Terrorist Fraud in Quantum Distance Bounding

Sebastian Verschoor

Institute for Quantum Computing
David R. Cheriton School of Computer Science
University of Waterloo

June 18th, 2020

Institute for Quantum Computing

UNIVERSITY OF WATERLOO

Outline

Distance Bounding

Use cases

- Contactless payments
- Remote “keyless” entry systems
- Building access

Solution

- measure round-trip time

Alternative solutions

- Signal strength
  - Wi-Fi positioning system (WPS)
- Faraday cage
- do nothing

Distance Bounding

Use cases

- Contactless payments
- Remote “keyless” entry systems
- Building access

Solution

- measure round-trip time

Alternative solutions

- Signal strength
  - Wi-Fi positioning system (WPS)
- Faraday cage
- do nothing

BlueSniper [Fle04]

Distance Bounding

Measure round-trip time in challenge-response protocol:

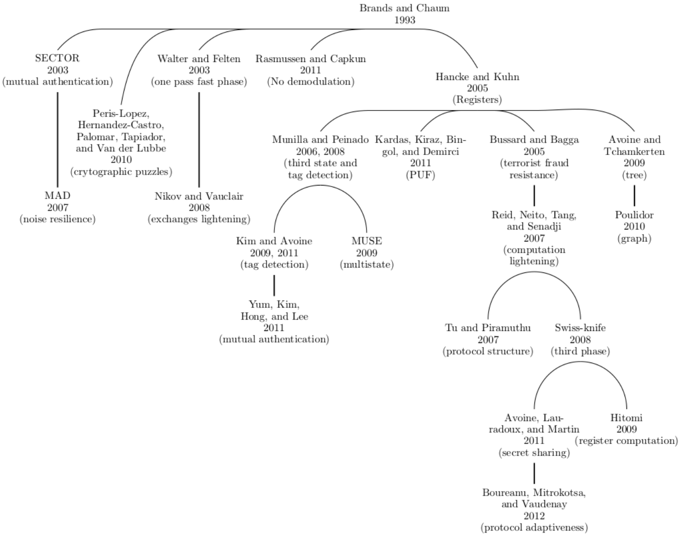
- speed of information is bound by $c \approx 300{,}000\text{km/s}$
- distance $\leq c \cdot$ round-trip-time

Problem: computers are slow

- typical smartcard clock 13.56MHz
- one clock cycle corresponds to 11 meter
- more overhead from analog-to-digital conversion and back

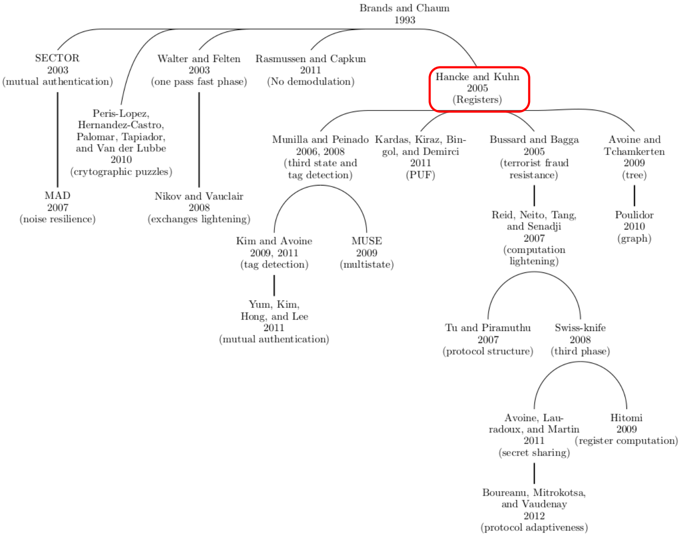
Solution: multiple phase protocol

- slow phase for crypto
- timed phase:
  - implement directly in hardware
  - only very simple operations



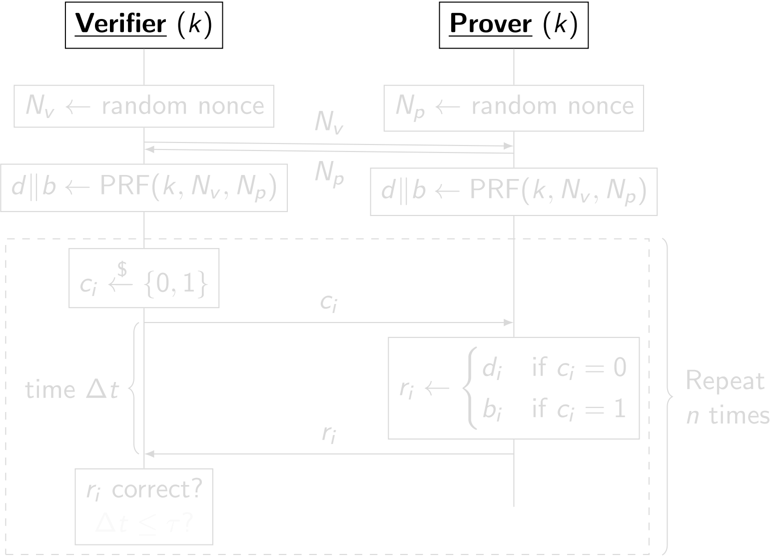
Distance bounding protocols, 2018 survey [Avo+18]

Distance Bounding

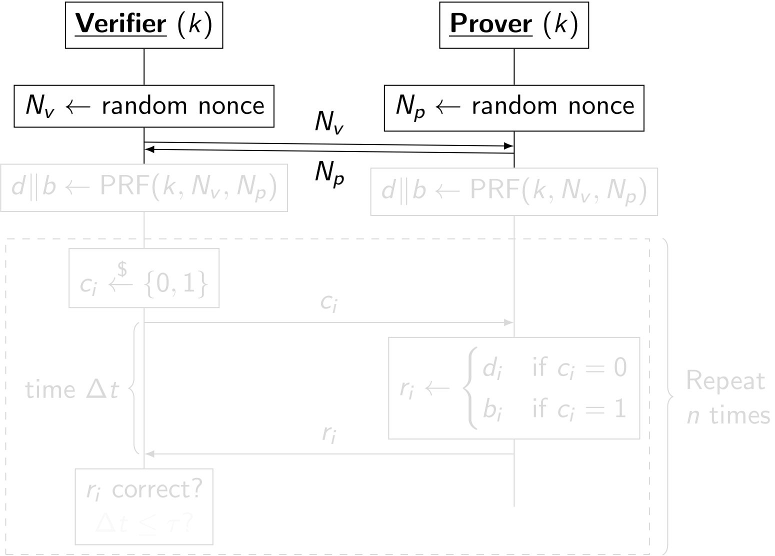


Distance bounding protocols, 2018 survey [Avo+18]

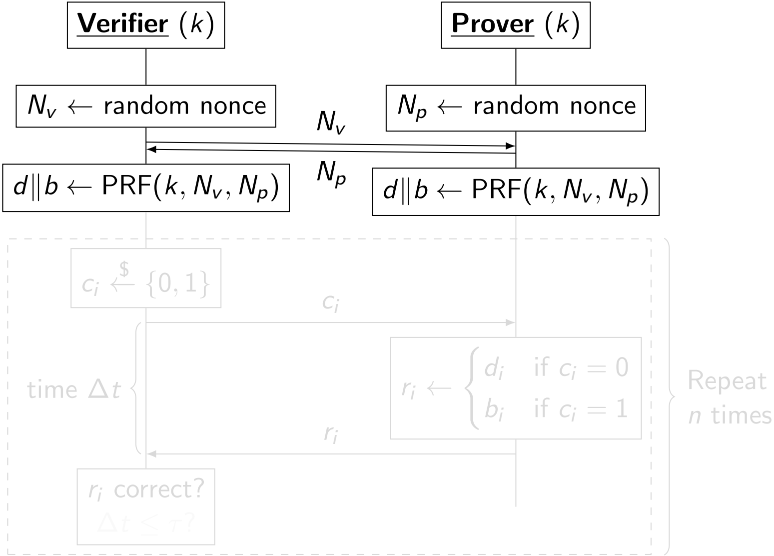
Hancke & Kuhn 2005 [HK05]



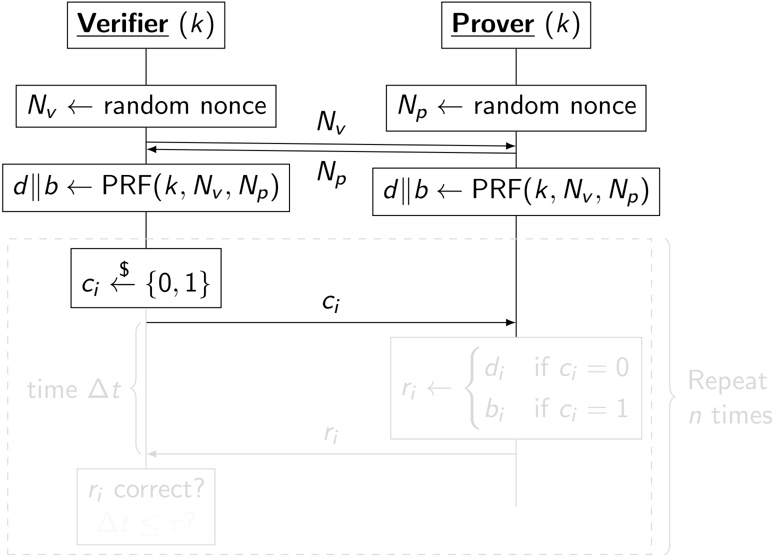
Hancke & Kuhn 2005 [HK05]



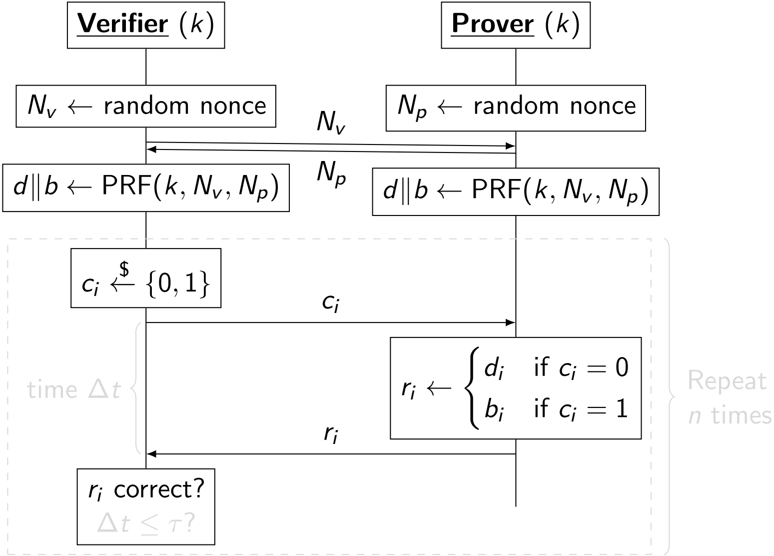
Hancke & Kuhn 2005 [HK05]



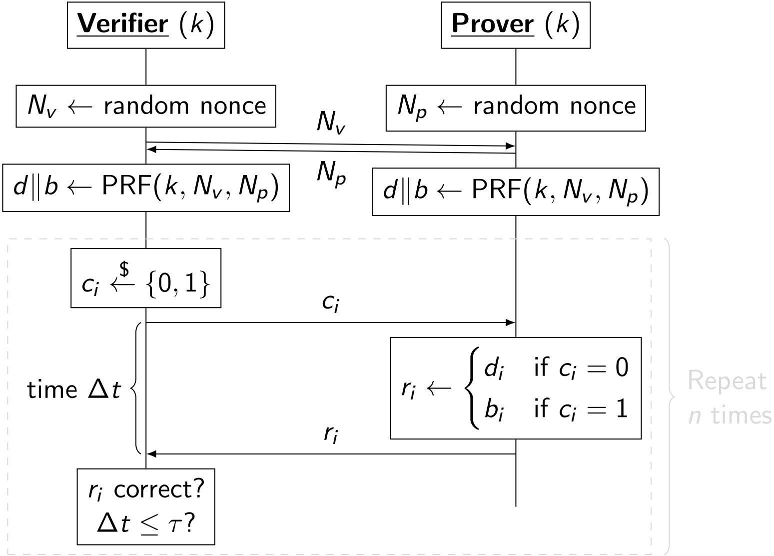
Hancke & Kuhn 2005 [HK05]



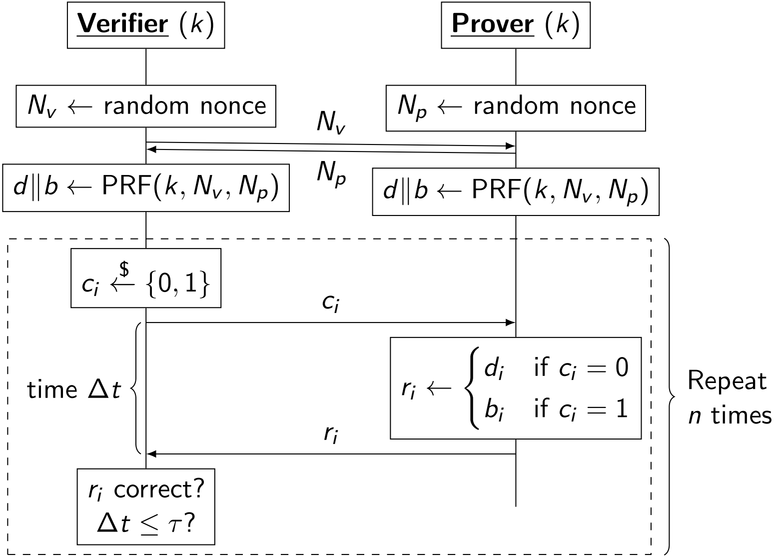
Hancke & Kuhn 2005 [HK05]



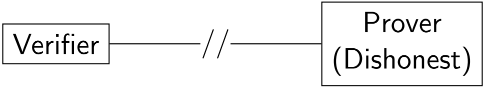
Hancke & Kuhn 2005 [HK05]



Hancke & Kuhn 2005 [HK05]

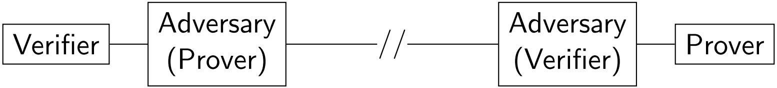


Distance Fraud



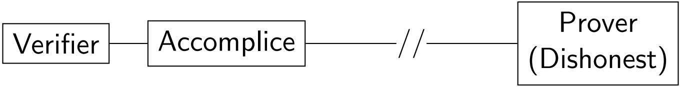
- Prover attempts to convince the verifier that they are nearby
- Countermeasure:
  - Randomize challenges c_i: preventing the prover from sending responses early

Mafia Fraud (relay attack)



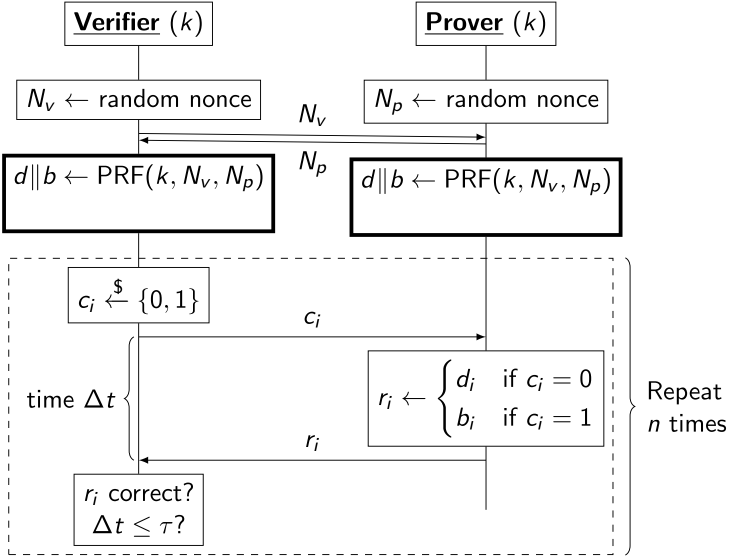
- Adversary attempts to convince the verifier that they are the prover
- Countermeasure:
  - Adversary cannot create correct responses without knowledge of secret key k
  - Relaying the challenges to the prover is too slow

Terrorist Fraud (assisted relay attack)



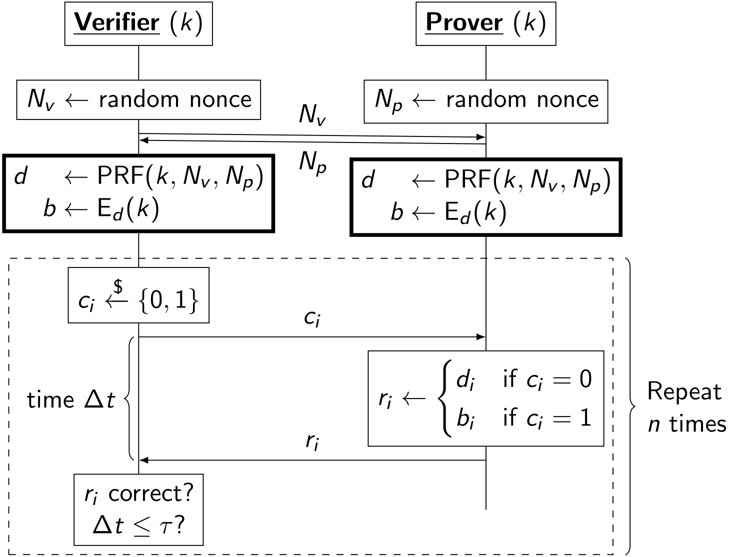
- Variation on Mafia fraud, but now the prover assists the accomplice
  - Trivial: Prover gives secret key k to the accomplice
- To exclude the trivial attack, assume the prover only wants to provide one-time access
- There is much debate about the usefulness and formalization of terrorist fraud
- Hancke-Kuhn does not resist terrorist fraud

Hancke-Kuhn



Verifier (k)
Prover (k)
$N_v \leftarrow$ random nonce
$N_p \leftarrow$ random nonce
N_v
N_p
$d \| b \leftarrow \mathrm{PRF}(k, N_v, N_p)$
$d \| b \leftarrow \mathrm{PRF}(k, N_v, N_p)$
$c_i \xleftarrow{\$} \{0, 1\}$
c_i
time Δt
$r_i \leftarrow \begin{cases} d_i & \text{if } c_i = 0 \\ b_i & \text{if } c_i = 1 \end{cases}$
r_i
r_i correct?
$\Delta t \leq \tau$?
Repeat
n times

Hancke-Kuhn with terrorist fraud resistance*



Out of scope

- Noise
- Anonymity
- Distance Hijacking
- Position based cryptography

Notation:

- initial phase is identical: omitted from the slides
    - no information theoretic security: initial phase relies on a PRF

qubit: $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$

- (complex) amplitudes α, β

$x \leftarrow$ measure $|\psi\rangle$

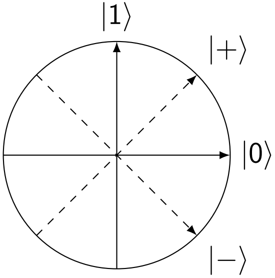
- $\Pr[x = 0] = |\alpha|^2$
- $\Pr[x = 1] = |\beta|^2 = 1 - |\alpha|^2$

Hadamard basis

- $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$
- $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$

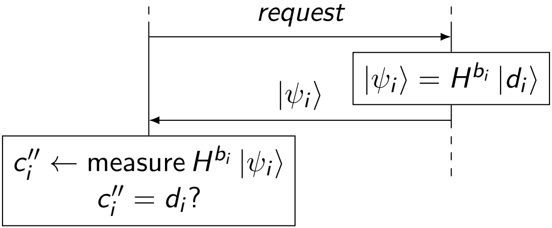
Hadamard gate H

- $H\,|0\rangle = |+\rangle$; $H\,|1\rangle = |-\rangle$
- $H\,|+\rangle = |0\rangle$; $H\,|-\rangle = |1\rangle$



Relay attacks detection protocol

RAD protocol by Jannati & Ardeshir-Larijani [JA16]



- no randomized challenge
- no timed phase
- security proof assumes that relaying requires measurement
- flaws observed by Abidin [Abi20]

Improved RAD, 2020

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

$$\xrightarrow{\quad c_i \quad}$$

$$|\psi_i\rangle = \begin{cases} H^{d_i}\,|0\rangle & \text{if } c_i = 0 \\ H^{b_i}\,|1\rangle & \text{if } c_i = 1 \end{cases}$$

$$\xleftarrow{\quad |\psi_i\rangle \quad}$$

$$c_i'' \leftarrow \text{measure} \begin{cases} H^{d_i}\,|\psi_i\rangle & \text{if } c_i = 0 \\ H^{b_i}\,|\psi_i\rangle & \text{if } c_i = 1 \end{cases}$$

$$c_i = c_i''?$$

- response is timed
- type of encryption E is unspecified (it matters!)

Extracting k from Improved RAD, 2020

If E is a one-time pad ($b = k \oplus d$):

- alter one rapid round in a session between honest participants
- extract a key bit $k_i = 1$
  - flip challenge c_i
  - forward response $|\psi_i\rangle$
  - observe if the verifier accepts
- if $k_i = 0$, then $d_i = b_i$:
  - verifier measures in "correct" basis
  - $c_i \neq c_i''$
  - verifier rejects
- if $k_i = 1$, then $d_i \neq b_i$:
  - verifier measures in non-orthogonal basis
  - verifier maybe accepts
- to extract $k_i = 0$, flip c_i and reply $H|\psi_i\rangle$
- repeat until all key bits are extracted ($3.5n$ sessions expected)

Extracting k from Improved RAD, 2020

If E is a one-time pad ($b = k \oplus d$):

- alter one rapid round in a session between honest participants
- extract a key bit $k_i = 1$
  - flip challenge c_i
  - forward response $|\psi_i\rangle$
  - observe if the verifier accepts
- if $k_i = 0$, then $d_i = b_i$:
  - verifier measures in "correct" basis
  - $c_i \neq c_i''$
  - verifier rejects
- if $k_i = 1$, then $d_i \neq b_i$:
  - verifier measures in non-orthogonal basis
  - verifier maybe accepts
- to extract $k_i = 0$, flip c_i and reply $H\,|\psi_i\rangle$
- repeat until all key bits are extracted ($3.5n$ sessions expected)

Extracting k from Improved RAD, 2020

If E is a one-time pad ($b = k \oplus d$):

- alter one rapid round in a session between honest participants
- extract a key bit $k_i = 1$
  - flip challenge c_i
  - forward response $|\psi_i\rangle$
  - observe if the verifier accepts
- if $k_i = 0$, then $d_i = b_i$:
  - verifier measures in "correct" basis
  - $c_i \neq c_i''$
  - verifier rejects
- if $k_i = 1$, then $d_i \neq b_i$:
  - verifier measures in non-orthogonal basis
  - verifier maybe accepts
- to extract $k_i = 0$, flip c_i and reply $H|\psi_i\rangle$
- repeat until all key bits are extracted (3.5n sessions expected)

Extracting k from Improved RAD, 2020

If E is a one-time pad ($b = k \oplus d$):

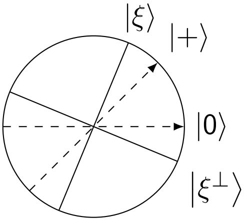
- alter one rapid round in a session between honest participants
- extract a key bit $k_i = 1$
  - flip challenge c_i
  - forward response $|\psi_i\rangle$
  - observe if the verifier accepts
- if $k_i = 0$, then $d_i = b_i$:
  - verifier measures in "correct" basis
  - $c_i \neq c_i''$
  - verifier rejects
- if $k_i = 1$, then $d_i \neq b_i$:
  - verifier measures in non-orthogonal basis
  - verifier maybe accepts
- to extract $k_i = 0$, flip c_i and reply $H\,|\psi_i\rangle$
- repeat until all key bits are extracted ($3.5n$ sessions expected)

Terrorist fraud on Improved RAD, 2020

If E is a computational cipher (e.g. $b = \mathrm{AES}_d(k)$):

- extracting one bit of $d \oplus b$ is insufficient
- terrorist fraud is possible
  - prover completes the (slow) initial phase
  - prover sends $(H^{d_i}|0\rangle, H^{b_i}|1\rangle)$ to the accomplice
  - accomplice selects correct reply to c_i
- the accomplice cannot learn d_i (or b_i) with certainty

- best attempt: measure in basis $\{|\xi\rangle, |\xi^\perp\rangle\}$
- $|\xi\rangle = \cos\frac{3\pi}{8}|0\rangle + \sin\frac{3\pi}{8}|1\rangle$
- $|\xi^\perp\rangle = \cos\frac{-\pi}{8}|0\rangle + \sin\frac{-\pi}{8}|1\rangle$



- $|\langle\xi|+\rangle|^2 = |\langle\xi^\perp|0\rangle|^2 = (2+\sqrt{2})/4 \approx 0.85$

Terrorist fraud on Improved RAD, 2020 (cont.)

By the Holevo-Helstrom theorem, distinguishing equal probability pure states $|\psi\rangle, |\phi\rangle$ succeeds with probability at most

$$\frac{1}{2} + \frac{1}{2}\sqrt{1 - |\langle\phi|\psi\rangle|^2}$$

Since $\langle 0|+\rangle = 1/\sqrt{2}$, the optimum is indeed $(2 + \sqrt{2})/4$.
The accomplice learns k by getting all $2n$ bits of d and b.

- assuming the PRF and E are secure, these are independent
- so[1] the accomplice succeeds in extracting k with probability

$$\left(\frac{2 + \sqrt{2}}{4}\right)^{2n} \approx 0.73^n$$

[1] should be true, but I haven't proved it yet

$$c_i \xleftarrow{\$} \{0,1\}$$
$$|\phi_i\rangle = H^{d_i}\,|c_i\rangle$$

$$\xrightarrow{\quad |\phi_i\rangle \quad}$$

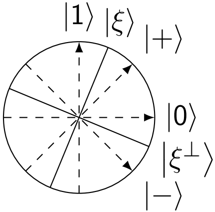
$$c_i' \leftarrow \text{measure } H^{d_i}\,|\phi_i\rangle$$
$$|\psi_i\rangle = H^{b_i}\,|c_i'\rangle$$

$$\xleftarrow{\quad |\psi_i\rangle \quad}$$

$$c_i'' \leftarrow \text{measure } H^{b_i}\,|\psi_i\rangle$$
$$c_i = c_i''?$$

If E is a one-time pad ($b = k \oplus d$), we can extract k:

- previous attack works (flip challenge qubit with XZ-gate), but we can do better
- interact only with the prover
  - send challenge $|\xi\rangle$ in every rapid round
  - measure response in $\{|\xi\rangle, |\xi\perp\rangle\}$ basis
  - associated guesses $k_i = 0$ or $k_i = 1$ (resp.)



Assume $d_i = 0$, then

$$\Pr[\text{guess } 0 \mid k_i = 0] = |\langle\xi|1\rangle|^2 |\langle 1|\xi\rangle|^2 + |\langle\xi|0\rangle|^2 |\langle 0|\xi\rangle|^2$$
$$= \left(\frac{2+\sqrt{2}}{4}\right)^2 + \left(\frac{2-\sqrt{2}}{4}\right)^2 = \frac{3}{4}$$

and

$$\Pr[\text{guess } 0 \mid k_i = 1] = |\langle \xi | + \rangle|^2 |\langle 0 | \xi \rangle|^2 + |\langle \xi | - \rangle|^2 |\langle 1 | \xi \rangle|^2$$
$$= 2\left(\frac{2+\sqrt{2}}{4}\right)^2 \left(\frac{2-\sqrt{2}}{4}\right)^2 = \frac{1}{4}$$

and similar when $d_i = 1$.

- repeat the experiment, with majority vote of guesses per bit
- error in guess for k_i becomes negligible by standard tail bounds on the binomial distribution

Terrorist fraud on Abidin, 2019

If E is a computational cipher (e.g. $b = \mathrm{AES}_d(k)$), terrorist fraud is possible:

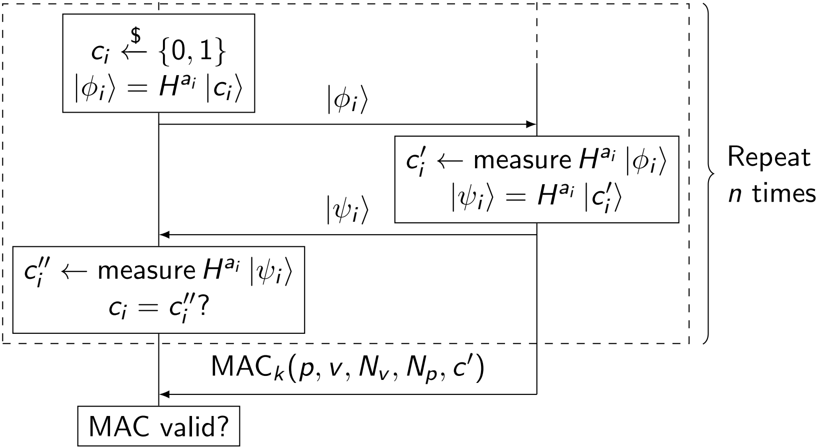
- $|\psi_i\rangle = H^{d_i \oplus b_i} |\phi_i\rangle$ (no measurement required)
- prover sends $d \oplus b$ to the accomplice

The challenge $|\phi_i\rangle = H^{d_i} |c_i\rangle$ does not leak d:

$$\frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) = \frac{1}{2}\left(|+\rangle\langle +| + |-\rangle\langle -|\right)$$

Abidin, Marin, Singelée, Preneel, 2017 [Abi+17]

For $b, d \in \{0,1\}^{n/2}$, let $a = d \| b$ in



If E is a one-time pad ($b = k \oplus d$), we can extract k:

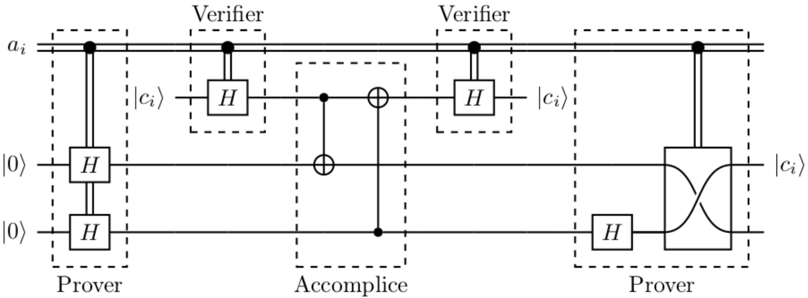
- interact only with the prover
- for every round: guess a_i' for encoding basis a_i
- send challenge $|\phi_i\rangle = H^{a_i'} |c_i\rangle$ (for some c_i)
- $c_i'' \leftarrow$ measure $H^{a_i'} |\psi_i\rangle$
  - if $a_i' = a_i$, then $|\psi_i\rangle = |\phi_i\rangle$ and $\Pr[c_i'' = c_i] = 1$.
  - if $a_i' \neq a_i$, then $|\psi_i\rangle \neq |\phi_i\rangle$ and $\Pr[c_i'' = c_i] = 1/2$.
- $\Pr[a_i' \neq a_i, c_i'' \neq c_i] = 1/4$
- if both d_i (round i) and b_i (round $i + n/2$) leak, then k_i leaks
  - probability $1/16$
  - can improve this by using partial information gained in previous attacks
- repeat the attack until all bits have leaked

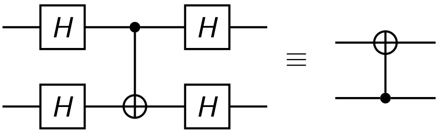
Terrorist fraud on AMSP

If E is a computational cipher (e.g. $b = \mathsf{AES}_d(k)$), terrorist fraud is possible:

- cloning the challenge would allow it
  - reflect one copy to the verifier
  - forward the other copy to the prover (to compute the MAC)
- no-cloning theorem prevents direct cloning
- the prover can assist the accomplice:
  - give $|00\rangle$ if $a_i = 0$
  - give $|{+}{+}\rangle$ if $a_i = 1$
- the prover can clone once using two CNOT gates

Terrorist fraud on AMSP (cont.)





Terrorist fraud on AMSP (cont.)

This does not leak a to the accomplice.

- challenge qubit does not help here either
- prover provided information reveals too little: best guess for a_i is correct with probability

$$\frac{1}{2} + \frac{1}{2}\sqrt{1 - |\langle 00|{+}{+}\rangle|^2} = \frac{2+\sqrt{3}}{4}$$

- so[2] accomplice guesses a correct with probability

$$\left(\frac{2+\sqrt{3}}{4}\right)^n \approx 0.93^n$$

[2] should be true but I don't have a proof yet

IT secure distance bounding

- most quantum cryptography aims to eliminate computational assumptions
- but these protocols require a one-way function
- one-time (classical) distance bounding protocols are already IT secure
  - $d \| b = k$
- combine with QKD to do multiple sessions
  - use the unused bits for authenticating a QKD session
- is that really quantum distance bounding?

Thank you

References

[Abi+17] Aysajan Abidin et al. "Towards Quantum Distance Bounding Protocols". In: *Radio Frequency Identification and IoT Security 2016*. Ed. by Gerhard P. Hancke and Konstantinos Markantonakis. Cham: Springer International Publishing, 2017, pp. 151–162. ISBN: 978-3-319-62024-4. DOI: 10.1007/978-3-319-62024-4_11.

[Abi19] Aysajan Abidin. "Quantum Distance Bounding". In: *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. WiSec '19. Miami, Florida: Association for Computing Machinery, 2019, pp. 233–238. ISBN: 9781450367264. DOI: 10.1145/3317549.3323414.

[Abi20] Aysajan Abidin. "On Detecting Relay Attacks on RFID Systems Using Qubits". In: *Cryptography* 4.2 (May 2020). DOI: 10.3390/cryptography4020014.

[Avo+18] Gildas Avoine et al. "Security of Distance-Bounding: A Survey". In: *ACM Comput. Surv.* 51.5 (2018), 94:1–94:33. DOI: 10.1145/3264628.

[Ben+91] Samy Bengio et al. "Secure Implementations of Identification Systems". In: *Journal of Cryptology* 4.3 (1991), pp. 175–183. DOI: 10.1007/BF00196726.

[Fle04] Flexilis. *BlueSniper*. 2004. URL: https://defcon.org/html/links/dc_press/archives/12/esato_bluetoothcracking.htm.

[HK05] Gerhard P. Hancke and Markus G. Kuhn. "An RFID Distance Bounding Protocol". In: *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*. Sept. 2005, pp. 67–73. DOI: 10.1109/SECURECOMM.2005.56.

[JA16] Hoda Jannati and Ebrahim Ardeshir-Larijani. "Detecting relay attacks on RFID communication systems using quantum bits". In: *Quantum Information Processing* 15.11 (2016), pp. 4759–4771. DOI: 10.1007/s11128-016-1418-5.