方圆

Around

由灵光一现和持续热爱驱动
的服务器非官方期刊

10
2023
总第 21 期

封面：凛泉谷
摄影：nuo_mi_

头条
24Kgule 30266
二三年的最终假期，
于秋风习习中落幕

杂谈
Meapuchino
MC 中的
小品建筑浅考

你问我答
Code_C431
夏天的末地，
夏眠的猫猫

发行 抹岚报社

方圆
Around

2023 年 10 月刊
总第 21 刊

凛泉谷　池塘
摄影：nuo_mi_

主编：30266
执行主编：24Kgule

编辑：BCMonomial, send_9
审校：Dong_Bo_Jue_233
排版：Aunst
摄影：nuo_mi_

版式设计：Aunst
Logo 设计：Arthals

社长：30266
副社长：Aunst, BCMonomial

方圆　2023 年 10 月

主办：抹岚报社
发行：抹岚文宣部
（零洲西北地区抹岚市市南区府前路 3 号西栋 201）
期号：#21 / 2023-10
发行范围：RIA Zeroth Minecraft 服务器（内部发行）
定价：0
出版日期：2023-10-21
书号：C-4-2023-10（莉亚书籍刊物出版物统一编号）
页面尺寸：210 毫米 ×297 毫米（A4）

II 目录

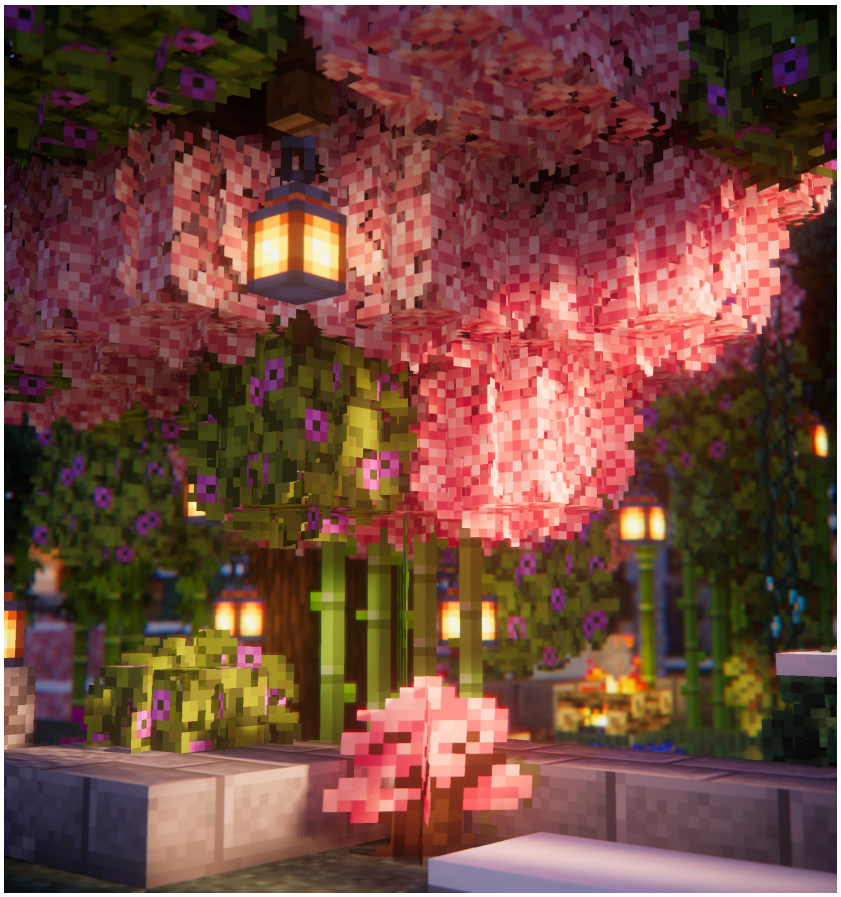
目录

封面故事

30266

本期的插图选材自零洲的 212 号鸟居凛泉谷。凛泉谷位于零洲西北大陆最南端的雪原上，被西界海和列宁湖夹在中间，南接西沙洲。凛泉谷为一座日式小镇，虽然在卫星上这座小镇规模不大，但只有实地到访后才发现，这座小镇的细节十分走心。漫步其中，就会被温馨而神秘的氛围包围着。

本期的摄影师是糯米，非常感谢糯米拍摄的好看图片。我们从中选出了 4 张备选封面。



映入眼帘的是新版本中添加的樱花树。这棵樱花树位于小镇主干道北端的宅院外，树荫下是一方小池塘。初升的太阳刚好照耀在樱花树上，昭示着这座小镇的生生不息。这幅图片相当优秀，但并未展现出明显的聚落特色，因此它被选为了本期目录的背景图片。

图 2 的拍摄地点与图 1 相同，只是角度有所改变。这张图片的主体为池塘。夜色之下，池塘波光粼粼，让人想起《记承天寺夜游》中的“庭下如积水空明，水中藻、荇交横，盖竹柏影也”这写景名句。这张图片的意境也相当优秀，但还是因为未能展现出明显的聚落特色，故落选了封面之位。

图 3 拍摄于凛泉谷最北端的神社中。这张图片拥有以上两张图片的优点，而且也很好地展示了聚落的特色。背后山坡的皑皑白雪与近处植物的姹紫嫣红形成了有趣的反差，令人印象深刻。这幅图片一直被认为是最有希望当选封面的图片，直到获得一致好评的图 4 的出现，才让图 3 不幸失宠。

图 4 摄于凛泉谷主干道。这张图片让人眼前一亮，巧妙的构图展现了凛泉谷城区的烟火气，同时也表现出了凛泉谷城区特有的闲适之感。这幅图片既表现出了凛泉谷的独特特色，又易于安排封面元素，因此这张图片顺利当选了本期的封面。

至此，本期的封面故事就结束了。

二三年的最终假期、于秋风习习中落幕

头条 • 24Kgule 30266

回想二〇二三年的最初一个月，那种对未来的未知和恐惧又浮现出来。但好在回忆及时停止，思绪又返回了当下。举目四望，世界似乎又回到了三年大疫之前的状态，但总有中说不上来的不协调感。现代社会是个很脆弱的整体，环境稍有变化就有可能造成变故，面对疫情这种如山倒的灾难，现代生活更显得渺小。疫情打破了社会脆弱的平衡，即使罪首逐渐消匿，但若想恢复这样的平衡，人们仍有很长的路要走。

我对着屏幕右下角的日期发呆，突然惊醒——原来今年已经过去了四分之三，地球也将要绕着太阳绕过一整圈。今年最后的假期已告结束，未来在远处向着我们招手。见证了诸多历史的我们，面对未来的机遇和挑战，会更有直面未来的底气。

笔者对 2020 年的中秋国庆九天假期仍记忆犹新，没想到三年后的 2023 年又逢双节长假，今的九天假期，RIA 举办了第二届迷你社博会和「伐桂行动」活动。MiniExpo2 延续第一届迷你社博的随性风格，而伐桂行动则是之前中秋节抓兔子活动的升级版。

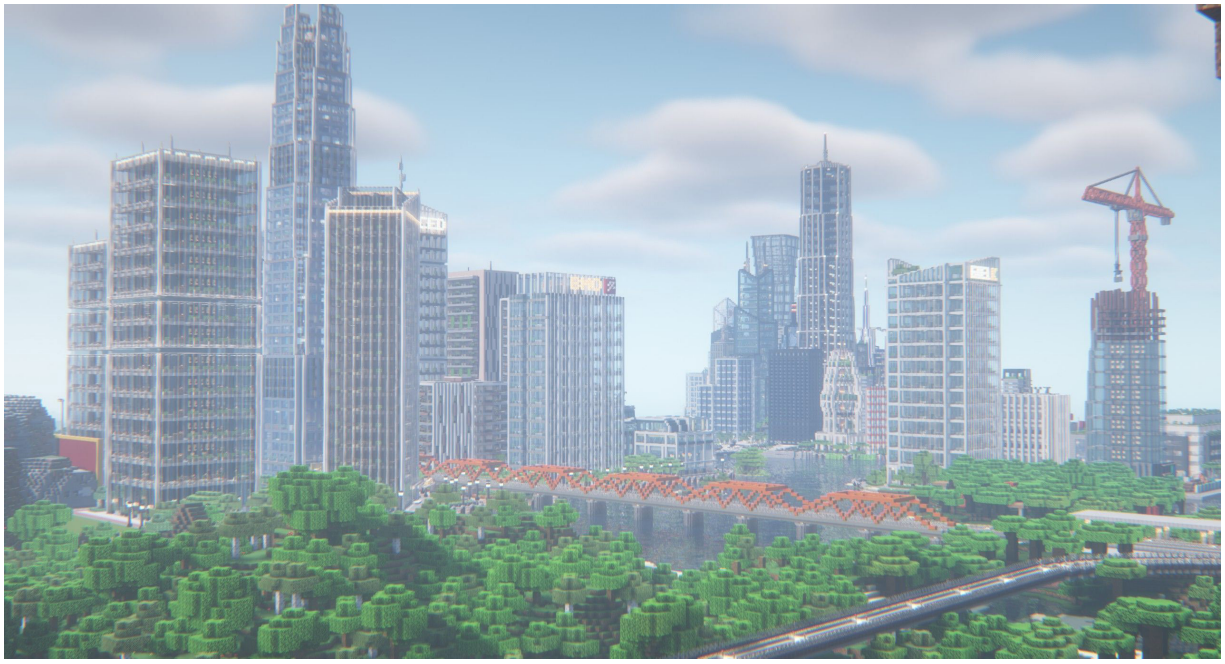
第二届迷你社博会举办于零洲 192 号鸟居湛蓝遥阔附近。本次的 minipo 持续三天，在国庆节的假期中为大家提供了和其他玩家互动交流、参与新鲜活动的平台。minipo 作为春秋季定期开展的活动，为想在 RIA 世界中稍作放松，但是又比较缺乏时间的玩家提供了轻松随性的舞台。本次在春季的 minipo1 的基础上，新增加了赛马比赛等小游戏，更充实的活动内容也体现着布展者的丰富热情。

右：赛马活动宣传图

下：MiniExpo2 地图

但是不可避免的，毕竟 RIA 目前还处在滑行期，参加的人数相较于寒暑假也有所减少，毕竟即将到来的期中考试和大大小小的任务工作仍是最为重要的。

「伐桂行动」于 9 月 30 日晚八点举行，在剧情上承接了往年的中秋活动，整体内容形式上更接近于不久前的除声行动，玩家多人组队，于后土向未知进发。DeerEyes 制作了详细的活动攻略 为后续来参加自主挑战模式的玩家提供了许多有用的信息。



10 月 9 日，零洲的第 203 号鸟居——际云已评为赤级，际云位于零洲西南角。始建于去年 11 月的际云是一座巨大的现代建筑群，并成为了最年轻的赤居，也是新赤居标准评出的第一个赤居。新的赤居评判标准从「规模」、「环境」、「建筑」和「文化」四个方面量化评判，以更加客观、易量化的视角给出发展评级。

寒露已至，深秋已达。冬天还有不到一个月就将统治整片大地。休整过后，旅途重启。在秋天最后的日子里，我们终于重新发现了自己：原来我们内心深处真的相信世界会好起来。

夏天的末地，夏眠的猫猫

你问我答 × Code_C431 — 《方圆》2023 年 10 月

猫猫都喜欢玩什么游戏，为什么喜欢它们?

匿名

喜欢玩的游戏比较乱七八糟的，什么种类都有，唯独不喜欢 pvp（物理手残，菜的）比如 warframe，一个枪战游戏，但重点不在打枪而是爆肝刷材料的同时和大伙聊天，这游戏我在 steam 的记录能有 1w 小时（主要是在用 steam 打开之前都是独立客户端，没算进去的更多），主要是认识的全是华人而不是国人，朋友真的是游戏最高的配置

还有泰拉瑞亚，以前和朋友玩过，

但是后面因为一些现实原因朋友们都忙自己的生活去了

星露谷物语，前段时间去摸了一下，养成类里为数不多比较喜欢的一个，

经常玩完发现几个小时过去了（体验比较综合，养成，战斗，下矿也算是肉鸽？）

以撒的结合系列，经典肉鸽，背后的故事更有意思，

就是宗教暗喻类的 + 一定的血腥色彩相对而言比较微妙

魂 3，哦它是我喜欢看实况，趁机补票的，

自己只打得过古达（笑死），魂系列就不用说了很经典

当然手游也有，星铁，原，明日方舟，

甚至是阴阳师，碧蓝航线，赛马娘，坎公骑冠剑，奇迹暖暖……

网游也有 eve，FF14，魔兽（非常早年了），激战 2 等经历

对于我来说，无论是手游，单机又或者是网游，都是游戏，没什么区别也不分贵贱，有也只有我喜不喜欢和会不会玩的区别，而我玩的话很多时候喜欢的也是它们的故事或者其玩法，是我那时候比较中意的。

猫猫每天处理那么多服内事务不累吗 awa

匿名

喵？其实并没有大家想象中的那么多，只不过因为它们都是要持续盯着，或者是大家都忙，所以就帮忙盯上啦，毕竟大家都有自己的生活就我特 别 闲，所以也不会很累（催鱼头特别开心 x 催小片 3 更开心了）

431 最喜欢的事情是什么

匿名

我最喜欢的大概就是做饭，做饭比读书还要喜欢多一点点，做饭的话对于我来说就像是各种奇妙的组合在自己的手上变成了美味的菜式，而且因为从小就学会了以至于会的花样挺多，包括但不限于自己包饺子包包子或者是基础煎炸炒蒸煮以及著名广 door 人都会的煲汤煲凉茶（草）

你是笨蛋嘛

匿名

我是笨蛋，真的，没有比我更笨的末影猫猫 w 这么笨不好吃 w

听闻您住在孤独峰，那么您和 NashBan 是什么关系呢，是朋友吗出了远境活动，我就没见到过活的鲨鱼了，去过孤独峰一次，但是当时她在挂机，好像她有 3D 眩晕，那么平时也都是在挂机吗？

孤独峰听起来很像小波奇的聚集地，很像鲨鱼的感觉，这个名字在人口暴增 2000% 后真的会改吗？

河川也住在那里，他以前就会到处撅人了吗？

你们是怎么合作建设孤独峰的呢？

wiki 上写 431 的建筑技能只有 1，那么除了建自己的家之外还建过什么公共建筑，比如雕塑之类的

（第一次提问，问的有点多而且都只是我个人感兴趣的话题，431 老师可以选择性回答）

匿名

算是朋友？也给鲨姐送过鲑鱼，聊过几句（悄悄投喂凶猛鲨鱼），她的话确实是 3D 眩晕挺严重的，所以确实日常挂机（而且常年活跃榜前列 233333）

孤独峰名字不会改的，因为其实本质上也符合，指孤独峰的人经常神龙见首不见尾，多少带点自闭属性（？）

河川的话我不是很熟，这个问题可能要询问孤独峰的黑猫（这里艾特一只 kz）

合作建设的话，孤独峰的话也会有自己的小群，平常都是安格姐在指挥（虽然但是我们很咕，什么是赤？）

我的话建筑确实只有 1，冰道上面那个巨型蘑菇就是我的杰作（特别丑而且还未完工，寄），但除了自己家以外我还真做过别的，除了 expo4 花了 12h 清理了墙面以外就是 fst 主城以及初生水殿的部分内饰了（等下上工算吗草）

倒悬、隐秘、明辨

你问我答 x magic_owl233 — 《方圆》2023 年 10 月

猫头鹰虽然是运营社成员，但似乎存在感很低？猫头鹰在运营社有参与什么项目吗，为什么存在感这么低

匿名

这是个好问题，我相信有很多人都有这样的疑惑。首先来日啊的首要目的是觉得氛围不错来养老，所以一般我都是自己玩自己的，社交圈非常小所以看着就透明，之后加入运营之后基本都是幕后工作，再加上本身就透明，关注的人更少了，所以没存在感正常，要说参与什么项目的话，基本上绝大部分项目我都有参与讨论，一些项目也有直接实践，再就是提出一些新的项目提案，总之人本来透明，干的活也不在前台，所以我是“隐形鸟”

怎么和 DumFish 用情头！画得还怪好看的

匿名

因为甜蜜双排 x 头像是达姆画的，欢迎向达姆约稿

麻吉克嗷会下蛋吗

DumFish123

在你头上下蛋

猫头鹰腿长吗　猫头鹰穿毛裤吗　猫头鹰白天睡觉吗　猫头鹰晚上困吗

匿名

猫头鹰没有腿，只有毛裤，在树上靠毛裤毛挂住树枝站立，猫头鹰是黄色眼底，想什么时候睡就什么时候睡，比如现在！ ZZZzzzzzzz…

写一首关于感情的詩

匿名

咕↑咕→咕↑咕↓咕→咕→，咕↑咕↑咕↑，咕→咕→咕↓咕↑，咕→咕→，咕↓咕↓咕↑（猫头鹰语）

余志枭

听书七夜之四

小说 • A_lavender

夜色压城，月光如泻，映照出乌云的形状。空中云月，一黑一白，棋大如斗，以天地为盘，化而为子，密布其间。时而乌云涌动，时而辉月皎洁，黑白之间的无声缠斗，在万籁寂静的时刻上演。一身墨色的青年躺在城中最高的屋檐之上，看着这一出自然之间的博弈。远处传来打更的声音，他毫不为之所动，容身与黑暗之中，享受只属于自己的静谧时光。

檐角铜铃忽然无风自动，发出清脆的声响，一只白鸽扑棱着翅膀，落到他肩头。白鸽左脚绘着奇特的火焰图案，右脚绑着一小卷纸。黑衣男子坐起身来，取下书信，将白鸽放走了。在他低头看书信之时，另一青衣男子悄无声息地翻身上屋檐，并肩坐在他身旁。黑衣男子将信看完，暗力一催，书信顿时化为粉碎。

“这次的任务如何？”闯来的不速之客问道。黑衣男子没有说话，只是略微点了下头。

“我就知道你会答应，你这挑三拣四的毛病，从来就未改过，永夜楼来者不拒的规矩，你怕是根本没放在心上。”“我只杀该杀之人，别的，与我无关。“说着，黑衣男子站起身来。“……这次任务极其艰难，切记多加小心，林。”被称为林的黑衣男子待他说完，纵身离去之时，回头说道：“这是我最后一次任务，成功与否，我于永夜，再无拖欠。”青衣男子窒了一窒，一时间不知道还说什么。林的身影消失在黑暗中，青衣男子孤身一人站在檐角，心下顿生苍凉。

“……别了，兄弟。”

半月之后，苏杭商会迎来一名柔柔弱弱的账房先生，自称姓张。商会正好要北上买卖，张先生便随船队一路北上。只是张先生这柔弱的体质，哪里受的住海浪的颠簸？一天没到，便吐得晕头转向。“先生，您要不吃点什么药？”船夫好心提醒道，脸上却憋着笑。“不，不必了……小生吃了那些药也没什么用……”张先生扶着船板，虚弱地说完，便东倒西歪地进了舱房，留下身后一片窃笑声。

夜里，粒米未进的张先生肚中一片哀嚎，翻来覆去睡不着，便决定起身去厨房找些吃的。他才将冷馒头放入嘴中，船身便传来一阵剧烈的抖动，馒头落地，张先生脚下不稳，也滚倒在地。“哎哟……到底是怎么开船的……”张先生扶着腰想站起来，又一次更强烈的抖动传来，张先生随着船体晃动在地上滚来滚去。

“船破了！大家快逃啊！”外面传来惊呼声，张先生听得声音，连滚带爬地起来，跑出船舱。只见甲板上站满了惊慌失

措的船夫，船体破开一个大洞，正在往内灌水。“这这这是怎么回事？”早上的船夫看到他，赶紧将手中的小木桶塞到他手上：“先生，黑沙帮的人来抢劫了，您还是快逃吧！”说完，船夫一个猛子扎进海中。张先生抬头张望，果见不远处海面数不清的船只逡巡，船上人头攒动，映照的四周灯火通明。

这黑沙帮是江浙一带最大的水匪帮派，杀人掳掠，无恶不作，因来去迅猛，行踪不定，连官府也无法查证到据点。先前苏杭两地商人捐赠钱财，召集天下义士，狠狠地打击了一下黑沙帮，这才磨灭了其嚣张气焰；黑沙帮很是销声匿迹了一阵子，直到最近突然重现江湖，如今的黑沙帮势力滔天，进退有度，听说全是新来的军师的功劳。

此时甲板上船夫已跳海大半，张先生紧紧抱着水桶，一副欲哭无泪的表情。“小生，小生不会水啊！”黑沙帮靠拢商船，水匪们蜂拥而上，张先生被登船的水匪一顿揍，并蒙住双眼绑住手脚带回营寨。

“老大，这次可是大丰收啊！”张先生听到有人谈话，便支起耳朵来仔细听着。“好！军师的情报果然准确，这次可是报了上次的一箭之仇！哈哈哈哈！”粗犷的笑声震耳欲聋，四周的人也跟着大笑起来。张先生不自然地向后挪了挪身子，立即听到那男声“嗯？”的一声、“怎么还有个活的？”“大当家有所不知，此人是新来投靠商会的一个账房先生，我此前调查船队行程时，已经调查过此人，身家清白，和那帮人并无关系。在下想到寨中尚缺管账的先生，便嘱咐二当家，将此人活捉回来。”一个斯文的男声说道。“好！不愧是军师，想得就是周到！老子今天好好赏赐兄弟们，大家不醉不归！”此言一出，欢呼声响彻云霄。

张先生被人如拎小鸡一般提起，扔到一个房间。他略微一挣扎，发现已经被松了绑，支撑着起来取下遮眼布，看了看四周。“唉，小生此番便真是误入贼窟，为虎作伥了。”门外的看守听到这酸气扑鼻的话语，大笑两声，也不担心他逃走，自顾自喝酒去了。看守直到深夜才酩酊大醉的回来。他想起那白白嫩嫩的账房先生，心中燃起无名烈焰。自己已经多久没沾过女人了？看守脑子浑浑噩噩，只想找个地方发泄，便一脚踢开房门：“兔儿爷，哥哥我来……”一句话尚未说完，看守只觉脖上一凉，便再也发不出声来，惊恐地倒地而亡。眼前，伪装成账房先生的杀手林手握匕首，眼神冰冷。他跨过温热的尸体，摸索着向着黑沙帮首领沙角的房间而去。

林此次的任务，正是刺杀黑沙帮首领沙角。为了知道沙角的藏身之所，他暗中调查沙角，发现黑沙帮曾与苏杭商会有过接触，便打算伪装成不会武功的账房先生想办法伺机潜入，原本应该大费周折的事，却不想阴差阳错之间，竟进展得如此顺利。这可得感谢你的好军师。林心中暗道，不多时便找到沙角的房间。沙角房前守卫如

云,林只好从后窗潜入,慢慢摸到沙角床前。

他抽出匕首，只见寒光一闪，霎那间便到了沙角胸口。此时沙角却霍然睁眼，闪电般伸手，抓住了林的手腕。“想杀我的人，坟头草已经几丈高了。”沙角狰狞一笑，林只觉手腕一股巨力传来，发出了骨折的脆响，林心中大惊，此人气力甚大，需速战速决！思绪转瞬即逝，林反手化指，一招“无形指”直点沙角双目。此指无形有形，虚幻化影，沙角看不清招式，一招击中，沙角的右眼立马变成血洞。疼得他撒开了手。

门外守卫听得动静，破门而入，团团围住了林。“给我杀了他！剁了去喂鱼！”沙角捂住眼睛，大声嘶吼着。守卫拔刀蜂拥而上，林眉头微皱，身形闪动，右手食指射出一道青气，恰将一名上前的守卫胸口射穿，乘势夺过其手中长刀，持刀一抖，挽出数片刀花，将来人兵器尽皆隔开，随后微退一步，手中长刀划出一道圆弧，两式之下，已有数人丧命。黑沙帮众人平日如何见得此等绝妙刀招，一时之间，竟不敢上前。“一帮蠢货，怕什么，他只是一个人！”沙角怒吼道。“仇陌，黄岩，你们上，给我拿下他，这次抢来的财物我分你们一半！”沙角对着门外两名身材高大之人喝道。两人相视而笑，手提长刀加入了战团，但见一人持刀高高跃起，手中兵器直劈林的颈部，一人贴地滑行，持刀斜撩林的下盘，一上一下，封住了林的退路，却见林双臂一张，行云流水般向后纵出，避开了两人的凌厉攻势。经此一下，周遭黑沙帮帮众方才回过神来，继续涌向林周遭，一时间刀光剑影闪烁，铿锵声不绝于耳。只是林已然负伤，又有高手围攻，唯有凭借精妙轻功，腾转挪移，但百招过后，渐渐气力不支，逐渐便落得下风。

恰巧此时，黑沙帮的军师也闻声赶到。沙角瞪着剩余的一只眼睛，嚎叫道：“军师来得正好我被这野小子伤了右眼，快快拿了伤药给我。我要生撕了这小子！”年轻的军师吩咐手下拿来药箱，径直走到沙角身侧后方的桌台旁放下药箱。“军师你快些个，可疼死我了！”“放心，大当家的，马上，你就再也不会痛了。“什……”沙角感到胸口一阵刺痛，猛然低头看向胸口。只见一把闪着幽光的匕首插在胸口之上。而手握匕首之人，正站在自己身后。他喉咙深处发出一串浑浊的呜噜声，便轰然倒地。“沙角已死！尔等还想要陪葬吗？！军师大喝一声，翻手便朝着守卫掷出暗器，只听的“嗖嗖”几声，两名守卫应声而倒。原本还在和林缠斗的守卫纷纷丢下刀，四散逃走。黑沙帮一下子乱了套，沙角的房间也只剩下军师与林二人。

林喘息一声，跌坐在地上。军师提着药箱走到他跟前，拿出药物，开始替他包扎伤口。”你……为何？“林满脸写满惊讶。军师根本没有回答他的问题。“我还以为永夜楼皆是之辈，没想到你不擅这种手段，反而是个一等一的使刀好手。只是，你决然猜不到刺杀任务的雇主便是我吧。”军

师微微一笑，笑容中满是狡黠。“我十四岁那年,沙角因一宝物害我全家,这些年来,我忍辱负重带在他身边，苦苦寻求报仇的机会，却未想到此人防范之心极重，连拜把兄弟都从未真正信任过，更何况我这个凭空出世的军师了。”“无奈之下，我也只能雇佣你这等永夜楼高手为我创造机会,沙角全部注意力被你吸引而去之时，便是我下手的绝佳时机。”林盯着军师的眼睛,他眼中满是平静，波澜不惊，仿佛刚才之事从未发生一般。此人年纪轻轻，心计手段竟如此厉害。军师替林包扎好伤口，说道：“我想壮士既然接下这任务，就该明白自己将面临多大的危险。付出将会有回报，酬金我会尽数交给你的。”林摇了摇头。“我已不是永夜中人，报酬不必给我。”我欠她的，都还清了。从此我二人，再无瓜葛。

林闭上眼，少女风华卓绝的容貌又出现在眼前。

“呵，人人都有过去，看来壮士也是性情中人。既然你不再是永夜中人，不妨和我一同收服黑沙帮，自立为帮，过些逍遥快活的日子，将过去的不如意统统抛诸脑后，如何？”林将手中沾满血的利刃扔开，望着军师的盈盈笑脸，陷入沉思。何妨？离开永夜，离开兄弟们和她的身边，自己本就是孑然一身，天地茫茫，再无自己的容身之所。半晌，林不置可否地点点头。军师眼中亮起光芒，笑道：“在下顾炎封，敢问兄长如何称呼？”“兄……”林的眼睛暗淡了下来。“唉，是在下孟浪了，刚见面便唤您兄长，还请莫要见怪。”“请莫要自责，是小可的过失，让您误会了。在下余志枭，请多指教。”

从此，世间再无杀手林。他自黑暗中涅盘而出，心中光明，再无迷茫。

MC 中[1]的小品建筑浅考

杂谈 • Meapuchino

小品建筑一般被定义为具有一定功能，或者具有装饰、美化作用的，从属于某一建筑空间环境的小体量建筑。

而其中又以兼具实用功能和园林美化的园林小品最为人熟知——体量较小，造型新颖、往往不具有可供内部游览的空间，却兼具了园林技术要求和造型美感要求，成为了现在许多城市公园里的一道独特风景线。

不过也正是因此，在 Minecraft 中提起“建筑小品”，大家第一时间想到的是一个更为耳熟能详的词：外饰[2]。

诚然，这种联想是不无道理的——甚至与建筑小品的本身定义十分贴切，毕竟外饰本身就是作为一种“给建筑外部做装饰”的概念出现的。

但这种简单的，划等号式的定义却忽略了一个问题：试想一下，一片人工制造出来的童话森林，其中并没有类似于村镇小屋的建筑（群），那么这片森林可否被叫做外饰呢?

显然是可以的。因为从更大的整体空间来看，这片人造的森林存在于开放空间，又以装饰和美化功能为主，只是体量会比“小品”大上很多——往往是几十个甚至更多区块的建设量。

那么 Minecraft 中的“小品建筑”又该从何而定义呢? 这可能要从 MC 小品类建筑的发展历程说起。

在早期的 MC 版本里，建筑方块和自然方块[3]的种类较为匮乏，建筑玩家们的精力也主要集中在对建筑本身的研究上。随着时间的推移，MC 建筑圈里大致形成了中世纪、欧式、现代、中式等几大建筑派系。但在这一段时间里，出现了一批对功能性建筑进行装饰的“Building Tutorial[4]”——他们以对现有的建筑里一些元素进行装饰为中心，例如装饰附魔台、装饰地狱门[5]等。

而在这一时期，同样也出现了一批 MC 中园林小品的雏形——简单的石质建材和木制建材，已经足以让一些充满想象

* 若无特别说明，本文所有注释均为原注

1 如无说明，特指 Minecraft 国际版，即更新至 1.20.2 快照版的版本。

2 “外饰”的定义此处来源于对在视频网站“bilibili”中搜索“mc 外饰”词条得到的结果进行分析归纳。

3 这一方块分类来源于 1.20 版本对于创造物品栏的更新。

4 外网的建筑教程一般都以此命名，故本文如此引用该名称。

5 准确称呼应该是“下界传送门”，但 fandom wiki 同样能使用“地狱门”搜索到“下界传送门”，故此处如此。

力和创造力的玩家，在家门口的空地上搭起一篇野餐营地，或是一片树荫下的乘凉小椅。这时的此类建筑教程无论中外，都已经开始以“装饰方案”“设计方案”等字眼命名——这或许正是玩家们开始设计“外部装饰类建筑”的开端。

但此时的建筑虽然体量较小，且具有“以装饰为主”的特性，但早期版本带来的建材限制使得此时的“小品建筑”种类较为单一（一般为花园或公园常见建筑），规模也停留在微小型的程度。而也正是此时，玩家们的创造力产生了一次爆发，带来了一次“外饰”上的重大革命——第一批 Minecraft 大型服务器出现了。

服务器的建设需求带来了对出生区域，也就是主城的美化需求。这种美化需求一般是极端完美主义的，这也使得主城的设计者们更多的专注于建筑整体内外环境的设计，以及大型建筑周围细节处的装饰设计，例如街道或绿地等。玩家们的创造力开始突破了原版 MC 的限制，而造树科学的出现更是将其推上了一个小顶峰——人造树破除了原版树的造型限制，使得一大批魔幻 / 仙境 [6] 地图竞相出现，也为小品建筑设计者带来了全新的建造思路。

而这时，MC 的第一个革命性更新出现了：海洋更新。一大批水生动植物和建筑方块的出现，直接成就了小品类建筑的一个重要分支：“小池塘”。水景的实现使得人造景观的和谐程度进一步加强，玩家们也开始将早已磨合充分的人造树和花园营地与“小池塘”结合在了一起，大量的 MC 花园整体装饰和建筑展示视频开始涌现。

至此，小品建筑在 MC 的第一片江山算是成功“打下来”了。

可 MC 的更新脚步并不会停留于此。1.14 的村庄更新还没捂热乎，1.16 的下界更新和 1.18 的深度广度更新使得 MC 的世界群系变得更加丰富。群系的更新引入了大量的建筑方块和自然方块，也一并引入了很多崭新的建筑可能。玩家们开始不满足于原本的花园设计，想要将全新的自然方块塞进自己略显空荡的花园。于是原本安静的小池塘里响起了美西螈的啾啾声，湖畔的甘蔗也开始与竹子和垂滴叶相映成辉。

多种多样的世界景观丰富了玩家对于小品建筑门类的知识库，同样也使得一款名为 LEGO Minecraft[7] 的玩具再次进入人们的视野。这一批 LEGO 玩具本质上是与 MC 的联名主题产品，但其在景观

6 数据来源于 PlanetMinecraft 的相关地图发布时间查询。

7 1.16 下界更新位于 2019 年，而 LEGO MC 的第一款主题性质的玩具“洞穴”推出于 2014 年。虽然 LEGO MC 的早期玩具大多已经停售，但从官网宣传图中仍可看出，2014 年以前的“微型世界”系列质量还并不高，而这款玩具开始结合冒险和生存主题，也正是从“洞穴”（编号 21113）开始的。

主题上的设置却创造性的加入了“冒险主题”这一元素。例如 21120 款雪中藏匿处（停售）、21240 沼泽大冒险（现售）、21246 款漆黑世界之战（现售），精妙的还原了玩家们的冒险历程。

而恰巧的是，这一时期的玩家们也开始在自己的“外饰建造”里融入了“故事”的要素。例如花园茶歇、海滩烧烤派对等。这时玩家口中的“外饰”不再是单纯的装饰性设施，而是承载了基于玩家强大想象力的“功能”，诸如和朋友一起野餐，一起挂机钓鱼等等。

这一时期的其他早期“外饰建筑”也开始变得更加精致，形式上也逐渐趋于独立成景，而不是附属于某一特定的功能建筑。例如经过精心装饰，但可以摆放在任何位置的池塘或者温泉等。

这时，外饰圈里又有一支势力开始异军突起——他们凭着巧夺天工的建筑水平，还原 MC 中各种生物群系或者世界角落的风景。繁茂洞穴，深暗古城，海底神殿…只要是存在于这个世界里的景观，经他们的手都能够有模有样的在小空间中建造出来，甚至有时候比原版景色更胜一筹。

“复刻派”的出现，虽然脱胎于 MC 世界本身，但却为“外饰”领域注入了一股强大的新鲜血液。这些经过精妙设计的世界景观与现有的玩家建筑达成了近乎完美的组合——哪怕玩家的小房子朴素至极，依旧能融入这些令人惊异的人造风景。这些人造风景同样使得玩家们开始思考：“外饰”真的只能作为一种辅助性的建筑而存在吗？

至此，“小品类建筑”的概念才算是真正诞生了。

MC 里的小品类建筑是一类精致的“艺术品”建筑。它们没有固定的建筑模式，却往往以世界美化和风景塑造为主。相比于其他建筑流派对于方块色彩和“纹理[8]”的应用，小品类建筑更着眼于“布景”的考究和对自然方块的应用，同时也更注重于建筑的隐含主题，而不是使用功能。

当然相对于其他的几大建筑流派，MC 的小品类建筑经过不断地发展，内部同样拥有着几大特征性比较强的“流派”：

1. 装饰派

这类小品建筑者专注于建造诸如“附魔台装饰”、“地狱门装饰”的美化工程，将自然手法融入单调的建筑结构，使得结构的外形更加生动自然；

2. 风景派

这类小品建筑者专注于建造诸如“小池塘”、“小温泉”类的景观。不是自然，却又融入自然，风景派小品建筑者更像是

8 这一说法并不准确。“Texture”在 MC 里特指方块材质，但很多人却将利用方块的碰撞箱差异制作的“雕花”称为“纹理。”

一名园林设计师，用别致的小品景观设施为自己的小镇增添姿色。

3. 自然派

“取之于自然，用之于自然”是对这类小品建筑者的最好形容，装饰一棵樱花树，手搓一篇小群系等是这类建筑者最爱的事情。营造地形，手工搭树，用灯笼和蜡烛制造点点萤火。虽然没有“堑山堙谷，凿川贯江”的气势，但浓缩起来的一小片世界风景，同样是许多人梦中的心灵归宿。

4. 故事派

“没有建筑的建筑[9]是没有灵魂的！”带着这样的理念，这类小品建筑者的作品中往往伴随着一些小型的建筑设施，例如一片野餐营地，一顶旅居帐篷，或是一个小巧的凉棚，一条精致的渔船……充满意境的风景间，小巧的建筑也许正在静静等待着一段故事的续写。

总而言之，MC 里的小品类建筑是一个十分有趣的建筑流派。虽然其发展较早，但由于和其他建筑流派融合程度较高，在很长一段时间内都被简单的被划入了“外饰”的范畴。而当小品类建筑逐渐脱离了“装饰”的约束，开始以其自身的美观与精致独立的出现在玩家的眼前时，我们也开始逐渐体会并接纳了这种充满生命活力的“灵动”美学。

小品类建筑虽然没有房屋类建筑的诸多考究，但却需要建筑者对于自然风景和布景视角等具有独到的理解，而这其中的佼佼者往往具有不俗的造景天赋。可能也正是因此，至今我们也无法找到一个如同《Xk 形式美》一样的教程作为小品建筑的设计指南。但笔者相信在不久的未来，随着 Minecraft 世界的不断丰富，小品类建筑能够走进越来越多玩家的视野，让玩家们在惊叹于巨构建筑的宏伟和生存小屋的精致时，也能于闲暇中漫步花园野景，找回心底最为朴实的那一片美好期愿。

9 前一个“建筑”指房屋等，后一个建筑指的是一切“玩家建造物”的广义“建筑”概念。

文明世界万国志：
东罗马帝国篇

杂谈 • ruijam

《文明世界万国志》作为对已发行《堺屋史书》的补充与完善，选择在《方圆》发行与连载。《文明世界万国志》记载了文明世界中极具影响力与存在感的十三个政权，其中不少对堺屋及其前身产生了重要影响。

免责声明：《文明世界万国志》将会涉及部分现实世界相关实体的名词，但其完全为虚拟游戏世界之产物，仅有名称与现实世界相关，其他事件等等均与现实世界无关。若有生草，不胜荣幸。

老三强

一、东罗马帝国

东罗马帝国，全名 Basileia Romanion，又称拜占庭，首都位于君士坦丁堡，是堺屋创始成员（Badstudentchen、ruijam、OMG22K、Wang_jr）的出生地。东罗马帝国在文明世界属于“老三强”地位之国家，拥有工业体系之先发优势与强大的软实力。

地理

东罗马帝国国旗

东罗马帝国领土横跨亚、欧、非三大洲，包括了希腊、安纳托利亚半岛、叙利亚与巴勒斯坦及上埃及，同时在利比亚的班加西设立了殖民地。全境地形多样复杂，以山地为主、上埃及则遍布坦荡的漠原。境内的死海为文明世界的陆地最低点。地缘上，东罗马帝国西与天际联盟于克罗地亚接壤，东则与半岛联邦在约旦——伊拉克一线划界。全境大部属地中海气候，少部分地区为温带大陆性气候、高原山地气候及热带沙漠气候为主。

大致历史

（详情请参阅《堺屋史书》）

依据堺屋成员的回忆及其所现有史料，东罗马帝国的历史从 2021 年 3 月君士坦丁堡的建立开始；当年 5 月，Badstudentchen 到达雅典并大兴土木。2021 年 7 月，战争贩子进攻

东罗马帝国本土，东罗马帝国军队大溃退，次月雅典伪退出东罗马帝国止战。2022 年 2 月雅典与东罗马帝国爆发央地矛盾，雅典独立，雅典人遭东罗马帝国通缉并流亡至莉亚世界。2022 年 6-7 月，东罗马帝国随文明世界灭亡。

政治

东罗马帝国为君主专制，国家元首掌握绝对权力且世袭。但国家元首对地方的掌控并不稳定，因此也有人认为东罗马帝国在国体上实际为联邦制。外交上东罗马帝国与大多数国家缔结了互不侵犯条约与军事同盟条约，但其对美国在雅典独立之前长期采取敌视态度。

经济与社会

东罗马帝国经济发达，其中雅典为文明世界的经济金融中心之一，雅典拥有强大的文化产业与建筑业，《东罗日报》（《堺屋日报》前身）为文明世界最早发行及发行量最大的报纸，雅典同时也是堺屋创始成员建立的城市及石匠公社的建立地；格拉伦萨是东罗马帝国的工业中心，具备了从高速熔炉至全树种树厂的完善工业体系。东正教是东罗马帝国的国教，官方同时采取宗教自由政策，使得石匠信仰与希腊多神教流行于希腊地区。

雅典风光

黑猫

诗歌 • Meapuchino

(一)

我的家里，溜进了一只黑猫。
夕阳的余晖中，精巧的身影一闪而过，融进了墙角的一片阴影里。
“那是只猫吗？”我难以置信的揉了揉眼睛，
回应我的却只有一声简单的喵叫，
在空荡的屋子里格外清晰。

(二)

微光中，两双眼睛互相默视，
惊异却很快变成了乏味——
印象中的那个墙角，是一个简单却不乏舒适的猫窝，
而数不清的猫曾在那里驻足，
纯白，狸花，美短，英短 .....
但无一例外都很快跑掉不见。
“嗯，这次大概也一样的吧。”

(三)

第二天，一切照旧。
离开的时候，我没有留意那片墙角，
却在回家的路上买了一盒猫罐头。
而当门扉敞开，灯光点亮，墙角却并没有黑猫的身影。
“什么嘛，我就说。”
清脆的撞击声间，猫罐头被顺手丢在了地上。

（四）

晨起时分，屋外传来细微的喵叫，
我揉着眼睛打开门——
那只黑猫正静静的蹲在门口。
“噗——”我不禁笑了出来，
可我到底为什么会笑呢?

（五）

家中的氛围发生了微妙的变化，
伴随着一抹纯黑的身影，和不时的轻声喵叫。
从墙角里，到饭桌下，再到沙发的扶手边 .....
这间屋子里，有了一只黑猫。

（六）

闹铃响起，晨曦入户，
初醒的我正好遇上枕边爱人的目光。
“做梦了吗？”
我笑了笑，回以一个轻柔的拥抱——
“我梦见了一只几年前，来到这个家里的黑猫。”

ECH 的出现改变了什么

身边物语 · 简单说说之二 • Venti_Lynn

网络的隐私问题一直是人们关心的焦点。随着技术的进步，保护个人信息和在线活动变得越来越重要。Cloudflare 最近推出的 Encrypted Client Hello（ECH）技术，为我们打开了通往更安全网络世界的新门户。那么，ECH 到底是什么？它又如何改变了我们的网络体验？让我们简单了解一下。

回望过去：隐私的保护

有哪些技术在保护我们的网络安全?

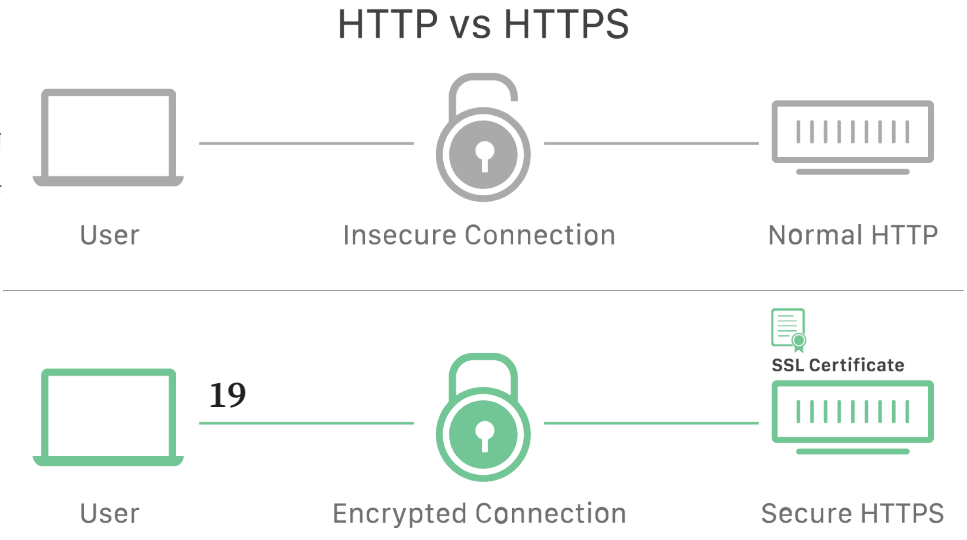
- **SSL（安全套接层）**和 **TLS（传输层安全）**：这两种协议为我们的网络通信提供了基本的加密保护。它们确保了数据在传输过程中的安全，防止中间人攻击和数据泄露。
- **HTTPS（超文本传输安全协议）**：HTTPS 是在 HTTP 上加入 SSL/TLS 加密层的协议，它为网站和用户之间的通信提供了加密保护，确保了数据的私密性和完整性。
- **DNS over HTTPS（DoH）**：传统的 DNS 查询是明文的，任何人都可以看到你正在访问哪个网站。DoH 通过加密 DNS 查询来提高用户的网络隐私。
- **ESNI（Encrypted Server Name Indication）**：在 ECH 出现之前，ESNI 是一个尝试保护 SNI 数据的技术，但它并没有得到广泛的支持和采用。

SSL/TLS、HTTPS：基本的加密保护

什么是 SSL？

安全套接字层（SSL）是一种安全加密协议，由 Netscape 在 1995 年创立，目的是保障 Internet 通信的隐私、身份验证和数据完整性。SSL 可视为现今广泛使用的传输层安全（TLS）加密技术的前身。

采用 SSL/TLS 技术的网站的 URL 会显示为“**https**”，而非“http”。



什么是 TLS？

传输层安全（TLS）是一种被广泛采纳的安全协议，其主要目的是确保互联网通信的私密性和数据安全。TLS 主要应用于加密 web 应用程序和服务器之间的通信（例如，web 浏览器加载网站时），同时也可以用于加密其他类型的通信，如电子邮件、消息传送和 IP 语音（VoIP）等。

TLS 是由互联网工程任务组（Internet Engineering Task Force，IETF）所提出，协议的首个版本于 1999 年发布，而最新的版本，TLS 1.3，则于 2018 年发布。

TLS 和 SSL 有什么区别?

TLS 实际上是由 Netscape 最初开发的**安全套接字层（SSL）**协议所演变而来的。TLS 1.0 版本最初作为 SSL 3.1 版本开发，但在发布前更名，以表明它不再与 Netscape 有关联。由于这个历史背景，人们有时会交替使用 TLS 和 SSL 这两个术语。

林恩：简单来说，要快速判断一个网站是否采用了 SSL/TLS 加密技术，你只需查看浏览器地址栏左侧是否有一个小锁图标。如果有，那就表示该网站启用了安全连接。

什么是 HTTPS？

超文本传输协议安全（HTTPS）是 HTTP 的安全版，而 HTTP 是用于在 Web 浏览器和网站之间传输数据的主要协议。HTTPS 提供加密服务，以增强数据传输的安全性，这在用户传输敏感数据（例如登录银行账户、电子邮件服务或健康保险提供商时）尤为重要。

所有网站都应使用 HTTPS，特别是那些需要用户登录的网站。在现代的 Web 浏览器（如 Chrome）中，使用 HTTPS 的网站和未使用 HTTPS 的网站在显示上有所区别。如果 URL 栏显示有锁图标，那就表示该网页是安全的。Web 浏览器非常重视 HTTPS；例如，**Google Chrome 和其他浏览器会将所有未启用 HTTPS 的网站标记为不安全**。

HTTPS、SSL/TLS 之间的关系是什么?

技术上讲，HTTPS 不是一个独立于 HTTP 的协议，而是在 HTTP 协议基础上应用了 TLS/SSL 加密。HTTPS 的传输依赖于 **TLS/SSL 证书**，该证书验证了特定提供者的身份就是他们所声称的身份。

林恩：可能很多人不理解为什么需要用到 HTTPS 技术，我在这里举一个简单的例子：

加密前：

```
这是完全可读的文本字符串
```

加密后：

```
ITM0IRyiEhVpa6VnKyExMiEgNveroyWBPlgGyfkflYjDaaFf/Kn3bo3OfghBPDWo6
AfSHlNtL8N7ITEwIXc1gU5X73xMsJormzzX
```

> 在不使用 HTTPS 的网站中，Internet 服务提供商（ISP）或其他中间人有可以在未经网站所有者批准的情况下将内容注入网页。这通常采用广告形式，希望增加收入的 ISP 将付费广告注入其客户的网页中。毋庸置疑，当这种情况发生时，绝不会与网站所有者共享广告的利润和这些广告的质量控制。HTTPS 杜绝了未经审核的第三方将广告注入 Web 内容的可能。
>
> 摘自 Cloudflare[2]

DNS over HTTPS 技术：加密的 DNS

DNS over HTTPS（DoH）是一种用于加密 DNS 查询的技术。在传统的 DNS 查询中，通信是明文的，这使得可能对用户的 DNS 流量进行监视和操纵。为了提高安全性和隐私性，DoH 引入了加密来保护 DNS 查询的隐私。

实际上前段时间出现的 Minecraft 验证服务器无法访问，被强制跳转到国家反诈中心这种情况，根据其表现出来的特征，我们可以认为出现了 DNS 污染，强制将 Minecraft 域名解析到国家反诈中心的地址而导致无法访问。

如果使用了 DoH 技术，可以一定程度上避免这个问题。

DoH 和 DoT 的区别?

DoH（DNS over HTTPS）和 DoT（DNS over TLS）都是将 DNS 查询加密的技术，以提高安全性和隐私保护。

1. DoH（DNS over HTTPS）：
   - 它通过 HTTPS（一个安全的网页访问协议）来发送和接收 DNS 查询和回应，就像你安全地浏览网站一样。
2. DoT（DNS over TLS）
   - 它使用 TLS（传输层安全协议）来加密 DNS 的通信，这是另一种常用的安全协议。

两者的目的都是为了保护你的 DNS 查询不被窃听或篡改，但它们使用不同的方法来实现这一点。**DoH 更像是在安全的网页环境中进行 DNS 查询，而 DoT 则是直接在传输层提供加密保护。**

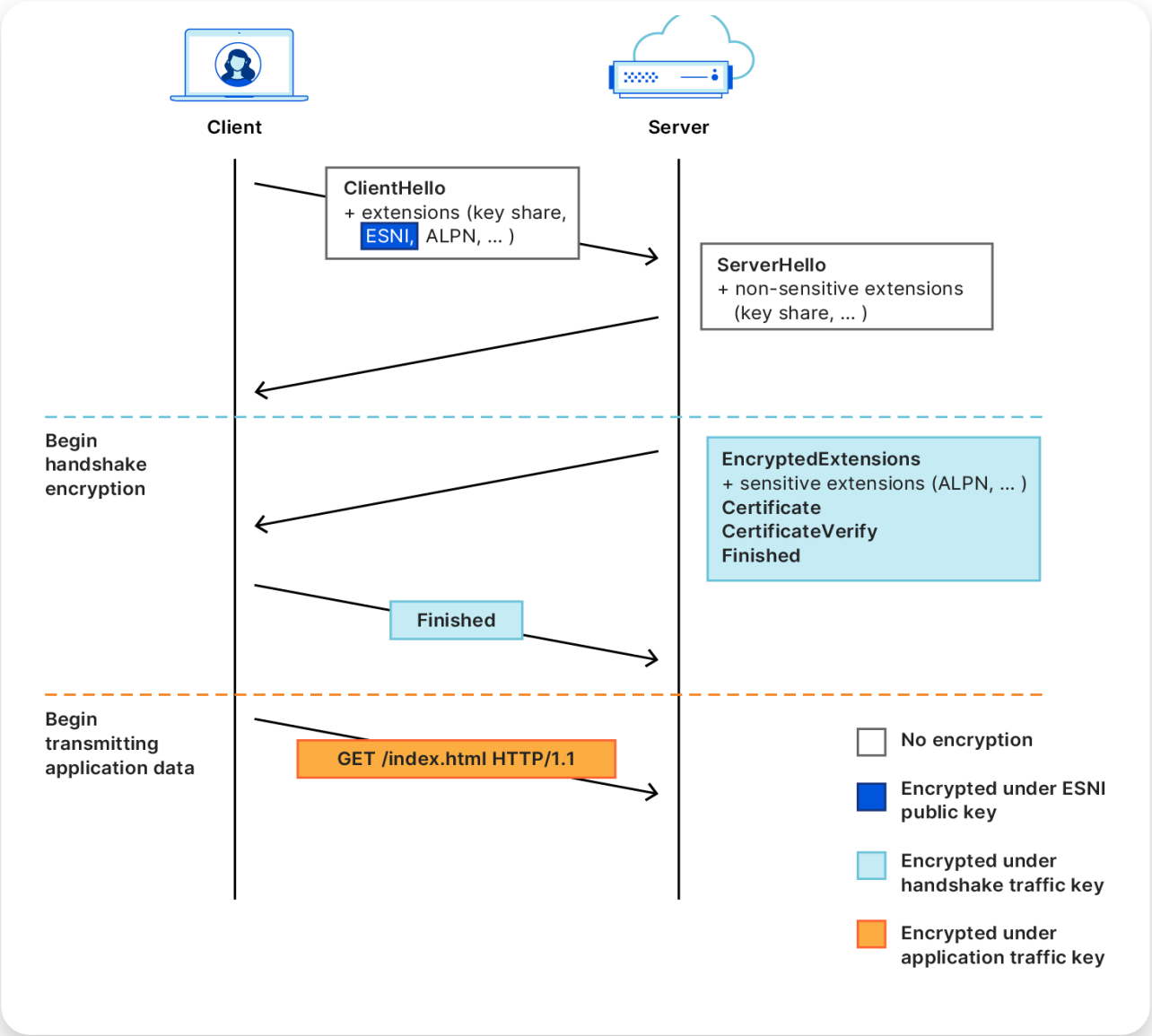
SNI 技术 [1][3]

SNI（Server Name Indication）是 TLS 的一个扩展，它允许客户端在握手过程开始时告知服务器它想要连接的主机名称。**这主要解决了一个服务器拥有多个域名时的问题。**在 TLS 握手期间，通过在第一阶段的 ClientHello 报文中添加主机名称，服务器能识别客户端想要连接的虚拟主机，从而选择正确的证书进行通信。这与 HTTP 协议中通过请求头的 Host 字段指定想要访问的域名的方法相似。

ESNI：SNI 的加密保护

> 以下内容译自 Cloudflare Blog，仅摘录部分内容。[1]

ECH 的前身是加密 SNI（ESNI）扩展。顾名思义，ESNI 的目标是提供 SNI 的机密性。为此，客户端将在服务器的公钥下加密其 SNI 扩展名，并将密文发送到服务器。服务器将尝试使用与其公钥对应的密钥解密密文。如果解密成功，则服务器将使用解密的 SNI 继续连接。否则，它只会中止握手。这个简单协议的高级流程如图所示。



ECH 技术：姗姗来迟的大修

什么是 ECH？

> The goal of ECH is to encrypt the entire ClientHello, thereby closing the gap left in TLS 1.3 and ESNI by protecting all privacy-sensitive handshake-parameters. Similar to ESNI, the protocol uses a public key, distributed via DNS and obtained using DoH, for encryption during the client's first flight. But ECH has improvements to key distribution that make the protocol more robust to DNS cache inconsistencies. Whereas the ESNI server aborts the connection if decryption fails, the ECH server attempts to complete the handshake and supply the client with a public key it can use to retry the connection.

> ECH 的目标是加密整个 ClientHello，以此来填补 TLS 1.3 和 ESNI 留下的空白，保护所有隐私敏感的握手参数。与 ESNI 类似，该协议利用一个公钥，在客户端的首次通信（first flight）期间进行加密，该公钥通过 DNS 分发并利用 DoH（DNS over HTTPS）获取。但是，ECH 在密钥分发方面做了改进，使得该协议对 DNS 缓存不一致的情况具有更强的适应性。与在解密失败时会中止连接的 ESNI 服务器不同，ECH 服务器会尝试完成握手，并向客户端提供一个可用于重新尝试连接的公钥。
>
> 摘自 Cloudflare[2]

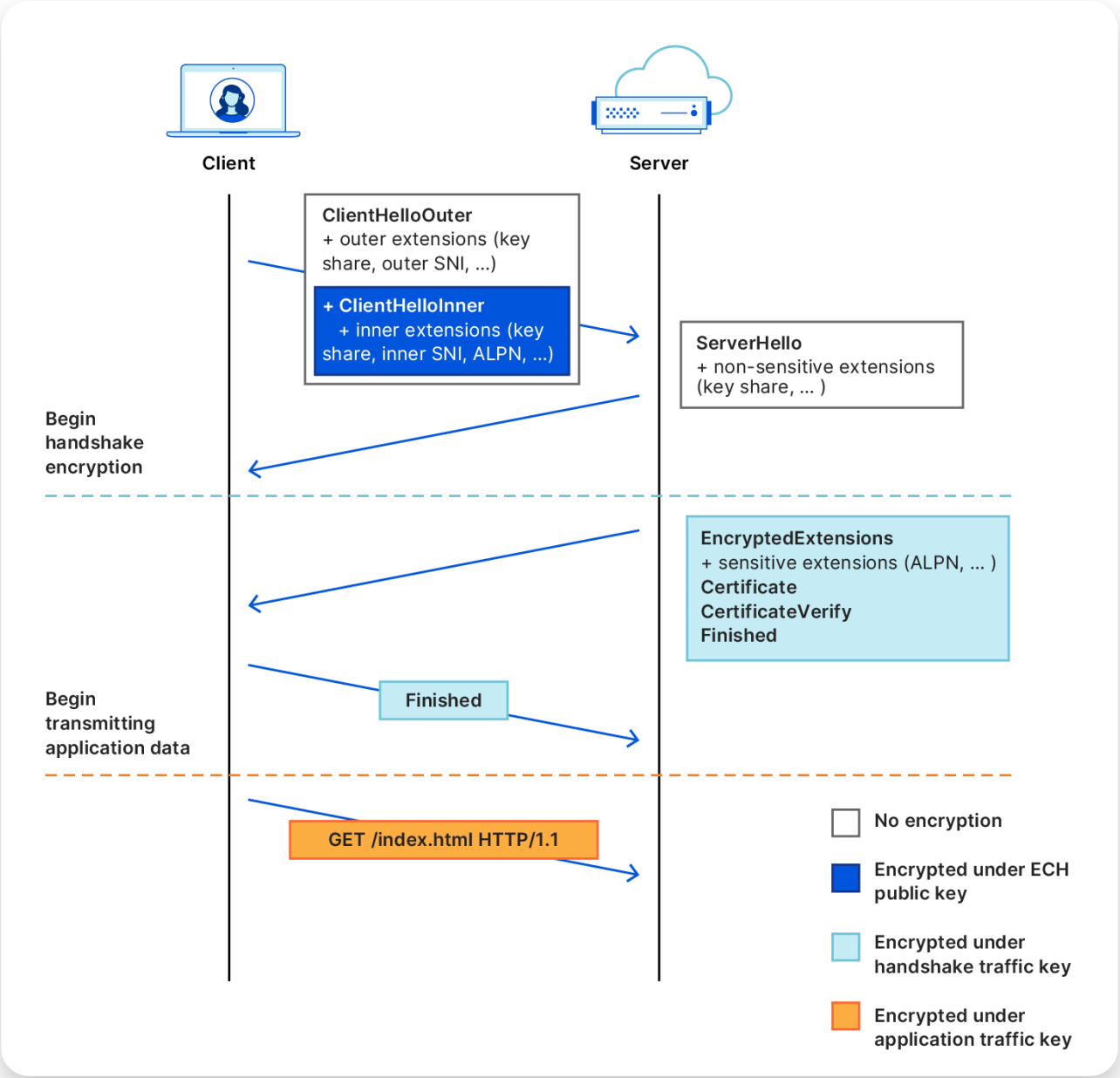
简单来说，ECH 是一个新的网络技术，它的目标是保护用户的网络隐私，特别是在访问不同网站时。在之前，当你访问一个网站时，你的浏览器会通过一个叫做 TLS 握手的过程与网站的服务器建立安全连接。然而，在这个过程中，你正在访问的网站的名称（被称为服务器名称指示或 SNI）是可见的，这意味着网络中间人（比如你的网络服务提供商）可以看到你正在访问哪个网站。ECH 的出现，使得这一信息得以加密，从而保护了你的网络隐私。

划重点：

- ECH 是一个旨在保护用户隐私的新技术，它能隐藏用户在访问哪些网站的信息。
- ECH 是 ESNI（Encrypted Server Name Indication）的继承者，专注于在 TLS 握手过程中保护服务器名指示（SNI）。

ECH 是如何工作的

林恩：ECH 通过加密 SNI 来保护你的网络隐私。具体来说，它将原来的 ClientHello 消息分为两部分：一个外部部分和一个内部部分。外部部分包含一些非敏感信息，而内部部分（被加密）包含你想要访问的网站的实际名称。这样，即使网络中间人可以看到 TLS 握手的过程，他们也无法确定你正在访问哪个网站。



ECH 带来了什么变化?

> Ultimately, the goal of ECH is to ensure that TLS connections made to different origin servers behind the same ECH service provider are indistinguishable from one another. In other words, when you connect to an origin behind, say, Cloudflare, no one on the network between you and Cloudflare should be able to discern which origin you reached, or which privacy-sensitive handshake-parameters you and the origin negotiated. Apart from an immediate privacy boost, this property, if achieved, paves the way for the deployment of new features for TLS without compromising privacy.

> Encrypting the ClientHello is an important step towards achieving this goal, but we need to do a bit more. An important attack vector we haven't discussed yet is traffic analysis. This refers to the collection and analysis of properties of the communication channel that betray part of the ciphertext's contents, but without cracking the underlying encryption scheme. For example, the _length_ of the encrypted ClientHello might leak enough information about the SNI for the adversary to make an educated guess as to its value (this risk is especially high for domain names that are either particularly short or particularly long). It is therefore crucial that the length of each ciphertext is independent of the values of privacy-sensitive parameters. The current ECH specification provides some mitigations, but their coverage is incomplete. Thus, improving ECH's resistance to traffic analysis is an important direction for future work.
>
> 摘自 Cloudflare[2]

ECH 的最终目标是确保与同一 ECH 服务提供商后面的不同源服务器建立的 TLS 连接彼此不可区分。换句话说，当你连接到一个在 Cloudflare 后面的源时，你和 Cloudflare 之间的网络上的任何人都不能分辨出你到达的是哪个源，以及你和源之间协商的哪些涉及隐私的握手参数。除了立即提升隐私外，如果实现这个目标，它还为 TLS 的部署新功能铺平了道路，而不会损害隐私。

加密 ClientHello 是实现这一目标的重要步骤，但我们还需要做更多工作。我们尚未讨论的一个重要攻击媒介是**流量分析**。这指的是收集和分析通信通道的属性，这些属性透露了一部分密文的内容，但不会破解基础加密方案。例如，加密的 ClientHello 的长度可能泄漏足够的关于 SNI 的信息，使得攻击者可以对其值做出有根据的猜测（对于特别短或特别长的域名，这种风险尤其高）。因此，每个密文的长度独立于涉及隐私的参数值是至关重要的。当前的 ECH 规范提供了一些缓解措施，但覆盖范围不完全。因此，改进 ECH 对抗流量分析的能力是未来工作的一个重要方向。

林恩：从我们普通人的角度来看，ECH 技术给我们带来的体验很可能是无缝的，ECH 就像是一座摩天大厦的基石，他给我们带来了更好的网络隐私保护。同时也大大降低了因为网络攻击与运营商审查而导致的网页无法访问等问题出现的概率。

拓展阅读

ECH 技术的影响和重要性的关键点

1. 增强隐私
   - ECH 加密了 TLS 握手过程的某些部分，从而掩盖了服务器名称指示（SNI）。SNI 是客户端与哪个服务器通信的明确信号，加密 SNI 对于保护用户隐私至关重要。
   - 该技术加密了以前明文协商的 TLS 连接的隐私敏感参数，从而防止网络观察者访问大量元数据，包括端点的身份和它们如何使用连接。
2. 为未来的安全功能奠定基础
   - ECH 为在最小化对终端用户隐私影响的同时向 TLS 添加未来的安全功能和性能增强奠定了基础。
3. 合作努力
   - ECH 的开发是学术界和技术产业领袖之间在 IETF（互联网工程任务组）的协助下进行紧密合作的产物，包括 Cloudflare、Fastly 和 Mozilla 等。
4. 对 TLS 的重大升级
   - ECH 代表了对 TLS 协议的重大升级，构建了像 DNS-over-HTTPS 这样的新技术。然而，据指出，该协议尚未准备好进行互联网规模的部署。
5. 解决其他隐私敏感的握手参数问题
   - 除了 SNI，ECH 还旨在保护客户端和服务器协商的其他隐私敏感的握手参数，例如用于决定 TLS 连接建立后使用哪个应用层协议的 ALPN 扩展。
6. 握手加密
   - ECH 朝着完全握手加密的方向迈进，这对解决与握手过程相关的各种隐私泄漏至关重要。握手加密确保除了完成密钥交换所必需的参数外，所有握手参数都被加密。

7. 协议扩展
   - ECH 作为传输层安全协议（TLS）的协议扩展，强调了其在增强现有协议以实现更好的隐私和安全措施方面的作用。
8. 客户端 - 浏览器交互
   - 使用 ECH 时，浏览器将与 Cloudflare 执行 TLS 握手，而不是特定于客户的主机名，这进一步使客户端与服务器之间的交互更为匿名。

我的浏览器是否支持 ECH 技术?

你可以访问这个页面来验证你的浏览器是否 ECH 技术。
链接：https://defo.ie/ech-check.php

同时你可以参考下面两篇文档来设置你的浏览器。

- “Feature: TLS Encrypted Client Hello (ECH)”
- “You can now Enable Encrypted Client Hello (Encrypted SNI or ESNI/ECH) in Microsoft Edge - 微软技术社区”

后记

本篇文章到这里就结束了，如果你仍然对文章提到的技术感兴趣，你可以尝试阅读一下扩展内容和参考资料。

如果你喜欢我的文章，可以考虑在爱发电赞助我，这会激励我更有动力地写更多的文章。

个人博客：https://blog.lynn6.cn
爱发电：https://afdian.net/a/lynnguo666

1 What Is SNI? Encrypted SNI (ESNI and ECH)
2 Cloudflare Blog - Good-bye ESNI, hello ECH!
3 什么是 SNI？ - PamShao

告别 ESNI，迎接 ECH

身边物语 · Christopher Patton；Venti_Lynn、ChatGPT（译）

现代互联网上的大多数通信都是加密的，以确保其内容只能被端点（即客户端和服务器）理解。然而，加密需要一个密钥，因此端点必须在不向潜在攻击者透露密钥的情况下达成对加密密钥的协议。为此任务而广泛使用的密码协议叫做密钥交换，是**传输层安全协议（TLS）**的握手过程。

在这篇文章中，我们将深入探讨 **Encrypted Client Hello（ECH）**，这是 TLS 的一个新扩展，它有望显著增强这个关键互联网协议的隐私保护。如今，TLS 连接的许多对隐私敏感的参数都是明文协商的。这使网络观察者可以获取大量的元数据，包括端点的身份、它们如何使用连接等。

ECH 加密完整的握手过程，以保密这些元数据。关键的是，它通过保护**服务器名称指示（SNI）**免受网络上的窃听者的侵犯，从而解决了一个长期存在的隐私泄露问题。加密 SNI 很重要，因为它是客户端与特定服务器通信的最明确信号。然而，或许更重要的是，ECH 为将来向 TLS 添加安全特性和性能增强提供了基础，同时最大程度地减少了它们对最终用户隐私的影响。

ECH 是学术界和技术产业领袖之间紧密合作的产物，由 IETF 促成，包括 Cloudflare、我们在 Fastly 和 Mozilla 的朋友（两者都是标准的合作者），以及许多其他人。这个特性代表了对 TLS 协议的重大升级，它依赖于一些尖端技术，比如 **DNS-over-HTTPS**，这些技术现在才刚刚开始展现它们的价值。目前，该协议还没有准备好进行互联网规模的部署。本文旨在作为实现完整握手加密道路上的一个指示标志。

背景

TLS 的故事就是互联网的故事。随着我们对互联网的依赖不断加深，这个协议也在不断地演进，来满足日益变化的操作需求、使用场景和威胁模型。客户端和服务器不仅仅是在交换一个密钥。他们协商了许多功能和参数：确切的密钥交换方式；加密算法；谁进行身份验证以及如何验证；握手之后使用哪个应用层协议等等。这些参数都以某种方式影响通信通道的安全性。

SNI 是一个对通道安全产生重要影响的参数。客户端使用 SNI 扩展来告诉服务器它想要访问的网站。对于现代互联网来说，这是至关重要的，因为如今很多源服务器都位于同一个 TLS 运营商后面。在这种情境下，运营商使用 SNI 来确定谁将对连接进行身份验证：如果没有 SNI，就不知道向客户端展示哪个 TLS 证书了。问题是，SNI 泄露了客户端想要连接的源服务器的身份，可能使窃听者推断出他们通信的许多信息。（当然，网络观察者还有其他方法来识别源头，例如源的 IP 地址。但是，将多个源放在同一个 IP 地址上会使这种识别方法变得更加困难。）

尽管保护 SNI 是推动 ECH 发展的动机，但这并不是客户端和服务器协商的唯一涉及隐私的握手参数。另一个是 **ALPN 扩展**，它用于确定一旦建立了 TLS 连接，要使用哪种应用层协议。客户端发送其支持的应用程序列表，无论是 HTTPS、电子邮件、即时通讯还是其他众多使用 TLS 进行传输安全的应用程序，服务器从这个列表中选择一个，并将其发送给客户端。通过这样做，客户端和服务器向网络泄露了关于它们能力以及连接可能用于何种用途的明确信号。

有些功能非常关心隐私，所以在握手中包括它们是不可能的。有一个提议是用密码认证的密钥交换（PAKE）替代 TLS 的核心的密钥交换。这将允许基于密码的身份验证与（或替代）基于证书的身份验证一起使用，使 TLS 更加稳健，适用于更广泛的应用程序。这里的隐私问题与 SNI 类似：服务器通常给每个客户端分配一个唯一标识符（例如，用户名或电子邮件地址），用于检索客户端的凭证；在握手过程中，客户端必须以某种方式将此身份传达给服务器。如果明文发送，那么这些个人身份信息将容易被任何网络观察者获取。

解决所有这些隐私泄露的必要条件是握手加密，也就是除了应用数据之外的握手消息的加密。听起来很简单，但这个解决方案提出了另一个问题：如果握手本身是一种交换密钥的方式，那么客户端和服务器如何选择加密密钥呢？当然，某些参数必须明文发送，所以 ECH 的目标是加密所有握手参数，除了那些完成密钥交换所必需的参数。

为了理解 ECH 以及支撑它的设计决策，了解一下 TLS 中握手加密的历史是很有帮助的。

TLS 握手加密

在最新版本 TLS 1.3 之前，TLS 根本没有握手加密功能。在 2013 年 Snowden 的爆料之后，IETF 社区开始考虑如何对抗大规模监控对开放互联网的威胁。当 2014 年开始标准化 TLS 1.3 的过程时，其设计目标之一是尽可能加密握手过程。遗憾的是，最终的标准并没有达到完全

的握手加密，包括 SNI 在内的几个参数仍然是明文传输。让我们更深入地了解其中的原因。

TLS 1.3 协议流程如图 1 所示。握手加密开始于客户端和服务器计算出一个新的共享秘密之后。为此，客户端在其 ClientHello 消息中发送一个密钥分享，服务器在其 ServerHello 中响应自己的密钥分享。交换了这些分享后，客户端和服务器可以推导出一个共享的秘密。每一个随后的握手消息都使用从共享秘密中推导出的握手流量密钥加密。应用数据使用另一个密钥加密，称为应用流量密钥，它也是从共享秘密中推导出来的。这些派生的密钥有不同的安全属性：为了强调这一点，它们用不同的颜色表示。

第一个被加密的握手消息是服务器的 EncryptedExtensions。这个消息的目的是保护服务器的敏感握手参数，包括服务器的 ALPN 扩展，其中包含从客户端的 ALPN 列表中选出的应用程序。密钥交换参数在 ClientHello 和 ServerHello 中未加密传输。

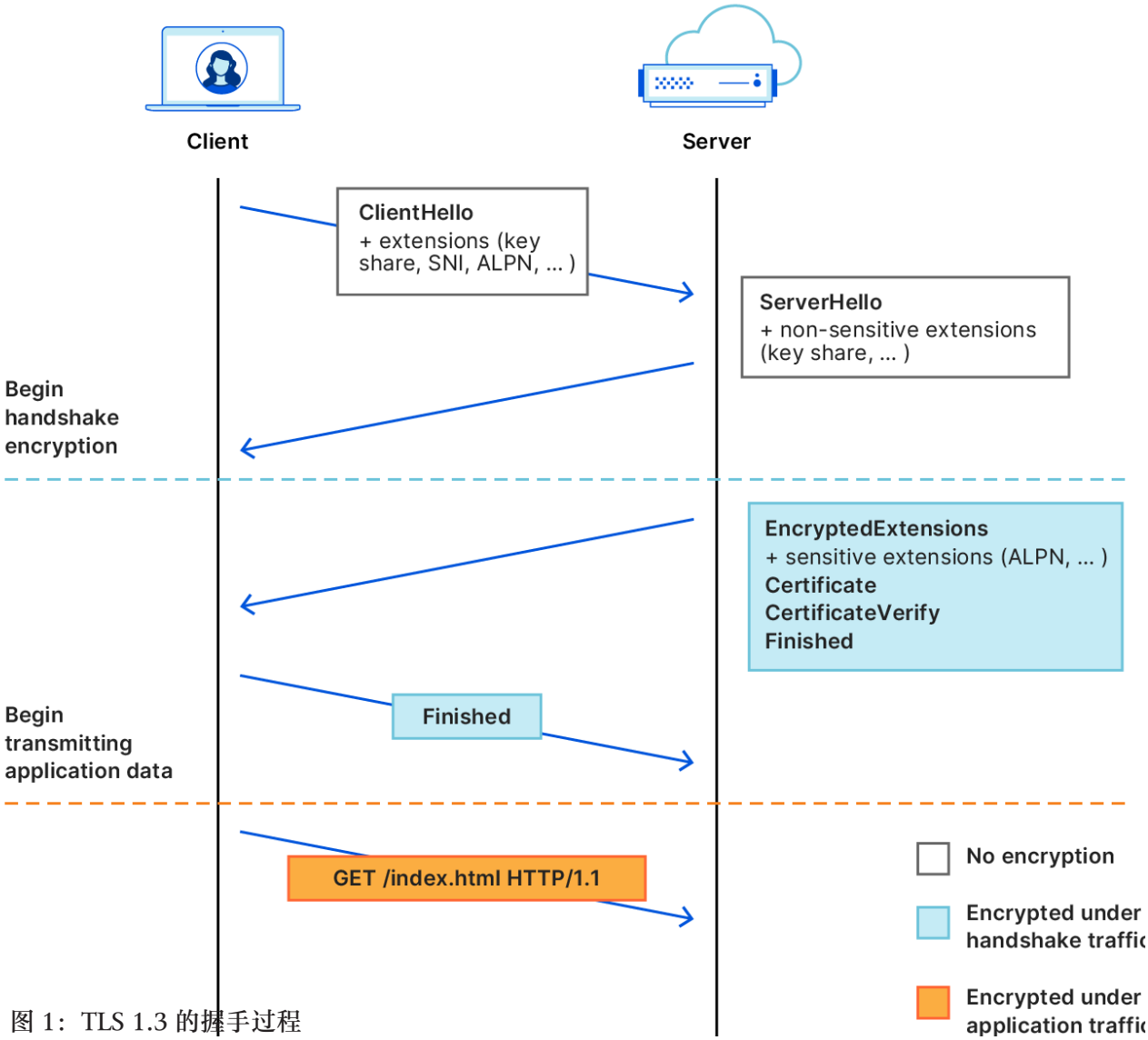


图 1：TLS 1.3 的握手过程

客户端的所有握手参数，无论是否敏感，都会在 ClientHello 消息中发送。从图 1 中可以看出，您可能会考虑重新设计握手方式，以增加延迟为代价，使其中一些参数可以加密（即进行更多往返）。然而，像 SNI 这样的扩展产生了一种“先有鸡还是先有蛋”的问题。

客户端在验证服务器的身份（这是证书和 CertificateVerify 消息的工作）并且服务器确认知道共享密钥（这是 Finished 消息的工作）之前不会加密任何内容。这些措施确保密钥交换是经过身份验证的，从而防止**中间人攻击（MITM）**，在这种攻击中，攻击者以允许客户端解密客户端发送的消息的方式将服务器模拟给客户端。由于服务器需要 SNI 来选择证书，因此需要在对密钥交换进行身份验证之前传输它。

总的来说，确保用于身份验证的握手参数的机密性只有在客户端和服务器已经共享了加密密钥的情况下才可能。但这个密钥可能从哪里来呢?

在 TLS 1.3 的早期，完整的握手加密曾经被提议作为 TLS 1.3 的核心特性。在该协议的早期版本（大约在 2015 年的草案 10）中，服务器会在握手过程中向客户端提供一个长时间有效的公钥，客户端在后续的握手中使用这个公钥进行加密。（这种设计来自一个叫做 OPTLS 的协议，而这个协议又是从原始的 QUIC 提案中借鉴来的。）这种模式叫做“0-RTT”，其主要目的是允许客户端在完成握手之前开始发送应用数据。此外，它还允许客户端在 ClientHello 之后加密其第一批握手消息，包括它自己的 EncryptedExtensions，这可能被用来保护客户端的敏感握手参数。

最终，这个特性没有被包含在最终的标准中（2018 年发布的 RFC 8446），主要是因为它的复杂性超过了它的实用性。尤其是，它对于客户端在初始握手中学习服务器公钥的操作没有任何保护。用于服务器认证的初始握手的参数，如 SNI，仍然会明文传输。

尽管如此，这种方案是其他握手加密机制，如 ECH，使用公钥加密来保护敏感的 ClientHello 参数的前身。这些机制必须解决的主要问题是密钥分发。

在 ECH 之前就有（并且现在也是）ESNI

ECH 的直接前身是加密 SNI（ESNI）扩展。顾名思义，ESNI 的目标是提供 SNI 的机密性。为了实现这一目标，客户端会使用服务器的公钥加密其 SNI 扩展，并将密文发送给服务器。服务器将尝试使用与其公钥对应的私钥解密密文。如果解密成功，则服务器将使用解密后的 SNI 进行连接。否则，它将中止握手过程。这个简单协议的高级流程如图 2 所示。

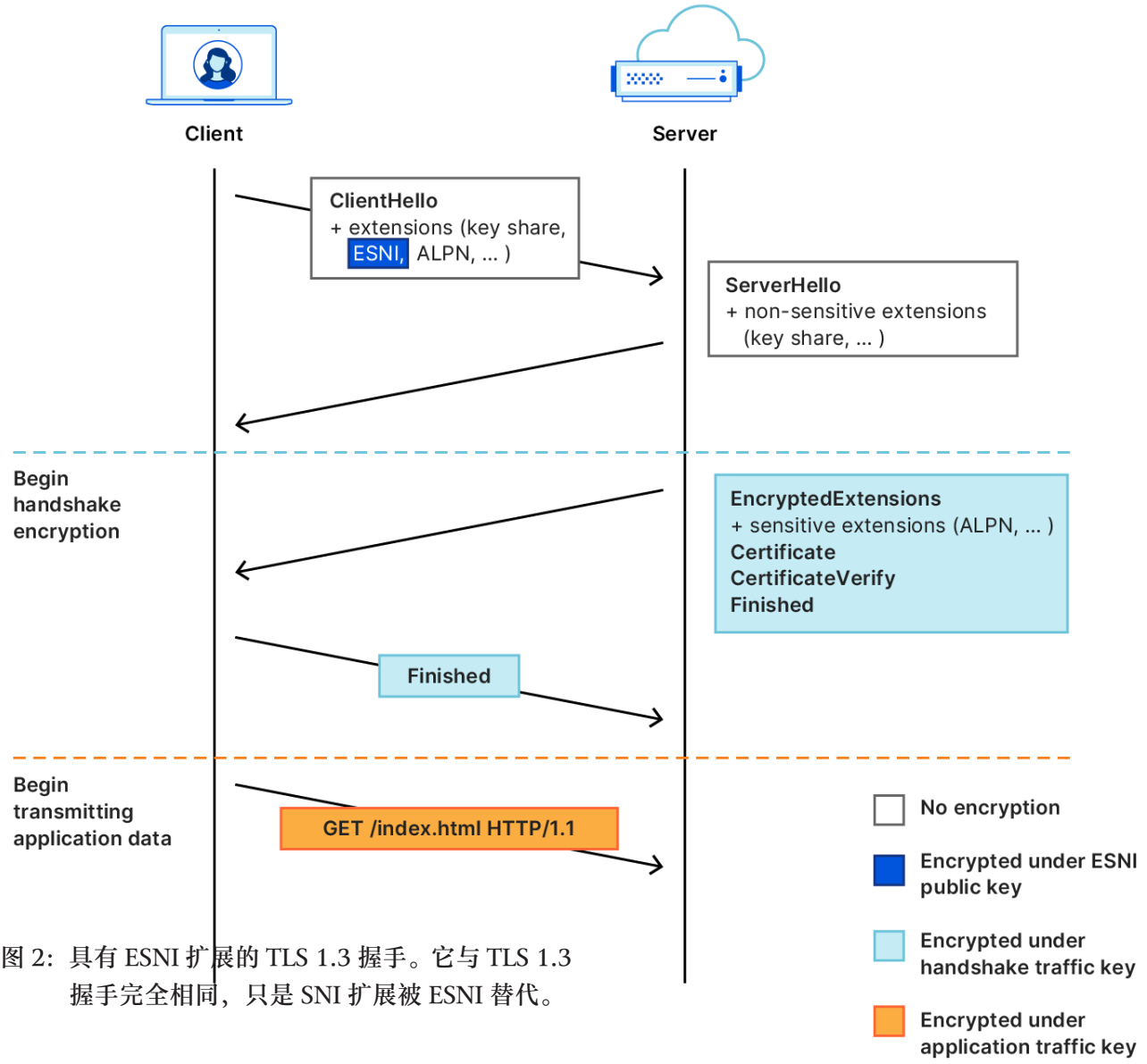


图 2：具有 ESNI 扩展的 TLS 1.3 握手。它与 TLS 1.3 握手完全相同，只是 SNI 扩展被 ESNI 替代。

对于密钥分发，ESNI 依赖于另一个关键协议：域名服务（DNS）。为了使用 ESNI 连接到一个网站，客户端会在其标准的 A/AAAA 查询中附加一个请求，请求获取带有 ESNI 公钥的 TXT 记录。例如，要获取 crypto.dance 的密钥，客户端会请求 _esni.crypto.dance 的 TXT 记录：

```
$ dig _esni.crypto.dance TXT +short
"/wGuNThxACQAHQAgXzyda0XSJRQWzDG7lk/r01r1ZQy+MdNxKg/mAqSnt0EAAhM
BAQQAAAAAX67XsAAAAABftsCwAA="
```

Base64 编码的字符串包含 ESNI 公钥和相关参数，如加密算法。

但是，如果我们通过明文 DNS 查询向网络观察者泄漏服务器名称，那么加密 SNI 的意义何

在？通过引入 DNS-over-HTTPS（DoH），部署 ESNI 成为可能。DoH 可以将 DNS 查询加密到提供 DoH 服务的解析器（1.1.1.1 就是这样一个服务）中。DoH 的另一个重要特性是，它提供了一个经过身份验证的通道，用于将 ESNI 公钥从 DoH 服务器传输到客户端。这可以防止源自客户端本地网络的缓存污染攻击：在没有 DoH 的情况下，本地攻击者可以通过返回空的 TXT 记录阻止客户端提供 ESNI 扩展，或者迫使客户端使用它们控制的密钥。

虽然 ESNI 迈出了重要的一步，但它没有达到我们实现完全握手加密的目标。除了不完整（仅保护 SNI），它还容易受到一些复杂攻击的影响，虽然实施难度较大，但指向了协议设计上的理论弱点，需要解决。

2018 年，Cloudflare 在 Firefox 上进行了 ESNI 部署，并以自愿选择的方式启用，这一经历揭示了依赖 DNS 进行密钥分发的一些挑战。Cloudflare 每小时更换其 ESNI 密钥，以尽量减少密钥被泄露时的附带损害。DNS 的参数有时会被缓存更长时间，结果是客户端可能具有过期的公钥。虽然 Cloudflare 的 ESNI 服务在一定程度上可以容忍这种情况，但每个密钥最终都必须过期。ESNI 协议留下的问题是，如果解密失败 * 并且 * 无法访问当前的公钥（通过 DNS 或其他方式），客户端应该如何继续进行。

依赖 DNS 进行密钥分发的另一个问题是，多个端点可能是同一源服务器的授权端点，但具有不同的功能。例如，对“example.com”的 A 记录的请求可能返回两个不同的 IP 地址，每个 IP 地址由不同的 CDN 操作。“_esni.example.com”的 TXT 记录将包含这些 CDN 之一的公钥，但肯定不会包含两者的公钥。DNS 协议没有提供一种将对应于同一端点的资源记录原子地绑定在一起的方法。特别是，客户端可能无意中将 ESNI 扩展提供给不支持它的端点，导致握手失败。解决这个问题需要对 DNS 协议进行更改。（下文详述。）

ESNI 的未来：在接下来的部分中，我们将描述 ECH 规范以及它如何解决 ESNI 的局限性。然而，尽管 ESNI 存在一些限制，但它提供的实际隐私保护效果是显著的。Cloudflare 打算继续支持 ESNI，直到 ECH 准备就绪。

ECH 的详细信息

ECH 的目标是加密整个 ClientHello，从而弥补 TLS 1.3 和 ESNI 遗留的漏洞，保护所有涉及隐私的握手参数。与 ESNI 类似，该协议使用通过 DNS 分发并使用 DoH 获取的公钥，在客户端的首次连接中进行加密。但是，ECH 在密钥分发方面有一些改进，使协议更能够应对 DNS 缓存不一致性的问题。ESNI 服务器在解密失败时中止连接，而 ECH 服务器会尝试

完成握手，并提供一个客户端可以用来重试连接的公钥。

但是，如果服务器无法解密 ClientHello，它如何完成握手呢？如图 3 所示，ECH 协议实际上涉及到两个 ClientHello 消息：ClientHelloOuter 和 ClientHelloInner。ClientHelloOuter 按照通常的方式明文发送，而 ClientHelloInner 则作为 ClientHelloOuter 的扩展进行加密发送。服务器只需用其中一个 ClientHello 完成握手：如果解密成功，则使用 ClientHelloInner 进行握手；否则，使用 ClientHelloOuter 进行握手。

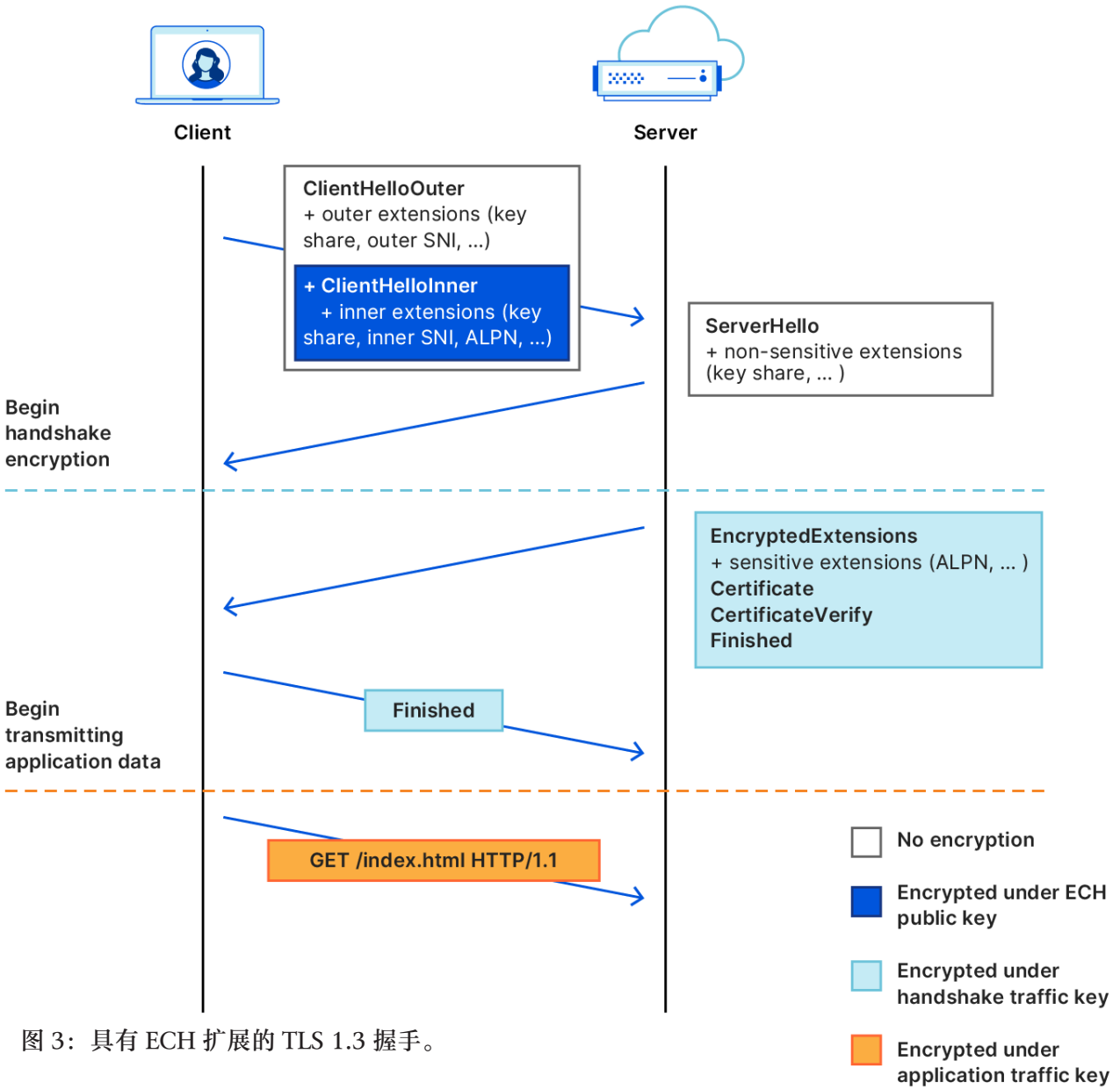


图 3：具有 ECH 扩展的 TLS 1.3 握手。

ClientHelloInner 由客户端用于连接的握手参数组成。这包括敏感值，例如客户端想要连接的源服务器的 SNI（在 ECH 术语中称为“backend server”），ALPN 列表等等。虽然

ClientHelloOuter 也是一个完整的 ClientHello 消息，但它不用于预期的连接。相反，握手由 ECH 服务提供商本身（称为“client-facing server”）完成，向客户端发出信号，告知由于解密失败而无法到达预期的目的地。在这种情况下，服务提供商还会发送正确的 ECH 公钥，客户端可以使用该公钥重试握手，从而“纠正”客户端的配置（这个机制类似于在 TLS 1.3 早期阶段服务器分发公钥用于 0-RTT 模式的方式）。

至少，两个 ClientHello 都必须包含用于服务器身份验证的握手参数。特别是，ClientHelloInner 包含真实的 SNI，而 ClientHelloOuter 也包含一个 SNI 值，客户端在 ECH 解密失败的情况下（即 client-facing server）期望进行验证。如果使用 ClientHelloOuter 建立连接，客户端应立即中止连接，并使用服务器提供的公钥重试握手。客户端不需要在 ClientHelloOuter 中指定 ALPN 列表，也不需要包含任何用于指导握手后行为的其他扩展。所有这些参数都由加密的 ClientHelloInner 封装。

这个设计相当优雅地解决了之前机制在安全部署握手加密时遇到的大部分挑战。重要的是，ECH 的设计不是孤立的。该协议反映了 IETF 社区的多元化观点，并与其他对 ECH 的成功至关重要的 IETF 标准的发展相互配合。

第一个是一个重要的新 DNS 功能，称为 HTTPS 资源记录类型。在高层次上，此记录类型旨在允许为同一域名授权的多个 HTTPS 端点广告不同的 TLS 功能。这使得依赖 DNS 进行密钥分发成为可能，解决了初始 ESNI 部署中发现的部署挑战之一。如果您想深入了解这个新的记录类型以及它对互联网的更广泛意义，请查看 Alessandro Ghedini 最近的博文。

第二个是 CFRG 的混合公钥加密（HPKE）标准，该标准规定了一个可扩展的框架，用于构建适用于各种应用程序的公钥加密方案。特别是，ECH 将其握手加密机制的所有细节委托给了 HPKE，从而实现了更简单、更易于分析的规范。（顺便说一句，HPKE 也是 Oblivious DNS-over-HTTPS 的主要组成部分之一。）

未来的路

当前的 ECH 规范是多年合作的成果。目前，协议的整体设计相对稳定。实际上，下一个规范草案将是首个针对实施之间互操作测试的版本。不过，仍然有一些细节需要解决。让我们用一个简短的概述来结束这篇文章，展望未来的道路。

对抗流量分析

ECH 的最终目标是确保与同一 ECH 服务提供商后面的不同源服务器建立的 TLS 连接彼此不可区分。换句话说，当你连接到一个在 Cloudflare 后面的源时，你和 Cloudflare 之间的网络上的任何人都不能分辨出你到达的是哪个源，以及你和源之间协商的哪些涉及隐私的握手参数。除了立即提升隐私外，如果实现这个目标，它还为 TLS 的部署新功能铺平了道路，而不会损害隐私。

加密 ClientHello 是实现这一目标的重要步骤，但我们还需要做更多工作。我们尚未讨论的一个重要攻击媒介是流量分析。这指的是收集和分析通信通道的属性，这些属性透露了一部分密文的内容，但不会破解基础加密方案。例如，加密的 ClientHello 的长度可能泄漏足够的关于 SNI 的信息，使得攻击者可以对其值做出有根据的猜测（对于特别短或特别长的域名，这种风险尤其高）。因此，每个密文的长度独立于涉及隐私的参数值是至关重要的。当前的 ECH 规范提供了一些缓解措施，但覆盖范围不完全。因此，改进 ECH 对抗流量分析的能力是未来工作的一个重要方向。

僵化的幽灵

ECH 面临的一个重要未解问题是它对网络运营的影响。

从部署 TLS 1.3 的经验中学到的一个教训是，升级核心互联网协议可能触发意外的网络行为。Cloudflare 是最早部署 TLS 1.3 的主要 TLS 运营商之一；当像 Firefox 和 Chrome 这样的浏览器开始以实验性基础启用它时，他们观察到与 TLS 1.2 相比，连接失败率显著增加。这些失败的根本原因是网络的僵化，中间盒（位于客户端和服务器之间的网络设备）会监视并拦截流量，使期望流量呈现特定方式的展示。若在中间盒有机会更新其软件之前更改协议，会导致中间盒尝试解析它们时，遇到无法识别的数据包，触发软件错误，有时会导致连接完全中断。

> 译者注：中间盒是指在网络上的客户端和服务器之间运行的设备或软件组件。它们可能包括防火墙、负载均衡器、入侵检测系统和其他负责监视、过滤或操纵网络流量的设备。

这些中间盒通常需要检查和理解通过它们的流量。然而，如果网络协议发生变化，而中间盒软件没有相应地更新，它可能无法正确解释新的流量模式。这种对协议变化缺乏适应性被称为“网络僵化”。

这个问题如此普遍，以至于在等待网络运营商更新其软件的过程中，TLS 1.3 的设计被修改，以减轻网络僵化的影响。聪明的解决方案是使 TLS 1.3" 看起来像 " 另一个中间盒已知可以容忍的协议。具体而言，线路格式甚至握手消息的内容被设计成类似于 TLS 1.2。当然，这两个协议并不相同 —— 一个好奇的网络观察者仍然可以区分它们 —— 但它们看起来和行为相似到足以确保现有的大多数中间盒不会对它们采取不同的对待。根据经验，这种策略降低了连接失败率，使得 TLS 1.3 的部署变得可行。

同样，ECH 代表了 TLS 的重要升级，而网络僵化的阴影仍然存在。ClientHello 包含了很长时间以来一直存在于握手中的参数，例如 SNI，我们尚不清楚对它们进行加密的影响。为了预防僵化可能引起的部署问题，ECH 协议被设计成尽可能看起来像标准的 TLS 1.3 握手。最显著的区别是 ECH 扩展本身：如果中间盒忽略它，如果它们符合 TLS 1.3 标准的话，那么握手的其余部分看起来和行为上都会很接近正常情况。

尚不清楚这种策略是否足以确保 ECH 的广泛部署。如果 ECH 成功部署并广泛使用，那么这个新功能将有助于减轻未来 TLS 升级对网络运营的影响。加密整个握手过程减少了僵化的风险，因为这意味着软件可以僵化的可见协议特性变少。我们相信这将对互联网的整体健康有益。

结论

旧的 TLS 握手（无意中）泄漏了信息。客户端和服务器的操作需求导致涉及隐私的参数，如 SNI，完全明文进行协商，并可供网络观察者获取。ECH 扩展旨在通过启用完整握手的加密来填补这一漏洞。这代表了 TLS 的重大升级，将在协议不断发展的过程中帮助保护终端用户的隐私。

ECH 标准是一个正在进行的工作。在这个工作继续进行的过程中，Cloudflare 致力于履行自己的责任，确保 TLS 的这一重要升级达到互联网规模的部署。

信息台

稿约

给《方圆》投稿吧！

自助投稿处：https://wj.qq.com/s2/9303354/e607/

稿费标准：

- 小说、散文类：6.0~3.0 〇 / 百字
- 杂谈类：6.0~3.0 〇 / 百字
- 诗歌类：13~7 〇 / 五行
- 影视 / 音乐 / 书籍推荐、教程类：55~30 〇 / 篇
- 其他类：最高不超过 80 〇 / 篇

也可投稿已在社群内部（例如论坛、服务器）中公开发表过的稿件。

详见完整稿约：https://bbs.ria.red/topic/5809/

鸣谢

使用字体

汉仪玄宋

汉仪书仿

思源宋体 SC / Noto Serif CJK SC / Source Han Serif SC

思源黑体 SC / Noto Sans CJK SC / Source Han Sans SC

造字工房尚雅准宋体

霞鹜文楷 / LXGW WenKai

Source Serif 4

Ysabeau

本刊使用的字体大都遵循 SIL 开放字体协议（第 1.1 版），除了：

- “造字工房尚雅准宋体”为专有字体，有其单独的协议，但可以免费用作非商业性用途。
- “汉仪玄宋”“汉仪书仿”为专有字体，有其单独的协议，但可以免费用作非商业性用途。

在此对所有字体贡献者表示感谢和敬意！

图像

尾页公益广告来自青岛市精神文明建设委员会

其他

- Microsoft Word、Adobe InDesign — 排版
- Microsoft Excel — 图表制作
- pdf.js — PDF 预览
- Material Design Icons — 图标
- RIA 运营社 — 大力支持

“文明健康 绿色环保”公益广告

健康生活
合理规划

青岛市精神文明建设委员会办公室

方圆 II

2023 年 10 月刊 / 总第 21 刊

抹岚报社　呈献

服务器 # 杂志 # 儿童读物 // 待续…