arXiv:2305.01083v3 [cs.IT] 4 Sep 2023

计算放宽局部可解码码，再探*

Alexander R. Block† 和 Jeremiah Blocki‡
†乔治城大学和马里兰大学帕克分校。电子邮箱：alexander.r.block@gmail.com
‡普渡大学。电子邮箱：jblocki@purdue.edu

摘要——我们重新审视计算放宽局部可解码码（crLDC）（Blocki 等人，Trans. Inf. Theory '21），并给出两种新的构造。我们的第一种构造是汉明 crLDC，其概念上比先前的构造更简单，利用了数字签名方案和适当选取的汉明码。第二种构造将汉明 crLDC 扩展到可处理插入删除（InsDel）错误，从而得到 InsDel crLDC。这一扩展关键依赖于 Block 等人（FSTTCS '20）的带噪二分搜索技术来处理插入删除错误。两种 crLDC 构造的码字字母表都是二进制的，分别能够抵抗常数比例的汉明错误和插入删除错误；在适当选择参数的情况下，它们具有多对数局部性，且编码长度关于消息长度呈线性、关于安全参数呈多项式。这些参数在多对数局部性范围内优于先前的构造。

I. 引言

局部可解码码（LDCs）是这样一类纠错码：通过仅查询接收字中的少数位置，即可超高效地（即在多对数时间内）恢复编码后的消息中的单个符号。对于字母表 Σ 和一个（归一化的）度量 dist，若一对算法 Enc: $\Sigma^k \to \Sigma^K$和 Dec : $[k] \to \Sigma$（对于 $[k] := \{1, \ldots, k\}$）是一个 (ℓ, ρ, p) -LDC，则 Dec 是一个随机化预言机算法，满足：对于任意消息 x 和任意接收字 y'，如果 $\text{dist}(\text{Enc}(x)\ y') \leqslant \rho$，那么对于每个 i，$\text{Dec}^{y'}(i)$至多向 y' 进行 ℓ 次查询，并以至少 p的概率输出 x_i 。其中， k 和 K 分别是消息 和 码长， k/K 是码率， ℓ 是局部性， ρ 是错误率，而 p 是 成功概率。

在最坏情况下的汉明错误背景下已得到广泛研究 [KT00, STV01, KdW04, Yek08,DGY11, Efr12, Yek12, KS16, KMRZS 17] 其中 dist 表示归一化汉明距离（HAM），汉明局部可解码码似乎在码率、错误率和局部性之间存在难以调和的权衡。对于常数错误率（大多数应用的目标），已知的最佳构造中，具有常数 $\ell \geqslant 3$ 局部性的码率为超多项式级 [Yek08, DGY11, Efr12], 对于 $\ell = 2$，已知 $K = \Theta(\exp(k))$ [KdW04], ；而已知的最佳构造中，具有常数码率的局部性为超对数级（次多项式级） [KMRZS17]。此外，已知的最佳】【。】【"】【

一般汉明局部可解码码（LDC）的下界：当错误率和局部性为常数时 $\ell \geqslant 3$ 为 $K = \Omega(k^{\frac{\ell+1}{\ell-1}})$ [Woo07],，而任意局部性为 $\ell = 3$ 线性汉明局部可解码码满足 $K = \Omega(k^2/\log(k))$[Woo12]。更多详情请参阅综述 [Yek12，KS16]。

为了解决这些显著的权衡问题，Ben-Sasson 等人[BGH+06] 引入了松弛局部可解码码（rLDCs）。松弛局部可解码码是指在 LDC 的基础上，进一步允许解码器输出一个符号 $\perp \notin \Sigma$，表示解码器不知道正确值，但需满足以下限制：解码器（a）不会"过于频繁"地输出 $\perp$ ；以及（b）当所查询的码字未被篡改时，绝不会输出 $\perp$。这种松弛使得 LDC 能够在（较小的）常数 $\varepsilon > 0$ 下实现恒定局部性和码长 $K = k^{1+\varepsilon}$。Blocki 等人进一步考虑了 rLDC 的一种松弛形式，称为计算松弛局部可解码码（ crLDCs ）[BGGZ21]：这类 rLDC 仅能抵御计算能力受限的对抗信道（即概率多项式时间（PPT）信道）。这种受到 Lipton 的工作 [Lip94],启发的松弛形式，使 crLDC 能够实现恒定码率、恒定错误率和多对数局部性。

近年来，编码理论的研究重点转向理解和构造能够抵御插入删除错误（InsDel errors）的码 [Lev66, KLM04, GW17, BGZ18, HSS18, HS18, CHL+19, CJLW19, GL19, HRS19, Hae19, LTX19, CGHL21, GL20, CL21, GHS21, HS21, SB21, CJLW22], 。在这类对抗信道中，信道会在编码后的消息中插入或删除数量有界的符号。这种码称为插入删除码，其采用的度量 dist 是（归一化）编辑距离 ED，定义为将一个字符串 u 变换为另一个字符串 v所需的最少符号插入和删除次数，并除以 2 $\max\{|u|, |v|\}$。直到最近，人们才充分理解如何构造具有渐近最优码率和错误率的高效插入删除码[HS18, Hae19, HRS19, LTX19, GHS21]。

关于能够抵御插入删除错误的局部可解码码（插入删除局部可解码码）的研究寥寥无几，迄今仅有少数成果。据我们所知，Ostrovsky 和 Paskin-Cherniavsky [OPC15],首次提出了这类码，而此后所有插入删除局部可解码码的构造都遵循 [OPC15]，并采用所谓的"汉明到插入删除编译器" [BBG+20, CLZ20, BB21], 。该编译器可将任意汉明局部可解码码转换为插入删除局部可解码码，使码率和错误率均增加一个常数因子，并使局部性增加一个多对数因子。例如，任何局部性为 3、码长为 K 、错误率为 ρ 的汉明局部可解码码，都可以编译为局部性为 $3 \cdot \text{polylog}(K)$、码长为$\Theta(K)$且错误率为 $\Theta(\rho)$ 的插入删除局部可解码码。

*与 ISIT 2023 上发表的同名论文的完整版，可通过以下网址获取：https://doi.org/10.1109/ISIT54713.2023.10206655。©2023 IEEE。允许个人使用此材料。其他所有用途均须获得 IEEE 的许可，无论是在当前还是未来的任何媒体中，包括为广告或宣传目的而转载/再版此材料、创建新的合集、转售或重新分发至服务器或列表，或在其他作品中重复使用本作品的任何受版权保护的部分。

A. 结果概述

在这项工作中，我们重新考察针对汉明错误和插入删除错误的计算放宽局部可解码码。我们首先定义计算放宽局部可解码码。

定义 1（计算放宽局部可解码码）。设 $\mathcal{C} = \{C_\lambda[K, k, q_1, q_2]\}_{\lambda\in\mathbb{N}}$ 为一个具有编码算法 $\{\mathsf{Enc}_\lambda\colon \Sigma_1 \to \Sigma_2\}_{\lambda\in\mathbb{N}}$ 的码族，其中 $|\Sigma_i| = q_i$。我们称 $\mathcal{C}$ 为一个（ℓ，ρ，p，δ，dist）-计算放宽局部可解码码（抗腐化局部可解码码）（crLDC），如果存在一族随机化预言机解码算法 $\{解码器_\lambda\colon [k] \to \Sigma_1\}_{\lambda\in\mathbb{N}}$，使得：

1) 对于所有 $\lambda \in \mathbb{N}$ 和任意 $\tilde{y} \in \Sigma_2^*$，解码器$^{\tilde{y}}_\lambda(i)$ 对于任意 $i \in [k]$，最多向 $\tilde{y}$ 发出 ℓ次查询；
2) 对于所有 $\lambda \in \mathbb{N}$ 和任意 $x \in \Sigma_1^k$，我们有

$$\Pr[\mathsf{Dec}_\lambda^{\mathsf{Enc}_\lambda(x)}(i) = x_i] = 1$$

对于所有 $i \in [k]$;

3) 定义二元谓词 $\mathsf{Fool}(\tilde{y}, \rho, p, x, y, \lambda) = 1$ 当且仅当
a) 距离$(y, \tilde{y}) \leqslant \rho$；并且
b) $\exists i \in [k]$ 使得

$$\Pr[\mathsf{Dec}_\lambda^{\tilde{y}}(i) \in \{x_i, \perp\}] < p,$$

其中概率是针对解码器$_\lambda$取的；
否则 欺骗$(\tilde{y}, \rho, p, x, y, \lambda) = 0$。我们要求，对于所有概率多项式时间对手 $\mathcal{A}$，都存在一个可忽略函数$\varepsilon_{\mathsf{F}}(\cdot)$，使得对于所有 $\lambda \in \mathbb{N}$ 和所有 $x \in \Sigma_1^k$，我们有

$$\Pr[\mathsf{Fool}(\mathcal{A}(y), \rho, p, x, y, \lambda) = 1] \leqslant \varepsilon_{\mathsf{F}}(\lambda),$$

其中概率是针对 $\mathcal{A}$ 和 y =编码$_\lambda(x)$取的。*4)* 定义二元谓词 极限$(\tilde{y}, \rho, \delta, x, y, \lambda) = 1$ 当且仅当
a) 距离$(y, y') \leqslant \rho$；并且
b) |良好$(y')| < \delta \cdot k$，其中

$$\mathsf{Good}(y') := \{i \in [k]\colon \Pr[\mathsf{Dec}_\lambda^{y'}(i) = x_i] > 2/3\}$$

并且该概率取自解码器$_\lambda$；
否则 *Limit*$(\tilde{y}, \rho, \delta, x, y, \lambda) = 0$。我们要求，对于所有概率多项式时间对手 $\mathcal{A}$，都存在一个可忽略函数 $\varepsilon_{\mathsf{L}}(\cdot)$，使得对于所有 $\lambda \in \mathbb{N}$ 和所有 $x \in \Sigma_1^k$，均有概率[*Limit*($\mathcal{A}(y)$ ρ, δ, x, y, λ) $= 1] \leqslant \varepsilon_{\mathsf{L}}(\lambda)$，其中概率取自 $\mathcal{A}$ 和 y =*Enc*$_\lambda(x)$。

如果dist 是归一化汉明距离HAM，我们称该码为汉明 抗腐化局部可解码码；如果dist 是归一化编辑距离编辑距离，我们称该码为插入删除 抗腐化局部可解码码。这里，ℓ 是局部性，ρ 是错误率，p 是成功概率，若函数对于所有常数$c > 0$都满足 $o(x^{-c})$，则称其为可忽略 。如果 $q_2 = 2$，我们称 $\mathcal{C}$ 是一个二进制 抗腐化局部可解码码族，而如果 $q_1 = q_2$，我们就简单地写作 $C_\lambda[K, k, q_1]$。

定义 1与以下内容非常接近：抗腐化局部可解码码Blocki 等人的定义。[BGGZ21]，但做了一些修改。首先，[BGGZ21] 利用碰撞抗性哈希函数的公开随机种子，因此其抗腐化局部可解码码定义对种子生成算法的随机性进行量化。我们的构造不需要公开随机种子，因此在定义中省略了该算法，转而对我们的抗腐化局部可解码码码族 $\{C_\lambda\}_{\lambda\in\mathbb{N}}$的安全性进行量化。这种量化方式还刻画了与概率多项式时间对手交互时的渐近安全性，这与针对信息论对手的标准（r）LDC 定义不同。此外，[BGGZ21] 要求公开随机种子以诚实（即可信）的方式生成，而我们的定义和构造避免了这一要求。其次，我们通过调整谓词 Fool 略微加强了安全性定义：在定义 1 中，如果存在一个索引 i（对手不一定知道该索引），使得解码器在输入 i 时正确输出的概率小于 p，则对手获胜。相比之下，[BGGZ21]要求对手输出受损码字 y' 和目标索引 i，使得解码器在索引 i 上正确输出的概率小于 p。注意，若要求定义 1 对 $p = 2/3$, $\varepsilon_{\mathsf{F}}(\lambda) = \varepsilon_{\mathsf{L}}(\lambda) = 0$成立，并且对所有计算能力不受限的对手 $\mathcal{A}$ 均成立，则得到原始 rLDC 定义 [BGH+06]。

我们的首项贡献是构造一族满足定义 1的二元汉明抗腐化局部可解码码。我们的构造借鉴了码拼接技术 [对于 66]，，该技术使用外码 $C_{out} = (\mathsf{Enc}_{out}$,解码器$_{out})$ 和内码 $C_{in} = (\mathsf{Enc}_{in}$,解码器$_{in})$，并将消息 x 编码如下：

1) 计算 y =$\mathsf{Enc}_{out}(x)$；2) 将 y分割为若干个 d块 $y^{(1)}\|\ldots\|y^{(d)}$；3) 对所有 i，计算 $Y^{(i)} = \mathsf{Enc}_{in}(y^{(i)})$；4) 输出 $Y = Y_{(1)}\|\cdots\|Y_{(d)}$；其中，$\|$表示字符串拼接。

在我们的构造中，我们使用恒等函数作为 C_{out}，使用合适的数字签名方案对每个块$y^{(i)}$进行签名，并使用经典汉明码作为 C_{in}。简而言之，签名长度为 $r(\cdot)$ 的数字签名方案是由以下概率多项式时间算法组成的元组 $\Pi =$ (Gen,Sign,Ver)，并满足以下性质：

1) Gen 的输入为安全参数 $\lambda \in \mathbb{N}$（一元表示），输出一个密钥对 (pk,sk)，其中 pk 是公钥/验证密钥，sk 是私钥/签名密钥；2) Sign 的输入为任意长度的消息 m 和签名密钥 sk，输出消息 m的签名 $\sigma \in \{0,1\}^{r(\lambda)}$。3) Ver 是确定性的，其输入为消息 m、某个签名 σ和验证密钥 pk；当且仅当 σ 是消息 m 的有效签名时输出 1，否则输出 0。4) 对所有概率多项式时间对手 $\mathcal{A}$，对于 (pk,sk) $\leftarrow$ Gen(1^λ)，若向 $\mathcal{A}$提供 pk 作为输入，并允许其访问 Sign$_{\mathsf{sk}}(\cdot)$ 预言机，则称 Π 是安全的，如果除 λ 中可忽略的概率外，$\mathcal{A}$无法输出一对 $(\tilde{m}, \tilde{\sigma})$，使得 Ver$_{\mathsf{pk}}$ $(\tilde{m}, \tilde{\sigma}) = 1$，且 $\mathcal{A}$ 从未查询过 Sign$_{\mathsf{sk}}(\tilde{m})$。

给定一个安全数字签名方案和任意二元汉明码，我们得到第一个主要结果。

定理 1。设 Π 是一个 $r := r(\lambda)$ 长度的签名方案。设 C_{in} 是一个码率为 β_{in}、错误率为 ρ_{in} 的二元汉明码。那么，对于每个正多项式 $k(\cdot)$和常数 $c \in (0, 1/2)$，存在一个码族

$\mathcal{C}_{\mathsf{H}} := \{C_{\mathsf{H},\lambda}[K, k(\lambda)\ 2]\}_{\lambda\in\mathbb{N}}$和函数 $\mu := \mu(\lambda)$ 使得 $\mathcal{C}_{\mathsf{H}}$ 是一个 $(\ell,\ \rho,\ p,\ \delta)$-汉明 抗腐化局部可解码码，其中

- $K = O((1/\beta_{in})\max\{k(1+\log(k)/r)\ r\})$,
- $\ell = O((\mu/\beta_{in})\cdot(r+\log(k)))$,
- $\rho = c\cdot\rho_{in}$,
- $p = 1-\exp(-\mu(1/2-c)^2/2(1-c)) > 2/3$，以及
- $\delta = 1/2$,

其中 $k := k(\lambda)$。

当 $\beta_{in} = \Theta(1)$ 且 $\Omega(\log(k(\lambda))) = r(\lambda) \leqslant k(\lambda)$ 时，我们的码族 $\mathcal{C}_{\mathsf{H}}$ 具有恒定码率。我们的构造允许 $r(\lambda) > k(\lambda)$，但这会导致局部性 $\ell \geqslant K$，因此使用码率和错误率相近的汉明码更有效。任何满足 $p > 2/3$ 的 μ 都能保证 $\delta = 1/2$；例如，对于常数 $\epsilon > 0$，取 $\mu(\lambda) := O(\log^{1+\epsilon}(\lambda))$，即可得到多对数局部性和成功概率 $1-\mathsf{negl}(\lambda)$，其中 negl 表示某个未具体指定的可忽略函数。

我们可以采用恒定码率、恒定错误率的二元汉明码 C_{in}（例如 [Jus72]）以及适当的签名方案来实例化定理 1，从而得到具有多对数局部性的恒定码率、恒定错误率汉明 crLDC。当 $r(\lambda) = \mathsf{polylog}(\lambda)$ 时，我们的构造尤为出色；并且在标准理想化模型下，存在 $r(\lambda)$ 小至 $\Theta(\log^{1+\epsilon}(\lambda))$ 的签名方案，其中 $\epsilon > 0$ [是较小的常数，参见 Sch90、BL22]。假设这些方案满足以下具体安全性概念：对于安全参数 λ，任何运行时间为 $2^{\lambda/2}$ 的对手，针对长度为 $r(\lambda) = \lambda$ 的签名，破坏方案安全性的概率至多为 $2^{-\lambda/2}$。代入 $\lambda' = \Theta(\log^{1+\epsilon}(\lambda))$ 后，这些方案可抵御超多项式时间对手，并在 λ 下具有可忽略安全性，这意味着它们满足我们对签名方案的安全性定义。使用此类方案、恒定码率且恒定错误率的汉明码 C_{in}，以及 $\mu(\lambda) := O(\log^{1+\epsilon}(\lambda))$，我们得到以下推论。

推论 1. 设 Π 是一个 $r(\lambda) = \Theta(\log^{1+\epsilon}(\lambda))$ 长度的签名方案，其中常数为 $\epsilon > 0$。那么，对于所有充分大的正多项式 $k(\cdot)$，存在码族$\{C_{\mathsf{H},\lambda}[K, k(\lambda)\ 2]\}_{\lambda\in\mathbb{N}}$，它是一个 (ℓ, ρ, p, δ)-汉明抗腐化局部可解码码，满足

- $K = O(k)$，• $\ell = O(\log^{2(1+\epsilon)}(\lambda))$,
- $\rho = \Theta(1)$,
- $p = 1-\mathsf{negl}(\lambda)$，且
- $\delta = 1/2$,

其中 $k := k(\lambda)$。

推论 1 的参数与汉明 抗腐化局部可解码码 构造 [BGGZ21], 所达到的$K = O(k)$、 $\ell = \mathrm{polylog}(k)$、 $\rho = \Theta(1)$、 $p = 1-\mathsf{negl}(\lambda)$以及$\delta = \Theta(1)$相当。可以说，我们的构造在概念上比 [BGGZ21],的构造更简单：后者使用局部扩展图和抗碰撞哈希函数（并采用可信设置），而我们的构造只需进行分割、签名和编码。此外，我们使用签名无需依赖公钥基础设施，因为这类方案可由单向函数构造[Lam79]。

1）扩展至插入删除错误：我们的第二项贡献是将定理 1的构造扩展到能够处理插入删除错误。此前的插入删除局部可解码码构造采用了一种所谓的“汉明码到插入删除码”编译器 [OPC15，BBG+20]。该编译器的关键是带噪二分搜索算法，直观而言，它可以在近似有序列表中搜索，并以高概率找到大多数条目。我们使用该算法来寻找未被“过度腐化”的码字块，从而处理更一般的插入删除错误。我们采用 Block 等人的带噪二分搜索工具 [BBG+20]以及著名的 Schulman-Zuckerman 插入删除码 [SZ99]来 C_{in} 扩展定理 1，使其适用于插入删除设置。结合安全数字签名方案，我们得到了第二个主要结果。

定理 2. 设 Π 是一个 $r := r(\lambda)$ 长度的签名方案。存在一个常数 $c \in (0, 1/2)$，使得对于每个正多项式 $k(\cdot)$ 和常数 $\rho^* \in (0, 1/3)$，都存在一个码族 $\mathcal{C}_{\mathsf{Ins}} := \{C_\lambda[K, k(\lambda)\ 2]\}_{\lambda\in\mathbb{N}}$ 以及一个函数 $\mu := \mu(\lambda)$，使得 $\mathcal{C}_{\mathsf{Ins}}$ 是一个(ℓ, ρ, p, δ)-插入删除抗腐化局部可解码码，且

- $K = O(\max\{k(1+\log(k)/r), r\})$,
- $\ell = O((\log^3(K)+\mu)\cdot(r+\log(k)))$,
- $\rho = \Theta(1)$,
- $p = 1-\rho^*-\exp(-\mu(1/2-c)^2/2(1-c)) > 2/3$, *and*
- $\delta = 1-\Theta(\rho)$,

其中 $k := k(\lambda)$。

与定理 1 一样，只要 $\Omega(\log(k(\lambda))) = r(\lambda) \leqslant k(\lambda)$，我们的码族 $\mathcal{C}_{\mathsf{Ins}}$ 就具有恒定码率；此外，当 $r(\lambda) > k(\lambda)$ 时，它也有同样的缺点。在这种情况下，直接使用（渐近）最优插入删除码（例如 [SZ99]）进行编码会更有效。我们再次选择 μ，使得 $p = 1-\mathsf{negl}(\lambda) > 2/3$；此外，在对底层签名方案作出与我们的汉明 crLDC 相同的一组假设时（例如 [Sch90, BL22]），对于 $\mu(\lambda) = \Theta(\log^{1+\epsilon}(\lambda))$ 且小常数 $\epsilon > 0$，我们得到以下推论。

推论 *2.* 设 Π 是一个 $r(\lambda) = \Theta(\log^{1+\epsilon}(\lambda))$ 长度的签名方案，其中常数 $\epsilon > 0$。那么，对于所有充分大的正多项式 $k(\cdot)$，存在码族$\{C_{\mathsf{I},\lambda}[K, k(\lambda)\ 2]\}_{\lambda\in\mathbb{N}}$，它是一个 (ℓ, ρ, p, δ)-*InsDel crLDC*，且 $K = O(k)$、 $\ell = O(\log^{4+\epsilon}(\lambda))$、 $\rho = \Theta(1)$、 $p = 1-\mathsf{negl}(\lambda)$ 和 $\delta = 1-\Theta(\rho)$，其中 $k := k(\lambda)$。

据我们所知，我们的 InsDel 抗腐化局部可解码码是同类中的首创，并且相比于 Block 等人提出的先前 InsDel 局部可解码码表现良好 [BBG+20]，且与 Block 和 Blocki 提出的私有及资源受限局部可解码码相当 [BB21]。

B. 相关工作

经典插入删除码最初由以下文献研究 [Lev66]，由此开启了对这类码的一系列丰富研究；综述见[Slo02、Mit08、MBT10]以了解更多信息。最近，k构造了具有最优码率的删除纠错码，回答了一个长期悬而未决的问题 [SB21]。文献研究了具有正码率且能纠正大量删除的随机码，见 [KLM04、GW17]。另一类研究将列表解码扩展到插入删除码 [HSS18、LTX19、GHS21]。最后， [HS18] 构造了显式同步码

可以通过以下方式对字符串进行“局部解码”：字符串中的每个索引都可以利用字符串中其他少数位置上的符号计算得到。这些同步字符串被用于构造针对插入删除错误的近线性时间交互式编码方案。

[Lip94] 开创了对能够抵御计算受限信道所引入错误的码的研究。随后有多项工作采用了这一信道模型，构造出参数优于经典对应码的汉明码[MPSW05、GS16、SS21]。有人指出，任何现实世界中的通信信道都可以合理地建模为计算受限信道 [Lip94、BKZ20],因此可以合理地预期，自然界中遇到的错误模式可由某种（可能未知的）概率多项式时间算法建模。这一信道模型也已扩展到 局部可解码码 设置，涵盖汉明 [OPS07、HO08、HOSW11、BKZ20、BGGZ21]以及较近提出的插入删除错误 [BB21]。

[BGH+06] 提出了宽松局部可解码码的概念。随后， [GRR20] 提出并构造了宽松局部可纠错码（rLCC），用于纠正汉明错误：这类码配有局部纠错算法，通过查询接收字中的少数几个位置，即可纠正受损码字中的符号。与经典汉明LCC相比，他们的构造具有显著更优的参数，实现了常数局部性、常数错误率和多项式码长。此外，他们的rLCC也是一种宽松局部可解码码，因为其码具有系统性。后续工作继续改进rLCC构造 [AS21、CY22、CGS22] [BGGZ21] 则在计算受限信道的背景下研究汉明错误下的宽松局部可解码码和宽松局部可纠错码（抗腐化局部可解码码和抗腐化局部可纠错码）。我们的工作直接采用了这一模型，但针对的是插入删除错误。

[OPC15] 开创了对插入删除局部可解码码的研究。他们给出了一种编译器，可将任意汉明局部可解码码转换为插入删除局部可解码码，同时渐近保持底层汉明局部可解码码的码率和错误率，代价是局部性增加一个多对数因子。 [BBG+20] 借鉴了对一种称为内存困难函数的密码学对象的研究技术 [EGS75, ABH17, ABP18, BH22]，通过概念上更简单的分析重新证明了这一结果。 [CLZ20]随后提出了在不同设置下采用随机化编码的汉明/插入删除局部可解码码的概念，包括编码器与解码器共享随机性，或信道非自适应地添加错误模式的情形。在插入删除情形下， [CLZ20] 调用了 [OPC15] 的编译器，并得到码长为$O(k)$或 $O(k\log(k))$、局部性为 $\mathrm{polylog}(k)$的码。近期， [BB21]将 [BBG+20] 的编译器扩展到 [OPS07], 的私钥设置，其中编码器和解码器共享信道未知的密钥；还扩展到了 [BKZ20], 的资源受限设置，其中假设信道以某种方式受到资源限制。尽管很可能将“汉明码到插入删除码”编译器应用于 [BGGZ21]的抗腐化局部可解码码或我们的抗腐化局部可解码码，就能得到插入删除抗腐化局部可解码码，但此前的工作并未正式提出或证明这一点。最后，近期在获得插入删除局部可解码码的下界方面取得了进展。 [BCG+22] 证明，即使在私钥设置下，具有常数局部性的插入删除局部可解码码也需要指数级.....码长，并且还证明了线性 2 查询插入删除局部可解码码并不存在。因此，在多对数局部性范围内存在恒定码率的插入删除抗腐化局部可解码码，就更加令人惊讶了。

II. 技术概述

我们的汉明码和 InsDel crLDC 构造所需的主要技术要素，是使用数字签名方案 Π，其签名长度为 r，并搭配合适的内码 C_{in}。两种码的编码算法几乎完全相同，主要区别在于 C_{in} 的选择。解码算法也很相似：插入删除解码器是在汉明解码器基础上进行的（非平凡）修改，以便利用带噪二分搜索技术处理插入删除错误。

1）汉明码抗腐化局部可解码码构造：令 C_{in} 为合适的汉明码（即非局部码），并令 $\Pi = (\mathrm{Gen}, \mathrm{Sign}, \mathrm{Ver})$ 为一个长度为 r 的签名方案。

汉明编码器：我们定义一族编码算法 $\{\mathrm{Enc}_{H,\lambda}\}_\lambda$。令 $\lambda \in \mathbb{N}$ 为安全参数。对于任意消息 $x \in \{0,1\}^k$，编码器 $\mathrm{Enc}_{H,\lambda}$ 将其分割成 $d = \lceil k/r(\lambda) \rceil$ 个块，其中对所有 i（必要时用 0 填充）。随后使用 Π 对每个 $x^{(i)}$ 进行签名：$\mathrm{Enc}_{H,\lambda}$ 通过 $(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathrm{Gen}(1^\lambda)$ 生成密钥对，并计算签名 $\sigma^{(i)} \leftarrow \mathrm{Sign}_{\mathrm{sk}}(x^{(i)} \| i)$。接着，使用 C_{in} 对块 $x^{(i)} \| \sigma^{(i)} \| \mathrm{pk} \| i$ 进行编码，得到码字 $c^{(i)}$，其中 pk 是先前生成的公钥。最后，$\mathrm{Enc}_{H,\lambda}$ 输出 $C = c^{(1)} \| \cdots \| c^{(d)} \in \{0,1\}^K$。如果 $r(\lambda) \geqslant k$，则只需对一个块进行签名和编码，代价是局部性 $\geqslant K$；因此，与使用 $\mathrm{Enc}_{H,\lambda}$ 相比，采用码率和错误率相近的汉明码更有效。形式化的编码算法见算法 1。

算法 1： 汉明编码器 $\mathrm{Enc}_{H,\lambda}$

输入：一条消息 $x \in \{0,1\}^k$。
输出：一个码字 $C \in \{0,1\}^K$。
硬编码： 汉明码 C_{in}；$r(\cdot)$ 长度的签名方案 Π；且 $\lambda \in \mathbb{N}$ 以一元表示。

采样 $(\mathrm{pk},\mathrm{sk}) \leftarrow$ 密钥生成算法(1^λ)
集合 $d = \lceil k/r(\lambda) \rceil$
分割 $x = x^{(1)} \| \cdots \| x^{(d)}$ 满足 $x^{(j)} \in \{0,1\}^{r(\lambda)}$
　对于每个 $j \in [d]$ （必要时填充最后一个块）
对每个 $j \in [d]$ **执行**
　$\sigma^{(j)} \leftarrow$签名$_{\mathrm{sk}}(x^{(j)} \| j)$
　$C^{(j)} =$Enc$_{in}(x^{(j)} \| \sigma^{(j)} \| \mathrm{pk} \| j)$
定义 $C := C^{(1)} \| \cdots \| C^{(d)} \in \{0,1\}^K$
返回C

朴素解码器：给定 $\mathrm{Enc}_{H,\lambda}$，存在一种自然的解码算法，但它不满足定义 1。朴素解码器的过程如下。设 $x \in \{0,1\}^k$，$C = \mathrm{Enc}_{H,\lambda}(x) \in \{0,1\}^n$，并设 $\tilde{C} \in \{0,1\}^n$ 满足 $\mathrm{HAM}(C, \tilde{C}) \leqslant \rho n$。设 $i \in [k]$ 为提供给朴素解码器的输入，并设 $\tilde{C}$ 为其预言机。由于目标是从字符串 C中恢复比特 x_i，朴素解码器首先计算索引 $j \in [d]$，使得比特 x_i 位于块 $x^{(j)}$中。

由于 $\tilde{C}$ 仅包含汉明错误，朴素解码器将其预言机 $\tilde{C}$ 视为块 $\tilde{C}_{(1)}\|\cdots\|\tilde{C}_{(d)}$，并恢复块 $\tilde{C}^{(j)}$。随后，朴素解码器运行C_{in}的解码器，以 $\tilde{C}^{(j)}$ 为输入，得到某个字符串 $\tilde{m}_{(j)}$，该字符串可视为某个（可能已损坏的）字符串 $\tilde{x}^{(j)}\|\tilde{\sigma}^{(j)}\|\widetilde{\mathsf{pk}}\|\tilde{j}$。接着，朴素解码器使用签名方案验证该解码消息的内容，检查 $\mathsf{Ver}_{\tilde{\mathsf{pk}}}(\tilde{x}^{(j)}\|j,\ \tilde{\sigma}^{(j)}) \stackrel{?}{=} 1$。如果验证失败，则解码器输出 $\perp$；否则，解码器输出 $\tilde{x}^{(j)}_{i^*}$，其中 i^* 是与比特 x_i对应的 $x^{(j)}$ 的索引。

注意，如果$\tilde{C}$，那么这个朴素解码器以概率 1 输出正确的比特 x_i，满足定义 1 中的条目 2。然而，如果我们要求错误率为 $\rho = \Theta(1)$，这个朴素解码器就无法满足定义 1 中的条目 3。考虑以下简单攻击。令 $\mathcal{A}$ 为一个概率多项式时间对手，其操作如下：(1) 给定码字 C，对手 $\mathcal{A}$ 对块 $C^{(1)}$ 进行解码，得到 $x^{(1)}\|\sigma^{(1)}\|\mathsf{pk}\|1$。(2) $\mathcal{A}$ 随后生成自己的密钥对 $(\mathsf{pk}', \mathsf{sk}')$、一条消息 $x' = 1 - x^{(1)}$，并计算 $\sigma' =$ 签名算法$_{\mathsf{sk}'}(x'\|1)$。(3) $\mathcal{A}$随后计算 $C' = \mathsf{Enc}_{in}(x'\|\sigma'\|\mathsf{pk}'\|1)$ 并输出 $\tilde{C} = C'\|C^{(2)}\|\cdots\|C^{(d)}$。直观地说，这种攻击成功有两个原因。第一个原因是，将 $C^{(1)}$ 篡改为 C'所需的篡改量只是允许用于将 C 转换为 C的总篡改量中的一小部分。第二个原因是，朴素解码器依赖公钥 pk'来执行验证。要阻止这种攻击，关键在于解决公钥恢复问题。注意，如果解码器恢复了 $\mathsf{Enc}_{\mathsf{H},\lambda}$所用的真实公钥 pk，那么这种攻击就会失败，因为验证过程会失败，解码器会输出 bot。因此，我们修改朴素解码器以恢复真实公钥，从而得到最终的汉明解码器。

汉明解码器：我们定义一个解码算法族 $\{\mathsf{Dec}_{\mathsf{H},\lambda}\}_\lambda$。令 $\lambda \in \mathbb{N}$, $\mu \in \mathbb{N}$ 为我们选择的参数，$x \in \{0,1\}^k$, $C = \mathsf{Enc}_{\mathsf{H},\lambda}(x)$，并且 $\tilde{C} \leftarrow \mathcal{A}(C)$ 满足 $\mathrm{HAM}(C,\tilde{C}) \leqslant \rho$，其中 $\mathcal{A}$ 是一个概率多项式时间对手。在输入 $i \in [k]$ 并获得对 C的预言机访问后，解码器 $\mathsf{Dec}_{\mathsf{H},\lambda}$通过两步过程尝试恢复 x_i。首先，$\mathsf{Dec}_{\mathsf{H},\lambda}$ 尝试恢复真实的公钥 pk。它首先均匀采样 $j_1, \ldots, j_\mu \leftarrow [d]$。将 $\tilde{C}$解析为 $\tilde{C}_{(1)}\|\cdots\|\tilde{C}_{(d)}$后，对于每个 $\kappa \in [\mu]$，$\mathsf{Dec}_{\mathsf{H},\lambda}$ (1)恢复某个 $\tilde{m}_{(j_\kappa)} \leftarrow \mathsf{Dec}_{in}(\tilde{C}_{(j_\kappa)})$；(2) 将 $\tilde{m}_{(j_\kappa)}$解析为 $\tilde{x}^{(j_\kappa)}\|\tilde{\sigma}^{(j_\kappa)}\|\widetilde{\mathsf{pk}}_{(j_\kappa)}\|\tilde{j}$；并且 (3) 恢复 $\widetilde{\mathsf{pk}}_{(j_\kappa)}$。然后，解码器将 pk^* 设置为 $\mathrm{majority}(\widetilde{\mathsf{pk}}_{(j_1)}, \ldots, \widetilde{\mathsf{pk}}_{(j_\mu)})$。其次，$\mathsf{Dec}_{\mathsf{H},\lambda}$ 计算 j，使得 x_i属于 $x^{(j)}$，计算 $\tilde{m}(j) \leftarrow \mathsf{Dec}_{in}(\tilde{C}^{(j)})$，将其解析为 $\tilde{x}^{(j)}\|\tilde{\sigma}^{(j)}\|\widetilde{\mathsf{pk}}_{(j)}\|\tilde{j}$，然后检查 $\mathsf{Ver}_{\mathsf{pk}^*}(\tilde{x}^{(j)}\|j, \tilde{\sigma}^{(j)}) = 1$，输出 $\tilde{x}^{(j)}_{i^*}$，其中 i^*是当结果为真时与 x_i对应的 $x^{(j)}$ 的索引；否则，$\mathsf{Dec}_{\mathsf{H},\lambda}$ 输出 $\perp$。这里至关重要的是，$\mathsf{Dec}_{\mathsf{H},\lambda}$ 必须使用其计算出的值 j，否则对手可能交换两个块$C^{(j_1)}$和 $C^{(j_2)}$，其中 $x^{(j_1)} \neq x^{(j_2)}$，从而违反条目 3。我们在算法 2 中给出形式化的解码算法。

定理 1 证明概述：我们概述一下定理 1的证明；完整细节见第 IV 节。证明定理 1的主要技术挑战在于证明 $\{(\mathsf{Enc}_{\mathsf{H},\lambda}, \text{解码器}_{\mathsf{H},\lambda})\}_\lambda$ 满足 条目 3 和 4

算法 2： 汉明解码器 解码器$_{\mathsf{H},\ \lambda}$

输入 ：索引 $i \in [k]$。
预言机 ：比特串 $\tilde{C} \in \{0,1\}^K$.
输出 ：一个符号 $\tilde{x} \in \{0,1\}$ 或 $\perp$。
硬编码： 汉明码 C_{in}； $r(\cdot)$ 长签名方案 Π； $\lambda \in \mathbb{N}$ 以一元表示；以及 $\mu \in \mathbb{N}$。

集合 $d = \lceil k/r(\lambda) \rceil$ 和 $\mathrm{bl} = n/d$
采样 $j_1, \ldots, j_\mu \xleftarrow{\$} [d]$
初始化 $\mathsf{pk}^*, \mathsf{pk}_1, \ldots, \mathsf{pk}_\mu = 0$
对于每个 $\kappa \in [\mu]$，**执行** // 恢复 pk
  $\tilde{m}_{(j_\kappa)} \leftarrow$ 解码器$_{in}(\tilde{C}[(j_\kappa - 1)\cdot \mathrm{bl} + 1,\ j_\kappa \cdot \mathrm{bl}])$
  将 $\tilde{m}^{(j_\kappa)}$ 解析为 $\tilde{x}^{(j_\kappa)}\|\tilde{\sigma}^{(j_\kappa)}\|\widetilde{\mathsf{pk}}_{(j_\kappa)}\|\tilde{j}$
  设置 $\mathsf{pk}_\kappa = \widetilde{\mathsf{pk}}^{(j_\kappa)}$
设置 $\mathsf{pk}^* =$ 多数表决$(\mathsf{pk}_1, \ldots, \mathsf{pk}_\mu)$
计算 $j \in [d]$ 使得 $(j-1)\cdot r(\lambda) < i \leqslant j \cdot r(\lambda)$
$\tilde{m}^{(j)} \leftarrow$ 解码器$_{in}(\tilde{C}[(j-1)\cdot \mathrm{bl} + 1, j \cdot \mathrm{bl}])$
解析 $\tilde{m}^{(j)}$ 为 $\tilde{x}^{(j)}\|\tilde{\sigma}^{(j)}\|\widetilde{\mathsf{pk}}_{(j)}\|\tilde{j}$
如果 $\mathsf{Ver}_{\mathsf{pk}^*}(\tilde{x}^{(j)}\|j, \tilde{\sigma}^{(j)}) = 0$ **则返回** $\perp$
返回 $\tilde{x}^{(j)}_{i^*}$ 对于 $i^* = i - (j-1)\cdot r(\lambda)$。

定义 1 的条目 3。对于任意 $x \in \{0,1\}^k$、概率多项式时间对手 $\mathcal{A}$ 和 $i \in [k]$，我们分析以下概率：$\mathsf{解码器}^{C}_{\mathsf{H},\lambda}(i) \in \{x_i, \perp\}$ 针对 $\tilde{C} \leftarrow \mathcal{A}(\mathsf{Enc}_{\mathsf{H},\lambda}(x))$，且 $\mathrm{HAM}(\tilde{C}, \mathsf{Enc}_{\mathsf{H},\lambda}(x)) \leqslant \rho$。若 $\mathsf{Dec}^{\tilde{C}}\mathsf{H}_\lambda(i) = x_i$，则 $\tilde{x}^{(j)}_{i^*} = x_i$ 且 $\mathsf{Ver}_{\mathsf{pk}^*}(\tilde{x}^{(j)}\|j, \tilde{\sigma}^{(j)}) = 1$。在条件化于 $(\tilde{x}^{(j)}\|j, \tilde{\sigma}^{(j)})$ 未破坏 Π 的安全性后，验证成功意味着 $\tilde{x}^{(j)} = x^{(j)}$ 和 $\tilde{\sigma}^{(j)} = \sigma^{(j)}$，并且只要 $\mathsf{pk}^* = \mathsf{pk}$，验证就会成功。根据切尔诺夫界，只要超过一半的块 $\tilde{C}^{(j)}$ 中汉明错误所占比例低于 ρ_{in}，就能以高概率（取决于 μ）确保 $\mathsf{pk}^* = \mathsf{pk}$；通过对任意 $c \in (0, 1/2)$ 设置 $\rho = c\rho_{in}$ 即可实现这一点。根据定义，$\tilde{\sigma}^{(i)}$ 以至少 $1 - \varepsilon_\Pi(\lambda)$ 的概率不会破坏 Π 的安全性（即，它要么是正确签名，要么验证失败），其中 $\varepsilon_\Pi(\lambda)$ 是针对 Π 安全性的可忽略函数。由于此处索引 i 是任意的，我们通过并集界得到条目 3：对于$p = 1 - \exp(-\mu(1/2 - c)^2/2(1-c))$，以及 $\varepsilon_{\mathsf{F}}(\lambda) = k \cdot \varepsilon_\Pi(\lambda)$，其中 $\varepsilon_{\mathsf{F}}(\lambda)$ 是可忽略函数，因为 $k = \mathrm{poly}(\lambda)$。

为得到条目 4，定义 $\mathcal{J} := \{j : \mathrm{HAM}(\tilde{C}^{(j)}, C^{(j)}) \leqslant \rho_{in}\}$。那么，对于 $c \in (0, 1/2)$，$\rho = c\rho_{in}$意味着 $|\mathcal{J}| \geqslant d/2$。此外，对于任意 $j \in \mathcal{J}$，解码器$_{in}(\tilde{C}^{(j)}) = x^{(j)}\|\sigma^{(j)}\|\mathsf{pk}\|j$。现在，对于任意$i \in [k]$，如果 x_i 属于 $j \in \mathcal{J}$的 $x^{(j)}$，那么解码器$_{\mathsf{H},\lambda}$输出 x_i 的概率，等于解码器$_{\mathsf{H},\lambda}$ 正确恢复 $\mathsf{pk}^* = \mathsf{pk}$ 的概率。我们选择 μ 以确保概率$[\mathsf{pk}^* = \mathsf{pk}] > 2/3$。这与 $|\mathcal{J}| \geqslant d/2$ 一起意味着 $|\text{良好}(C)| \geqslant k/2$ 且 $\delta = 1/2$。根据我们对 ρ $|\mathcal{J}| \geqslant d/2$ | C | $\geqslant k/2$ 的选择，对于任意满足 $\mathrm{HAM}(C, \tilde{C}) \leqslant \rho$的 $\tilde{C}$，良好$(\cdot)$ 都成立；因此，条目 4 对 $\delta = 1/2$ 和 $\varepsilon_{\mathsf{L}}(\lambda) := 0$ 成立。

2) 插入删除抗腐化局部可解码码构造：令 C_{in} 为 Schulman-Zuckerman 插入删除码（SZ 码） [SZ99]并令 $\Pi =$ (密钥生成算法，签名，验证) 为一个长度为 r的签名方案。

解码插入删除错误的挑战：插入删除错误允许对手向码字中插入符号并删除符号，这会带来汉明错误中不会出现的挑战。我们或许希望直接使用我们的族 $\{(\mathsf{Enc}_{H,\lambda}, \mathsf{Dec}_{H,\lambda})\}_\lambda$，结合 $C_{in} = \mathsf{SZ}$ 来实现定理 2；然而，这会得到一个平凡的 InsDel 抗腐化局部可解码码。令 $\mathsf{Enc}'_{H,\lambda}$ 与 $\mathsf{Enc}_{H,\lambda}$ 完全相同，只是将 SZ 码用作码 C_{in}。对于任意 x 和 $C = \mathsf{Enc}'_{H,\lambda}(x)$，存在一种简单攻击，确保 $\mathsf{Dec}_{H,\lambda}$ 始终输出 $\perp$：对手只需将 $C = C^{(1)}\|\ldots\|C^{(d)}$ 变换为 $\tilde{C} = C_1^{(d)}\|C^{(1)}\|\cdots\|C^{(d-1)}\|C_0^{(d)}$，其中 $C_0^{(d)}, C_1^{(d)}$ 分别是 $C^{(d)}$的前半部分和后半部分。这意味着$\{(\mathsf{Enc}'_{H,\lambda}, \mathsf{Dec}_{H,\lambda})\}_\lambda$ 是一个满足 $\delta = 0$的插入删除抗腐化局部可解码码；也就是说，给定受损码字时，它总是输出 $\perp$。不过，我们可以利用 Block 等人 [BBG+20] 的带噪二分搜索技术来应对这种以及更一般的攻击。

带噪二分搜索概述：要理解含噪二分搜索算法 NBS 及其保证，我们需要引入 γ-良好的概念。对于 $x, y \in \{0,1\}^*$，如果 $\mathrm{ED}(x,y) \leqslant \gamma$，我们称 y相对于 x γ-良好。γ-良好的概念（尽管其正式定义有所不同）在深度鲁棒图的设计与分析中十分有用。深度鲁棒图是一种组合对象，在内存困难函数的研究中被广泛使用 [ABH17, ABP18, EGS75],，并且对 NBS 的成功至关重要。直观而言，对于固定的“正确”字符串有序列表 $A = (a_1, \ldots, a_n)$，其中每个字符串长度为 κ，以及另一个字符串列表 $B = (b_1, \ldots, b_{n'})$，NBS 算法能够找到任意一个相对于字符串 a_j 而言对$j \in [n]$ γ-良好的字符串 b_j，除非发生可忽略的概率事件。在我们的场景中，每个b_j 对应于（可能已损坏的）码字中的块。给定容忍参数 $\rho^* \in (0, 1/2)$, NBS 算法以 $j \in [n]$ 为输入，对至少占 $1-\rho^*$ 的γ-良好索引 j 中的比例输出 b_j，除非发生可忽略的概率事件。此外，NBS 的运行时间为 $\kappa \cdot \mathrm{polylog}(n')$；只有允许 NBS 在一小部分 γ-良好索引上失败，才能实现这一点，否则该算法需要 $\Omega(\kappa n')$ 的时间。

假设 $\tilde{C} \in \{0,1\}^{n'}$ 对于某个 n' 是一个受损码字（由适当的编码算法生成），并令 $i \in [k]$。我们使用 NBS 算法搜索 C，寻找某个（可能受损的）块 $\tilde{m}^{(j)}$，其中包含所需的符号 x_i。只要 $\tilde{C}$ 和 $\tilde{m}^{(j)}$ “没有过度受损”，NBS 就能以高概率输出 $\tilde{m}^{(j)}$。为进行搜索，NBS 使用块解码算法 Block Dec，在 $\tilde{C}$ 中查找 $\tilde{m}^{(j)}$，其保证如下：对于输入 i，如果 i 位于某个 γ-良好块 $\tilde{m}^{(j)}$附近的一个（较小）球内，那么 BlockDec 至少以 $1-\gamma$的概率输出 $\tilde{m}^{(j)}$。假设 $\tilde{m}^{(j)}$ 没有过度受损，我们可以将其解析为 $\tilde{x}^{(j)}\|\tilde{\sigma}^{(j)}\|\tilde{\mathrm{pk}}\|\tilde{j}$，并使用 Ver 确保 $\tilde{x}^{(j)}$ 正确。注意，NBS 和 BlockDec 都可能失败并输出 $\perp$，我们的解码器会将这一点考虑在内。

插删编码器：我们定义一族编码算法 $\{\mathsf{Enc}_{I,\lambda}\}_\lambda$。令 $\lambda \in \mathbb{N}$ 为安全参数，α 为 NBS 算法 [BBG+20]指定的常数。对于任意消息 $x \in \{0,1\}^k$，编码器 $\mathsf{Enc}_{I,\lambda}$ 的行为与 $\mathsf{Enc}_{H,\lambda}$ 完全相同：将 x 划分为 $d = \lceil x/r(\lambda)\rceil$ 个块，生成 $(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$，计算 $\sigma^{(j)} \leftarrow \mathsf{Sign}_{\mathrm{sk}}(x^{(j)}\|j)$，并为每个 j计算 $c^{(j)} = \mathsf{SZ.Enc}(x^{(j)}\|\sigma^{(j)}\|\mathrm{pk}\|j)$。接下来，编码器为每个 j计算缓冲码字 $C^{(j)} = 0^{\alpha r(\lambda)}\|c^{(j)}\|0^{\alpha r(\lambda)}$，其中 $0^{\alpha r(\lambda)}$ 是长度为 $\alpha r(\lambda)$ 的全零向量，并确保 NBS 和 BlockDec 算法成功。最后，$\mathsf{Enc}_{I,\lambda}$ 输出 $C = C^{(1)}\|\cdots\|C^{(d)}$。同样，如果 $r(\lambda) \geqslant k$，直接使用 SZ 码编码 x 会更高效。我们在算法 3 中给出正式的编码算法；此编码器与汉明编码器（算法 1）之间的任何差异都以蓝色标出，并附有行内注释。

算法 3： 插入删除编码器 $\mathsf{Enc}_{I,\lambda}$

输入：一条消息 $x \in \{0,1\}^k$。
输出：一个码字 $C \in \{0,1\}^K$。
硬编码： SZ 插入删除码；$r(\cdot)$ 长度签名方案 Π；$\alpha \in \mathbb{N}$；以及以一元表示给出的 $\lambda \in \mathbb{N}$。

采样 $(\mathrm{pk},\mathrm{sk}) \leftarrow$ 密钥生成算法(1^λ)
集合 $d = \lceil k/r(\lambda)\rceil$
分割 $x = x^{(1)}\|\cdots\|x^{(d)}$　　其中 $x^{(j)} \in \{0,1\}^{r(\lambda)}$
　对于每个 $j \in [d]$ （必要时填充最后一个块）
对每个 $j \in [d]$ **执行**　　// $\mathsf{Enc}_{H,\lambda}$ Diff
　$\sigma^{(j)} \leftarrow$签名$_{\mathrm{sk}}(x^{(j)}\|j)$
　$c^{(j)} =$SZ.Enc$(x^{(j)}\|\sigma^{(j)}\|\mathrm{pk}\|j)$
　$C^{(j)} = (0^{\alpha\cdot|\mathrm{ml}|}\|c^{(j)}\|0^{\alpha\cdot|\mathrm{ml}|})$ ；机器学习 $= |x^{(j)}\|\sigma^{(j)}\|$公钥$\|j|$
定义 $C := C^{(1)}\|\cdots\|C^{(d)} \in \{0,1\}^K$。
返回C

插入删除解码器：我们定义一族解码算法 $\{\mathsf{Dec}_{I,\lambda}\}_\lambda$。令 $\lambda \in \mathbb{N}$, $\mu \in \mathbb{N}$ 为我们选择的参数，$x \in \{0,1\}^k$, $C = \mathsf{Enc}_{I,\lambda}(x)$，且 $\tilde{C} \leftarrow \mathcal{A}(C)$ 满足 $\mathrm{ED}(C,\tilde{C}) \leqslant \rho$，其中 $\mathcal{A}$是一个概率多项式时间对手，且对于某个 K'，$\tilde{C} \in \{0,1\}^{K'}$。然后，在输入 $i \in [k]$并获得对 C的预言机访问后，解码器 $\mathsf{Dec}_{I,\lambda}$ 尝试通过与 $\mathsf{Dec}_{H,\lambda}$相同的两步过程恢复 x_i：首先，恢复公钥 pk；其次，找到预计包含 x_i 的块 j，并使用恢复出的 pk 验证其完整性。pk 的恢复方式与 $\mathsf{Dec}_{H,\lambda}$类似，但我们利用 BlockDec 查找可能包含公钥的块：先均匀随机采样$i_1, \ldots, i_\mu \xleftarrow{\$} [n]$，然后对每个 $\kappa \in [\mu]$获取 $\tilde{m}(j_\kappa) \leftarrow$BlockDec$(i_\kappa)$，其中 $j_\kappa \in [d]$。直观来说，在插入删除设置中，我们需要搜索每个块 j_κ；而在汉明设置中，我们确切知道每个块的位置。若 $\tilde{m}(j_\kappa) = \perp$，则我们设置 $\mathrm{pk}_\kappa = \perp$；否则，将 $\tilde{m}^{(j_\kappa)}$ 解析为 $\tilde{x}^{(j_\kappa)}\|\tilde{\sigma}^{(j_\kappa)}\|\tilde{\mathrm{pk}}(j_\kappa)\|\tilde{j}$，并设置 $\mathrm{pk}_\kappa = \tilde{\mathrm{pk}}(j_\kappa)$。最后，我们令 $\mathrm{pk}^* =$为 majority$(\mathrm{pk}1, \ldots, \mathrm{pk}_\kappa)$。接下来，$\mathsf{Dec}_{I,\lambda}$ 计算 j，使得 x_i 位于 $x^{(j)}$ 中，并获取 $\tilde{m}(j) \leftarrow$ NBS(j)。如果 $\tilde{m}(j)$ 或 pk^* 为 $\perp$，则 $\mathsf{Dec}_{I,\lambda}$ 中止并输出 $\perp$。否则，将 $\tilde{m}(j)$ 解析为 $\tilde{x}^{(j)}\|\tilde{\sigma}^{(j)}\|\tilde{\mathrm{pk}}(j)\|\tilde{j}$，然后 $\mathsf{Dec}_{I,\lambda}$ 检查 $\mathrm{Ver}_{\mathrm{pk}^*}(\tilde{x}^{(j)}\|j, \tilde{\sigma}^{(j)}) = 1$ 是否成立。若不成立，$\mathsf{Dec}_{I,\lambda}$ 输出 $\perp$；否则，$\mathsf{Dec}_{I,\lambda}$ 输出 $\tilde{x}_{i^*}^{(j)}$，其中 $x_i = x_{i^*}^{(j)}$。我们在算法 4 中给出形式化的解码算法；该编码器与汉明解码器（算法 2）之间的任何差异，均以蓝色标出并附有行内注释。

算法 4： 插入删除解码器 解码器[I, λ]

输入 ：一个索引 $i \in [k]$。
预言机 ：比特串 $\tilde{C} \in \{0,1\}^{K'}$ 对于某个 K'。
输出 ：一个符号 $\tilde{x} \in \{0,1\}$ 或 $\perp$。
硬编码： BlockDec 和 NBS； $r(\cdot)$ 长签名方案 Π；码长 K； $\lambda \in \mathbb{N}$ 在一元表示；以及 $\mu \in \mathbb{N}$。

集合 $d = \lceil k/r(\lambda) \rceil$
采样 $i_1, \ldots, i_\mu \xleftarrow{s} [n]$ // $\mathsf{Dec}_{\mathsf{H},\lambda}$ Diff
初始化 $\mathsf{pk}^*, \mathsf{pk}_1, \ldots, \mathsf{pk}_\mu = 0$
对于每个 $\kappa \in [k]$ **执行** // 解码器$_{\mathsf{H},\lambda}$ Diff
  $\tilde{m}^{(j_\kappa)} \leftarrow \mathsf{BlockDec}^{\tilde{C}}(i_\kappa)$
  若 $\tilde{m}^{(j_\kappa)} = \perp$ **则** st $\mathsf{pk}_\kappa = \perp$ **并 继续**
  解析 $\tilde{m}^{(j_\kappa)}$ 为 $\tilde{x}^{(j_\kappa)} \| \tilde{\sigma}^{(j_\kappa)} \| \tilde{\mathsf{pk}}^{(j_\kappa)} \| \tilde{j}$
  设 $\mathsf{pk}_\kappa = \tilde{\mathsf{pk}}^{(j_\kappa)}$
设 $\mathsf{pk}^* =$ 多数表决$(\mathsf{pk}_1, \ldots, \mathsf{pk}_\mu)$
计算 $j \in [d]$ 使得 $(j-1) \cdot r(\lambda) < i \leqslant j \cdot r(\lambda)$
$\tilde{m}^{(j)} \leftarrow \mathsf{NBS}^{\tilde{C}}(j)$ // 解码器$_{\mathsf{H},\lambda}$ Diff
如果 $\tilde{m}^{(j)} = \perp$ **或者** $\mathsf{pk}^* = \perp$ **则返回** $\perp$ // 解码器$_{\mathsf{H},\lambda}$ Diff
解析 $\tilde{m}^{(j)}$ 作为 $\tilde{x}^{(j)} \| \tilde{\sigma}^{(j)} \| \tilde{\mathsf{pk}}^{(j)} \| \tilde{j}$
如果 $\mathsf{Ver}_{\mathsf{pk}^*}(\tilde{x}^{(j)} \| j, \tilde{\sigma}^{(j)}) = 0$ **则返回** $\perp$
返回 $\tilde{x}^{(j)}_{i^*}$ 用于 $i^* = i - (j-1) \cdot r(\lambda)$

定理 2 的证明概述：我们对定理 2 的证明作高层次概述；完整细节见第 V 节。证明定理 2 的主要技术挑战在于证明 $\{(\mathsf{Enc}_\lambda, \mathsf{Dec}_\lambda)\}_\lambda$ 满足定义 1 中的条目 3 和条目 4。对于条目 3，给定任意 $x \in \{0,1\}^k$、概率多项式时间对手 $\mathcal{A}$以及 $i \in [k]$，我们分析概率，即对于满足 $\tilde{C}$ED$(C, \mathsf{Enc}_\lambda(x)) \leqslant \rho$ 的 $\tilde{C} \leftarrow \mathcal{A}(\mathsf{Enc}_\lambda(x))$，$\mathsf{Dec}^{\tilde{C}}_\lambda(i) \in \{x_i, \perp\}$。证明过程与汉明 crLDC 的证明完全相同，但有以下关键变化。首先，在恢复公钥时，我们必须在切尔诺夫界中考虑 BlockDec 的成功概率，以确保以高概率有 $\mathsf{pk}^* = \mathsf{pk}$。其次，在恢复包含 x_i 的块 j 时，我们必须考虑 NBS 的成功概率。仔细选择参数，并利用 BlockDec 和 NBS 的保证，即可确保条目 3 成立。

关于 条目 4，证明过程与汉明 抗腐化局部可解码码情形几乎完全相同，只是同样必须考虑通过 $\mathsf{BlockDec}^* =$ 恢复公钥 以及通过 BlockDec恢复块 j，再通过 NBS。带噪二分搜索算法以大于 γ 的概率恢复任意 $2/3$ -良好块（在适当选择参数的情况下），但失败概率可忽略不计。这直接转化为我们能够从中解码的索引比例 $\delta = 1 - \Theta(\rho)$，适用于 条目 4。

III. 预备知识

我们用 $\lambda \in \mathbb{N}$ 表示安全参数。对于任意 $n \in \mathbb{Z}^+$，我们令 $[n] := \{1, \ldots, n\}$。若函数 $\mu\colon \mathbb{N} \to \mathbb{R}_{\geqslant 0}$ 满足以下条件，则称其为可忽略函数：对于任意固定的非零多项式 p，$\mu(n) = o(1/|p(n)|)$。我们用 PPT 表示概率多项式时间。对于任意随机算法 A，我们用 $y \leftarrow A(x)$ 表示在输入 x时运行算法 A 并获得输出 y 的过程。对于有限集 S，我们用 $s \xleftarrow{s} S$ 表示从 S 中均匀随机抽取元素的过程。

我们用“$\|$”表示字符串拼接操作。对于比特串 $x \in \{0,1\}^*$，我们用下标表示 x 的各个位；例如，$x_i \in \{0,1\}$ 是 x 的第 i 位。此外，我们常常将比特串 $x \in \{0,1\}^k$ 分割成若干个等长的块 $x = x^{(1)} \| \cdots \| x^{(d)}$，$x^{(j)} \in \{0,1\}^{k/d}$；例如，$j \in [d]$，$(\,)$，其中对所有 。我们也会在方便时使用数组表示法：例如，对于比特串 $x \in \{0,1\}^k$ 和索引 a，$b \in [k]$，满足 $a \leqslant b$，我们令 $x[a,b] := (x_a \| x_{a+1} \| \cdots \| x_b)$。对于两个字符串 $x \in \{0,1\}^k$ 和 $y \in \{0,1\}^*$，我们将 ED(x, y) 定义为将 x 转换为 y （或反之）所需的最少插入和删除次数，再除以 $2k$。

在本文中，我们使用数字签名，并给出如下形式化定义。

定义 2（数字签名方案）。一个数字签名方案 的签名长度为 $r(\cdot)$，它是由以下概率多项式时间算法组成的元组： Π =（密钥生成算法,签名,Ver），并满足以下性质：

1）密钥生成算法 *Gen* 的输入为安全参数 1^λ，输出一对密钥 *(pk, sk)* $\in \{0,1\}^* \times \{0,1\}^*$，其中 *pk* 是公钥，*sk* 是秘密密钥。假设 $|pk|$、$|sk| \geqslant \lambda$ 均为 λ 的多项式，并且可以根据 *pk* 或 *sk* 高效地确定 λ。不失一般性，我们假设$|pk| = r(\lambda)$。*2*）签名算法 *Sign* 的输入为秘密密钥 *sk* 和任意长度的消息 $m \in \{0,1\}^*$，输出签名 $\sigma \leftarrow \mathit{Sign}_{\mathsf{sk}}(m) \in \{0,1\}^{r(\lambda)}$，其中 *Sign* 的运行时间为 *poly*$(|sk|, |m|)$。*3*）*Ver* 是确定性验证算法，其输入为公钥 *pk*、消息 m 和签名 σ，输出比特 $b = \mathit{Ver}_{\mathsf{pk}}(m, \sigma) \in \{0,1\}$。此外，*Ver* 的运行时间为 *poly*$(r(\lambda) \quad |m|)$。

*A*此外，我们要求满足以下两个性质：*1*）完备性：对于所有消息 $m \in \{0,1\}^*$ 以及所有(公钥，私钥) $\in \mathrm{supp}$(密钥生成算法(1^λ))，都有[1]*2*）安全性：对于所有概率多项式时间对手 $\mathcal{A}$，存在一个可忽略函数 $\varepsilon_\Pi(\cdot)$，使得对于所有 $\lambda \in \mathbb{N}$，都有，其中实验签名-伪造定义见图 *1*。

$$\Pr[\mathsf{Sig\text{-}forge}_{\Pi,\mathcal{A}}(\lambda) = 1] \leqslant \varepsilon_\Pi(\lambda),$$

为完整起见，我们也给出纠错码的经典定义。

[1]其他定义（例如， [KL14]）要求该条件在 (pk,sk) $\leftarrow$ 密钥生成算法(1^λ) 上的概率除可忽略概率外均成立。

签名实验 $\mathbf{Sign}_{\Pi,\mathcal{A}}(\lambda)$

1) 获取 (pk,sk) $\leftarrow$ 密钥生成算法(1^λ)。2) 对手 $\mathcal{A}$ 将 pk 作为输入，并可访问算法 $\mathsf{Sign}_{\mathsf{sk}}(\cdot)$ 的预言机。我们将其记为 $\mathcal{A}^{\mathsf{Sign}_{\mathsf{sk}}(\cdot)}(\mathsf{pk})$。令 Q 表示 $\mathcal{A}$ 向其预言机发出的所有查询所构成的集合。对手输出一对 (m,σ)。3) 仅当 a) $\mathsf{Ver}^{\mathsf{pk}^*}(m,\sigma)=1$；且 b) $m\notin Q$ 时，对手 $\mathcal{A}$ 才获胜。若 $\mathcal{A}$ 获胜，我们定义签名伪造$_{\Pi,\mathcal{A}}(\lambda):=1$；否则，我们定义签名伪造$_{\Pi,\mathcal{A}}(\lambda):=0$。

图 1. 签名伪造实验签名伪造的描述。

定义 *3.* 编码方案 $C[K,k,q_1,q_2]=$*(Enc, Dec)* 是一对编码与解码算法 *Enc:* $\Sigma_1^k\to\Sigma_2^K$和 *Dec :* $\Sigma_2^*\to\Sigma_1^k$，其中 $|\Sigma_i|=q_i$。码 $C[K,k,q_1,q_2]$是针对 $\rho\in[0,1]$ 且分数距离为 *dist* 的 *(ρ, dist)* 纠错码，当且仅当对于所有 $x\in\Sigma_1^k$ 和 $y\in\Sigma_2^*$，满足 *dist(Enc(x) y)* $\leqslant\rho$ 时，都有 *Dec(y)* $=x$。这里，ρ 是 C的错误率。如果 $q_1=q_2$，我们就简记为$C[K,k,q_1]$。如果 *dist* $=$ *HAM*，则 C 是汉明码；如果 *dist* $=$*ED*，则 C 是插入删除码（*InsDel* 码）。

我们构造的关键是所谓的“S Z码”，这是一种具有恒定码率和恒定纠错能力的插入删除纠错码。

引理 1 (SZ码 [SZ99])。存在正常数$\beta_{\mathsf{sz}}\leqslant 1$ 和 $\rho_{\mathsf{sz}}>0$，使得对于足够大的 $t\in\mathbb{Z}^+$，存在一个(ρ_{sz}, 编辑距离) 码$\mathsf{SZ}(t)=(\mathsf{SZ.Enc},\mathsf{SZ.}$解码器)，其中SZ.Enc: $\{0,1\}^t\to\{0,1\}^{(1/\beta_{\mathsf{sz}})\cdot t}$，且SZ.解码器: $\{0,1\}^*\to\{0,1\}^t\cup\{\perp\}$，满足以下性质：

1) SZ.Enc 和SZ.解码器 的运行时间为$\mathrm{poly}(t)$；以及 *2)* 对所有 $x\in\{0,1\}^t$，$\mathsf{Enc}(x)$ 中的任意长度为$2\log(t)$ 的区间，其相对汉明重量为 $\geqslant 2/5$。

当上下文明确时，我们省略参数 t。

IV. 定理证明定理 1

本节将证明 $\mathcal{C}_{\mathsf{H},\lambda}=\{($编码器$_{\mathsf{H},\lambda}$,解码器$_{\mathsf{H},\lambda})\}_{\lambda\in\mathbb{N}}$ 满足定理 1，其中 编码器$_{\mathsf{H},\lambda}$ 和解码器$_{\mathsf{H},\lambda}$ 分别定义于 算法 1 和2中。下面回顾该定理。

定理 1。设 Π 是一个 $r:=r(\lambda)$ 长度的签名方案。设 C_{in} 是一个码率为 β_{in}、错误率为 ρ_{in}的二元汉明码。那么，对于每个正多项式 $k(\cdot)$和常数 $c\in(0,1/2)$，存在一个码族$\mathcal{C}_{\mathsf{H}}:=\{C_{\mathsf{H},\lambda}[K,k(\lambda)\ 2]\}_{\lambda\in\mathbb{N}}$ 以及函数 $\mu:=\mu(\lambda)$ 使得 $\mathcal{C}_{\mathsf{H}}$ 是一个 (ℓ,ρ,p,δ)- 汉明抗腐化局部可解码码，且

- $K=O((1/\beta_{in})\max\{k(1+\log(k)/r)\ r\})$,
- $\ell=O((\mu/\beta_{in})\cdot(r+$对数$(k)))$,
- $\rho=c\cdot\rho_{in}$,
- $p=1-\exp(-\mu(1/2-c)^2/2(1-c))>2/3$，以及
- $\delta=1/2$,

其中 $k:=k(\lambda)$。

证明。首先注意，根据构造，$x^{(j)}$，$\sigma^{(j)}\in\{0,1\}^{r(\lambda)}$以及 $j\in\{0,1\}^{\log(d)}$。此外，不失一般性地，我们假设 $\mathsf{pk}\in\{0,1\}^\lambda$且 $r(\lambda)\geqslant\lambda$。注意我们还有 $\log(d)=O(\log(k))$。因此，如果 C_{in} 的码率为β_{in}，那么我们的码的码长 K 恰好是

$$\begin{aligned}K&=d\cdot(1/\beta_{in})\cdot(2r(\lambda)+\lambda+\log(d))\\&=(\lceil k/r(\lambda)\rceil)\cdot(1/\beta_{in})\cdot(2r(\lambda)+\lambda+\log(\lceil k/r(\lambda)\rceil))\\&=O((1/\beta_{in})\cdot k\cdot(3+\log(k)/r(\lambda)))\\&=O((1/\beta_{in})\cdot k(1+\log(k)/r(\lambda)))\end{aligned}$$

当 $k\geqslant r(\lambda)$ 时。如果 $r(\lambda)>k$，那么我们在输入消息 x 的末尾填充 $k-r(\lambda)$ 个 0，从而得到一个长度为 $r(\lambda)$ 的字符串，这将形成一个长度为...的单一码字块。

$$\begin{aligned}K&=(1/\beta_{in})\cdot(2r(\lambda)+\lambda+1)\\&=O((1/\beta_{in})\cdot r(\lambda)).\end{aligned}$$

由此，我们得到了指定的码长。

$$K=O((1/\beta_{in})\cdot\max\{k\cdot(1+\log(k)/r(\lambda)),r(\lambda)\}).$$

对于局部性 ℓ，根据构造可知，任意块 j的长度为

$$\begin{aligned}&(1/\beta_{in})\cdot(2r(\lambda)+\lambda+\log(d))\\&=(1/\beta_{in})\cdot(2r(\lambda)+\lambda+\log(k)-\log(r(\lambda)))\\&=O((1/\beta_{in})\cdot(r(\lambda)+\log(k))).\end{aligned}$$

由于我们解码 $\mu+1$ 块，因此总局部性为

$$\ell=O((\mu/\beta_{in})\cdot(r(\lambda)+\log(k))).$$

此外，解码器$_{\mathsf{H},\lambda}$对 $O((\mu/\beta_{in})\cdot(r(\lambda)+\log(k)))$ 在任意输入上向其预言机发起查询 i，满足条目 1 和定义 1。

对于条目 Item 2，假设 $\mathsf{Dec}_{\mathsf{H},\lambda}$ 可通过预言机访问 $\tilde{C}=C$，其中给定某个 $C=\mathsf{Enc}_{\mathsf{H},\lambda}(x)$ 和 $x\in\{0,1\}^k$。接下来我们分析，对于任意 $i\in[k]$，$\mathsf{Dec}^{C}_{\mathsf{H},\lambda}(i)=x_i$ 的概率。首先，由于 C 是一个正确的码字，公钥恢复成功的概率为 1。也就是说，对于每个 $\kappa\in[\mu]$，在第 5 行恢复的字符串 $\tilde{m}(j_\kappa)\leftarrow\mathsf{Dec}_{in}(C[(j_\kappa-1)\cdot\mathsf{bl}+1,j_\kappa\cdot\mathsf{bl}])$ 等于 $x^{(j_\kappa)}\|\sigma^{(j_\kappa)}\|\mathsf{pk}\|j_\kappa$（即所有内容均正确）。此处，$\mathsf{bl}=n/d$ 是 $C=C^{(1)}\|\cdots\|C^{(d)}$中每个块 $C^{(j)}$的长度。因此，$\mathsf{pk}^*=\mathsf{pk}$ 的概率为 1。现在固定 $j\in[d]$ 为这样一个块：位 x_i 位于 $x^{(j)}$中。根据上述讨论，我们知道在第 10 行恢复的 $\tilde{m}^{(j)}$ 是正确的，并且解析为 $x^{(j)}\|\sigma^{(j)}\|\mathsf{pk}\|j$。结合 $\mathsf{pk}^*=\mathsf{pk}$ 这一事实可知，第 12 行以概率 0 为真（即 $\mathsf{Ver}^{\mathsf{pk}^*}(x^{(j)}\|j,\sigma^{(j)})=1$ 的概率为 1）。这意味着 $\mathsf{Dec}^{C}_{\mathsf{H},\lambda}(i)=x_i$ 的概率为 1。

对于错误率，令 $\rho_{in}\in(0,1)$ 为 C_{in} 的错误率。直观地说，我们希望将最终错误率 ρ 设定为：对于任意 ρ 比例的篡改，包含超过 ρ_{in} 比例错误的块少于 d 块的一半。等价地，超过一半的 d 块至多包含 ρ_{in} 比例的错误。

处错误。令 bl 表示码字C中一个块的长度。若 $\widetilde{}$中至少有 $\rho_{in}\mathsf{bl}+1$ 个错误，则 Dec_{in} 无法正确解码任何块 $j\in[d]$。令 $J\subset[d]$ 为索引 $\widetilde{}$的集合，其中块 $j\in J$ 至少有 $\rho_{in}\mathsf{bl}+1$ 个汉明错误。那么我们有

$$|\widetilde{J}|\cdot(\rho_{in}\mathsf{bl}+1)\leqslant\rho\cdot d\cdot\mathsf{bl}\ (=\rho K),$$

这意味着

$$\begin{aligned}|\widetilde{J}|&\leqslant(\rho\cdot d\cdot\mathsf{bl})/(\rho_{in}\mathsf{bl}+1)\\&<(\rho\cdot d\cdot\mathsf{bl})/(\rho_{in}\mathsf{bl})\\&=\rho d/\rho_{in}.\end{aligned}$$

$\widetilde{}$我们希望 $|J|<d/2$ 确保超过一半的块至多包含 ρ_{in} 个错误。令$(d\rho)/\rho_{in}<d/2$ 意味着$\rho<\rho_{in}/2$。因此，对于任意常数$c\in(0,1/2)$，我们令 $\rho=c\cdot\rho_{in}=\Theta(\rho_{in})$。

接下来，我们分析成功概率 p 和条目 3。对于谓词 Fool，固定消息 x，并令 $C=\mathsf{Enc}_{\mathsf{H},\lambda}(x)$。我们希望证明：对于所有概率多项式时间算法 $\mathcal{A}$，都存在一个可忽略函数ε_{F}，使得对于所有 λ 和 $x\in\{0,1\}^k$，有

$$\Pr[\mathsf{Fool}(\tilde{C},\rho,p,x,C,\lambda)=1]\leqslant\varepsilon_{\mathsf{F}}(\lambda)$$

$\widetilde{}$对于 $C\leftarrow\mathcal{A}(C)$。等价地，我们希望证明

$$\Pr[\exists i\in[k]\colon\Pr[\mathsf{Dec}^{\tilde{C}}_{\mathsf{H},\lambda}(i)\in\{x_i,\perp\}]<p]\leqslant\varepsilon_{\mathsf{F}}(\lambda)$$

$\widetilde{}$对于 $C\leftarrow\mathcal{A}(C)$，使得 $\mathrm{HAM}(C,C)\leqslant\rho$。换言之，我们希望证明

$$\Pr[\forall i\in[k]\colon\Pr[\mathsf{Dec}^{\tilde{C}}_{\mathsf{H},\lambda}(i)\in\{x_i,\perp\}]\geqslant p]\geqslant1-\varepsilon_{\mathsf{F}}(\lambda).$$

我们分析 $\mathsf{Dec}^{C}_{\mathsf{H},\lambda}(i)\in\{x_i,\perp\}$ 的概率，并令E_i表示该事件；同时令 Frg_i 表示 $\mathcal{A}$ 生成签名伪造$(\tilde{x}^{(j)}\|j,\ \tilde{\sigma}^{(j)})$的事件，其中 $j\in[d]$ 满足$(j-1)\cdot r(\lambda)<i\leqslant j\cdot r(\lambda)$，且 $\tilde{x}^{(j)}$ 和 $\tilde{\sigma}^{(j)}$ 由 $\mathsf{Dec}_{\mathsf{H},\lambda}$ 恢复。于是有 $\Pr[E_i]=\Pr[E_i|\mathsf{Frg}_i]$。注意，解码器不可能同时输出 $\perp$ 和 x_i。令$E_i(x)$表示 $\mathsf{Dec}^{C}_{\mathsf{H},\lambda}(i)=x$ 对于符号 x的事件，则有

$$\Pr[E_i\mid\overline{\mathsf{Frg}_i}]=\Pr[E_i(x_i)\mid\overline{\mathsf{Frg}_i}]+\Pr[E_i(\perp)\mid\overline{\mathsf{Frg}_i}].$$

分析 $\Pr[E_i(x_i)|\mathsf{Frg}_i]$，由于我们假设 $(\tilde{x}^{(j)}\|j,\tilde{\sigma}^{(j)})$ 不是伪造，因此必有

1) $\tilde{x}^{(j)}=x^{(j)}$ and $\tilde{\sigma}^{(j)}=\sigma^{(j)}$; and
2) $\mathsf{Ver}_{\mathsf{pk}^*}(\tilde{x}^{(j)}\|j,\tilde{\sigma}^{(j)})=1$.

现在，只有当 $\mathsf{pk}^*=\mathsf{pk}$ 时，此验证才会成功，这意味着

$$\Pr[E_i(x_i)\mid\overline{\mathsf{Frg}_i}]=\Pr[\mathsf{pk}^*=\mathsf{pk}].$$

接下来我们分析 $\Pr[E_i(\perp)|\overline{\mathsf{Frg}_i}]$。注意，只有当 $\mathsf{Ver}_{\mathsf{pk}^*}(\tilde{x}^{(j)}\|j,\tilde{\sigma}^{(j)})=0$ 时，$\mathsf{Dec}_{\mathsf{H},\lambda}$ 才会输出 $\perp$。令 $\mathcal{E}_1$ 表示事件 Frg_i，$\mathcal{E}_2$ 表示事件 $\tilde{x}^{(j)}\neq x^{(j)}$，$\mathcal{E}_3$ 表示事件 $\tilde{\sigma}^{(j)}\neq\sigma^{(j)}$，并令 $\mathcal{E}_4$ 表示事件 $\mathsf{pk}^*=\mathsf{pk}$。然后，我们对上述概率给出如下下界：

$$\Pr[E_i(\perp)|\overline{\mathsf{Frg}_i}]\geqslant\Pr\left[\mathsf{Ver}_{\mathsf{pk}^*}(\tilde{x}^{(j)}\|j,\tilde{\sigma}^{(j)})=0\,\middle|\,\begin{array}{l}\mathcal{E}_1\ \wedge\\(\mathcal{E}_2\ \vee\ \mathcal{E}_3)\ \wedge\\\mathcal{E}_4\end{array}\right]\cdot\Pr[\mathcal{E}_4].$$

由于我们假设 $\overline{\mathsf{Frg}_i}$ 为真（即 $\mathcal{E}_1$ 为真），因此可知

$$\Pr\left[\mathsf{Ver}_{\mathsf{pk}^*}(\tilde{x}^{(j)}\|j,\tilde{\sigma}^{(j)})=0\,\middle|\,\begin{array}{l}\mathcal{E}_1\ \wedge\\(\mathcal{E}_2\ \vee\ \mathcal{E}_3)\ \wedge\\\mathcal{E}_4\end{array}\right]=1.$$

这意味着

$$\Pr[E_i(\perp)\mid\mathcal{E}_1]\geqslant\Pr[\mathcal{E}_4]=\Pr[\mathsf{pk}^*=\mathsf{pk}],$$

这意味着

$$\Pr[E_i\mid\overline{\mathsf{Frg}_i}]\geqslant2\cdot\Pr[\mathsf{pk}^*=\mathsf{pk}]\geqslant\Pr[\mathsf{pk}^*=\mathsf{pk}].$$

现在我们分析 $\Pr[\mathsf{pk}^*=\mathsf{pk}]$。令 pk 为 $\mathsf{Enc}_{\mathsf{H},\lambda}(x)$ 为生成 C 而采样得到的公钥。根据我们的参数选择$c\in(0,1/2)$，至少 $(1-c)d>d/2$ 个块的 C' 中，汉明错误所占比例至多为 ρ_{in}。令 $\mathsf{bl}=K/d$ 表示 C 中任意块的长度，并令 $\mathcal{J}$ 表示汉明错误所占比例至多为 ρ_{in} 的块的集合。那么

$$x^{(j)}\|\sigma^{(j)}\|\mathsf{pk}\|j=\mathsf{Dec}_{in}(\tilde{C}[(j-1)\cdot\mathsf{bl}+1,j\cdot\mathsf{bl}])$$

对任意 $j\in\mathcal{J}$；也就是说，这是一次正确解码，因为受损码字 $\tilde{C}^{(j)}=\tilde{C}[(j-1)\cdot\mathsf{bl}+1,\ j\cdot\mathsf{bl}]$ 位于 C_{in}的唯一译码半径内。定义随机变量 X_κ，对于 $\kappa\in[\mu]$，其定义为

$$X_\kappa:=\begin{cases}1 & x^{(j)}\|\sigma^{(j)}\|\mathsf{pk}\|j=\mathsf{Dec}_{in}(\tilde{C}[(j-1)\mathsf{bl}+1,j\mathsf{bl}])\\0 & \text{otherwise}\end{cases}.$$

Then

$$\begin{aligned}&\Pr[X_\kappa=1]\\&=\Pr\left[x^{(j)}\|\sigma^{(j)}\|\mathsf{pk}\|j=\mathsf{Dec}_{in}(\tilde{C}[(j-1)\cdot\mathsf{bl}+1,j\cdot\mathsf{bl}])\right]\\&=\Pr[j_\kappa\in\mathcal{J}_{\mathsf{Good}}]\\&\geqslant(1-c)>1/2.\end{aligned}$$

令 $q=(1-c)>1/2$。根据切尔诺夫界，我们有

$$\Pr\left[\sum_{\kappa\in[\mu]}X_\kappa>\frac{\mu}{2}\right]\geqslant1-\exp(-\mu\cdot(q-1/2)^2/(2q)).$$

这意味着其概率至少为

$$p:=1-\exp(-\mu\cdot(q-1/2)^2/(2q)),$$

我们有 $\mathsf{pk}^*=\mathsf{pk}$。因此

$$\Pr[E_i\mid\overline{\mathsf{Frg}_i}]\geqslant p.$$

在上述分析过程中，我们只假设没有发生伪造。对于任意的 i，发生 Frg_i 的概率至少为 $1-\varepsilon_{\Pi}(\lambda)$，其中 $\varepsilon_{\Pi}(\cdot)$ 是一个可忽略函数

该函数取决于数字签名方案 Π 的安全性。因此，对所有 i 应用并集界，我们得到

$$\Pr[\exists i \in [k]\colon \Pr[\mathsf{Dec}^{\tilde{C}}_{\mathsf{H},\lambda}(i) \in \{x_i, \perp\}] < p] \geqslant k \cdot \varepsilon_{\Pi}(\lambda).$$

令 $\varepsilon_{\mathsf{F}}(\lambda)\colon = k \cdot \varepsilon_{\Pi}(\lambda)$，我们有 $\varepsilon_{\mathsf{F}}(\lambda)$ 在λ中是可忽略的，因为 $k(\lambda)$ 是一个多项式，这证明了 条目 3。

最后，我们分析 δ 和 条目 4。根据我们对 $\rho = c \cdot \rho_{in}$的选择，我们知道，对于 任意 $\tilde{C} \in \{0,1\}^n$ 满足 $\mathsf{HAM}(\tilde{C}, C) \leqslant \rho$，至少有 $(1-c)\cdot d$ 块 C 中至多包含 ρ_{in}比例的汉明错误。再次令 $\mathcal{J} \subset [d]$ 表示这些块的索引，我们有 $|\mathcal{J}| > d/2$。对于 $\mathsf{bl} = K/d$，这再次意味着

$$x^{(j)} \| \sigma^{(j)} \| \mathsf{pk} \| j = \mathsf{Dec}_{in}(\tilde{C}[(j-1)\cdot \mathsf{bl} + 1, j \cdot \mathsf{bl}])$$

对于任意 $j \in \mathcal{J}$，这意味着对于任意 $j \in \mathcal{J}$，我们有

$$\Pr[\mathsf{Dec}^{\tilde{C}}_{\mathsf{H},\lambda}(i) = x_i | \mathsf{pk}^* = \mathsf{pk}] = 1$$

每当 $(j-1)\cdot r(\lambda) < i \leqslant j \cdot r(\lambda)$ 时。因此，对于任意 $j \in \mathcal{J}$ 和 $i \in [k]$，只要 $(j-1)\cdot r(\lambda) < i \leqslant j \cdot r(\lambda)$，根据切尔诺夫界，我们有

$$\begin{aligned}\Pr[\mathsf{Dec}^{\tilde{C}}_{\mathsf{H},\lambda}(i) = x_i] &= \Pr[\mathsf{pk}^* = \mathsf{pk}] \\ &\geqslant 1 - \exp(-\mu \cdot (1/2 - c)^2/2(1-c)).\end{aligned}$$

通过对 μ 进行适当选择，我们可以确保

$$1 - \exp(-\mu \cdot (1/2-c)^2/2(1-c)) > 2/3.$$

最后，我们注意到集合

$$\mathcal{I} := \{i \in [k]\colon j \in \mathcal{J} \ \wedge \ (j-1)\cdot r(\lambda) < i \leqslant j \cdot r(\lambda)\}$$

大小为 $|\mathcal{I}| > k/2$。因此我们可以设定 $\delta = 1/2$。

这里我们已经证明，对于任意 $\tilde{C} \in \{0,1\}^n$，只要满足 $\mathsf{HAM}(C, \tilde{C}) \leqslant \rho$，就存在一个集合 $\mathsf{Good}(C) := \mathcal{I}$，使得 $|\mathcal{I}| \geqslant \delta \cdot k$。这对任意 C 都成立，尤其适用于概率多项式时间对手能够生成的任意受损码字。因此，对于任意概率多项式时间对手 $\mathcal{A}$、任意 $x \in \{0,1\}^k$，以及 $C = \mathsf{Enc}_{\mathsf{H},\lambda}(x)$，我们有

$$\Pr[\mathsf{Limit}(\mathcal{A}(C), \rho, \delta, x, C, \lambda) = 1] = 0.$$

□

V. 定理 2 的证明

本节旨在证明$\mathcal{C}_{\mathsf{I},\lambda} = \{(\mathsf{Enc}_{\mathsf{I},\lambda}, \text{解码器}_{\mathsf{I},\lambda})\}_{\lambda \in \mathbb{N}}$ 满足定理 2，其中$\mathsf{Enc}_{\mathsf{I},\lambda}$ 和解码器$_{\mathsf{I},\lambda}$ 分别定义于算法 3 和 4中。下面我们重述该定理。

定理 2。 设 Π 是一个 $r := r(\lambda)$ 长度的签名方案。存在常数 $c \in (0, 1/2)$，使得对于每个正多项式 $k(\cdot)$ 和常数 $\rho^* \in (0, 1/3)$，都存在一个码族 $\mathcal{C}_{\mathsf{Ins}} := \{C_\lambda[K, k(\lambda)\ 2]\}_{\lambda \in \mathbb{N}}$ 以及一个函数 $\mu := \mu(\lambda)$，使得 $\mathcal{C}_{\mathsf{Ins}}$ 是一个(ℓ, ρ, p, δ)-*InsDel* 抗腐化局部可解码码，且

- $K = O(\max\{k(1 + \log(k)/r)\ r\})$,
- $\ell = O((\log^3(K) + \mu) \cdot (r + \log(k)))$,
- $\rho = \Theta(1)$,
- $p = 1 - \rho^* - \exp(-\mu(1/2-c)^2/2(1-c)) > 2/3$，以及
- $\delta = 1 - \Theta(\rho)$,

其中 $k := k(\lambda)$。

证明。 任取 $x \in \{0,1\}^k$，并令 $C = \mathsf{Enc}_{\lambda}(x)$。根据 Enc_{λ} 的定义，我们知道对于 $d = \lceil k/r(\lambda) \rceil$，有 $C = C^{(1)} \| \cdots \| C^{(d)}$。首先假设 $k \geqslant r(\lambda)$。每个块 $C^{(j)}$都是 $x^{(j)} \| \sigma^{(j)} \| \mathsf{pk} \| j$ 的 SZ 编码，并在前后附加零缓冲区。注意， j 的比特长度为 $\log(d) = \log(k/r(\lambda)) \leqslant \log(k)$；为简单起见，我们假设（否则可以填充至长度 $\log(k)$）。于是我们有 $\tau := |x^{(j)} \| \sigma^{(j)} \| \mathsf{pk} \| j| = 3 \cdot r(\lambda) + \log(k)$。由此可得 $|c^{(j)}| = \tau/\beta_{\mathsf{sz}}$，并且

$$\begin{aligned}|C^{(j)}| &= 2\alpha\tau + \tau/\beta_{\mathsf{sz}} \\ &= (2\alpha + (1/\beta_{\mathsf{sz}}))\tau.\end{aligned}$$

最后，这给出

$$\begin{aligned}|C| = K &= d \cdot (2\alpha + (1/\beta_{\mathsf{sz}})) \cdot \tau \\ &= \left(\frac{k}{r(\lambda)}\right) \cdot (2\alpha + (1/\beta_{\mathsf{sz}})) \cdot (3 \cdot r(\lambda) + \log(k)) \\ &= O\left(k \cdot \left(1 + \frac{\log(k)}{r(\lambda)}\right)\right),\end{aligned}$$

其中，最后一个等号成立是因为 $\alpha, \beta_{\mathsf{sz}}$ 是常数。注意，只要对所有 $t \geqslant \log(k)$ 都存在 $\mathsf{SZ}(t)$，k 就足够大。现在，只要 $r(\lambda) > k$，我们就有 $d = 1$，并且只需对一个长度为 τ 的块进行签名和编码，从而得到一个长度为

$$\begin{aligned}(2\alpha + (1/\beta_{\mathsf{sz}}))\tau &= (2\alpha + (1/\beta_{\mathsf{sz}})) \cdot (3r(\lambda) + \log(k)) \\ &= \Theta(r(\lambda))\end{aligned}$$

因为 $r(\lambda) > k$，且 $\alpha, \beta_{\mathsf{sz}}$ 是常数。因此我们有

$$K = O(\max\{k(1 + \log(k)/r(\lambda)), r(\lambda)\}).$$

在证明的其余部分，令 $\beta := (2\alpha + (1/\beta_{\mathsf{sz}}))$ 并令 $\tilde{C} \in \{0,1\}^{K'}$，使得 编辑距离$(C, \tilde{C}) \leqslant \rho$。我们引入一些预备定义（定义 4 至 5）和引理引理 2 至 5），它们由 Block 等人提出， [BBG+20]，并用于证明。

定义 4。 （可能被篡改的）码字 $\tilde{C} \in \{0,1\}^{K'}$ 的块分解是一个非递减映射 $\phi\colon [K'] \to [d]$，其中 K'、$d \in \mathbb{N}$。

对于任意分块分解 ϕ，由于 ϕ 是一个非递减映射，我们有，对于任意 $j \in [d]$，$\phi^{-1}(j)$ 是一个区间。也就是说，对于整数 $l_j, r_j \in [K']$ 和 $l_j \leqslant r_j$，$\phi^{-1}(j) = \{l_j, l_j+1, \ldots, r_j\}$。因此，$\phi$ 将 $[K']$ 分割为 d 个形如 $\{\phi^{-1}(j)$ 的区间：$j \in [d]\}$。回顾一下，$C = \mathsf{Enc}_{\lambda}(x)$ 具有 $C^{(1)} \| \cdots \| C^{(d)}$ 的形式，我们有如下结论。

引理 2。 存在一个分块分解 $\phi_0\colon [K'] \to [d]$使得

$$\sum_{j \in [d]} \mathsf{ED}\left(\tilde{C}[\phi_0^{-1}(j)], C^{(j)}\right) \leqslant \rho\,. \tag{1}$$

直观地说，引理 2表明，存在一个分块分解，使得 C' 与 C' 之间的总编辑距离恰好等于（可能已损坏的）块 $\tilde{C}[\phi_0^{-1}(j)]$ 与块 $C^{(j)}$之间编辑距离之和。接下来我们定义 γ-良好块的概念。

定义 5. 对于 $\gamma \in (0, 1)$ 和 $j \in [d]$，若块 j 相对于分块分解 ϕ 是 γ-良好的，则称其为良好块；若编辑距离 $(\tilde{C}[\phi^{-1}(j)], C^{(j)}) \leqslant \gamma$。否则，称块 j 为 γ-坏块。

对于分块分解 ϕ_0，γ-坏块的数量有界，并且对于每个 γ-良好块 j，区间 $\phi_0^{-1}(j)$ 的长度有界。

引理 3. 令 α 为引理 *4* 给出的常数，令 β_{sz} 为引理 *1* 给出的常数，且令 $\beta = (2\alpha + (1/\beta_{\mathsf{sz}}))$。

1）C 中 γ-坏块所占的总比例至多为 $2 \cdot \beta \cdot \rho/(\gamma \cdot \alpha)$。*2*）对于任意 γ-良好块 j，有 $(\beta - \alpha\gamma) \cdot \tau \leqslant |\phi_0^{-1}(j)| \leqslant (\beta + \alpha\gamma) \cdot \tau$，其中 $\tau = |x^{(j)} \| \sigma^{(j)} \| \mathsf{pk} \| j|$。

给定 γ-良好的概念后，我们现在可以正式介绍算法 NBS 和 BlockDec 及其保证。

引理 *4.* 令 ρ_{sz} 为引理 *1* 给出的常数。存在常数 $\alpha = \Omega(\rho_{\mathsf{sz}})$ 以及一个具有以下性质的随机化预言机算法 *NBS*。令 $\rho^* \in (0, 1/2)$ 为固定常数，令 t 足够大，d 为参数，令 $b = (b^{(1)}, \ldots, b^{(d)}) \in \{0,1\}^t$ 为任意字符串，其中对所有 $i \in [d]$ 均有 $b^{(i)} \in \{0,1\}^{t/d}$，并令 $c = (c^{(1)}, \ldots, c^{(d)})$ 为

$$c^{(i)} = 0^{\alpha(t/d)} \| \mathsf{SZ.Enc}(b^{(i)} \| i) \| 0^{\alpha(t/d)}$$

对所有 $i \in [d]$ 均成立。则存在一个可忽略函数 $\vartheta(\cdot)$，使得对于满足 $\mathsf{ED}(c, c') \leqslant \rho = \Theta(\rho^* \cdot \rho_{\mathsf{sz}})$ 的任意 $c' \in \{0,1\}^{K'}$，我们有

$$\Pr[\Pr[\mathsf{NBS}^{c'}(j) \neq b^{(j)} \mid j \text{ is } \gamma\text{-good}] \geqslant \rho^*] \leqslant \vartheta(n'), \quad (2)$$

其中概率取自NBS 和 $j \xleftarrow{s} [d]$的随机硬币。此外，对于任意输入$j \in [d]$，算法 NBS 进行 O(对数$^3(K') \cdot (t/d +$ 对数$(d))$) 次预言机查询，并且如果 $c = c'$，则上述概率为0。

引理 5。 设 ρ_{sz} 为 引理 *1*给出的常数。存在常数 $\alpha = \Omega(\rho_{\mathsf{sz}})$ 以及随机化预言机算法BlockDec，具有以下性质。设 $\rho^* \in (0, 1/2)$ 为一个固定常数，设 t 足够大，设 d 为一个参数，设 $b = b^{(1)} \ldots b^{(d)} \in \{0,1\}^t$ $b^{(i)} \in (,,)$ 为 $\{0,1\}^{t/d}$ $i \in [d]$ $c = c^{(1)} \ldots c^{(d)}$ 任意一个字符串，其中对所有，均有，并设 $(,,)$ 对于

$$c^{(i)} = 0^{\alpha(t/d)} \| \mathsf{SZ.Enc}(b^{(i)} \| i) \| 0^{\alpha(t/d)}$$

对所有 $i \in [d]$ 均成立。因此，对于任意满足 编辑距离$(c, c') \leqslant \rho = \Theta(\rho^* \cdot \rho_{\mathsf{sz}})$ 的 $c' \in \{0,1\}^{n'}$，我们有

1) 对任意 γ-良好块 $j \in [d]$:

$$\Pr_{i \in \phi_0^{-1}(j)} \left[\mathsf{BlockDec}^{c'}(i) \neq b^{(j)} \right] \leqslant \gamma\,. \quad (3)$$

此外，如果 $c' = c$，该概率等于零。*2)* BlockDec 的查询复杂度为 $O(t/d + \log(d))$。

现在我们已有完成定理 2证明所需的各项要素。我们首先证明定义 1中的条目 2。令 $x \in \{0,1\}^k$, $C = \mathsf{Enc}_\lambda(x)$，并令 (pk,sk) 为 $\mathsf{Enc}_{\tilde{}}$ ı λ x ,在将 as C编码期间采样的公私钥对。假设 $C = C$，并令 $i \in [k]$ 为任意索引。我们 ~要证明 $\Pr[$解码器^{C} ,λ(*i*) $= x_i] = 1$。为此，首先注意，对于 $(j-1) \cdot r(\lambda) < i \leqslant j \cdot r(\lambda)$，我们有

$$\Pr[\mathsf{Dec}^{\tilde{C}}_{\mathsf{I},\lambda}(i) = x_i]$$
$$= \Pr[\mathsf{pk}^* = \mathsf{pk}] \cdot \Pr[\tilde{x}^{(j)} = x^{(j)}] \cdot \Pr[\tilde{\sigma}^{(j)} = \sigma^{(j)}],$$

其中 $x^{(j)}$ 是 j的第 x 块，$\sigma^{(j)}$ 是 $x^{(j)} \| j$ 的签名，pk^* 是通过多数表决恢复的公钥，且 $\tilde{x}^{(j)}$、$\tilde{\sigma}^{(j)}$ 是从 $\mathsf{NBS}(j)$ 的输出中解析得到的。首先注意到，由于~ ~$C = C$，每个 $j \in [d]$ 块 C 均相对于 0-良好 C。根据 引理 5，对于每个 $j \in [d]$，我们有

$$\Pr_{i \in \phi_0(j)} \left[\mathsf{BlockDec}^{\tilde{C}}(i) = C^{(j)} \right] = 1.$$

这意味着对于每个 $\kappa \in [\mu]$，我们有

$$\Pr[\mathsf{pk}^{(i_\kappa)} = \mathsf{pk}] = 1,$$

这意味着

$$\Pr[\mathsf{pk}^* = \mathsf{pk}] = 1.$$

~接下来，由于 $C = C$ 根据 引理 4，我们有

$$\Pr_{\tilde{m}^{(j)} \leftarrow \mathsf{NBS}^{\tilde{C}}(j)} \left[\tilde{m}^{(j)} = x^{(j)} \| \sigma^{(j)} \| \mathsf{pk} \| j \right] = 1.$$

这意味着 $\mathsf{Ver}_{\mathsf{pk}^*}(x^{(j)} \| j,\ \sigma^{(j)}) = 1$ 以概率 1，

~ 从而得到 概率[解码器^{C}, λ(*i*) $= x_i] = 1$。

我们现在着手证明条目 3 和4。设 $\mathcal{A}$ 为一个概率多项式时间对手，并设 $\tilde{C} \leftarrow \mathcal{A}\ C$ $\tilde{C} \in \{0,1\}^{K'}$ ( )，使得对某个 K' 和 编辑距离$(C,\ C) \leqslant \rho$成立。我们先证明条目 3。令 D_i :=解码器^{C}, λ(*i*) 表示以 i 为输入、以 C为预言机运行~解码器所得的随机变量。我们的目标是证明

$$\Pr[\exists i \in [k]\colon \Pr[D_i \in \{x_i, \perp\}] < p] \leqslant \varepsilon_{\mathsf{F}}(\lambda),$$

其中 $\varepsilon_{\mathsf{F}}(\lambda)$ 是某个可忽略函数。等价地说，我们要证明

$$\Pr[\forall i \in [k]\colon \Pr[D_i \in \{x_i, \perp\}] \geqslant p] \geqslant 1 - \varepsilon_{\mathsf{F}}(\lambda).$$

现在我们直接分析概率$[D_i \in \{x_i, \perp\}]$。这里的分析与定理 1的分析几乎相同，只是现在必须考虑算法BlockDec和NBS。令Frg_i 表示事件：$\mathcal{A}$ 产生一个签名伪造($\tilde{x}^{(j)} \| j$ $\tilde{\sigma}^{(j)}$ $j \in [d]$ $j - 1 \cdot r\ \lambda\ <$,), 满足 $i \leqslant j \cdot r\ \lambda$ $\tilde{x}^{(j)}$ $\tilde{\sigma}^{(j)}$ () () () 并且这些内容是从 NBS 的输出中恢复出来的$\mathsf{NBS}(j)$。于是有

$$\Pr[D_i \in \{x_i, \perp\}] = \Pr[D_i \in \{x_i, \perp\} \mid \overline{\mathsf{Frg}_i}].$$

由于解码器不可能同时输出 $\perp$ 和 x_i，因此有

$$\Pr[D_i \in \{x_i, \perp\} \mid \overline{\mathsf{Frg}_i}]$$
$$= \Pr[D_i = x_i \mid \overline{\mathsf{Frg}_i}] + \Pr[D_i = \perp \mid \overline{\mathsf{Frg}_i}].$$

我们首先分析 $\Pr[D_i = x_i \mid \mathsf{Frg}_i]$。首先注意到，在这种情况下，有

1) $\mathsf{pk}^* \neq \perp$ and $\tilde{m}^{(j)} \neq \perp$; and
2) $\mathsf{Ver}_{\mathsf{pk}^*}(\tilde{x}^{(j)} \| j, \tilde{\sigma}^{(j)}) = 1$.

由于我们假设 $(\tilde{x}^{(j)} \| j, \tilde{\sigma}^{(j)})$ 不是伪造，因此根据上述内容，必有

1) $\tilde{x}^{(j)} = x^{(j)}$ and $\tilde{\sigma}^{(j)} = \sigma^{(j)}$; and
2) $\mathsf{pk}^* = \mathsf{pk}$.

NBS 和 BlockDec 的独立运行意味着

$$\begin{aligned}\Pr[D_i = x_i \mid \overline{\mathsf{Frg}_i}] &= \Pr[\mathsf{pk}^* = \mathsf{pk} \ \wedge \ \tilde{m}^{(j)} \neq \perp] \\ &= \Pr[\mathsf{pk}^* = \mathsf{pk}] \cdot \Pr[\tilde{m}^{(j)} \neq \perp].\end{aligned}$$

接下来我们分析 $\Pr[D_i = \perp | \overline{\mathsf{Frg}_i}]$。如果 $\mathsf{pk}^* = \perp$ 或 $\tilde{m}^{(j)} = \perp$ 或 $\mathsf{Ver}_{\mathsf{pk}^*}(\tilde{x}^{(j)} \| j, \tilde{\sigma}^{(j)}) = 0$，则解码器输出 bot。注意，只有在 $\mathsf{pk}^* \neq \perp$ and $\tilde{m}^{(j)} \neq \perp$ 的条件下才会检查最终验证。令 $\mathcal{E}_1$ 表示事件 $\mathsf{pk}^* = \perp$，并令 $\mathcal{E}_2$ 表示事件 $\tilde{m}^{(j)} = \perp$。于是有

$$\begin{aligned}&\Pr[D_i = \perp \mid \overline{\mathsf{Frg}_i}] \\ &= \Pr[\mathcal{E}_1] + \Pr[\mathcal{E}_2] - \Pr[\mathcal{E}_1 \ \wedge \ \mathcal{E}_2] \\ &+ \Pr\left[\mathsf{Ver}_{\mathsf{pk}^*}(\tilde{x}^{(j)} \| j, \tilde{\sigma}^{(j)}) = 0 \,\middle|\, \begin{array}{l}\overline{\mathcal{E}}_1 \ \wedge \\ \overline{\mathcal{E}}_2 \ \wedge \\ \overline{\mathsf{Frg}_i}\end{array}\right] \cdot \Pr[\overline{\mathcal{E}}_1 \ \wedge \ \overline{\mathcal{E}}_2].\end{aligned}$$

由于我们假设未发生伪造，上述概率的最后一个求和项可下界为

$$\begin{aligned}&\Pr\left[\mathsf{Ver}_{\mathsf{pk}^*}(\tilde{x}^{(j)} \| j, \tilde{\sigma}^{(j)}) = 0 \,\middle|\, \begin{array}{l}\overline{\mathcal{E}}_1 \ \wedge \\ \overline{\mathcal{E}}_2 \ \wedge \\ \overline{\mathsf{Frg}_i}\end{array}\right] \cdot \Pr[\overline{\mathcal{E}}_1 \ \wedge \ \overline{\mathcal{E}}_2] \\ &\geqslant \Pr\left[\mathsf{Ver}_{\mathsf{pk}^*}(\tilde{x}^{(j)} \| j, \tilde{\sigma}^{(j)}) = 0 \,\middle|\, \begin{array}{l}\overline{\mathsf{Frg}_i} \ \wedge \\ (\tilde{x}^{(j)} \neq x^{(j)} \ \vee \\ \tilde{\sigma}^{(j)} \neq \sigma^{(j)}) \ \wedge \\ \mathsf{pk}^* = \mathsf{pk}\end{array}\right] \\ &\quad \cdot \Pr[\overline{\mathcal{E}}_2 \ \wedge \ \mathsf{pk}^* = \mathsf{pk}] \\ &= \Pr[\overline{\mathcal{E}}_2 \ \wedge \ \mathsf{pk}^* = \mathsf{pk}],\end{aligned}$$

其中，在求下界时，我们忽略事件 $\mathsf{pk}^* \neq \mathsf{pk} \ \wedge \mathsf{pk}^* \neq \perp$。因此有 $\Pr[D_i \in \{x_i, \perp\} | \overline{\mathsf{Frg}_i}] \geqslant \Pr[\mathsf{pk}^* = \perp] + \Pr[\tilde{m}^{(j)} = \perp] - \Pr[\mathsf{pk}^* \equiv \perp] \cdot \Pr[\tilde{m}^{(j)} \perp] + [\tilde{m}^{j} \neq \perp] \cdot [{}^{*} =]$, Pr() Pr pk pk

$$\begin{aligned}\Pr[D_i \in \{x_i, \perp\} \mid \overline{\mathsf{Frg}_i}] &\geqslant \Pr[\mathcal{E}_1] + \Pr[\mathcal{E}_2] - \Pr[\mathcal{E}_1] \cdot \Pr[\mathcal{E}_2] \\ &\quad + \Pr[\overline{\mathcal{E}}_2] \cdot \Pr[\mathsf{pk}^* = \mathsf{pk}]\end{aligned}$$

其中不等式成立，是因为 NBS 和 BlockDec 是彼此独立地运行的。

在确立上述下界后，我们转而分析 $\Pr[\mathsf{pk}^* = \mathsf{pk}]$。设 pk 是由 Enc. $\lambda(x)$ 采样得到、用于生成码字 C 的公钥。恢复 pk 的过程是：˜均匀采样 μ 个 C的索引，在这些索引上运行 BlockDec，并对所恢复的公钥取多数表决。直观地说，我们希望通过切尔诺夫界以高概率恢复 pk^*。定义随机变量 X_κ 关于 $\kappa \in [\mu]$ 为

$$X_\kappa := \begin{cases} 1 & x^{(j)} \| \sigma^{(j)} \| \mathsf{pk} \| j = \mathsf{BlockDec}(i_\kappa) \text{ for } j \in [d] \\ 0 & \text{otherwise} \end{cases}.$$

因此，我们需要确保 $\Pr[X_\kappa = 1] > 1/2$。根据 引理 5，我们知道，只要索引 i_κ 位于某个 γ-良好块 j的范围内，那么 $X_\kappa = 1$ 以至少$1 - \gamma$的概率成立。令 $\mathcal{J} \subset [d]$ 表示 γ-良好块在 C中的索引。则有

$$\Pr[X_\kappa = 1] \geqslant \Pr[i_\kappa \in \phi_0^{-1}(j) \mid j \in \mathcal{J}_{\mathsf{Good}}] \cdot (1 - \gamma)$$

根据 引理 3，我们知道至少有 $(1 - 2\beta\rho/(\gamma\alpha))$- 比例的块是 γ-良好的，这意味着 $|\mathcal{J}| \geqslant d \cdot (1 - 2\beta\rho/(\gamma\alpha))$。由于我们要求 概率$[X_\kappa = 1] > 1/2$，根据引理 2 可得

$$(d/n) \cdot (1 - (2\beta\rho)/(\gamma\alpha)) \cdot (\beta - \alpha\gamma) \cdot \tau \cdot (1 - \gamma) > 1/2.$$

对上面的 ρ 求解可得

$$\rho < \frac{\gamma \cdot \alpha}{2 \cdot \beta} \cdot \left(1 - \frac{\beta}{2 \cdot (1 - \gamma) \cdot (\beta - \alpha \cdot \gamma)}\right).$$

借用 Block 等人 [BBG+20 的参数，命题 22], 中，我们设定 $\gamma = 1/12$ 和 $\alpha = 2\gamma\rho_{in}/(\gamma + 6)$。还记得 $\beta = 2\alpha + (1/\beta_{\mathsf{sz}})$。于是我们有

$$\begin{aligned}\alpha &= (2/73) \cdot \rho_{in} \\ \beta &= (4/73) \cdot \rho_{in} + (1/\beta_{\mathsf{sz}}) \\ \frac{\gamma \cdot \alpha}{2 \cdot \beta} &= \frac{(1/12) \cdot (2/73) \cdot \rho_{in}}{2 \cdot (4/73) \cdot \rho_{in} + 2/\beta_{\mathsf{sz}}} < 1 \\ \frac{\beta}{2(1-\gamma)(\beta - \alpha \cdot \gamma)} &= \frac{6}{11} \cdot \frac{(4/73)\rho_{in} + (1/\beta_{\mathsf{sz}})}{(23/438)\rho_{in} + (1/\beta_{\mathsf{sz}})} < 1.\end{aligned}$$

给定上述参数，由于 $\rho_{in} < 1$，我们还有

$$\frac{\gamma \cdot \alpha}{2 \cdot \beta} \geqslant \frac{(2/876) \cdot \rho_{in}}{(8/73) + 2/\beta_{\mathsf{sz}}}.$$

因此设定

$$\begin{aligned}\rho :=& \left(\frac{(2/876)\rho_{in}}{(8/73) + 2/\beta_{\mathsf{sz}}}\right)\left(1 - \frac{6}{11} \cdot \frac{(4/73)\rho_{in} + (1/\beta_{\mathsf{sz}})}{(23/438) \cdot \rho_{in} + (1/\beta_{\mathsf{sz}})}\right) \\ &= \Theta(1)\end{aligned}$$

可确保概率$[X_\kappa = 1] > 1/2$。现在令 $q :=$ 概率$[X_\kappa = 1] > 1/2$。根据切尔诺夫界，我们有

$$\Pr\left[\sum_{\kappa \in [\mu]} X_\kappa > \frac{\mu}{2}\right] \geqslant 1 - \exp(-\mu \cdot (q - 1/2)^2/(2q)).$$

这意味着以至少 $1 - \exp(-\mu(q - 1/2)^2/(2q))$的概率有$\mathsf{pk}^* = \mathsf{pk}$，这意味着

$$\Pr[\mathsf{pk}^* = \perp] \leqslant \exp(-\mu(q - 1/2)^2/(2q)).$$

鉴于

$$\Pr[\mathsf{pk}^* = \mathsf{pk}] \geqslant 1 - \exp(-\mu(q - 1/2)^2/(2q)),$$

我们现在分析 概率$[\tilde{m}^{(j)} \neq \perp]$。注意，根据 引理 4 中的带噪二分搜索算法，如果块 j 是 γ-良好，则我们以至少 $(1 - \rho^*)$ 的概率恢复正确的块 $x^{(j)} \| \sigma^{(j)} \| \mathsf{pk} \| j$，但仍有 $\vartheta(K')$ 的概率失败，其中 ρ^* 是

某个常数，且 ϑ 是一个可忽略函数。以我们以至少 $(1-\rho^*)$ 的概率恢复任意 γ-良好块为条件，我们有

$$\Pr[\tilde{m}^{(j)} \neq \perp \mid j \text{ is } \gamma\text{-good}] \geqslant (1-\rho^*).$$

等价地，我们有

$$\Pr[\tilde{m}^{(j)} = \perp \mid j \text{ is } \gamma\text{-good}] \leqslant \rho^*.$$

综合以上结果，我们有

$$\begin{aligned}
&\Pr[D_i \in \{x_i, \perp\} \mid \overline{\mathsf{Frg}_i}] \\
&\geqslant (1-\rho^*) \cdot \left(1 - \exp\left(-\mu \cdot \frac{(q-1/2)^2}{2q}\right)\right) \\
&- \rho^* \cdot \exp\left(-\mu \cdot \frac{(q-1/2)^2}{2q}\right) \\
&= 1 - \rho^* - \exp\left(-\mu \cdot \frac{(q-1/2)^2}{2q}\right),
\end{aligned}$$

其中 $\rho^* \in (0,\ 1/2)$ 是一个固定常数，我们可以自由选择。特别地，我们选择 $\rho^* < 1/3$，以帮助确保在适当选择 μ 后满足 $p > 2/3$。

在上述分析中，我们以 Frg_i 发生以及 $\overline{\mathsf{NBS}}$ 成功为条件。根据数字签名方案的安全性，Frg_i 发生的概率至少为 $1-\varepsilon_\Pi(\lambda)$，其中 $\varepsilon_\Pi(\lambda)$ 是针对该数字签名方案安全性的一个可忽略函数。根据引理 4，NBS 正确输出的概率至少为 $1-\vartheta(n')$。最后，对 $i \in [k]$ 使用并集界，我们令 $\varepsilon_{\mathsf{F}}(\lambda, n) := k \cdot \varepsilon_\Pi(\lambda) \cdot \vartheta(n)$，它关于 λ 是可忽略的，因为 $k(\lambda) = \mathrm{poly}(\lambda)$。

接下来我们着手证明[引理 4]。再次令 $C \leftarrow \mathcal{A}(C)$; 对于 $x \in \{0,1\}^k$，$\lambda(x)$。我们的目标是证明存在一个可忽略函数 $\varepsilon_{\mathsf{L}}(\cdot)$，使得对所有 $\lambda \in \mathbb{N}$ 和所有 $x \in \{0,1\}^k$，都有

$$\Pr[\mathsf{Limit}(\mathcal{A}(C), \rho, \delta, x, y) = 1] \leqslant \varepsilon_{\mathsf{L}}(\lambda).$$

我们直接分析集合 $\mathsf{Good}(C)$ 的大小。与之前一样，令 D_i 为随机变量，表示 $\mathsf{Dec}^C_{,\lambda}(i)$ 的输出。于是，我们希望对固定的 $i \in [k]$ 给出 $\Pr[D_i = x_i]$ 的下界。根据 $\mathsf{Dec}_{,\lambda}$ 的定义，解码器只有在以下条件成立时才会输出一个比特：

1) $\mathsf{pk}^* \neq \perp$；2) $\tilde{m}_{(j)} \neq \perp$；以及 3) $\mathsf{Ver}_{\mathsf{pk}^*}(\tilde{x}^{(j)} \| j, \tilde{\sigma}^{(j)}) = 1$。

与之前一样，令 $\mathcal{E}_1$ 表示事件 $\mathsf{pk}^* = \perp$，令 $\mathcal{E}_2$ 表示事件 $\tilde{m}^{(j)} = \perp$。根据定义，我们有

$$\begin{aligned}
\Pr[D_i = x_i] = &\Pr[\overline{\mathcal{E}}_1] \cdot \Pr[\overline{\mathcal{E}}_2 | \overline{\mathcal{E}}_1] \\
&\cdot \Pr[\mathsf{Ver}_{\mathsf{pk}^*}(\tilde{x}^{(j)} \| j, \tilde{\sigma}^{(j)}) = 1 \mid \overline{\mathcal{E}}_1 \ \wedge \ \overline{\mathcal{E}}_2].
\end{aligned}$$

由于 pk^* 和 $\tilde{m}^{(j)}$ 是独立计算的，因此上式等于

$$\begin{aligned}
&\Pr[D_i = x_i] \\
&= \Pr[\overline{\mathcal{E}}_1] \cdot \Pr[\overline{\mathcal{E}}_2] \cdot \Pr[\mathsf{Ver}_{\mathsf{pk}^*}(\tilde{x}^{(j)} \| j, \tilde{\sigma}^{(j)}) = 1 \mid \overline{\mathcal{E}}_1 \ \wedge \ \overline{\mathcal{E}}_2] \\
&\geqslant \Pr[\mathsf{pk}^* = \mathsf{pk}] \cdot \Pr[\tilde{m}^{(j)} = m^{(j)}] \\
&\cdot \Pr[\mathsf{Ver}_{\mathsf{pk}^*}(\tilde{x}^{(j)} \| j, \tilde{\sigma}^{(j)}) = 1 \mid \mathsf{pk}^* = \mathsf{pk} \ \wedge \ \tilde{m}^{(j)} = m^{(j)}],
\end{aligned}$$

其中，不等式成立是因为它是所考虑的所有可能事件的子集。以及 $m^{(j)} := x^{(j)} \| \sigma^{(j)} \| \mathsf{pk} \| j$。现在我们分析上述下界中的每一项。首先注意最后一项

$$\Pr[\mathsf{Ver}_{\mathsf{pk}^*}(\tilde{x}^{(j)} \| j, \tilde{\sigma}^{(j)}) = 1 \mid \mathsf{pk}^* = \mathsf{pk} \ \wedge \ \tilde{m}^{(j)} = m^{(j)}] = 1$$

根据定义。因此我们分析另外两个概率项。根据我们之前的工作，我们知道

$$\Pr[\mathsf{pk}^* = \mathsf{pk}] \geqslant 1 - \exp(-\mu(q-1/2)^2/(2q)).$$

现在我们给出 概率 $[\tilde{m}^{j} = m^{(j)}]$ $\tilde{m}^{(j)} = {}_{()}$。回顾 $\mathsf{NBS}^C(j)$。根据 引理 4 我们有

$$\Pr\left[\Pr_{j \xleftarrow{\$} [d]}\left[\tilde{m}^{(j)} \neq C^{(j)} \mid j \text{ is } \gamma\text{-good}\right] \geqslant \rho^*\right] \leqslant \vartheta(K').$$

固定 j 为一个 γ-良好块。于是我们有

$$\Pr\left[\Pr[\tilde{m}^{(j)} \neq C^{(j)}] \geqslant \rho^*\right] \leqslant \vartheta(K');$$

或者等价地

$$\Pr\left[\Pr[\tilde{m}^{(j)} = C^{(j)}] \leqslant 1-\rho^*\right] \leqslant \vartheta(K').$$

这意味着

$$\Pr\left[\Pr[\tilde{m}^{(j)} = C^{(j)}] \geqslant 1-\rho^*\right] \geqslant 1 - \vartheta(K').$$

因此，以至少 $1-\vartheta(K')$ 的概率，我们有

$$\Pr[\tilde{m}^{(j)} = C^{(j)}] \geqslant 1-\rho^*.$$

根据引理 3，我们知道至少有 $1-(2\beta\rho)/(\gamma\alpha)$比例的块属于 C，且是 γ-良好的。由于对于每个 $i \in [k]$，都存在唯一一个块 $j \in [d]$ 使得 $(j-1)r(\lambda) < i \leqslant jr(\lambda)$，对于集合

$$\mathcal{G} := \{i \in [k] \colon i \text{ is in a } \gamma\text{-good block}\},$$

我们有

$$|\mathcal{G}| \geqslant r(\lambda) \cdot \left(1 - \frac{2\beta\rho}{\gamma\alpha}\right) \cdot d = \left(1 - \frac{2\beta\rho}{\gamma\alpha}\right) \cdot k.$$

因此，至少有 $1-(2\beta\rho)/(\gamma\alpha)$ 比例的索引 $i \in [k]$位于一个 γ-良好的块中。

综上，对于任意 γ-良好的块，以至少 $1-\vartheta(K')$ 的概率，我们有：

$$\Pr[D_i = x_i] \geqslant (1 - \exp(-\mu \cdot (q-1/2)^2/(2q))) \cdot (1-\rho^*).$$

适当选择 μ 和 $\rho^* \in (0, 1/3)$，使得

$$(1 - \exp(-\mu(q-1/2)^2/(2q))) \cdot (1-\rho^*) > 2/3,$$

结合至少有 $1-(2\beta\rho)/(\gamma\alpha)$ 比例的索引 $i \in [k]$ 位于一个 γ-良好的块中的事实，我们有

$$\Pr[|\mathsf{Good}(\tilde{C})| \geqslant (1-(2\beta\rho)/(\gamma\alpha)) \cdot k] \geqslant 1 - \vartheta(K'),$$

这意味着

$$\begin{aligned}
\Pr[\mathsf{Limit}(\tilde{C}, \rho, \delta, x, C) = 1] &\leqslant \vartheta(K') \\
&= \vartheta(\Theta(k)) =: \varepsilon_{\mathsf{L}}(\lambda)
\end{aligned}$$

for $\delta = 1-(2\beta\rho)/(\gamma\alpha) = 1-\Theta(\rho)$. □

VI. 致谢

Alexander R. Block 的部分研究经费由美国国家科学基金会通过 NSF CCF #1910659 项目提供，另有部分经费来自美国国防高级研究计划局，依据协议编号 HR00112020022 和 HR00112020025。Jeremiah Blocki 的部分研究经费由美国国家科学基金会通过 CNS # 2047272、CNS #1931443 和 CCF #1910659 项目提供。本材料中表达的观点、意见、研究结果、结论和/或建议仅代表作者，不应被解释为反映美国国防部或美国政府的立场或政策，也不应据此推断获得了官方认可。

参考文献

[ABH17] Joël Alwen、Jeremiah Blocki 和 Ben Harsha。用于构建最优抗侧信道内存困难函数的实用图。在 Bhavani M. Thuraisingham、David Evans、Tal Malkin 和 Dongyan Xu（编者）的 ACM CCS 2017 论文集中，第 1001–1017 页。ACM出版社，2017年10月/11月。doi:10.1145/3133956. 3134031.[ABP18] Joël Alwen、Jeremiah Blocki 和 Krzysztof Pietrzak。持续空间复杂度。在 Jesper Buus Nielsen 和 Vincent Rijmen（编者）的 EUROCRYPT 2018 第二部分，《计算机科学讲义》第 10821 卷，第 99–130 页。施普林格，海德堡，2018年4月/5月。doi: 10.1007/978-3-319-78375-8_4.[AS21] Vahid R. Asadi 和 Igor Shinkar。参数更优的宽松局部可纠错码。在 Nikhil Bansal、Emanuela Merelli 和 James Worrell（编者）的 ICALP 2021 论文集中，《信息学论文集》第 198 卷，第 18:1–18:12 页。达格施图尔城堡，2021年7月。doi: 10.4230/LIPIcs.ICALP.2021.18.[BB21] Alexander R. Block 和 Jeremiah Blocki。面向插入和删除的私有且资源有界局部可解码码。在 2021年IEEE国际信息论研讨会（ISIT）论文集中，第 1841–1846 页，2021年。doi:10.1109/ISIT45174. 2021.9518249.[BBG+20] Alexander R. Block、Jeremiah Blocki、Elena Grigorescu、Shub- hang Kulkarni 和 Minshen Zhu。面向插入和删除的局部可解码/可纠错码。在 Nitin Saxena 和 Sunil Simon（编者）的第 40 届 IARCS 软件技术基础与理论计算机科学年会论文集中，《信息学论文集》第 182 卷，第 16:1–16:17 页。达格施图尔城堡—莱布尼茨信息学中心，2020年。doi:10.4230/ LIPIcs.FSTTCS.2020.16.[BCG+22] Jeremiah Blocki、Kuan Cheng、Elena Grigorescu、Xin Li、Yu Zheng 和 Minshen Zhu。面向插入和删除的局部可解码与可纠错码的指数下界。在第62届FOCS论文集中，第 739–750 页。IEEE计算机学会出版社，2022年2月。doi:10.1109/FOCS52979.2021.00077.[BGGZ21] Jeremiah Blocki、Venkata Gandikota、Elena Grigorescu 和 Samson Zhou。计算受限信道中的宽松局部可纠错码。《IEEE信息论汇刊》，67(7):4338–4360，2021年。doi:10.1109/TIT.2021. 3076396.[BGH+06] Eli Ben-Sasson、Oded Goldreich、Prahladh Harsha、Madhu Sudan 和 Salil P. Vadhan。鲁棒邻近性PCP、更短的PCP及其编码应用。《SIAM计算杂志》，36 974，2006 4 889 10 1137 0097539705446810 ( ): – 。doi: . /S 。[BGZ18] Joshua Brakensiek、Venkatesan Guruswami 和 Samuel Zbarsky。用于纠正多次删除的高效低冗余码。《IEEE信息论汇刊》，64(5):3403–3410，2018年。doi:10. 1109/TIT.2017.2746566.[BH22] Jeremiah Blocki 和 Blake Holman。数据相关内存困难函数的持续空间复杂度与累积复杂度权衡。在 Yevgeniy Dodis 和 Thomas Shrimpton（编者）的 CRYPTO 2022 第三部分论文集中，《计算机科学讲义》第 13509 卷，第 222–251 页。施普林格，海德堡，2022年8月。doi: 10.1007/978-3-031-15982-4_8。

[BKZ20] Jeremiah Blocki、Shubhang Kulkarni 和 Samson Zhou。关于资源受限信道中的局部可解码码。载于 Yael Tauman Kalai、Adam D. Smith 和 Daniel Wichs（编），ITC 2020，第16:1–16:23页。达格施图尔城堡，2020年6月。doi:10.4230/LIPIcs.ITC.2020.16。[BL22] Jeremiah Blocki 和 Seunghoon Lee。关于带预处理的短 Schnorr 签名的多用户安全性。载于 Orr Dunkelman 和 Stefan Dziembowski（编），EUROCRYPT 2022，第二部分，《计算机科学讲义》第13276卷，第614–643页。施普林格出版社，海德堡，5月/6月 2022 10 1007 978 3 031 07085 3_ 。doi: . / - - - - 21。[CGHL21] Kuan Cheng 、 Venkatesan Guruswami 、 Bernhard Haeupler 和 Xin Li。用于纠正插入/删除的高效线性码和仿射码。载于 Dániel Marx（编），第32届SODA，第1–20页。ACM-SIAM，2021年1月。doi:10.1137/1. 9781611976465.1。[CGS22] Alessandro Chiesa、Tom Gur 和 Igor Shinkar。具有近线性码长和常数查询复杂度的宽松局部可纠错码。《SIAM计算杂志》，51(6):1839–1865，2022年。doi:10.1137/20m135515x。[CHL+19] Kuan Cheng、Bernhard Haeupler、Xin Li、Amirbehshad Shahrasbi 和 Ke Wu。同步字符串：小字母表上的高效确定性构造。载于 Timothy M. Chan（编），第30届SODA，第2185–2204页。ACM-SIAM，2019年1月。doi:10.1137/1.9781611975482.132。[CJLW19] Kuan Cheng、Zhengzhong Jin、Xin Li 和 Ke Wu。带转置的块编辑错误：确定性文档交换协议和近乎最优的二进制码。载于 Christel Baier、Ioannis Chatzigiannakis、Paola Flocchini 和 Stefano Leonardi（编），ICALP 2019，《信息学论文集》第132卷，第37:1–37:15页。达格施图尔城堡，2019年7月。doi:10.4230/LIPIcs. ICALP.2019.37。[CJLW22] Kuan Cheng、Zhengzhong Jin、Xin Li 和 Ke Wu。编辑错误的确定性文档交换协议和近乎最优的二进制码。《ACM期刊》，69(6):44:1–44:39，2022年。doi:10. 1145/3561046。[CL21] Kuan Cheng 和 Xin Li。具有非对称信息的高效文档交换与纠错码。载于 Dániel Marx（编），第32届SODA，第2424–2443页。ACM-SIAM，2021年1月。doi:10.1137/1.9781611976465.144。[CLZ20] Kuan Cheng、Xin Li 和 Yu Zheng。具有随机编码的局部可解码码。密码学电子印本档案，报告2020/031，2020年。https://eprint.iacr.org/2020/031。[CY22] Gil Cohen 和 Tal Yankovitz。宽松局部可解码码和可纠错码：超越张量化。载于第63届FOCS，第24–35页。IEEE计算机学会出版社，2022年10月/11月。doi:10.1109/FOCS54457.2022.00010。[DGY11] Zeev Dvir、Parikshit Gopalan 和 Sergey Yekhanin。匹配向量码。《SIAM计算杂志》，40(4):1154–1178，2011年。doi: 10.1137/100804322。[Efr12] Klim Efremenko。次指数长度的3查询局部可解码码。《SIAM计算杂志》，41(6):1694–1703，2012年。[EGS75] Paul Erdös、Ronald L. Graham 和 Endre Szemeredi。关于具有稠密长路径的稀疏图。技术报告，斯坦福大学，美国加利福尼亚州斯坦福，1975年。[For66] G. Forney。广义最小距离解码。《IEEE信息论汇刊》，12(2):125–131，1966年。doi: 10.1109/TIT.1966.1053873。[GHS21] Venkatesan Guruswami、Bernhard Haeupler 和 Amirbehshad Shahrasbi。对插入和删除进行列表解码的最优弹性码。《IEEE信息论汇刊》，67(12):7837–7856，2021年。doi:10.1109/TIT.2021.3120910。[GL19] Venkatesan Guruswami 和 Ray Li。二进制删除信道上的多项式时间可解码码。《IEEE信息论汇刊》，65(4):2171–2178，2019年。doi:10.1109/TIT.2018. 2876861。[GL20] Venkatesan Guruswami 和 Ray Li。针对无知模型和在线模型中的删除进行编码。《IEEE信息论汇刊》，66(4):2352–2374，2020年。doi:10.1109/TIT.2020. 2968298。[GRR20] Tom Gur、Govind Ramnarayan 和 Ron Rothblum。宽松局部可纠错码。《计算理论》，16:1–68，2020年。doi: 10.4086/toc.2020.v016a018。

[GS16] Venkatesan Guruswami 和 Adam Smith。计算简单信道的最优码率编码构造。《ACM期刊》，63(4)，2016年9月。doi:10.1145/2936015。[GW17] Venkatesan Guruswami 和 Carol Wang。高噪声和高码率区域中的删除码。《IEEE信息论汇刊》，63(4):1961–1970，2017年。doi:10.1109/TIT.2017. 2659765。[Hae19] Bernhard Haeupler。最优文档交换以及用于插入和删除的新码。载于 David Zuckerman（编），第60届FOCS，第334–347页。IEEE计算机学会出版社，2019年11月。doi:10.1109/FOCS.2019.00029。[HO08] Brett Hemenway 和 Rafail Ostrovsky。公钥局部可解码码。载于 David Wagner（编），CRYPTO 2008，《计算机科学讲义》第5157卷，第126–143页。施普林格出版社，海德堡，2008年8月。doi:10.1007/978-3-540-85174-5_8。[HOSW11] Brett Hemenway、Rafail Ostrovsky、Martin J. Strauss 和 Mary Wootters。具有短密钥的公钥局部可解码码。载于第14届国际研讨会暨第15届近似、随机化与组合优化国际会议：算法与技术，APPROX'11/RANDOM'11，第605–615页，柏林、海德堡，2011年。施普林格出版社。[HRS19] Bernhard Haeupler、Aviad Rubinstein 和 Amirbehshad Shahrasbi。近线性时间插入删除码，以及通过索引近似编辑距离。在 Moses Charikar 和 Edith Cohen（编），第51届ACM STOC，第697–708页。ACM出版社，2019年6月。doi:10.1145/3313276.3316371。[HS18] Bernhard Haeupler 和 Amirbehshad Shahrasbi。同步字符串：显式构造、局部解码及应用。载于 Ilias Diakonikolas、David Kempe 和 Monika Henzinger（编），第50届ACM STOC，第841–854页。ACM出版社，2018年6月。doi:10.1145/3188745.3188940。[HS21] Bernhard Haeupler 和 Amirbehshad Shahrasbi。同步字符串：逼近Singleton界的插入删除码。《ACM期刊》，68(5):36:1–36:39，2021年。doi:10.1145/3468265。[HSS18] Bernhard Haeupler、Amirbehshad Shahrasbi 和 Madhu Sudan。同步字符串：插入和删除的列表解码。载于 Ioannis Chatzigiannakis、Christos Kaklamanis、Dániel Marx 和 Donald Sannella（编），ICALP 2018，《信息学论文集》第107卷，第76:1–76:14页。达格施图尔城堡，2018年7月。doi:10.4230/LIPIcs.ICALP.2018.76。[Jus72] J. Justesen。构造性渐近良好代数码类。《IEEE信息论汇刊》，18 656，1972 5 652 10 1109 1972 1054893 ( ): – 。doi: 。/TIT. 。 。[KdW04] Iordanis Kerenidis 和 Ronald de Wolf。通过量子论证证明2查询局部可解码码的指数下界。《计算机与系统科学杂志》，69(3):395–420，2004年。[KL14] Jonathan Katz 和 Yehuda Lindell。《现代密码学导论》第二版。CRC出版社，2014年。[KLM04] Marcos A. Kiwi、Martin Loebl 和 Jirí Matousek。大字母表中最长公共子序列的期望长度。载于 Martin Farach-Colton（编），LATIN 2004，《计算机科学讲义》第2976卷，第302–311页。施普林格出版社，海德堡，2004年4月。[KMRZS17] Swastik Kopparty、Or Meir、Noga Ron-Zewi 和 Shubhangi Saraf。具有次多项式查询复杂度的高码率局部可纠错码和局部可测试码。《ACM期刊》，64(2)，2017年5月。doi:10.1145/3051093。[KS16] Swastik Kopparty 和 Shubhangi Saraf。客座专栏：高码率纠错码的局部测试与解码。《SIGACT新闻》，47(3):46–66，2016年8月。doi:10.1145/2993749. 2993761。[KT00] Jonathan Katz 和 Luca Trevisan。关于纠错码局部解码过程的效率。载于第32届ACM STOC，第80–86页。ACM出版社，2000年5月。doi:10.1145/ 335305.335315。[Lam79] Leslie Lamport。利用单向函数构造数字签名。技术报告 CSL-98，1979年10月。该论文由IEEE发表于2010年1月的HICSS-43会议论文集。URL: https://www.microsoft.com/en-us/research/publication/constructing-digital-signatures-one-way-function/。[Lev66] Vladimir Iosifovich Levenshtein。能够纠正删除、插入和反转的二进制码。《苏联物理学》《苏联科学院学报》，10(8):707–710，1966。《苏联科学院学报》，V163 第4期，845-848，1965。

[Lip94] Richard J. Lipton。信息论的新方法。载于 Patrice Enjalbert、Ernst W. Mayr 和 Klaus W. Wagner（编辑），*STACS 94*，第699–708页，柏林、海德堡，1994年。Springer Berlin Heidelberg。

[LTX19] Shu Liu、Ivan Tjuawinata 和 Chaoping Xing。关于插入错误和删除错误的列表解码。*CoRR*，abs/1906.09705，2019年。网址：http://arxiv.org/abs/1906.09705，arXiv:1906.09705。

[MBT10] H. Mercier、V. K. Bhargava 和 V. Tarokh。符号同步错误信道的纠错码综述。*IEEE Communications Surveys Tutorials*，12(1):87–96，2010。doi:10.1109/SURV.2010.020110.00079。

[Mit08] MichaelMitzenmacher。删除信道及相关同步信道的研究成果综述。载于 Joachim Gudmundsson（编辑），*算法理论 – SWAT 2008*，第1–3 页，柏林、海德堡，2008 年。Springer Berlin Heidelberg。

[MPSW05] Silvio Micali、Chris Peikert、Madhu Sudan 和 David A. Wilson。针对计算有界噪声的最优纠错。在 Joe Kilian（编辑），*TCC 2005*，收录于《计算机科学讲义》第 3378 卷，《计算机科学讲义》，第 1–16 页。施普林格，海德堡，2005 年 2 月。doi:10.1007/ 978-3-540-30576-7 1。_

[OPC15] Rafail Ostrovsky 和 Anat Paskin-Cherniavsky。用于编辑距离的局部可解码码。载于 Anja Lehmann 和 Stefan Wolf 编，《信息论安全》，第236–249 页，Cham，2015 年。Springer International Publishing。

[OPS07] Rafail Ostrovsky、Omkant Pandey 和 Amit Sahai。私有局部可解码码。载于 Lars Arge、Christian Cachin、Tomasz Jurdzinski 和 Andrzej Tarlecki 编，*ICALP 2007*，第 4596 卷，出自《计算机科学讲义》，第 387–398 页。施普林格，海德堡，2007 年 7 月。doi:10.1007/978-3-540-73420-8_35。

[SB21] Jin Sima 和 Jehoshua Bruck。关于最优 k-删除纠错码。《*IEEE*信息论汇刊》，67(6):3360–3375，2021 年。doi: 10.1109/TIT.2020.3028702。

[Sch90] Claus-Peter Schnorr。智能卡的高效身份识别与签名。在 Gilles Brassard（编者）主编的*CRYPTO'89*，第 435 卷《计算机科学讲义》，第239–252 页。施普林格，海德堡，1990 年 8 月。doi:10.1007/0-387-34805-0_22。

[Slo02] N.J.A. Sloane。关于单删除纠错码。*arXiv*：组合学，2002 年。

[SS21] Ronen Shaltiel 和 Jad Silbak。针对计算能力受限信道的最优码率显式列表可解码码。*Comput. Complex.*，30(1):3，2021 年。doi:10.1007/ s00037-020-00203-w。

[STV01] Madhu Sudan、Luca Trevisan 和 Salil P. Vadhan。无需 XOR 引理的伪随机生成器。《计算机与系统科学杂志》，62(2)：236–266，2001年。doi:10.1006/jcss.2000.1730。

[SZ99] Leonard J. Schulman 和 David Zuckerman。可纠正插入、删除和换位的渐近良好码。《*IEEE*信息论汇刊》，45(7)：2552–2557，1999年。doi:10. 1109/18.796406。

[Woo07] David P. Woodruff。一般局部可解码码的新下界。《计算复杂性电子讨论组》（ECCC），2007年。https://eccc.weizmann.ac.il//eccc-reports/2007/ TR07-006/index.html。

[Woo12] David P. Woodruff。任意域上三查询局部可解码码的二次下界。载于《计算机科学与技术杂志》，第 27 卷，第 678–686 页，2012 年。doi:https:// doi.org/10.1007/s11390-012-1254-8。

[Yek08] Sergey Yekhanin。迈向次指数长度的三查询局部可解码码。《*ACM*期刊》，55(1)，2008 年 2 月。doi: 10.1145/1326554.1326555。

[Yek12] Sergey Yekhanin。局部可解码码。理论计算机科学基础与趋势®，6(3):139–255，2012 年。网址：http://dx.doi.org/10.1561/0400000030，doi:10.1561/ 0400000030。