Computationally sound formal blind signature

Hideki Sakurada
NTT Communication Science Laboratories
Nippon Telephone and Telegraph Corporation
Joint work with Masami Hagiya

Motivation

- Bridging the gap between
  - Computational, probabilistic model
  - Symbolic, non-deterministic model

  of protocol security [Micciancio-Warinschi][Cortier-Warinschi]
- Symbolic model with blind signature [Kremer-Ryan]
  - Voting protocols and digital cash protocols

Contributions

1. Construct symbolic model with blind signature

Computational model

Assumptions on blind signature

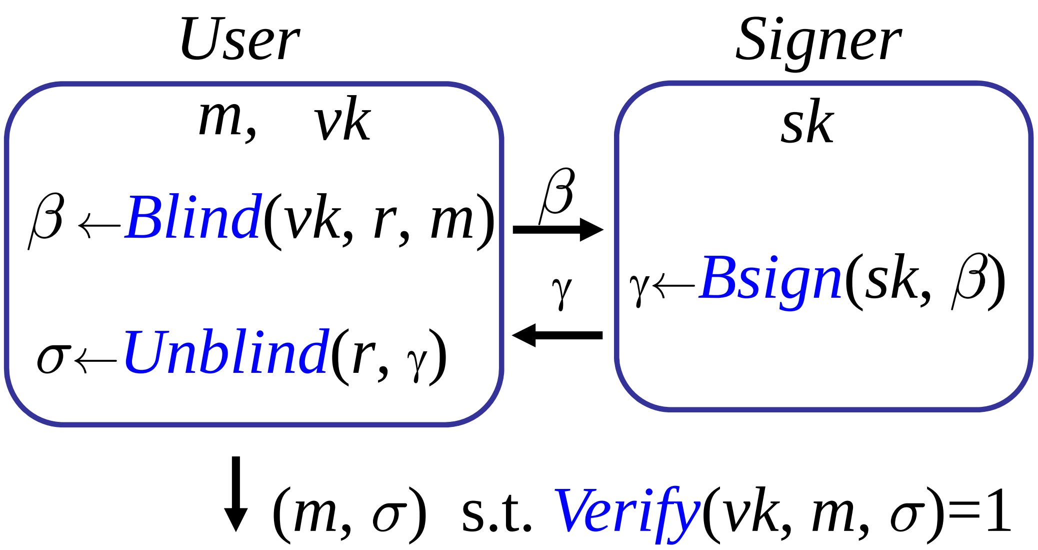
2. Prove soundness

Symbolic model

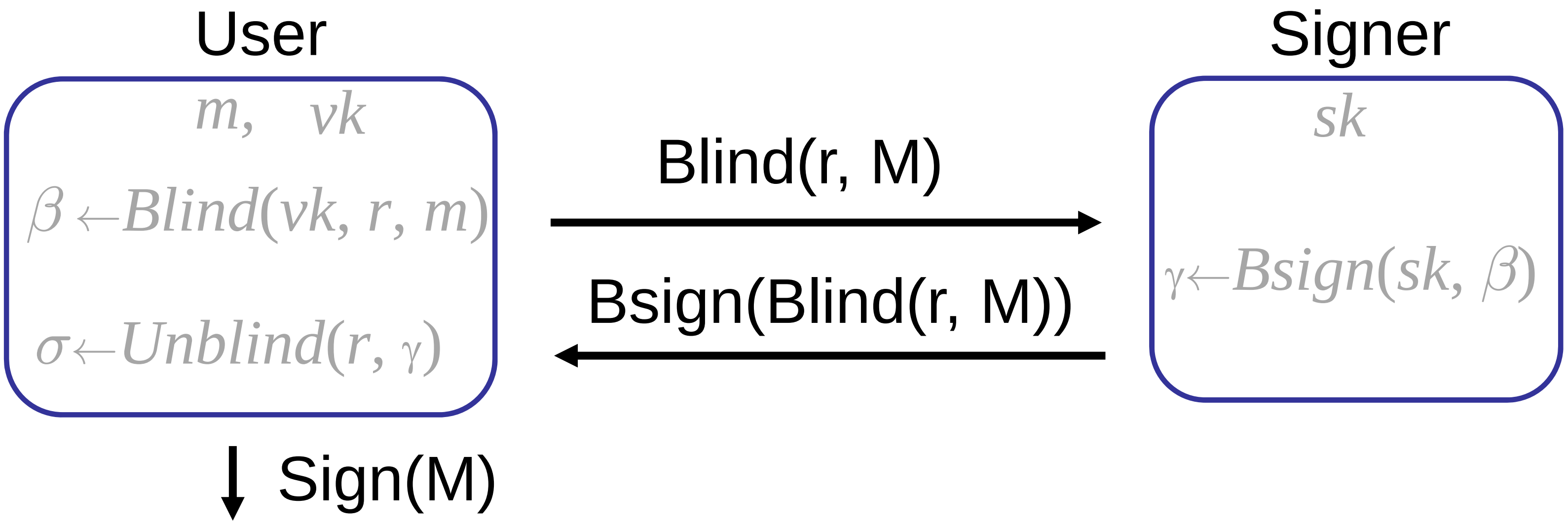
Adversary's ability

Blind Signature Scheme

- Enables user to obtain signature σ to message m keeping m secret to signer (blindness)
- In voting scheme, voter is enabled to obtain ballot σ keeping his vote m secret to administrator



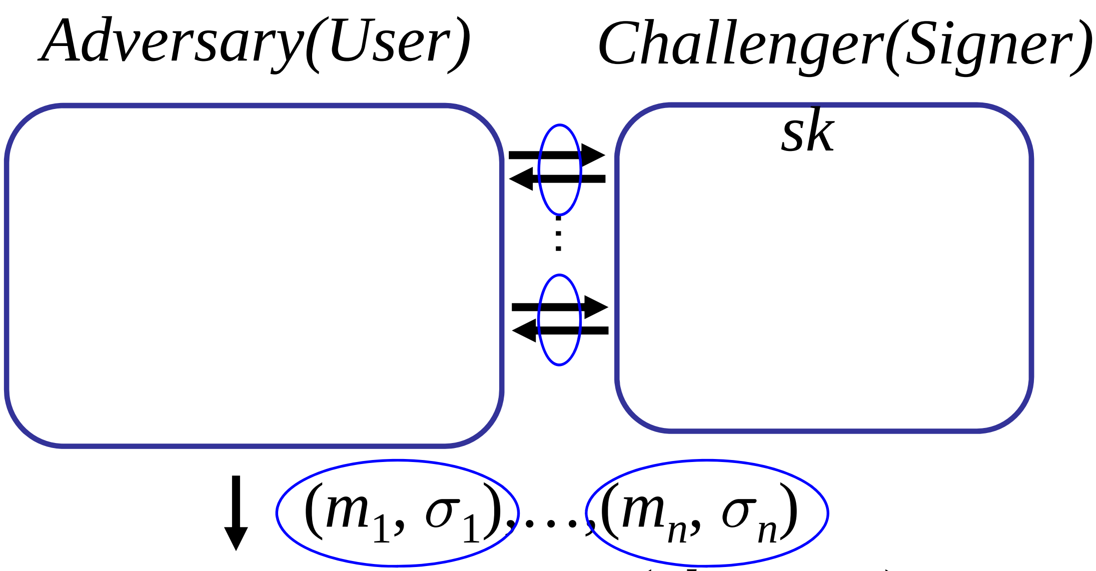
Symbolic Blind Signature



- How can we define symbolic adversary's ability reflecting assumptions in *computational model?*

Computational Assumptions

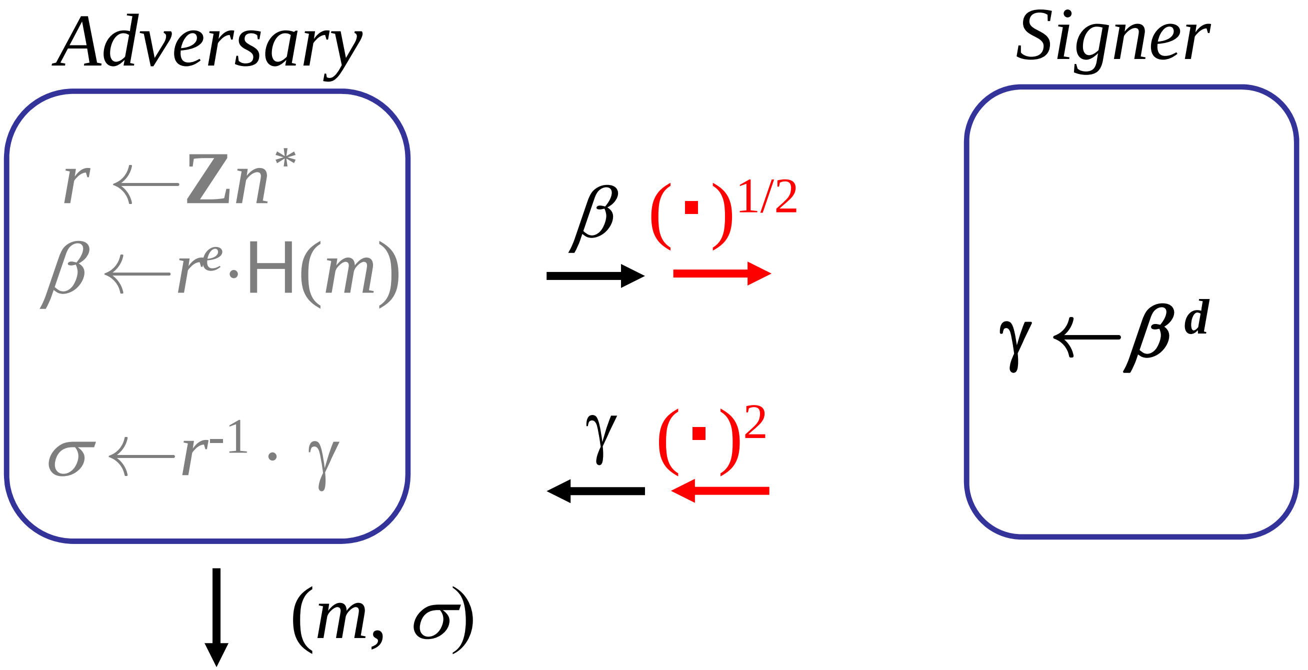
1. Blindness: Information on message m is not revealed from blinded message $\beta \leftarrow Blind(vk, r, m)$
2. Unforgeability: Number of sigs. obtained by adv $\leq$ Number of times signer signs



s.t. $m_i \neq m_j$, $V(vk, m_i, \sigma_i)=1$

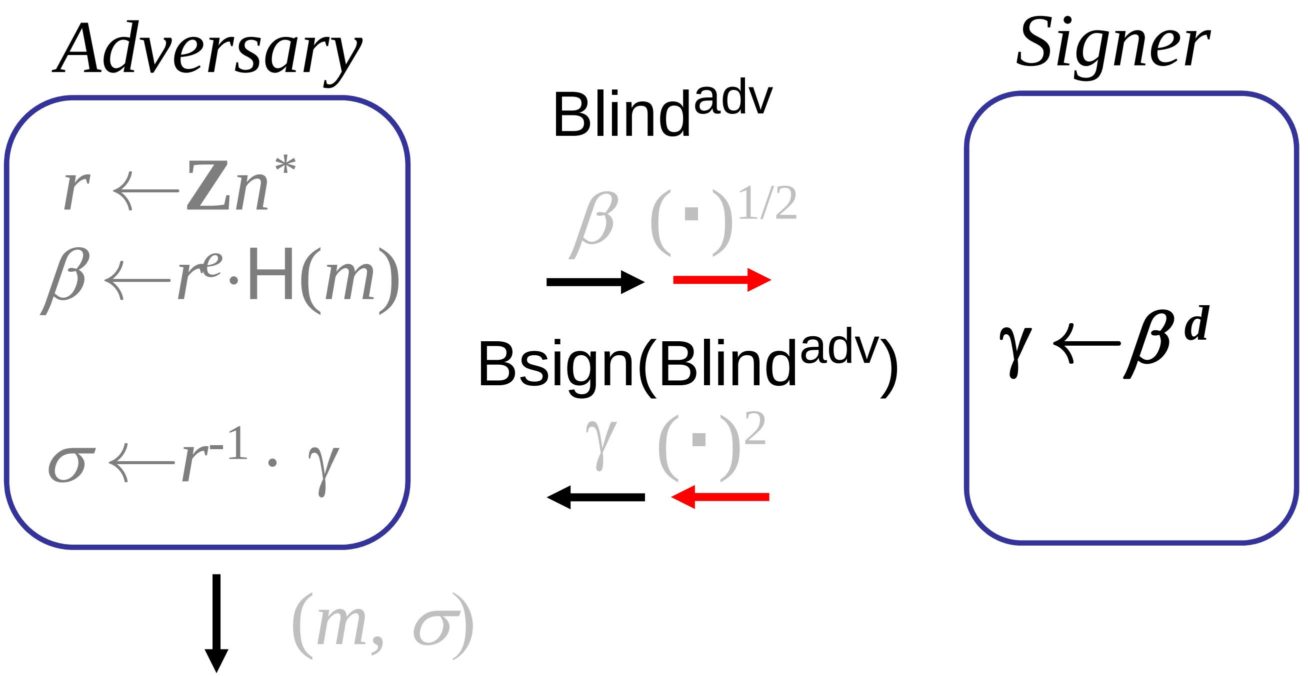
E.g. FDH-RSA blind signature

- Adversary may not follow the scheme to obtain valid signature



Adversary's blinded message

- Introduce adversary's blinded message Blind^{adv} to the symbolic model
- Also represents "irregular" blinded message



Symbolic Adversary's Ability

- From a set Γ, adv. can obtain message m
  1. Deducible by the rules below, where
  2. Num. of times he uses the unblind rules $\leq$ Num. of Bsign(Blind^{adv}) received
- No rule for Blind(r, M) because we assume honest party never disclose random r

$$\Gamma \vdash C \qquad \Gamma \vdash N^{adv} \qquad \Gamma \vdash Blind^{adv} \qquad \frac{\Gamma \vdash Bsign(Blind^{adv}) \quad \Gamma \vdash M}{\Gamma \vdash Sign^{adv}(M)}\ \text{unblind}$$

$$\frac{M \in \Gamma}{\Gamma \vdash M} \qquad \frac{\Gamma \vdash M_0 \quad \Gamma \vdash M_1}{\Gamma \vdash \{M_0, M_1\}} \qquad \frac{\Gamma \vdash \{M_0, M_1\}}{\Gamma \vdash M_i} \qquad \frac{\Gamma \vdash Sign(M)}{\Gamma \vdash M}$$

Examples

- Symbolic adversary can not deduce

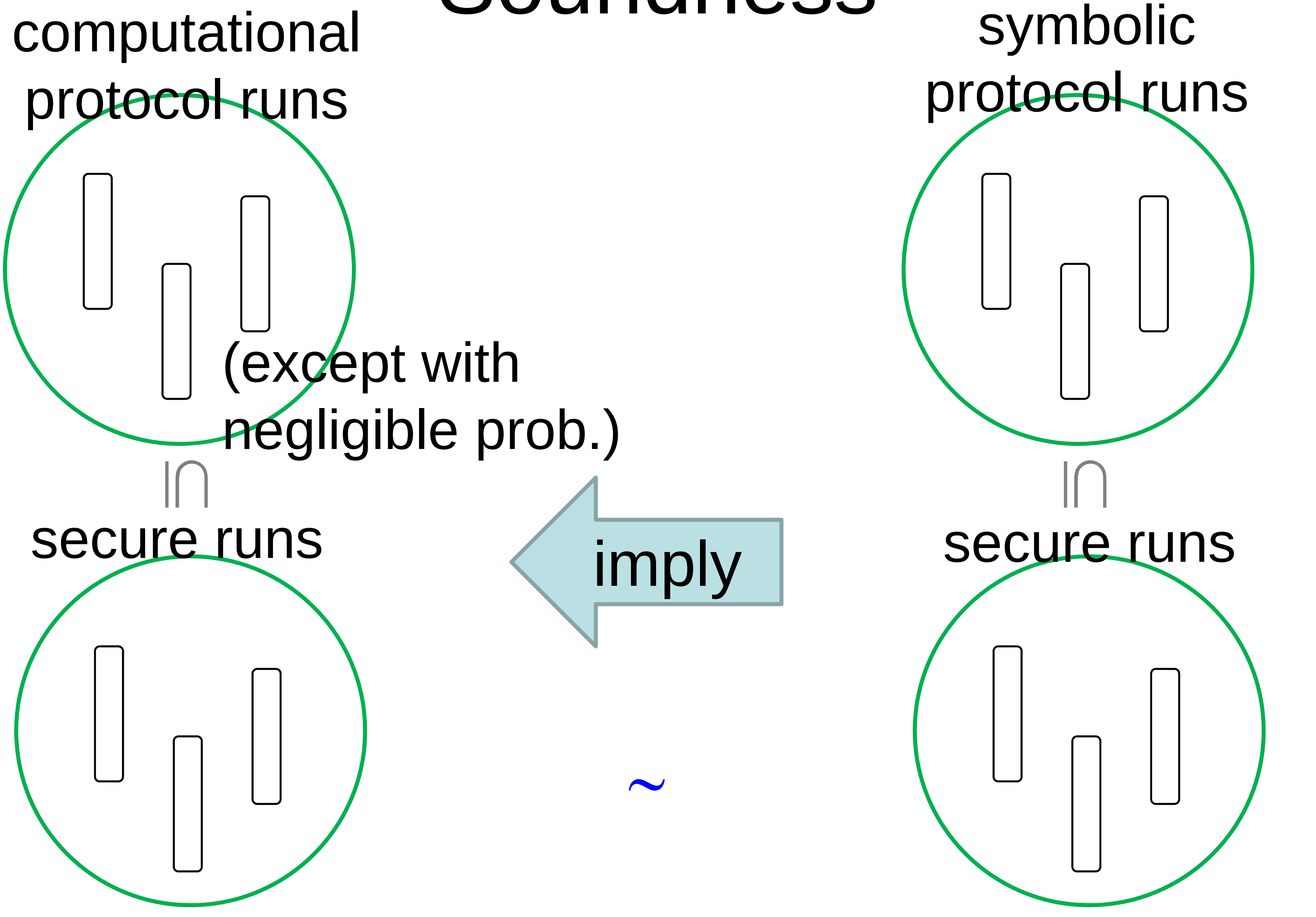
Blindness

$$\begin{cases} \mathsf{Blind}(\mathsf{r}, \mathsf{N}) \nvdash \mathsf{N} \\ \mathsf{Bsign}(\mathsf{Blind}(\mathsf{r}, \mathsf{N})) \nvdash \mathsf{N} \end{cases}$$

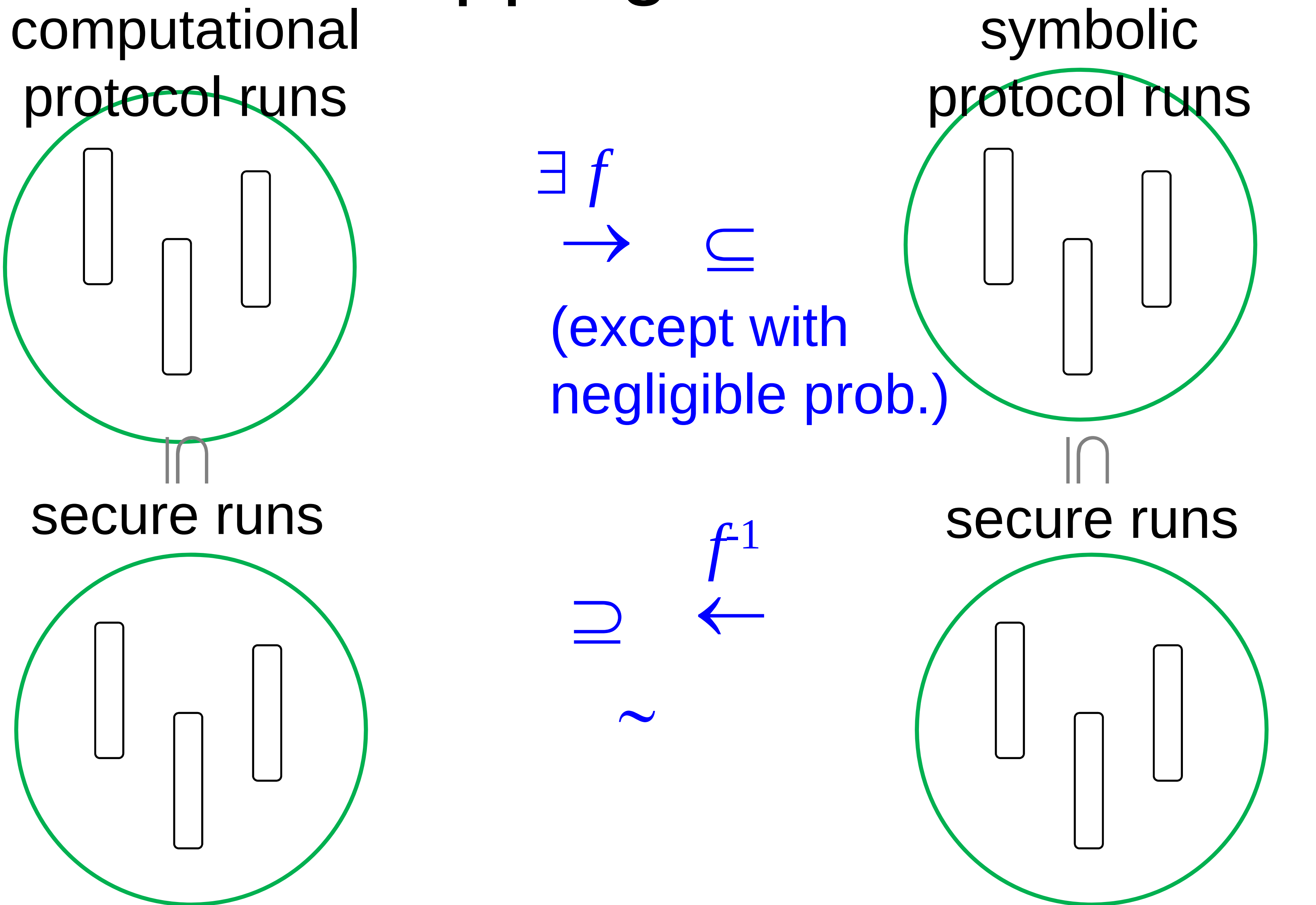
Unforgeability

$$\begin{cases} \mathsf{M} \nvdash \mathsf{Sign}(\mathsf{M}) \\ \mathsf{Bsign}(\mathsf{Blind}^{\mathsf{adv}}), \mathsf{N}, \mathsf{N}' \nvdash \{\mathsf{Sign}^{\mathsf{adv}}(\mathsf{N}), \mathsf{Sign}^{\mathsf{adv}}(\mathsf{N}')\} \end{cases}$$

Soundness


computational
protocol runs
symbolic
protocol runs
(except with
negligible prob.)
secure runs
imply
secure runs

Mapping Lemma



Outline of Proof

Similar to [Cortier-Warinschi]

I. Construct mapping from computational runs into symbolic runs:

<"blind", m> $\mapsto$ Blind(r, M), if generated by honest party

$\mapsto$ Blind^{adv}, otherwise

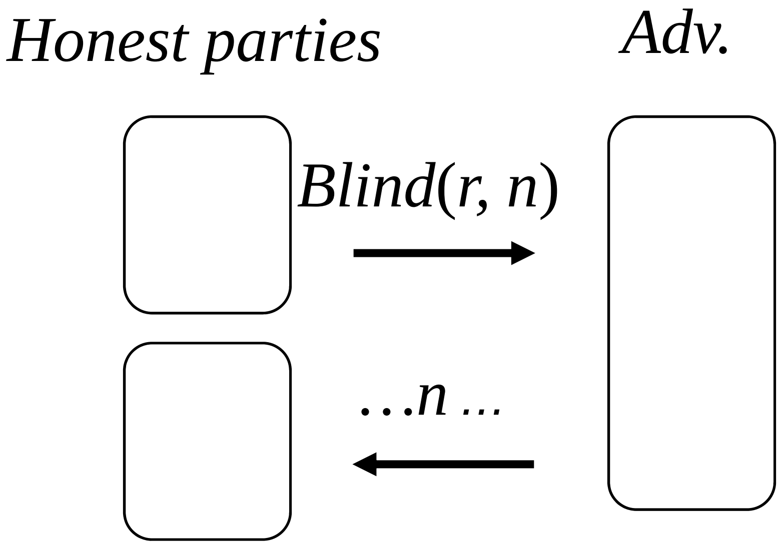
<"bsign", m> $\mapsto$ Bsign(Blind(r, M)),

if successfully unblinded and verified

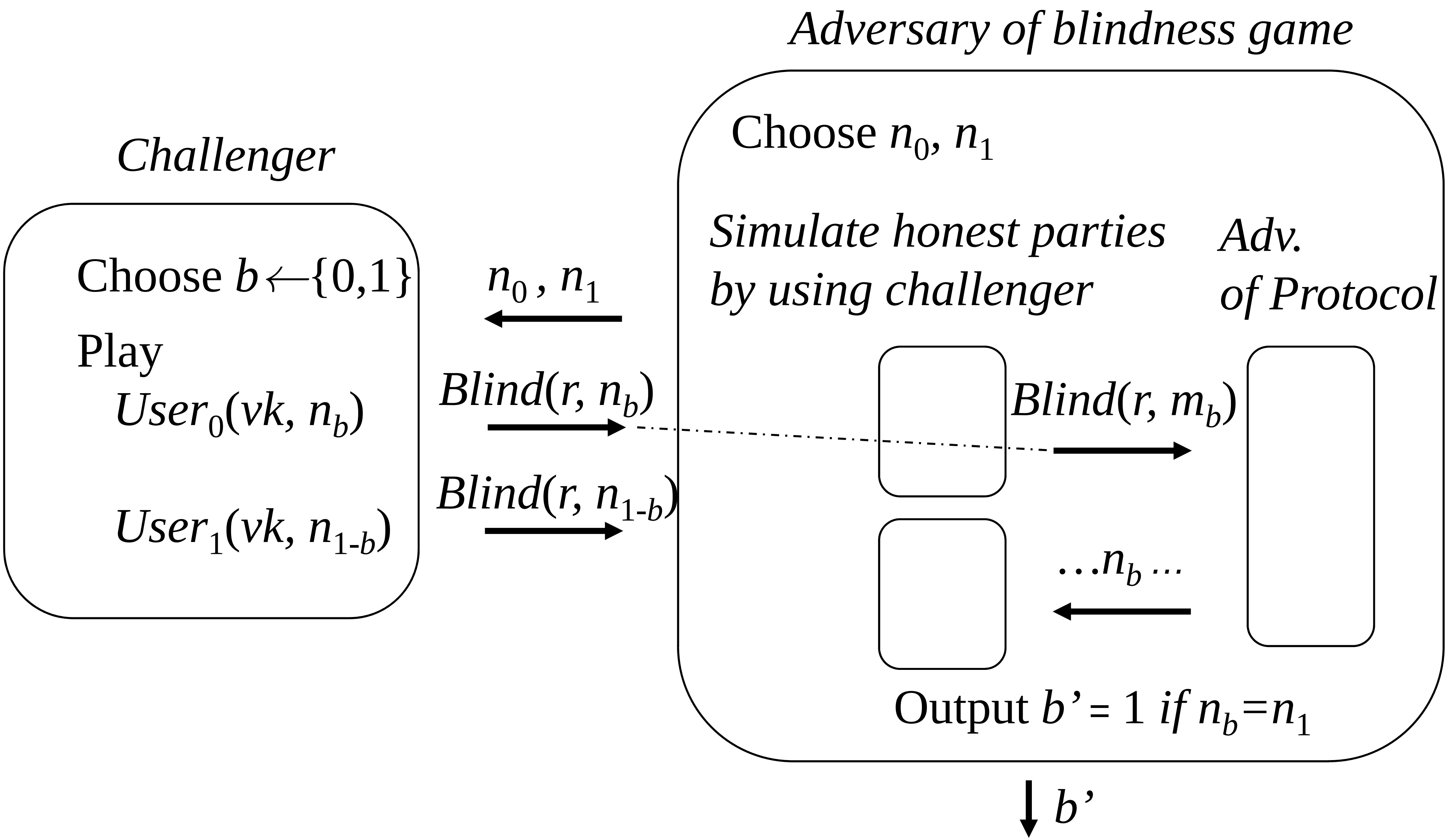
II. Show the symbolic runs satisfy the conditions

1. Message sent by adv. can be deduced by the rules
2. Num. of sign^{adv}(-) $\leq$ Num. of $\text{bsign}(\text{blind}^{adv})$

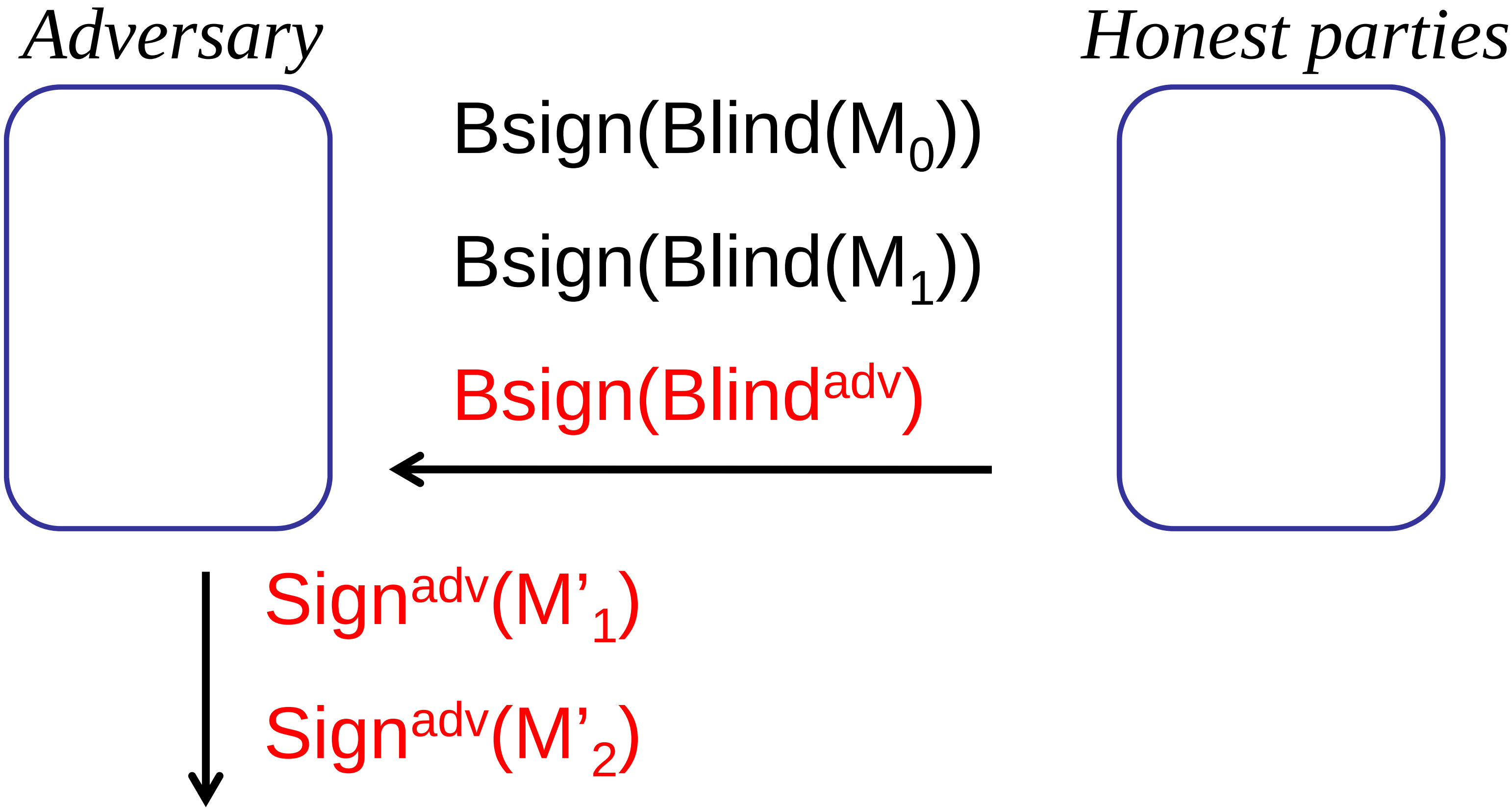
If the cond.1 is not satisfied



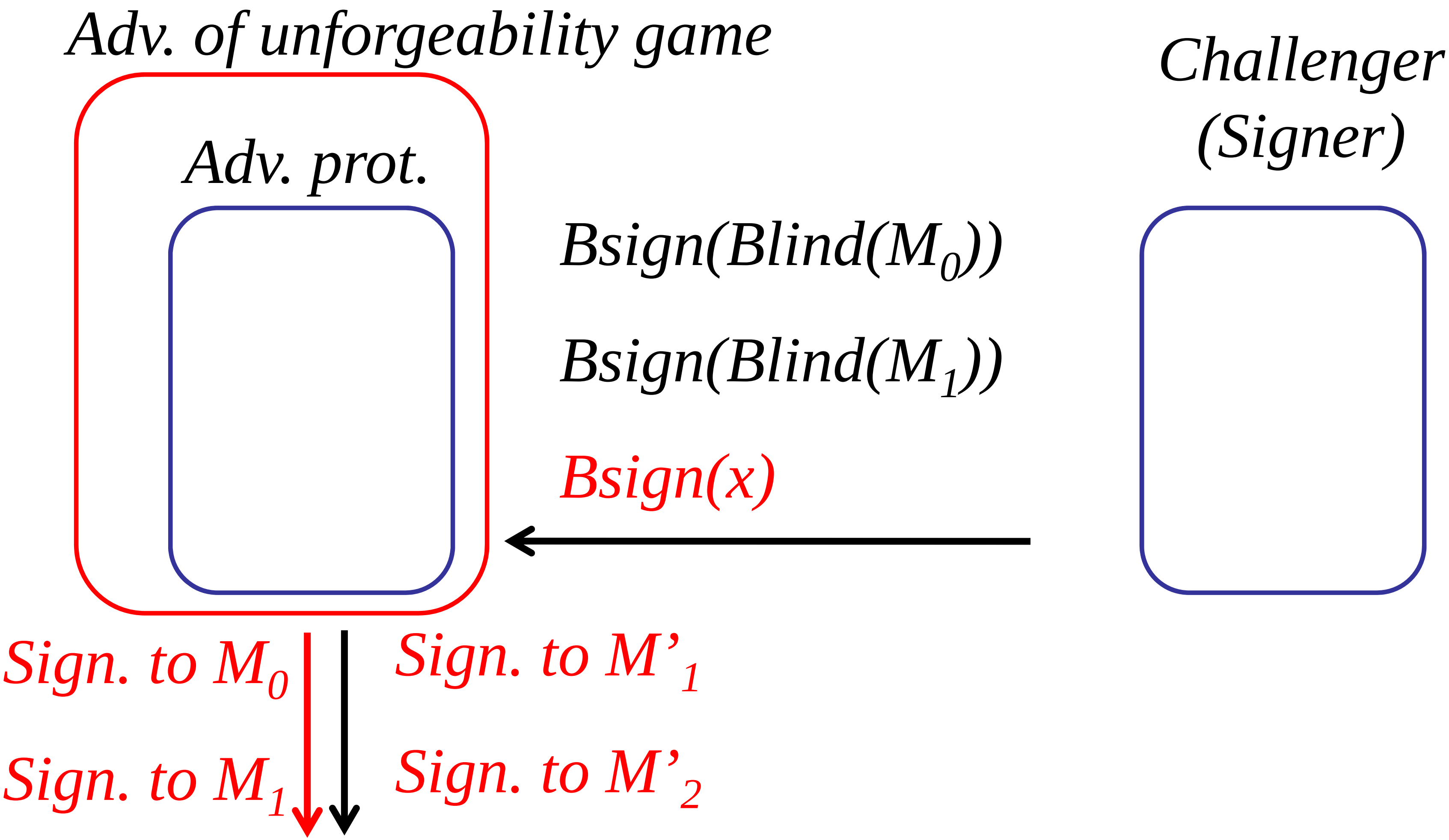
If the cond.1 is not satisfied



If the cond.2 is not satisfied

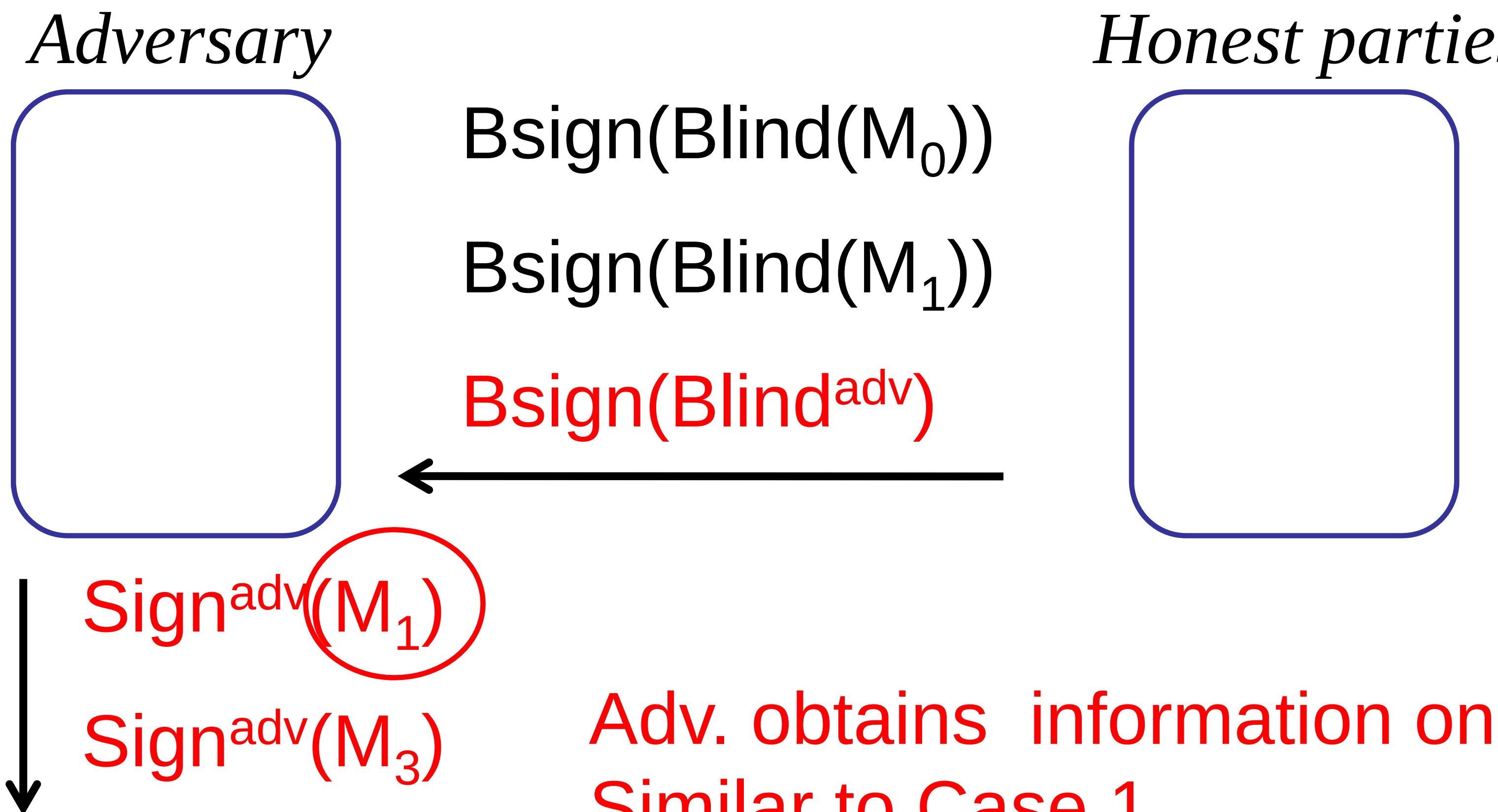


If the cond.2 is not satisfied



Wins the unforgeability game.

Case 2



Adv. obtains information on M_1 .
Similar to Case 1.

Conclusion

- We have constructed a symbolic protocol model with *blind signature*
- Shown the soundness of the model with respect to the computational model where
  - Blindness
  - Unforgeability

  of blind signature are assumed.