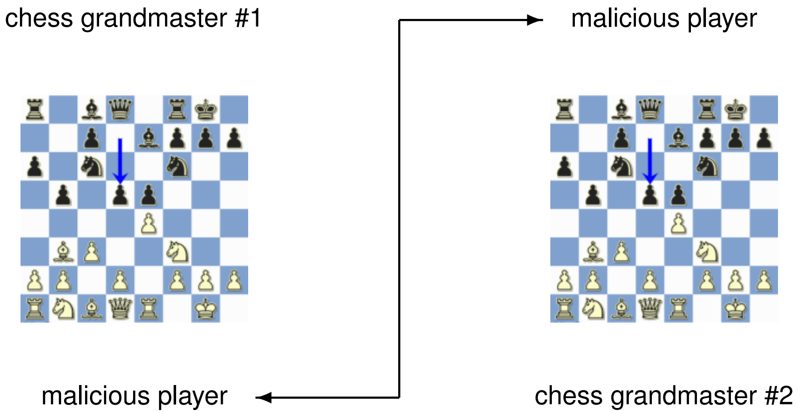
Towards Secure Distance Bounding

Ioana Boureanu, Katerina Mitrokotsa, Serge Vaudenay

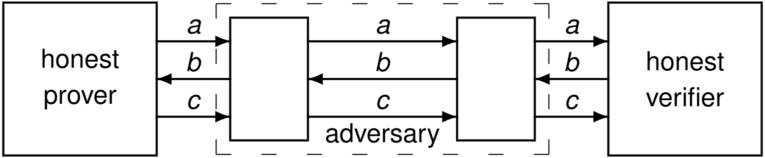
ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

http://lasec.epfl.ch/

Playing against two Chess Grandmasters

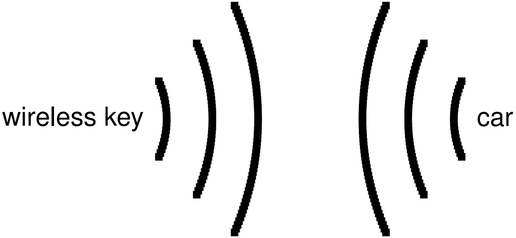


Relay Attacks



A Nice Playground for Relay Attacks

Wireless Car Locks



A Nice Playground for Relay Attacks

Corporate RFID Card for Access Control

A Nice Playground for Relay Attacks

Contactless Credit Card Payment

wireless credit card payment

The Brands-Chaum Protocol

Distance-Bounding Protocols [Brands-Chaum EUROCRYPT 1993]

Verifier		Prover
public key: y		secret key: x
	initialization phase	
	$\xleftarrow{\text{Commit}(m)}$	pick m
	distance bounding phase	
	for $i = 1$ to n	
pick c_i		
start clock	$\xrightarrow{c_i}$	
stop clock	$\xleftarrow{r_i}$	$r_i = m_i \oplus c_i$
check timers		
	termination phase	
check responses	$\xleftarrow{\text{open commitment}}$	
check signature	$\xleftarrow{\text{Sign}_x(c,r)}$	
	$\xrightarrow{\text{Out}_V}$	

The Speed of Light

time error of $1\mu s$ = distance error of 300m

Distance Bounding

- **interactive proof** for proximity
  a verifier (honest)
  a prover (may be malicious)
  a secret to characterize the prover (may be symmetric)
  concurrency: many provers and verifiers around, plus malicious participants
- **completeness**:
  if the honest prover is close to the verifier, the verifier accepts
- **soundness**:
  if the verifier accept, then a close participant must hold the secret
- **secure**:
  when honestly run, the secret must not leak

Distance Fraud

$$\underbrace{P^* \longleftrightarrow V}_{\text{far away}}$$

a malicious prover P^* tries to prove that he is close to a verifier V

Mafia Fraud

Major Security Problems with the “Unforgeable” (Feige)-Fiat-Shamir Proofs of Identity and How to Overcome Them [Desmedt SECURICOM 1988]

$$\underbrace{P \longleftrightarrow \mathcal{A} \longleftrightarrow V}_{\text{far away}}$$

an adversary $\mathcal{A}$ tries to prove that a prover P is close to a verifier V

Terrorist Fraud

Major Security Problems with the "Unforgeable" (Feige)-Fiat-Shamir Proofs of Identity and How to Overcome Them [Desmedt SECURICOM 1988]

$$\underbrace{P^* \longleftrightarrow \mathcal{A} \longleftrightarrow V}_{\text{far away}}$$

a malicious prover P^* helps an adversary $\mathcal{A}$ to prove that P^* is close to a verifier V without giving $\mathcal{A}$ another advantage

Impersonation Fraud

An Efficient Distance Bounding RFID Authentication Protocol
[Avoine-Tchamkerten ISC 2009]

$$\mathcal{A} \longleftrightarrow V$$

an adversary $\mathcal{A}$ tries to prove that a prover P is close to a verifier V

Distance Hijacking

Distance Hijacking Attacks on Distance Bounding Protocols
[Cremers-Rasmussen-Schmidt-Čapkun IEEE S&P 2012]

$$\underbrace{P^* \longleftrightarrow P' \longleftrightarrow V}_{\text{far away}}$$

a malicious prover P^* tries to prove that he is close to a verifier V by taking advantage of other provers P'

A General Threat Model

- **distance fraud**:
  - $P(x)$ far from all $V(x)$'s want to make one $V(x)$ accept (interaction with other $P(x')$ and $V(x')$ possible anywhere)
  - $\rightarrow$ also captures distance hijacking
- **man-in-the-middle**:
  - *learning phase*: $\mathcal{A}$ interacts with many P's and V's
  - *attack phase*: $P(x)$'s far away from $V(x)$'s, $\mathcal{A}$ interacts with them and possible $P(x')$'s and $V(x')$'s
    $\mathcal{A}$ wants to make one $V(x)$ accept
  - $\rightarrow$ also captures impersonation
- **collusion fraud**:
  - $P(x)$ far from all $V(x)$'s interacts with $\mathcal{A}$ and makes one $V(x)$ accept, but $\text{View}(\mathcal{A})$ does not give any advantage to mount a man-in-the-middle attack

Known Protocols and Security Results

success probability of best known "regular" attacks
(TF with no tolerance to noise + no malicious PRF)

Protocol	Success Probability		
	Distance-Fraud	MiM	Collusion-Fraud
Brands & Chaum	$(1/2)^n$	$(1/2)^n$	1
Bussard & Bagga	1	$(1/2)^n$	1
Čapkun *et al.*	$(1/2)^n$	$(1/2)^n$	1
Hancke & Kuhn	$(3/4)^n$	$(3/4)^n$	1
Reid *et al.*	$(3/4)^n$	1	$(3/4)^\nu$
Singelée & Preneel	$(1/2)^n$	$(1/2)^n$	1
Tu & Piramuthu	$(3/4)^n$	1	$(3/4)^\nu$
Munilla & Peinado	$(3/4)^n$	$(3/5)^n$	1
Swiss-Knife	$(3/4)^n$	$(1/2)^n$	$(3/4)^\nu$
Kim & Avoine	$(7/8)^n$	$(1/2)^n$	1
Nikov & Vauclair	$1/k$	$(1/2)^n$	1
Avoine *et al.*	$(3/4)^n$	$(2/3)^n$	$(2/3)^\nu$

The Hancke-Kuhn Protocol

An RFID Distance-Bounding Protocol [Hancke-Kuhn SECURECOMM 2005]

Verifier		Prover
secret: x		secret: x
	initialization phase	
pick N_V	$\xrightarrow{N_V}$	
	$\xleftarrow{N_P}$	pick N_P
$a_1 \| a_2 = f_x(N_P, N_V)$		$a_1 \| a_2 = f_x(N_P, N_V)$
	distance bounding phase	
	for $i = 1$ to n	
pick $c_i \in \{1, 2\}$		
start clock	$\xrightarrow{c_i}$	
stop clock	$\xleftarrow{r_i}$	$r_i = \begin{cases} a_{1,i} & \text{if } c_i = 1 \\ a_{2,i} & \text{if } c_i = 2 \end{cases}$
check responses		
check timers	$\xrightarrow{\text{Out}_V}$	

A Terrorist Fraud against The Hancke-Kuhn Protocol

Verifier secret: x		**Adversary**		**Malicious Prover** secret: x
		initialization phase		
pick N_V	$\xrightarrow{N_V}$		$\xrightarrow{N_V}$	pick N_P
$a_1 \| a_2 = f_x(N_P, N_V)$	$\xleftarrow{N_P}$		$\xleftarrow{N_P, a_1, a_2}$	$a_1 \| a_2 = f_x(N_P, N_V)$
		distance bounding phase for $i = 1$ to n		
pick $c_i \in \{1, 2\}$				
start clock	$\xrightarrow{c_i}$			
stop clock	$\xleftarrow{r_i}$	$r_i = a_{c_i,i}$		
check responses				
check timers	$\xrightarrow{\text{Out}_V}$			

The Reid et al. Protocol (DBENC)

Detecting Relay Attacks with Timing-based Protocols [Reid-Nieto-Tang-Senadji ASIACCS 2007]

Verifier secret: x		Prover secret: x
	initialization phase	
pick N_V	$\xrightarrow{N_V}$	pick N_P
$a_1 = f_x(N_P, N_V)$	$\xleftarrow{N_P}$	$a_1 = f_x(N_P, N_V)$
$a_2 = a_1 \oplus x$		$a_2 = a_1 \oplus x$
	distance bounding phase	
	for $i = 1$ to n	
pick $c_i \in \{1,2\}$		
start clock	$\xrightarrow{c_i}$	
stop clock	$\xleftarrow{r_i}$	$r_i = a_{c_i,i}$
check responses		
check timers	$\xrightarrow{\text{Out}_V}$	

resist to terrorist fraud: if a_1 and a_2 leak, then x as well!

A Man-in-the-Middle against DBENC

The Swiss-Knife RFID Distance Bounding Protocol
[Kim-Avoine-Koeune-Standaert-Pereira ICISC 2008]

Verifier		**Adversary**		**Prover**
secret: x				secret: x
		initialization phase		
pick N_V	$\xrightarrow{N_V}$	select j, b	$\xrightarrow{N_V}$	pick N_P
$a = f_x(N_P, N_V)$	$\xleftarrow{N_P}$		$\xleftarrow{N_P}$	$a = f_x(N_P, N_V)$
		distance bounding phase		
		for $i = 1$ to n		
pick $c_i^* \in \{1,2\}$				
start clock	$\xrightarrow{c_i^*}$	$c_i = c_i^* \oplus 1_{i=j}$	$\xrightarrow{c_i}$	
stop clock	$\xleftarrow{r_i^*}$	$r_i^* = r_i \oplus b.1_{i=j}$	$\xleftarrow{r_i}$	$r_i = a_i \oplus x_i.1_{c_i=2}$
check responses				
check timers	$\xrightarrow{\text{Out}_V}$			

fact 1: r_j is the correct response to c_j

fact 2: $\text{Out}_V = 1$ iff r_j^* is the correct response to $c_j \oplus 1$

consequence: the adversary deduces a_j and $a_j \oplus x_j$, so x_j as well

A Man-in-the-Middle against Other DBENC

The Bussard-Bagga and Other Distance-Bounding Protocols under Attacks
[Bay-Boureanu-Mitrokotsa-Spulber-Vaudenay Inscrypt 2012]

set $a_2 = \mathrm{Enc}_{a_1}(x)$

- **one-time pad**: $\mathrm{Enc}_{a_1}(x) = x \oplus a_1$
- **addition modulo** q: $\mathrm{Enc}_{a_1}(x) = x - a_1 \bmod q$
- **modular addition with random factor**:
  $\mathrm{Enc}_{a_1}(x; u) = (u, ux - a_1 \bmod q)$
  for a random invertible u

all instances broken

The TDB Protocol

How Secret-Sharing can Defeat Terrorist Fraud
[Avoine-Lauradoux-Martin ACM WiSec 2011]

Verifier		**Prover**
secret: x		secret: x
	initialization phase	
	$\xleftarrow{N_P}$	pick N_P
pick N_V	$\xrightarrow{N_V}$	
$a_1 \| a_2 = f_x(N_P, N_V)$		$a_1 \| a_2 = f_x(N_P, N_V)$
	distance bounding phase	
	for $i = 1$ to n	
pick $c_i \in \{1,2,3\}$		
start clock	$\xrightarrow{c_i}$	
stop clock	$\xleftarrow{r_i}$	$r_i = \begin{cases} a_{1,i} & \text{if } c_i = 1 \\ a_{2,i} & \text{if } c_i = 2 \\ x_i \oplus a_{1,i} \oplus a_{2,i} & \text{if } c_i = 3 \end{cases}$
check responses		
check timers	$\xrightarrow{\text{Out}_V}$	

resist to man-in-the-middle: two answers to c_i don't leak x_i!

Security Proofs Based on PRF

- if the adversary can break the scheme with a PRF, then he can break an idealized scheme with the PRF replaced by a truly random function
- this argument is valid when both these conditions are met:
  - the adversary does not have access to the PRF key
  - the PRF key is only used by the PRF
- as far as distance fraud is concerned, condition 1 is not met!
- for most of terrorist fraud protections, condition 2 is not met!

Programming a PRF

On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols [Boureanu-Mitrokotsa-Vaudenay Latincrypt 2012]

given a PRF g, let

$$f_x(N_P, N_V) = \begin{cases} x\|x & \text{if } N_P = x \\ g_x(N_P, N_V) & \text{otherwise} \end{cases}$$

f is a PRF!

Distance Fraud with a Programmed PRF against the TDB Protocol

On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols [Boureanu-Mitrokotsa-Vaudenay Latincrypt 2012]

Verifier		Malicious Prover
secret: x		secret: x
	initialization phase	
	$\xleftarrow{N_P}$	pick $N_P = x$
pick N_V	$\xrightarrow{N_V}$	
$a_1 \| a_2 = f_x(N_P, N_V)$	$a_1 = a_2 = x$	$a_1 \| a_2 = f_x(N_P, N_V)$
	distance bounding phase	
	for $i = 1$ to n	
pick $c_i \in \{1, 2, 3\}$		
start clock		$r_i = x_i$
	c_i → / ← r_i	
stop clock		
check responses		
check timers	$\xrightarrow{\text{Out}_V}$	

Using PRF Masking

Verifier		Prover
secret: x		secret: x
	initialization phase	
pick a, N_V	$\xleftarrow{N_P}$	pick N_P
$M = a \oplus f_x(N_P, N_V)$	$\xrightarrow{M,N_V}$	$a = M \oplus f_x(N_P, N_V)$
	distance bounding phase	
	for $i = 1$ to n	
pick $c_i \in \{1,2,3\}$		
start clock	$\xrightarrow{c_i}$	
stop clock	$\xleftarrow{r_i}$	$r_i = \begin{cases} a_{1,i} & \text{if } c_i = 1 \\ a_{2,i} & \text{if } c_i = 2 \\ x_i \oplus a_{1,i} \oplus a_{2,i} & \text{if } c_i = 3 \end{cases}$
check responses		
check timers	$\xrightarrow{\text{Out}_V}$	

a is now chosen by the verifier

Man-in-the-Middle Attack with a Programmed PRF

On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols [Boureanu-Mitrokotsa-Vaudenay Latincrypt 2012]

- take a PRF g
- define a predicate $\text{trapdoor}_x(\bar{\alpha}\|t) \iff t = g_x(\bar{\alpha}) \oplus \text{right\_half}(x)$,

$$f_x(N_P, N_V) = \begin{cases} a_1\|a_2 = \alpha\|\beta\|\gamma\|\beta \oplus g_x(\alpha) & \text{if } \neg\text{trapdoor}_x(N_V) \\ & \text{where } (\alpha,\beta,\gamma) = g_x(N_P, N_V) \\ a_1 = a_2 = x & \text{otherwise} \end{cases}$$

  f is a PRF!
- attack:
  1: play with P and send $c = (1,\ldots,1,3,\ldots,3)$ to obtain from the responses $\bar{\alpha}\|t$ satisfying trapdoor_x
  2: play with P again with $N_V = \bar{\alpha}\|t$ and get x!

Other Results based on Programmed PRFs

On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols [Boureanu-Mitrokotsa-Vaudenay Latincrypt 2012]

protocol	distance fraud	man-in-the-middle attack
TDB Avoine-Lauradoux-Martin [ACM WiSec 2011]	$\surd$	$\surd$
Dürholz-Fischlin-Kasper-Onete [ISC 2011]	$\surd$	–
Hancke-Kuhn [Securecomm 2005]	$\surd$	–
Avoine-Tchamkerten [ISC 2009]	$\surd$	–
Reid-Nieto-Tang-Senadji [ASIACCS 2007]	$\surd$	$\surd$
Swiss-Knife Kim-Avoine-Koeune-Standaert-Pereira [ICISC 2008]	–	$\surd$

Using Circular-Keying Security

Verifier		**Prover**
secret: x		secret: x
	initialization phase	
pick a, N_V	$\xleftarrow{N_P}$	pick N_P
$M = a \oplus f_x(N_P, N_V)$	$\xrightarrow{M, N_V}$	$a = M \oplus f_x(N_P, N_V)$
	distance bounding phase	
	for $i = 1$ to n	
pick $c_i \in \{1,2,3\}$		
start clock	$\xrightarrow{c_i}$	
stop clock	$\xleftarrow{r_i}$	$r_i = \begin{cases} a_{1,i} & \text{if } c_i = 1 \\ a_{2,i} & \text{if } c_i = 2 \\ x_i \oplus a_{1,i} \oplus a_{2,i} & \text{if } c_i = 3 \end{cases}$
check responses		
check timers	$\xrightarrow{\text{Out}_V}$	

f is a PRF with circular-keying security

Circular Keying Security

- if $\mathcal{A}$ makes queries

$$y_i, a_i, b_i \mapsto (a_i \cdot x') + (b_i \cdot f_x(y_i))$$

  $\mathcal{A}$ cannot distinguish if $x = x'$ or x and x' are independent
- caveat: queries must be such that

$$\forall i_1, \ldots, i_q, c_1, \ldots, c_q \qquad \left.\begin{array}{l} y_{i_1} = \cdots = y_{i_q} \\ \sum_{j=1}^{q} c_j b_{i_j} = 0 \end{array}\right\} \Longrightarrow \sum_{j=1}^{q} c_j a_{i_j} = 0$$

- sanity check: easily constructed in the random oracle model

Problem with Noise

Verifier secret: x		Prover secret: x
	initialization phase	
pick a, N_V	$\xleftarrow{N_P}$	pick N_P
$M = a \oplus f_x(N_P, N_V)$	$\xrightarrow{M, N_V}$	$a = M \oplus f_x(N_P, N_V)$
	distance bounding phase for $i = 1$ to n	
pick $c_i \in \{1,2,3\}$		
start clock	$\xrightarrow{c_i}$	
stop clock	$\xleftarrow{r_i}$	$r_i = \begin{cases} a_{1,i} & \text{if } c_i = 1 \\ a_{2,i} & \text{if } c_i = 2 \\ x_i \oplus a_{1,i} \oplus a_{2,i} & \text{if } c_i = 3 \end{cases}$
check at least τ correct responses		
check timers	$\xrightarrow{\text{Out}_V}$	

Terrorist Fraud based on Tolerance to Noise

Distance Bounding for RFID: Effectiveness of Terrorist Fraud [Hancke IEEE RFID-TA 2012]

Verifier		**Adversary**		**Malicious Prover**
secret: x				secret: x
		initialization phase		
pick a, N_V	$\xleftarrow{N_P}$		$\xleftarrow{N_P}$	pick N_P
$M = a \oplus f_x(N_P, N_V)$	$\xrightarrow{M,N_V}$		$\xrightarrow{M,N_V}$	$a = M \oplus f_x(N_P, N_V)$
			$\xleftarrow{F_i, i \in I}$	$I = g(x)$
		distance bounding phase		
		for $i = 1$ to n		
pick $c_i \in \{1, 2, 3\}$				
start clock	$\xrightarrow{c_i}$			
stop clock	$\xleftarrow{r_i}$	$r_i = F_i^*(c_i)$		
check $\geq \tau$ responses				
check timers	$\xrightarrow{\text{Out}_V}$			

$$F_i(c) = \begin{cases} a_{1,i} & \text{if } c = 1 \\ a_{2,i} & \text{if } c = 2 \\ x_i \oplus a_{1,i} \oplus a_{2,i} & \text{if } c = 3 \end{cases}$$

$\#I = \tau$

$F_i^* = F_i$ if $i \in I$

$F_i^* =$ random otherwise

Why SKI?

- Symmetric Key Infrastructure?
- Sheffield Kidney Institute?
- Serial Killers Incorporated?

Serge Katerina Ioana

The SKI Protocol

Verifier secret: x		Prover secret: x
	initialization phase	
	$\xleftarrow{N_P}$	pick N_P
pick a, L_μ, N_V $M = a \oplus f_x(N_P, N_V, L_\mu)$ $x' = L_\mu(x)$	$\xrightarrow{M, L_\mu, N_V}$	$a = M \oplus f_x(N_P, N_V, L_\mu)$ $x' = L_\mu(x)$
	distance bounding phase for $i = 1$ to n	
pick $c_i \in \{1,2,3\}$ start clock	$\xrightarrow{c_i}$	
stop clock	$\xleftarrow{r_i}$	$r_i = \begin{cases} a_{1,i} & \text{if } c_i = 1 \\ a_{2,i} & \text{if } c_i = 2 \\ x'_i \oplus a_{1,i} \oplus a_{2,i} & \text{if } c_i = 3 \end{cases}$
check $\geq \tau$ responses check timers	$\xrightarrow{\mathrm{Out}_V}$	

f is a circular-keying secure PRF, $L_\mu(x) = (\mu \cdot x, \ldots, \mu \cdot x)$

Completeness of SKI

$$B(n,\tau,q) = \sum_{i=\tau}^{n} \binom{n}{i} q^i (1-q)^{n-i}$$

- assume honest execution of the protocol
- let p_{noise} be the probability that one round is incorrect
- probability to pass is $B(n,\tau,1-p_{\text{noise}})$
- (Chernoff) for $\frac{\tau}{n} < 1 - p_{\text{noise}} - \varepsilon$, this is more than $1 - e^{-2\varepsilon^2 n}$

Best Distance Fraud against SKI

Verifier		**Malicious Prover**
secret: x		secret: x
	initialization phase	
	$\xleftarrow{N_P}$	pick N_P
pick a, L_μ, N_V	$\xrightarrow{M, L_\mu, N_V}$	
$M = a \oplus f_x(N_P, N_V, L_\mu)$		$a = M \oplus f_x(N_P, N_V, L_\mu)$
$x' = L_\mu(x)$		$x' = L_\mu(x)$
	distance bounding phase	
	for $i = 1$ to n	
pick $c_i \in \{1, 2, 3\}$		
start clock		pick r_i with largest preimage by F_i
	c_i (→), r_i (←), crossing	
stop clock		
check $\geq \tau$ responses		
check timers	$\xrightarrow{\text{Out}_V}$	

$$\Pr[\text{round } i \text{ correct}] = \frac{3}{4}$$

Best Distance Fraud against SKI

$$\begin{aligned}\Pr[\text{round } i \text{ correct}] &= \Pr[F_i \text{ constant}] + \frac{2}{3}(1 - \Pr[F_i \text{ constant}]) \\ &= \frac{1}{4} + \frac{2}{3} \times \left(1 - \frac{1}{4}\right) \\ &= \frac{3}{4}\end{aligned}$$

- F_i is a 3-to-2 mapping
  so, the largest preimage has 3 (if F_i is constant) or 2 elements
- it is constant iff $a_{1,i} = a_{2,i} = x_i$, i.e. with probability $\frac{1}{4}$
- probability to pass is $B(n, \tau, \frac{3}{4})$
- (Chernoff) for $\frac{\tau}{n} > \frac{3}{4} + \varepsilon$, this is less than $e^{-2\varepsilon^2 n}$

Best Mafia Fraud against SKI

Verifier		Adversary		Prover
secret: x				secret: x
		initialization phase		
	$\xleftarrow{N_P}$		$\xleftarrow{N_P}$	pick N_P
pick a, L_μ, N_V	$\xrightarrow{M, L_\mu, N_V}$		$\xrightarrow{M, L_\mu, N_V}$	
		distance bounding phase		
		for $i = 1$ to n		
		pick c_i^*		
			$\xrightarrow{c_i^*}$	
			$\xleftarrow{r_i^*}$	$r_i^* = F_i(c_i^*)$
		for $i = 1$ to n		
pick $c_i \in \{1, 2, 3\}$				
start clock	$\xrightarrow{c_i}$			
stop clock	$\xleftarrow{r_i}$	$r_i = r_i^*$		
check $\geq \tau$ responses				
check timers	$\xrightarrow{\text{Out}_V}$			

$$\Pr[\text{round } i \text{ correct}] = \frac{2}{3}$$

Best Mafia Fraud against SKI

$$\begin{aligned} \Pr[\text{round } i \text{ correct}] &= \Pr[c_i = c_i^*] + \frac{1}{2}(1 - \Pr[c_i = c_i^*]) \\ &= \frac{1}{3} + \frac{1}{2} \times \left(1 - \frac{1}{3}\right) \\ &= \frac{2}{3} \end{aligned}$$

- probability to pass is $B(n, \tau, \frac{2}{3})$
- (Chernoff) for $\frac{\tau}{n} > \frac{2}{3} + \varepsilon$, this is less than $e^{-2\varepsilon^2 n}$

Best Terrorist Fraud against SKI

Verifier secret: x		Adversary		Malicious Prover secret: x
		initialization phase		
	$\xleftarrow{N_P}$		$\xleftarrow{N_P}$	pick N_P
pick a, L_μ, N_V	$\xrightarrow{M, L_\mu, N_V}$		$\xrightarrow{M, L_\mu, N_V}$	pick $c_1^*, \ldots, c_n^*$ $F_i^*(c) = F_i(c)$ if $c \neq c_i^*$
			$\xleftarrow{F^*}$	$F_i^*(c) = \text{rnd else}$
		distance bounding phase for $i = 1$ to n		
pick $c_i \in \{1, 2, 3\}$				
start clock	$\xrightarrow{c_i}$			
stop clock	$\xleftarrow{r_i}$	$r_i = F_i^*(c_i)$		
check $\geq \tau$ responses				
check timers	$\xrightarrow{\text{Out}_V}$			

$$\Pr[\text{round } i \text{ correct}] = \frac{5}{6}$$

Best Terrorist Fraud against SKI

$$\begin{aligned} \Pr[\text{round } i \text{ correct}] &= \Pr[c_i \neq c_i^*] + \frac{1}{2}(1 - \Pr[c_i \neq c_i^*]) \\ &= \frac{2}{3} + \frac{1}{2} \times \left(1 - \frac{2}{3}\right) \\ &= \frac{5}{6} \end{aligned}$$

- probability to pass is $B(n, \tau, \frac{5}{6})$
- (Chernoff) for $\frac{\tau}{n} > \frac{5}{6} + \varepsilon$, this is less than $e^{-2\varepsilon^2 n}$

Summary

for

$$p_{\text{noise}} < \frac{1}{6} - 2\varepsilon$$

we can adjust τ and have completeness up to $e^{-2\varepsilon^2 n}$, and security up to $e^{-2\varepsilon^2 n}$

- completeness
- resistance to distance fraud
- resistance to mafia fraud
- resistance to terrorist fraud

SKI Security

Theorem

If f is a circular-keying secure PRF and V requires at least τ correct rounds,

- *there is no DF with* $\Pr[\text{success}] \geq B(n, \tau, \frac{3}{4})$
- *there is no MiM with* $\Pr[\text{success}] \geq B(n, \tau, \frac{2}{3})$
- *for all CF such that* $\Pr[\text{CF succeeds}] \geq B(\frac{n}{2}, \tau - \frac{n}{2}, \frac{2}{3})^{1-c}$ *there is an assosiated MiM with P^* such that* $\Pr[\text{MiM succeeds}] \geq \left(1 - B(\frac{n}{2}, \tau - \frac{n}{2}, \frac{2}{3})^c\right)^n$

$$B(n, \tau, \rho) = \sum_{i=\tau}^{n} \binom{n}{i} \rho^i (1-\rho)^{n-i}$$

Conclusion

- several proposed protocols from the literature are insecure
- several security proofs from the literature are incorrect
- SKI offers provable security