Software Engineering and Applications 软件工程与应用, 2023, 12(3), 543-552
Published Online June 2023 in Hans. https://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2023.123053

Hans汉斯

基于SM9和FALCON的密钥交换协议设计

郑惠敏，李子臣，王东飞

北京印刷学院数字版权保护技术研究中心，北京

收稿日期：2023年4月28日；录用日期：2023年6月22日；发布日期：2023年6月30日

摘　要

SM9是我国首个全体系纳入ISO/IEC标准的标识密码算法，FALCON是NIST后量子竞赛优胜算法。本文基于SM9和FALCON设计了一个新的密钥交换协议。协议通过校验FALCON签名的有效性来鉴别信息发送方的身份，基于SM9公钥加密算法保障共享的256比特秘密数据串的机密性，通过密钥派生函数，利用双方生成的随机数据串和双方的标识信息生成一个定长的共享会话密钥。结合BAN逻辑证明和非形式化分析方法，对协议的安全性进行了证明。本文协议具有抵抗重放攻击、中间人攻击和拒绝服务攻击的能力。基于FALCON数字签名算法实现参与双方身份的真实性和不可否认性，具有抗量子攻击的特性。

关键词

SM9，FALCON，密钥交换协议，BAN逻辑

Design of Key Exchange Protocol Based on SM9 and FALCON

Huimin Zheng, Zichen Li, Dongfei Wang

Digital Rights Management Research Center, Beijing Institute of Graphic Communication, Beijing

Received: Apr. 28th, 2023; accepted: Jun. 22nd, 2023; published: Jun. 30th, 2023

Abstract

SM9 is the first identity cryptographic algorithm in China whose whole system is included in the ISO/IEC standard, and FALCON is the winner of the NIST post-quantum competition. The protocol identifies the message sender by verifying the validity of the FALCON signature, guarantees the confidentiality of the shared 256-bit secret data string based on the SM9 public key encryption algorithm, and generates a fixed-length shared session key using the random data string generated by both parties and the identification information of both parties through a key derivation function. The security of the protocol is proved by combining BAN logic and non-formal analysis me-

文章引用: 郑惠敏, 李子臣, 王东飞. 基于SM9和FALCON的密钥交换协议设计[J]. 软件工程与应用, 2023, 12(3): 543-552.
DOI: 10.12677/sea.2023.123053

thods. This protocol has the ability to resist replay attacks, man in the middle attacks, and denial of service attacks. The protocol designed in this paper achieves the authenticity and non-repudiation of the identities of the participating parties and is resistant to quantum attacks through the application of the FALCON digital signature algorithm.

Keywords

SM9, FALCON, Key Exchange Protocol, BAN Logic

1. 引言

现代密码学的密码体制主要分为对称密码体制和非对称密码体制。非对称密码体制又称为公钥密码体制，可以解决对称密码体制中密钥分发和管理的问题，常用于会话密钥协商。对称密码体制也称为单钥密码体制，利用协商的会话密钥执行加密和解密的速度非常快，在如今互联网传输中主要用于保障传输数据的机密性。根据柯克霍夫原则，密码算法不需要保密，仅密钥需要保密。因此，系统的保密性主要取决于密钥的保密性，设计出在不安全的信道安全地协商出共享密钥的密钥交换协议具有重要意义。

按照构建密钥交换协议所使用的密码技术的不同，密钥交换协议可分为需要使用数字证书的基于公钥密码体制和基于标识密码技术(Identity-Based Cryptograph，简称 IBC)两种。由于 IBC 不需要使用数字证书，密钥管理环节可以得到简化。1984 年，文献[1]首次提出标识密码的概念，最主要的观点是系统中不需要证书。IBC 使用用户独有的标识如姓名、电子邮箱地址、手机号等作为生成用户公钥的关键信息，用户私钥由可信任的密钥生成中心(Key Generation Center，简称 KGC)计算得出。2001 年，文献[2]提出了用椭圆曲线配对构造标识公钥加密算法，该方案在随机谕言机模型下是可证明安全的并且效率较高。基于文献[2]的 BF-IBC 模式，我国自主制定了国产商用密码算法标准 SM9 [3]，该算法是我国首个全体系纳入 ISO/IEC 标准的非对称密码算法。

本文通过结合国家密码局认定的国产密码算法 SM9 标识加密算法、SM3 杂凑算法[4]、国密系列算法中通用的密钥派生函数(Key Derivation Function，简称 KDF) [3]、以及美国国家标准与技术研究院(National Institute of Standards and Technology，简称 NIST)后量子密码竞赛优胜算法 FALCON [5]设计了一个密钥交换协议，该协议具有机密性与认证性，可以在非保护信道中建立对称密码的秘密密钥。并且，通过形式化的 BAN 逻辑[6] [7] [8]和非形式化方法证明、分析了所设计协议的安全性。效率方面，本文设计协议应用到的 SM9 和 FALCON 算法都以高效率和适合资源受限场景为主要特点。经文献[5]分析，FALCON 算法的功耗非常低。而且，SM9 标识密码算法不需要证书的申请与校验，可以减少公钥证书基础设施部署和存储的开销。

随着量子计算机的发展，传统的基于大数分解难题和离散对数难题的密码算法将不再安全[9]，对称密码算法的比特安全性也将降低为原来的一半[10]。根据文献[11]，密钥大小为 128 比特的密钥系统对暴力攻击具有鲁棒性。为了达到 2^{128} 的量子计算安全，对称密码的有效密钥尺寸应该至少设计为 256 比特。SM9 算法中加密明文方法分为基于密钥派生函数的序列密码算法和分组密码算法，序列密码算法采用的密钥长度与明文等长，通过密钥与明文逐比特加密生成密文，安全性很强；而分组密码算法一般使用国家密码管理主管部门批准的 SM4 分组密码算法[12]，该算法是对称密码算法，暂未推出从 128 比特密钥

升级到256比特或者更高比特的密钥，安全性较低。

在本文协议中，SM9算法的主公钥通过人工管理，除了密钥生成中心外只有参与方持有。不公开主公钥的操作保障了主密钥对的安全性。并且，SM9算法中加密明文的方法仅采用基于密钥派生函数的序列密码算法，先生成不全为0的256比特有效密钥，再通过密钥与明文逐比特异或的方法保障协商信息的机密性。为了进一步提高安全性，本文设计的密钥交换协议在使用SM9算法生成加密私钥时，将用户标识设置为用户名拼接当前时间戳值，使得同一对密钥协商双方在不同次密钥协商过程中的SM9加密私钥与自身的标识都会发生变化，进而增强了协议的前向安全性。结合文献[6]和[13]对每条交互信息添加时间戳的方法，本文协议可以抵抗重放攻击、中间人攻击和拒绝服务攻击。本文协议使用FALCON数字签名算法实现参与双方身份的可认证性，FALCON是NTRU (Number Theory Research Unit)格上基于文献[14]描述的GPV框架构建的签名方案，它使用快速傅里叶采样算法作为陷门采样器，是Hash-then-Sign签名方案中最高效的代表，并且具有抗量子的特性。

2. 预备知识

2.1. 密码杂凑函数

1) SM3密码杂凑算法[4]

SM3密码杂凑算法基于MD结构[15] [16]，杂凑函数hash可将一个任意有限比特长度的信息m压缩到某一固定长度为n比特的杂凑值h，即$\mathrm{hash}(m)=h$。

2) 密码函数$\mathrm{H}_1(\cdot)$ [3]

密码函数$\mathrm{H}_1(Z,n)$的输入为比特串Z和整数n，输出为一个整数$h_1\in[1,n-1]$。本协议使用的$\mathrm{H}_1(Z,n)$需要调用密码杂凑函数SM3。

3) 密钥派生函数KDF(·) [3]

密钥派生函数$\mathrm{KDF}(Z,n)$的作用是从一个共享的秘密比特串Z中派生出一固定长度为n比特的密钥数据，本协议使用的密钥派生函数需要调用杂凑函数SM3。

2.2. SM9标识加密算法[3]

在基于标识的加密算法SM9中，解密用户持有一个标识和一个相应的加密私钥，该加密私钥由可信第三方——密钥生成中心KGC通过加密主私钥和解密用户的标识结合产生。KGC通常为可信第三方机构或可信硬件。加密用户用解密用户的标识加密数据，解密用户用自身加密私钥解密数据。

该公钥加密算法涉及5类辅助函数：SM3、KDF、消息认证码函数(Message Authentication Code，简称MAC)、随机数发生器、序列密码算法或者分组密码算法。其中，MAC函数使用KDF生成的密钥对密文比特串求取消息认证码，选用的随机数发生器应该符合文献[17]的要求。

2.3. FALCON数字签名算法[5]

FALCON在NTRU格上构建，是目前Hash-then-Sign签名方案中最高效的代表，安全性由NTRU格上的SIS困难问题保证。FALCON工作在环$R_q=Z_q[x]/(x^n+1)$上，其中$q=12289$，$n=512$或$n=1024$。

3. 基于SM9和FALCON的密钥交换协议

本文设计了一个基于SM9标识公钥加密算法和FALCON数字签名算法的密钥交换协议，利用协商双方的标识信息和生成的随机数据串派生出一个共享的会话密钥。

3.1. 参数选取

SM3：消息分组长度为512比特，输出摘要长度为256比特。

SM9：椭圆曲线基域 F_q (素数 $q>3$)，曲线的识别符 cid 用一个字节表示，0 × 10 表示 F_q 上常曲线，0 × 11 表示 F_q 上超奇异曲线，0 × 12 表示 F_q 上常曲线及其扭曲线(扭曲线参数为 β)；F_q 中的两个元素 a 和 b，它们定义椭圆曲线的方程 E：$y^2=x^3+ax+b$；曲线阶的素因子 N 和相对于 N 的余因子 cf；曲线 $E\left(F_q\right)$ 相对于 N 的嵌入次数 k，N 阶循环群 $G_T\subset\left(F_{q^k}\right)^*$，规定 $q^k>2^{1536}$；N 阶循环群 $\left(G_1,+\right)$ 的生成元 $P_1=\left(x_1,y_1\right)\neq O$；$N$ 阶循环群 $\left(G_2,+\right)$ 的生成元 $P_2=\left(x_2,y_2\right)\neq O$；双线性对 e：$G_1\times G_2\to G_T$，用一个字节的识别符 eid 表示：0 × 01 表示 Tate 对，0 × 02 表示 Weil 对，0 × 03 表示 Ate 对，0 × 04 表示 R-ate 对；为了进一步增强安全性，用户标识 ID 设置为用户名拼接生成加密私钥时的时间戳值。

FALCON：根据文献[18]，在保障安全性的前提下，SM3 的综合性能指标与 SHA-256 同等条件下相当。由于 FALCON-512 满足 NIST 第二级的安全强度即与 SHA-256 相当，所以本协议令 FALCON 算法采用的环的度 n 为 512，模量 q 为 12289，标准偏差为 165.736617183，允许的最高的签名平方的范数为 34034726，公钥长度为 897 字节，生成的签名长度为 666 字节。

3.2. 协议流程

设用户 A 为发起方，用户 B 为响应方。用户 A 和 B 协商获得共享的 256 比特秘密比特串，之后通过 KDF 派生出 *klen* 长度的共享密钥。

设计的基于 SM9 和 FALCON 的密钥交换协议执行过程中交互的每个信息在传输之前，都先对整个信息增加时间戳信息，然后做 SM3 杂凑变换，最后再对消息进行传输。接收方接收到信息后，也先做 SM3 杂凑变换，将计算出的杂凑值与接收到的杂凑值做比较，如果两者相同，则可以认为消息在传输过程中没有被篡改，否则消息就是非法的。然后接收方分析时间戳，进一步判断接收到的消息的有效性。假设发送方要传输信息给接收方时的时间戳为 T，该网络中信息传输的时间为 Δt，可能存在的时间偏差为 Δs，则接收方接收信息后，分析时间戳，判断接收时间是否在时间窗口 $\left[T+\Delta t-\Delta s,T+\Delta t+\Delta s\right]$ 区间内，如果在，则继续执行密钥交换协议；如果不在，则判定该信息为非法信息，丢弃不予处理。其中，Δt 和 Δs 的取值可经过多次实验确定。

在本文设计的协议中，SM9 算法中加密明文的方法仅采用基于密钥派生函数的序列密码算法，通过一次一密的方法保障协商信息的机密性。由于每次交互的信息都带有 SM3 杂凑值保障信息的完整性，且通过 FALCON 签名保障交互双方的身份真实性，此时 SM9 公钥加密算法中 MAC 码存在就显得冗余了，故本协议不做 MAC 码的计算与校验。

用户 A 和 B 执行密钥交换协议之前先从 KGC 处安全地获取到根据加密主私钥和自己的标识 ID 结合产生的加密私钥，分别记为 de_A 和 de_B。用户 A 和 B 共用 KGC 的加密主公钥 P_{pub}。

若用户 A 和 B 都拥有系统参数，为了获得相同的会话密钥，双方应实现如下运算步骤：

用户 A：

步骤 A1：从 KGC 获取加密主公钥 P_{pub} 和根据用户 A 的标识 ID_A 生成的加密私钥 de_A、加密私钥生成函数识别符 hid。

步骤 A2：通过 FALCON 数字签名算法的密钥产生算法计算出签名公钥 pk_{AS} 与签名私钥 sk_{AS}。

步骤 A3：用随机数发生器产生 256 比特随机数据串 r_A。

步骤 A4：通过 FALCON 数字签名算法，使用签名私钥 sk_{AS} 对 r_A 进行签名，得到签名 r_S。

步骤 A5：生成时间戳 T_A。

步骤 A6：使用 SM3 密码杂凑算法计算出要传输消息的杂凑值 $H_A=\mathrm{hash}\left(ID_A\|pk_{AS}\|r_A\|r_S\|T_A\right)$。

步骤 A7：将 $M_1=\left(ID_A,pk_{AS},r_A,r_S,T_A,H_A\right)$ 发送给用户 B。

用户 B：

步骤 B1：使用 SM3 密码杂凑算法计算出接收到的消息的杂凑值 $\mathrm{H}'_{\mathrm{A}}=\mathrm{hash}\left(\mathrm{ID}_{\mathrm{A}}\|pk_{\mathrm{AS}}\|r_{\mathrm{A}}\|r_{\mathrm{S}}\|T_{\mathrm{A}}\right)$，验证 $\mathrm{H}'_{\mathrm{A}}=\mathrm{H}_{\mathrm{A}}$ 是否成立，如果不成立将中断密钥交换过程；如果成立，继续执行后续步骤。

步骤 B2：分析时间戳 T_{A}，判断接收时间是否在时间窗口 $\left[T_{\mathrm{A}}+\Delta t-\Delta s,T_{\mathrm{A}}+\Delta t+\Delta s\right]$ 区间内，如果不在，将中断密钥交换过程；如果在时间窗口区间内，继续执行后续步骤。

步骤 B3：通过 FALCON 数字签名验证算法，使用用户 A 的签名公钥 pk_{AS} 验证 r_{A} 的签名 r_{S}，如果签名验证失败，将中断密钥交换过程；如果签名验证成功，继续执行后续步骤。

步骤 B4：从 KGC 获取加密主公钥 P_{pub}。

步骤 B5：通过 FALCON 数字签名算法的密钥产生算法计算出签名公钥 pk_{BS} 与签名私钥 sk_{BS}。

步骤 B6：用随机数发生器产生 256 比特随机数据串 r_{B}。

步骤 B7：通过 SM9 加密算法，使用加密主公钥 P_{pub} 和用户 A 的标识 ID_{A} 加密 r_{B}，得到密文 c_{B}，具体为：

计算群 G_1 中的元素 $Q_{\mathrm{A}}=\left[H_1\left(\mathrm{ID}_{\mathrm{A}}\|\mathrm{hid},N\right)\right]P_1+P_{\mathrm{pub}}$

产生随机数 $r\in[1,N-1]$

计算群 G_1 中的元素 $C_1=[r]Q_{\mathrm{A}}$，将 C_1 的数据类型转换为比特串

计算群 G_T 中的元素 $g=e\left(P_{\mathrm{pub}},P_2\right)$

计算群 G_T 中的元素 $w=g^r$，将 w 的数据类型转换为比特串

计算 $K=\mathrm{KDF}\left(C_1\|w\|\mathrm{ID}_{\mathrm{A}},256\right)$，若 K 为全 0 比特串，则返回步骤(2)重新选择随机数 r

计算 $C_2=r_{\mathrm{B}}\oplus K$

输出密文 $c_{\mathrm{B}}=C_1C_2$

步骤 B8：通过 FALCON 数字签名算法，使用签名私钥 sk_{BS} 对 c_{B} 进行签名，得到签名 c_{S}。

步骤 B9：计算出共享密钥 $SK=\mathrm{KDF}\left(\mathrm{ID}_{\mathrm{A}}\|\mathrm{ID}_{\mathrm{B}}\|r_{\mathrm{A}}\|r_{\mathrm{B}},klen\right)$。

步骤 B10：使用 SM3 密码杂凑算法计算出 SK 的杂凑值计算 $\mathrm{H}_{SK}=\mathrm{hash}\left(SK\right)$。

步骤 B11：生成时间戳 T_{B}。

步骤 B12：使用 SM3 密码杂凑算法计算出要传输消息的杂凑值 $\mathrm{H}_{\mathrm{B}}=\mathrm{hash}\left(\mathrm{H}_{SK}\|\mathrm{ID}_{\mathrm{B}}\|pk_{\mathrm{BS}}\|c_{\mathrm{B}}\|c_{\mathrm{S}}\|T_{\mathrm{B}}\right)$。

步骤 B13：将 $M_2=\left(\mathrm{H}_{SK},\mathrm{ID}_{\mathrm{B}},pk_{\mathrm{BS}},c_{\mathrm{B}},c_{\mathrm{S}},T_{\mathrm{B}},\mathrm{H}_{\mathrm{B}}\right)$ 发送给用户 A。

用户 A：

步骤 A8：使用 SM3 密码杂凑算法计算出接收到的消息的杂凑值 $\mathrm{H}'_{\mathrm{B}}=\mathrm{hash}\left(\mathrm{H}_{SK}\|\mathrm{ID}_{\mathrm{B}}\|pk_{\mathrm{BS}}\|c_{\mathrm{B}}\|c_{\mathrm{S}}\|T_{\mathrm{B}}\right)$，验证 $\mathrm{H}'_{\mathrm{B}}=\mathrm{H}_{\mathrm{B}}$ 是否成立，如果不成立将中断密钥交换过程；如果成立，继续执行后续步骤。

步骤 A9：分析时间戳 T_{B}，判断接收时间是否在时间窗口 $\left[T_{\mathrm{B}}+\Delta t-\Delta s,T_{\mathrm{B}}+\Delta t+\Delta s\right]$ 区间内，如果不在，将中断密钥交换过程；如果在时间窗口区间内，继续执行后续步骤。

步骤 A10：通过 FALCON 数字签名验证算法，使用用户 B 的签名公钥 pk_{BS} 验证 c_{B} 的签名 c_{S}，如果签名验证失败，将中断密钥交换过程；如果签名验证成功，继续执行后续步骤。

步骤 A11：通过 SM9 解密算法，使用 de_{A} 和 ID_{A} 对 c_{B} 进行解密，得到明文 r_{B}，具体为：

从 c_{B} 中取出比特串 C_1，将 C_1 的数据类型转换为椭圆曲线上的点，验证 $C_1\in G_1$ 是否成立，若不成立则报错并退出

计算群 G_T 中的元素 $w'=e\left(C_1,\mathrm{de}_\mathrm{A}\right)$，将 w' 的数据类型转换为比特串

计算 $K'=\mathrm{KDF}\left(C_1\|w'\|\mathrm{ID}_\mathrm{A},256\right)$，若 K' 为全 0 比特串，则报错并退出

计算 $r_\mathrm{B}=C_2\oplus K'$

步骤 A12：计算出共享密钥 $SK'=\mathrm{KDF}\left(\mathrm{ID}_\mathrm{A}\|\mathrm{ID}_\mathrm{B}\|r_\mathrm{A}\|r_\mathrm{B},klen\right)$。

步骤 A13：使用 SM3 密码杂凑算法计算出 SK' 的杂凑值 $\mathrm{H}'_{SK}=\mathrm{hash}\left(SK\right)$，验证 $\mathrm{H}'_{SK}=\mathrm{H}_{SK}$ 是否成立，如果不成立，从用户 B 到用户 A 的密钥确认失败；如果成立，从用户 B 到用户 A 的密钥确认成功，可以选择继续执行下一步骤。

步骤 A14 (可选项)：通过 FALCON 数字签名算法，使用签名私钥 sk_AS 对 H'_{SK} 进行签名，得到签名得到签名 s_H，并将 $M_3=s_\mathrm{H}$ 发送给用户 B。

用户 B：

步骤 B14 (可选项)：通过 FALCON 数字签名验证算法，使用用户 A 的签名公钥 pk_AS 验证 s_H 是否是 H_{SK} 的有效签名，如果签名验证失败，从用户 A 到用户 B 的密钥确认失败；如果签名验证成功，从用户 A 到用户 B 的密钥确认成功。

基于 SM9 和 FALCON 的密钥交换协议流程如图 1。

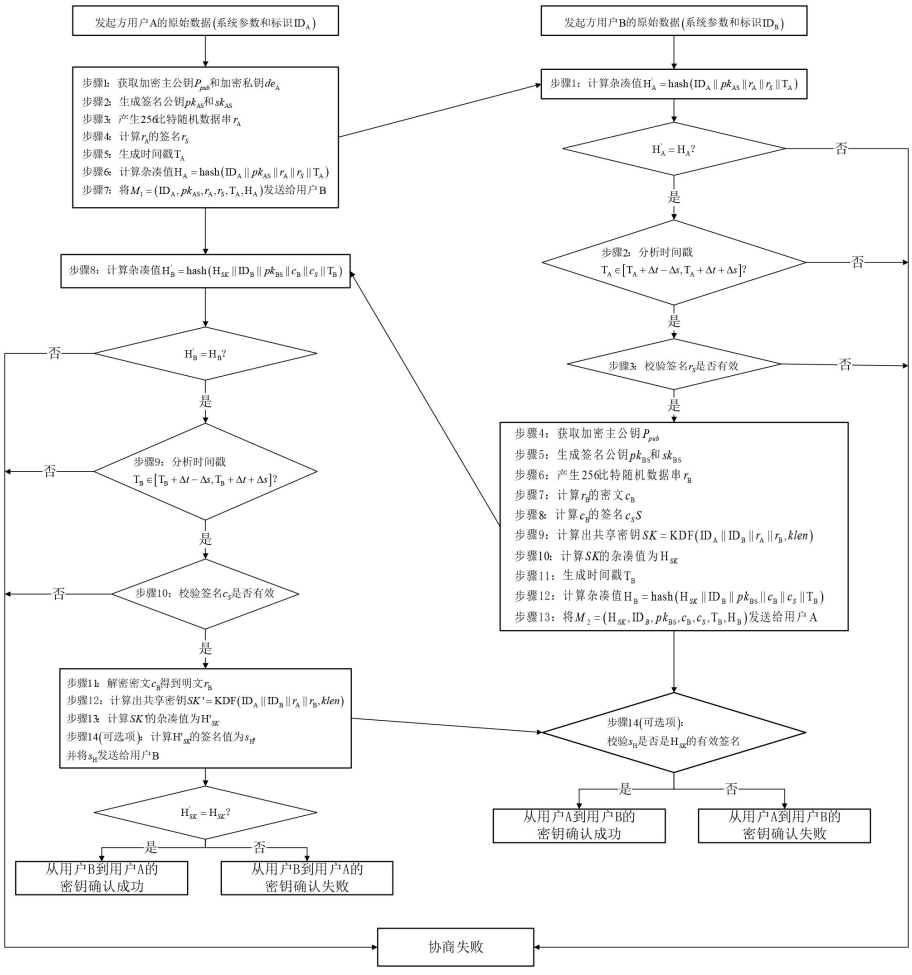

Figure 1. Flowchart of key exchange protocol based on SM9 and FALCON
图 1. 基于 SM9 和 FALCON 的密钥交换协议流程图

4. 安全性分析

4.1. BAN 逻辑分析

本文采用 BAN 逻辑证明协议的安全性，形式化说明协议能够达到预期的安全目标。表 1 给出了本文涉及的 BAN 逻辑符号和含义，表 2 给出了本文使用的 BAN 逻辑规则。

Table 1. Symbols and meanings of BAN logic
表 1. BAN 逻辑符号和含义

符号	含义
$P \mid\equiv X$	P 相信 X
$P \lhd X$	P 曾经收到包含 X 的信息
$P \mid\sim X$	P 曾经发送包含 X 的信息
$\#X$	X 是新生成的随机数
$P \mid\Rightarrow X$	P 对 X 有仲裁权
$P \overset{K}{\longleftrightarrow} Q$	K 是 P 和 Q 之间共享的密钥
$\{X\}_K$	使用 K 加密 X
A/B	A 表示协议发起方，B 表示协议响应方

Table 2. Rules of BAN logic
表 2. BAN 逻辑规则

符号	含义
R_1	$\dfrac{A \mid\equiv A \overset{K}{\longleftrightarrow} B, A \lhd \{X\}_K}{A \mid\equiv B \mid\sim X}$
R_2	$\dfrac{A \mid\equiv \#X, A \mid\equiv B \mid\sim X}{A \mid\equiv B \mid\equiv X}$
R_3	$\dfrac{A \mid\equiv B \mid\Rightarrow X, A \mid\equiv B \mid\equiv X}{A \mid\equiv X}$
R_4	$\dfrac{A \mid\equiv B, B \mid\equiv X}{A \mid\equiv B \mid\equiv X}$

协议的理想化过程如下。

消息 $M_1 = (\mathrm{ID_A}, pk_{\mathrm{AS}}, r_{\mathrm{A}}, r_{\mathrm{S}}, T_{\mathrm{A}}, \mathrm{H_A})$、$M_2 = (\mathrm{H}_{SK}, \mathrm{ID_B}, pk_{\mathrm{BS}}, c_{\mathrm{B}}, c_{\mathrm{S}}, T_{\mathrm{B}}, \mathrm{H_B})$ 在不安全信道传输，则其对应的理想化形式分别为 $M_1(\mathrm{B} \lhd r_{\mathrm{A}}, \mathrm{B} \lhd r_{\mathrm{S}})$、$M_2(\mathrm{A} \lhd c_{\mathrm{B}}$ 即 $\mathrm{A} \lhd \{r_{\mathrm{B}}\}_{\mathrm{ID_A}}, \mathrm{A} \lhd c_{\mathrm{S}})$。

协议初始化假设如下。

P_1：$A \mid\equiv A \overset{P_{\mathrm{pub}}}{\longleftrightarrow} B$，$B \mid\equiv B \overset{P_{\mathrm{pub}}}{\longleftrightarrow} A$

P_2：$A \mid\equiv \#r_{\mathrm{B}}$，$B \mid\equiv \#r_{\mathrm{B}}$，$A \mid\equiv \#r_{\mathrm{S}}$，$B \mid\equiv \#r_{\mathrm{S}}$

P_3：c_{S} 是 c_{B} 的签名，则 $c_{\mathrm{S}} \mid\equiv c_{\mathrm{B}}$

P_4：$A \mid\equiv c_{\mathrm{S}} \mid\Rightarrow c_{\mathrm{B}}$，$A \mid\equiv c_{\mathrm{B}} \mid\Rightarrow r_{\mathrm{B}}$

P_5：B 验证 r_{S} 是有效签名，则 $B \mid\equiv r_{\mathrm{S}}$，$B \mid\equiv A \mid\sim r_{\mathrm{S}}$

P_6：A 验证 c_{S} 是有效签名，则 $A \mid\equiv c_{\mathrm{S}}$，$A \mid\equiv B \mid\sim c_{\mathrm{S}}$

P_7：$A \models A \xleftrightarrow{ID_A} B$，$B \models B \xleftrightarrow{ID_A} A$

P_8：通过可选项的操作，B 验证 s_H 是 H_{SK} 的有效签名后，$B \models A \models r_B$

由于共享密钥的生成与安全性取决于随机数据串 r_B，所以本文协议需要证明的目标如下。

G_1：$A \models B \models r_B$，即 A 相信 B 也相信协商出的共享秘密数据串 r_B

G_2：$A \models r_B$，即 A 相信与 B 协商出的共享秘密数据串 r_B

G_3：$B \models A \models r_B$，即 B 相信 A 也相信协商出的共享秘密数据串 r_B

G_4：$B \models r_B$，即 B 相信与 A 协商出的共享秘密数据串 r_B

根据协议初始化假设、协议理想化以及 BAN 逻辑规则来证明协议目标，具体的证明过程如下。

目标 G_1 证明过程

根据 P_7 和 M_2，通过规则 R_1，可以得到 Q_1；根据 Q_1 和 P_2，通过规则 R_2，可以得到目标 G_1。具体为：

$$\frac{A \models A \xleftrightarrow{ID_A} B, A \lhd \{r_B\}_{ID_A}}{A \models B \mid\sim r_B}：Q_1$$

$$\frac{A \models \#r_B,\ A \models B \mid\sim r_B}{A \models B \models r_B}：G_1$$

目标 G_2 证明过程

根据 P_2 和 P_6，通过规则 R_4，可以得到 Q_2；根据 Q_2 和 P_4，通过规则 R_3，可以得到 Q_3；根据 Q_3 和 P_3，通过规则 R_4，可以得到 Q_4；根据 Q_4 和 P_4，通过规则 R_3，可以得到目标 G_2。具体为：

$$\frac{A \models c_S, c_S \models c_B}{A \models c_S \models c_B}：Q_2$$

$$\frac{A \models c_S \models\Rightarrow c_B, A \models c_S \models c_B}{A \models c_B}：Q_3$$

$$\frac{A \models c_B, c_B \models r_B}{A \models c_B \models r_B}：Q_4$$

$$\frac{A \models c_B \models\Rightarrow r_B, A \models c_B \models r_B}{A \models r_B}：G_2$$

目标 G_3 证明过程

根据 P_8，可以直接得到目标 G_3，即

$B \models A \models r_B$：G_3

目标 G_4 证明过程

由于 r_B 由 B 生成，所以可以直接得到 G_4，即

$B \models r_B$：G_4

4.2. 非形式化分析

4.2.1. 相互认证性

参与方 A 和 B 分别通过验证 r_S 和 c_S 两个签名是否有效来认证对方的身份。因为 r_S 和 c_S 通过 FALCON 签名算法生成，安全性由 NTRU 格上的 SIS 困难问题保证，攻击者不能在多项式时间内解决该问题，从而攻击者不能冒充合法参与者通过身份认证。因此，本文协议实现了发起方 A 和响应方 B 之间的相互认证性。

4.2.2. 抗重放攻击

本文协议中，参与方接收到信息会先校验时间戳的有效性，只有在时间窗口内的信息才认为是合法

信息，再进行下一步操作。因此，攻击者无法直接转发消息发起重放攻击。并且，本文协议中每个时间戳都添加到 SM3 杂凑值中，若攻击者通过替换新的时间戳发起重放攻击，则杂凑值无法通过验证，参与方将会中断与攻击者间协议的执行。因此，本文协议可以抵抗重放攻击。

4.2.3. 抗中间人攻击

为了发起中间人攻击，攻击者拦截通信双方的信息后，必须修改截获的信息，并让对方相信篡改的信息是真实的。由于攻击者无法得到参与方的加密私钥与签名私钥，因此，攻击者不能正确地修改传输中的信息，不能达到攻击目的。并且如前文所述，每个参与方都会检查时间戳的有效性，如果有第三方攻击者进行截取或转发两者之间的信息，由于消耗的时间大概率会远超过消息的传输时间，从而导致时间戳非法，接受者通过时间戳也可以辨认出该消息不是合法的消息。因此，本文协议可以抵抗中间人攻击。

4.2.4. 抗拒绝服务攻击

由于每个参与方接收到信息后都会先检查时间戳的有效性然后校验 SM3 杂凑值，任何一个验证失败，参与方都会中断执行的协议。因此，当参与方接收到大量非法信息时，计算资源并不会被大量浪费。因此，本文协议可以抵抗拒绝服务攻击。

4.2.5. 完全前向安全性

本文协议每次被执行时，都会根据通信参与双方重新生成的随机数创建新的共享会话密钥，并且保障协议协商过程的机密性与认证性所使用的 SM9 与 FALCON 的公私钥对也都会进行更新，因此协商生成的每个新密钥都与以前协商生成的密钥不可区分，任何会话密钥的泄露都不会影响其他会话密钥的安全性。因此，本文协议达到了完全的前向安全性要求。

4.2.6. 完善保密性

完善保密性主要是指明文与密文相互独立，知道密文并不能改善对于明文的认识[19]。本协议应用 SM9 公钥加密算法时，使用基于密钥派生函数的序列密码算法加密明文的方法，先生成与要加密的 256 比特随机数据串等长的密钥，再通过逐比特异或运算进行加密。这种一次一密的加密方法具有完善保密性。

5. 结束语

本文设计了一个基于 SM9 和 FALCON 的密钥交换协议，与 SM9 标识密码算法中的密钥交换协议[3]相比，该协议增加了签名，让协商双方可以鉴别对方的身份。并且，本文协议增加了时间戳信息，可以更好地抵抗重放攻击。经过安全性分析，该协议具有相互认证性、抗重放攻击、抗中间人攻击、抗拒绝服务攻击、完全前向安全性、完善保密性。本文协议采用抗量子安全的 FALCON 签名算法来提供身份认证和数据完整性。本文协议在使用 SM9 标识密码算法时，为了进一步增强加密主密钥对的安全性，主公钥随着私钥安全地发送给协议的参与方，通过人为管理的方式保证主公钥除了协议参与双方外无人知道。在文件共享、视频会议、无线网络安全通信等数据传输场景中，都可以应用本文所设计的基于 SM9 和 FALCON 的密钥交换协议来协商出一致的会话密钥，然后用此密钥对通信内容进行加密，从而达到安全地传输信息的目的。

基金项目

国家自然科学基金(61370188)；北京市教委科研计划(KM202010015009)；北京市教委科研计划资助(No. KM202110015004)；北京印刷学院博士启动金项目(27170120003/020)；北京印刷学院科研创新团队项目(Eb202101)；北京印刷学院校内学科建设项目(21090121021)；北京印刷学院重点教改项目(22150121033/009)；北京印刷学院科研基础研究一般项目(Ec202201)；北京印刷学院博士启动金项目(27170122006)；北京印

刷学院基础研究一般项目(Ec202201)；北京市高等教育学会 2022 年立项面上课题(MS2022093)；北京市教育委员会科学研究计划项目资助(KM202310015002)；北京印刷学院网络空间安全培育学科建设项目(21090123010)。

参考文献

[1] Shamir, A. (1985) Identity-Based Cryptosystems and Signature schemes. In: Blakley, G.R. and Chaum, D., Eds., *Advances in Cryptology*: *Proceedings of CRYPTO*'84, Springer, Berlin, 47-53. https://doi.org/10.1007/3-540-39568-7_5

[2] Boneh, D. and Franklin, M. (2001) Identity-Based Encryption from the Weil Pairing. *Advances in Cryptology—CRYPTO* 2001: 21*st Annual International Cryptology Conference*, Santa Barbara, 19-23 August 2001, 213-229. https://doi.org/10.1007/3-540-44647-8_13

[3] 陈晓, 程朝晖, 张振峰, 等. GB/T 38635.2-2020, 信息安全技术 SM9 标识密码算法第 2 部分: 算法[S]. 2020.

[4] 王小云, 李峥, 王永传, 等. GB/T 32905-2016, 信息安全技术 SM3 密码杂凑算法[S]. 2016.

[5] Fouque, P.A., Hoffstein, J., Kirchner, P., *et al*. (2018) FALCON: Fast-Fourier Lattice-Based Compact Signatures over NTRU. https://falcon-sign.info/falcon.pdf

[6] 王圣宝, 周鑫, 文康, 翁柏森. 适用于智能电网的三方密钥交换协议[J]. 通信学报, 2023, 44(2): 210-218.

[7] Burrows, M., Abadi, M. and Needham, R. (1990) A Logic of Authentication. *ACM Transactions on Computer Systems* (*TOCS*), **8**, 18-36. https://doi.org/10.1145/77648.77649

[8] 张敏, 许春香, 张建华. 无人机网络中基于多因子的认证密钥协商协议研究[J]. 信息网络安全, 2022, 22(9): 21-30.

[9] Shor, P.W. (1999) Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Review*, **41**, 303-332. https://doi.org/10.1137/S0036144598347011

[10] 梁敏, 罗宜元, 刘凤梅. 抗量子计算对称密码研究进展概述[J]. 密码学报, 2021, 8(6): 925-947. https://doi.org/10.13868/j.cnki.jcr.000488

[11] 宋昭阳, 王一诺, 王浩文, 马鸿洋. 基于 Hopfield 网络"伪吸引子"与交替量子随机行走的抗攻击彩色图像加密方案[J/OL]. 电子学报: 1-13. http://kns.cnki.net/kcms/detail/11.2087.tn.20230330.0928.008.html, 2023-04-11.

[12] 吕述望, 李大为, 邓开勇, 等. GB/T 32907-2016, 信息安全技术 SM4 分组密码算法[S]. 2016.

[13] 何烜, 王红军, 袁泉. 可证明安全的射频识别双向认证协议[J]. 空军工程大学学报(自然科学版), 2018, 19(5): 41-46.

[14] Gentry, C., Peikert, C. and Vaikuntanathan, V. (2008) Trapdoors for Hard Lattices and New Cryptographic Constructions. *Proceedings of the* 40*th Annual ACM Symposium on Theory of Computing*, Victoria, 17-20 May 2008, 197-206. https://doi.org/10.1145/1374376.1374407

[15] Damgard, I. (1990) A Design Principle for Hash Functions. In: Brassard, G., Ed., *CRYPTO*'1989, Springer, Berlin, 416-427. https://doi.org/10.1007/0-387-34805-0_39

[16] Merkle, R.C. (2001) A Certified Digital Signature. In: Brassard, G., Ed., *Advances in Cryptology—CRYPTO*'89 *Proceedings*, Springer, New York, 218-238. https://doi.org/10.1007/0-387-34805-0_21

[17] 李大为, 冯登国, 陈华, 等. GB/T 32915-2016, 信息安全技术二元序列随机性检测方法[S]. 2016.

[18] 王小云, 于红波. SM3 密码杂凑算法[J]. 信息安全研究, 2016, 2(11): 983-994.

[19] 陆成刚, 王庆月. 一次一密理论的再认识[J]. 高校应用数学学报 A 辑, 2022, 37(4): 426-430. https://doi.org/10.13299/j.cnki.amjcu.002240