科普：自适应算法 HTTPS 加密

2025 年 11 月 24 日

上周的热门话题是零信浏览器联合阿里铜锁 SSL 成功拿到 IANA (互联网号码分配机构)正式分配的后量子密码混合算法 SM2MLKEM768 编号-4590，无论是铜锁密码学开源项目公众号还是零信密码应用研究院公众号都收到了大量的浏览、转发和点赞，也收到了一些质疑。笔者看到这些质疑充分认识到 HTTPS 加密科普还很不够，今天就继续科普一下，有利于我国普及 HTTPS 加密应用，保障我国互联网数据传输安全。

一、 什么是自适应算法？

笔者已经在上周的博文《解读 SM2MLKEM768 = 4590》科普了 TLS 协议中最“明星级”的参数-TLS 密码套件（Cipher Suites）：这是 TLS 加密的“配方本”，定义了加密通信的具体“配方”：用什么算法交换密钥（key exchange）、加密数据（symmetric cipher）、验证完整性（hash function ）。注册表中列出了上百种套件，从老旧的已经禁用的“TLS_RSA_WITH_RC4_128_MD5”(值 0x0004) 到现代的 “TLS_AES_128_GCM_SHA256”(值 0x1301)。为什么设置这些参数？因为加密算法日新月异，早期的如 MD5 已被证明不安全（容易被破解），所以 IANA 通过专家审查标准化它们，标记“推荐”（Y）、“不推荐”（N）或“已弃用”（D），防止开发者误用弱套件。这确保了全球 TLS 加密实现的安全底线。有什么用途？在浏览器访问网站时，浏览器和服务器会通过“ClientHello”消息协商一个密码套件。如果协商失败，就无法建立安全连接。

关键词是“握手协商”，这就是一个自适应密码算法的实现过程，浏览器和服务器之间协商一个双方都支持的最安全的密码套件和协议实现 HTTPS 加密。也就是说：如果浏览器支持 SM2 算法，Web 服务器也支持，那大家就用 SM2 算法来实现 HTTPS 加密；如果 Web 服务器不支持 SM2 算法，那大家就用国际 RSA 或 ECC 算法来实现 HTTPS 加密。所以，这就能理解国密改造方案是需要同时申请和部署国密 SSL 证书、升级 Web 服务器支持国密算法，和采用支持国密算法的浏览器，或者采购支持国密算法的 SSL 网关，则 Web 服务器无需改造。

二、什么是自适应 PQC 算法？

对于后量子密码(PQC)算法 HTTPS 加密，只有浏览器和 Web 服务器都支持 PQC 算法，才

能实现 PQC 算法 HTTPS 加密。目前国际上通用的方案是传统密码算法(X25519)和后量子密码算法(MLKEM768)混合算法实现 HTTPS 加密，好处是可以仍然使用网站部署的传统密码算法 SSL 证书，只是在密钥封装阶段生成混合共享密钥：一个基于 X25519 的共享密钥，一个基于 ML-KEM 的量子安全的共享密钥，两个共享密码直接拼接成为新的共享密钥，实现了后量子密码算法的密钥保护。这种方式实现了最大的兼容，不支持 PQC 算法的浏览器采用 X25519 算法，支持 PQC 算法的浏览器采用 MLKEM768 算法，这就是算法自适应方式实现后量子密码 HTTPS 加密，是最稳健的 PQC 迁移方案，已成为全球业界的主流方案，全球互联网流量中已有 **51**%流量都是采用了这种混合算法后量子密码 HTTPS 加密，确保了在线隐私数据经得起“未来量子考验”。

铜锁 SSL 和零信浏览器也正是参考了这个国际解决方案，在我国后量子密码算法还没有出台的情况下，采用了 SM2 算法和后量子密码算法 MLKEM768 实现混合算法密钥封装的 HTTPS 加密，这个混合算法就是 SM2MLKEM768，IANA 分配的编号是 4590。如下左图所示，IANA 已经分配了 4 个传统密码算法和后量子密码算法混合算法编号：4587、4588、4589、4590，前 3 个的传统密码算法是国际 ECC 算法 SecP256r1、X25519、SecP384r1，第 4 个我国的商用密码算法 SM2；这 4 个混合算法的后量子密码算法有 3 个都是采用 MLKEM768 算法，因为这个算法的密钥长度适中，加密强度也足够强。有了这个列入国际标准体系的编号，全球浏览器就可以采用 SM2MLKEM768 来实现混合 PQC 算法 HTTPS 加密了。

Value	Description
4587	SecP256r1MLKEM768
4588	X25519MLKEM768
4589	SecP384r1MLKEM1024
4590	curveSM2MLKEM768

如上右图所示，为零信浏览器实现的 SM2 算法+PQC 算法 HTTPS 加密，就是采用了 SM2MLKEM768 算法，在密钥封装阶段生成混合密钥：一个基于 SM2 的共享密钥，一个基于 MLKEM768 的量子安全的共享密钥，两个共享密码直接拼接成为新的共享密钥来实现，实现了后量子密码算法的密钥保护。这种方式实现了最大的兼容，不支持 PQC 算法的国密浏览器采用 SM2 算法，支持 PQC 算法的浏览器采用 MLKEM768 算法，这就是算法自适应方式实现后量子密码 HTTPS 加密，是目前最佳的商密改造和后量子密码迁移方案，并非某些“专家”所担心的没有采用合规的商密算法，这是比单用 SM2 算法更安全的 HTTPS 加密，比单采用 SM2

算法多加了一把锁，能保证采用 SM2 算法加密的数据在量子时代的持续安全。当然，将来我国后量子密码算法出台后只需简单替换 MLKEM768 即可，将实现混合的双算法都是国产密码算法。

为了保障我国互联网数据传输安全，我们不能等到发布了国产后量子密码算法-新一代商用密码后才实现后量子密码 HTTPS 加密，因为现在已经存在“先收集后解密”的安全威胁，绝对不能听信某些“专家”所讲的“只能用 SM2 算法，采用 SM2MLKEM768 算法就是不合规”，这明显是“宁可光屁股冻死，也不能穿别人家的棉裤”的错误思想，也不符合现在我国普遍采用的部署双算法 SSL 证书(RSA/ECC 和 SM2)的 HTTPS 加密应用实践。

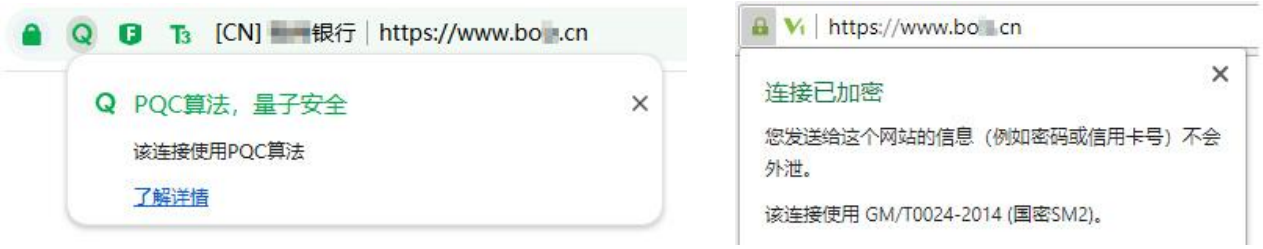
采用 SM2MLKEM768 算法不是“不合规”的，它就是合规的，而且是更高级别的合规—符合国家长远战略利益的合规，是在新时代安全挑战下，对“合规”内涵的一次重新定义和拓展，是在坚持自主可控的根本原则下，积极利用全球先进技术成果，以我为主，集成创新，最终服务于保障国家网络安全和提升国际影响力的战略目标。

三、 零信技术 HTTPS 加密算法自适应是什么样的？

零信技术打造了 HTTPS 加密全生态产品，这就为 HTTPS 加密算法提供了自家生态的无缝自适应支持。零信浏览器和零信国密 HTTPS 加密自动化网关采用的密码算法优先顺序是：(1) 纯国产 PQC 算法(将来)、(2) 纯国际 PQC 算法(将来)、(3) SM2+国产 PQC 混合算法(将来)、(4) SM2+PQC 混合算法、(5) ECC+PQC 混合算法、(6) RSA+PQC 混合算法、(7) SM2 算法、(8) ECC 算法、(9) RSA 算法。这是根据国产密码算法优先和后量子密码算法优先的原则设定的自适应算法选择顺序。

还是先睹为快，看看零信浏览器和零信国密 HTTPS 加密自动化网关是如何实现这个商密算法和后量子密码算法优先的。如下左图所示，这个银行的官网支持不安全的 HTTP 明文方式访问，零信浏览器和其他浏览器都会提示“不安全”。如下右图所示，如果使用 HTTPS 方式访问，则零信浏览器能显示加密锁标识，并显示 **R** 标识，表明网站部署的是 RSA 算法 SSL 证书，采用 RSA 算法实现 HTTPS 加密。

而部署了零信国密 HTTPS 加密自动化网关后，则零信浏览器则采用 SM2MLKEM768 算法实现后量子密码算法 HTTPS 加密，地址栏会显示 Q 标识。但其他不支持 SM2MLKEM768 的国密浏览器访问这个网站采用 SM2 算法实现 HTTPS 加密。这也可以说明此网站已经是商密合规的，并且比商密合规更安全的是同时支持后量子密码算法，表明这个网站已经完成了后量子密码迁移，确保了采用传统商密算法加密的数据在量子时代也是持续安全的。



可以看出：在零信网关同时支持 PQC 算法/SM2 算法/ECC 算法/RSA 算法的情况下，零信浏览器优先采用了 PQC 算法。如果网站仅支持 SM2 和 RSA 算法，则零信浏览器优先采用 SM2 算法，如下左图所示，兴业银行部署了双算法(RSA/SM2) SSL 证书，不支持 PQC 算法，所以，零信浏览器采用 SM2 算法实现 HTTPS 加密。而不支持 SM2 算法的谷歌浏览器则采用 RSA 算法，如下右图所示。

这就是自适应算法 HTTPS 加密，仅支持 RSA 算法的浏览器采用 RSA 算法实现 HTTPS 加密，支持 SM2 算法的国密浏览器采用 SM2 算法实现 HTTPS 加密，支持 X25519MLKEM768 算法的谷歌浏览器采用 X25519MLKEM768 算法实现后量子密码算法 HTTPS 加密，而支持 SM2MLKEM768 算法的零信浏览器采用 SM2MLKEM768 算法实现商用密码和后量子密码算法 HTTPS 加密，同时满足用户商密合规和后量子密码迁移需求。

四、 获得 IANA 编号是实现算法自适应的基础

TLS 1.3 标准的设计是最典型的、最佳的遵循“密码敏捷”原则的先进设计，只需 IANA 增加一个 TLS 支持组协议编号，大家就可以依据这个编号的 RFC 草案开发相应的协议支持系统了，这种机制能快速实现先进算法的及时应用，同时又可以通过算法自适应做到最大程度的兼

容。

我国的商用密码改造非常重要，这是无可争议的。但是，随着量子计算机的快速发展，传统密码算法加密的数据正在面临“先收集后解密”的安全威胁，所以，我国网络安全业界和密码业界必须与时俱进，及时尽快实现商用密码算法和后量子密码算法的混合算法 HTTPS 加密，同时满足关基用户的商密改造需要和后量子密码迁移需要。而 IANA 为 SM2MLKEM768 分配了协议编号 4590 则是加快实现这个急需双改造的应用提供了实现的可能，这绝对是值得业界超赞的大事，是在商密合规的基础上增强了量子安全，绝对应该是我国目前 HTTPS 加密商密改造和后量子密码迁移的首选算法。

SM2MLKEM768 协议编号 4590 的获得意味着该算法成为了全球四个可选的后量子密码混合算法之一，是该算法走向国际应用舞台的“官方身份证”和“通行证”。同时为国内网络安全厂商、云服务商、设备制造商、密码厂商等提供了明确的技术方向。中国企业可以放心地投入资源，在产品中集成和支持该算法，从而推动整个国产密码产业的繁荣和夯实我国互联网安全基石。

王高华

2025 年 11 月 24 日于深圳
