doi:10.3969/j.issn.1000-436x.2014.10.016

基于短整数解问题的伪随机函数新构造

陈和风[1]，马文平[1]，高胜[2]，张成丽[1]
(1.西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071；2.数据通信科学技术研究所，北京 100191)

摘 要：伪随机函数是构造密码原型的重要工具。基于短整数解问题，在格上设计出 2 个伪随机函数，第一个利用树状伪随机综合器的思想，达到并行化效果，第二个虽是串行构造，但降低了公钥尺寸。二者均具有小模数，而且是可证明安全的。与 A Banerjer，C Peikert 和 A Rosen 3 人提出的方案（EUROCRYPT 2012）相比，此提出的伪随机函数具有渐少的密钥量；在构造方法上，由于避免了凑整技术的使用，伪随机函数的生成效率得到了提高。

关键词：伪随机函数；格；短整数解问题；混合论证
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)10-0138-07

New pseudorandom functions based on SIS

CHEN He-feng[1], MA Wen-ping[1], GAO Sheng[2], ZHANG Cheng-li[1]
(1. State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China;
2. Data Communication Science and Technology Research Institute, Beijing 100191, China)

Abstract: Pseudorandom functions are vital tools in the construction of cryptographic primitives. Under the hard assumption of SIS (short integer solution), two lattice-based pseudorandom functions are proposed. The first one has parallel structure by the ideal of tree-like pseudorandom synthesizer, and the second one is serial structure whose public key size is reduced. Both constructions have small modulus and provable security. Compared with A Banerjer, C Peikert and A Rosen's construction (EUROCRYPT 2012), their key sizes are asymptotically smaller, and efficiency are improved by avoiding the "rounding" technology.

Key words: pseudorandom function; lattice; short integral solution problem; hybrid argument

1 引言

伪随机函数是密码学的基础，最早由 O Goldreich、S Goldwasser 和 S Micali[1]定义。通过有效地利用伪随机函数，可构造加密方案、认证方案和身份认证方案等。通俗地说，一簇确定性函数是伪随机的，指的是不存在有效的攻击者能判断出一个函数是随机地选取该簇，还是从真正随机的函数簇中选取的。3 人给出的由伪随机序列构造伪随机函数的递归树状构造方法被称为“GGM”构造，GGM 基于长度翻倍的密码强伪随机比特数（CSB）生成器构造的，当输入 x 为 k bit 时，需要连续 k 次调用 CSB 生成器，如果 CSB 生成器计算 $G(x)$的步数为 T_k，那么函数的计算需要 kT_k 步，构造效率比较低。

M Nao 和 O Reingold[2]针对判决 Diffie-Hellman 问题，RSA 和整数分解问题等一般数论问题，提出了“伪随机综合器”（pseudorandom synthesizer）分析方法。这种方法非常有效，原理上可在低复杂度电路下并行计算，但是实际上，基于数论的构造要实现低的复杂度，需要进行大量的预处理和大量

收稿日期：2014-07-01；**修回日期**：2014-08-19
基金项目：国家自然科学基金资助项目(61072140, 61373171)；高等学校创新引智计划基金资助项目(B08038)；高等学校博士学科点专项科研基金资助项目(20100203110003)；“十二五”国家蜜码发展基金资助项目(MMJJ201401003)
Foundation Items: The National Natural Science Foundation of China (61072140, 61373171); Base for Introducing Talents of Discipline to Universities (B08038); The Research Fund for the Doctoral Program of Higher Education of China (20100203110003); The National Development Foundation for Cryptological Research (MMJJ201401003)

的电路。一个伪随机综合器，指的是一个双变量函数 $S(\cdot,\cdot)$，其满足对随机独立的输入序列 $x_1,\cdots,x_m$ 和 $y_1,\cdots,y_m$（任意 $m=\text{poly}(n)$），$m\times m$ 输出矩阵 $(z_{i,j})_{1\leqslant i,j\leqslant m}=(S(x_i,y_j))_{1\leqslant i,j\leqslant m}$ 是伪随机的。M Nao 和 O Reingold 的主要思想是将输入序列均分，分别调用 2 个独立的伪随机函数 F_0 和 F_1，其输出作为伪随机综合器的 2 个输入，调用综合器得到函数最后输出。即给定一个综合器 $S(\cdot,\cdot)$ 和 2 个独立的、输入为 t bit 的伪随机示例 F_0 和 F_1，得到一个输入为 $2t$ bit 的伪随机函数 F。利用递归的树状构造，对输入为 k bit 的伪随机函数簇进行定义。

后量子时代的到来，使格密码在密码学领域占据越来越重要的地位。基于格构造的密码方案，其安全性证明大多基于最坏情况的困难问题，具有好的渐近效率和抵抗量子攻击等优点。在 Ajtai[3]提出格上困难问题具有从最坏情况到平均情况的归约这一里程牌工作后，近年来，基于格构造公钥密码、基于身份密码方案和同态密码方案取得了突破性进展[4~9]。但是，基于格构造对称密码如消息认证码和分组密码等的进展却很少。

理论上，利用单向函数可以直接构造很多对称密码方案，而格密码中很多单向函数本身直接构造方法的效率很低，基于它的密码方案的效率更低，这导致了基于单向函数直接构造的密码方案，无法应用到对效率高要求的场景。另外，很多格密码原型效率都相对比较高，而且在实际当中可有效的并行化，可在相对小的低深度电路下计算，这种优势在一般的串行环境下完全消失。

A Banerjer、C Peikert 和 A Rosen[10]于 2012 年基于格上的困难问题，利用伪随机综合器，提出了渐近高效的、可并行计算的伪随机函数构造方案。但方案具有以下缺点：方案安全性基于环上容错学习（RLWE, ring-learning with error）问题[11]及其变形环上凑整学习（RLWR, ring-learning with round）问题，要求模数 q 是安全参数的亚指数，第 1 个方案要求 $q\geqslant pBn^{\omega(1)}$，第 2 个方案要求 $q\geqslant pk\ (Cr\sqrt{n})^k n^{\omega(1)}$，而这样大的 q 影响了整个方案的性能；方案采用随机凑整函数，一次凑整运算的复杂度为 $O(\log q\log(\log q)\ \log\log(\log q))$，在一个方案中多次进行凑整运算会影响方案的效率，第 1 个方案中凑整运算的复杂度至少为 $O(kn^2\omega(1))$，第 2 个方案中凑整运算的复杂度为 $O(nm\omega(1))$，其中 $n<m$。

现有的基于数论问题的伪随机函数构造方法效率比较低，理论意义大于实际意义。另外，现有的可并行化的伪随机函数大多基于离散对数问题，无法抗击多项式时间的量子攻击。因此构造相对有效的、可并行计算的、基于格的伪随机函数具有重要的研究意义和实用价值。

本文基于短整数解问题，避开凑整技术，利用树状伪随机综合方法，构造出更高效、可并行的伪随机函数，与此同时，还构造了一个公钥尺寸相对小的伪随机函数。

2　预备知识

首先，对文中涉及的符号、参数、运算等做如下约定。

用 Z、N 分别表示整数集和自然数集。对任意 $s\in\text{N}$，记集合 $[s]=\{0,1,\cdots,s\}$。用 $x\leftarrow\mathcal{X}$ 表示按一个概率分布 $\mathcal{X}$ 选取元素 x 的运算。对集合 X 上的任意概率分布 $\mathcal{X}$ 和任意元 $x\in X$，令 $\Pr\{x\leftarrow\mathcal{X}\}$ 表示分布 $\mathcal{X}$ 下选取到 x 的概率。集合 A 上的一致分布记为 $\mathcal{U}(A)$。分布 $\mathcal{X}$ 的支集记为 $[\mathcal{X}]=\{x\in X\mid \Pr[x\leftarrow\mathcal{X}]>0\}$。一个函数簇 $(F,\mathcal{X})$ 是一个函数集合 $F=\{f_i:X\to R\}_{i\in I}$，其函数由 $i\in I$ 索引，具有公共的定义域 X 和值域 R，且输入服从概率分布 $\mathcal{X}$。群 G 的商群 $G_d=G/dG$，其中，dG 表示子群 $\{dg\mid g\in G\}$。

函数簇

$$\mathcal{K}=\mathcal{K}(G,\mathcal{X})=\{f_g:[\mathcal{X}]\to G\mid f_g(x)=gx\}$$

表示输入服从分布 $\mathcal{X}$，索引是 $g\in G^m$ 时定义为 $f_g(x)=gx$ 中函数 f_g 的集合。

其次，给出几个相关定义。

定义 1　伪随机函数(PRF, pseudorandom function)[10]。令 A 和 B 为有限集合，令 $\Gamma=\{F:A\to B\}$ 为一个函数簇，连带一个有效的抽样分布（即 Γ，A，B 由安全参数 n 进行索引）。称 Γ 是一个伪随机函数簇，若下述 2 个交互游戏是计算不可区分的。

Game 0：选取函数 $F\leftarrow\Gamma$，给予敌手对 $F(\cdot)$ 适应性的 oracle 预言访问权。

Game 1：选取一致随机函数 $U:A\to B$，给予敌手对 $U(\cdot)$ 适应性 oracle 预言访问权。

称游戏 Game 0 和 Game 1 是计算不可区分的（computationally indistinguishable），如果对任意概率多项式时间算法敌手 $\mathcal{A}$，其优势为

$\mathrm{Adv}_{\mathrm{Game0,Game1}}(\mathcal{A})$

$=|\Pr[\mathcal{A}\text{ accepts in Game 0}]-\Pr[\mathcal{A}\text{ accepts in Game 1}]|$

是可忽略的。记 Game $0\overset{c}{\approx}$Game 1 。

定义 2 伪随机综合(pseudorandom synthesizer)[10]。令函数 $S:A\to B$，其中，A 和 B 为有限域，S 由安全参数索引。令 S 的组合函数为 $C_S:A^k\times A^l\to B^k$，对 $\boldsymbol{X}=(x_1,\cdots,x_k)\in A^k$，$\boldsymbol{Y}=(y_1,\cdots,y_l)\in A^l$ 有

$$\boldsymbol{C}_S(\boldsymbol{X},\boldsymbol{Y})=\left(c_{ij}=S(x_i,y_j)\right)_{1\leqslant i\leqslant k,1\leqslant j\leqslant l}$$

称函数 $S:A\to B$ 是一个伪随机综合器，如果它是多项式时间可计算的，且对任意 $k=\mathrm{poly}(n)$，$l=\mathrm{poly}(n)$，有

$$\boldsymbol{C}_s\left(U(A^k),U(A^l)\right)\overset{c}{\approx}U(B^{k\times l})$$

即对服从一致分布的随机变量 $\boldsymbol{X}\leftarrow A^k$ 和 $\boldsymbol{Y}\leftarrow A^l$，矩阵 $\boldsymbol{C}_S(\boldsymbol{X},\boldsymbol{Y})$ 与 B 上 $k\times l$ 一致随机矩阵计算不可区分。

定义 3 凑整学习问题(LWR, learning with rounding)[10]。令整数 $n\geqslant 1$ 为安全参数，模数 $q\geqslant p\geqslant 2$。凑整函数（round function）定义为

$$[\![x]\!]_p=[\![\overline{x}\cdot p/q]\!]\bmod p\,,x\in Z$$

其中，$\overline{x}\equiv x\bmod q$，$[\![\cdot]\!]$表示就近取整函数。

对向量 $\boldsymbol{s}\in Z_q^n$，如下定义 $Z_q^n\times Z_p$ 上 2 个分布。

$\mathrm{LWR}_{n,q,p}(\boldsymbol{s})$：选取一致随机向量 $\boldsymbol{a}\leftarrow Z_q^n$，输出 $\left(\boldsymbol{a},b=[\![\langle\boldsymbol{a},\boldsymbol{s}\rangle]\!]_p\right)$。

$U_{n,q,p}$：选取一致随机向量 $\boldsymbol{a}\leftarrow Z_q^n$ 和一致随机数 $b\in Z_p$，输出 $(\boldsymbol{a},b)$。

那么，对整数 n,q,p，一个给定分布上的向量 $\boldsymbol{s}\in Z_q^n$，称 $\mathrm{LWR}_{n,q,p}$ 判定问题是困难的，如果对任意概率多项式算法 $\mathcal{D}$，2 个分布是不可区分的，即

$$|\Pr\left[(\boldsymbol{a},b)\leftarrow U_{n,q,p}:\mathcal{D}(\boldsymbol{a},b)=1\right]$$
$$-\Pr\left[\boldsymbol{s}\leftarrow Z_q^n;(\boldsymbol{a},b)\leftarrow \mathrm{LWR}_{n,q,p}(\boldsymbol{s}):\mathcal{D}(\boldsymbol{a},b)=1\right]|$$

是可忽略的。

定义 4 （$\mathrm{SIS}_{q,n,m,d}$ 判决问题）[12]给定对 $(\boldsymbol{A},\boldsymbol{t})$，判断它选自 $\mathrm{SIS}_{q,n,m,d}$ 分布还是选自 $Z_q^{n\times m}\times Z_q^n$ 上的一致分布。其中，$\mathrm{SIS}_{q,n,m,d}$ 分布指随机选取矩阵 $\boldsymbol{A}\leftarrow Z_q^{n\times m}$ 和向量 $\overline{\boldsymbol{s}}\leftarrow\{-d,\cdots,0,\cdots,d\}^m$，输出 $(\boldsymbol{A},\boldsymbol{A}\overline{\boldsymbol{s}}\bmod q)$ 的分布。

引理 1[13] 设 $\mathcal{X}$ 是 $[s]^m\subset Z^m$ 上的分布，其中 $m=\mathrm{poly}(n)$，$s=\mathrm{poly}(n)$。G 是有限可换群。若函数簇 $\mathcal{K}=\mathcal{K}(G,\mathcal{X})$ 是单向的，且对 $d<s$，$\mathcal{K}_d=\mathcal{K}(G_d,\mathcal{X})$ 是伪随机的，那么 $\mathcal{K}=\mathcal{K}(G,\mathcal{X})$ 是伪随机的。

3 BPR 方案简述

A Banerjer, C Peikert 和 A Rosen[10] 在 EUROCRYPT 2012 会议上提出了 2 个伪随机函数构造方案（简记为 BPR 方案）。第 1 个方案是在 RLWR 困难假设下，利用凑整技术构造矩阵型 LWR 伪随机综合器 $T_{n,q,p}:Z_q^{n\times n}\times Z_q^{n\times n}\to Z_p^{n\times n}$

$$T_{n,q,p}(\boldsymbol{X},\boldsymbol{Y})=[\![\boldsymbol{X}\cdot\boldsymbol{Y}]\!]_p\,,\boldsymbol{X},\boldsymbol{Y}\in Z_q^{n\times n}$$

进而按照树状结构构造伪随机函数。

函数的输入长度 k 要求为 2 的 d 次幂，即 $k=2^d$。函数的索引用 $Z_{q_d}^{n\times n}$ 上 $2k$ 个一致随机矩阵表示。所采用的树状结构中：叶子节点处，根据输入 x 每一比特值选择相应的矩阵 $\boldsymbol{S}$ 存储；树内部，从下往上，两两分组调用 LWR 伪随机综合器；综合器的每一层模数成递减关系 $q_{d-1}\geqslant\cdots\geqslant q_0\geqslant 2$；最后将根节点的值作为函数值输出。

函数索引为 $\{\boldsymbol{S}_{i,b}\}_{i\in[k],b\in\{0,1\}}$ 的伪随机函数定义为

$$F(x)=F_{\{\boldsymbol{S}_{i,b}\}}(x_1x_2\cdots x_k)=$$
$$\left[\!\!\left[\cdots\left[\!\!\left[\left[\!\!\left[\boldsymbol{S}_{1,x_1}\cdot\boldsymbol{S}_{2,x_2}\right]\!\!\right]_{q_{d-1}}\left[\!\!\left[\boldsymbol{S}_{3,x_3}\cdot\boldsymbol{S}_{4,x_4}\right]\!\!\right]_{q_{d-1}}\right]\!\!\right]_{q_{d-2}}\cdots\left[\!\!\left[\boldsymbol{S}_{k-1,x_{k-1}}\cdot\boldsymbol{S}_{k,x_k}\right]\!\!\right]_{q_{d-1}}\cdots\right]\!\!\right]_{q_0}$$

第 2 个方案中，当函数长度为 k bit 时，索引用 $Z^{n\times n}$ 上的 k 个一致随机矩阵和 $Z_p^{m\times n}$ 上一个随机矩阵表示，在 RLWR 困难假设下，利用凑整技术直接构造伪随机函数。

函数索引为 $\{\boldsymbol{A},\{\boldsymbol{S}_i\}\}_{i\in[k]}$ 的伪随机函数定义为

$$F(x)=F_{\boldsymbol{A},\{\boldsymbol{S}_i\}}(x_1x_2\cdots x_k)=\left[\!\!\left[\boldsymbol{A}^T\cdot\prod_{i=1}^{k}\boldsymbol{S}_i^{x_i}\right]\!\!\right]_p$$

4 本文工作

本文首先证明一个不可区分性定理，根据该定理，在伪随机函数的构造中，就可以避开凑整技术，在短整数解问题的困难假设下，保证函数的伪随机性。所给出的伪随机函数新构造，一个利用伪随机

综合方法构造，可并行化计算；另一个以牺牲并行化为代价，降低了公钥尺寸。与现有方案相比，由于免去了凑整技术的使用，提高了效率。

4.1　基于短整数解问题的不可区分性定理

定理 1　设 n 是安全参数，$s=\mathrm{poly}(n)$，$m=\mathrm{poly}(n)$，$k=\mathrm{poly}(n)$，$l=\mathrm{poly}(n)$，$\mathcal{X}$ 是 $[s]^m \subset Z^m$ 上的分布，G 是有限交换群。假定 $\mathrm{SIS}_{q,n,m,d}$ 判决问题在 G 的 $\mathcal{X}$ 分布上是困难的，那么，随机地选取矩阵 $\boldsymbol{A}\in G^{l\times m}$ 和矩阵 $\boldsymbol{B}\in \mathcal{X}^{m\times k}$，可知集合 $\{(\boldsymbol{A},\boldsymbol{AB}):\boldsymbol{A}\in G^{l\times m},\boldsymbol{B}\in \mathcal{X}^{m\times k}\}$ 和集合 $U(G^{l\times m}, G^{l\times k})$ 不可区分。

证明　令 $\boldsymbol{A}=(\bar{x}_1,\cdots,\bar{x}_l)^{\mathrm{T}}$ 是 G^m 上的独立一致随机序列，$\boldsymbol{B}=\left(\bar{b}_1,\cdots,\bar{b}_k\right)$ 是 $\mathcal{X}^m$ 上的独立随机序列，假定 $\mathrm{SIS}_{q,n,m,d}$ 判决问题在 G 的 $\mathcal{X}$ 分布上是困难的前提下，利用混合论证方法，可知当 $\bar{\boldsymbol{x}}_i\ (i=1,\cdots,l)$ 服从随机均匀分布时，$\left(\bar{\boldsymbol{x}}_i,\left\langle\bar{\boldsymbol{x}}_i,\bar{\boldsymbol{b}}_1\right\rangle,\cdots,\left\langle\bar{\boldsymbol{x}}_i,\bar{\boldsymbol{b}}_k\right\rangle\right)\in G^{m+k}$ 的分布与 G^{m+k} 上的一致分布不可区分。

对 $i=1,\cdots,l$，分别独立地使用一系列交互游戏证明如下。

Game 0：设敌手在 G^m 上均匀随机地选取 $\bar{\boldsymbol{x}}_i$，当他向 oracle 询问 $\bar{\boldsymbol{x}}_i$ 时，oracle 选取 $\mathcal{X}^m$ 上的独立随机序列 $\bar{b}_1,\cdots,\bar{b}_k$，返回

$$\left(\bar{x}_i,\left\langle\bar{x}_i,\bar{b}_1\right\rangle,\cdots,\left\langle\bar{x}_i,\bar{b}_k\right\rangle\right)\in G^{m+k}$$

对 $j=1,\cdots,k-1$，定义如下。

Game j：设敌手在 G^m 上随机均匀地选取 $\bar{\boldsymbol{x}}_i$，当他向 oracle 询问 $\bar{\boldsymbol{x}}_i$ 时，oracle 独立均匀地选取 G 上随机元 $y_1,\cdots,y_j$，和 $\mathcal{X}^m$ 上的独立随机序列 $\bar{b}_{j+1},\cdots,\bar{b}_k$，返回

$$\left(\bar{x}_i,y_1,\cdots,y_j,\left\langle\bar{x}_i,\bar{b}_{j+1}\right\rangle,\cdots,\left\langle\bar{x}_i,\bar{b}_k\right\rangle\right)\in G^{m+k}$$

Game k：设敌手在 G^m 上随机均匀地选取 $\bar{x}_i$，当他向 oracle 询问 $\bar{x}_i$ 时，oracle 独立均匀地选取 G 上的随机元 $y_1,\cdots,y_k$，返回

$$\left(\bar{\boldsymbol{x}}_i,y_1,\cdots,y_k\right)\in G^{m+k}$$

对 $j=1,\cdots,k$，显然对于 oracle 的回答，Game j 和 Game $(j-1)$的区别仅在于第 $m+j$ 个元，前者是 G 上的随机元 y_j，后者是通过 $\left\langle\bar{x}_i,\bar{b}_j\right\rangle$ 计算得到的。由 G 的 $\mathcal{X}$ 分布中 $\mathrm{SIS}_{q,n,m,d}$ 判决问题的困难假设，可知 Game j 和 Game $(j-1)$是不可区分的。从而 Game 0 和 Game k 是不可区分的。即随机均匀选取 $\bar{x}_i\ (i=1,\cdots,l)$ 时，$\left(\bar{x}_i,\left\langle\bar{x}_i,\bar{b}_1\right\rangle,\cdots,\left\langle\bar{x}_i,\bar{b}_k\right\rangle\right)\in G^{m+k}$ 的分布与 G^{m+k} 上的一致分布不可区分。

因此，由引理 1 得 $\left(\left(\bar{x}_i\right)_{i\in[l]},\boldsymbol{AB}\right)$ 与 $U(G^{l\times(m+k)})$ 是统计不可区分的。

4.2　伪随机函数基于短整数解问题的并行构造

该平行构造方案中，函数的伪随机性通过 $\mathrm{SIS}_{q,n,m,d}$ 判决困难假设得到保证。函数的索引用矩阵 $\left\{\boldsymbol{S}_{i,b},\boldsymbol{B}_j\right\}$ 表示，其中矩阵 $\boldsymbol{S}_{i,b}$ 从有限交换群 G 一致选取，矩阵 $\boldsymbol{B}$ 按 $\mathcal{X}$ 分布选取。树状结构的构造思想如下：叶子节点根据输入 x 每一比特值选择相应的矩阵 $\boldsymbol{S}$ 存储；每一层的伪随机综合器，选取不同的矩阵 $\boldsymbol{B}$ 作为乘法因子，以子节点存储的矩阵为输入，两矩阵联结后与矩阵 $\boldsymbol{B}$ 的乘积作为输出；树状结构的内部，从下往上，两两分组调用伪随机综合器；根节点的值作为最后输出结果。

4.2.1　构造方法

对于参数 $n\in\mathrm{N}$，$m=2n$，输入长度 $k=2^d\geqslant 1$，G 为有限交换群。如下递归地构造伪随机函数簇 $F^{(j)},0\leqslant j\leqslant d$，其函数定义域为 $\{0,1\}^{2^j}$，值域为 $G^{n\times m}$。最终定义 $\mathcal{F}=\mathcal{F}^{(d)}$。

对 $j=0$，独立地随机选取 $G^{n\times m}$ 上 2 个矩阵 $\boldsymbol{S}_0,\boldsymbol{S}_1$，函数 $F\in\mathcal{F}^{(0)}$ 定义为

$$F(x)=F_{\{\boldsymbol{S}_b\}}(x)=\boldsymbol{S}_x,x\in\{0,1\}$$

对 $j\geqslant 1$，函数 $F\in\mathcal{F}^{(j)}$ 由 $F_0,F_1\in\mathcal{F}^{(j-1)}$ 递归式地定义如下

$$F_{F_0,F_1}(x_0,x_1)=T^j\left(F_0(x_0),F_1(x_1)\right)$$

这里 $|x_0|=|x_1|=2^{j-1}$，函数 F_0,F_1 是随机选取的，矩阵 $\boldsymbol{B}_j\leftarrow\mathcal{X}^{2m\times m}$，且

$$T^j\left(F_0(x_0),F_1(x_1)\right)=\left(F_0(x_0)\|F_1(x_1)\right)\boldsymbol{B}_j$$

方案可以更明确地叙述如下。

每个元素按 $\mathcal{X}$ 分布生成 d 个 $2m\times m$ 阶矩阵 $\boldsymbol{B}_i,1\leqslant i\leqslant d$，设输入长度 $k=2^d$，矩阵 $\boldsymbol{S}_{i,b}$，其中 $i\in[k],b\in\{0,1\}$ 是 G 上的 $n\times m$ 阶矩阵，定义索引为 $\{\boldsymbol{S}_{i,b},\boldsymbol{B}_j\}_{i,j\in[k],b\in\{0,1\}}$ 的函数 $F\in\mathcal{F}$

若 $x=(x_1,\cdots,x_k)\in\{0,1\}^k$，有

$$\begin{aligned}F(x)&=F_{\{\boldsymbol{S}_{i,b},\boldsymbol{B}_j\}}(x)\\&=[\cdots\{[\boldsymbol{S}_{1,x_1}\|\boldsymbol{S}_{2,x_2}]\times\boldsymbol{B}_d\|[\boldsymbol{S}_{3,x_1}\|\boldsymbol{S}_{4,x_2}]\times\boldsymbol{B}_d\}\times\boldsymbol{B}_{d-1}\cdots]\times\boldsymbol{B}_1\end{aligned}$$

4.2.2 参数选取方法

现代密码学中，最基本的问题是单向函数是否存在，从而，伪随机序列和伪随机函数的存在问题取决于单向函数的存在性问题。根据已有结果[12]，群 G 可做如下选取。

1) 设 p 是$|G|$的最小素因子，$\mathcal{X}$ 满足$[\mathcal{X}]\subset[s]^m$，这里$s\leqslant p$，并假定$\mathcal{K}(G,\mathcal{X})$是单向的。

2) 分布 $\mathcal{X}$ 满足 $[\mathcal{X}]\subset[s]^m$，$d\,|\,k$，$d<s$，$\mathrm{Col}(X_d)=\mathrm{negl}(n)/d^k$，假定$\mathcal{K}(Z_q^k,\mathcal{X})$是单向的。

3) 若$\mathcal{K}(Z_q^k,\mathcal{X})$是单向的，$k\leqslant m-\omega(\log n)$，$\mathcal{X}$是$[s]^m\subset Z^m$上的分布，且是$Z_q^k$上一致打折分布。

4.2.3 安全性证明

为了便于叙述，取 $\boldsymbol{A}_0,\boldsymbol{A}_1$ 为 $n\times 2n$ 阶矩阵，$\boldsymbol{B}_j$ 为 $4n\times 2n$ 阶矩阵。

定理 2 假定 $T^{(j)}(\boldsymbol{A}_0,\boldsymbol{A}_1)=(\boldsymbol{A}_0\,\|\,\boldsymbol{A}_1)\boldsymbol{B}_j$ 是一个伪随机综合，这里 $j\in[d]$，则上述构造是一个伪随机函数簇。

证明 对于 $j=0,1,\cdots,d$，证明每一个 $\mathcal{F}^{(j)}$ 是伪随机函数。$j=0$ 时，$\mathcal{F}^{(0)}$ 是真正的随机函数，当然也是伪随机函数。

对 $j=1,\cdots,d$，假定 $\mathcal{F}^{(j-1)}$ 是伪随机函数，通过混合论证，证明 $\mathcal{F}^{(j)}$ 是伪随机函数如下。

Game 0: 设 $\mathcal{A}$ 是一个针对 $\mathcal{F}^{(j)}$ 的攻击者，选择 $F\leftarrow\mathcal{F}^{(j)}$,即独立地随机选取 $F_0,F_1\leftarrow\mathcal{F}^{(j-1)}$，为攻击者的 oracle 接入 $F_{F_0,F_1}(x_0,x_1)=T^j(F_0(x_0),F_1(x_1))$，其中，$|x_0|=|x_1|=2^{j-1}$。

Game 1: 用真正的随机函数替代 F_0,F_1。即随机地选取 2 个矩阵 $\boldsymbol{A}_0,\boldsymbol{A}_1\in Z_q^{n\times 2n}$，当 $\mathcal{A}$ 询问量 $x_0,x_1\in\{0,1\}^{2^j}$ 时，输出 $T^{(j)}(\boldsymbol{A}_0,\boldsymbol{A}_1)=(\boldsymbol{A}_0\,\|\,\boldsymbol{A}_1)\boldsymbol{B}_j$。

Game 2: 为攻击者 $\mathcal{A}$ 接入真正的随机函数 $U:\{0,1\}^{2^j}\to Z_q^{n\times 2n}$。

显然，由于 $T^{(j)}(\boldsymbol{A}_0,\boldsymbol{A}_1)=(\boldsymbol{A}_0\,\|\,\boldsymbol{A}_1)\boldsymbol{B}_j$ 是一个伪随机综合，Game 0 和 Game 1 计算不可区分。

假定攻击者最多作 $Q=\mathrm{poly}(n)$ 次询问，设计一个有效的模拟器 $\mathcal{S}$，给定输入 $\left(\boldsymbol{Z}_{ij}\right)_{i,j\in[Q]}\in\left(Z_q^{n\times 2n}\right)^{Q\times Q}$，这里 $\boldsymbol{Z}_{ij}=T^j(\boldsymbol{X}_i,\boldsymbol{Y}_j)$，$i,j\in[Q]$。对于一致随机选取的 $\boldsymbol{X}_i,\boldsymbol{Y}_j\in Z_q^{n\times 2n}$，$\boldsymbol{Z}_{ij}$ 是一致随机选取的。从而，模拟器 $\mathcal{S}$模拟了 Game 1 和 Game 2。模拟器 $\mathcal{S}$的输入是计算不可区分的，故 Game 1 和 Game 2 是计算不可区分的。

因此，Game 0 和 Game 2 计算不可区分。

4.3 基于短整数解问题的伪随机函数的串行构造

该串行构造中，函数的伪随机性也是通过 $\mathrm{SIS}_{q,n,m,d}$ 判决困难假设得到保证。函数的索引用矩阵 $(\boldsymbol{A},\{\boldsymbol{S}_i\})$ 表示，其中矩阵 $\boldsymbol{A}$ 为有限交换群 G 上一致选取的 $n\times m$ 矩阵，$\{\boldsymbol{S}_i\}$ 为按 $\mathcal{X}$ 分布选取的 $m\times m$ 矩阵。而函数的构造思想是：每一输入比特位 i 均对应一个服从 $\mathcal{X}$ 分布的矩阵 $\boldsymbol{S}_i$，但只选取输入比特值为 1 所对应的矩阵，与矩阵 $\boldsymbol{A}$ 按比特顺序相乘，将最后的乘积结果作为输出。

4.3.1 构造方法

设 n 是安全参数，$s=\mathrm{poly}(n)$，$m=\mathrm{poly}(n)$，输入比特长度 $k>1$。

1) 随机地选取 G 上 $n\times m$ 阶矩阵 $\boldsymbol{A}$。

2) 对于任意的 i，$1\leqslant i\leqslant k$，每个元素按分布 $\mathcal{X}$ 生成 $m\times m$ 阶矩阵 $\boldsymbol{S}_i$。

3) 定义函数

$$F(x)=F_{\boldsymbol{A},\{\boldsymbol{S}_i\}}(x_1,x_2,\cdots,x_k)=\boldsymbol{A}\prod_{i=1}^{k}\boldsymbol{S}_i^{x_i}$$

即伪随机函数簇 $\Gamma^{(k)}$ 为

$$\Gamma^{(k)}=\{F_{\boldsymbol{A},\{\boldsymbol{S}_i\}_{i=1,2,\cdots,k}}:\{0,1\}^k\to G^{n\times m}\,|\,\boldsymbol{A}\leftarrow U(G)^{n\times m},\ \boldsymbol{S}_i\leftarrow\mathcal{X}^{m\times m},i=1,\cdots,k\}$$

其中，对 $x=(x_1,x_2,\cdots,x_k)\in\{0,1\}^k$，$F(x)=F_{\boldsymbol{A},\{\boldsymbol{S}_i\}}(x_1,x_2,\cdots,x_k)=\boldsymbol{A}\prod_{i=1}^{k}\boldsymbol{S}_i^{x_i}$。

4.3.2 安全证明

定理 3 设每一个矩阵 $\boldsymbol{S}_i$ 独立地选取自分布 $\mathcal{X}^{m\times m}$，并假定判决 $\mathrm{SIS}_{n,m,\chi}$ 问题是困难的，那么，上述函数簇 $\Gamma^{(k)}$ 是伪随机的。

证明 用归纳法依次证明每一个 $\Gamma^{(j)}$ $(j=1,\cdots,k)$ 是伪随机函数。对 j=1，设 $\mathcal{A}$ 是一个针对 $\Gamma^{(1)}$ 的攻击者，如下定义游戏 Game1 和 Game2，通过二者的不可区分性可证 $\Gamma^{(1)}$ 是伪随机函数。对于 $j=1,\cdots,d$，用归纳法证明每一个 $\Gamma^{(j)}$ 是伪随机函数；对 $j=1$，通过游戏 Game 1 和 Game 2 的不可区分性可证 $\Gamma^{(1)}$ 是伪随机函数如下，设 $\mathcal{A}$ 是一个针对 $\Gamma^{(1)}$ 的攻击者。

Game 1：选取 $F\leftarrow\Gamma^{(1)}$，即独立地选取 $\boldsymbol{A}\leftarrow Z_q^{n\times m}$ 和 $\boldsymbol{S}\leftarrow\mathcal{X}^{m\times m}$，为攻击者 $\mathcal{A}$ 的 oracle 接入 $F_{\boldsymbol{A},\boldsymbol{B}}(x)=\boldsymbol{A}\boldsymbol{S}^x$，其中，$x\in\{0,1\}$。

Game2：为攻击者 $\mathcal{A}$ 接入真正的随机函数 $U:\{0,1\}\to Z_q^{n\times m}$。

设计一个有效的模拟器 $\mathcal{S}$ 模拟 Game 1 和 Game 2。模拟器 $\mathcal{S}$ 随机选取元素

$$(\boldsymbol{A},\boldsymbol{AS})\in Z_q^{n\times m}\times Z_q^{n\times m}$$

其中，$\boldsymbol{S}\leftarrow\mathcal{X}^{m\times m}$，或 $(\boldsymbol{A}',\boldsymbol{S}')\in Z_q^{n\times m}\times Z_q^{n\times m}$。

显然 $\mathcal{S}$ 模拟了 Game 1 和 Game 2，在判定 $\mathrm{SIS}_{n,m,\chi}$ 的困难假设下，上述 2 个矩阵是计算不可区分的，从而 Game 1 和 Game 2 是计算不可区分的。

方便起见，定义函数簇 $\mathcal{H}^{(i)}$，$n,m,q,\mathcal{X}$ 含义同上，对于任意的 $i\geqslant 1$，函数簇 $\mathcal{H}^{(i)}$ 是一簇 $\{0,1\}^i$ 映射到 $Z_q^{n\times m}$ 上的函数，函数 $H\in\mathcal{H}^{(i)}$ 定义为

$$H(x)=H_{\boldsymbol{A}_i,\boldsymbol{S}_i}(x',x_i)=\boldsymbol{A}_i(\boldsymbol{S}_i)^{x_i}$$

这里 $x=(x',x_i)$，$|x'|=i-1$，$\boldsymbol{A}_i\leftarrow Z_q^{n\times m}$，$\boldsymbol{S}_i\leftarrow\mathcal{X}^{m\times m}$。

对于 $j>1$，假定 $\Gamma^{(j-1)}$ 是伪随机函数，通过下面一系列挑战应答游戏的不可共分性，可证明 $\Gamma^{(j)}$ 是伪随机函数。

Game 3：设 $\mathcal{A}$ 是一个针对 $\Gamma^{(j)}$ 的攻击者，随机选取 $F\leftarrow\Gamma^{(j)}$，给定 $\mathcal{A}$ 的 oracle 接入 $F(\cdot)$。

Game 4：随机选取 $H\leftarrow\mathcal{H}^{(j)}$，给定 $\mathcal{A}$ 的 oracle 接入 $H(\cdot)$。

为证明 Game 3 和 Game 4 是计算不可区分的，如下设计一个有效的模拟器 $\mathcal{S}$ 模拟 Game3 和 Game4。

给定 $\mathcal{S}$ 接入 oracle 函数 $F:\{0,1\}^{j-1}\to Z_q^{n\times m}$，其中 F 随机地选自真正随机函数，或者随机地选自 $\Gamma^{(j-1)}$。$\mathcal{S}$ 为攻击者模拟 Game 3 和 Game 4：$\mathcal{S}$ 选取 $\boldsymbol{S}_i\leftarrow\mathcal{X}^{m\times m}$，若攻击者询问 $x=(x',x_i)$，$|x'|=i-1$，$\mathcal{S}$ 询问 oracle 函数 F 得到 $F(x')$，计算 $F(x')(\boldsymbol{S}_i)^{x_i}$ 返回给攻击者，显然模拟器 $\mathcal{S}$ 模拟了 Game 3 和 Game 4。由归纳假设，Game 3 和 Game 4 不可区分。

Game 5：为攻击者接入真正的随机函数 $U:\{0,1\}^{2^j}\to Z_q^{n\times 2n}$，给其 $U(\cdot)$。

类似于 $j=1$ 的情形，Game 4 和 Game 5 是计算不可区分的。

故 Game 5 和 Game 3 计算不可区分。

综上所述，函数簇 $\Gamma=\Gamma^{(k)}$ 是伪随机的。

5　分析比较

与 BPR 方案比较，本方案有如下特点。

1) 渐近少的密钥量。首先，BPR 方案需要 $2k$ 个 $n\times n$ 阶矩阵，本方案需要 $2k$ 个 $n\times 2n$ 阶矩阵的同时需要 $\mathrm{lb}k$ 个 $4n\times 2n$ 阶矩阵，虽然本方案需要的矩阵比较多，但最大的元素取自 Z_q，而文献[10]中的最大元素取自 Z_{q_d}。其次，BPR 方案的安全性基于 RLWE 问题，其中条件 $q_i\geqslant qBn^{\omega(1)}$ 表示 BPR 方案的密钥最多 $2kn^2(\mathrm{lb}q+\mathrm{lb}B+\omega(1)\mathrm{lb}n)$ bit，而本文方案需要 $4kn^2\mathrm{lb}\,\mathrm{poly}(n)+8\mathrm{lb}kn^2\mathrm{lb}s$ bit，考虑到 $n^{-\omega(1)}$ 是可忽略参数，所以 $\omega(1)$ 渐近很大，s 是常数，显然 BPR 方案中的密钥量渐近地大于本文方案的密钥量。

2) 更大的值域范围。本方案的值域选取满足条件的有限可换群，与格上构造的其他伪随机函数相比（比如 BPR 方案的值域为 $Z_p^{m\times n}$），更具一般性。

3) 参数优化。参数选取优于基于大整数分解和离散对数问题构造的伪随机函数。当有限可换群 $G=\mathrm{Z}_{2^{l(n)}}$ 时，一般认为 $l(n)>1.062\,9n$，$\mathcal{K}(G,\mathcal{X})$ 的单向性问题可规约到寻找格上最短向量问题。因此，可取 $\mathcal{X}$ 为 0~1 分布，$l(n)=1.063n$。实际上，当 $l(n)=n$ 时，攻击 $\mathcal{K}(G,\mathcal{X})$ 单向性的时间复杂度为 $O(2^{n/2})$，空间复杂度为 $O(2^{n/4})$，所以取 $n=256$，采用上面方法就可以构造伪随机函数。假定 $\mathcal{K}(Z_{p^e}^k,U(Z_{p^i}^m))$ 是单向函数，其中 p 是素数，$i\leqslant e$，$p^i=\mathrm{poly}(n)$，那么本方案的多项式模数明显优于 BPR 方案的亚指数模数。

4) 渐近快速。BPR 方案每次运算是在模 $q_j(0\leqslant j\leqslant\mathrm{lb}k-1)$ 的 $n\times n$ 阶矩阵运算，本方案是模 q 上的 $n\times 4n$ 阶矩阵和稀疏的 $4n\times 2n$ 阶矩阵乘积，虽然这么看，本方案矩阵比 BPR 方案的大。但矩阵元素小，可采用快速算法。关键在于模数小。要保证 BPR 方案的安全性，其模数 q_j $(0\leqslant j\leqslant\mathrm{lb}k-1)$ 要远大于本方案的模数 q，这就导致了 BPR 方案中矩阵元素很大，而本方案矩阵中元素较小，通过适当选取模数 q 可以使矩阵乘法速度加快。若在整数环中实现，利用快速傅里叶变换，速度可以更快。

6　结束语

本文第 1 个伪随机函数的构造基于格上 SIS 问题，避免了凑整技术的大量使用，提高了效率；将伪随机函数的值域从 $Z_q^{n\times m}$ 扩大到一般有限可换群；利用伪随机综合器思想，使结果达到并行化效果；在保证可证安全性的同时，把模数 q 从亚指数降低到多项式。第 2 个构造中，公钥个数为 k+1，小于

第 1 个方案的公钥个数 $2k+\log k$，降低了公钥尺寸；而与 BPR 第 2 个方案相比，其使用凑整技术，产生了 $O(nm\omega(1))$ 的计算复杂度，本方案舍弃了凑整技术，降低了计算复杂度，与此同时，在 SIS 问题假设下保证了方案的可证安全性。显然，本文的构造优于 BPR 方案，具有一定的理论意义和实际价值。

参考文献：

[1] GOLDREICH O, GOLDWASSER S, MICALI S. How to construct random functions[J]. J ACM, 1986, 33(4): 792-807.

[2] NAOR M, REINGOLD O. Synthesizers and their application to the parallel construction of pseudorandom functions[J]. Journal of Computer and System Sciences, 1999, 58: 336-375.

[3] AJTAI M. Generating hard instances of lattice problems[A]. STOC 1996[C]. Philadelphia, Pennsylvania, 1996. 99-108.

[4] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM, 2009, 56(6):1-40.

[5] PEIKERT C, WATERS B. Lossy trapdoor functions and their applications[A]. STOC 2008[C]. Victoria, British Columbia, 2008. 187-196.

[6] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[A]. STOC 2008[C]. Victoria, British Columbia, 2008.197-206.

[7] GENTRY C. Fully homomorphic encryption using ideal lattices[A]. STOC 2009[C]. Bethesda, Maryland, USA, 2009.169-178.

[8] CASH D, HOFHEINZ D, KILTZ E, *et al*. Bonsai trees, or how to delegate a lattice basis[A]. Cryptology-EUROCRYPT 2010[C]. French Riviera, 2010. 523-552.

[9] AGRAWAL S, BONEH D, BOYEN X. Efficient lattice (H)IBE in the standard model[A]. Cryptology–EUROCRYPT 2010[C]. French Riviera, 2010.553-572.

[10] BANERJER A, PEIKERT C, ROSEN A. Pseudorandom functions and lattices[A]. Cryptology – EUROCRYPT 2012[C]. Cambridge, UK, 2012.719-737.

[11] GORDON S D, KATZ J, VAIKUNTANATHAN V. A group signature scheme from lattice assumptions[A]. Cryptology- ASIACRYPT 2010[C]. Singapore, 2010. 395-412.

[12] LYUBASHEVSKY V. Lattice signatures without trapdoors[A]. Cryptology-EUROCRYPT 2012[C]. Cambridge, UK, 2012. 738-755.

[13] MICCIANCIO D, MOL P. Pseudorandom knapsacks and the sample complicity of LWE search-to-decision reductions[A]. Cryptology-CRYPTO 2011[C]. Santa Barbara, CA, USA, 2011. 465-484.

作者简介：

陈和风（1982-），女，福建厦门人，西安电子科技大学博士生，主要研究方向为格密码。

马文平（1965-），男，陕西凤翔人，博士，西安电子科技大学教授、博士生导师，主要研究方向为通信理论、纠错码和信息安全等。

高胜（1982-），男，山西朔州人，博士，数据通信科学技术研究所高级工程师，主要研究方向为信息安全。

张成丽（1985-），女，吉林长春人，西安电子科技大学博士生，主要研究方向为格密码。

（上接第 137 页）

ZHAO J, FENG D G, YANG L, *et al*. CCA-secure type-based proxy re-encryption without pairings[J]. Acta Electronica Sinica, 2011,(11): 2513-2519.

[12] 顾鑫, 徐正全, 涂洪涛等. 云环境下可信服务的时效策略[J]. 武汉大学学报(信息科学版), 2013,(5):626-630.
GU X, XU Z Q, XU H T, *et al*. Time effectiveness in trust services under cloud environment[J]. Geomatrics and Information Science of Wuhan University, 2013,(5):626-630.

作者简介：

熊礼治（1988-），男，湖北荆州人，武汉大学博士生，主要研究方向为多媒体通信、可信网络、网络安全等。

徐正全[通信作者]（1962-），男，湖北黄冈人，武汉大学教授、博士生导师，主要研究方向为多媒体通信、信息加密、网络通信安全等。E-mail:xuzq@whu.edu.cn。

顾鑫（1982-），男，河北景县人，武汉大学博士生，主要研究方向为多媒体通信、可信网络、网络安全等。

第 1 个方案的公钥个数 $2k+\log k$，降低了公钥尺寸；而与 BPR 第 2 个方案相比，其使用凑整技术，产生了 $O(nm\omega(1))$ 的计算复杂度，本方案舍弃了凑整技术，降低了计算复杂度，与此同时，在 SIS 问题假设下保证了方案的可证安全性。显然，本文的构造优于 BPR 方案，具有一定的理论意义和实际价值。

参考文献：

[1] GOLDREICH O, GOLDWASSER S, MICALI S. How to construct random functions[J]. J ACM, 1986, 33(4): 792-807.

[2] NAOR M, REINGOLD O. Synthesizers and their application to the parallel construction of pseudorandom functions[J]. Journal of Computer and System Sciences, 1999, 58: 336-375.

[3] AJTAI M. Generating hard instances of lattice problems[A]. STOC 1996[C]. Philadelphia, Pennsylvania, 1996. 99-108.

[4] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM, 2009, 56(6):1-40.

[5] PEIKERT C, WATERS B. Lossy trapdoor functions and their applications[A]. STOC 2008[C]. Victoria, British Columbia, 2008. 187-196.

[6] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[A]. STOC 2008[C]. Victoria, British Columbia, 2008.197-206.

[7] GENTRY C. Fully homomorphic encryption using ideal lattices[A]. STOC 2009[C]. Bethesda, Maryland, USA, 2009.169-178.

[8] CASH D, HOFHEINZ D, KILTZ E, *et al*. Bonsai trees, or how to delegate a lattice basis[A]. Cryptology-EUROCRYPT 2010[C]. French Riviera, 2010. 523-552.

[9] AGRAWAL S, BONEH D, BOYEN X. Efficient lattice (H)IBE in the standard model[A]. Cryptology–EUROCRYPT 2010[C]. French Riviera, 2010.553-572.

[10] BANERJER A, PEIKERT C, ROSEN A. Pseudorandom functions and lattices[A]. Cryptology – EUROCRYPT 2012[C]. Cambridge, UK, 2012.719-737.

[11] GORDON S D, KATZ J, VAIKUNTANATHAN V. A group signature scheme from lattice assumptions[A]. Cryptology- ASIACRYPT 2010[C]. Singapore, 2010. 395-412.

[12] LYUBASHEVSKY V. Lattice signatures without trapdoors[A]. Cryptology-EUROCRYPT 2012[C]. Cambridge, UK, 2012. 738-755.

[13] MICCIANCIO D, MOL P. Pseudorandom knapsacks and the sample complicity of LWE search-to-decision reductions[A]. Cryptology-CRYPTO 2011[C]. Santa Barbara, CA, USA, 2011. 465-484.

作者简介：

陈和风（1982-），女，福建厦门人，西安电子科技大学博士生，主要研究方向为格密码。

马文平（1965-），男，陕西凤翔人，博士，西安电子科技大学教授、博士生导师，主要研究方向为通信理论、纠错码和信息安全等。

高胜（1982-），男，山西朔州人，博士，数据通信科学技术研究所高级工程师，主要研究方向为信息安全。

张成丽（1985-），女，吉林长春人，西安电子科技大学博士生，主要研究方向为格密码。

（上接第 137 页）

ZHAO J, FENG D G, YANG L, *et al*. CCA-secure type-based proxy re-encryption without pairings[J]. Acta Electronica Sinica, 2011,(11): 2513-2519.

[12] 顾鑫, 徐正全, 涂洪涛等. 云环境下可信服务的时效策略[J]. 武汉大学学报(信息科学版), 2013,(5):626-630.
GU X, XU Z Q, XU H T, *et al*. Time effectiveness in trust services under cloud environment[J]. Geomatrics and Information Science of Wuhan University, 2013,(5):626-630.

作者简介：

熊礼治（1988-），男，湖北荆州人，武汉大学博士生，主要研究方向为多媒体通信、可信网络、网络安全等。

徐正全[通信作者]（1962-），男，湖北黄冈人，武汉大学教授、博士生导师，主要研究方向为多媒体通信、信息加密、网络通信安全等。E-mail:xuzq@whu.edu.cn。

顾鑫（1982-），男，河北景县人，武汉大学博士生，主要研究方向为多媒体通信、可信网络、网络安全等。