チュートリアル：
暗号プロトコルの結合可能安全性とその形式検証

2014/9/5

米山 一樹

NTTセキュアプラットフォーム研究所

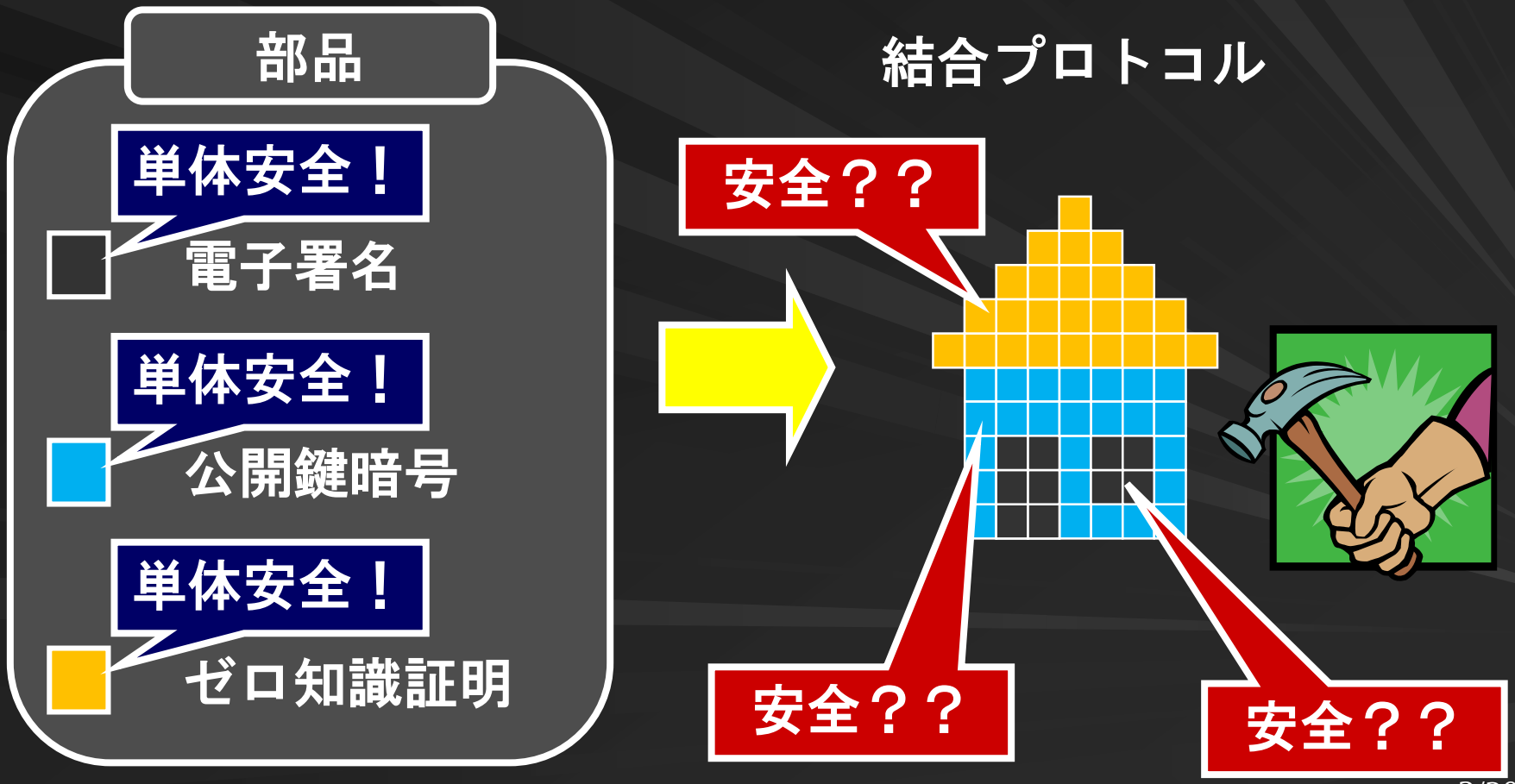
本チュートリアルの概要

汎用結合可能形式検証（Universally Composable Symbolic Analysis）の紹介

- 汎用結合可能安全性
- 形式検証と計算論的健全性
- 汎用結合可能形式検証

暗号プロトコル設計によくある問題

- 単体では安全な部品プリミティブでも
  組み合わせると安全でなくなる



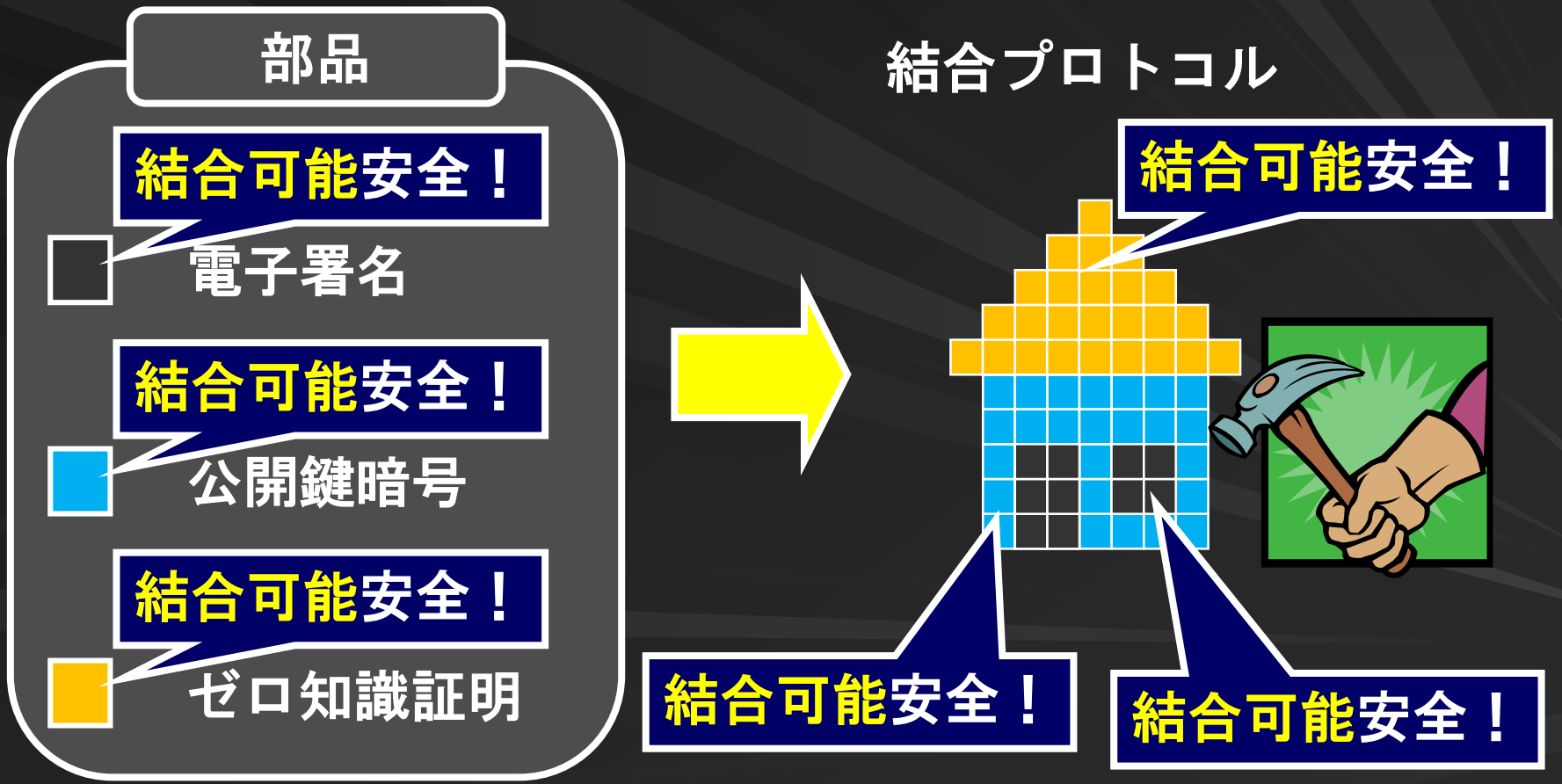
結合プロトコルの安全性証明

- 単体での安全性と多重同時実行時の安全性のギャップ
  - 入力・出力の部品間における流用
  - 部品による参加者の変化

- 解決のアプローチ
  - まとめて1つの巨大なプロトコルとして扱う
    - ⇒ 安全性証明の複雑化
  - **結合可能安全性**を持つ部品同士を結合する
    - ⇒ **モジュール的**に安全性証明可能

汎用結合可能安全性

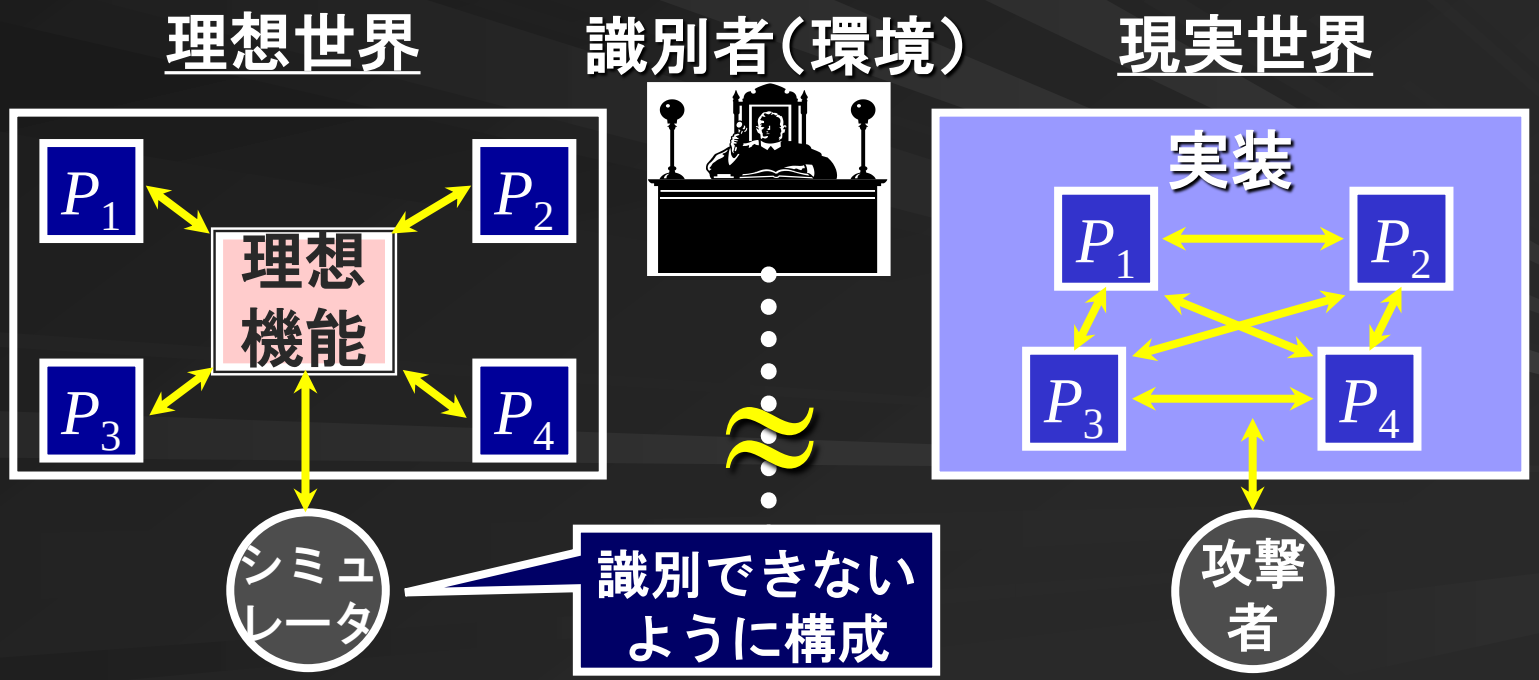
- 汎用結合可能安全性を満たした部品は
  結合後も安全性を保つ



汎用結合可能性安全性の定義と証明

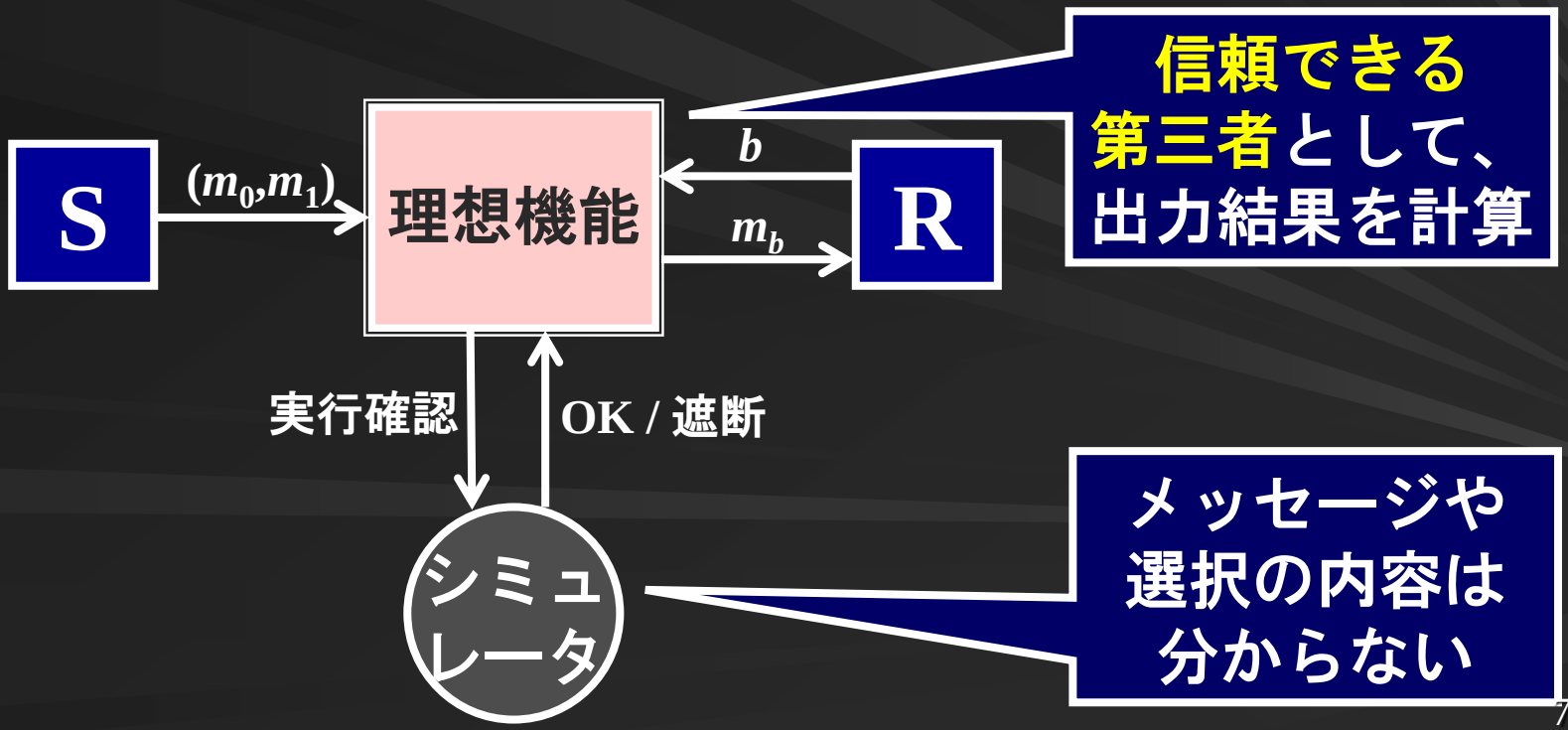
- その部品の機能要件と確保したい安全性をあらわす**理想機能**を定義
- 部品の具体的な実現法（実装）がその理想機能と**識別できない**ことを示す

∀攻撃者 ∃シミュレータ s.t. ∀識別者 理想世界≈現実世界



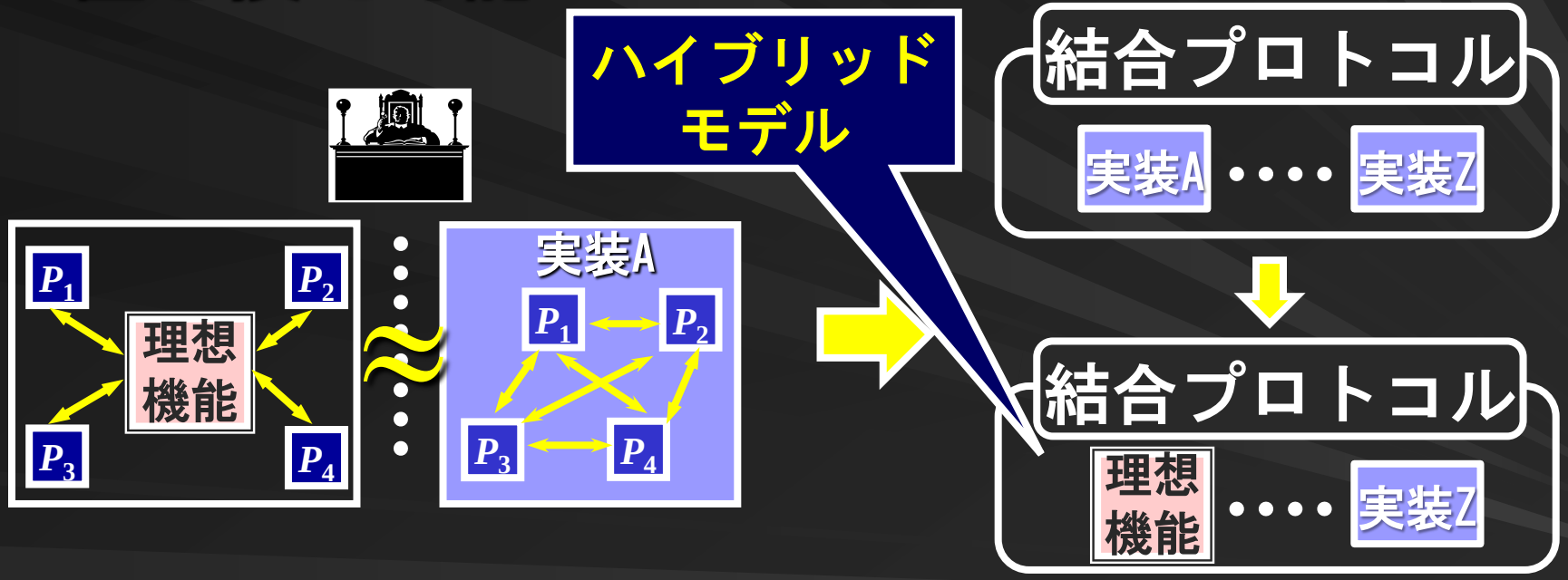
理想機能の例

- 紛失通信
  - 受信者 R は送信者 S から(m_0,m_1)の片方を得る
    - S は R がどちらを受け取ったか分からない
    - R は受け取らなかった方の値は分からない



結合定理

- 部品の実装が汎用結合可能性を満たすならば、結合プロトコル内の部品を**理想機能に置き換え可能**



- 結合プロトコル内で**理想的なモジュール**として利用可能
- 汎用結合可能性の証明は**依然として必要**

本チュートリアルの概要

汎用結合可能形式検証（Universally Composable Symbolic Analysis）の紹介

- 汎用結合可能安全性
- **形式検証と計算論的健全性**
- 汎用結合可能形式検証

形式検証

- 暗号プロトコルの安全性を**誤りなく自動的に検証**するための手法
  - 値、メッセージ、操作を**記号の集合**として表し、プロトコルを**抽象化**することで、機械的に検証

- **Dolev-Yao (DY) モデル [DY81]**

メッセージ：$M = 11001\ldots$ ⇒ 項 t

暗号文：$CT = \mathrm{Enc}_{sk}(t)$ ⇒ 項 $\{t\}_{sk}$

復号操作：$\mathrm{Dec}_{sk}(CT)$ ⇒ $\dfrac{E \vdash sk \quad E \vdash \{t\}_{sk}}{E \vdash t}$

skを知っている時だけ復号可能

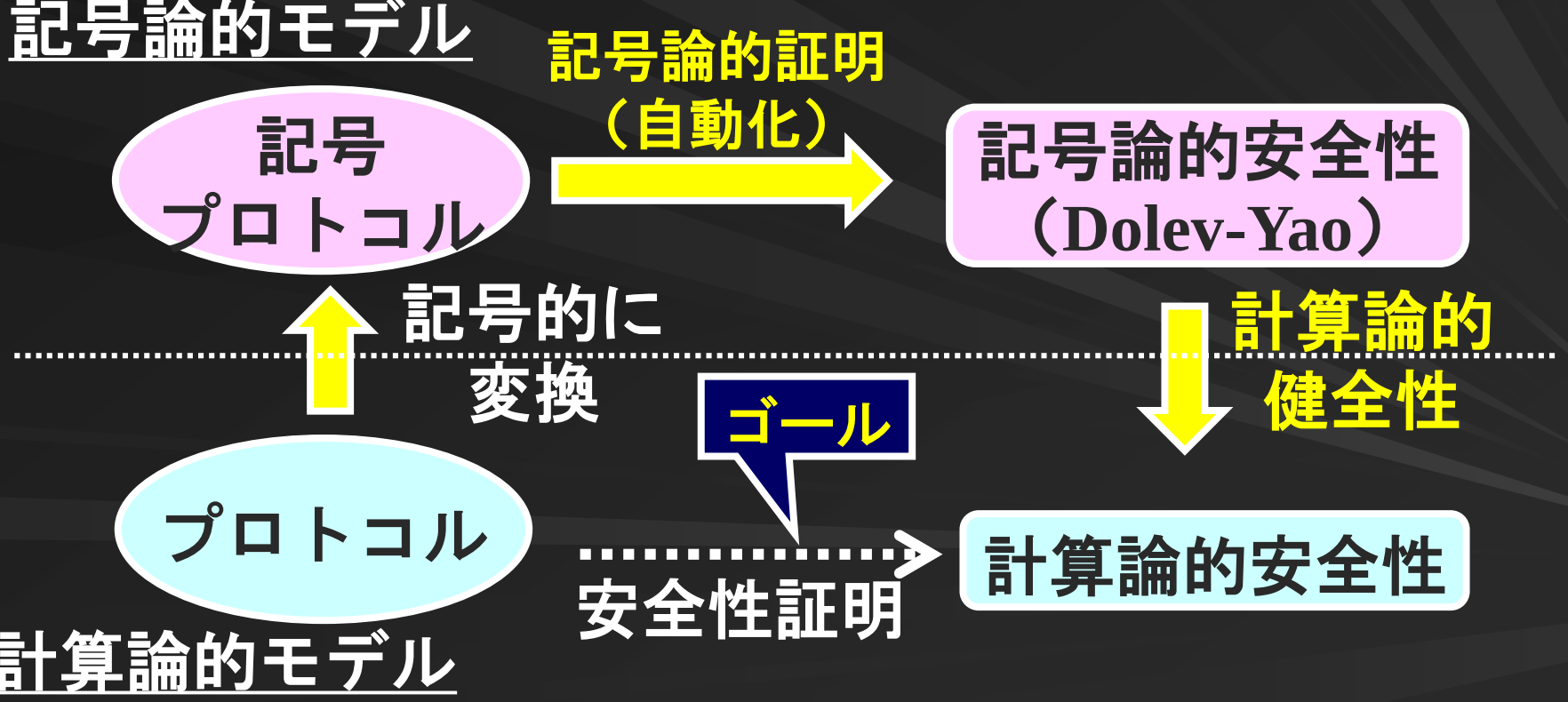
記号論的モデルと計算論的モデル

- 記号論的モデル
  -  安全性証明が**自動化**できる
  -  構成要素が**理想的に安全**であることを仮定
- 計算論的モデル
  -  安全性証明がしばしば**複雑化**
  -  **計算量的**に制限された攻撃者を扱える

いいとこ取り（**計算量的**な攻撃者に対する安全性を**自動**で証明）したい！

計算論的健全性

- Abadi-Rogaway [AR00]による橋渡し
  - 記号論的モデルが**計算論的健全**ならば、**記号論的安全なプロトコルは計算論的安全**



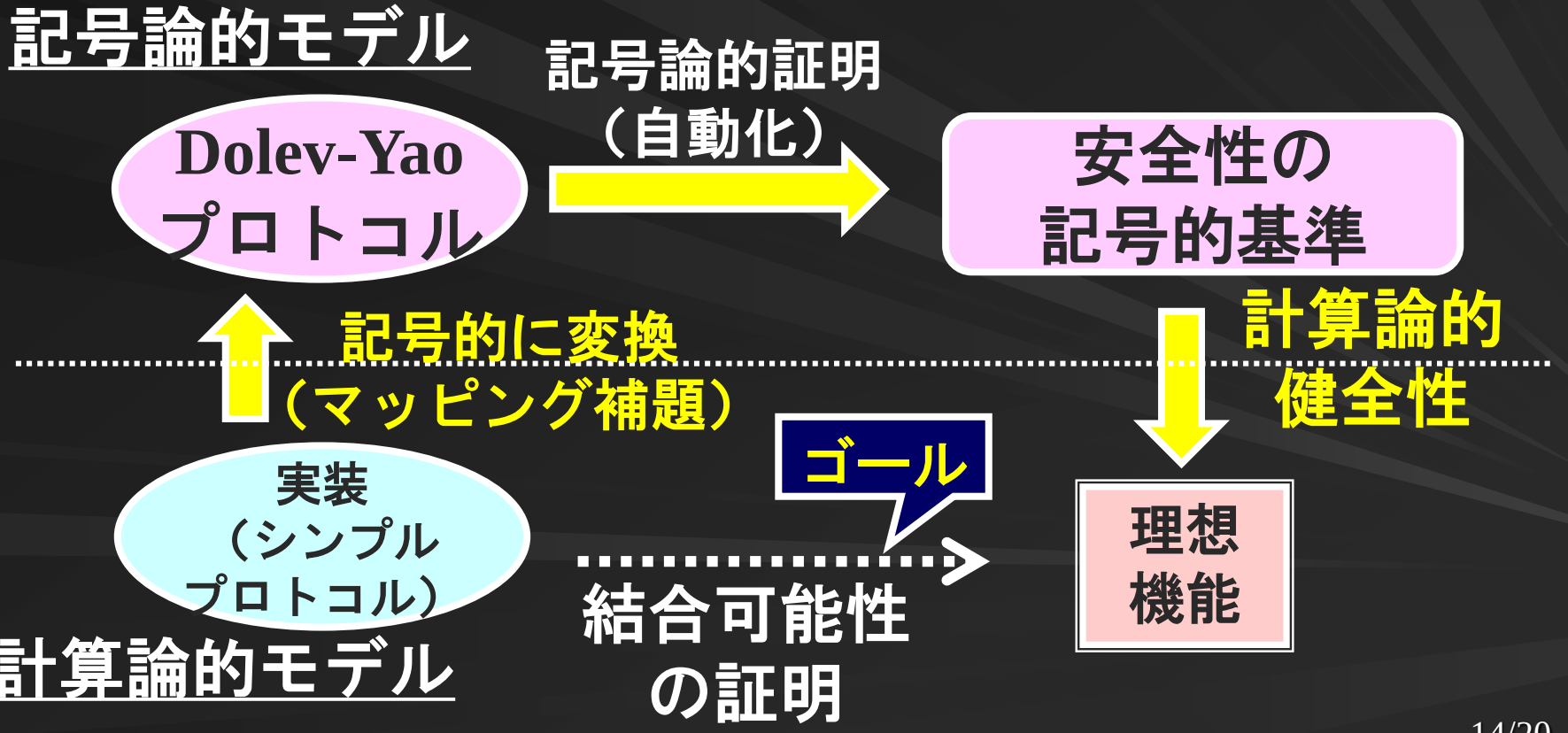
本チュートリアルの概要

汎用結合可能形式検証（Universally Composable Symbolic Analysis）の紹介

- 汎用結合可能安全性
- 形式検証と計算論的健全性
- **汎用結合可能形式検証**

汎用結合可能形式検証の目的

- 汎用結合可能性の証明自体の平易化
  - 記号論的証明 ⇒ 汎用結合可能安全性



Canneti-Herzog [CH06]

- 相互認証・鍵交換の汎用結合可能形式検証
  - プロトコル：
    公開鍵暗号の理想機能を用いた実装の記号化
  - 記号的基準：
    機能ごと（**相互認証と鍵交換**）に定義

- 計算論的健全性と完全性（等価）
  - Dolev-Yaoプロトコルが記号的基準を満たす
    iff
    実装が汎用結合可能安全性を満たす

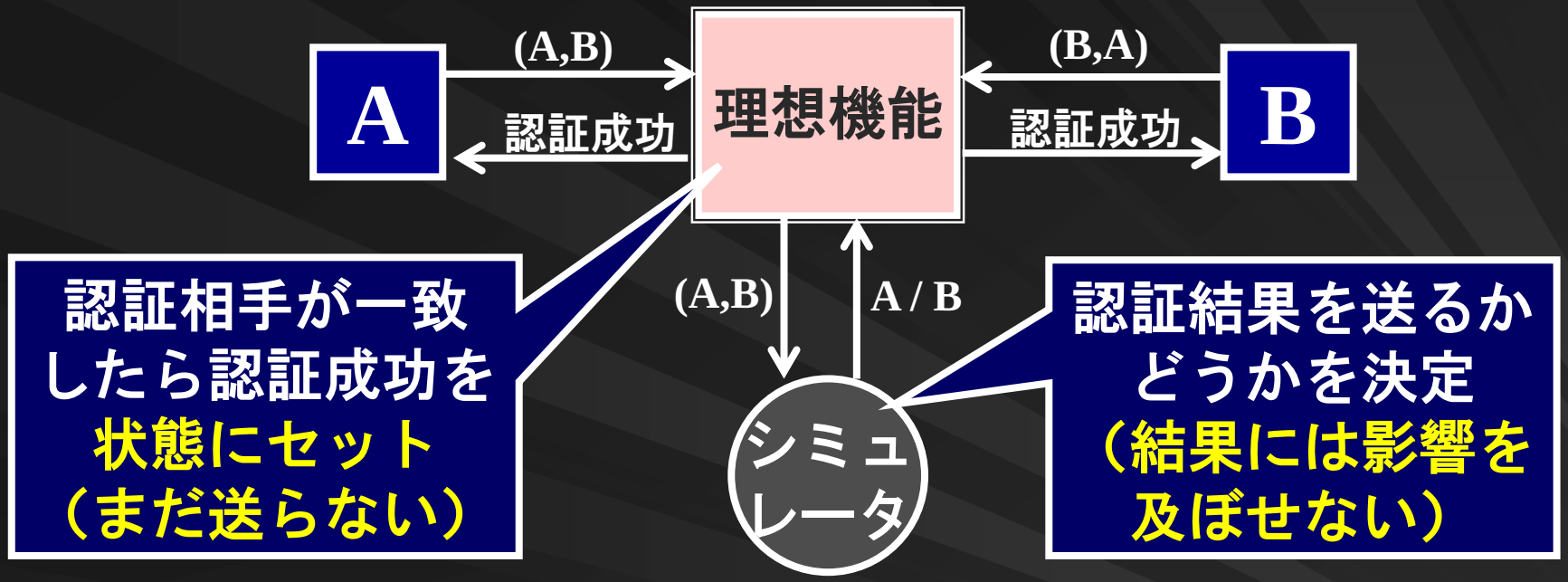
シンプルプロトコルとDolev-Yaoプロトコル

- シンプルプロトコル p（計算論的）
  - 一般的操作（乱数生成など）と**公開鍵暗号の理想機能**の組み合わせに動作を限定
  - **ハイブリッドモデル**に相当
- Dolev-Yaoプロトコル p’（記号論的）
  - **理想的な公開鍵暗号**を仮定
- マッピング補題
  - **p の任意の実行列**に対応する **p’ の正当な実行列**が無視できる確率を除いて存在する

記号的基準（相互認証の例）

- Dolev-Yaoプロトコルの実行列が、Aによる出力 ⟨Finished|A|B|m⟩ を含んでいるならば、それより前に、B による出力 ⟨Started|B|A|m′⟩ を含む

理想機能（相互認証）



- 健全性の証明
  - Bが理想機能にメッセージを送る前にAが認証成功を受け取ったとすると、⟨Finished|A|B|m⟩が⟨Started|B|A|m′⟩ より前に実行列に現れる

関連研究

- 公開鍵暗号以外を用いたプロトコルへの拡張
  - [Pat05] **電子署名**を用いた相互認証
  - [CG10] 電子署名と**DH鍵交換**を用いた認証鍵交換

- 相互認証と鍵交換以外の理想機能の実現
  - [ZZLW12] 電子署名と双線形写像を用いた**グループ認証鍵交換**
  - [DD14] 準同型暗号、コミットメント、ゼロ知識証明を用いた**任意の理想機能**

次のチュートリアルで詳しく解説

まとめ

- 汎用結合可能性は結合プロトコルの安全性証明を**モジュール化**することで、平易化することができる
  - しかし、汎用結合可能性の証明自体は簡単ではない
- 汎用結合可能形式検証を利用することで、汎用結合可能性の証明を**自動的に**行うことが可能となる