密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research,2016,3(3):211–228

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-81033101

从双线性对到多线性映射*

张方国[1,2]

1. 中山大学 数据科学与计算机学院, 广州 510006
2. 广东省信息安全技术重点实验室, 广州 510006
通讯作者: 张方国, E-mail: isszhfg@mail.sysu.edu.cn

摘 要: 自从 2000 年 Sakai 等人利用椭圆曲线上的双线性对提出了基于身份的密钥协商方案, 特别是 2001 年 Boneh 和 Franklin 利用双线性对实现了基于身份的加密, 基于双线性对的密码体制的研究曾一度成了密码研究领域特别是公钥密码研究中的一个热点. 这一研究领域所取得的研究成果在密码学研究领域创造了一个不小的奇迹. 在这篇文章中, 我们首先介绍什么是双线性对, 然后介绍双线性对在密码中的应用, 从三方一轮密钥协商到 IBE, 到基于属性的加密(ABE), 断言(或谓词)加密(PE), 函数(或功能)加密(FE), 可搜索的加密等, 从短签名到各种各样的签名等. 我们介绍双线性对密码系统的实现现状和安全现状. 双线性对可以推广到多线性映射. 多线性映射可以实现双线性对所实现的所有体制, 更强大的是它可以实现电路, 从而可以构造任意布尔电路的断言加密和设计任意多项式电路的不可区分的混淆(iO)等. 由于多线性映射的强大功能, 使得基于多线性映射的密码体制的研究成为了当前的研究热点. 文章第二部分介绍多线性映射定义和构造思想, 以及在密码中的应用. 最后我们给出一些公开问题和一些讨论.

关键词: 双线性对; 椭圆曲线; 多线性映射; 格; 混淆
中图法分类号: TP309.7 **文献标识码**: A DOI: 10.13868/j.cnki.jcr.000122

中文引用格式: 张方国. 从双线性对到多线性映射[J]. 密码学报, 2016, 3(3): 211–228.
英文引用格式: ZHANG F G. From bilinear pairings to multilinear maps[J]. Journal of Cryptologic Research, 2016, 3(3): 211–228.

From Bilinear Pairings to Multilinear Maps

ZHANG Fang-Guo[1,2]

1. School of Data and Computer Science, Sun Yat-sen University, Guangzhou 510006, China
2. Guangdong Key Laboratory of Information Security, Guangzhou 510006, China
Corresponding author: ZHANG Fang-Guo, E-mail: isszhfg@mail.sysu.edu.cn

Abstract: Since 2000 Sakai et al. proposed the identity based key agreement scheme using bilinear pairings on elliptic curves, especially, when Boneh and Franklin implemented the identity based encryption using bilinear pairing in 2001, the research of pairing based cryptography has become a hot topic in the field of public key cryptography. The pairing based research has achieved a great amount of results. In this paper, we firstly introduce the concept of bilinear pairing, then introduce pairing based cryptosystems, from the three party one round key agreement to identity based encryption (IBE), attribute based encryption (ABE), predicate encryption (PE), function encryption (FE) and searchable encryption, from short signature to a variety of signatures. We also introduce the current status of implementation and security of pairing. Bilinear pairing can be generalized to

* 基金项目: 国家自然科学基金项目(61379154)
收稿日期: 2016-03-06 定稿日期: 2016-05-25

multilinear mapping. Multilinear maps can be used for all kinds of pairing based cryptography, a more powerful feature of multilinear mapping is that it can realize circuits. Multilinear maps can be used to design Attribute-based encryption and indistinguishability obfuscation for all circuits. Due to the strong functionality of multilinear mapping, the research of multilinear mapping based cryptosystems has become a hot research topic. In the second part of this paper, we introduce the definition, construction, and applications of multilinear mapping. Finally, we briefly discuss some open problems and interesting issues for further study in this area.
Key words: bilinear pairing; elliptic curve; multilinear mapping; lattice; obfuscation

1 引言

双线性对最早是由Weil在1946年提出的定义在代数曲线上的一个可有效计算的双线性映射(即Weil对). 它是代数几何, 特别是代数曲线理论研究中一个非常重要的概念和工具. 双线性对在密码中的最早应用是1993年Menezes、Okamoto和Vanstone[1]给出的归约超奇异椭圆曲线上离散对数问题到有限域的离散对数问题的MOV攻击. 2000年, Sakai等人[2]、Joux[3]、Boneh等人[4]发现了双线性对在密码中的正面的应用——能够用来构造基于身份的密码体制(IBE)、三方一轮密钥协商等. 之后, 双线性对引起了密码学家们的极大兴趣并被发现了更多各种各样的应用, 如短签名、一些带有特殊性质的签名(聚合签名、可验证加密的签名、部分盲签名等)等. 再之后, 由于发现双线性对可以实现基于属性的加密(ABE)、断言(或谓词)加密(PE)、函数(或功能)加密(FE)、可搜索的加密等, 使得基于双线性对密码体制被应用在云计算等领域. 双线性对密码的研究一度成为一个热点, 并持续了十多年. 所取得的研究成果(特别是发表的文章数量)在密码学研究领域创造了一个不小的奇迹. 不过随着对双线性对的深入挖掘和研究, 发现双线性对的功能有限, 在设计一些新的密码协议时功能上欠完善. 例如我们可以利用双线性对设计函数加密, 但这样的函数只能是一些简单函数, 对复杂的函数或者任意函数它做不到. 另外, 双线性对密码被研究了近15年了, 新颖的或有意义的结果较难出现了(能想到的有趣的方案都基本被设计出来了). 同时, 由于最近几年对小特征有限域上离散对数的计算的研究, 影响了双线性对密码的安全性, 所以双线性对密码的研究热度已经降下来了.

双线性对可以推广到多线性映射, 但在2012年之前, 多线性映射只是一个空想. 2012年, Garg、Gentry和Halevi[5]利用理想格实现了第一个密码多线性映射, 之后Coron等人[6]给出了整数环上的实现. 2015年Gentry、Gorbunov和Halevi[7]构造了基于一般格的多线性映射GGH15方案. 由于多线性映射的提出, 多数研究人员把目光投到了这上面. 多线性映射不仅可以实现双线性对所实现的所有体制, 同时提供了更强大的功能. 多线性映射不仅可以实现多方一轮密钥协商、广播加密等, 它所体现出来的更强大的应用是实现电路. 布尔电路是计算机的构建模块, 是一切计算函数的底层构架. 利用多线性映射可以构造任意布尔电路的基于属性的加密和断言加密. 最近, 多线性映射被用来设计任意多项式电路的不可区分的混淆(iO), 利用不可区分的混淆, 可以设计出各种各样非常有趣和创意的协议, 如充当随机预言函数、任意函数加密、多方非交互式密钥协商、可否认加密等. 很多应用甚至是解决了密码学领域的一些多年的公开难题. iO是一个很有意思的东西, 估计利用它还可以设计出更多好的新颖密码协议.

当前基于双线性对的密码体制的研究基本被基于多线性映射的密码体制的研究所取代, 这是一个很自然的推广, 当然更取决于多线性映射所体现出来的强大功能.

本文主要综述基于双线性对和多线性映射的密码体制, 从它们的理论、实现到应用. 本文分两部分, 第2–4节为第一部分, 主要讲双线性对的理论、实现、应用和安全现状; 第5–7节为第二部分, 主要讲多线性映射的构造、安全现状和应用. 最后探讨双线性对和多线性映射密码体制中有待进一步研究的问题.

2 双线性对及其实现

椭圆曲线或超椭圆曲线的双线性对一般是指Weil对和Tate对. 双线性对在密码中的应用最早归于Menezes、Okamoto和Vanstone以及Frey和Rück的工作, 即著名的ECDLP的MOV攻击[1]和FR攻击[8]. 2000年,

Sakai等人[2]和Joux[3]同时发现了双线性对在密码中的正面的应用——能够用来构造新的密码方案. 之后, 特别是2001年Boneh和Franklin[4]利用双线性对实现了基于身份的加密, 双线性对引起了密码学家们的极大兴趣, 在密码学领域又被发现了更多各种各样的应用.

什么是双线性对呢? 令 G_1, G_2 和 G_T 是三个 n 阶循环群(n 可以是素数, 也可以是合数, 如RSA模数), 我们考虑 G_1, G_2 和 G_T 都是乘法群(早期的双线性对密码方案中 G_1 和 G_2 一般都是考虑成加法群, 这主要是因为用以构造双线性对的椭圆曲线群的运算是"加法"). 一个双线性对 e 就是一个从 $G_1 \times G_2$ 到 G_T 的双线性映射, 并满足下面性质: (1) 双线性性: 设 $g_1 \in G_1$, $g_2 \in G_2$, $a,b \in Z_q$, 有 $e\left(g_1^a, g_2^b\right) = e\left(g_1, g_2\right)^{ab}$; (2) 非退化性: 对每一个 $g_1 \in G_1 / \{1\}$, 总存在 $g_2 \in G_2$, 使得 $e\left(g_1, g_2\right) \neq 1$; (3) 有效可计算性. 利用椭圆曲线或超椭圆曲线构造的双线性对有下面三种类型[9]:

类型1 $G_1 \to G_2$ 有一个有效可计算的同构, 这时一般可假定 $G_1 = G_2$ (可以通用"G"表示), 这样的双线性对也成为对称双线性对. 这类双线性对一般可以用超奇异椭圆曲线或超椭圆曲线来实现.

类型2 有一个有效计算群同态 $G_2 \to G_1$, 但无从 G_1 到 G_2 的有效同态. 这类双线性对一般用素数域上的一般椭圆曲线实现, G_1 是基域上椭圆曲线群, G_2 是扩域上椭圆曲线子群, G_2 到 G_1 的同态一般取迹映射.

类型3 没有任何 $G_1 \to G_2$ 或 $G_2 \to G_1$ 的有效可计算的同态(同态甚至同构一定是存在的, 这里是指没有有效计算的同构). 这类双线性对也是用素域上的一般曲线来构造, G_2 一般取迹映射的核.

三类不同的双线性对在构造密码方案时展现的功能不同, 有些方案或系统只能用类型3的双线性对实现, 因为它们的安全性恰恰就依赖于 G_1, G_2 之间没有有效可计算同态. 为了便于问题的描述, 后面多数应用的例子我们取在类型1的双线性对上做讨论. 阶为 n 的循环群 G 中的离散对数问题(DLP)定义为: 给定群元素 g, g^a, 计算 a. 计算Diffie-Hellman问题(CDH)是给定 g, g^a, g^b, 计算 g^{ab}. 判定Diffie-Hellman问题(DDH)是给定 g, g^a, g^b, g^z, 判定是否 $z = ab \bmod n$. 若 e 是从 $G \times G$ 到 G_T 的双线性映射, 则 G 中的DLP可以归结为求解 G_T 中的DLP, 且 G 中的DDH不再困难: 给定 $g, g^a, g^b, g^z \in G$, 测试是否 $e\left(g, g^z\right) = e\left(g^a, g^b\right)$ 即可解决 G 中的DDH问题. CDHP有两个变型, 即求逆Diffie-Hellman问题(Inv-CDHP: $g, g^a \Rightarrow g^{1/a}$)和平方Diffie-Hellman问题(Squ-CDHP: $g, g^a \Rightarrow g^{a^2}$). Maurer[10]和Sadeghi等人[11]证明: CDHP, Inv-CDHP和Squ-CDHP是多项式时间计算等价的. 在双线性对密码应用中, 有两类与双线性对相关的常用的困难问题:

计算双线性Diffie-Hellman(CBDH): 给定 $g, g^a, g^b, g^c \in G$, 计算 $e\left(g, g\right)^{abc}$.

判定双线性Diffie-Hellman(DBDH): 给定 $g, g^a, g^b, g^c \in G$ 和 $g' \in G_T$, 判定是否 $g' = e\left(g, g\right)^{abc}$.

最早用于设计密码体制的双线性是超奇异椭圆曲线的Weil对和Tate对, 之后, 一般曲线(多数是带有复乘CM的)也被发现可以用来构造双线性对. 由于大多数情况下计算Tate对比计算Weil对要有效的多, 所以对双线性对的实现大都关注Tate对及其一些有效变形. 实现双线性对的主要算法是利用Miller算法[12], 目前提出的许多改进算法也都是基于Miller算法的. 也有学者探讨用其他的技术来计算Weil对和Tate对, 如椭圆网方法等, 但仍然没有Miller算法效率高. 影响双线性对快速实现的因素很多, 其中一个很重要的因素就是Miller算法中的循环次数: 循环次数越少, 计算速度越快. 围绕如何减少Miller算法中的循环次数, 提出了一些新的双线性对, 从最初的Tate对, 到Eta对[13]、Ate对[14]、广义的Ate对[15]、Rate对[16], 一直到最优对[17]. 这些变型的双线性对的详细讨论可以参见赵等人在文献[18]中给出的计算双线性对的研究综述. 2010年以后在椭圆曲线双线性对的构造方面的工作就比较少了. 构造适用于双线性对的椭圆曲线主要是利用CM方法. 在素数域上已经利用CM方法构造出了大量适用于各种双线性对的椭圆曲线, 但在二元域上, 目前还没有有效的方法构造适用于双线性对的非超奇异椭圆曲线. 尽管CM方法也可以应用在特征 2

的有限域上, 但由于有限域先给定了, 满足条件的适合双线性对的椭圆曲线就更稀疏了, 并且对于一些特征 2 的域上就没有适合双线性对的椭圆曲线存在. 有限域 $\mathrm{GF}\left(2^m\right)$ 上适合双线性对的椭圆曲线 E 应该满足以下几个基本条件: (1) m 是大于160的素数; (2) $\#E\left(\mathrm{GF}\left(2^m\right)\right)$ 有大于 2^{160} 小于 2^m 的素因子 r; (3) r 整除 $2^{mk}-1$ (实际上是 $r\left|\varphi_k\left(2^m\right)\right.$, 这里 $\varphi_k(x)$ 是第 k 次分圆多项式), 这里 k 就是嵌入次数, 并且 $mk>1024$. 为了计算的有效性, 有时我们还要求 k 是偶数. 在这些限定下, 给定一个有限域 $\mathrm{GF}\left(2^m\right)$, 可以通过分解 $2^{mk}-1$ 去检测是否有满足条件的素因子 r 存在, 从而先判定 $\mathrm{GF}\left(2^m\right)$ 上适合双线性对的椭圆曲线是否有存在的可能. 例如, $m=167$, 利用一些分解工具可以分解 $\varphi_6\left(2^{167}\right),\varphi_8\left(2^{167}\right),\varphi_{10}\left(2^{167}\right),\varphi_{12}\left(2^{167}\right)$, 可以发现, 这些分解中都没有位于 $\left[2^{160},2^{167}\right]$ 的素因子, 从而我们断定, 不管用什么方法也构造不出 $\mathrm{GF}\left(2^{167}\right)$ 上嵌入次数为 6,8,10 和12的适用于安全双线性对的椭圆曲线. 只要 $\varphi_k(q)$ 可以有效分解, 这种判定方法适合于所有给定的有限域 $\mathrm{GF}(q)$. 但是由于小特征有限域上的离散对数问题求解算法的提高, 使得对小特征有限域上适合双线性对椭圆曲线的构造的研究基本没有什么意义了.

PBC(Pairing-Based Cryptography Library)是实现双线性对运算的函数库. 这个开源代码C函数库是由Stanford大学开发, 库的地址为http://crypto.stanford.edu/pbc/. PBC函数库为双线性对实现提供了接口, 是基于双线性对密码体制研究的一个非常有用的辅助工具. 目前双线性的计算已经非常有效. 下面是128比特安全级别的双线性对(相当于256比特的ECC和3000比特的RSA)利用BN曲线实现的时间竞赛: 2007年的双线性对会议上, Devigili等人[19]在32-bit Intel Pentium IV @ 3.0 GHZ的机器上的实现用了23 ms; 2008年, Grabher, Großschädl, Page[20]在64-bit Intel Core 2 Duo @ 2.4 GHz的机器上用了6 ms; 同年, Hankerson, Menezes, Scott[21]也是在64-bit Intel Core 2 Duo @ 2.4 GHz的机器上的实现只用了4.2 ms; 2010年, Naehrig等人[22]在64-bit Intel Core 2 Duo @ 2.8 GHz机器上的实现用了1.5 ms; 2010年, Beuchat等人[23]对254比特BN曲线上的最优Ate对在64-bit Intel Core i7 @ 2.8 GHz机器上的实现用了0.8 ms. 目前对这一安全级别的双线性对实现的最好记录是2011年Aranha等人[24]在欧密会上的结果: 0.56 ms(64-bit AMD Phenom II @ 3.0 GHz), 相当安全级别的256比特的ECDSA验证是0.8 ms, 而2048比特和4096比特的RSA签名分别是2.6 ms和18.8 ms. 现在仍然有一些在双线性对实现方面的工作, 有软件方面的, 也有在硬件方面的实现.

3 基于双线性对的密码体制

3.1 密钥协商

密钥协商协议允许两个或多个用户在公开网络中建立一个共享密钥, 是密码学的一个基本原语. 第一个密钥协商协议是Diffie-Hellman协议[25], 这一成果在密码学研究中起到了一个里程碑的作用, 开启了公钥密码体制研究的大门. Diffie-Hellman密钥协商协议是一个两方协议, 如果不考虑通信的复杂度, 双方的密钥协商协议很容易推广到三方或多方. 使用双线性对的好处是可以设计一个一轮通信的三方密钥协商协议. Joux[3]首次提出了这样的一个密钥协商协议. 假定双线性对 $e: G\times G\to G_T$, $\langle g\rangle = G$. 参与方Alice, Bob和Carol各自产生秘密随机值 a,b,c 并广播 g^a,g^b,g^c. 利用双线性对, 他们就可以分别计算共享密钥

$$K=K_A=e\left(g^b,g^c\right)^a=K_B=e\left(g^a,g^c\right)^b=K_C=e\left(g^a,g^b\right)^c$$

就像原始的Diffie-Hellman协议一样, Joux的三方一轮密钥协商协议不是认证的, 容易受到中间人攻击. 基于这一基本协议, 许多认证的三方密钥协商协议被提出. 这一基本的协议也被推广到基于身份的体制.

3.2 基于身份的加密体制及其变型

双线性对在密码构造中的一个重要应用是实现基于身份的加密. 基于身份的加密体制的思想早在

1984年就由Shamir提出[26], 最初的动机就是为了简化传统的PKI公钥体系架构中CA对各用户证书的管理, 其基本的想法就是将用户的身份与其公钥以最自然的方式捆绑在一起. 在提出基于身份的密码体制概念的同时, Shamir给出了一个采用RSA算法的基于身份的签名方案(IBS), 但是基于身份的加密算法(IBE)长时期内都未能找到有效的解决方法. 虽然有一些早期学者的努力(例如Maurer和Yacobi[27]、Tanaka[28]和Tsuji[29]等人), 不过第一个真正实用的IBE方案是使用椭圆曲线上的双线性对构造的, 它们分别被Sakai、Ohgishi和Kasahara[2]及Boneh和Franklin[4]在2001年发现.

下面我们给出Boneh和Franklin的基于双线性对的基本IBE方案的描述:

系统建立: 双线性对 $e:G\times G\to G_T$, 哈希函数 $H:\{0,1\}^*\to G$, 密钥生成中心PKG生成系统主密钥 $\mathrm{MSK}=a$, 系统公钥是 $\mathrm{MPK}=g^a$.

私钥提取: 对身份信息 ID, 计算 $g_{\mathrm{ID}}=H(\mathrm{ID})$, 对应的私钥是 $\mathrm{SK}_{\mathrm{ID}}=g_{\mathrm{ID}}^a$.

加密: 随机取 r, 计算 $K=e\left(g^a,g_{\mathrm{ID}}\right)^r$, 消息 m 的密文计算如下: $C=\left(g^r,\mathrm{SymEnc}_K(m)\right)$. 这里SymEnc是任一对称加密算法.

解密: 计算 $K=e\left(\mathrm{SK}_{\mathrm{ID}},g^r\right)$, 用 K 解密出 m .

Boneh和Franklin在文章中假定双线性计算Diffie Hellman问题是困难的, 上述Boneh-Franklin的基本IBE方案在随机预言模型(RO)下被证明是IND-ID-CPA的. 利用Fujisaki-Okamoto变换技术, Boneh和Franklin在随机预言模型下也证明了他们的IBE方案对选择密文攻击(CCA)是安全的. Waters在Eurocrypt 2005上[30]给出了一个有效的在标准模型下可证明安全的基于身份的加密方案. 在基于身份的密码体制中, 用户的公钥可以是任何唯一识别用户身份的任何信息, 如身份证号、email地址、驾驶证号等, 当然可以唯一识别用户的一些生物特征, 如指纹、虹膜等也自然可以作为基于身份的公钥体制中的用户公钥. 然而由于生物特征具有非精确再生性, 即同一个生物特征的两个测量值不完全相同, 所以将生物特征作为公钥信息时, 就带有了模糊性. Sahai和Waters[31]在对IBE和生物特征进行了研究后, 提出了基于模糊身份的加密体制(FIBE). 由于生物特征信息看成是具有某些特定属性的一个集合, Sahai和Waters将基于模糊身份的加密体制加以简单推广, 得到了基于属性的加密体制(ABE). 基于属性的加密体制有两种方法可以用在接入控制结构的设计中, 它们分别是密钥策略(Key-Policy)ABE和密文(Ciphertext-Policy)策略ABE. 断言(或谓词)加密(Predicate encryption)[32]是基于身份的加密的一个推广, 密钥对应于一个断言 f, 密文关联着一些属性, 对应于断言 f 的密钥 SK_f 能够用来解密具有属性 I 的密文当且仅当 $f(I)=1$. Boneh和Hamburg在Asiacrypt 2008上给出了广义的基于身份的加密(GIBE)的概念[33]. 一个广义的基于身份的加密方案, 允许一些策略的参与来进行加密信息, 这些策略来自一些允许的策略集合 P. 2004年, Boneh等人提出了带有关键字搜索的公钥加密方案(PEKS)[34], 并基于双线性对给出了实现. Abdalla等人[35]指出, 带有关键字搜索的公钥加密实际上和匿名IBE等价, 所以PEKS也是基于身份的加密体制的一种变型. 2008年, Sahai和Waters首次在PPT演讲中提出了函数(或功能)加密的概念; 第一次正式出现在文献中是2010年欧密会Lewko等人[36]的论文. 广义上来说, 诸如基于身份的加密、匿名IBE、基于属性的加密ABE、隐藏向量加密HVE、内积断言加密、广播加密、基于身份的广播加密、基于分层身份的广播加密、可搜索加密等都属于功能加密的各种不同特例. 可见, 功能加密的应用极为广泛, 可用来确定对加密数据的访问权, 实现不同权限用户访问不同加密数据的功能. 一般的, 函数或功能加密就是对于消息 m 的密文 C, 用对应于函数 f 的密钥 SK_f 解密可以得到函数 f 作用在 m 上的结果 $f(m)$. 利用双线性对可以实现函数加密, 不过所涉及的函数 f 都是比较简单的函数. 由于基于属性的加密可以在云存储中实现高效、精细、灵活的密文访问控制, 函数加密和可搜索的加密可以实现对加密消息的操作, 所以基于身份的密码体制及其推广方案被广泛应用于隐私保护和访问控制, 特别是在当前比较热门的安全云计算领域有重要的应用.

3.3 数字签名

双线性对在密码构造中另一个重要的应用是构造短签名，短的数字签名在某些环境下特别是通信带宽和存储空间受限制的情况下是需要的. 例如当在一个掌上驱动设备(象Palm或PDA)上激活一个软件时，用户常常被要求键入一个提供在CD上的签名. 类似的，因为空间的限制，当在一个数字邮戳上加一个条码时，短的签名也是需要的. 两个最常用的数字签名方案是RSA和DSA. 在80比特的安全级别下，这两个签名方案分别提供1024比特和320比特长度的签名. ECDSA提高了DSA的效率，但签名长度依然是320比特. 基于双线性对的签名可以是G中一个元素，相当160比特的ECDSA安全级别的椭圆曲线的有理点可以用160比特表示. 目前利用双线性对构造的短签名方案主要有三个，这些短签名方案同时也是很多其他基于双线性对密码协议的设计基础. 第一个利用双线性对构造的短签名是Boneh等人[37]2001年提出的BLS方案，它的构造和安全性是基于CDHP. BLS签名需要一个特殊Hash函数，即将任意消息映射到椭圆曲线上的点(消息嵌入编码). 在2007年之前，到任意椭圆曲线上的消息嵌入都是概率算法. 2007年美密会上，Icart[38]提出了一个确定性多项式时间算法. 在2004年PKC上，张等人[39]提出了第二个基于双线性对的短签名方案ZSS04,同年Boneh和Boyen[40]在欧密会上给出了标准模型下安全的构造BB04. ZSS04和BB04的构造和安全性是基于Inv-CDHP，这个问题与CDHP等价. ZSS04和BB04方案比BLS方案有效，且不需要特殊Hash函数. 在2006年的越南密码会上，张等人[41]基于计算指数平方根问题(CSREP: $g, g^a \Rightarrow g^{a^{1/2}}$)提出了ZCSM06方案. 对于计算指数平方根问题的困难性，张[42]证明了当群的阶是某种特殊的素数时，CSREP与平方计算Diffie-Hellman问题(Squ-CDHP)等价，从而与CDHP等价. Roh等人[43]证明了在大多数情况下CSREP与CDHP等价.

我们将这三个基于双线性对的短签名方案描述如下:

系统参数 $e: G\times G\to G_T$, $\langle g\rangle = G$, $q=\mathrm{ord}(G)$, $H_1:\{0,1\}^*\to G$, $H_2:\{0,1\}^*\to Z_q$.

公钥: $v=g^s$, 签名私钥是 s.

BLS01方案: 签名: $\sigma = H_1(m)^s$, 验证: $e(\sigma, g)=e(H_1(m), v)$.

ZSS04, BB04方案: 签名: $\sigma = g^{1/(s+H_2(m))}$, 验证: $e(\sigma, vg^{H_2(m)})=e(g,g)$.

ZCSM06方案: 签名: $\sigma = g^{(s+H_2(m))^{1/2}}$, 验证: $e(\sigma,\sigma)=e(vg^{H_2(m)}, g)$.

除了这几个短签名方案，还有几个非常重要的利用双线性对构造的签名方案，它们是:

Waters05签名方案[30]:

公钥: $g, g_1=g^a, g_2, u', u_1, \cdots, u_n\in G$; 私钥: g_2^a; 消息签名对: $m, \sigma=\left(g_2^a\left(u'\prod_{i:m_i=1}u_i\right)^r, g^r\right)$.

验证: $e(g_1,g_2)e\left(g^r, u'\prod_{i:m_i=1}u_i\right)=e\left(g_2^a\left(u'\prod_{i:m_i=1}u_i\right)^r, g\right)$.

Camenisch-Lysyanskaya签名(CL04)方案[44]:

公钥: $g, X=g^x, Y=g^y\in G$; 私钥: x, y; 消息签名对: $m, \sigma=(a,b,c)=\left(a, a^y, a^{x+mxy}\right)$.

验证: $e(a,Y)=e(g,b)$, $e(X,a)e(X,b)^m=e(g,c)$.

Okamoto签名(TCC06)方案[45]:

公钥: $g, w=g^x, u, v\in G$; 私钥: x; 消息签名对: $m, \left(r, s, \sigma=\left(g^m uv^s\right)^{1/(x+r)}\right)$

验证: $e(\sigma, wg^r)=e(g, g^m uv^s)$.

给定一签名方案 $(\mathrm{PK},\mathrm{SK})$, $\sigma\leftarrow\mathrm{Sign}(\mathrm{SK}:m)$, 按照消息签名对的关联情况，我们把签名分成三种级别:

1级: 给定一消息签名对(m,σ), 任何人都可以通过签名验证算法检验(m,σ)是否是一对合法的消息签名对;

2级: 只给出消息 m, 签名拥有者可以给出一个他拥有签名者对消息 m 的签名 σ 的证明, 但不泄露签名 σ 的任何信息;

3级: 消息 m 和签名 σ 都不公开, 拥有者可以给出一个证明他有签名者的一个合法的消息签名对.

1级是数字签名的基本要求, 所有的签名方案都必须满足这个要求. 如果一个签名方案满足2级的要求, 则这个签名方案可以用来设计基于身份的签名: 签名者是 PKG, 消息 m 是签名拥有者的身份信息, m 的签名 σ 就是签名拥有者的私钥. 签名拥有者对他拥有 m 的签名 σ 的知识证明就是基于身份的签名. 如果一个签名方案达到了3级水平, 则这个签名方案可以用来构造匿名群认证、群签名、直接匿名认证(DAA)等方案. 上面提到的几个基于双线性对的密码体制都可以达到1级和2级的水平, 但并不是所有的方案都达到了3级水平. ZSS04、BB04和CL04都达到了签名的3级水平, 所以这些方案被广泛用来设计隐私保护方案.

除了以上提到的关于双线性对在密码中的应用, 双线性对还有其他形形色色的应用: 如聚合签名、可验证加密的签名、部分盲签名、代理重加密、秘密握手协议等.

这几年, 基于双线性对的密码体制, 特别是基于身份的密码体制在工业界已经有了许多应用实例. 随着应用的逐渐广泛, 国际上许多标准组织也在积极地进行这一密码体制的标准化工作. 2006年, 国际标准化组织ISO在ISO/IEC 14888-3中给出了两个利用双线性对设计的基于身份的签名体制的标准; IEEE也组织了专门的基于身份的密码体制的工作组(IEEE P1363.3). 2007年8月, NIST也在着手制定基于身份的密码体制和基于双线性对的密码体制的标准. 我国也启动了基于身份的密码体制的标准化工作, 制定了商用密码标准SM9(IBC标识密码算法).

4 双线性对面临的安全挑战

如果双线性对群 G_1,G_2 或 G_T 中的离散对数可解, 那么基于双线性对的密码体制是显然不安全的. 例如, 如果 G_T 中的离散对数可解, 则双线性对逆问题(BPI, 即给定 $P,e(g,X)=a$, 去计算 X)迎刃而解了. G_T 是有限域的乘法子群, 所以有限域的DLP如果可解, 那么双线性对就不安全了. 有限域 $\mathrm{GF}(q)$ 上的DLP的有亚指数时间算法: 数域筛法或函数域筛法, 其计算复杂度是:

$$L_q\left(\frac{1}{3},c\right)=\exp\left((c+O(1))(\log q)^{1/3}(\log\log q)^{2/3}\right)$$

这里 $q=p^n$, c 是一个常数. 2013年, Joux[46]对于小特征有限域改进了这个算法, 将 $1/3$ 降为 $1/4+O(1)$. 这使得小特征有限域上的DLP计算效率大大提高, 从而出现了一些新的DLP的计算记录, 如Menezes等人在2014年2月用1201个CPU时间计算出了1551比特的有限域 $\mathrm{GF}(3^{6\times 163})$ 上的DLP; Robert Granger等人在2014年1月计算出了9234比特的有限域 $\mathrm{GF}(2^{9234})$ 上的DLP等. 更多的结果可以参看Joux和Pierrot发表在今年DCC上的关于小特征有限域DLP的综述文章[47]. 这些结果使得基于小特征有限域特别是合数扩域已经不适合用来构造基于离散对数的密码体制, 并且建立在特征为2,3或中小规模特征的有限域上的双线性对密码体制也基本不安全了. 这使得一型的双线性对($e:G\times G\to G_T$)基本不能用了. 因为一型双线性对主要是利用超奇异椭圆曲线实现, 主要是用下面两种选择: 一是利用特征为2,3的有限域, 此时嵌入次数是 4 和 6. 这种选择能使得 G 中群元素有短的表示, 从而可以实现短签名. 但由于Joux的算法, 这类双线性对已经不安全了. 另一种选择是利用大素数域 $\mathrm{GF}(p)$ 上嵌入次数为1或2的超奇异椭圆曲线, 为了达到2^{80}的安全性, 这里的 p 至少是1024或512比特(分别对应于嵌入次数1和2)的素数, 这使得这样构造的类型1的双线性对所设计

出的签名不再是短的了，并且实现效率也不高了．现在只有大素数域上类型2和类型3双线性对可以使用．

另一方面，随着对双线性对的挖掘和研究，发现双线性对的功能有限，在设计一些新的密码协议时功能上欠完善．例如我们可以利用双线性对设计函数加密，但这样的函数只能是一些简单函数，对复杂的函数利用双线性对就很难设计了．另外，基于双线性对的密码体制的研究已经超过15年了，能想到的有趣的方案都基本被设计出来了，新颖的或有意义的结果较难出现．为了给学术界和工业提供一个关于双线性对的研究和应用的交流平台，Pairing 2007作为一个国际会议第一次在日本召开．之后每年举办一届．但随着双线性对密码体制研究热度的减退，这个会议的投稿数量逐年减少，最终在召开了Pairing 2013后，Pairing会议停止举办了．这也宣告着双线性对的研究热潮已经过去了．

双线性对的定义可以推广到多线性映射，从而可以利用多线性映射设计密码协议，使得一些利用双线性映射无法完成的密码协议，可以借助多线性映射实现，如一轮多方密钥协商协议、广播加密、支持一般电路的属性加密方案等，即使在实用的多线性映射没有出现之前，就已经有一些利用多线性映射设计的密码体制．2013年，Garg、Gentry和Halve于EUROCRYPT 2013[5]上提出了第一个候选的基于理想格的多线性映射．自从有了这一多线性映射的实例，密码界掀起了基于多线性映射的密码体制研究热潮，出现了各种各样的功能新颖的密码协议．

5 多线性映射及其构造

5.1 多线性映射与分级编码系统

Boneh与Silverberg[48]于2003年提出双线性对的推广概念——多线性映射．相对于双线性对，多线性映射将更多循环群关联到目标循环群．若用符号 $G_i=\langle g_i\rangle$ 表示循环群及其生成元，k,i,a 表示整数，假设所有的循环群的阶数相等，那么映射 $e:G_1\times G_2\times\cdots\times G_k\to G_T$ 称为多线性映射，当且仅当其具有以下性质：

(1) $e\left(g_1,\cdots,g_i^a,\cdots,g_k\right)=e\left(g_1,\cdots,g_k\right)^a$；

(2) 映射 e 非退化．即当 g_i 分别是 G_i 的生成元时，$e\left(g_1,\cdots,g_k\right)$ 是 G_T 的生成元．

上面描述的多线性映射属于非对称类型．如果连接成笛卡尔积的各个群是相同的，则多线性映射是对称类型的．实际上，双线性对是一个线性等级为 2 的多线性映射．用在密码中的多线性映射需要一些相关联的问题是计算困难的，如多线性离散对数问题：对每一个 i，给定 g_i 和 $g_i^a\in G_i$，计算 a．考虑 k 级对称多线性映射，推广双线性计算Diffie-Hellman问题和判定Diffie-Hellman问题到多线性映射的情形，我们有如下两类重要的问题：

多线性计算Diffie-Hellman(MCDH)问题：给定 $g,g^{a_i},i=1,2,\cdots,k+1$，计算 $e\left(g,\cdots,g\right)^{a_1\cdots a_{k+1}}$．

多线性判定Diffie-Hellman(MDDH)问题：给定 $g,g^{a_i}\in G,i=1,2,\cdots,k+1,g'^c\in G_T$，判定是否 $c=a_1\cdots a_{k+1}$．

这些问题是利用多线性映射设计密码协议时常用到的困难假设．

多线性映射的构造在很长一段时间困扰着研究人员．一种直接的想法是以双线性对为跳板，从椭圆曲线、代数几何中寻找构造方法．Boneh和Silverberg[48]在尝试这种方式的过程中总结出一个令人遗憾的结论——多线性映射可能很难从代数几何中得到，或者说多线性映射的构造方法不能用看似自然的几何知识来解释．这项工作提醒了研究人员，多线性映射的构造也许得借助新开发的工具．分级编码系统提供了一个构造多线性映射的新方法．分级编码系统和多线性映射非常类似，和代数中的分级代数相似，一个分级编码方案的编码元素都对应一个分级．下面给出分级编码系统的定义，详细的讨论可参看文献[5].

一个***k*-分级编码系统**由环 R 与集合 $S=\left\{S_i^{(\alpha)}\subset\{0,1\}^*:\alpha\in R,0\leqslant i\leqslant k\right\}$ 组成，并且满足以下性质：

(1) 对每一个固定的指标 i，集合 $\left\{S_i^{(\alpha)}\subset\{0,1\}^*:\alpha\in R\right\}$ 是不相交的，从而不同元素所对应的集合构成 S_i

的一个划分, 即 $S_i=\bigcup_\alpha S_i^{(\alpha)}$;

(2) 存在加操作‘+’和取反操作‘−’, 使得对于任意的 $\alpha_1,\alpha_1\in R$, 所有的 i, 以及每一个 $u_1\in S_i^{\alpha_1}$, $u_2\in S_i^{\alpha_2}$, 满足 $u_1+u_2\in S_i^{\alpha_1+\alpha_2}$ 和 $u_1-u_2\in S_i^{\alpha_1-\alpha_2}$.

(3) 存在乘法操作‘×’, 使得对于任意的 $\alpha_1,\alpha_1\in R$, 任意满足 $0\leqslant i_1+i_2\leqslant k$ 的级数 i_1,i_2 和任意的 $u_1\in S_i^{\alpha_1}$, $u_2\in S_i^{\alpha_2}$, 则有 $u_1\times u_2\in S_i^{\alpha_1\alpha_2}$.

另外, 分级编码系统会带有一个零检测算法 ZT (即给定一个编码 u, 判定它是否是0元素的一个 i 级编码, 即是否 $u\in S_i^0$)和提取算法 Ext (即给定一个 i 级编码 u, 可产生 u 的一个规范表示, 使得如果 $u,v\in S_i^\alpha$, 那么 $\mathrm{Ext}(u)=\mathrm{Ext}(v)$). 分级编码系统从 i 级到 $i+1$ 级编码一般要求是容易计算的, 但从 $i+1$ 级编码去计算对应的 i 级编码是困难的, 也即从任何一级编码去求这个编码的源像是计算困难的, 这就类似于离散对数问题在编码系统中的模拟.

5.2 多线性映射的实现与安全性现状

2013 年, Garg、Gentry 和 Halve 于 EUROCRYPT 2013 会议上提出了第一个候选的基于理想格的多线性映射. GGH13 多线性映射实际上是一种构建于理想格之上的带噪声的分级编码系统, 可分别实现对称和非对称两种形式的多线性映射. GGH13 多线性映射的构造中包含着三个集合(它们都是交换环): $R=Z[x]/(x^n+1)$, $Rq=R/qR$, 以及 R/I. I 是多项式 $g(x)$ 生成的理想. 被编码的消息取自 R/I. 消息 d 的编码是具有如下形式的多项式 $c=\left[(dv+rX)/z^k\right]_q$, 以参数 k 标定编码的等级. 这里 g 和 z 都是秘密参数, 且 g 和 g^{-1} 都有短的表示. y 是元素 1 的一级编码, $X=(x_1,\cdots,x_m)^{\mathrm{T}}$, x_i 是元素 0 的一级随机编码. 同级编码之间可以相加, 以此来模拟群运算. 不同级的编码相乘得到更高级的编码, 以此来模拟线性映射运算. 由于编码带有噪声, 所以即使是相同的消息编码两次也很难判定原像是否相等. 幸运的是, 关键的零检测参数 Pzt ($=\left[hz^k/g\right]_q$, 这里 h 是某个小的环元素)能够排除掉合法编码中噪声的干扰, 从而实现判定相等的功能. GGH13 多线性映射不完全符合 Boneh 等人[48]对多线性映射的原始定义. GGH13 的支撑集并不是循环群而是编码集合, 映射的中间结果是可得的, 即 k 级多线性映射可以拆分成许多 $0<j<k$ 级的多线性映射, 并且一些预期困难的问题如线性判定, 子群关系判定等问题在分级编码系统中并不困难. 尽管存在参数大、运行效率低等缺陷, GGH13 方案的出现带动了一波多线性映射的研究热, 并且奠定了以分级编码构造多线性映射的模式.

几个月后的 CRYPTO 2013 会议上, Coron、Leipoint 和 Tibouchi[6]发现了基于整数环设计的多线性映射. CLT13 多线性映射亦属于对环元素进行操作的分级编码系统, 可实现非对称与对称形式的多线性映射. 与 GGH13 不同的是, CLT13 采用的是整数剩余类环. 出于对功能和安全性的考虑, 方案将编码所在的整数剩余类环经由中国剩余定理直和分解成多个小环, 并且隐藏与小环相关的各个模数. 被编码的消息实际上由各个小环中选出, 隐藏模数使得被它们拥有看似很强的隐蔽性. 消息 m_i 的编码是具有如下形式的整数 $c=(r_ig_i+m_i)/z^k \bmod p_i$. 2015 年 TCC 会议上, Gentry、Gorbunov 和 Halevi[7]通过借鉴全同态加密方案[49]中矩阵特征值的思想, 构造了基于图的多线性映射 GGH15. 本质上, GGH15 也属于对环元素的分级编码系统, 不过这里的环不同于之前两个多线性映射方案中的环, GGH15 所基于的环是矩阵环, 这是一个非交换环. 系统首先初始化与应用相符合的图, 每个点对应一个随机矩阵, 编码的等级由图中的边标定. 被编码的元素 S 为范数小的矩阵, 以 LWE[50]假设确保了求逆 S 的难度. 生成的编码为范数小的矩阵 D, 以 SIS 假设[51]排除了伪造编码的可能性. 最终, 消息 S 关于边 $u\to v$ 的编码 D 可以形式化定义为 $DA_u=A_vS+E \bmod q$ 的小解. 这里 E 是一个小错误向量. 如果 S 是 0, 那么 $DA_u=E$ 是小的. 所以 GGH15

的零检测非常简单，就是检测 DA_i 是不是小的. 由于与图中点相关的矩阵 A_i 是随机矩阵，使得方案的安全性与格中的困难问题相关. 这意味着 GGH15 相较于 GGH13 可能有更强的可证明安全性. 事实上，分别与 D 和 S 关联的 SIS 问题和 LWE 问题已经被证明与最坏情况下格困难问题的难度相当. GGH15 的原始方案实现的是非对称类型的多线性映射，并且难以直观地将其转化为对称形式. 2014 年，Langlois、Stehle 和 Steinfeld[52]对 GGH13 方案中的重随机化程序提出改进建议，将新方案命名为 GGHLite. 与 GGH13 相比，GGHLite 的公共参数比特位数和重随机化参数(噪声分量)的个数都有较大幅度减少. 同年，Albrecht 等人[53]在 GGHLite 方案的基础上，继续改进了系统参数 q 与零检测程序中最高比特位的选取位数 l，进一步提高 GGHLite 的效率，并且使用免费软件库实现了基于新 GGHLite 方案的 N 方一轮 DH 密钥协商协议. 其实验结果表明，GGHLite 方案性能明显优越于 CLT13 方案.

除了多线性映射的构造与效率改进，安全性也是多线性映射能否投入实用的重要因素. 传统的双线性对，如 Weil 对、Tate 对，已基本有一套建立在椭圆曲线上的安全性证明，保证了其中离散对数问题、Diffie-Hellman 问题，双线性 Diffie-Hellman 问题等问题的难度. 以分级编码系统为主的多线性映射目前还没有达到这样的水平. 由于分级编码系统(可理解为分级环)与循环群本质上的区别，传统双线性对中困难问题的规约方法不能被借鉴到多线性映射的分析上来. 从目前的情况来看，仅对于模拟的离散对数问题来说，GGH13 多线性映射在形式上非常接近于与理想格相关的 LWE 问题和 NTRU 假设[54]，但是研究人员无法证明这些问题是等价的. CLT13 多线性映射存在着同样的烦恼，它在形式上与近似最大公因子(AGCDP)相似，却不存在有效的规约算法. 目前看起来，这些有效规约的存在性都很困难证明. GGH15 的情况比较乐观，随机格上的 LWE 问题与 SIS 问题有效地保证了它的安全性. 关于格上的一些困难问题的研究在这里我们不做讨论，有兴趣的可以参见文献[55]. 不管是原方案还是改进的方案，没有被完善证明的安全性会留下了一些安全隐患，这为接下来一系列的攻击工作埋下了伏笔.

2014 年，Lee 与 Seo[56]依照 CLT13 多线性映射方案的特点，定义了新问题 n-MPACD. 在对该问题的困难程度进行分析时，借鉴了 Chen 和 Nguyen 的中间相遇算法[57]，将这个问题的求解时间从 CLT13 的分析中的 $O\left(2^{\rho}\right)$ 降低至 $O\left(2^{\rho/2}\right)$. 参数中的 ρ 是 CLT13 方案中随机数的比特长度. 该文章由此对 CLT13 方案零检测参数生成过程中用到的随机数矩阵 H 提出了改进建议，矩阵 H 的范数需要足够大才能将算法求解该问题的时间提升至安全级别. 同年，Cheon 等人[58]将零化攻击方法引入 CLT13 方案的分析当中，将 CLT13 所有系统隐藏参数逐一恢复，这意味着 CLT13 方案被完全攻破. 该攻击算法利用到了这样一个事实，大量公开的重随机化参数(噪声)能够帮助敌手获得大量的 0 元素的最高级编码，这些编码在零检测程序中的模运算下实际上是没有进行任何取余数操作的. 没多久，Gentry 等人在工作[59]中指出，CLT13 方案即便不公开 0 的一级编码(重随机化参数属于这一类)，依然可能遭受 Cheon 等人零化攻击的威胁. 简单来说，如果参数具有一定的特性，便能够利用已知的参数构造 0 元素的编码. 通过这些信息依然能够生成 0 的最高级编码进而使用零化攻击. 后来的工作中将这种具有一定特性的编码称为正交编码. 为了弥补 CLT13 方案的漏洞，Boneh 等人对 CLT13 提出了改进建议[60]，目的是消除编码中的线性关系，使零化攻击中特别是构造矩阵求特征值这一步无法进行. 不过这种方案增加了 CLT13 的规模，效率有所降低. 与此同时，Garg 等人[61]在工作中提出了将重随机化参数嵌入矩阵进行隐藏. 这种做法能够在不影响重随机化参数功能的情况下令零化攻击得不到运行所必须的参数. 以矩阵隐藏公共参数，同样导致了 CLT13 性能的降低. 遗憾的是，CLT13 的漏洞的修复方案并没有经受住太久的考验. Coron 等人在文献[62]中指出了两种 CLT13 修复方案的缺点. 对于 Boneh 等人的修改方案，CLT13 的作者指出其依然存在线性关系，修改方案的原始目的并未达到. 对于 Garg 等人的修改方案，其中构造的矩阵，存在着各分块对角排列的事实. 这类矩阵的特征多项式等于各小分块的特征多项式之积，只要稍加改进零化攻击算法，便可对新方案进行攻击. 2015 年初，Coron、Lepoint 和 Tibouchi[63]提出新的基于整数的多线性映射 CLT15，试图从破坏编码与零检测结果之间的线性关系入手阻挡零化攻击. CLT15 主要改动了 CLT13 的编码过程和零检测过程. 为了顺利地进行零检

测步骤, CLT15 公布了新的参数 N 和新构造的零检测参数. 由于特殊的缩减编码的方法和模 N 操作, 作者认为 CLT15 不存在零化攻击算法所要求的线性关系和必要参数, 方案是安全的. 不过, Cheon 等人[64]以及 Minaud 和 Fouque 在 EUROCRYPT 2016 的工作中指出, CLT15 可以被算法退化为 CLT13 而继续受到零化攻击的威胁.

CLT13 被完全攻破之后, GGH13 方案也遭受了攻击. 攻击 GGH13 方案的目标是利用公开的参数要么恢复出秘密参数, 要么是找其他方法攻击模拟的 DLP、CDHP 或 DDHP. 目前 GGH13 方案的多线性判定 Diffie-Hellman(MDDH)问题被胡等人[65]攻破, 这个问题的困难性影响着部分多线性映射应用的安全性(如多方一轮 DH 密钥协商). 胡等人[65]首先使用弱化的离散对数攻击恢复出各个一级编码对应的零级编码, 但是其范数大小没有达到合法编码的要求. 随后, 他们利用自行设计的修改的编译码算法直接计算出了与合法的最高级编码和零检测参数相乘之后相互等效的结果. 这个等效结果可以解决 MDDH 问题. 胡等人还对基于 GGH13 的证据加密方案进行了攻击, 同时对 GGH13 方案的两个修改方案也进行了有效攻击. 胡等人的算法需要使用系统公共参数中 0 和 1 的一级编码, 古[66]针对这个情况提出了一种不包含这些参数的改进方案. 最近, Cheon 等人[67]提出了一种计算 NTRU 问题的算法, 并直接利用该方法构造 0 的零级编码从而多项式时间攻击了无零元素编码的 GGH13 方案. Miles 等人[68]利用非线性多项式提出了一种称为零化或湮灭(Annihilation)攻击的方法, 该攻击可以在没有零的低级编码情况下工作, 从而将 GGH13 多线性映射方案不管有没有公开零元素的编码信息都可以被多项式时间攻破. 借助零化攻击, Miles 等人对基于 GGH13 的不可区分混淆方案给出了一个多项式时间攻击. 该攻击的核心是找可有效表示的零化多项式. 虽然 GGH15 拥有较为优秀的困难性规约, 其应用方案的安全性却受到了密码研究人员的分析. 2015 年, Coron[69]发布了其针对基于 GGH15 方案的 DH 密钥交换协议的的攻击算法, 该算法借鉴了 Cheon 等人[58]的攻击方法, 完成类似于胡等人对多线性映射衍生问题的攻击, 显露出分级编码系统可能存在着许多未被发现的安全问题. 基于 GGH15 实现的多方一轮 DH 密钥协商遭受攻击后, 古[70]提出了此种多线性映射的一个变种.

还存在另外一种构造多线性映射的方法就是利用自线性对来构造. 自线性对是特殊的双线性对, 其目标循环群与组成原像的循环群相同, 即 $e: G\times G\to G$. 这样, 一旦构造出可用的自线性对 e, 通过首尾拼接 k 个 e 能够获得一个 $k+1$ 级的多线性映射. 然而自线性对的构造前景因为 Cheon 和 Lee[71]的结论“已知阶数的素数阶循环群中不存在自线性对”而变得渺茫. 所以要构造出安全的自线性对, G 只有考虑为以下两种情况: (1) G 不是素数阶群或群的阶不知道; (2) G 不是群. CRYPTO 2014 上, Yamakawa 等人[92]给出一种弱化的自线性对的构造. 该方案选择模 N 的二次剩余类 QRN 作为底层支撑的循环群, 其中 $N=pq$ 是 RSA 模, 群的阶不作为参数公开. 方案利用 iO 电路隐藏了一部分帮助有效计算线性映射的参数, 并公布这些 iO 电路作为辅助信息. 辅助信息的加入是该自线性对与原始定义不同的地方, 之所以称之为弱化的自线性对也是这个原因. 就目前看来, 由该自线性对组成的多线性映射相较于分级编码系统实现的多线性映射, 有映射等级无需事先确定的优点. 受其启发, 张等人[73]发现集合一旦具有某些特殊性质, 即可用于构造弱化的自双线性映射, 并将具有这类特殊性质的集合总结定义为单向编码系统, 并在抽象的概念上给出弱化自线性对的通用构造方法和困难问题的规约过程. 尽管以上两种自线性对的构造都用到了混淆, 并且后面会看到通用混淆也是利用多线性映射构造的. 但这些自线性对的构造并不矛盾, 因为用来构造自线性对的混淆可能只是某一特定函数的混淆, 这个混淆的构造可能不需要利用多线性映射也能实现. 也存在利用不可区分混淆来构造多线性映射的方法. 2015 年 Albrecht 等人[74]在假设不可区分混淆存在的前提下给出了多线性映射的构造方法. 后面会讲到, 目前不可区分混淆的构造都是依赖多线性映射的构造. 虽然目前还没有出现不依赖多线性映射的不可区分混淆的实现, 但这个研究的确带来了一种新的多线性映射的构造模式.

6 多线性映射在密码中的应用

多线性映射在密码中具有广泛和重要的应用, 在没有具体的多线性映射构造之前就已经有一些应用协议被设计出. 多线性映射的具体构造被提出后密码研究领域马上掀起了基于多线性映射的研究热潮, 更多更新颖的密码应用被发现. 作为双线性对的推广, 多线性映射很自然的可以用以实现多方一轮密钥协商和广播加密. 下面我们用分级编码为基础的多线性映射给出 N 方一轮密钥协商协议的设计思路:

假定有一个多线性映射方案, 该方案所采用的分级编码系统有一个在 $N-1$ 级的零检测算法(零检测参数是 Pzt)和一个提取算法 Ext. N 个参与方首先各自秘密选取一个 0 级编码 s_i, 将 s_i 升为 1 级编码 a_i, 然后将 1 级编码 a_i 公布出去. N 方中的任何一个参与者都知道自己公开的 1 级编码所对应的 0 级编码元素, 利用其它 $N-1$ 方的 1 级编码元素相乘, 再乘上自己的 0 级元素, 就得到了 $s_1 s_2 \cdots s_N$ 的 $n-1$ 级编码. 例如参与方 j 可计算如下: $s_j \times a_1 \times \cdots \times a_{j-1} a_{j+1} \times \cdots \times a_N \in S_{N-1}^{s_1 s_2 \cdots s_N}$.

每个参与者利用 $N-1$ 级提取算法作用在上面的乘积上. 根据提取算法的正确性, 每个参与者都可以得到相同的共享值. 目前存在的几个多线性映射的方案都可以利用这个设计思路给出 N 方一轮密钥协商协议的实现.

伪随机函数在密码中有着重要的应用. ASIACRYPT 2013 上, Boneh 和 Waters[75]提出了限制型伪随机函数(CPF)的概念. 限制伪随机函数与通常的伪随机函数不同, 它公布了一个函数定义域的子集 S. 主密钥持有者能够计算并发布跟子集 S 相关的子密钥 K. 拥有密钥 K 的用户, 可以有效计算子集 S 中元素的函数值, 但对于 S 之外的元素无能为力. Boneh 和 Waters 在给出限制型伪随机函数的定义的同时, 基于多线性映射构造了该类函数.

基于属性的加密(ABE)是基于身份的加密的推广, 当加密消息 m 时, 与一组属性变量 x 绑定. 生成用户的解密密钥时, 与对应的策略函数 f 绑定. ABE 要求用户用密钥解密密文时, 当且仅当 $f(x)=1$ 时才能解密出正确的明文消息 m. 策略函数一般利用布尔函数或电路来实现. 利用双线性对可以实现布尔电路, 但由于双线性对的映射只能执行一层, 因此在应用到电路模型中时无法往下拓展. 多线性映射可以实现多项式级别的层数, 因此非常适合在电路上作用. 利用多线性映射可以实现对任意多项式规模电路的策略函数的基于属性的加密[76]. 基本的实现步骤如下: (1) 将策略函数 f 表示成多项式规模的布尔电路, 该电路包括与、或、非三种门. 对电路的每个输入端, 每根连线, 每一个门按顺序编号. (2) 对策略函数生成对应的密钥时, 对电路中的每根连线, 根据其层数及对应的门的类别, 生成不同的编码. 属于同一层的连线编码到同一级中. (3) 加密消息 m 时, 选取一个随机数, 与其属性变量 x 绑定, 将消息 m 盲化. (4) 用户用私钥解密时, 将密文输入到电路中, 利用多线性映射, 逐层计算到输出端. 如果满足 $f(x)=1$, 则会得到去盲的变量, 解密出 m; 如果 $f(x)=0$, 则电路计算到中间某一步时会无法往下计算, 得不到最后的解盲变量. 韩等人[77]基于多线性映射给出了支持电路结构的属性签密方案.

证据加密(Witness Encryption)是基于多线性映射的一个新概念. 它是一类解密凭证与 NP 问题相关的加密协议. 传统公钥加密、基于身份的加密和基于属性的加密等方案都可以以证据加密为基础来构造. STOC 2013 上, Garg 等人[78]在给出证据加密定义的同时, 利用“近似”多线性映射构造了基于精确覆盖问题的证据加密方案. 基于身份的聚合签名能够在基于身份的密码构架下将不同用户的对不同消息的签名聚合成一个签名. 基于多线性映射, Hohenberger 等人[79]于 CRYPTO 2013 上首次给出了这类聚合签名的构造. 利用多线性映射还可以实现聚合的可验证加密的签名、可编程的哈希函数、同态 MAC 等.

多线性映射引起密码界甚至计算机领域学者重视的一个原因是它可以构造不可区分的混淆(Indistinguishability Obfuscation a.k.a. iO). 混淆(Obfuscation)的概念最早提出于计算机程序处理领域, 早期的程序混淆大多体现在计算机领域的代码混淆(Code obfuscation). 2001 年, Barak 等人[80]首次给出了程序混

淆(Program obfuscation)的形式化定义及安全性要求, 使得程序混淆有了严格的理论依据及安全性证明方法. Barak 等人在他们的文章中提出了在图灵机模型下及电路模型下的混淆的形式化定义. 定义从功能性、效率性及安全性三个方面来描述. Barak 等人在给出“虚拟黑盒混淆”安全性定义的同时, 也指出其局限性: 即不存在对任意函数的通用虚拟黑盒混淆. 因此针对虚拟黑盒混淆的研究主要局限在针对具体函数类的安全混淆, 如点函数, 重加密函数, 加密的签名函数, 函数加密等. 关于早期混淆的研究和一些特殊函数的混淆的工作, 请参看成和张在这方面的综述文献[81]. 同混淆研究的另外一条路径就是弱化安全混淆的定义以求达到对任意函数的混淆. Barak 等人[80]建议对通用程序(电路)实现一种弱化的混淆目标, 也就是不可区分的混淆. 功能相同规模相当的两个电路经过不可区分混淆技术处理后, 所得到的混淆电路在计算上是不可区分. 根据 Goldwasser 和 Rothblum[82]的说法, 不可区分的混淆虽然是一种弱化的概念, 但是达到了最优混淆(Best-Possible Obfuscation)的效果, 即对于所有同类型电路, 最优混淆的结果隐藏了最多的输入信息. 不可区分的混淆的概念提出后, 其构造成为了公开问题. 直到多线性映射得以实现, Garg、Gentry、Halevi、Raykova、Sahai 和 Waters[83]才于 FOCS 2013 上给出了第一个可以对任意多项式规模电路进行不可区分混淆的方法. Garg 等人的不可区分混淆的实现分为两个步骤, 先借助全同态加密实现对所有多项式规模电路的加密, 然后实现对 NC1 电路(深度是变量个数的对数级别且每个门是扇入为 2 的电路)的不可区分混淆(注意到解密电路通常是属于 NC1 的), 从而实现了通用程序混淆器的构造. 借助全同态加密, 对任意函数的不可区分混淆的构造就集中在 NC1 电路的混淆了. NC1 电路的混淆方法如下: 先把 NC1 电路转化为布尔表达式, 然后借助 Barrington 定理将其表示成分支程序(Branching program), 再将分支程序用置换矩阵表示出来, 最后将置换矩阵中的每个元素用多线性映射中的分级编码进行随机编码. 编码之后的所有元素即为混淆后的结果. 该混淆过程的功能性体现在, 将编码后的矩阵执行乘积的过程可以用多线性映射来实现, 将最终映射的结果与检测矩阵的编码做对比(利用多线性映射的零检测算法)得出最后函数的输出.

目前的 iO 方案需要以多线性映射作为底层工具. 2015 年 Albrecht 等人[74]在假设 iO 存在的前提下给出了多线性映射的构造方法. 这一工作出现后, 引发了一个很自然的猜想——多线性映射与 iO 是否本质上是等价的, 即多线性映射与 iO 之间是否可以互相转化? Paneth 和 Sahai[84]通过定义新的多项式拼图(PJP), 完成了 PJP 与 iO 之间的转化. PJP 是多线性拼图(MJP)的一个替代, 它们都是一类特殊的多线性映射. 这一工作将多线性映射的研究和不可区分混淆的研究紧密联系起来了.

Garg 等人给出 iO 的构造之后, 陆续有很多研究者[85–91]在他们工作的基础上, 用各种多线性编码模型构造或改进了不可区分混淆器方案甚至 VBB 混淆器方案. 这些构造主要可分为以下两种方法: 一种是通过 Barrington 定理和 Killian 定理, 将电路的布尔公式转化为矩阵形式的分支程序, 再对矩阵进行编码; 另一种方法是直接绕开上面那种转化为矩阵分支程序的方法, 用合数阶多线性映射直接对布尔函数的算术电路形式做编码操作. 当前程序混淆的构造方法都是基于多线性分级编码的形式, 在具体实现效率方面将是一个很大的瓶颈. 由于现有的几个多线性映射都是带噪声的, 它们都要依赖噪声去隐藏所要编码的元素. 因此在具体编码时, 编码元素和运算操作会随着电路规模的增大而指数级的增多. Apon 等人[92]首次给出了密码学程序混淆的具体软件仿真实现. 他们混淆过最复杂的函数是由 15 个与门构成的 16 比特点函数, 所用的机器是 Amazon EC2 上 32 核、244 GB RAM 的云服务器. 整个混淆程序执行过程就用了 9 个小时, 混淆后的程序空间规模占用了 31.1 GB. 而让人惊讶的是, 单单对这 16 比特点函数, 输入一个单一输入值后, 整个混淆程序的估值需要 3.3 个小时. 诚然, 通过更高核数和内存的计算机来运行这混淆的程序, 效率会提升很多. 然而, 从这看出, 利用当前混淆的构造方案, 若要实现对一个秘密函数或一个通用的函数混淆将消耗大量的计算资源、存储空间. Horv´ath[93]在密码 eprint 上有一个关于混淆的综述, 将最近几年混淆在安全定义、构造等方面的研究工作做了一个比较全面的总结.

有了Garg等人iO的构造之后, 许许多多令人惊奇的密码应用不断被提出, 如任意电路的功能加密[83]、可否认加密[94]、随机预言函数[95]、安全多方计算[96,97]、非交互式零知识证明NIZK[98]、叛徒追踪[98]、快速签名[99]、可验证的对称可搜索加密[100]、安全云服务方案[101]等. iO强大的让你感到震惊, 它把所有你想实

现的东西整成一个黑匣子, 只要你想到让这个黑匣子做什么功能, 并且这个功能在带秘密的情况下多项式电路可以实现, 那么就可以利用iO设计这样的功能的东西. 这些功能可能使用现有的密码工具无法实现或很难实现的. 所以, 利用iO设计密码协议和应用, 没有做不到, 只怕想不到! 因为iO的强大功能, 可以想象, 新奇的协议会不断被提出, 不只是在密码理论方面, 也可以渗透到各种各样的密码应用领域, 如云计算, 大数据, 网络, 图像处理等. 就像原来基于双线性对的密码学一样, 马上就要(或正已经)兴起基于混淆的密码学. 同时, iO的实用性也将被关注, 而实现iO的主要工具目前是多线性映射, 所以对多线性映射的安全性, 实效性的研究也将继续深入下去.

7 展望与结束语

双线性对和多线性映射是密码研究领域中两个非常重要的工具, 一个已经创造了辉煌, 一个正在创造着辉煌! 我们从学术研究角度展望一下这两个密码工具未来进一步可开展的有兴趣的研究.

首先, 考虑双线性对的安全性, 我们能不能攻破双线性对的最后防线. 对于当前实用的双线性对的构造, 如果有限域中的离散对数或者椭圆曲线(以及超椭圆曲线)的离散对数问题有了有效的求解算法的话, 相对应的双线性对密码体制将不再安全. 目前中小特征有限域上的离散对数问题指标计算算法有了明显的提高, 大特征有限域能否也能得以改进? 对于一些特殊的椭圆曲线的离散对数问题已经有了有效的算法, 但对于素数域 $\mathrm{GF}(p)$ 和特征2域 $\mathrm{GF}(2^n)$ 上的一般随机椭圆曲线的离散对数问题目前还没有快过平方根攻击(Pollard rho算法)方法出现. 这些问题不只是关系到双线性对密码体制的安全, 也是DSA和ECC的安全基石.

第二, 多线性映射的有效实现. 密码学是实用性很强的学科. 只要有用, 就值得做, 并会做的很深入. 双线性对就是一个例子, 双线性对刚被提出来的时候计算效率很差, 但后来就已经非常有效了. 多线性映射也会一样, 如今发现了它这么多的应用, 有些应用在理论上都是填补空白的, 所以对它的有效实现的研究一定会深入下去. 目前主流的构造多线性映射的方式主要是分级编码系统. 分级编码系统效率低规模大, 根本原因有两方面: (1) 噪声随着编码的等级快速增长; (2) 零检测程序一般是通过比较编码与“标杆”的大小来断定编码的合法性. 这造成“标杆”的量级很大, 进而引发相关参数取值很大. 所以, 研究这些构造中的“去噪”技巧是一个提高多线性映射效率的有效解决办法. 然而这些方案中的噪声是为了确保安全性而引入的, 依赖噪声去隐藏所要编码的元素. 我们把不带噪声的多线性映射称为“纯净”的多线性映射. 是否存在“纯净”的多线性映射? 如果存在, 如何去构造? 或者考虑是否存在不借助分级编码系统的多线性映射的构造? 如果要探索纯净的多线性映射, 或不借助分级编码的多线性映射的话, 格可能就不太适合了. 目前借助格工具构造的多线性映射, 主要是借助格引入的噪声来保证安全的. 如果不借助混淆的自线性对可以构造出来的话, 那么“纯净”的对称多线性映射就可以构造出来, 所以新的自线性对的设计也值得探索.

第三, 考虑多线性映射的安全性. 安全性是一切密码方案的核心. 多线性映射的研究中关注最多的还是安全问题. 基于分级编码的多线性不断被提出, 又不断被攻击, 然后又不断的被改进, 又被攻击. 目前除了基于一般格的GGH15方案的处境好一些外, 其他GGH13、CLT13以及它们的修正方案都不断的被分析. 不公开0编码信息的GGH13方案的攻击最近刚刚被攻破. 接下来, GGH15多线性映射方案将会是下一个攻击的目标, 估计不久就会有相应的攻击结果出现. 尽管GGH15的困难问题很接近环上的LWE问题, 但这是一个高维的情形. 攻击, 改进, 然后再攻击, 再改进, 这是所有密码体制走向应用的必经之路. 然而基于格的多线性映射的情形似乎太频繁了, 一个方案刚刚提出, 很快就被攻击了. 这段时间, 基于格的多线性映射方案的紧锣密鼓的攻击与修正. 这种状况延续下去可能会出现两个结果: (1)我们终于找到了安全有效的基于格上分级编码的多线性映射(或者设计出的方案较长时间内没有发现它的弱点); (2)也可能一直没有找到基于格的多线性映射. 如果出现第二种情况, 那我们不得不考虑这样的问题: 格是不是构造多线性映射的合适工具? 基于格的多线性映射和基于椭圆曲线的双线性对有很多不同, 它们基于的代数问题也不一

样. 深入挖掘格理论还是很必要的. 探索实现多线性映射的新工具值得深入研究.

最后一个是关于混淆的. 混淆的新应用一定会被不断的被发现, 这个我们这里不必去说. 我们关注的是混淆的安全性和有效实现. 尽管当前的混淆实现基本基于多线性映射, 但前面提到的对于多线性映射的攻击还不能用于混淆上, 这主要是因为混淆的构造所用到的多线性映射是不需要公开零元素的编码信息的, 而这些信息正是的前面所提到的攻击多线性映射时所需要的. 基于GGH13的混淆也被攻击了. CLT13被攻破了, 但利用它实现的不可区分混淆目前还是安全的. 一个公开问题是CLT13方案是否可以不借助0元素的公开编码信息也能被攻破? 如果这样的话, 基于CLT13的混淆实现也不安全了. 多线性映射及其在混淆构造中的应用, 只有GGH15还算是安全的, 但GGH15能抗多久是个未知数. 另外, 目前的混淆在实现效率上也非常低, 即使是一个简单的函数的混淆, 也要消耗大量的时间和内存. 所以提高效率是混淆走向实用的比较重要的研究工作.

致谢: 本文部分内容来自台湾第24届资讯安全会议(2014年5月)上的邀请报告, 在此对会议的组织者的邀请表示感谢! 同时感谢西安电子科技大学的胡予濮教授在多线性映射安全分析方面的讨论与建议!

References

[1] MENEZES A J, OKAMOTO T, VANSTONE S A. Reducing elliptic curve logarithms to logarithms in a finite field[J]. IEEE Transactions on Information Theory, 1993, 39(5): 1639–1646.

[2] SAKAI R, OHGISHI K, KASAHARA M. Cryptosystems based on pairing[C]. In: Symposium on Cryptography and Information Security, 2000: 135–148.

[3] JOUX A. A one round protocol for tripartite Diffie–Hellman[C]. In: Algorithmic number theory. Springer Berlin Heidelberg, 2000: 385–393.

[4] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]. In: Advances in Cryptology—CRYPTO 2001. Springer Berlin Heidelberg, 2001: 213–229.

[5] GARG S, GENTRY C, HALEVI S. Candidate multilinear maps from ideal lattices[C]. In: Advances in Cryptology—EUROCRYPT 2013. Springer Berlin Heidelberg, 2013: 1–17.

[6] CORON J S, LEPOINT T, TIBOUCHI M. Practical multilinear maps over the integers[C]. In: Advances in Cryptology—CRYPTO 2013. Springer Berlin Heidelberg, 2013: 476–493.

[7] GENTRY C, GORBUNOV S, HALEVI S. Graph-induced multilinear maps from lattices[C]. In: Theory of Cryptography. Springer Berlin Heidelberg, 2015: 498–527.

[8] FREY G, RÜCK H G. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves[J]. Mathematics of Computation, 1994, 62(206): 865–874.

[9] GALBRAITH S D, PATERSON K G, SMART N P. Pairings for cryptographers[J]. Discrete Applied Mathematics, 2008, 156(16): 3113–3121.

[10] MAURER U M. Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms[C]. In: Advances in Cryptology—CRYPTO 1994. Springer Berlin Heidelberg, 1994: 271–281.

[11] SADEGHI A R, STEINER M. Assumptions related to discrete logarithms: Why subtleties make a real difference[C]. In: Advances in Cryptology—EUROCRYPT 2001. Springer Berlin Heidelberg, 2001: 244–261.

[12] MILLER V. Short programs for functions on curves[J]. Unpublished manuscript, 1986, 97: 101–102.

[13] DUURSMA I, LEE H S. Tate pairing implementation for hyperelliptic curves $y^2=x^p-x+d$[C]. In: Advances in Cryptology—AsiaCrypt 2003. Springer Berlin Heidelberg, 2003: 111–123.

[14] HESS F, SMART N P, VERCAUTEREN F. The eta pairing revisited[J]. IEEE Transactions on Information Theory, 2006, 52(10): 4595–4602.

[15] ZHAO C A, ZHANG F, HUANG J. A note on the Ate pairing[J]. International Journal of Information Security, 2008, 7(6): 379–382.

[16] LEE E, LEE H S, PARK C M. Efficient and generalized pairing computation on abelian varieties[J]. IEEE Transactions on Information Theory, 2009, 55(4): 1793–1803.

[17] VERCAUTEREN F. Optimal pairings[J]. IEEE Transactions on Information Theory, 2010, 56(1): 455–461.

[18] ZHAO C A, ZHANG F G. Research and development on efficient pairing computations[J]. Journal of Software, 2009, 20(11): 3001–3009.
赵昌安, 张方国. 双线性对有效计算研究进展[J]. 软件学报, 2009, 20(11): 3001–3009.

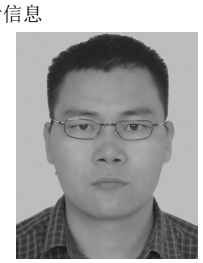
[19] DEVEGILI A J, SCOTT M, DAHAB R. Implementing cryptographic pairings over Barreto-Naehrig curves[C]. In: Pairing-Based Cryptography—Pairing 2007. Springer Berlin Heidelberg, 2007: 197–207.

[20] GRABHER P, GROßSCHÄDL J, PAGE D. On software parallel implementation of cryptographic pairings[C]. In: Selected Areas in Cryptography. Springer Berlin Heidelberg, 2008: 35–50.
[21] HANKERSON D, MENEZES A, SCOTT M. Identity-Based Cryptography[M]. IOS press, 2009: 188–206.
[22] NAEHRIG M, NIEDERHAGEN R, SCHWABE P. New software speed records for cryptographic pairings[C]. In: Progress in Cryptology—LATINCRYPT 2010. Springer Berlin Heidelberg, 2010: 109–123.
[23] BEUCHAT J L, GONZÁLEZ-DÍAZ J E, MITSUNARI S, et al. High-speed software implementation of the optimal ate pairing over Barreto–Naehrig curves[C]. In: Pairing-Based Cryptography-Pairing 2010. Springer Berlin Heidelberg, 2010: 21–39.
[24] ARANHA D F, KARABINA K, LONGA P, et al. Faster explicit formulas for computing pairings over ordinary curves[C]. In: Advances in Cryptology—EUROCRYPT 2011. Springer Berlin Heidelberg, 2011: 48–68.
[25] DIFFIE W, HELLMAN M E. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644–654
[26] SHAMIR A. Identity-based cryptosystems and signature schemes[C]. In: Advances in Cryptology—CRYPTO 1984. Springer Berlin Heidelberg, 1984: 47–53.
[27] MAURER U M, YACOBI Y. Non-interactive public-key cryptography[C]. In: Advances in Cryptology—EUROCRYPT 1991. Springer Berlin Heidelberg, 1991: 498–507.
[28] TANAKA H. A realization scheme for the identity-based cryptosystem[C]. In: Advances in Cryptology—CRYPTO 1987. Springer Berlin Heidelberg, 1987: 340–349.
[29] TSUJII S, ITOH T. An ID-based cryptosystem based on the discrete logarithm problem[J]. IEEE Journal on Selected Areas in Communications, 1989, 7(4): 467–473.
[30] WATERS B. Efficient identity-based encryption without random oracles[C]. In: Advances in Cryptology—EUROCRYPT 2005. Springer Berlin Heidelberg, 2005: 114–127.
[31] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]. In: Advances in Cryptology—EUROCRYPT 2005. Springer Berlin Heidelberg, 2005: 457–473.
[32] KATZ J, SAHAI A, WATERS B. Predicate encryption supporting disjunctions, polynomial equations, and inner products[C]. In: Advances in Cryptology—EUROCRYPT 2008. Springer Berlin Heidelberg, 2008: 146–162.
[33] BONEH D, HAMBURG M. Generalized identity based and broadcast encryption schemes[C]. In: Advances in Cryptology—ASIACRYPT 2008. Springer Berlin Heidelberg, 2008: 455–470.
[34] BONEH D, DI CRESCENZO G, OSTROVSKY R, et al. Public key encryption with keyword search[C]. In: Advances in Cryptology— Eurocrypt 2004. Springer Berlin Heidelberg, 2004: 506–522.
[35] ABDALLA M, BELLARE M, CATALANO D, et al. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions[J]. Journal of Cryptology, 2008, 21(3): 350–391.
[36] LEWKO A, OKAMOTO T, SAHAI A, et al. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption[C]. In: Advances in Cryptology—EUROCRYPT 2010. Springer Berlin Heidelberg, 2010: 62–91.
[37] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[C]. In: Advances in Cryptology—ASIACRYPT 2001. Springer Berlin Heidelberg, 2001: 514–532.
[38] ICART T. How to Hash into elliptic curves[C]. In: Advances in Cryptology—CRYPTO 2009. Springer Berlin Heidelberg, 2009: 303–316.
[39] ZHANG F, SAFAVI-NAINI R, SUSILO W. An efficient signature scheme from bilinear pairings and its applications[C]. In: Public Key Cryptography—PKC 2004. Springer Berlin Heidelberg, 2004: 277–290.
[40] BONEH D, BOYEN X. Short signatures without random oracles[C]. In: Advances in Cryptology—EUROCRYPT 2004. Springer Berlin Heidelberg, 2004: 56–73.
[41] ZHANG F, CHEN X, SUSILO W, et al. A new signature scheme without random oracles from bilinear pairings[C]. In: Progress in Cryptology—VIETCRYPT 2006. Springer Berlin Heidelberg, 2006: 67–80.
[42] ZHANG F. The computational square-root exponent problem-revisited[J]. IACR Cryptology ePrint Archive, 2011, 2011: 263.
[43] ROH D, HAHN S G. The square root Diffie–Hellman problem[J]. Designs, Codes and Cryptography, 2012, 62(2): 179–187.
[44] CAMENISCH J, LYSYANSKAYA A. Signature schemes and anonymous credentials from bilinear maps[C]. In: Advances in Cryptology—CRYPTO 2004. Springer Berlin Heidelberg, 2004: 56–72.
[45] OKAMOTO T. Efficient blind and partially blind signatures without random oracles[C]. In: Theory of Cryptography. Springer Berlin Heidelberg, 2006: 80–99.
[46] JOUX A. A new index calculus algorithm with complexity L(1/4+o(1)) in small characteristic[C]. In: Selected Areas in Cryptography—SAC 2013. Springer Berlin Heidelberg, 2013: 355–379.
[47] JOUX A, PIERROT C. Technical history of discrete logarithms in small characteristic finite fields[J]. Designs, Codes and Cryptography, 2016, 78(1): 73–85.
[48] BONEH D, SILVERBERG A. Applications of multilinear forms to cryptography[J]. Contemporary Mathematics, 2003, 324(1): 71–90.

[49] GENTRY C, SAHAI A, WATERS B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based[C]. In: Advances in Cryptology—CRYPTO 2013. Springer Berlin Heidelberg, 2013: 75–92.
[50] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM, 2009, 56(6): 34.
[51] AJTAI M. Generating hard instances of lattice problems[C]. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing. ACM, 1996: 99–108.
[52] LANGLOIS A, STEHLé D, STEINFELD R. GGHLite: More efficient multilinear maps from ideal lattices[C]. In: Advances in Cryptology —EUROCRYPT 2014. Springer Berlin Heidelberg, 2014: 239–256.
[53] ALBRECHT M R, COCIS C, LAGUILLAUMIE F, et al. Implementing candidate graded encoding schemes from ideal lattices[C]. In: Advances in Cryptology—ASIACRYPT 2015. Springer Berlin Heidelberg, 2014: 752–775.
[54] HOFFSTEIN J, PIPHER J, SILVERMAN J H. NTRU: A ring-based public key cryptosystem[C]. In: Algorithmic Number Theory. Springer Berlin Heidelberg, 1998: 267–288.
[55] WANG X Y, LIU M J. Survey of lattice-based cryptography[J]. Journal of Cryptologic Research, 2014, 1(1): 13–27.
王小云, 刘明洁. 格密码学研究[J]. 密码学报, 2014, 1(1): 13–27.
[56] Lee H T, Seo J H. Security analysis of multilinear maps over the integers[C]. In: Advances in Cryptology—CRYPTO 2014. Springer Berlin Heidelberg, 2014: 224–240.
[57] CHEN Y, NGUYEN P Q. Faster algorithms for approximate common divisors: Breaking fully-homomorphic-encryption challenges over the integers[C]. In: Advances in Cryptology—EUROCRYPT 2012. Springer Berlin Heidelberg, 2012: 502–519.
[58] CHEON J H, HAN K, LEE C, et al. Cryptanalysis of the multilinear map over the integers[C]. In: Advances in Cryptology—EUROCRYPT 2015. Springer Berlin Heidelberg, 2015: 3–12.
[59] GENTRY C, HALEVI S, MAJI H K, et al. Zeroizing without zeroes: Cryptanalyzing multilinear maps without encodings of zero[J]. IACR Cryptology ePrint Archive, 2014, 2014: 929.
[60] BONEH D, WU D J, ZIMMERMAN J. Immunizing multilinear maps against zeroizing attacks[J]. IACR Cryptology ePrint Archive, 2014, 2014: 930.
[61] GARG S, GENTRY C, HALEVI S, et al. Fully secure functional encryption without obfuscation[J]. IACR Cryptology ePrint Archive, 2014, 2014: 666.
[62] CORON J S, LEPOINT T, TIBOUCHI M. Cryptanalysis of two candidate fixes of multilinear maps over the integers[J]. IACR Cryptology ePrint Archive, 2014, 2014: 975.
[63] CORON J S, LEPOINT T, TIBOUCHI M. New multilinear maps over the integers[C]. In: Advances in Cryptology—CRYPTO 2015. Springer Berlin Heidelberg, 2015: 267–286.
[64] CHEON J H, FOUQUE P, LEE C, et al. Cryptanalysis of the new CLT multilinear maps over the integers[C]. Accepted by EUROCRYPT 2016. Cryptology ePrint Archive, Report 2015/934+941, 2015.
[65] HU Y P, JIA H. Cryptanalysis of GGH map[J]. IACR Cryptology ePrint Archive, 2015, 2015: 301.
[66] GU C. Multilinear maps using ideal lattices without encodings of zero[R]. Cryptology ePrint Archive, Report 2015/023, 2015.
[67] CHEON J H, JEONG J, LEE C. An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without an encoding of zero[R]. Cryptology ePrint Archive, Report 2016/139, 2016.
[68] MILES E, SAHAI A, ZHANDRY M. Annihilation attacks for multilinear maps: Cryptanalysis of indistinguishability obfuscation over GGH13[R]. Cryptology ePrint Archive, Report 2016/147, 2016.
[69] CORON J S. Cryptanalysis of GGH15 multilinear maps[R]. Cryptology ePrint Archive, Report 2015/1037, 2015.
[70] GU C. Variation of GGH15 multilinear maps[R]. Cryptology ePrint Archive, Report 2015/1245, 2015
[71] CHEON J H, LEE D H. A note on self-bilinear maps[J]. Korean Mathematical Society, 2009, 46(2): 303–309.
[72] YAMAKAWA T, YAMADA S, HANAOKA G, et al. Self-bilinear map on unknown order groups from indistinguishability obfuscation and its applications[C]. In: Advances in Cryptology—CRYPTO 2014. Springer Berlin Heidelberg, 2014: 90–107.
[73] ZHANG H, ZHANG F, WEI B, et al. Self-bilinear map from one way encoding system and indistinguishability obfuscation[R]. Cryptology ePrint Archive, Report 2015/747, 2015.
[74] ALBRECHT M R, FARSHIM P, HOFHEINZ D, et al. Multilinear maps from obfuscation[C]. In: Theory of Cryptography. Springer Berlin Heidelberg, 2016: 446–473.
[75] BONEH D, WATERS B. Constrained pseudorandom functions and their applications[C]. In: Advances in Cryptology—ASIACRYPT 2013. Springer Berlin Heidelberg, 2013: 280–300.
[76] GARG S, GENTRY C, HALEVI S, et al. Attribute-based encryption for circuits from multilinear maps[C]. In: Advances in Cryptology—CRYPTO 2013. Springer Berlin Heidelberg, 2013: 479–499.
[77] HAN Y L, LU W Y, YANG X Y. Attribute-based signcryption for circuits from multi-linear maps[J]. Journal of Sichuan University: Engineering Science Edition, 2013, 45(6): 27–32.
韩益亮, 卢万谊, 杨晓元. 支持电路结构的多线性映射属性签密方案[J]. 四川大学学报: 工程科学版, 2013, 45(6): 27–32.
[78] GARG S, GENTRY C, SAHAI A, et al. Witness encryption and its applications[C]. In: Proceedings of the 45th Annual ACM Symposium on Theory of Computing. ACM, 2013: 467–476.

[79] HOHENBERGER S, SAHAI A, WATERS B. Full domain hash from (leveled) multilinear maps and identity-based aggregate signatures[C]. In: Advances in Cryptology—CRYPTO 2013. Springer Berlin Heidelberg, 2013: 494–512.
[80] BARAK B, GOLDREICH O, IMPAGLIAZZO R, et al. On the (im) possibility of obfuscating programs[C]. In: Advances in cryptology—CRYPTO 2001. Springer Berlin Heidelberg, 2001: 1–18.
[81] CHENG R, ZHANG F G. An overview on the secure program obfuscation[J]. Netinfo Security, 2014, (8): 6–16.
成荣, 张方国. 安全的程序混淆研究综述[J]. 信息网络安全, 2014, (8): 6–16.
[82] GOLDWASSER S, ROTHBLUM G N. On best-possible obfuscation[C]. In: Theory of Cryptography. Springer Berlin Heidelberg, 2007: 194–213.
[83] GARG S, GENTRY C, HALEVI S, et al. Candidate indistinguishability obfuscation and functional encryption for all circuits[C]. In: 2013 IEEE 54th Annual Symposium on Foundations of Computer Science (FOCS). IEEE, 2013: 40–49.
[84] PANETH O, SAHAI A. On the equivalence of obfuscation and multilinear maps[R]. Cryptology ePrint Archive, Report 2015/791, 2015.
[85] ANANTH P, GUPTA D, ISHAI Y, et al. Optimizing obfuscation: avoiding barrington's theorem[C]. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014: 646–658.
[86] APPLEBAUM B, BRAKERSKI Z. Obfuscating circuits via composite-order graded encoding[C]. In: Theory of Cryptography. Springer Berlin Heidelberg, 2015: 528–556.
[87] BARAK B, GARG S, KALAI Y T, et al. Protecting obfuscation against algebraic attacks[C]. In: Advances in Cryptology—EUROCRYPT 2014. Springer Berlin Heidelberg, 2014: 221–238.
[88] BRAKERSKI Z, ROTHBLUM G N. Black-box obfuscation for d-CNFs[C]. In: Proceedings of the 5th Conference on Innovations in Theoretical Computer Science. ACM, 2014: 235–250.
[89] BRAKERSKI Z, ROTHBLUM G N. Virtual black-box obfuscation for all circuits via generic graded encoding[C]. In: Theory of Cryptography. Springer Berlin Heidelberg, 2014: 1–25.
[90] PASS R, SETH K, TELANG S. Indistinguishability obfuscation from semantically-secure multilinear encodings[C]. In: Advances in Cryptology—CRYPTO 2014. Springer Berlin Heidelberg, 2014: 500–517.
[91] ZIMMERMAN J. How to obfuscate programs directly[C]. In: Advances in Cryptology—EUROCRYPT 2015. Springer Berlin Heidelberg, 2015: 439–467.
[92] APON D, HUANG Y, KATZ J, et al. Implementing cryptographic program obfuscation[J]. IACR Cryptology ePrint Archive, 2014, 2014: 779.
[93] HORVÁTH M. Survey on cryptographic obfuscation[J]. IACR Cryptology ePrint Archive, 2015, 2015: 412.
[94] SAHAI A, WATERS B. How to use indistinguishability obfuscation: deniable encryption, and more[C]. In: Proceedings of the 46th Annual ACM Symposium on Theory of Computing. ACM, 2014: 475–484.
[95] HOHENBERGER S, SAHAI A, WATERS B. Replacing a random oracle: Full domain hash from indistinguishability obfuscation[C]. In: Advances in Cryptology—EUROCRYPT 2014. Springer Berlin Heidelberg, 2014: 201–220.
[96] CANETTI R, GOLDWASSER S, POBURINNAYA O. Adaptively secure two-party computation from indistinguishability obfuscation[C]. In: Theory of Cryptography. Springer Berlin Heidelberg, 2015: 557–585.
[97] GARG S, GENTRY C, HALEVI S, et al. Two-round secure MPC from indistinguishability obfuscation[C]. In: Theory of Cryptography. Springer Berlin Heidelberg, 2014: 74–94.
[98] BONEH D, ZHANDRY M. Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation[C]. In: Advances in Cryptology—CRYPTO 2014. Springer Berlin Heidelberg, 2014: 480–499.
[99] RAMCHEN K, WATERS B. Fully secure and fast signing from obfuscation[C]. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014: 659–673.
[100] CHENG R, YAN J, GUAN C, et al. Verifiable searchable symmetric encryption from indistinguishability obfuscation[C]. In: Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. ACM, 2015: 621–626.
[101] BONEH D, GUPTA D, MIRONOV I, et al. Hosting services on an untrusted cloud[C]. In: Advances in Cryptology—EUROCRYPT 2015. Springer Berlin Heidelberg, 2015: 404–436.

作者信息



张方国(1972–), 山东淄博人, 博士, 中山大学数据科学与计算机学院教授, 博士生导师, 中国密码学会常务理事. 主要研究领域为密码学理论及其应用, 特别是椭圆曲线密码体制、安全多方计算、可证明安全性等.
E-mail: isszhfg@mail.sysu.edu.cn