



UMBC

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 Ziegler, Technical Director, NSA

Ian Blumenfeld, Consultant, PhD student in computer science, CSEE Dept., UMBC

This presentation was given at the 2023 National Cybersecurity Education Colloquium

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)

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Agenda

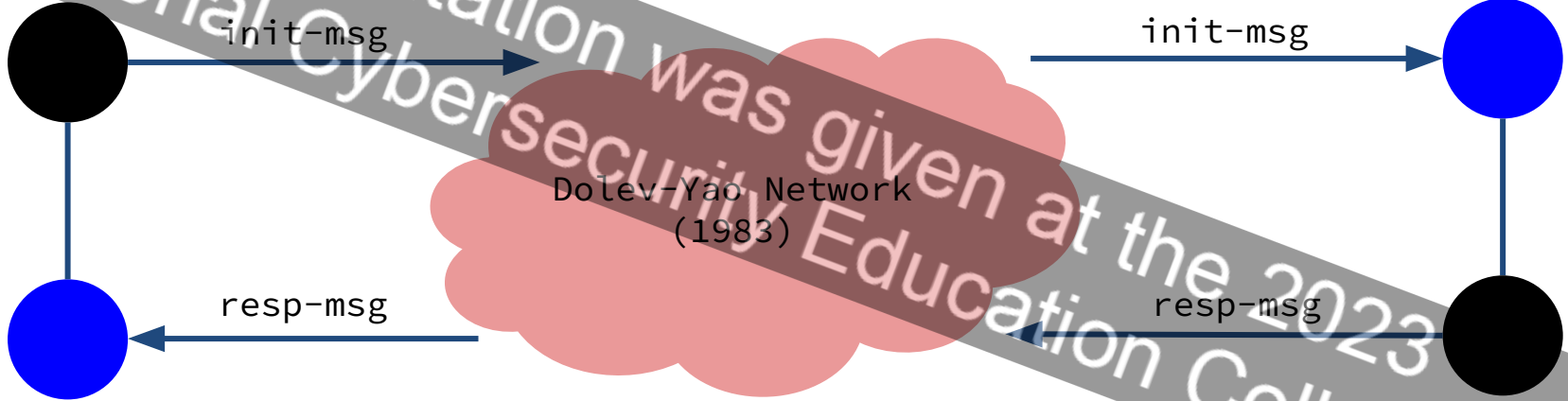
- Cryptographic Context
- Automatic Binding
- Security Goal Generation
- Costs of Contexts
- Post-Quantum Context Operations

This presentation was given at the 2023 National Cybersecurity Education Colloquium

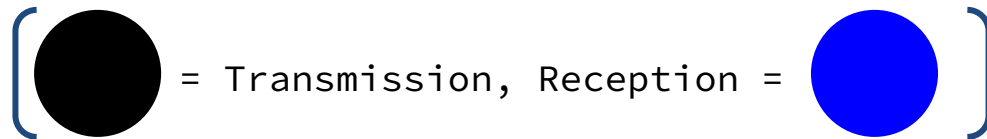
Strand Spaces

Initiator

Responder

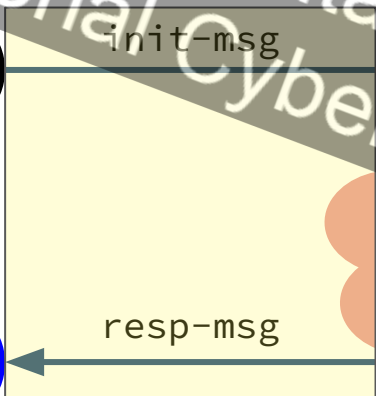
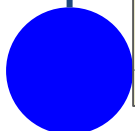


Dolev-Yao Network
(1983)



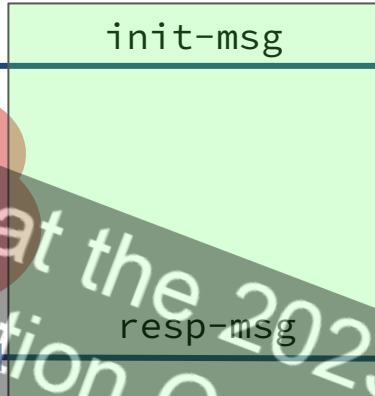
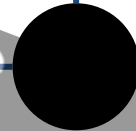
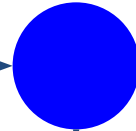
This presentation was given at the 2023 National Cyber Security Education Colloquium

Initiator



Dolev-Yao Network (1983)

Responder

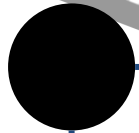


Same protocol?

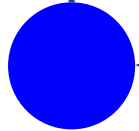
Protocol Interference

Initiator

Responder



init-msg

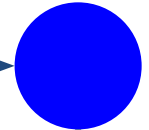


resp-msg

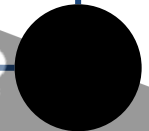
Protocol P

Dolev-Yao Network
(1983)

init-msg'



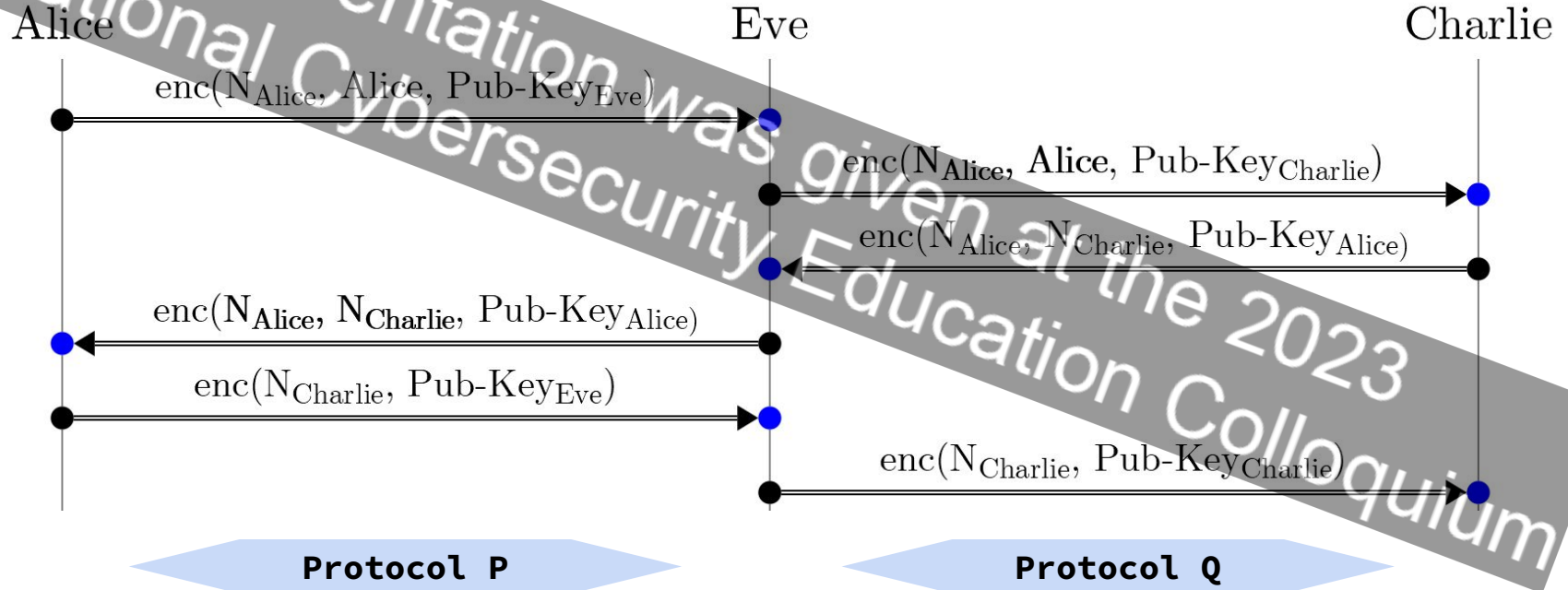
resp-msg'



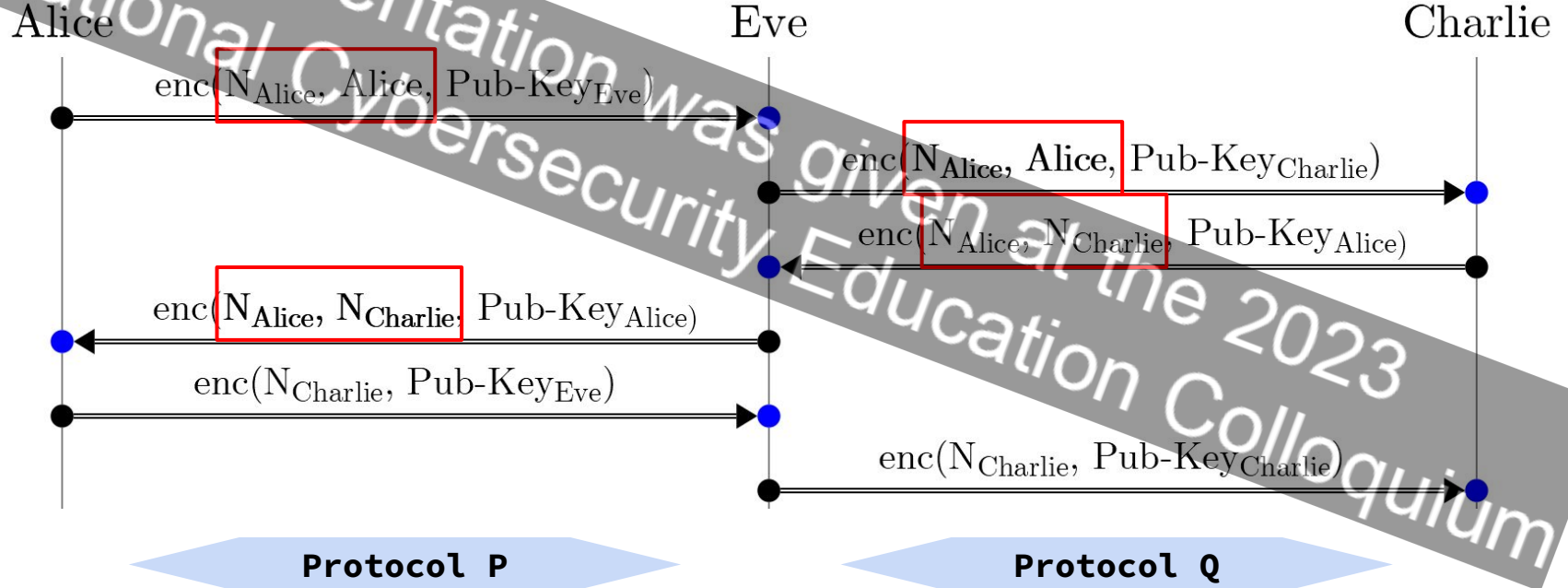
Protocol Q

This presentation was given at the 2023 National Cyber Security Education Colloquium

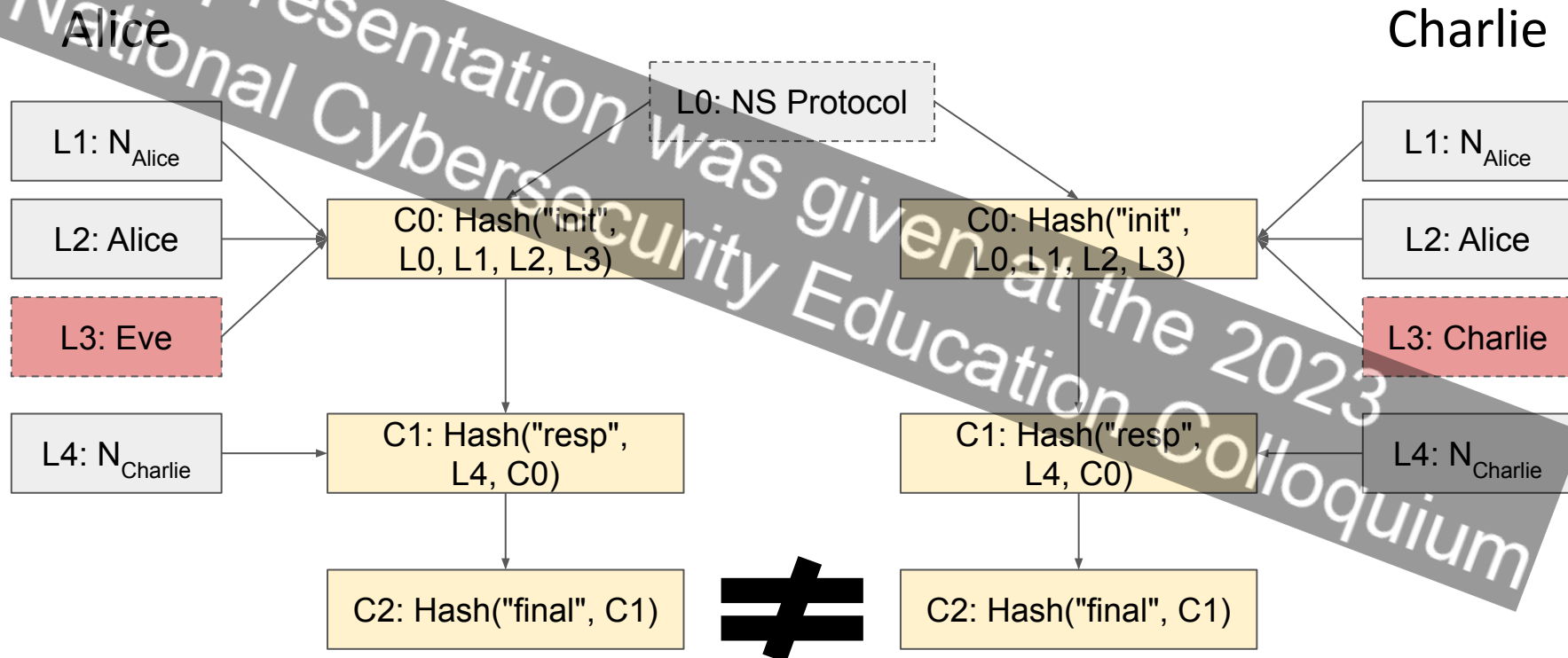
Needham-Schroeder (Lowe, 1995)



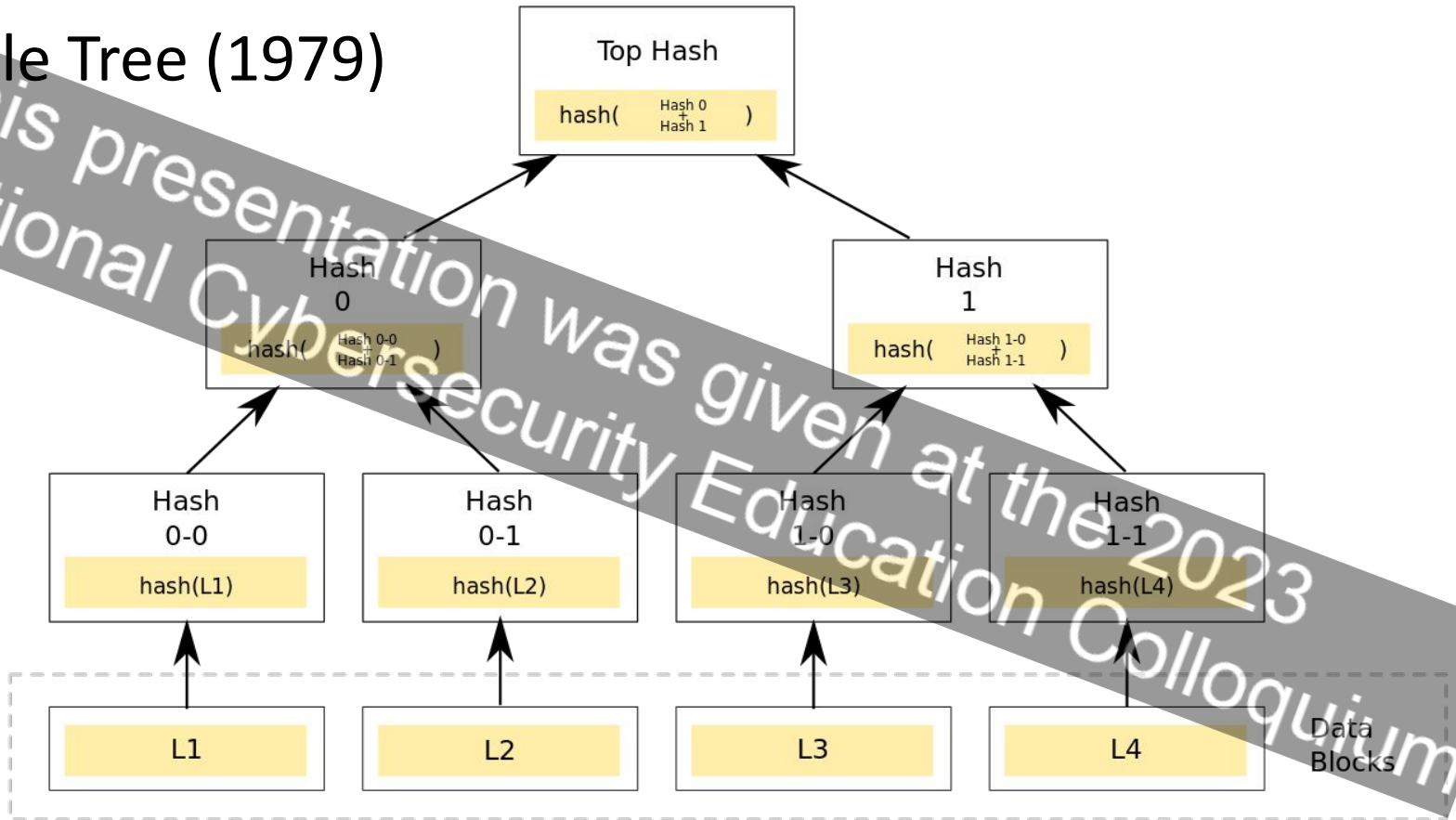
Protocol Interference



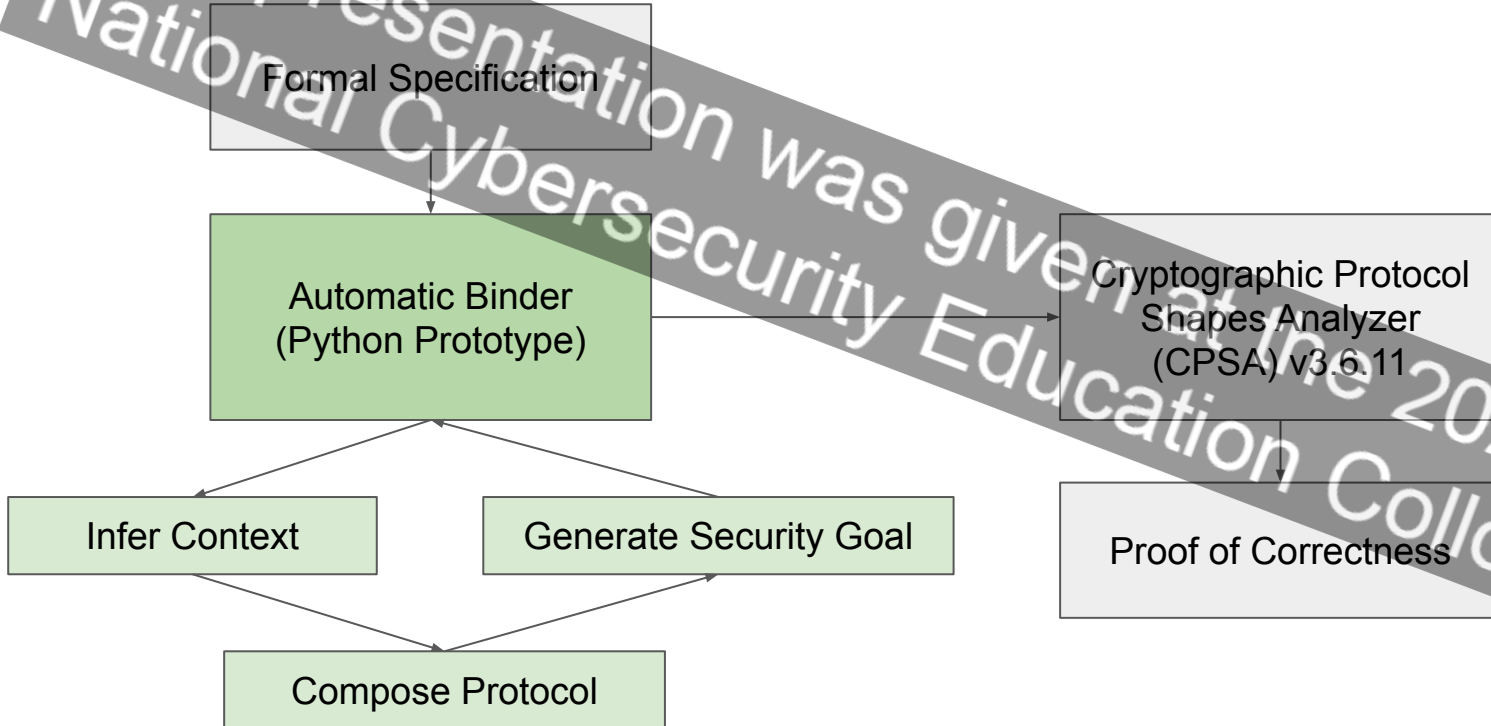
Cryptographic Context



Merkle Tree (1979)



Automatic Context Binding



This presentation was given at the 2023 National Cybersecurity Education Colloquium

Needham-Schroeder

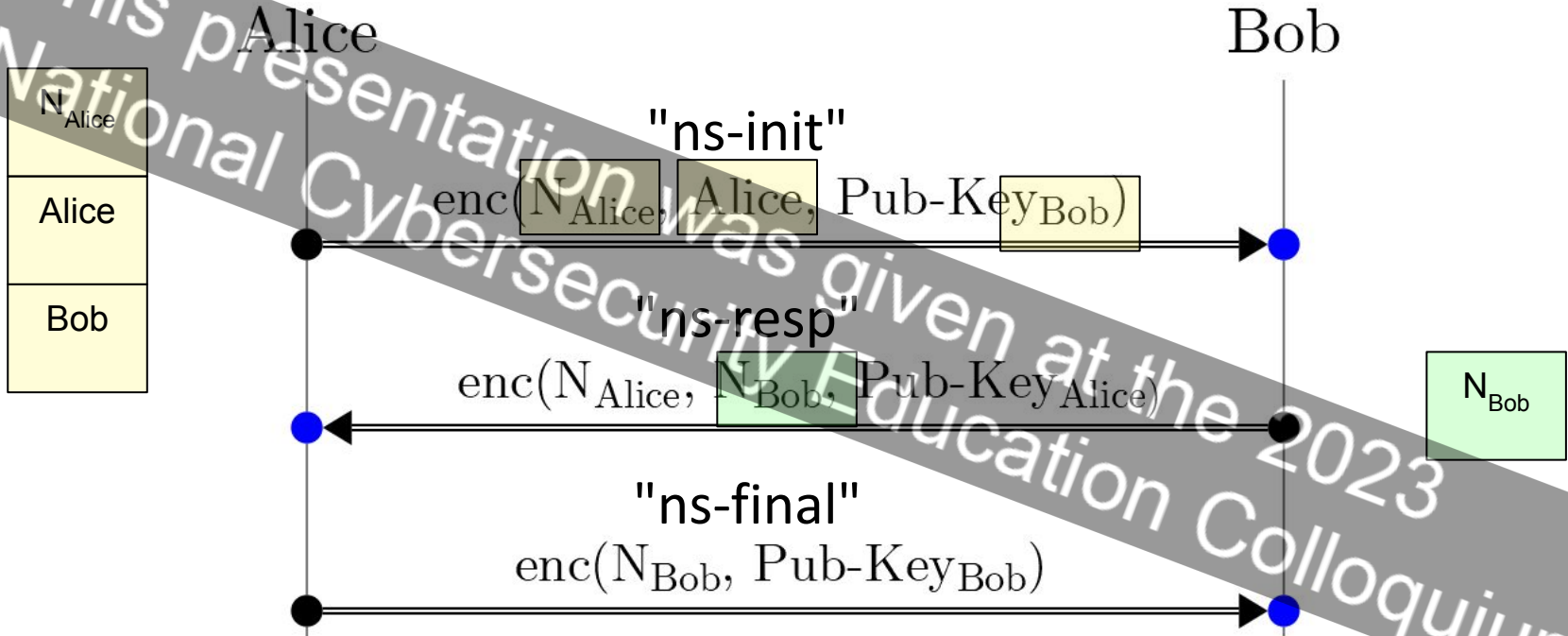
Alice

Bob



This presentation was given at the 2023 National Cybersecurity Education Colloquium

Inferring Context



Introduced Variables

Context Operations

init(protocol, version, instantiation, vars)

append(context, msg_type, vars)

sign(context, key)

verify(context)

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Alice

Bob

$Ctx_{Init} =$
 $init(meta-ns, meta-init, Alice, Bob, N_{Alice})$

$enc(N_{Alice}, Alice, Pub-Key_{Bob}),$
 $sign(Ctx_{Init}, Priv-Key_{Alice})$

$Ctx_{Resp} =$
 $append(Ctx_{Init-Signed}, meta-resp, N_{Bob})$

$enc(N_{Alice}, N_{Bob}, Pub-Key_{Alice}),$
 $sign(Ctx_{Resp}, Priv-Key_{Bob})$

$Ctx_{Final} =$
 $append(Ctx_{Resp-Signed}, meta-final)$

$enc(N_{Bob}, Pub-Key_{Bob}),$
 $sign(Ctx_{Final}, Priv-Key_{Alice})$

$sign(Ctx_{Final-Signed}, Priv-Key_{Bob})$

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Alice

Bob

$Ctx_{Init} =$
 $init(meta-ns, meta-init, Alice, Bob, N_{Alice})$

$enc(N_{Alice}, Alice, Pub-Key_{Bob}),$
 $sign(Ctx_{Init}, Priv-Key_{Alice})$

$Ctx_{Resp} =$
 $append(Ctx_{Init-Signed}, meta-resp, N_{Bob})$

$enc(N_{Alice}, N_{Bob}, Pub-Key_{Alice}),$
 $sign(Ctx_{Resp}, Priv-Key_{Bob})$

$Ctx_{Final} =$
 $append(Ctx_{Resp-Signed}, meta-final)$

$enc(N_{Bob}, Pub-Key_{Bob}),$
 $sign(Ctx_{Final}, Priv-Key_{Alice})$

$sign(Ctx_{Final-Signed}, Priv-Key_{Bob})$

This presentation was given at the 2023 National Cybersecurity Education Colloquium

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

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Context Cost

Hashing

Message Overhead

Digital Signatures

Privacy

This presentation was given at the 2023
National Cybersecurity Education Colloquium

Post-Quantum Context Operations

init/append:

Hash using existing cryptographic hash functions
(>256 bit digests)

sign/verify:

XMSS: eXtended Merkle signature schemes

This presentation was given at the 2023 National Cybersecurity Education Colloquium

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.