文章编号:1671-4598(2017)05-0258-04 DOI:10.16526/j.cnki.11—4762/tp.2017.05.071 中图分类号:TP3 文献标识码:A

电网智能单元加密算法效率评估

张 跃,张 骞,黄益彬,金倩倩
(南瑞集团公司(国网电力科学研究院),南京 210000)

摘要:随着智能电网发展和电力终端设备智能化和网络化的提升,基于TCP/IP协议的数据通信面临着传统的网络安全隐患;智能电网单元是电网控制的关键组成部分,负责电网业务数据的采集处理、控制指令的收发和执行等工作,涉及大量数据传输,如何保证数据的机密性,是电网系统正常运作的关键因素之一;针对智能单元的传输规约和传输数据的特点,通过模拟智能单元计算环境,在保密性需求的基础上,结合智能单元计算资源的实际情况,综合分析电力行业和国内常见密码算法,包括对称算法和非对称算法,从运算时间及稳定性,数据长度相关性,密钥长度相关性和加密模式几个方面对算法的性能进行综合性评估;为不同智能单元的机密性保护尤其是加密算法的选取提供理论基础和实验数据。

关键词:智能单元;加密算法;加解密效率;加密模式;机密性

Efficiency Evaluation of Cryptographic Algorithms in Smart Grid

Zhang Yue, Zhang Qian, Huang Yibin, Jin Qianqian
(NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing 210000, China)

Abstract: With the development of smart grid and the improvement of intelligence and networking of power terminal equipment, the data communication based on TCP/IP protocol is facing the traditional network security risk. The key part of power grid control is the smart grid unit, which is responsible for the collection and processing of the business data of the power grid, and the receiving and dispatching of the control command and the execution of the data, involving much data transmission. How to ensure the data confidentiality is one of the key factors for the operation of power grid system. In this paper, according to the characteristics of the data and transmission protocol of intelligent unit, through the simulation of intelligent computing environment, on the basis of security requirements, combined with the actual situation of intelligent computing resources, we analysis the power industry and the common national cryptographic algorithm, and evaluate the computing time and stability , correlation of data length, correlation of key length and working mode of the cryptographic algorithms. Providing theoretical basis and experimental data for the selection of confidentiality protection, especially encryption algorithm for different intelligent units.

Keywords: intelligent unit; cryptographic algorithm; encryption and decryption efficiency; cryptographic mode; confidentiality

0 引言

电网智能单元承载了电网业务中重要的生产数据汇总、分析处理和上送业务,需进行大量的数据传输,在此过程中数据若被窃听或破坏,会对电网业务造成影响,并可能导致不可估量的后果。因此,保证数据的机密性是电网系统正常运行的关键因素之一。由于智能单元对数据传输的实时性要求较高,而对数据进行加解密会对数据传输的实时性产生影响。因此,电力行业需要对各密码算法进行加解密效率进行评估,在保证数据安全的前提下,选择适用于电网智能单元的密码算法。同时,电网智能单元运行特性,在保证数据机密性和实时性的同时需要充分考虑数据加解密占用的计算资源和可用性影响。

本文主要分析了现有电力行业及国内外常见密码算法,并通过实验对各加密算法运算时间及稳定性、数据长度相关性、密钥生成和分发复杂度等方面对算法的综合性能进行评估,为不同智能单元的机密性保护尤其是加密算法的选取提供理论基础和实验数据,具有提升智能单元的信息安全防护水平的重要意义。

1 国内外密码算法研究现状

密码是一种通信双方按照一定的规则进行信息变换的保密手段。主要分为对称密码算法和非对称密码算法两大类。这类算法又分为分组密码和流密码两大类。分组密码算法不需要空间存储密钥序列,因此它适合用于存储空间有限的加密场合。

1.1 国内外常见密码算法现状

业界常见的非对称密码算法有RSA算法和国密SM2算法,分组算法有SM4、AES、DES、CAST、RC2、Blowfish、IDEA,流密码算法有RC4。密钥主流长度可选1024bit、2048bit、3072等。加密信息的保密等级随着RSA密钥长度的增加而提高。目前1024位已不是足够安全,SET(Secure Electronic Transaction)协议中要求CA采用2048bits长的密钥[1]。RSA公钥加密算法是应用比较广泛。文献[2]中运用RSA数字签名的技术评估云存储和数据安全。在云计算环境中,用户上传数据使用RSA算法进行加密,管理员可以通过私钥进行解密[3]。SM2算法采用ECC椭圆曲线密码机制,是基于椭圆曲线数学的一种公钥密码方法,ECC算法安全性是建立在计算椭圆曲线的离散对数非常困难的基础上[4]。SM2推荐了一条256位的曲线作为标准曲线。与RSA相比,基于ECC的算法可使用比RSA短得多的密钥并得到相同的安全性。国密SM1算法是由国家密码管理局编制的一种商用密码分组标准对称算法,该算法基于PKI技术,是一种基于硬件芯片的对称算法,该算法是国家密码管理部门审批的SM1分组密码算法,分组长度和密钥长度都为128比特,算法安全保密强度及相关软硬件实现性能与AES相当,该算法不公开,仅以IP核的形式存在于芯片中[5]。SM4分组密码算法,是国

收稿日期:2017-02-04; **修回日期**:2017-03-13。
基金项目:国家电网科技(SGFJXT00YJJS1600064)。
作者简介:张 跃(1985-),男,江苏盐城人,初级工程师,硕士研究生,主要从事信息安全方向的研究。

家密码管理局发布对称加密算法。分组长度为 128 比特，密钥长度为 128 比特。加密算法与密钥扩展算法都采用 32 轮非线性迭代结构[6]。SM4 密码算法的结构图如图 1 所示。

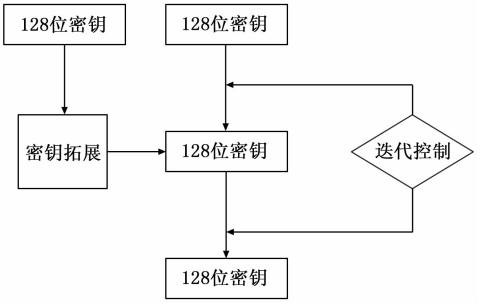

图 1　SM4 算法结构图

DES（data encryption standard），即数据加密标准，采用 64 位分组长度和 56 位密钥长度，将 64 位输入经过一系列变换得到 64 位输出[7]。算法主要分为两步：初始置换和逆置换。AES 和 Rijndael 加密法并不完全一样，因为 AES 的区块长度固定为 128 比特，密钥长度则可以是 128，192 或 256 比特，而 Rijndael 使用的密钥和区块长度可以是 32 位的整数倍，以 128 位为下限，256 位为上限[8]。文献［9］使用 AES 算法为 RFID（radio frequency identification）认证引进一个新的认证协议，主要工作是一个新 AES 硬件的实现方法，在 1000 个时钟周期里对 128bit 数据块加密。1996 年，C. Adams 和 S. Tavares 给出了 CAST 算法的一种改进形式 CAST－128，该算法能有效的抵抗差分攻击和线性攻击。文献［10］分析了 CAST 算法的两个缺陷，并提出了一个改进算法 E－CAST 算法，并用三组不同的基因数据集进行测试比较。RC2 是一种传统对称分组加密算法，它可作为 DES 算法的建议替代算法。它的输入和输出都是 64 比特。密钥的长度目前的实现是 8 字节。RC4 加密算法的速度可以达到 DES 加密的 10 倍左右，且具有很高级别的非线性[11]。RC4 起初是用于保护商业机密的。由于 RC4 算法加密采用的 xor，所以，一旦子密钥序列出现重复，密文就有可能破解[12]。随着科技的进步，该算法存在越来越多的安全隐患[13]。文献［14］对 Blowfish 安全性进行研究，并测试了内存大小与算法运行速度之间的关系。Blowfish 算法以其出色的性能被广泛应用于众多的加密软件，但是单纯使用 Blowfish 算法在实际应用中存在一些不足，如，等价密钥、重复初始化等，所以当前 Blowfish 算法也多与其他算法结合使用[15]。国际数据加密算法（IDEA，international data encryption algorithm）是对称加密算法，类似于三重 DES。IDEA 算法的一个安全缺陷是存在大量弱密钥。目前 IDEA 算法在工程中已有大量应用实例，文献［16］运用 IDEA 算法对 DNA 加密，可以抵御密码分析攻击，增加了数据的机密性；PGP（Pretty Good Privacy）使用 IDEA 算法作为其分组加密算法 IDEA 算法专利的所有者 Ascom 公司也推出了系列基于 IDEA 算法的安全产品，包括：基于 IDEA 的 Exchange 安全插件、IDEA 加密芯片、IDEA 加密软件包等[17]。

1.2　电力行业密码算法现状

电力行业的非对称算法加密时间慢，使用于数据量较小的情况下，因此常用于加密密钥加密解密和数字签名验签情况，电力行业中使用此类算法的有纵向加密认证网关、网络安全隔离装置（反向）、装置管理等设备。根据文献［18］，在安全性方面，基于各类算法实现的原理，算法 ECC 160bit 与 RSA 1024bit 具有相同的安全等级，ECC 224bit 与 RSA 2048bit 具有相同的安全等级，由于 SM2 是基于 ECC 椭圆密码机制，因此 SM2 256bit 比 RSA 2048bit 具有更高的安全等级；在效率方面，相较于 RSA 算法，SM2 密钥长度短，加解密计算开销小，处理速度快和占用存储空间小。随着密码科技的进步，常用的 1024 位 RSA 算法将被淘汰，我们国家密码管理部门经过研究，将国密 SM2 算法替换 RSA 算法。但是，由于历史原因，仍有 RSA 算法运行在一些电力设备中。

电力行业常用的分组算法主要有国密 SM4 算法，国密 SM1 算法。SM1 算法和 SM4 算法是我国自主设计的分组对称密码算法，保证数据和信息的机密性。SM1 算法和 SM4 算法均可用于网络数据和文件的加密保护以及数据存储。其中，SM4 算法分组长度和密钥长度为 128 bit。SM4 是我国制定 WAPI 标准的组成部分，同时也可以用于其他环境下的数据加密保护。

电力行业常用的哈希算法主要有国密 MD5 算法、SHA－1 算法和 SM3 算法。杂凑算法在密码学中具有重要的地位，广泛应用于数字签名、消息认证、数据完整性监测等领域。SM3 算法是由中国密码管理局 2010 年公布的中国商用密码杂凑算法标准。该算法由王小云等人设计，消息分组 512 比特，输出杂凑值 256 比特，采用 Merkle－Damgard 结构。SM3 密码杂凑算法的压缩函数与 SHA－256 的杂凑函数具有类似结构，但 SM3 杂凑算法的设计更加复杂。目前对 SM3 密码杂凑算法的攻击还比较少，比较安全。

电力行业关系到国计民生，对安全性要求比较高，因此对以上算法通常选择通过调用加密卡实现，而不去使用软实现方法。

1.3　电力智能化单元终端设备

电网智能单元可以为客户的安全用电、合理用电与节约用电提供数据支持，也可以通过信息平台为供电部门提供丰富的实时数据、统计分析数据等[19]。企业客户端电力智能单元基于现代数据采集和通信技术的企业用电实时监测系统，系统由监测终端、通信转换器、网络、监控计算机及监控软件等部分组成，采用 C/S 结构。企业可根据需要布置多个数据采集终端，采集到的大量数据经过智能单元加密后，经过企业局域网传到服务器上，服务器对数据进行解密，并加工处理，客户端可以通过访问服务器了解到采集到的丰富数据。具体结构如图 2 所示。

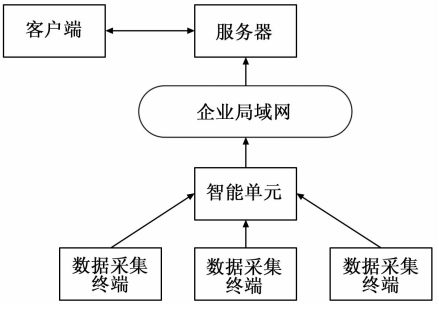

图 2　电网智能单元拓扑图

2　密码算法评估实验

2.1　实验环境

由于电网智能单元的 cpu 大多采用 ARM 架构和 PowerPC

架构，且 ARM 结构的纵向加密装置与电网智能单元拥有相似的加密解密功能和计算能力，因此，实验采用 ARM 结构纵向加密装置来模拟电网智能单元，实验网络拓扑如图 3 所示。

图 3 实验网络拓扑图

计算环境配置如下：

Linux 系统内核版本：3.14.0－xilinx

CPU：ARMv7 Processor rev 0 (v7l)

内存：512848 kB

2.2 实验设计步骤

由于非对称加密算法和对称加密算法的加密效率相差很大，而且非对称算法可以用于签名和验签，因此分开实验。非对称加密算法采用常用的国密算法 SM2 和 RSA 算法，分别测试加解密效率和签名验签效率。对称算法主要分为分组算法和流算法，其中分组算法有 SM4、DES，AES，CAST，RC2，Blowfish，IDEA 算法，典型流算法有 RC4 算法。由于 DES 的脆弱性，这里采用三重 3DES 加密算法进行实验，其中第一个密钥和第三个密钥采用同一个密钥，第二个密钥则采用另一个不同的密钥。算法通过测得给明文连续加密一百万次所用的时间，然后得出算法每秒钟加密次数，数据保留到个位，并得出数据每次加密所需要的时延，单位微秒（μs），保留小数点后面两位，作为算法的加密效率指标；解密同理。以上算法的实现通过调用 Openssl 里提供的算法，其中国密非对称算法 SM2 和国密对称算法 SM4 算法则自己实现，并封装到 Openssl 里。对以上对称算法测试它们的加解密效率，按以下几个方案实验进行比较。

（1）在相同的运行环境下，明文长度 128 B，不采用任何模式，对对称算法 SM4、AES、3DES、CAST、RC2、RC4、Blowfish、IDEA 进行实验，比较各算法的加解密效率。对非对称算法 SM2 和 RSA 算法进行实验，比较算法的加解密效率和签名验签效率。

（2）在相同的运行环境下，明文长度 128B，选择 SM4、AES、3DES 算法分别在不同的模式 ECB、CBC、CFB 下进行实验，比较各加密模式对加密算法效率的影响。

（3）在相同的运行环境下，明文长度 128B，选择 AES 算法测试在密钥长度为 128bit、192bit、256bit 长度下的算法的加解密效率，比较密钥长度对算法加解密效率的影响。

（4）改变明文数据长度，比较各对称密码的加解密效率，生成各密码一次加密时延与数据长度的关系曲线，和一次解密时延与数据的关系曲线。其中，明文数据长度选择 128B，256B，512B，1024B，2048B，时延选择微秒为单位。

2.3 实验与分析

实验一：加密算法对实时性的影响。

明文长度为 128，分组长度为 16 字节，对各算法依次加密一百万次和解密一百万次，得出各算法的加解密效率。结果数据如表 1 所示。

从表中可以得出，算法 AES 的加解密效率最高，一次加密和一次解密的时延分别为 5.89 μs 和 7.82 μs，速度较快，并且 AES 的安全性较高。其次是算法 CAST 和 RC4 算法，加解密时延为 8～9 μs，但安全性不如 AES 算法高。再其次是国密算法 SM4，加解密时延为 10 至 11 μs，安全性较高。其中，SM1 算法的测试环境为双核 Pentiem（R）Dual－Core CPU E5300 @2.6 GHz，内存 2 049 768 kB。国密算法 SM1 没有对外公开，仅以 IP 核的形式存在于芯片中，因此安全性最高，并广泛应用于电子商务、电子政务、网上银行证券等重要领域。通过实验发现，其加解密效率远不如 SM4 算法效率高。

表 1 对称算法的加解密效率比较

算法	每秒加密次数（次/s）	每秒解密次数（次/s）	加密时延（μs）	解密时延（μs）
SM1	10794	18214	92.64	54.90
SM4	94786	94696	10.55	10.56
AES	169779	127877	5.89	7.82
CAST	115754	118920	8.64	8.41
RC2	56557	52714	17.68	18.97
RC4	122309	122174	8.18	8.16
BF	5041	5048	198.37	198.10
IDEA	74962	29359	13.34	34.06

对于非对称密钥长度为 1024 位和 2048 位的 RSA 算法和密钥长度为 256 位的 SM2 算法，得出的加解密效率和签名验签效率如表 2 所示。

表 2 非对称算法 RSA 和 SM2 在不同密钥长度下的加解密效率表

算法	RSA_1024	RSA_2048	SM2_256
每秒加密次数(次/s)	2564	692	80
每秒解密次数(次/s)	137	21	154
每秒签名次数(次/s)	138	20	151
每秒验签次数(次/s)	2500	698	133
每秒生成密钥对次数(次/s)	1.16	0.21	154
加密时延(μs)	390.02	1445.09	12500.00
解密时延(μs)	7299.27	47619.05	6493.51
签名时延(μs)	7246.38	50000.00	6622.52
验签时延(μs)	400.00	1432.67	7518.50
每秒生成密钥对时延(μs)	862069	4761905	6494

从表中可以得出，RSA 的签名很慢，验签很快，公钥加密很快，私钥解密很慢。而 SM2 的的解密效率和签名效率相差不多，但 256 位 SM2 算法具有比 2048 位 RSA 算法有更高的安全等级，并且 SM2 密钥长度短，加解密计算开销小，处理速度快和占用存储空间小等优点。对于密钥对生成时间，SM2 算法生成 256bit 密钥的时间非常快，约为 RSA 算法生成 1024bit 密钥速度的 130 倍，RSA 算法生成 2048bit 密钥速度的 730 倍。因此，在同等安全等级下，SM2 算法加解密效率显著高于 RSA 算法，并且随着安全强度的不断增加，SM2 算法的优越性更加突出。

实验二：不同模式对加密算法效率的影响。

明文长度 128B，选取常用算法 SM4、AES、3DES 分别在 ECB、CBC、CFB 模式下进行实验，算法在 3 种模式下的加解密效率如表 3 所示：

从上表数据中得出，算法 SM4、3DES 在 ECB 和 CBC 模式

表 3　算法 SM4、AES、DES 在三种模式下的加解密效率表

算法	每秒加密次数（次/s）	每秒解密次数（次/s）	加密时延（μs）	解密时延（μs）
SM4_ECB	94517	94162	10.58	10.62
SM4_CBC	84817	84817	11.79	11.79
SM4_CFB	11914	11951	83.93	83.67
AES_ECB	167672	127000	5.96	7.87
AES_CBC	161838	124115	6.18	8.06
AES_CFB	145985	114823	6.85	8.71
3DES_ECB	28661	28636	34.89	34.92
3DES_CBC	28401	28457	35.21	35.14
3DES_CFB	3920	3893	255.10	256.87

下的加解密效率相差不错，但远高于 CFB 模式，而 AES 在三种模式下的加解密效率相差不多。但 ECB 一个重要的特点是如果明文有几个相同的明文分组，则加密后的密文也有几个相同的密文分组，而 CBC 模式却不存在这样的问题，并且 ECB 模式特别适用于数据较少的情况，比如密钥加密，对于数据较多情况却不适合。

实验三：不同密钥长度对算法加解密效率的影响。

明文长度为 128B，选取 AES 算法在密钥长度为 128b、192b、256b 长度下进行实验，算法在三种密钥长度下的加解密效率如下表所示：

表 4　算法 AES 在不同密钥长度下的加解密效率表

算法	每秒加密次数（次/s）	每秒解密次数（次/s）	加密时延（μs）	解密时延（μs）
AES_128	169779	127877	5.89	7.82
AES_192	144717	107758	6.91	9.28
AES_256	126582	96061	7.90	10.41

从上表数据中得出，算法 AES 随着密钥长度的变化，加解密效率有明显的降低，但是安全性得到了提升。

实验四：明文长度对各各对称密码加解密效率的影响。

选择长度为 128B，256B，512B，1024B，2048B 的明文，时延单位为微秒 μs，各算法加密时延与明文数据长度的曲线，解密时延与明文数据长度的曲线，如图 4 与图 5。

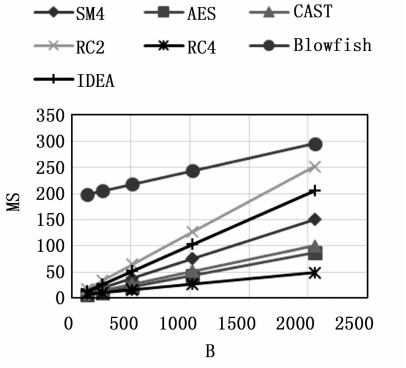

图 4　各算法加密时延与不同明文数据长度的曲线

从以上各图可以看出，各算法的加解密时延随着明文长度增加而增加，并且加解密时延与明文长度成线性关系。其中 RC4 加解密速度远高于其他算法，对于智能单元要求的实时

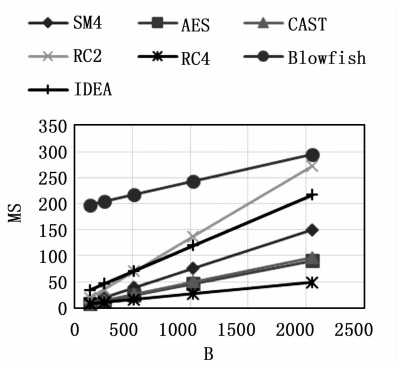

图 5　各算法加密时延与不同明文数据长度的曲线

性较高，虽然市面上还没有存在对其有效的攻击，但其存在理论上的安全隐患。加解密效率仅次于 RC4 算法的是 AES 算法、CAST 算法和 IDEA 算法，其中 AES 算法的安全性较高。加解密效率其次的是国密 SM4，安全性能较高。

2.4　实验结果

通过以上实验结果对比可见：

1）非对称算法加解密速度相对于对称算法较慢，因此，非对称算法一般用于少量数据的加解密，比如密钥协商时对对称密钥进行加解密，或用于身份认证的签名和验签。根据实验一非对称加密算法实验结果可知，国密 SM2 算法具有更高的效率及安全性，更适合在电网智能单元的签名验签和密钥协商过程进行使用。

2）对称密钥由于加解密速度快，效率高等特点，常用于大批量明文的加密。根据实验对称加密算法实验结果可知，RC4 加解密算法虽然效率高，但是存在安全隐患，所以对于智能变电站等对实时性要求较高的设备，推荐使用 AES 算法，并根据实验二，可以选择对于 AES 算法效率没有影响，但具有更高安全性的 CBC 模式加密。

3）根据实验三可知，在满足加解密效率要求的情况下，应尽量选择足够长度的密钥，以保证算法的安全。加解密效率仅次于 AES 的是国密 SM4，安全性能较高。国密算法 SM1 没有对外公开，因此安全性最高。通过实验发现，其加解密效率远不如 SM4 算法。因此，对于配电终端设备和用电信息采集终端设备的算法选型，考虑其安全性能，优先使用国密 SM1 算法，其次选择国密 SM4 算法。当 SM1 算法不能满足设备的加解密实时性要求时，则选择 SM4 算法。

3　小结

本文主要介绍了国内外常用的加密算法以及国内电力行业常用加密算法及安全性能，并主要研究了国内外不同算法的加解密效率，以及加密模式、密钥长度、明文长度对算法加解密效率的影响。对于非对称算法，分析了各自算法的特点和性能，以及产生密钥对所需时延等特点。通过本论文的研究，可以为电力行业等其他行业的密码选型提供一个理论参考依据和实验数据，各行业可根据自己所需的加密效率和安全性能选择合适的加密算法。

参考文献：

[1] Boneh D. Twenty Years of Attacks on the RSA Cryptosystem [J]. Notices of the American Mathematical Society, 2002, 46 (2): 203－213.

（下转第 272 页）

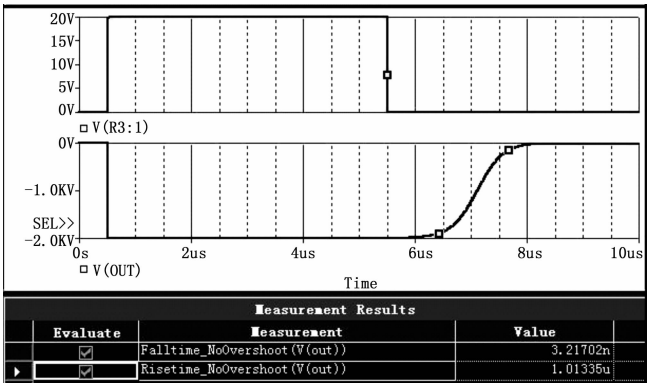

图 5 功能仿真结果

道为输出脉冲，第 3 通道为输入触发，测得如下结果：(1) 系统的延迟时间约为 140 ns；(2) 输出脉冲前沿约为 48 ns；(3) 负脉冲的幅值由超调参数给出，约为 1%，约为 20 伏。

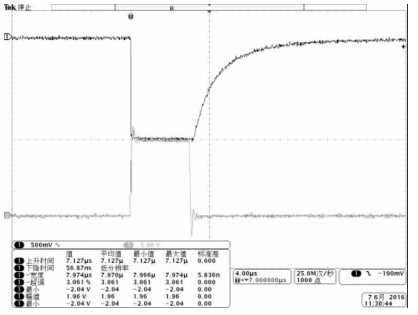

图 6 输出波形与驱动级输出波形

5 小结

本文基于单个功率 MOSFET 固体开关器件和高精度直流电源构建了一种高稳定性高压脉冲电源，用于产生脉冲宽度为

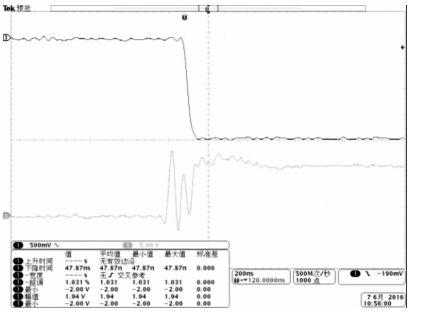

图 7 前沿波形时间放大图

2～10 微秒的脉冲，达到如下指标：输出波形为负极性脉冲、输出幅度约－2 KV、输出前沿约 48 ns、后沿约 7 μs、精度约 1%、固有延迟 140 ns。该系统具有结构简单、稳定可靠、精度较高的优点，可以为特定的光电器件提供优质的控制方式。

参考文献：

[1] 毛久兵，王 欣，唐 丹，等. 低抖动纳秒高压脉冲源研究 [J]. 原子能科学技术，2013，47 (5)：888－892.
[2] 杜继业，宋 岩，罗通顶，等. 像增强器高速选通脉冲发生器 [J]. 现代应用物理，2013，4 (3).
[3] 罗通顶，郭明安，杜继业，等. 远程控制高时间分辨多通道脉冲发生器设计 [J]. 计算机测量与控制，2015，23 (8)：2921－2923.
[4] 王雅丽，毛晓惠，邵 葵，等. HL－2A 脉冲高压电源测量系统的设计与应用 [J]. 计算机测量与控制，2011，19 (9)：2095－2097.
[5] 黄燕华. 可调脉冲电源的研制 [D]. 大连：大连理工大学，2006.
[6] 王庆峰，高国强，张政权，等. 紧凑型可重复运行的高功率纳秒脉冲源 [J]. 强激光与粒子束，2009，21 (6)：956－960.
[7] 刘锡三. 高功率脉冲技术 [M]. 北京：国防工业出版社，2005.
[8] IXYS，Advance Technical Information，IXTK5N250 (DS100280) [Z].

(上接第 261 页)

[2] Somani U，Lakhani K，Mundra M. Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing [A]. Parallel Distributed and Grid Computing (PDGC)，2010 1st International Conference on [C]. IEEE，2010：211－216.
[3] Dubey A K，Dubey A K，Namdev M，et al. Cloud－user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment [A]. Csi Sixth International Conference on Software Engineering [C]. 2012：1－8.
[4] 张永建. RSA 算法和 SM2 算法的研究 [D]. 赣州：江西理工大学，2015.
[5] 王 振. 基于嵌入式实现 SM1 算法的系统设计 [J]. 电子世界，2012 (3)：119－120.
[6] 国家密码管理局. 国家密码管理局公告第 23 号 [EB/OL]. (2012—03—21). http：//www.oscca.gov.cn/News/201204/News—l 227. htm.
[7] 王 翔. 密码学及 DES 算法探究 [J]. 中国科技博览，2015 (29)：31.
[8] Daemen J，Rijmen V. The Design of Rijndael：The Wide Trail Strategy Explained [M]. Neew York：Spring－Verlag，2000.
[9] Feldhofer M，Dominikus S，Wolkerstorfer J. Strong Authentication for RFID Systems Using the AES Algorithm [A]. Cryptographic Hardware and Embedded Systems － CHES 2004：，International Workshop [C]. Cambridge，Ma，Usa，2004：357－370.
[10] Bellaachia A，Portnoy D，Chen Y，et al. E－CAST：A Data Mining Algorithm for Gene Expression Data [A]. ACM SIGKDD Workshop on Data Mining in Bioinformatics [C]. 2002：49－54.
[11] 汪 建，方洪鹰. 云计算与无线局域网安全研究 [J]. 重庆师范大学学报自然科学版，2010，27 (3)：64－68.
[12] 王 磊，范会敏. 一种无线局域网传输短消息的加密算法 [J]. 现代电子技术，2010，33 (4)：119－121.
[13] 胡 亮，迟 令，袁 巍，等. RC4 算法的密码分析与改进 [J]. 吉林大学学报理学版，2012，50 (3)：511－516.
[14] Nie T，Zhang T. A study of DES and Blowfish encryption algorithm [A]. TENCON 2009－2009 IEEE Region 10 Conference [C]. 2009：1－4.
[15] 尚华益，姚国祥，官全龙. 基于 Blowfish 和 MD5 的混合加密方案 [J]. 计算机应用研究，2010，27 (1)：231－233.
[16] Rakheja P. Integrating DNA Computing in International Data Encryption Algorithm 'IDEA' [J]. International Journal of Computer Applications，2011，26 (3).
[17] 李 佳. IDEA 算法综述 [J]. 科技广场，2012 (9)：240－242.
[18] 王 魁，李立新，余文涛，等. 基于 ECC 算法的 TLS 协议设计与优化 [J]. 计算机应用研究，2014 (11)：3486－3489.
[19] 林伟斌. 智能电网环境下企业客户端电力智能单元 [J]. 科技信息，2010 (26)：357－357.