三星一直喜欢在A系列手机上给黑科技的导入做实验，这次也不例外。

据韩国媒体Etnews报道，三星5月份将联手本地运营商SK电信，在韩国推出Galaxy A71 5G手机，这将成为世界上第一款采用QRNG（Quantum Random Numeral Generator，量子随机数发生器）芯片的手机。

与非量子密码系统不同，QRNG芯片能够产生真正随机和不可预测的数字，对用户敏感信息的可信认证和加密，因此采用该芯片手机的安全性更高，能够有效防止黑客的攻击。

据悉，QRNG芯片主要面向移动手机、物联网和边缘设备应用，主要特色是利用CMOS图像传感器捕获的光源散粒噪声产生高熵随机数据，主要用于身份验证和加密应用程序的密钥。由于量子密码利用光粒子传递密码信息，一旦发现有收信方和发信方之外的第三方从外部介入，密码会立刻发生改变。从量子物理学上讲，这些都是概率性的，意味着它们可以以健壮、透明和受控的方式产生不可预测的结果。

由于QRNG芯片使用的基本模型提供并描述了完整的熵源，因此可以理解熵源的所有属性，并证明其安全性，从源头上防止黑客的入侵。

为什么要用量子加密？这里就要说到传统计算机和量子计算机在加密和破解上的差别。

以子之盾，防子之矛

加密算法建立在特定数学难题的基础之
上，
如大数分解和离散对数等数学问题构建出加密技术的底层机制，传统计算机如果要暴力破解经过加密的密码，
需要耗费大量的算力和时间
，甚至破解密文所花费的时间远大于该信息的有效时间，破解密文的成本远高于加密信息的价值。

这个时候，我们认为这种常规加密是安全的。

而量子计算
机呈指数增长的恐怖算
力，将对当今密码学构成直接威胁。
数学加密问题的困难性在
量子计算机面前，变得不堪一击

，导致当前保护我们信息安全的密码体系崩塌，涉密信息在量子计算面前只能裸奔。

国内专注数据安全的企业闪捷信息（Secsmart）认为，面对量子计算的威胁，只有量子加
密才是对手。
量子加密技术是量子通信科
学发展的成果之一，主要有量子密钥
（源于量子随机数生成器QRNG）和量子密钥分发（QKD，Quantum Key Distribution）手段。

密钥本质上是一串随机数。常用的软件随机数基于算法生成，又被叫做伪随机数，因为通过种子和算法可以得到确定的密钥，并非真随机数。另外常用的物理混沌随机数，是基于经典物理方法生成，输出结果是确定的，譬如掷骰子，看似随机，但在抛出的任何时刻，测量得到运动状态、受力状况、落地条件等因素，就可以知道确定的结果，也不是真随机。

量子密钥是通过测量光量子态得到的结果，量子态波粒二象性表现在空间分布和动量都是以一定概率存在的，测量只能展示随机的状态，本质上无法预测，是真随机的输出。

用量子密钥取代当前的伪随机数，从根本上消除了密钥随机性的问题，无疑将极大的提高加密的安全性。

除了密钥源的安全性，密钥的安全分发是保证密钥安全的基础保证。闪捷信息在科普文章中表示，传统密钥的安全分发，仍大量存在人工用密码箱传递的情况：因为一旦通过网络传输，现有的传输机制不足以保障密钥的安全。以物理原理为基础的量子密钥分发从根本上解决了密钥传输安全问题。其基本方法是使用量子态来编码信息，通过对量子态的制备、传输和检测来达到安全分发密钥的目的。

根据海森堡测不准原理（不确定性原理），攻击者即使截取了量子信号，也无法有效测准单量子的状态。如果攻击者根据测量结果重新制备一个量子发送给接收方，将不可避免地改变单量子状态，导致解码结果与编码不一致。

量子密钥分发双方可通过检测误码率来判断攻击行为及其强度，并在后处理中进行消除。同时量子相干叠加的特性使得不存在通用的方法获得任意未知单量子的多个精确一致拷贝。在量子密钥分发双方随机调制单量子态时，如果攻击者试图在截获量子信号后复制多个拷贝，将不可避免地导致复制态与初始态存在偏差，进而导致解码结果与编码不一致，量子密钥分发双方同样可进行检测发现和后处理消除。

关于IDQ这款量子随机数发生器芯片

据预计，Galaxy A71
5G使用的QRNG芯片由IDQuantique提供，或者可能是IDQ现有Quantis QRNG芯片的衍生产品。

IDQ官网截图

IDQ的QRNG芯片可提供三种型号，具体取决于尺寸，性能，功耗和认证，以适应各种行业特定需求。其中，Quantis QRNG
IDQ250C2
是第一款专门为手机，物联网和边缘设备设计和制造的量子随机数发生器，外形小巧，体积小巧，功耗低，可用于边缘敏感数据的收集和传输，估计也就是三星这款手机使用的芯片。

另外两个型号是——

Quantis QRNG
IDQ6MC1适合对外部环境干扰至关重要的应用，它已获得AEC-Q100车规认证，可以嵌入到互联汽车的安全系统中以确保可信任且安全的车载和V2X通信；

Quantis QRNG
IDQ20MC1
具有最高的熵吞吐量，并且可以为多个安全应用提供真正且不可预测的随机性。它可以嵌入计算机、便携式计算机、服务器或任何安全设备中。
作为IDQ6MC1，它嵌入了DRBG后处理，符合NIST SP800-90 A / B / C规范。

IDQ官网截图

报道称，为SK电信定制的Galaxy A71 5G可能更名为“Galaxy Quantum”。在包括美国在内的其他市场，标准版Galaxy A71 5G将于今年夏季推出。

该款手机由SK电讯在韩国独家销售，搭载Exynos 980处理器，配有6.7英寸Super AMOLED Plus Infinity-O显示屏和支持FHD+分辨率，拥有32MP前置镜头以及64MP主摄+12MP超广+5MP微距+5MP景深镜头后置四摄组合。电池容量为4500毫安时（典型值），支持25w加速充电功能，预计在韩国市场的价格为500000-60000韩元，约合人民币2900-3300元左右，与国行版本基本上在同一价位。