arXiv:2602.17301v1 [cs.CR] 19 Feb 2026

格罗滕迪克拓扑与密码学安全性的层论基础：

攻击者模型与 Σ-协议：第一步

Takao Inou´e

大和大学信息学系，大阪，日本*

2026年2月19日

摘要

密码学安全性传统上采用基于博弈或基于模拟的定义来表述。本文提出一种基于格罗滕迪克拓扑与层论的密码学安全性结构性重新表述。

我们的核心思想是将攻击者观察建模为一个 Grothendieck 位点，其中覆盖族表示由高效模拟所决定的部分信息的可容许分解。在此框架中，协议记录自然构成层，而安全性质则表现为几何条件。

首先，我们聚焦于 Σ-协议。我们证明，任何 Σ-协议的交互记录结构都会在相应的层拓扑斯中定义一个托orsor。该托orsor 的局部平凡性对应于零知识，而全局截面的缺失

*电子邮箱：inoue.takao@yamato-u.ac.jp；个人电子邮箱：takaoapple@gmail.com[我更希望使用个人电子邮箱地址进行通信。]

则反映了可靠性。我们通过对 Schnorr Σ-协议的具体分析来阐释这一构造。

这一层论视角从概念上解释了基于模拟的安全性，并为进一步的密码学抽象提出了几何基础。

关键词：密码学安全性、零知识证明、 Σ-协议、格罗滕迪克拓扑、层论、攻击者模型、基于模拟的安全性、扭子。
MSC2020：94A60、18F20、11T71。

目录

1 引言 **2**

2 相关工作 **3**

2.1 基于模拟的安全性与零知识安全性.3 2.2 基于游戏的安全性与攻击者模型. 3 2.3 安全性的范畴论与拓扑斯理论方法 4 2.4 本文的定位.4

3 将攻击者模型视为格罗滕迪克位点 4

4 将Schnorr Σ-协议视为攻击者层 5

5 示例：将Schnorr Σ-协议视为攻击者视图上的层 5

6 将一般 Σ-协议视为层与扭子 7 7 讨论与未来工作 8

1 引言

密码学安全性通常通过基于游戏或基于模拟的框架来定义。尽管这些方法在操作层面行之有效，但它们往往掩盖了安全保证背后的结构性原因。

本文基于格罗滕迪克拓扑和层论，提出了一种密码学安全性的几何重构。核心思想是将攻击者观测解释为一个位点，其中的覆盖编码由高效模拟所确定的部分信息的可接受分解。

在这一框架中，协议记录组合成层，安全性质则体现为内在的几何特征。作为构建一般理论的第一步，我们聚焦于 Σ-协议，并证明其交互记录结构在相关拓扑斯中自然定义了扭子。

本文聚焦于 Σ- 协议与格罗滕迪克拓扑模型之间的核心结构对应关系；更深入的技术细化与扩展留待未来工作。

2 相关工作

2.1 基于模拟的安全性与零知识安全

Goldwasser、Micali 和 Rackoff 将零知识证明引入为一种交互式证明系统，在该系统中，验证者除了命题的有效性之外一无所知 [6]。后续研究确立了基于模拟的安全性作为零知识的标准形式化方法，强调高效模拟器的存在，而非显式的结构性质。

Σ-协议被引入为一类基础的三步交互式证明系统，具有特殊可靠性和诚实验证者零知识性质 [5]。它们在密码学构造中发挥着核心作用，包括身份识别方案以及针对离散对数关系的证明系统 [10]。

尽管基于模拟的定义在操作层面十分有效，但它们仍处于协议结构本身之外。本文的不同之处在于，模拟并未被视为一种辅助算法，而是通过攻击者观察上的格罗滕迪克拓扑以几何方式编码。

2.2 基于游戏的安全性与攻击者模型

基于博弈的安全定义已成为现代密码学中的主流范式，尤其适用于分析复杂协议及其组合[3]。这些方法将安全性建模为高效敌手无法区分不同游戏的性质。

尽管博弈模型功能强大，但往往会抽象掉信息流的内部结构。相比之下，本文采用的层论方法将攻击者视图建模为位点中的对象，从而明确呈现信息的限制与重组。覆盖族编码的是信息的可接受分解，而非对抗策略。

2.3 安全性的范畴论与拓扑斯理论方法

范畴论方法已在多个领域应用于密码学，包括组合安全框架和协议语义 [9, 1]。近年来，人们也开始在计算语义和信息流领域探索拓扑斯理论方法与逻辑方法 [2]。

层论技术已广泛应用于逻辑、几何和分布式系统，用于形式化局部性和上下文依赖性。然而，它们在密码学安全性中的应用仍然有限。

本研究与现有范畴论方法的不同之处，在于明确运用格罗滕迪克拓扑来建模攻击者观察。我们不侧重于组合语义或进程演算，而是将密码安全性质解释为相关拓扑斯中层与扭子的内在几何特征。

2.4 本研究的定位

本文无意取代现有的密码安全定义，而是为 Σ-协议的基于模拟的安全性提供一种概念性和几何性的重新解释。

通过将零知识与局部平凡性相联系，并将可靠性与全局截面的缺失相联系，我们为众所周知的密码学现象提供了结构性解释。这一视角提出了一个统一框架，可借助几何工具对不同的安全概念进行比较和推广。

3 将攻击者模型视为格罗滕迪克位点

我们用一个范畴来建模攻击者观察，其中对象表示协议执行的部分视图，态射对应信息限制。这个范畴刻画了攻击者可能丢失或遗忘信息的方式。

格罗滕迪克拓扑的施加方式是：若目标对象中的信息能够由源对象高效模拟，则将一族态射声明为覆盖。我们将该拓扑称为攻击者拓扑。

4 T作为攻击者层的 Schnorr Σ-协议 af

我们以 Schnorr Σ-协议为例说明该框架。攻击者视图被建模为部分交互记录

$$a, \quad (a, e), \quad (a, e, z),$$

其态射由对话记录分量的擦除给出。

覆盖族对应于视图的可模拟分解。相关的转录预层将每个视图映射为与之兼容的内部随机性值集合。该预层在证明者的随机性重新随机化作用下具有自然作用，从而形成托orsor结构。

这个具体示例为下文发展的通用理论提供了指导性实例。

5 示例：作为攻击者视图上的层的 Schnorr Σ-协议

我们通过将 Schnorr Σ-协议建模为一个 Grothendieck 位点上的层来阐释我们的框架，该位点编码了攻击者观测。

定义 5.1（攻击者观察范畴）。 设 G 是一个素数阶循环群，生成元为 g。设 $y = g^x$ 是一个公开值，其中 $x \in \mathbb{Z}_q$ 是证明者的秘密。

我们定义范畴 $\mathcal{C}_{\mathrm{att}}$ 如下。

- 范畴 $\mathcal{C}_{\mathrm{att}}$ 的对象是攻击者视图，由 *Schnorr* 协议的部分交互记录表示，例如

$$a = g^r, \quad (a, e), \quad (a, e, z),$$

其中 $e \in \mathbb{Z}_q$ 是一个挑战， $z = r + ex$ 是一个响应。

- 态射是对应于遗忘交互记录部分分量的限制映射，例如

$$(a, e, z) \to (a, e), \qquad (a, e) \to a.$$

该范畴是一个偏序集型范畴，用于编码攻击者观察下的信息损失。

定义 5.2 (攻击者格罗滕迪克拓扑)。 如果攻击者能够根据 U_i 上可用的数据，在计算上模拟 U 上的联合分布，则称态射族 $\{U_i \to U\}$ *in* $\mathcal{C}_{\mathrm{att}}$ 为覆盖族。

这个格罗滕迪克拓扑称为攻击者拓扑。

覆盖族是按照计算不可区分性来理解的，而非要求精确重构。

示例。在 Schnorr 协议中，族

$$\{(a, e) \to a,\ (a, z) \to a\}$$

是对象 a 的一个覆盖族，因为承诺的分布可以在不知道秘密 x 的情况下进行模拟。

定义 5.3 (转录预层)。 定义一个预层

$$\mathcal{F} : \mathcal{C}_{\mathrm{att}}^{op} \to \mathbf{Set}$$

它为每个攻击者视图指定与该观察结果一致的交互记录集合。具体来说，

$$\begin{aligned}
\mathcal{F}(a) &= \{r \in \mathbb{Z}_q \mid a = g^r\}, \\
\mathcal{F}(a, e) &= \{(r, z) \in \mathbb{Z}_q^2 \mid z = r + ex\}, \\
\mathcal{F}(a, e, z) &= \begin{cases} \{*\}, & \textit{if } g^z = a \cdot y^e, \\ \varnothing, & \textit{otherwise.} \end{cases}
\end{aligned}$$

限制映射由遗忘对话记录分量诱导。

命题 5.1. 预层 $\mathcal{F}$ 满足关于攻击者拓扑的层条件。

证明概要。 给定覆盖族上的相容局部对话记录数据，标准的 Schnorr 模拟器可以重构出一个全局转录，且重构结果在计算上不可区分。这恰好对应于层的粘合条件。

□

命题 5.2. 层 $\mathcal{F}$ 是由证明者的随机数重新随机化所诱导的 $\mathbb{Z}_q$ 加法作用下的托*orsor*。

注 5.1. 托*orsor* $\mathcal{F}$ 相对于攻击者拓扑是局部平凡的，但不存在选取秘密 x的整体截面。因此，

- 零知识对应于局部平凡性，
- 知识可靠性对应于整体截面的缺失。

6 一般 Σ-协议作为层与托orsor s

现在，我们将前面的例子推广到任意的 Σ-协议，并证明它们的安全性质可以用统一的层论表述来描述。

注。作用群由证明者内部随机性的重新随机化诱导而来。

定义 6.1 (Σ-协议)。 一个 Σ-协议由三个多项式时间算法组成

$$(\mathsf{Commit}, \mathsf{Challenge}, \mathsf{Response})$$

满足完备性、特殊可靠性和诚实验证者零知识。该协议生成形式为 (a, e, z) 的交互记录。

定义 6.2 （攻击者视图范畴）。 设 Π 是一个 Σ-协议。我们定义攻击者观察范畴 $\mathcal{C}_\Pi$ 如下。

- 对象是通过隐藏(a, e, z)的一些分量而得到的部分交互记录。
- 态射是对应于擦除信息的限制映射。

因此， $\mathcal{C}_\Pi$ 编码了攻击者可用的所有可能观测上下文。

定义 6.3 (攻击者拓扑)。 *</style}*一族态射 $\{U_i \to U\}$ *in* $\mathcal{C}_\Pi$ 是一个覆盖族，当且仅当存在一个概率多项式时间模拟器，能够根据关于 U_i 的数据，重构 U 上的分布。

Th*is* 格罗滕迪克拓扑称为与 Π 相关联的攻击者拓扑 .

定义 6.4 (转录预层)。 定义一个预层

$$\mathcal{F}_\Pi : \mathcal{C}_\Pi^{op} \to \mathbf{Set}$$

通过为每个攻击者视图 U 指定与该视图一致的交互记录集合。

定理 6.1 （作为层条件的零知识）。 设 Π 是一个 Σ-协议。若 Π满足诚实验证者零知识，则预层 $\mathcal{F}_\Pi$ 关于攻击者拓扑是一个层。

证明概要。 诚实验证者零知识提供了一个模拟器，能够针对每个攻击者视图在局部生成不可区分的交互记录。局部数据的相容性对应于模拟交互记录的一致性，而全局交互记录在不可区分意义下的存在性则对应于层的粘合公理。 □

定义 6.5 (重新随机化群)。令 G_Π 表示一个群，该群通过对证明者的内部随机性进行重新随机化来作用于交互记录。

定理 6.2 （Σ-协议作为扭子）。设 Π 是一个具有诚实验证者零知识性质的 Σ-协议。那么，层 $\mathcal{F}_\Pi$ 在层拓扑斯中受 G_Π 的作用，是一个扭子。（$\mathcal{C}_\Pi$， J_Π）

证明概要。局部平凡化由模拟器诱导，它提供典范的局部截面。整体截面的不存在性可由可靠性推出：整体截面将确定一个见证，这与零知识性质相矛盾。 □

推论 6.1 （安全性质的结构性解释）。对于一个 Σ-协议Π:

- 诚实验证者零知识对应于扭子 $\mathcal{F}_\Pi$ 的局部平凡性，
- 特殊可靠性对应于整体截面存在性的障碍。

备注。这种表述独立于底层协议的具体代数结构，仅取决于其交互记录结构和模拟性质。

7 讨论与未来工作

本文提出的层论表述为 Σ-协议的基于模拟的安全性提供了结构性解释。模拟并非被视为外部产物，而是自然地从攻击者观察的几何中显现出来。

本研究是迈向密码学安全性几何基础的第一步。恶意验证者、协议组合以及更强安全性概念的扩展，有待未来进一步研究。

我们还希望深入研究这一方向上的可组合性。

参考文献

[1] M. Abadi 和 A. D. Gordon，密码协议演算：*Spi* 演算，Information and Computation，148(1):1–70，1999。

[2] S. Abramsky 和 B. Coecke，范畴量子力学，载于量子逻辑与量子结构手册，Elsevier，2009。

[3] M. Bellare 和 P. Rogaway，现代密码学导论，加州大学圣迭戈分校课程讲义，2005 年。[4] R. Cramer、I. Damg˚ard 和 B. Schoenmakers，部分知识证明与证人隐藏协议的简化设计，载于 密码学进展——*CRYPTO '94*，《计算机科学讲义》第 839 卷，施普林格，1994 年，第 174–187 页。[5] I. Damg˚ard，关于 Σ-协议，《讲义》，奥胡斯大学，2002 年。[6] S. Goldwasser、S. Micali 和 C. Rackoff，交互式证明系统的知识复杂度，《SIAM计算杂志》18(1)：186–208，1989 年。[7] O. Goldreich，密码学基础，第 *1* 卷：基础工具，剑桥大学出版社，2001 年。[8] O. Goldreich，密码学基础，第 *2* 卷：基础应用，剑桥大学出版社，2004 年。[9] J. C. Mitchell，程序设计语言基础，麻省理工学院出版社，1996 年。[10] C. P. Schnorr，智能卡的高效身份识别与签名，载于密码学进展——*CRYPTO '89*，《计算机科学讲义》第 435 卷，施普林格，1990 年。

Takao Inou´e 大和大学信息学系 日本大阪吹田市片山町 2-5-1，邮编 564-0082 inoue.takao@yamato-u.ac.jp（工作邮箱） takaoapple@gmail.com（我更常用个人邮箱）