TERRORIST-FRAUD RESISTANT, EXTRACTOR FREE, ANONYMOUS, DISTANCE BOUNDING PROTOCOL

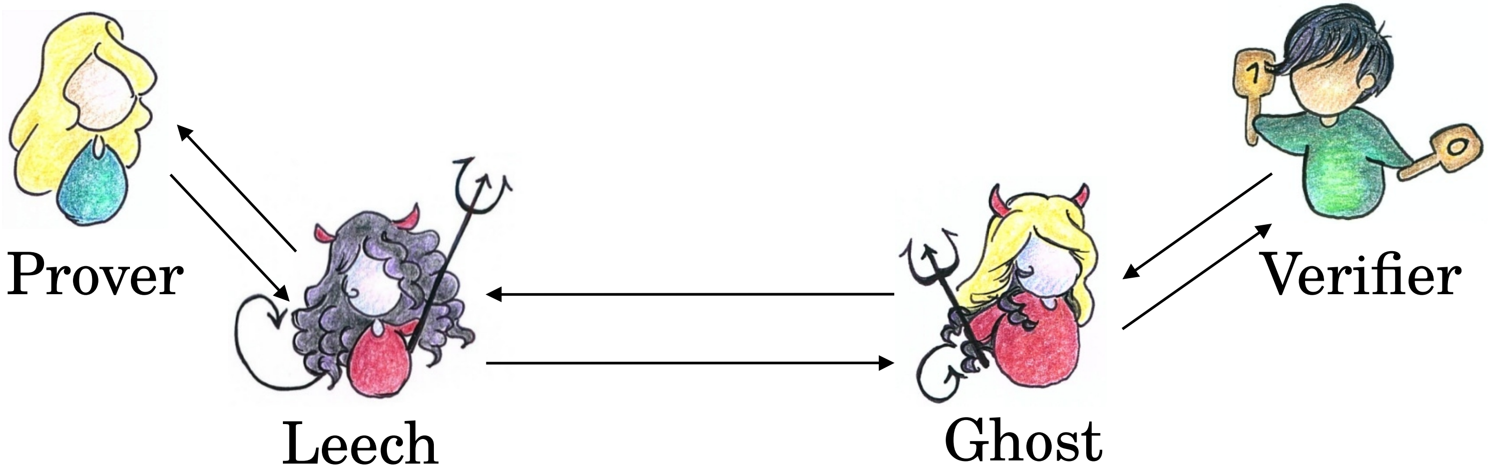
G. AVOINE (INSA/IRISA RENNES)

WITH X. **BULTEL,** D.**GÉRAULT,** P. **LAFOURCADE** (LIMOS/UCA, FRANCE),
S. **GAMBS** (UQAM, CANADA)
C. **ONETE** (UR1, FRANCE)
J.-M. **ROBERT** (ETS MONTRÉAL, CANADA)

CONTENTS

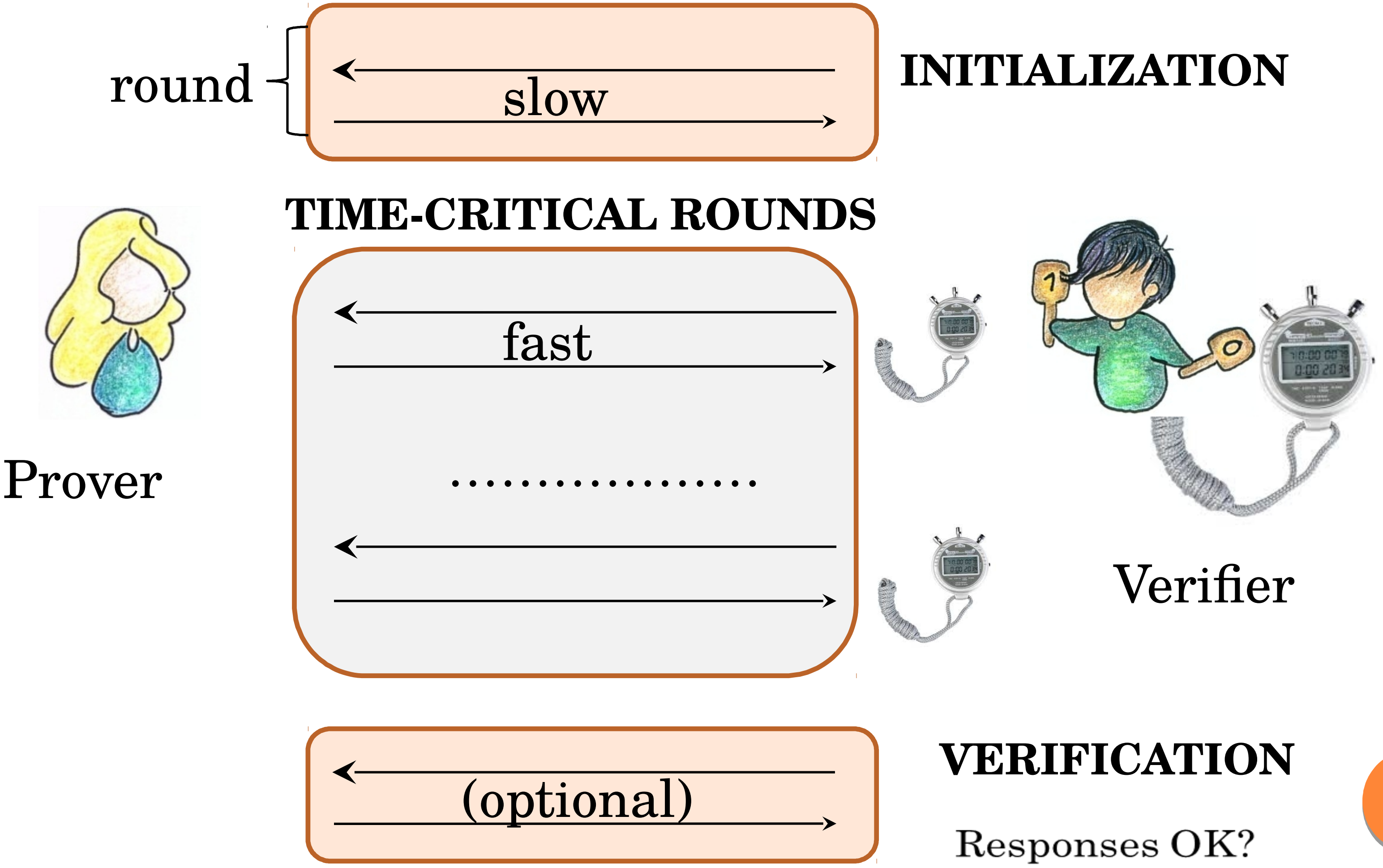
DISTANCE-BOUNDING AUTHENTICATION

- An authentication protocol that thwarts relay attacks



- Relay attacks exploit two main weaknesses:
  - Prover device automatically accepts to run protocol
  - The verifier cannot tell how far the response comes from

DB PROTOCOL STRUCTURE



round

slow

INITIALIZATION

TIME-CRITICAL ROUNDS

fast

....

Prover

Verifier

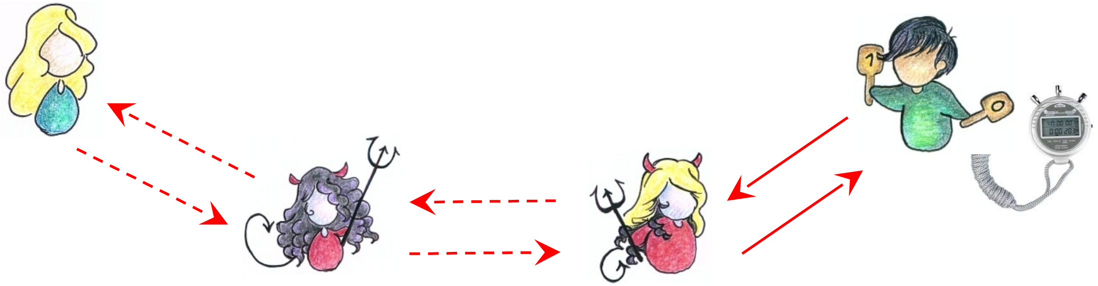
(optional)

VERIFICATION

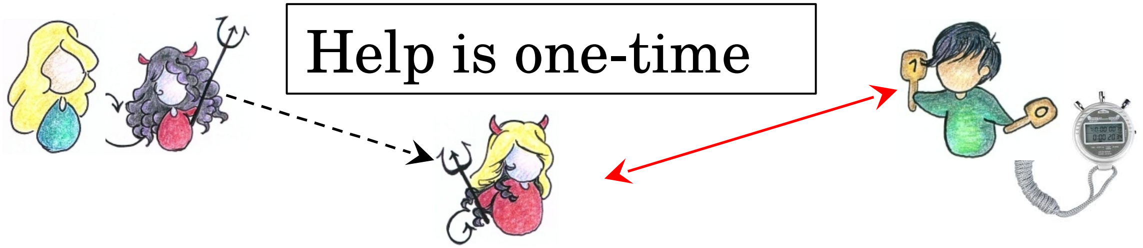
Responses OK?
$\Delta t_i \leq t_{max} \quad \forall i$?

ATTACKS DB SETS OUT TO PREVENT

- Mafia Fraud

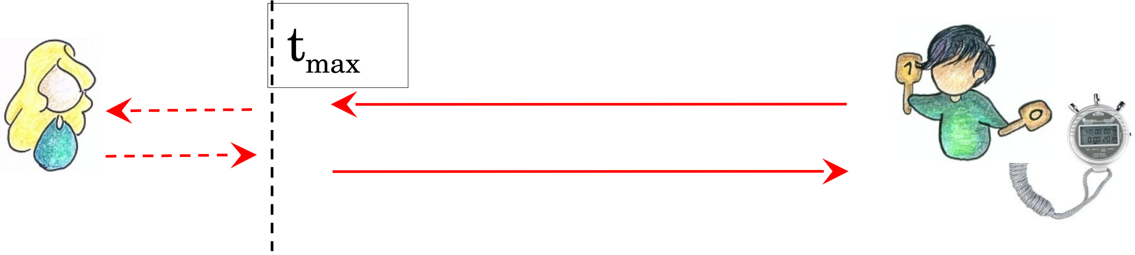


- Terrorist Fraud



Help is one-time

- Distance Fraud



Prover

Verifier

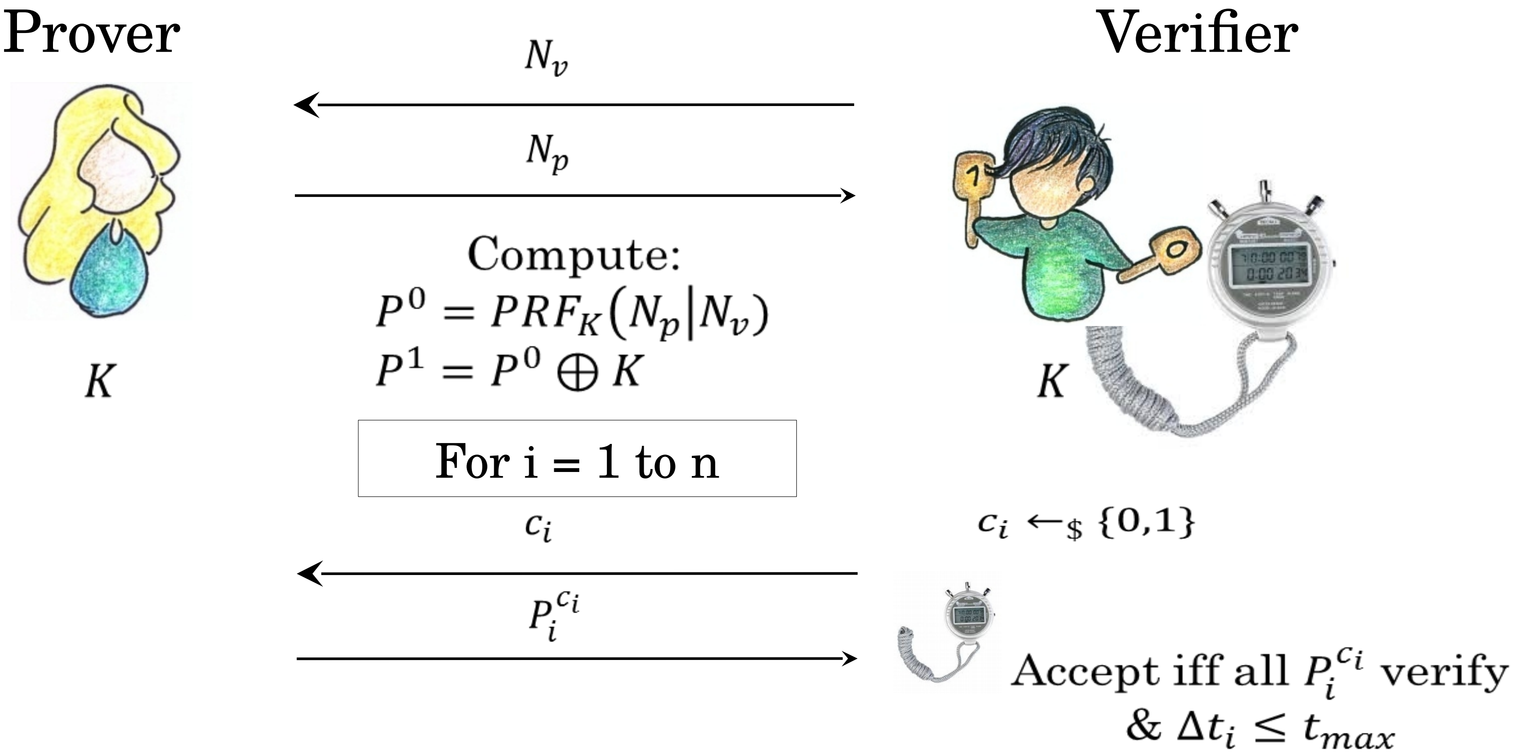
THE TERRORIST-FRAUD CONTROVERSY

- Terrorist fraud (TF) is a powerful insider attack
  - The prover helps the adversary authenticate
  - Trivial attack: physically give A the prover device!
  - We cannot prevent this trivial attack
    - However, a good question is what we **can** prevent

- Several flavours of TF-resistance exist:
  - Most guarantee that the P’s aid gives A secret key
  - P’s aid gives A no ulterior advantage
  - Yet others: P’s aid can be traced back to P

How can we achieve TF resistance?

THE KEY-LEAKING METHOD



Prover

Verifier

N_v

N_p

Compute:

$P^0 = PRF_K(N_p|N_v)$

$P^1 = P^0 \oplus K$

K

K

For i = 1 to n

c_i

$c_i \leftarrow_{\$} \{0,1\}$

$P_i^{c_i}$

Accept iff all $P_i^{c_i}$ verify

& $\Delta t_i \leq t_{max}$

- ➢ A needs both P^0, P^1 to respond
- ➢ If both P^0, P^1 are given, A learns K

NEW PROTOCOL : TREAD

- New paradigm to construct Terorist Fraud Resistant distance bounding
- Principle:
  - Achieve Terrorist Fraud Resistance by replay:
    - Successful A will replay a successful session to win
  - This means verifier randomness not input to PRF
  - Prover authenticates by a signature/MAC
    - And in time-critical rounds by knowledge of *ephemeral* key
  - Optional anonymity when using group signatures

GENERIC TREAD

Prover

ID_{pub}, ID_{priv}
eK, sK

Verifier

dK, vK

$\alpha, \beta \leftarrow_{\$} \{0,1\}^n$
$M := \alpha | \beta | ID_{priv}$
$\sigma := Sign_{sK}(M)$
$e := Enc_{eK}(M|\sigma)$

$\xrightarrow{e\ , ID_{pub}}$

Decrypt e with dK
Verify σ with vK

$\xleftarrow{\text{rd}}$

rd $\leftarrow_{\$} \{0,1\}^n$

For i = 1 to n

$c_i \leftarrow_{\$} \{0,1\}$

$\xleftarrow{c_i}$

If $c_i = 0,\ \ r_i = \alpha_i$
Else, $r_i = \beta_i \oplus \text{rd}_i$

$\xrightarrow{r_i}$

Accept iff all r_i verify
& $\Delta t_i \leq t_{max}$

GENERIC TREAD

Prover

ID_{pub}, ID_{priv}
eK, sK

Verifier

dK, vK

Ephemeral secret keys

$\alpha, \beta \leftarrow_{\$} \{0,1\}^n$
$M := \alpha|\beta|ID_{priv}$
$\sigma := Sign_{sK}(M)$
$e := Enc_{eK}(M|\sigma)$

$e\ , ID_{pub}$ →

Decrypt e with dK
Verify σ with vK

$rd \leftarrow_{\$} \{0,1\}^n$

← rd

Keys are encrypted and signed

For i = 1 to n

$c_i \leftarrow_{\$} \{0,1\}$

← c_i

If $c_i = 0, \;\; r_i = \alpha_i$
Else, $r_i = \beta_i \oplus \mathrm{rd}_i$

r_i →

Accept iff all r_i verify
& $\Delta t_i \leq t_{max}$

Responses reveal keys

THE SECURITY OF TREAD

- Mafia-fraud resistance
  - Prover & verifier are honest
  - Attacker must produce responses for fresh challenges
    - Responses require knowledge of α_i, β_i
    - Best strategy: reuse a previously seen e (and signature σ)
    - However, A only sees at most 1 honest session for e
    - … and thus r_i values only for one set of challenges

- Distance-fraud resistance
  - Prover is malicious but far
  - V chooses rd after P has sent α, β
    - Hence, P cannot predict what will be "convenient" α, β

TERRORIST-FRAUD RESISTANCE

- SimTF definition: game in 2 phases
- First, terrorist A helped by malicious P
  - The attacker authenticates w.p. p_A
- Then, Simulator inherits state of A
  - Denote Sim’s winning probability by p_{Sim}
- Protocol is TFR iff. $p_{\text{Sim}} \geq p_A$

- TREAD’s TFR:
  - Once A authenticates with P’s help…
  - … Sim inherits A’s full state
  - … and just replays what it got

INSTANTIATIONS OF TREAD

- Fast symmetric-key instantiation
  - Use IND-CPA symmetric encryption (so $eK = dK$)
  - Use EUF-CMA mac scheme (so $sK = vK$)
  - $ID_{priv} = null$

- Privacy with PKE
  - IND-CCA2 public-key encryption, EUF-CMA signatures
  - $ID_{pub} = null$
  - This provides privacy w.r.t. MiM attackers (but not V)

- Anonymity with PKE
  - Use secure group-signatures, $ID_{pub} = GID$, $ID_{priv} = null$
  - This provides privacy w.r.t. curious verifiers

CONCLUSIONS

NEW APPROACH IN DISTANCE BOUNDING

- TREAD is provably-secure
  - Generic approach to designing TFR distance bounding
  - Rely on tuple of temporary keys
  - Authentication by signature/MAC
  - Terrorist Fraud Resistance proof relies on replaying of information

- Three instantiations
  - Symmetric-key: fast, but no privacy
  - PKE with signatures: needs public keys, privacy w.r.t. MiM
  - PKE with group signatures: anonymity (even w.r.t. V)

THANKS! QUESTIONS?