三大密码会看密码的未来

贾音、来学嘉

第 36 届国际密码学年会（2016 年美密）于 2016 年 8 月 14 – 18 日在美国加州大学圣芭芭拉分校召开。会议由 IACR 主办，加州大学圣芭芭拉分校计算机科学系承办。会议共录用论文 70 篇。会议涵盖了对称密码的安全性分析、对称密码学原语、密码学理论与实践、算法数论、密码分析工具、面向硬件的密码学、安全计算和方案、混淆、量子技术等多个领域。

第 35 届欧洲密码学年会（2016 年欧密）于 2016 年 5 月 8–12 日在奥地利维也纳召开。会议由 IACR 主办。共录用论文 62 篇。会议邀请了 Karthikeyan Bhargavan 做了题为“Protecting Transport Layer Security from Legacy Vulnerabilities”的报告，邀请 Bart Preneel 做了题为“The Future of Cryptography”的报告，邀请 Christian Collberg 做了题为“Engineering Code Obfuscation”的报告。会议涉及伪随机、LPN/LWE、分析、掩码、全同态加密、数论、哈希函数、多线性映射、消息认证码、对 SSL/TLS 的攻击、协议、鲁棒性设计、格的规约、基于格的方案、零知识、伪随机函数、多方计算、分层、轮复杂度、泄露、不可区分性等多方面内容。

第 22 届亚洲密码学年会（2016 亚密）于 2016 年 12 月 4 – 8 日在越南河内召开。会议共录用论文 67 篇。会议邀请 Nadia Heninger 做了题为“The Reality of Cryptographic Deployments on the Internet”的报告，邀请 Hoeteck Wee 做了题为“Advances in Functional Encryption”的报告，邀请 Neal Koblitz 做了题为“Cryptography in Vietnam in the French and American Wars”的报告。会议涉及分组密码、AES 与白盒、哈希函数、随机性、认证加密、侧信道分析与抗泄露、数学分析、零知识、后量子密码、可证明安全、数字签名、功能和同态密码学、ABE 与 IBE、密码协议、多方计算等内容。

这三大会议代表了国际密码学术界的发展水平，受到了世界各国学者的广泛关注。会议共收录 199 篇，涵盖了公钥密码、对称密码、密钥交换、格和量子密码、安全多方计算以及密码学基础问题等各个领域，表明了 2016 年密码学领域的重要进展。

1. 最佳论文和荣誉奖

Chillotti 等人重新研究基于 GSW 及其环变体的完全同态加密（FHE）。他们注意到，GSW 的内部乘可以由 GSW 和 LWE 密文之间更简单的外部乘替换。

Chillotti 等人表明 Ducas 和 Micciancio 的自举方案 FHEW 只能由这个外部乘表示。结果，他们将速度从小于 1 秒改进为小于 0.1 秒。他们还将 1GB 自举密钥大小减少到 24MB，同时还保持相同的安全级别，他们通过用近似分解算法替代精确算法。

此外，他们的外部乘解释了 GSW 样本的噪声传播中的独特不对称性，并且使得可以以高效的方式同态地评估确定性自动机，其中噪声开销对测试字的长度仅仅是线性的。

最后，他们提供了基于 LWE 方案的替代实践分析，其直接将安全参数与 LWE 的错误率和 LWE 私密钥的熵相关。

Todo 等人介绍了一种新型的攻击，称为非线性不变攻击。作为应用示例，他们对全轮的（可调）分组密码 Scream，iScream 和 Midori64 进行了新的攻击，使得能在弱密钥的设置下将其区分开来。这些攻击仅需要少数几个明文 - 密文对，并且具有最小的计算复杂度。 此外，对（可调）分组密码的非线性不变攻击可以扩展到 CBC 或 CTR 等已有工作模式中的唯密文攻击。 认证加密方案 SCREAM 和 iSCREAM 的明文可以在 nonce-respecting 的设置下从密文中实际恢复。 这是第一个打破 SCREAM 安全性声明的结果。此外，在众所周知的模式中，Midori64 的明文可以被实际恢复。所有攻击都经过实验验证。

Kleptography，20 年 前 由 Young 和 Yung [Crypto'96] 介绍，考虑了将“后门”嵌入系统的标准加密原语的恶意实现（或实例化）的安全性。值得注意的是，即使破坏性的密码系统产生的输出与真正安全的“参考实现”无法区分，crippling subliminal 攻击仍然存在。Bellare，Paterson 和 Rogaway [Crypto'14] 最近启动了对这种对称密钥加密算法的攻击的正式研究，并声称对于密码系统的随机化组件，可以广泛普及克隆攻击。

Russell 等人通过允许敌手对（随机化的）密钥生成进行破坏来扩大当前关于该问题的研究范围；特别是，他们在完全破坏模型中开始密码学研究，其中所有相关的密码学原语都受到克隆攻击。他们在这个“完全破坏”模型中构造安全的单向置换和陷门单向置换，描述了通用的、严格的免疫策略来减弱克隆攻击的能力。他们的策略可以被看作是密码实践中一种正式的处理方法。他们还描述了一个相关的“分割程序”模型，可以直接用于实际部署。此外，他们应用他们的通用免疫策略构造了一个无后门的 PRG。这优化了之前的 Dodis，Ganesh，Golovnev，Juels 和 Ristenpart[Eurocrypt '15] 的结果，后者需要一个可信的随机密钥。

然后，他们在这个完全破坏模型中检查（陷门）单向置换的两个标准应用，并通过黑盒规约构造了“更高级”的原语。他们构造了一个数字签名方案，当所有算法（包括密钥生成，以前并不在攻击考虑范围内）遭受克隆攻击时，任然保留了不可伪造性。此外，他们证明，经典的 Blum-Micali 伪随机发生器（PRG），使用“免疫”单向置换，产生一个无后门的 PRG。

除了这些安全原语的发展，他们还对克隆攻击模型进行了分级，并使用该模型总结了

过去的成果和新贡献；这种分类法对未来的工作可能有一定价值。

Gay 等人提出了第一个基于 DDH 的 CCA 安全的公钥加密方案，其安全性损失与密文个数及解密机访问次数无关。他们的构造也可扩展至无配对群中的标准 k-Lin 假设，而先前从 Hofheinz 与 Jager(Crypto '12) 起的所有构造均依赖于配对。另外，他们的构造改进了已有方案的效率，将密文开销减少了约一半（在 DDH 下减少到仅用 3 个群元素），并且不再使用配对。

他们还指出如何在非交互零知识证明（NIZK）设定中使用他们的技术。特别地，他们构造了第一个不使用配对的对于线性语言完全模拟公正的指定验证器非交互零知识证明。使用配对，可以将他们的构造转换为一个具有完全模拟公正的高度优化的可公开验证的非交互零知识证明。

基于恒定度的算术电路可计算的亚指数级安全的伪随机数生成器的存在性假设以及有错学习（LWE）问题的亚指数级困难性，Lin 构造了一个恒定度分级的编码方案中的所有多项式尺寸电路的不可区分混淆（IO）方案。之前所有通用 IO 方案都依赖于多项式度分级的编码方案。

在 t-out-of-n 健壮的秘密共享方案中，秘密信息在 n 个参与方之间共享，他们可以通过组合共享的内容来重建消息。敌手可以选择贿赂至多 t 个参与者，获取或修改他们的共享内容。这个方案应满足隐私性，即敌手不能得到任何关于共享消息的信息，以及鲁棒性，即敌手不能使重建过程输出一个错误的信息。这种方案只存在于诚信主体之中，因此 Bishop 等人关注最多腐败者设定（n=2t+1）下的无条件安全。

在这种情景下，以重建失败率不高于 2^{-k} 来共享一个 m 比特消息时，已知的共享内容的大小下限为 m+k 比特。另一方面，先前所有构造的共享内容大小与参与方个数 n 成线性关系，并且先前 Cevallos 等人（EUROCRYPT‘12）提出的最好的方案达到了 $m+\tilde{O}(k+n)$。

Bishop 他们构造了第一个在最多腐败者设定下健壮的秘密共享方案。这个方案的共享内容的大小与参与方个数 n 不成线性关系，其大小仅为 $m+\tilde{O}(k)$ 比特。他们的方案基于图的最小分割问题的近似算法，可以有效地计算。

2. 白盒

白盒加密旨在为不可信环境中的加密算法提供安全，其中对手可以完全访问其实现过程。白盒密码的基本安全目标包括密钥提取安全性和分解安全性：实际上，从实现中恢复密钥应该是不可行的，并且在不恢复密钥的情况下找到更紧凑的表示来分解实现是困难的，以此减少代码移植。

鉴于所有已发布的针对诸如 DES 或 AES 等标准加密算法的白盒实现都容易受到实际的密钥提取攻击，已经存在两种用于白盒分组密码的专用设计方法：Birykov 等人在 ASIACRYPT'14 提出的 ASASA，以及 Bogdanov 和 Isobe 在 CCS'15 上提出的 SPACE。虽然 ASASA 遭受分解攻击，但是

SPACE 将在白盒中抵抗密钥提取和分解攻击的安全性降低到诸如标准黑盒设置中的 AES 等标准分组密码的安全性。然而，由于安全优先的设计策略，SPACE 在实际应用中强加了性能开销，例如它多次调用 AES 来加密单个分组。

Bogdanov 等人通过设计一系列专用的白盒分组密码 SPNbox 和一系列底层的小分组密码，通过软件工程和常数时间内执行来解决这个问题。虽然仍然依赖于标准黑盒密码安全性来抵抗密钥提取和分解，但是 SPNbox 在黑盒中将获得高达 6.5 倍的速度提升，在英特尔 Skylake 和 ARMv8 CPU 上的白盒加速高达 18 倍。这些设计允许在黑盒设置中在常数时间内实现，并且满足在现实世界应用（诸如 DRM 或移动支付）中对白盒加密的实际需求。此外，他们在各种安全级别中，形式化了抵抗分解的弱和强空间困难性。他们在所有这些敌手模型中得到空间困难性的界限。

因此， SPNbox 第一次提供了一个实用的白盒分组密码，其特点是能够达到已知的密钥提取安全性，严格的分解安全性，并在各种平台上有不错的实现性能。这为白盒密码在现实世界中应用铺平了道路。

近年来，已经进行了若干尝试来构造白盒分组密码，其实现的目标是不可压缩性。这包括来自 Asiacrypt 2014 的 Bouillaguet，Biryukov 和 Khovratovich 的弱白盒 ASASA 构造，以及最近从 CCS 2015 的 Bogdanov 和 Isobe 的 Space-hard 构造。Fouque 等人第一个构造出实现同一目标的白盒，同时提供可证明的安全保证。 此外，他们对所提出的白盒进行具体的实例化，证明与以前的工作相比具有更好的效率。并且，可证明的安全性具有令人惊异的低开销。

3. 密码分析工具

在对称密码分析中，跟踪分组密码的比特和优化攻击是必须处理的单调乏味的工作，如果程序可以自动处理这些问题，至少是自动使用已知攻击技术，对密码分析人员来说是很好的。然而，当前的自动化工具要么是针对特定的密码设计的，要么只能完成攻击中的特定步骤，还需要人工完成剩下的分析。

Derbez 等人描述了实现中间相遇攻击和不可能差分攻击的通用方法，适用于包括 SPN、Feistel 和 Lai-Massey 结构在内的很多分组密码。先前的工具主要用于寻找最佳的差分链或线性链，需要人工使用这些链完成剩余的攻击。与此不同，Derbez 等人提出的方法可以在考虑密码和密钥扩展算法的情况下自动寻找最佳攻击。目前该方法已经对 AES、mCRYPTON、SIMON、IDEA、KTANTAN、PRINCE 和 ZORRO 使用，取得了很好的效果。

在密码学和密码分析学中一个最常见的任务就是在一个指数级别（$N=2^n$）的事件大集合（干草堆）中寻找一些有趣的事件（针），或者证明这样的事件是不存在的，尤其是当“针”被定义为发生的可能性 p 远大于 1/N 的事件，即几乎是均匀分布的事件。当搜索算法只能在均匀分布中抽样查找时，已知最佳的时间和空间折中的方案需要 $O(\frac{1}{Mp^2})$ 时间和 O(M) 内存空间。

Dinur 等人开发了一种更快的搜索算法，其所针对的设定是常见的密码学设定，即通过将确定性函数应用于随机输入来得到定义的分布。这样的分布可以通过一个有 N 个节点的随机有向图来建立模型，其中几乎所有的节点都有 O(1) 个前趋节点，但需要寻找的节点拥有大量的前趋节点（O(pN) 个）。当给定的内存是一个定值，Dinur 等人提出了一种叫作 NestedRho 的搜索算法。与先前的最佳方案相比，当$\frac{1}{N}<p<1$ 时，NestedRho 方案比原有方案在时间复杂度上快了 O($\frac{1}{p^2}$)；当$N^{-0.75}<p<N^{-0.5}$ 时，该方案在运算速度上提升了$\sqrt{N}$倍。当给定的内存空间增加时，Dinur 等人展示了如何将 NestedRho 技术和并行碰撞搜索技术相结合，进一步降低时间复杂度。最后，Dinur 等人还介绍了如何使用这样技术应用于更复杂的分布。

根据 Shor 的算法，量子计算机是公钥密码学的重大威胁。密码学家需要寻找一个量子安全的解决方案。另一方面，量子计算在对称密码学中的影响还没被理解。Kaplan 等人研究了一种攻击，攻击者可以查询在不同状态的量子叠加中实现密码学原语的预言机。这个模型赋予了攻击者很强大的能力，但最近的研究表明仍然无法在此模型中构造安全的加密系统。

Kaplan 等人研究了一种量子过程的应用——Simon 算法，以此来攻击该模型下的对称密码学系统。Kaplan 等人认为，利用 Simon 算法，许多寻找冲突的经典攻击算法能得到显著提速。一个例子是，在经典设定中，寻找一个冲突需要 $\Omega(2^{n/2})$ 次查询；当冲突伴随一些隐藏的周期性时，利用量子模型只需要 O(n) 次查询即可找到冲突。

Kaplan 等人获取了影响力非常大的攻击。首先，他们证明了被广泛使用的认证和认证加密方案（例如，CBC-MAC，PMAC，GMAC，GCM 和 OCB）在此安全模型下都被完全破解。该攻击还适用于很多 CAESAR 竞赛的候选算法：CLOC，AEZ，COPA，OTR，POET，OMD 和 Minalpher。其次，Kaplan 等人证明了 Simon 算法还适用于滑动攻击，这使得经典对称密码分析学技术在量子模型下有显著的提速。

4. 密码协议

s2n 是一个 TLS 协议的实现，它于 2015 年 1 月由 Amazon 推出，由大约 6,000 行 C99 代码实现。相比之下，OpenSSL 需要大约 70,000 行代码来实现。在发布之时，Amazon 声明 s2n 进行了三次外部安全评估和渗透测试。Albrecht 等人指出，尽管如此，s2n 在 CBC 模式的密码套件下存在一个计时攻击，该攻击在某些情形下可以扩展至完全的明文恢复攻击。他们的攻击有两部分：第一部分是一个 Lucky 13 攻击的变种，即使在 s2n 中对 Lucky 13 进行了保护，该变种仍然有效；第二部分涉及 s2n 中为应对 Lucky 13 额外加入的随机延迟。他们的工作表明对抗复杂的计时攻击具有更大挑战，还说明标准代码审计不足以揭露所有加密攻击方向。

Brzuska 等人研究在 ACCE（authenticated and confidential channel establishment）安全概念下，如何安全地

从安全通道协议导出其他加密密钥。例如，EAP-TLS 协议使用 TLS 的握手过程来输出一个可用于 TLS 以外的额外共享密钥，另外 RFC 5705 标准指定了从 TLS 导出密钥的一般机制。他们指出对于 ACCE 协议中的一类“类 -TLS“协议，EAP-TLS 转换可以用于导出一个额外的密钥，并且在 Bellare-Rogaway 模型下是安全的 AKE 协议。有趣的是，他们的证明不需要了解 TLS 的细节（超越了它是”类 -TLS“的概念），但是可以半黑盒的方式使用 ACCE 的性质。为了方便模块化证明，他们开发了一种新技术，它是一种用于安全归约的基于加密的密钥检查机制。他们的结果意味着安全的 TLS 1.2 密码套件的 EAP-TLS 是一个安全的认证密钥交换协议。

距离边界协议变得越来越重要，因为它们是抵御中继攻击最准确的解决方案。它们由两方组成：验证者和证明者。证明者表明他与验证者足够接近。在诸如支付系统的一些应用中，公钥距离定界协议是实用的，因为在付款人和收款人之间不需要预共享秘密。然而，公钥密码比对称密钥密码需要更多的计算。Kilinc 等人专注于公钥距离边界协议的效率问题和它们的标准安全证明。他们构造了两个协议（一个没有隐私，一个有），与现有协议相比，证明者需要较少的计算，同时能保证最高的安全级别。他们的通用构造基于一个密钥协商模型。在两个协议中，证明者仅需要分别使用一次和三次椭圆曲线计算即可将其实例化。他们详细地证明了他们构造的安全性。

Baldimtsi 等人引入了一类新的协议，称为工作或知识证明（PoWorKs）。在 PoWorK 中，证明者可以说服验证者它已经执行了工作或者它具有公开声明的相关知识，而验证者不能区分两者中的哪一个已经发生。他们根据三个属性，完整性，f 可靠性和不可区分性（其中 f 是确定工作证明的紧密度函数），给出一种构造，将 3-move HVZK 协议变换为 3-move 公共货币 PoWorKs。为了在将在 PoWorK 协议中的工作形式化，他们定义了满足某些均匀性条件的密码谜题。他们通过构造适当困难的单向函数的“密集”版本，在随机预言机（RO）模型中实例化他们的谜题。

然后他们通过提出许多应用程序来展示 PoWorK 协议。他们首先展示非交互式 PoWorK 如何用来减少垃圾邮件，即通过强制用户发送电子邮件来向邮件服务器证明他们是被批准的收件人的联系人或执行计算工作。与之前这个问题的工作证明方法相反，他们所提出的 PoWorK 具有一定隐私性，因为其向邮件服务器隐藏了来自接收者的批准的联系人列表。他们的第二个应用程序显示了如何使用 PoWorK 来构建基于工作证明（“如比特币”）的加密货币与基于知识关联的加密货币（这些加密货币包括基于“利益证明”的加密货币，以及其他货币）。所产生的基于 PoWorK 的加密货币继承了底层两个系统的鲁棒性，而 PoWorK 不可区分性确保了矿工的总体均匀分布。