第 26 卷　第 2 期　　计　算　机　学　报　　Vol. 26　No. 2
2003 年 2 月　　CHINESE JOURNAL OF COMPUTERS　　Feb. 2003

无条件安全的不经意传输

杨　波[1)]　　陈　恺[2)]

[1)]（西安电子科技大学 ISN 国家重点实验室　西安 710071）

[2)]（贝尔实验室(中国)　北京 100080）

摘　要　讨论了基于阶大于 1、小于 2 的任意阶 Rényi 熵的保密增强在实现不经意传输协议时的安全性条件. 协议中未对接收方的计算能力做任何限制性假设,因而在所给的安全性条件下,协议是无条件安全的.

关键词　不经意传输;Rényi 熵;保密增强;无条件安全

中图法分类号: TP309

Unconditionally-Secure Oblivious Transfer

YANG Bo[1)]　CHEN Kai[2)]

[1)]（*National Laboratory on ISN*, *Xidian University*, *Xi'an* 710071）

[2)]（*Bell Labs Research*（*China*）, *Beijng* 100080）

Abstract　This paper investigates oblivious transfer protocol based on privacy amplification that uses Rényi entropy of order α for any $1<\alpha<2$, and the conditions under which the protocol is secure are given. The protocol makes no assumptions about receiver's computing power, so under the given conditions the protocol is unconditionally-secure.

Keywords　oblivious transfer; Rényi entropy; privacy amplification; unconditionally-secure

1　引　言

不经意传输是密码学中的一个基本协议,可用于实现比特承诺、零知识证明、安全的多方计算、电子支付等协议.

不经意传输有以下 5 种类型:

OT:Alice 可以 1/2 的概率向 Bob 传递一个比特 b,Bob 有一半的机会收到 Alice 送来的 b,另一半机会则得不到任何有关 b 的信息,而 Alice 不知道 Bob 是不是收到了 b[1].

$\binom{2}{1}$-OT:Alice 向 Bob 发送两个比特 b_0, b_1, Bob 只能收到其中一个比特,但 Alice 不知道 Bob 收到的是哪个比特[2].

$\binom{2}{1}$-OT^k:Alice 向 Bob 发送两个 k 比特的串, Bob 只能收到其中的一个串,但 Alice 不知道 Bob 收到的是哪个串[2].

GOT:Alice 向 Bob 发送两个比特 b_0,b_1,Bob 可任意选择一个函数 f:$\{0,1\}^2\rightarrow\{0,1\}$ 以获得 $f(b_0,b_1)$,但 Alice 不知道 f[3].

UOT:Alice 向 Bob 发送一个取值于集合 $\mathscr{X}$ 的随机变量 X(文中随机变量用大写字母表示,取值集合用相应的花体字母表示),Bob 对 X 的任一特定取值 x,可秘密指定 Y 的分布 $P_{Y|X=x}$ 以接收随机变量 Y,但由 Y 不能得出 X 的全部信息[4].

文献[2]使用称为自交叉码的一种特定类型的纠错码将 $\binom{2}{1}$-OT^k 的实现归约为 $\binom{2}{1}$-OT 的实现,文献

收稿日期:2000-12-04;修改稿收到日期:2002-07-04. 本课题得到国家自然科学基金(69972034)和国家“八六三”高技术研究发展计划项目(2002AA144010)资助. **杨　波**,男,1963 年生,博士,教授,研究方向为信息论、电子商务中的安全理论与技术. E-mail: yangbo@mail.xidian.edu.cn. **陈　恺**,男,1970 年生, 博士,研究方向为信息论、电子商务中的安全理论与技术.

[5]利用二阶 Rényi 熵的保密增强技术将 $\binom{2}{1}$-OT^k 和 GOT 的实现归约为 $\binom{2}{1}$-OT 的实现，文献[4]利用最小熵的保密增强技术将 $\binom{2}{1}$-OT^k 的实现归约为 UOT 的实现，其安全性证明中使用了称为破坏知识(spoiling knowledge)的边信息，这种边信息将使得 Bob 关于 Alice 的输入的 Rényi 熵增大. 然而对于不诚实的接收者来说，为了获得 Alice 发送的更多的信息，其目的应使自己关于 Alice 的输入的 Rényi 熵减少.

本文使用的协议与文献[4,5]相同，但使用阶大于 1、小于 2 的任意阶 Rényi 熵的保密增强，保密增强是从一个随机变量中提取一个更短的几乎均匀分布的值，从而减少原随机变量的部分信息的一个过程[6]. 文献[7,8]指出，使用阶大于 1 小于 2 的任意阶 Rényi 熵的保密增强效果优于使用二阶 Rényi 熵和最小熵的保密增强，而且本文的安全性证明中避免使用破坏知识的边信息.

2　一些概念和结果

定义 1[7~9].　$\alpha\geq 0$ 且 $\alpha\neq 1$，X 的 α 阶 Rényi 熵定义为 $H_\alpha(X)=\dfrac{1}{1-\alpha}\log\sum_{x\in\mathscr{X}}P_X(x)^\alpha$，其中对数以 2 为底，下同.

$\alpha=2$ 时为 $H_2(X)=-\log\sum_{x\in\mathscr{X}}P_X(x)^2$，而 Shannon 熵 $H(X)=-\sum_{x\in\mathscr{X}}P_X(x)\log P_X(x)$ 可看作是 $H_\alpha(X)$ 当 $\alpha\to 1$ 时的极限情况.

与 Shannon 熵不同，$H_\alpha(X|Y)>H_\alpha(X)$ 与 $H_\alpha(XY)=H_\alpha(X)+H_\alpha(Y|X)$ 一般不成立.

定义 2[7~9].　设 X,Y 为取值于同一集合 $\mathscr{X}$ 的两个随机变量，概率分布分别为 P_X,P_Y，X 与 Y 的相对熵定义为 $D(P_X\parallel P_Y)=\sum_{x\in\mathscr{X}}P_X(x)\log\dfrac{P_X(x)}{P_Y(x)}$.

如果 P_Y 是 X 上的均匀分布，则 $D(P_X\parallel P_Y)=\log|\mathscr{X}|-H(X)$.

下面引入平滑熵的概念，对随机变量 X，函数 $f:X\to Y$ 使得 $Y=f(X)$ 在其取值集合 $\mathscr{Y}$ 上是足够均匀分布的，则称 f 为平滑函数，$|\mathscr{Y}|$ 称为相对于完全均匀分布在允许的偏差范围内 X 的平滑熵. 用 $M(X)$ 来度量偏差，常取为相对熵 $D(P_X\parallel P_U)$，其中 $P_U(x)=\dfrac{1}{|\mathscr{X}|}$ 是 X 上的均匀分布. 正式定义如下：

定义 3[7~9].　设 M 是非均匀性度量，$\Delta:\mathscr{R}\to\mathscr{R}$ 是一递减的非负函数，X 是取值于集合 $\mathscr{X}$ 的随机变量，称 X 以概率 $1-\varepsilon$ 在偏差范围 $\Delta(s)$（关于 M）内有平滑熵 $\Psi(X)$，如果 $\Psi(X)$ 是满足以下条件的最大的 ψ：对任意安全参数 $s\geq 0$，存在一随机变量 T 和一个函数 $f:\mathscr{X}\times\mathscr{T}\to\mathscr{Y}$，$|\mathscr{Y}|=\lfloor 2^{\psi-s}\rfloor$，使得有一概率至多为 ε 的失败事件 E，在已知 T 和 $\bar{E}$ 时，$Y=f(X,T)$ 的非均匀性度量 M 在 T 上的均值至多为 $\Delta(s)$，即

$$\begin{aligned}\Psi(X)=\max_{\psi}\{\psi\mid\ &\forall s\geq 0:\exists T,\\ &f:\mathscr{X}\times\mathscr{T}\to\mathscr{Y},\ |\mathscr{Y}|=\lfloor 2^{\psi-s}\rfloor:\\ &Y=f(X,T),\exists E:P[E]\leq\varepsilon,\\ &M(Y\mid T\bar{E})\leq\Delta(s)\}.\end{aligned}$$

定理 1[7~9].　设 $1<\alpha<2$，$r,t>0$，m 是满足 $m-\log(m+1)>\log|\mathscr{X}|+t$ 的整数，s 是平滑熵的安全参数，则随机变量 X 在误差范围 $\dfrac{2^{-s}}{\ln 2}$（以相对熵度量）内的平滑熵 $\Psi(X)$ 以概率 $1-2^{-r}-2^{-t}$ 有以下关系：$\Psi(X)\geq H_\alpha(X)-\log(m+1)-\dfrac{r}{\alpha-1}-t-2$.

定义 4[10].　函数族 $\mathscr{F}:\mathscr{A}\to\mathscr{B}$ 称为 $\mathrm{Universal}_2$（简称 Universal）的条件是对 $\forall x_1,x_2\in\mathscr{A}$ 且 $x_1\neq x_2$，$f(x_1)=f(x_2)$ 成立的概率最多为 $1/|\mathscr{B}|$，其中 f 从 $\mathscr{F}$ 中均匀选择.

定理 2 是使用阶大于 1 小于 2 的任意阶 Rényi 熵的保密增强定理.

定理 2[7,8].　设 α,r,t,m,s 与定理 1 相同，v 是 W 的边信息 V 的一个特定值，G 是从 $\mathscr{W}\to\{0,1\}^k$ 的 Universal hash 函数族中随机选取的一个函数，$K=G(W)$，则 K 的长度 k 以概率 $1-2^{-r}-2^{-t}$ 有以下关系：

$$k\leq H_\alpha(W\mid V=v)-\log(m+1)-\frac{r}{\alpha-1}-t-2-s\ ,$$

且通过边信息 V 获得的关于 K 的信息量 $\leq\dfrac{2^{-s}}{\ln 2}$.

证明.　由平滑熵的定义，$|\mathscr{K}|=\lfloor 2^{\psi(W|V=v)-s}\rfloor\leq 2^{\psi(W|V=v)-s}$，$k=\log|\mathscr{K}|\leq\psi(W|V=v)-s$. 取 $k\leq H_\alpha(W|V=v)-\log(m+1)-\dfrac{r}{\alpha-1}-t-2-s$ 即满足平滑熵的定义（以概率 $1-2^{-r}-2^{-t}$）. 由定理 1 及相对熵的定义，$H(X)=\log|\mathscr{X}|-D(P_X\parallel P_U)\geq\log|\mathscr{X}|-\dfrac{2^{-s}}{\ln 2}$.

所以 $H(K|G,V=v)\geq\log|\mathscr{K}|-\dfrac{2^{-s}}{\ln 2}=k-\dfrac{2^{-s}}{\ln 2}$，等价

于通过边信息 V 获得的关于 K 的信息量$\le\frac{2^{-s}}{\ln 2}$.

证毕.

3 不经意传输协议

$\binom{2}{1}$-$OT^k(w_0,w_1)(c)$协议由 Alice 向 Bob 传送两个 k 比特的串 w_0 和 w_1，它的实现归约为$UOT(X,Y)$的实现，其中 $X=\{0,1\}^{2n}$. 具体过程如下：

Step1. 设 $X=X_0X_1$，其中 X_0 和 X_1 是由 Alice 随机选择的两个长为 n 的比特串，X 是 X_0 和 X_1 的级联.

Step2. Alice 和 Bob 运行 $UOT(X,Y)$，其中 Bob 对 X 的任一特定取值 x，秘密指定 Y 的分布 $P_{Y|X=x}$ 以获得 $Y=X_c$.

Step3. Alice 从$\{0,1\}^n\to\{0,1\}^k$的 Universal hash 函数族中随机选取两个函数 G_0，G_1，并通知 Bob.

Step4. Alice 计算 $M_0=G_0(X_0)$，$M_1=G_1(X_1)$，并将 $Z_0=M_0\oplus w_0$ 和 $Z_1=M_1\oplus w_1$ 发送给 Bob，其中$\oplus$表示逐比特异或.

Step5. Bob 计算 $w_c=G_c(Y)\oplus Z_c$.

协议对 Bob 是安全的是指 Alice 不知道 c，这可由 Step2 中的 $UOT(X,Y)$ 决定；协议对 Alice 是安全的是指 Bob 只能收到 w_0 和 w_1 中的一个，如果收到的是 w_0，则知道的有关 w_1 的信息应任意少，反之亦然. 由 Step4 可知，Alice 对 w_0 和 w_1 使用 M_0 和 M_1 进行一次一密加密，因此 Alice 的安全性取决于 M_0 和 M_1 的安全性，进而取决于 X 的安全性. 因为 w_0 和 w_1 的长度 k 是一定的，可以想象如果 X 的长度过短或已知 Y 时 X 的 α 阶 Rényi 熵过小，Step4 中 Alice 泄露给 Bob 的信息量将很大，从而无法保证自己的安全性. 下面考虑 X 的长度和已知 Y 时 X 的 α 阶 Rényi 熵的最小值.

为了比较 $H_\alpha(X_0|Y=y)$ 和 $H_\alpha(X_1|Y=y,X_0=x_0)$ 的大小，首先需要以下引理.

引理 1. 设 R 是长为 N 的比特串，对任意 N_1 元组$(i_1,i_2,\cdots,i_{N_1})$(其中 $1\le i_1<i_2<\cdots<i_{N_1}\le N$)，设 S 表示 R 的子串$(R_{i_1},R_{i_2},\cdots,R_{i_{N_1}})$，那么

$$H_\alpha(S)\ge H_\alpha(R)-(N-N_1).$$

证明. 对固定的串 $s=(r_{i_1},r_{i_2},\cdots,r_{i_{N_1}})$，$R$ 可有 2^{N-N_1} 个值$(r_1,r_2,\cdots,r_N)$与其对应，设 $p_1,p_2,\cdots,p_{2^{N-N_1}}$ 是这些串的概率，令$p_0=P_S(s)=\sum_{i=1}^{2^{N-N_1}}p_i$，则

$$\sum_{i=1}^{2^{N-N_1}}p_i^\alpha=p_0^{\alpha-1}\sum_{i=1}^{2^{N-N_1}}\left(\frac{p_i}{p_0}\right)^{\alpha-1}p_i\ge p_0^{\alpha-1}\left(\frac{1}{2^{N-N_1}}\right)^{\alpha-1}\sum_{i=1}^{2^{N-N_1}}p_i$$
$$=\frac{p_0^\alpha}{2^{(N-N_1)(\alpha-1)}},\ p_0^\alpha\le 2^{(N-N_1)(\alpha-1)}\sum_{i=1}^{2^{N-N_1}}p_i^\alpha，所以$$

$$\sum_{s\in\{0,1\}^{N_1}}P_S(s)^\alpha=\sum_{s\in\{0,1\}^{N_1}}p_0^\alpha\le 2^{(N-N_1)(\alpha-1)}\sum_{s\in\{0,1\}^{N_1}}\sum_{i=1}^{2^{N-N_1}}p_i^\alpha$$
$$=2^{(N-N_1)(\alpha-1)}2^{N_1}\sum_{i=1}^{2^{N-N_1}}p_i^\alpha=2^{(N-N_1)(\alpha-1)}\sum_{r\in\{0,1\}^N}P_R(r)^\alpha\cdot$$
$$\log\sum_{s\in\{0,1\}^{N_1}}P_S(s)^\alpha\le(N-N_1)(\alpha-1)+\log\sum_{r\in\{0,1\}^N}P_R(r)^\alpha.$$

两边同除以 $1-\alpha$ 得 $H_\alpha(S)\ge H_\alpha(R)-(N-N_1)$.

证毕.

由上述引理得以下推论.

推论 1. 设 $X=X_0X_1$，其中 X_0 和 X_1 是两个长为 n 的比特串，那么

$$H_\alpha(X_0\mid Y=y)\ge H_\alpha(X\mid Y=y)-n.$$

引理 2[9]. 设 $1<\alpha<2$，$r,t>0$，对任意随机变量 X 和 Y，Y 取值 y 使得

$$H_\alpha(X|Y=y)\ge H_\alpha(XY)-\log|\mathcal{Y}|-\frac{r}{\alpha-1}-t$$

成立的概率至少为 $1-2^{-r}-2^{-t}$.

由引理 2 可得

$$\begin{aligned}&H_\alpha(X_1\mid Y=y,X_0=x)\\&\ge H_\alpha(X_0X_1\mid Y=y)-\log|\mathcal{X}_0|-\frac{r}{\alpha-1}-t\\&=H_\alpha(X\mid Y=y)-n-\frac{r}{\alpha-1}-t.\end{aligned}$$

将 $H_\alpha(X_1|Y=y,X_0=x_0)$取为最小，$H_\alpha(X_1|Y=y,X_0=x)=H_\alpha(X|Y=y)-n-\frac{r}{\alpha-1}-t$ 可保证 $H_\alpha(X_0|Y=y)\ge H_\alpha(X_1|Y=y,X_0=x_0)$以至少 $1-2^{-r}-2^{-t}$ 的概率成立，所以对协议中的两次保密增强，只需考虑第二次(即将 $H_\alpha(X_1|Y=y,X_0=x_0)$ 用于 Universal hash 函数 G_1)的安全性要求.

定理 3. 设 $1<\alpha<2$，取常数 r 和 t 均大于 1，m 是满足 $m-\log(m+1)>n+t$ 的常数，$s\ge 0$ 是安全参数. 又设 $X=X_0X_1$ 是两个长为 n 的比特串 X_0 和 X_1 的级联. 则当

$$n\ge k+\log(m+1)+\frac{2r}{\alpha-1}+2t+2+s,$$

$$H_\alpha(X\mid Y=y)\ge 2\left[k+\log(m+1)+\frac{2r}{\alpha-1}+2t+2+s\right]$$

时，协议$\binom{2}{1}$-$OT^k(w_0,w_1)(c)$的实现可以至少 $1-2^{-r+1}-2^{-t+1}$ 的概率安全地归约为协议 $UOT(X,Y)$ 的实现.

证明. 由定理 2，$k\le H_\alpha(X_1|Y=y,X_0=x_0)-\log(m+1)-\frac{r}{\alpha-1}-t-2-s$，所以

$$H_\alpha(X_1 \mid Y=y, X_0=x_0) \geq k+\log(m+1)+\frac{r}{\alpha-1}+t+2+s \quad (1)$$

即

$$H_\alpha(X \mid Y=y)-n-\frac{r}{\alpha-1}-t \geq k+\log(m+1)+\frac{r}{\alpha-1}+t+2+s \quad (2)$$

所以

$$H_\alpha(X|Y=y) \geq n+k+\log(m+1)+\frac{2r}{\alpha-1}+2t+2+s \quad (3)$$

又因为 $2n \geq H_\alpha(X \mid Y=y)$，所以 $2n \geq n+k+\log(m+1)+\frac{2r}{\alpha-1}+2t+2+s$，即

$$n \geq k+\log(m+1)+\frac{2r}{\alpha-1}+2t+2+s \quad (4)$$

所以

$$H_\alpha(X \mid Y=y) \geq 2\left[k+\log(m+1)+\frac{2r}{\alpha-1}+2t+2+s\right].$$

证毕.

由式(1)及定理 2 知，Bob 获得 X_0 进而获得 w_0 后，得到的关于 X_1 进而关于 w_1 的信息量以至少 $1-2^{-r}-2^{-t}$ 的概率满足 $I(X_1, X_0 Y) \leq \frac{2^{-s}}{\ln 2}$.

因为式(1)和(2)成立的概率都至少为 $1-2^{-r}-2^{-t}$，所以以上过程不成立的概率至多为 $1-(1-2^{-r}-2^{-t})\cdot(1-2^{-r}-2^{-t})<2^{-r+1}+2^{-t+1}$.

4 结 论

用基于阶大于 1 小于 2 的任意阶 Rényi 熵的保密增强来实现对两个 k 比特消息的不经意传输协议时，只要发方在保密增强过程中输入的变量的长度及其条件 Rényi 熵(以接收方掌握的关于输入的信息为条件)分别大于与 k 相关的两个常量时，就可以一定的概率保证接收方得到其中一个 k 比特消息后，对另一 k 比特消息的信息量为任意小. 协议未对接收方的计算能力做任何限制性假设，因而是无条件安全的.

参 考 文 献

1 Rabin M O. How to exchange secrets by oblivious transfer. Harvard University：Technology Report：TR-81，1981

2 Even S，Goldreich O，Lempel A. A randomized protocol for signing contracts. In：Proc CRYPTO'82，1983. 205～210

3 Brassard G，Crépeau C，Robert J M. Information theoretic reductions among disclosure problems. In：Proc the 27th IEEE Symposium on Foundations of Computer Science，1986. 168～173

4 Cachin C. On the foundations of oblivious transfer. In：Proc EUROCRYPT'98，Lecture Notes in Computer Science，Springer-Verlag，1998. 361～374

5 Brassard G，Crépeau C. Oblivious transfer and privacy amplification. In：Proc EUROCRYPT'97，Lecture Notes in Computer Science，Springer-Verlag，1997. 334～347

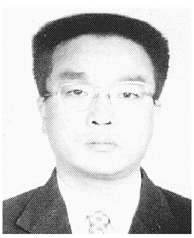
6 Bennett C H，Brassard G，Crepeau C，Maurer U M. Generalized privacy amplification. IEEE Trans Information Theory，1995，41(6)：1915～1923

7 Yang Bo，Zhang Tong，Wang Yu-Min. Distillation of unconditionally-secure secret-key based on smooth entropy. Acta Electronica Sinica，2001，29(7)：930～932(in Chinese)
(杨 波，张 彤，王育民. 基于平滑熵的无条件安全秘密钥的提取. 电子学报，2001，29(7)：930～932)

8 Yang Bo，Zhang Tong，Wang Yu-Min. Distillation of unconditionally-secure secret-key against active adversaries based on smooth entropy. Acta Electronica Sinica，2001，29(10)：1349～1351(in Chinese)
(杨 波，张 彤，王育民. 基于平滑熵的防主动攻击的无条件安全秘密钥的提取. 电子学报，2001，29(10)：1349～1351)

9 Cachin C. Smooth entropy and Rényi entropy. In：Proc EUROCRYPT'97，Lecture Notes in Computer Science，Springer-Verlag，1997. 193～208

10 Carter J L，Wegman M N. Universal classes of hash functions. Journal of Computer and System Sciences，1979，18(2)：143～154



YANG Bo，male，born in 1963，Ph. D.，professor. His research interests include information theory and electronic commerce.

Chen Kai，male，born in 1970，Ph. D.. His research interests include information theory and electronic commerce.