因子分解假设的复合模广义迪菲赫尔曼问题的伪随机提取

梅其祥[1),2)] 李 宝[1)] 路献辉[1)]

[1)](中国科学院研究生院信息安全国家重点实验室 北京 100049)

[2)](广东海洋大学信息学院 广东 湛江 524088)

摘 要 研究怎样在因子分解假设下有效地提取复合模数上的广义菲赫尔曼问题的伪随机比特串.证明了 Blum-Blum-Shub 生成器是一个合适的广义菲赫尔曼问题提取器.利用 Naor-Reingold-Rosen 伪随机函数中的技巧证明:在因子分解假设下,对于任意的$\{1,2,\cdots,n\}$上的真子集合 A,即使公开了 $g^{\prod_{i\in A}a_i}$,$BBS_r(g^{\prod_{i=1}^{n}a_i})$ 仍然是伪随机的(其中,g 是平方剩余群 QR_N 上的生成元,N 为 Blum 整数).利用该结论,在因子分解假设下,可以得到不可区分意义安全的公钥加密和密钥交换协议.

关键词 随机提取;Blum-Blum-Shub 生成器;因子分解假设;广义迪菲赫尔曼问题

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2011.01308

Pseudo-Randomness Extraction for Generalized Diffie-Hellman Problem over Composite Modulus Under Factoring Assumption

MEI Qi-Xiang[1),2)] LI Bao[1)] LU Xian-Hui[1)]

[1)](*State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing* 100049)

[2)](*School of Information, Guangdong Ocean University, Zhanjiang, Guangdong* 524088)

Abstract This paper studies how to efficiently extract the pseudo-random bits string from the Generalized Diffie-Hellman (GDH) problem over composite modulus under the factoring assumption. It is proven that Blum-Blum-Shub(BBS) generator is a suitable extractor for GDH problem over composite modulus. In particular, adapting the technique used in the proof of Naor-Reingold-Rosen pseudorandom function, it is proven that $BBS_r(g^{\prod_{i=1}^{n}a_i})$ is pseudo-random even if $g^{\prod_{i\in A}a_i}$ is given for any proper subset A of $\{1,2,\cdots,n\}$, where g is a random element of quadratic residues group QR_N, N is a Blum integer. The result can be used to obtain public key encryption and key exchange protocol secure in the sense of indistinguishability under factoring assumption.

Keywords randomness-extraction; Blum-Blum-Shub generator; factoring assumption; Generalized Diffie-Hellman problem

1 引 言

复合模数上的广义迪菲赫尔曼(Generalized Diffie-Hellman, GDH)问题有一个很好的性质:其难解性可以归结为因子分解假设[1-2].更确切地说,在因子分解下,对于任意的$[n]=\{1,2,\cdots,n\}$上的真子集 A,即使给定 $g^{\prod_{i\in A}a_i}$,$g^{\prod_{i=1}^{n}a_i}$ 仍然是难以计算的.如,当 $n=2$ 时,给定 g^{a_1},g^{a_2} 后,$g^{a_1a_2}$ 仍然是难以

收稿日期:2010-07-05;最终修改稿收到日期:2010-11-23.本课题得到国家自然科学基金(60862001、61070171)、国家"九七三"重点基础研究发展规划项目基金(2007CB311201)和中国博士后基金(20090460565)资助.**梅其祥**,男,1973 年生,博士后,副教授,研究方向为可证明安全公钥密码学.E-mail: nupf@163.com. **李 宝**,男,1962 年生,博士,教授,研究领域为密码学基础. **路献辉**,男,1980 年生,博士后,研究方向为可证明安全公钥密码学.

计算的；当 $n=3$ 时，给定 $g^{a_1}, g^{a_2}, g^{a_3}, g^{a_1a_2}, g^{a_2a_3}, g^{a_1a_3}$ 后，$g^{a_1a_2a_3}$ 是难以计算的.

基于 GDH 问题，可以构造密钥交换协议和公钥加密[3-4]. 当 $n=2$ 时，可以构造复合模数上的 Diffie-Hellman 密钥交换协议、复合模数上的 ElGamal 加密；$n\geq 3$ 时，可以构造复合模数上的多方 Diffie-Hellman 密钥交换协议. 但是，直接应用 GDH 问题，所得方案只是在单向性的意义下是安全的，原因是我们只能保证 $g^{\prod_{i=1}^{n}a_i}$ 的单向安全性. 在实际的密码方案中，我们还需要由 $g^{\prod_{i=1}^{n}a_i}$ 得到会话密钥，要求该会话密钥是在不可区分意义下是安全的. 为此，我们需要一个 GDH 问题的密钥提取器来对 $g^{\prod_{i=1}^{n}a_i}$ 进行随机提取.

一种方法是将通用散列函数作为的 GDH 问题密钥提取器[5]. 但这种方法需要假设判定性迪菲赫尔曼(Decisional Diffie-Hellman，DDH)问题是难解的. 还有一种方法是用难核预测器(hard-core predicate)来作为密钥提取器[6]. 这种方法的好处是可以基于因子分解假设，缺点是一次模指数运算只能一次提取一个比特，因而效率太低，不满足实际需要.

一个自然的问题是如何在因子分解假设下构造高效的复合模数上的 GDH 问题的密钥提取器.

本文中我们证明了 Blum-Blum-Shub(BBS)生成器[7]是复合模数上的 GDH 问题的满足前面要求的密钥提取器. 大致地说，我们证明了，假设分解模数 N 是困难的，对于任意的 $[n]$ 上的真子集 A，即使给定 $g^{\prod_{i\in A}a_i}$，$BBS_r(g^{\prod_{i=1}^{n}a_i})$ 仍然是伪随机的. 其中 BBS 生成器 $BBS_r(u)$ 提取比特串 $(B_r(u), B_r(u^2), \cdots, B_r(2^{\ell_K-1}))$，而 $B_r(u)$ 表示 r 与 u 的内积比特，$\langle u,r\rangle \bmod 2$. 由于提取一个比特只需要一次模平方运算，因此，该提取器的效率很高.

2　构造和安全性定义

2.1　提取器的构造

该提取器由密钥产生算法 KGE_{BBS} 和密钥提取算法 KEX_{BBS} 组成.

KGE_{BBS}：根据安全参数 λ，KGE_{BBS} 随机地选取两个 $m(\lambda)$ 比特的素数 P,Q 且满足 $P\equiv Q\equiv 3 \bmod 4$，取 $N=PQ$(因此 N 是 Blum 整数)；接着，KGE_{BBS} 从 $[(N-1)/4]$ 随机地选取 $n(\lambda)$ 个元素，用向量 $\boldsymbol{a}=(a_1,a_2,\cdots,a_n)$ 表示；从 QR_N 中随机地选取一个元素 g，并随机选取一个与 N 等长的比特串 r；最后，输出 $(g,\boldsymbol{a},N,r)$.

KEX_{BBS}：根据输入 $(g,\boldsymbol{a},N,r)$，KEX_{BBS} 计算长度为 ℓ_K 的比特串 K：$K=BBS_r(g^{\prod_{i=1}^{n}a_i}) \stackrel{\text{def}}{=} B_r(g^{\prod_{i=1}^{n}a_i}), B_r(g^{2\prod_{i=1}^{n}a_i}), \cdots, B_r(g^{2^{\ell_K-1}\prod_{i=1}^{n}a_i})$，其中，$B_r(u)$ 表示内积 $\langle u,r\rangle \bmod 2$.

2.2　安全性

对于上面的提取器，安全性要求对于任意的多项式时间攻击者 M 在下面的与挑战者 C 的游戏中获得的优势可以忽视：

首先，M 激起 KGE 询问，挑战者 C 运行 KGE_{BBS}，将 (g,N,r) 给 M；

接着，M 激起若干次 Observe 询问，每次使用不同的 $[n]$ 真子集，用 A 表示. C 计算 $g^{\prod_{i\in A}a_i}$，将结果给 M；

M 发起 Challenge 询问，C 随机地选取比特 b，计算 $K_0=KEX_{BBS}(g,\boldsymbol{a},N,r)$，并选取一个随机的比特串 $K_1=(b_0,\cdots,b_{\ell_K-1})$，将 K_b 给 M；

最后，M 输出一个比特 b' 作为对比特 b 的猜测.

M 的优势定义为 $Adv_{\mathrm{BBS,M}}^{\mathrm{IND}}(\lambda)=|Pr[M(K_0)=1]-Pr[M(K_1)=1]|$.

另外，我们用 $H_{g,\boldsymbol{a},N,r}^{J}(J=0,\cdots,\ell_K)$ 表示混合实验：该试验基本与上面定义的游戏相同，但对 Challenge 询问的回答改为

$$(b_0,b_1,\cdots,b_{J-1},B_r(g^{2^J\prod_{i=1}^{n}a_i}),B_r(g^{2^{J+1}\prod_{i=1}^{n}a_i}),\cdots,B_r(g^{2^{\ell_K-1}\prod_{i=1}^{n}a_i})),$$

即前 J 比特与 K_1 中相同，而后 ℓ_K-J 比特与 K_0 中相同. 这样，$H_{g,\boldsymbol{a},N,r}^{0}$ 中，攻击者看到的比特串的分布与 K_0 的分布相同，在 $H_{g,\boldsymbol{a},N,r}^{\ell_K}$ 中，攻击者看到的比特串的分布与 K_1 的分布相同.

3　安全性证明

本节证明上节构造的提取器在因子分解假设下是安全的.

证明可通过下面 3 个引理完成.

引理 1.　如果存在一个多项式时间攻击者 M 在上节构造的提取器中可以获得的优势 $Adv_{BBS,M}^{IND}(\lambda)$ 为 $\varepsilon(\lambda)$，则存在一个多项式时间攻击者 $D(v^2,N,r,$

α)可以区分 α 是 $B_r(uw)$ 或是一个随机比特 b 的优势为 $\varepsilon'(\lambda)$. 其中,u 是唯一满足 $u^2=v^2$ 的平方剩余,w 是一个由 v^2 和 D 所用的内部随机数决定的平方剩余,$\varepsilon'(\lambda)$ 等于 $(\varepsilon(\lambda)-n(\lambda)O(2^{-m(\lambda)}))/\ell_K$.

证明. 给定输入 (v^2,N,r,α),D 按如下进行定义:

(1) 当 M 激起 KGE 询问时,D 从 $\{0,1,\cdots,\ell_K-1\}$ 随机选取 $J=k$;随机地从 $[(N-1)/4]$ 选取 n 个元素 $\xi_i(i=1,\cdots,n)$,并用 $\boldsymbol{\xi}=(\xi_1,\xi_2,\cdots,\xi_n)$ 表示;取 $s=\ell_K\cdot n-k$ 和 $g=v^{2^s} \bmod N$;将 (g,N,r) 给 M;

(2) 当 M 用 $[n]$ 的真子集 A 发起 Challenge 询问时,D 定义每个 $a_i=(\xi_i+2^{-\ell_K}) \bmod \gamma(i=1,\cdots,n)$,其中 $\gamma=\mathrm{ord}(g)$;D 计算 $g^{\prod_{i\in A}a_i}$,并将结果给 M 作为回答;

(3) M 发起 Challenge 询问,D 将下列比特串给 M:b_0,b_1,$\cdots$,b_{k-1},α,$B_r(g^{2^{k+1}\prod_{i=1}^{n}a_i})$,$\cdots$,$B_r(g^{2^{\ell_K-1}\prod_{i=1}^{n}a_i})$;

(4) 当 M 输出一个猜测比特时,D 输出同样的比特.

我们需要证明 D 可以在关于参数 λ 的多项式时间内进行如上操作. 显然,(1)和(4)可以在多项式时间内进行. (2)和(3)可以在多项式时间内进行被下面描述和证明的声称 1 和声称 2、3 所隐含. 为此,我们先给出一些事实.

事实 1. 由如上定义的 D 选择的 g 是 QR_N 上一致分布的平方剩余,其阶 γ 为奇数.

事实 1 的证明. 由于 $P=Q=3 \bmod 4$,所以 $\frac{P-1}{2}$ 和 $\frac{Q-1}{2}$ 均为奇数. 而 QR_N 的阶 $|QR_N|=(P-1)(Q-1)/4$,所以 $|QR_N|$ 为奇数. 而 g 的阶 γ 整除 $|QR_N|$,所以 γ 为奇数. 由于 $(2,|QR_N|)=1$,所以 QR_N 上的模平方是置换. 由于 v^2 是 QR_N 上一致分布的平方剩余,而且一致分布元素的置换也是一致分布的,所以 $g=v^{2^s}$ 是 QR_N 上一致分布的平方剩余.

事实 2. 对于每个 $0<i<s$,$g^{2^{-i} \bmod \gamma}$ 等于 $v^{2^{s-i}} \bmod N$.

事实 2 的证明. 因为 g 的阶 γ 为奇数,所以 $2^{-1} \bmod \gamma$ 存在. 注意到 $2^{-1} \bmod \gamma$ 等于 $\frac{\gamma+1}{2}$. 而 $g=v^{2^s}$,所以 $g^{2^{-i} \bmod \gamma}$ 等于 $v^{2^{s-i}} \bmod N$.

事实 3. $u=g^{2^{-s}}$ 是唯一满足 $u^2=v^2 \bmod N$ 的平方剩余.

事实 3 的证明. 由于 $g=v^{2^s}$,所以 $u^2=(g^{2^{-s}})^2=v^{(2^s\cdot 2^{-s}\cdot 2)}=v^2 \bmod N$. 又因为 $2^{-1} \bmod \gamma$ 等于 $\frac{\gamma+1}{2}$,所以 $u=g^{2^{-s}}$ 是平方剩余. 但因为 N 是 Blum 整数,所以 $v^2 \bmod N$ 在 QR_N 上的平方剩余根是唯一的,则 $u=g^{2^{-s}}$ 是唯一满足 $u^2=v^2 \bmod N$ 的平方剩余.

声称 1. 对于任意的 $[n]$ 的真子集 A,D 可以在多项式时间内计算 $g^{\prod_{i\in A}a_i}$.

声称 1 的证明. 设 $|A|=j$,因为 A 是 $[n]$ 的真子集,所以 $j\leq n-1$. 设 $q(x)=\prod_{i\in A}(\xi_i+x)=\sum_{i=0}^{j}\delta_i x^i$. 由于 D 知道每个 ξ_i,所以他可以按整系数计算出多项式 $q(x)$,从而计算出 δ_i. 因此,

$$g^{\prod_{i\in A}a_i}=g^{\prod_{i\in A}(\xi_i+2^{-\ell_K} \bmod \gamma)}=g^{(\sum_{i=0}^{j}\delta_i 2^{-\ell_K\cdot i})}=v^{(\sum_{i=0}^{j}\delta_i 2^{(s-\ell_K\cdot i)})}=\prod_{i=0}^{j}(v^{2^{(s-\ell_K\cdot i)}})^{\delta_i}.$$

因为 $s=\ell_K\cdot n-k$,$i\leq j\leq n-1$,$k\leq\ell_K-1$,所以

$$s-\ell_K\cdot i=\ell_K(n-i)-k\geq\ell_K-k\geq 1.$$

又因为 D 知道 v^2,所以他可以计算 $v^{2^{(s-\ell_K\cdot i)}}$. 另外,由于 D 可以计算 σ_i,所以,D 可以计算 $\prod_{i=0}^{j}(v^{2^{(s-\ell_K\cdot i)}})^{\delta_i}$. 而 $g^{\prod_{i\in A}a_i}=\prod_{i=0}^{j}(v^{2^{(s-\ell_K\cdot i)}})^{\delta_i}$,因此,$D$ 可以计算 $g^{\prod_{i\in A}a_i}$.

定义 w:我们定义 $w=\prod_{i=0}^{n-1}(v^{2^{\ell_K(n-i)}})^{\beta_i}$,其中 β_i 是多项式 $P(x)=\prod_{i=1}^{n}(\xi_i+x)=x^n+\sum_{i=0}^{i=n-1}\beta_i x^i$ 在整数范围的系数.

由于 D 知道 $\boldsymbol{\xi}=(\xi_1,\xi_2,\cdots,\xi_n)$,所以他可以计算出每个 β_i. 另外,D 还被给定 v^2,所以,他可以计算如上定义的 w. 很显然,w 是平方剩余,而且 w 由 v^2 和 D 用来产生 $\boldsymbol{\xi}=(\xi_1,\xi_2,\cdots,\xi_n)$ 内部随机数决定.

声称 2. 对于如前面定义的 $(\boldsymbol{a},g,u,w)$,有 $g^{2^k\prod_{i=1}^{n}a_i}=uw$.

声称 2 的证明.

$$g^{2^k\prod_{i=1}^{n}a_i}=g^{2^k\prod_{i=1}^{n}(\xi_i+2^{-\ell_K} \bmod \gamma)}=g^{2^k\sum_{i=0}^{n}\beta_i 2^{-\ell_K\cdot i}}=g^{2^{k-\ell_K\cdot n}+\sum_{i=0}^{n-1}\beta_i 2^{-(\ell_K\cdot i-k)}}=g^{2^{-s}\sum_{i=0}^{n-1}\beta_i 2^{s-(\ell_K\cdot i-k)}}=uv^{\sum_{i=0}^{n-1}\beta_i 2^{\ell_K(n-i)}}=u\prod_{i=0}^{n-1}(v^{2^{\ell_K(n-i)}})^{\beta_i}=uw.$$

声称 3.　对于 $j=1,\cdots,\ell_K-k-1$，D 可以计算 $B_r(g^{2^{k+j}\prod_{i=1}^{n}a_i})$.

声称 3 的证明.　由声称 2 知，$g^{2^k\prod_{i=1}^{n}a_i}=uw$. 对于 $j=1,\cdots,\ell_K-k-1$，每个 $B_r(g^{2^{k+j}\prod_{i=1}^{n}a_i})$ 都等于 $B_r((uw)^{2^j})$ 由于 D 知道 v^2 和 w，从而可以计算 $(uw)^{2^j}$，进而计算 $B_r((uw)^{2^j})$.

为了分析 D 的成功概率，我们下面证明 D 模仿的 a_i 和 g 与实际定义的游戏中的 a_i 和 g 统计不可区分.

事实 4.　设 ξ_i 和 a_i' 是从 $[(N-1)/4]$ 一致随机选取，令 a_i 等于 $(\xi_i+2^{-\ell_K})\bmod\gamma$，则 a_i 与 $a_i'\bmod\gamma$ 的统计距离为 $O(2^{-m(\lambda)})$.

事实 4 的证明.　由于 γ 整除 $Q-1)(P-1)/4$，所以 a_i 在事件 $\xi_i\in[(Q-1)(P-1)/4]$ 的条件分布与 $a_i'\bmod\gamma$ 在事件 $a_i'\in[(Q-1)(P-1)/4]$ 的条件分布是相同的，二者都是 Z_γ 上的一致分布. 另外，我们有

$$\begin{aligned}&Pr[\xi_i\in(Q-1)(P-1)/4]=\\&\quad Pr[a'_i\in(Q-1)(P-1)/4]=\\&\quad(Q-1)(P-1)/4]/(N/4)=\\&\quad 1-(P+Q)/N+1/N=1-O(2^{-m(\lambda)})\end{aligned}$$

所以，a_i 与 $a_i'\bmod\gamma$ 的统计距离为 $O(2^{-m(\lambda)})$.

声称 4.　$(\boldsymbol{a}'\bmod\gamma,g,N,r)$ 与 $(\boldsymbol{a},g,N,r)$ 之间的统计距离为 $n(\lambda)O(2^{-m(\lambda)})$.

声称 4 的证明.　$\boldsymbol{a}'=(a_1',a_2',\cdots,a_n')$ 中每个元素都是从 $[(N-1)/4]$ 中一致随机选取，而 $\boldsymbol{a}$ 中的每个 a_i 都等于 $(\xi_i+2^{-\ell_K})\bmod\gamma$. 由事实 4 知，对于每个 $1\le i\le n$，a_i 与 $a_i'\bmod\gamma$ 的统计距离为 $O(2^{-m(\lambda)})$. 因此，$(\boldsymbol{a}'\bmod\gamma,g,N,r)$ 与 $(\boldsymbol{a},g,N,r)$ 之间的统计距离为 $n(\lambda)O(2^{-m(\lambda)})$.

由声称 2 我们知道，如果 $\alpha=B_r(uw)$，则 M 观察到的信息的分布与 $H^J_{g,\boldsymbol{a},N,r}$ 中一样，而 α 是一个随机比特 b 时，M 观察到的信息的分布与 $H^{J+1}_{g,\boldsymbol{a},N,r}$ 中一样.

由事实 1 和 D 的描述，我们知道 (g,N,r) 被完美模仿. 另外，由于 $\boldsymbol{a}'=(a_1',a_2',\cdots,a_{n'}')$ 中每个元素都从 $[(N-1)/4]$ 中一致随机选取，所以，我们有

$$|Pr[M(H^0_{g,\boldsymbol{a}',N,r})=1]-Pr[M(H^{\ell_K-1}_{g,\boldsymbol{a}',N,r})=1]|=\varepsilon(\lambda).$$

根据声称 4，我们有

$$\begin{aligned}&|Pr[M(H^0_{g,\boldsymbol{a},N,r})=1]-Pr[M(H^{\ell_K-1}_{g,\boldsymbol{a},N,r})=1]|\ge\\&\quad|Pr[M(H^0_{g,\boldsymbol{a}',N,r})=1]-Pr[M(H^{\ell_K-1}_{g,\boldsymbol{a}',N,r})=1]|-\\&\quad n(\lambda)O(2^{-m(\lambda)}).\end{aligned}$$

因此，D 的优势为

$$\begin{aligned}&|Pr[D(B_r(uw))=1]-Pr[D(b)=1]|=\\&\frac{1}{\ell_K}\Big|\sum_{j=0}^{\ell_K-1}\{Pr[D(B_r(uw))=1\mid J=j]-\\&\quad Pr[D(b)=1\mid J=j]\}\Big|=\\&\frac{1}{\ell_K}\Big|\sum_{j=0}^{\ell_K-1}\{Pr[M(H^j_{g,\boldsymbol{a},N,r})=1]-\\&\quad Pr[M(H^{j+1}_{g,\boldsymbol{a},N,r})=1]\}\Big|=\\&\frac{1}{\ell_K}|Pr[M(H^0_{g,\boldsymbol{a},N,r})=1]-\\&\quad Pr[M(H^{\ell_K-1}_{g,\boldsymbol{a},N,r})=1]|\ge\\&\frac{1}{\ell_K}\{|Pr[M(H^0_{g,\boldsymbol{a}',N,r})=1]-\\&\quad Pr[M(H^{\ell_K-1}_{g,\boldsymbol{a}',N,r})=1]|-n(\lambda)O(2^{-m(\lambda)})\}=\\&\frac{\varepsilon(\lambda)-n(\lambda)O(2^{-m(\lambda)})}{\ell_K}.\end{aligned}$$

证毕.

由于引理 1 中定义的 D 自己选择 $\boldsymbol{\xi}=(\xi_1,\xi_2,\cdots,\xi_n)$，而 w 依赖于 v^2 和 $\boldsymbol{\xi}$，这样，D 每次被调用时，w 的值有变化的可能. 另外，D 不是 $B_r(uw)$ 的预测器而是区分器. 因此，D 不适合直接作为 Goldreich-Levin 重构算法的预言机[6]. 为了克服第一个问题，我们将 $\boldsymbol{\xi}=(\xi_1,\xi_2,\cdots,\xi_n)$ 在调用 D 之前就固定下来. 为了克服第 2 个问题，我们将难核区分器归结为难核预测器. 具体地，根据输入 r，我们按如下定义难核预测器 $D'_{N,\boldsymbol{\xi},v^2}$：

(1) 一致随机选择比特 α 和 β；

(2) 以 $\langle v^2,N,r,\alpha\rangle$ 为输入激起 D，并将 $\boldsymbol{\xi}$ 给 D（从而 D 不再自己产生 $\boldsymbol{\xi}$）；

(3) 如果 D 输出 1 时，则 $D'_{N,\boldsymbol{\xi},v^2}$ 输出 α，如果 D 输出 0，则 $D'_{N,\boldsymbol{\xi},v^2}$ 输出 β.

这样，w 的值不会随着 $D'_{N,\boldsymbol{\xi},v^2}$ 的调用而变化，因此，可以作为 Goldreich-Levin 重构算法的预言机来恢复 uw.

引理 2.　如果存在一个多项式时间攻击者 M 在上节构造的提取器中可以获得的优势 $Adv^{IND}_{BBS,M}(\lambda)$ 为 $\varepsilon(\lambda)$，则以概率 $\varepsilon'(\lambda)/2$（概率定义在 $N,v^2,\boldsymbol{\xi}$ 的选取上），上面定义的 $D'_{N,\boldsymbol{\xi},v^2}$ 可以 $\varepsilon'(\lambda)/4$ 的优势（定义在 r 的选取上）预测 $B_r(uw)$ 的值，其中 $\varepsilon'(\lambda)$ 等于 $(\varepsilon(\lambda)-n(\lambda)O(2^{-m(\lambda)}))/\ell_K$.

证明.　根据引理 1，D 有 $\varepsilon'(\lambda)$ 的优势可以区分 $B_r(uw)$ 和随机比特 b. 因此，对于至少 $\varepsilon'(\lambda)/2$ 比例的随机选择中的 N、v^2 和 $\boldsymbol{\xi}$，D 有 $\varepsilon'(\lambda)/2$ 的优势区分 $B_r(uw)$ 和随机比特 b. 很显然，$D'_{N,\boldsymbol{\xi},v^2}$ 可以以

$\varepsilon'(\lambda)/4$的优势预测 $B_r(uw)$. 证毕.

引理 3. 如果存在一个多项式时间攻击者 M 在上节构造的提取器中可以获得的优势 $Adv^{IND}_{BBS,M}(\lambda)$ 为 $\varepsilon(\lambda)$,则存在一个多项式时间算法 A 可以以概率 $\Omega(\varepsilon'(\lambda)^2)$分解 N.

证明. 根据输入 N,A 可以按如下进行定义:

(1)从$[(N-1)/4]$一致随机选择 $\xi_i(i=1,\cdots,n)$,用向量表示为 $\boldsymbol{\xi}=(\xi_1,\cdots,\xi_n)$;从 Z_N^* 中一致随机选择 v,计算 $v^2 \bmod N$;

(2)计算 $w=v^{\sum_{i=0}^{i=n-1}\beta_i 2^{\ell_K(n-i)}} \bmod N$,其中 β_i 是多项式 $P(x)=\prod_{i=1}^{n}(\xi_i+x)=x^n+\sum_{i=0}^{i=n-1}\beta_i x^i$ 的(在整数集合 Z 的)系数;

(3)调用 Goldreich-Levin 重构算法 $R(1^\lambda)$:当要求回答 $B_{r_i}(z)$的值时,以 r_i 为输入调用 D'_{N,ξ,v^2},并以 D'_{N,ξ,v^2} 的输出作为回答;用 z 表示 R 的输出;

(4)计算 $u=zw^{-1} \bmod N$. 若 R 输出的值 z 等于 uw,则一定有 $u^2=v^2 \bmod N$,当 $u\neq\pm v \bmod N$,计算并输出 $\gcd(u-v,N)$;若 R 输出的值 z 不等于 uw,则输出"失败".

由前面引理知,以概率 $\varepsilon'(\lambda)/2$,D'_{N,ξ,v^2} 能够以优势 $\varepsilon'(\lambda)/4$ 来预测 $B_r(uw)$的值. 根据 Goldreich-Levin 定理,R 能够以概率 $\Omega(\varepsilon'(n)^2)$提取 uw 的值. 注意到 uw 和 w 均是平方剩余,所以 u 也是平方剩余. 因此,以概率 1/2,u 不等于 $\pm v$. 当 u 不等于 $\pm v$ 时,$\gcd(u-v,N)$是 N 的一个非平凡因子. 所以,以概率 $\Omega(\varepsilon'(n)^2)$,$A$ 能够分解 N. 证毕.

应用举例.

考虑一个二方密钥交换协议:甲方随机选取私钥 a_1,将 $A_1=g^{a_1}$ 发送给乙方;乙方随机地选取私钥 a_2,将 $A_2=g^{a_2}$ 发送给甲方;甲和乙的共同密钥为 $BBS_r(g^{a_1a_2})$. 根据我们的结论,即使攻击者看到了 g^{a_1},g^{a_2} 后,甲和乙的共同密钥 $BBS_r(g^{a_1a_2})$ 仍然是伪随机的. 从而这个密钥交换协议是被动攻击下不可区分意义安全的.

我们再考虑一个三方密钥交换协议:甲方随机地选取私钥 a_1,将 g^{a_1} 发送给乙方;乙方收到 g^{a_1} 后,随机地选取私钥 a_2,将$(g^{a_1},g^{a_2},g^{a_1a_2})$发送给丙方;丙方收到信息后,随机地选取私钥 a_3,将$(g^{a_3},g^{a_1a_3},g^{a_2a_3})$发送给甲方和乙方;根据各自的私钥,甲、乙、丙三方可以计算出共同密钥 $BBS_r(g^{a_1a_2a_3})$. 根据我们的结论,攻击者即使看到了$(g^{a_1},g^{a_2},g^{a_3},g^{a_1a_2},g^{a_1a_3},g^{a_2a_3})$,甲、乙、丙 3 方的共同密钥 $BBS_r(g^{a_1a_2a_3})$仍然是伪随机的,从而该密钥交换协议是被动攻击下不可区分意义安全的.

4 相关工作比较

在文献[8]中,BBS 生成器被用作在因子分解假设下具有单向安全性的 Rabin 公钥加密方案的密钥提取器,得到了具有不可区分安全性的 Blum-Goldwasser 公钥加密方案. 具体地说,他们证明了即使给定了 $u^{2^{\ell_K}}$,$BBS_r(u)$仍然是伪随机的.

Naor、Reingold 与 Rosen 基于 BBS 生成器提出了基于因子分解假设的伪随机函数[9]. 具体地说,他们提出的伪随机函数是 $BBS_r(g^{\prod_{i=1}^{n}a_{i,x_i}})$,其中$(x_1,x_2,\cdots,x_n)$是 X 的比特表示,$\boldsymbol{a}=(a_{1,0},a_{1,1},\cdots,a_{n,0},a_{n,1})$,每个 $a_{i,j}\in[(N-1)/4]$. 其安全性要求即使攻击者获得了对于任意的 $Y\neq X$ 的 $BBS_r(g^{\prod_{i=1}^{n}a_{i,y_i}})$,$BBS_r(g^{\prod_{i=1}^{n}a_{i,x_i}})$ 仍然是伪随机的.

与之不同的是,在我们的方案中,安全性要求即使攻击者看到了 $g^{\prod_{i\in A}a_i}$(而不仅仅是 $BBS_r(g^{\prod_{i\in A}a_i})$),$BBS_r(g^{\prod_{i=1}^{n}a_i})$ 仍然是伪随机的. 攻击者从 $g^{\prod_{i\in A}a_i}$ 可以计算 $BBS_r(g^{\prod_{i\in A}a_i})$,但从 $BBS_r(g^{\prod_{i\in A}a_i})$ 却未必可以计算 $g^{\prod_{i\in A}a_i}$,所以直接获得 $g^{\prod_{i\in A}a_i}$ 可能使攻击者获得更多的信息. 这个区别在公钥加密和密钥交换的应用非常重要:在公钥加密和二方密钥交换协议中,攻击者可以看到 g^{a_1} 和 g^{a_2}. 在多方密钥交换协议中,攻击者可以看到相应于$[n]$一些子集 A 的 $g^{\prod_{i\in A}a_i}$.

在证明方法上,我们借鉴了 NRR 中的证明技巧. 我们的证明与 NRR 中的证明都是分为 3 个步骤:第 1 步是将方案的安全性归结为难核区分器(hardcore distinguisher);第 2 步将难核区分器归结为难核预测器;第 3 步将难核预测器归结为因子分解算法. 在后两步的具体证明也基本相同. 不同之处在第 1 步:在我们的证明中,对于攻击者的任意询问 A,我们必须模仿 $g^{\prod_{i\in A}a_i}$(而不是 $BBS_r(g^{\prod_{i\in A}a_i})$),而在他们的证明中,对于攻击者的任意询问 Y,他们必须模仿 $BBS_r(g^{\prod_{i=1}^{n}a_{i,y_i}})$.

在 2010 年国际理论密码学年会上,Cramer、

Hofheinz 和 Kiltz 得到了一个基于 RSA 假设的选择密文安全公钥密码方案[10]. 但他们需要一个在 RSA 假设(或更弱的因子分解假设)下的迪菲赫尔曼问题的提取器. 即,他们需要一个提取器 Ext 满足:即使给定(g^x,g^y),$Ext(g^{xy})$仍然是伪随机的. 而我们的结论说明了 BBS 生成器(取 $n=2$ 时)正是满足这种要求的提取器.

参 考 文 献

[1] Biham E, Boneh D, Reingold O. Breaking generalized diffie-hellmann modulo a composite is no easier than factoring. Information Processing Letters, 1999, 70(2): 83-87

[2] McCurley K. A key distribution system equivalent to factoring. Journal of Cryptology, 1988, 1(2): 95-105

[3] Steiner M, Tsudik G, Waidner M. Diffie-hellman key distribution extended to group communication//Proceedings of the 3rd ACM Conference on Computer and Communications Security. New Delhi, 1996: 31-37

[4] ElGama T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 1985, 31(4): 469-472

[5] Hastad J, Impagliazzo R, Levin L, Luby M. Construction of a Pseudo-random generator from any one-way function. SIAM Journal on Computing, 1999, 28(4): 1364-1396

[6] Goldreich O, Levin L. A hard-core predicate for all one-way functions//Proceedings of the 21st Annual ACM Symposium on Theory of Computing. Washigton, 1989: 25-32

[7] Blum L, Blum M, Shub M. A simple unpredictable pseudo-random number generator. SIAM Journal on Computing, 1986, 15(2): 364-383

[8] Blum M, Goldwasser S. An efficient probabilistic public-key encryption scheme which hides all partial information//Proceedings of CRYPTO'84. Santa Barbara, 1985: 289-302

[9] Naor M, Reingold O, Rosen A. Pseudo-random functions and factoring. SIAM Journal on Computing, 2002, 31(5): 1383-1404

[10] Cramer R, Hofheinz D, Kiltz E. A twist on the naor-yung paradigm and its application to efficient cca-secure encryption from hard search problems//Proceedings of the 7th Theory of Cryptography Conference. Zurich, 2010: 146-164

MEI Qi-Xiang, born in 1973, post-doctor, associate professor. His research interests focus on provable secure public key cryptography.

LI Bao, born in 1962, Ph. D., professor. His research interests focus on the foundation of cryptography.

LU Xian-Hui, born in 1980, post-doctor. His research interests focus on provable secure public key cryptography.

Background

This work is supported by the National Natural Science Foundation of China (Nos. 60862001,61070171), the National Basic Research Program of China (No. 2007CB311201), and the Postdoctoral Science Foundation of China (No. 20090460565).

The Generalized Diffie-Hellman (GDH) problem over composite modulus has been proved as hard as the standard factoring assumption. The GDH has been used as the base to construct key exchange and public key encryption over composite modulus. But both the deduced encryption and key exchange schemes are only secure in the sense of one-wayness under the factoring assumption. In practice, we need to extract pseudo-random bit string from the GDH element to ensure the deduced schemes secure in the sense of indistinguishability. The known proved secure and efficient pseudorandom extractors for GDH problem have to rely on the much stronger Decisional Diffie-Hellman assumption.

We prove that Blum-Blum-Shub generator is a suitable pseudo-randomness extractor for GDH problem over the composite modulus since it is efficient and secure under factoring assumption. The result implies efficient public key encryption and key exchange schemes secure in the sense of indistinguishability under factoring assumption.