doi:10.11835/j.issn.1000-582X.2022.05.003

一种适用于基于身份的认证密钥协商的逆向防火墙协议

刘 畅[1],王 晋[1],田 里[1],王 捷[1],叶净宇[2],秦 帆[3],周雨阳[4]
(1. 国网湖北省电力有限公司电力科学研究院 能源互联网技术中心,武汉 430077;2. 数字广西集团政企事业部,南宁 530219;3.重庆大学 大数据与软件学院,重庆,400044;4. 电子科技大学计算机科学与工程学院,成都 611731)

摘要:基于身份的认证密钥协商允许两方或者多方在不安全信道上建立安全的会话密钥。目前的认证密钥协商协议无法抵抗导致随机数泄露的后门攻击,比如已知特定于会话的临时攻击。基于此,我们设计了一种适用于基于身份的两方认证密钥协商的逆向防火墙协议。该协议在随机预言机模型下是安全的,能够抵抗强的临时会话秘密值泄露攻击,提供了消息抗泄露性。同时该协议不使用双线性对,节省了系统运行时间。最后,利用 JPBC 库实现了该协议。实验结果表明了该协议与同类型的协议相比,具有较小的带宽和较短的运行时间,十分适合应用于资源受限的系统中。

关键词:基于身份密码体制;认证密钥协商;逆向防火墙;抗信息泄露;离散对数
中图分类号:TP391 **文献标志码**:A **文章编号**:1000-582X(2022)05-021-012

A reverse firewall protocol for identity-based authenticated key agreement

LIU Chang[1], *WANG Jin*[1], *TIAN Li*[1], *WANG Jie*[1], *YE Jingyu*[2], *QIN Fan*[3], *ZHOU Yuyang*[4]
(1. Energy Internet Technology Center, State Grid Hubei Electric Power Research Institute, Wuhan 430077, P. R. China; 2. Government and Enterprise Department, Digital Guangxi Group, Nanning 530219, P. R. China; 3. School of Big Data and Software Engineering, Chongqing University, Chongqing 400044, P. R. China; 4. School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, P. R. China)

Abstract: Identity-based authenticated key agreement allows two or more parties to establish secure session keys over insecure channels. Current authenticated key agreement protocols are unable to resist the backdoor attacks that lead to random number disclosure, such as known session-specific temporary attack. Therefore, we propose a reverse firewall protocol for identity-based authenticated key agreement. The protocol is secure under the random oracle model. In addition, it can resist strong temporary session secret value leakage attack and can provide message leakage resistance. Meanwhile, the protocol saves the system's running time because it does not use bilinear pairing. Finally, we implement the protocol using JPBC library. The experimental results show that the protocol has smaller bandwidth and shorter running time compared with other protocols of the same type. It is very suitable for resource-

收稿日期:2021-02-12
基金项目:四川省科学技术资助项目(2020JDRC0100)。
Supported by Sichuan Science and Technology Program (2020JDRC0100).
作者简介:刘畅(1992—),男,硕士研究生,工程师,主要从事信息安全、电力通信、大数据方向研究,(E-mail)liuchang.sgcc@foxmail.com.

constrained systems.

Keywords: identity-based cryptosystem; authenticated key agreement; reverse firewall; anti-information leakage; discrete logarithm

密钥协商是在不安全信道上建立会话密钥的一种重要方式。Diffie 和 Hellman[1]基于离散对数困难问题,为密钥分发系统(PKDS, public key distribution system)设计了两方密钥协商协议(DH 协议)。该协议在公网上提供了会话密钥服务,防止来自被动攻击者的消息泄露,但不能抵抗来自主动攻击者的扰乱、删除消息等行为:如中间人攻击(MITM, man-in-the-middle)。为了抵抗中间人攻击,Matsumoto 等[2]基于 DH 协议设计了 3 个密钥协商协议:MTI/A0,MTU/B0,MTI/C0。这些协议能够为通信双方建立双方的认证会话密钥,且不利用签名就能抵抗主动攻击。然而,如果一个长期密钥泄露,攻击者就能计算出两方的会话密钥。Kunz-Jacques 和 Pointcheval[3]提出了 2 个新的概念:认证密钥协商(AKA, authenticated key agreement)和带密钥确认的认证密钥协商(AKAC, AKA with key confirmation)。AKA 保证只有特定的参与者能够计算出该次会话密钥。AKAC 在 AKA 的基础上,确认了通信实体都获得该次会话密钥。Law 等[4]设计了一个两方的 AKA 协议(MQV 协议),同时利用消息认证码(MAC, message authentication code)技术设计了一个三方的 AKAC 协议。该协议实现了已知密钥安全、前向安全、密钥控制。Krawczyk[5]指出这些协议在 CK 模型[6]下是不安全的,并且在 MQV 协议的基础上提出了 HMQV 协议。为了增强安全模型中攻击者的能力,LaMacchina 等[7]在 CK 模型的基础上提出了 eCK 模型,允许敌手对临时私钥进行询问。目前,eCK 模型成为了 AKA 协议的主流安全证明模型。Yao 和 Zhao[8]结合了 KEA[9]和 HMQV,设计了一个“最优”的 AKA 协议。KEA 是由 NSA 设计的一个 AKA 协议,能保证最优的在线效率,但不能在 eCK 模型中被证明安全。以上这些协议都是基于公钥基础设施 (PKI, public key infrastructure)。在 PKI 中,为了抵抗公钥替换攻击,采用称为证书权威(CA, certificate authority)的可信机构来颁发数字证书,用于绑定用户身份和公钥。因此,PKI 不可避免带来了证书管理的问题,如证书颁发、存储、验证、回收等。

为了解决 PKI 中的证书管理问题,Shamir[10]提出了基于身份的密码学(IBC, identity-based cryptography)。2002 年,受 Boneh 和 Franklin 基于身份加密(identity-based encryption, IBE)[11]和 Joux 的三方 DH 协议[12]的启发,Smart 提出了一个基于身份的密钥协商(identity-based authenticated key agreement, ID-AKA)协议。该协议基于 Weil 双线性对,消除了证书管理的问题,但由于用户私钥都由一个可信的私钥生成器(PKG, private key generator)生成,带来密钥托管问题,影响会话密钥的前向安全性。这意味着如果 PKG 被妥协了,敌手将能计算出之前的会话密钥。Chen 和 Kudla[13-14]利用 PKG 只能获知长期密钥而非临时密钥实现会话密钥的前向安全性。同时,设计了一个基于身份的密钥协商确认(ID-AKAC, ID-AKA with key confirmation)协议,主要思想是在用户身份信息上加上 MAC 值。之后,一系列 ID-AKA 协议[15-17]被提出,这些协议的安全性证明都没基于 eCK 模型。最近,Daniel 等[18]提出了一个适用于 eCK 模型的无双线性对的 ID-AKA 协议,能够抵抗公钥替换攻击和已知临时会话秘密值泄露攻击(KSTIA, known session-specific temporary attack)。通过以上分析,发现这些密钥协商协议都是在经典安全模型下被证明安全的。攻击者能够通过设置一些不被发现的后门程序来扰乱这些算法的执行,从而导致用户秘密信息的泄露。

2014 年,Bellare 等[19]研究算法替换攻击(ASA, algorithm substitution attack),证明了一个攻击者能够通过替换对称加密方案来监视用户,得出了 ASA 能在任何随机或者无状态的加密方案中发生。ASA 的研究为密码学提出了一个新问题:在敌手秘密干扰下,如何保证密码方案的安全性?(这个方向也叫做后斯诺登密码学[20])。为了回答这个问题,Mironov 等[21]在 2015 年的欧密会上提出了逆向防火墙(RF, reverse firewall)的概念。RF 处在用户计算机和外界网络之间,能够修改用户收到或者发送的消息。即使用户计算机被妥协了,攻击者也无法辨认所接收的消息是否为真。RF 可以取得以下 3 个性质:1)维持功能性,即如果用户的计算机正确工作,RF 不会破坏密码算法的功能;2)保持安全性,即无论用户的计算机如何被敌手搅乱,RF 的使用将保持与正确执行密码算法一样的安全性;3)抗泄露性,即无论用户的计算机如何被搅乱

运行，逆向防火墙将将阻止计算机向外泄露秘密信息。同年，Ateniese 等[22]探讨了 RF 在数字签名上的应用，得出了任何随机化的数字签证都难抵抗 ASA。在 2016 年的美密会上，Dodis 等[23]利用 RF，在被妥协机器上实现了安全消息传输。在 2016 年的亚密会上，Chen 等[24]利用可延展平滑映射哈希函数，给出了用于安全消息传输协议、不经意的基于签名的信封和不经意传输协议的 RF 方案。2018 年，Ma 等[25]设计了一个适用于在线/离线的基于属性加密（ABE，Attribute-based encryption）的 RF 方案。方案中含有 3 个 RF，分别部署于发送者、接收者和 PKG。2019 年，Hong 等[26]设计了一个可以在 ABE 中实现属性分发的 RF 方案。Zhou 等[27]设计了一个适用于 IBE 的 RF 方案，其中一个实现了选择明文攻击安全性，另一个在适应性选择密文攻击下达到了半语义安全性。最近，Zhou 等[28]为无证书加密和无证书签名设计了 RF 方案。

目前，认证密钥协商协议中抗后门攻击的方案存在抗攻击能力弱、性能不高等缺点。通过对 RF 的研究和分析，提出了能否使用 RF 来提高两方认证密钥协商协议中信息抗泄露问题。将 RF 与两方密钥协商相结合，设计了一种无需双线性对的基于身份认证密钥协商的逆向防火墙（ID-AKA-RF，reverse firewall for ID-AKA）协议。

1　预备知识

定义 1 椭圆曲线上的离散对数问题（ECDLP，discrete logarithm problem on elliptic curve）：已知椭圆曲线上的点 P，给定（P，mP）求整数 $m\in\mathbb{Z}_q$。这个问题称为椭圆曲线上的离散对数问题。当点有大素数阶时，求解 ECDLP 被认为是计算困难的。

定义 2 逆向防火墙：假设是 W 是一个 RF，$P=$（receive，next，output）是一个组。如果以下等式满足，则 W 是一个为 P 设置的 RF。其中，σ 是初始公共参数，m 是传输的消息。

$$W^{\circ}P:=(\mathrm{receive}_{W^{\circ}P}(\sigma,m)=\mathrm{receive}_P(\sigma,W(m)),$$
$$\mathrm{next}_{W^{\circ}P}(\sigma)=W(\mathrm{next}_P(\sigma)),$$
$$\mathrm{output}_{W^{\circ}P}(\sigma)=W(\mathrm{output}_P(\sigma)).$$

一个合格的 RF 满足以下 3 个性质：1）维持功能性；2）保持安全性；3）抗泄露性。

定义 3 维持功能性：假设是 W 是一个 RF，P 是一个组，S 是一个协议，F 是一个函数。$W^k{}^{\circ}P$ 表示在 S 中有限个 $k\geqslant 1$ 里，对于 P 维持 F。当 P，S 和 F 被清空，就说 W 维持了原协议的功能。同时，$W_k{}^{\circ}P=W^{\circ}(W^{k-1}{}^{\circ}P)$ 表示 RF 能够堆砌。

定义 4 保持安全性：假设是 W 是一个 RF，P 是一个组，S 是一个协议，F 是一个函数，A 表示安全性要求。如果 $S_{P\Rightarrow W^{\circ}P^*}$ 也满足 A，就说对于 S 中的 P 能够抵抗攻击 F 的敌手，则 W 维持了原协议的安全要求性。其中 $S_{P\Rightarrow W^{\circ}P^*}$ 表示用 $W^{\circ}P^*$ 代替 P，P^* 是抵抗功能维护性的实现组。当 P、S、F 和 A 被清空，就说 W 维持了原协议的弱安全性。

定义 5 抗泄露性：假设是 W 是一个 RF，P 是一个组，S 是一个协议，F 是一个函数，A 表示安全性要求。如果不存在敌手能够攻破信息泄露 LEAK（S，P_1，P_2，W，λ）游戏，那么 W 对于 P_1 而言提供了弱抗泄露性。其中，λ 表示安全性参数，P_1 是 P_2 的一个抗攻击 F 的敌手。

2　系统模型

抗泄露认证密钥协商协议包括一个注册服务器（RS），一个注册服务器的逆向防火墙（W_{RS}），一个用户 Alice，另一个用户 Bob 和他的逆向防火墙（W_{B}），系统模型如图 1 所示。

整个方案由系统建立、随机化系统参数、密钥生成、重随机化用户密钥、身份认证与密钥协商 5 部分组成，具体算法描述如下：

1）系统建立（Setup）：该算法由注册服务器根据输入的安全参数 k，运行产生系统所需的公共参数 par 和系统主密钥 s。

2）随机化系统参数（W_{RS}.Setup）：W_{RS} 对系统参数 par 进行随机化处理，生成新的系统参数 par′。

3）密钥生成（KeyGen）：用户 Alice 和 Bob 分别将自己的身份信息 ID_A 和 ID_B 提交给注册服务器。注册服务器根据输入的身份信息 ID_A、ID_B 和系统主密钥 s，分别生成 Alice 和 Bob 的用户私钥 S_A 和 S_B。

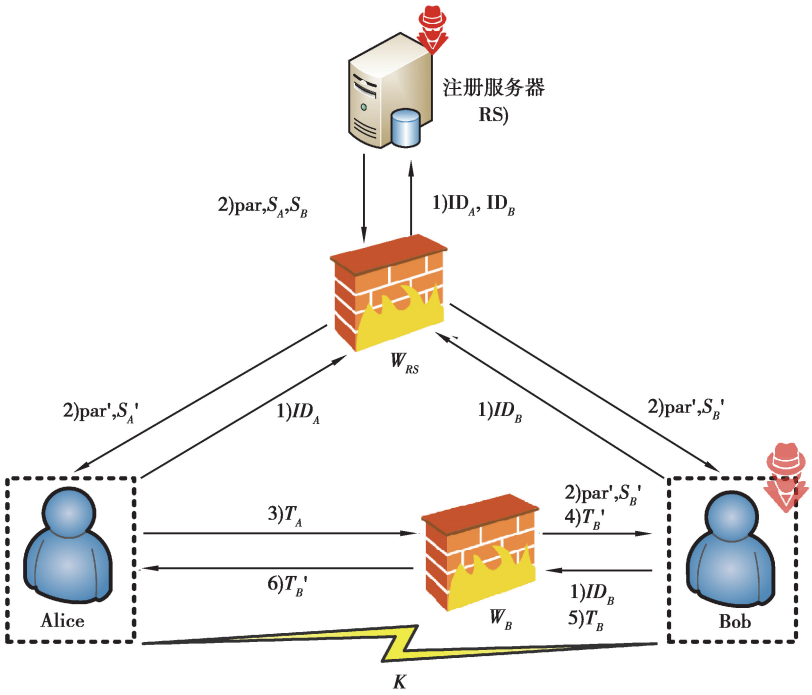

图 1 系统模型

Fig. 1 System model

4)重随机化用户密钥(W_{RS}.KeyGen):W_{RS}对S_A、S_B进行重随机化处理,生成S'_A、S'_B分别作为 Alice 和 Bob 的长期用户私钥,并通过安全信道分别回传给 Alice 和 Bob。

此处的用户私钥需要通过安全信道回传,安全信道的实现有离线和在线 2 种方法.

①离线方式:注册服务器将用户私钥和公共参数输入到智能卡中,并将智能卡安全的交到注册用户手中。

②在线方式:注册服务器通过安全的传输层安全(TLS)回传用户私钥和公共参数给注册用户。

5)身份认证与密钥协商(KeyAgreement):Alice 和 Bob 分别产生会话令牌T_A和T_B。在发送给对方的过程中,W_B对T_A、T_B进行随机化处理生成新的会话令牌T'_A、T'_B(这一过程也称为W_B.KeyAgreement)。收到新的会话令牌后,双方利用自己的私钥完成身份认证并生成会话密钥K。

3 安全模型

一个认证密钥协商协议的安全目标主要包括已知会话密钥安全性、前向安全性、PKG 前向安全性、抗密钥泄露伪装和已知会话相关临时秘密信息安全性等。eCK 模型[7]是目前安全性表达能力最强的安全模型,明确表达了密钥协商协议中最大可能损害安全的秘密泄露情况,也覆盖了最多的安全属性。基于 eCK 模型,设计了一个逆向防火墙环境下的密钥协商安全性游戏:关于挑战者C和敌手A之间的游戏,如图 2 所示。具体步骤如下:

1)系统建立阶段:挑战者C输入安全参数k,运行系统建立算法,生成系统公共参数 par 和系统主密钥s,并将公共参数 par 发送给敌手A,保存系统主密钥s。

2)询问阶段:敌手A在此阶段可以进行以下多项式有界次数的询问。

①MasterKeyReveal(k):敌手A获得系统在安全参数k下的主密钥。

②Corrupt(i):敌手A获得ID_i的经过逆向防火墙重新随机化后的长期私钥。

③Send($\Pi^k_{i,j}$,M):如果M为空,则$\prod^k_{i,j}$为由ID_i发起的会话;否则为由ID_j发起的会话。

④EphemeralKeyReveal($\prod^k_{i,j}$):敌手A获得会话$\Pi^k_{i,j}$中的临时会话密钥。

⑤Reveal($\prod_{i,j}^{k}$)：敌手 A 获得会话 $\prod_{i,j}^{k}$ 中经过逆向防火墙重新随机化后的会话密钥。

3)挑战阶段：敌手 A 决定询问阶段何时结束，然后选择一个新鲜会话 $\prod_{i,j}^{k}$ 作为其想挑战的会话发送给挑战者 C。挑战者 C 随机选择一比特数据 $b\in\{0,1\}$。如果 $b=0$，则获得 $\prod_{i,j}^{k}$ 的真实会话密钥；否则选择个随机数作为 $\prod_{i,j}^{k}$ 的会话密钥。挑战者 C 将挑战会话密钥发送给敌手 A。

4)二次询问阶段：敌手 A 可以继续如第一次询问阶段一样进行多次询问，但需保证会话 $\prod_{i,j}^{k}$ 是新鲜的。

5)猜测阶段：敌手 A 输出一比特数据 b'。如果 $b'=b$，则 A 赢得游戏。

定义 A 赢得游戏的概率为 $\mathrm{Adv}AKA_A=|\Pr[b'=b]-1/2|$，其中 $\Pr[b'=b]$ 表示 $b'=b$ 的概率。

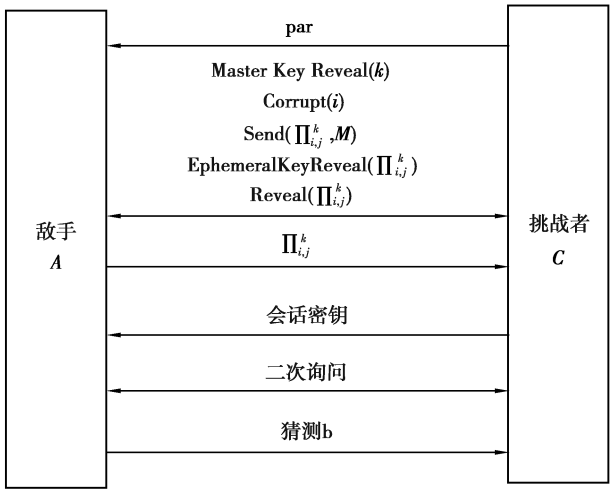

图 2　挑战者 *C* 和敌手 *A* 之间的游戏

Fig. 2　The game between challenger *C* and adversary *A*

4　协议构造

协议设计基于 Kumar 和 Saxena 的认证密钥协商协议[22]，分为系统建立、随机化系统参数、密钥生成、重随机化用户密钥、身份认证与密钥协商 5 个部分。

4.1　系统建立(Setup)

注册服务器首先根据给定的安全参数 k，选择一个 q（$q\geqslant 2^k$ 的素数）阶循环加法群 G_1，P 为 G_1 的生成元，然后注册服务器按照如下步骤进行操作：

1)随机选取系统的主密钥 $s\in\mathbb{Z}_q^*$，计算 $P_{\mathrm{pub}}=sP$。

2)选择 2 个安全的 Hash 函数：$H1:\{0,1\}^*\times G_1\rightarrow\mathbb{Z}_q^*$ 和 $H_2:\{0,1\}^*\times\{0,1\}^*\times G_1\rightarrow\mathbb{Z}_q^*$。

3)设置系统参数 $\mathrm{par}=(q,G_1,P,P_{\mathrm{pub}},H_1,H_2)$，发送 par 给自己的防火墙 W_{RS}，且保密系统主密钥 s。

4.2　随机化系统参数(W_{RS}.Setup)

注册服务器的防火墙 W_{RS} 收到 par 后，随机选择一个秘密值 $\alpha\in\mathbb{Z}_q^*$，重随机化 P_{pub} 得 $P'_{\mathrm{pub}}=\alpha P_{\mathrm{pub}}$，公开系统参数 $\mathrm{par}'=(q,G_1,P,P'_{\mathrm{pub}},H_1,H_2)$。

4.3　密钥生成(KeyGen)

用户提交自己身份信息给注册服务器，注册服务器生成相应的用户私钥。注册服务器收到 Alice 的身份信息 ID_A，Bob 的身份信息 ID_B 后，开始进行如下操作：

1)随机选择一个秘密值 $r_A\in\mathbb{Z}_q^*$，计算 $R_A=r_AP$，$Q_A=H_1(\mathrm{ID}_A\parallel R_A)$ 和 $S_A=sr_AQ_A$，将 (R_A,S_A) 发送给 W_{RS}。

2)随机选择一个秘密值 $r_B\in\mathbb{Z}_q^*$，计算 $R_B=r_BP$，$Q_B=H_1(\mathrm{ID}_B\parallel R_B)$ 和 $S_B=sr_BQ_B$，将 (R_B,S_B) 发送

给 W_{RS}。

4.4 重随机化用户密钥(W$_{RS}$.KeyGen)

注册服务器的防火墙 W_{RS} 收到(R_A,S_A)和(R_B,S_B)后,利用秘密值 α 重随机化用户私钥得 $S'_A=\alpha S_A$ 和 $S'_B=\alpha S_B$,分别发送(R_A,S'_A)和(R_B,S'_B)给 Alice 和 Bob 作为他们的长期私钥。

注册服务器的防火墙 W_{RS} 可以总结为图 3。

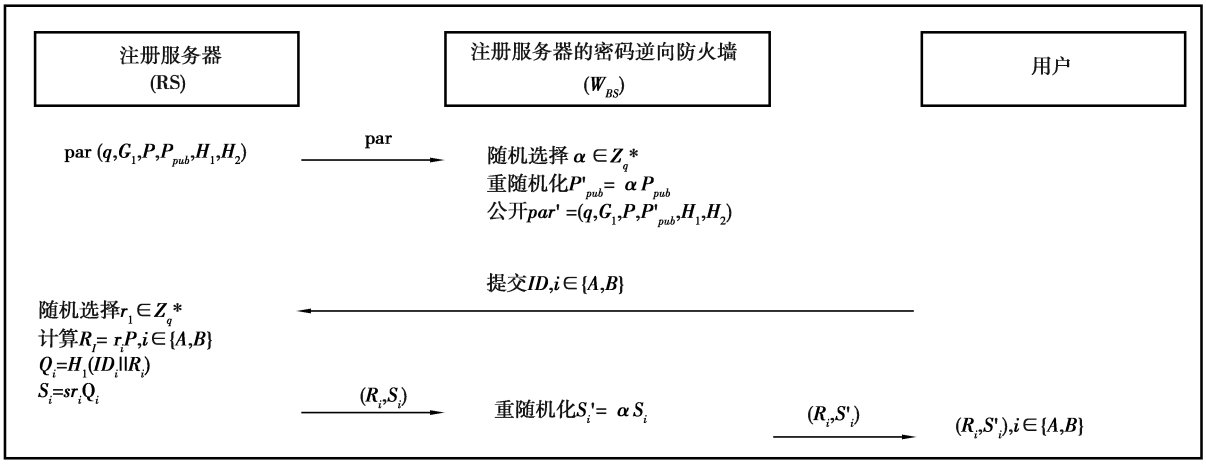

图 3 注册服务器的逆向防火墙

Fig. 3 Reverse firewall for registration server

4.5 身份认证与密钥协商(KeyAgreement)

通过双方计算生成的会话令牌完成用户身份认证,生成相同的会话密钥。图 4 描述了该部分的过程,以下将介绍具体的协议过程。

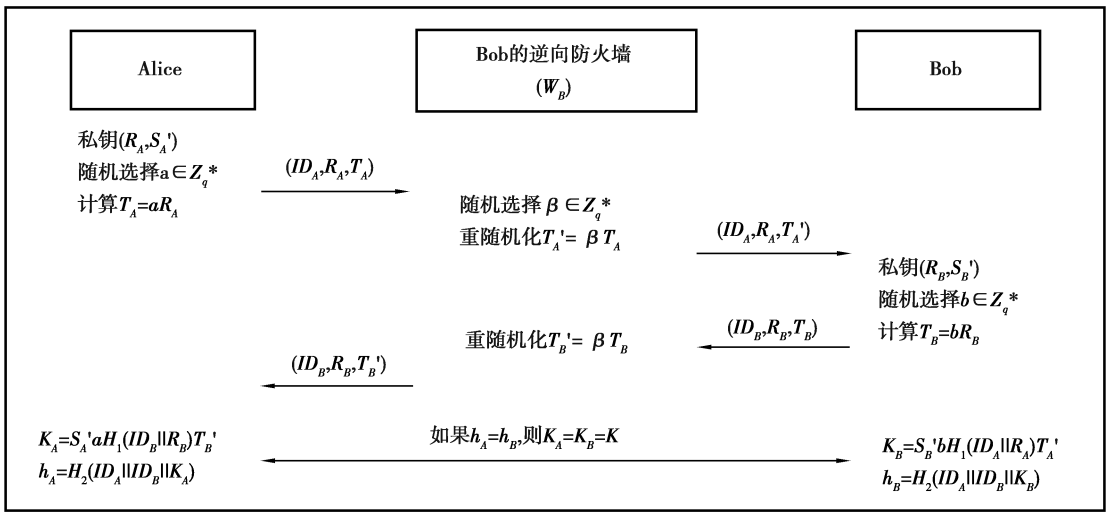

图 4 Bob 的逆向防火墙

Fig. 4 Reverse firewall for Bob

Alice 的会话令牌:

1)Alice 随机选择临时私钥 $a\in\mathbb{Z}_q^*$,计算会话令牌 $T_A=aR_A$,发送(ID_A,R_A,T_A)给 Bob 的防火墙 W_B。

2)W_B 随机选择一个秘密值 $\beta\in\mathbb{Z}_q^*$,重随机化 T_A 得 $T'_A=\beta T_A$,发送(ID_A,R_A,T'_A)给 Bob。这一过程也称为 W_B.KeyAgreement。

Bob 的会话令牌:

1)Bob 随机选择临时私钥 $b\in\mathbb{Z}_q^*$,计算会话令牌 $T_B=bR_B$,发送(ID_B,R_B,T_B)给 W_B。

2）W_B利用秘密值 β 重随机化 T_B 得 $T'_B=\beta T_B$，发送（ID_B，R_B，T'_B）给 Alice。这一过程也称为 W_B.KeyAgreement。

Alice 和 Bob 收到（ID_A，R_A，T'_A）和（ID_B，R_B，T'_B）后，利用各自的长期私钥 S'_A、S'_B 和临时私钥 a、b 计算会话密钥 K_A、K_B。

1）Alice 计算 $K_A=S'_A aH_1(\mathrm{ID}_B \| R_B)T'_B$ 和 $h_A=H_2(\mathrm{ID}_A \| \mathrm{ID}_B \| K_A)$，发送 h_A 给 Bob。

2）Bob 计算 $K_B=S'_B bH_1(\mathrm{ID}_A \| R_A)T'_A$ 和 $h_B=H_2(\mathrm{ID}_A \| \mathrm{ID}_B \| K_B)$，发送 h_B 给 Alice。

如果 $h_A=h_B$，则 $K_A=K_B=K$ 为会话密钥，用户认证与密钥协商结束。

对于 W_{RS}的功能，它保证了注册服务器被妥协后用户私钥 S_A 和 S_B 的机密性。在文献[22]协议中，当主密钥 s 泄露后，敌手能够获得用户私钥。但在协议中，随机化系统参数（W_{RS}.Setup）利用随机数 α 随机化了主密钥，阻止了敌手获取用户私钥。同样，协议重随机化了用户长期私钥（W_{RS}.KeyGen），抵抗了用户长期密钥泄露攻击。

对于 W_B的功能，它保证了 Alice 或者 Bob 被妥协后双方协商会话密钥的机密性。在文献[22]协议中，如果用户的长期私钥和临时私钥同时泄露，敌手能够计算出本次的会话密钥。但在协议中，W_B会重随机化会话令牌（W_B.KeyAgreement），使得 T_{ID}和 T'_{ID}对于敌手是不可区分的。

5　安全性证明与性能分析

5.1　安全性证明

通过定理 1 证明所提的 ID-AKA-RF 协议维持了 Kumar 和 Saxena[29] 中的 ID-AKA 协议所具有的安全特性。同时，通过注释 1，补充说明了即使被妥协注册服务器能进行 EphemeralKeyReveal（$\prod_{i,j}^{k}$）询问，所提的 ID-AK-RF 协议也能保持密钥协议的安全性。这体现了协议的强安全性。

定理 1 在随机预言模型中，如果 Kumar 和 Saxena 的 ID-AKA 协议[29] 满足认证密钥安全性，则 ID-AKA-RF 协议能够 1）维持功能性；2）保持安全性；3）提供抗泄露性。

证明：以下为 3 个功能的叙述。

1）维持功能性：对于 Alice，计算

$$\begin{aligned}K_A &= S'_A aH_1(\mathrm{ID}_B \| R_B)T'_B = \\ &\alpha S_A aH_1(\mathrm{ID}_B \| R_B)\beta T_B = \\ &\alpha sr_A Q_A aH_1(\mathrm{ID}_B \| R_B)\beta bR_B = \\ &\alpha\beta absr_A r_B Q_A Q_B P,\end{aligned}$$

对于 Bob，计算

$$\begin{aligned}K_B &= S'_B bH_1(\mathrm{ID}_A \| R_A)T'_A = \\ &\alpha S_B bH_1(\mathrm{ID}_A \| R_A)\beta T_A = \\ &\alpha sr_B Q_B bH_1(\mathrm{ID}_A \| R_A)\beta aR_A = \\ &\alpha\beta absr_A r_B Q_A Q_B P,\end{aligned}$$

因为 $K_A=K_B$，所以会话密钥

$$h_A=H_2(\mathrm{ID}_A \| \mathrm{ID}_B \| K_A)=h_B=H_2(\mathrm{ID}_A \| \mathrm{ID}_B \| K_B)。$$

2）保持安全性：通过被篡改的算法 Setup*、KeyGen*、KeyAgreement* 来证明协议和 Kumar 和 Saxena 的 ID-AKA 协议[29] 的密钥协商安全性具有不可区分性。

首先，证明 ID-AKA-RF 密钥协商安全性的游戏已经被介绍，同时文献[29]中也介绍了 ID-AKA 密钥协商安全性的标准安全游戏。接下来，考虑以下游戏：

①游戏 0：和介绍的游戏一样。

②游戏 1：和游戏 0 一样，除了系统公共参数 P_{pub}是由标准安全游戏中的 Setup 产生，而不是询问阶段和二次询问阶段中的 Setup* 和 W_{RS}. Setup 产生。

③游戏 2：和游戏 1 一样，除了用户长期私钥 S_i，$i\in\{D,C\}$是由标准安全游戏中的 KeyGen 产生，而不是

询问阶段和二次询问阶段中的 KeyGen * 和 W_{RS}. KeyGen 产生。

④游戏 3:和游戏 2 一样,除了会话令牌 T_i,$i\in\{A,B\}$是由标准安全游戏中的 KeyAgreement 产生,而不是询问阶段和二次询问阶段中的 KeyAgreement * 和 W_B. KeyAgreement 产生。此时,游戏 3 是 Kumar 和 Saxena 中的 ID-AKA 标准安全游戏[29]。

接着,证明游戏 0 和游戏 1、游戏 1 和游戏 2、游戏 2 和游戏 3 的不可区分性。

①游戏 0 和游戏 1 的不可区分性:假设存在一个被篡改的算法 Setup * 生成系统公共参数 P_{pub},系统利用算法 W_{RS}. Setup 产生了一个更新后的系统公共参数 P'_{pub}。P'_{pub}对于系统来说是一个一致的随机数,因为 P_{pub}具有密钥延展性,所以 P'_{pub}可以看作是由算法 Setup 生成的。因此,游戏 0 和游戏 1 是不可区分的。

②游戏 1 和游戏 2 的不可区分性:假设存在一个被篡改的算法 KeyGen * 生成用户长期私钥 S_i,系统利用算法 W_{RS}.KeyGen 产生了一个更新后的用户长期私钥 S'_i。S'_i 对于用户来说是一个一致的随机数,因为 S_i 具有密钥延展性,所以 S'_i 可以看作是由算法 KeyGen 生成的。因此,游戏 1 和游戏 2 是不可区分的。

③游戏 2 和游戏 3 的不可区分性:假设存在一个被篡改的算法 KeyAgreement * 生成会话令牌 T_i,系统利用算法 W_B.KeyAgreement 产生了一个更新后的会话令牌 T_i'。T_i'对于算法 KeyAgreement 来说是一个一致的随机数,因为原 ID-AKA 协议是可重随机化的,所以 T_i'可以看作由是算法 KeyAgreement 而不是 KeyAgreement * 生成的。因此,游戏 2 和游戏 3 是不可区分的。

因为 Kumar 和 Saxena 的 ID-AKA 协议[29]具有密钥协商安全性,所以 ID-AKA-RF 协议也具有密钥协商安全性。

3)提供抗泄露性:游戏 0 和游戏 3 之间的不可区分性意味着对于注册服务器和 Bob 逆向防火墙能够提供消息抗泄露性。

注释 1 在 Kumar 和 Saxena 中的 ID-AKA 协议的安全模型[29]中,被妥协的 PKG 不能对会话的临时私钥进行询问。例如,当一次会话进行,敌手获得了一次会话的临时私钥 a 和 b。如果被妥协的 PKG 泄露了用户长期私钥的秘密值 r_A 和 r_B,敌手可以通过以下等式计算出会话密钥

$$\begin{aligned}K=&S_AaH_1(\text{ID}_B\parallel R_B)T_B=\\&S_AaQ_BbR_B=\\&r_Ar_BsabQ_AQ_BP=\\&r_Ar_BabQ_AQ_BP_{\text{pub}}。\end{aligned}$$

但是在 ID-AKA-RF 协议中,即使 r_A、r_B 和 a、b 都被敌手获知,因为 Bob 的逆向防火墙对会话令牌进行了重随机化处理 $T'_i=\beta T_i$。同时因为 ECDLP,即使 $T_i=kR_i$,$k\in\{a,b\}$和 T'_i 可以被敌手获知,敌手也无法计算出 β。因为如下等式,无法计算出会话密钥

$$\begin{aligned}K=&S'_AaH_1(ID_B\parallel R_B)T'_B=\\&S'_AaQ_B\beta bR_B=\\&\alpha S_AabQ_B\beta r_BP=\\&\alpha br_Ar_BQ_AQ_B\alpha sP=\\&\alpha br_Ar_BQ_AQ_B\beta P'_{\text{pub}}。\end{aligned}$$

所以协议通过密码防火墙提高了原协议的信息抗泄露性。

5.2 性能分析

为了分析 ID-AKA-RF 协议的性能,将该协议与 4 个无需双线性对的 ID-AKA 协议进行比较,包括 Cao 等[16]、Tseng 等[30]、Islam 等[31]、Kumar 等[29]。为了方便后面的统计,首先用符号定义协议中所用到的运算,如表 1 所示。

表 2 给出了这几个协议的计算成本和通信成本。因为每个用户只需要注册一次,而每次会话都需要进行认证密钥协商,所以这里只考虑认证密钥协商阶段的计算成本和通信成本。通过表 2 可以看出,只有 Kumar 等[29]与 ID-AK-RF 协议在 eCK 模型进行了安全性证明,并且实现了抗临时会话秘密值攻击。相比于 Kumar 等[29]的 ID-AKA 协议,ID-AKA-RF 协议允许敌手进行更强的 KSTIA 攻击,表现在于敌手在获得一次会话的临时秘密值的同时,还能够获得用户长期私钥的秘密值。

表 1　符号定义

Table 1　Symbol definition

符号	定义
PM	循环加法群中 2 个点之间的加法运算
PA	循环加法群中元素的标量乘运算
PE	循环乘法群中元素的幂运算
TH	哈希运算
TX	任意 2 个元素之间的异或运算
$\|G_1\|$	群 G_1 中元素的比特数
$\|G_2\|$	群 G_2 中元素的比特数
$\|Z_q\|$	群 Z_q 元素的比特数
|ID|	字符串 ID 的比特数

表 2　与以往 ID-AKA 协议比较

Table 2　Comparison with the previous ID-AKA protocols

协议	计算成本	通信成本	轮数	eCK 模型	抗 KSTIA
Cao 等	4PA+8PM+4TH	$\|ID\|+2\|G_1\|$	2	否	否
Tseng 等	6PA+8PM+8TH+2TX	$\|ID\|+\|Z_q\|+2\|G_1\|$	3	否	否
Islam 等	18PA+16PM+8TH	$\|ID\|+\|Z_q\|+3\|G_1\|$	3	否	是
Kumar 等	8PM+4TH	$\|ID\|+2\|G_1\|$	2	是	是
研究算法	10PM+4TH	$\|ID\|+2\|G_1\|$	3	是	强

在通信成本方面,设置了 3 个不同的安全等级:80、120 和 128[32]。这 3 个安全等级分别对应于 2TDEA (2-key triple-DES)[33],3TDEA (3-key triple-DES)[33]和 AES-128。选择了基于有限域 $E(F_p)$ 上的椭圆曲线 $y^2=x^3+x \bmod p$。G_1 和 G_2 分别是循环加法群和循环乘法群,它们的阶都为 q。表 3 列举了在不同安全等级下 p 和 q 的值。根据表 3,在 80 安全等级下,$|Z_q|=160$ bits,$|G_1|=|G_2|=1\ 024$ bits。同样可以计算出其他两个安全等级下群 G_1 和 G_2 中的元素值。

表 3　不同安全等级下的 p 和 q (bits)

Table 3　p and q under different security levels (bits)

安全等级	$\|p\|$	$\|q\|$
80	1 024	160
120	2 048	224
128	3 072	256

图 5 展示了不同安全等级下的 ID-AKA 协议通信成本,其中取用户的身份信息 ID 为 512 比特。通过比较后发现,ID-AKA-RF 协议在身份认证与密钥协商阶段所需要的通信带宽窄。随着安全等级的提高,ID-AKA-RF 协议带宽优势更加明显,特别是与 Islam 等[31]相比。

在计算成本方面,使用开源库 JPBC 库编程实现这 5 个协议,采用了上述的椭圆曲线 $y^2=x^3+x \bmod p$,

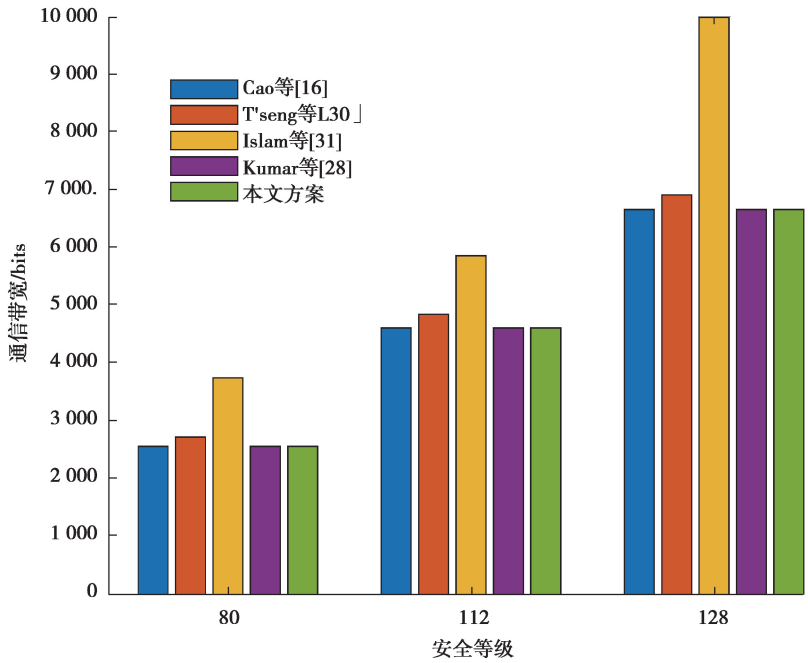

图5 不同安全等级下通信成本的比较

Fig. 5 Comparison of communication costs under different security levels

设计嵌入度数为2。所以相比于表3中的 p 值，实验中的参数应该为 $\left|\frac{p}{2}\right|$。实验环境为 Intel(R) Core (TM) i5-5200U CPU@2.20GHz 处理器，8GB 的 RAM 和 64 位的操作系统上配备的 Eclipse, Neon.1a Release。在不同的安全等级下，对每个算法执行 100 次以取平均值。图 6 比较了不同安全等级下会话密钥协商和整个过程需要的时间。通过图 6，可以得知 ID-AKA-RF 协议在会话密钥认证与协商阶段所花的时间较小，仅大于 Kumar 等[29]等的 ID-AKA 协议。表 4 列出了不同安全等级下，这些协议运行所花的总时间。在安全等级为 80bits 时，相比于 Cao 等[16]、Tseng 等[30]、Islam 等[31]的 ID-AKA 协议，ID-AKA-RF 协议在时间方面减少了：(654－557)/654＝14.8%，(751－557)/751＝25.8%和(823－557)/823＝32.3%。由图 6 和表 4 可知，ID-AKA-RF 协议在计算成本上具有一定优势，且随着安全等级的提高，优势明显加大。所以协议适合在资源受限的系统中应用。

表4 不同安全等级下的运行时间

Table 4 The running time under different security levels /ms

安全等级	Cao 等[31]	Tseng 等[31]	Islam 等[30]	Kumar 等[29]	研究算法
80	654	751	823	454	557
120	1 994	2 211	2 381	1 701	1 895
128	5 879	6 000	6 330	5 425	5 735

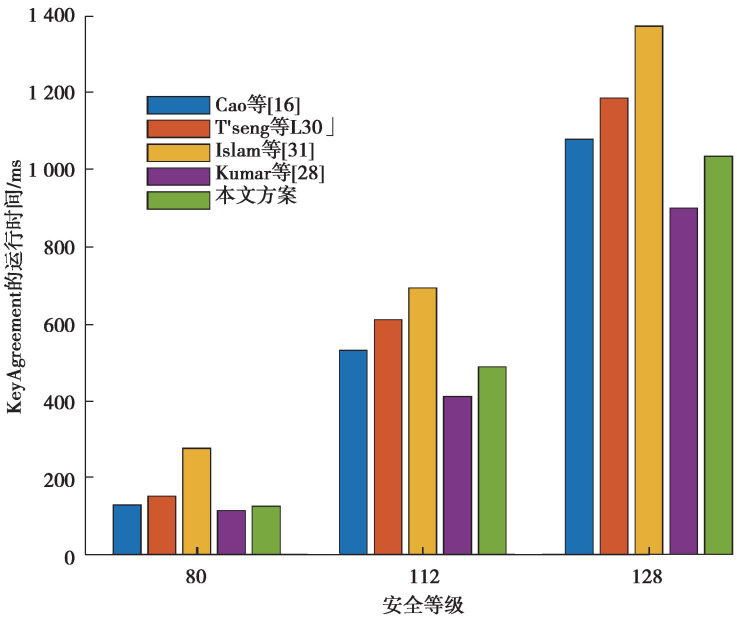

图 6　不同安全等级下会话密钥协商运行时间的比较

Fig. 6　Comparison of session key agreement running time under different security levels

5.3　协议应用

研究提出的协议可以应用到需要建立会话密钥的场景。例如，在移动客户端——服务器环境中，用户（客户端）使用低功耗移动设备访问强大的服务器以便得到某种服务，如移动电子邮件、移动 Web 访问等。为了防止未经授权的用户访问服务器的服务，需要对用户进行身份验证。此外，客户端和服务器之间传输的消息可能是敏感的，需要在它们之间建立会话密钥。最后，为了防止后门程序扰乱认证密钥协商协议的执行，需要加装逆向防火墙功能。

6　结　论

在不使用双线性对运算的情况下构造了一种适用于基于身份认证密钥协商的逆向防火墙协议。同时在随机预言机模型中，证明了该协议能够抗泄露攻击，特别是能够抵抗强的临时秘密值泄露攻击。最后利用 JPBC 库，实现了该协议并进行了性能分析。在通信成本方面，该协议具有较低的带宽；在计算成本方面，虽然该协议相比于 Cao 等[16]和 Kumar 等[29]的 ID-AKA 协议有一定的增加，但处于合理范围内。综合安全性方面的考虑，协议与其他同类型 ID-AKA 协议相比具有很大的性能优势，十分适合应用于资源受限的设备中。

参考文献：

[1] Diffie W, Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[2] Matsumoto T, Takashima Y, Imai H. On seeking smart public-key-distribution systems[J]. Ieice Transactions (1976-1990), 1986, 69(2): 99-106.

[3] Kunz-Jacques S, Pointcheval D. About the Security of MTI/C0 and MQV[C]// International Conference on Security and Cryptography for Networks. Berlin, Heidelberg: Springer, 2006: 156-172.

[4] Law L, Menezes A, Qu M H, et al. An efficient protocol for authenticated key agreement[J]. Designs, Codes and Cryptography, 2003, 28(2): 119-134.

[5] Krawczyk H. HMQV: A high-performance secure diffie-Hellman protocol[C]// Advances in Cryptology-CRYPTO 2005,

2005：546-566.

[6] Canetti R，Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels[C]// Advances in Cryptology-EUROCRYPT May 6-10，2001. Innsbruck，Austria. Berlin：Springer，2001：453-474.

[7] LaMacchia B，Lauter K，Mityagin A. Stronger security of authenticated key exchange[C]// International Conference on Provable Security-ProvSec 2007. Berlin：Springer，2007：1-16.

[8] Yao C，Zhao Y. OAKE. A new family of implicitly authenticated Diffiee-Hellman protocols[C]// Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications-CCS. November 4-8，2013. New York：Association for Computing Machinery，2013：1113-1128.

[9] Lauter K，Mityagin A. Security analysis of KEA authenticated key exchange protocol[C]// Public Key Cryptography-PKC 2006. New York：Springer-Verlag，2006：378-394.

[10] Shamir A. Identity-based cryptosystems and signature schemes[C]// Workshop on the theory and application of cryptographic techniques. Berlin，Heidelberg:Springer，1984：47-53.

[11] Boneh D，Franklin M. Identity-based encryption from the weil pairing[C]// Advances in Cryptology-CRYPTO 2001. Tokyo：Springer，2001：213-229.

[12] Joux A. A one round protocol for tripartite diffie-Hellman[J]. Journal of Cryptology，2004，17(4)：263-276.

[13] Smart N P. Identity-based authenticated key agreement protocol based on Weil pairing[J]. Electronics Letters，2002，38(13)：630.

[14] Chen L，Kudla C. Identity based authenticated key agreement protocols from pairings[C]// 16th IEEE Computer Security Foundations Workshop，2003. Proceedings. June 30-July 2，2003，Pacific Grove，CA，USA：IEEE，2003：219-233.

[15] Huang H，Cao Z. An id-based authenticated key exchange protocol based on bilinear Diffiee-Hellman problem[C]// Proceedings of the 4th International Symposium on Information，Computer，and Communications Security-ASIACCS'09. Sydney，Australia. :ACM，2009：333-342.

[16] Cao X F，Kou W D，Du X N. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges[J]. Information Sciences，2010，180(15)：2895-2903.

[17] Islam S H，Biswas G P. An improved pairing-free identity-based authenticated key agreement protocol based on ECC[J]. Procedia Engineering，2012，30：499-507.

[18] Daniel R M，Rajsingh E B，Silas S. An efficient ECK secure identity based two party authenticated key agreement scheme with security against active adversaries[J]. Information and Computation，2020，275：104630.

[19] Bellare M，Paterson K G，Rogaway P. Security of symmetric encryption against mass surveillance[C]// Advances in Cryptology-CRYPTO'04. 2004. Berlin：Springer，2014：1-19.

[20] Tang Q，Yung M. Cliptography：Post-Snowden cryptography[C]// Proceedings of ACM SIGSAC Conference on Computer and Communications Security-CCS'17. October 30-November 3，2017. Dallas，TX，USA：ACM，2017：2615-2616.

[21] Mironov I，Stephens-Davidowitz N. Cryptographic reverse firewalls[M]// Advances in Cryptology-EUROCRYPT 2015. Berlin，Heidelberg：Springer，2015：657-686.

[22] Ateniese G，Magri B，Venturi D. Subversion-resilient signature schemes[C]// Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security-CCS'15. October 12-16，2015. USA：ACM，2015：364-375.

[23] Dodis Y，Mironov I，Stephens-Davidowitz N. Message transmission with reverse firewall-secure communication on corrupted machines[C]// Advances in Cryptology-CRYPTO 2016. Berlin：Springer，2016：341-372.

[24] Chen R，Mu Y，Yang G，et al. Cryptographic reverse firewall via malleable smooth projective hash functions[C]// Advances in Cryptology-ASIACRYPT 2016. Berlin：Springer，2016：844-876.

[25] Ma H，Zhang R，Yang G，et al. Concessive online/offline attribute based encryption with cryptographic reverse firewalls secure an efficient fine-grained access control on corrupted machines[C]// European Symposium on Research in Computer Security-ESORICS 2018. Berlin：Springer，2018：507-526.

(下转第42页)

Systems，2007，31(18)：6-10.(in Chinese)

[13] 马秀娟，马福祥，赵海兴. 基于耦合映像格子的有向网络相继故障[J]. 计算机应用，2011，31(7)：1952-1955.
Ma X J，Ma F X，Zhao H X. Cascading failure in coupled map lattices with directed network[J]. Journal of Computer Applications，2011，31(7)：1952-1955.(in Chinese)

[14] 曲朝阳，杨琴，杨杰明，等. 基于贝叶斯网络的智能变电站风险关联模型[J]. 电力系统自动化，2016，40(2)：95-99.
Qu Z Y，Yang Q，Yang J M，et al. Risk associated model of smart substations based on Bayesian network[J]. Automation of Electric Power Systems，2016，40(2)：95-99.(in Chinese)

[15] 王力军，周凯，吴迪，等. 基于风险传递网络的智能变电站二次系统风险评估[J]. 电力系统保护与控制，2018，46(6)：97-105.
Wang L J，Zhou K，Wu D，et al. Risk assessment for smart substation secondary system using risk transfer network model[J]. Power System Protection and Control，2018，46(6)：97-105.(in Chinese)

[16] Holovaty A，Kaplan-Moss J. The definitive guide to django[M]. Berkeley，CA：Apress，2008.

[17] Bennett J. Practical django projects[M]. Berkeley，CA：Apress，2009.

（编辑 侯 湘）

(上接第 32 页)

[26] Hong B，Chen J，Zhang K，et al. Multi-authority non-monotonic KP-ABE with cryptographic reverse firewall[J]. IEEE Access，2019，7：159002-159012.

[27] Zhou Y，Guan Y，Zhang Z，et al. Cryptographic reverse firewalls for identity-based encryption[C]// Frontiers in Cyber Security，FCS 2019. Singapore：Springer 2019：36-52.

[28] Zhou Y Y，Guo J，Li F G. Certificateless public key encryption with cryptographic reverse firewalls[J]. Journal of Systems Architecture，2020，109：101754.

[29] Kumar M，Saxena P. PF-AID-2KAP：Pairing-free authenticated identity-based two-party key agreement protocol for resource-constrained devices [C] // Futuristic Trends in Network and Communication Technologies. Singapore：Springer. 2018：425-440.

[30] Tseng Y M，Huang S S，You M L. Strongly secure ID-based authenticated key agreement protocol for mobile multi-server environments[J]. International Journal of Communication Systems，2017，30(11)：e3251.

[31] Islam S H，Biswas G P. A pairing-free identity-based two-party authenticated key agreement protocol for secure and efficient communication[J]. Journal of King Saud University-Computer and Information Sciences，2017，29(1)：63-73.

[32] Barker E B，Barker W C，Burr W E，et al. Recommendation for key management，part 1：[R]. National Institute of Standards and Technology，2005.

[33] Barker E，Mouha N. Recommendation for the triple data encryption Algorithm（TDEA）block cipher[R]. National Institute of Standards and Technology，2017.

（编辑 侯 湘）