arXiv:2304.00077v2 [econ.TH] 1 Sep 2023

去中心化攻击搜索与漏洞赏金计划的设计*

Hans Gersbach Akaki Mamageishvili经济研究中心
Offchain Labs苏黎世联邦理工学院、KOF 和 CEPR 苏黎世，瑞士Leonhardstrasse21
amamageishvili@offchainlabs.com8092 苏黎世，瑞士
hgersbach@ethz.chFikri Pitsuwan 经济研究中心 苏黎世联邦理工学院 Leonhardstrasse 21 8092 苏黎世，瑞士
fpitsuwan@ethz.ch最后更新：2023年9月6日

*本文的一页摘要发表于《第16届算法博弈论国际研讨会论文集》（SAGT 2023）。感谢SAGT 2023的三位匿名审稿人提出宝贵建议。感谢Kari Kostiainen、Tapas Kundu、Priel Levy，以及参加2023年经济设计会议、2023年竞赛年度会议、2023年石溪大学博弈论国际会议和ETH Z¨urich的会议参与者提出意见。本研究部分得到了苏黎世信息安全与隐私中心（ZISC）的支持。Otto T.P. Schmidt和Pio Blieske提供了出色的研究协助。文中如有错误，概由作者负责。

摘要

系统和区块链往往存在安全漏洞，可能遭到对手攻击，并造成潜在的严重负面后果。因此，基础设施提供商越来越依赖漏洞赏金计划：外部个体对系统进行探查，并报告发现的漏洞，以换取奖励（悬赏金）。我们建立了一个简单的漏洞赏金竞赛模型，邀请任意数量的个体开展有成本的漏洞搜索。这些个体的能力各不相同，我们以其在漏洞存在时发现漏洞所需的成本差异来刻画这种差异。成本属于私人信息。我们研究竞赛中的均衡，并刻画漏洞赏金计划的最优设计。具体而言，设计者可以调整受邀搜索的个体数量、增加一名付费专家、以一定概率植入人工漏洞，以及发放多个奖项。我们得出以下结果。第一，我们刻画了均衡，并证明任何均衡策略都必须是阈值策略，即只有搜索成本低于某个（可能因人而异的）阈值的代理人才会参与漏洞赏金计划。第二，我们给出了均衡唯一且对称的充分条件。第三，我们证明，即使邀请无限人群，也不能保证能找到漏洞（若漏洞确实存在），除非有代理人的成本为零，或者等价地说，他们参与该计划具有内在收益。甚至可能出现这样一种情况：扩大潜在参与者人才池中的代理人数量，反而会降低发现漏洞的概率。第四，增加一名付费专家可能提高或降低漏洞赏金计划的效率。第五，我们说明，加入（已知）漏洞是提高发现未知漏洞可能性的另一种方式。考虑到支付奖励所产生的额外成本，以一定概率植入已知漏洞可能是最优的。第六，我们证明，在一个设有多个奖项的模型中，设置一个奖项（赢家通吃）能使发现漏洞的概率达到最高。第七，我们指出了非对称均衡出现的情形。最后，我们讨论如何扩展基准模型，以允许存在多个漏洞、多名专家，以及代理人在成本分布、搜索时间和技能方面存在异质性。

关键词：竞赛设计、均衡、漏洞赏金

JEL分类：D82、C72、H41

1 引言

软件和区块链往往存在安全漏洞，可能遭到攻击者攻击，并造成严重的社会或经济负面后果。2019 年，瑞士计划推出的新电子投票系统被发现存在一个“重大缺陷”，便是一例。由于投票可能遭到操纵，联邦委员会暂停了该系统的开发，并下令重新设计（瑞士联邦总理府，2019）。此次攻击发现是在一项公开入侵测试中完成的，任何人都可以测试该软件，并报告发现的漏洞，以换取金钱奖励（悬赏金）。[1] 这种计划通常称为漏洞赏金或众包安全，如今已成为政府、科技公司和区块链领域用于搜索软件漏洞的重要工具。[2] 漏洞赏金对区块链基础设施提供商尤为重要，因为这类项目没有专门的安全团队来测试软件升级。软件一经部署，便无法撤回，也没有任何法律防御机制可以应对系统利用。[3]

关于漏洞赏金计划参与规则的全面论述（Laszka 等，2018）、此类计划的有效性与最佳实践（Walshe 和 Simpson，2020；Malladi 和 Subramanian，2020），以及研究人员参与漏洞赏金计划的激励因素（Maillart 等，2017）已有不少。本文基于 Ghosh 和 Kleinberg （2016）及Sarne 和 Lepioshkin （2017）的重要研究，使用一个简单竞赛的博弈论模型，探讨漏洞赏金设计的若干维度。在该模型中，具有不同能力的代理人决定是否投入有成本的努力来搜索漏洞。

漏洞赏金的若干显著特征使我们的方法区别于标准的最优竞赛文献。传统竞赛的设计目标是促使参赛者付出最高努力（或努力总和）。这可以通过适当分配奖品（Moldovanu 和 Sela，2001）、选择合适的保留努力（Chawla 等，2019）、设置报名费（Taylor，1995），或设计揭示机制，从候选人才池中选出部分参赛者（Mercier，2018）来实现。

我们关注这样一个简单问题：在奖励资金总额既定的情况下，如何最大限度地提高发现漏洞的可能性。具体而言，我们将重点研究漏洞赏金系统的三个设计变量。应邀请多大的代理人众包群体来发现漏洞？是否应将付费专家加入受邀的漏洞发现者群体？是否应

[1]参与者通常被称为道德黑客、白帽黑客或安全研究人员。[2]近年来取得的成功促使有关当局将漏洞赏金计划系统性地采用为政府网络安全的一项主要措施。在最近的一份新闻稿中，瑞士联邦委员会表示：“标准化的安全测试已不足以发现隐藏的漏洞。因此，未来计划让道德黑客作为所谓漏洞赏金计划的一部分，在瑞士联邦行政当局的生产性 IT 系统和应用中搜索漏洞。”（瑞士联邦财政部，2022）[3]至少在下一次硬分叉之前。

在软件中加入人工漏洞，以提高人们参与漏洞发现的积极性，并增加发现真正漏洞的可能性?

为回答这些问题以及有关漏洞赏金计划中均衡性质的其他一般性问题，我们建立了一个简单的众包安全模型。邀请任意规模的一群个体搜索漏洞。漏洞是否存在并不确定。个体发现漏洞的能力各不相同，我们通过他们在漏洞确实存在时达到某一发现概率所需的不同成本来刻画这种差异。成本属于私人信息。漏洞悬赏计划的设计者向发现漏洞的个体或个体组合颁发奖品。设计者可以调整受邀搜索漏洞的个体人数，可以在众包群体中加入一名付费专家，也可以按一定概率植入一个人工漏洞。

我们得到了以下结果。第一，我们证明，任何均衡策略都必须是阈值策略，即只有搜索成本低于某个（可能因人而异的）阈值的代理人才会参与漏洞悬赏计划。第二，我们给出了均衡唯一且对称的充分条件。第三，我们表明，即使邀请无限人群，也不能保证一定能发现漏洞，除非有些代理人的成本为零，或者说，他们参与该计划具有内在收益。潜在参与者人才池中的代理人增多，甚至可能降低发现漏洞的概率。第四，加入付费代理人可以提高漏洞悬赏计划的效率，尽管因此吸引来的众包群体规模会缩小。第五，我们说明，加入（已知）漏洞是提高发现未知漏洞可能性的另一种方式。考虑到支付奖励所增加的成本，最优做法可能是仅以一定概率植入已知漏洞。第六，我们证明，在设有多个奖项的模型中，设置一个奖项（赢家通吃）能使发现漏洞的概率达到最高。最后，我们指出了非对称均衡出现的情形。

本文结构安排如下：下一节将介绍模型。在第 3 节中，我们刻画均衡，并推导其在寻找漏洞方面的性质。在第 4 节中，我们讨论加入专家或人工漏洞，以及颁发多个奖项时的扩展。我们还将讨论非对称均衡的存在性与性质。在第 5 节中，我们讨论基准假设，并说明如何在不增加太多技术难度的情况下放宽这些假设。第 6 节作总结。证明见附录。

2 模型

有 $n \geq 2$ 名代理人受邀搜索漏洞。将代理人集合记为 $N = \{1, \ldots, n\}$，并令 $\boldsymbol{s} = (s_1, \ldots, s_n) \in \{0,1\}^n$ 表示代理人的行动组合，其中 $s_i = 1$ 若代理人 i 进行搜索，否则为 $s_i = 0$。如果代理人 i 决定进行搜索， i 会发现

该漏洞的概率为 $q \in (0,1]$ 在随机时间 t_i发现，该时间在可能的搜索时间 $[0,T]$上均匀分布，其中 T为搜索的最大时间。这些到达时间t_i 在各代理人之间随机独立。否则，i 不会发现该漏洞。为简单起见，我们假设漏洞确实存在，但也可以将该模型重新解释为漏洞以某种概率存在的模型。

搜索需要付出成本。如果 $s_i = 1$，代理人 i 承担成本 c_i ，该成本属于私人信息，并且来自连续分布 F ，其支撑集为$[\underline{c}, \overline{c}]$，$0 \leq \underline{c} < \overline{c} \leq \infty$ 且概率密度有限 f。[4] 我们考虑这样的 *winner-takes-all* 竞赛：只有第一个发现漏洞的代理人才能获得奖品 $V > 0$。[5] 如果两个（或更多）代理人同时发现漏洞，他们将平分奖品。然而，由于漏洞发现到达时间服从均匀分布，并且在离散数量的代理人之间随机独立，因此这种情况发生的概率为零，可以忽略不计。该假设还意味着，决定进行搜索的代理人赢得竞赛的概率相同。

我们记作 $\boldsymbol{s}_{-i} = (s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$，并令$S = \sum_j s_j$和 $S_{-i} = \sum_{j \neq i} s_j$分别表示进行搜索的代理人总数，以及除代理人 i 之外进行搜索的代理人总数。在给定上述设定的情况下，代理人 i 的收益为

$$u_i(s_i, \boldsymbol{s}_{-i}, c_i) = s_i \left(p(\boldsymbol{s}_{-i}) V - c_i \right), \tag{1}$$

其中

$$p(\boldsymbol{s}_{-i}) \equiv q \sum_{t=0}^{S_{-i}} \binom{S_{-i}}{t} q^t (1-q)^{S_{-i}-t} \frac{1}{t+1} \tag{2}$$

是给定代理人正在搜索的条件下，代理人 i 最先发现漏洞的概率。给定行动组合 $\boldsymbol{s}$，令 $B(\boldsymbol{s})$ 表示漏洞被发现这一事件。一个重要变量是漏洞被发现的概率 $\Pr(B(\boldsymbol{s})) = 1 - (1-q)^S$，该概率取决于参与搜索的代理人总数。

策略组合记为 $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n)$，其中策略 $\sigma_i \colon [\underline{c}, \overline{c}] \to \{0,1\}$ 将代理人的私人信息映射为一项行动。当不会引起混淆时，我们用 σ 表示对称策略组合 $(\sigma, \ldots, \sigma)$，并采用关于 $\boldsymbol{\sigma}(\boldsymbol{c})$、$\boldsymbol{\sigma}_{-i}$、$\boldsymbol{c}_{-i}$ 和 $\boldsymbol{\sigma}_{-i}(\boldsymbol{c}_{-i})$ 的常用记号约定。给定策略组合 $\boldsymbol{\sigma}$，漏洞被发现的事前概率为 $\mathbb{E}[\Pr(B(\boldsymbol{\sigma}(\boldsymbol{c})))]$。

一类重要的策略是阈值策略。阈值为 $\hat{c}$ 的阈值策略记为 $\sigma_{\hat{c}}$，其特征是

$$\sigma_{\hat{c}}(c_i) = \begin{cases} 1 & \text{if} \quad c_i \leq \hat{c} \\ 0 & \text{if} \quad c_i > \hat{c} \end{cases}. \tag{3}$$

[4]该模型可以扩展为允许 $\underline{c} < 0$。[5]我们在扩展模型中考虑多个奖项，并表明赢家通吃竞赛能够诱导代理人实现最高水平的参与。

对于某个阈值向量 $\hat{\boldsymbol{c}} = (\hat{c}_1, \ldots, \hat{c}_n)$，阈值策略组合记为 $\boldsymbol{\sigma}_{\hat{\boldsymbol{c}}} = (\sigma_{\hat{c}_1}, \ldots, \sigma_{\hat{c}_n})$。在阈值策略组合下，漏洞被发现的事前概率为

$$\mathbb{E}[\Pr(B(\boldsymbol{\sigma}_{\hat{\boldsymbol{c}}}(\boldsymbol{c})))] = 1 - \prod_i (1 - qF(\hat{c}_i)). \tag{4}$$

如果所有代理人都采用相同的阈值策略 $\sigma_{\hat{c}}$，那么事前发现漏洞的概率为

$$P(\hat{c}, q, n) \equiv 1 - (1 - qF(\hat{c}))^n, \tag{5}$$

我们将其称为成功概率。

策略组合 $\boldsymbol{\sigma}^*$ 是贝叶斯纳什均衡（BNE），当且仅当对于所有 i、c 和 s_i，

$$\mathbb{E}[u_i(\sigma_i^*(c_i), \boldsymbol{\sigma}_{-i}^*(\boldsymbol{c}_{-i}), c_i) | c_i = c] \geq \mathbb{E}[u_i(s_i, \boldsymbol{\sigma}_{-i}^*(\boldsymbol{c}_{-i}), c_i) | c_i = c].$$

3 均衡分析

本节分析该博弈。我们将刻画均衡，讨论一些重要的比较静态分析，并考察代理人数量大幅增加时博弈的极限行为。

3.1 均衡刻画

我们将按如下方式展开。首先，我们证明任何均衡策略都必须是阈值策略。其次，我们证明，如果阈值成本向量位于内部，则它满足一组无差异条件。第三，我们提出一组条件，以确保均衡唯一且对称。最后，我们为唯一均衡推导出一个简单直观的不动点条件。

第一个结果表明，均衡策略是阈值策略。

命题1. $\boldsymbol{\sigma}^* = \boldsymbol{\sigma}_{\boldsymbol{c}^*}$ 对某个阈值向量 $\boldsymbol{c}^* = (c_1^*, \ldots, c_n^*)$成立。

因此，我们可以将博弈视为策略就是阈值，而均衡策略的刻画归结为均衡阈值向量 $\boldsymbol{c}^* = (c_1^*, \ldots, c_n^*)$ 的刻画。进一步假设均衡阈值向量位于内部，即对所有 i，$c_i^* \in (\underline{c}, \overline{c})$。那么，它必须满足以下无差异条件系统：对所有 i，

$$c_i^* = V\Psi(\boldsymbol{c}_{-i}^*), \tag{6}$$

其中，函数 $\Psi : [\underline{c}, \overline{c}]^{n-1} \to \mathbb{R}$ 由下式给出

$$\Psi(\hat{\boldsymbol{c}}_{-i}) \equiv q \sum_{K \subseteq N \setminus \{i\}} \left\{ \prod_{j \in K} F(\hat{c}_j) \prod_{j \notin K} (1 - F(\hat{c}_j)) \left[\sum_{t=0}^{|K|} \binom{|K|}{t} q^t (1-q)^{|K|-t} \frac{1}{t+1} \right] \right\}. \tag{7}$$

事实上，$\Psi(\hat{\boldsymbol{c}}_{-i})$表示在其他代理人 i 采用由某个阈值向量 $\hat{}$ $n-1$ 刻画的阈值策略时，代理人$\boldsymbol{c}_{-i}$成为获胜者的概率。[6] (6)中的条件因此将每个代理人搜索的成本与预期收益相等起来，刻画了这样一个阈值成本：在该成本下，代理人搜索与不搜索漏洞无差异。以下命题给出了 Ψ的一些重要性质。

命题 2。以下性质成立

(i) $\Psi(\hat{c}_1,\ldots,\hat{c}_{i-1},\hat{c}_{i+1},\ldots,\hat{c}_n)=\Psi(\hat{c}_{\pi(1)},\ldots,\hat{c}_{\pi(i-1)},\hat{c}_{\pi(i+1)},\ldots,\hat{c}_{\pi(n)})$ *for any permutation* π,

(ii) $\partial\Psi(\hat{\boldsymbol{c}}_{-i})/\partial\hat{c}_j<0$ 对所有 j 以及所有 $\hat{\boldsymbol{c}}_{-i}\in[\underline{c},\overline{c}]^{n-1}$ 均成立,

(iii) $\Psi(\underline{c},\ldots,\underline{c})=q$以及 $\Psi(\overline{c},\ldots,\overline{c})=\frac{1-(1-q^n)}{n}$。

第一个性质表明，Ψ 具有对称性。由于代理人事前对称，代理人的身份并不重要。第二个性质是，Ψ 关于其所有自变量均严格递减。这是因为，其他代理人采用更高的阈值会提高他们的搜索概率，进而降低代理人 i 赢得奖品的概率。为了得到更明确的预测，我们现在对 Ψ施加两个假设。

假设 1。$|\partial\Psi(\hat{\boldsymbol{c}}_{-i})/\partial\hat{c}_j|\neq 1/V$对所有 j 以及所有 $\hat{\boldsymbol{c}}_{-i}\in[\underline{c},\overline{c}]^{n-1}$ 均成立。

假设 2. $\underline{c}<V\Psi(\underline{c},\ldots,\underline{c})=qV$和 $V\frac{1-(1-q^n)}{n}=V\Psi(\overline{c},\ldots,\overline{c})<\overline{c}$。

第一个假设确保均衡是唯一的。请注意，由于选择阈值实际上就是代理人 i的策略，因此函数 $V\Psi(\boldsymbol{c}_{-i})$ 可以解释为代理人 i在其他代理人选择的阈值给定时的最佳响应函数。 假设 1 进而要求该最佳响应函数的斜率绝不等于 1。这确保最佳响应函数只相交一次，从而产生唯一均衡。 假设 2 对参数值加以限制，以确保（6）中的无差异条件系统的解位于内部。在这两个假设下，我们现在刻画漏洞赏金博弈的唯一均衡。为此，定义 $\Phi:\ [\underline{c},\overline{c}]\times(0,1]\times\mathbb{N}\to\mathbb{R}$ 如下：

$$\Phi(\hat{c},q,n)\equiv\frac{P(\hat{c},q,n)}{nF(\hat{c})}=\frac{1-(1-qF(\hat{c}))^n}{nF(\hat{c})} \tag{8}$$

若 $\hat{}c>\underline{c}$ 且 $\Phi(\underline{c}、\ q、\ n)\equiv q$。事实上，$\Phi$ 是代理人 i 获胜的概率，条件是其他所有代理人都采用相同的阈值策略。换言之，Φ 是 Ψ 沿“对角线”的“切片”，即 Ψ 的自变量都相同时的情形。如（8）所定义，Φ 具有

[6] $\Psi(\hat{\boldsymbol{c}}_{-i})$ 实际上是对 $p(\boldsymbol{s}_{-i})$ 的成本分布取期望。在其他代理人遵循阈值策略的情况下，

一种直观的解释，即它等于漏洞被发现的概率除以进行搜索的代理人预期数量。原因在于，只要漏洞被发现，参与搜索的代理人获得奖励的机会就相同。我们得到

命题3。在假设 1 和假设 2下，唯一均衡为 $\boldsymbol{\sigma}_{c^*}$。均衡阈值 $c^* \equiv c^*(V,\ q,\ n) \in (\underline{c},\ \overline{c})$ 是以下方程的解

$$c^* = V\Phi(c^*, q, n). \tag{9}$$

下文将 $\boldsymbol{\sigma}_{c^*}$ 简称为均衡。为便于阐述，在适当情况下，我们省略 c^* 和 Φ 对 V、q以及 n 的显式依赖关系。条件（9）是（6）的特例。这是一个无差异条件，体现了均衡中类型为 c^* 的代理人在搜索与不搜索之间无差异。左边是搜索成本，右边是期望奖励：V乘以 Φ。

3.2 比较静态分析

现在我们对均衡进行比较静态分析。为此，我们首先陈述 $\Phi(c,q,n)$ 的性质。随后可得出 $c^*(V,q,n)$ 的性质，因为 c^* 是 $V\Phi(c,q,n)$ 的唯一不动点。我们得到关于 c^* 的以下比较静态分析结果。

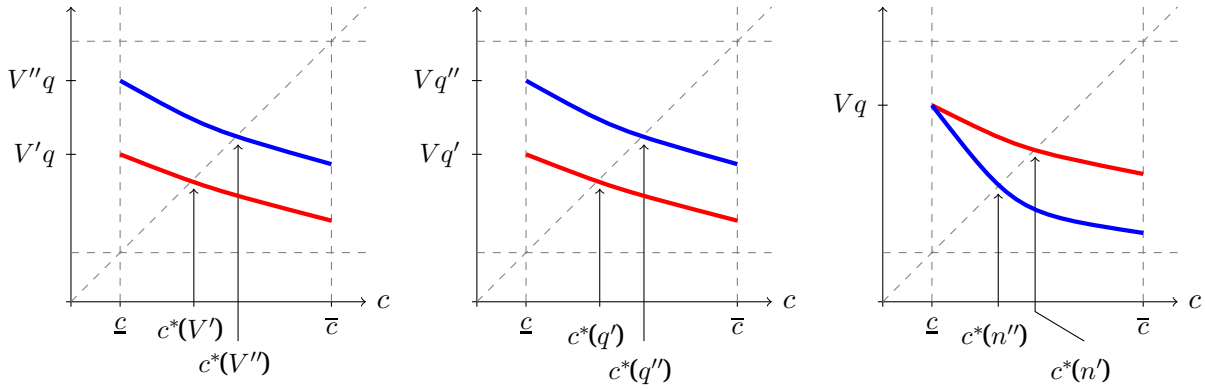
命题4. $\Phi(c,q,n)$关于 c 严格递减，关于 q严格递增。对于$c > \underline{c}$，$\Phi(c,q,n)$关于 n严格递减。均衡阈值 $c^*(V,q,n)$

(i) 关于 V递增，

(ii) 关于 q递增，且

(iii) 关于 n递减。

这些结果符合直觉。如果奖品 V 增加，代理人会更有动力进行搜索。成本较高的代理人现在也会进行搜索，而在此之前他们不会这样做。当 q（即在进行搜索的条件下发现漏洞的概率）增加时，情况也一样。最后，参与漏洞搜索的代理人越多，竞争越激烈，从而降低了代理人赢得奖品的概率。图 1 展示了 $V\Phi$ 如何随 V、q和 n变化。此外，图 1 展示了均衡阈值 $c^*(V,q,n)$的比较静态分析，该阈值是 $V\Phi(c,q,n)$的不动点。图 1 的图（a）表明，对于 $V' < V''$，作为 c 函数的 $V\Phi$ 会随着 V增加而上移，同时保持 q 和 n 不变。因此，我们有 $c^*(V') < c^*(V'')$。图（b）展示了 $q' < q''$的情况。最后，图（c）表明 $V\Phi$ 会随着 n 增加而下移，因此对于 $n' < n''$，我们有$c^*(n'') < c^*(n')$。



(a) $V''\Phi(c)$ 和 $V'\Phi(c)$　(b) $V\Phi(c, q'')$ 和 $V\Phi(c, q')$　(c) $V\Phi(c, n'')$ 以及 $V\Phi(c, n')$

图 1: $c^*(V, q, n)$的比较静态分析。

3.3 成功概率

对于漏洞悬赏计划的设计，我们关注的量是均衡下的成功概率，$P(c^*(V, q, n)\ q, n) = 1 - (1 - qF(c^*(V, q, n)))^n$，为简便起见，我们将其记为 $P^*(V, q, n)$。[7] 均衡成功概率如何随模型参数变化？我们有如下结果。

命题5. $P^*(V, q, n)$随 V和 q增加，而随n增加或减少。

显然，P^* 会随着 V 和 q 的增加而增加。然而，关于 n的比较静态分析则更为有趣。结果表明，颇令人意外的是，成功概率可能会随着代理人数量 n的增加而降低，也可能随之增加。直觉上，发现漏洞的概率应当随着代理人数量的增加而上升。然而，正如我们所见，更多的代理人会导致竞争加剧，从而降低参与阈值。也就是说，代理人会挤出彼此搜索的个体激励。根据成本分布和模型参数的具体设定，两种力量中的任一种都可能占据主导地位。

由于 $P^*(n) = 1 - (1 - qF(c^*(n))^n$，当 n 增加时，挤出效应可能占据主导地位的渠道有两种。第一种渠道通过成本分布 F 发挥作用，因为它会放大 $c^*(n)$的下降。第二种渠道则是直接通过 $c^*(n)$的大幅下降发挥作用。当 $c^*(n)$一开始就很高时，就会出现这种情况，这可能是由于奖励较高，使得之后每个 $c^*(n)$相对于 n的增加都会大幅下降。以下示例说明了这两种渠道。

例1。考虑 $F(c) = c^{20}$ 对于 $0 \le c \le 1$，并令 $q = 1$ 和 $V = 1$。表1a给出了 $c^*(n)$ 和 $P^*(n)$ 的数值。均衡阈值 $c^*(n)$ 为

[7]同样，为了便于阐述，我们省略在分析过程中保持不变的 P^* 自变量。例如，当有 n 个代理人时，我们分别用 $c^*(n)$和 $P^*(n)$表示均衡阈值和均衡中的成功概率，并注意到 V 和 q 是固定的。

n	$c^*(n)$	$P^*(n)$
2	0.9151	0.3106
3	0.8951	0.2924
4	0.8828	0.2917
5	0.8739	0.2948
6	0.8669	0.2989

(a) $F(c) = c^{20}$、 $q = 1$和 $V = 1$。

n	$c^*(n)$	$P^*(n)$
2	0.9998	0.9999
3	0.8136	0.9935
4	0.7042	0.9923
5	0.6301	0.9931
6	0.5755	0.9941

(b) $F(c) = c$、 $q = 1$和 $V = 1.999$。

表1： $c^*(n)$ 和 $P^*(n)$ 对于 例1 和 例 2。

按照预期，随着 n 递减。对于 $P^*(n)$，我们可以看到，它在 $n = 2$ 到 $n = 4$ 期间递减，并在 $n \geq 5$ 及以后递增。 □

直观地说，例1 展示了这样的分布函数：预计大多数个体的成本接近 1，而人才池中预计只有少数极具天赋的代理人。此时，扩大代理人人才池可能会适得其反，因为随着阈值下降，参与的预期众包群体大幅缩小，从而降低找到漏洞的可能性。 例 2 考虑了高奖励下的均匀成本分布。由于 V 较高，阈值起初接近 1，并且相对于拥有更多代理人的直接影响而言会急剧下降。

例 2。 考虑 $F(c) = c$ 对于 $0 \leq c \leq 1$，并令 $q = 1$ 和 $V = 1.999$。 表1b展示了数值 $c^*(n)$ 和 $P^*(n)$。均衡阈值 $c^*(n)$ 按预期随 n 递减。对于 $P^*(n)$，我们看到它在 $n = 2$ 至 $n = 4$ 之间递减，并在 $n \geq 5$ 之后递增。

□

我们的分析表明，漏洞赏金系统的设计者应密切关注受邀代理人的数量，以权衡代理人数量过多所产生的挤出效应。

为进一步考察其中发挥作用的力量，我们现在将 n 视为连续变量，并计算[8]

$$\frac{\mathrm{d}P^*(n)}{\mathrm{d}n} = (1 - qF(c^*(n)))^n \left[\frac{nqf(c^*(n))}{1 - qF(c^*(n))} \frac{\mathrm{d}c^*(n)}{\mathrm{d}n} - \ln\left(1 - qF(c^*(n))\right) \right]. \tag{10}$$

由（10）可知，$\mathrm{d}P^*(n)/\mathrm{d}n \geq 0$ 当且仅当 $\mathrm{d}c^*(n)/\mathrm{d}n$的绝对值不太大时，而根据命题4，该值为负。利用均衡条件（9），我们可以推导出以下命题。

命题6。$\mathrm{d}P^*(n)/\mathrm{d}n \geq 0$ 当且仅当

$$\frac{(1 - qF(c^*(n)))\ln\left(1 - qF(c^*(n))\right)}{-qF(c^*(n))} \geq \frac{1}{1 + \frac{F(c^*(n))}{c^*(n)f(c^*(n))}}. \tag{11}$$

[8]详细推导见命题6的证明。

3.4 大型竞赛

在本节中，我们固定所有参数，并考察均衡的渐近行为。在整节中，为便于记号起见，当邀请 n代理人参与时，我们用 $c_n = c^*(n)$和$P_n = P^*(n)$分别表示均衡阈值和均衡成功概率。我们的第一个结果表明，均衡阈值收敛于 $\underline{c}$。

命题 7。对于任意 $\underline{c} \geq 0$，我们有 $c_n \to \underline{c}$。

换言之，随着代理人数量增加，搜索的个体激励会减弱；在极限情况下，只有成本最低的代理人会进行搜索。Archak 和 Sundararajan（2009）在全支付拍卖的背景下也指出了类似结果。接下来值得关注的问题是 P_n的行为。我们将证明，尽管搜索的个体激励会减弱，总体激励却会增强。

命题 8。以下结论成立：

(i) 如果 $\underline{c} = 0$，那么 $nF(c_n) \to \infty$。如果 $\underline{c} > 0$，那么

$$nF(c_n) \to \kappa(\underline{c}), \tag{12}$$

其中，常数 $\kappa \equiv \kappa(\underline{c})$ 是满足 $\underline{c} = V\frac{1-e^{-q\kappa}}{\kappa}$ 的唯一解。

(ii) 如果 $\underline{c} = 0$，那么 $P_n \to 1$。如果 $\underline{c} > 0$，那么

$$P_n \to 1 - e^{-q\kappa(\underline{c})}. \tag{13}$$

命题 8 对漏洞赏金计划的成功具有重要影响。合理地说，$\underline{c} > 0$ 因为即使是高能力参与者也必须付出努力才能找到漏洞。那么，即使邀请无限人群来寻找漏洞，也不能保证一定能找到漏洞。原因在于——鉴于预期中的激烈竞争——只有相对较少的参与者会决定参加，因此漏洞以一定概率无法被找到。然而，如果能够邀请一大群具有部分内在动机或出于声誉考量的参与者，那么也可能成为可能，并且还可能确保找到漏洞。

接下来，我们考察收敛速率。我们有如下结果。

命题 9。以下结论成立：

(i) $c_nF(c_n) \in \Theta(n^{-1})$,

(ii) 如果 $\underline{c} > 0$，那么 $F(c_n) \in \Theta(\{v5)$。

命题 9 的一个推论是，对于 $F(c) = c^\alpha$ 在 $[0,1]$, $\alpha > 0$, $c_n \in \Theta(n^{-\frac{1}{1+\alpha}})$ 的情形，以及对于 $F(c) = \left(\frac{c-\underline{c}}{\overline{c}-\underline{c}}\right)^\alpha$ 在 $[\underline{c}, \overline{c}]$, $\alpha > 0$, $c_n - \underline{c} \in \Theta(n^{-\frac{1}{\alpha}})$ 的情形。特别是，这意味着对于 $\mathcal{U}[0,1]$， c_n 以 $n^{-\frac{1}{2}}$ 的速率收敛到 0；而对于 $\mathcal{U}[\underline{c}, \overline{c}]$， c_n 以速率 n^{-1} 收敛到 $\underline{c}$。

现在我们研究 P_n 的尾部行为。在上一节中，我们已经证明，成功概率可能随着代理人数量的增加而上升或下降。然而，在这两个例子中，我们都看到，当 n 足够大时，P_n 最终会增加。这是一个普遍性质，下面我们将对此进行探讨。为帮助得出这一结果，我们针对成本分布引入一个额外假设。

假设 3。$\liminf_{c \to \underline{c}^+} \frac{F(c)}{cf(c)} = \delta$，其中 $\delta > 0$。

于是我们得到以下结果。

命题 10。设 F 满足假设 3。则存在 N，使得对于所有 $n > N$， P_n 均为递增。

这里有几点需要说明。注意， $cf(c)/F(c)$ 是累积分布函数 F 的弹性。因此，假设 3 表明，F 的弹性的倒数不会在 c 趋近于支撑集下界时趋于零。换言之，我们要求 F 在 $\underline{c}$ 附近不会变化得过于剧烈。假设 3 对一大类分布成立。例如，对于 $F(c) = c^\alpha$， $\alpha > 0$，其支撑集为 $[0,1]$,，我们有 $\frac{F(c)}{cf(c)} = \frac{1}{\alpha} > 0$。它对贝塔分布和指数分布同样成立。最后，假设 3 是一个充分条件，我们推测“P_n 最终增加”这一结论在更一般的情形下也成立。

3.5 均匀成本分布

本节考虑均匀成本分布这一特殊情形。给定 $0 \leq \underline{c} < \overline{c} < \infty$，支撑集上的累积分布函数由 $F(c) = \frac{c-\underline{c}}{\overline{c}-\underline{c}}$ 给出。于是有

$$\Phi(c,q,n) = \begin{cases} \frac{\overline{c}-\underline{c}}{n(c-\underline{c})}\left[1 - \left(1 - \frac{q}{\overline{c}-\underline{c}}(c-\underline{c})\right)^n\right] & \text{for} \quad \underline{c} < c \leq \overline{c} \\ q & \text{for} \quad c = \underline{c}. \end{cases} \tag{14}$$

容易看出，在适当的定义域上， Φ 关于 c 严格递减，关于 q 严格递增，并且关于 n 严格递减。

为说明我们关于极限行为的结果，我们现在考虑两个具有均匀成本分布的数值示例。令 $V = 1$ and $q = 1/2$。首先，考虑 $F \sim \mathcal{U}[0,1]$。均衡阈值 $c^*(n)$ 满足

$$(c^*(n))^2 n = 1 - (1 - c^*(n)/2)^n. \tag{15}$$

n	$c^*(n)$	$P^*(n)$
10	0.2787	0.7771
100	0.0997	0.9939
1000	0.0316	0.9999
2000	0.0224	0.9999

(a) $F \sim \mathcal{U}[0,1]$

n	$c^*(n)$	$P^*(n)$
10	0.3780	0.4839
100	0.2767	0.7395
1000	0.2531	0.7904
2000	0.2516	0.7936

(b) $F \sim \mathcal{U}[1/4, 5/4]$

表 2： $c^*(n)$ 和 $P^*(n)$ 对于 (a) $\mathcal{U}[0,1]$ 和 (b) $\mathcal{U}[1/4, 5/4]$。

根据命题 7和命题 8， $c^*(n) \to 0$ 以及 $P^*(n) \to 1$ 对于该分布，因为$\underline{c} = 0$ 且 $\kappa(0) = \infty$。

现在，考虑 $F \sim \mathcal{U}[1/4, 5/4]$。均衡阈值 $c^*(n)$ 满足

$$nc^*(n)(c^*(n) - 1/4) = 1 - (9/8 - c^*(n)/2)^n. \tag{16}$$

对于此分布， $c^*(n) \to \frac{1}{4}$和 $P^*(n) \to 1 - e^{-\frac{1}{2}\kappa} \approx 0.797$，因为 $\kappa = 3.188$。表 2 展示了 $c^*(n)$ 和 $P^*(n)$ 在两种设定下的数值，适用于$n = 10$、100、1000和2000。

4 扩展

本节将进一步分析漏洞赏金博弈。首先，我们研究加入一个非策略性代理人（即专家）如何改变均衡行为。其次，我们探讨在软件中加入一个漏洞如何提高代理人的积极性。第三，我们将分析扩展到多个奖项的情况。最后，我们展示了即使没有外加假设，非对称均衡也可能存在。

4.1 加入专家

接下来，我们考察增加一名专家是否会改善扩大后的群体（众包群体加专家）的漏洞发现。其权衡关系是显而易见的。众包群体往往会减少搜索，但专家的搜索可能会对此进行过度补偿。因此，假设存在一名非策略性代理人，即一名专家，他无论成本如何都会进行搜索，并以概率 $q_e \in (0,1]$, 这是共同知识）发现漏洞。如果漏洞赏金系统设计者将搜索外包给专家并支付其成本，就可能出现这种情况。请注意，我们并不假设 q_e（我们称之为专业能力）大于 q。这使我们能够描述这样一种情形：内部安全团队，即“专家”，未必比众包群体更有能力发现漏洞。[9] 我们进一步假设专家

[9]事实上，这种情况在实践中很常见，正如Malladi 和 Subramanian (2020)所报告的：“系统日益复杂，漏洞的性质也变得难以预测，从而限制了企业追踪关键弱点的能力。有鉴于此，企业越来越多地借助漏洞赏金计划

以与策略性代理人相同的方式获得奖励。[10]

现在我们刻画带专家的博弈的均衡。为便于阐述，我们只关注对称均衡。与原始博弈（没有专家参与的漏洞搜索）类似，关键量是代理人在带专家的博弈中赢得奖品的概率。为推导这一量，记为 Φ^e，我们根据两种情况对获胜概率进行条件化：专家未发现漏洞（概率为 $1-q_e$）和专家发现漏洞（概率为 q_e）。经过一些代数运算，我们得到

$$\Phi^e(c,q,q_e,n) \equiv \Phi(c,q,n) - q_e \frac{1-(1-qF(c))^n(1+nqF(c))}{n(n+1)qF(c)^2} \tag{17}$$

如果 $c > \underline{c}$ 且 $\Phi^e(\underline{c},\ q,\ q_e,\ n) \equiv q(1-q_e/2)$。现在，我们假设带专家的博弈满足与假设 2 类似的条件，以确保均衡的内部性，并得到

命题11. 假设 $\underline{c} < \Phi^e(\underline{c},q,q_e,n)$ 和 $\Phi^e(\overline{c},q,q_e,n) < \overline{c}$。那么，带专家的博弈的唯一对称均衡 $q_e \in (0,1]$ 是 $\boldsymbol{\sigma}_{c^e}$。均衡阈值$c^e \equiv c^e(V,q,q_e,n) \in (\underline{c},\overline{c})$ 是下式的解

$$c^e = V\Phi^e(c^e,q,q_e,n). \tag{18}$$

将 $c^e(q_e)$ 记为存在专家 q_e 时博弈的均衡阈值，将 $c^*(n)$ 记为存在 n 个代理人的原始博弈的均衡阈值。由于式（17）中的第二项为正，因此可得 $c^e(q_e) < c^*(n)$，从而 $\Phi^e < \Phi$ 是 c的函数。直观而言，专家挤出了代理人的搜索努力，因为随着回报前景下降，决定进行搜索的代理人数量减少了。此外，我们有 $\lim_{q_e\to 0} c^e(q_e) = c^*(n)$，因为当 $q_e \to 0$时，Φ^e 趋近于 Φ。这意味着对于足够小的 q_e，我们有

$$c^*(n+1) < c^e(q_e) < c^*(n). \tag{19}$$

此外，由于专家是不论成本如何都会进行搜索的非策略性代理人，因此加入一个具有 $q_e = q$ 的专家，比加入一个额外代理人更能挤出个体的搜索激励。也就是说，我们有

$$c^e(q) < c^*(n+1) < c^*(n). \tag{20}$$

式（19）和（20）共同表明，存在一个临界专业水平 $\hat{}q_e \in$（0，q），使得带专家的博弈中的均衡阈值等于带有额外策略性代理人的博弈中的均衡阈值，即 c^e（$\hat{}q_e$）$= c^*$（$n+1$）。下一个命题

[漏洞赏金计划]，以通过众包群体发现并修复漏洞。”[10]也就是说，发现漏洞的专家和策略性代理人以相同概率获得奖励。如果专家发现了漏洞（若确实发现），且其发现时间也在$[0,T]$上均匀分布，就会出现这种情况。另一种奖励方案是，在专家发现漏洞时由专家保留奖品。然而，在该方案下，均衡仅满足 $c = V(1-q_e)\Phi(c)$。

总结了上述分析。

命题 12。临界专业水平由 $\hat{q}_e = qF(c^*(n+1))$ 给出。如果 $q_e < \hat{q}_e$，则 $c^*(n+1) < c^e(q_e)$；而如果 $q_e > \hat{q}_e$，则 $c^e(q_e) < c^*(n+1)$。

现在考察专家在场时的成功概率。该概率为

$$P^e(q_e, n) \equiv (1 - q_e)P(c^e(q_e), q, n) + q_e, \tag{21}$$

由两项组成。如果专家未发现漏洞，那么众包群体以 $P(c^e(q_e), q, n)$ 的概率成功；而如果专家成功，成功则是必然的。这两项体现了两种效应。首先是挤出效应，它会降低参与度，从而降低发现漏洞的概率。其次是专家搜索的直接收益，它会提高发现漏洞的概率。因此，自然的问题是，第一种效应还是第二种效应占主导地位，也就是说，$P^e(q_e, n)$ 是大于还是小于 $P^*(n)$。

我们先考虑极端情形。如果 $q_e = 1$，那么由于直接收益占主导地位，成功是必然的。另一方面，$P^e(q_e, n) \to P^*(n)$，因为两种效应都消失了。于是人们可能会推测，随着专业能力的提高，发现漏洞的概率也会提高。事实证明并非如此。为说明这一点，考虑 例1 或例 2 中的设定，并令 $q_e = \hat{q}_e$。根据命题 12以及 $\hat{}$ 的定义q_e，我们有

$$\begin{aligned} P^e(\hat{q}_e, n) &= (1 - \hat{q}_e)P(c^e(\hat{q}_e), q, n) + \hat{q}_e \\ &= (1 - \hat{q}_e)(1 - (1 - qF(c^e(\hat{q}_e)))^n) + \hat{q}_e \\ &= 1 - (1 - \hat{q}_e)(1 - qF(c^e(\hat{q}_e)))^n \\ &= P(c^*(n+1)). \end{aligned} \tag{22}$$

因此，聘用一名专家的成功概率等于增加一名策略性代理人时的成功概率。表1中的数值随后表明，增加一名外部专家可能会使成功概率下降或上升。

这表明，q_e 直接收益或挤出效应的中间值可能占主导地位。换言之，就专业能力而言，成功概率是非单调的。这意味着，在聘用内部团队时，必须确保其专业能力相对于众包群体足够高。

4.2 添加 ArtificialBug

在本节中，我们允许设计者向软件中添加一个人工漏洞，该漏洞为设计者所知，但漏洞悬赏计划的参与者并不知情。这样做的目的是提高代理人参与有成本的搜索过程的积极性。

不利之处在于，设计者的支出会增加，因为可能需要支付更多奖励。

我们假设，发现人工漏洞这一事件与发现真实漏洞这一事件是随机独立的。由于设计者对真实漏洞一无所知，这一假设是合理的。设计者选择代理人发现此类已知漏洞的概率，该概率记为 q_a。设计者可以通过让参与者更容易（更难）发现漏洞悬赏计划中的人工漏洞，来选择较高（较低）的值。

因此，我们假设，一旦代理人决定投资于有成本的漏洞搜索，以概率 q ，他/她会发现真实漏洞；以概率 q_a ，他/她会发现人工漏洞。鉴于搜索被视为对发现漏洞的一项投资，而在我们的模型中这是一项二元决策，这一假设是合理的。存在已知漏洞时的均衡条件为 $c^* = V\Phi(c^*, q, n) + V_a\Phi(c^*, q_a, n)$，其中 V_a 是人工漏洞被发现时给予代理人的奖励。

我们从 命题4 可以看出， $\Phi(c, q, n)$ 随 q增大。因此，如果委托人想最大化发现真实漏洞的概率，最优做法是将其设为 $q_a = 1$ 。将 $q_a = 1$设为该值后，参与漏洞悬赏计划的代理人人数达到最大，从而发现真实漏洞的机会也最大。因此， q_a 的最优选择对应于添加一个极其容易的漏洞，只要每个人付出搜索成本，所有人都能以概率 1 找到它。

当然，添加一个极其容易的漏洞会增加设计者需要支付给参与者的预期奖励。因此，接下来我们将考察更广泛的目标：委托人希望在考虑真实漏洞的成本以及奖励支付的情况下最大化其效用。假设委托人从发现真实漏洞中获得效用 W 。那么，设计者的问题可以写为：

$$\max_{V_a, q_a} (W - V)P(c^*, q, n) - V_a P(c^*, q_a, n) \quad \text{subject to} \quad c^* = V\Phi(c^*, q, n) + V_a\Phi(c^*, q_a, n).$$

让我们用一个简单的例子来说明这些权衡。假设 $F(c) = c$ 且令$W = 4$ 和 $V = 1$, $q = 0.5$，以及 $n = 2$。如果不插入已知漏洞，即 $V_a = 0$ 或$q_a = 0$，均衡为 $c^* = 4/9 \approx 0.444$ ，设计者的收益为 $96/81 \approx 1.185$。若加入一个参数为 $V_a = 1$ 和 $q_a = 0.3$的已知漏洞，则 $c^* = 0.684$ ，收益为 1.333。

考虑在 $n \to \infty$ 时插入一个已知漏洞的问题。我们知道，无论参数如何， c_n 都会趋于 $\underline{c}$ 。现在推导目标函数的渐近行为。均衡条件收敛于

$$\underline{c} = V\frac{1 - e^{-q\kappa}}{\kappa} + V_a\frac{1 - e^{-q_a\kappa}}{\kappa}$$

其中，$\kappa = \kappa(\underline{c}, q, q_a, V, V_a)$ 关于 V_a 和 q_a 均递增。目标函数现在为

$$\max_{V_a, q_a} (W - V)(1 - e^{-q\kappa}) - V_a(1 - e^{-q_a\kappa}) \quad \text{subject to} \quad \underline{c} = V\frac{1 - e^{-q\kappa}}{\kappa} + V_a\frac{1 - e^{-q_a\kappa}}{\kappa}.$$

注意，如果 $\underline{c} = 0$，那么 $\kappa = \infty$ 和 V_a 应为 0。如果 $\underline{c} > 0$，则可以如以下示例所示插入一个已知漏洞。

假设 F 的支撑集为 $[1/4, 5/4]$，并令 $W = 4$ 和 $V = 1$，$q = 0.5$。在不插入已知漏洞的情况下，即 $V_a = 0$ 或 $q_a = 0$，则 $\kappa = 3.188$，且设计者的收益为 $3 \cdot 0.797 = 2.390$。若已知漏洞的参数为 $V_a = 1$ 和 $q_a = 0.05$，则 $\kappa = 4.313$，收益为 2.459。

我们已经说明，可以向系统中插入已知漏洞。刻画最优已知漏洞是未来研究的一个课题。

4.3 多个奖项

本节将我们的分析扩展到多个奖项的情形。设置与之前相同，但增加如下规定：如果代理人 i 发现漏洞，并且是第 m 个发现该漏洞的代理人，则代理人 i 将获得奖品 v^m $(m = 1, \ldots\ldots, n)$。我们将 $\boldsymbol{v} = (v^1, \ldots\ldots, v^n$ 称为奖项向量，并考虑 $\boldsymbol{v} \in \mathcal{V} \equiv \{\boldsymbol{v} : v^1 \geq \cdots \geq v^n \geq 0$ 和 $\sum_j v^j = V\}$。代理人 i 从（1）获得的收益现在变为

$$u_i(s_i, \boldsymbol{s}_{-i}, c_i) = s_i \left(\sum_{m=1}^{n} p^m(\boldsymbol{s}_{-i}) v^m - c_i \right), \tag{23}$$

其中，$p^m(\boldsymbol{s}_{-i})$ 现在表示在进行搜索的条件下，代理人 i 是第 m 个发现漏洞的代理人的概率。$p^m(\boldsymbol{s}_{-i})$ 的表达式为

$$p^m(\boldsymbol{s}_{-i}) = \begin{cases} q \sum_{t=m-1}^{S_{-i}} \binom{S_{-i}}{t} q^t (1-q)^{S_{-i}-t} \frac{1}{t+1} & \text{if} \quad m - 1 \leq S_{-i} \\ 0 & \text{if} \quad m - 1 > S_{-i}. \end{cases} \tag{24}$$

注意，赢家通吃竞赛是一个特殊情况，其中 $v^1 = V$ 和 $p^1(\boldsymbol{s}_{-i}) = p(\boldsymbol{s}_{-i})$ 如（2）所示。

现在，我们刻画采用（23）中修正后收益的博弈的均衡。我们首先注意到，命题 1 仍然成立，其证明基本无需修改。均衡阈值向量 $\boldsymbol{c}^*$（如果是内点）现在必须满足以下无差异条件系统：对所有 i，$c_i^* = \sum_{m=1}^{n} v^m \Psi^m(\boldsymbol{c}_{-i}^*)$，其中

对于 $m=1$，...，n，$\Psi^m:\ [\underline{c},\overline{c}]^{n-1}\to\mathbb{R}$ 由下式给出

$$\Psi^m(\hat{\boldsymbol{c}}_{-i})\equiv q\sum_{\substack{K\subseteq N\setminus\{i\}\\ |K|\geq m-1}}\left\{\prod_{j\in K}F(\hat{c}_j)\prod_{j\notin K}(1-F(\hat{c}_j))\left[\sum_{t=m-1}^{|K|}\binom{|K|}{t}q^t(1-q)^{|K|-t}\frac{1}{t+1}\right]\right\}. \tag{25}$$

Ψ^m 表示在其他 $n-1$ 位代理人采用某些阈值策略且确实满足 $\Psi^1=\Psi$的情况下，代理人 i成为第 m位发现该漏洞的代理人的概率。 Ψ^m的函数有以下一些重要性质。

命题13。函数族 $\Psi^m(m=1,\ldots,n)$具有以下性质：

(i) $\sum_{m=1}^n\Psi^m=q$,

(ii) $\Psi^m>\Psi^{m+1}$,

(iii) Ψ^m 关于 c_j 严格递减，当且仅当 $m=1$,

(iv) $\Psi^1(\underline{c},\ldots,\underline{c})=q$ 且 $\Psi^1(\overline{c},\ldots,\overline{c})=\frac{1-}{(1-q\ n)}$，(v) 对于 $m\neq1$，$\Psi^m(\underline{c},\ldots,\underline{c})=0$ 且 $\Psi^m(\overline{c},\ldots,\overline{c})=q\sum_{t=m-1}^{n-1}\binom{n-1}{t}q^t(1-\frac{n}{}q)^{n-1-t}\frac{1}{t+1}$。

有必要作出一些说明。首先，由于代理人一旦发现漏洞，就必然会赢得某种奖金（不一定为正），$\sum_{m=1}^n\Psi^m=q$。其次，赢得一等奖的概率高于赢得二等奖的概率。其直觉是，对于固定数量的发现漏洞的代理人，代理人 i 的排名是均匀随机的。在此情况下，只要代理人 i 发现漏洞，无论还有多少其他代理人也发现了漏洞，一等奖始终对其可得。然而，只有在至少有另一名代理人发现漏洞时，二等奖才可获得。这一推理表明，$\Psi^m>\Psi^{m+1}$。第三，尽管随着参与者数量增加，赢得一等奖的概率会下降，但赢得其他奖金的概率可能会上升。也就是说，对于 $m\neq1$而言，Ψ^m 不一定会随着 c_j 严格递减。为说明这一点，请考虑 Ψ^2。直观地说，如果其他代理人所使用的阈值非常低，那么参与者会更少，从而发现漏洞的代理人也会更少。反过来，这也会使代理人 i 排名第二的概率较低，因为没有人可以排在其前面。提高其他代理人的阈值，会使他们更有可能参与并发现漏洞，从而提高代理人 i 排名第二的机会。

与基准情形一样，我们对 Ψ^m 施加假设，以确保均衡阈值的唯一性和内部性，并刻画博弈的均衡。

命题14。假设 $\sum_m v^m\partial\Psi^m/\partial c_j\neq-1$，且 $\underline{c}<\sum_m v^m\Psi^m(\underline{c})$ 和 $\sum_m v^m\Psi^m(\overline{c})<\overline{c}$。那么，奖项向量为 $\boldsymbol{v}$ 的博弈的唯一均衡是 $\boldsymbol{\sigma}_{c^{\boldsymbol{v}}}$。均衡阈值 $c^{\boldsymbol{v}}$ 是以下方程的解：

$$c^{\boldsymbol{v}}=\sum_{m=1}^n v^m\Phi^m(c^{\boldsymbol{v}}), \tag{26}$$

其中

$$\Phi^m(\hat{c}) \equiv q \sum_{k=m-1}^{n-1} \left\{ \binom{n-1}{k} F(\hat{c})^k (1-F(\hat{c}))^{n-1-k} \left[\sum_{t=m-1}^{k} \binom{k}{t} q^t (1-q)^{k-t} \frac{1}{t+1} \right] \right\}. \tag{27}$$

我们现在聚焦于这一唯一均衡，并考察哪种奖项分配会导致均衡中的最高和最低参与水平。根据命题13的性质以及均衡刻画，可得以下结果。

命题15。对于任意 $\boldsymbol{v} \in \mathcal{V}$,

$$V\Phi^1(\hat{c}) \geq \sum_{m=1}^{n} v^m \Phi^m(\hat{c}) \geq \frac{V}{n} q \tag{28}$$

对于所有 $\hat{c}$，均成立。因此，

(i) 奖项向量 $\boldsymbol{v} = (V, 0, \ldots, 0)$，即赢家通吃竞赛，使 $c^{\boldsymbol{v}}$ 最大，并因此使成功概率最大，

(ii) 奖项向量 $\boldsymbol{v} = (V/n, \ldots, V/n)$ 使 $c^{\boldsymbol{v}}$ 最小，并因此使成功概率最小。

类似的结果也出现在Sarneand Lepioshkin (2017）所研究的另一种简单竞赛模型中。因此，由于 P^* 随 c^* 增加，将竞赛设置为赢家通吃竞赛会使成功概率最大。

不过请注意，允许设置多个奖品时，最大化成功概率通常并非委托人的目标。相反，假设委托人从发现漏洞中获得效用 W。那么，委托人的问题就是最大化

$$U(\boldsymbol{v}) \equiv WP(c^{\boldsymbol{v}}) - \sum_{m=1}^{n} v^m P^m(c^{\boldsymbol{v}}), \tag{29}$$

其中，P^m 是至少有 m 个代理人发现漏洞的概率，其表达式为

$$P^m(c^{\boldsymbol{v}}) = \sum_{k=m}^{n} \binom{n}{k} F(c^{\boldsymbol{v}})^k (1-F(c^{\boldsymbol{v}}))^{n-k} \sum_{t=m}^{k} \binom{k}{t} q^t (1-q)^{k-t}. \tag{30}$$

事实上，$P^1(c^{\boldsymbol{v}}) = P(c^{\boldsymbol{v}})$ 和 $U(\boldsymbol{v})$ 可简化为 $(W - v^1)P(c^{\boldsymbol{v}}) - \sum_{m=2}^{n} v^m P^m(c^{\boldsymbol{v}})$。

最优奖项向量取决于模型的参数，通常并非赢家通吃的结构。刻画奖金的一般最优结构是未来研究的一个方向。这里我们给出一个简单的示例。

示例3。当 $n=2$、 $v^1+v^2=V$时，奖项向量可以由一个变量 v^1刻画。进一步假设 $F\sim\mathcal{U}[0,1]$。委托人最大化

$$U(v^1)=2(W-v^1)qc^{\boldsymbol{v}}-(W+V-2v^1)q^2(c^{\boldsymbol{v}})^2. \tag{31}$$

现在，均衡阈值 $c^{\boldsymbol{v}}$ 满足

$$c^{\boldsymbol{v}}=v^1\underbrace{\left(q-\frac{q^2}{2}c^{\boldsymbol{v}}\right)}_{\Phi^1(c^{\boldsymbol{v}})}+(V-v^1)\underbrace{\frac{q^2}{2}c^{\boldsymbol{v}}}_{\Phi^2(c^{\boldsymbol{v}})}=v^1q-(2v^1-V)\frac{q^2}{2}c^{\boldsymbol{v}}. \tag{32}$$

结合可得

$$U(v^1)=2(W-v^1)q\frac{v^1q}{1+(2v^1-V)\frac{q^2}{2}}-(W+V-2v^1)q^2\left(\frac{v^1q}{1+(2v^1-V)\frac{q^2}{2}}\right)^2. \tag{33}$$

考虑 $W=2$、 $V=1$和 $q=1$。于是有 $U(1)=8/9<24/25=U(3/4)$。

□

4.4 非对称均衡

命题1 指出，漏洞赏金博弈的任何均衡都是采用阈值策略的均衡。主要分析聚焦于对称均衡，即所有代理人都采用相同的阈值。然而，若不施加 假设 1，该博弈可能存在多个均衡，包括对称均衡和非对称均衡。我们以 $n=2$ 的情况为例，其中 $\Psi(c_{-i})=q[1-\frac{q}{2}F(c_{-i})]$。假设均衡阈值向量（$c_1^*$， c_2^*）位于内部，则它必须满足（6）中的方程组。在此例中，该方程组为

$$c_1=qV\left[1-\frac{q}{2}F(c_2)\right]\qquad\text{and}\qquad c_2=qV\left[1-\frac{q}{2}F(c_1)\right]. \tag{34}$$

令 $q=1$ 和 $V=5/7$，并将 F 定义为关于 $c\in[0,1]$ 的函数：

$$F(c)=\begin{cases}\frac{14}{15}c & \text{if}\quad 0\le c<\frac{3}{7}\\ \frac{14}{5}c-\frac{4}{5} & \text{if}\quad \frac{3}{7}\le c\le\frac{4}{7}\\ \frac{14}{30}c+\frac{8}{15} & \text{if}\quad \frac{4}{7}<c\le 1.\end{cases} \tag{35}$$

式（34）中的系统如图2所示，其中表明任意

$$(c_1^*,c_2^*)\in\left\{(c_1,c_2):c_1\in\left[\frac{3}{7},\frac{4}{7}\right]\text{ and }c_1+c_2=1\right\} \tag{36}$$

构成一个均衡阈值向量。事实上，对称均衡阈值$c^*=1/2$ 是其中一个解。

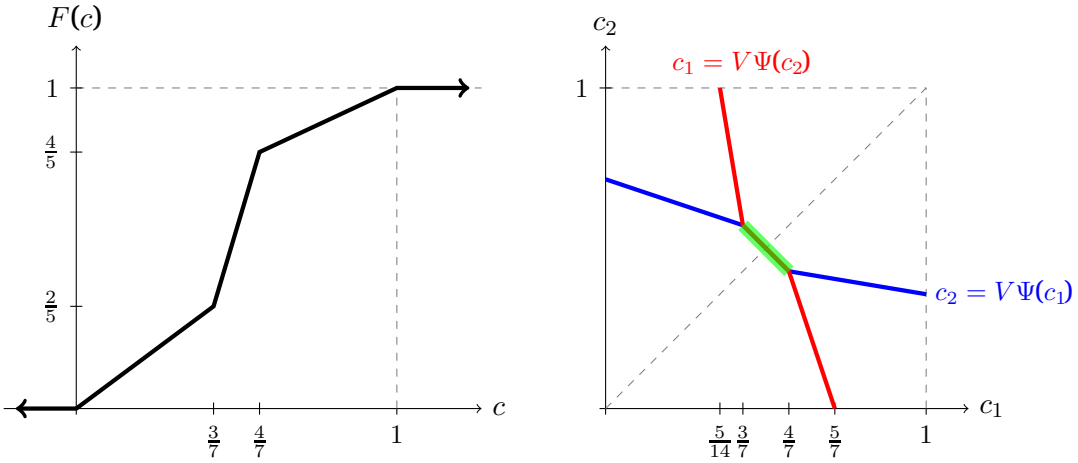


图2：非对称均衡示例。

5 讨论

的基准模型中的若干假设可以在概念上无困难地放宽。本节将讨论这些假设，并说明如何放宽它们。

5.1 成本分布

在基准模型中，我们假设代理人的成本分布相同，因为当代理人不知道他人的身份时，这一假设很自然。由于我们对 F施加的假设非常少，我们认为模型涵盖了广泛的应用场景。分布可以是无界的，因为拥有 $\underline{c} < 0$ 不会显著改变结果。例如，极限结果变为 $c_n \to \max\{0, \underline{c}\}$。分布也可以是双峰的，这或许可以模拟由两类总体构成的两个人才池： $F = aF_1 + (1-a)F_2$。

此外，即使均衡唯一，放宽共同成本分布假设也会使阈值有所不同。假设 $n = 2$，且参与者2的成本分布在一阶随机占优意义上占优于参与者1的成本分布，即 $F_1 \geq F_2$。也就是说，参与者1更有可能具有较低的成本。因此，我们预期 $c_1^* > c_2^*$，因为参与者2认为参与者1更有可能成本较低，所以参与者2在付出努力时会更加谨慎。为说明这一点，令 $F_1(c) = c^\alpha$ 和 $F_2(c) = c^\beta$ 在 $[0,1]$ 上，其中$\alpha < \beta$，于是 $c^\alpha > c^\beta$。阈值 c_1^* 和 c_2^* 满足

$$c_1 = qV\left[1 - (c_2)^\beta \frac{q}{2}\right] \quad \text{and} \quad c_2 = qV\left[1 - (c_1)^\alpha \frac{q}{2}\right].$$

通过图示可在（c_1, c_2）空间中验证，这些方程在对角线下方相交： $c_1^* > c_2^*$。

5.2 搜索时间

我们的模型是静态的，因为代理人只决定一次是否进行搜索；奖品分配方案规定，如果有多个代理人成功，则在成功者中均匀随机地分配奖品。搜索时间分布相同这一假设为这种奖品分配方案提供了（微观）基础。不过，可以按如下方式放宽这一假设。

假设搜索时间的分布不同，那么“更快”的代理人将具有更高的阈值，因为该代理人知道自己很可能第一个成功，因此能够承担成本更高的搜索努力。为说明这一点，设 $n = 2$，且令 $t_1 \sim \mathcal{U}[0, T_1]$ 和$t_2 \sim \mathcal{U}[0, T_2]$，其中 $T_1 < T_2$。这意味着参与者1是更快的代理人。于是，阈值 c_1^* 和 c_2^* 满足

$$c_1 = qV\left[1 - qF(c_2)\frac{T_1}{2T_2}\right] \quad \text{and} \quad c_2 = qV\left[1 - qF(c_1)\left(1 - \frac{T_1}{2T_2}\right)\right].$$

令 $F(c) = c$，从图形上很容易看出 $c_1^* > c_2^*$。对于其他成本分布，也应当成立同样的结论。此外，这一直觉还可以扩展到一种搜索时间分布在一阶随机意义上支配另一种分布的情形。在这种情况下，具有随机占优搜索时间分布的代理人（即较慢的代理人）具有较低的均衡阈值。

5.3 技能

第三，我们还可以扩展该模型，以纳入具有共同知识的异质技能 q_i。均衡策略仍将采用阈值策略，但阈值现在将满足如下形式的系统：

$$c_i^* = q_i V \Xi(c_{-i}^*, q_{-i}),$$

其中，当技能具有异质性时，Ξ 是 Ψ/q 的对应形式。同样，阈值也会发生变化。对于具有 $q_1 > q_2$的两个代理人，我们可以证明，当 F 满足使均衡阈值 c_1^* 和 c_2^* 唯一的条件时，$c_1^* > c_2^*$。

5.4 多个专家

第 4.1 节讨论了加入一位专家的影响。拥有多个专家不会从定性上改变结果。这是因为专家被建模为技能不同的非策略性（总是付出努力）代理人 q_e。加入一位专家会使均衡阈值发生变化，变化幅度与加入一名（分数）玩家相同。因此，例如，可以将模型扩展到这样一种情形：一组技能为q 的策略性代理人，以及另一组技能为 q_e的专家。

此外，假设有两位专业能力分别为 q_e 和 q_f的专家。那么，命题11中的均衡条件将修改为 $c^{ef} = V\Phi^{ef}(c^{ef}, q, q_e, q_f, n)$，其中 Φ^{ef}的表达式会更复杂，而 $c^{ef}(q_e, q_f)$ 是该博弈的均衡阈值。观察（19）现在将表述为：对于较小的 q_e和 q_f， $c^*(n+1) < c^{ef}(q_e, q_f) < c^*(n)$。观察（20）则将表述为： $c^{ef}(q, q) < c^*(n+2) < c^*(n)$。由此可得相同的结论：存在临界值 $\hat{}q_e$ 和 $\hat{}q_f$，使得新的阈值与一个有 $n+2$ 名（策略性）代理人的博弈中的阈值相同。有两位专家时，也可以用例1和例 2来说明同一点，即加入专家可能会降低成功概率。

5.5 多个漏洞

本文的模型可以直接扩展，以允许存在多种漏洞类型及不同数量的漏洞。假设存在 L 种漏洞类型，编号为 $l \in \{1, \ldots, L\}$。类型 l 漏洞的数量是一个离散随机变量 R^l，其分布于 $\{0, 1, \ldots\}$ 上，且具有有限期望。[11] 代理人可以独立地以概率 q^l 发现每个类型 l 漏洞，并且每个漏洞可获得 V^l 的奖励。（内部且对称的）均衡阈值 $c^* = c^*(\boldsymbol{V}, \boldsymbol{R}, \boldsymbol{q}, n)$ 满足：

$$c^* = \sum_{l=1}^{L} V^l \mathbb{E}[R^l] \Phi(c^*, q^l, n). \tag{37}$$

均衡的许多性质都可以从单个漏洞的情形延续而来，因为（37）的右端是函数 Φ的线性组合。设计者的目标将是最大化

$$\sum_{l=1}^{L} (W^l - V^l) \mathbb{E}[R^l] P(c^*, q^l, n). \tag{38}$$

6 结论

正如实证文献所表明的，漏洞赏金计划能够为企业、公共基础设施和私营公司的安全作出重要贡献。我们建立了一个简单模型，用于研究此类计划可以据以设计的重要维度。当然，还可以进一步探索许多方向。例如，可以引入有关安全研究人员声誉和过往成就的准入审查，从而建立一个有利于漏洞发现的人才池。或者，采取相反的方法（只允许新手参与）是否会对漏洞悬赏计划有益，因为这将激励更多人参与？此外，还可以考虑更广泛的奖励选项，因为

[11]注意， $R^l = 0$ 意味着该漏洞不存在。在实践中， R^l 的支撑集是有限的，因为漏洞的最大数量可以取为例如代码中的字符数。

研究人员可能既受到金钱奖励的激励，也受到声誉收益的激励；后者可以通过成功证书加以记录，并可作为参与未来漏洞赏金计划的宝贵入场券。最后，还可以进一步制定成功发现漏洞时应如何确定奖金的公式。

参考文献

Archak, N. 和 Sundararajan, A.（2009）。众包竞赛的最优设计。ICIS 2009论文集，第17页。11 Chawla, S.、Hartline, J. D. 和 Sivan, B.（2019）。最优众包竞赛。《博弈与经济行为》，113：80–96。3 瑞士联邦总理府（2019）。源代码的发布促使人们发现瑞士邮政新电子投票系统中的漏洞。
h
tt
ps://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74307.html。3 瑞士联邦财政部（2022）。瑞士联邦行政当局采购漏洞赏金计划平台。https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-89868.html。3 Ghosh, A. 和 Kleinberg, R.（2016）。简单代理人的最优竞赛设计。《ACM经济学与计算汇刊》，4(4)：22:1–22:41。3 Laszka, A.、Zhao, M.、Malbari, A. 和 Grossklags, J.（2018）。漏洞赏金计划的参与规则。载于 Meiklejohn, S. 和 Sako, K.（编），《金融密码学与数据安全》，《计算机科学讲义》，第138–159页，柏林、海德堡：Springer。3 Maillart, T.、Zhao, M.、Grossklags, J. 和 Chuang, J.（2017）。足够多双眼睛，所有漏洞都很浅显？借助漏洞赏金计划重新审视 Eric Raymond。《网络安全期刊》，3(2)：81–90。3 Malladi, S. S. 和 Subramanian, H. C.（2020）。网络安全漏洞赏金计划：实践、问题与建议。《IEEE软件》，37(1)：31–39。3、13 Mercier, J.-F.（2018）。为寻租竞赛挑选参赛者。《国际博弈论杂志》，47(3)：927–947。3 Moldovanu, B. 和 Sela, A.（2001）。竞赛中奖金的最优分配。《美国经济评论》，91(3)：542–558。3 Sarne, D. 和 Lepioshkin, M.（2017）。具有参与成本的简单众包竞赛的有效奖金结构。载于第五届AAAI人类计算与众包会议。3、19 Taylor, C. R.（1995）。挖掘金色胡萝卜：研究锦标赛分析。《美国经济评论》，85(4)：872–890。3

Walshe, T. 和 Simpson, A.（2020）。漏洞赏金计划的实证研究。载于2020年IEEE第二届智能漏洞修复国际研讨会（IBF），第35–44页。3

A 预备知识

我们从二项式定理 $\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}=(x+y)^n$ 的一些推广开始。

引理 A.1. 对于 $n\in\mathbb{N}$ 和 $x\neq 0$,

$$\sum_{k=0}^{n}\binom{n}{k}\frac{x^k y^{n-k}}{k+1}=\frac{1}{n+1}\frac{(x+y)^{n+1}-y^{n+1}}{x}. \tag{39}$$

引理 A.1 的证明引理 A.1。注意 $\binom{n}{k}\frac{1}{k+1}=\binom{n+1}{k+1}\frac{1}{n+1}$。于是,

$$\begin{aligned}\sum_{k=0}^{n}\binom{n}{k}\frac{x^k y^{n-k}}{k+1}&=\frac{1}{n+1}\sum_{k=0}^{n}\binom{n+1}{k+1}x^k y^{n-k}=\frac{1}{n+1}\frac{1}{x}\sum_{k=0}^{n}\binom{n+1}{k+1}x^{k+1}y^{(n+1)-(k+1)}\\&=\frac{1}{n+1}\frac{1}{x}\left[\sum_{k=0}^{n+1}\binom{n+1}{k}x^k y^{n+1-k}-y^{n+1}\right]\\&=\frac{1}{n+1}\frac{(x+y)^{n+1}-y^{n+1}}{x}.\end{aligned} \tag{40}$$

□

引理 A.2. 对于 $n\in\mathbb{N}$ 和 $x\neq 0$,

$$\sum_{k=0}^{n}\binom{n}{k}\frac{x^k y^{n-k}}{(k+1)(k+2)}=\frac{1}{(n+1)(n+2)}\frac{(x+y)^{n+2}-[(n+2)x+y]y^{n+1}}{x^2}. \tag{41}$$

引理 A.2 的证明。注意, $\binom{n}{k}\frac{1}{(k+1)(k+2)}=\binom{n+2}{k+2}\frac{1}{(n+1)(n+2)}$。于是,

$$\begin{aligned}\sum_{k=0}^{n}\binom{n}{k}\frac{x^k y^{n-k}}{(k+1)(k+2)}&=\frac{1}{(n+1)(n+2)}\sum_{k=0}^{n}\binom{n+2}{k+2}x^k y^{n-k}\\&=\frac{1}{(n+1)(n+2)}\frac{1}{x^2}\sum_{k=0}^{n}\binom{n+2}{k+2}x^{k+2}y^{(n+2)-(k+2)}\\&=\frac{1}{(n+1)(n+2)}\frac{1}{x^2}\left[\sum_{k=0}^{n+2}\binom{n+2}{k}x^k y^{n+2-k}-(n+2)xy^{n+1}-y^{n+2}\right]\\&=\frac{1}{(n+1)(n+2)}\frac{(x+y)^{n+2}-[(n+2)x+y]y^{n+1}}{x^2}.\end{aligned} \tag{42}$$

□

引理 A.3。对于 $n \in \mathbb{N}$ 和 $x \neq 0$,

$$\sum_{k=0}^{n} \binom{n}{k} \frac{x^k y^{n-k}}{k+2} = \frac{1}{(n+1)(n+2)} \frac{[(n+1)x - y](x+y)^{n+1} + y^{n+2}}{x^2}. \tag{43}$$

引理 A.3 的证明。注意，$\binom{n}{k}\frac{1}{k+2} = \binom{n}{k}_{k+1}{}^{1}{}_{()(k+2)} + \binom{n}{k}_{k+1}{}^{k}{}_{()(k+2)}$。于是

$$\sum_{k=0}^{n} \binom{n}{k} \frac{x^k y^{n-k}}{k+2} = \sum_{k=0}^{n} \binom{n}{k} \frac{x^k y^{n-k}}{(k+1)(k+2)} + \sum_{k=0}^{n} \binom{n}{k} \frac{k x^k y^{n-k}}{(k+1)(k+2)}. \tag{44}$$

根据引理 A.2，第一项为

$$\frac{1}{(n+1)(n+2)} \frac{(x+y)^{n+2} - [(n+2)x + y]y^{n+1}}{x^2}.$$

对于第二项，我们有

$$\begin{aligned}
&\sum_{k=0}^{n} \binom{n}{k} \frac{k x^k y^{n-k}}{(k+1)(k+2)} = x \sum_{k=1}^{n} \binom{n}{k} \frac{k x^{k-1} y^{n-k}}{(k+1)(k+2)} = x \frac{\mathrm{d}}{\mathrm{d}x} \left[\sum_{k=1}^{n} \binom{n}{k} \frac{x^k y^{n-k}}{(k+1)(k+2)} \right] \\
&= x \frac{\mathrm{d}}{\mathrm{d}x} \left[\frac{1}{(n+1)(n+2)} \frac{(x+y)^{n+2} - [(n+2)x + y]y^{n+1}}{x^2} - \frac{y^n}{2} \right] \\
&= x \left[\frac{[(n+2)(x+y)^{n+1} - (n+2)y^{n+1}]x^2 - 2x\{(x+y)^{n+2} - [(n+2)x + y]y^{n+1}\}}{(n+1)(n+2)x^4} \right] \\
&= \frac{1}{(n+1)(n+2)} \frac{(n+2)x(x+y)^{n+1} - (n+2)xy^{n+1} - 2(x+y)^{n+2} + 2(n+2)xy^{n+1} + 2y^{n+2}}{x^2} \\
&= \frac{1}{(n+1)(n+2)} \frac{[(n+2)x - 2(x+y)](x+y)^{n+1} + (n+2)xy^{n+1} + 2y^{n+2}}{x^2} \\
&= \frac{1}{(n+1)(n+2)} \frac{(nx - 2y)(x+y)^{n+1} + [(n+2)x + 2y]y^{n+1}}{x^2}.
\end{aligned} \tag{45}$$

将两项合并可得

$$\begin{aligned}
\sum_{k=0}^{n} \binom{n}{k} \frac{x^k y^{n-k}}{k+2} &= \frac{1}{(n+1)(n+2)} \frac{(x+y)^{n+2} - [(n+2)x + y]y^{n+1}}{x^2} \\
&\quad + \frac{1}{(n+1)(n+2)} \frac{(nx - 2y)(x+y)^{n+1} + [(n+2)x + 2y]y^{n+1}}{x^2} \\
&= \frac{1}{(n+1)(n+2)} \frac{[(x+y) + nx - 2y)](x+y)^{n+1} + y^{n+2}}{x^2} \\
&= \frac{1}{(n+1)(n+2)} \frac{[(n+1)x - y](x+y)^{n+1} + y^{n+2}}{x^2}.
\end{aligned} \tag{46}$$

□

对于 c 为了完整起见，我们给出伯努利不等式的一个版本，本文中会反复用到它 t-

文中反复提及。

引理 A.4（伯努利不等式）。对于 $0 < x < 1$ 和一个正整数 m,

$$(1-x)^m < \frac{1}{1+mx}.$$

引理 A.4 的证明。对于 $0 < x < 1$, $\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$。对恒等式取第（$m-1$）阶导数可得

$$\sum_{k=0}^{\infty} k(k-1)\cdots(k-(m-2))x^{k-(m-1)} = (m-1)!\frac{1}{(1-x)^m}. \tag{47}$$

（47）的左侧为 $\sum_{k=m-1}^{\infty} k(k-1)\cdots(k-(m-2))x^{k-(m-1)} = \sum_{k=0}^{\infty} \frac{(k+m-1)!}{k!}x^k$。因此，可得

$$\frac{1}{(1-x)^m} = 1 + mx + \frac{(m+1)m}{2}x^2 + \frac{(m+2)(m+1)m}{6}x^3 + \cdots > 1 + mx. \tag{48}$$

□

B 证明

命题1的证明。如果 σ_i^*: $[\underline{c}, \overline{c}] \to \{0, 1\}$ 是代理人 i的均衡策略，那么它是非递增的。我们通过反证法证明这一点，并假设存在一对成本 $c < c'$，使得 $\sigma_i^*(c) = 0$ 以及 $\sigma_i^*(c') = 1$。那么， $c < c'$ 意味着

$$\begin{aligned} 0 &= \mathbb{E}[u_i(0, \sigma_{-i}^*(c_{-i}), c_i | c_i = c] \\ &\geq \mathbb{E}[u_i(1, \sigma_{-i}^*(c_{-i}), c_i) | c_i = c] \\ &> \mathbb{E}[u_i(1, \sigma_{-i}^*(c_{-i}), c_i) | c_i = c'] \\ &\geq \mathbb{E}[u_i(0, \sigma_{-i}^*(c_{-i}), c_i | c_i = c'] = 0, \end{aligned} \tag{49}$$

其中，第一个和最后一个不等式由均衡定义推出。由 u_i 的定义可得严格不等式，从而导致矛盾。因此，任何均衡策略都是阈值策略。因此，对于所有 i，存在某个 $\sigma_i^* = \sigma_{c_i^*}$ $c_i^* \in [\underline{c}, \overline{c}]$。

□

命题 2的证明。 函数 Ψ是给定其他玩家采用某些阈值策略时，对成本分布的期望： $p(\boldsymbol{s}_{-i})$，对所有$s_j = \sigma_{\hat{c}_j}(c_j)$。此外，由于 $p(\boldsymbol{s}_{-i})$ 仅取决于其他代理人中进行搜索的数量

搜索，我们定义 $\tilde{p}(S_{-i}) \equiv p(\boldsymbol{s}_{-i})$。那么，

$$\begin{aligned}\Psi(\hat{\boldsymbol{c}}_{-i}) &= \mathbb{E}[p(\sigma_{\hat{c}_1}(c_1), \ldots, \sigma_{\hat{c}_{i-1}}(c_{i-1}), \sigma_{\hat{c}_{i+1}}(c_{i+1}), \ldots, \sigma_{\hat{c}_n}(c_n))] \\ &= \mathbb{E}[\tilde{p}(\sigma_{\hat{c}_1}(c_1) + \cdots + \sigma_{\hat{c}_{i-1}}(c_{i-1}) + \sigma_{\hat{c}_{i+1}}(c_{i+1}) + \cdots + \sigma_{\hat{c}_n}(c_n))],\end{aligned} \tag{50}$$

其中，期望是对 c_j 取的。性质 (i) 成立，是因为 c_j 服从相同且相互独立的分布。

对于性质 (ii)，注意到 $\tilde{p}(S_{-i})$ 严格递减。利用 引理 A.1 并对 S_{-i} 求导即可证明这一点。现在，固定 $j \neq i$，并考虑某个 $\hat{c}'_j > \hat{c}_j$。定义两个随机变量

$$\Sigma \equiv \sigma_{\hat{c}_1}(c_1) + \cdots + \sigma_{\hat{c}_j}(c_j) + \cdots + \sigma_{\hat{c}_n}(c_n) \quad \text{and} \quad \Sigma' \equiv \sigma_{\hat{c}_1}(c_1) + \cdots + \sigma_{\hat{c}'_j}(c_j) + \cdots + \sigma_{\hat{c}_n}(c_n).$$

我们声称 Σ' 一阶随机占优于 Σ。对于任意 x，有 $\{\Sigma \geq x\} \subset \{\Sigma + \sigma_{\hat{c}'_j} - \sigma_{\hat{c}_j} \geq x\} = \{\Sigma' \geq x\}$，其中第一个包含关系成立，是因为对于所有 c_j，$\sigma_{\hat{c}'_j}(c_j) - \sigma_{\hat{c}_j}(c_j) \geq 0$。因此，对于所有 x，$\Pr(\Sigma' \geq x) \geq \Pr(\Sigma \geq x)$，如所声称。

于是可得，$\tilde{p}(\Sigma)$ 一阶随机占优于 $\tilde{p}(\Sigma')$，因为 $\tilde{p}$ 严格递减。根据随机占优，我们有

$$\Psi(\hat{c}_1, \ldots, \hat{c}'_j, \ldots, \hat{c}_n) = \mathbb{E}[\tilde{p}(\Sigma')] < \mathbb{E}[\tilde{p}(\Sigma)] = \Psi(\hat{\boldsymbol{c}}_{-i}),$$

由此完成了 (ii) 的证明。

性质 (iii) 成立，因为 $F(\underline{c}) = 0$，且求和中只有第一项（$K = \varnothing$）保留下来：$\Psi(\underline{c}, \ldots, \underline{c}) = q$。另一方面，$F(\overline{c}) = 1$，且求和中只有最后一项（$K = N \setminus \{i\}$）保留下来：根据引理 A.1，$\Psi(\overline{c}, \ldots, \overline{c}) = q \sum_{t=0}^{n-1} \binom{n-1}{t} q^t (1-q)^{n-1-t} = 1 - (1-q)^n$。 □

命题3的证明 命题3。 证明分三步进行。首先，我们证明在假设 1下，所有代理人都必须采用相同的均衡阈值。其次，我们推导出内点均衡阈值必须满足的一个简单表达式。最后，我们证明阈值 c^* 是唯一的，并且在假设 2下位于内点。

步骤 1. 不失一般性，设 $\boldsymbol{c}^* = (c_1^*, \ldots, c_n^*)$ 为满足 $c_1^* \leq \cdots \leq c_n^*$ 的内点均衡阈值向量。现在，姑且假设 $c_1^* < c_n^*$，以导出矛盾。根据定义，我们有

$$c_1^* = V\Psi(c_2^*, \ldots, c_n^*) \qquad \text{and} \qquad c_n^* = V\Psi(c_1^*, \ldots, c_{n-1}^*). \tag{51}$$

合并后得到

$$\begin{aligned}c_n^* - c_1^* &= V\left[\Psi(c_1^*, c_2^*, \ldots, c_{n-1}^*) - \Psi(c_2^*, \ldots, c_{n-1}^*, c_n^*)\right] \\ &= -V\left[\Psi(c_2^*, \ldots, c_{n-1}^*, c_n^*) - \Psi(c_1^*, c_2^*, \ldots, c_{n-1}^*)\right] \\ &= -V\left[\Psi(c_n^*, c_2^*, \ldots, c_{n-1}^*) - \Psi(c_1^*, c_2^*, \ldots, c_{n-1}^*)\right],\end{aligned} \tag{52}$$

其中，第二个等式将括号中的负号提了出来，最后一个等式则利用了 Ψ 关于其自变量是对称的这一事实。重新整理后得到

$$\frac{\Psi(c_n^*, c_2^*, \ldots, c_{n-1}^*) - \Psi(c_1^*, c_2^*, \ldots, c_{n-1}^*)}{c_n^* - c_1^*} = -\frac{1}{V}. \tag{53}$$

左侧是将所有其他自变量保持不变时， Ψ 从 c_1^* 到 c_n^*的斜率。由于 Ψ 连续，根据中值定理，存在 $\tilde{c} \in (c_1^*, c_n^*)$，使得

$$\left.\frac{\partial \Psi(c_1, c_2^*, \ldots, c_{n-1}^*)}{\partial c_1}\right|_{c_1=\tilde{c}} = -\frac{1}{V}, \tag{54}$$

这与假设 1矛盾。

步骤 2。我们已在命题1中证明，任何均衡策略都是假设 1下的阈值策略，阈值均衡向量具有以下形式：$\boldsymbol{c}^* = (c^*, \ldots, c^*)$，其中存在满足以下条件的 c^*

$$c^* = V\Psi(c^*, \ldots, c^*). \tag{55}$$

现在我们来简化 $\Psi(c, \ldots, c)$的表达式。由（7），

$$\Psi(c, \ldots, c) = q\sum_{k=0}^{n-1}\left\{\binom{n-1}{k}F(c)^k(1-F(c))^{n-1-k}\left[\sum_{t=0}^{k}\binom{k}{t}q^t(1-q)^{k-t}\frac{1}{t+1}\right]\right\}. \tag{56}$$

根据引理 A.1，方括号中的项为

$$\sum_{t=0}^{k}\binom{k}{t}q^t(1-q)^{k-t}\frac{1}{t+1} = \frac{1}{k+1}\frac{1-(1-q)^{k+1}}{q}. \tag{57}$$

那么，对于$c > \underline{c}$,

$$\begin{aligned}
&\Psi(c, \ldots, c) = \\
&= \sum_{k=0}^{n-1}\binom{n-1}{k}F(c)^k(1-F(c))^{n-1-k}\frac{1-(1-q)^{k+1}}{k+1} \\
&= \sum_{k=0}^{n-1}\binom{n-1}{k}\frac{F(c)^k(1-F(c))^{n-1-k}}{k+1} - (1-q)\sum_{k=0}^{n-1}\binom{n-1}{k}\frac{(F(c)(1-q))^k(1-F(c))^{n-1-k}}{k+1} \\
&= \frac{1-(1-F(c))^n}{nF(c)} - (1-q)\left(\frac{(1-qF(c))^n - (1-F(c))^n}{nF(c)(1-q)}\right) \\
&= \frac{1-(1-qF(c))^n}{nF(c)} = \frac{P(c)}{nF(c)}.
\end{aligned} \tag{58}$$

适用于 $c = \underline{c}$，$F(\underline{c}) = 0$ 且总和中只有第一项（$k = 0$）非零 s:

$\Psi(\underline{c}, \ldots\ldots, \underline{c}) = q$。因此，确实有 $\Psi(c, \ldots\ldots, c) = \Phi(c, q, n)$，如（8）中所定义。由此可知，若存在内点均衡阈值，则它满足 $c^* = V\Phi(c^*, q, n)$。

步骤 3。接下来，我们证明 c^* 确实是内部的且唯一的。首先注意到，$\Phi(c, q, n)$ 关于 c 严格递减：

$$\begin{aligned}\frac{\partial \Phi}{\partial c} &= \frac{[-n(1-qF(c))^{n-1}(-qf(c))]nF(c) - nf(c)[1-(1-qF(c))^n]}{(nF(c))^2} \\ &= \frac{nf(c)(1-qF(c))^{n-1}}{(nF(c))^2}\left[nqF(c) - \frac{1}{(1-qF(c))^{n-1}} + (1-qF)\right] \\ &= \frac{f(c)(1-qF(c))^{n-1}}{nF(c)^2}\left[1 + (n-1)qF(c) - \frac{1}{(1-qF(c))^{n-1}}\right] < 0.\end{aligned} \tag{59}$$

这由伯努利不等式可得。因此，根据连续性，$V\Phi(c, q, n)$ 至多有一个不动点 c^*。我们声称，当满足以下条件时，这样的 c^* 位于内部 $c^* \in (\underline{c}, \bar{c})$：

$$\underline{c} < V\Phi(\underline{c}, q, n) \quad \text{and} \quad V\Phi(\bar{c}, q, n) < \bar{c}. \tag{60}$$

由于 $\Phi(\underline{c}, q, n) = q$ 且 $F(\bar{c}) = 1$，条件变为

$$\underline{c} < qV \quad \text{and} \quad V\frac{1-(1-q)^n}{n} < \bar{c}, \tag{61}$$

其表述为假设 2。

证明至此完成。 □

命题4的证明命题4。我们证明 $\Phi(c, q, n)$具有所声称的性质。对于c，证明可由命题3的证明推出。对于 q，可直接得到：$\partial\Phi/\partial q = (1-qF(c))^{n-1} > 0$。对于 n，我们证明若 $c > \underline{c}$，

$$\underbrace{\frac{1-(1-qF(c))^n}{nF(c)}}_{\Phi(c,q,n)} > \underbrace{\frac{1-(1-qF(c))^{n+1}}{(n+1)F(c)}}_{\Phi(c,q,n+1)}. \tag{62}$$

不等式（62）可简化为 $(1-qF(c))^n < (1+nqF(c))^{-1}$ 根据伯努利不等式，该式成立。关于 $c^*(V, q, n)$的比较静态分析结果随后可由 Φ 的性质推出，因为 c^* 是 $V\Phi$的不动点。

□

命题5的证明。$P(c, q, n)$关于 c和 q递增。因此，$P^*(V, q, n) = P(c^*(V, q, n)\ q, n)$随 V 和 q增加。正文中的例子表明，P^*可能随 n增加或减少。

□

命题6的证明命题6。我们从函数 $g(n)$ 这一事实出发，

$$\frac{\mathrm{d}}{\mathrm{d}n}(g(n))^n = (g(n))^n\left(\frac{ng'(n)}{g(n)} + \ln g(n)\right). \tag{63}$$

为说明这一点，令 $h(n) \equiv (g(n))^n$。于是，$\ln h(n) = n \ln g(n)$，对两边关于 n 求导，得到 $\frac{h'(n)}{h(n)} = n\frac{g'(n)}{g(n)} + \ln g(n)$，经过一些整理即可得到结果。将这一事实应用于 $g(n) = 1 - qF(c(n))$，得到

$$\begin{aligned}\frac{\mathrm{d}P_n}{\mathrm{d}n} &= \frac{\mathrm{d}}{\mathrm{d}n}1 - (1 - qF(c_n))^n = -\frac{\mathrm{d}}{\mathrm{d}n}(1 - qF(c_n))^n \\ &= (1 - qF(c_n))^n \left[\frac{nqf(c_n)}{1 - qF(c_n)}\frac{\mathrm{d}c_n}{\mathrm{d}n} - \ln(1 - qF(c_n))\right],\end{aligned} \tag{64}$$

为便于表述，我们使用 $c_n = c^*(n)$ 和 $P_n = P^*(n)$。

现在，对均衡条件 $c_n n F(c_n) = V P_n$ 进行隐式微分，得

$$c_n F(c_n) + n\frac{\mathrm{d}c_n}{\mathrm{d}n}F(c_n) + nc_n f(c_n)\frac{\mathrm{d}c_n}{\mathrm{d}n} = V\frac{\mathrm{d}P_n}{\mathrm{d}n} = \frac{c_n nF(c_n)}{P_n}\frac{\mathrm{d}P_n}{\mathrm{d}n}. \tag{65}$$

结合（64）和（65）可得

$$\begin{aligned}\frac{\mathrm{d}P_n}{\mathrm{d}n} &= (1 - qF(c_n))^n \left[\frac{nqf(c_n)}{1 - qF(c_n)}\left(\frac{\frac{c_n nF(c_n)}{P_n}\frac{\mathrm{d}P_n}{\mathrm{d}n} - c_n F(c_n)}{nF(c_n) + nc_n f(c_n)}\right) - \ln(1 - qF(c_n))\right] \\ &= (1 - qF(c_n))^{n-1}\frac{qf(c_n)c_n nF(c_n)}{F(c_n) + c_n f(c_n)}\frac{1}{P_n}\frac{\mathrm{d}P_n}{\mathrm{d}n} \\ &\quad + (1 - qF(c_n))^n \left[\frac{-qf(c_n)c_n F(c_n)}{(1 - qF(c_n))(F(c_n) + c_n f(c_n))} - \ln(1 - qF(c_n))\right].\end{aligned} \tag{66}$$

由（66）解出 $\mathrm{d}P_n/\mathrm{d}n$，得

$$\frac{\mathrm{d}P_n}{\mathrm{d}n} = (1 - qF(c_n))^n \frac{\left[\frac{-qf(c_n)c_n F(c_n)}{(1-qF(c_n))(F(c_n)+c_n f(c_n))} - \ln(1 - qF(c_n))\right]}{\left[1 - (1 - qF(c_n))^{n-1}\frac{qf(c_n)c_n nF(c_n)}{P_n(F(c_n)+c_n f(c_n))}\right]}. \tag{67}$$

（67）中的分母为

$$\begin{aligned}1 - (1 - qF(c_n))^{n-1}&\frac{qf(c_n)c_n nF(c_n)}{P_n(F(c_n) + c_n f(c_n))} \\ &= \frac{P_n(F(c_n) + c_n f(c_n)) - (1 - qF(c_n))^{n-1}qf(c_n)c_n nF(c_n)}{P_n(F(c_n) + c_n f(c_n))} \\ &= \frac{P_n F(c_n) + c_n f(c_n)[P_n - (1 - qF(c_n))^{n-1}qnF(c_n)]}{P_n(F(c_n) + c_n f(c_n))}.\end{aligned} \tag{68}$$

根据伯努利不等式，它非负，因为 $P_n F(c_n) \geq 0$ 且 $P_n - (1 - qF(c_n))^{n-1}qnF(c_n) = 1 - (1 - qF(c_n))^{n-1}(1 + (n-1)qF(c_n)) \geq 0$。

有　因此，我们有 $\mathrm{d}P_n/\mathrm{d}n \geq 0$ 当且仅当（67）中的分子项为非　-

负。也就是说，

$$\frac{-qf(c_n)c_nF(c_n)}{(1-qF(c_n))(F(c_n)+c_nf(c_n))} \geq \ln(1-qF(c_n)). \tag{69}$$

两边同时除以 $-qF(c_n)$ 并重新整理，可得命题中所述的条件。

□

命题 7 的证明。均衡条件可写为 $c_nnF(c_n) = VP_n$。假设 $\lim_{n\to\infty} c_n$ 不等于 $\underline{c}$。那么，由于根据命题4，c_n 关于 n 递减，我们有存在某个值 $c' > \underline{c}$，使得对于任意$n \in \mathbb{N}$，$c_n > c'$。在这种情况下，$c_nnF(c_n) > c'nF(c')$。这是因为 F是一个递增函数，因此 $F(c_n) > F(c')$。注意，由于 $c' > \underline{c}$，$F(c') > 0$。因此，$\lim_{n\to\infty} c_nnF(c_n) \geq \lim_{n\to\infty} c'nF(c') = \infty$，不可能等于 VP_n，这就产生了矛盾。

□

命题 8 的证明。

(i) 考虑 $\underline{c} = 0$ 的情形。证明采用反证法。首先，假设 $\lim_{n\to\infty} nF(c_n) \neq \infty$。这意味着存在 $m \in \mathbb{N}$，使得有一个无限的自然数序列 $n_1, n_2, \ldots$，满足 $n_iF(c_{n_i}) < m$。于是

$$c_{n_i} = V\frac{1-(1-qF(c_{n_i}))^{n_i}}{n_iF(c_{n_i})} \geq Vq\frac{1-e^{-qn_iF(c_{n_i})}}{qn_iF(c_{n_i})} > Vq\frac{1-e^{-qm}}{qm} > 0. \tag{70}$$

对任意 $i \in \mathbb{N}$，这与命题 7 中 c_n 收敛于 0 相矛盾。(70) 的第一个等号由均衡条件得出。第一个不等式由以下事实得出：$(1-x)^n \leq e^{-nx}$。第二个不等式成立，是因为函数 $\frac{1-e^{-x}}{x}$ 严格递减。

$\underline{c} > 0$ 的情形则不那么直接。主要难点在于序列 $nF(c_n)$ 是否收敛；它可能是单调的，也可能不是。假设它确实收敛，且收敛到常数 κ，那么

$$\frac{1-(1-qF(c_n))^n}{nF(c_n)} = \frac{1-\left[\left(1-\frac{q}{1/F(c_n)}\right)^{\frac{1}{F(c_n)}}\right]^{nF(c_n)}}{nF(c_n)} \tag{71}$$

意味着

$$\frac{1-(1-qF(c_n))^n}{nF(c_n)} \to \frac{1-e^{-q\kappa}}{\kappa} \tag{72}$$

根据 $F(c_n) \to 0$ 这一事实、e^x 的定义以及该函数的连续性。均衡条件随后确定了 κ 的值。在不假设 $nF(c_n)$ 收敛的情况下，证明会更加复杂，并且需要经过多个步骤。

步骤 1。注意，由于以下原因， $nF(c_n)$ 是有界的：

$$nF(c_n) = V\frac{1-(1-qF(c_n))^n}{c_n} \le \frac{V}{\underline{c}}. \tag{73}$$

这意味着 $\lim_{n\to\infty} nF(c_n) \neq \infty$。

此外， $nF(c_n)$ 不收敛于零。否则，若 $nF(c_n) \to 0$，则取极限并对右侧应用洛必达法则

$$c_n \ge Vq\frac{1-e^{-qnF(c_n)}}{qnF(c_n)} \tag{74}$$

可得 $\underline{c} \ge Vq$，这与均衡的内部性相矛盾。

步骤 2。我们声称

$$(1-qF(c_n))^n = e^{-qnF(c_n)} + o(1). \tag{75}$$

为说明 (75) 成立，固定 n ，并回忆恒等式 $e^{-nx} = \sum_{k=0}^{\infty}\frac{(-1)^k(nx)^k}{k!}$以及 $(1-x)^n = \sum_{k=0}^{\infty}\binom{n}{k}(-1)^k x^k$，其中 $\binom{n}{k} = 0$ 对于 $n < k$。

将它们应用于 $\xi_n \equiv qF(c_n)$，可得

$$\begin{aligned} e^{-n\xi_n} - (1-\xi_n)^n &= \sum_{k=0}^{\infty}\frac{n^k}{k!}(-1)^k\xi_n^k - \sum_{k=0}^{\infty}\binom{n}{k}(-1)^k\xi_n^k \\ &= \sum_{k=0}^{\infty}(-1)^k\left[\frac{1}{k!} - \frac{1}{n^k}\binom{n}{k}\right](n\xi_n)^k. \end{aligned} \tag{76}$$

设 B 为 $n\xi_n$的上界。于是，根据三角不等式以及以下事实：$1/k! - \frac{1}{n^k}\binom{n}{k} \ge 0$ 和 $(n\xi_n)^k \ge 0$，我们有

$$\begin{aligned} \left|e^{-n\xi_n} - (1-\xi_n)^n\right| &\le \sum_{k=0}^{\infty}\left[\frac{1}{k!} - \frac{1}{n^k}\binom{n}{k}\right](n\xi_n)^k \\ &\le \sum_{k=0}^{\infty}\left[\frac{1}{k!} - \frac{1}{n^k}\binom{n}{k}\right]B^k. \end{aligned} \tag{77}$$

对于每个 k,

$$\begin{aligned} \frac{1}{n^k}\binom{n}{k} &= \frac{1}{k!}\frac{n(n-1)\cdots(n-(k-1))}{n^k} \\ &= \frac{1}{k!}\frac{n^k + O(n^{k-1})}{n^k} = \frac{1}{k!} + O(n^{-1}). \end{aligned} \tag{78}$$

因此，将 $n \to \infty$ 代入（77）即可得到（75）中的结论。

步骤 3。将 $\kappa \in (0,\infty)$ 定义为以下方程的唯一解

$$\underline{c} = V\frac{1-e^{-q\kappa}}{\kappa}. \tag{79}$$

现在记作

$$\begin{aligned} c_n - \underline{c} &= V\left[\frac{1-(1-qF(c_n))^n}{nF(c_n)} - \frac{1-e^{-q\kappa}}{\kappa}\right] \\ &= Vq\left[\frac{1-e^{-qnF(c_n)}}{qnF(c_n)} - \frac{1-e^{-q\kappa}}{q\kappa}\right] + o(1), \end{aligned} \tag{80}$$

其中，第二个等式使用了此前证明的事实：$\lim_{n\to\infty} nF(c_n) \notin \{0,\infty\}$ 以及 $(1-qF(c_n))^n = e^{-qnF(c_n)} + o(1)$。

重新整理（80），得到

$$\frac{1}{Vq}(c_n - \underline{c}) = \left[\frac{1-e^{-qnF(c_n)}}{qnF(c_n)} - \frac{1-e^{-q\kappa}}{q\kappa}\right] + o(1). \tag{81}$$

由于根据命题 7，LHS 趋于零，因此有

$$\frac{1-e^{-qnF(c_n)}}{qnF(c_n)} \to \frac{1-e^{-q\kappa}}{q\kappa}. \tag{82}$$

然后注意到 $\zeta(x) = (1-e^{-x})/x$ 是严格单调且连续的，因此具有连续逆函数。由此可得 $\zeta^{-1}\left(\frac{1-e^{-qnF(c_n)}}{qnF\ c_n}()\right) = qnF(c_n) \to q\kappa = \zeta^{-1}\left(\frac{1-e^{-q\kappa}}{q\kappa}\right)$.

证明完毕。

(ii) 由 (i) 的证明可知，

$$P_n = 1-(1-qF(c_n))^n = 1-e^{-qnF(c_n)} + o(1).$$

结论由 (i) 和连续性得出。

□

命题 9 的证明。

(i) 由命题 8可知，P_n 趋于一个严格正常数。记 $c_nF(c_n) = V\frac{P_n}{n}$。由此可得 $c_nF(c_n) \in O(n^{-1})$，并且还可得 $c_nF(c_n) \in \Omega(n^{-1})$。

(ii) 若 $\underline{c} > 0$，则 $c_n \to \underline{c} > 0$。于是，$F(c_n) = V\frac{P_n/c_n}{n}$，由于 P_n/c_n 趋于一个严格正常数，结论得证。

□

命题的证明：命题 10。 对（11）左侧取极限，并使用洛必达法则，得到

$$\lim_{n\to\infty}\frac{\ln\left(1-qF(c_n)\right)}{\frac{-qF(c_n)}{1-qF(c_n)}}=\lim_{n\to\infty}\frac{\frac{-qf(c_n)}{1-qF(c_n)}}{\frac{-qf(c_n)(1-qF(c_n))-q^2f(c_n)F(c_n)}{(1-qF(c_n))^2}}=\lim_{n\to\infty}1-qF(c_n)=1. \tag{83}$$

因此，如果（11）的右侧与 1 保持一定距离，那么当 n 足够大时，左侧最终会超过右侧。假设 3 足以保证这一点成立，命题得证。

□

命题的证明：命题11。证明步骤与命题3 的证明相同，但有两处修改。首先， c^e 具有内部性的条件现在为 $\underline{c}<\Phi^e(\underline{c},\ q,\ q_e,\ n)$ 和 $\Phi^e(\overline{c},\ q,\ q_e,\ n)<\overline{c}$。其次，均衡阈值 c^e 现在满足以下均衡条件：

$$c=V(1-q_e)\Phi(c,q,n)+Vq_e\tilde{\Phi}(c,q,n), \tag{84}$$

其中

$$\tilde{\Phi}(c,q,n)\equiv q\sum_{k=0}^{n-1}\binom{n-1}{k}F(c)^k(1-F(c))^{n-1-k}\left[\sum_{t=0}^{k}\binom{k}{t}q^t(1-q)^{k-t}\frac{1}{t+2}\right]. \tag{85}$$

（84）右侧有两项。首先，如果专家没有发现漏洞（概率为 $1-q_e$），那么代理人的期望奖励与之前相同。其次，如果专家发现漏洞（概率为 q_e），奖品便会以另一种额外方式分配，因此 $\frac{1}{t+2}$出现在 $\tilde{\Phi}$的表达式中。现在，我们利用给定的引理简化 $\tilde{\Phi}(c,\ q,\ n)$，并证明它关于 c严格递减。

首先假设 $c>\underline{c}$。根据引理 A.3，

$$\sum_{t=0}^{k}\binom{k}{t}q^t(1-q)^{k-t}\frac{1}{t+2}=\frac{1}{(k+1)(k+2)}\frac{(k+2)q-1+(1-q)^{k+2}}{q^2}. \tag{86}$$

因此

$$\begin{aligned}\tilde{\Phi}(c,q,n)=&\sum_{k=0}^{n-1}\binom{n-1}{k}F(c)^k(1-F(c))^{n-1-k}\frac{1}{k+1}\\&-\frac{1}{q}\sum_{k=0}^{n-1}\binom{n-1}{k}F(c)^k(1-F(c))^{n-1-k}\frac{1}{(k+1)(k+2)}\\&+\frac{(1-q)^2}{q}\sum_{k=0}^{n-1}\binom{n-1}{k}(F(c)(1-q))^k(1-F(c))^{n-1-k}\frac{1}{(k+1)(k+2)}.\end{aligned} \tag{87}$$

应用 引理 A.1 于右侧的第一项，并将 引理 A.2 应用于第二项和第三项，可得

$$\begin{aligned}\tilde{\Phi}(c,q,n) = &\frac{1-(1-F(c))^n}{nF(c)} \\ &- \frac{1-(1+nF(c))(1-F(c))^n}{n(n+1)qF(c)^2} \\ &+ \frac{(1-qF(c))^{n+1}-(1+nF(c)-(n+1)qF(c))(1-F(c))^n}{n(n+1)qF(c)^2},\end{aligned} \tag{88}$$

从而化简为

$$\tilde{\Phi}(c,q,n) = \frac{1}{nF(c)} + \frac{(1-qF(c))^{n+1}-1}{n(n+1)qF(c)^2}, \tag{89}$$

可以直接验证其关于 c 严格递减。于是，均衡条件的右侧为

$$V(1-q_e)\Phi(c,q,n) + Vq_e\left[\frac{1}{nF(c)} + \frac{(1-qF(c))^{n+1}-1}{n(n+1)qF(c)^2}\right]. \tag{90}$$

化简可得表达式

$$V\Phi(c,q,n) - Vq_e\frac{1-(1-qF(c))^n(1+nqF(c))}{n(n+1)qF(c)^2} \tag{91}$$

~对所有 $c > \underline{c}$均成立。如果 $c = \underline{c}$，那么 $\Phi = q/2$ 且 $\Phi = q$。于是，均衡条件的右侧为 $Vq - Vq_eq/2 = Vq(1-q_e/2)$，如（17）所定义。该~函数 Φ^e 关于 c 严格递减，Φ 因为它是 Φ 和 c的组合，而二者关于 c^e 均严格递减。因此，不动点的存在性与唯一性 □

证明 关于命题 12。 利用无差异条件（9）和（18），可得

$$\Phi^e(c^e(\hat{q}_e),q,n,\hat{q}_e) = \Phi(c^*(n+1),n+1,q). \tag{92}$$

经过一些代数运算即可得到^q_e 的表达式。证明的其余部分已在正文中概述。

□

命题13的证明命题13。 回顾一下， Ψ^m 是指在其他代理人采用阈值策略的条件下，代理人 i 是搜索时第 m个发现漏洞的代理人的概率的期望。也就是说，

$$\Psi^m(\hat{\boldsymbol{c}}_{-i}) = \mathbb{E}[p^m(\sigma_{\hat{c}_1}(c_1),\ldots,\sigma_{\hat{c}_{i-1}}(c_{i-1}),\sigma_{\hat{c}_{i+1}}(c_{i+1}),\ldots,\sigma_{\hat{c}_n}(c_n))].$$

我们将 $\tilde{p}^m(S_{-i})$ 写作 $\equiv p^m(\boldsymbol{s}_{-i})$。固定 S_{-i}，则性质 (i) 成立，因为

$$\begin{aligned}
\frac{1}{q}\sum_{m=1}^{n}\tilde{p}^m(S_{-i}) &= \sum_{m=1}^{S_{-i}+1}\sum_{t=m-1}^{S_{-i}}\binom{S_{-i}}{t}q^t(1-q)^{S_{-i}-t}\frac{1}{t+1} \\
&= \sum_{t=0}^{S_{-i}}\sum_{m=1}^{t+1}\binom{S_{-i}}{t}q^t(1-q)^{S_{-i}-t}\frac{1}{t+1} \\
&= \sum_{t=0}^{S_{-i}}(t+1)\binom{S_{-i}}{t}q^t(1-q)^{S_{-i}-t}\frac{1}{t+1} \\
&= \sum_{t=0}^{S_{-i}}\binom{S_{-i}}{t}q^t(1-q)^{S_{-i}-t} \\
&= 1.
\end{aligned} \tag{93}$$

对于性质（ii），注意到

$$\tilde{p}^m(S_{-i}) - \tilde{p}^{m+1}(S_{-i}) = \begin{cases} 0 & \text{if} \quad S_{-i} < m-1 \\ q\binom{S_{-i}}{m-1}q^{m-1}(1-q)^{S_{-i}-(m-1)}\frac{1}{m} & \text{if} \quad S_{-i} \geq m-1, \end{cases} \tag{94}$$

对于所有 S_{-i}，该值均非负，并且对某些 S_{-i} 严格为正。在上述差值中用$\sum_{j\neq i}\sigma_{\hat{c}_j}(c_j)$替换 S_{-i}，并对 c_j 取期望，即可推出性质（ii）。

对于性质（iii），Ψ^1 随 c_j 严格递减，这可由命题 2得出。只需证明，当 $m \neq 1$时，Ψ^m 可以随 c_j增加。这由性质（v）可知。最后，性质（iv）由命题 2 得出，性质（v）则显而易见。 □

命题命题14的证明。证明步骤与命题3 相同，只需针对唯一性和内部性条件作适当修改。 □

命题命题15的证明。为了求出 $\sum_{m=1}^{n} v^m\Phi^m(\hat{c})$在 $\boldsymbol{v} \in \mathcal{V}$上的最大和最小不动点，我们只需针对一个固定的 $\hat{c}$求解以下两个线性规划：

$$\max_{\boldsymbol{v}\in\mathbb{R}^n} v^1\Phi^1 + \cdots + v^n\Phi^m \quad \text{subject to} \quad v^1 \geq \cdots \geq v^n \geq 0 \quad \text{and} \quad v^1 + \cdots + v^n = V$$

and

$$\min_{\boldsymbol{v}\in\mathbb{R}^n} v^1\Phi^1 + \cdots + v^n\Phi^m \quad \text{subject to} \quad v^1 \geq \cdots \geq v^n \geq 0 \quad \text{and} \quad v^1 + \cdots + v^n = V$$

现在，由于 Φ^m 是沿着“对角线”的 Ψ^m 一个“切片”，命题13可推出，对所有的 $\hat{c}$，$\Phi^1(\hat{c}) > \Phi^2(\hat{c}) > \cdots > \Phi^n(\hat{c})$，并且 $\sum_{m=1}^{n}\Phi^m(\hat{c}) = q$。由此可知，$(V, 0, \ldots, 0)$ 是第一个线性规划的解，而 $(V/n, \ldots, V/n)$ 是第二个线性规划的解。命题14进而推出了关于最大化和最小化成功概率的结论。 □