计算机科学与探索
Journal of Frontiers of Computer Science and Technology
1673-9418/2024/18(12)-3348-11
doi: 10.3778/j.issn.1673-9418.2310034

基于SM9的前向安全公钥加密方案

黄文峰[1],许胜民[1],马金花[1+],宁建廷[1],伍　玮[2]
1. 福建师范大学 计算机与网络空间安全学院,福州 350117
2. 福建师范大学 数学与统计学院,福州 350117
+ 通信作者 E-mail: jinhuama55@hotmail.com

摘　要:在传统的混合密码机制中,用户的私钥一旦泄露,攻击者就可以生成该用户前期使用的会话密钥,从而解密出用该会话密钥加密的会话内容。针对这种私钥泄露带来的安全问题,使用密钥封装技术,提出了一个基于标识密码SM9的前向安全的公钥加密方案(FS-SM9),并且在标准模型下,证明了该方案在(q,n)-DBDHI困难问题假设下是IND-FS-CPA安全的。在该方案中,系统可使用总时长分为多个时间段,同时使用二叉树管理时间段,将开销降至对数级别。在加密时将时间信息嵌入到密文中,只有特定时间段的私钥才能解密该密文,而私钥在每个时间段都会通过更新算法更新一次,生成新私钥,并删除旧私钥,该更新过程是单向的,所以能实现前向安全。此外,性能分析和实验结果都表明,该方案在实现前向安全的同时引入的额外时间开销在一定条件下是可忽略的。因此,该方案具有较好的实用性,可以运行在特定的资源受限的设备上,为这些设备提供前向安全保障。

关键词:前向安全;SM9;密钥封装;选择明文安全
文献标志码:A　**中图分类号:**TP311

Forward-Secure Public-Key Encryption Scheme Based on SM9

HUANG Wenfeng[1], XU Shengmin[1], MA Jinhua[1+], NING Jianting[1], WU Wei[2]
1. College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China
2. School of Mathematics and Statistics, Fujian Normal University, Fuzhou 350117, China

Abstract: In the traditional hybrid cryptosystem, an attacker can generate the previously used session key to decrypt session contents encrypted under the session key due to the leakage of the current private key. To address this issue of leakage of the private key, this paper applies the key encapsulation mechanism and proposes a forward-secure public-key encryption scheme (FS-SM9) based on identity cryptosystem SM9. This paper also proves that the scheme is IND-FS-CPA under the hardness assumption (q, n)-DBDHI in the standard model. In the encryption scheme, the lifetime of the system is divided into multiple periods which are managed by a binary tree, which reduces the overheads of the system to a logarithmic level. The time information is embedded into the ciphertext when encrypting messages. Only the private key of the specific period can decrypt the ciphertext. Each private key is updated via an updating procedure and this updating procedure is unidirectional, during which a new private key is generated while the old one is deleted, so the forward security is preserved. Moreover, as shown by the performance analysis and experimental results, the scheme only introduces negligible overheads in achieving forward security under certain conditions.

基金项目:国家重点研发计划(2023YFB3106200);国家自然科学基金(62372108,62102090,62032005)。
This work was supported by the National Key Research and Development Program of China (2023YFB3106200), and the National Natural Science Foundation of China (62372108,62102090,62032005).
收稿日期:2023-10-11　**修回日期:**2024-01-26

Therefore, the proposed scheme is practical and can be run on specific resource-constrained devices, providing forward security for these devices.

Key words: forward security; SM9; key encapsulation; chosen-plaintext security

现有的很多密码算法都运行在安全防护不足的电子设备（如智能终端一体机，智能手机和个人电脑）上[1]，并且都未能考虑到由于用户粗心大意、设备丢失、黑客攻击等原因，而导致设备长期使用的密钥被泄露的情况。长期密钥一旦被泄露，攻击者就可以解密出与其相关的所有密文。因此，密文的机密性和设备的安全性都处于潜在风险之中。尤其是智能终端机，承担着内部服务器和外部用户通信的责任，如果该通信过程的会话密钥泄露，便会导致用户隐私泄露，甚至整个服务器的数据泄露。为了应对密钥泄露带来的威胁，常用的方法是通过秘密分享（secret sharing）技术[2-3]把密钥分为多个份额，每个份额由不同的服务器保存。根据这一思想可以使用阈值签名[4]和主动签名[5]来实现密钥份额的分配。但密钥份额分配的过程开销较大，只有企业或公司才有能力把密钥份额分配给不同的部门，而普通用户仅有一台设备，难以实现该操作。加密方案需要多个设备的参与才能避免密钥泄露带来的危害，这种加密模式不符合实际应用需求。此外，分配密钥份额并不能完全解决以上问题，如果一个公司部门的设备有漏洞，导致密钥份额泄露，攻击者可以使用该漏洞攻击公司其他部门的设备，获取到其他的密钥份额，从而恢复出密钥，最终密钥还是被攻击者获取到[6]。另一种解决方案是使用密钥协商协议，在每次会话之前，发送者和接收者协商出新密钥，并删除旧密钥，使用新密钥作为会话密钥加密消息。如果当前新密钥被泄露，由于以前的会话密文是使用旧密钥加密而来，所以即使攻击者得到新密钥，也不能解密以前的会话密文。此方案的缺点，每次会话之前都要协商出一个会话密钥，增加了通信开销，导致通信效率较低[1]。

为解决上述问题，需要前向安全的概念。前向安全性最早是从密钥协商[7]中发展而来，其含义是长期密钥的泄露不会导致短期会话密钥的泄露[6]，而公钥加密方案中的前向安全性是指当前私钥的泄露不会威胁到以前密文的机密性[8]。早在2003年，Canetti等[1]提出了前向安全的公钥加密方案（forward-secure public-key encryption，FS-PKE）。与传统公钥加密方案[9]相比，该方案有一个Update算法，该算法可以更新私钥，且私钥的更新是单向的，更新后的私钥不能解密更新前的密文。而且，在更新过程中，发送者和接收者不需要交互。

为解决以上密钥泄露问题，本文使用密钥封装技术[10-11]，提出了基于商用密码SM9的前向安全的公钥密码方案。在本方案中，系统使用总时长由 T 个时间段组成，每个时间段用 $0,1,\cdots,T-1$ 表示，每个时间段 t 都对应一个私钥 sk，发送者运行密钥生成算法生成系统的公钥 pk 和时间段0的私钥 sk_0。私钥的更新如图1所示，接收者可以更新时间段0的私钥 sk_0 得到时间段1的私钥 $sk_1=Update(sk_0)$，用前一时间段 $t-1$ 的私钥 sk_{t-1} 计算当前时间段 t 的私钥 $sk_t=Update(sk_{t-1})$。

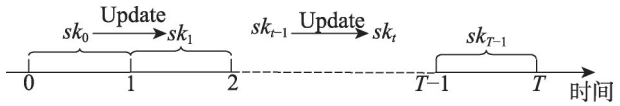

图1 前向安全密钥更新示意图

Fig.1 Key update with forward security

本文加密方案的运行流程如图2所示，其仅给出了密钥封装流程，而未给出对称加密流程。接收者A首先生成公钥 pk 和时间段0的私钥 sk_0，然后将公钥 pk 发送给公钥基础设施PKI，并秘密保存私钥 sk_0。如果发送者B想向接收者A发送明文 M，发送者B首先需要从公钥基础设施PKI获取公钥 pk，根据公钥 pk 和当前时间段 t 计算封装密钥 K 和封装密文 C。然后，发送者B用封装密钥 K 加密明文 M 计算出消息密文 C_M，把封装密文 C 和消息密文 C_M 发送给接收者A。接收者A收到封装密文 C 和消息密文 C_M 后，根据当前时间段 t 的私钥 sk_t 和封装密文 C 计算出封装密钥 K，最后用封装密钥 K 解密消息密文 C_M 得出明文 M。在本方案中，私钥的更新是单向的，即使当前时间段的私钥 sk_t 泄露了，也不会威胁到以前密文的机密性，攻击者不能使用私钥 sk_t 解密在时间段 t 之前的密文。因此，解决了上述私钥泄露带来的安全问题，实现了前向安全。同时，本文的方案还采用密钥封装机制，在保证前向安全的同时又提高了加密算法的效率。

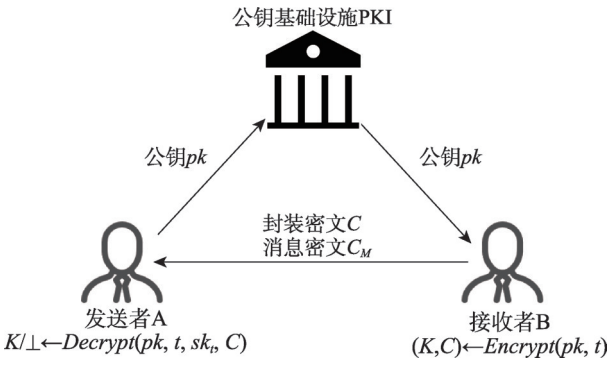

图2 前向安全公钥加密方案示意图

Fig.2 Forward-secure public-key encryption scheme

1 相关工作

前向安全最早在文献[8]中被提出，起源于会话密钥协商协议。文献[12]给出了更完整的表述，长期密钥的泄露不会导致短期会话密钥的泄露，即当前的会话密钥被泄露，之前的短期会话密钥仍能保持机密性。该安全概念也同样适用于签名和加密，因此具有前向安全的数字签名和公钥加密方案相继被提出。在1997年，Anderson受邀在ACM CCS会议上作报告，首次提出了前向安全数字签名，但未能提出具体方案，该问题一直未能得到解决。直到1999年，Bellare等[6]提出了第一个前向安全数字签名方案。到2003年，Bellare等[13]又提出了具有前向安全性的伪随机数生成器，并使用该伪随机数生成器构造出了具有前向安全性的消息认证和对称加密方案。同年Canetti等[1]提出了第一个前向安全公钥加密方案。此后随着密码学的发展，前向安全的概念得到广泛应用。越来越多的密码算法和密码协议都具有前向安全性。Boneh等[14]提出具有固定长度密文的HIBE方案时，也同时提出了具有前向安全性的HIBE方案。Green等[15]在2015年NDSS会议上提出了可穿刺加密，并和前向安全公钥加密结合形成了前向安全的可穿刺加密方案，提升了穿刺效率的同时，也实现了细粒度与粗粒度结合的解密撤销操作。

我国自主研发的商用标识密码算法SM9，自从被提出以来，SM9就一直得到了广泛的应用与研究。该算法作为我国密码行业标准，已被广泛应用在云计算[16]、物联网[17]、区块链[18]等多个领域，并且已经成为ISO/IEC国际标准。到目前为止，SM9的标准文档包含了密钥协商协议、数字签名算法、密钥封装机制和公钥加密算法[19]，得到了国内外许多学者的积极研究。在2019年，文献[20]等结合盲签名和SM9算法的优点，提出了基于SM9的盲签名方案。为解决区块链交易中的数据泄露问题，文献[21]基于SM9算法提出了可证明安全的区块链隐私保护方案。为了实现高效安全的密钥分发方案，文献[22]提出了一种关于SM9的可分离匿名分布式密钥分发方案。在标识密码算法SM9的基础上，文献[23]提出了高效的分层标识加密（HIBE）方案，该方案具有固定长度的密文。基于标识密码算法SM9的广播加密方案[19]不仅是可证明安全的，而且与现有的标识广播加密方案相比，效率相当。但相关单位公布标识密码算法SM9时，只公布了算法描述而未公布算法的安全性分析。2018年，文献[24]给出了基于SM9密钥交换协议，密钥封装机制和加密算法的安全性分析。文献[25]后来基于 q-SDH困难问题证明了基于SM9的签名算法的安全性，并基于 q-BDHI困难问题使用密钥封装机制提出了具有IND-CCA安全的加密方案Twin-SM9。据作者所知，目前还没有基于SM9的前向安全的公钥加密方案，本文首次构造出基于SM9的具有前向安全性的公钥加密方案，弥补了标识密码算法SM9不提供前向安全性的缺陷。

2 预备知识

2.1 双线性对

本节介绍双线性对的概念及其相关符号[26-27]，设群 $\mathbb{G}_1$，$\mathbb{G}_2$ 是两个（加法）循环群，群 $\mathbb{G}_T$ 是一个（乘法）循环群，这三个群的阶都是一个大素数 p，群元素 P、Q 分别是群 $\mathbb{G}_1$、$\mathbb{G}_2$ 的生成元，e 是一个双线性对映射 $e:\mathbb{G}_1\times\mathbb{G}_2\rightarrow G_T$，双向性对映射 e 满足的性质有：

（1）双线性。对于任意的 $a,b\in\mathbb{Z}_p$ 都有 $e(aP,bQ)=e(P,Q)^{ab}$。

（2）非退化性。$e(P,Q)\neq 1$。

（3）可计算性。双线性对映射 e 可以在多项式时间内计算。

双线性群可以分为两类，第一种类型为对称双线群，群 $\mathbb{G}_1$ 和群 $\mathbb{G}_2$ 相同，或群 $\mathbb{G}_1$ 和群 $\mathbb{G}_2$ 不同，但群 $\mathbb{G}_1$ 和群 $\mathbb{G}_2$ 存在一个同态映射，第二种类型为非对称双线性群，群 $\mathbb{G}_1$ 和群 $\mathbb{G}_2$ 不同，且群 $\mathbb{G}_1$ 和群 $\mathbb{G}_2$ 不存在任何同态映射。本文使用符号 $\mathcal{BP}=(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,p)$ 表示非对称双线性群[28]。

2.2 困难问题假设

本方案的安全性基于 (q, n)-DBDHI问题[23]，设非对称双线性对 $\mathcal{BP}=(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,p)$，设生成元 $P_1\in\mathbb{G}_1$，

$P_2\in\mathbb{G}_2$，给出群元素 $(c,P_1,bP_1,aP_1,a^2P_1,\cdots,a^{n+1}P_1,P_2,bP_2,aP_2,a^2P_2,\cdots,a^qP_2,\frac{1}{(a+c)^2}P_2,\frac{1}{(a+c)^3}P_2,\cdots,\frac{1}{(a+c)^n}P_2)$ 和元素 $X\in\mathbb{G}_T$，判断 X 等于 $e(P_1,P_2)^{b/(a+c)}$ 还是群 $\mathbb{G}_T$ 的一个随机元素，其中 a，b，c 都是随机数，且 a，b 未知。

3 前向安全公钥加密方案

3.1 方案定义

本文的前向安全公钥加密方案（forward-secure SM9，FS-SM9）由4个多项式时间算法描述，这4个算法分别是Setup、Update、Encrypt和Decrypt，每个算法的形式化定义及简单说明如下：

$(pk,sk_0)\leftarrow Setup(1^\lambda,T)$。该算法的输入为安全参数 1^λ 和时间段的总数量 T，输出为公钥 pk 和时间段0的私钥 sk_0，公钥 pk 是公开的，所有人都能获取到，而私钥 sk_0 由用户秘密保存，用于生成下一个时间段的私钥。

$sk_{t+1}\leftarrow Update(pk,t,sk_t)$。该算法的输入为公钥 pk，当前时间段 $t<T$ 和当前时间段对应的私钥 sk_t，输出下一个时间段的私钥 sk_{t+1}。

$(K,C)\leftarrow Encrypt(pk,t)$。该算法的输入为公钥 pk 和当前时间段 $t<T$，输出为封装密钥（又称会话密钥）K 和封装密文 C。如果需要加密的消息为 M，加密者生成封装密钥 K 后，选取安全的对称加密系统以 M 和 K 为输入，运行对称加密算法生成数据密文 C_M。

$K/\perp\leftarrow Decrypt(pk,t,sk_t,C)$。该算法的输入为公钥 pk，当前时间段 $t<T$ 以及当前时间段对应的私钥 sk_t 和封装密文 C，如果解密成功则输出为封装密钥 K，否则输出 $\perp$。如果解密者正确恢复出封装密钥 K，则以 K 和 C_M 为输入，运行对称解密算法恢复出消息 M。本文只给出密钥封装形式，而忽略对称加解密算法部分。

前向安全公钥加密方案的正确性要求为：对于任意的由系统建立算法生成的公私钥对 $(pk,sk_0)\leftarrow Setup(1^\lambda,T)$，任何时间段 $0<t<T$，以及该时间段对应的正确私钥 sk_t，都有由加密算法生成的封装密钥 $(K,C)\leftarrow Encrypt(pk,t)$ 和由解密算法生成的封装密钥 $K'\leftarrow Decrypt(pk,t,sk_t)$ 相等 $K=K'$。

3.2 安全模型

本文选用的安全模型[29]通过挑战者和攻击者之间的交互游戏定义[1]，攻击者在攻击方案之前要把挑战时间提前告知挑战者，该游戏分为5个阶段，攻击者在和挑战者进行交互游戏之前，攻击者需要提前告知挑战者挑战时间 t^*，具体定义如下：

初始化。攻击者将挑战时间 t^* 发送给挑战者，其中 $0<t^*<T$。

系统建立。挑战者根据安全参数 1^λ 和时间段的总数量 T，运行系统建立算法Setup，生成公钥和私钥对 (pk,sk_0)，并将公钥 pk 发送给攻击者，秘密保存私钥 sk_0。

询问1。攻击者可以适应性地询问时间段 t 的私钥 sk_t，但要求攻击者询问的时间 $t>t^*$，挑战者多次运行密钥更新算法Update更新当前时间段的私钥，直到生成攻击者询问的时间段 t 的私钥 sk_t，并将私钥 sk_t 返回给攻击者。

挑战。询问1阶段结束后，挑战者运行加密算法 $Encrypt(pk,t^*)$ 生成挑战封装密钥 K^* 和封装密文 C^*，随机选取一个比特 $\mu\in\{0,1\}$，设置 $K_\mu=K^*$，随机从封装密钥空间中选择一个封装密钥，并用 $K_{1-\mu}$ 表示该封装密钥，把挑战信息 (C^*,K_0,K_1) 发送给攻击者。

询问2。攻击者可以继续适应性地向挑战者询问时间段 t 的私钥 sk_t，但要求 $t>t^*$，挑战者的回复与询问1阶段相同。

猜测。攻击者输出一个对比特 μ 的猜测比特 $\mu'\in\{0,1\}$，如果 $\mu=\mu'$，则攻击者获胜，否则失败。

攻击者 $\mathcal{A}$ 成功攻破方案的优势定义为：

$$Adv_{\mathcal{A}}^{\text{IND-FS-CPA}}(1^\lambda)=|\Pr[\mu'=\mu]-\frac{1}{2}|$$

定义1 如果没有任何攻击者 $\mathcal{A}$ 能在多项式时间内以不可忽略的优势赢得以上游戏，则称该方案是IND-FS-CPA安全的。

3.3 具体构造

实现前向安全的关键在于使用一棵二叉树，将时间轴上的时间段按先序遍历的顺序映射到一棵完全二叉树的节点，即每个时间段对应二叉树上的一个节点。同时，每个二叉树的节点 w 对应着一个私钥 k。二叉树上的每个节点到根节点 ϵ 的路径由一个路径向量表示，二叉树中的左分支用 I_0 表示，右分支 I_1 表示。因此，路径向量的形式为 $(x_0,x_1,\cdots,x_d)$，其中 $x_0=\epsilon$，$x_i\in\{I_0,I_1\}$，d 为节点 w 的层次数，要求 d 小于等于二叉树的深度 ℓ，如图3所示。时间段 t 的私钥 sk_t 由一个栈 S 构成，设时间段 t 在二叉树上对应

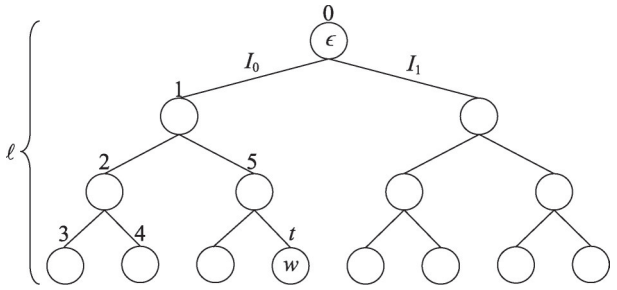

图3 二叉树示意图

Fig.3 Binary tree

节点为 w，栈 S 里面保存节点 w 到根节点 ϵ 的路径节点的右兄弟节点的私钥和节点 w 的私钥。私钥 sk_t 的栈顶私钥为节点 w 的私钥，加密时使用 pk 和时间段 t 对应的二叉树节点 w 的路径向量 $(x_0,x_1,\cdots,x_d)$ 加密名明文 M，解密时使用栈顶二叉树节点 w 的私钥 k 解密密文 C。栈 S 里的其他节点的私钥用于派生这些节点的子节点的私钥，即使当前时间段的私钥被泄露，攻击者仍不能用栈 S 中节点的私钥去解密以前时间段的密文，这样实现了前向安全。

加密时需要将时间段转换成二叉树节点的路径向量，设函数 $T2PV$ 为时间转换函数，该函数的输入为时间段 t，输出为时间段 t 在二叉树上对应节点 w 的路径向量，$T2PV(t)=(x_0,x_1,\cdots,x_d)$。本方案的4个算法的具体构造如下。

Setup。设 1^λ 为安全参数，最大时间段的数量为 T，计算二叉树的深度为 $\ell=\lceil\log T\rceil$，首先根据安全参数 1^λ 生成非对称双线性群 $\mathcal{BP}=(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,p)$，随机选取生成元 $P\in\mathbb{G}_1$，Q，Q_1，Q_2，$\cdots$，$Q_\ell\in\mathbb{G}_2$，随机选择 h_ϵ，h_0，$h_1\in\mathbb{Z}_p^*$，并设函数 $H:\{\epsilon,I_0,I_1\}\rightarrow\mathbb{Z}_p^*$ 为：

$$H(x)=\begin{cases}h_\epsilon,x=\epsilon\\h_0,x=I_0\\h_1,x=I_1\end{cases}$$

选择合适的密钥派生函数 $KDF:\{0,1\}^*\rightarrow\{0,1\}^L$，其中 L 为封装密钥的比特长度，随机选择 $\alpha\in\mathbb{Z}_p^*$，计算 $R=\alpha P$，$A=e(R,Q)$，设时间转换函数 $T2PV$ 的输入为时间段 t，输出为时间段 t 在二叉树上对应节点 w 的路径向量。系统的公钥 pk 为：

$$pk=(P,R,Q,Q_1,Q_2,\cdots,Q_\ell,A,H,KDF,T,T2PV)$$

私钥 sk_0 由一个栈 S 构成，随机选择 $r\in\mathbb{Z}_p^*$，并生成根节点密钥 k：

$$k=\left(\frac{\alpha}{\alpha+H(\epsilon)}Q,r(\alpha+H(\epsilon))P,rQ_1,rQ_2,\cdots,rQ_\ell\right)$$

然后，把密钥 k 压入栈中 $S.push(k)$，时间段0的私钥为 $sk_0=S$。输出系统的公钥 pk 和时间段0的私钥 sk_0。

Update。已知当前时间段的私钥为 sk_t，用栈 S 表示私钥 sk_t，从栈中弹出一个私钥 $k=S.pop()$，调用函数 $T2PV$ 生成时间段 t 对应的二叉树节点 w 的路径向量 $(x_0,x_1,x_2,\cdots,x_d)$，如果节点 w 为叶子节点则设置下一个时间段的私钥 $sk_{t+1}=S$，运行结束并返回。如果节点 w 为非叶子节点，则要分别生成节点 w 的左右子节点的私钥 k_0，k_1，并先将右节点的私钥 k_1 压入栈中，再将左节点的私钥 k_0 压入栈中。设节点 w 的私钥 k 的形式为：$(a_0,a_1,b_{d+1},b_{d+2},\cdots,b_\ell)$，随机选取 $r_0\in\mathbb{Z}_p^*$，左子节点的私钥 k_0 的计算方式为：

$$a_0'=a_0+H(I_0)b_{d+1}+r_0\sum_{i=1}^{d}H(x_i)Q_i+r_0H(I_0)Q_{d+1}$$
$$a_1'=a_1+r_0(R+H(\epsilon)P)$$
$$b_{d+2}'=b_{d+2}+r_0Q_{d+2}$$
$$\vdots$$
$$b_\ell'=b_\ell+r_0Q_\ell$$
$$k_0=(a_0',a_1',b_{d+2}',\cdots,b_\ell')$$

随机选取 $r_1\in\mathbb{Z}_p^*$，右子节点私钥 k_1 的计算方式为：

$$a_0''=a_0+H(I_1)b_{d+1}+r_1\sum_{i=1}^{d}H(x_i)Q_i+r_1H(I_1)Q_{d+1}$$
$$a_1''=a_1+r_1(R+H(\epsilon)P)$$
$$b_{d+2}''=b_{d+2}+r_1Q_{d+2}$$
$$\vdots$$
$$b_\ell''=b_\ell+r_1Q_\ell$$
$$k_1=(a_0'',a_1'',b_{d+2}'',\cdots,b_\ell'')$$

分别把 k_1 和 k_0 压入栈中，即 $S.push(k_1)$，$S.push(k_0)$，把更新后的栈 S 设为下一时间段的私钥 $sk_{t+1}=S$。

Encrypt。设当前时间段为 t，加密者调用函数 $T2PV$ 得到时间段 t 对应的二叉树节点 w 的路径向量 $(x_0,x_1,x_2,\cdots,x_d)$，随机选取 $s\in\mathbb{Z}_p^*$，分别计算：

$$W=A^s,C_1=s(R+H(\epsilon)P),C_2=s\sum_{i=1}^{d}H(x_i)Q_i$$

计算 $K=KDF(C_1\|C_2\|W\|t\|L)$，如果 K 为全为0的比特串，则重新选择一个随机数 s，重新运行上述算法，设 $C=(C_1,C_2)$，最后输出封装密钥和封装密文 (K,C)。

Decrypt。设封装密文为 $C=(C_1,C_2)$，当前时间段为 t，对应的私钥为 sk_t，用栈 S 表示私钥 $sk_t=S$，从

栈中获取二叉树节点的私钥 $k=S.getTop()$，设私钥 k 的形式为 $(a_0,a_1,b_{d+1},b_{d+2},\cdots,b_\ell)$，计算：

$$W'=\frac{e(C_1,a_0)}{e(a_1,C_2)}$$

然后计算封装密钥 $K'=KDF(C_1\|C_2\|W'\|t\|L)$，如果 K' 不为全0比特串，输出封装密钥 K'，成功返回，否则，输出错误信息 $\perp$。

3.4 正确性分析

设 $C=(C_1,C_2)$ 为正确的封装密文，当前时间段 t 对应的私钥为 sk_t，用栈 S 表示私钥 $S=sk_t$，调用函数 $T2PV$ 生成时间 t 对应二叉树节点的路径向量 $(x_0,x_1,x_2,\cdots,x_d)$，从栈 S 中获取栈顶密钥 $k=S.getTop()$，密钥 k 具有形式 $(a_0,a_1,b_{d+1},b_{d+2},\cdots,b_\ell)$，则有：

$$W'=\frac{e(C_1,a_0)}{e(a_1,C_2)}=\frac{e\left(s(R+H(\epsilon)P),\frac{\alpha}{\alpha+H(\epsilon)}Q+r\sum_{i=1}^{d}H(x_i)Q_i\right)}{e\left(r(\alpha+H(\epsilon))P,s\sum_{i=1}^{d}H(x_i)Q_i\right)}=\frac{e\left(s(R+H(\epsilon)P),\frac{\alpha}{\alpha+H(\epsilon)}Q\right)}{e\left(r(\alpha+H(\epsilon))P,s\sum_{i=1}^{d}H(x_i)Q_i\right)}\cdot e\left(s(R+H(\epsilon)P),r\sum_{i=1}^{d}H(x_i)Q_i\right)=e(R,Q)^s=W$$

因为 (C_1,C_2) 是正确的封装密文，所以有 $W'=W$，$K'=KDF(C_1\|C_2\|W'\|sk_t\|L)=KDF(C_1\|C_2\|W\|sk_t\|L)=K$，满足前向安全公钥加密方案的正确性要求。

3.5 安全性分析

定理1 如果 (q,n)-DBDHI 问题在双线性群 $\mathcal{BP}=(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,p)$ 上面是困难的，则本文提出的前向安全公钥加密方案FS-SM9在标准模型下是IND-FS-CPA安全的。

证明 假设存在攻击者 $\mathcal{A}$ 在多项式时间内能以不可忽略的优势攻破方案，则可以构造一个模拟算法 $\mathcal{B}$ 通过与 $\mathcal{A}$ 交互，在多项式时间内以不可忽略的优势求解 (q,n)-DBDHI 问题。在证明过程中，模拟算法 $\mathcal{B}$ 扮演IND-FS-CPA安全模型游戏中的挑战者。给模拟者 $\mathcal{B}$ 的 (q,n)-DBDHI 问题实例为：

$$(c,P_1,bP_1,aP_1,a^2P_1,\cdots,a^{n+1}P_1,P_2,bP_2,aP_2,a^2P_2,\cdots,a^qP_2,\frac{1}{(a+c)^2}P_2,\frac{1}{(a+c)^3}P_2,\cdots,\frac{1}{(a+c)^n}P_2,X)$$

模拟算法 $\mathcal{B}$ 的目标是判断 X 是否等于 $e(P_1,P_2)^{b/(a+c)}$，其中 q 表示一个正整数，n 表示二叉树的深度。

初始化。攻击者 $\mathcal{A}$ 输出挑战时间 t^*，其中 $0<t^*<T$。

系统建立。模拟者 $\mathcal{B}$ 首先设置 $H(\epsilon)=c$，$H(I_0)=w_0$，$H(I_1)=w_1$，其中 w_0，$w_1\in\mathbb{Z}_p^*$ 是随机数，模拟者 $\mathcal{B}$ 在不知道 a 的情况下，设置 $\alpha=a$，$\beta=a+c+1$，并通过已知问题的实例计算：

$$P=P_1,R=aP_1,Q=\beta P_2,A=(R,Q)$$

选取 ℓ 个随机数 y_1，y_2，$\cdots$，$y_\ell\in\mathbb{Z}_p^*$，对于 $i=1$ 和任意 $2<i<\ell$ 分别计算：

$$Q_1=\frac{y_1}{(a+c)^2}P_2,Q_i=\frac{y_i}{(a+c)^3}P_2$$

最后选取恰当的密钥派生函数 KDF 和时间转换函数 $T2PV$，并输出系统的公钥：

$$pk=(P,R,Q,Q_1,Q_2,\cdots,Q_\ell,A,H,KDF,T,T2PV)$$

询问1。在此阶段，挑战者 $\mathcal{A}$ 可以询问任何时间 $t>t^*$ 的私钥 sk_t，私钥 sk_t 由时间段 t 对应的节点 w 到根节点 ϵ 的路径节点的右兄弟节点的私钥和节点 w 的私钥构成，这些节点的私钥生成方式基本一样。本文只详细说明节点 w 的私钥 k 的模拟过程。模拟者 $\mathcal{B}$ 调用函数 $T2PV$ 生成二叉树的节点 w 的路径向量 $(x_0,x_1,x_2,\cdots,x_d)$，其中 $d\geqslant 1$，选取随机数 $Z\in\mathbb{Z}_p^*$，设：

$$Y_i=\begin{cases}y_iH(I_0),x_i=I_0\\y_iH(I_1),x_i=I_1\end{cases},1\leqslant x\leqslant d$$

$$r=Z+(a+c)Y_1^{-1}$$

然后分别计算 a_0 和 a_1：

$$a_0=\frac{\alpha}{\alpha+H(\epsilon)}Q+r\sum_{i=1}^{d}H(x_i)Q_i=\frac{a(a+c+1)}{a+c}P_2+\left(Z+c(a+c)Y_1^{-1}\right)\cdot\left(\frac{Y_1}{(a+c)^2}P_2+\sum_{i=2}^{d}\frac{Y_i}{(a+c)^3}P_2\right)=(a+1)P_2-\frac{c}{a+c}P_2+Z\left(\frac{Y_1}{(a+c)^2}P_2+\sum_{i=2}^{d}\frac{Y_i}{(a+c)^3}P_2\right)+\frac{c}{a+c}P_2+cY_1^{-1}\sum_{i=2}^{d}\frac{Y_i}{(a+c)^2}P_2=(a+1)P_2+Z\left(\frac{Y_1}{(a+c)^2}P_2+\sum_{i=2}^{d}\frac{Y_i}{(a+c)^3}P_2\right)+cY_1^{-1}\sum_{i=2}^{d}\frac{Y_i}{(a+c)^2}P_2$$

$$a_1 = r(\alpha + H(\epsilon))P = (Z + (a+c)Y_1^{-1})(a+c)P_1 = Z(a+c)P_1 + Y_1^{-1}(a+c)^2 P_1 = Z(a+c)P_1 + Y_1^{-1}(a^2 + 2ac + c^2)P_1$$

对于任意 $d+1 \leqslant i \leqslant \ell$，计算：

$$b_i = rQ_i = (Z + (a+c)Y_1^{-1})\frac{y_i}{(a+c)^3}P_2 = Z\frac{y_i}{(a+c)^3}P_2 + Y_1^{-1}\frac{Y_1^{-1}}{(a+c)^2}$$

不难看出，以上式子都可以由给出的困难问题实例求出，因此，节点 w 的私钥 $k=(a_0,a_1,b_{d+1},b_{d+2},\cdots,b_\ell)$ 也可以由给出的困难问题实例求出。同理，可以构造出私钥 sk_t 中其他节点的私钥，将这些私钥按照正确的顺序压入栈中，形成时间段 t 的私钥 sk_t。之后，模拟者 $\mathcal{B}$ 把私钥 sk_t 发送给挑战者 $\mathcal{A}$。

挑战。询问1阶段结束后，模拟者 $\mathcal{B}$ 调用 *T2PV* 函数生成时间段 t^* 对应二叉树节点 w^* 的路径向量 $(x_0^*,x_1^*,x_2^*,\cdots,x_{d^*}^*)$，将挑战密文的随机数设为 $s^* = \frac{b}{a+c}$，并分别计算 C_1^*、C_2^* 和 W^*：

$$C_1^* = s^*(R + H(\epsilon)P) = \frac{b}{a+c}(a+c)P_1 = bP_1$$

$$C_2^* = s^*\sum_{i=1}^{d^*} H(x_i^*)Q_i = \frac{b}{a+c}\left(\frac{H(x_1^*)y_1}{(a+c)^2}P_2 + \sum_{i=2}^{d^*}\frac{H(x_i^*)y_i}{(a+c)^3}P_2\right) = b\left(\frac{H(x_1^*)y_1}{(a+c)^3}P_2 + \sum_{i=2}^{d^*}\frac{H(x_i^*)y_i}{(a+c)^4}P_2\right)$$

$$W^* = e(bP_1,(a+1)P_2)\cdot X^{-c}$$

如果 $X = e(P_1,P_2)^{\frac{b}{a+c}}$，则有：

$$W^* = e(bP_1,(a+1)P_2)\cdot X^{-c} = e(bP_1,(a+1)P_2)\cdot\left(e(P_1,P_2)^{\frac{b}{a+c}}\right)^{-c} = \left(e\left(P_1,\left(a+1-\frac{c}{a+c}\right)P_2\right)\right)^b = (e(aP_1,(a+c+1)P_2))^{\frac{b}{a+c}} = e(R,Q)^{s^*}$$

不难看出，以上式子都可以由给出的困难问题实例求出，计算 $K^* = KDF(C_1^*||C_2^*||W^*||t^*||L)$，当 $X = e(P_1,P_2)^{b/(a+c)}$ 时，(C_1^*,C_2^*) 是密钥 K^* 的合法密文。随机选择一个比特 $\mu \in \{0,1\}$，设置 $K_\mu = K^*$，随后从密钥空间中选取一个随机密钥，将其设为 $K_{1-\mu}$，然后将挑战信息 (C_1^*,C_2^*,K_0,K_1) 发送给攻击者 $\mathcal{A}$。

询问2。攻击者 $\mathcal{A}$ 可以继续适应性地询问私钥，模拟者 $\mathcal{B}$ 的回复与询问1阶段相同。

猜测。以上阶段都结束后，攻击者 $\mathcal{A}$ 输出对 μ 的猜测值 $\mu' \in \{0,1\}$，如果 $\mu' = \mu$，模拟者 $\mathcal{B}$ 输出“1”，表示 (q, n)-DBDHI 困难问题实例中的 $X = e(P_1,P_2)^{b/(a+c)}$，如果 $\mu' \neq \mu$，则输出“0”，表示困难问题中实例 X 是群 $\mathbb{G}_T$ 中的随机元素。

从上面的证明过程可知，模拟方案和真实方案是不可区分的，且模拟过程不会发生中断。然后分析 $\mathcal{B}$ 解决困难问题的优势。当 $X = e(P_1,P_2)^{b/(a+c)}$ 时，因为模拟方案和真实方案是不可区分的，假设攻击者 $\mathcal{A}$ 攻破方案的优势为 η，则有：

$$\Pr\left[\mu = \mu' | X = e(P_1,P_2)^{\frac{b}{a+c}}\right] = \eta + \frac{1}{2}$$

当 $X \in \mathbb{G}_T$ 是不等于 $e(P_1,P_2)^{b/(a+c)}$ 的随机元素时，则 $W^* = e(bP_1,(a+1)P_2)\cdot X^{-c}$ 是群 $\mathbb{G}_T$ 中的随机元素，对 $\mathcal{A}$ 来说，即 W^* 与 C_1^* 和 C_2^* 相互独立，所以有：

$$\Pr\left[\mu = \mu' | X \neq e(P_1,P_2)^{\frac{b}{a+c}}\right] = \frac{1}{2}$$

综上所述，模拟者 $\mathcal{B}$ 正确解决 (q, n)-DBDHI 问题的优势为：

$$Adv_{\mathcal{B}}^{(q,n)-\mathrm{DBDHI}}(1^\lambda) = \left|\frac{1}{2}\Pr\left[\mu = \mu' | X = e(P_1,P_2)^{\frac{b}{a+c}}\right] + \frac{1}{2}\Pr\left[\mu = \mu' | X \neq e(P_1,P_2)^{\frac{b}{a+c}}\right] - \frac{1}{2}\right| = \left|\frac{1}{2}\left(\eta + \frac{1}{2}\right) + \frac{1}{2}\times\frac{1}{2} - \frac{1}{2}\right| = \frac{1}{2}\eta$$

上述安全性分析证明本方案是 IND-FS-CPA 安全的。在上述证明过程中，没有把哈希函数假设为随机喻言机[30]，即上述证明过程是在标准模型下进行论证的。

4 实验分析

4.1 性能分析

本节从理论上分析 FS-SM9 方案的计算开销、存储开销和安全性，并与类似方案（FS-PKE[1]，PFSE[15]）和不具备前向安全性的 SM9 算法（Basic SM9，Basic-SM9[31]）进行对比，结果如表1所示。对比只涉及密钥封装，而忽略对称加密算法的开销。系统初始算

表1 FS-SM9和其他方案的对比

Table 1 Comparison of FS-SM9 and other schemes

Schemes	Computational overhead			Storage overhead			Assumption	Security	Standard model
	Update	Encrypt	Decrypt	Public key size	Private key size	Ciphertext overhead			
FS-PKE[1]	$O(\mathrm{lb}T)$	$O(\mathrm{lb}T)$	$O(\mathrm{lb}T\cdot\mathcal{P})$	$O(\mathrm{lb}T)$	$O(\mathrm{lb}T)$	$O(\mathrm{lb}T)$	DBDH	Selective	Yes
PFSE[15]	$O(\mathrm{lb}T)$	$O(\mathrm{lb}T\cdot d)$	$O((\mathrm{lb}T+d)\cdot\mathcal{P})$	$O(\mathrm{lb}T+d)$	$O(d\cdot\mathrm{lb}T)$	$O(d)$	q-DBDHI,DBDH	Selective	No
Basic-SM9[31]	—	$O(1)$	$O(1)$	$O(1)$	$O(1)$	$O(1)$	—	—	—
FS-SM9	$O(\mathrm{lb}T)$	$O(\mathrm{lb}T)$	$O(1)$	$O(\mathrm{lb}T)$	$O(\mathrm{lb}T)$	$O(1)$	(q, n)-DBDHI	Selective	Yes

法Setup只在系统建立时运行，随后便不再运行，其开销并不影响方案的实用性，所以本文只对比除Setup算法的其他三种算法的计算开销。椭圆曲线上的加法运算和乘法运算开销较小，一般视为常数，而双线性群上的配对运算则不能忽略。用$\mathcal{P}$表示双线性群上一次配对运算所需要的时间，用T表示具有前向安全的公钥加密系统中的时间段总数。FS-PKE和PFSE都具有前向安全，因此在计算开销和存储开销方面，与本文方案类似，都与$\mathrm{lb}\,T$因子成正比。但这两种方案的密文长度都比FS-SM9长，所以解密开销也明显大于本方案FS-SM9。在安全性方面，FS-PKE和PFSE与FS-SM9都是可证明安全的。由于Basic-SM9方案不具备前向安全性，故该方案没有Update算法。由表1中的对比结果可知，在时间开销方面，FS-SM9的加密算法比Basic-SM9的加密算法多了$\mathrm{lb}\,T$因子，效率有所降低。但在实际应用中，由于$\mathrm{lb}\,T$的增长是随时间段的总数T的增长而以对数速率增长，即使时间段的总数T很大，加密算法的运行时长也不会明显增加，符合实际应用需求，具体实验结果见下一节。FS-SM9的私钥更新算法的时间开销和加密算法类似。在解密效率上，FS-SM9的所需时长要比Basic-SM9稍长，因为FS-SM9的解密算法更复杂，涉及更多的双线性群上的运算和其他操作。在安全性方面，相关单位目前只公布了Basic-SM9方案的算法，而未公布其安全性分析，本文提出的方案FS-SM9基于(q, n)-DBDHI困难问题假设，具有IND-FS-CPA安全性。

4.2 实验结果

本节通过实验分析方案的可行性，并与Basic-SM9方案进行对比。由于FS-PKE和PFSE并非基于国密，在一些特定应用场景中，难以满足需求，所以本文并未实现这些方案。Basic-SM9和FS-SM9两种方案的加解密运行时间对比如图4所示。本方案（FS-SM9）使用C++编程语言和Miracl密码库实现，曲线使用SM9标准推荐的曲线[32]，安全性满足128 bit。实验设备的配置为：台式电脑，64位Windows 7中文操作系统，Intel® Core™ i5-4590 CPU@3.30 GHz，运行内存为4 GB。该实验环境在可以模拟资源受限的设备（智能终端机[33]）。在测试之前，将FS-SM9方案的参数T设为$T=10^6$，加解密时间段t设为$t=1$，测试方法为多次测量单次加解密时间并取平均值，在给定参数的条件下，与Basic-SM9的单次加解密时间开销进行对比。通过对比实验结果可知，由于本方案在Basic-SM9的基础上，保证了前向安全性，FS-SM9的加解密运行时间比Basic-SM9的运行时间稍长。FS-SM9的加密运行时间为10.0 ms，仅比Basic-SM9多出5.6 ms。对于绝大多数需要与用户交互的应用场景而言，5.6 ms是可以忽略的，用户一般不会察觉到几毫秒的延迟。同时，FS-SM9方案也赋予了系统前向安全性，避免了系统私钥泄露带来的威胁。

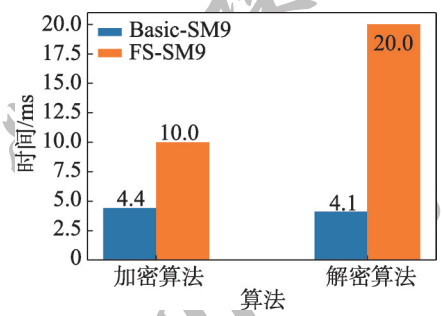

图4 Basic-SM9和FS-SM9的加解密时间对比

Fig. 4 Comparison of encryption and decryption time between Basic-SM9 and FS-SM9

本方案FS-SM9的私钥更新算法和加密算法与时间段的总数有关。由前面的理论分析可知，加密时间和私钥更新的时间开销会随着时间段总数量T

的增加而以对数速率增加，而解密时间为常数。如图5所示，实验结果和理论分析相符。为测试时间段总数对加密算法、私钥更新算法和解密算法的运行时间的影响，将时间段总数量 T 分别设为 10^0，10^1，10^2，10^3，10^4，10^5，10^6，加解密时间段 t 对应分别设为1，5，25，50，150，200，250。依次在每种情况下多次测量单次加密算法，私钥更新算法和解密算法的运行时间，最后取平均值得到最终测量时间。由图5可知，解密时间与时间段总数量 T 无关。私钥更新算法Update的运行时长比加密算法Encrypt稍多，这是由于私钥更新算法Update需要额外的运算操作，但都以对数速率增长。在时间段总数量 $T=10^6$，时间段 $t=250$ 时，加密算法和私钥更新算法的运行时长分别为41.4 ms和42.8 ms，即使时间段总数量达到 10^6 数量级，本方案FS-SM9的加密算法和私钥更新算法的运行时间的数量级依然是毫秒级。在绝大多数需要与用户交互的应用之中，这些时间可以忽略。

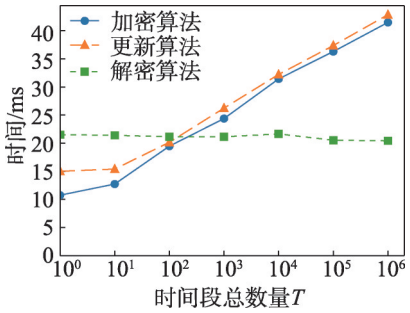

图5 时间段总数对每个算法的影响

Fig. 5 Impact of total time periods on each algorithm

5 总结

基于我国商用标识密码算法SM9，本文首次提出了具有前向安全性的公钥加密方案，并在 (q, n)-DBDHI困难问题假设下证明了方案的安全性。该方案使用密钥封装机制，同时兼顾了对称加密和非对称加密的优点。该方案的优势在于前向安全，可通过Update算法来更新用户的私钥，即使当前私钥被泄露，攻击者仍不能使用泄露的私钥解密以前的会话密文，这避免了密钥泄露带来的安全风险。本文在给出具体算法的同时，也给出了详细的安全性证明，在标准模型下，证明了本方案FS-SM9在 (q, n)-DBDHI困难问题假设下是IND-FS-CPA安全的。与不具有前向安全性的标识密码算法SM9相比，FS-SM9只引入了可忽略的时间开销，不会降低方案的实用性。

参考文献：

[1] CANETTI R, HALEVI S, KATZ J. A forward-secure public key encryption scheme[C]//Proceedings of the 2003 International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, May 4-8, 2003. Berlin, Heidelberg: Springer, 2003: 255-271.

[2] BLAKLEY G R. Safeguarding cryptographic keys[C]//Proceedings of the 1979 International Workshop on Managing Requirements Knowledge, New York, Jun 4-7, 1979. Washington: IEEE Computer Society, 1979: 313-318.

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

[4] DESMEDT Y. Threshold cryptosystems[C]//Proceedings of the 1992 International Workshop on the Theory and Application of Cryptographic Techniques. Berlin, Heidelberg: Springer, 1992: 1-14.

[5] HERZBERG A, JAKOBSSON M, JARECKI S, et al. Proactive public key and signature systems[C]//Proceedings of the 4th ACM Conference on Computer and Communications Security, Zurich, Apr 1-4, 1997. New York: ACM, 1997: 100-110.

[6] BELLARE M, MINER S K. A forward-secure digital signature scheme[C]//Proceedings of the Annual International Cryptology Conference, Santa Barbara, Aug 15-19, 1999. Berlin, Heidelberg: Springer, 1999: 431-448.

[7] DIFFIE W, VAN OORSCHOT P C, WIENER M J. Authentication and authenticated key exchanges[J]. Designs, Codes and Cryptography, 1992, 2(2): 107-125.

[8] GÜNTHER C G. An identity-based key-exchange protocol [C]//Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Houthalen, Apr 10-13, 1989. Berlin, Heidelberg: Springer, 1990: 29-37.

[9] DIFFIE W, HELLMAN M E. New directions in cryptography[M]//Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman. New York: ACM, 2022: 365-390.

[10] ABE M, GENNARO R, KUROSAWA K, et al. Tag-KEM/DEM: a new framework for hybrid encryption and a new analysis of Kurosawa-Desmedt KEM[C]//Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer, 2005: 128-146.

[11] KUROSAWA K, DESMEDT Y. A new paradigm of hybrid encryption scheme[C]//Proceedings of the 24th Annual International Cryptology Conference, Santa Barbara, Aug 15-19, 2004. Berlin, Heidelberg: Springer, 2004: 426-442.

[12] DI-CRESCENZO G, ISHAI Y, OSTROVSKY R. Universal service-providers for database private information retrieval [C]//Proceedings of the 17th Annual ACM Symposium on Principles of Distributed Computing, Puerto Vallarta, Jun 28-Jul 2, 1998. New York: ACM, 1998: 91-100.

[13] BELLARE M, YEE B. Forward-security in private-key cryptography[C]//Proceedings of the Cryptographers' Track at the RSA Conference, San Francisco, Apr 13-17, 2003. Berlin, Heidelberg: Springer, 2003: 1-18.

[14] BONEH D, BOYEN X, GOH E J. Hierarchical identity based encryption with constant size ciphertext[C]//Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer, 2005: 440-456.

[15] GREEN M D, MIERS I. Forward secure asynchronous messaging from puncturable encryption[C]//Proceedings of the 2015 IEEE Symposium on Security and Privacy, San Jose, May 17-21, 2015. Washington: IEEE Computer Society, 2015: 305-320.

[16] 涂彬彬, 王现方, 张立廷. 两种分布式SM2/9算法应用[J]. 密码学报, 2020, 7(6): 826-838.
TU B B, WANG X F, ZHANG L T. Two distributed applications of SM2 and SM9[J]. Journal of Software, 2020, 7(6): 826-838.

[17] 董一潇, 全建斌, 王明儒, 等. 国密SM9算法在物联网安全领域的应用研究[J]. 电信工程技术与标准化, 2022, 35(9): 22-27.
DONG Y X, QUAN J B, WANG M R, et al. Research on the application of SM9 algorithm in the security field of Internet of things[J]. Telecom Engineering Technics and Standardization. 2022, 35(9): 22-27.

[18] 唐飞, 甘宁, 阳祥贵, 等. 基于区块链与国密SM9的抗恶意KGC无证书签名方案[J]. 网络与信息安全学报, 2022, 8(6): 9-19.
TANG F, GAN N, YANG X G, et al. Anti malicious KGC certificateless signature scheme based on blockchain and domestic cryptographic SM9[J]. Chinese Journal of Network and Information Security, 2022, 8(6): 9-19.

[19] 赖建昌, 黄欣沂, 何德彪, 等. 基于SM9的CCA安全广播加密方案[J]. 软件学报, 2023, 34(7): 3354-3364.
LAI J C, HUANG X Y, HE D B, et al. CCA secure broadcast encryption based on SM9[J]. Journal of Software. 2023, 34(7): 3354-3364.

[20] 张雪锋, 彭华. 一种基于SM9算法的盲签名方案研究[J]. 信息网络安全, 2019(8): 61-67.
ZHANG X F, PENG H. Blind signature scheme based on SM9 Algorithm[J]. Netinfo Security, 2019(8): 61-67.

[21] 杨亚涛, 蔡居良, 张筱薇, 等. 基于SM9算法可证明安全的区块链隐私保护方案[J]. 软件学报, 2019, 30(6): 1692-1704.
YANG Y T, CAI J L, ZHANG X W, et al. Privacy preserving scheme in block chain with provably secure based on SM9 algorithm[J]. Journal of Software, 2019, 30(6): 1692-1704.

[22] 许盛伟, 任雄鹏, 袁峰, 等. 一种关于SM9的安全密钥分发方案[J]. 计算机应用与软件, 2020, 37(1): 314-319.
XU S W, REN X P, YUAN F, et al. A secure key issuing scheme of SM9[J]. Computer Applications and Software, 2020, 37(1): 314-319.

[23] 赖建昌, 黄欣沂, 何德彪, 等. 基于商用密码SM9的高效分层标识加密[J]. 中国科学:信息科学, 2023, 53(5): 918-930.
LAI J C, HUANG X Y, HE D B, et al. An efficient hierarchical identity-based encryption based on SM9[J]. Scientia Sinica (Informationis), 2023, 53(5): 918-930.

[24] CHENG Z H, ZHAO H. Security analysis of SM9 key agreement and encryption[C]//Proceedings of the 14th International Conference on Information Security and Cryptology, Fuzhou, Dec 14-17, 2018. Cham: Springer, 2019: 3-25.

[25] 赖建昌, 黄欣沂, 何德彪, 等. 国密SM9数字签名和密钥封装算法的安全性分析[J]. 中国科学: 信息科学, 2021, 51(11): 1900-1913.
LAI J C, HUANG X Y, HE D B, et al. Security analysis of SM9 digital signature and key encapsulation[J]. Scientia Sinica (Informationis), 2021, 51(11): 1900-1913.

[26] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[C]//Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Heidelberg: Springer, 2001: 514-532.

[27] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]//Proceedings of the 21st Annual International Cryptology Conference. Berlin, Heidelberg: Springer, 2001: 213-229.

[28] GALBRAITH S D, PATERSON K G, SMART N P. Pairings for cryptographers[J]. Discrete Applied Mathematics, 2008, 156(16): 3113-3121.

[29] GOLDWASSER S, MICALI S. Probabilistic encryption & how to play mental poker keeping secret all partial information[M]//Providing Sound Foundations for Cryptography: on the Work of Shafi Goldwasser and Silvio Micali. New York: ACM, 2019: 173-201.

[30] BELLARE M, ROGAWAY P. Random oracles are practical: a paradigm for designing efficient protocols[C]//Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, Nov 3-5, 1993. New York: ACM, 1993: 62-73.

[31] 密码行业标准化技术委员会. SM9标识密码算法第4部分: 密钥封装机制和公钥加密算法: GM/T0044.4—2016[S]. 北京: 中国标准出版社, 2016.
Technical Committee for Standardization of Cryptographic Industry. Identity- based cryptographic algorithm SM9 - part 4: key encapsulation mechanism and public key encryption algorithm: GM/T0044.4—2016[S]. Beijing: China Standards Press, 2016.

[32] 密码行业标准化技术委员会. SM9标识密码算法第5部分: 参数定义: GM/ T0044.5—2016[S]. 北京: 中国标准出版社, 2016.
Technical Committee for Standardization of Cryptographic Industry. Identity- based cryptographic algorithm SM9 - part 5: parameter definition: GM/T0044.5—2016[S]. Beijing: China Standards Press, 2016.

[33] 曾凡斐, 宋春地, 江大维, 等. 水电厂智能终端网联安全方案设计与实现[J]. 水电与抽水蓄能, 2022, 8(5): 54-61.
ZENG F F, SONG C D, JIANG D W, et al. Design and implementation of networked security solutions for intelligent terminals in hydropower plants[J]. Hydropower and Pumped Storage, 2022, 8(5): 54-61.

黄文峰(2000—),男,湖北孝感人,硕士研究生,主要研究方向为密码学、应用密码学等。
HUNG Wenfeng, born in 2000, M.S. candidate. His research interests include cryptography, applied cryptography, etc.

许胜民(1989—),男,山东荣成人,博士,教授,博士生导师,主要研究方向为密码学、应用密码学等。
XU Shengmin, born in 1989, Ph.D., professor, Ph.D. supervisor. His research interests include cryptography, applied cryptography, etc.

马金花(1990—),女,江苏新沂人,博士,讲师,主要研究方向为密码学、应用密码学等。
MA Jinhua, born in 1990, Ph.D., lecturer. Her research interests include cryptography, applied cryptography, etc.

宁建廷(1988—),男,浙江衢州人,博士,教授,博士生导师,CCF会员,主要研究方向为密码学、数据安全等。
NING Jianting, born in 1988, Ph.D., professor, Ph.D. supervisor, CCF member. His research interests include cryptography, data security, etc.

伍玮(1981—),女,江苏南京人,博士,教授,主要研究方向为密码学、应用密码学等。
WU Wei, born in 1981, Ph.D., professor. Her research interests include cryptography, applied cryptography, etc.