Hash Function Games and Two-Channel Authentication

Atefeh Mashatan and Douglas R. Stinson

University of Waterloo

December 1, 2006

Cornerstones of Secure Communication

- Entity authentication or user integrity.
- Message authentication or data integrity.
- Confidentiality.

Ad Hoc Network

- Ad hoc means "for this [purpose]."
- An Ad hoc Network is spontaneous: The connection is established for the duration of one session.
- It should be easy to quickly add new users and delete users.
- Examples: passengers in an airport, shoppers in a mall, etc.

Authentication in an Ad hoc Network

- Secret-key techniques not practical.
  - No secure channel.
- Public-key techniques too expensive.
  - No PKI.
- Identity-based systems need some structure.
  - No structure.
- What can we do in absence of a public or private key?!

Authentication in an Ad hoc Network

- Secret-key techniques not practical.
  - No secure channel.
- Public-key techniques too expensive.
  - No PKI.
- Identity-based systems need some structure.
  - No structure.
- What can we do in absence of a public or private key?!

Two-channel Authentication!

Applications

- Pairing of wireless devices, e.g. Wireless USB and Bluetooth,
- Personal Area Networks (PAN),
- A disaster case where a trusted infrastructure is compromised.

Two-channel Authentication

Two channels are accessible for communication:

- Insecure broadband channel: $\rightarrow$
  - e.g. Wireless channel
- Authenticated narrow-band channel: $\Rightarrow$
  - human aided channels: e.g. voice, data comparison, data imprinting, etc.
  - near field communication: e.g. visible light, infra red signals, laser, etc.
  - Also referred to as the manual channel.

The First Suggestion

Rivest and Shamir (1984) suggested using human voice in authentication protocols [RS84].

- Two parties want to authenticate a key.
- No TTP or secret key.
- The two parties can recognize each others voice.

Communication Model

Two small devices, Alice and Bob, wish to establish a secure key, M, in the presence of an active adversary, Eve.
Communication over the narrow-band channel is more expensive:

- Broadband Channel can be used to send long messages.
- Narrow-band channel can be used to authenticate messages.

Adversarial Capabilities

Eve has full control over the broadband channel. She can

- listen to, modify, delay or remove any message in this channel,
- initiate a new flow at any time

Eve has limited control over the narrow-band channel.

- It is possible to listen to, delay or remove any message.
- Adversary cannot modify a message or initiate a new flow.
- Adversary can replay a previous flow.
- The channel is equipped with user authenticating features, i.e., the recipient of any message can be sure about who sent it.

Message Authentication Protocols

- Alice wants to authenticate a message, $M \in \mathcal{M}$, to Bob along with her identity.
- Once the MAP is carried out, either Bob rejects or he outputs (Alice, M'), where $M' \in \mathcal{M}$.
- If there is no active adversary, then $M = M'$.

Adversarial Goals

- Eve is trying to make Bob accept a message M' along with the identity of Alice, when Alice has never sent M'.
- In case of a successful attack, Bob outputs (Alice, M'), where Alice has never sent M'.

Attack Model

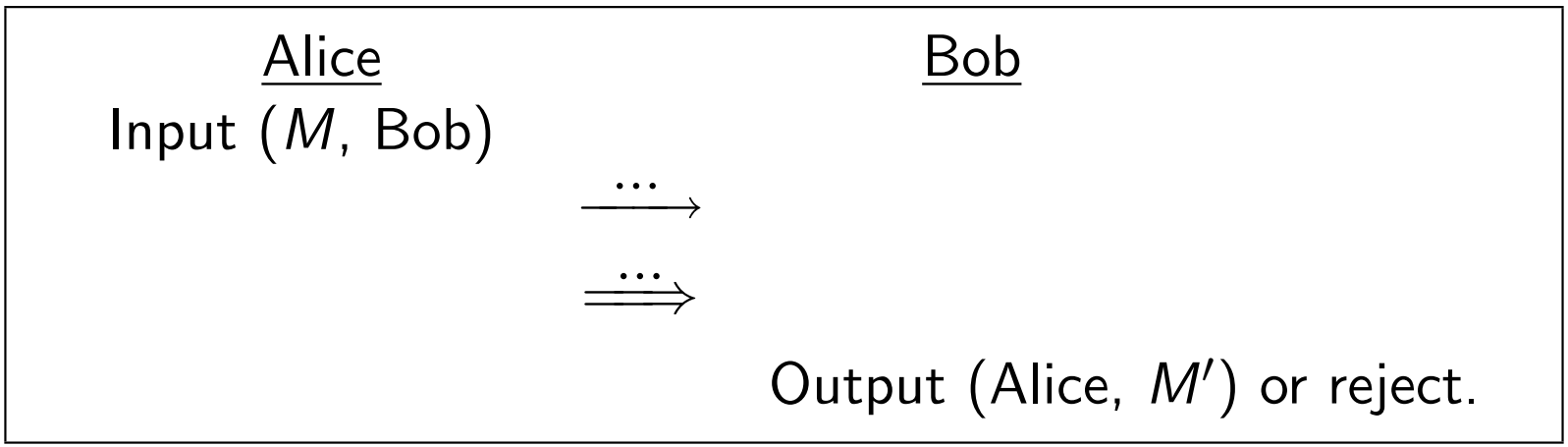
Adaptive Chosen Plaintext Attack (ACPA) model.

- Information gathering stage:
  Eve adaptively makes Alice send $M_1, M_2, \ldots, M_q$ to Bob.
- Deception stage:
  Eve tries to make Bob accept a single message M' along with the identity of Alice, where $M' \notin \{M_1, M_2, \ldots, M_q\}$.

Offline computational complexity: T.
Online complexity: q.

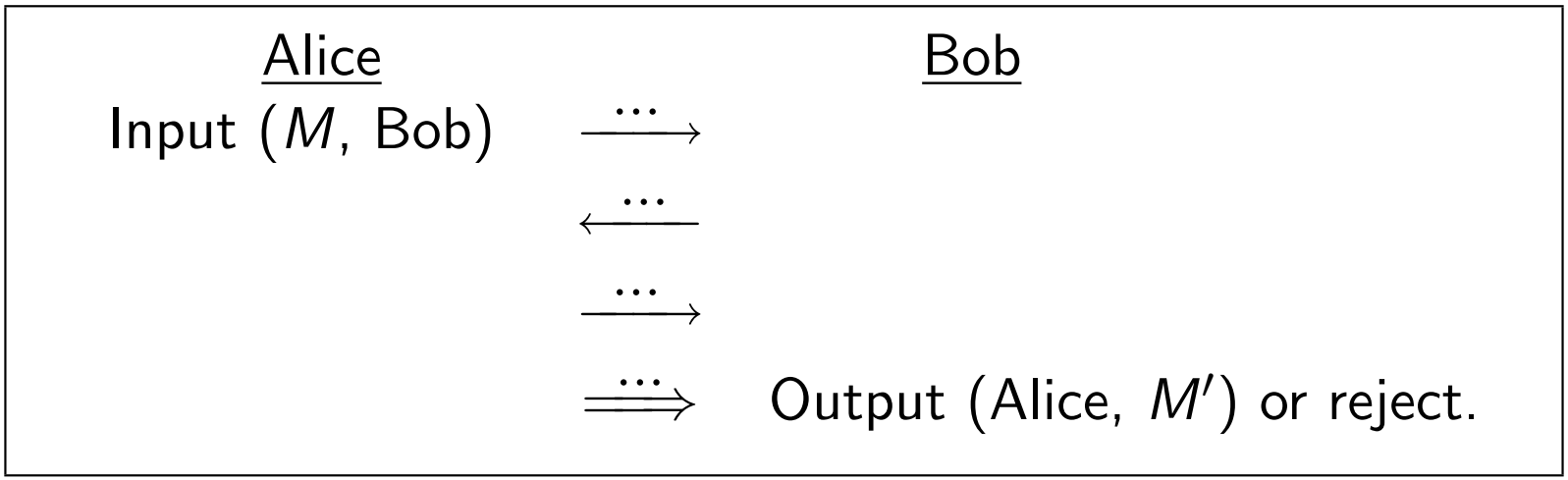
Non-interactive MAP

A typical flow structure:



Interactive MAP

A typical flow structure:



Collision Resistance

Definition

A **Collision Resistant (CR) Hash Function**, H, is a hash function where it is hard to find distinct elements x and y such that $H(x) = H(y)$.

The pair (x, y) is called a collision pair.
For security purposes, the length of the hash value is required to be more than 160 bits. Otherwise, an adversary has a good chance of finding a collision pair using an offline birthday attack.

Second-Preimage Resistance

Definition

A **Second-Preimage Resistant (SPR) Hash Function**, H, is a hash function where given a value x, it is hard to find a value y, $x \neq y$, such that $H(x) = H(y)$.

The best known generic attack is the exhaustive search. Hence, the length of the hash value is required to be at least 80 bits.

Hybrid-Collision Resistance

Definition

A **Hybrid-Collision Resistant (HCR) Hash Function**, H, is a hash function where the following **HCR Game** is hard to win. The pair $(L, M\|K)$ is a *hybrid-collision*.

Oscar		Challenger
Choose M, $\|M\| = l_1$.	$\xrightarrow{M}$	Choose $K \in_R \{0,1\}^{l_2}$.
	$\xleftarrow{K}$	
Choose L, $\|L\| = l_1 + l_2$.	$\xrightarrow{L}$	Oscar wins if $L \neq M\|K$ and $H(M\|K) = H(L)$.

If an adversary with computational complexity T wins the HCR game with probability at most ϵ, the H is a (T, ϵ)-HCR hash function.

Hardness of HCR Game

Let H be a hash function randomly chosen from $\mathcal{F}^{\mathcal{X},\mathcal{Y}}$, where $|\mathcal{Y}| = 2^k$.
Assume that, we are only permitted oracle access to H, $T = 2^t$ times.
Let ϵ be the probability of Oscar wining the HCR Game.
Let distinct random values $X_1, X_2, \ldots, X_T$ be Oscar's inputs to the random oracle.
Let the hybrid-collision be $(L, M\|K)$. We write $X_i = M_i\|K_i$, where $|K_i| = l_2$ and $|M_i| = l_1$, for all $i = 1, \ldots, T$.

Hardness of HCR Game continued

Recall $T = 2^t$. When Oscar wins, there are two cases to consider:

Case 1. $M\|K$ is a random value that happens to collide with $L = X_j$, for some j, $1 \leq j \leq T$.

Case 2. $M\|K$ is a precomputed value, X_i, that collides with $L = X_j$, for some i and j, $1 \leq i, j \leq T$ and $X_i \neq X_j$.

Probability of Case 1: $\epsilon_1 \approx 2^{t-k}$

Probability of Case 2: $\epsilon_2 \leq 2^{2t-k-l_2}$.

This yields

$$\epsilon = \epsilon_1 + \epsilon_2 \leq 2^{t-k} + 2^{2t-k-l_2}.$$

Detailed analysis: [MS06]

Balfanz-Smetters-Stewart-Wong NIMAP

Balfanz et. al [BSSW02] let H be a collision resistant hash function.

Alice		Bob
Input M	$\xrightarrow{M}$	Receive M'
Compute $h = H(M)$	$\xrightarrow{h}$	Receive h' and accept if $h' = H(M')$. Reject otherwise.

An offline birthday attack finds a collision M_1 and M_2.
Then, M_1 is given to Alice in the information gathering stage.
The adversary replays $H(M_1)$ along with M_2.
Avoid this attack by increasing the size of the message digest to 160 bits.

Gehrmann-Mitchell-Nyberg NIMAP: MANA I

Gehrmann et. al [GMN04] assume that H is an ϵ-universal hash function family and the authenticated channel provides confidentiality as well.

Alice		Bob
input M	$\xrightarrow{M}$	
Choose $K \in_R \{0,1\}^k$		
Compute $h = H_K(M)$	$\xrightarrow{h, K}$	
		Accept if $h' = H_{K'}(M')$ and reject otherwise.

Vaudenay [Vau05] proved that a "stall-free" channel is enough. MANA I is not secure in our model. The adversary records a pair $(H_K(M), K)$ from the information gathering stage and finds M' such that $H_K(M) = H_K(M')$.

Pasini-Vaudenay NIMAP

Let H be a Second-Preimage Resistant hash function [PV06].

Alice		Bob
input M		
$(c, d) \leftarrow commit(K_p, M)$	$\xrightarrow{(c\|d)}$	$M' \leftarrow open(K_p, c', d')$
Compute $h = H(c)$	$\xRightarrow{h}$	Accept if $h' = H(c')$ and reject otherwise.

Common Reference String model: random string K_p.
The adversary is reduced to a player who finds second-preimages or breaks the trapdoor of the commitments.
Offline complexity of 2^{70} and $q = 2^{10}$: authenticate 100 bits.
Security level of 2^{-20} is obtained.
Authenticity of K_p needs to be verified.
Trapdoor commitment schemes exist.

Our Contributions: General Framework

We provide a general framework for NIMAPs.
Formal model for protocols of this type: GNIMAP
Prove GNIMAP is secure under certain conditions.
The conditions can be easily checked for all proposed NIMAPs.

Our Contributions: New NIMAP

We propose a new NIMAP

- that is as efficient as the best known NIMAP, and
- benefits from a simple and easy to implement structure.

Let H be an HCR hash function.

Alice		Bob
Input $(M$, Bob$)$, $\|M\| = l_1$,		
Choose $K \in_R \{0,1\}^{l_2}$.	$\xrightarrow{M, K}$	Receive M', K'.
Compute $h = H(M \| K)$.	$\xrightarrow{h}$	Receive h', accept if $h' = H(M' \| K')$, reject otherwise.

The *Split* and *Reconstruct* Functions

Randomized algorithm $split : \mathcal{M} \rightarrow \mathcal{M}_1 \times \mathcal{M}_2$: takes any message M as input and maps it into a pair (m_1, m_2), where m_1 is shorter than m_2.
Deterministic function $reconstruct : \mathcal{M}_1 \times \mathcal{M}_2 \rightarrow \mathcal{M} \cup \{\perp\}$: takes a pair (m_1, m_2) and maps it into a message $M \in \mathcal{M}$ or a "reject" sign $\perp$.

- Correctness property: Any message can be uniquely recovered. That is, for any $M \in \mathcal{M}$, $reconstruct(split(M)) = M$.
- Binding property: It is computationally infeasible to find a message M such that given (m_1, m_2), where $split(M) = (m_1, m_2)$, one can efficiently find an $m_2' \in \mathcal{M}_2 \setminus \{m_2\}$ so that $reconstruct(m_1, m_2') \in \mathcal{M}$ with non-negligible probability.

GNIMAP

Alice		Bob
Input $(M$, Bob$)$		
Compute $split(M) = (m_1, m_2)$	$\xrightarrow{m_2}$	Receive m_2'
	$\xRightarrow{m_1}$	Receive m_1' and compute
		$reconstruct(m_1', m_2') = M'$ Output (Alice, M') if $M' \in \mathcal{M}$, and reject otherwise.

Binding Game

Oscar		Challenger
Choose $M \in \mathcal{M}$	$\xrightarrow{M}$	Compute $split(M) = (m_1, m_2)$
	$\xleftarrow{m_1, m_2}$	
Send m_2',	$\xrightarrow{m_2'}$	Compute $M' = reconstruct(m_1, m_2')$.
where $m_2 \neq m_2'$.		Oscar wins if $M' \in \mathcal{M}$ and $M \neq M'$

With (m_1, m_2) corresponding to M, for all m_2' either $reconstruct(m_1, m_2') = M$ or $reconstruct(m_1, m_2') = \perp$ with high probability.

A pair of functions $(split, reconstruct)$ to be (T, ϵ)-binding, if any adversary bounded by a complexity T wins the Binding game with a probability of success at most ϵ.

Proof Outline

We would like to prove

(Binding Game is hard) $\Longrightarrow$ (GNIMAP is secure).

We prove that

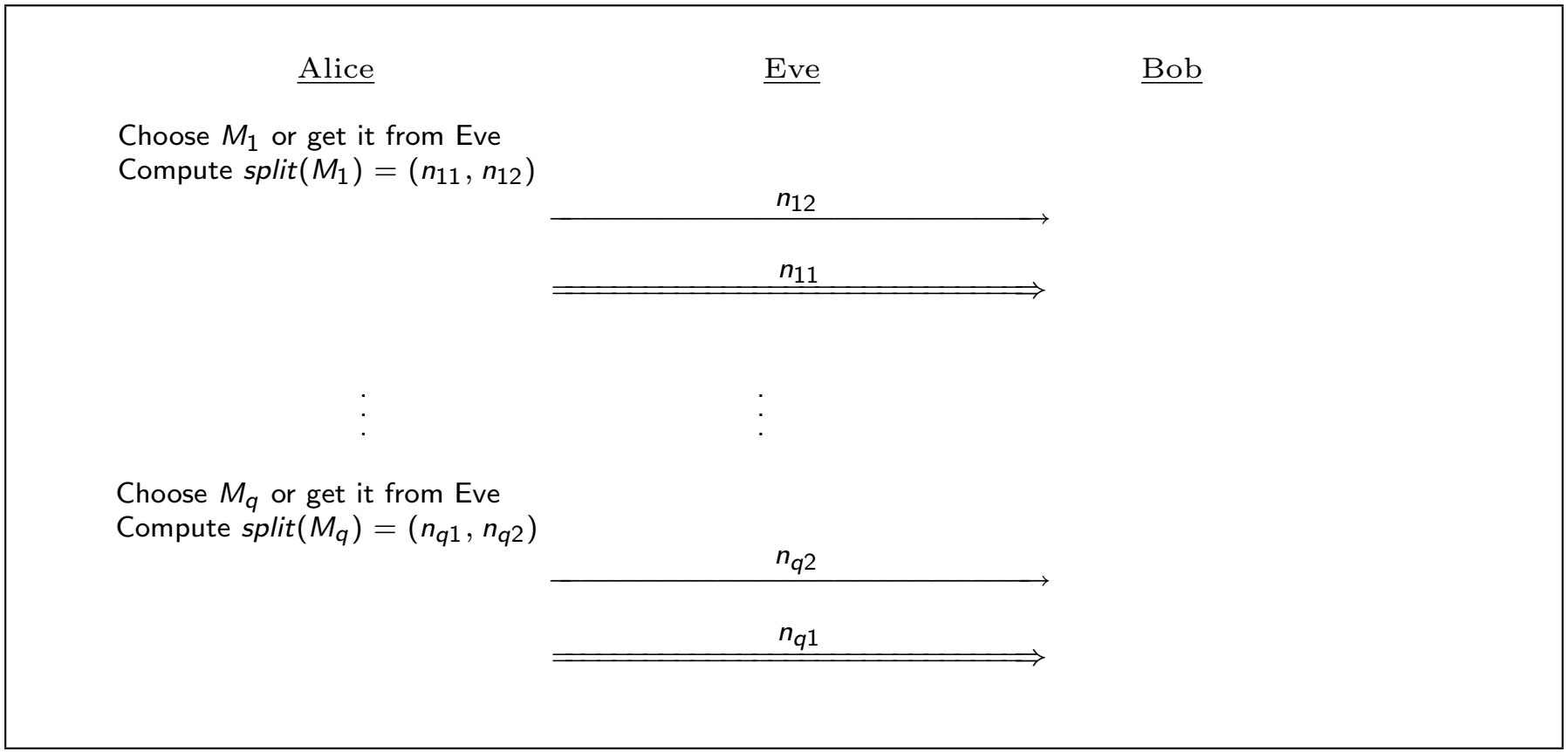
(Binding Game is hard) $\Longrightarrow$ (GNIMAP Game is hard)

$\Updownarrow$

(GNIMAP is secure).

There is a factor of q in the first reduction.

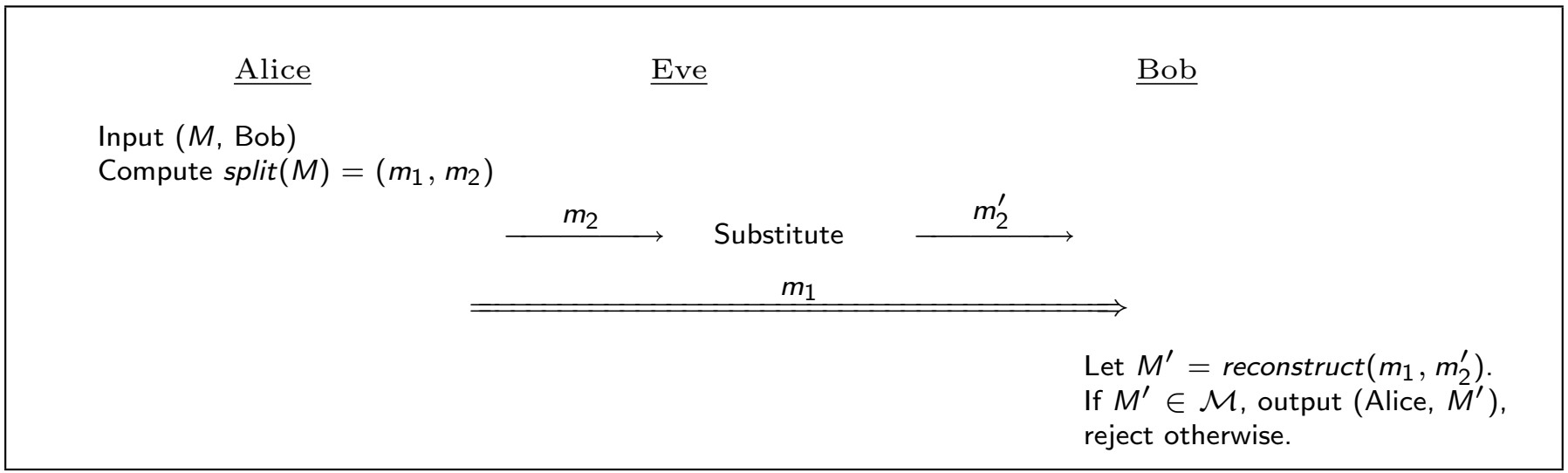
Information Gathering Stage



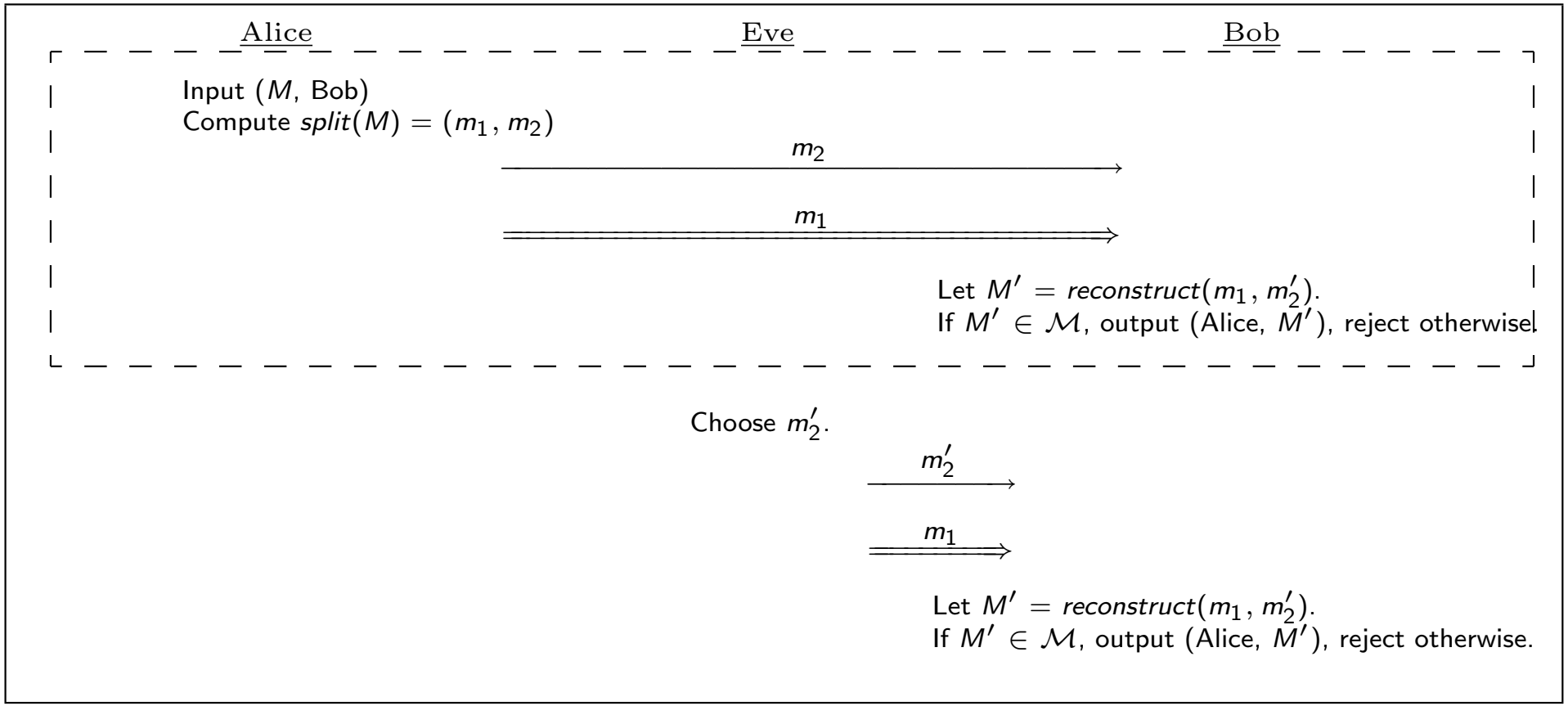
Impersonation Attack

Eve		Bob
Choose m_2'	$\xrightarrow{m_2'}$	
Let $m_1' = m_1$, where Alice has sent m_1 in a previous flow	$\xrightarrow{m_1'}$	Compute $M' = \mathit{reconstruct}(m_1', m_2')$. If $M' \in \mathcal{M}$, then output (Alice, M'), reject otherwise.

Substitution Attack



Equivalence of Impersonation and Substitution attacks



Deception Stage

WLOG we assume that the attempted deception is an impersonation.

Eve		Bob
Choose m_2'	$\xrightarrow{m_2'}$	
Replay $m_1' = n_{i1}$ for some $i \in \{1, \ldots, q\}$	$\xrightarrow{m_1'}$	Accept if $reconstruct(m_1', m_2') \in \mathcal{M}$ and reject otherwise.

GNIMAP Game

We consider the following game:

Eve		Challenger
Choose M_1	$\xrightarrow{M_1}$	Compute $Split(M_1) = (n_{11}, n_{12})$
	$\xleftarrow{(n_{11}, n_{12})}$	
$\vdots$	$\vdots$	$\vdots$
Choose M_q	$\xrightarrow{M_q}$	Compute $Split(M_q) = (n_{q1}, n_{q2})$
	$\xleftarrow{(n_{q1}, n_{q2})}$	
Replay $m'_1 = n_{i1}$ for some $i \in \{1, \ldots, q\}$	$\xrightarrow{(m'_1, m'_2, i)}$	Eve wins if $reconstruct(m'_1, m'_2) = M' \neq M_i$.

GNIMAP Game continued

Theorem

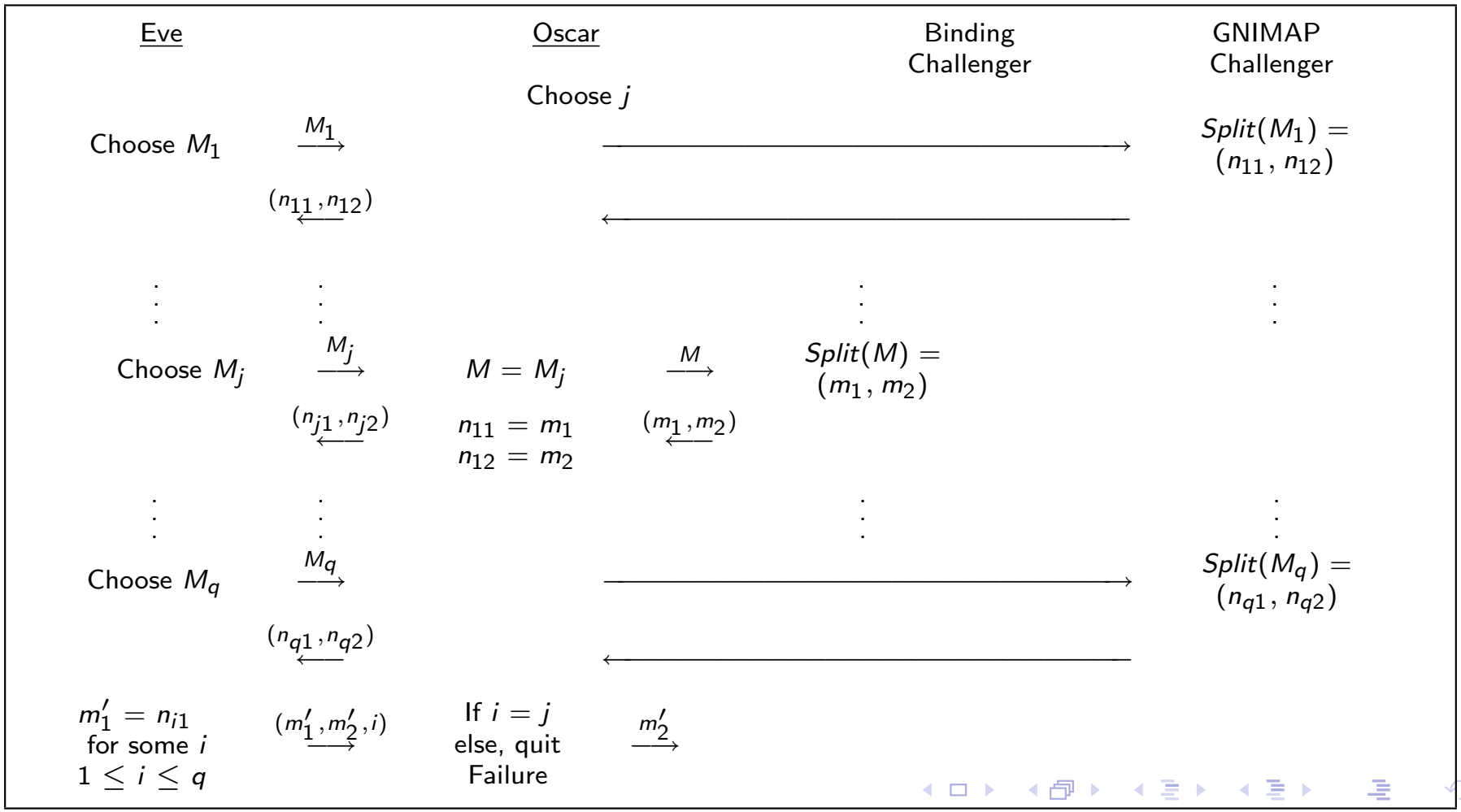
Consider the GNIMAP in the ACPA model. Then, GNIMAP Game is hard if and only if GNIMAP is secure.

(GNIMAP Game is hard)

$$\Updownarrow$$

(GNIMAP is secure).

Reducing Binding Game to GNIMAP Game



Result

Theorem

Consider a GNIMAP Game where the pair $(split, reconstruct)$ *is* (T, ϵ)*-binding. Any player with online complexity* q *and offline complexity* T *has a probability of success at most* $q\epsilon$ *in winning the GNIMAP Game.*

(Binding Game is hard) $\Longrightarrow$ (GNIMAP Game is hard)

$\Updownarrow$

(GNIMAP is secure).

Main Result

Theorem

Assume that there is a GNIMAP where the pair $(split, reconstruct)$ *is* (T, ϵ)*-binding. In the ACPA model, any adversary against this GNIMAP with online complexity* q *and offline complexity* T *has a probability of success* p *at most* $q\epsilon$*.*

(Binding Game is hard) $\Longrightarrow$ (GNIMAP Game is hard)

$\Updownarrow$

(GNIMAP is secure).

Mashatan-Stinson NIMAP

Let H be an HCR hash function.

Alice		Bob
Input $(M$, Bob$)$, $\|M\| = l_1$,		
Choose $K \in_R \{0,1\}^{l_2}$.	$\xrightarrow{M, K}$	Receive M', K'.
Compute $h = H(M \| K)$.	$\xrightarrow{h}$	Receive h', accept if $h' = H(M' \| K')$, reject otherwise.

Theorem

Let H be a (T, ϵ)-HCRHF. Any adversary against Mashatan-Stinson NIMAP, with online complexity q and offline complexity T, has a probability of success p at most $q\epsilon$.

Parameters

Recall that $\epsilon \leq 2^{t-k} + 2^{2t-k-l_2}$.
Typical choices: $k = 100$, $q \leq 2^{10}$, $t \leq 70$, [PV06], and the probability of success of the adversary be less that 2^{-20}.
We get: $\epsilon \approx 2^{-30} + 2^{40-l_2}$. Hence, $\epsilon \approx 2^{-30}$.
Thus, $l_2 \geq 100$ will achieve the same security.

Parameters continued

Other choices of parameters are possible.
Reduce the size of l_2 to 70:
$q \leq 2^{10}, t \leq 70, k = 101$, and $l_2 = 70$ achieves the same level of security $p \leq 2^{-20}$.

Vadenay-Pasini NIMAP: $2 \log N$ bits over the insecure channel, where $\log N$ is the size of the message.
Our protocol: $l_1 + l_2$ bits over the insecure channel where l_1 is the size of the message and l_2 is significantly less that l_1.

Advantages

Simple and easy to implement structure.
Based on a single assumption that HCR hash functions exist.
No commitment scheme, no previously distributed public parameters (CRS).
Information sent over the authenticated channel is as low as the most secure NIMAP proposed so far, while achieving the same level of security.

Mashatan-Stinson IMAP

We obtain a new IMAP

- that has an efficient and easy to use structure, and
- achieves the same level of secure as the best known IMAP.

Alice		Bob
Input (M, Bob)		
Send M	$\xrightarrow{M}$	Receive M'
	$\xleftarrow{R}$	Choose $R \in \{0,1\}^{l_2}$ uniformly at random
Receive R' and		
Compute $h = H(M \Vert R')$	$\xrightarrow{h}$	Output (Alice, M') if $h = H(M' \Vert R)$,
		and reject otherwise.

Interactive-Collision Resistance

Definition

A hash function H is **Interactive-Collision Resistant (ICR)** if the following **ICR Game** is hard to win. The pair $(M\|R, M'\|R')$ is an *interactive-collision*.

Oscar		Challenger
Choose M, $\|M\| = l_1$.	$\xrightarrow{M}$	Choose $R \in \{0,1\}^{l_2}$ uniformly at random.
	$\xleftarrow{R}$	
Choose M', $\|M'\| = l_1$.	$\xrightarrow{M'}$	Choose $R' \in \{0,1\}^{l_2}$ uniformly at random.
	$\xleftarrow{R'}$	Oscar wins if $H(M\|R) = H(M'\|R')$.

If an adversary with computational complexity T wins the ICR game with probability at most ϵ, the H is a (T, ϵ)-ICR hash function.

Hardness of ICR Game

Let $\mathcal{X} = \{0,1\}^{l_1+l_2}$ be the set of all possible binary strings of size $l_1 + l_2$. Consider a hash function, H, randomly chosen from $\mathcal{F}^{\mathcal{X},\mathcal{Y}}$. Assume that, we are only permitted oracle access to H, $T = 2^t$ times.

Let ϵ be the probability of Oscar wining the ICR Game.

We have proved that $\epsilon \leq 2^{-k}(1 + 2^{2t-2l_2} + 2^{t-l_2})$

Summary

We provide a general framework for two-channel NIMAPs.
GNIMAP is secure when the Binding Game is hard to win. Security of any NIMAP can be analyzed in terms of the difficulty of the Binding Game.
Our new NIMAP achieves the best known security level among NIMAPs while benefiting from a simple structure. The assumptions are minimal compared to other NIMAPs.
Our IMAP achieves the same level of security as the best IMAP present in the literature, while having a much simpler structure and under fewer security assumptions.

Future Work

- Fewer authenticated bits!
- Unconditional security in two-channel NIMAPs?
- A general framework for two-channel-IMAPs.
- Mutual authentication.
- Mutual key generation.

Dirk Balfanz, Diana K. Smetters, Paul Stewart, and H. Chi Wong.

Talking to strangers: Authentication in ad-hoc wireless networks.
In *Network and Distributed Sytem Security Symposium*, San Diego, California, U.S.A., February 2002.

Christian Gehrmann, Chris J. Mitchell, and Kaisa Nyberg.

Manual authentication for wireless devices.
RSA Cryptobytes, 7(1):29–37, January 2004.

Atefeh Mashatan and Douglas R. Stinson.

Noninteractive two-channel message authentication based on hybrid-collision resistant hash functions.
Cryptology ePrint Archive, Report 2006/302, 2006.
http://eprint.iacr.org/.

Sylvain Pasini and Serge Vaudenay.

An optimal non-interactive message authentication protocol.
In David Pointcheval, editor, *Topics in Cryptography*, volume 3860 of *Lecture Notes in Computer Science*, pages 280–294, San Jose, California, U.S.A., February 2006. Springer-Verlag.

Ronald L. Rivest and Adi Shamir.

How to expose an eavesdropper.
Commun. ACM, 27(4):393–394, 1984.

Serge Vaudenay.

Secure communications over insecure channels based on short authenticated strings.
In Victor Shoup, editor, *Advances in Cryptography*, volume 3621 of *Lecture Notes in Computer Science*, pages 309–326, Sanra Barbara, California, U.S.A., August 2005. Springer-Verlag.