Recent Results on the Design and Analysis of Manual Authentication Protocols

Atefeh Mashatan and Douglas R. Stinson

David R. Cheriton School of Computer Science, University of Waterloo

Fields Institute Workshop on New Directions in Cryptography
University of Ottawa
June 26, 2008

What is Two-channel Cryptography?

- Two channels are accessible for communication. They have different properties in terms of security and cost.
- broadband insecure channel: wireless channel,
- narrow-band authenticated channel: voice, data comparison, data imprinting, near field communication: visible light, infra red signals, laser.
- Goal: to achieve a certain cryptographic goal by means of the two channels while optimizing the cost.

The First Suggestion of Two-channel Cryptography

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

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

Two-channel Cryptography in Ad Hoc Networks

- 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 remove users.

- Secret-key techniques not practical.
- Public-key techniques too expensive.
- Identity-based systems need some structure.
- What can we do in absence of a public or secret key?!

Two-channel Authentication!

Our approach

- The focus is on authentication in ad hoc networks.
- A totally insecure broadband channel: $\longrightarrow$
- A moderately secure narrow-band channel: $\Rightarrow$
- The attack model is Adaptive Chosen Plaintext Attack (ACPA) model.

Communication Model

Two small devices, Alice and Bob, wish to establish a secure key, M, in the presence of an active adversary, Eve.

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

Eve has full control over the broadband channel.
Eve has limited control over the narrow-band channel. She cannot modify a message or initiate a new flow. The channel is equipped with user authenticating features.

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

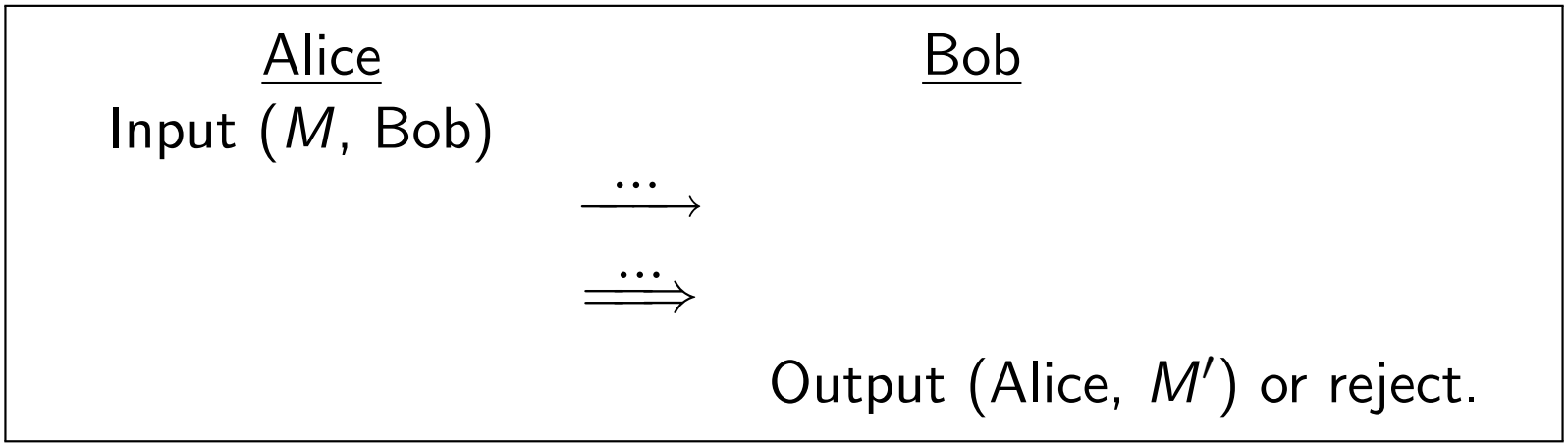
Adaptive Chosen Plaintext Attack (ACPA) model.

- 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: $2^{t_{off}}$.
Online computational complexity: $2^{t_{on}}$.
Querying complexity: q.

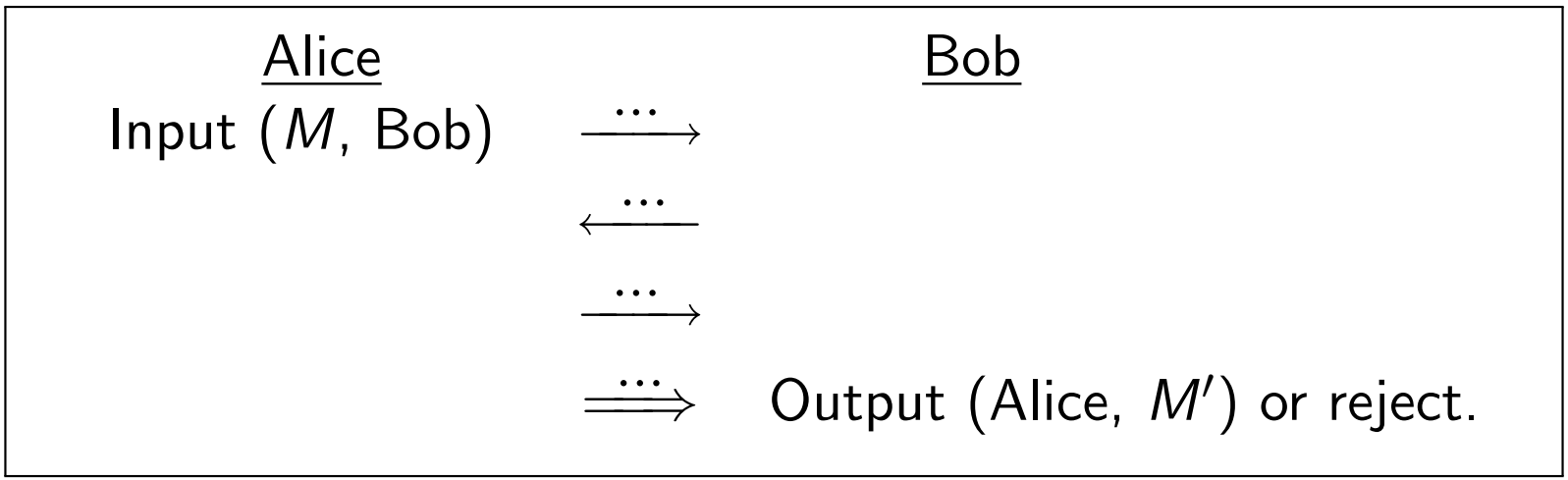
Non-interactive MAP

A typical flow structure:



Interactive MAP

A possible flow structure:



Computational versus Unconditional Security

- Unconditionally Secure Protocol:
  Adversary has unlimited computational resources, but she does not have enough information to defeat the system.
- Computationally Secure Protocol:
  The computational power of the adversary is bounded. However, the best currently-known methods to defeat a system exceeds the computational resources of the adversary, by a comfortable margin.

Provable Security for NIMAPs and IMAPs

A successful adversary is reduced to solving a well-known problem which is proven, or widely believed, to be secure.
For instance:

- finding collisions for a Collision Resistant hash function,
- computing second-preimages for a Second-Preimage Resistant hash function, or
- breaking the trapdoor of a trapdoor commitment scheme.

Balfanz-Smetters-Stewart-Wong NIMAP

In BSSW02, Balfanz et. al 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.

Suppose 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.
To avoid this attack, the message digest should be at least 160 bits long (attack complexity 2^{80}, so $t_{off} = 80$).

Gehrmann-Mitchell-Nyberg NIMAP: MANA I

In GMN04, Gehrmann et. al 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.

In Vau05, Vaudenay 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

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.

- H is a Second-Preimage Resistant hash function.
- "commit" and "open" refer to a trapdoor commitment scheme.
- Common Reference String model: random string K_p known to both parties.

The protocol authenticates 100 bits to have the success probability of the adversary less than 2^{-20}.

Our Contributions

Proposing a New NIMAP

- that is as efficient as the best known NIMAP,
- benefits from a simple and easy to implement structure, and
- the security depends on certain collision properties of a hash function.

Mashatan-Stinson NIMAP

Let H be a hash function (which satisfies a certain property, to be defined later).

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

Attacking Mashatan-Stinson NIMAP

Alice		Eve		Bob
	$\xleftarrow{M}$	$M \in \{0,1\}^{l_1}$		
Choose $K \in_R \{0,1\}^{l_2}$.	$\xrightarrow{M, K}$	$\lvert M' \rvert = l_1, \lvert K' \rvert = l_2$	$\xrightarrow{M', K'}$	
Compute $h = H(M \Vert K)$.	$\xRightarrow{h}$		$\xRightarrow{h}$	Accept if $h = H(M' \Vert K')$.

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

We analyze the HCR game in the random oracle model.
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, at most $T = 2^t$ times.
Let ϵ be the probability of Oscar winning the HCR Game. Then,

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

Security of Mashatan-Stinson NIMAP

Theorem ([MS07b])

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

Typical choices (*a la* Vaudenay-Pasini): $k = 100$ (# of bits sent over the authenticated channel), $q \leq 2^{10}$, $t \leq 70$, and suppose that we want the probability of success of the adversary to be less than 2^{-20}. Hence, we want $\epsilon \approx 2^{-30}$.

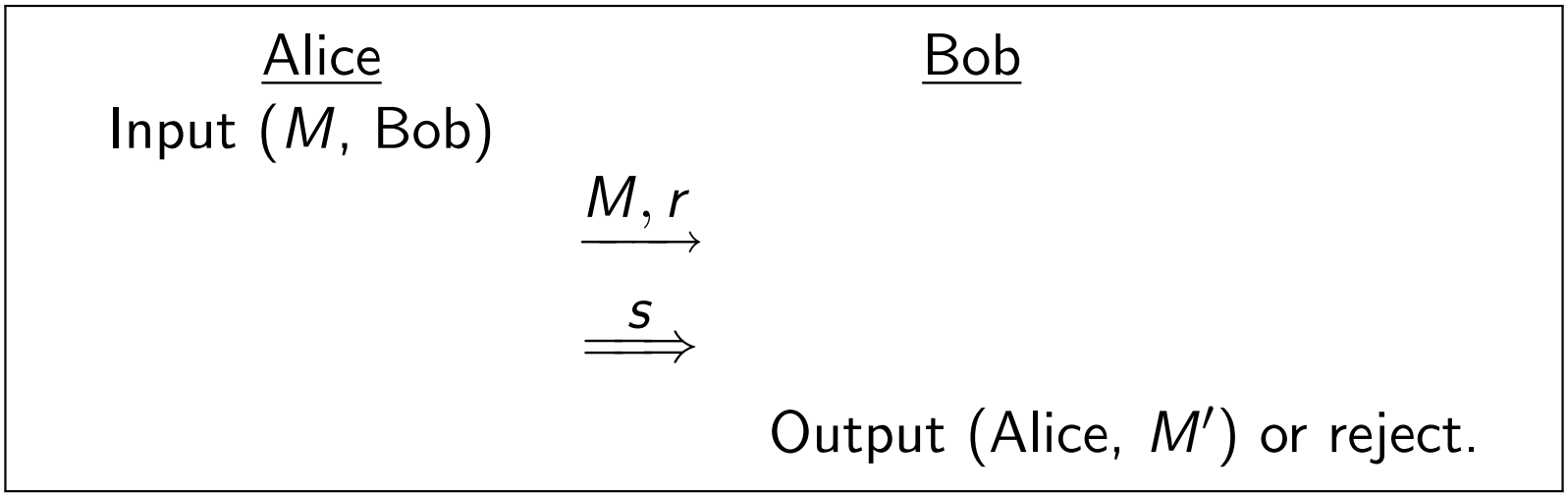
From the Theorem, we have $\epsilon \approx 2^{-30} + 2^{40-l_2}$. Hence, $\epsilon \approx 2^{-30}$ if l_2 is large enough.

Impossibility of designing non-trivial unconditionally secure NIMAPs

- In WS08, Wang and Safavi-Naini prove that it is impossible to build non-trivial unconditionally secure NIMAPs.
- They use probability distribution arguments.
- We provide a new simpler proof in the form of a counting argument.

The new proof

Let $M \in \mathcal{M}$, $r \in \mathcal{R}$, and $s \in \mathcal{S}$.



Let $\mathcal{V} = \{(M, r, s) : \text{ Bob accepts the triple } (M, r, s)\}$.
Note that, $\mathcal{V}$ is public knowledge and for a non-trivial NIMAP we must have $|\mathcal{M}| > |\mathcal{S}|$.

The new proof, continued

- For $s \in \mathcal{S}$, let $\mathcal{M}_s := \{M : \exists (M, r, s) \in \mathcal{V} \text{ for some } r\}$.
- Let $\mathcal{U} := \{s : |\mathcal{M}_s| = 1\}$ and $\mathcal{M}_{\mathcal{U}} = \bigcup_{s \in \mathcal{U}} \mathcal{M}_s$.
- Since $|\mathcal{S}| < |\mathcal{M}|$, it is easily shown that $\mathcal{M} \neq \mathcal{M}_{\mathcal{U}}$.
- Eve chooses any $M \in \mathcal{M} \setminus \mathcal{M}_{\mathcal{U}}$ and gives it to Alice.
- Now, for any $(M, r, s) \in \mathcal{V}$, there exists $(M', r', s) \in \mathcal{V}$ with $M \neq M'$. Therefore, when she receives (M, r, s) from Alice, Eve can find (M', r') such that $(M', r', s) \in \mathcal{V}$.

The new proof, continued

Finally, Eve replaces (M, r) with (M', r'), which is a successful attack.

Alice		Eve		Bob
	$\xleftarrow{M}$			
	$\xrightarrow{M, r}$			
	$\xRightarrow{s}$			
			$\xrightarrow{M', r'}$	
			$\xRightarrow{s}$	Verify $(M', r', s) \in \mathcal{V}$.

Vaudenay IMAP

Alice		Bob
Input (Bob, M), Choose $R_A \in \{0,1\}^k$ uniformly at random		Choose $R_B \in \{0,1\}^k$ uniformly at random
$(c, d) \leftarrow commit(M, R_A)$	$\xrightarrow{(M\|c)}$	Receive (M', c')
Receive R'_B	$\xleftarrow{R_B}$	
	$\xrightarrow{d}$	Receive d' and compute $R'_A \leftarrow open(M', c', d')$
Compute $R = R_A \oplus R'_B$	$\xrightarrow{R}$	If $R = R'_A \oplus R_B$, then output (Alice, M') and reject otherwise.

Common Reference String model: random string K_p.
An equivocable commitment: *commit*.
Offline complexity of 2^{70} and $q = 2^{10}$: authenticate 50 bits.
Probability of success of the adversary is at most 2^{-20}.

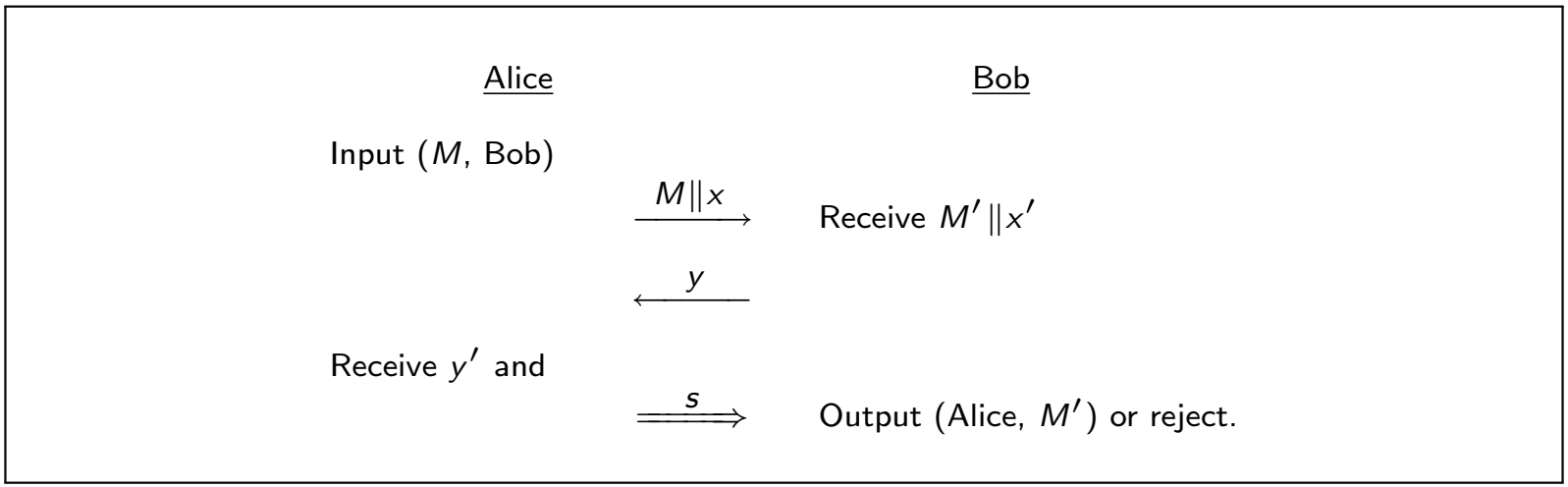
Our Contributions

From [MS07a]:

- propose a new IMAP
- with three flows only
- using hash functions only
- not in the CRS model
- analyze security in the random oracle model

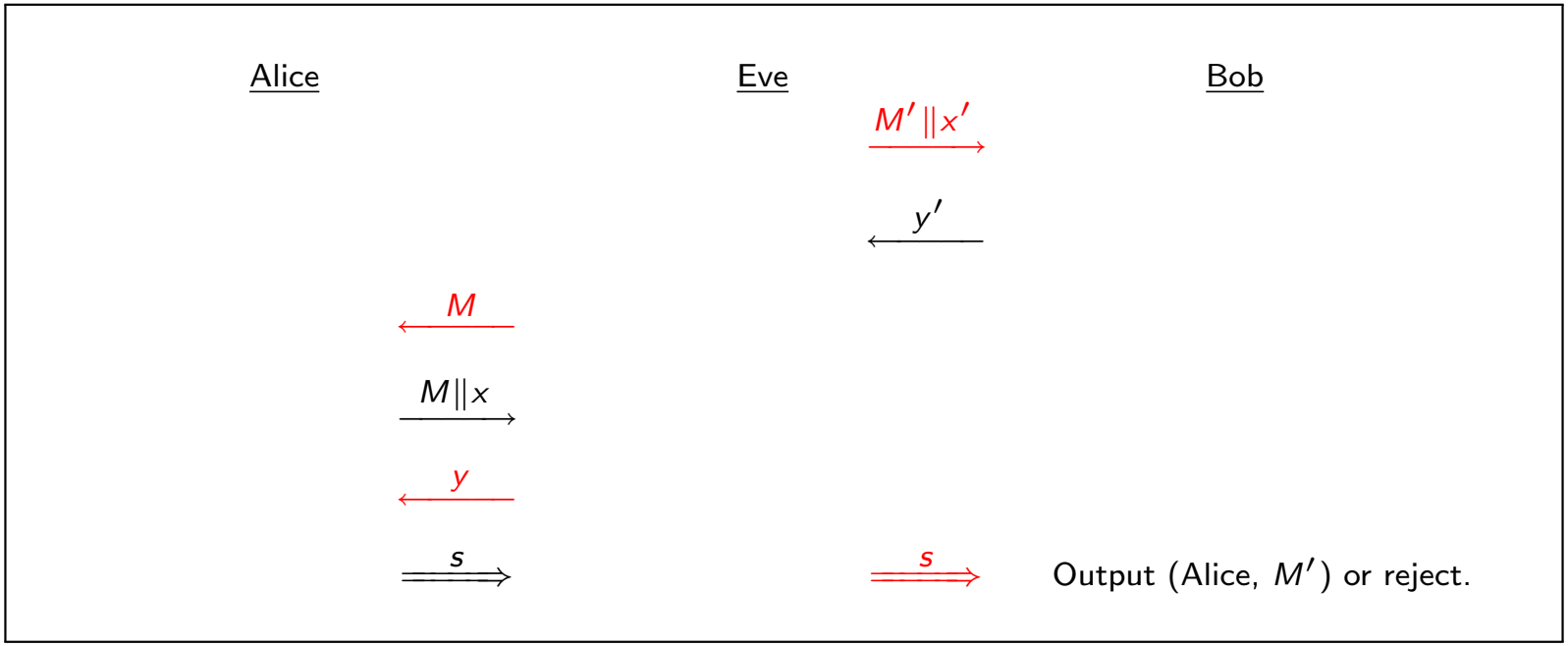
3-round Generic IMAP

A 3-round generic IMAP (3GIMAP) is depicted below:

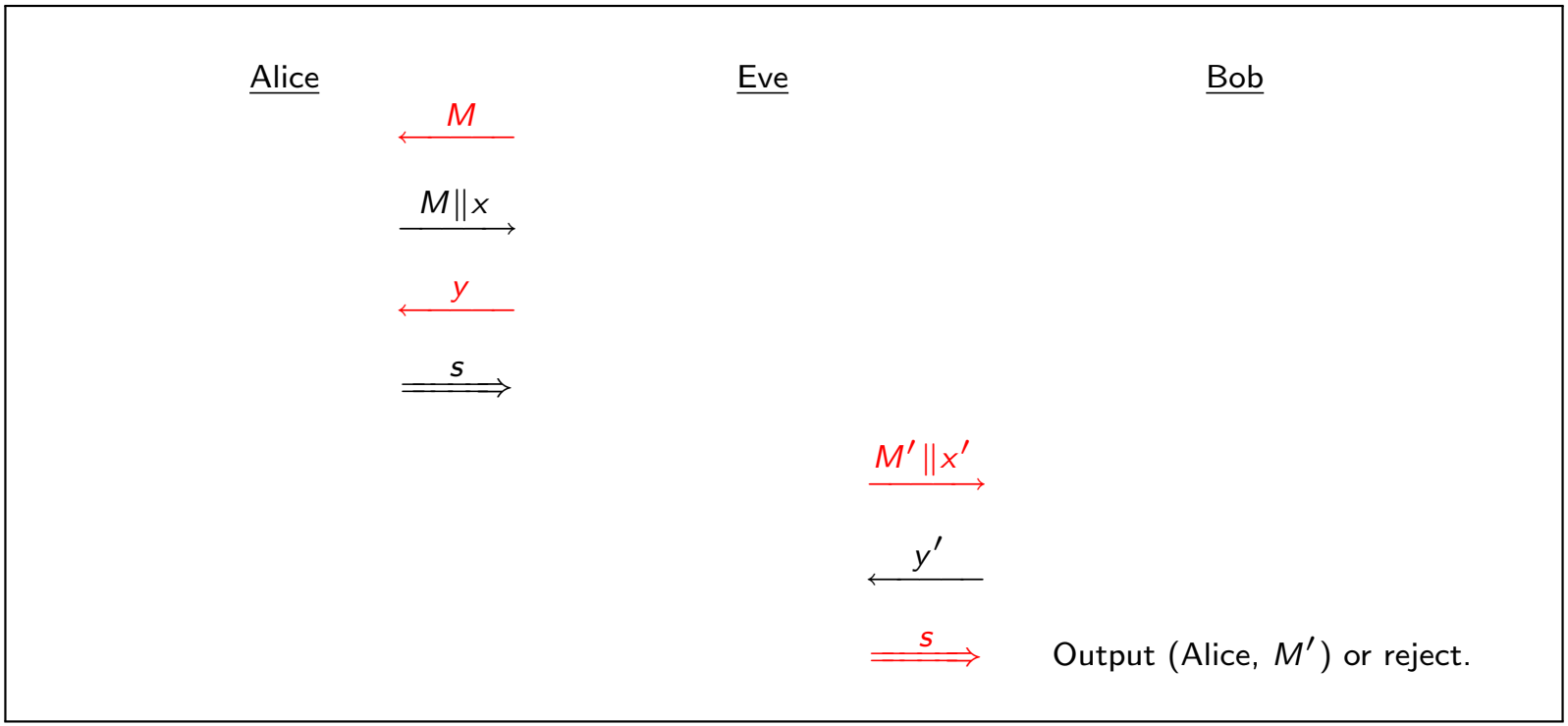


We now investigate possible attacks against this 3GIMAP.

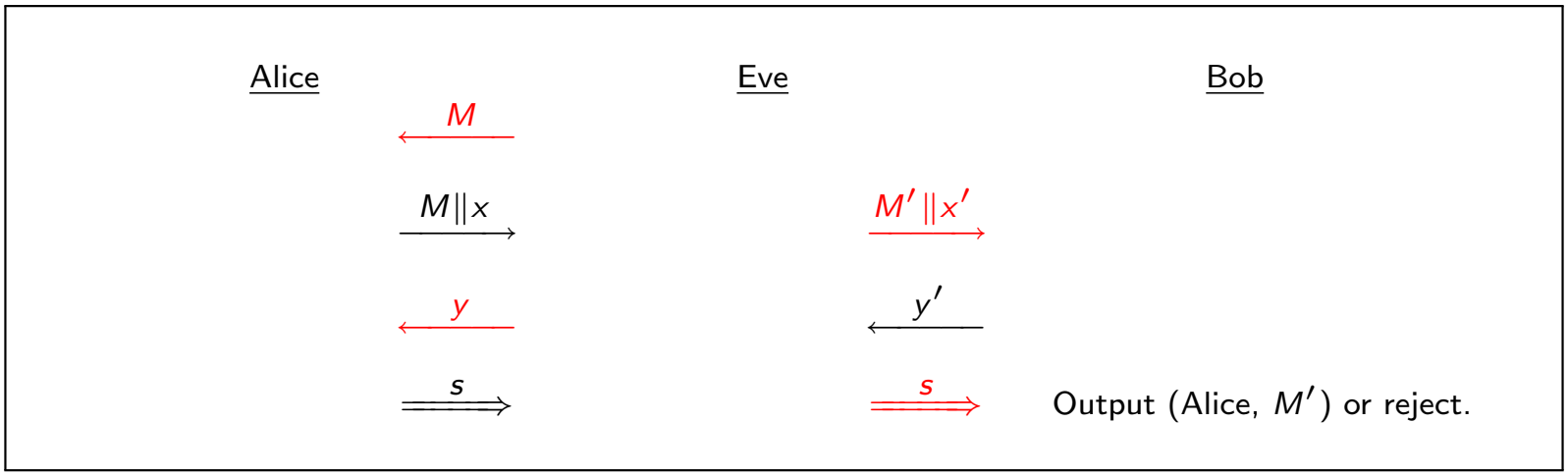
An attack of the form BAAB



An attack of the form AABB



An attack of the form ABAB



Mashatan-Stinson IMAP

Let H be a hash function.

Alice		Bob
Input (M, Bob)		
Choose $K \in \{0,1\}^{\ell_2}$ uniformly at random	$\xrightarrow{M \| K}$	Receive $M' \| K'$
	$\xleftarrow{R}$	Choose $R \in \{0,1\}^{\ell_3}$ uniformly at random
Receive R' and		
Compute $h = H(M \| K \| R')$	$\xRightarrow{h}$	Output (Alice, M') if $h = H(M' \| K' \| R)$, and reject otherwise.

The three attacks, BAAB, AABB, and ABAB, translate to ICRI, ICRII, and ICRIII hash function games.

Interactive-Collision Resistance I

Oscar		Challenger
Choose M, $\lvert M\rvert = \ell_1$	$\xrightarrow{M}$	
	$\xleftarrow{K}$	Choose $K \in \{0,1\}^{\ell_2}$ uniformly at random
Choose R', $\lvert R'\rvert = \ell_3$	$\xrightarrow{R'}$	
Choose M', $\lvert M'\rvert = \ell_1$	$\xrightarrow{M'}$	
Choose K', $\lvert K'\rvert = \ell_2$	$\xrightarrow{K'}$	
	$\xleftarrow{R}$	Choose $R \in \{0,1\}^{\ell_3}$ uniformly at random
		Oscar wins if $H(M\|\|K\|\|R') = H(M'\|\|K'\|\|R)$ and $M\|\|K\|\|R' \neq M'\|\|K'\|\|R$.

Interactive-Collision Resistance II

Oscar		Challenger
Choose M, $\lvert M\rvert = \ell_1$	$\xrightarrow{M}$	
	$\xleftarrow{K}$	Choose $K \in \{0,1\}^{\ell_2}$ uniformly at random
Choose M', $\lvert M'\rvert = \ell_1$	$\xrightarrow{M'}$	
Choose K', $\lvert K'\rvert = \ell_2$	$\xrightarrow{K'}$	
	$\xleftarrow{R}$	Choose $R \in \{0,1\}^{\ell_3}$ uniformly at random
Choose R', $\lvert R'\rvert = \ell_3$	$\xrightarrow{R'}$	
		Oscar wins if $H(M\|\|K\|\|R') = H(M'\|\|K'\|\|R)$ and $M\|\|K\|\|R' \neq M'\|\|K'\|\|R$.

Interactive-Collision Resistance III

Oscar		Challenger
Choose M', $\lvert M' \rvert = \ell_1$	$\xrightarrow{M'}$	
Choose K', $\lvert K' \rvert = \ell_2$	$\xrightarrow{K'}$	
	$\xleftarrow{R}$	Choose $R \in \{0,1\}^{\ell_3}$ uniformly at random
Choose M, $\lvert M \rvert = \ell_1$	$\xrightarrow{M}$	
	$\xleftarrow{K}$	Choose $K \in \{0,1\}^{\ell_2}$ uniformly at random
Choose R', $\lvert R' \rvert = \ell_3$	$\xrightarrow{R'}$	
		Oscar wins if $H(M\|\|K\|\|R') = H(M'\|\|K'\|\|R)$ and $M\|\|K\|\|R' \neq M'\|\|K'\|\|R$.

Interactive-Collision Resistance

T_{off}: computational complexity of Oscar before he receives the last flow from the Challenger, i.e. R in the ICRII and K in the ICRIII.

T_{on}: computational complexity of Oscar after he receives the last flow from the Challenger and before he sends the value of R' in ICRII and ICRIII.

Definition

A hash function H is **Interactive-Collision Resistant (ICR)** if the ICRI, ICRII, and ICRIII Games are all hard to win. Furthermore, H is said to be a $(T_{\text{off}}, T_{\text{on}}, \epsilon_1, \epsilon_2)$-ICR hash function if it is a $(T_{\text{off}}, \epsilon_1)$-ICRI hash function, a $(T_{\text{off}}, T_{\text{on}}, \epsilon_2)$-ICRII hash function, and a $(T_{\text{off}}, T_{\text{on}}, \epsilon_2)$-ICRIII hash function.

Security of Mashatan-Stinson IMAP

Theorem

Let $\mathcal{X} = \{0,1\}^{\ell_1+\ell_2+\ell_3}$ and H be a hash function chosen randomly from $\mathcal{F}^{\mathcal{X},\mathcal{Y}}$, where $|\mathcal{Y}| = 2^k$. Then, any adversary against our IMAP, with offline complexity $T_{\text{off}} = 2^{t_{\text{off}}}$ and online complexity $T_{\text{on}} = 2^{t_{\text{on}}}$ who can make q message queries, has a probability of success

$$p \leq 2^{-k} \max(q(2+2^{2t_{\text{off}}-\ell_2-\ell_3}+2^{t_{\text{off}}-\ell_3}), 2+2^{2t_{\text{off}}-\ell_2-\ell_3}+2^{t_{\text{off}}-\ell_3}+2^{t_{\text{on}}}).$$

Parameters of Mashatan-Stinson IMAP

Recall that

$$p \leq 2^{-k} \max(q(2+2^{2t_{\text{off}}-\ell_2-\ell_3}+2^{t_{\text{off}}-\ell_3}), 2+2^{2t_{\text{off}}-\ell_2-\ell_3}+2^{t_{\text{off}}-\ell_3}+2^{t_{\text{on}}}).$$

- We target typical values for $q \leq 2^{10}$, $t_{\text{off}} \leq 70$, and $p \leq 2^{-20}$.
- If we take $\ell_2, \ell_3 \geq 80$, then we can ignore the factors $(2 + 2^{2t_{\text{off}}-\ell_2-\ell_3})$ and $2^{t_{\text{off}}-\ell_3}$.
- Hence, we obtained the simplified bound

$$p \leq 2^{-k} \max(q, 2^{t_{\text{on}}}).$$

Parameters of Mashatan-Stinson IMAP, continued

- We want the overall success probability of the adversary be less than or equal to 2^{-20}; hence, we require that $\max(q, 2^{t_{\text{on}}}) \leq 2^{k-20}$.
- Hence, letting $t_{\text{on}} = 10$ along with typical parameters $q \leq 2^{10}$, $t_{\text{off}} \leq 70$, and $p \leq 2^{-20}$, we get that $k = 30$.
- This is a distinct improvement over previous protocols, especially when hash functions are the only primitives available in a pervasive network.
- Note that, we can allow t_{off} to get bigger as well by just choosing $\ell_2 + \ell_3$ according to the size of t_{off}.

Parameters of Mashatan-Stinson IMAP, continued

- In practice, there needs to be a relation between the size of the messages M, ℓ_1, and the choice of t_{on}.
- In attacks of the form BAAB or ABAB, the adversary is making $2^{t_{\text{on}}}$ hash computations while Alice is waiting to get a value R from Bob. Generating a random value R does not take long.
- For our application, in particular, these devices are in close proximity and as a results the delay in the system should be low as well.
- This means that when Alice does not hear back from Bob, she suspects that some active adversary is trying to intervene.

Naor-Segev-Smith IMAP

In NSS06, Naor et al. proposed an unconditionally secure IMAP using evaluation of polynomials over finite fields.

For every integer r, the sender authenticates an n-bit message in r rounds, such that the length of the authenticated string is about $2\log(1/\epsilon) + 2\log^{r-1} n + O(1)$.

By setting $r = \log(n)$, the manually authenticated string is of length $2\log(1/\epsilon)$.

Generalization of Naor-Segev-Smith IMAP

We consider 3-round protocols. Let

- $\mathcal{M}$: set of all messages, $\mathcal{K}$: set of all possible keys, and
- $\mathcal{H}$: set of keyed hash functions of the form $h_y : \mathcal{M} \to \mathbb{F}_q$ for $y \in \mathcal{K}$.

Alice		Bob
Input (M, Bob)		
Choose $x \in \mathbb{F}_q$ uniformly at random	$\xrightarrow{M \Vert x}$	Receive $M' \Vert x'$
	$\xleftarrow{y}$	Choose $y \in \mathcal{K}$ uniformly at random
Receive y and		
Compute $t = h_y(M) + x$	$\xrightarrow{y,\, t}$	Output (Alice, M') if $t = h_y(M') + x'$, and reject otherwise.

BAAB Attack

- Eve is required to set $y = y'$.
- She is successful iff $h_{y'}(M) + x = h_{y'}(M') + x'$, or

$$x = h_{y'}(M') + x' - h_{y'}(M).$$

- Since x is randomly chosen by Alice, Eve succeeds with probability $1/q$.

AABB Attack

- Eve receives M, x and has to guess the key y' ahead of time to set $y = y'$.
- Then, she chooses M' and x such that $h_y(M) + x = h_y(M') + x'$.
- The probability that Eve guesses the right key y' is $1/|\mathcal{K}|$.

ABAB Attack

- Eve receives M, x and fixes M', x' before y' is chosen by Bob.
- She is successful iff $h_{y'}(M) + x = h_{y'}(M') + x'$, or

$$h_{y'}(M) - h_{y'}(M') = x' - x.$$

Note that, $x' - x$ is fixed.

Definition

A hash family $\mathcal{H}$ is an ϵ-ΔU hash family if for all choices of M, M', x'' and ϵ, it holds that

$$\Pr[h_y(M) - h_y(M') = x''] \leq \epsilon,$$

where the probability is over a random choice of y.

Pick an ϵ-ΔU hash family, $\mathcal{H}$, then

- Eve succeeds with probability $\max\{\epsilon, 1/q, 1/|\mathcal{K}|\}$, and
- the size of the authenticator is $\log_2 |\mathcal{K}| + \log_2 q$ bits

Note that, $\epsilon \geq 1/q$, since Eve can always guess y with probability $1/q$. So, Eve succeeds with probability

$$\max\{\epsilon, 1/|\mathcal{K}|\}.$$

The 3-round NSS06 protocol is a special case of this construction, where the ϵ-ΔU hash family is constructed from a Reed-Solomon code.

Related Work: Recognition in Ad hoc Pervasive Networks

Entity recognition: two parties meet initially and one party can be assured in future conversations that it is communicating with the same second party.

Message recognition provides data integrity with respect to the data origin and it ensures that the entity who sent the message is the same in future conversations.

We suggest an improvement to a previously known message recognition protocol in [MS08b].

Also, we propose a new message recognition protocol in [MS08a].

Atefeh Mashatan and Douglas R. Stinson.

Interactive two-channel message authentication based on interactive-collision resistant hash functions.
Technical Report 24, Centre for Applied Cryptographic Research (CACR), University of Waterloo, Canada, 2007.

Atefeh Mashatan and Douglas R. Stinson.

Noninteractive two-channel message authentication based on hybrid-collision resistant hash functions.
IET Information Security, 1(3):111–118, September 2007.

Atefeh Mashatan and Douglas R. Stinson.

A new recognition protocol for ad hoc pervasive networks.
2008.
In preparation.

Atefeh Mashatan and Douglas R. Stinson.

Recognition in ad hoc pervasive networks.
Technical Report 12, Centre for Applied Cryptographic Research (CACR), University of Waterloo, Canada, 2008.