摩石观察

密码是保障网络安全的核心技术和基础支撑，在维护国家安全、促进经济社会发展、保护人民群众利益中发挥着不可替代的重要作用。“云物移大智”的蓬勃发展，5G、智慧城市、互联网＋政务服务的全力推进，离不开用密码技术来保障网络安全、保护数据安全、保证网上诚信，需要密码学与其他学科深入合作，需要密码产业与其他产业的深度融合，需要产学研管用的真诚协作，需要全社会共同传播密码知识与政策、研究密码应用技术、推进密码应用方案。

为激浊扬清，构建以密码技术为核心、多种技术相互融合的新网络安全体系，推进密码技术科学规范应用，长期深耕于信息安全一线的卫士通公司凝聚了一批国内顶尖的密码专家于 2016 年建立了摩石实验室。依托密码基础理论，探索密码创新实践，解决密码应用难题，培养密码专业人才，摩石实验室致力于让密码技术更好地服务于网络强国、数字中国和智慧社会。

本着共同的愿景，《信息安全与通信保密》杂志社与摩石实验室精诚合作，专门开辟《摩石观察》栏目。立足于密码本真，反思密码实践，《摩石观察》将以密码人的细致严谨叩问密码创新的真理之门，为广大读者了解、认识、掌握、使用密码技术提供准确规范的参考依据；同时我们期望以密码会友，与理想作伴，热忱邀请有志之士共同探索密码理论与应用的最佳实践，为推动金融等重要领域密码应用与创新发展而奋斗。

密码技术在 5G 安全中的应用

郑东[1,2]，张应辉[1]

（1. 西安邮电大学 无线网络安全技术国家工程实验室，陕西省 西安市 710121

2. 摩石实验室 成都卫士通信息产业股份有限公司，北京 100070）

[摘要] 随着第五代移动通信（Fifth Generation：5G）技术标准的完善，5G 在各个领域受到前所未有的关注，然而 5G 依然面临一些安全挑战。针对 5G 终端的接入安全和数据安全问题，指出合适的密码技术解决方案。对于接入认证问题，可以采用无证书密码体制、基于同态加密的数据聚合机制，以及基于身份的聚合签密等密码技术来解决。对于数据存储和共享安全问题，可以采用属性基加密和抗密钥泄露技术来解决。随着 5G 的商用，上述密码技术与 5G 安全研究将具有重要的理论与实际意义。

[关键词] 第五代移动通信；5G 安全；密码学技术；认证

[中图分类号] TP393;TN918　　[文献标识码] A　　[文章编号] 1009−8054（2019）01−

0 引言

随着人们对通信网络的性能和安全需求不断提高，第五代移动通信技术发展迅猛并得到了前所未有的关注。5G 是为实现万物互联而提出的新一代移动通信技术，5G 技术越来越受到各行各业的关注，也成为学术领域研究的一个热点。在 5G 安全研究方面，3GPP、5G PPP、NGMN、ITU-2020 推进组、爱立信、诺基亚和华为也发布了各自的 5G 安全需求白皮书 [1-5]。

目前 5G 还处于发展的初期，面对的挑战也各式各样。未来的 5G 无线网络将具有灵活性、开放性和高度异构性，不仅可以提供传统的语音和数据通信，也有很多新的应用案例，包括从车辆到车辆、车辆到基础设施的通信、智能电网、智能城市以及智慧医疗等等。大规模的设备使用异构无线接入系统进行通信，可能会导致许多互联互通问题，因此需要考虑安全性机制以及无缝切换等问题。5G 无线网络进行通信时，庞大的数据流在网络中含有大量隐私和敏感信息，为了确保隐私不被泄漏，在终端受限的情况下，还需要考虑高效的数据与隐私保护技术。总之，为了促进 5G 的健康快速发展，有必要将 5G 和密码学知识 [6] 相结合。在 5G 安全方面，接入认证、数据采集、数据存储与共享等环节的安全问题值得深入研究。

1 5G 安全中的密码学技术

1.1 无证书密码体制

作为一种新型公钥密码体制，无证书密码体制解决了基于身份密码体制中固有的密钥托管问题，同时克服了传统公钥密码体制所面临的复杂证书管理问题。Al-Riyami 和 Paterson[7] 在 2003 年的亚密会上首次提出了无证书的公钥密码体制，基于椭圆曲线上的双线性对构造了第一个无证书签名方案。Liu 等人 [8] 提出了一种基于无证书短签名的匿名相互认证方案，用于实现车联网中的车辆与路边单元互相认证，该方案在随机预言机模型中的自适应选择消息攻击下具有不可伪造性。Yeh 等人 [9] 提出了一个新的无证书签名方案，适用于物联网环境下的资源受限的智能设备。Jia 等人 [10] 指出 Yeh 等人的无证书签名方案存在安全缺陷，说明敌手可以冒充密钥生成中心为任何用户颁发部分私钥而不被检测到，而且该方案无法抵抗公钥替换攻击。宋等人 [11] 针对当前车联网中匿名认证的安全性与效率问题，提出一种基于非线性对的车联网无证书批量匿名认证方案。该方案采用无证书无双线性对运算的批量认证方式，计算与存储开销较低，这对于高动态的车载网络来说有着重要意义。无证书签名方案是在资源有限的物联网设备中提供安全认证的潜在方法之一，设计可证明安全且高效的无证书签名方案值得进一步研究。

1.2 基于同态加密的数据聚合技术

目前应用最广的同态加密技术是 Paillier 同态加密算法，其特性是对加密后得到的密文实施某种操作的结果。不过这种做法虽然实现了隐私保护，但不具备防伪性，敌手可以伪装成用户伪造密文或篡改密文发给上一级网点，敌手也可以伪装成网点伪造聚合密文或者篡改密

文发送给控制中心。为了解决这个问题，需要把身份身份认证技术融合到具有隐私保护的数据聚合方案中。对于具有隐私保护的数据聚合方案，现已有一些研究成果。Lu 等人[12]结合数字签名技术，基于 Paillier 同态加密算法提出了一种适用于智能电网的数据聚合方案；Zhang 等人[13]通过引入先哈希后点加的思想，提出了一个数据聚合方案；针对智能电网多级网络环境，周等人设计了一种多维数据聚合方案[14]。

1.3 聚合签密技术

在 5G 网络环境下，大量物联网设备的接入认证安全问题也是 5G 网络安全所需要考虑的一个基本问题。签密能够在合理的逻辑步骤内同时实现对消息的签名和加密。随着用户终端数量的增长，现有的接入认证方式会引起系统资源消耗过大和信令拥塞，为了解决这些问题可将基于身份的聚合签密方案引入终端与网络之间的认证，由多个终端生成的多个签密密文可聚合成一个密文，在提高认证效率的同时可以实现数据机密性。2009 年，Selvi 等人提出了一个基于身份的聚合签密方案，并给出了形式化安全性证明[15]。Lu 等人[16]提出一个基于双线性对的无证书聚合签密方案，但方案不具有公开可验证性，且签密和验证阶段的双线性运算个数较多，计算效率不高。为了保护发送者的身份隐私，Hong 等人[17]提出了一个具有隐私保护的聚合签密方案，并说明了该方案在车载网络中的应用。Cao 等人[18]利用聚合签密技术高效地实现了 5G 环境下的设备认证与数据安全传输。

1.4 属性基加密技术

属性基加密 (Attribute-Based Encryption: ABE) 的概念由 Sahai 等人于 2005 年提出[19]。ABE 在保护数据机密性的同时能实现细粒度的访问控制，根据访问策略的实现方式不同，ABE 分为密钥策略下的 ABE (Key-Policy ABE: KP-ABE) 和密文策略下的 ABE(Ciphertext-Policy ABE: CP-ABE) 两大类[20]。在云计算环境下，作为数据拥有者的用户总是希望由自己来制定并实施访问策略。CP-ABE 允许数据拥有者自己制定访问策略，然后将策略直接嵌入在数据密文中，当且仅当数据的使用者的属性满足访问控制策略时，数据使用者才能正确地解密密文，从而达到数据的细粒度访问控制。为了使用户能够快速地找到所需的密文，Wang 等人[21]提出了支持关键字搜索的 ABE 方案；为了减少属性授权中心的权力，文献[22-23]研究了多中心的 ABE 方案；为了提高用户的效率，Li 等人[24]设计了具有外包解密功能的 ABE 方案；为了支持属性的动态撤销，Cui 等人[25]提出了属性可撤销的 ABE 方案；为了缓解数据加密过程的计算负担，文献[26-27]提出了支持离线计算的 ABE 方案；为了防止私钥的滥用，Ning 等人[28]提出了叛逆者可追踪的 ABE 方案。上述方案的访问控制策略是以明文的方式进行存储，这样可能会泄漏一些用户的隐私，因此支持用户属性隐私保护的 ABE 方案值得进一步研究。

1.5 抗泄漏加密技术

抗泄漏密码学旨在设计现实生活中安全的密码方案，即在现实生活中能够抵抗一定程度的边信道攻击的密码学方案。抗泄漏密码方案的

设计已经成为了密码学界研究的热点。2009 年 Akavia 等人首次提出公钥密码体制下的抗边信道攻击方案 [29]。紧接着 Alwen 等人也相继提出新的抗泄漏公钥加密机制，使新方案能抵抗更多泄漏并且是选择密文攻击安全的 [30]。2017 年，Li 等人提出了抗连续密钥泄漏的基于身份的广播加密并证明了其安全性 [31]。2018 年，Zhou 等人基于抗连续泄漏模型构造了一个新的基于身份的加密方案 [32]。Zhan 等人设计了一个抗密钥泄漏的双态仿射函数加密方案，保证在攻击者获得主密钥部分信息的情况下仍具有语义安全性 [33]。Sun 等人构造了抗密钥泄漏基于身份加密的密码方案，并且证明是选择密文安全的 [34]。Hu 等人提出了抗泄漏的基于身份分层的加密方案 [35]。

2 密码技术在 5G 安全中的应用

随着移动互联网、物联网及行业应用的爆发式增长，未来移动通信将面临千倍数据流量增长和千亿设备联网需求。5G 安全机制除了要满足基本通信安全要求之外，还需要为不同业务场景提供差异化安全服务，能够适应多种网络接入方式及新型网络架构，保护用户隐私，并提供开放的安全能力。5G 不同的接入技术有不同的安全需求和接入认证机制，同一个终端在不同接入方式之间进行切换时或用户在使用不同终端进行同一个业务时，要求能进行快速认证以保持业务的延续性从而获得更好的用户体验。5G 作为第五代移动通信网络，把人与人的连接拓展到了万物互联，为智慧城市、智慧医疗和智能电网等领域的发展提供了一种更优的无线解决方案 [36]。由于实际通信的需求及业务类型的多样性、未知性及复杂性等特点，通信网络需适度超前，提前储备，提前满足未来多元化的业务承载需求。5G 网络新的发展趋势，尤其是 5G 新业务、新架构、新技术，对数据安全和用户隐私保护都提出了新的挑战。在 5G 环境下，不仅是人与物的通信，更多的是物与物的通信。面对成百上亿的物联网设备接入与通信，数据的安全与隐私保护非常具有挑战性。

2.1 无证书密码体制在 5G 物联网数据安全采集中的应用

该密码体制可应用于 5G 无线网络环境下基于物联网设备的安全数据采集，减轻传统公钥基础设施中的证书管理负担 [9]。不依赖于受信任的第三方，无证书公钥加密技术便于用户建立私钥和相应的公钥。在 5G 物联网应用场景下，无证书签名系统模型描述如下：首先由密钥生成中心产生一个秘密钥，一个公钥和公开系统参数，密钥生成中心根据接入设备的身份信息以及秘密钥产生接入设备的部分秘密钥。紧接着密钥生成中心把部分秘密钥发送给接入设备，接入设备首先检查部分秘密钥的有效性，若检测通过，那么接入设备选择一个随机数作为秘密钥的另一部分。这样接入设备就依据系统参数、密钥生成中心产生的部分秘密钥和自己产生的另一部分秘密钥最终生成完整的私钥，依据系统参数和自己产生的另一部分秘密钥最终生成公钥。设备可通过自己的私钥来对消息签名，而验证方即可根据设备的公钥来进行认证。

2.2 同态加密在 5G 智能电网电力安全回收中的应用

作为 5G 的一个代表性用例，智能电网的一个重要目标是提高能源利用率。随着物联网技术的快速发展，车联网的研究受到了极大的关注，车联网与智能电网的结合具有非常重要的意义。在智能电网中，为了实时满足海量用户对于电能的需求，把车联网中的海量电动汽车作为储存电能的备用设备具有重要的实际意义 [12]。在用电低峰期，电动汽车停车期间可以通过智能电网进行充电；在用电高峰期，电动汽车可以把多余的电能注入到智能电网中以获取收益。为了保障智能电网的稳定运行，电力公司必须对电动汽车注入的电量进行统计。由于智能电网中的交易敏感性以及电动汽车用电情况涉及到用户隐私，有必要保证电力公司只能获得电动汽车注入的总电量，不能获得某个时隙的电量注入份额。基于同态加密，电动汽车等电能存储单元可以对每一个时隙要注入的电力进行同态加密后发送给聚合网关，网关基于收到的密文，利用同态加密算法的性质可以得到总回收电量的密文，并将密文发送给电力公司。电力公司最后利用自己的私钥进行解密可以得到回收的总电量。

2.3 聚合签密技术在 5G 大规模物联网设备接入认证中的应用

随着无线通信技术的快速发展，出现了种类繁多、数量巨大的物联网终端设备接入网络获得相应的服务。例如智能电网、智能家居、智能城市等，覆盖了能源、家庭、安防等多个行业领域。而大多数物联网终端设备都处于开放的网络环境下，对于安全性需求未给予足够重视的设备很容易遭受到恶意攻击。物联网终端接入方式在 5G 中主要是无线接入，在海量的接入场景下，如果对每个终端逐一进行认证将带来高昂的认证成本，效率也不尽人意。特别地，在很多数据感知应用中，大量的物联网设备通常被同时唤醒，以实现对采集数据的统一收集和处理。在这一过程中，既要考虑设备身份的有效性，又需要考虑未来通信的机密性。采用聚合签密技术，可以让每个物联网设备对采集的数据进行签密，将签密密文发送给一个指定的设备，该设备采用聚合算法对收到的签密密文进行聚合，得到长度很小的密文发送给处理中心。最后由处理中心对签密密文进行验证和解密，同时实现设备的身份认证和所发送数据的可靠性检验 [17]。

2.4 属性基加密技术在云存储安全中的应用

在云计算环境下，为了防止数据拥有者的隐私泄漏，在共享数据前，数据拥有者需要将文件进行加密，当密文上传到云服务前，可以将访问控制策略或属性隐藏 [20]。可以使用属性布隆过滤器将属性隐藏在匿名的访问控制结构中，这样能够实现数据和属性的同时隐藏。在云环境下的数据共享模型中涉及到四个实体：数据拥有者、数据使用者、云服务器和属性授权中心。属性中心负责系统的初始化，然后得到系统的主私钥和公开参数，公布系统参数，同时保存系统主私钥。系统用户，包含数据拥有者和数据使用者，根据自身的属性通过属性中心进行注册，然后属性中心为其分发相应的私钥。数据拥有者通过制定的策略加密文件资

源，然后上传到云服务器上。云服器负责密文的存储。最后，数据使用者下载密文，仅当数据使用者属性满足访问控制结构时才能正确解密密文。

2.5 抗泄漏密码技术在数据安全中的应用

5G 网络中业务和场景的多样性，以及网络的开放性，使用户隐私信息从封闭的平台转移到开放的平台上，隐私泄漏的风险也因此增加 [29]。在公开的云存储网络环境中，数据的共享能够给数据的使用者带来很多便利。在加密过程中，数据拥有者根据指定访问数据的用户身份作为公钥加密数据，在解密过程中，只有数据拥有者指定的用户才能够正确地解密密文。在 5G 环境下，上述过程可以实现数据共享，但用户私钥泄漏的风险也增加了。若解密过程中的私钥部分泄漏或者完全泄漏，则用户的数据隐私将得不到保障。为了避免现有密码算法没有考虑各种攻击存在的情况下而导致的部分隐私泄漏问题，可以采用抗密钥泄漏的基于身份加密算法来进行数据加密上传，解密下载。在抗密钥泄漏的基于身份加密系统中，共有四个实体：数据所有者、共享数据使用者、权威中心、云端数据存储中心。权威中心负责生成系统公开参数和主私钥，并进一步生成公私钥给数据所有者和共享数据使用者；云端数据存储中心负责存储数据；数据所有者负责利用公开参数和共享数据使用者的身份信息加密文件并上传到云存储中心，数据使用者负责下载密文并用自己的私钥解密密文，得到原始数据。只有数据拥有者指定的用户才能够正确解密密文。

3 结语

移动通信技术的每一次更新都为我们的日常生活与工作带了巨大的便利，第五代移动通信发展更是受到各个领域前所未有的关注。在 5G 网络中，大量隐私和敏感信息进行通信传输时，确保隐私不被泄漏已成为人们首要关注的问题。本文对 5G 通信中存在的安全问题进行分析，并且针对该安全问题提出了相应的解决方案。此外，给出了密码学技术在 5G 中的潜在应用场景。

参考文献：

[1] Huawei Technologies Co. 5G opening up new business opportunities. White Paper, 2016.

[2] 3GPP. Study on the security aspects of the next generation system. Technical Report, TR 33.899 v1.1.0, 2017.

[3] 5G PPP. 5G PPP phase 1 security landscape. 2017.

[4] NGMN.5G security recommendations (networking slicing, mobile edge computing). White Paper, 2016.

[5] Nokia. Security challenge and opportunities for 5G mobile networks. White Paper, 2017.

[6] 郑东 , 赵庆兰 , 张应辉 . 密码学综述 [J]. 西安邮电大学学报 , 2013, 18(6):1–10.

[7] Al–Riyami S S, Paterson K G. Certificateless public key cryptography[C]//International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2003: 452–473.

[8] Liu J, Li Q, Sun R, et al. An Efficient Anonymous Authentication Scheme for Internet of Vehicles[C]//2018 IEEE International Conference on Communications (ICC). IEEE, 2018: 1–6.

[9] Yeh K H, Su C, Choo K K R, et al. A Novel Certificateless Signature Scheme for Smart Objects in the Internet of Things[J]. Sensors, 2017, 17(5): 1001.

[10] Jia X, He D, Liu Q, et al. An efficient provably–secure certificateless signature scheme for Internet of Things deployment[J]. Ad Hoc Networks, 2018, 71: 78–87.

[11] 宋成 , 张明月 , 彭维平 , 等 . 基于非线性对的车联网无证书批量匿名认证方案研究 [J]. 通信学报 , 2017, 38(11): 35–43.

[12] Lu R, Liang X, Li X, et al. Eppa: An efficient and privacy–preserving aggregation scheme for secure smart grid communications[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(9): 1621–1631.

[13] Zhang Y, Zhao J, Zheng D. Efficient and privacy–aware power injection over AMI and smart grid slice in future 5G networks[J]. Mobile Information Systems, 2017.

[14] 周华 , 陈杰 , 张跃宇 , 等 . 智能电网多级网络下多维数据聚合方案 [J]. 密码学报 , 2017, 4(2):114–132.

[15] Selvi S S D, Vivek S S, Shriram J, et al. Identity based aggregate signcryption schemes[C]// International Conference on Cryptology in India. Springer, Berlin, Heidelberg, 2009: 378–397.

[16] Lu H, Xie Q. An efficient certificateless aggregate signcryption scheme from pairings[C]// Electronics, Communications and Control (ICECC), 2011 International Conference on. IEEE, 2011: 132–135.

[17] Hong Z, Tang F, Luo W. Privacy–Preserving Aggregate Signcryption for Vehicular Ad Hoc Networks[C]//Proceedings of the 2nd International Conference on Cryptography, Security and Privacy. ACM, 2018: 72–76.

[18] Cao J, Yu P, Ma M, et al. Fast Authentication and Data Transfer Scheme for Massive NB–IoT Devices in 3GPP 5G Network[J]. IEEE Internet of Things Journal, 2018.

[19] Sahai A, Waters B. Fuzzy identity–based encryption[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2005: 457–473.

[20] Goyal V, Pandey O, Sahai A, et al. Attribute–based encryption for fine–grained access control of encrypted data[C] ACM Conference on Computer and Communications Security. ACM, 2006:89–98.

[21] Wang H, Dong X, Cao Z, et al. Secure and Efficient Attribute–Based Encryption with Keyword Search[J]. The Computer Journal, 2018.

[22] Li J, Chen X, Chow S S M, et al. Multi–authority fine–grained access control with accountability and its application in cloud[J]. Journal of

Network and Computer Applications, 2018, 112: 89–96.

[23] 关志涛 , 杨亭亭 , 徐茹枝 , 等 . 面向云存储的基于属性加密的多授权中心访问控制方案 [J]. 通信学报 , 2015, 36(6):116–126.

[24] Li Q, Zhu H, Ying Z, et al. Traceable Ciphertext–Policy Attribute–Based Encryption with Verifiable Outsourced Decryption in eHealth Cloud[J]. Wireless Communications and Mobile Computing, 2018, 2018.

[25] Cui J, Zhou H, Zhong H, et al. AKSER: Attribute–based keyword search with efficient revocation in cloud computing[J]. Information Sciences, 2018, 423: 343–352.

[26] Ma H, Zhang R, Yang G, et al. Concessive Online/Offline Attribute Based Encryption with Cryptographic Reverse Firewalls—Secure and Efficient Fine–Grained Access Control on Corrupted Machines[C]//European Symposium on Research in Computer Security. Springer, Cham, 2018: 507–526.

[27] 张凯 , 马建峰 , 张俊伟 , 等 . 在线 / 离线的可追责属性加密方案 [J]. 计算机研究与发展 , 2018, 55(1):216–224.

[28] Ning J, Cao Z, Dong X, et al. White–box traceable CP–ABE for cloud storage service: How to catch people leaking their access credentials effectively[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(5): 883–897.

[29] Akavia A, Goldwasser S, Vaikuntanathan V. Simultaneous hardcore bits and cryptography against memory attacks[C]//Theory of Cryptography Conference. Springer, Berlin, Heidelberg, 2009: 474–495.

[30] Alwen J, Dodis Y, Wichs D. Leakage–resilient public–key cryptography in the bounded–retrieval model[M]//Advances in Cryptology–CRYPTO 2009. Springer, Berlin, Heidelberg, 2009: 36–54.

[31] Li J, Yu Q, Zhang Y. Identity–based broadcast encryption with continuous leakage resilience[J]. Information Sciences, 2018, 429: 177–193.

[32] Zhou Y, Yang B, Mu Y. Continuous Leakage–Resilient Identity–Based Encryption without Random Oracles[J]. The Computer Journal, 2018, 61(4): 586–600.

[33] 张明武 , 杨波 . 抗主密钥泄露和连续泄露的双态仿射函数加密 [J]. 计算机学报 , 2012: 1856–1867.

[34] Sun S F, Gu D, Liu S. Efficient chosen ciphertext secure identity–based encryption against key leakage attacks[J]. Security and Communication Networks, 2016, 9(11): 1417–1434.

[35] Hu C, Liu P, Guo S, et al. Anonymous hierarchical identity–based encryption with bounded leakage resilience and its application[J]. International Journal of High Performance Computing and Networking, 2017, 10(3): 226–239.

[36] Zhang Y, Li J, Zheng D, et al. Privacy–preserving communication and power injection over vehicle networks and 5G smart grid slice[J].

Journal of Network and Computer Applications, 2018, 122: 50–60.

作者简介：

郑东，西安邮电大学教授，博士，主要研究方向为无线网络安全与编码密码学，摩石实验室兼职专家。

张应辉，西安邮电大学教授，博士，主要研究方向为公钥密码学、无线网络安全和云存储安全。

The Application of Cryptography in 5G Security

ZHENG Dong[1,2] ZHANG Ying-hui[1]

(1. National Engineering Laboratory for Wireless Security, Xi'an University of Posts & Telecommunications, Xi’an 710121, China；

2. Westone Cryptologic Research Center, Westone Information Industry Inc. Beijing 100070, China)

[Abstract] With the improvement of technology standards of the fifth generation (5G) mobile communication, 5G has received unprecedented attention in various fields. However, many security challenges remain in 5G. To address the access security and data security issues of 5G terminals, the appropriate solutions based on cryptographic technology are specified. As for the access authentication problem, some cryptographic technologies can be adopted, such as certificateless cryptography, data aggregation mechanisms based on homomorphic encryption, and identity-based aggregation signcryption. For the security problems of data storage and sharing, attribute-based encryption and leakage resilience techniques can be exploited. With the commercialization of 5G, the above cryptography and 5G security research will be of theoretical and practical significance.

[Keywords] The 5th Generation Mobile Communication; 5G Security; Cryptography Technology; Authentication