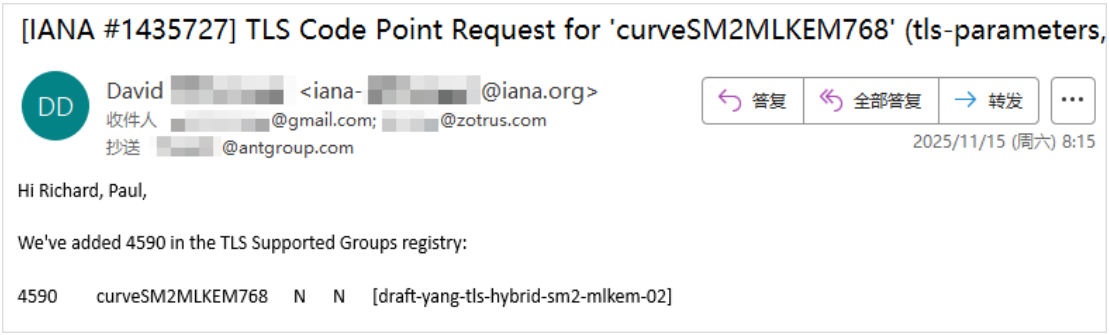
解读 SM2MLKEM768 = 4590

2025 年 11 月 17 日

这是周六早上发生的一件值得大写特写的大事 – IANA (互联网号码分配机构)正式分配了我国密码研究团队申请的后量子密码混合协议编号-4590，标志着我国密码研究团队推出的商用密码和后量子密码混合协议获得了权威的国际标准组织认可，正式成为国际标准 TLS 协议组的后量子密码混合协议之一。这是一件关系到我国互联网数据在量子时代的安全、同时也关系到全球互联网数据在量子时代的安全的大事，必须写篇文章好好讲一讲这事。更有意义的是，这是一次中美科技界在国际 TLS 标准制定方面的友好互动和相互支持行动，值得一书。


[IANA #1435727] TLS Code Point Request for 'curveSM2MLKEM768' (tls-parameters,

DD David [redacted] <iana-[redacted]@iana.org>
收件人 [redacted]@gmail.com; [redacted]@zotrus.com
抄送 [redacted]@antgroup.com

答复 全部答复 转发 ...
2025/11/15 (周六) 8:15

Hi Richard, Paul,

We've added 4590 in the TLS Supported Groups registry:

4590 curveSM2MLKEM768 N N [draft-yang-tls-hybrid-sm2-mlkem-02]

一、 什么是 curveSM2MLKEM768？

SM2 算法是我国制定的一种椭圆曲线算法，同国际标准算法 ECC 和 X25519 是同一类算法，只是不同曲线参数。而 MLKEM 则是美国 NIST 制定的后量子密码算法- FIPS 203，基于模块格的密钥封装机制，该机制能够生成用于数据加密的安全密钥，能够抵御量子攻击。根据密钥长度分为 MLKEM-512、MLKEM-768 和 MLKEM-1024，目前常用的是 MLKEM-768。

全球互联网正在面临“先收集后解密”的安全威胁，也就是，攻击者现在就开始收集互联网加密数据，待量子计算机可用时就可以解密这些机密数据。所以，全球互联网业界和密码业界已经快速行动起来，从 8 月份开始，美欧政府官网、网银系统、大学官网、主流互联网大流量网站都纷纷启用了后量子密码 HTTPS 加密，这个加密方式仍然是基于传统密码算法签发的 SSL 证书，只是密钥封装同时采用了传统密码算法 X25519 和后量子密码算法 MLKEM768，这就是笔者在之前多篇博文中讲过的混合算法-X25519MLKEM768，混合算法的设计提供了“双保险”：X25519 确保当前兼容和速度，MLKEM768 则是抵抗量子攻击，确保了机密数据在现在和量子时代的持续安全。

我国互联网正在抓紧实施 SM2 算法 HTTPS 加密改造，但是即使所有系统都完成了改造，还是无法保障机密数据在量子时代的安全，而我国自己的后量子密码算法还未出台，怎么办？阿里铜锁 SSL 参考国际标准算法-X25519MLKEM768 成功研发并集成了一个商密后量子密码混合算法-SM2MLKEM768，并提出了一个 RFC 标准提案。这是传统密码算法 SM2 和后量子密码 MLKEM768 的混合算法，同样可以用于基于传统密码算法 SSL 证书实现的 HTTPS 加密握手过程中的密钥封装，也就是实现了商用密码+后量子密码混合算法的 HTTPS 加密。

相信读者朋友现在应该能理解了“curveSM2MLKEM768”是什么了，这是 SM2 算法和 MLKEM768 的混合算法，同 X25519MLKEM768 一样用于 HTTPS 加密的密钥交换过程，同时满足了我国的商用密码改造和后量子密码改造的两大紧迫的合规安全需求，这是目前的最佳解决方案。

二、 4590 又是什么？

这就要先科普一下 TLS 参数注册表了。

在互联网数字时代，我们每天上网浏览网页、购物、聊天，都离不开一个看不见的“护盾”—传输层安全协议（Transport Layer Security，简称 TLS）。它就像互联网数字世界的“加密快递员”，确保你的数据在传输过程中不被偷窥或篡改。TLS 的前身是 SSL（Secure Sockets Layer），如今已是 HTTPS 网站的标配。但要让 TLS 在全球无数设备间顺畅工作，就需要一套统一的“规则手册” - TLS 参数注册表。这个注册表由 IANA 维护，记录了 TLS 协议中各种关键代码和标识符，就像交通规则里的红绿灯，确保大家“说同一门语言”。为什么要有这些 TLS 参数？简单说，互联网是开放的，如果没有统一标准，开发者们可能会各搞各的，导致兼容问题或安全漏洞。设置这些参数是为了实现互操作性（不同系统能无缝协作）和安全性（避免弱算法被滥用）。它们的用途呢？从建立连接的握手，到加密数据传输，再到处理错误，都离不开这些参数。

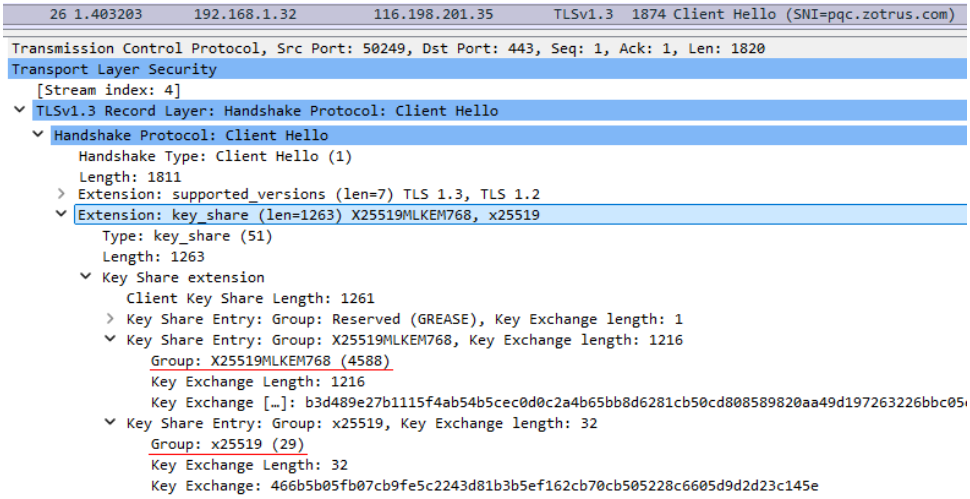
TLS 协议中最“明星级”的参数就是 TLS 密码套件（Cipher Suites），加密的“配方本”，定义了加密通信的具体“配方”：用什么算法交换密钥（key exchange）、加密数据（symmetric cipher）、验证完整性（hash function）。注册表中列出了上百种套件，从老旧的已经禁用的“TLS_RSA_WITH_RC4_128_MD5”(值 0x0004) 到现代的 “TLS_AES_128_GCM_SHA256”(值 0x1301)。为什么设置这些参数？因为加密算法日新月异，早期的如 MD5 已被证明不安全（容易被破解），所以 IANA 通过专家审查标准化它们，标记“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。

第二个重要的参数就是 TLS 支持组（TLS Supported Groups），这是指定密钥交换的数学“基石”，如 x25519（编号 29，推荐的曲线）或 ffdhe2048（编号 256，Diffie-Hellman 组）。为什么设置这些参数？就是要锁定安全算法。有什么用途？在现代 TLS 加密中用于“前向保密”（即使服务器密钥泄露，旧会话也是安全的）。

重点讲一下 IANA 新增的后量子密码算法支持组编号。编号 512 /513 /514，分别是 MLKEM512 /MLKEM768 /MLKEM1024 的编号，编号 4587 /4588 /4589 则分别是传统密码椭圆曲线算法和后量子密码算法 ML-KEM 的三个混合协议 SecP256r1MLKEM768 / X25519MLKEM768 / SecP384r1MLKEM1024 的编号。IANA 在 TLS 支持组注册表中新增了后量子密码的这些条目，就是为了实现混合算法后量子密码 HTTPS 加密。其中目前常用的 X25519MLKEM768 编号为 4588，通过 IANA 标准化，它避免了实现冲突，标记为“不推荐”（N）表示仍处于实验阶段，但鼓励早期采用以推动生态迁移。有什么用途？在 TLS 1.3 的 HTTPS 连接中，客户端通过“supported_groups”扩展提出 4588，服务器若支持，便在密钥共享阶段生成混合密钥：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，使得攻击者即使窃取了服务器加密密钥，也无法使用量子计算机解密历史会话（增强前向保密）。这已经成为浏览器的主流方案和事实标准，全球互联网流量中已有 47%流量采用了混合协议后量子密码 HTTPS 加密，确保了在线隐私数据经得起“未来量子考验”。

目前四大浏览器(谷歌 Chrome、微软 Edge 等)和零信浏览器支持的 X25519MLKEM768 协议可以通过抓包发现，如下图所示，可以看出混合后量子密码算法 X25519MLKEM768 的编号是 4588，传统密码算法 X25519 的编号是 29。



而 4590 则是刚刚获得 IANA 批准的后量子密码支持组协议-curveSM2MLKEM768 的编号，有了这个编号，上述讲解的商用密码算法混合后量子算法实现的混合协议 SM2MLKEM768 才

真正成为了可用的协议，也就是正式成为了交通规则里的红绿灯中的一种全球可识别的信号灯，为我国基于 SM2 算法 SSL 证书实现商用密码和后量子密码混合算法 HTTPS 加密提供了可行的实施基础，也为我国正在制定的《传输层密码协议（TLCP）2.0》支持 TLS 1.3 和后量子密码算法提前铺平了全球通行的道路。

三、 补充介绍 RFC 8998 和相关 IANA 编号

RFC 8998 是阿里铜锁 SSL 在 2019 年 8 月干的一件大事，直到 2021 年 3 月才正式获得国际标准组织 IETF(互联网工程任务组)的批准并分配 RFC 标准序列号-RFC 8998：商用密码 TLS 1.3 密码套件，这个标准使得商密 HTTPS 加密可以使用先进的 TLS 1.3 协议来实现。为何需要 TLS 1.3？因为 TLS 1.3 不仅禁用了不安全的静态 RSA 密钥交换，支持前向保密，更重要的是设计机制遵循“密码敏捷”原则，为后续后量子密码算法和协议提供了实现的基础。所以，商密 HTTPS 加密必须支持 TLS 1.3，RFC 8998 的确立意味着 SM2 算法正是成为国际 TLS 1.3 标准支持的算法之一，这是 RFC 8998 的重要意义。有国内专家认为这个标准只是 Informational 分类而否定其国际标准的地位，这是错误理解了 RFC 标准。

RFC 标准分为三类：标准跟踪类、非标准跟踪类和当前最佳实践类(BCP)，其中标准跟踪类又分为建议标准(Proposed)、草案标准(Draft)和正式标准，目前只有很少部分能成为草案标准，成为正式标准则更是非常少，互联网上被广泛使用的协议规范大多数处于建议标准这个级别。而非标准跟踪类又分为实验类(Experimental)、情报类(Informational)和历史类(Historic)，实验类是指使用范围有限的协议，已经为超过 200 亿张 SSL 证书从 2013 年就开始使用的 RFC6962 (证书透明)也只是实验类标准；情报类是指一些有关特定议题的互联网社区的信息，并不代表是社区共识和建议，仅供下一步考虑和验证是否成为实验类标准，RFC 8998 属于这一类。而历史类则是已经没有任何价值的历史标准。这是 RFC 2026 定义的互联网标准制定流程的各种不同的标准分类。简单讲，只要能拿到 RFC 标准编号，最终是否能成为正式标准需要相关产业界达成共识和应用支持。而成为了情报类(Informational)标准已经起到了制定标准需要达到的基本目的-实现应用的互操作(produce interworking implementations)，成为交通规则中大家都能识别的红绿灯信号。

RFC 8998 还有一个重要的贡献是拿到了 IANA 分配的两个商用密码算法 TLS 密码套件编号：TLS_SM4_GCM_SM3 (值 0x00C6)、TLS_SM4_CCM_SM3 (值 0x00C7)，一个 TLS 签名方案编号：sm2sig_sm3 (值 0x0708)，还有一个是 SM2 算法的 TLS 支持组编号：41 (curveSM2)，就是同本次分配的 4590 同类协议编号，用于密钥交换，这三个编号使得 TLS 1.3 国际标准真正能支持 SM2 算法实现 HTTPS 加密和为中国后量子密码算法的国际化打下了标准基础。

目前 360 浏览器已经支持 RFC 8998 标准 HTTPS 加密，零信浏览器也将在支持商用密码和后量子密码混合协议 SM2MLKEM768 的同时支持 RFC 8998，因为只有实现了 RFC 8998 的商密算法支持 TLS 1.3，才能实现 SM2MLKEM768 混合协议 HTTPS 加密。

四、 中美科技界在 TLS 标准制定合作大有作为

本次成功把后量子密码的“中国方案”纳入国际标准体系，不仅证明了中国密码界能够跟进国际前沿技术，更是具备了源头创新和参与制定国际标准规范的能力。这是相关产业多方协作的成功：铜锁 SSL 社区提出并撰写了 SM2MLKEM768 的 IETF 草案，铜锁 SSL 按照草案实现了中国商用密码算法和美国后量子密码算法的混合密钥交换机制，零信浏览器则是率先支持这种混合机制实现商用密码和后量子密码混合算法 HTTPS 加密，为标准草案提供了落地的应用场景和真实标准需求，这是通过 IANA 专家审核的关键，因为一个标准如果没有落地应用的实际需求是没有价值的。这种“密码开源库+产业应用”的紧密联动，是技术创新最终产生价值的典范。

更值得一提的是：在申请材料上，我们是从保障全球互联网安全的大局出发，强调了中美密码算法特别是后量子密码算法互为备胎的重要性，因为谁也不能保证后量子密码算法一定是真正抗量子安全的，目前认为的安全只是理论安全，还没有量子计算机可以用于验证算法的安全。所以，全球互联网安全不仅需要美国主导的后量子密码算法，而且也需要“中国方案”，为全球互联网安全提供宝贵的技术多样性和更多可选方案，大大增强了全球互联网 TLS 生态的韧性和安全性，因为全球只有一个互联网。相信正是这个站在保障全球互联网安全的高度提出的解决方案打动了 INAN 审查专家，让“中国方案”顺利成为了保障全球互联网 TLS 流量安全的可选方案之一，中美科技界在 TLS 标准制定合作大有作为。

王高华

2025 年 11 月 17 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 238 篇(共 70 万 9 千多字)和英文 102 篇(13 万 9 千多单词)。