Secure Communications over Insecure Channels Using an Authenticated Channel

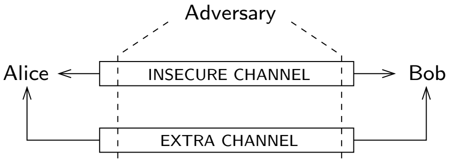
Sylvain Pasini

EPFL / LASEC

21^{st} of September 2005

Introduction

- One key issue in cryptography:
  Setup a secure communication
- Suppose Alice and Bob want to communicate securely:

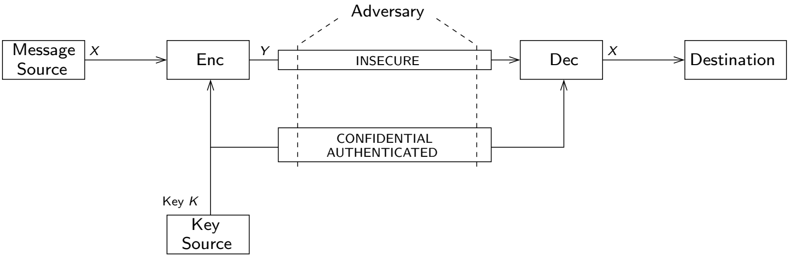


- No prior exchanged key
- Insecure channel:
  - Adversaries have full control
    i.e. can replay, delay, modify,
    remove, and change addresses.
- Extra channel:
  - Other assumptions?
  - e.g. confidentiality, integrity, **authenticity** ?

Overview

Symmetric Cryptography

The Shannon model:



- Confidentiality is required
- Short keys (e.g. 128 bits for AES)

Human Being Channels

	Interactive		Non-interactive	
	Encounter	Telephone	Mail	Email
Authenticity	✓	✓	✓	
Confidentiality	✓			
Cost		✓	✓	✓
Availability		✓	✓	✓

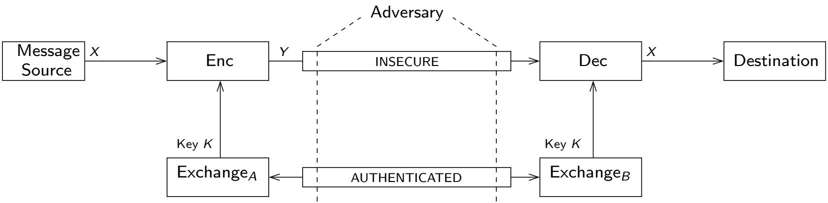
For symmetric cryptography, we need confidentiality:

- The only way: encounter

  cost and availability are bad

Relaxing the Confidentiality

The Merkle-Diffie-Hellman model:



- After the exchange, they share a key K
- No confidentiality required

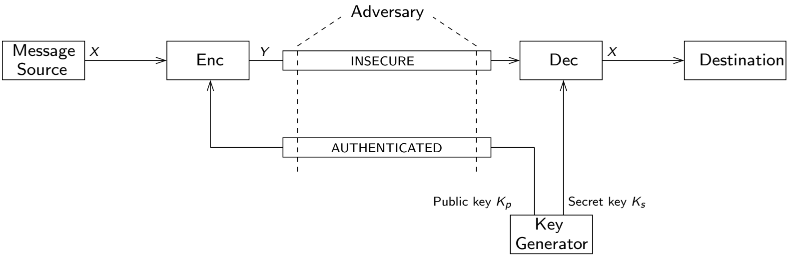
The Diffie-Hellman Protocol

Alice		Bob
pick x		pick y
$X \leftarrow g^x$	$\xrightarrow{X}$	
	$\xleftarrow{Y}$	$Y \leftarrow g^y$
$K \leftarrow Y^x = g^{xy}$		$K \leftarrow X^y = g^{xy}$

- Based on discrete logarithm (DL) problem
  - Given g, x, computing $X \leftarrow g^x$ is **easy**
  - Given g, X, computing $x \leftarrow \log_g X$ is **hard**
- Vulnerable to man-in-the-middle (MITM) attacks
  - Requires message authentication

Public-Key Cryptography

The semi-authenticated key transfer:



- We no longer need confidentiality
- An authenticated channel is enough:
  - Telephone can be used: cheaper than encounter
- Note: a public key is long (e.g. 1024 bits for RSA)

Authentication Problem

In a nutshell:

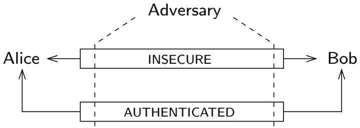
- Setup a secure communication
  $\longrightarrow$ Exchange and authenticate a public key
- Exchange by phone is tedious (1024 bits)
- Objective: reduce the amount of authenticated data
  $\longrightarrow$ use message authentication protocols

Different authentication ways:

- Biometrics-based (e.g. voice)
- Distance bounding
- Others?

Authenticated Channel

Channels model:



Extra authenticated channel:

- The recipient is insured on the message source
- Weak: adversary can read, replay, delay, remove (not modify)
- Stronger: offers additional properties

Example from Balfanz et al. (in SSH and GPG):

Alice		Bob
input: m		
	$\xrightarrow{\quad m \quad}$	$\hat{h} \leftarrow \mathrm{H}(\hat{m})$
$h \leftarrow H(m)$	$\xrightarrow{\text{authenticate}_{Alice}(h)}$	check $h = \hat{h}$
		output: $Alice, \hat{m}$

An Interactive Biometrics-based Protocol

Wu-Boa-Deng(2005) proposed the following

Alice		Bob
pick $x \in_U \{0,1\}^k$		pick $y \in_U \{0,1\}^k$
$X \leftarrow g^x$		$Y \leftarrow g^y$
$K_A \leftarrow \mathrm{h}(X)$		$K_B \leftarrow \mathrm{h}(Y)$
$C_A \leftarrow \mathrm{record}()$		
$E_{C_A} \leftarrow \mathrm{Enc}_{K_A}(C_A)$	$\xrightarrow{E_{C_A}}$	$C_B \leftarrow \mathrm{record}()$
	$\xleftarrow{E_{C_B}}$	$E_{C_B} \leftarrow \mathrm{Enc}_{K_B}(C_B)$
$\mathrm{start}(clk1)$	$\xrightarrow{X}$	deduce $\hat{K}_A, K_{BA}, \hat{C}_A$
		check identity$(\hat{C}_A)$
		$R_B \leftarrow \mathrm{record}()$
$t_a \leftarrow \mathrm{stop}(clk1)$	$\xleftarrow{E_{R_B} \vert\vert Y}$	$E_{R_B,K_{BA}} \leftarrow \mathrm{Enc}_{K_{BA}}(R_B)$
deduce $\hat{K}_B, K_{AB}, \hat{C}_B, \hat{R}_B$		
check $t_a, \hat{C}_B, \hat{R}_B$		
output: Bob, K_{AB}		**output**: K_{BA}

- Duration of records must be at least T
- $t_a = |C_A| + |R_B| + \delta \geq 2T + \delta$

Why a timer?

The timer helps to detect man-in-the-middle attacks

Alice		Adversary		Bob
K_A		K_Z		K_B
	$\xrightarrow{E_{C_A}}$			
	$\xleftarrow{\hat{E}_{C_B}}$	$\hat{E}_{C_B} \leftarrow \text{Enc}_{K_Z}(C_B^{old})$		
$\text{start}(clk1)$	$\xrightarrow{X}$	$C_A \leftarrow \text{Dec}_{K_A}(E_{C_A})$		
		$\hat{E}_{C_A} \leftarrow \text{Enc}_{K_Z}(C_A)$	$\xrightarrow{\hat{E}_{C_A}}$	
			$\xleftarrow{E_{C_B}}$	$C_B \leftarrow \text{record}()$
			$\xrightarrow{Z}$	$\text{listen}(C_A)$
		$R_B \leftarrow \text{Dec}_{K_B}(E_{R_B})$	$\xleftarrow{E_{R_B}\vert\vert Y}$	$R_B \leftarrow \text{record}()$
$t_a \leftarrow \text{stop}(clk1)$	$\xleftarrow{\hat{E}_{R_B}\vert\vert Z}$	$\hat{E}_{R_B} \leftarrow \text{Enc}_{K_Z}(R_B)$		
check $t_a, \hat{C}_B, \hat{R}_B$				
output: Bob, K_{AZ}				**output**: K_{BZ}

- $t_a = |C_B| + |C_A| + |R_B| + \delta \geq 3T + \delta$

Distance Bounding-based

Beth-Desmedt idea (1990), formalized by Brands-Chaum (1993):

- Successive 1-bit challenge-response
- Measure the round trip time (RTT)
- Deduce the maximal distance
- Hypothesis: computation time negligible

$\mathcal{P}$		$\mathcal{V}$
$\forall i \in 1..k\ \beta_i \in_R \{0,1\}$		$\forall i \in 1..k\ \alpha_i \in_R \{0,1\}$
	Begin of rapid exchange	
	$\xleftarrow{\alpha_i}$	
	$\xrightarrow{\beta_i}$	
	End of rapid exchange	

Possible attacks:

- Mafia fraud, man-in-the-middle ($\mathcal{P}' + \mathcal{V}'$)
- Adversary sends bits out too soon

Preventing Both Types of Frauds

- Commit on a message m
- Response depends on the challenge (can not be sent too soon)
- Signature (no mafia fraud)

$\mathcal{P}$		$\mathcal{V}$
$\forall i \in 1..k \;\; m_i \in_R \{0,1\}$		$\forall i \in 1..k \;\; \alpha_i \in_R \{0,1\}$
$(c,d) \leftarrow \text{commit}(m_1 \| \cdots \| m_k)$	$\xrightarrow{c}$	
	Begin of rapid exchange	
	$\xleftarrow{\alpha_i}$	
$\beta_i \leftarrow \hat{\alpha}_i \oplus m_i$	$\xrightarrow{\beta_i}$	$\hat{m}_i \leftarrow \hat{\beta}_i \oplus \alpha_i$
	End of rapid exchange	
$\gamma \leftarrow \alpha_1 \| \beta_1 \| \cdots \| \alpha_k \| \beta_k$		
$\sigma \leftarrow \text{sign}(\gamma)$	$\xrightarrow{d \| \sigma}$	$\gamma \leftarrow \alpha_1 \| \hat{\beta}_1 \| \cdots \| \alpha_k \| \hat{\beta}_k$
		check $(c,d) = \text{commit}(\hat{m}_1 \| \cdots \| \hat{m}_k)$
		check signature $\hat{\sigma}$

- Signature $\longrightarrow$ prior exchanged key?

A Key Agreement Protocol

Cagalj-Capkun-Hubaux idea (2005):

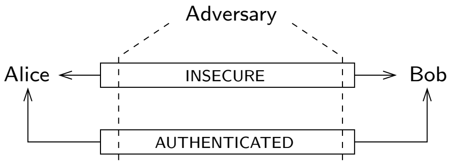
- Based on the Brands-Chaum distance bounding
- Uses Diffie-Hellman values
- Authentication
  - without signature
  - by checking *Integrity area* (done by the user)
- *Integrity area* is considered as an authenticated channel
  - MITM attack prevented

Distance bounding applications:

- Device pairing, RFID (close)
- NOT worldwide

Generic Attacks

Channels model



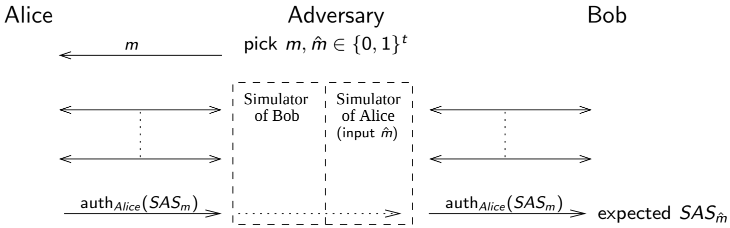
Consider any authentication protocol

- using an authenticated channel
- either interactive or non-interactive

Let k be the bit-length of the authenticated string.

Generic One-shot Attack

The following MITM attack works:



Success probability:

$$\Pr[\text{success}] \geq \Pr[SAS_m = SAS_{\hat{m}}] - \Pr[m = \hat{m}]$$
$$\geq 2^{-k} - 2^{-t}$$

k: bit-length of the authenticated strings
t: bit-length of the message

Generic One-shot Attack

Theorem 1

For any message authentication protocol using an authenticated channel, there exists a generic one-shot attack s.t.

$$\Pr[\text{success}] \geq 2^{-k} - 2^{-t}$$

There does not exist any protocol s.t

$\Pr[\text{success}] < 2^{-k}$

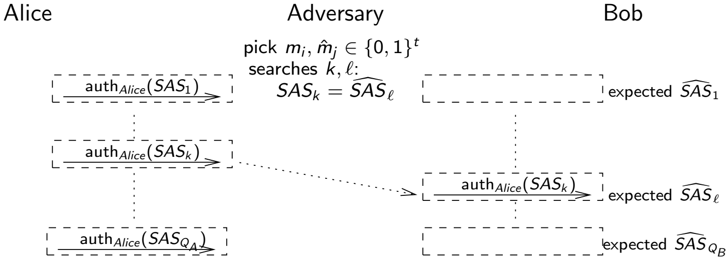
Bound reached → the protocol is *optimal*.

k: bit-length of the authenticated string

t: bit-length of the message

Generic Multi-shot Attack

Using several instances:



Notes:

- Lowest collision probability: when D is uniform
- Weak authentication (delay): $Q_A Q_B$ compatible pairs

$$\begin{aligned}\Pr[\text{success}] &\geq \Pr[\exists\, i,j \text{ s.t. } SAS_i = \widehat{SAS}_j] - \Pr[\exists\, i,j \text{ s.t. } m_i = \hat{m}_j] \\ &\approx 1 - e^{-\frac{Q_A Q_B}{2^k}} - Q_A Q_B 2^{-t}\end{aligned}$$

Generic Multi-shot Attack

Theorem 2

For any message authentication protocol using a weak authenticated channel, there exists a generic attack s.t.

$$\Pr[\text{success}] \approx 1 - e^{-\frac{Q_A Q_B}{2^k}}.$$

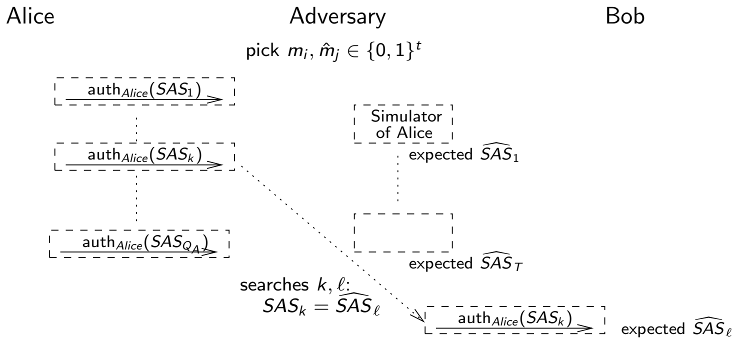
No protocol can remain secure when
$Q_A Q_B$ is non negligible against 2^k

Security level reached → the protocol is *optimal*.

k: bit-length of the authenticated string
t: bit-length of the message
$Q_\cdot$: number of instances used for Alice or Bob

Generic Attack against NIMAP

Instances of Bob can be simulated.



Success probability:

$$\Pr[\text{success}] \approx 1 - e^{-\frac{T \cdot Q_A}{2^k}}$$

Generic Attack against NIMAP

Theorem 3

For any NIMAP which uses a weak authenticated channel, there exists a generic attack s.t.

$$\Pr[\text{success}] \approx 1 - e^{-\frac{T \cdot Q_A}{2^k}}$$

No protocol can remain secure when
$T \cdot Q_A$ is non negligible against 2^k

Security level reached → the protocol is *optimal*.

k: bit-length of the authenticated string
Q_A: number of instances of Alice
T : time complexity

Generic Attacks Overview

Generic attacks exist:

Theorem 1: one-shot attacks against *any* MAP
which use an authenticated channel
with $\Pr[\text{success}] = \mathcal{O}\left(\frac{1}{2^k}\right)$

Theorem 2: multi-shot attacks against *any* MAP
which use a weak authenticated channel
with $\Pr[\text{success}] \approx 1 - e^{-\frac{Q_A Q_B}{2^k}}$

Theorem 3: multi-shot attacks against *any* **NI**MAP
which use a weak authenticated channel
with $\Pr[\text{success}] \approx 1 - e^{-\frac{T \cdot Q_A}{2^k}}$

k: bit-length of the authenticated string
$Q_.$: number of instance used of Alice or Bob
T: offline complexity

Security Analysis of the Usual Protocol

- Formalized by Balfanz et al.
- Used in SSH, GPG, ...
- Based on a collision-resistant hash function

Alice		Bob
input: m		
	$\xrightarrow{\quad m \quad}$	$\hat{h} \leftarrow \mathrm{H}(\hat{m})$
$h \leftarrow H(m)$	$\xrightarrow{\text{authenticate}_{Alice}(h)}$	check $h = \hat{h}$
		output: $Alice, \hat{m}$

- Authenticated values are foreseeable given m, i.e. $H(m)$
- Vulnerable to collision attacks:
  - $\longrightarrow$ collision resistance requires 160 bits
  - $\longrightarrow$ attack complexity $\mathcal{O}(2^{80})$

Proposed Protocol: Idea

The proposed idea

Avoid being able to predict the authenticated message

Our protocol is based on

- a commitment scheme
- a hash function

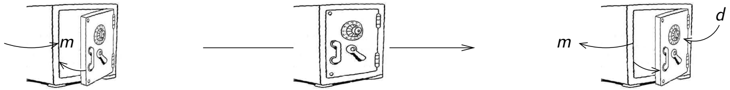
Given an input message m:

1. use a commitment scheme (not deterministic)
2. reveal commit and decommit values: (c, d)
   - given (c, d), everyone can recover m (deterministic)
3. authenticate the hash of c
   - c is not foreseeable, thus $H(c)$ neither

Commitment Schemes

A commitment is like a locked combination safe:

- When Alice wants to commit on a message m: she places m inside the safe and closes it.
- The safe is the commit object c: it can be given to Bob.
- When Alice wants to reveal m: gives the combination d.



Must be hiding:

m cannot be known before c is opened

Must be binding:

m cannot be modified after c is closed

Commitment Schemes, More Formally

There are two algorithms:

- $(c, d) \leftarrow \text{commit}(m)$
- $m \leftarrow \text{open}(c, d)$

Keyed commitment schemes have a third algorithm:

- $(K_p, K_s) \leftarrow \text{setup}()$
  can be in the CRS model

Completeness property:

for any (K_p, K_s), any m, and any $(c, d) \leftarrow \text{commit}(m)$,
we have $m = \text{open}(c, d)$

Commitment Schemes, Binding Property

Binding property:

for any (K_p, K_s), any m, and any $(c, d) \leftarrow \text{commit}(m)$,
it is impossible to find d' s.t. $m' \neq m$
where $m' \leftarrow \text{open}(c, d')$

A commitment scheme is (T, ϵ)-binding if
a T-adversary wins the following game with $\Pr[\text{success}] \leq \epsilon$.

$\mathcal{A}$		$\mathcal{C}$
	$\xleftarrow{K_p}$	$(K_p, K_s) \leftarrow \text{setup}()$
select c, d, d'	$\xrightarrow{c\|\|d\|\|d'}$	$m \leftarrow \text{open}(K_p, c, d)$
		$m' \leftarrow \text{open}(K_p, c, d')$

Winning condition: $m, m' \neq \perp$ and $m' \neq m$

Trapdoor Commitment Schemes

They have an additional algorithm: $d \leftarrow \textbf{equivocate}(K_s, m, c)$

$\longrightarrow$ defeats the binding property using K_s

Properties:

- Commitment

  setup-commit-open algorithms form a (T, ϵ)-commitment scheme

- Trapdoor

  for any (K_p, K_s), any m,

  $$(c, d) \leftarrow \text{commit}(K_p, m)$$

  and

  $$\left(c \in_U \mathcal{C}, d \leftarrow \text{equivocate}(K_s, m, c)\right)$$

  are indistinguishable.

Proposed Protocol

Appears to CT-RSA 2006 (Pasini-Vaudenay):

$$
\begin{array}{rcl}
K_p & & K_p \\
\downarrow & & \downarrow \\
\text{Alice} & & \text{Bob} \\
\textbf{input}:\ m & & \\
(c,d) \leftarrow \mathsf{commit}(K_p, m) & \xrightarrow{\quad c||d \quad} & \hat{m} \leftarrow \mathsf{open}(K_p, \hat{c}, \hat{d}) \\
h \leftarrow H(c) & \xrightarrow{\mathsf{authenticate}_{Alice}(h)} & \text{check } h = H(\hat{c}) \\
 & & \textbf{output}:\ Alice, \hat{m}
\end{array}
$$

Security Proof

Adversaries play the following game:

$K_p \downarrow$ Alice	$K_p \downarrow$ $\mathcal{A}$	$K_p \downarrow$ Bob
	$\xleftarrow{m}$	
$(c, d) \leftarrow \text{commit}(K_p, m)$	$\xrightarrow{c\|\|d}$ $\quad$ $\xrightarrow{\hat{c}\|\|\hat{d}}$	$\hat{m} \leftarrow \text{open}(K_p, \hat{c}, \hat{d})$
$h \leftarrow H(c)$	$\xrightarrow{h}$	

Winning condition: $H(\hat{c}) = h$ and $\hat{m} \neq m$

Reduced game:

$\mathcal{A}$		$\mathcal{C}$
	$\xleftarrow{K_p}$	$(K_p, K_s) \leftarrow \text{setup}()$
	$\xrightarrow{m}$	
	$\xleftarrow{c\|\|d}$	$(c, d) \leftarrow \text{commit}(K_p, m)$
	$\xrightarrow{\hat{c}\|\|\hat{d}}$	$\hat{m} \leftarrow \text{open}(K_p, \hat{c}, \hat{d})$

Winning condition: $H(\hat{c}) = H(c)$ and $m \neq \hat{m}$

Security Proof ($\hat{c} = c$)

Reduction to the binding game:

We use an algorithm $\mathcal{B}$ bounded by the complexity μ

$\mathcal{A}$		$\mathcal{B}$		$\mathcal{C}$
	$\xleftarrow{K_p}$		$\xleftarrow{K_p}$	$(K_p, K_s) \leftarrow \text{setup}()$
	$\xrightarrow{m}$			
	$\xleftarrow{c\|\|d}$	$(c, d) \leftarrow \text{commit}(K_p, m)$		
$(\hat{c} = c)$	$\xrightarrow{\hat{c}\|\|\hat{d}}$		$\xrightarrow{c\|\|d\|\|\hat{d}}$	$m \leftarrow \text{open}(K_p, c, d)$
				$\hat{m} \leftarrow \text{open}(K_p, c, \hat{d})$

Winning condition: $\hat{m}, m \neq \perp$ and $\hat{m} \neq m$

- $\mathcal{B}$ simulates a challenger for $\mathcal{A}$
- $\mathcal{B}$ plays the binding game
- $\mathcal{A}$ and $\mathcal{AB}$ win at the same time
  - $\longrightarrow$ same probability of success ϵ_c

Security Proof ($\hat{c} \neq c$)

Reduction to the weakly collision resistant (WCR) game:

We use an algorithm $\mathcal{B}$ bounded by complexity μ

One equivocate query is allowed

$\mathcal{A}$		$\mathcal{B}$		$\mathcal{C}$
	$\xleftarrow{K_p}$	$(K_p, K_s) \leftarrow \text{setup}()$		
	$\xrightarrow{m}$			
			$\xleftarrow{c}$	pick $c \in_U \mathcal{C}$
	$\xleftarrow{c\|\|d}$	$d \leftarrow \text{equivocate}(K_s, m, c)$		
	$\xrightarrow{\hat{c}\|\|\hat{d}}$	$\hat{m} \leftarrow \text{open}(K_p, \hat{c}, \hat{d})$		
			$\xrightarrow{\hat{c}}$	

Winning condition: $H(\hat{c}) = H(c)$ and $m \neq \hat{m}$

- $\mathcal{B}$ simulates a challenger for $\mathcal{A}$
- $\mathcal{B}$ plays the WCR game
- $\mathcal{A}$ and $\mathcal{AB}$ win at the same time
  - $\longrightarrow$ same probability of success ϵ_h

Security Proof (end)

Lemma

Assuming

- any one-shot adversaries $\mathcal{A}$ bounded by complexity T
- a $(T + \mu, \epsilon_c)$-trapdoor commitment scheme
- a $(T + \mu, \epsilon_h)$-weakly collision resistant hash function H

There exists μ s.t. $\mathcal{A}$ win with $p \leq \epsilon_c + \epsilon_h$

Powerful Attacks

Theorem 4

Assuming

- any adversaries $\mathcal{A}$ bounded by
  - complexity T
  - Q_A instances of Alice
- a $(T + \mu, \epsilon_c)$-trapdoor commitment scheme
- a $(T + \mu, \epsilon_h)$-weakly collision resistant hash function H

There exists μ s.t. $\mathcal{A}$ win with $p \leq Q_A(\epsilon_c + \epsilon_h)$.

Comparison with the Usual Protocol

Proposed protocol: $\Pr[\text{success}] \leq Q_A(\epsilon_c + \epsilon_h)$

Note:

- c sent over the broadband channel,
  c can be long,
  ϵ_c can be as small as desired
- h sent over the authenticated channel,
  h must be as short as possible

Assuming that H is optimally WCR:

attack complexity $T = \Omega(2^k)$

The usual protocol has $T = \Omega(2^{k/2})$.

With equal SAS length, our protocol is more secure

Optimality of the Proposed Protocol

If WCRHF and TC s.t. $\epsilon_c \ll \epsilon_h = \mathcal{O}(T2^{-k})$ exist, we have $p = \mathcal{O}(Q_A \cdot T2^{-k})$.

Optimal in the sense of Theorem 3.

Example with an adversary bounded by

$$Q_A \leq 2^{10}, \qquad T \leq 2^{70}$$

and with $p \leq 2^{-20}$

$\longrightarrow$ The usual protocol requires 160 bits.

$\longrightarrow$ The proposed protocol requires 100 bits.

The Vaudenay SAS-based Protocol

Published at Crypto '05

Alice		Bob
input: m		
pick $R_A \in_U \{0,1\}^k$		pick $R_B \in_U \{0,1\}^k$
$(c,d) \leftarrow \text{commit}(m \| R_A)$	$\xrightarrow{m\|\|c}$	
	$\xleftarrow{R_B}$	
	$\xrightarrow{d}$	$\hat{R}_A \leftarrow \text{open}(\hat{m}, \hat{c}, \hat{d})$
$\text{SAS} \leftarrow R_A \oplus \hat{R}_B$	$\xrightarrow{\text{authenticate}_{Alice}(\text{SAS})}$	check $\text{SAS} = \hat{R}_A \oplus R_B$
		output: $Alice, \hat{m}$

This protocol allows very short SAS, e.g. 15 bits

A proposed application: a P2P file authentication

Demonstrations

We will authenticate the same public key twice:

- using an interactive protocol:

  the Vaudenay SAS-based protocol

- using a non-interactive protocol:

  the just proposed protocol

Differences:

- Usability?
- SAS length?

Interactivity vs. Non-Interactivity

	Interactive	Non-interactive
Usability	Shorter SAS	Asynchronous
Security		Offline attacks
Cost	Shorter SAS	
Complexity		

As expected, it depends on the application

- Interactivity: well adapted to devices pairing
- SSH, PGP, GPG: non-interactive is better
- PGPfone: we already have interactivity

Conclusion

- Three generic attacks against authentication protocols
  - bound the security of any protocol
- New proposed non-interactive protocol
  - compared to the usual protocol
    $\longrightarrow$ better security using less authenticated bits
- New applications
  - an interactive P2P file authentication
  - a non-interactive file authentication

Further work:

- Biometrics-based protocols