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，然后在通过网站翻译功能进行了自动翻译，原始翻译后的文档

1

单向函数的功率和限制。例如，

该协议进行如下：

如果我们要理解内在的东西，工作是必不可少的

Q中选择一个随机元素

N

.

协议的安全性。更根本的是，这样的框架——

M到M 。让E

一种

是 Alice 的公钥，由

可以开发 mon 证明技术来证明

格斯和Q

N

是所有 1-1 到函数的集合

所有这些应用程序都可以相关

值）。让M 是所有N位非负整数的集合

最好有一个统一的框架，其中

他们最终唯一知道的事情（除了他们自己的

怀疑方将产生一个不偏不倚的位。它

让他们决定是否i < j ，这样这也是

线和“硬币翻转”（Blum [6]），其中两个相互

有j百万，其中1 < i ， j < 10 。我们需要一个协议

玩家通过电话交流发牌

对于确定性，假设 Alice 有i 百万和鲍勃

包括“心理扑克”（Shamir, et.al. [5]），其中两个

我们有三种解决方案。

破坏者 [1, 2, 3, 4]。第二种应用

在本摘要中，我们将仅详细描述其中一个

它们对于窃听者来说是不可读和不可更改的

3.1 百万富翁问题的解决方案

消息的加密和传输

种类的应用。第一类与

3 确定性计算

（ Diffie和 Hellman [1]），它们已被用于两个

自 1976 年首次提出单向函数以来

另一个病例的结果将在别处报告。

没有外部破坏者的计算密集型案例。

2 安全计算的统一视图

将在此处仅报告与

下一节中的安全计算视图。

一起。然而，由于长度的考虑，我们

首先考虑一个统一的

讨论这两种特殊情况是很自然的

在描述这些结果之前，我们想把

m方通信的情况。

用单向函数来完成”。

以上描述，所有讨论都可以扩展到

作弊。最后，我们研究“什么不能

请注意，虽然我们在

”，并描述防止参与者

这个问题的版本也将被讨论。）

“需要为计算交换多少位-

（心理扑克和掷硬币代表随机

扑克等。我们还将讨论复杂性问题

我们得到了本文要研究的问题。

的谈判，玩心理

nored ，但f和g的计算是非平凡的，那么

结果适用于秘密投票，私人查询 -

，当这种外部威胁可能是

易于评估但难以反转）。这些

基本的关切是窃听和破坏。在

使用单向函数（即函数

前面提到的第一种应用程序，其中

解释这个一般问题并描述三种方式

微不足道的，例如如果f =常数和g ( i , j ) = i ，那么我们得到

0否则。在本文中，我们将给出精确的公式-

在一种极端情况下，当计算组件是

1

2

1

2

当m = 2和f ( x

， X

) = 1如果x

< x

， 和

成立。

变量？百万富翁的问题对应于

可能不希望透露i )的确切值可以满足-

泄露有关他们自己价值观的任何信息

*应变* （反对破坏者）和*隐私限制*（Alice

f ，通过彼此之间的交流，而不是过度

爱丽丝和鲍勃跟随，这样某些*安全控制*

其他x的。他们是否有可能计算出

协议的构成是设计一个算法

一世

一世

假设最初人P

知道x的值

和不

人或破坏者。纯- \_

一世

m个整数变量x的函数

有界范围。作为-

Bob 函数g ( i , j ) 。可能有人偷听——

1

2

3

米

函数f ( x

， X

， X

, . . . ， X

) ，这是一个整数值

nicate以便 Alice 可以计算函数f ( i , j ) ，并且

莱姆。假设 m 个人希望计算 a 的值

私有变量i 和j分别希望通勤-

问题的特例-

低视图。两方爱丽丝和鲍勃，占有

进行这样的对话？

因应此需要，我们建议采用以下-

有关彼此财富的信息。他们怎么能

1 / e ？”

他们不想无意中发现任何额外的

期待各方以互动方式产生一些偏见

两个百万富翁想知道谁更富有；然而，

诸如“三者之间是否有可能——

1 简介

没有精确的模型很难回答

加州大学伯克利分校，加利福尼亚 94720

安德鲁·C·姚

（扩展摘要）

安全计算协议

2

可能会在过程中作弊，偏离约定

协议执行结束。届时，

人们可能已经注意到有一种可能性

有一个特殊的符号，它的出现意味着

在 3.2 节中给出，我们将精确定义它。

根据协议发送一个字符串。我们同意

获取这些信息的时间。在正式定义中

胆小。现在轮到 Bob 计算字符串和

无法在合理范围内进行计算

向 Bob 发送一个字符串，再次选择该字符串概率-

协议指定的交换，但它们

折腾。在她完成这个计算之后，她将

2

8

只有参与者不会因此获得信息

计算α

+ 3 α

基于一些硬币的结果

还必须在正式定义中包括不

概率，即她将决定评估E (4) ，或

乙

一种

是上一个结论的结果。因此，

申请或是否评估E

或D

一般来说

i ≥ j ，则 Bob 不应该发现的信息

已经获得的字符串。选择哪个功能

一种

乙

一种

找出是否i ≥ 9 。那将是额外的一块

字符串，或形式为E

( ) , E \_

( y )或D

( y )其中y是

9

你

为t ，并且知道z的值

，这使他能够

其中每个新字符串α

是之前的函数

9

+1 \_

+2 \_

秒

k − j + 9 ;如果他成功了，他就知道y的值

她应该在私人字符串中计算α

, α

, . . . , α

一种

随机选择一个数字t并检查是否E

( t ) =

在她和鲍勃之间，协议规定了如何

进行更多的计算。例如，鲍勃可能会尝试

1 's);基于迄今为止传输的比特

乙

3

9

8

Bob 可能会尝试通过以下方式计算出另一个人的价值

字符串（例如E

( α

) = α

, α

有一个奇数

1

2

吨

这还没有结束论证，因为爱丽丝或

字符串α

, α

, . . . , α

，以及一些关系

你

你

远在她手中，由一些序列组成

他，他不知道他们是不是z

或z

+ 1 。

你

完成传输，Alice 检查信息，以便

其他z的使用

，并通过查看爱丽丝发送的数字

j

字符串相互交替。每次鲍勃有

因此z

.然而，他没有关于瓦尔的信息——

j

Bob 应该按照以下方式进行通信。爱丽丝和鲍勃发送

鲍勃知道什么？他认识你

（这是x ）和

放置一个函数f ( i , j )精确指定 Alice 和

一种

乙

是随机的，所有10种可能性都相等。

k − j + 1到k − j + 10之间的一些s 。作为函数

N位整数上的函数。用于通信的协议A

N

domly取自Q

，所有可能的 1-1 的集合

一种

来自鲍勃的是鲍勃知道价值 D的

( s )对于

乙

一种

乙

D

.假设E

和E

是独立和运行的

鲍勃告诉她的，因为唯一的其他信息

乙

j ，除了最终重新定义对j的约束

冰;类似地，Bob 有一个公共E

，和一个私有逆

一种

一种

首先，Alice 对 Bob 的财富一无所知

重刑 乙

, 其反函数D

只有Al-

**协议**。假设 Alice 有一个公共单向函数-

遇见了。

在这里，我们将非正式地讨论为什么要求是

2人案件中不存在的“勾结” 。

建立一个精确的模型，这将在 3.2 节中完成。

有额外的安全考虑，例如可能

关于对方的财富，我们需要去

一般情况涉及额外的技术并发症，和

他们不能获得更多信息的要求——

将在第 5 节中简要讨论。

正确的是谁是更富有的人。为了表明它满足

和鲍勃）。将结果推广到一般m将

该协议清楚地使 Alice 和 Bob 能够决定

当f为0 − 1值且m = 2 （Alice

7. Bob 告诉 Alice 结论是什么。

为简单起见，我们将只给出定义和重新

对应于第一个解决方案的模型。

mod p ，否则i < j 。

每个解决方案的尾巴。在这个摘要中，我们将只给出

来自 Alice，并决定i ≥ j 如果它等于x

假设，必须指定一个精确的模型

6. Bob 查看发送的第j 个数字（不计算p ）

由于这三种解决方案的安全性基于不同的

在mod p中提出 感觉。

3.2 一般问题的模型

10

1 、。 . . , z

+ 1 ;上面的数字应该是

Goldwasser和Micali [2] 。

1

2

一世

一世

我+1

对B : z \_

, z

, . . . , z

后跟z

+ 1 , z

+

利用发明的概率加密方法

5. Alice 发送素数p和后面的10 数量-

一种

乙

乙

一种

ity属性，即E

乙

( x ) = E

乙

( × ) 。另一种解决方案

你

, z \_

表示这最后一组数字；

函数，其中这些函数满足可交换性-

你

泥炭过程直到所有z

至少相差2 ;让

假设Alice 和 Bob 各自拥有一个私人单向

否则生成另一个随机素数并重新

lem基于不同的原则。他们中的第一个——

你

所有z

在mod p中至少相差2 感觉，停止；

问题，我们还有另外两种解决方案——

你

你

计算值z

= y

( mod p )对于所有u ;如果

Shamir 等人的心理扑克协议。阿尔。 [5]。）

4. Alice 生成一个N/ 2位的随机素数p ，并且

要求而不是在使用的可验证性要求

j + u )对于u = 1 , 2 , . . . ， 10 。

可能在第 3.3 节中。 （请注意，这是一个更强的重新

你

一种

3. Alice 私下计算y的值

= D

( k -

揭示i的值 和j ?我们将证明这是

成功的作弊变得微乎其微，没有

2. Bob 向 Alice 发送数字k − j + 1 ；

设计协议的方式，以便有机会

一种

私下E的值

( x ) ;调用结果k 。

最后一步，告诉爱丽丝错误的结论。有没有

1. Bob 选择一个随机的N位整数，并计算

协议。例如，鲍勃可能在以下情况下对爱丽丝撒谎

3

时间S ，那么协议可以这样实现

其他成员。此外，该协议使

事实上，如果f可以由图灵机计算

最终行动f ，没有人知道任何人的意见

在本文中意味着有可能就

δ

1

2

3

米

哦

C ( f ) 日志

*.*

作为函数f ( x

， X

， X

, . . . ， X

) 。得到的结果

1

一世

“

”

写意见x

，最后的动作可以看作

*满足*( ** , δ ) *-隐私约束，使得：* T ( A ) =

希望决定是-否行动。每个成员都要

*大小*C ( f ) *，那么有一个协议*A*计算*f*饱和*

**秘密投票**。假设一个由m个成员组成的委员会

*重刑。如果*f*可以通过布尔电路计算*

**定理 2***令*1 > , δ > 0*且*f ( i , j )*为 0-1函数-*

3.4 应用

A时，Alice 和 Bob 之间发生了变化。

*pant 至多为*γ *。*

tocol ，让T ( A )表示最大位数 ex-

*另一方成功作弊的能力-*

我们可以证明事实并非如此。让A成为专业人士

*2. 如果一名参与者按照*A行事*，则概率-*

在额外的隐私约束下不可行。幸运的是，

 δγ

无需隐私要求即可计算，但成为

γ

*1.* T ( A ) = O

C ( f ) 日志

日志

*， 和*

1

1

应变。可以想象，有些功能很容易

“

”

计算 f 的协议满足( , δ ) -privacy con-

*以至于*

确定任何所需的最小位数

*由定理 2 可知，存在计算 f的协议*A

n成正比。那么一个有趣的问题是，

**定理 4***令*1 > γ > 0 *。在同样的假设下*

i , j变大，因为传输的比特数

为 n ，狮子王的问题将变得不切实际

*Bob的完全欺骗也有类似的定义。*

**(A) 复杂性**。前面给出的解决方案是

i*的任何值* *但是鲍勃没有检测到它。成功-*

***ing*** *爱丽丝，如果爱丽丝的行为与*

3.3 附加要求

*协议。我们会认为这是一次****成功的作弊——***

概率计算的情况。

**定义 1***考虑一个正在执行的实例*

进入这里。在第 4 节中，这成为一个特殊的

( i , j )的初始分布是不均匀的。我们不会

是爱丽丝（或鲍勃）唯一能做的作弊。

可以考虑更一般的情况，当

一个协议可以实现的最多的就是确保这个

表现得好像她有一个不同的变量值i 0 ，

*隐私约束。*

由于协议永远不能禁止 Alice（或 Bob）

*存在一个计算*f的协议，*它满足*( , δ ) *-*

作弊，而不要求任何一方透露变量。

**定理 1***对于任何*, δ > 0*和任何函数*f *，有*

背部。以下结果将表明可以阻止

稍后给出，这有时可能是一个严重的抽奖-

3. 上述要求也适用于 Bob。

他们的变量。将在应用程序中变得清晰

推定。然而，这将迫使双方透露

j上得到上述分布，并且

双方都必须披露他们所有的私人信息

和D的，那么概率至少为1 − δ她会

如果之后有验证阶段，则涵盖

E的评估不超过O ( N k )次

的确，根据我们的协议，任何作弊行为都将被禁止

2. 如果 Alice 之后尝试执行更多计算-

还是误导对方得到错误答案？

一世

他们可能会作弊以获得更多信息

其中G

是f ( i , j ) = v的j集合，

一世

由商定的协议规定的规则。如果其中任何一个怎么办

| G

|

对于j ∈ G

,否则为0 ,

一世

1. p

( j ) =

1 + O (  )

一世

1

讨论假设 Bob 和 Alice 遵守

`

´

**(B) 相互怀疑的参与者**。到目前为止，dis-

如果满足以下条件，则*约束：*

一世

这个p

( j ) 。一个协议被称为*满足*( , δ ) *-privacy*

*大*n *.*

计算j值的概率分布；称呼

( , δ ) *- 隐私约束必须有*T ( A ) > 2 n/ 2*所有*

值v和她所拥有的字符串，

n

F*的元素*

*计算*f*的协议*A

5

最后，爱丽丝原则上可以从她计算的

**定理 3***令*1

> , δ > 0*是固定的。设*f*是一个随机数*

根据协议忠实地进行计算。

值的可能性相同。假设 Bob 和 Alice 携带

进一步讨论）。

值函数。假设最初所有( i , j )

在没有隐私约束的情况下（参见 Yao [7]

**隐私约束**。令, δ > 0 , f ( i , j )为 0-1

最多n位传输信息可以计算f ，

函数f ( i , j )与i j是n位整数。清楚地，

n

k是预先选择的整数。

隐私约束。让F

成为价值 0-1 的家庭

Bob 和 Alice 的 D 的边界为O ( N k ) ，其中

Bob 和 Alice 之间传输的许多比特

E的评估总数

然而，存在需要指数级增长的函数

将函数值f设为私有。最后，我们要求

O执行协议

S log(1 /δ )

.

`

´

协议对每个参与者都有一个说明

Alice 和 Bob 都有图灵机算法



4

W是{ 1 , 2 , .的所有5元素子集的集合。 . . , 52 } ,

被K的所有参与者检测到。

以下情况： I = J = { 0 } ， q是一个常数， V =

r

r

∈ X

没有

例如，心理扑克将对应于

r ∈ K 0的行为与任何x不一致

r

执行A ，其中至少有一个参与者A

和

j∈J \_ \_

x∈W \_ \_

ij

| J |

F

( v, x )

由K 0 （相对于协议A ）是

我，v

磷

ij

在j上等于q

( j )(1 + O (  )) 。成功的*作弊*

1

F

( v, w )

X

以至少1 − δ的概率推断分布

到

T ( A )中的多项式计算量，它们仍然会

根据隐私约束，done 应该是相等的

K的参与者可以私下表演

h ( w ) Alice 可以从她的计算中推断出

( , δ ) - 私有*约束*如果对于每个非空K ，即使

情况q =常数。在这种特殊情况下，分布

可以推断。）令, δ > 0 。协议A被称为*满足*

这里，只是简单地举例说明特殊

我，v

重刑 f具有值v ，然后q

( j )是它们的分布

q和F方面进行精确；我们省略了它的完整代

除了它们唯一的变量值i之外，还有func -

对 Bob 的响应约束）。这个说法可以

其他参与者，如果唯一可用的信息，

可以从她的i值推断出 和v （加上一个cor -

推断变量值的概率分布

Alice 可以得到关于j和w不超过什么

r

ij

除此以外。 （如果所有参与者A

与r ∈ K 0共谋

F

( v, w ) 。隐私约束是信息

我，v

一世

( j ) = 1 / | G

( v ) |对于j ∈ G

( v )和0

一世

f ( x ) = v 。让q

一个值v ∈ V和 Bob 一个值w ∈ W的概率

钾

在H

和H

等于我 和j分别满足

0 \_

他们之间的圣人，所以最后爱丽丝将获得

1

2

米

(唯一向量) x = ( x

， X

, . . . ， X

) ，其投影

概率密度 q ∈ P ( I, J ) 。他们想送我——

一世

钾

钾

G

( v ) ⊆ H

是所有j ∈ H的集合

使得

知道j ∈ J ； ( i , j )的值服从某个初始值

钾

定义H

并且v ∈ V ，令

0 \_

相似地。对于任何我 ∈ H 0

关系。最初，Alice 知道i的值 ∈ I , 和 Bob

1

2

|克|

{ t

, t

, . . . , t

} = K。 \_令K 0 = { 1 , 2 , . . . , m } − K , 和

I, j ∈ J } ⊆ P ( V, W )是一个概率密度族-

1

2

|克|

钾

吨

吨

吨

ij

定义H

=

X

× X

× · · · × ×

， 在哪里

设I , J是整数的有限集。让F = { f

|一世 ∈

一世

∈ X

.对于任何非空K ⊆ { 1 , 2 , . . . , 米} ,

一世

其中x

P ( V, W )是所有这些概率密度的集合。

1

2

米

令V为函数f ( x

， X

, . . . ， X

) ,

如果p ( v, w )在v和w上的总和等于1 。让

我们现在使它精确。

V × W到区间[0 , 1]称为*概率密度*

如果多达m - 1 个不诚实的人试图帮助掩盖）。

( m = 2 )。设V和W是有限集。函数p来自

被所有诚实方（甚至

让我们考虑两方 Bob 和 Alice 的情况

有多少参与者可能串通，任何作弊行为都会

4 概率计算

可以在以下意义上满足约束：无论

勾结作弊。我们将证明，即使是最严重的

不知道爱丽丝询问了什么。

1

2

米

函数f ( x

， X

, . . . ， X

) ，多于一方可以

关于其中的数据的其他事情，而数据库系统

1

2

米

当m方A

， 一种

, . . . ， 一种

协作计算

爱丽丝可以在不知道任何事情的情况下得到查询的答案-

m - Party 案例的推广

数据库，Alice 正在询问查询编号i ，然后

gard Bob 作为一个数据库查询系统， j是

大约c ( log n ) 2位。

我一无所知 到底。如果我们重新

在 Bob 和 Alice 之间，而我们的方案只需要

计算一个平凡的函数g ( i , j ) =常数，意思是

众所周知的解决方案传输cn 一点信息

可能希望计算函数f ( i , j )并且 Bob 希望

依次从牌组中随机抽取一张牌。所有预

一世

一世

磷

正在计算不同的函数f

.特别是爱丽丝

有一副n张牌，爱丽丝和鲍勃各自想要

证明可以推广到每个人的情况

卡的数量变得更多。假设我们

**数据库的私有查询**。我们有的定理

此外，本解决方案使用更少的位作为

所涉及的单向函数的特殊性质。）

与结果一致，反之亦然。

tal poker 在 [2] 中为人所知，但该解决方案取决于

关于鲍勃的谈判策略的信息，除了它是

带有公开键的单向功能，用于玩男人-

显然，在爱丽丝不会获得任何

（而不是使用私钥）。 （一个特殊的解决方案

作为f ( i , j ) ，则可以进行谈判-

tative ，并且我们可以使用公钥系统播放它

一世

j

一种

,乙

已确定使用。写出结果

通勤的单向功能-

x美元，。 . . ) 将在实际策略后决定

它与 Shamir 等人不同。 al 的解决方案 [5]，因为我们这样做

1

2

你

作为B

,乙

, . . . ,乙

，然后是结果（没有交易，或以

扑克可以用任何通用的公钥系统来玩。

1

2

吨

Alice 作为A 的策略

， 一种

, . . . ， 一种

，以及鲍勃的那些

我们结果的一个有趣的推论是心理

记住谈判的例子。如果我们编号所有可能的

施加压力。我们不会在这里提供详细信息。

卖给鲍勃房子。原则上，每个人都有一个策略——

当隐私权受到限制时，tic 计算仍然可行

**不经意的谈判**。假设 Alice 试图

概率情况。基本上，一个合理的概率-

第 3 节中的结果对

偏僻的。

否则不变。

00

任何人成功作弊的概率非常高

F

( v, w )是0如果v和w 不相交且等于



5

对方的秘密。

越过，即被骗出它的秘密而没有得到

1979 年。

一种协议，使得诚实的一方不会双重

*(STOC'79)* ，第 209–213 页，美国佐治亚州亚特兰大，4 月

一种

乙

解x , y与E

( x ) = 1和E

( y ) = 1 。在那儿

*第 11 届 ACM 计算理论研讨会*

3.2 .假设 Alice 和 Bob 希望交换一对

到分布式计算。在*会议记录中*

第二个结果对 Sec- 中定义的模型有效

[7] Andrew C. Yao.一些相关的复杂性问题

加利福尼亚州，伯克利，美国，1981 年。

*带有先验偏差α*可以*是稳健的。*

指定的电子邮件。技术报告，大学

**定理 7***没有具有有限*T ( A )*的协议*A*生成-*

如何交换秘密；第三部分：如何发送证书-

如果有人作弊，偏见仍然是正确的。

转账：第一部分：电话抛硬币；第二部分：

如果\_ *\_* \_

[6] 曼努埃尔·布鲁姆。遗忘的三个应用

的人通过产生有偏见的位来作弊。让我们

萨科塞特理工学院。

α的性质是它保持无偏，即使

心理扑克。技术报告 LCS/TR-125, Mas-

1

2

3

一个。现在让α = α

+ α

+ α

，我们得到一个无偏的

[5] Adi Shamir、RL Rivest和 Leonard M. Adleman 。

3

将其发送给C ， C生成一个随机α

并将其发送到

1

2

21(2):120–126，1978 年 2 月。

位α

并将其发送给B ， B生成一个随机α

和

密钥密码系统。 *ACM的通讯*，

米 > 2 。例如A生成一个随机无偏

一种获取数字签名和公共信息的方法

带有偏差α的位。很容易看出它是如何做到的

[4] RL Rivest 、 Adi Shamir 和 Leonard M. Adleman 。

本文中给出。假设m个人试图产生一个

技术，1979 年。

第一个不可能结果对所有三个模型都有效

cal报告 LCS/TR-212，麻省理工学院

通过任何协议。我们在这里只会提到两个结果。

函数像因式分解一样难以处理。技术-

存在无法实现的安全约束

[3] 莫拉宾。数字签名和公钥

6 什么不能做？

1982 年。

定理 5。

第 365–377 页，美国加利福尼亚州旧金山，5 月

安全标准仅比中给出的稍微放宽

*计算理论研讨会（STOC'82）* ，

1

2

米

1

2

米

f ( x

， X

, . . . ， X

) = x

+ x

+ · · · + x

(mod q ) , 在 a 下

部分信息。在*第 14 届 ACM 会议记录中*

是多项式，对于m 计算函数的各方

重刑以及如何玩心理扑克保密所有

运行时间为O ( p ( m ) log q )的协议，其中p ( m )

[2] S. Goldwasser和 S. Micali 。概率加密-

这么不严格的要求。例如，有

*理论*，IT-22(6):644–654, 1976 *。*

可以设计具有更好运行时间的tocols

密码学中的问题。 *IEEE Transactions on Infor -*

计算为某个值。）有时亲

[1] Whitfield Diffie和 Martin E. Hellman。新方向——

要求没有子集K 0能够强制结果

肯定是足够的。 （例如，一个人可能只

参考

强的。对于某些目的，不太严格的测量

交换秘密的协议。

我们上面考虑的安全措施是

甚至（私人通讯，1981）也设计了一些

m中的多项式。

特殊类型的秘密），作弊的机会消失了。

有运行时间满足定理 5 的协议

大合数的交换因子（一个特殊的-

x中 1 的数量（ x是布尔变量）

以前站在一边。 Blum [6] 表明

2

米

1

2

米

X

⊕ · · · ⊕ x

和*计数函数*f ( x

， X

, . . . ， X

) =

不同类型的交换秘密已经成为

1

2

米

1

例如，*奇偶函数*f ( x

， X

, . . . ， X

) = x

⊕

运行时间超过定理 5 中给出的界限。对于

*任何人双交叉成功的次数都以*为界*。*

乙

在特殊情况下，协议可以设计得更好

*小白点* D

( w )*和*D

一种

( u ) *，并且在该概率下*

*多项式（以*N为单位*）运行时间交换 se-*

1

2

米

T ( A ) = Ω

| X

| · | X

| · . . . · | X

|

*.*

1 / 4

**定理 9***令* > 0*是固定的。有一个协议*A

`

´

“

”

*满足定理 5 条件的col* A必须有

一种

乙

函数E

和E

操作。

**定理 6***存在函数*f *，其中任何原型*

认识你。令N为加密的位数

如下一个定理所示。

Bob 不知道w的值， Alice 也不知道

2

米

一种

| X

| · . . . · | X

| · | V | ) ，这在一般情况下几乎是最佳的

鲍勃想知道E的解x

( x ) = u ，但是

1

乙

上述定理中T ( A )的值为O ( | X

| ·

姿势 Alice 想知道E的解y

( y ) = w

在同一模型中可以更改秘密。超-

*作弊不能超过*γ *。*

值得一提的是，另一种类型的前

{ 1 , . . . , m } *,* K 0*成功的概率*

*应变并且具有以下性质，对于任何*K 0 =

*以至少*1 / 2的概率成功交叉*。*

A*用于计算满足*(  , δ ) *-private con-*

*克里特。那么爱丽丝或鲍勃将能够加倍*

**定理 5***对于任意*, δ, γ > 0 *，存在一个协议*

**定理 8***设*A*是任何交换服务的协议*