可证明安全 - 2. 等式理论与静态等价

钱宸

网络空间安全学院
山东大学

2025/10/15

Contents

引言与动机

引言

- 演绎推理系统可推导出敌手可以明确的知道哪些数值

引言

- 演绎推理系统可推导出敌手可以明确的知道哪些数值
- 无法处理敌手观察两种不同的行为而做出判断

引言

- 演绎推理系统可推导出敌手可以明确的知道哪些数值
- 无法处理敌手观察两种不同的行为而做出判断
- 举例: 电子投票

等式理论

等式理论

演绎推理无法解决函数内部的等式推理问题

异或 XOR

- 对于任意密钥 k 和任意消息 m,
- 有 $\mathsf{senc}(m, k \oplus k) = \mathsf{senc}(m, 0)$ 或者 $\mathsf{senc}(m \oplus m, k) = \mathsf{senc}(0, k)$

上面例子中的推导关系**并不能**被演绎推理系统所捕捉

等式理论

- 等式理论 (Equational Theory) 是对函数符号的等式进行建模

等式理论

- 等式理论 (Equational Theory) 是对函数符号的等式进行建模
- 等式理论 E 是一个包含若干等式的集合

等式理论

- 等式理论 (Equational Theory) 是对函数符号的等式进行建模
- 等式理论 E 是一个包含若干等式的集合
- 每个等式形如 $l = r$, 其中 l 和 r 是术语

等式理论

- 等式理论 (Equational Theory) 是对函数符号的等式进行建模
- 等式理论 E 是一个包含若干等式的集合
- 每个等式形如 $l = r$, 其中 l 和 r 是术语
- 等式理论定义了一个最小的等价关系 $=_E$

等式理论

- 等式理论 (Equational Theory) 是对函数符号的等式进行建模
- 等式理论 E 是一个包含若干等式的集合
- 每个等式形如 $l = r$, 其中 l 和 r 是术语
- 等式理论定义了一个最小的等价关系 $\equiv_E$

等式理论

- 等式理论 (Equational Theory) 是对函数符号的等式进行建模
- 等式理论 E 是一个包含若干等式的集合
- 每个等式形如 $l = r$, 其中 l 和 r 是术语
- 等式理论定义了一个最小的等价关系 $\equiv_E$

定义 (等式理论)

$\equiv_E$ 是包含 E 中所有等式的最小关系, 并且满足:

- 反身性: $t \equiv_E t$
- 对称性: 如果 $t_1 \equiv_E t_2$, 则 $t_2 \equiv_E t_1$
- 传递性: 如果 $t_1 \equiv_E t_2$ 且 $t_2 \equiv_E t_3$, 则 $t_1 \equiv_E t_3$
- 上下文封闭性: 如果 $t_1 \equiv_E t_2$, 则对于任意上下文 $C[\cdot]$, 有 $C[t_1] \equiv_E C[t_2]$
- 替换封闭性: 如果 $t_1 \equiv_E t_2$, 则对于任意替换 σ, 有 $t_1\sigma \equiv_E t_2\sigma$

异或操作

- 异或操作的等式理论 $E_{\oplus}$ 包含以下等式:

异或操作

- 异或操作的等式理论 $E_{\oplus}$ 包含以下等式:
  - $x \oplus 0 = x$

异或操作

- 异或操作的等式理论 $E_\oplus$ 包含以下等式:
  - $x \oplus 0 = x$
  - $x \oplus x = 0$

异或操作

- 异或操作的等式理论 $E_{\oplus}$ 包含以下等式:
  - $x \oplus 0 = x$
  - $x \oplus x = 0$
  - $x \oplus y = y \oplus x$

异或操作

- 异或操作的等式理论 $E_\oplus$ 包含以下等式:
  - $x \oplus 0 = x$
  - $x \oplus x = 0$
  - $x \oplus y = y \oplus x$
  - $(x \oplus y) \oplus z = x \oplus (y \oplus z)$

异或操作

- 异或操作的等式理论 $E_\oplus$ 包含以下等式:
  - $x \oplus 0 = x$
  - $x \oplus x = 0$
  - $x \oplus y = y \oplus x$
  - $(x \oplus y) \oplus z = x \oplus (y \oplus z)$
- 例如, 根据 $E_\oplus$, 有 $(a \oplus b) \oplus b \equiv_{E_\oplus} a$

异或操作

- 异或操作的等式理论 $E_{\oplus}$ 包含以下等式:
  - $x \oplus 0 = x$
  - $x \oplus x = 0$
  - $x \oplus y = y \oplus x$
  - $(x \oplus y) \oplus z = x \oplus (y \oplus z)$
- 例如, 根据 $E_{\oplus}$, 有 $(a \oplus b) \oplus b \equiv_{E_{\oplus}} a$

异或操作

- 异或操作的等式理论 $E_{\oplus}$ 包含以下等式:
  - $x \oplus 0 = x$
  - $x \oplus x = 0$
  - $x \oplus y = y \oplus x$
  - $(x \oplus y) \oplus z = x \oplus (y \oplus z)$
- 例如, 根据 $E_{\oplus}$, 有 $(a \oplus b) \oplus b \equiv_{E_{\oplus}} a$

例子

令 $u = k_1 \oplus k_2$, $v = k_2 \oplus k_3$, 且 $w = k_1 \oplus k_3$, 证明 $u \oplus v \equiv_{E_{\oplus}} w$

模幂函数

- 模幂函数的等式理论 E_{exp} 包含以下等式:

模幂函数

- 模幂函数的等式理论 E_{exp} 包含以下等式:
  - $\exp(\exp(x,y),z) = \exp(\exp(x,z),y)$

模幂函数

- 模幂函数的等式理论 E_{exp} 包含以下等式:
  - $\exp(\exp(x, y), z) = \exp(\exp(x, z), y)$
  - $\exp(\mathsf{mult}(x, y)) = \exp(\exp(x), y)$

模幂函数

- 模幂函数的等式理论 E_{exp} 包含以下等式:
  - $\exp(\exp(x, y), z) = \exp(\exp(x, z), y)$
  - $\exp(\mathsf{mult}(x, y)) = \exp(\exp(x), y)$

模幂函数

- 模幂函数的等式理论 E_{exp} 包含以下等式:
  - $\exp(\exp(x, y), z) = \exp(\exp(x, z), y)$
  - $\exp(\mathsf{mult}(x, y)) = \exp(\exp(x), y)$

例子

令 $u = \exp(g, x)$, $v = \exp(g, y)$, 且 $w = \exp(g, \mathsf{mult}(x, y))$, 证明 $u^y \equiv_{E_{\mathsf{exp}}} w$

加密

$$\mathcal{F}_{\mathsf{dec}} = \{\mathsf{sdec}, \mathsf{adec}, \mathsf{fst}, \mathsf{snd}\}.$$

- $\mathcal{F}_0$ 为任意个额外的函数符号集合，且 $\mathcal{F}_0 \cap (\mathcal{F}_{\mathsf{std}} \cup \mathcal{F}_{\mathsf{dec}}) = \emptyset$.

加密

$$\mathcal{F}_{\mathsf{dec}} = \{\mathsf{sdec}, \mathsf{adec}, \mathsf{fst}, \mathsf{snd}\}.$$

- $\mathcal{F}_0$ 为任意个额外的函数符号集合，且 $\mathcal{F}_0 \cap (\mathcal{F}_{\mathsf{std}} \cup \mathcal{F}_{\mathsf{dec}}) = \emptyset$.
- 加密函数的等式理论 E_{dec} 定义在 $\mathcal{T}(\mathcal{F}_{\mathsf{std}} \cup \mathcal{F}_{\mathsf{dec}} \cup \mathcal{F}_0, \mathcal{X})$ 包含以下等式:

加密

$$\mathcal{F}_{\mathsf{dec}} = \{\mathsf{sdec}, \mathsf{adec}, \mathsf{fst}, \mathsf{snd}\}.$$

- $\mathcal{F}_0$ 为任意个额外的函数符号集合，且 $\mathcal{F}_0 \cap (\mathcal{F}_{\mathsf{std}} \cup \mathcal{F}_{\mathsf{dec}}) = \emptyset$.
- 加密函数的等式理论 E_{dec} 定义在 $\mathcal{T}(\mathcal{F}_{\mathsf{std}} \cup \mathcal{F}_{\mathsf{dec}} \cup \mathcal{F}_0, \mathcal{X})$ 包含以下等式:
  - $\mathsf{sdec}(\mathsf{senc}(x, y), y) = x$

加密

$$\mathcal{F}_{\mathsf{dec}} = \{\mathsf{sdec}, \mathsf{adec}, \mathsf{fst}, \mathsf{snd}\}.$$

- $\mathcal{F}_0$ 为任意个额外的函数符号集合，且 $\mathcal{F}_0 \cap (\mathcal{F}_{\mathsf{std}} \cup \mathcal{F}_{\mathsf{dec}}) = \emptyset$.
- 加密函数的等式理论 E_{dec} 定义在 $\mathcal{T}(\mathcal{F}_{\mathsf{std}} \cup \mathcal{F}_{\mathsf{dec}} \cup \mathcal{F}_0, \mathcal{X})$ 包含以下等式:
  - $\mathsf{sdec}(\mathsf{senc}(x, y), y) = x$
  - $\mathsf{adec}(\mathsf{aenc}(x, \mathsf{pk}(y)), y) = x$

加密

$$\mathcal{F}_{\mathsf{dec}} = \{\mathsf{sdec}, \mathsf{adec}, \mathsf{fst}, \mathsf{snd}\}.$$

- $\mathcal{F}_0$ 为任意个额外的函数符号集合，且 $\mathcal{F}_0 \cap (\mathcal{F}_{\mathsf{std}} \cup \mathcal{F}_{\mathsf{dec}}) = \emptyset$.
- 加密函数的等式理论 E_{dec} 定义在 $\mathcal{T}(\mathcal{F}_{\mathsf{std}} \cup \mathcal{F}_{\mathsf{dec}} \cup \mathcal{F}_0, \mathcal{X})$ 包含以下等式:
  - $\mathsf{sdec}(\mathsf{senc}(x, y), y) = x$
  - $\mathsf{adec}(\mathsf{aenc}(x, \mathsf{pk}(y)), y) = x$
  - $\mathsf{fst}(\langle x, y\rangle) = x$

加密

$$\mathcal{F}_{\mathsf{dec}} = \{\mathsf{sdec}, \mathsf{adec}, \mathsf{fst}, \mathsf{snd}\}.$$

- $\mathcal{F}_0$ 为任意个额外的函数符号集合，且 $\mathcal{F}_0 \cap (\mathcal{F}_{\mathsf{std}} \cup \mathcal{F}_{\mathsf{dec}}) = \emptyset$.
- 加密函数的等式理论 E_{dec} 定义在 $\mathcal{T}(\mathcal{F}_{\mathsf{std}} \cup \mathcal{F}_{\mathsf{dec}} \cup \mathcal{F}_0, \mathcal{X})$ 包含以下等式:
  - $\mathsf{sdec}(\mathsf{senc}(x, y), y) = x$
  - $\mathsf{adec}(\mathsf{aenc}(x, \mathsf{pk}(y)), y) = x$
  - $\mathsf{fst}(\langle x, y\rangle) = x$
  - $\mathsf{snd}(\langle x, y\rangle) = y$

加密

$$\mathcal{F}_{\mathsf{dec}} = \{\mathsf{sdec}, \mathsf{adec}, \mathsf{fst}, \mathsf{snd}\}.$$

- $\mathcal{F}_0$ 为任意个额外的函数符号集合，且 $\mathcal{F}_0 \cap (\mathcal{F}_{\mathsf{std}} \cup \mathcal{F}_{\mathsf{dec}}) = \emptyset$.
- 加密函数的等式理论 E_{dec} 定义在 $\mathcal{T}(\mathcal{F}_{\mathsf{std}} \cup \mathcal{F}_{\mathsf{dec}} \cup \mathcal{F}_0, \mathcal{X})$ 包含以下等式:
  - $\mathsf{sdec}(\mathsf{senc}(x, y), y) = x$
  - $\mathsf{adec}(\mathsf{aenc}(x, \mathsf{pk}(y)), y) = x$
  - $\mathsf{fst}(\langle x, y \rangle) = x$
  - $\mathsf{snd}(\langle x, y \rangle) = y$

加密

$$\mathcal{F}_{\mathsf{dec}} = \{\mathsf{sdec}, \mathsf{adec}, \mathsf{fst}, \mathsf{snd}\}.$$

- $\mathcal{F}_0$ 为任意个额外的函数符号集合，且 $\mathcal{F}_0 \cap (\mathcal{F}_{\mathsf{std}} \cup \mathcal{F}_{\mathsf{dec}}) = \emptyset$.
- 加密函数的等式理论 E_{dec} 定义在 $\mathcal{T}(\mathcal{F}_{\mathsf{std}} \cup \mathcal{F}_{\mathsf{dec}} \cup \mathcal{F}_0, \mathcal{X})$ 包含以下等式:
  - $\mathsf{sdec}(\mathsf{senc}(x, y), y) = x$
  - $\mathsf{adec}(\mathsf{aenc}(x, \mathsf{pk}(y)), y) = x$
  - $\mathsf{fst}(\langle x, y\rangle) = x$
  - $\mathsf{snd}(\langle x, y\rangle) = y$

例子

令 $u = \mathsf{senc}(m, k)$, $v = k$, 且 $w = m$, 证明 $\mathsf{sdec}(u, v) \equiv_{E_{\mathsf{dec}}} w$

演绎 (deduction) 系统

演绎与归纳

- **演绎 (deduction)**是从一般到特殊的推理过程
- **归纳 (induction)**是从特殊到一般的推理过程
- **演绎系统**是基于一组公理和推理规则，用于从已知事实推导出新事实的形式系统
- **归纳系统**是基于观察和实例，用于从具体例子中总结出一般规律的形式系统

演绎 (deduction) 系统

演绎与归纳

- **演绎 (deduction)**是从一般到特殊的推理过程
- **归纳 (induction)**是从特殊到一般的推理过程
- **演绎系统**是基于一组公理和推理规则，用于从已知事实推导出新事实的形式系统
- **归纳系统**是基于观察和实例，用于从具体例子中总结出一般规律的形式系统

定义 (演绎系统)

给定一组初始术语 S 和等式理论 E，演绎系统定义了一组推理规则，用于生成新的术语. 记为 $S \vdash_E t$，表示术语 t 可以从初始术语集 S 通过有限次应用推理规则得到.

$$\frac{t_1 \quad \cdots \quad t_n}{f(t_1, \ldots, t_n)} \qquad \frac{t}{t'} \text{ if } t =_E t'$$

例子

加密例子

考虑定义在 $\mathcal{T}(\mathcal{F}_{\mathsf{std}} \cup \mathcal{F}_{\mathsf{dec}} \cup \{\oplus\}, \mathcal{X})$ 上的等式理论 $E_{\oplus} \cup E_{\mathsf{enc}}$. 考虑

$$S = \{\mathsf{senc}(a, a \oplus c), a \oplus b, b \oplus c\}.$$

证明 $S \vdash_{E_{\oplus} \cup E_{\mathsf{enc}}} a$.

语境

定义 (语境)

语境 (Context) 是一个包含零个或多个空位 (holes) 的术语. 记为 $C[\cdot]$, 其中每个空位可以被任意术语替换. 例如, $C[\cdot] = \mathsf{senc}(\cdot, k)$ 是一个语境, 可以将空位替换为任意术语 t 得到 $\mathsf{senc}(t, k)$.

定理 (语境等价 [Abadi and Cortier, 2006])

对于任意术语 t, $S \vdash_E t$ 当且仅当对于任意语境 $C[\cdot]$, 有 $\mathcal{N}(C) = \emptyset$ 且存在 $t_1, \ldots, t_m \in S$ 使得 $t =_E C[t_1, \ldots, t_m]$.

演绎与归纳等价

定理 (演绎与归纳等价)

对于任意项集合 S, 以及 t 为项代数 $\mathcal{T}(\mathcal{F}_{std}, \mathcal{X})$ 中的项, 有 $S \vdash_{\mathcal{I}_{DY}} t$ 当且仅当 $S \vdash_{E_{enc}} t$.

静态等价性

静态等价性

演绎也不能完全捕捉敌手的推理能力. 敌手可以观察到消息发送的顺序, 并利用这一信息进行推理.

定义 (框架)

- 一个框架 (frame) 为一个表达式 $\phi = \nu\tilde{n}\theta = \nu\tilde{n}\{M_1/x_1, \ldots, M_n/x_n\}$. 其中 $\tilde{n} \subseteq \mathcal{N}$ 为 ϕ 中的一组名称, θ 为一个替换, 且 ν 为一个术语.
- 其中 $M_1, \ldots, M_n$ 表示敌手不知道在 $\tilde{n}$ 中的消息的时候获得的信息.
- 我们简写 $\phi = \nu k\theta = \nu(\tilde{n} \cup \{k\})\theta$.
- $\mathsf{Dom}(\phi) = \mathsf{Dom}(\theta)$

框架样例

例子

令 $\phi = \nu k\{1/x_1, 0/x_2, \mathsf{senc}(0,k)/x_3\}$ 为一个框架，表示敌手看见两个常数 0, 1, 以及一个用密钥 k 加密的消息 $\mathsf{senc}(0,k)$. 并且敌手一开始并不知道 k.

框架下的演绎系统

定义 (框架下的演绎系统)

给定一个框架 $\phi = \nu\tilde{n}\theta$ 和等式理论 E, 一个项 t 能够被演绎自 ϕ, 记为 $\phi \vdash_E t$, 如果

$$\mathsf{Dom}(\phi) \cup (\mathcal{N} \setminus \tilde{n}) \vdash_E t$$

框架下的演绎系统

样例

$\phi_1 = \nu_1(n,k)\theta_1$, 其中 $\theta_1 = \{\mathsf{senc}(\langle n,n\rangle,k)/x_1, k/y\}$. 则 $\nu_1 \vdash_{E_{\mathsf{Enc}}} n$.

框架下的演绎系统

样例

$\phi_1 = \nu_1(n, k)\theta_1$, 其中 $\theta_1 = \{\mathsf{senc}(\langle n, n\rangle, k)/x_1, k/y\}$. 则 $\nu_1 \vdash_{E_{\mathsf{Enc}}} n$.

$M = \mathsf{fst}(\mathsf{sdec}(x, y))$ 被称为策略 (recipe).

定义 (策略)

给定一个框架 $\phi = \nu\tilde{n}\theta$ 和等式理论 E, 一个项 M 是自由的如果 $\mathsf{n}(M) \cap \tilde{n} = \emptyset$. 一个项 t 能够被策略 M 生成, 记为 $\phi \vdash_E^M t$, 如果 M 关于 ϕ 是自由的且 $t =_E M\theta$.

框架下的演绎系统

定义

给定一个框架 $\phi = \nu\tilde{n}\theta$ 和等式理论 E, 一个项 t 能够被演绎自 ϕ, 记为 $\phi \vdash_E t$, 当且仅当存在一个策略 M 使得 $\phi \vdash_E^M t$.

静态等价的定义

考虑 $\phi_1 = \{0/x, 1/y\}$ 和 $\phi_2 = \{1/x, 0/y\}$. 敌手显然观测到同样的项.

定义 (α-换位)

给定两个框架 $\phi_1 = \nu_1\tilde{n}_1\theta_1$ 和 $\phi_2 = \nu_2\tilde{n}_2\theta_2$, 如果存在一个双射 $\pi : \mathsf{Dom}(\theta_1) \to \mathsf{Dom}(\theta_2)$ 使得对于任意 $x \in \mathsf{Dom}(\theta_1)$, 有 $x\theta_1 =_\alpha x\pi\theta_2$, 则称 ϕ_1 和 ϕ_2 是换位的, 记为 $\phi_1 \sim_\alpha \phi_2$.

静态等价的定义

考虑 $\phi_1 = \{0/x, 1/y\}$ 和 $\phi_2 = \{1/x, 0/y\}$. 敌手显然观测到同样的项.

定义 (α-换位)

给定两个框架 $\phi_1 = \nu_1\tilde{n}_1\theta_1$ 和 $\phi_2 = \nu_2\tilde{n}_2\theta_2$, 如果存在一个双射 $\pi : \mathsf{Dom}(\theta_1) \to \mathsf{Dom}(\theta_2)$ 使得对于任意 $x \in \mathsf{Dom}(\theta_1)$, 有 $x\theta_1 =_\alpha x\pi\theta_2$, 则称 ϕ_1 和 ϕ_2 是换位的, 记为 $\phi_1 \sim_\alpha \phi_2$.

定义

我们说 $M =_E N$ 在框架 ϕ 下成立, 记为 $(M =_E N)_\phi$, 如果存在 $\tilde{n}$ 和 θ 满足 $\phi =_\alpha \mu\tilde{n}\theta$, 且 M, N 都是自由的关于 $\tilde{n}$, 并且 $M\theta \equiv_E N\theta$.

静态等价

定义 (静态等价)

给定两个框架 ϕ_1 和 ϕ_2 关于等式理论 E 静态等价, 如果对于任意项 M, N, 有

$$(M =_E N)_{\phi_1} \iff (M =_E N)_{\phi_2}$$

静态等价

样例 1

令 $\phi_1 = \nu\{0/x, 1/y\}$ 和 $\phi_2 = \nu\{1/x, 0/y\}$. 则 ϕ_1 和 ϕ_2 关于任意等式理论静态不等价.

静态等价

样例 1

令 $\phi_1 = \nu\{0/x, 1/y\}$ 和 $\phi_2 = \nu\{1/x, 0/y\}$. 则 ϕ_1 和 ϕ_2 关于任意等式理论静态不等价.

样例 2

令 $\phi_1 = \nu k\{\mathsf{aenc}(0, \mathsf{pk}(k))/x, \mathsf{pk}(k)/y\}$ 和 $\phi_2 = \nu k\{\mathsf{aenc}(1, \mathsf{pk}(k))/x, \mathsf{pk}(k)/y\}$. 则 ϕ_1 和 ϕ_2 关于等式理论 E_{enc} 静态不等价.

静态等价

样例 1

令 $\phi_1 = \nu\{0/x, 1/y\}$ 和 $\phi_2 = \nu\{1/x, 0/y\}$. 则 ϕ_1 和 ϕ_2 关于任意等式理论静态不等价.

样例 2

令 $\phi_1 = \nu k\{\mathsf{aenc}(0, \mathsf{pk}(k))/x, \mathsf{pk}(k)/y\}$ 和 $\phi_2 = \nu k\{\mathsf{aenc}(1, \mathsf{pk}(k))/x, \mathsf{pk}(k)/y\}$. 则 ϕ_1 和 ϕ_2 关于等式理论 E_{enc} 静态不等价.

样例 3

令 $\phi_1 = \nu(k, r)\{\mathsf{aenc}(\langle 0, r\rangle, \mathsf{pk}(k))/x, \mathsf{pk}(k)/y\}$ 和 $\phi_2 = \nu(k, r)\{\mathsf{aenc}(\langle 1, r\rangle, \mathsf{pk}(k))/x, \mathsf{pk}(k)/y\}$. 则 ϕ_1 和 ϕ_2 关于等式理论 E_{enc} 静态等价.

静态等价的性质

静态等价在限缩和组合下是封闭的

定义

给定两个静态等价的框架 ϕ_1 和 ϕ_2 关于等式理论 E, 则对于任意名称 $n \notin \mathsf{n}(\phi_1) \cup \mathsf{n}(\phi_2)$, 有 $\nu n.\phi_1$ 和 $\nu n.\phi_2$ 关于等式理论 E 静态等价. 并且对于任意静态等价的框架 ϕ_3, 有 $\phi_1 \cup \phi_3$ 和 $\phi_2 \cup \phi_3$ 关于等式理论 E 静态等价.

References I

Abadi, M. and Cortier, V. (2006).
Deciding knowledge in security protocols under equational theories.
Theoretical Computer Science, 367(1-2):2–32.