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，需要密码学与其它学科深入合作，需要密码产业与其它产业的深度融合，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。

全同态加密的发展与应用

王付群
（杭州师范大学理学院 讲师、卫士通摩石实验室兼职专家）

1976年，Diffie和Hellman[DH76]开创了公钥密码学，在密码学发展中具有划时代的意义。不久，Rivest等人[RSA78]提出第一个公钥加密方案：RSA加密方案。Rivest等人[RAD78]随后就指出RSA加密系统具有乘法同态性质：给定两个密文$C_1=m_1^8 \bmod N$和$C_2=m_2^8 \bmod N$，通过计算，$c_1 \cdot c_2 \bmod N=(m_1m_2)^8 \bmod N$，我们就可以在不掌握私钥信息的情况下“同态”计算出明文$m_1 \cdot m_2$的有效密文。根据此发现，他们提出了“全同态加密”(Fully Homomorphic Encryption, FHE)的概念(当时称为私密同态，Privacy Homomorphism)。

尽管上述RSA公钥加密方案是乘法同态的，但是由于它是一个确定性的公钥加密方案，因而不是语义安全的。第一个语义安全的公钥

加密方案由 Goldwaser 和 Micali[GM82] 提出，并且当明文空间为 {0,1} 时，它是加法同态的。另外，ElGamal[ElG84] 语义安全加密方案是乘法同态的。上述方案具有一个共同点：它们都只能支持同态计算一种运算，或者加法，或者乘法，因此被称为单同态加密。

近年来，云计算受到广泛关注，它拥有强大的计算能力，可以帮助人们执行复杂的计算。但是，在保护用户数据私密性的前提下，如何利用云计算的强大计算能力是云计算从理论走向实用必须解决的关键问题。在此迫切需求下，全同态加密如约而至。从数学上说，同态就是保持运算，即先运算再同态与先同态再运算所得到的结果是一样的。而全同态加密是一类特殊的加密方案，它允许用户通过加密保护数据的私密性，同时允许服务器（比如“云”）对密文执行任意可计算的运算 (同时包含加法、乘法)，得到的结果是对相应明文执行相应运算结果的某个有效密文。这个特性对保护信息的安全具有重要意义：利用全同态加密可对多个密文进行同态计算之后再解密，不必对每个密文解密而花费高昂的计算代价；利用全同态加密可以实现无密钥方对密文的计算，既可以减少通信代价，又可以转移计算任务，由此可平衡各方的计算代价；利用全同态加密可以实现让解密方只能获知最后的结果，而无法获得每个密文的消息与同态计算方式，可以提高信息的安全性。正是由于全同态加密技术在计算复杂性、通信复杂性与安全性上的优势，越来越多的研究力量投入到其理论和应用的探索中。

鉴于全同态加密的强大功能，一经提出便成为密码界的公开问题，被誉为“密码学圣杯”，由 Gentry 在 2009 年摘取。之后，全同态加密迅速吸引了一批资深专家、学者对之进行广泛、深入的研究，并取得了一系列的成果。目前可以构造全同态加密的密码学假设主要有：理想格上的理想陪集问题（Ideal Coset Problem, ICP）、整数上的近似最大公因子问题（Approximate Greatest Common Devisior, AGCD）、带错学习问题（Learning with Errors, LWE）等等。

下面我们先从从构造技术的发展来分类介绍全同态加密的研究进展，然后给出一个简单易懂的全同态加密实例，最后介绍全同态加密的典型应用。

1 全同态加密的发展现状

1.1 第一代全同态加密

2009 年，Gentry [Gen09] 取得突破性进展，构造出第一个全同态加密方案（Fully Homomorphic Encryption, FHE）摘取了“密码学圣杯”。Gentry 设计了一个构造全同态加密方案的 “蓝图”：首先构造一个类同态加密（Somewhat Homomorphic Encryption, SHE）方案（这类方案能够同态计算一定深度的电路）；然后压缩解密电路（需要稀疏子集和假设），使得它能够同态计算它本身的增强的解密电路，得到一个可以“自举”（Bootstrapping）的同态加密方案；最后有序执行自举操作（需要循环安全假设），得到一个可以同态计算任意电路的方案，即全同态加密。同时，基于理想格上的 ICP 假设，并结合稀疏子集和与循环安全假设，他也开创性地构造了一个具体的方案。

随后，van Dijk 等人 [vDGHV10] 提出了一个整数上的全同态加密方案，这个设计完全模仿了 Gentry 的蓝图。该方案的安全性基于 AGCD 假设和稀疏子集和假设。它的主要优点在于概念简单，易于理解，其缺点在于公钥太大。

这些被称为第一代全同态加密方案。

1.2 第二代全同态加密

随着 Gentry 全同态加密方案的提出，人们开始尝试基于 (R)LWE 构造全同态加密方案，并结合理想格的代数结构、快速运算等优良性质来进行方案的优化和实现，最终取得了巨大的成功。

2011 年，Brakerski 和 Vaikuntanathan [BV11a, BV11b] 基于 LWE 与 RLWE 分别提出了全同态加密方案，其核心技术是再线性化和模数转换。这些新技术的出现使得我们无需 压缩解密电路，从而也就不需要稀疏子集和假设，这样方案的安全性完全基于 (R)LWE 的困难性。Brakerski 和 Vaikuntanathan [BV11b] 还提出了循环安全的类同态加密方案。但是，他们的方案不能够利用自举以达到全同态的目的，这是因为他们所得到的循环安全是相对于私钥作为环元素表示的，而不是自举算法所需要的比特表示。构造循环安全的可自举的同态加密依然是一个公开问题。

Brakerski 等人 [BGV12] 指出：依次使用模数转换能够很好的控制噪音的增长。据此他们设计了一个层次型的全同态加密方案：BGV。层次型全同态加密可以同态计算任意多项式深度的电路，从而在实际应用中无需启用计算量过大的自举。

研究人员对 BGV 方案做了大量的优化、实现 [GHS12a, GHS12b, GHS12c, AP13, HS14, HS15, HS18]，对 BGV 方案的研究越来越深刻、完善，效率也越来越高。其中，Halevi 和 Shoup [HS14] 先是针对 BGV 算法开发了 Helib 库，随后实现了 BGV 自举算法 [HS15]：在打包的情形下（对约 300 比特消息实施自举），一次自举算法大约耗费 5 分钟。分销来看，1 个比特的自举大约需要 1 秒。最近，Halevi 和 Shoup [HS18] 又改进了该自举技术，最快可提升速度大约 75 倍，使得自举时间降到了大约 13ms。目前来看，（优化后的）BGV 方案是最高效的全同态加密方案之一。

2012 年，Brakerski [Bra12] 又提出了一个基于 LWE 的无模数转换的全同态加密方案，该方案不需要模数转换管理噪音，也能够很好地控制噪音的增长。

以上方案与第一代方案相比，无需压缩解密电路，也就不需要稀疏子集和假设。这样一来，方案的效率与安全性都得到极大的提升，但在同态计算时仍然需要计算密钥的辅助，故被称为第二代全同态加密方案。

1.3 第三代全同态加密

上述所有方案无论是层次型的还是纯的全同态加密，都需要“计算密钥”（私钥信息的加密，可以看做公钥的一部分）的辅助才能达到全同态的目的。但是计算密钥的尺寸一般来说都很大，是制约全同态加密效率的一大瓶颈。

2013 年，Gentry 等人 [GSW13] 利用“近似特征向量”技术，设计了一个无需计算密钥的全同态加密方案：GSW，标志着第三代全同态加密方案的诞生。他们进而还设计了基于身份

和基于属性的全同态加密方案，掀起了全同态加密研究的一个新高潮。此后，研究人员在高效的自举算法、多密钥全同态加密、CCA1 安全的全同态加密和电路私密的全同态加密等方面进行了大量的研究，得到了丰硕的成果。下面逐一介绍。

1.3.1 高效的自举算法

Brakerski 和 Vaikuntanathan [BV14] 在 GSW 的基础上，设计了第一个安全性与普通的基于 LWE 的公钥加密算法的安全性相当的全同态加密算法，使得全同态加密的安全性进一步得到了保障。他们的主要技术就是利用 GSW 方案的噪音增长是非对称的性质，结合 Barrington 定理构造了一个能够很好控制噪音增长的自举算法。

Alperin-Sheriff 和 Peikert [AP14] 基于上述新成果 [GSW13, BV14]，提出了一个更简单的对称的 GSW 方案，并用之设计了一个快速的自举算法：直接同态计算解密函数。该自举方法直接、简单、高效，向实际应用迈出了坚实的一步。Hiromasa 等人 [HAO15] 提出了一个打包形式的 GSW 方案（要假定循环安全假设成立），并结合 [AP14] 巧妙地设计了一个打包形式的自举算法，效率得到了一定的提高。

Ducas 和 Micciancio [DM15] 在 [AP14] 的基础上，利用一个变形的基于 RLWE 的 GSW 方案来直接同态计算解密函数，大大提升了效率，他们的测试表明：1 秒内就可以完成一次自举过程。Chillotti 等人 [CGGI16] 改进了 [DM15] 的方案，在自举时，他们巧妙地用矩阵与向量间的运算来代替矩阵与矩阵间的运算，有效地降低了自举所花费的时间：0.1 秒内就可以完成一次自举过程。随后，Chillotti [CGGI17] 等人又改进这一自举过程至 13ms。从公开发表的文献来看，这是目前最高效的自举方案之一。

此外，Gama 等人 [GINX16] 也在 [AP14] 的基础上设计了一个更高效的自举算法：运行一次自举算法累积的噪音的上界是线性的。这意味着全同态加密的安全性与公钥加密的安全性是一致的（除了额外的循环安全要求）。

1.3.2 多密钥全同态加密

López-Alt 等人 [LTV12] 最先开始研究多密钥全同态加密，他们基于 NTRU 构造了第一个多密钥全同态加密，并利用它设计了一个多方安全计算协议。但是，他们的方案用到了一个非标准的假设，并且近年来也遭受到比较严重的攻击。所以设计安全的多密钥全同态加密引起了人们的注意，并研究出多个基于 LWE 的多密钥全同态加密 [CM15, MW16, PS16, BP16]。其中，[CM15, MW16] 的多密钥全同态加密方案的密文会随着不同的密钥数的增长而膨胀，而且同态计算后的密文不能继续执行同态运算。Peikert 等人 [PS16] 利用全同态加密 [GSW13] 与全同态签名 [GVW15]，一定程度上解决了上述两个问题。Brakerski 等人 [BP16] 提出了完全动态的多密钥全同态加密，基本解决了上述两个问题。但是，他们利用了笨重的自举技术，并不实用。

1.3.3 CCA1 安全的全同态加密

CCA 安全对于加密来说已经成为标准的安全性要求。遗憾的是 CCA 安全与同态性质是矛盾的，不可能同时实现。但是，可以通过控制同态计算来达到 CCA 安全。赖俊祚等人 [LDM+16] 提出了第一个 CCA2 安全的密钥控制的全同态加

密方案。但是他们的方案利用了不可区分混淆器来验证密文的合法性。

众所周知，CCA1 安全与同态性质并无矛盾之处，它们可以共存。Canetti 等人 [CRRV17] 研究了 CCA1 安全的全同态加密方案，给出了 3 个构造：前两个都是由多身份全同态加密转化而来（我们也提出了这个转化方式，遗憾的是未能及时发表），并构造了两个多身份全同态加密方案，第三个使用了 SNARKs，得到了一个紧凑的方案。前两个构造的缺点是密文不紧凑，第三个构造建立在非标准的假设上。

1.3.4 电路私密的全同态加密

在全同态加密领域，有时不但要保护好数据的私密性，而且要保护好电路的私密性。电路的私密性是指同态计算出来的密文不泄露电路的任何信息，也就是说只有执行同态运算的人才知道电路，而其他人 (包括解密者) 都不能从同态计算出来的密文挖掘出电路的信息。

Gentry[Gen09a] 在提出全同态加密的时候就已经考虑了这个问题，他建议在输出同态计算密文之前，给它增加一个大的噪音，完全掩盖该密文所隐含的同态计算所积累的噪音。这一方法的缺点也是明显的：这样的密文所含的噪音太大，故不能再对它执行同态运算了。

Ducas 等人 [DS16] 多次调用自举算法来控制同态计算后的噪音分布，使得同态计算后的密文的噪音分布与新鲜密文的噪音分布是统计不可区分的。他们的方法可以运用到所有 (理想) 格全同态加密方案 [Gen09a, Gen09b, BGV12, Bra12, GSW13]。这个方法依赖于高效的自举算法，目前并不可行。

Bourse 等人 [BPMW16] 利用高斯噪音的特性，巧妙地部分解决了上述方案的缺点：在同态计算的每一步，只需要增加一个与当前噪音大小相当的高斯噪音，即可一定程度上保证电路的私密性。这个技巧的优点是避免了复杂的自举，缺点是泄露了电路的深度。

Chongchitmate 等人 [CO17] 研究了存在恶意用户情形下的多密钥全同态加密，提出了一个一般的转换，可以把任意非电路私密的多密钥全同态加密转换为电路私密的多密钥全同态加密。

在短短的 10 年内，国际上在全同态加密技术方面已经取得了丰硕的成果，全同态加密也从第一代发展到了第三代，其效率与安全性都得到了极大地提升。

2 全同态加密实例：GSW

2013 年，Gentry 等人 [GSW13] 利用“近似特征向量”技术，设计了一个无需计算密钥的层次型全同态加密方案：GSW，标志着第三代全同态加密方案的诞生。在很多应用场景下，层次型全同态加密的同态能力就足够了。由于 GSW 无需计算密钥参与同态计算，所以它是最简单最易理解的全同态加密。这里我们以 GSW 为例，说明全同态加密的设计思想。

全同态加密除了传统公钥加密拥有的密钥生成、加密、解密等算法外，还有一个同态计算算法。为了清晰地叙述 GSW，我们增加了参数设置算法 Setup，并把密钥生成算法分解为私钥生成算法和公钥生成算法。注意到任意电路可以分解为一系列的加法和乘法运算，因此

我们还把同态计算算法分解为同态加法和同态乘法。

为了详细描述 GSW，我们需要两个工具：一个是 Regev [Reg05] 提出的 LWE，用来保证 GSW 的安全性，另一个是 Micciancio 和 Peikert [MP12] 提出的矩阵 G，用来支持同态计算。

· 考虑有限域 Zq, 判定型 LWE 就是区分 (B, sB + e) 与 (B, u)， 这里 $B \leftarrow Z_q^{(n-1)\,m}$, $s \leftarrow Z_q^{n-1}$, $e \leftarrow D^m$, $u \leftarrow Z_q^m$。Regev 证明了 LWE 是困难的。目前人们普遍认为LWE 甚至是抵抗量子攻击的。

· 设 G 是一个具有下面性质的公开矩阵：对任意的 u，容易抽取满足 $G\,G^{-1}(u) = u$ 的短向量 $G^{-1}(u)$。

现在我们详细描述 GSW 方案：

· Setup(1^n,1^L): 给定安全参数 n，最大同态深度 L，选取公共参数 prms = (n,m,q,D), 令 $K=\lfloor \log q \rfloor +1$。

· SKGen(prms): 随机选取 $s \leftarrow Z_q^{n-1}$, 令私钥 $sk = t = (-s\|1) \in Z_q^n$。

· PKGen(sk): 随机选取矩阵 $B \leftarrow Z_q^{(n-1)\times m}$, 抽取高斯错误 $e \leftarrow Dm$, 计算 b = sB+e, 令公钥 $pk = A = (B, b) \in Z_q^{n\times m}$。

· Enc(μ,pk): 给定明文消息 $\mu \in \{0,1\}$, 随机选取矩阵 $R \leftarrow Z_2^{m\times nk}$, 计算密文 $C = AR+\mu G \in Z_q^{n\times nk}$。

· Dec(sk, C): 令 $w = (0,0,...,q/2)^T$, 先计算 $tC-G^{-1}(w) = \mu tw+e= \mu q/2 + e$，再根据该数值的大小判定出消息是 0 还是 1。

注意：只要密文满足形式 C = AR+μG（称为解密形式）且 R 是一个小矩阵，就可以成功解密。

· Add: $C_1 \oplus C_2 = C_1 + C_2 = B(R_1+R_2) + (\mu_1+\mu_2)G$，可见同态加法满足解密形式。

Multi: $C_1 \oplus C_2 = C_1 - G^{-1}(C_2)$

注意到 $C_1\,G^{-1}(C_2) = (BR_1 + \mu_1 G)\,G_{-1}(C2)$

$= BR_1\,G_{-1}(C_2) + \mu_1\,G\,G^{-1}(C_2)$

$= BR_1\,G^{-1}(C2) + \mu_1\,C_2$

$= BR_1\,G_{-1}(C2) + \mu_1(BR_2 + \mu_2 G)$

$= B(R_1\,G{-}1(C_2) + \mu_1 R_2) + \mu_1\mu_2 G$

可见，同态乘法也满足解密形式。

方案说明：GSW 是一个层次型的全同态加密方案，可以设置最大深度 L=poly(n)。但是，如果想同态计算任意的电路，还是需要利用自举来增强同态计算能力。必须注意的是 GSW 尽管是最简单最易理解的全同态加密，但它并不是最高效的。在 GSW 基础上，除了可以设计具有访问控制功能的全同态加密 [GSW13, CM15]，它还可以用来加速自举 [AP14, DM15, CGGI16, CGGI17]，也许这才是 GSW 的最大意义之所在。

3 全同态加密的若干应用

该节我们举例说明全同态加密的潜在应用。我们将展示全同态加密在各个领域应用的广泛性，以此说明这项技术的重要性。

3.1 全同态加密在基因组学中的应用案例

隐私数据共享已经大大限制了基因组学的发展。DNA 和 RNA 序列可以迅速而廉价产生，因此大量的此类序列在不同的实验室和医疗机构累积。预计在二十年内，世界上大多数人将拥有全基因组序列。这是一个在生物学，医学和人类历史的研究中强大的工具，许多复杂疾病或流行病学研究需要数千个样本来探究致病

模式，并设计治疗方案。然而，人类 DNA 和 RNA 序列就像指纹一样是生物识别标识符，它们可以传达重大疾病风险或国民身份标志等信息起源，例如阿尔茨海默氏症等位基因的存在或非亲属的检测（亲子鉴定）。一旦这些数据被释放后，他们永远无法取回或撤回。因此，广泛分享这些隐私数据存在很大的挑战。

目前用于保护基因组学数据的策略具有很高的开销，更好的解决方法是将基因组数据共享的一些用例映射到数据的简单操作，这就非常适合全同态加密。人类在 3B 碱基对基因组序列中彼此几乎相同，这意味着基因组数据可以简化为简单的差异向量。基因组序列的改变，变体或突变，可以从序列中挑选出来，这些基因型和表型的共享在许多设置中很有用。

例如，医生在乳腺癌患者或他们的家庭成员中测试乳腺癌基因会经常检测出具有未知意义的新变种，但却无法为他们的患者乳腺癌复发或家族性风险提供建议。检测到的变体实际上是致病性的吗？或者它是变异正常背景的一部分？如果可以收集和分析这些来自世界上成千上万诊所的基因型和表型数据，那么更多未知意义的变种或变异就可以被人们理解。因此，差异基因统计可以统计出哪些变异会导致疾病，哪些不会。

基因匹配是类似的，带有遗传疾病的儿童可以通过寻找在任一亲本中未发现的从头变体来检测具有遗传疾病的原因。通过与长辈的基因比对，从而发现孩子疾病的根源，多个实例就可以推断出致病的基因。确定疾病的遗传原因有时可以导致治疗得到很大改善，比如 Beery 双胞胎，他们在经历了多年的严重身体残疾之后现在过着正常的生活。

这些例子都依赖于类似的可用全同态加密来支持的基本数据操作。全同态加密的使用可以允许将不同的基因组数据集上传到云中并用于精确医疗，从而改善患者的健康和福祉。上述案例是许多基因组应用的代表，可以从全同态加密技术中受益。

3.2 全同态加密在国家安全 \ 关键基础设施中的应用案例

假定智能电网提供具有 n 个节点的网络，其中每个节点产生大量数据（每个节点可以代表单个发电机 / 建筑物或单个微电网等）。大型智能电网 / 市政 / 政府监控每个节点产生的数据。监控机构可以将监控和计算工作外包给公共云，并使用同态加密对来自网格上每个节点的状态数据进行计算。如果每个节点代表一个单独的微电网，那么状态测量可能包括发电和使用，物理设备温度，能量流等。如果节点代表不同的智能建筑，那么状态测量可能包括当前的能量使用（此类信息可用于检测建筑系统中的异常和入侵，例如，受恶意软件感染的设备的存在）。由于此基础设施的关键作用，保护信息不受影响并确保它不能被敌手干扰，对来自电网的数据执行分析并用于控制电网和电力分配。因此，为了允许云计算用于分析数据，必须确保云对潜在的攻击具有敏感性。

全同态加密可以提供这样的安全性。在这个场景中，不断地对网格中每个节点进行测量，得到的测量值被同态加密后发送到基于云的平台进行计算和分析。能量使用和这些度量被发

送到基于云的平台，在那里计算它们，计算的加密结果被发送到决策中心进行分析。

智慧城市提供类似的重要场景。例如，如果发生需要城市警察，消防部门和多辆救护车的汽车事故，城市的基于云的平台可以快速加载服务器，向特定的城市部门发送信息请求（例如，警察，消防，救护车，运输等），从每个部门分配物资，规划从事故现场到合适医院的最佳路线。这些应用需要不同类型的计算，其中一些使用全同态加密相对容易，例如计算描述性统计。然而，计算的某些方面可能需要额外的研究，例如实体统一和比较等。

3.3 全同态加密在健康保健中的应用案例

健康保健系统必须在保护敏感信息不被泄露的环境中运行，并且可用于日常操作。但是泄露风险与可操作功能之间难以平衡：2015 年，健康保险公司 Anthem 泄露了 8000 万条记录，该泄露事件的总损失成本预计将超过 10 亿美元，证明了这种平衡未得到正确维护。

尽管网络保险可以提供一些保护免受此类损害，但是小型医院和诊所通常会发现此类保险不可用。实际上，此类保险最低政策的价值目标是收入至少为 20 亿美元的公司，而且保费很高：每 100 万美元的保险费通常为 3500 美元。据统计，缺乏实用保护措施导致 60% 小型公司受重大数据泄露影响后在 6 个月内倒闭。

全同态加密有助于解决风险 – 功能平衡问题并且可在医疗保健行业的一些应用中实现信息共享。计费和报告生成是两个应用程序，在这两种应用场景下，分析师都需要访问个人医疗记录来计算其内容的某些部分。通过允许这样的计算而隐性显示那些记录，可以避免隐私泄露，且不会破坏日常操作。全同态加密在医疗环境中实现防止泄露的工作流程如下：分析师查询当前的医疗记录，以收集诸如诊所提供的处方或医疗交流的统计数据等信息。不受信任的服务器可能拥有加密的相关数据集，包括受 HIPAA 保护或其他相关隐私法规和政策约束的个人医疗记录。全同态加密允许在保持加密的同时对查询进行计算，并向分析师返回加密的查询结果。然后，分析师在可信平台上解密查询结果，得到相关报告或单据中包含的查询结果。由于数据在存储和计算时都保持加密状态，因此任何敌手都不会了解数据或此类查询的结果。

可见，医疗保健组织（尤其是小型医疗机构）的数据隐私和公用事业需求之间需要较好的权衡，否则会对医疗保健组织和他们的病人都会带来灾难性后果。全同态加密可为此类平衡提供新颖的解决方案，并且成本是比较小的。

3.4 全同态加密在保护控制系统中的应用案例

控制系统或网络物理系统是一个控制信号操作物理系统的计算机系统，它由具有传感器和执行器的设备和控制器组成。控制器从传感器接收传感数据，利用用户输入对其进行处理以计算命令数据，并发送到按照命令操作设备的执行器。它涵盖了许多系统，包括智能汽车，无人机和核电站等。有很多关于黑客控制系统的报告：在 2010 年，铀浓缩设施中的恶意计算机蠕虫进入计算机系统，并且改变了离心机的转速以破坏它们。2015 年，一名黑客展示了如何远程控制汽车的制动器和加速器。防止黑客

攻击控制系统非常重要，但被认为是一个难题。人们建议传感器在加密后向控制器发送数据，并在加密后向控制器发送控制数据。它可以防止黑客攻击敏感数据和控制命令，但不能阻止控制器内部的恶意软件泄露数据。

最近，一些研究人员建议使用全同态加密来保护控制系统[KLS+16]，即利用FHE加密传感数据。在这种情况下，控制器不需要解密敏感数据后，再来对之处理，因此可以对控制器本身保密。此外，黑客对加密数据的任何操纵都可能被执行器的检测系统检测到。为了更加保证，可以考虑使用同态认证加密或者全同态签密。对该问题的挑战应该是实时运行，目前还没有如此高效的全同态加密。

随着全同态加密效率的提高，其应用也逐步提上议程，学术界与工业界联合，于2017年启动了同态加密的标准化工作与应用研究[ACC+18a, ACC+18b]，以此推动同态技术的快速发展与工业应用。据专家预测，在3–5年内，全同态加密就会在一些场合得到启用。

参考文献

[ACC+18a] D. Archer, L. Chen, J. Cheon, et al. Homomorphic Encryption Standard. Available at http://homomorphicencryption.org/standard/

[ACC+18b] D. Archer, L. Chen, J. Cheon, et al. Applications of Homomorphic Encryption. Available at http://homomorphicencryption.org/standard/

[AP13] J. Alperin–Sheriff and C. Peikert. Practical Bootstrapping in Quasilinear Time. In CRYPTO 2013, LNCS vol. 8042, pp. 1–20. Springer, 2013.

[AP14] J. Alperin–Sheriff and C. Peikert. Faster Bootstrapping with Polynomial Error. In CRYPTO (I) 2014, LNCS vol. 8616, pp. 297–314. Springer, 2014.

[BGV12] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. Fully Homomorphic Encryption without Bootstrapping. In ITCS 2012, pp. 309–325.

[BPMW16] F. Bourse, R. Del Pino, M. Minelli and H. Wee. FHE Circuit Privacy Almost For Free. In CRYPTO 2016.

[BP16] Z. Brakerski and R. Perlman. Lattice–Based Fully Dynamic Multi–Key FHE with Short Ciphertexts. In CRYPTO 2016.

[Bra12] Z. Brakerski. Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. In CRYPTO 2012, LNCS vol. 7417, pp. 868–886.

[BV11a] Z. Brakerski and V. Vaikuntanathan.. Efficient Fully Homomorphic Encryption from (Standard) LWE. In FOCS 2011, pp. 97–106.

[BV11b] Z. Brakerski and V. Vaikuntanathan. Fully Homomorphic Encryption from Ring–LWE and Security for Key Dependent Messages. In CRYPTO 2011, LNCS vol. 6841, pp. 505–524. Springer, 2011.

[BV14] Z. Brakerski and V. Vaikuntanathan. Lattice–Based FHE as Secure as PKE. In ITCS 2014, pp. 1–12.

[CGGI16] I. Chillotti, N. Gama, M. Georgieva and M. Izabach è ne. Faster Fully Homomorphic Encryption: Bootstrapping in less than 0.1 Seconds. In ASIACRYPTO2016.

[CGGI17] I. Chillotti, N. Gama, M. Georgieva and M. Izabach è ne. Faster Packed Homomorphic Operations and Efficient Circuit Bootstrapping for TFHE. In ASIACRYPT 2017.

[CM15] M. Clear and C. McGoldrick. Multi-identity and multi-key leveled FHE from learning with errors. In CRYPTO (II) 2015, LNCS vol. 9216, pp. 630-656. Springer, 2015.

[CO17] W. Chongchitmate and R. Ostrovsky. Circuit-Private Multi-Key FHE. In PKC 2017.

[CRRV17] R. Canetti, S. Raghuraman, S. Richelson and V. Vaikuntanathan. Chosen-Ciphertext Secure Fully Homomorphic Encryption. In PKC 2017, Part II, LNCS 10175, pp. 213-240, 2017.

[DH76] W. Diffie and M. Hellman. New directions in cryptography, IEEE Transactions on Information Theory, vol.IT-22, pp. 644-654, 1976.

[DM15] L. Ducas and D. Micciancio. FHEW: Bootstrapping Homomorphic Encryption in Less Than a Second. In EUROCRYPT (I) 2015, LNCS vol. 9056, pp. 617-640. Springer, 2015.

[DS16] L. Ducas and D. Stehl é . Sanitization of FHE Ciphertexts. In EUROCRYPT 2016, pp. 294-310. Springer 2016. Available at http://eprint.iacr.org/2016/164.

[ElG84] T. ElGamal. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In Crypto '84, pp. 469-472.

[Gen09] Craig Gentry. A Fully Homomorphic Encryption Scheme (Ph.D. thesis). Available at http://crypto.stanford.edu/craig/, 2009.

[GHS12a] C. Gentry, S. Halevi and N. Smart. Better Bootstrapping in Homomorphic Encryption. In PKC 2012, LNCS vol. 7293, pp. 1-16. Springer, 2012.

[GHS12b] C. Gentry, S. Halevi and N. Smart. Fully Homomorphic Encryption with Polylog Overhead. In EUROCRYPT 2012, LNCS vol. 7485, pp. 465-482.

[GHS12c] C. Gentry, S. Halevi and N. Smart. Homomorphic Evaluation of the AES Circuit. with polylog overhead. In CRYPTO 2012, LNCS vol. 7417, pp. 850-867. Springer, 2012.

[GINX16] N. Gama, M. Izabachene, P. Q. Nguyen and X. Xie. Structural Lattice Reduction: Generalized Worst-Case to Average-Case Reductions and Homomorphic Cryptosystems. In EUROCRYPT 2016. Available at http://eprint.iacr.org/2014/283.

[GM82] S. Goldwasser and S. Micali. Probabilistic Encryption and How to Play Mental Poker Keeping Secret all Partial Information. In Proc. of STOC' 82, pp. 365-377, 1982.

[GSW13] C. Gentry, A. Sahai and B. Waters. Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based. In CRYPTO 2013, LNCS vol. 8042, pp. 75-92.

[GVW15] S. Gorbunov, V. Vaikuntanathan and D. Wichs. Leveled Fully Homomorphic Signatures from Standard Lattices. In STOC 2015, pp. 469–477.

[HAO15] R. Hiromasa, M. Abe and T. Okamoto. Packing Messages and Optimizing Bootstrapping in GSW–FHE. In PKC 2015, LNCS vol. 9020, pp. 699–715.

[HS14] S. Halevi and V. Shoup. Algorithms in HElib. In CRYPTO (I) 2014. LNCS, vol. 8616, pp. 554–571. Springer, 2014.

[HS15] S. Halevi and V. Shoup. Bootstrapping for HElib. In EUROCRYPT (I) 2015, LNCS vol. 9056, pp. 641–670. Springer, 2015.

[HS18] S. Halevi and V. Shoup. Faster Homomorphic Linear Transformations in HElib. In CRYPTO 2018. Available at https://eprint.iacr.org/2018/244

[KLS+16] J. Kim, C. Lee, H. Shim, et al. Encrypting Controller using Fully Homomorphic Encryption for Security of Cyber–Physical Systems. In IFAC 2016, Vol.49, Issue 22，pp. 175–180, 2016.

[LDM+16] J. Lai, R. H. Deng, C. Ma, K. Sakurai and J. Weng. CCA–Secure Keyed–Fully Homomorphic Encryption. In PKC 2016, LNCS vol. 9614, pp. 70–98. Springer, 2016.

[LTV12] A. López–Alt, E. Tromer and V. Vaikuntanathan. On–the–fly Multiparty Computation on the Cloud via Multikey Fully Homomorphic Encryption. In STOC 2012, pp. 1219–1234. ACM, 2012.

[MW16] P. Mukherjee and D. Wichs. Two Round Multiparty Computation via Multi–Key FHE. In EUROCRYPT 2016. Available at http://eprint.iacr.org/2015/345

[PS16] C. Peikert and S. Shiehian. Multi–Key FHE from LWE, Revisited. In TCC 16–B. Available at http://eprint.iacr.org/2016/196.

[RAD78] R. L. Rivest, L. Adleman, and M. L. Dertouzos. On Sata Banks and Privacy Homomorphisms. In FOSC 1978, pp. 169–179.

[RSA78] R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public–key cryptosystems (reprint), Commun. ACM, vol. 21, no. 2, pp. 120–128, 1978.

[vDGHV10] M. van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan. Fully Homomorphic Encryption over the Integers. In EUROCRYPT 2010, LNCS vol. 6110, pp. 24–43. Springer, 2010.

作者简介

王付群，杭州师范大学理学院 讲师、卫士通摩石实验室兼职专家。研究方向主要包括全同态加密与签名、格密码、公钥密码等。承担多项国家自然科学基金面上、重点项目，参与一项国家重点研发计划项目，主持一项浙江省自然科学基金项目等，发表密码与信息安全相关论文多篇。