Bit Security of Quantum Key Search

Marc Fischlin   **Evangelos Gkoumas**

Technische Universität Darmstadt

Selected Areas in Cryptography, Toronto 2025

With funding from the:

Federal Ministry of Research, Technology and Space

Quantum Threats and Cryptographic Key Sizes

Grover's algorithm **halves the bit security**

Example: Transition from AES-128 bits to AES-256 bits

Quantum Threats and Cryptographic Key Sizes

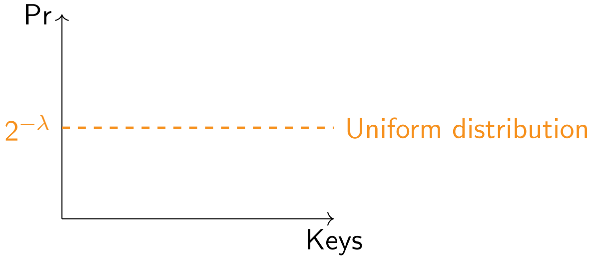
Grover's algorithm **halves the bit security**

↓

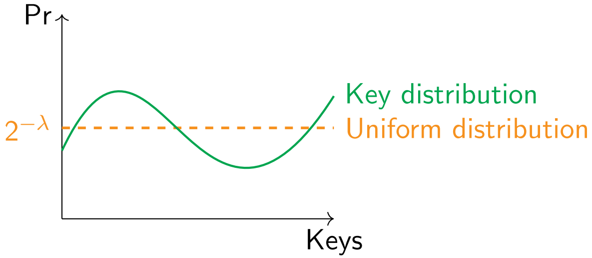
Example: Transition from AES-128 bits to AES-256 bits

Do we really get uniforms keys in practice?

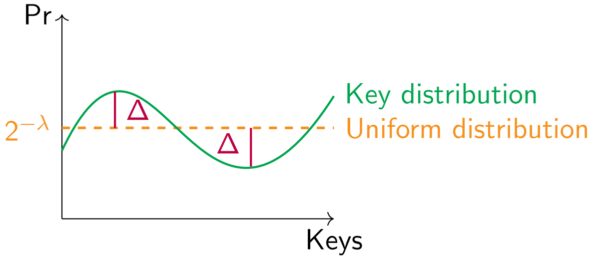
From Statistical Distance to Bit Security



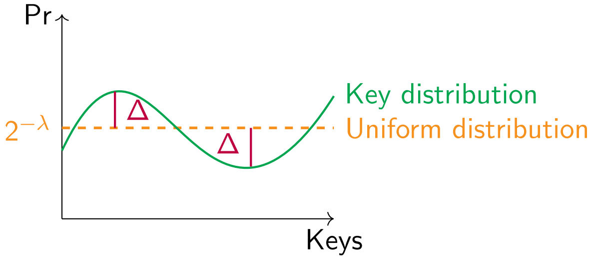
From Statistical Distance to Bit Security



From Statistical Distance to Bit Security

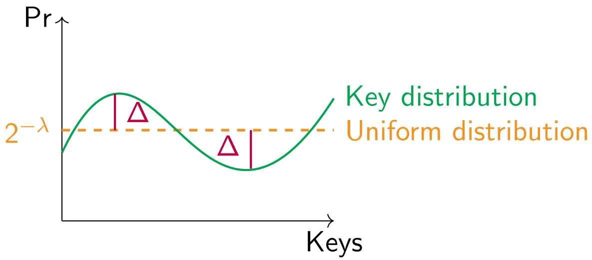


From Statistical Distance to Bit Security



What is the reasonable range for the statistical distance?

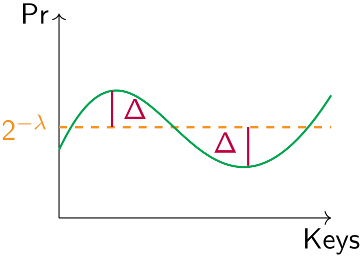
From Statistical Distance to Bit Security



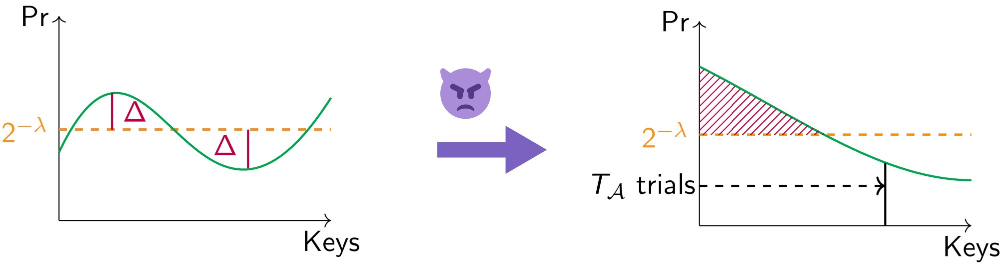
What is the reasonable range for the statistical distance?

QKD $\Rightarrow$ Keys are close to uniform keys

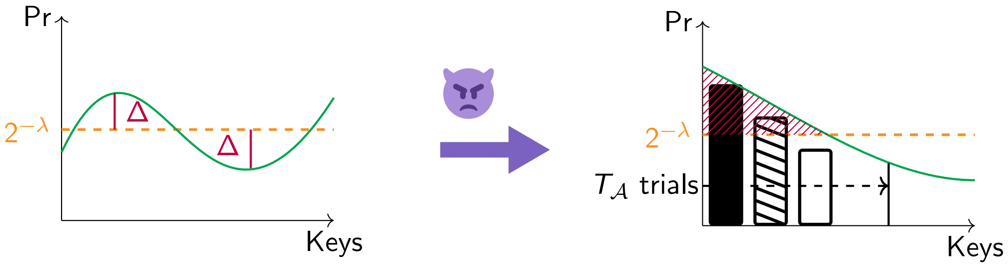
Key Search in the Classical Setting



Key Search in the Classical Setting

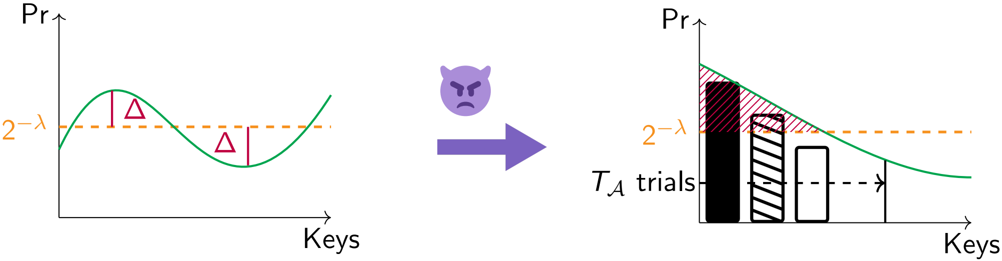


Key Search in the Classical Setting



Strategy: Check the most probable keys first

Key Search in the Classical Setting



Strategy: Check the most probable keys first

Success probability of adversary

$$\epsilon_{\mathcal{A}} \leq T_{\mathcal{A}} \cdot 2^{-\lambda} + \Delta$$

Bit Security: Intuitively Definitions

A cryptographic system offers λ-bit security if any attacker is expected to require the effort of at least 2^λ to break the system.

Bit Security: Intuitively Definitions

$$Bs = \min_{\mathcal{A}} \log \frac{T_{\mathcal{A}}}{\epsilon_{\mathcal{A}}}$$

Bit Security: Key Definitions

Bit Security

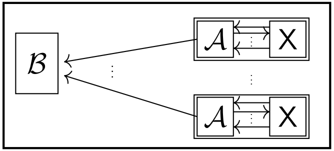
- $Bs_{MW} = \min_{\mathcal{A}} \log \left(\frac{T_{\mathcal{A}}}{\mathsf{adv}_{MW}(\mathcal{A})} \right)$ [MW18]

[MW18]: Micciancio, Walter. *On the bit security of cryptographic primitives*. Eurocrypt 2018

Bit Security: Key Definitions

Bit Security

- $Bs_{MW} = \min_{\mathcal{A}} \log\left(\frac{T_{\mathcal{A}}}{\mathsf{adv}_{MW}(\mathcal{A})}\right)$ [MW18]



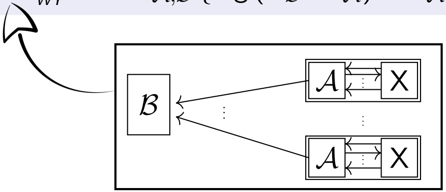
[MW18]: Micciancio, Walter. *On the bit security of cryptographic primitives*. Eurocrypt 2018

[WY21]: Watanabe, Yasunaga. *Bit security as computational cost for winning games with high probability*. Asiacrypt 2021

Bit Security: Key Definitions

Bit Security

- $Bs_{MW} = \min_{\mathcal{A}} \log\left(\frac{T_{\mathcal{A}}}{\mathrm{adv}_{MW}(\mathcal{A})}\right)$ [MW18]
- $Bs_{WY} = \min_{\mathcal{A},\mathcal{B}} \{\log(N_{\mathcal{B}} \cdot T_{\mathcal{A}}) : \Pr_{\mathcal{A},\mathcal{B}} \geq 1 - \delta\}$ [WY21]

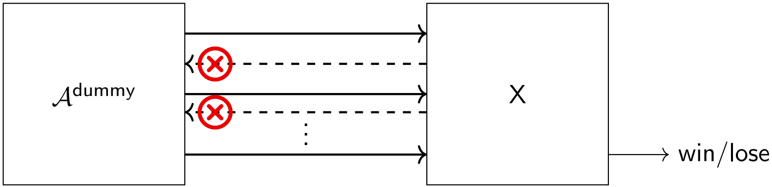


[MW18]: Micciancio, Walter. *On the bit security of cryptographic primitives*. Eurocrypt 2018

[WY21]: Watanabe, Yasunaga. *Bit security as computational cost for winning games with high probability*. Asiacrypt 2021

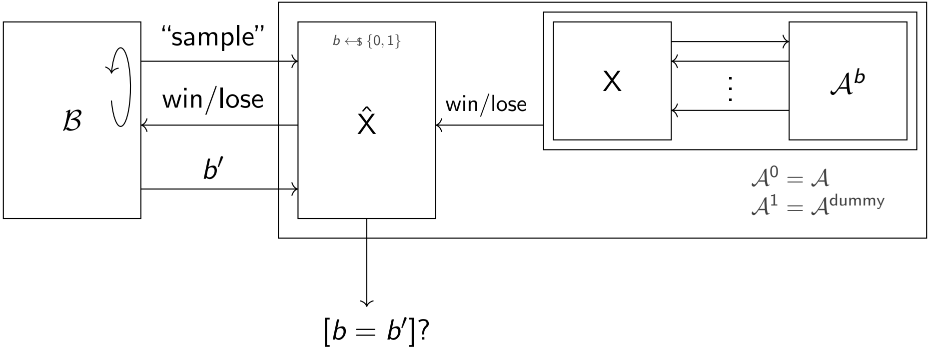
Bit Security via Observation Game

Baseline (Dummy) Adversary [Lee24]



Bit Security via Observation Game

Advantage Observation Game [Lee24]



Bit Security: Key Definitions

Bit Security

- $Bs_{MW} = \min_{\mathcal{A}} \log \left(\frac{T_{\mathcal{A}}}{\mathsf{adv}_{MW}(\mathcal{A})} \right)$ [MW18]
- $Bs_{WY} = \min_{\mathcal{A},\mathcal{B}} \{\log(N_{\mathcal{B}} \cdot T_{\mathcal{A}}) : \Pr_{\mathcal{A},\mathcal{B}} \geq 1 - \delta\}$ [WY21] 👈

👉 $$d_{\mathbf{Hell}}(\mathcal{P}, \mathcal{Q})^2 = \frac{1}{2} \sum_{x \in \Omega} \left(\sqrt{\mathcal{P}(x)} - \sqrt{\mathcal{Q}(x)} \right)^2$$

[MW18]: Micciancio, Walter. *On the bit security of cryptographic primitives*. Eurocrypt 2018

[WY21]: Watanabe, Yasunaga. *Bit security as computational cost for winning games with high probability*. Asiacrypt 2021

[Lee24]: Lee. *Bit security as cost to demonstrate advantage*. Communications in Cryptology, Vol. 1, No. 1, 2024

Bit Security: Key Definitions

Bit Security

- $Bs_{MW} = \min_{\mathcal{A}} \log\left(\frac{T_{\mathcal{A}}}{\mathsf{adv}_{MW}(\mathcal{A})}\right)$ [MW18]
- $Bs_{WY} = \min_{\mathcal{A},\mathcal{B}} \{\log\left(N_{\mathcal{B}} \cdot T_{\mathcal{A}}\right) : \Pr_{\mathcal{A},\mathcal{B}} \geq 1-\delta\}$ [WY21]

Sample Complexity Bounds [Lee24]

$$\frac{1}{4\ln 2} \cdot \frac{\ln\left(\frac{1}{4\delta(1-\delta)}\right)}{d_{\mathrm{Hell}}(\mathcal{P},\mathcal{Q})^2} \leq N_\delta(\mathcal{P},\mathcal{Q}) \leq \frac{\ln\left(\frac{1}{2\delta}\right)}{d_{\mathrm{Hell}}(\mathcal{P},\mathcal{Q})^2}$$

[MW18]: Micciancio, Walter. *On the bit security of cryptographic primitives*. Eurocrypt 2018

[WY21]: Watanabe, Yasunaga. *Bit security as computational cost for winning games with high probability*. Asiacrypt 2021

[Lee24]: Lee. *Bit security as cost to demonstrate advantage*. Communications in Cryptology, Vol. 1, No. 1, 2024

Bit Security: Key Definitions

Bit Security

- $Bs_{MW} = \min_{\mathcal{A}} \log\left(\frac{T_{\mathcal{A}}}{\mathrm{adv}_{MW}(\mathcal{A})}\right)$ [MW18]
- $Bs_{WY} = \min_{\mathcal{A},\mathcal{B}} \{\log(N_{\mathcal{B}} \cdot T_{\mathcal{A}}) : \Pr_{\mathcal{A},\mathcal{B}} \geq 1 - \delta\}$ [WY21]
- $Bs_{Lee} = \min_{\mathcal{A}} \log\left(\frac{T_{\mathcal{A}}}{d_{\mathrm{Hell}}(\Pr^{G}_{\mathcal{A}}, \Pr^{G}_{\mathcal{A}_{\mathrm{dummy}}})^2}\right)$ [Lee24]

Sample Complexity Bounds [Lee24]

$$\frac{1}{4\ln 2} \cdot \frac{\ln\left(\frac{1}{4\delta(1-\delta)}\right)}{d_{\mathrm{Hell}}(\mathcal{P},\mathcal{Q})^2} \leq N_{\delta}(\mathcal{P},\mathcal{Q}) \leq \frac{\ln\left(\frac{1}{2\delta}\right)}{d_{\mathrm{Hell}}(\mathcal{P},\mathcal{Q})^2}$$

[MW18]: Micciancio, Walter. *On the bit security of cryptographic primitives*. Eurocrypt 2018

[WY21]: Watanabe, Yasunaga. *Bit security as computational cost for winning games with high probability*. Asiacrypt 2021

[Lee24]: Lee. *Bit security as cost to demonstrate advantage*. Communications in Cryptology, Vol. 1, No. 1, 2024

Bit Security: Key Definitions

Bit Security

- $Bs_{MW} = \min_{\mathcal{A}} \log\left(\frac{T_{\mathcal{A}}}{\mathrm{adv}_{MW}(\mathcal{A})}\right)$ [MW18]
- $Bs_{WY} = \min_{\mathcal{A},\mathcal{B}} \{\log\left(N_{\mathcal{B}} \cdot T_{\mathcal{A}}\right) : \Pr_{\mathcal{A},\mathcal{B}} \geq 1 - \delta\}$ [WY21]
- $Bs_{Lee} = \min_{\mathcal{A}} \log\left(\frac{T_{\mathcal{A}}}{d_{\mathrm{Hell}}(\Pr^{G}_{\mathcal{A}}, \Pr^{G}_{\mathcal{A}^{\mathrm{dummy}}})^2}\right)$ [Lee24]

Classic!

Sample Complexity Bounds [Lee24]

$$\frac{1}{4\ln 2} \cdot \frac{\ln(\frac{1}{4\delta(1-\delta)})}{d_{\mathrm{Hell}}(\mathcal{P}, \mathcal{Q})^2} \leq N_{\delta}(\mathcal{P}, \mathcal{Q}) \leq \frac{\ln(\frac{1}{2\delta})}{d_{\mathrm{Hell}}(\mathcal{P}, \mathcal{Q})^2}$$

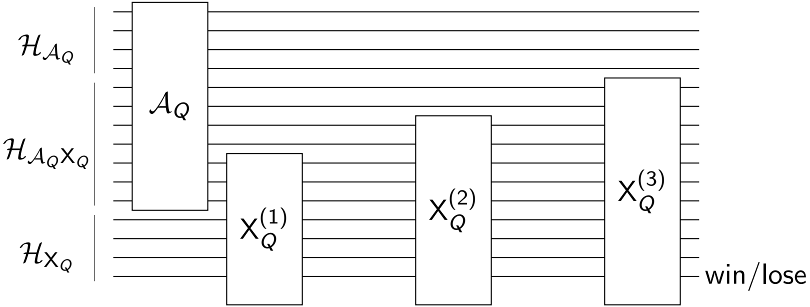
[MW18]: Micciancio, Walter. *On the bit security of cryptographic primitives*. Eurocrypt 2018

[WY21]: Watanabe, Yasunaga. *Bit security as computational cost for winning games with high probability*. Asiacrypt 2021

[Lee24]: Lee. *Bit security as cost to demonstrate advantage*. Communications in Cryptology, Vol. 1, No. 1, 2024

Proposed Hybrid Observation Game

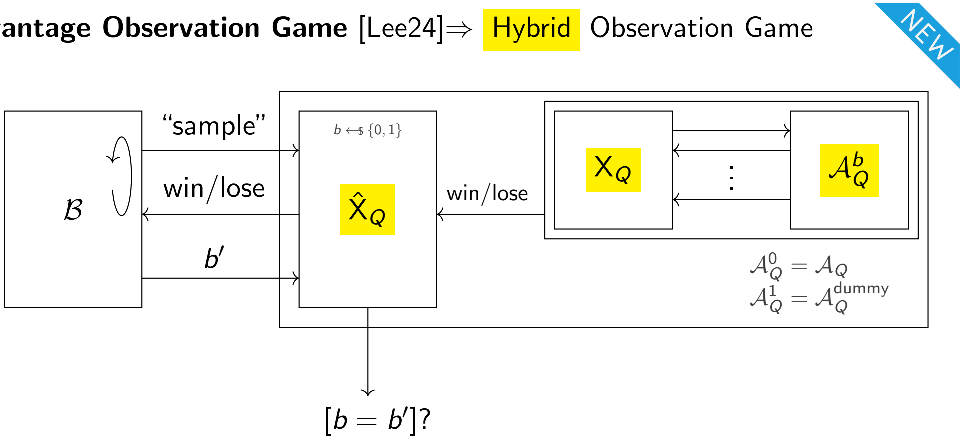
Baseline Adversary [Lee24] $\Rightarrow$ Quantum Dummy Adversary



NEW

Proposed Hybrid Observation Game

Advantage Observation Game [Lee24] ⇒ Hybrid Observation Game



Our Definition of Post-Quantum Bit Security

Definition (Post-Quantum Bit Security)

$$\mathsf{PQBS}^{\mathsf{G}_Q,\delta}_{\mathsf{Dem}}(\lambda) := \min_{\mathcal{A}_Q,\mathcal{B}} \left\{ \log(T_{\mathcal{A}_Q} \cdot N_{\mathcal{B}}) \ : \ \Pr^{\hat{\mathsf{G}}_Q}_{\mathcal{B}}(\lambda) \geq 1 - \delta(\lambda) \right\}$$

Our Definition of Post-Quantum Bit Security

Definition (Post-Quantum Bit Security) NEW

$$\mathsf{PQBS}^{\mathsf{G}_Q,\delta}_{\mathsf{Dem}}(\lambda) := \min_{\mathcal{A}_Q,\mathcal{B}} \left\{ \log(T_{\mathcal{A}_Q} \cdot N_{\mathcal{B}}) \ : \ \Pr^{\hat{\mathsf{G}}_Q}_{\mathcal{B}}(\lambda) \geq 1 - \delta(\lambda) \right\}$$

Our Definition of Post-Quantum Bit Security

Definition (Post-Quantum Bit Security) NEW

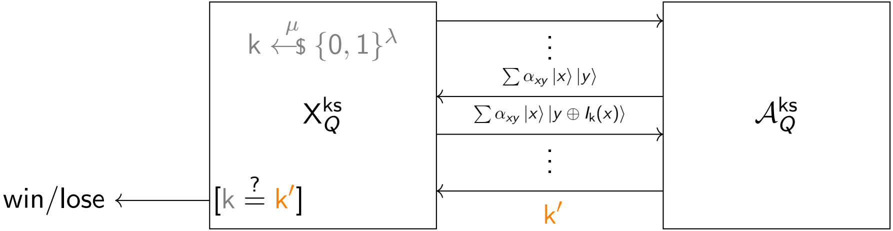
$$\mathsf{PQBS}^{\mathsf{G}_Q,\delta}_{\mathsf{Dem}}(\lambda) := \min_{\mathcal{A}_Q,\mathcal{B}} \left\{ \log\left(T_{\mathcal{A}_Q} \cdot N_{\mathcal{B}}\right) \ : \ \Pr^{\hat{\mathsf{G}}_Q}_{\mathcal{B}}(\lambda) \geq 1 - \delta(\lambda) \right\}$$

⇓

Definition (Hellinger Post-Quantum Bit Security)

$$\mathsf{PQBS}^{\mathsf{G}_Q}_{\mathsf{Hell}^2}(\lambda) = \min_{\mathcal{A}_Q} \log\left(\frac{T_{\mathcal{A}_Q}}{d_{\mathsf{Hell}}\left(\Pr^{\mathsf{G}_Q}_{\mathcal{A}_Q}(\lambda), \Pr^{\mathsf{G}_Q}_{\mathbf{D}[T_{\mathcal{A}_Q}]}(\lambda)\right)^2} \right)$$

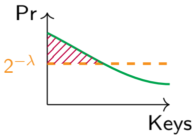
Quantum Key Search Game Model



Baseline and Success Probability

Quantum Dummy Adversary:

$$2^{-\lambda} \leq \Pr^{\mathsf{G}_Q^{\mathsf{ks},\mu,\Delta}}_{\mathbf{D}[T_Q]}(\lambda) \leq 2^{-\lambda} + \Delta$$

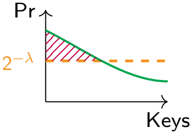


Independent of runtime !

Baseline and Success Probability

Quantum Dummy Adversary:

$$2^{-\lambda} \leq \Pr_{\mathbf{D}[T_Q]}^{\mathsf{G}_Q^{\mathsf{ks},\mu,\Delta}}(\lambda) \leq 2^{-\lambda} + \Delta$$



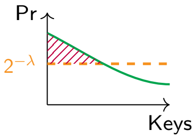
Independent of runtime **!**

Quantum Adversary:

Baseline and Success Probability

Quantum Dummy Adversary:

$$2^{-\lambda} \leq \Pr_{\mathbf{D}[T_Q]}^{\mathsf{G}_Q^{\mathsf{ks},\mu,\Delta}}(\lambda) \leq 2^{-\lambda} + \Delta$$



Independent of runtime!

Quantum Adversary:

$$T_{\mathcal{A}_Q^{\mathsf{ks}}}^2 \cdot 2^{-\lambda} \leq \Pr_{\mathcal{A}_Q^{\mathsf{ks}}}^{\mathsf{G}_Q^{\mathsf{ks},\mu,\Delta}}(\lambda)$$

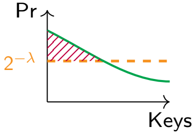
[Mon11]: Montanaro. Quantum search with advice. 2011

[HSZ24]: He, Sun, Zhang. Quantum search with prior knowledge. 2024

Baseline and Success Probability

Quantum Dummy Adversary:

$$2^{-\lambda} \leq \Pr_{\mathbf{D}[T_Q]}^{\mathsf{G}_Q^{\mathsf{ks},\mu,\Delta}}(\lambda) \leq 2^{-\lambda} + \Delta$$



Independent of runtime!

Quantum Adversary:

$$T_{\mathcal{A}_Q^{\mathsf{ks}}}^2 \cdot 2^{-\lambda} \leq \Pr_{\mathcal{A}_Q^{\mathsf{ks}}}^{\mathsf{G}_Q^{\mathsf{ks},\mu,\Delta}}(\lambda) \leq 16\, T_{\mathcal{A}_Q^{\mathsf{ks}}}^2 \cdot 2^{-\lambda} + 2 \cdot \Delta$$

[BBHT98]: Boyer, Brassard, Høyer, Tapp. Tight bounds on quantum searching. 1998
[Zal99]: Zalka. Grover's quantum searching algorithm is optimal. 1999

Bounds with $\Delta \leq 2^{-\lambda}$

Assumption: Adversary runtime is $T_{\mathcal{A}_Q^{\mathsf{ks}}} \leq 2^{\lambda/2}$

Lower-Upper Bound

$$\min_{\mathcal{A}_Q^{\mathsf{ks}}}(\lambda - \log T_{\mathcal{A}_Q^{\mathsf{ks}}} - 5) \;\leq\; \mathsf{PQBS}^{\mathsf{G}_Q}_{\mathsf{Hell}^2}(\lambda) \;\leq\; \min_{\mathcal{A}_Q^{\mathsf{ks}}}(\lambda - \log T_{\mathcal{A}_Q^{\mathsf{ks}}} + 3)$$

Implications:

- Bounds match up to a constant number of bits
- For $T_{\mathcal{A}_Q^{\mathsf{ks}}} = 2^{\lambda/2} \Rightarrow \mathsf{PQBS}^{\mathsf{G}_Q}_{\mathsf{Hell}^2}(\lambda) \approx \lambda/2$
- No further gain when $\Delta < 2^{-\lambda}$

Bounds for $2^{-\lambda} \leq \Delta \leq 2^{-\lambda/2}$

Example: Let $\Delta = 2^{-\lambda/2}$

Lower-Upper Bound

$$\min_{\mathcal{A}_Q^{\mathsf{ks}}}(\lambda/2 + \log T_{\mathcal{A}_Q^{\mathsf{ks}}} - 5) \;\leq\; \mathsf{PQBS}^{\mathsf{G}_Q}_{\mathsf{Hell}^2}(\lambda) \;\leq\; \min_{\mathcal{A}_Q^{\mathsf{ks}}}(\lambda - \log T_{\mathcal{A}_Q^{\mathsf{ks}}} + 3)$$

Implications:

- $T_{\mathcal{A}_Q^{\mathsf{ks}}} = 1 \Rightarrow$ Lower bound offers at least $\lambda/2$ bit security
- $T_{\mathcal{A}_Q^{\mathsf{ks}}} = 2^{\lambda/2} \Rightarrow$ Bounds matching

Example: When $\Delta = 2^{-\lambda}$

$$\Rightarrow \mathsf{PQBS}^{\mathsf{G}_Q}_{\mathsf{Hell}^2}(\lambda) \approx \lambda - \log T_{\mathcal{A}_Q^{\mathsf{ks}}}$$

Bounds when $\Delta > 2^{-\lambda/2}$

Lower-Upper Bound

$$\min_{\mathcal{A}_Q^{\mathsf{ks}}}(\log T_{\mathcal{A}_Q^{\mathsf{ks}}} - \log \Delta - 5) \leq \mathsf{PQBS}_{\mathsf{Hell}^2}^{\mathsf{G}_Q}(\lambda) \leq \min_{\mathcal{A}_Q^{\mathsf{ks}}}(\lambda - \log T_{\mathcal{A}_Q^{\mathsf{ks}}} + 3)$$

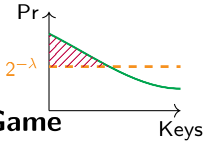
Example: For $\Delta = 2^{-\lambda/4}$ and $T_{\mathcal{A}_Q^{\mathsf{ks}}} = 1$

$$\min_{\mathcal{A}_Q^{\mathsf{ks}}}(\lambda/4 - 5) \leq \mathsf{PQBS}_{\mathsf{Hell}^2}^{\mathsf{G}_Q}(\lambda) \leq \min_{\mathcal{A}_Q^{\mathsf{ks}}}(\lambda + 3)$$

Interpretation:

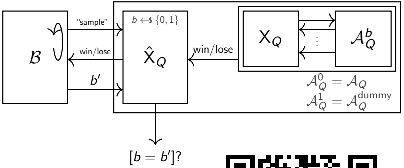
- Notably decreased lower bound
- Upper bound is not tight compared with the lower bound
- Worst-case testing only one key

Takeaways



- ✓ Studied the **Bit Security** of the with **Statistical Distance**
- ✓ Proposed **a definition** for PQBS based on **Hybrid Observation Game**
- ✓ Fixed **bounds** for the PQBS based on a **Quantum Key Search Game**
- ✓ Gave the interpretation of the bounds:

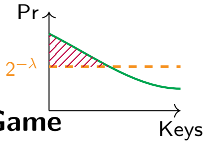
> $\Rightarrow \Delta < 2^{-\lambda}$, not any advantage for the bit security
> $\Rightarrow 2^{-\lambda} \leq \Delta \leq 2^{-\lambda/2}$, $\Delta = 2^{-\lambda}$ is conservative choice
> $\Rightarrow \Delta > 2^{-\lambda/2}$, is unclear as result for the bit security



evangelos.gkoumas@tu-darmstadt.de

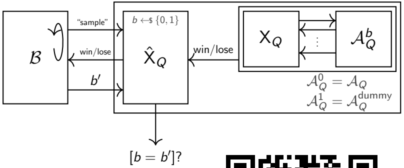
pre-proceeding version **SAC 2025**

Takeaways



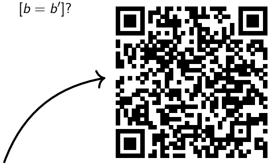
- ✓ Studied the **Bit Security** of the 🔑 with **Statistical Distance**
- ✓ Proposed **a definition** for PQBS based on **Hybrid Observation Game**
- ✓ Fixed **bounds** for the PQBS based on a **Quantum Key Search Game**
- ✓ Gave the interpretation of the bounds:

> $\Rightarrow \Delta < 2^{-\lambda}$, not any advantage for the bit security
> $\Rightarrow 2^{-\lambda} \leq \Delta \leq 2^{-\lambda/2}$, $\Delta = 2^{-\lambda}$ is conservative choice
> $\Rightarrow \Delta > 2^{-\lambda/2}$, is unclear as result for the bit security



evangelos.gkoumas@tu-darmstadt.de

Thank you !



pre-proceeding version 🔗 **SAC 2025**

References I

[BBHT98] Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp.
Tight bounds on quantum searching.
Fortschritte der Physik, 46(4-5):493–505, 1998.

[BGKE20] Darius Bunandar, Luke Govia, Hari Krovi, and Dirk Englund.
Numerical finite-key analysis of quantum key distribution.
npj Quantum Information, 6, 12 2020.

[HSZ24] Xiaoyu He, Xiaoming Sun, and Jialing Zhang.
Quantum search with prior knowledge.
Science China Information Sciences, 67(9):192503, 2024.

[Lee24] Keewoo Lee.
Bit security as cost to demonstrate advantage.
CiC, 1(1):1, 2024.

[LYW+21] Hang Liu, Zhenqiang Yin, Rong Wang, Ze-Hao Wang, Shuang Wang, Wei Chen, Guang-Can Guo, and Zheng-Fu Han.
Tight finite-key analysis for quantum key distribution without monitoring signal disturbance.
npj Quantum Information, 7, 12 2021.

References II

[MCIT15] Akihiro Mizutani, Marcos Curty, Nobuyuki Imoto, and Kiyoshi Tamaki.
Finite-key security analysis of quantum key distribution with imperfect light sources.
New Journal of Physics, 17, 09 2015.

[Mon11] Ashley Montanaro.
Quantum search with advice.
In Wim van Dam, Vivien M. Kendon, and Simone Severini, editors, *Theory of Quantum Computation, Communication, and Cryptography*, pages 77–93, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[MQR09] Jörn Müller-Quade and Renato Renner.
Composability in quantum cryptography.
New Journal of Physics, 11:085006, 2009.

[MW18] Daniele Micciancio and Michael Walter.
On the bit security of cryptographic primitives.
In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 3–28. Springer, Cham, April / May 2018.

[PR22] Christopher Portmann and Renato Renner.
Security in quantum cryptography.
Rev. Mod. Phys., 94:025008, Jun 2022.

References III

[RK05] Renato Renner and Robert König.
Universally composable privacy amplification against quantum adversaries.
In Joe Kilian, editor, *Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005, Proceedings*, volume 3378 of *Lecture Notes in Computer Science*, pages 407–425. Springer, 2005.

[RW23] Renato Renner and Ramona Wolf.
Quantum advantage in cryptography.
AIAA Journal, 61(5):1895–1910, 2023.

[TGR12] Marco Tomamichel, Nicolas Gisin, and Renato Renner.
Tight finite-key analysis for quantum cryptography.
Nature communications, 3:634, 01 2012.

[TL17] Marco Tomamichel and Anthony Leverrier.
A largely self-contained and complete security proof for quantum key distribution.
Quantum, 1:14, 07 2017.

References IV

[WY21] Shun Watanabe and Kenji Yasunaga.
Bit security as computational cost for winning games with high probability.
In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part III*, volume 13092 of *LNCS*, pages 161–188. Springer, Cham, December 2021.

[Zal99] Christof Zalka.
Grover's quantum searching algorithm is optimal.
Physical Review A, 60(4):2746–2751, October 1999.

[ZLR+22] Wei Zhang, Tim Leent, Kai Redeker, Robert Garthoff, René Schwonnek, Florian Fertig, Sebastian Eppelt, Wenjamin Rosenfeld, Valerio Scarani, Charles Lim, and Harald Weinfurter.
A device-independent quantum key distribution system for distant users.
Nature, 607:687–691, 07 2022.

Extra Slides

Upper Bound for the Post-Quantum Bit Security I

- $d_{\text{Hell}}(\mathcal{P}, \mathcal{Q})^2 = 1 - \sqrt{\epsilon_{\mathcal{P}} \cdot \epsilon_{\mathcal{Q}}} - \sqrt{(1-\epsilon_{\mathcal{P}}) \cdot (1-\epsilon_{\mathcal{Q}})}$

Use upper bounds on $\epsilon_{\mathcal{P}}$ and $\epsilon_{\mathcal{Q}}$ to lower-bound the distance:

$$\epsilon_{\mathcal{P}} \cdot \epsilon_{\mathcal{Q}} = \left(16\, T^2_{\mathcal{A}^{\text{ks}}_Q} \cdot 2^{-\lambda} + 2\Delta\right) \cdot \left(2^{-\lambda} + \Delta\right)$$

$$(1-\epsilon_{\mathcal{P}}) \cdot (1-\epsilon_{\mathcal{Q}}) = \left(1 - T^2_{\mathcal{A}^{\text{ks}}_Q} \cdot 2^{-\lambda}\right) \cdot \left(1 - 2^{-\lambda}\right)$$

- **Case 1:** $\Delta \leq 2^{-\lambda},\ T_{\mathcal{A}^{\text{ks}}_Q} \geq 48$:

$$d_{\text{Hell}}\left(\Pr^{\mathsf{G}_Q}_{\mathcal{A}_Q}(\lambda), \Pr^{\mathsf{G}_Q}_{\mathbf{D}[T_{\mathcal{A}^{\text{ks}}_Q}]}(\lambda)\right)^2 \geq \frac{1}{8} T^2_{\mathcal{A}^{\text{ks}}_Q} \cdot 2^{-\lambda} \quad \text{[Lower bound]}$$

$$\Rightarrow \text{[Upper bound]} \quad \mathsf{PQBS}^{\mathsf{G}_Q}_{\text{Hell}^2}(\lambda) \leq \min_{\mathcal{A}^{\text{ks}}_Q}(\lambda - \log T_{\mathcal{A}^{\text{ks}}_Q} + 3).$$

Upper Bound for the Post-Quantum Bit Security II

- **Case 2:** $2^{-\lambda} < \Delta \leq \frac{1}{48^2} T^2_{\mathcal{A}_Q^{\mathsf{ks}}} \cdot 2^{-\lambda}$, with $\sqrt{\gamma} \leq \frac{1}{48}$, then:

$$d_{\mathsf{Hell}}\left(\Pr^{\mathsf{G}_Q}_{\mathcal{A}_Q}(\lambda), \Pr^{\mathsf{G}_Q}_{\mathbf{D}[T_{\mathcal{A}_Q^{\mathsf{ks}}}]}(\lambda)\right)^2 \geq \frac{1}{8} T^2_{\mathcal{A}_Q^{\mathsf{ks}}} \cdot 2^{-\lambda} \quad \text{[Lower bound]}$$

$$\Rightarrow \text{[Upper bound]} \quad \mathsf{PQBS}^{\mathsf{G}_Q}_{\mathsf{Hell}^2}(\lambda) \leq \min_{\mathcal{A}_Q^{\mathsf{ks}}}(\lambda - \log T_{\mathcal{A}_Q^{\mathsf{ks}}} + 3).$$

Lower Bound for the Post-Quantum Bit Security I

- Hellinger Distance:

$$d_{\mathsf{Hell}}(\mathcal{P},\mathcal{Q})^2 \leq d_{\mathsf{TV}}\left(\Pr^{G_Q}_{\mathcal{A}_Q}(\lambda), \Pr^{G_Q}_{\mathbf{D}[T_{\mathcal{A}_Q^{\mathsf{ks}}}]}(\lambda)\right) \leq 16\,T^2_{\mathcal{A}_Q^{\mathsf{ks}}} \cdot 2^{-\lambda} + 2\cdot\Delta$$

- **Case 1:** $\Delta \leq T^2_{\mathcal{A}_Q^{\mathsf{ks}}} \cdot 2^{-\lambda}$

$$d_{\mathsf{Hell}}\left(\Pr^{G_Q}_{\mathcal{A}_Q}(\lambda), \Pr^{G_Q}_{\mathbf{D}[T_{\mathcal{A}_Q^{\mathsf{ks}}}]}(\lambda)\right)^2 \leq 18\,T^2_{\mathcal{A}_Q^{\mathsf{ks}}} \cdot 2^{-\lambda} \quad \text{[Upper bound]}$$

$$\Rightarrow \text{[Lower bound]} \quad \mathsf{PQBS}^{G_Q}_{\mathsf{Hell}^2}(\lambda) \geq \min_{\mathcal{A}_Q^{\mathsf{ks}}}(\lambda - \log T_{\mathcal{A}_Q^{\mathsf{ks}}} - 5)$$

Lower Bound for the Post-Quantum Bit Security II

- **Case 2:** $\Delta > T^2_{\mathcal{A}_Q^{\mathsf{ks}}} \cdot 2^{-\lambda}$

$$d_{\mathsf{Hell}}\left(\Pr^{\mathsf{G}_Q}_{\mathcal{A}_Q}(\lambda), \Pr^{\mathsf{G}_Q}_{\mathbf{D}[T_{\mathcal{A}_Q^{\mathsf{ks}}}]}(\lambda)\right)^2 < 18 \cdot \Delta \quad [\text{Upper bound}]$$

$$\Rightarrow [\text{Lower bound}] \quad \mathsf{PQBS}^{\mathsf{G}_Q}_{\mathsf{Hell}^2}(\lambda) \geq \min_{\mathcal{A}_Q^{\mathsf{ks}}}(\log T_{\mathcal{A}_Q^{\mathsf{ks}}} - \log \Delta - 5)$$

If $\Delta = \gamma \cdot T^2_{\mathcal{A}_Q^{\mathsf{ks}}} \cdot 2^{-\lambda}$, with $\gamma > 1$, then

$$\mathsf{PQBS}^{\mathsf{G}_Q}_{\mathsf{Hell}^2}(\lambda) \geq \min_{\mathcal{A}_Q^{\mathsf{ks}}}(\lambda - \log T_{\mathcal{A}_Q^{\mathsf{ks}}} - \log \gamma - 5)$$

QKD Error Parameters

Error Decomposition in QKD
[RK05, MQR09, TGR12, MCIT15, TL17, BGKE20, PR22, LYW+21, RW23]:

$$\varepsilon = \varepsilon_{\text{correct}} + \varepsilon_{\text{secure}}$$

$\Rightarrow \varepsilon_{\text{correct}}$: Not **Identical keys** for both parties.
$\Rightarrow \varepsilon_{\text{secure}}$: Adversary has **information about key**.

- In [RK05, MQR09, TL17, BGKE20, PR22, RW23] **trace distance** $\approx$ statistical distance.

Discussion Points:

- $\varepsilon_{\text{secure}}$ corresponds to our **statistical distance**.
- Choosing $\varepsilon_{\text{correct}} = \varepsilon_{\text{secure}}$ is **cryptographically problematic**:
  - Correctness is verifiable; secrecy is not.
  - So: $\varepsilon_{\text{secure}} \ll \varepsilon_{\text{correct}}$ is often preferable.
  - The more realistic option is maybe $\varepsilon = 10^{-5}$ by [ZLR+22].

Privacy Amplification and Bit Security

Impact of $\varepsilon_{\text{secure}}$ on Privacy Amplification:

$$\textbf{Cut bits} \approx 2\log\frac{1}{\varepsilon_{\text{secure}}}$$

Example: AES-256 Key

- For $\varepsilon_{\text{secure}} = 2^{-40}$: need **80** extra bits.
  $\Rightarrow 256 + 80 = 336$ reconciled bits for $\varepsilon_{\text{secure}} = 2^{-40}$.
- For $\varepsilon_{\text{secure}} = 2^{-256}$: need **512** extra bits.
  $\Rightarrow 256 + 512 = 768$ reconciled bits for $\varepsilon_{\text{secure}} = 2^{-256}$.

Thoughts:

- The value ε in literature is maybe **optimistic**.
- The security level depends sensitively on $\varepsilon_{\text{secure}}$, **not just the sum**.