doi:10.3969/j.issn.1000-436x.2013.08.024

无双线性对的基于身份的在线/离线门限签名方案

杨小东，李春梅，徐婷，王彩芬
（西北师范大学 计算机科学与工程学院，甘肃 兰州 730070）

摘 要：为了减少公钥密码体制中证书管理带来的开销和提高在线/离线门限签名方案的性能，利用分布式密钥生成协议和可验证秘密共享协议，提出了一种基于身份的在线/离线门限签名方案，并在离散对数假设下证明了新方案满足顽健性和不可伪造性。分析结果表明，新方案避免了传统公钥证书的管理问题和复杂的双线性对运算，大大降低了离线门限签名算法和签名验证算法的计算复杂度，在效率上优于已有的在线/离线门限签名方案。
关键词：在线/离线门限签名；基于身份的密码体制；双线性对；可模拟性
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2013)08-0185-06

ID-based on-line/off-line threshold signature scheme without bilinear pairing

YANG Xiao-dong, LI Chun-mei, XU Ting, WANG Cai-fen
(College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China)

Abstract: Based on the distributed key generation (DKG) protocol and verifiable secret sharing (VSS) protocol, an identity-based on-line/off-line threshold signature scheme was proposed in order to eliminate the cost of the certificate management in the public key cryptosystem and improve the performance of on-line/off-line threshold signature schemes. This scheme was proven to be robust and unforgeable under the discrete logarithm assumption. Analysis results show that the proposed scheme eliminates the problem of certificate management and pairing operation, and it greatly reduces computation cost of off-line threshold signature generation algorithm and signature verification algorithm. The new scheme is more efficient than the available on-line/off-line threshold signature schemes.
Key words: on-line/off-line threshold signature; identity-based cryptography; bilinear pairing; simulability

1 引言

门限签名能有效解决单个成员权力过于集中的问题，在分布式数据存储系统、分布式证书授权系统等领域已得到了广泛的应用[1]。为了改善门限签名方案的性能，Crutchfield 等[2]提出了在线/离线门限签名的思想。在一个在线/离线门限签名方案中，门限签名算法分成离线和在线 2 个阶段，离线阶段在给定消息之前进行门限签名操作所需要的绝大部分计算；在线阶段利用离线阶段存储的预计算结果，进行一些轻量级的计算（如模乘法或模加法等）便可生成给定消息的签名。由于在线阶段能在很短的时间内产生消息的签名，所以在线/离线门限签名大大改进了门限签名方案的签名速度和实时性。

Crutchfield 等[2]利用 hash-sign-switch 模式[3]提出了一个在线/离线门限签名方案，该方案的安全性基于 one-more discrete-log 假设，但该假设的安全性强于传统的离散对数假设。Bresson 等[4]利用双门限变色龙散列函数[5,6]提出了一个改进的在线/离线门限签名方案，其安全性基于离散对数假设，但离线签名算法具有较高的计算复杂度。为了降低 Crutchfield

收稿日期：2012-09-29；**修回日期**：2012-12-20
基金项目：国家自然科学基金资助项目（61262057, 61163038, 61063041, 61163036）；西北师范大学青年教师科研提升计划基金资助项目（NWNU-LKQN-10-22, NWNU-LKQN-11-24）
Foundation Items: The National Natural Science Foundation of China (61262057, 61163038, 61063041, 61163036); The Foundation for Excellent Young Teachers by Northwest Normal University (NWNU-LKQN-10-22, NWNU-LKQN-11-24)

方案的计算复杂度，LIANG 等[7]提出一个在线/离线门限签名方案，但需要零知识证明验证部分签名的正确性，因此该方案的签名效率并不高。CHEN 等[8]提出了一个无可信中心的在线/离线门限签名方案，但该方案是基于公钥证书的。TANG 等[9]提出了一个在自适应安全的在线/离线门限签名方案，但该方案基于 hash-sign-switch 模式，具有较高的计算复杂度。GAO 等[10]提出了一个可分离的在线/离线签名方案，然后基于该方案利用可模拟性的安全性证明方法构造了一个在线/离线门限签名方案，使在线/离线门限签名方案的安全性归约到在线/离线签名方案的安全性，但该方案的签名验证算法需要双线性对运算。然而，双线性对是已知最复杂的密码操作，运行一次双线性对所需要的时间至少是椭圆曲线上点乘运算所需时间的 20 倍以上[11]。因此，无双线性对的在线/离线门限签名方案将具有更大的效率优势。

基于身份的密码体制能有效避免基于公钥证书的密码系统的证书管理问题[12]。LIU 等[13]提出了一个适用于传感器网络的基于身份的在线/离线签名方案（下文简称 LIU 方案）。然而，基于身份的密码体制存在密钥托管问题，即需要一个可信的密钥生成中心生成每个用户的私钥，但实际中不存在绝对可信的第三方密钥生成中心。本文结合基于身份的密码系统和在线/离线门限签名的优点，基于 LIU 方案提出了一个无可信中心的基于身份的在线/离线门限签名方案。新方案利用分布式密钥生成协议，避免了密钥生成中心权力过大的问题。密钥生成只需要成员之间协商完成，因此并不需要可信的第三方密钥生成中心。利用可模拟性的安全性证明思想，给出了新方案的安全性证明。整个方案不需要双线性对运算，与现有的同类方案相比，新方案具有更低的算法复杂度。在离散对数假设下，新方案可容忍攻击者攻陷 $t<n/3$ 个成员。所有算法不需要可信中心，只需要成员交互协商完成。目前还没有关于无双线性对的基于身份的在线/离线门限签名研究的公开文献。

2 预备知识

2.1 离散对数假设

定义 1 离散对数问题。设 G 是一个阶为素数 p 的循环群，g 是 G 的一个生成元。已知 $(g,g^a)\in G^2$，计算 $a\in Z_p^*$。

定义 2 离散对数假设。对任意的概率多项式时间算法 A，解决离散对数问题的概率为 $Pr[A(G,p,g,g^a)=a]=\varepsilon$。若概率 ε 是可忽略的，则称离散对数问题是困难的[12]。

2.2 2 个基本协议

可验证秘密共享(VSS)协议：所有成员 $P_1,\cdots,P_n$ 联合运行 Pedersen 等提出的可验证秘密共享协议[14]，生成一个随机的秘密值 α。在协议结束后，每个成员 P_i 获得随机值 α 的秘密份额 α_i。假设协议选择 t 次多项式进行秘密信息的分发，f 个成员被攻击者攻陷，若通过 error-correcting 重构方法[15]恢复秘密 α，则要求参与成员的个数 $n\geqslant t+2f+1$。为了叙述方便，用符号 $\alpha=\text{EC-Interplate}(\alpha_1,\cdots,\alpha_n)$ 表示运行一次 error-correcting 的重构方法。

分布式密钥 (DKG)协议 [16]：在门限签名方案中，利用分布式密钥生成协议可生成一个群公钥 $h=g^a$ 和一个所有成员未知的私钥 a。协议结束后，每个成员 P_i 获得私钥 a 的秘密份额 a_i。DKG 协议在自适应性选择消息攻击下是安全的，并具有良好的密码学性质。只有攻击者攻陷了 t+1 个成员，才能恢复出私钥 a；若攻击者攻陷了 t 个成员，则存在一个模拟器 SIM_{DKG} 能模拟 DKG 协议的执行。当 SIM_{DKG} 的输入是 h 时，SIM_{DKG} 的输出也恰好是 h，同时输出已被攻陷成员所拥有的秘密份额。

3 基于身份的在线/离线门限签名的安全性定义

定义 3 设 IDOTS=(Setup, T-Extract, T-OfflineSign, T-OnlineSign, Verify)是一个基于身份的在线/离线门限签名方案，则该方案由以下 5 个算法组成。

1) Setup 是系统参数生成算法。输入一个安全参数 η，输出系统参数 cp。

2) T-Extract 是分布式密钥生成算法。输入系统参数 cp 和用户身份 ID，输出主密钥 msk 和每个成员 $P_i(1\leqslant i\leqslant n)$ 对应于用户身份 ID 的子密钥 sk_i。

3) T-OfflineSign 是离线门限签名算法。输入系统参数 cp 和每个成员 P_i 的子密钥 sk_i，输出离线签名 σ^{off} 和每个成员 P_i 的秘密状态信息 st_i。

4) T-OnlineSign 是在线门限签名算法。输入系统参数 cp，一个待签名的消息 m，每个成员 P_i 的子密钥 sk_i 和秘密状态信息 st_i，输出消息 m 的在线签名 σ^{on}。定义消息 m 的最终签名 $\sigma=(\sigma^{\text{off}},\sigma^{\text{on}})$。

5) Verify 是签名验证算法。输入用户身份 ID，一个消息 m 和一个待验证的签名 σ，如果 σ 是对应于身份 ID 的合法签名，输出 1；否则，输出 0。

一个基于身份的在线/离线门限签名方案至少应满足顽健性和不可伪造性。攻击者攻陷 t 个成员后，顽健性保证方案仍能生成正确的签名。不可伪造性保证攻击者不能生成一个新消息的合法签名。为了证明基于身份的在线/离线门限签名方案的不可伪造性，引入可模拟性的概念。

定义 4　若以下条件都成立，则称基于身份的在线/离线门限签名方案是可模拟的。

1) T-Extract 是可模拟的。已知系统参数 cp，用户身份 ID 和 t 个已被攻陷成员的子密钥，存在一个模拟器 $\mathrm{SIM}_{\mathrm{Extract}}$ 能模拟分布式密钥生成算法执行时攻击者的视图（view）。

2) T-OfflineSign 是可模拟的。已知系统参数 cp，离线签名 σ^{off}，t 个已被攻陷成员的子密钥 sk_i 和秘密状态信息 st_i，存在一个模拟器 $\mathrm{SIM}_{\mathrm{OfflinSign}}$ 能模拟离线门限签名算法执行时攻击者的视图。

3) T-OnlineSign 是可模拟的。已知系统参数 cp，一个消息 m，一个在线签名 σ^{on}，t 个已被攻陷成员的子密钥 sk_i 和秘密状态信息 st_i，存在一个模拟器 $\mathrm{SIM}_{\mathrm{OnlinSign}}$ 能模拟在线门限签名算法执行时攻击者的视图。

下面的定理阐述了可分离的基于身份的在线/离线签名方案的安全性与基于身份的在线/离线门限签名方案的安全性之间的关系。

定理 1　若一个可分离的基于身份的在线/离线签名方案 IDOS 是不可伪造的，相应的基于身份的在线/离线门限签名方案 IDOTS 是可模拟的，则门限方案 IDOTS 是不可伪造的。

证明　用 A_{IDOTS} 表示基于身份的在线/离线门限签名方案的攻击者，A_{IDOS} 表示可分离的基于身份的在线/离线签名方案的攻击者。如果基于身份的在线/离线门限签名方案 IDOTS 是可模拟的，且 A_{IDOTS} 输出一个 IDOTS 的签名伪造，那么 A_{IDOS} 利用 A_{IDOTS} 的伪造也能输出一个在线/离线签名方案 IDOS 的签名伪造。A_{IDOTS} 和 A_{IDOS} 执行如下的交互操作。

1) 将 A_{IDOTS} 的系统参数设置为 A_{IDOS} 的系统参数。

2) 当 A_{IDOTS} 发起用户身份 ID 的密钥提取询问时，以 ID 作为输入，运行模拟器 $\mathrm{SIM}_{\mathrm{Extract}}$ 模拟分布式密钥生成算法的执行，然后将模拟的结果发送给 A_{IDOTS}。

3) 当 A_{IDOTS} 发起离线签名询问时，将这个询问请求发送给 A_{IDOS} 的挑战者询问离线签名 σ^{off}，然后以 σ^{off} 作为输入，运行模拟器 $\mathrm{SIM}_{\mathrm{OfflinSign}}$ 模拟离线门限签名算法的执行，并将模拟的结果发送给 A_{IDOTS}。

4) 当 A_{IDOTS} 发起消息 m 的在线签名询问时，将消息 m 发送给 A_{IDOS} 的挑战者询问消息 m 的在线签名 σ^{on}，然后以 (m,σ^{on}) 作为输入，运行模拟器 $\mathrm{SIM}_{\mathrm{OnlinSign}}$ 模拟在线门限签名算法的执行，并将模拟的结果发送给 A_{IDOTS}。

如果攻击者 A_{IDOTS} 输出一个 IDOTS 的签名伪造 (m^*,σ^*)，那么 (m^*,σ^*) 也是 A_{IDOS} 对 IDOS 的一个签名伪造。由于 IDOTS 是可模拟的，因此从攻击者的角度看，整个模拟过程与算法的实际执行过程在计算上是不可区分的。

4　基于身份的在线/离线门限签名方案

基于 LIU 方案[7]，本节提出了一个无双线性对的基于身份的在线/离线门限签名方案。新方案由以下 5 个算法组成。

1) 系统参数生成算法(setup)

设 G 是一个阶为素数 p 的循环群，g 是 G 的一个生成元，$H:\{0,1\}^*\to Z_p^*$ 是一个安全的密码学散列函数，$\theta_i=g^{2^i}$，$i=0,\cdots,|p|-1$。n 个成员为 $(P_1,\cdots,P_n)$，公开系统参数 $cp=(G,p,g,H,\{\theta_i\}_{i=0}^{|p|-1})$。

2) 分布式密钥生成算法(T-extract)

利用分布式密钥生成协议输出公开值 (X,K) 和对应于身份 ID 的子密钥 sk_i，具体步骤如下。

① 所有成员联合运行一次 DKG 协议，生成 $X=g^x$ 和主密钥 $msk=x$。协议结束后，每个成员 $P_i(1\leqslant i\leqslant n)$ 获得主密钥 x 的秘密份额 x_i。

② 所有成员联合运行一次 DKG 协议，生成 $K=g^k$。协议结束后，每个成员 $P_i(1\leqslant i\leqslant n)$ 获得秘密值 k 的秘密份额 k_i。

③ 对于用户身份 ID，每个成员 $P_i(1\leqslant i\leqslant n)$ 计算子密钥 $sk_i=k_i+H(K,ID)\ x_i\ (\mathrm{mod}\ p)$。

每个成员 $P_i(1\leqslant i\leqslant n)$ 都知道 (X,K)，但 x，k 是每个成员未知的。

3) 离线门限签名算法(T-offlinesign)

利用可验证秘密共享协议生成离线签名和每个成员的秘密状态信息，具体步骤如下。

① 所有成员联合运行一次 VSS 协议，生成一个随机值 r。协议结束后，每个成员 $P_i(1\leqslant i\leqslant n)$ 获得秘密值 r 的秘密份额 r_i。

② 所有成员联合运行一次 VSS 协议，使得每个成员 $P_i(1\leqslant i\leqslant n)$ 获得 0 的秘密份额 ϖ_i。即 $(\varpi_1,\cdots,\varpi_n)$ 是 0 的一个(t, n)秘密共享，这里 t 是分发信息的多项式的次数。

离线签名 $\sigma^{\text{off}}=K$，每个成员 $P_i(1\leqslant i\leqslant n)$ 的秘密状态信息 $st_i=(r_i,\varpi_i)$。

4) 在线门限签名算法(T-onlinesign)

对于给定的待签名消息 m，每个成员 $P_i(1\leqslant i\leqslant n)$ 进行以下操作。

① 广播自己的秘密份额 r_i，然后计算 r =*EC-Interplate* $(r_1,\cdots,r_n)$。

② 计算 $Y=\prod_{j\in\tilde{R}}\theta_{j-1}$，这里 $\tilde{R}\subset\{1,\cdots,|p|\}$ 是 $r[j]=1$ 的索引的集合，$r[j]$ 是 r 的第 j bit 的值。

③ 广播 $z_i=r+H(Y,K,m)\cdot sk_i+\varpi_i(\text{mod}\,p)$，然后计算 z =*EC-Interplate* $(z_1,\cdots,z_n)$。

消息 m 的在线签名 $\sigma^{\text{on}}=(Y,z)$ 和最终门限签名

$$\sigma=(\sigma^{\text{off}},\sigma^{\text{on}})=(\sigma_1,\sigma_2,\sigma_3)=(K,Y,z)。$$

5) 签名验证算法(verify)

给定用户身份 ID，一个消息 m 和一个待验证的签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$，验证等式

$$g^{\sigma_3}=\sigma_2\sigma_1^{H(\sigma_2,\sigma_1,m)}X^{H(\sigma_2,\sigma_1,m)H(\sigma_1,ID)}$$

如果上述等式成立，输出 1；否则，输出 0。

5 安全性证明与性能比较

5.1 安全性分析

本文提出的新方案基于 LIU 方案[13]，而 LIU 方案允许离线签名在离线阶段发送给接受者，所以 LIU 方案是一个可分离的基于身份的在线/离线签名方案。文献[13]已在随机预言模型下证明 LIU 方案是不可伪造的，其安全性可归约到离散对数假设。因此，根据定理 1 只需证明新方案是可模拟的，也就证明了新方案具有不可伪造性。

定理 2 本文提出的基于身份的在线/离线门限签名方案是可模拟的。

证明 不失一般性，假定攻击者攻陷了 t 个成员 $P_1,\cdots,P_t$。下面根据定义 4 分别证明分布式密钥生成算法、离线门限签名算法和在线门限签名算法是可模拟的。

1) 分布式密钥生成算法是可模拟的。给定参数 $cp=(G,p,g,H,X,K,\{\theta_i\}_{i=0}^{|p|-1})$，分布式密钥生成算法的模拟器 $\text{SIM}_{\text{Extract}}$ 用 DKG 协议的模拟器 SIM_{DKG} 替代 DKG 协议。当输入 $(p,g,X=g^x)$ 和 $(p,g,K=g^k)$ 时，模拟器 SIM_{DKG} 在第 1 步的输出是 X，第 2 步的输出是 K，并且每个成员 $P_i(1\leqslant i\leqslant n)$ 获得相应的秘密份额 (x_i,k_i)。由于 $\text{SIM}_{\text{Extract}}$ 知道 t 个已被攻陷成员的秘密份额 $\{(x_i,k_i)\}_{i=1}^{t}$，于是能计算出这些成员对应于身份 ID 的子密钥 $sk_i=k_i+H(K,ID)\cdot x_i\ (\text{mod}\,p)$。$\text{SIM}_{\text{Extract}}$ 接着选择一个 t 次多项式 f_{sk}，使得 $f_{sk}(0)=k+H(K,ID)x(\text{mod}\,p)$，$f_{sk}(i)=sk_i$，然后计算未被攻陷成员 P_j 对应于身份 ID 的子密钥 $sk_j=f_{sk}(j)$，$j=t+1,\cdots,n$。由上述过程可知子密钥 sk_j 是正确的，且与分布式密钥生成算法输出的子密钥在计算上是不可区分的。因此，$\text{SIM}_{\text{Extract}}$ 能模拟分布式密钥生成算法执行时攻击者的视图。

2) 离线门限签名算法是可模拟的。给定离线签名 $\sigma^{\text{off}}=K$，离线门限签名算法的模拟器 $\text{SIM}_{\text{OfflinSign}}$ 代替未被攻陷成员执行 VSS 协议，使每个成员获得随机值 r 和 0 的秘密份额。因为 K 是模拟器 SIM_{DKG} 在分布式密钥生成算法中输出的公开值，所以 $\text{SIM}_{\text{OfflinSign}}$ 能模拟离线门限签名算法执行时攻击者的视图。

3) 在线门限签名算法是可模拟的。在线门限签名算法的模拟器 $\text{SIM}_{\text{OnlinSign}}$ 知道已被攻陷 t 个成员所拥有的秘密份额 $\{(r_i,z_i)\}_{i=1}^{t}$。给定消息 m 和对应的在线签名 $\sigma^{\text{on}}=(Y,z)$，$\text{SIM}_{\text{OnlinSign}}$ 首先选择一个 t 次多项式 f_r，使得 $f_r(0)=r$，$f_r(i)=r_i$，$i=1,\cdots,t$；然后计算未被攻陷成员 P_j 的秘密份额 $r_j=f_r(j)$，$j=t+1,\cdots,n$。显然，这些秘密份额 $\{r_i\}_{i=1}^{n}$ 能正确重构出秘密值 r。当 r 确定后，$\text{SIM}_{\text{OnlinSign}}$ 很容易计算出 $Y=\prod_{j\in\tilde{R}}\theta_{j-1}$。$\text{SIM}_{\text{OnlinSign}}$ 接着再选择一个 t 次多项式 f_z，使得 $f_z(0)=z$，$f_z(i)=z_i$，$i=1,\cdots,t$；然后计算未被攻陷成员 P_j 的秘密份额 $z_j=f_z(j)$，$j=t+1,\cdots,n$。因此，$\text{SIM}_{\text{OnlinSign}}$ 能模拟在线门限签名算法执行时攻击者的视图。

综上所述，攻击者的视图和模拟器输出的值在计算上是不可区分的，所以本文提出的新方案是可

表 1　　**在线/离线门限签名方案的性能比较**

方案	离线门限签名算法	在线门限签名算法	签名验证算法	签名长度/bit
CRUTCHFIELD 等方案[2]	3 *DKG*+*T-Sign*	6 *E*	2 *E*+*T-Ver*≥3 *E*	$\lvert\sigma\rvert+2\lvert p\rvert\geqslant 480$
BRESSON 等方案[4]	7 *VSS*+*T-Sign*	2 *EC-Interplate*	3 *E*+*T-Ver*≥4 *E*	$\lvert\sigma\rvert+3\lvert p\rvert\geqslant 640$
GAO 等方案[10]	*DKG*+4 *VSS*+*EC-Interplate*	2 *EC-Interplate*	3 *E*+1 *P*	$3\lvert p\rvert\approx 480$
本文新方案	2 *VSS*	2 *EC-Interplate*	3 *E*	$3\lvert p\rvert\approx 480$

模拟的。

定理 3　本文提出的基于身份的在线/离线门限签名方案满足顽健性。

证明　新方案中的门限密钥生成算法运行了 2 次 DKG 协议，离线门限签名算法运行了 2 次 VSS 协议。攻击者攻陷了 t 个成员，DKG 协议[16]和 VSS 协议[14]已被证明满足顽健性。因此，门限密钥生成算法和离线门限签名算法具有顽健性。在线门限签名算法运行了 2 次 error-correcting 重构方法[15]重构 r 和 z。而整个方案选择 t 次多项式进行秘密信息的分发，当攻击者攻陷了 t 个成员后，要正确恢复出 r 和 z 至少需要 $n\geqslant t+2t+1$ 个成员。所以，在 $t<n/3$ 个成员被攻击者攻陷的情况下，本文提出的新方案满足顽健性。

定理 4　在随机预言模型下，LIU 方案在适应性选择消息和身份攻击下是不可伪造的[13]。

根据定理 1、定理 2、定理 3 和定理 4，可得定理 5。

定理 5　在离散对数假设下，即使攻击者攻陷了 $t<n/3$ 个成员，本文提出的基于身份的在线/离线门限签名方案是安全的。

5.2　性能比较

下面将本文提出的新方案与已有的 3 个在线/离线门限签名方案进行计算开销和签名长度的比较。由于指数运算等价于椭圆曲线上的点乘运算，所以假定所有方案选择相同长度的素数 $|p|=160$ bit。记 P 表示双线性对运算，E 表示指数运算，*T-Sign* 表示运行一次普通门限签名方案中的门限签名算法，*T-Ver* 表示运行一次普通门限签名方案中的签名验证算法，*DKG* 表示运行一次 DKG 协议，*VSS* 表示运行一次 VSS 协议，*EC-Interplate* 表示运行一次 error-correcting 重构方法，$|\sigma|$ 表示普通数字签名的长度。相对于双线性对和指数运算而言，模乘法运算、模加法运算和普通散列函数的计算量都比较小，因此将不再对这些运算操作进行讨论。所有方案的比较结果如表 1 所示。

从表 1 可以看出，本文提出的新方案不需要执行普通门限签名方案，而运行一次普通门限签名方案中的门限签名算法或签名验证算法至少需要 1 次指数运算。新方案的所有算法不需要计算量很大的双线性对，与其他方案相比，新方案具有较高的计算效率。由于普通数字签名的长度至少是 160 bit，新方案的签名长度与 GAO 方案的相同，但比其他 2 个方案短，所以本文提出的新方案具有较高的带宽效率。

6　结束语

结合门限签名、在线/离线签名和基于身份的密码系统，提出了一个无双线性对的基于身份的在线/离线门限签名方案。新方案可容忍攻击者攻陷 $t<n/3$ 个成员，分布式密钥生成算法不需要可信中心，只需成员交互协商完成；离线门限签名算法不需要用户身份和成员的子密钥。与已有的同类方案相比，新方案避免了复杂的双线性对运算，具有较高的计算效率和带宽效率。如何设计更高效的基于身份的在线/离线门限签名方案是下一步的工作。

参考文献：

[1] ANITHA T N, JAYANTH A. Efficient threshold signature scheme[J]. International Journal of Advanced Computer Science and Applications, 2012, 3(1):112-116.

[2] CRUTCHFIELD C, MOLNAR D, TURNER D, *et al*. Generic on-line/off-line threshold signatures[A]. Proceedings of Public Key Cryptography[C]. New York, NY, USA, 2006. 58-74.

[3] SHAMIR A, TAUMAN Y. Improved online/offline signature schemes[A]. Proceedings of Advances in Cryptology[C]. Santa Barbara, CA, USA, 2001. 355-367.

[4] BRESSON E, CATALANO D, GENNARO R. Improved on-line/off-line threshold signatures[A]. Proceedings of Public Key Cryptography[C]. Beijing, China, 2007. 217-232.

[5] KRAWCZYK H, RABIN T. Chameleon signature[A]. Proceedings of NDSS'00[C]. San Diego, CA, USA, 2000. 143-154.

[6] HARN L, HSIN W J, LIN C L. Efficient on-line/off-line signature schemes based on multiple-collision trapdoor hash families[J]. The Computer Journal, 2010, 53(9):1478- 1484.

[7] LIANG B H, HUANG T H. A novel and effective on-line/off-line threshold signature project[J]. Computer Simulation, 2009, 26(9):92-95.

[8] CHEN X F, ZHANG F G, TIAN H B, *et al*. Efficient generic on-line/off-line (threshold) signatures without key exposure[J]. Information Sciences, 2008, 178(21):4192-4203.

[9] TANG C M, YAO Z G, XIE D Q. Adaptively secure on-line/off-line threshold signatures[A]. Proceedings of NSWCTC '09[C]. Guangzhou, China, 2009. 508-511.

[10] GAO C Z, WEI B D, XIE D Q, *et al*. How to construct efficient on-line/off-line threshold signature schemes through the simulation approach[J]. Concurrency and Computation: Practice and Experience, 2009, 21(10):1351-1372.

[11] WANG S, LIU W, XIE Q. Certificateless signature scheme without bilinear pairings[J]. Journal on Communications, 2012, 33(4):93-98.

[12] CHEN X F, SUSILO W, ZHANG F G, *et al*. Identity-based trapdoor mercurial commitment and applications[J]. Theoretical Computer Science, 2011, 42(39):5498-5512.

[13] JOSEPH K L, BAEK J, ZHOU J Y, *et al*. Efficient online/offline identity-based signature for wireless sensor network[J]. International Journal of Information Security, 2010, 9(4):287-296.

[14] PEDERSEN T P. Non-interactive and information-theoretic secure verifiable secret sharing[A]. Proceedings of CRYPTO[C]. Santa Barbara, California, USA, 1991. 129-140.

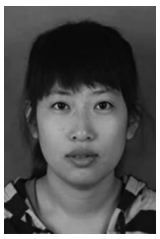
[15] MCELIECE R J, SARWATE D V. On sharing secrets and reed-solomon codes[J]. Communications of the ACM, 1981, 24(9):583-584.

[16] CANETTI R, GENNARO R, JARECKI S, *et al*. Adaptive security for threshold cryptosystems[A]. Proceedings of CRYPTO[C]. California, USA, 1999. 98-115.

作者简介：

杨小东（1981-），男，甘肃甘谷人，西北师范大学副教授、硕士生导师，主要研究方向为密码学及云计算安全。

李春梅（1987-），女，甘肃白银人，西北师范大学硕士生，主要研究方向为网络安全。



徐婷（1989-），女，甘肃兰州人，西北师范大学硕士生，主要研究方向为信息安全。

王彩芬（1963-），女，河北安国人，西北师范大学教授、博士生导师，主要研究方向为密码学、网络安全、信息安全。