Automatically Binding Cryptographic Context to Messages in Network Protocols using Formal Methods

September 22, 2023
INSuRE+C Report

Enis Golaszewski
golaszewski@umbc.edu

Cyber Defense Lab, CSEE Department, UMBC

Problem: Inadequate cryptographic binding

Needham-Schroeder (1978)

FIDO UAF v1.2 (2020)

Solution: Bind automatically to eliminate protocol interference.

The Team

Enis Golaszewski, PhD student in computer science, CSEE Dept., UMBC
Jonathan Fuchs, PhD student in computer science, CSEE Dept., UMBC
Sophia Hamer, BS student in computer science and mathematics, UMBC

Dr. Alan T. Sherman, Professor of Computer Science, CSEE Dept., UMBC
Dr. Edward Zieglar, Technical Director, NSA
Ian Blumenfeld, Consultant, PhD student in computer science, CSEE Dept., UMBC

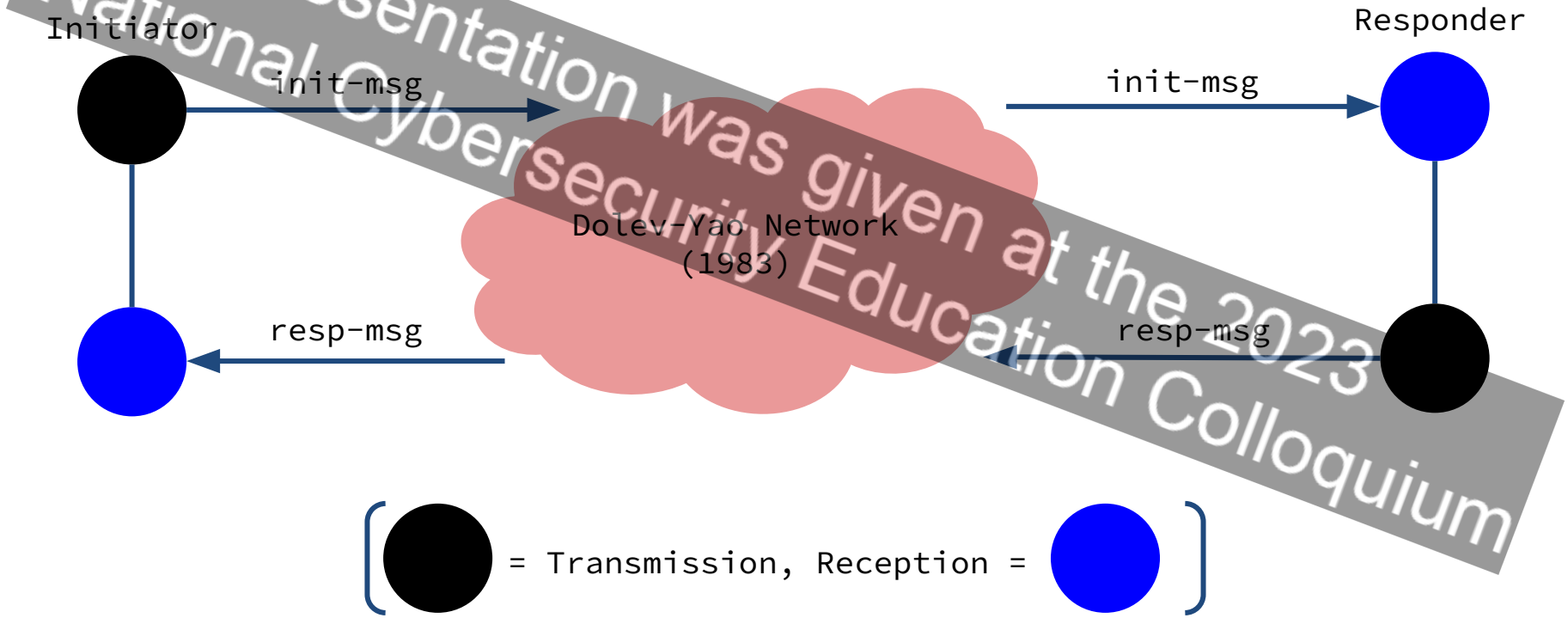
Publication Plan

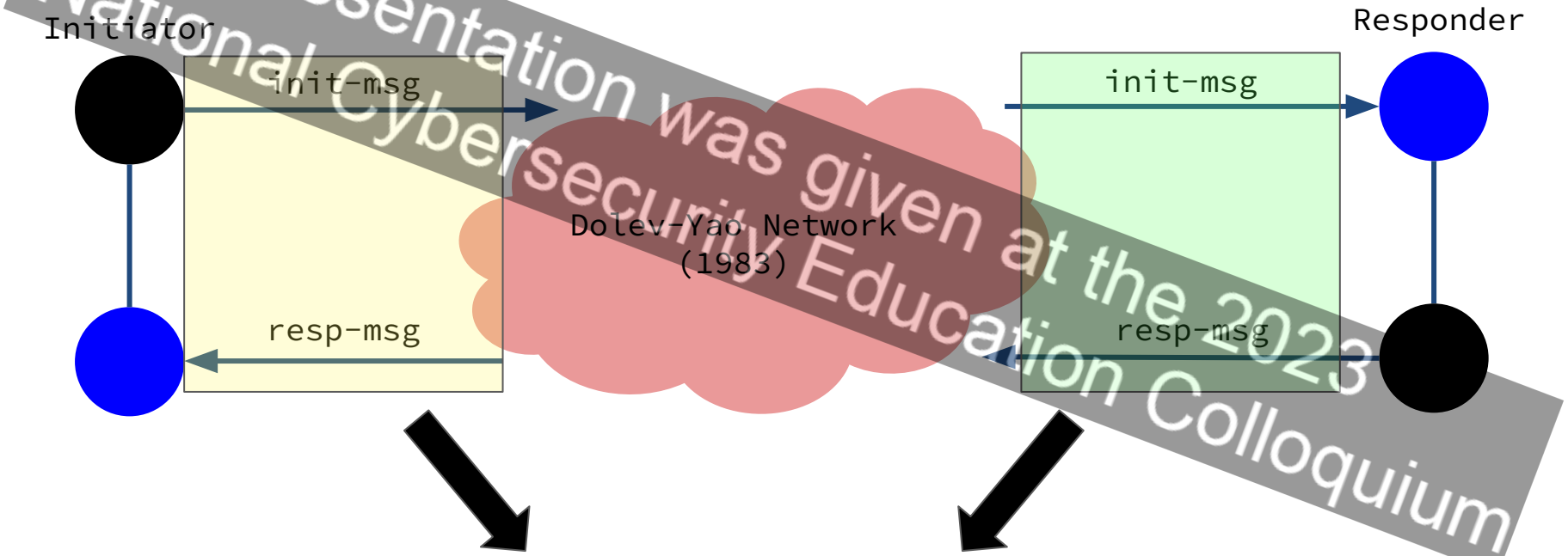
FIDO UAF Binding Conference Paper (Under Review, ACNS)
FIDO Combined Journal Paper (Submit to JSCORE)
Session Binding Proxy Paper (Submit to ACNS by October 20)
Automatic Binding (TBD)

Agenda

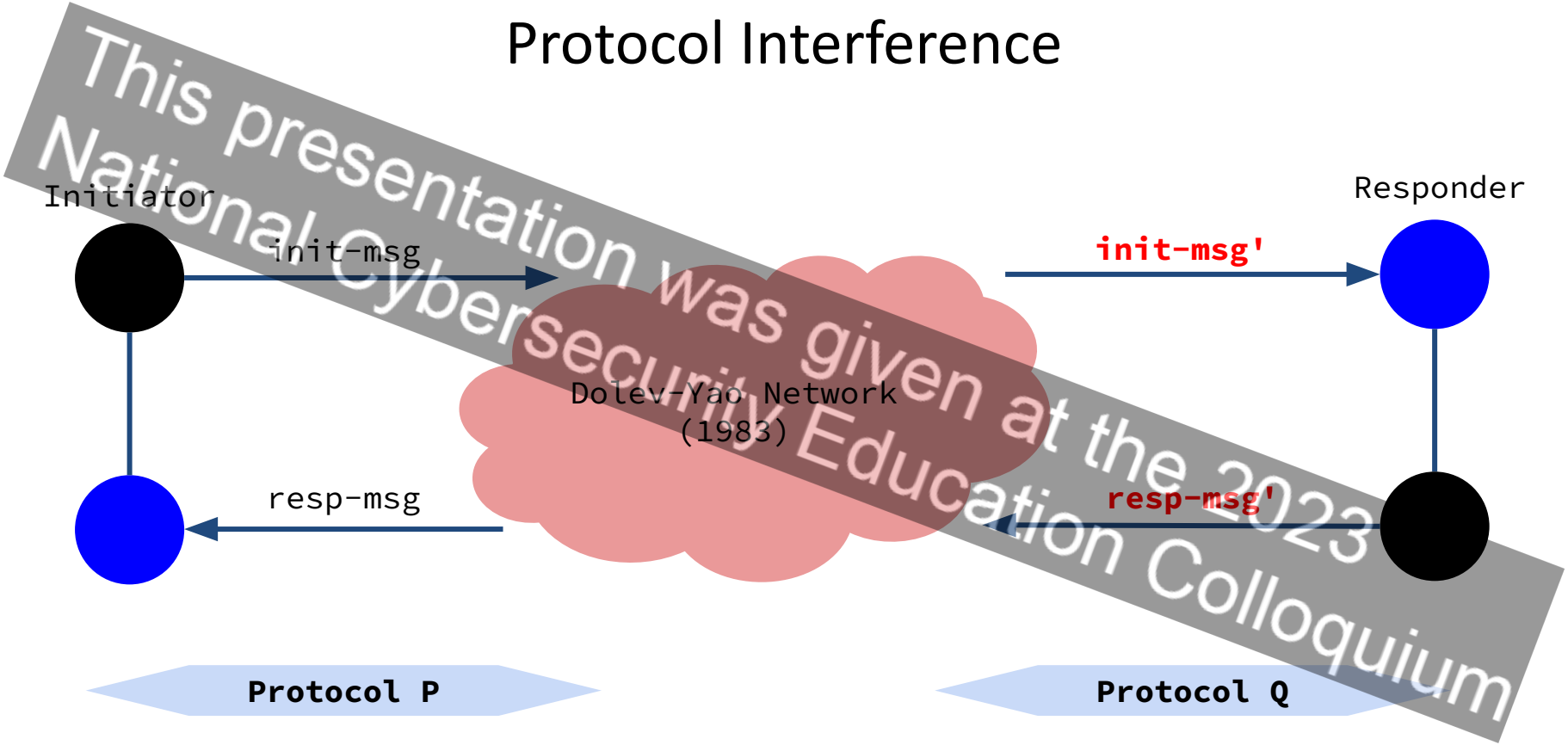
- Cryptographic Context
- Automatic Binding
- Security Goal Generation
- Costs of Contexts
- Post-Quantum Context Operations

Strand Spaces

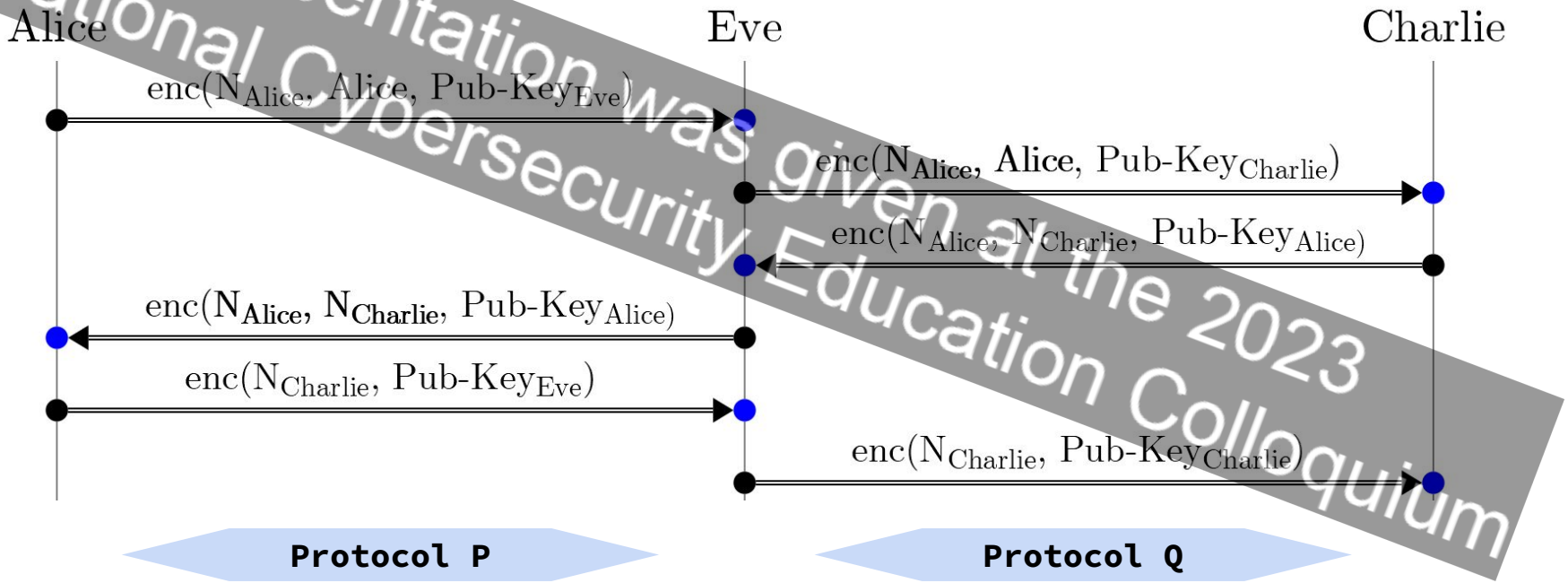




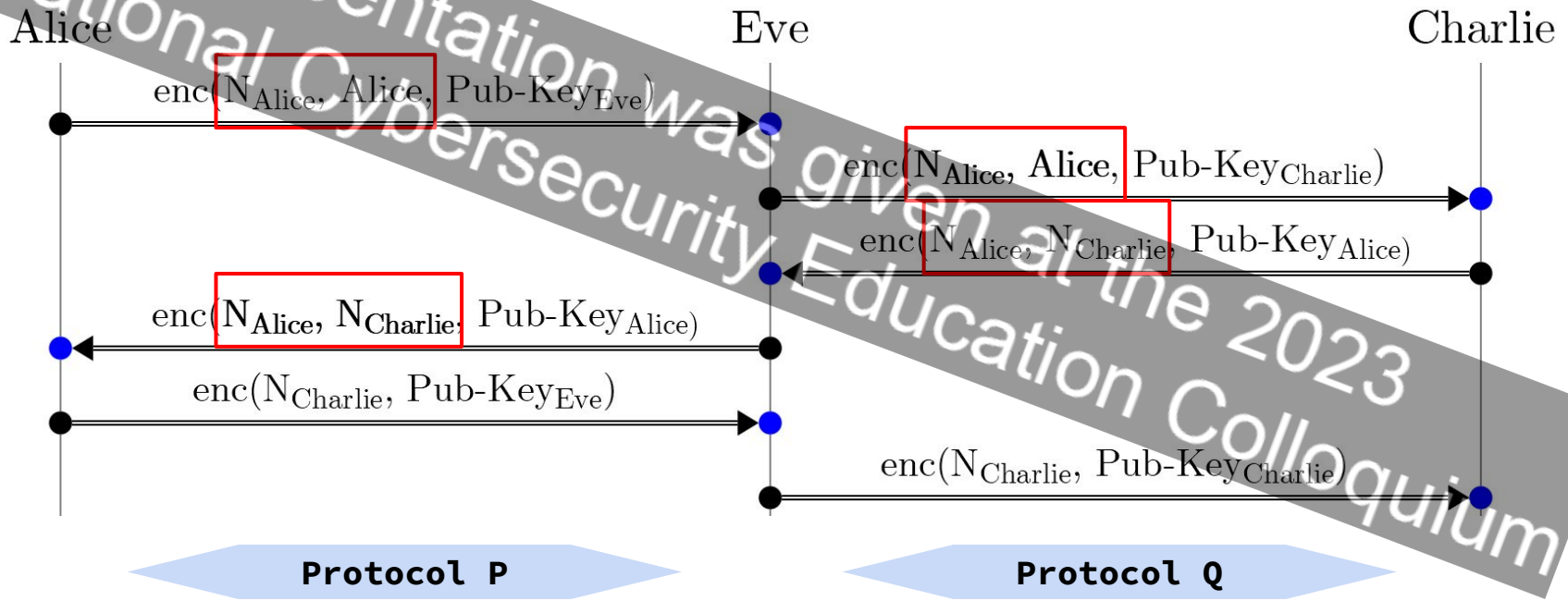
Protocol Interference



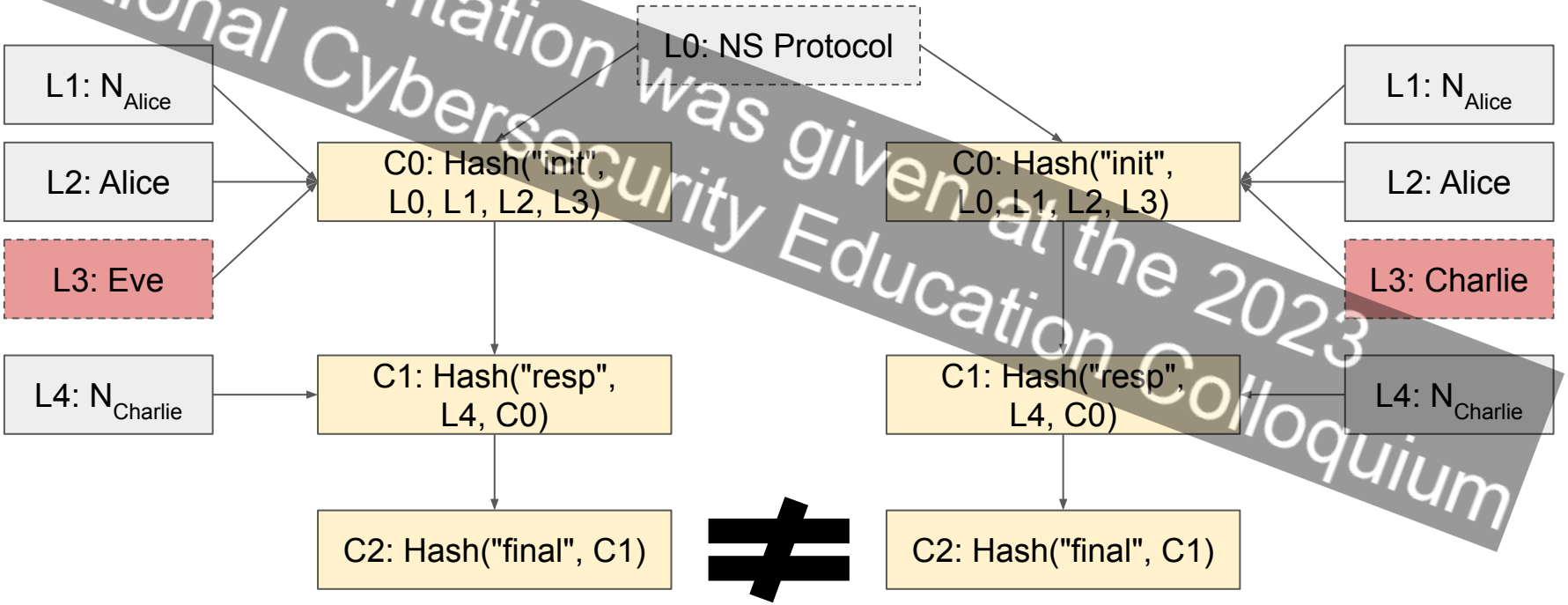
Needham-Schroeder (Lowe, 1995)



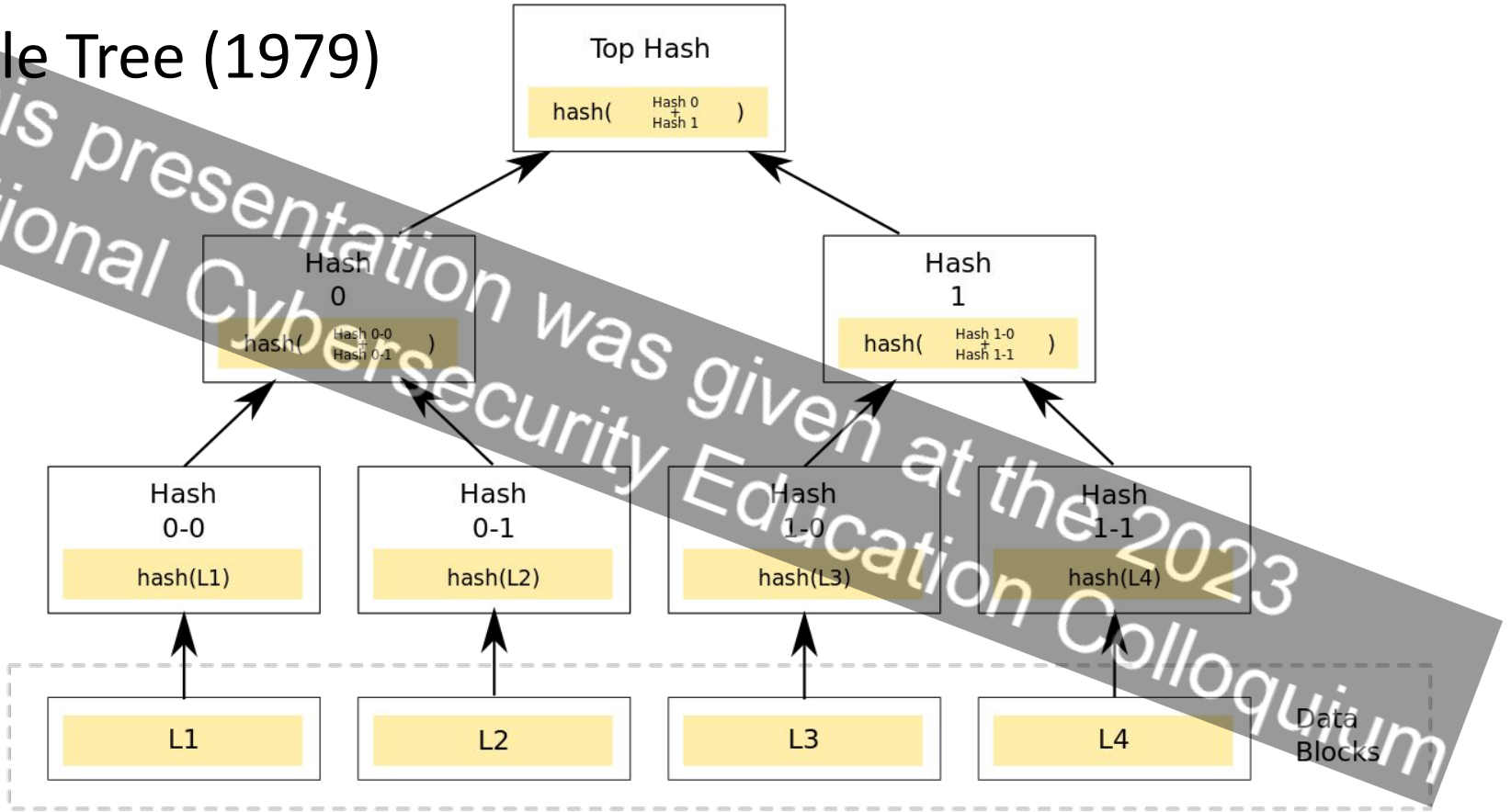
Protocol Interference



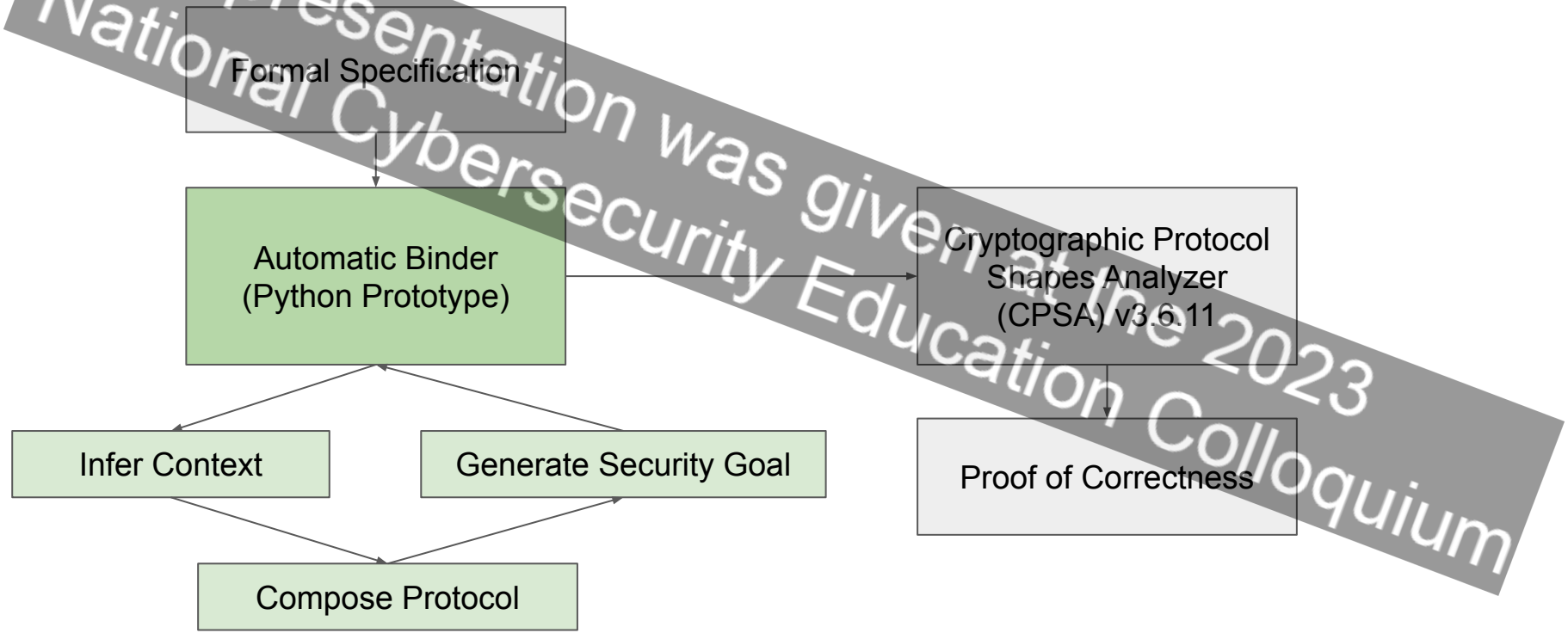
Cryptographic Context



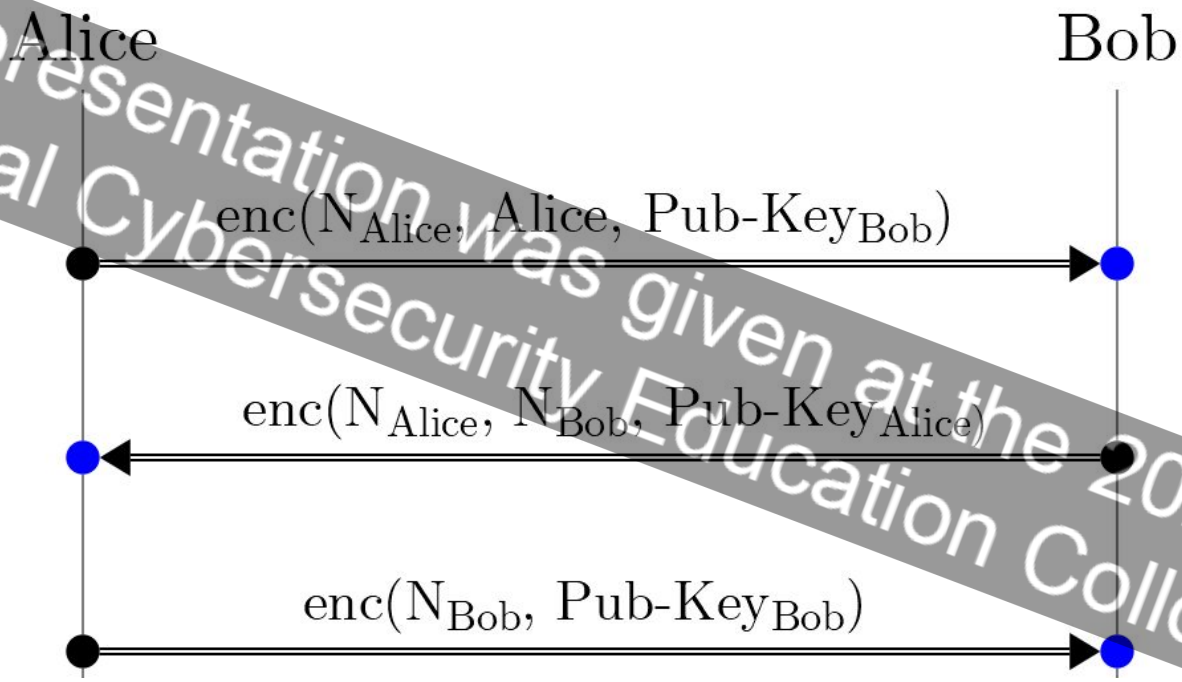
Merkle Tree (1979)



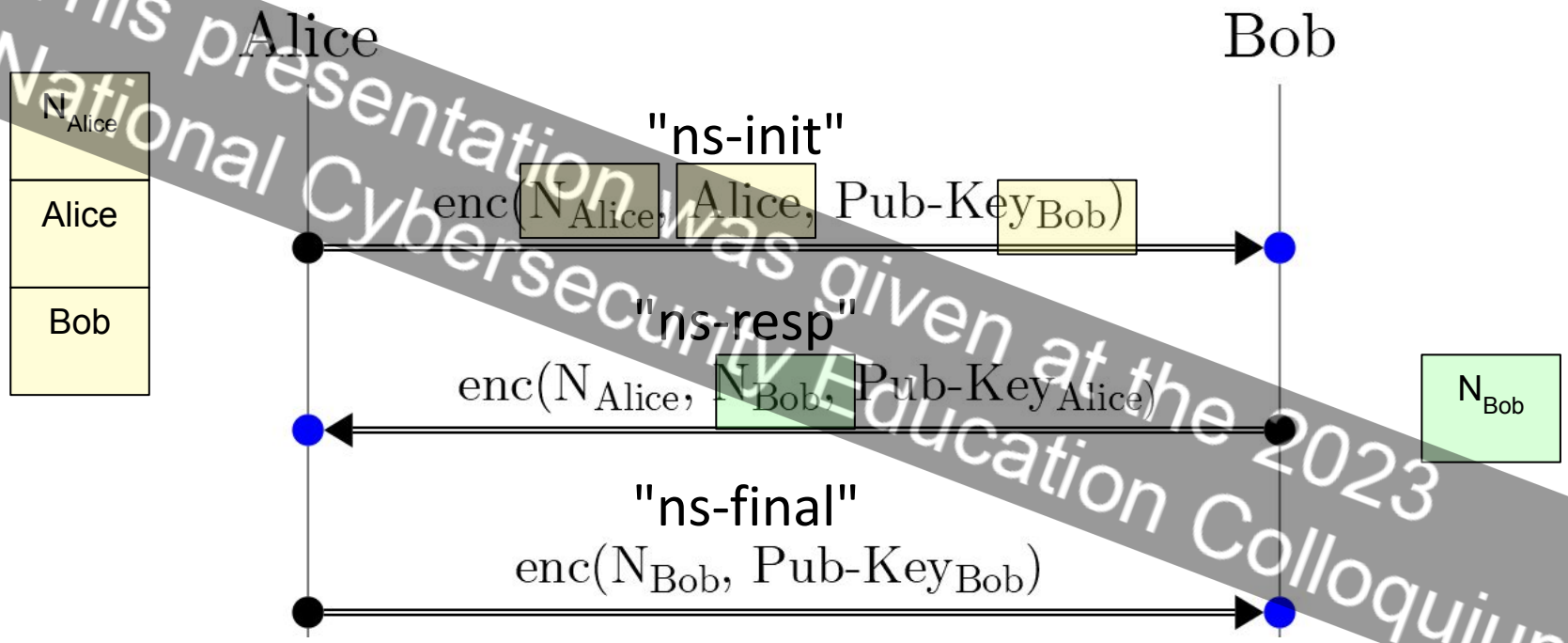
Automatic Context Binding



Needham-Schroeder



Inferring Context



Introduced Variables

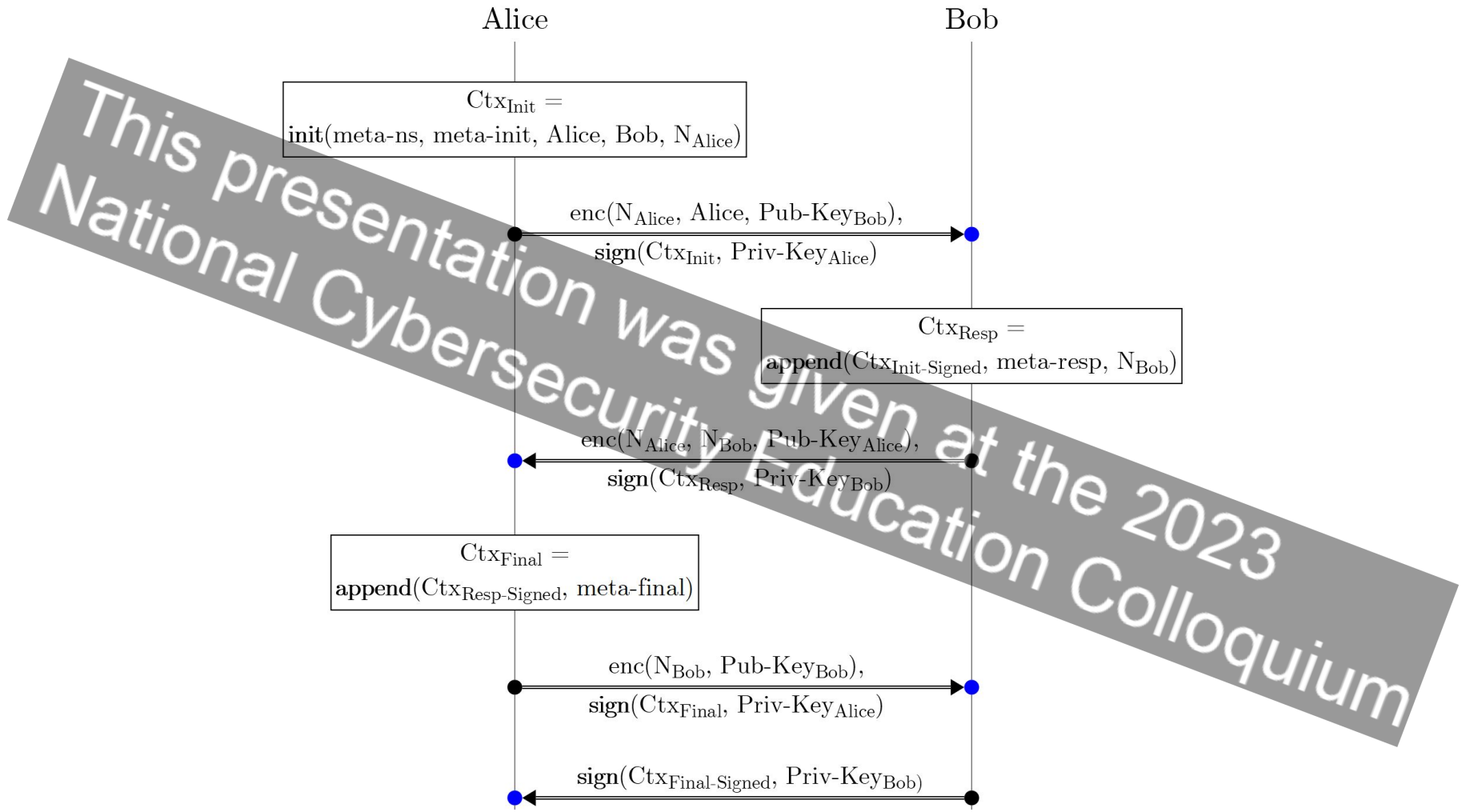
Context Operations

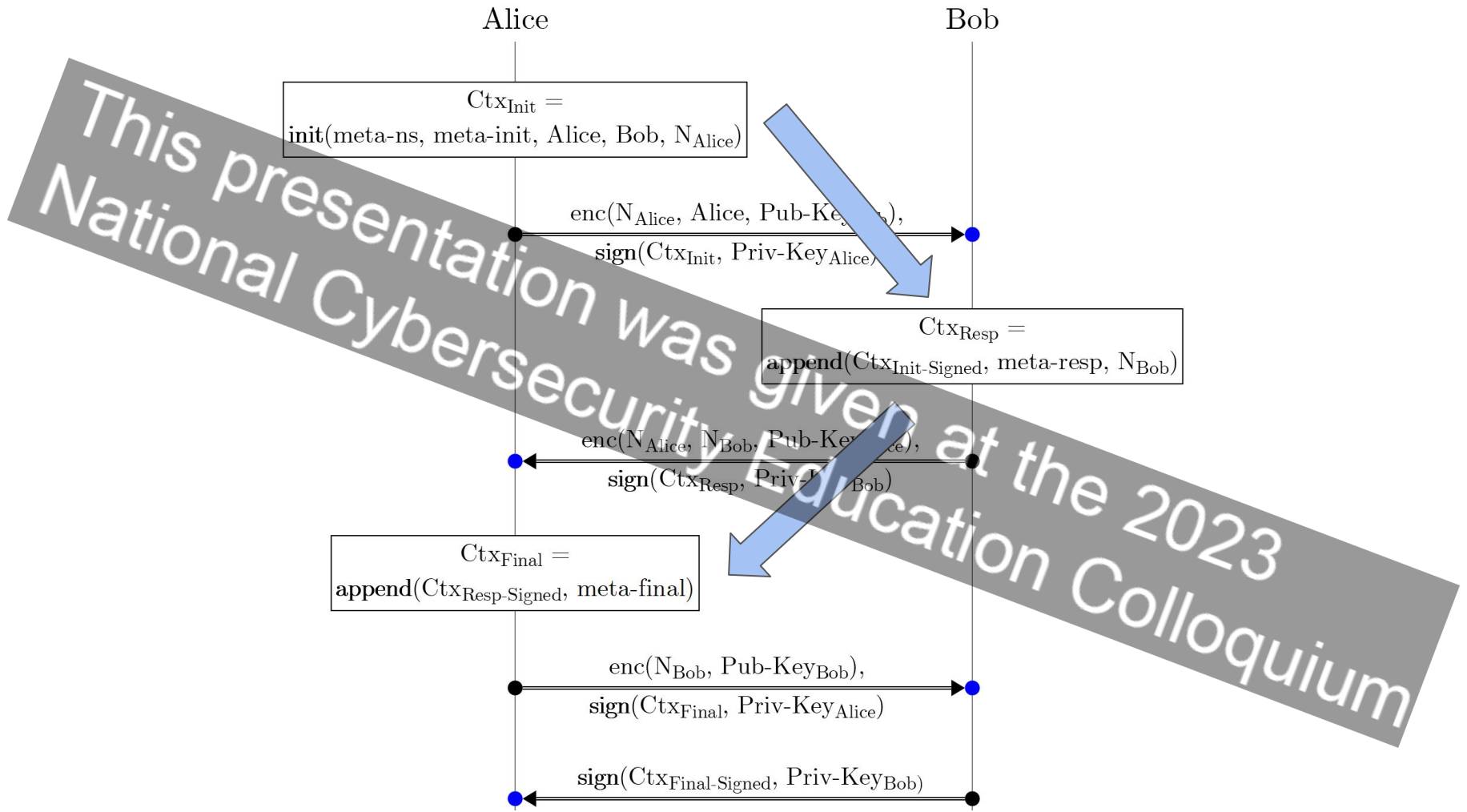
```
init(protocol, version, instantiation, vars)

append(context, msg_type, vars)

sign(context, key)

verify(context)
```





Generating Security Goals

Goal (Context Agreement, Initiator Perspective):
Let Priv-Key$_{Alice}$ and Priv-Key$_{Bob}$ be non-originating.
Let N$_{Alice}$ uniquely originate on the legitimate initiator strand.

The two properties must hold:
Property 1: For any legitimate initiator strand, there exists a responder strand that completes the protocol and agrees on the values N$_a$, N$_b$, a, and b.
Property 2: There exists no strand for which these values do not match.

Security Goal Proofs

Goal: Context Agreement	Unbound NS Protocol	*Bound NS Protocol	Unbound Blanchet's Protocol	*Bound Blanchet's Protocol
Client Perspective	✔	✔	✔	✔
Responder Perspective	✖	✔	✖	✔

* As produced by our automatic binding tool

Context Cost

Hashing
Message Overhead
Digital Signatures
Privacy

Post-Quantum Context Operations

init/append:
Hash using existing cryptographic hash functions
(>256 bit digests)

sign/verify:
XMSS**:** eXtended Merkle signature schemes

Summer 2023

Completed Automatic Binding Tool Prototype + Context-Equivalence Proofs

Fall 2023

Submit paper for publication. Investigate 3+ party context exchange, zero-knowledge verification, and generalized proof of correctness.

Future

Generate executable protocol source code with formal verification.