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。实现网络安全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，更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。

模糊提取器及其应用

刘胜利 [1,2]，温云华 [1]
（1 上海交通大学计算机科学与工程系，上海 200240
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] 本文介绍模糊提取器的定义和应用及局限性。模糊提取器的局限性在于：只能对有熵的信息源进行一次提取，以及公开信息受到篡改后会导致生成错误的密钥。因此，本文引入了可重用鲁棒性模糊提取器，并给出了定义、构造，指出了其潜在的应用场景。

[关键词] 模糊提取器；可重用性；鲁棒性
[中图分类号] TP309.7　　[文献标识码] A　　[文章编号] 1009−8054(2019)02−0054−10

0 引言

分布均匀的随机变量在密码领域广泛应用。例如，密码系统中最重要的元素是密钥，而密码系统的安全性取决于密钥的均匀随机性。此外，对于公钥加密或者数字签名方案，加密算法或者签名算法还需要随机数的参与，以保证加密算法的 CPA 安全或者不可伪造性。一个重要的问题是：如何产生分布均匀的随机比特?

我们将产生具有一定熵的随机比特的源称为“随机源”(Randomness Source)。如果“随机源”所产生的字符串不但在密钥空间中“均匀分布”，还可以“精确再生”。那么，“随机源”就可以用于产生密码算法的加密密钥和解密密钥。然而，在现实生活中，这样均匀随机且精确再生的随机源几乎没有。现实中确实有很多带有噪音的随机源，有很高的（最小）熵，但不是均匀随机的，而且每次的采样结果虽然相近，但都有一些小的偏差（噪音）。例如：

- 人的生物信息，如指纹、声纹、虹膜等；
- 电子元器件的噪声（不可克隆函数）；
- 量子信息。

我们能否将这些有噪随机源通过密码技术转变为好的随机源，使其产生“均匀分布”且“精确再生”的随机比特？如果可以，那么这些随机源就可以为我们所用，并为密码系统提供源源不断的、可重现的随机数。

1 模糊提取器

近二十年来，许多密码学者致力于这项研究：如何利用密码技术使有噪随机源来产生均匀随机且可以精确再生的字符串。

1.1 模糊提取器的定义

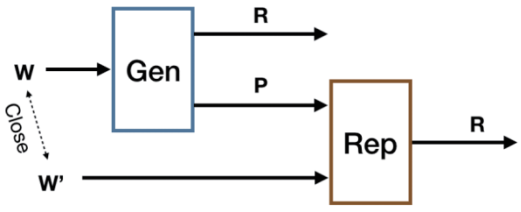
2004 年，Dodis 等人提出了模糊提取器（fuzzy extractor）的概念，旨在解决这一问题。模糊提取器 FE=(Gen,Rep) 有两个算法，生成算法和再生算法。提取器具体描述如下，请参见图 1。

- Gen → (P,R). 生成算法 Gen 输入字符串 w（噪音随机源的一次采样），输出一个字符串 R 和一个公开的帮助串 P；
- Rep(w',P) → R'. 再生算法输入 w'（噪音随机源的另一次采样）和公开帮助串 P，输出一个字符串 R'。

正确性：正确性要求是如果两次采样 w 和 w' 的距离足够近，那么 R'=R，即 R 可以精确再生；

安全性：安全性要求是如果随机源有足够多的熵，那么 R 是均匀随机的。

图 1：模糊提取器



Dodis 等人所提出模糊提取器构造依赖两个构件，即（普通的，不是模糊的）提取器（extractor）和安全梗概（secure sketch）。提取器 [13] 可以将不均匀的字符串转化成均匀的字符串，可以使用 universal function 来实现；而安全梗概（secure sketch）致力于纠错，因此可以用线性纠错码来实现。

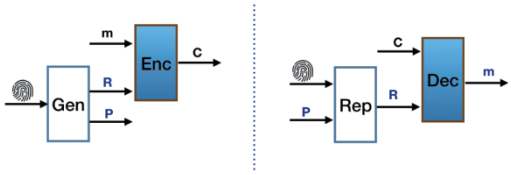
1.2 模糊提取器的应用

使用模糊提取器，就可以将有噪音的随机源转化成均匀随机且精确再生的字符串。模糊提取器可以应用在密码系统中。

1.2.1 对称密钥生成

利用模糊提取器，用户可以将自己的生物信息（即有噪随机源）做为输入，调用生成算法 Gen(w) → (P,R)，就可以提取出一个随机字符串 R 和一个公开帮助串 P。这个随机的字符串 R 即可用做密码系统的密钥，进行参与密码系统，公开帮助串 P 存储下来，无需保密。密码系统运行完毕后，密钥 R 随即销毁。当密码系统再次需要密钥进行密码操作时，用户将自己的生物信息（即有噪随机源）和公开帮助串 P 做为输入，调用再生算法 Rep(w',P) → R'，可以重现密钥 R。可见，用户不需要存储密钥，每次需要密钥时，只需录入自己的生物信息，模糊提取器就可以把密钥安全可靠的恢复出，解决了密钥生成和存储的问题。之后，密钥 R 应用于对称密码算法中，可以使用 Enc(R,m) 对明文 m 进行加密得到密文 c，使用 Dec(R,c) 对密文 c 进行解密并恢复明文 m。具体如图 2 所示。

图 2：利用模糊提取器生成对称密钥进行加解密



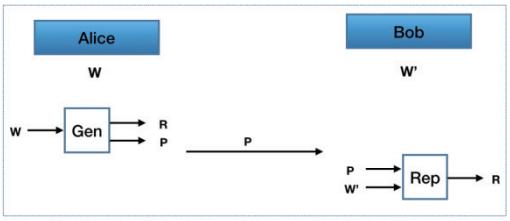
1.2.2 密钥协商 (Key agreement from close secret)

利用模糊提取器技术还可以进行两方密钥协商。设 Alice 有一个秘密信息 w, Bob 有一个秘密信息 w'。其中 w 和 w' 的距离是相近的。例如

- Alice 和 Bob 在进行量子密钥分发；
- Alice 和 Bob 在同时收听一个有噪音的电台；
- Alice 知道 Bob 的虹膜信息。

Alice 可以用模糊提取器作用在 w 上获得安全密钥 R 和一个公开帮助字符串 P，将 P 发送给 Bob，Bob 调用模糊提取器再生算法 Rep(w',P) → R，可以重现密钥 R。由此，Alice 和 Bob 完成密钥协商。见图 3。

图 3：利用模糊提取器进行密钥协商



1.2.3 在公钥密码系统中的应用

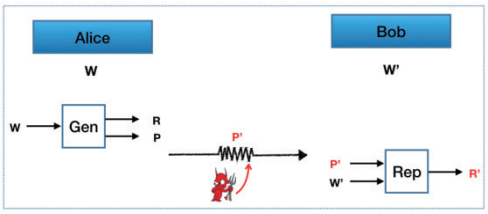
公钥密码一般会依赖于困难假设。而困难假设一般要求均匀随机的字符串。例如 ElGamal 加密方案，依赖于与离散对数困难问题相关的“判定性 Diffie–Hellman”假设。离散对数问题描述如下：给定一个群$\mathcal{G}$，$\mathcal{G}$的大小为 p， p 是一个大素数，g 是群$\mathcal{G}$的生成元，对于一个均匀随机选取的 $x \leftarrow \mathbb{Z}_p$， 令 $y=g^x$。给定 y,g，计算 y 的离散对数 $x=\log_g y$ 即为离散对数问题。对于 $z=g^{x'}$，如果 x' 不是均匀分布，求解 z 的离散对数问题则可能不再困难。

通过模糊提取器，用户可以从有噪音的随机源中提取一个均匀随机的 x 作为 ElGamal 加密方案的私钥，$y=g^x$ 作为 ElGamal 加密方案的公钥。

1.3 鲁棒性模糊提取器

模糊提取器的安全性只考虑了被动攻击。即，公开帮助串 P 可以让敌手知道，但是 P 不能被敌手篡改。如果敌手篡改 P，那么模糊提取器的恢复算法 Rep 就很有可能得到一个错误的输出 R'。但是在现实生活中，主动攻击的敌手可能会篡改 P。例如在密钥协商过程中，一个主动攻击的敌手可以将 P 截取，然后将一个错误的 P' 送给 Bob（见图 4）。那么 Bob 调用模糊提取器的恢复算法 Rep 就很有可能得到一个错误的输出 R'。如果 $R \neq R'$，密钥协商失败。

图 4：主动攻击的敌手



为了解决上述问题，Boyen 等 [4] 在 2005 年提出了鲁棒性模糊提取器 (robust fuzzy extractor) 的概念。模糊提取器的鲁棒性有两种安全性定义，即“应用前”鲁棒性和“应用后”鲁棒性。应用前的鲁棒性保证敌手在只看到公开帮助字符串 P 的情况下，提交一个篡改的 $\widetilde{p}$，模糊提取器的恢复算法只能输出 $\perp$，不能再产生出一个错误的 $\widetilde{R}$。然而在实际应用中，如果用户在某些密码方案中使用 R，那么 R 的部分信息甚至是所有的信息会泄露给敌手。在这种情况下，“应用前”鲁棒性不再适用。“应用后”鲁棒性可以解决这一问题。应用后鲁棒性保证了敌手在看到 P 和 R 的情况下，提交一个篡改的 $\widetilde{p}$，模糊提取器的恢复算法只能输出 $\perp$。

Boyen 等在 [4] 提出了一种将模糊提取器转化成“应用前”鲁棒模糊提取器的通用方法，方法是使用 Hash 函数。但是其安全性证明中将 Hash 函数当做为随机预言机，故安全性建立在 Random Oracle 模型之上。

2006 年，Dodis 等在 [7] 首次在标准模型下构造了“应用后”鲁棒模糊提取器。在他们的构造中，输入一个长度为 n，最小熵为 m 的比特串 w，提取器可以提取长度为 l=(2m−n)/3 的均匀分布的比特串。可见，所提取出的随机串不超过最小熵为 m 的 1/3。

2008 年，Kanukurthi 和 Reyzin\cite{Kanukurthi2008} 构造了“应用后”鲁棒模糊提取器，所提取出的随机串的长度更长：l=(2m−n)/2 比特。

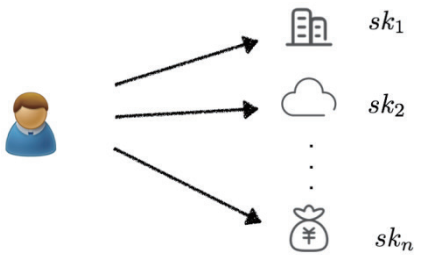
2009 年，Dodis 等在 [9] 证明在平凡模型下，如果输入 w 的熵率 (m/n) 小于一半，那么模糊提取器的鲁棒性是不可能实现的。为了解决这一问题，Cramer 等 [6] 在 2008 年提出了一个新的密码学原语—“代数操作检测码”（algebraic manipulation detection，简称为 AMD）。同时，在共同参考字符串（Common Reference String，简称为 CRS）模型下，利用 AMD 码构造了一个（“应用后”）鲁棒的模糊提取器。CRS 模型指 Common Reference String 固化在硬件中，任何人都不能对 CRS 进行篡改。他们所提出的提取器打破了在平凡模型下随机源熵率需要大于其长度的一半的界线。尽管如此，该提取器的熵损还是巨大的。

1.4 可重复提取的模糊提取器

利用模糊提取器，用户可以从自己的生物信息中提取安全的密钥进行加解密，且不需要保存密钥。在享受了上述便利之后，用户可能会希望可以从自己的生物信息中提取多个安全可靠的密钥应用在不同的机构，不同的场景下。然而

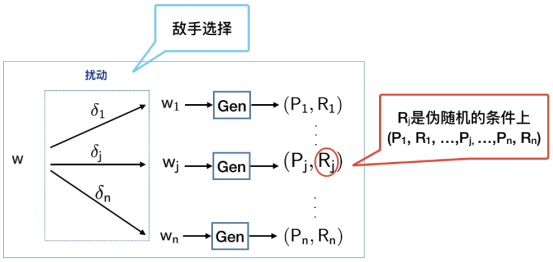
- 人的生物信息是唯一的，不能被更改或者创造；
- 模糊提取器保证了从一个噪音随机源中提取一次密钥的安全性。而从相同的随机源中提取多个不同的密钥的安全性是无法保证的。

图 5：从相同的随机源中提取多个不同的安全密钥



为了解决上述问题，Boyen[3] 在 2004 年提出了可重用模糊提取器 (Reusable Fuzzy Extractor) 的概念。可重用模糊提取器 (Reusable Fuzzy Extractor) 允许模糊提取器的产生算法 $Gen(w) \rightarrow (P,R)$ 对随机源 W 的多个有噪版本进行多次提取 Gen。假设 $w,w_1,\cdots,w_\rho$ 是随机源 W 的多次读取的结果，则它们之间统计相关。调用 $(P,R) \leftarrow Gen(w),(P_i,R_i) \leftarrow Gen(w_i)$ 可以得到多组输出 $(P,R)\ \{P_i,R_i\}\_(i \in \{1,2,\cdots,\rho\})$。设 $[\rho]:=\{1,2,\cdots,\rho\}$，模糊提取器的可重用要求是：给定 $\{P\_i,R\_i\}_{i \in [\rho]}$ 和 P 的条件下，R 仍然具有伪随机特性。

图 6：可重用模糊提取器安全性定义



在 [3] 中，Boyen 提出了两个可重用模糊提取器的构造方案，并定义了“外向安全性”(outsider security) 和“内向安全性”(insider security)。外向安全性的定义如下：敌手动态地选择 δ_i，并得到 P_i，其中 $(P_i,R_i) \leftarrow Gen(w+\delta_i)$。最终的 $(P,R)\ \{P_i,R_i\}_{i \in \{1,2,\cdots,\rho\}}$ 中的 R 对敌手来说应该是伪随机的。内向安全性的定义如下：敌手不但得到了 $\{P_i\}_{i \in [\rho]}$ 也看到了 $\widetilde{R}_i \leftarrow Rep(\widetilde{p}_i, w+\widetilde{\delta}_i)$，其中 $\widetilde{p}_i$ 和 $\widetilde{\delta}_i$ 由敌手选择，R 要求对敌手仍是伪随机。可见内向安全性比外向安全性要强，但是实现起来也更加困难。在 [3] 中，实现内向安全性可重用模糊提取器是建立在“随机预言机”模型上的。而且窜扰量 δ_i 必须与 w 独立。

2017 年，Apon 等 [2] 对 Fuller 等人所提出的方案 [10] 进行升级，得到了一个弱的可重用模糊提取器，其弱安全性依赖 LWE 假设。其安全模型类似于 [3] 中的“外向安全”，但是只要求敌手提交的偏移量 δ_i 满足 $dis(\delta_i) \leqslant t$。但是如 [10] 中的方案，Apon 等人的可重用模糊提取器可以容忍的错误只是对数级的。2018 年，我们提出了一个基于 LWE 假设的可重用模糊提取器，方案可以容忍线性级的错误 [14]。

2016 年，Canetti 等 [5] 提出了一种可重用模糊提取器的通用构造方案，通用构造中所使用

的一个重要的模块是“digital locker”。其安全模型中对 $w,w_1,\cdots,w_\rho$ 的相关性没有任何限制。因此，安全模型也是目前最强的一种模型。然而目前“digital locker”的实现却只有两种：一种使用 Hash 函数构造 digital locker，而 digital locker 安全性依赖于“随机预言机”；另一种实现是基于非标准的 DDH 变种假设。此外，他们的方案只能容忍 sub-linear 级错误且对噪音随机源的分布有结构上的要求。

之后，使用 Canetti 等 [5] 所提出的“digital locker”这一技术工具，Alamelou 等 [1] 构造出一种可重用模糊提取器，既适用于汉明距离，也可以用于集合间的距离。他们的方案容忍错误的能力提高到了线性级。但是，它们需要将随机源细分为多个块，每块所在的字符集足够大，且拥有足够多的熵。

2018 年，我们 [16] 基于标准的 DDH 困难假设，提出了一个可重用模糊提取器的具体方案。方案的特点是：基于标准模型标准假设，且可以容忍线性级的错误。但是要求对同一个随机源 W 的任意两次读取结果 w_i 和 w_j 来讲，其差 w_i-w_j 不泄漏关于信息源 W 太多的信息量。

根据对同一个随机源 W 的多次读取结果 $w_1,\cdots,w_n$ 之间的统计相关性，可重用模糊提取器方面的发展主要有三条方向：(1) w_i 间可以任意相关，但是安全性只能依赖于“随机预言机”或者不标准假设；(2) 同一个随机源 W 的任意两次读取结果 w_i 和 w_j 来讲，其差 w_i-w_j 不泄漏关于信息源 W 太多的信息量；(3) 任意两次读取结果 w_i 和 w_j 的差 δ_i $(=w_i-w)$ 由敌手控制。图 7 对此进行了总结。表 1 对各种方案具体的性能进行了总结。

图 7：可重用模糊提取器及鲁棒性模糊提取器。代表条件下的的平均熵

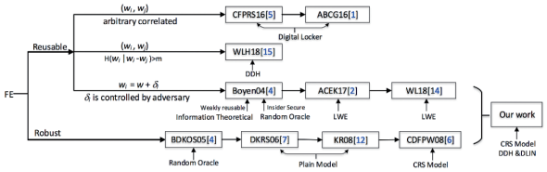


表 1：相关方案比较。“Robustness？”指方案是否有鲁棒性；“Reusability？”指方案是否有重用性；“Standard Assumption？”指方案是否基于标准假设；“Linear Errors？”指方案是否要容忍线性错误；“–”指方案是信息论意义下的方案

FE Sechemes	Robustness?	Reusability?	Standard Assumption?	Linear Errors?
FMR12 [10]	×	×	√	×
DRS04 [8],Boy04 [3]	×	weak		√
CFPRS16 [5]	×	√	×	×
Boy04 [3] ABCG16 [1]	×	√	×	√
ACEK17 [2]	×	√	√	×
BDKOS05 [4]	√	×	×	√
DKRS06 [7], KR08 [12], CDFPW08 [6]	√	×		√
WL18 [14, WLH18 [16]	×	√	√	√
Ours	√	√	√	√

2018 年之前，尚没有研究学者在标准模型下提出模糊提取器的构造，使之既满足鲁棒性又满足可重复使用性，而我们首次实现了两者兼备的模糊提取器，研究结果发表在 2018 亚密会上。

2 我们的成果：可重用鲁棒模糊提取器

2018 年，我们定义了可重用鲁棒模糊提取器，并给出了一种通用构造方法。简单的说可重用鲁棒模糊提取器既满足可重用性又满足鲁棒性。

我们通用构造方法所使用的模块如下：

● 对称性密钥封装机制 (Symmetric Key Encapsulation Mechanism，简称为 SKEM)，其安全性要求为 Key-Shift (KS) 安全性；

● 具有同态性的安全梗概 (Secure Sketch，简称为 SS)；

● 具有同态性的提取器 (Extractor，简称为 Ext)；

● 具有同态性的有损代数滤波器 (Lossy Algebraic Filter，简称为 LAF)。

我们基于 DDH 问题构造了 Key-Shift (KS) 安全的 SKEM；使用线性纠错码技术可以构造具有同态性的 SS；使用 universal hash 可以构造具有同态性的 Ext；基于 DLIN 问题可以构造具有同态性的有损代数滤波器 [11]。通过这样的具体构造，我们得到了第一个即具有重用性也具有鲁棒性的模糊提取器（可重用鲁棒模糊提取器）构造方案，具有以下的性质：

● 方案中有 CRS，故建立在 CRS 模型上；

● 鲁棒性为“应用后”鲁棒性；

● 方案可以容忍线性级错误；

● 重用性和鲁棒性可以在标准模型下基于 DDH 和 DLIN 假设来证明；

● 安全模型中，敌手可以控制偏移量 δ_i 满足 $dis(\delta\_i) \leqslant dt$。

我们的工作发表在 AsiaCrypt2018 上（eprint 版见 [15]），与之前的相关工作的比较列在图 7 和表 1。

2.1 我们的具体方案

可重用鲁棒模糊提取器 rrFE=(rrFE.Init,rrFE.Gen,rrFE.Rep) 的构造如图 8 和图 9，组件的要求如下：

● 对称性密钥封装机制 (Symmetric Key Encapsulation Mechanism，简称为 SKEM) SKem=(SKem.Init,SKem.Enc,SKem.Dec)，其密钥空间为 $\delta\ \kappa$，所封装的密钥空间为 κ。

● 具有同态性的$\left(m-\lceil \log p \rceil, \hat{m}, 2t\right)$-安全梗概 (Secure Sketch，简称为 SS)SS=(SS.Gen,SS.Rec)，测量空间为 $\mathcal{M}$，且$\hat{m}-\lceil \log p \rceil \geq \omega(\log \lambda)$。

● 具有同态性的 (M, $\hat{m}$,SK, ε _ext 提取器 (Extractor，简称为 Ext)。

● 具有同态性的 (l_{LAF},n) 有损代数滤波器 (Lossy Algebraic Filter，简称为 LAF)LAF=(FGen,FEval,FTag)，其定义域为$\mathbb{Z}_p^n$且 $l_{LAF}=\lceil \log p \rceil$，标签空间为 {0,1}* × τ '。

图 8：可重用鲁棒模糊提取器的构造

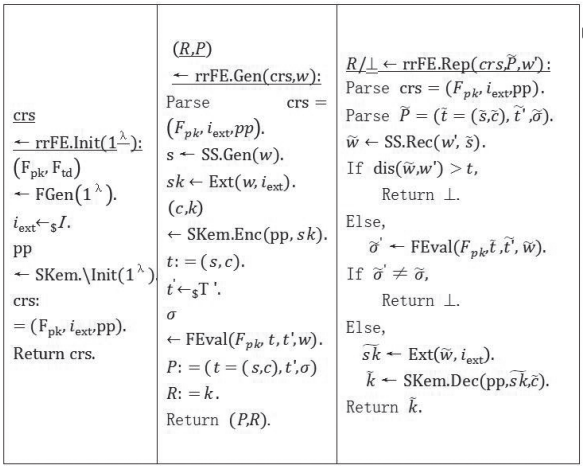
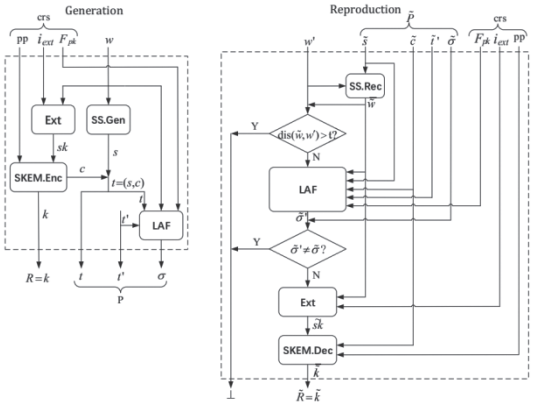


图 9：可重用鲁棒模糊提取器构造示意图



3 应用前景

利用可重用鲁棒模糊提取器 rrFE=(rrFE.Init,rrFE.Gen,rrFE.Rep)，用户可以将自己的生物信息 W 做为有噪随机源，例如指纹，用户可以通过指纹读取设备获得 $(w_1,\cdots,w_j,\cdots,w_n)$，然后调用生成算法生成 $(P_1,R_1),\cdots,(P_j,R_j),\cdots,(P_n,R_n)$，将 R_j 作为私钥应用在不同的场景中，例如门禁设备，银行系统和智能家居等。具体操作如下（参见图 9 及图 11）：

CRS 产生：使用 rrFE.Init 产生 crs，固化在硬件中；

密钥产生：将生物信息 W 做为输入，调用生成算法 rrFE.Gen(CRS,W)，产生密钥 R 和一个公开帮助串 P；

使用密钥并销毁：密钥 R 参与密码系统的算法运算，使用后销毁。但是公开帮助串 P 存储起来（不必保密）；

密钥恢复：再次使用密码系统时，以公开帮助串 P 和（有噪声）生物信息 W^' 为输入，调用恢复算法 rrFE.Rep(crs,P,W')。如果输出为⊥，则认为认证不通过；否则输出的 R' 即为所恢复的密钥。使用密钥 R' 后销毁。

由可重用鲁棒性模糊提取器的性质，我们有以下几点成立：

- 模糊提取器的正确性保证了，当用户需要 R_j 时，读取指纹信息，调用恢复算法即可恢复出 R_j；
- 模糊提取器的可重复使用性保证了每一个 $R_j,j \in [n]$ 都是伪随机的，而且即使某个 R_i 被泄漏了，$R_j,j \neq i$ 仍然是伪随机的；
- 模糊提取器的鲁棒性保证了，如果某个公开帮助字符串 P_j 被篡改了，那么模糊提取器会输出⊥告知 用户 P_j 已经被篡改。

图 10：可重用鲁棒性模糊提取器的应用

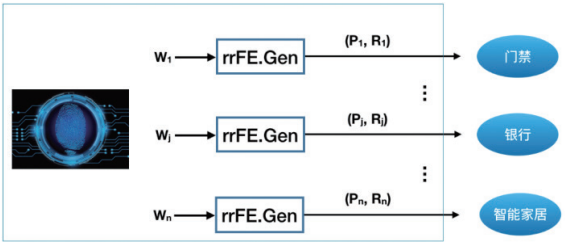
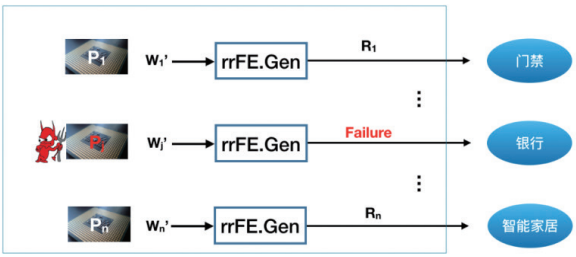


图 11：可重用鲁棒性模糊提取器的应用



现在仍然以密钥协商为例来说明可重用鲁棒模糊提取器的具体使用方法。利用可重用鲁棒模糊提取器，拥有相近的秘密信息的两个用户 Alice 和 Bob 可以进行“多次”密钥协商，参见图 12 和图 13。

CRS 产生：Alice 使用 rrFE.Init 产生 crs，固化在硬件中，同时将 crs 通过安全的信道发送给 Bob。

密钥产生：Alice 将她所拥有的秘密信息 W 做为输入，调用生成算法 rrFE.Gen(crs,W)，产生密钥 R 和一个公开帮助串 P；

密钥协商：Alice 将密钥一个公开帮助串 P 发送给 Bob，Bob 调用恢复算法 rrFE.Rep(crs,P,W')，如果 W 和 W' 足够接近，R 即可被正确的恢复出来。

图 12：可重用鲁棒性模糊提取器的应用

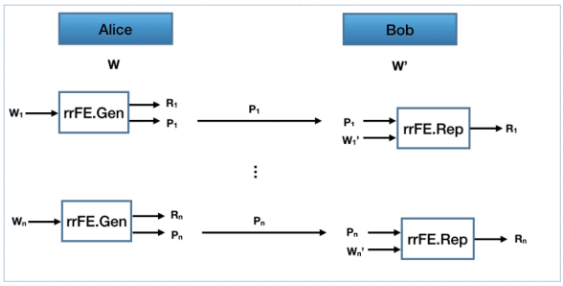
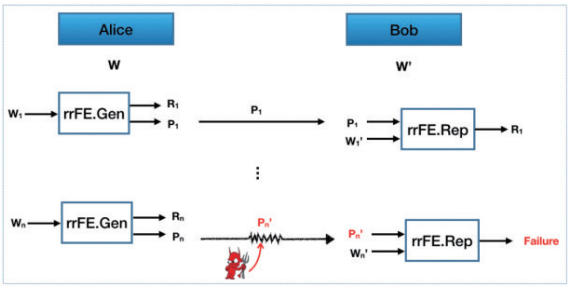


图 13：可重用鲁棒性模糊提取器的应用（敌人篡改公开信息）



由可重用鲁棒性模糊提取器的性质，我们有以下几点成立：

● 模糊提取器的正确性保证了，如果公开帮助字符串 P_j 没有被篡改，Alice 和 Bob 会得到相同的 R_j；

● 模糊提取器的可重复使用性保证了每一个 R_j,$j \in [n]$ 都是伪随机的，而且即使某个 R_i 被泄漏了，R_j,$j \neq i$ 仍然是伪随机的；

● 模糊提取器的鲁棒性保证了，如果某个公开帮助字符串 P_j 被篡改了，那么模糊提取器会输出⊥告知用户 P_j 已经被篡改，密钥协商失败，需要再一次协商。

参考文献

[1] Q. Alam é lou, P. Berthier, C. Cachet, S. Cauchie, B. Fuller, P. Gaborit, and S. Simhadri. Pseudoentropic isometries: A new framework for fuzzy extractor reusability. In J. Kim, G. Ahn, S. Kim, Y. Kim, J. L ó pez, and T. Kim, editors, AsiaCCS 2018, pages 673 – 684. ACM, 2018.

[2] D. Apon, C. Cho, K. Eldefrawy, and J. Katz. Efficient, reusable fuzzy extractors from LWE. In S. Dolev and S. Lodha, editors, CSCML 2017, volume 10332 of LNCS, pages 1 – 18. Springer,Heidelberg, 2017.

[3] X. Boyen. Reusable cryptographic fuzzy extractors. In V. Atluri, B. Pfitzmann, and P. D. McDaniel, editors, CCS 2004, pages 82 – 91. ACM, 2004.

[4] X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky, and A. D. Smith. Secure remote authentication using biometric data. In R. Cramer, editor, EUROCRYPT,volume 3494 of LNCS, pages 147 – 163. Springer, Heidelberg, 2005.

[5] R. Canetti, B. Fuller, O. Paneth, L. Reyzin, and A. D. Smith. Reusable fuzzy extractors for low–entropy distributions. In M. Fischlin and J. Coron, editors, EUROCRYPT 2016, volume 9665 of LNCS, pages 117 – 146. Springer,Heidelberg, 2016.

[6] R. Cramer, Y. Dodis, S. Fehr, C. Padr ó , and D. Wichs. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. In N. P. Smart, editor, EUROCRYPT 2008, volume 4965 of LNCS, pages 471 – 488. Springer, Heidelberg, 2008.

[7] Y. Dodis, J. Katz, L. Reyzin, and A. D. Smith. Robust fuzzy extractors and authenticated key agreement from close secrets. In C. Dwork, editor, CRYPTO 2006, volume 4117 of LNCS, pages 232 – 250. Springer, Heidelberg, 2006.

[8] Y. Dodis, L. Reyzin, and A. D. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In C. Cachin and J. Camenisch, editors, EUROCRYPT

2004, volume 3027 of LNCS, pages 523 – 540. Springer, Heidelberg, 2004.

[9] Y. Dodis and D. Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In M. Mitzenmacher, editor, STOC 2009, pages 601 – 610. ACM, 2009.

[10] B. Fuller, X. Meng, and L. Reyzin. Computational fuzzy extractors. In K. Sako and P. Sarkar, editors, ASIACRYPT 2013, volume 8269 of LNCS, pages 174 – 193. Springer, Heidelberg, 2013.

[11] D. Hofheinz. Circular chosen-ciphertext security with compact ciphertexts. In T. Johansson and P. Q. Nguyen, editors, EUROCRYPT 2013, volume 7881 of LNCS, pages 520 – 536. Springer, Heidelberg, 2013.

[12] B. Kanukurthi and L. Reyzin. An improved robust fuzzy extractor. In R. Ostrovsky, R. D. Prisco, and I. Visconti, editors, SCN 2008, volume 5229 of LNCS, pages 156 – 171. Springer, Heidelberg, 2008.

[13] V. Shoup. A computational introduction to number theory and algebra. Cambridge University Press, 2006.

[14] Y. Wen and S. Liu. Reusable fuzzy extractor from LWE. In W. Susilo and G. Yang, editors, ACISP 2018, volume 10946 of LNCS, pages 13 – 27. Springer, Heidelberg, 2018.

[15] Y. Wen and S. Liu. Robustly reusable fuzzy extractor from standard assumptions. Cryptology ePrint Archive, Report 2018/818, 2018. https://eprint.iacr.org/2018/818.

[16] Y. Wen, S. Liu, and S. Han. Reusable fuzzy extractor from the decisional diffie-hellman assumption. Designs Codes and Cryptography, 2018.

作者简介：

刘胜利，卫士通摩石实验室兼职专家，上海交通大学计算机科学与工程系教授、博士生导师，主要研究公钥密码理论与实践。

温云华，上海交通大学 2013 级博士生，主要研究是有噪提取器的可重用性和稳健性。

Fuzzy Extractor and its Application

LIU Sheng-li [1,2], WEN Yun-hua[1]

1Department of Computer Science and Engineering,Shanghai Jiao Tong University, Shanghai 200240, China

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

[Abstract] This paper introduced the definition of fuzzy extractor and its application and limitations. The limitations of Fuzzy Extractor are that it can be extracted only once from the information with entropy, and results in generating incorrect key when the public information has been tampered. Therefore, we put forward robustly reusable fuzzy extractor, and gives the definition, construction and figured out its potential application scenarios.

[Keywords] Fuzzy extractor; Reusability; Robustness