

Distributed New Energy Remote Control Message Integrity Authentication Method Based on SM3

Chen Yingda, Heng Xingchen, Ou Yongtong*, Chen Chongchen, Lin Junhong, Deng Ke

China Southern Power Grid Digital Grid Group Co., Ltd, Guangzhou, China

Email address:

fifachen@qq.com (Chen Yingda), hengxc@csg.cn (Heng Xingchen), ouyt@csg.cn (Ou Yongtong), chencc2@csg.cn (Chen Chongchen), linjh@csg.cn (Lin Junhong), dengke@csg.cn (Deng Ke)

*Corresponding author

To cite this article:

Chen Yingda, Heng Xingchen, Ou Yongtong, Chen Chongchen, Lin Junhong, Deng Ke. Distributed New Energy Remote Control Message Integrity Authentication Method Based on SM3. *Science Discovery*. Vol. 10, No. 3, 2022, pp. 168-172. doi: 10.11648/j.sd.20221003.24

Received: May 9, 2022; Accepted: May 31, 2022; Published: June 9, 2022

Abstract: Distributed energy has the characteristics of wide geographical distribution. Fuoh-distributed energy needs to use various communication methods to access grid information exercise. For remote control and other key information, this information is vulnerable to third-party attacks, attacks can cause grid operations to malfunction. This paper proposes a message integrity authentication method about distributed new energy remote control system, it is designed based on SM3 message. First of all, analysis of the content of the transmitted telecontrol message, use SM3 hash calculation to generate the corresponding hash value, the hash value in this article is 1. And sent to the opposite side together with the remote control message. The receiver will receive the sent information, when the receiver has completely received the sent content and continue to calculate the remote control message information, the calculation process is to use the hash operation to process and get the hash value 2, compare this value with the hash value of 1, and continue to transmit together with the remote control message. This paper exemplifies the specific operation steps, provide reference for readers to use. And developed special test software, the designed method was tested with this software, the test results show that the designed method is feasible, meet the design requirements, realize the safe communication of power grid information.

Keywords: SM3 Operation, Integrity Verification, Power Network Information Security

基于SM3的分布式新能源遥控报文完整性认证方法

陈英达, 衡星辰, 区永通*, 陈重辰, 林俊宏, 邓轲

南方电网数字电网集团有限公司, 广州, 中国

邮箱

fifachen@qq.com (陈英达), hengxc@csg.cn (衡星辰), ouyt@csg.cn (区永通), chencc2@csg.cn (陈重辰), linjh@csg.cn (林俊宏), dengke@csg.cn (邓轲)

摘要: 地理分布广泛的分布式能源需以多样化的通信方式接入电网信息系统, 对于遥控等关键信息, 容易遭受第三方恶意篡改导致电网操作误动。本文提出了基于SM3的分布式新能源遥控报文完整性认证方法。首先通过对所传输的遥控报文内容进行SM3哈希计算后生成哈希值1, 与遥控报文一起发送。接收方在收到发送内容后, 拆分出遥控报文进行哈希运算处理得到哈希值2, 再对所接收到的哈希值1比对, 完成传输内容的完整性验证。论文提出了操作的具体步骤, 并开发测试软件证明了该认证方法的可行性, 达到了实现电网信息安全传递的目的。

关键词: SM3运算, 完整性验证, 电网信息安全

1. 引言

在新型电力系统背景下,分布式能源广泛接入电网中,接入设备类型多,数量大,需要交互的信息日趋丰富,潜在的信息风险点也日趋增大。另外,由于分布式能源地理分布广泛,需要借助各种灵活的通信方式实现电网“最后一公里”的信息交互,多样化的通信直接导致了电网信息潜在安全风险的增加。

以明文为呈现方式的电力信息报文已无法满足新型电力系统的信息安全要求,当前已逐步采用加密等方法对电力报文信息进行安全处理。考虑到当前电力智能电子设备多以嵌入式控制器为主,相较于服务器等高性能计算机,主频较低,而且内存、计算能力相对有限,现有的智能电子设备在完成保护、控制等基本功能基础上,还要另外增加耗时较大的加解密算法。因此,现在多采用在通信两端额外增加加密机的做法。加密机专门处理报文的加解密算法,不仅增加了设备成本,而且额外增加了通信环节,增加了通信系统的复杂性,降低了分布式能源信息传递的实时性[1, 2]。在不改变硬件结构的基础上,国家密码局推行SM系列密码算法对电力报文的私

密性、完整性和不可否认性进行保护[3-6]。对于电力遥控报文而言,保证报文没有篡改或伪造,即报文的完整性校验而成为重要的研究热点。因此,本文分析了遥控报文的特点,并利用国密算法SM3对报文提出一种完整性认证方法。

2. 遥控报文完整性分析

2.1. 完整性分析

对于分布式能源与主电网的信息交互来说,除了信息的保密性,报文的完整性也是电力信息的关键内容。对于分布式新能源,涉及设备开关的操作,在由调控中心对开关进行传递报文的过程中,都有可能受到来自黑客网络的袭击,黑客在对传输信号进行伪造和篡改,来自于原调控中心的信号变成黑客伪造和篡改之后的信号,电网执行篡改信号之后,可能会对整个电网的安全运行造成较大的影响。因此对于接收到的报文,如何确定报文的完整性是一个重要的内容[7-10]。

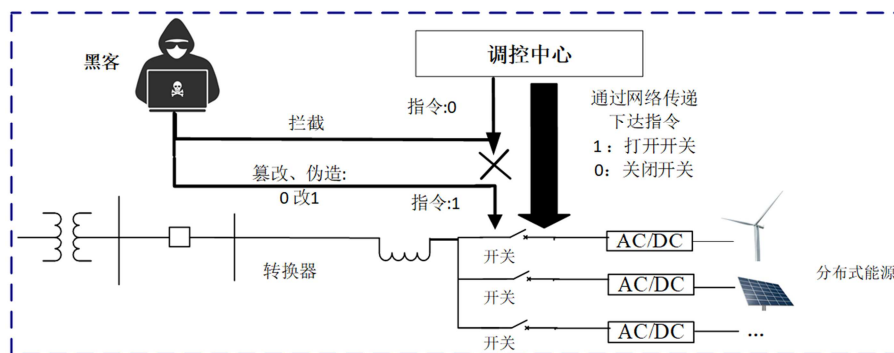


图1 分布式新能源报文遭篡改示意图。

在新型电力系统中,电能传递是从分布式新能源诸如太阳能、风能等发电,经过交直流转换,再通过并网开关接入到主电网。分布式新能源发电端接入主电网的环节中,并网开关等各类开关控制是重要的内容,远端的调控中心可以通过遥控报文下达相应指令到智能并网开关等执行具体操作命令。例如,调控中心以命令“1”作为开关断开的指令,“0”作为开关闭合的指令,在调控中心下达相应的指令之后,开关装置就会执行对应的指令。但是在调控中心下达指令后,指令信息经过多种通信方式进行传递的过程当中,传递的信息容易被黑客入侵攻击,将传递的指令拦截,并且篡改、伪造成另一种指令进行传递,例如将调控中心下达的闭合指令“0”篡改成断开指令“1”后传递到开关装置,如图1所示。开关装置在接收到错误的指令后执行与调控中心所下达的指令完全不同的操作,对电网的安全运行造成了极大的影响。

2.2. 遥控表规范分析

分布式新能源在发电控制、接入主电网的并网等多个环节,涉及到开关的控制,开关的控制直接关系到分布式

新能源甚至整个主电网的安全运行。分布式新能源的各类重要开关,除了智能电子设备可以就地进行开关操作外,远端的调控中心也可以通过遥控报文进行开关操作。为了实现遥控报文在不同厂家的自动化设备和信息系统间无缝切换,采用统一的遥控报文格式,如表1所示,主要包括对应的遥信点号、遥控量描述、遥控点号和RTU号等内容。

表1 遥控表表头。

对应遥信点号	遥控量描述	遥控点号	RTU号	备注
1	2	3	4	5

1、对应遥信点号:

整型,不能为空。除主变档位相关遥控点外,每个遥控点均需关联遥信点,对应点号与遥信表一致。

不需填写对应遥信点号的遥控量包括(遥控量描述应严格按照下列命名):

#x主变调档(适用于升档和降档使用同一个遥控点的情况。默认升档为控合,降档为控分)

#×主变升档（适用于升档和降档使用 不同遥控点的情况。默认升档为控合）
#×主变降档（适用于升档和降档使用不同遥控点的情况。默认降档为控合）
#×主变急停（默认急停为控合）
现场控分控合情况与默认不一致的，需填写备注。
2、遥控量描述：
字符串类型，不能为空。除主变档位相关遥控点外，遥控点描述应与关联的遥信点描述一致。
3、遥控点号：
整型，不能为空。起始点号为0。
4、RTU号：
整型，不能为空。RTU号为远动的标识号，由主站分配，应与主站保持一致。遥控点RTU号应与其关联遥信点的RTU号保持一致。
5、备注：字符串类型，可以为空。用于填写一些需要说明的内容。

为了更好了解遥控表内容的要求，以主变变高101开关遥控命令为例，根据表头和内容规则可以编制遥信表，部分如表2所示。对应的遥信点号为416，对应的RTU设备为78号设备。

表2 遥控表示例。

对应遥信点号	遥控量描述	遥控点号	RTU号
416	#1主变调档	4	78
	#1主变变高101开关	1	78

3. SM3的完整性校验

随着新型电力系统的发展，电力信息的遥控命令在广域交换中容易遭受篡改等恶意第三方攻击，存在电力信息安全。本文基于SM3算法实现新能源遥控报文完整性的验证方法，以抵御第三方恶意篡改攻击。通过对遥控信息进行含密码的SM3哈希运算后，产生信息摘要，并将该信息摘要传递到通信接收方后，由互享密码的接收方进行同样的SM3运算后得到本地的计算信息摘要，并与接收到的信息摘要进行一致性校验，从达到了验证遥控报文完整性的目的，提高电网信息传递的安全性，有助于电网稳定运行[11]。

3.1. SM3算法介绍

SM3是中华人民共和国政府采用的一种密码散列函数标准，由国家密码管理局于2010年12月17日发布。在商用密码体系中，SM3主要用于数字签名及验证、消息认证码生成及验证、随机数生成等，属于哈希算法的一种。SM3算法将任意长度的二进制值映射为较短的固定长度的二进制值，这个小的二进制值称为哈希值。哈希值是一段数据唯一且极其紧凑的数值表示形式。即它是一个从明文到密文的不可逆的映射，只有加密过程，没有解密过程。
SM3算法完整性检验原理，如图2所示，其将接收到的消息经过SM3算法运算后，得以对应的哈希值。通过将单向数学函数应用到任意数量的数据.所得到的固定大小的结果。若输入数据中有变化，则哈希也随之发生变化。要找到散列为同一个值的两个不同的输入，在计算上是不

可能的，所以数据的哈希值可以检验数据的完整性，一般用于快速查找和加密算法。还可用于许多操作等，包括身份验证和数字签名，也称为“消息摘要”。

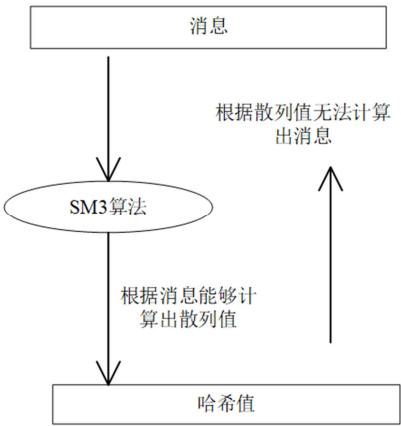


图2 SM3算法完整性检验示意图。

SM3算法是在SHA-256基础上的一种改进算法，使用Merkle-Damgard结构，消息分组为512位，摘要值为256位。虽然SM3与SHA-256在结构上有相似之处，但SM3算法的设计会更为复杂。因此SM3算法在目前的应用中是安全性较高的一种加密算法。SM3算法具有很好的创新性和高效性。其加密方法的压缩功能与SHA-256的编码功能类似，但更为复杂。如压缩函的每一轮都使用2个消息字。由于SM3算法自身的消息扩充和函数的局部处理比较复杂，因此它的安全性优于当前哈希算法SHA2-256。

SM3算法的具体运算过程可以分为填充、迭代压缩和生成杂凑值几个阶段填充，它是用一组比特来填充所输入的数据。在进行了填充处理之后，报文m的位长度正好是512的倍数，用于进一步的处理。分组扩展过程是将已填充的报文按512比特的数据包进行运算，然后将512比特的报文块扩大，产生132个字供随后的压缩功能处理，并按顺序利用压缩函数对扩展后的报文进行迭代压缩。最后一次迭代压缩得到的是一个杂数值[12-15]。

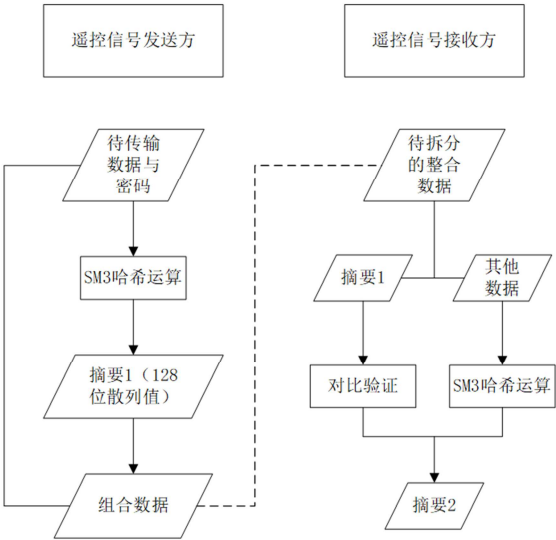


图3 SM3遥控信号完整性实验示意图。

3.2. 基于SM3的遥控信号完整性实现

M3的遥控信号完整性实现过程如图3所示, 信号的发送是将传输数据和密码经过SM3哈希运算后, 取128位哈希值的摘要1与原传输数据和密码进行组合然后发送。在对发送数据接收之后首先需要进行拆分, 将接收内容拆分成摘要1和接收数据, 然后对接收数据进行SM3哈希运算提取出摘要2, 最后将摘要1和摘要2进行对比, 实现遥控信号的完整性验证。如果摘要1与摘要2一致, 则证明报文未被篡改, 符合完整性校验。如果不一致, 则证明报文不可用。

在进行完整性验证之前, 需要将GmSSL国密算法库移植入Linux操作系统中, 以实现国密算法的移植, 进行加解密验证。

首先, 新建一个test.txt文件, 在里面输入一段信息串作为源遥控报文。如图4所示。



图4 新建test.txt文件。

其次, 用国密SM3算法对test文件进行报文完整性验证。如图5。

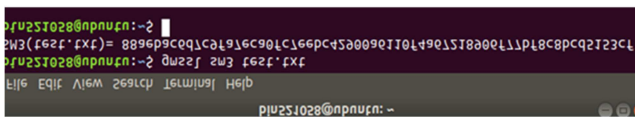


图5 SM3加密test文件。

图6为移植了GmSSL的SM3使用代码。

```
$ gmssl sm3 <yourfile>
SM3(yourfile)= 66c7f0f462eedd9d1f2d46bdc10e4e24167c4875cf2f7a2297da02b84ba8e0
```

图6 已移植GmSSL的SM3使用代码。

gmssl sm3 <yourfile>代码中yourfile为新建的test文件 SM3(test.txt)=88aebac6d7c9fa7eca0fc7eebc42900a6110f4a67218906f77bf8c8bcd5153cf就是使用SM3算法对test文件加密后的消息摘要。

4. 算例分析

利用Visual Studio community 2017+QT软件, 通过所移植的国密算法SM3, 开发相应的测试软件如下图7所示, 用来对SM3算法完整性的校验。



图7 软件界面示意图。

所开发的软件, 可以输入相应的遥控报文, 并得到相应的哈希值和测试出对报文进行哈希计算所需要计算开销。

4.1. SM3算法对遥控报文可靠性验证

为了得出遥控报文的哈希值, 设置4个不同的初始消息作为算例, 将这4个算例逐一进行五次哈希运算, 通过各个算例所得SM3值是否都是唯一值及是否符合SM3值的形式判断其可靠性。将每个算例输入进程序“明文”框内, 点击“加密”执行计算, “密文”框内将生成对应的哈希, 每个算例重复得到结果为下面表格所示:

表3 SM3哈希计算值。

待加密信息	输出的SM3哈希值
admin123	0192023a7bbd73250516f069df18b500
ABCDEFGF	bb747b3df3130fe1ca4afa93fb7d97c9
147* (we) @-	9971d9d5acbd04778b9d482f454b2119
00000000	dd4b21e9ef71e1291183a46b913ae6f2
346666	321023a7bbd73250516f069df18b543

以上算例的输出SM3值均为16进制形式, 32位的单向散列值, 且通过每一个算例的5次结果对比可以看出输出的结果稳定、均为一个唯一值。由此可知, SM3算法可以满足遥控报文的。

4.2. SM3算法对遥控报文时效性验证

遥控报文对算法的时效性也有一定的要求。为了验证SM3算法的时效性, 设置两组不同长度的算例作为对照, 每组算例均运算3次, 将运算所用时间取平均值, 通过对比分析算法的时效性。随意设置两组报文的初始值, 其中A组都为16位字符串, B组都为64位字符串。

表4 SM3算法的时效性检验A组。

待加密信息	加密时间 (us)	平均用时 (us)
LBWNB1234567REFD	0.001975	0.002370
	0.002765	
	0.002370	
417SSEZ@yhwMYJJ5	0.002370	0.002370
	0.002765	
	0.001975	

表5 SM3算法的时效性检验B组。

待加密信息	加密时间 (us)	平均用时 (us)
~*MKJTM0&*j481489+asqEWQ	0.003951	0.003292
EDAMKpqkjlmgcumzme-#6635468	0.002370	
/Dagrlh7983	0.003556	
JMFSDGNTUTNSUJTNI898jmfso85	0.001975	0.002238
462jfpk*Eoirgsd983546DEWYGE	0.002765	
WTGSRGET	0.001975	

从表4、5给出的结果可以看出SM3算法的运算速度快, 运算上述算例所需时间均为微秒级别, 并且通过对比可以看出16位字符串与64位字符串运算所用平均时间相差甚微, 几乎可以归于系统误差, SM3算法在完整性校验上时效高。

4.3. SM3算法对遥控报文有效性验证

为了验证SM3算法的有效性, 通过设置遥控报文算例进行哈希计算。将算例随机选择任一位进行加1位、减1

位、修改值，并利用所设计的软件生成哈希值，通过对比分析得出有效性。结果如下表6所示。由表可得，不管是修改还是增加减少其中的报文，可得的哈希结果是完全不同的。从而验证了算法的有效法。

表6 算法的安全性验证。

——	待加密信息	输出的SM3值
报文	1111	C245b2c6f0bb79b72657a40e8831745
增加	11111	56GH78HR7fe0824c0579d9507d9052
缺失	111	1234340d6b3e56GESQ24FBGG5RR
篡改	1211	RFDE34TYUJJ6444sdde1eca46b8b6a8

5. 结论

本文研究基于SM3的分布式新能源遥控报文完整性认证方法，首先从分布式新能源报文遭篡改的过程引入传统方法与本文所使用的方法进行比较，然后介绍了哈希算法如何应用在分布式新能源的遥控报文之上，最后通过算法举例演示，实现对报文的加密运算，达到了实现电网信息安全传递的目的。

参考文献

[1] 张长泽.SM3算法在硬件加密模块中的实现与应用[J].信息通信, 2019 (09): 15-16。

[2] 谢敏敏,王勇,周林.基于SM2-SM3的IEC61850通信报文加密算法[J].自动化博览, 2021, 38 (01): 108-112。

[3] 李丹枫,王飞,赵国鸿.一种大流量报文HMAC-SM3认证实时加速引擎[J].计算机工程与科学, 2021, 43 (01): 82-88。

[4] 吴克河,程瑞,郑碧煌,崔文超.电力物联网安全通信协议研究[J].信息安全, 2021, 21 (09): 8-15。

[5] 张喜铭,李金,邱荣福,许艾.国密体系在智能变电站的研究与应用[J].南方电网技术, 2020, 14 (01): 39-45. DOI: 10.13648/j.cnki.issn1674-0629.2020.01.006。

[6] 沈雯婷,张惠刚,李忠安.智能变电站GOOSE报文数字签名实现[J].南京工程学院学报(自然科学版), 2019, 17 (03): 38-44. DOI: 10.13960/j.issn.1672-2558.2019.03.007。

[7] 杨庆成.数据加密技术在计算机网络安全中的应用[J].网络安全技术与应用, 2021 (09): 23-24。

[8] 陈清. 基于国密算法的智能变电站信息安全研究[D].东南大学, 2019: 1-20。

[9] 孙杨.基于MD5加密算法的系统安全登录研究[J].计算机光盘软件与应用, 2013, 16 (06): 228-229。

[10] 安子畅,杨硕,郑景.电力系统信息通信的网络安全及防护研究[J].通信电源技术, 2020, 37 (05): 216-217。

[11] 牛晓刚.电力自动化通信技术如何确保信息安全研究[J].科技创新导报, 2017, 14 (35): 91-92。

[12] 冯瑞珏,曾献煜,刘飘,等.高级加密标准算法在智能电网数据保护中的应用分析[J].广东电力, 2021, 34 (06): 98-104。

[13] 侯宪锋,韩磊,王兴元,等.国密算法在智能家居数据安全应用研究[J].中国新通信, 2021, 23 (20): 49-51。

[14] 曾献煜,刘飘,冯瑞珏,等.SM3算法在GOOSE报文中的安全应用[J].广西电力, 2021, 44 (04): 38-43。

[15] 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。