文章编号:1007-5321(2020)04-0083-05 **DOI**:10.13190/j.jbupt.2019-239

一种基于对偶 Regev 加密的门限公钥加密方案

李增鹏[1], 王九如[2], 张问银[2], 马春光[3]
(1. 青岛大学 计算机科学与技术学院, 青岛 266071; 2. 临沂大学 信息科学与工程学院, 临沂 276000;
3. 山东科技大学 计算机科学与工程学院, 济南 266071)

摘要: 针对 Regev 方案不能有效地抵抗密钥恢复攻击的问题,提出一种基于 Gentry-Peikert-Vaikuntanathan (GPV)方案的门限公钥加密方案. 方案主要由分布式密钥生成协议和有效非交互的解密协议构成,融合了 Shamir 秘密共享算法和拉格朗日算法,使之能够抵抗静态和被动敌手收买的攻击. 通过理论分析证明了所提方案的正确性. 在通用可组合的框架下,验证了所提方案的安全性.

关 键 词: 格基密码学; 门限密码; 容错学习; 安全协议
中图分类号: TP309 **文献标志码**: A

A Threshold Public Key Encryption via Dual Regev Scheme

LI Zeng-peng[1], WANG Jiu-ru[2], ZHANG Wen-yin[2], MA Chun-guang[3]
(1. College of Computer Science and Technology, Qingdao University, Qingdao 266071, China;
(2. School of Information Science and Engineering, Linyi University, Linyi 276000, China;
(3. School of Computer Science and Engineering, Shandong University of Science and Technology, Jinan 266071, China)

Abstract: Aiming at the problem that Regev scheme cannot effectively resist key recovery attack, a threshold public key encryption scheme is proposed based on Gentry-Peikert-Vaikuntanathan (GPV) scheme. The scheme is mainly composed of a distributed key generation protocol and an effective non-interactive decryption protocol. It combines Shamir's secret sharing algorithm and Lagrangian algorithm, which make it resistant to static and passive adversary buying attacks. The correctness of the proposed scheme is proved through theoretical analysis. Moreover, under the universal composable framework, the security is verified.

Key words: lattice-based cryptography; threshold cryptosystem; learning with errors; security protocol

门限密码学是密码学的一个重要分支,是门限方案与密码方案(如加密和签名)的有机集成. 秘密共享和门限密码的主要思想是将一个密钥分割成若干份额(share)分散存储于多个服务器成员,当需要重构密钥或使用它进行某种密码运算时,必须多于特定数量的成员联合才能共同完成,少于特定数量的任何成员组都不能计算得到此密钥. 也就是说,少数成员的秘密份额泄露不会影响整个系统密钥的安全. 这种方法直接降低了密钥泄露的可能性. 例如,(k,u)门限公钥加密需要一个私钥被 u 个解密

收稿日期: 2019-11-09
基金项目: 国家自然科学基金项目(61802214, 61932005); 山东省自然科学基金项目(ZR2019BF009, ZR2018LF007); 山东重点研发计划项目(2019GNC106027, 2019JZZY010134); 青岛市应用基础研究计划项目(19-6-2-6-cg); 贵州省公共大数据重点实验室(贵州大学)开放课题项目(2019BDKFJJ007)
作者简介: 李增鹏(1989—), 男, 助理教授.
通信作者: 王九如(1983—), 男, 副教授, E-mail: wangjiuru@lyu.edu.cn.

服务器共享,且至少有 k 个解密服务器被要求解密密文. 该方案可看作委托计算中委托者(dealer)希望通过解密服务器(worker)解密密文 c,委托者将密文发送给 k 个解密服务器,解密服务器拿到密文 c 的部分解密,并将其发送给委托者. 如果委托者收到至少 k 个 c 的解密共享,即可恢复出密文 c 的解密.

2010 年,Bendlin 等[1]给出基于 Regev 密码系统[2]的一种能够抵抗强敌手攻击的门限密码方案. 2011 年 Frederiksen[3]在文献[1]的基础上给出了一种基于 Regev 公钥加密方案的门限多比特公钥加密方案,但方案本身并不完善. Li 和 Brakerski 等[4-6]则分别指出基于 Regev 构造门限密码系统存在泄露私钥的风险. 近年来,Boneh 等[7-8]利用全同态加密技术,给出了基于格的秘密共享系统. 但是,这些方案都是基于 Regev 加密方案的.

基于此,提出一种基于 Gentry-Peikert-Vaikuntanathan (GPV)[9]的非交换门限公钥加密方案(TGPV, threshold-based GPV). TGPV 方案具有一个分布式密钥生成协议和一个有效非交互的解密协议,使其能够抵抗静态且被动敌手的收买. 最后,在通用可组合(UC, universal composability)框架下对方案的密钥生成协议及分布式解密协议进行安全性证明.

1 GPV 公钥加密方案

Regev 在 2005 年首次给出基于容错学习(LWE, learning with errors)假设的格公钥加密算法[2]. 随后,Gentry 等[9]在 2008 年提出一种对偶格(Dual Regev)的加密算法,即 GPV 公钥加密方案. 其区别在于,GPV 公钥加密方案将 Regev 方案私钥的随机数充当加密的随机数;在 LWE 假设中,Regev 方案的密文尺寸依赖于参数 $m \geqslant n\lceil \log q \rceil + 2\lambda$,为 $O(n\log^2 q)$,而 GPV 方案的密文尺寸则为 $O(m\log^2 q)$.

GPV 方案的构造、安全性、正确性证明可参考文献[9],此处不再赘述.

2 基于门限的 GPV 公钥加密方案

下面将分别介绍基于 GPV 方案的门限加密 TGPV 方案初始化、密钥生成、加密和解密算法设计思路.

2.1 初始化算法

$$\text{params} \leftarrow \text{TGPV. Setup}(1^\lambda, n, m, q, u, k) \quad (1)$$

算法输入安全参数 1^λ,输出参数 params. 参数 m、n、u 和 k,分别表示游戏参与者的总数以及解密时所需参与者的个数.

2.2 密钥生产算法

$$(\text{pk}, \text{sk}) \leftarrow \text{TGPV. KeyGen}(\text{params}) \quad (2)$$

假设每个参与者参与游戏的序号是唯一且在范围[1,u]内,其主要功能是能够诚实且无偏向地生成、分发密钥和密钥份额(key-shares)给参与者.

1) sk←TGPV. SecretKeyGen(params)

① 参与者允许以与 GPV 密码系统相同的方式来选取私钥共享.

② 调用 Shamir 秘密共享算法[10],以给定参与者的数量来确定拉格朗日多项式次数,同时共享参与方的私钥,对应的秘密共享作为输出向量,实际上,秘密共享输出向量由 $k-1$ 个从被收买的参与者中得到的 $(p, e_i)_{i=1}^n$ 值和实际计算得到的 1 个 $(0, e_i)_{i=1}^n$ 值组成,其中,$\boldsymbol{e} = (e_1, e_2, \cdots, e_n)$,秘密 $e_i \in Z_q$,$i \in [n]$. 因此,有 n 对候选者中的 k 对,所以通过拉格朗日插值可以得到次数至多为 $k-1$ 的 n 元多项式,记这些多项式为 $q_i(x)_{i=1}^n$.

③ 使用多项式 $q_i(x)_{i=1}^n$ 为其他诚实的参与者生成私钥共享,编号为 x 的参与者,将会从多项式 $q_i(x)_{i=1}^n$ 中得到第 y 个向量.

④ 对于大小为 k 的 $\binom{\eta}{k}$ 群组,可以选出 η 个参与者,并选取一个随机整数模 q,记为 K_A,其中,$A \in \left[1, \binom{\eta}{k}\right]$ 为群组编号. 若每个参与者不在给定的组 A 内接收这个组的 K_A 值,这就意味着指定的参与者将会接收到 $\binom{\eta}{k}(\eta - k)/\eta$ 值. 这里参数 η 是为刻画秘密恢复阶段(即 TGPV. Dec)被收买的参与者的数目.

2) pk←TGPV. PublicKeyGen(sk,params)

① 选取随机矩阵 $\boldsymbol{A} \in Z_q^{n \times m}$ 公共参数,随机选取向量 $\boldsymbol{e} \in Z_q^m$ 为私钥.

② 计算 $\boldsymbol{u} = f_A(\boldsymbol{e}) = \boldsymbol{A}\boldsymbol{e} (\bmod q) \in Z_q^n$.

③ 输出 $\text{pk} = [\boldsymbol{A} \mid \boldsymbol{u}] \in Z^{n \times m} \times Z^n$,并发送给所有的参与者.

2.3 加密算法

$$\boldsymbol{c} \leftarrow \text{TGPV. Enc}(\text{pk}, m) \quad (3)$$

与 GPV. Enc(·)相同,故此处省略.

2.4 解密算法

$$\mu \leftarrow \text{TGPV. Dec}(\text{sk}, c) \tag{4}$$

解密协议执行步骤如下:

1) 所有参与者均计算 $\boldsymbol{c}_1 - \boldsymbol{e}^{\mathrm{T}}\boldsymbol{c}_0 = \boldsymbol{e}'$,用于解密计算. 其中,$\boldsymbol{e}$ 是给所有参与者的私钥共享,$\boldsymbol{c} = (\boldsymbol{c}_0, \boldsymbol{c}_1)$为密文.

2) 参与者均计算一个唯一值 $x = \sum_A \phi_{K_A}(\boldsymbol{c}_0, \boldsymbol{c}_1) \in [-\sqrt{q}, \sqrt{q}]$,并返回需要解密的部分 $x + \boldsymbol{e}'$. 其中,函数 $\phi_{K_A}(\boldsymbol{c}_0, \boldsymbol{c}_1)$定义为输入 $\boldsymbol{c}_0$、$\boldsymbol{c}_1$、K_A 的伪随机函数,并返回一个数 r^{ϕ},该函数的目的是获得一个伪随机秘密共享.

3) 当解密器从参与者收到至少 k 个解密部分时,使用参与者个数作为 x 值,使用他们的 $x + \boldsymbol{e}'$值作为 y 值,执行拉格朗日算法.

4) 计算合成拉格朗日多项式的 $q(0)$值,则

$$q(0) = \begin{cases} 0, & q(0) \approx 0 \\ 1, & q(0) \approx \left\lfloor \dfrac{q}{2} \right\rfloor \end{cases}$$

3 性能分析

3.1 正确性证明

定理 1　令$\binom{u}{k} < \frac{1}{2t}\sqrt{q} - 1$,假设在分布式解密协议中,利用$\left\lfloor \frac{q}{t}\boldsymbol{u} \right\rceil + \boldsymbol{x}_2 - \boldsymbol{E}^{\mathrm{T}}\boldsymbol{x}_1 + \boldsymbol{r}^{\phi}$ 重构向量,此外,对于矩阵向量 $\boldsymbol{x}_1$ 和 $\boldsymbol{x}_2$ 中的每一个值 x,有 $\Pr[|x| \geqslant \lceil \sqrt{q} \rceil] \leqslant 2^{-O(n)}$,那么解密错误的概率是可以忽略的.

证明　对于给定结果向量,这个向量中所有的值都是以与指定加密相同的方式构造的.

1) 给定一个 $0 \in Z_t$,其加密结果是通过给定 $\boldsymbol{c}_1[i] - \boldsymbol{E}_i^{\mathrm{T}}\boldsymbol{c}_0 + r_i^{\phi} = x_{2i} - \boldsymbol{E}_i^{\mathrm{T}}x_{1i} + \left\lfloor \frac{q}{t} \cdot 0 \right\rceil + r_i^{\phi}$,其中,向量 $\boldsymbol{S}_i^{\mathrm{T}}$ 为 $\boldsymbol{S}$ 的第 i 行.

2) 由假设$\binom{u}{k} < \frac{1}{2t}\sqrt{q} - 1$ 可知$|r_i^{\phi}| < \frac{q}{2t} - \sqrt{q}$,又因为对于每个 $\phi_{K_A}(\boldsymbol{c}_0, \boldsymbol{c}_1) \in [-\sqrt{q}, \sqrt{q}]$,将这些$\binom{u}{k}$相加. 现在结合对 $|x|$ 的假设可以得到$|x_i + r_i^{\phi}| < \frac{q}{2t}$的概率至少为 $1 - 2^{-O(n)}$. 在这种情形下,相比$\frac{q}{t}$的任意倍小于 q,结果更接近于 0,所以解密是正确的.

此外,若解密值在[1,t]也可进行类似证明. x 的分布由分布 $\chi^{*\Sigma r_i}$给出,密钥生成器 KeyGen 用于生成密钥. 因此,由文献[1]中定理 1 可得,假设噪声的绝对值$|x|$具有至少 $1 - 2^{-O(n)}$ 的概率小于$\sqrt[3]{q}$,那么同样可以假设,在解密向量中对于每个 i 值至少有 $1 - 2^{-O(n)}$的概率使得$|x_i| < \lfloor \sqrt[3]{q} \rfloor$. 因此,对于 l 个错误,若合理选择参数 l 和 n,对于整个消息最终解密错误的概率为一个可忽略概率$(1 - 2^{-O(n)})^l$.

3.2 安全性分析

采用 Canetti[7] 于 2001 年提出的建立在计算复杂性理论基础上的 UC 框架来证明.

定义 1　真实协议 π UC-仿真一个理想协议 ξ. 如果对于任意的函数 F,存在一个仿真器函数 S,使得对于任意的环境机 M 及其任意的输入,环境机 M 分别与执行真实协议的函数 F 和执行理想协议的仿真器函数 S 相互作用后输出的不同结果的概率是可忽略的.

为简单起见,引入一个虚拟的实体 client,仅是希望帮助参与者解密密文的实体,因此,在真实环境中 client 可能也是参与者.

对于理想函数 $F_{\text{Gen-Dec}}$,有如下特性:

1) 所有诚实参与者准备好选取的私钥和构建的公钥之后,将公钥发送给所有的参与者(包括 client和敌手);

2) 当 client 请求解密密文$(\boldsymbol{c}_0, \boldsymbol{c}_1)$时,密文被发送给所有的参与者及敌手;

3) 在解密过程中,明文被重构并发送给 client 和敌手.

所以函数 $F_{\text{Gen-Dec}}$可以被看作一个执行密钥生成和解密的黑盒,而不需要知道私钥或者诚实参与者看到私钥.

定理 2　给定密钥生成器 KeyGen,并假设伪随机函数 ϕ,那么可以使用函数 $F_{\text{Gen-Dec}}$ 安全地解密. 假设敌手是静态且被动的,在协议开始时就选取要收买的参与者,且被收买参与者的数目少于 k 个.

为证明(协议)安全性,需要构建一个工作在理想函数 $F_{\text{Gen-Dec}}$之上的仿真器 S,以至于敌手(将敌手定义为 A)使用密钥生成器 KeyGen 无法区分出是处在具有理想函数的仿真器中还是处在真实环境的协议里.

这里需说明,仅通过使用理想函数 $F_{\text{Gen-Dec}}$ 就可以仿真在真实协议中的一切,通过这种方式使敌手以可忽略的概率区分其不同.

另外可以知道,被动攻击者只是窃听参与者的输入输出,但是参与者还是按照协议规定的程序执行规定的程序;如果攻击者在协议一开始就确定买通任意的一组参与者(数量有一定限制)作为恶意被收买参与者,在协议执行以后就不再改变,则称这种攻击者是静态攻击者. 定义的攻击者是静态被动攻击者.

1) 仿真密钥生成协议

定义集合 $B=\{$被 A 收买的参与者$\}$.

① 在真实协议中,敌手 A 将被收买的参与者选取的私钥发送给密钥生成器 KeyGen.

② 当所有的参与者准备好时,诚实参与者的密钥生成器 KeyGen 使用拉格朗日插值(对从敌手 A 获得的共享份额和密钥生成器 KeyGen 随机选取的私钥)来计算秘密共享. 密钥生成器 KeyGen 同样也计算公钥和需要的 K_A 值.

③ 密钥生成器 KeyGen 首先将公钥发送给所有的参与者、client 及敌手 A,然后发送给正确的参与者私钥共享和 K_A 值.

现在假设使用仿真器 S 替代敌手 A 与理想协议通信.

① 敌手 A 将从被收买参与者中选取的私钥发送给仿真器 S,仿真器 S 继而将这个共享传递给理想函数 $F_{\text{Gen-Dec}}$,而理想函数 $F_{\text{Gen-Dec}}$ 充当密钥生成器 KeyGen 功能,并选取私钥进而计算公钥.

② 理想函数 $F_{\text{Gen-Dec}}$ 发送公钥给 client、所有的参与者,也包括仿真器 S 和敌手 A. 这里,仿真器 S 去仿真诚实参与者被认为具有的秘密共享,只需在 $Z_q^{n\times l}$ 中选取全0矩阵. 仿真器 S 同样随机选取被收买的参与者,希望取回 K_A 值.

③ 仿真器 S 发送给被收买的参与者和敌手恰当的 K_A 值以及起初被收买的参与者发送给仿真器 S 的相同私钥共享.

2) 仿真解密协议

当 client 想要在真实协议下解密时,它将密文 $(\boldsymbol{c}_0,\boldsymbol{c}_1)$ 发送给所有的参与者,在收到参与者的解密共享后,对其执行拉格朗日插值并获得明文 $\boldsymbol{u}'$ 进而获得明文 $\boldsymbol{u}$.

① 在理想环境下,client 发送密文给理想函数 $F_{\text{Gen-Dec}}$,之后发送密文给所有的参与者及敌手 A 和仿真器 S.

② 理想函数 $F_{\text{Gen-Dec}}$ 发送明文 $\boldsymbol{u}$. 然而,由 UC-仿真定义可以看出,敌手 A 是该环境的一部分,所以需要假设敌手能够看到 client 和诚实参与者之间的通信,因此,为证明安全性,需仿真该通信. 故仿真器 S 的工作是仿真诚实参与者发送的解密共享,即给定一个解密共享 $\boldsymbol{r}^{\phi}+\boldsymbol{e}'=(r_i^{\phi}+e_i')_{i=1}^{l}$,其中,$i\in[0,1]$,故 $e_{i'}=\left\lfloor\frac{q}{t}\mu_i\right\rfloor+x_2-\boldsymbol{E}_i^{\mathrm{T}}x_1$ 的共享.

③ 对于 r_i^{ϕ},仿真器 S 形成 y_i 值作为 $\phi_{K_A}(\boldsymbol{c}_0,\boldsymbol{c}_1[i])$ 的和,敌手 A 知道在 $[-\sqrt{q},\sqrt{q}]$ 间的一个均匀随机值,但不知道每一个 K_A 值. 对于所有参与恢复秘密份额的参与者,即可以得到向量 $\boldsymbol{y}$. 使用 $\boldsymbol{y}+\boldsymbol{u}'=\left(y_i+\left\lfloor\frac{q}{t}\mu_i\right\rfloor\right)_{i=1}^{l}$ 替换会在真实协议中被泄露的向量

$$\boldsymbol{r}^{\phi}+\boldsymbol{e}'=\boldsymbol{r}^{\phi}+\underbrace{(\boldsymbol{x}_2-\boldsymbol{E}^{\mathrm{T}}\boldsymbol{x}_1)+\boldsymbol{u}'}_{\boldsymbol{e}'}=\left(r_i^{\phi}+x_{2i}-\boldsymbol{E}_i^{\mathrm{T}}x_{1i}+\left\lfloor\frac{q}{t}v_i\right\rfloor\right)_{i=1}^{l}$$

即在使用 $f^{-1}(\cdot)$ 前可得到明文. 为简单起见,这里记 $\boldsymbol{ee}:=(\boldsymbol{x}_2-\boldsymbol{E}^{\mathrm{T}}\boldsymbol{x}_1)$.

④ 仿真器 S 计算被收买参与者发送的解密共享,使用步骤1)中的私钥共享. 仿真器 S 使用拉格朗日插值计算多项式次数至多为 k 的多项式 $q_i(x)_{i=1}^{l}$,包括 $q_i(0)_{i=1}^{l}=y_i+\left\lfloor\frac{q}{t}v_i\right\rfloor$ 和被收买参与者的解密共享. 之后仿真器 S 利用这些多项式去计算诚实参与者的仿真共享.

定理3 对于任意的敌手 A,存在一个仿真器 S,对于任意的环境机 M,不能区分真实的解密协议与仿真协议.

该定理可归结为证明能够恢复加密明文的解密协议,即真实协议与仿真解密共享分布的仿真协议是计算不可区分的.

证明 在密钥生成协议中,私钥共享在真实协议和理想协议下以相同的方式分布,显然这种情形下 K_A 值均为均匀选取.

注意到在真实协议和仿真协议中,可以确定密钥生成过程中发送的信息在解密步骤中被泄露共享,分别在理想协议向量 $\boldsymbol{y}+\boldsymbol{u}'$ 和真实协议使用的 $\boldsymbol{r}^{\phi}+(\boldsymbol{x}_2-\boldsymbol{E}^{\mathrm{T}}\boldsymbol{x}_1)+\boldsymbol{u}'$ 中,敌手 A 对这些值是计算不可区分的.

对此,注意到在真实的协议中并没有给敌手 A

所有的 K_A 值，所以通过使用伪随机函数 ϕ 和构造的向量 $\boldsymbol{y}$，在敌手 A 看来，$\boldsymbol{y}+\boldsymbol{u}'$ 与 $\boldsymbol{r}^{\phi}+(\boldsymbol{x}_2-\boldsymbol{E}^{\mathrm{T}}\boldsymbol{x}_1)+\boldsymbol{u}'$ 计算不可区分.

由于每一个 y_i 至少包含在一个均匀值和为 $2\sqrt{q}$，指数大于每一个 $ee_i(\boldsymbol{ee}:=(\boldsymbol{x}_2-\boldsymbol{E}^{\mathrm{T}}\boldsymbol{x}_1))$ 分布的区间 $[-\sqrt[3]{q},\sqrt[3]{q}]$ 中，因此可以发现 $\boldsymbol{y}+\boldsymbol{u}'$ 与 $\boldsymbol{y}+(\boldsymbol{x}_2-\boldsymbol{E}^{\mathrm{T}}\boldsymbol{x}_1)+\boldsymbol{u}'$ 是统计不可区分的.

最后，在仿真协议中，将会输出构造正确的解密向量.

4　结束语

在 Bendlin 等[1]的基础上，构造了基于 GPV 方案的门限公钥加密方案. 门限密码的实质是引入一个可信第三方来执行密钥生成分发，并给出一个分布式解密协议，使之能够抵抗相对弱的被动敌手攻击，但不能够抵抗主动攻击. 直接使用文献[1]方案的结果，可以推广得到抵抗强敌手的单比特门限加密方案. 另外，非交互性和健壮性是门限密码系统需要的，方案对比如表 1 所示.

表 1　方案的性能对比

性能	所提方案	BD10[1]	Fre11[3]
困难性假设	Dual-LWE (GPV)	LWE (Regev)	LWE (Regev)
加密消息尺寸	l	l	l
关键技术	PVW 密文打包[12]/门限	门限	门限
非交互性	√	√	√
健壮性	×	√	×
安全性	静态被动敌手	主动敌手	静态被动敌手

健壮性问题并没有解决. 在下一步工作中，将引入可验证加密机制，使委托者能够验证解密服务器发送的是有效还是无效的部分解密共享，从而健全所构造的多比特门限密码方案的健壮性. 此外，基于容错学习问题构造全同态加密方案是当前公钥密码学领域研究的另外一个热点问题，但现有的全同态加密方案多集中在方案的优化效率的提升上，构造基于门限的全同态加密方案相对较少. 提出的方案可以很容易地推广到基于门限的全同态加密方案，这也是下一步的主要工作[13].

参考文献：

[1] Bendlin R, Damgard I. Threshold decryption and zero-knowledge proofs for lattice-based cryptosystems [C]// Theory of Cryptography Conference. Heidelberg: Springer, 2010: 201-218.

[2] Regev O. On lattices, learning with errors, random linear codes, and cryptography [C]// Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing. New York: ACM, 2005: 84-93.

[3] Frederiksen T. A multi-bit threshold variant of Regev's LWE-based cryptosystem [J/OL]. Cryptology ePrint Archive, 2011: 1 [2019-11-18]. http://daimi.au.dk/~jot2re/lwe/resources/report2.pdf.

[4] Li Zengpeng, Ma Chunguang, Wang Ding. Leakage resilient leveled FHE on multiple bit message [J]. IEEE Transactions on Big Data, 2017: 7.

[5] Brakerski Z, Halevi S, Polychroniadou A. Four round secure computation without setup [J/OL]. Cryptology e Print Archive, 2017: 386 [2019-10-12]. http://eprint.iacr.org/2017/386.

[6] Brakerski Z, Gentry C, Halevi S. Packed ciphertexts in LWE-based homomorphic encryption[C]// 16th International Conference on Practice and Theory in Public-Key Cryptography. Heidelberg: Springer, 2013: 1-13.

[7] Boneh D, Gennaro R, Goldfeder S, et al. Threshold cryptosystems from threshold fully homomorphic encryption [C]// 38th Annual International Cryptology Conference. Heidelberg: Springer, 2018: 565-596.

[8] Boneh D, Gennaro R, Goldfeder S, et al. A lattice-based universal thresholdizer for cryptographic systems [J/OL]. IACR Cryptology ePrint Archive, 2017: 251 [2019-10-21]. https://eprint.iacr.org/2017/251.pdf.

[9] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions [C]// 40th Annual ACM Symposium on Theory of Computing. New York: ACM, 2008: 197-206.

[10] Shamir A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612-613.

[11] Canetti R. Universally composable security: a new paradigm for cryptographic protocols [C]// 42nd IEEE Symposium on Foundations of Computer Science. Los Alamitos: IEEE Computer Society, 2001: 136-145.

[12] Peikert C, Vaikuntanathan V, Waters B. A framework for efficient and composable oblivious transfer [C]// 28th Annual International Cryptology Conference on Cryptology: Advances in Cryptology. Heidelberg: Spinger, 2008: 554-571.

[13] Li Zengpeng, Wang Jiuru, Zhang Wenyin. Revisiting post-quantum hash proof systems over lattices for internet of thing authentications [J]. Journal of Ambient Intelligence and Humanized Computing, 2019: 10.