Terrorist Fraud resistant nanosecond-scale Distance Bounding

Boris Škorić
TU Eindhoven

Crypto Working Group
May 13, 2011

Terrorist fraud resilient distance Bounding with Analog components

Work in progress.

Joint work with
Srdjan Čapkun, Aanjhan Ranganathan, Nils Ole Tippenhauer
(System Security Group, ETH Zürich).

Outline

- Types of relay attack
- Distance bounding
  - Swiss Knife
- Analog hardware
  - challenge reflection
  - channel selection
  - limitations
- New scheme
  - modified analog circuit
  - adapted Swiss Knife

Why distance bounding?

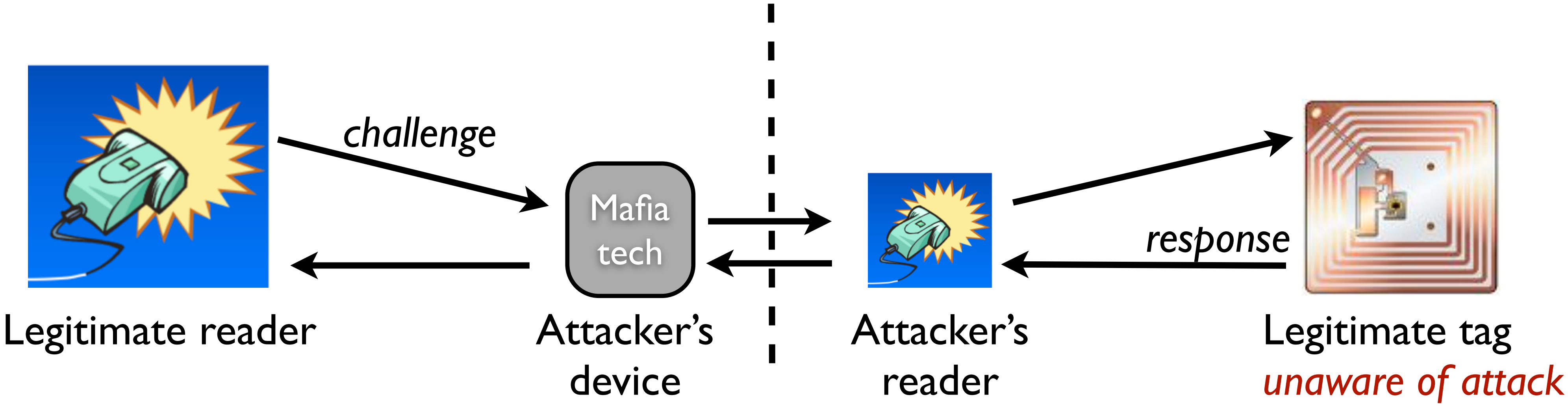
Authentication alone may not be sufficient

- physical access to buildings etc.
  - watch out for relay attack

Two main types of attack

- *Mafia Fraud*
- *Terrorist Fraud*

Relay attacks: Mafia Fraud

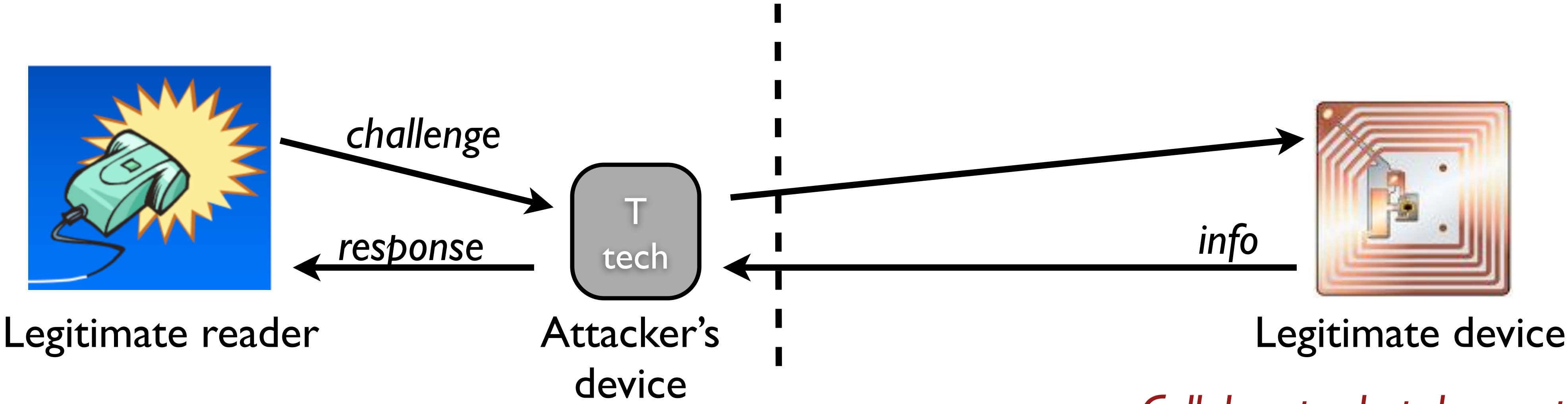


Authentication without distance checking

- *Correct response*
- *from legitimate tag*
- *... but attacker gets access!*

Famous urban myth: Mig-in-the-middle attack

Relay attacks: Terrorist Fraud



Collaborates but does not reveal long-term secrets

More powerful than Mafia fraud:

- *legit device does not have to be tricked*
- *device can provide more info than just response*

Countermeasures

What to do against relay attacks?

- Ask the prover where he is
  - but he could be lying
- Signal strength
  - can be spoofed
- Measure the distance to the prover
  - “distance bounding”
  - nothing travels faster than light $c = 2.99792458 \cdot 10^8$ m/s
  - infer distance from traveling time of signal

300 meters per microsecond

Distance bounding

Demand response within time t_{max}

- travel time to distance x_{max} and back
- allow some "slack" time for computations
- dist. measurement & demonstration of knowledge at the same time

$$t_{\max} = 2\frac{x_{\max}}{c} + t_{\text{slack}}$$

$$x_{\text{spoofable}} = \tfrac{1}{2}c\,t_{\max} = x_{\max} + \tfrac{1}{2}c\,t_{\text{slack}}$$

has to be very small

Distance bounding: practical problems

t_{slack} must be very small

- no (heavy) computations
  - addition lasts too long
  - *but still cryptographic challenge-response protocol !*
- delays inside prover device become problematic
  - missed cycles, bus speed, etc
- no error correction
  - live with transmission errors

Solving the practical problems

- no (heavy) computations
  - split protocol into slow and quick phase
  - prover creates LUT in slow crypto phase
  - verifier: unpredictable selection from LUT in quick phase
- delays inside prover
  - LUT sitting right "next to" emitter
- no error correction
  - decide afterwards if there were transmission errors

Swiss Knife protocol (Kim et al. 2008)

<u>Reader</u> has DB {ID, x} | <u>Tag</u> (ID, x)

Random N_A;
random d (Hamm.weight m)

$\xrightarrow{N_A,\, d}$

Random N_B

$\xleftarrow{N_B}$

$Z^0 = f_x(C_B, N_B)$; $Z^1 = Z^0 \oplus x$;
For $i = 1$ to m { j = index of next 1 in d;
$R^0_i = Z^0_j$; $R^1_i = Z^1_j$ }

Rapid bit exchange

For $i = 1$ to m

Random bit c_i ; start clock $\xrightarrow{c_i'}$

$$r_i = \begin{cases} R^0_i & \text{if } c_i' = 0 \\ R^1_i & \text{if } c_i' = 1 \end{cases}$$

Stop clock; store Δt_i $\xleftarrow{r_i}$

$t_B = f_x(c_1', \ldots, c_m', \mathrm{ID}, N_A, N_B)$

$\xleftarrow{t_B,\, c_1',\, \ldots,\, c_m'}$

Find matching (ID, x) in DB;
compute R^0, R^1;
$\mathrm{err}_c = \#\{i: c_i' \neq c_i\}$;
$\mathrm{err}_r = \#\{i: c_i' = c_i \wedge r_i \neq R^{c_i}_i\}$;
$\mathrm{err}_t = \#\{i: c_i' = c_i \wedge \Delta t_i > \Delta t_{\max}\}$;
if $\mathrm{err}_c + \mathrm{err}_r + \mathrm{err}_t \geq T$ reject;
$t_A = f_x(N_B)$

$\xrightarrow{t_A}$

Check t_A

Still too slow!

State of the art hardware:

- analog → digital conversion: 50 ns
- all conversion steps together: 170 ns (26 meters)

Only analog processing is fast enough!

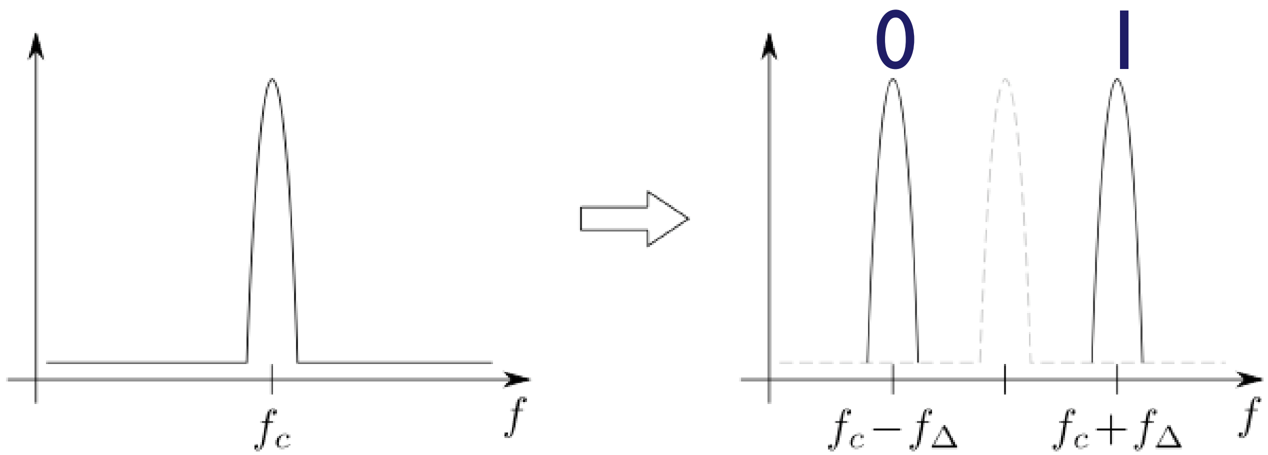
Analog challenge-response

Rasmussen & Čapkun 2010

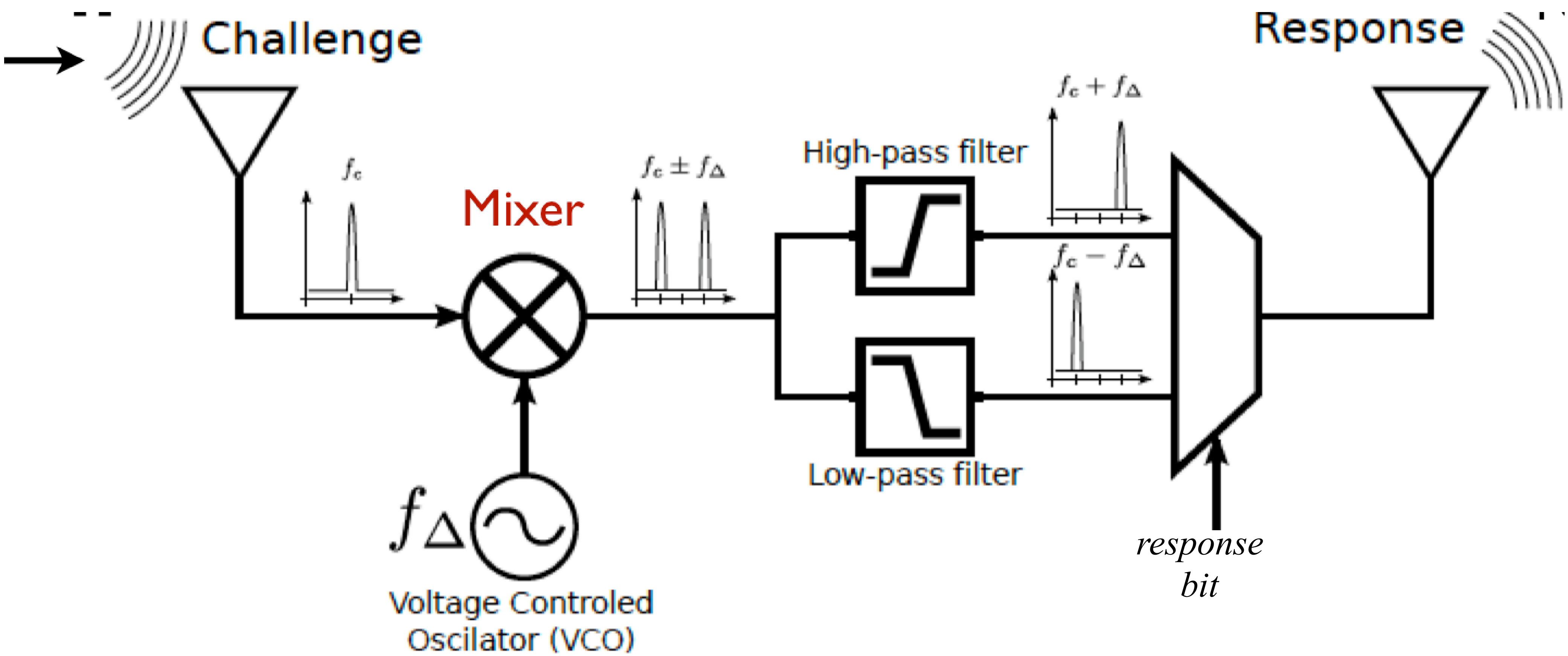
- Brands-Chaum with analog response.
- **CRCS**: *Challenge Reflection with Channel Selection.*

Challenge: unpredictable signal c(t) at frequency f_c

Response: reflection of c(t) at shifted frequency



Challenge Reflection with Channel Selection



< 1 nanosecond !

Security of Rasmussen-Čapkun

- [Same as Brands-Chaum]
- Secure against Mafia Fraud
- NOT against Terrorist Fraud
  - need AD conversion for challenge interpretation

Swiss Knife

Rapid bit exchange

For $i = 1$ to m

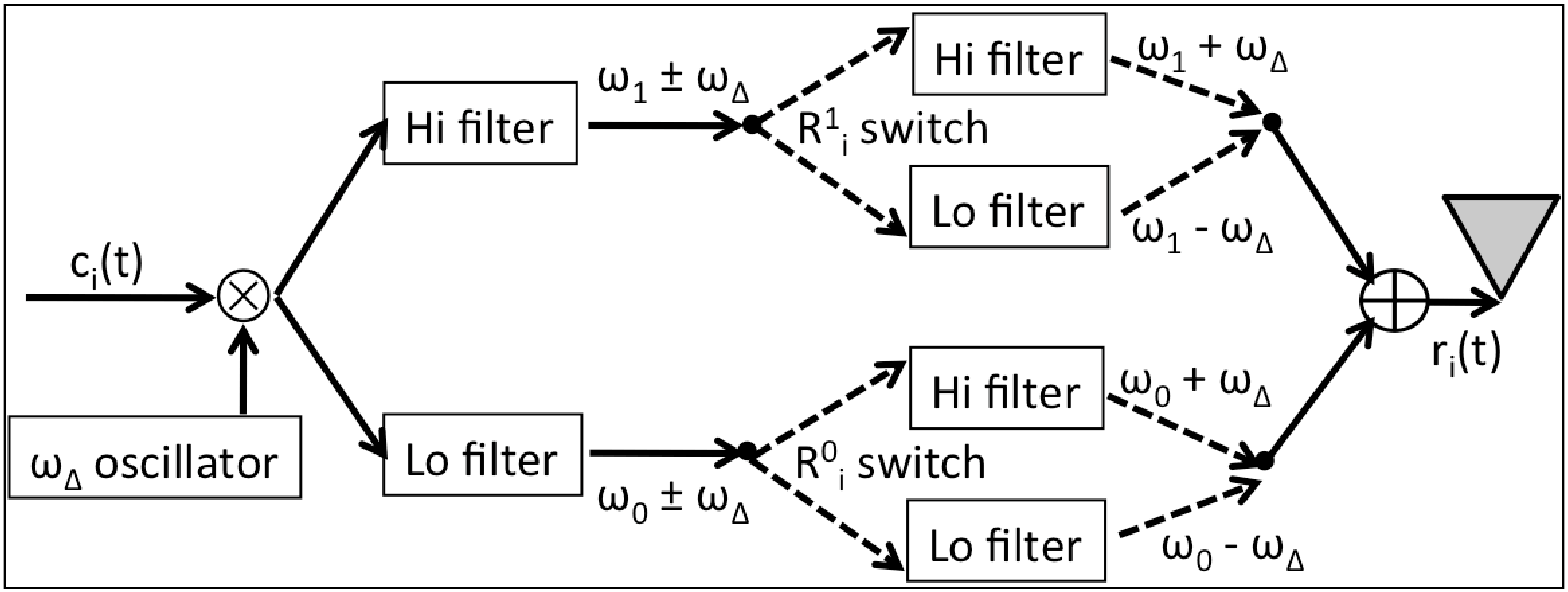
Random bit c_i ; start clock $\xrightarrow{c_i'}$ $r_i = \begin{cases} R^0_i & \text{if } c_i' = 0 \\ R^1_i & \text{if } c_i' = 1 \end{cases}$

Stop clock; store Δt_i $\xleftarrow[r_i]{}$

Generalized CRCS

Doing the register choice with <u>analog</u> hardware

- Challenge $c(t)$ at freq ω_0 or ω_1.
- Two CRCS circuits in parallel.



Danger: malicious verifier may read out both registers.

Protocol adaptation

- Problem: readout of *both* registers
  - attacker learns the secret
  - detection takes time
  - need to respond immediately
- Solution: masking
  - commit to random mask
  - do rapid part with masked registers
  - if no cheating, then open commitment

Verifier has DB {ID, x}

Prover (ID, x)

Random N_A;
random d (Hamm.weight m)

$\xrightarrow{N_A,\, d}$

Random M^0, M^1, N_B; $F = f_x(M^0, M^1)$

$Z^0 = f_x(C_B, N_B)$; $Z^1 = Z^0 \oplus x$;

For i = 1 to m { j = index of next 1 in d;
$R^0{}_i = Z^0{}_j$; $R^1{}_i = Z^1{}_j$ }

$T^0 = R^0 \oplus M^0$; $T^1 = R^1 \oplus M^1$

$\xleftarrow{F,\, N_B}$

Rapid bit exchange using CRCS

For i = 1 to m

Random bit b_i;
Random signal $c_i(t)$
at freq. ω_{bi}

$\xrightarrow{c_i(t)}$

Circuit reflects signal at freq. $\omega_{bi} + (2\, T^{bi}{}_i - 1)\, \omega_\Delta$

Slow interpretation of b'_i.

$\xleftarrow{r_i(t)}$

Record $r_i(t)$ and delays Δt_i

Proceed only if no cheating detected;
$t_B = f_x(b_1', \ldots, b_m', \text{ID}, M^0, M^1, N_A, N_B)$

$\xleftarrow{t_B,\, b_1',\, \ldots,\, b_m'}$ M^0, M^1

Find matching (ID, x) in DB;
Check if $F = f_x(M^0, M^1)$;
Compute T^0, T^1;
$\text{err}_b = \#\{i: b_i' \neq b_i\}$;
$\text{err}_f = \#\{i: b_i' = b_i \wedge r_i$ has wrong freq.$\}$;
$\text{err}_r = \#\{i: b_i' = b_i \wedge r_i$ differs too much from $c_i\}$;
$\text{err}_t = \#\{i: b_i' = b_i \wedge \Delta t_i > \Delta t_{max}\}$;
Reject if $\text{err}_b + \text{err}_f + \text{err}_r + \text{err}_t$ too large;
$t_A = f_x(N_B)$ $\xrightarrow{t_A}$ Check t_A

Summary

- Distance bounding: absurd timing requirements
- Analog challenge-response, CRCS
  - secure against Mafia Fraud, but not Terrorist Fraud
- Generalized CRCS and extra masking step
  - ➡ nanosecond-scale responses
  - ➡ security against Terrorist Fraud
  - not restricted to Swiss Knife
- Embarrassingly trivial-looking