}, q is a constant, V =

r

r

∈X

without

For example, mental poker would correspond to the

r∈K0 behaves inconsistently with any x

r

execution of A, in which at least one participant A

with

j∈J

x∈W

ij

|J|

f

(v, x)

by K0 (with respect to a protocol A) is an instance of the

i,v

P

ij

on j is equal to q

(j)(1 +O()). A  *successful cheating*

1

f

(v, w)

X

infer, with probability at least 1−δ, that the distribution

to

amount of calculation polynomial in T(A), they will still

done should, according to the privacy constraint, is equal

the participants in K are allowed to perform in private an

h(w) that Alice can infer from the computation she has

(, δ)*-private constraint* if for every nonempty K, even if

case q = constant. In this special case, the distribution

can infer.) Let , δ >0. A protocol A is said to  *satisfy the*

erality here but simply give an illustration for the special

i,v

tion f has value v, then q

(j) is the distribution they

made precise in terms of q and F; we omit its full gen-

in addition to their only variable values i, is that the func-

responding constraint on Bob). This statement can be

other participants, and if the only information available,

can be inferred from her values of i and v (plus a cor-

to infer the probabilty distribution of the variable values of

Alice can obtain about j and w is no more than what

r

ij

otherwise. (If all the participants A

with r∈K0 collude

f

(v, w). The privacy constraint is that the information

i,v

i

(j) = 1/|G

(v)| for j ∈ G

(v) and 0

i

f(x) = v. Let q

a value v ∈ V and Bob a value w ∈ W with probability

K

on H

and H

equals i and j respectively, satisﬁes

K0

sages between them, so that at the end Alice will obtain

1

2

m

(unique vector) x = (x

, x

, . . . , x

), whose projection

probability desity q ∈ P(I, J). They wish to send mes-

i

K

K

G

(v) ⊆ H

be the set of all j ∈ H

such that the

knows j ∈ J; the values of (i, j) obey a certain initial

K

deﬁne H

and v ∈ V , let

K0

similarly. For any i ∈ H0

ties. Initially, Alice knows the value of i ∈ I, and Bob

1

2

|K|

{t

, t

, . . . , t

}=K. Let K0 ={1,2, . . . , m} −K, and

I, j ∈ J} ⊆ P(V, W) be a family of probability densi-

1

2

|K|

K

t

t

t

ij

deﬁne H

=

X

× X

× · · · × X

, where

Let I, J be ﬁnite sets of integers. Let F = {f

|i ∈

i

∈ X

. For any nonempty K ⊆ {1,2, . . . , m},

i

where x

P(V, W) be the set of all such probability densities.

1

2

m

Let V be the range of the function f(x

, x

, . . . , x

),

if the sum of p(v, w) over v and w is equal to 1. Let

We now make it precise.

V ×W to the interval [0,1] is called a  *probability density*

if as many as m−1 dishonest guys try to help cover up).

(m= 2). Let V and W be ﬁnite sets. A function p from

be detected and identiﬁed by all the honest parties (even

Let us consider the case with two parties Bob and Alice

how many participants may collude, any cheating act will

4 Probabilistic Computations

constraint can be met in the following sense: No matter

collude to cheat. We will show that even the most severe

does not know what Alice has queried.

1

2

m

a function f(x

, x

, . . . , x

), more than one parties may

thing else about the data in it, while the database system

1

2

m

When m parties A

, A

, . . . , A

collaborate to compute

Alice can get answer to the query without knowing any-

5 Generalization tom-Party Case

the database, and Alice is asking query number i, then

gard Bob as a database query system with j the state of

about c(logn)2 bits.

that Bob will know nothing about i in the end. If we re-

between Bob and Alice, while our scheme only needs

to compute a trivial function g(i, j) = constant, meaning

viously known solutions transmit cn bits of information

may wish to compute a function f(i, j) and Bob wishes

to draw a random card from the deck in turn. All the pre-

i

i

P

is computing a different function f

. In particular, Alice

have a deck of n cards, and Alice and Bob each want

proved can be extended to the case when each person

the number of cards becomes greater. Suppose we

**Private Querying of Database**. The theorems we have

Moreover, the present solution uses much fewer bits as

the special properties of the one-way function involved.)

consistent with the outcome, and vice versa.

tal poker was known in [2], but that solution depends on

information on Bob’s negotiation tactics except that it is

one-way function with publicized keys for playing men-

tion obliviously, in the sense that Alice will not gain any

(instead of using private keys). (A solution with a special

as f(i, j), then it is possible to carry out the negotia-

tative, and that we can play it with a public-key system

i

j

A

, B

used have been determined. Write the outcome

not require the one-way functions used to be commu-

x dollars, . . . ) will be decided once the actual strategies

It differs from Shamir et. al’s solution [5] in that we do

1

2

u

as B

, B

, . . . , B

, then the outcome (no deal, or sell at

poker can be played with any general public-key system.

1

2

t

strategies of Alice as A

, A

, . . . , A

, and those of Bob’

One interesting corollary of our results is that mental

egy of negotiation in mind. If we number all the possible

straints are imposed. We will not give the details here.

sell Bob a house. In principle, each one has a strat-

tic computation remains feasible when the privacy con-

**Oblivious Negotiation**. Suppose that Alice is trying to

probabilistic case. Basically, a reasonable probabilis-

The results in Section 3 have generalizations to the

remote.

constant otherwise.

00

probability of anyone having a successful cheating very

f

(v, w) is 0 if v and w are not disjoint and equal to a



5

secret from the other party.

crossed, i.e. swindled out of its secret without getting the

1979.

a protocol such that an honest party will not be double-

*(STOC’79)*, pages 209–213, Atlanta, GA, USA, April

a

b

of solutions x, y with E

(x) = 1 and E

(y) = 1. Is there

*the 11th ACM Symposium on Theory of Computing*

tion 3.2. Suppose Alice and Bob wish to exchange a pair

to distributive computing. In  *Conference Record of*

The second result is valid for the model deﬁned in Sec-

[7] Andrew C. Yao. Some complexity questions related

California, Berkeley, CA, USA, 1981.

*ates a bit with a transcendental bias* α  *can be robust.*

tiﬁed electronic mail. Technical report, University of

**Theorem 7** *No protocol* A *with ﬁnite* T(A)  *which gener-*

How to exchange secrets; part III: How to send cer-

the bias remains correct if somebody has cheated.

transfer: Part I: Coin ﬂipping by telephone; part II:

call a protocol for generating a bit with bias α *robust*, if

[6] Manuel Blum. Three applications of the oblivious

of the persons cheats by generating a biased bit. Let us

sachusetts Institute of Technology, April 1979.

α with the property that it remains unbiased even if one

Mental poker. Technical Report LCS/TR-125, Mas-

1

2

3

A. Now let α=α

+α

+α

, and we get an unbiased

[5] Adi Shamir, R. L. Rivest, and Leonard M. Adleman.

3

sends it to C, C generates a random α

and sends it to

1

2

21(2):120–126, February 1978.

bit α

and sends it to B, B generates a random α

and

key cryptosystems. *Communications of the ACM*,

m > 2. For example A generates a random unbiased

A method for obtaining digital signatures and public-

bit with bias α. It is easy to see how it can be done for

[4] R. L. Rivest, Adi Shamir, and Leonard M. Adleman.

given in this paper. Suppose m people try to generate a

Technology, 1979.

The ﬁrst impossibility result is valid for all three models

cal Report LCS/TR-212, Massachusetts Institute of

by any protocols. We will only mention two results here.

functions as intractable as factorization. Techni-

There are security constraints that can not be achieved

[3] M. O. Rabin. Digitalized signatures and public-key

6 What Cannot be Done?

1982.

Theorem 5.

pages 365–377, San Francisco, CA, USA, May

security criterion only slightly relaxed from that given in

*Symposium on Theory of Computing (STOC’82)*,

1

2

m

1

2

m

f(x

, x

, . . . , x

) =x

+x

+· · ·+x

(mod q), under a

partial information. In  *Proceedings of the 14th ACM*

is a polynomial, for m parties to compute the function

tion and how to play mental poker keeping secret all

a protocol with running time O(p(m) logq), where p(m)

[2] S. Goldwasser and S. Micali. Probabilistic encryp-

such less stringent requirements. For example, there is

*mation Theory*, IT-22(6):644–654, 1976.

tocols with better running time can be designed under

tions in cryptography. *IEEE Transactions on Infor-*

the computation to be a certain value.) Sometimes pro-

[1] Whitﬁeld Difﬁe and Martin E. Hellman. New direc-

require that no subset K0 be able to force the outcome of

sures would be adequate. (For example, one may only

References

strong one. For some purposes, less stringent mea-

protocols for exchanging secrets.

The security measure as we considered above is a

Even (private communication, 1981) also devised some

polynomial in m.

cial type of secrets) with vanishing chance for cheating.

have protocols satisfying Theorem 5 with running time

exchange factors of a large composite numbers (a spe-

# of 1’s in the x’s (the x’s are boolean variables) both

sidered previously. Blum [6] showed that it is possible to

2

m

1

2

m

x

⊕ · · · ⊕x

and the *tally function* f(x

, x

, . . . , x

) =

Different kinds of exchanging secrets have been con-

1

2

m

1

example, the *parity function* f(x

, x

, . . . , x

) = x

⊕

running time than the bound given in Theorem 5. For

*of anyone double-crossing successfully is bounded by**.*

b

In special cases protocols can be designed with better

*crets* D

(w) *and* D

a

(u)*, and under which the probability*

*with polynomial (in* N*) running time which exchanges se-*

1

2

m

T(A) = Ω

|X

| · |X

| ·. . .· |X

|

*.*

1/4

**Theorem 9** *Let*  > 0 *be ﬁxed. There is a protocol* A

`

´

“

”

*col* A  *satisfying the conditions in Theorem 5 must have*

a

b

functions E

and E

operate on.

**Theorem 6** *There exist functions* f  *for which any proto-*

know u. Let N be the number of bits that the encryption

as the next theorem shows.

Bob does not know the value of w and Alice does not

2

m

a

|X

| ·. . .· |X

| · |V|), which is almost optimal in general

and Bob wants to know the solution x to E

(x) =u, but

1

b

The value of T(A) in the above theorem is O(|X

| ·

pose Alice wants to know the solution y to E

(y) = w

changing secrets is possible in the same model. Sup-

*cheating can not be more than* γ*.*

It is of interest to mention that a different type of ex-

{1, . . . , m}*, the probability for* K0 *to have a successful*

*straint and which has the property that, for any* K0 =

*cross successfully with probability at least* 1/2*.*

A *for computing* f *which satisﬁes the* (, δ)*-private con-*

*crets. Then either Alice or Bob will be able to double-*

**Theorem 5** *For any* , δ, γ > 0*, there exists a protocol*

**Theorem 8** *Let* A  *be any protocol for exchanging se-*