'No Miracles' in Security Protocol Analysis

1st Will Nalls
Philosophy Department
Carnegie Mellon University
Pittsburgh, USA
will.nalls@googlemail.com

***Abstract*—*Dynamic Epistemic Logic* (DEL) and *Epistemic Temporal Logic* (ETL), from epistemic logic, have been proposed as frameworks well-suited to the analysis of security protocols. DEL offers a succinct representation of higher-order epistemic facts, while ETL lends itself to representing a sequence of epistemic actions. It is known that DEL cannot represent all of the protocols which ETL can; in particular, DEL can only represent protocols which satisfy the *No Miracles* principle. However, a recent generalization of DEL, *Action-Epistemic Logic*, promises to overcome this limitation; we summarize this result in this short paper.**

***Index Terms*—logic, epistemic logic, security protocol analysis, security protocol modeling, model checking**

I. Context

One means of verifying security protocols is via model-checking; one models the protocol in a suitable framework, articulates the properties one wants to preserve using a language defined on the framework, and checks that these properties are satisfied in the model given. Two successful frameworks for this approach may be found in epistemic logic; they are *Dynamic Epistemic Logic* (DEL) and *Epistemic Temporal Logic* (ETL). Both frameworks were developed for the study of how knowledge may evolve over time in light of new information, particularly in multi-agent settings. DEL lends itself to the study of complex informational actions, while ETL is geared towards modeling the evolution of a system of agents after multiple executions of actions. Both may be used to model security protocols, but one might reasonably ask whether the classes of security protocols which they represent overlap.

A correspondence between DEL and ETL was proposed in [1] whereby DEL models may generate certain ETL models. To be more precise, any epistemic model and sequence of action models generates an ETL model by repeatedly performing the update procedure from DEL; however, not all ETL models may be generated this way. It is shown in [1] that only those ETL models which satisfy certain conditions may be generated in this way. These conditions articulate the expressive limitations of DEL relative to the ETL framework; one such condition is the *No Miracles* principle. The *No Miracles* principle states, roughly, that if an agent learns something after an epistemic action, then they knew, prior to the epistemic action, that they would come to learn it. As is rightly pointed out in [2], requiring this principle excludes many natural scenarios, such as the following:

> Bob is waiting for an encrypted message from Anne about whether or not p is true (in fact, p is true). He is unsure that he has the right password to decrypt the message, but cannot test it until he receives the message. If his password is correct, he will learn that p; if not, he will learn nothing (in fact, the password he has is correct).

In this scenario, Bob will learn that p, but does not know this will happen until the epistemic action is actually performed. This scenario has a natural representation in the ETL framework which cannot be generated by a DEL model. However, a recently proposed generalization of DEL overcomes this restriction.

II. Result

Action-Epistemic Logic (AEL), developed in [3], was motivated by examples of higher-order uncertainty which cannot be represented in DEL. The action model in DEL is replaced by *action-indistinguishability functions* which specify an agent's ability to distinguish epistemic actions at any state of the epistemic model. The result is that in action-epistemic models, agents may be uncertain about their own abilities to distinguish different epistemic actions, as well as those abilities of others. DEL may be recovered from AEL by simply holding the action-indistinguishability functions constant.

We show that AEL generates a wider class of ETL models than DEL can. In particular, we show that AEL may generate ETL models which do not satisfy the *No Miracles* principle. Furthermore, we show that the principle can be recovered in the generated ETL models if one places an additional requirement on AEL models – that every agent knows his or her ability to distinguish epistemic actions; this highlights precisely *which* feature of DEL prevents it from generating the wider class of ETL models. The upshot of this result is that AEL is capable of representing a wider class of security protocols than DEL. Future work will investigate the implementation of a security protocol model checker in AEL.

References

[1] J. van Benthem, J. Gerbrandy, T. Hoshi, and E. Pacuit, "Merging Frameworks for Interaction," J. Philos. Logic, vol. 38: pp. 491–526, 2009.

[2] A. Bjorndahl and W. Nalls, "Endogenizing Epistemic Actions," TARK Proceedings, 2017.

[3] F. Dechesne and Y. Wang, "To know or not to know: epistemic approaches to security protocol verification," Synthese, vol. 177: 51–76, 2010.