Provable security from a cryptanalysis perspective

Tim Beyne

COSIC, KU Leuven

September 1, 2025

~~Provable~~ security from a cryptanalysis perspective

Information-theoretical

Tim Beyne

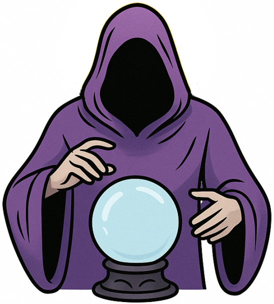
COSIC, KU Leuven

September 1, 2025

Three questions about provable security

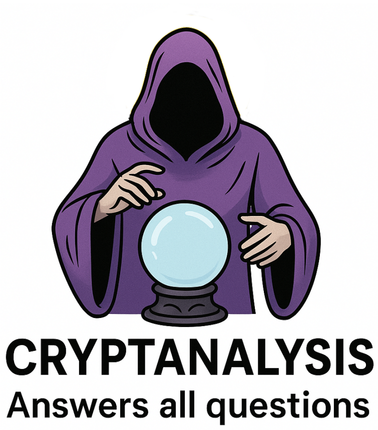
- How to define security?
- How to model primitives?
- What are the limits of information-theoretical security?

Answers from the point of view of cryptanalysis.



CRYPTANALYSIS

Answers all questions



… or maybe cryptanalysis can learn something too …

How to define security?

How to define security?

Cryptanalysis

- Key-recovery, message-recovery, forgery, collision, preimage, ...
- Attacks are often based on *distinguishers* (i.e. use the 'last round trick')
  ... but lines between key-recovery and distinguisher are blurring and will disappear

How to define security?

Cryptanalysis

- Key-recovery, message-recovery, forgery, collision, preimage, ...
- Attacks are often based on *distinguishers* (i.e. use the 'last round trick')
  ... but lines between key-recovery and distinguisher are blurring and will disappear

---

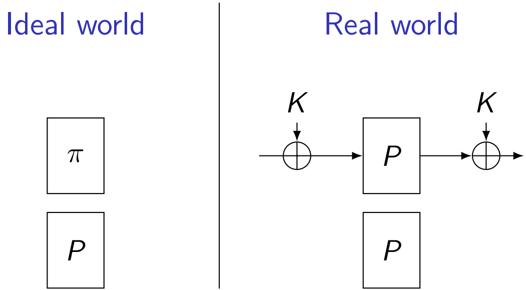
Information-theoretical security

- Indistinguishability as worst case security

End users don't care about indistinguishability from an idealized construction

Subtle difference in meaning of 'distinguisher'

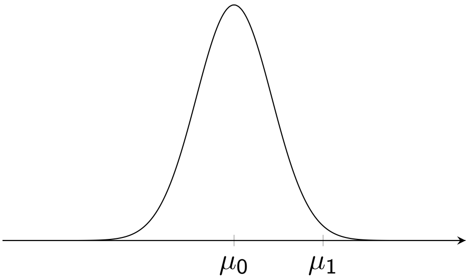
Indistinguishability



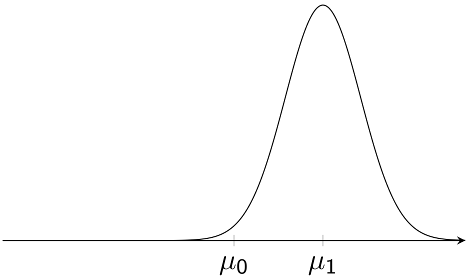
- Uniform random permutation π
- Public uniform random permutation P

Indistinguishability a.k.a. simple hypothesis testing

Null hypothesis



Alternative hypothesis



- Transcript set T
- Probability distributions P and Q: $2^T \to [0, 1]$

Indistinguishability

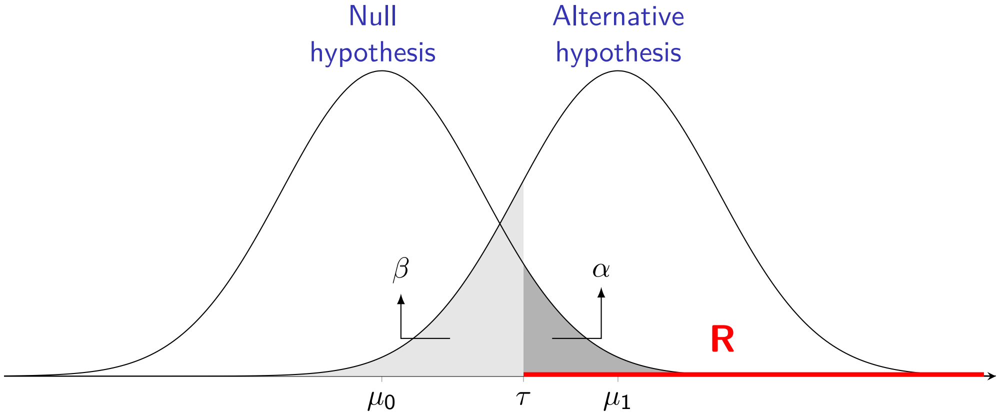
How to measure the power of adversaries?

- Provable security approach: *statistical distance* or total variation distance

$$\Delta(P, Q) = \max_{E \subset T} P(E) - Q(E)$$

- Statistical distance is usually not used in cryptanalysis (for good reasons)
- Neyman and Pearson (1930s):
  - False-positive (probability α) and false-negative (probability β) results
  - Minimize the overall cost of errors $C(\alpha, \beta)$

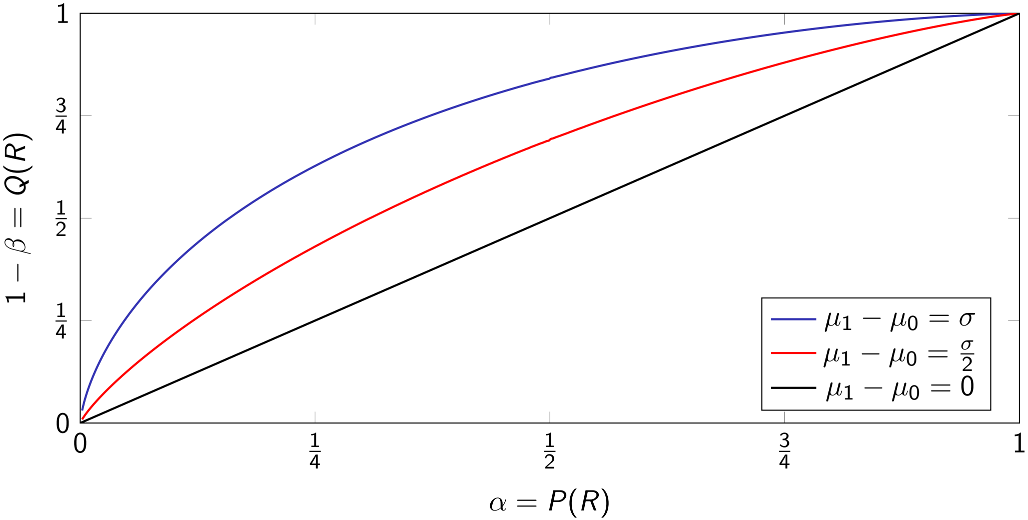
Neyman-Pearson theory of hypothesis testing



- If transcript is in R, reject the null hypothesis (❗ R is the adversary)
- False positive probability $\alpha = P(R)$ and false negative probability $\beta = 1 - Q(R)$

Neyman-Pearson theory of hypothesis testing

Receiver operating characteristic curve



Indistinguishability

How to measure the power of adversaries?

- *Advantage bound* for an advesary (i.e. a rejection region R) is

$$1 - \alpha - \beta = Q(R) - P(R) \leq \Delta(P, Q)$$

- Bounds cost function $C(\alpha, \beta) = \alpha + \beta$ from below

Indistinguishability

How to measure the power of adversaries?

- *Advantage bound* for an advesary (i.e. a rejection region R) is

$$1 - \alpha - \beta = Q(R) - P(R) \le \Delta(P, Q)$$

- Bounds cost function $C(\alpha, \beta) = \alpha + \beta$ from below

---

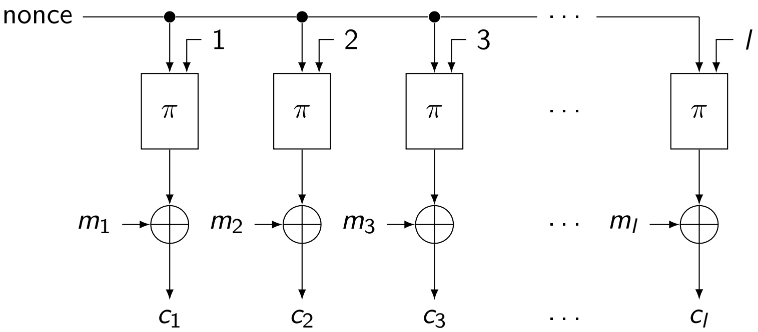
- *Power bound* (with YL Chen, Crypto 2024):

$$1 - \beta \le f(\alpha)$$

- Bounds any increasing cost function $C(\alpha, \beta)$ from below

Power bounds

Example: block cipher in counter mode



- Assume P is the ideal world and Q is the real world (! this matters)
- Proof comes down to prp-prf switching lemma

Power bounds

Example: block cipher in counter mode

- Conditional probability distribution (for event $E \subset T$):

$$P_E(R) = \frac{P(R \cap E)}{P(E)}$$

- Excluding a 'bad event' B of probability $\varepsilon = P(B)$:

$$P_{T \setminus B}(R) \leq \frac{P(R)}{1 - \varepsilon}$$

Power bounds

Example: block cipher in counter mode

- Conditional probability distribution (for event $E \subset T$):

$$P_E(R) = \frac{P(R \cap E)}{P(E)}$$

- Excluding a 'bad event' B of probability $\varepsilon = P(B)$:

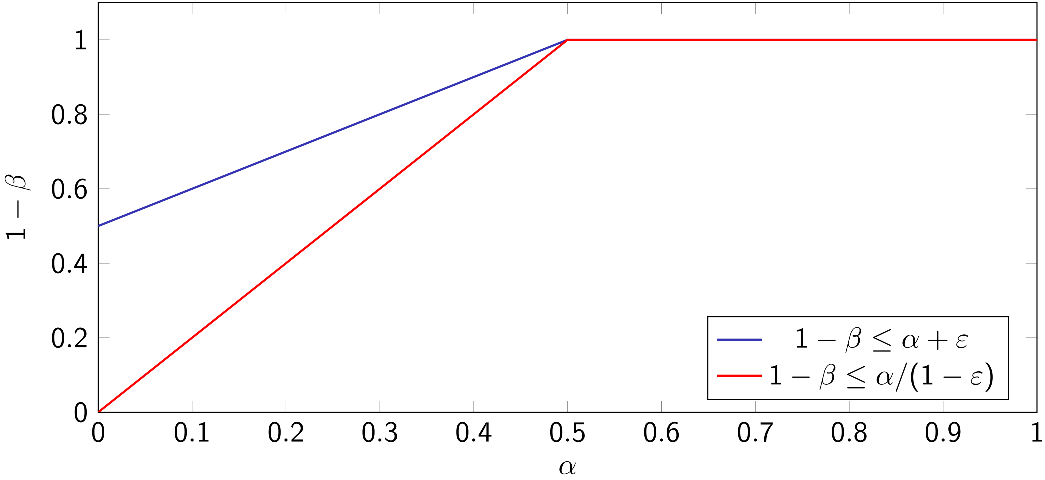
$$P_{T \setminus B}(R) \leq \frac{P(R)}{1 - \varepsilon}$$

- Since $Q = P_{T \setminus B}$ and $\varepsilon \leq \frac{1}{N}\binom{\sigma}{2}$ for $\sigma \leq \sqrt{2N}$ blocks,

$$1 - \beta \leq \frac{\alpha}{1 - \frac{\sigma(\sigma-1)}{2N}}$$

Power bounds

Example: block cipher in counter mode



Misconceptions about attacks

- Advantages and statistical distance are arbitrary
- Why is this a problem?

Misconceptions about attacks

- Advantages and statistical distance are arbitrary
- Why is this a problem?
- Examples of misconceptions about attacks:
  - ‘Attacks are symmetric’
  - ‘Reductions to indistinguishability are tight’
- See paper for applications such as multi-user security

https://eprint.iacr.org/2024/658

Misconceptions about attacks
#1. ‘Attacks are symmetric’

- Distinguishing P from Q is not the same as distinguishing Q from P
- $C(\alpha, \beta) \neq C(\beta, \alpha)$

Misconceptions about attacks

#1. 'Attacks are symmetric'

- Distinguishing P from Q is not the same as distinguishing Q from P
- $C(\alpha, \beta) \neq C(\beta, \alpha)$
- Example: counter mode

$$1 - \beta \leq \frac{\alpha}{1 - \frac{\sigma(\sigma-1)}{2N}} \quad \text{versus} \quad 1 - \beta \leq \frac{\sigma(\sigma-1)}{2N} + \left(1 - \frac{\sigma(\sigma-1)}{2N}\right)\alpha$$

Collision happens

Misconceptions about attacks

#2. 'Reductions to indistinguishability are tight'

- Example: full recovery of a b-bit message in counter mode
- Success probability P_S

Advantage bound

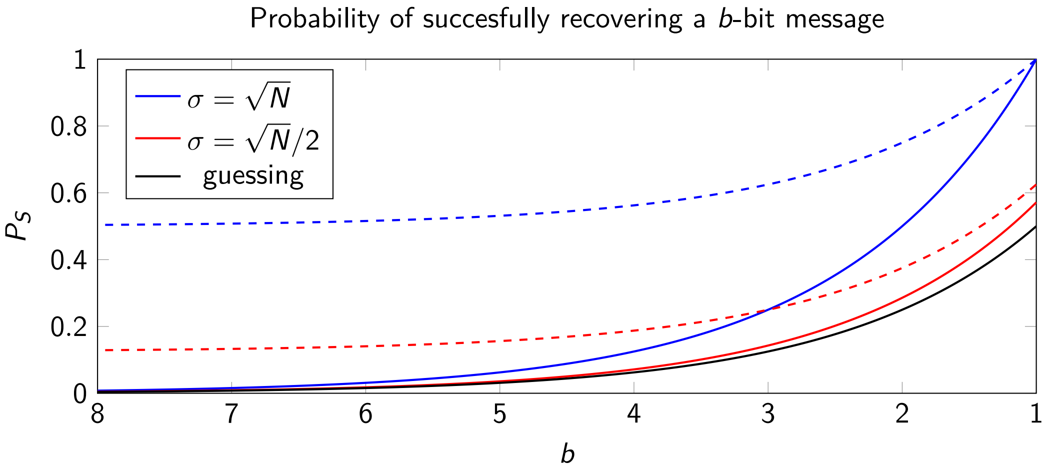
$$P_S \leq \frac{\sigma(\sigma-1)}{2N} + 2^{-b}$$

Power bound

$$P_S \leq \frac{2^{-b}}{1 - \frac{\sigma(\sigma-1)}{2N}}$$

Misconceptions about attacks

#2. 'Reductions to indistinguishability are tight'



How to model primitives?

How to model primitives?

Cryptanalysis

- Only model part of the primitive, using trails $(V_1, V_2, \ldots, V_{r+1})$
- Used to be probabilistic, but not anymore (for good reasons)

How to model primitives?

Cryptanalysis

- Only model part of the primitive, using trails $(V_1, V_2, \ldots, V_{r+1})$
- Used to be probabilistic, but not anymore (for good reasons)

Information-theoretical security

- Standard model:

$$\text{Block cipher} \approx \text{Uniform random permutation (prp-security)}$$

- Ideal model:

$$\text{Block cipher} \approx \text{Ideal cipher (idealization)}$$
$$\text{Permutation} \approx \text{Uniform random permutation}$$

How to model primitives?
Standard model

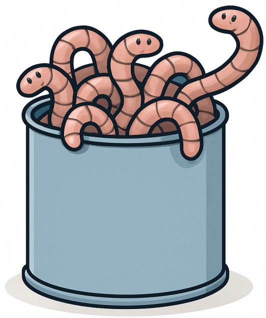
- In practice:
  - Replace PRP with uniform random permutation
  - Just another ideal model?
- Ignore the PRP term
  - Maybe cryptanalysts know what it is?

How to model primitives?

Standard model

- In practice:
  - Replace PRP with uniform random permutation
  - Just another ideal model? Yes
- Ignore the PRP term
  - Maybe cryptanalysts know what it is?
  - No, and actually ...

How to model primitives?
Standard model



- See Koblitz and Menezes, Bernstein and Lange

How to model primitives?

Standard model meets linear cryptanalysis

- Block cipher E_k and a mask v

$$\Pr_{\boldsymbol{k}}\left[v^T E_{\boldsymbol{k}}(00\cdots 0) = 0\right] = \frac{1}{2} + \varepsilon$$

- For an n bit key, typically $\varepsilon \approx 2^{-n/2}$ (cf. zero-correlation linear cryptanalysis)

How to model primitives?

Standard model meets linear cryptanalysis

- Block cipher E_k and a mask v

$$\Pr_{\boldsymbol{k}}\left[v^T E_{\boldsymbol{k}}(00\cdots0) = 0\right] = \frac{1}{2} + \varepsilon$$

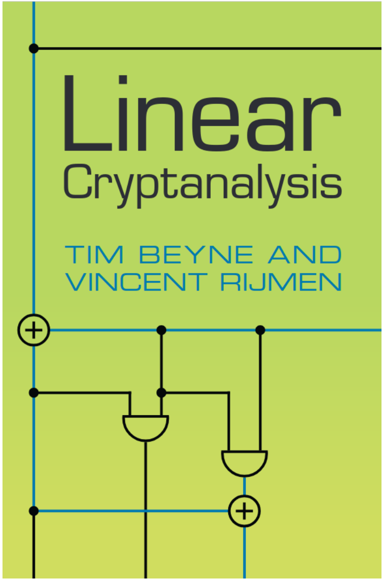
- For an n bit key, typically $\varepsilon \approx 2^{-n/2}$ (cf. zero-correlation linear cryptanalysis)

- Multidimensional linear cryptanalysis: with M memory and T time, for $\alpha = \frac{1}{2}$:

$$1 - \beta = \frac{1}{2} + \Omega\left(\sqrt{\frac{T \times M}{2^n}}\right)$$

- Actual block ciphers are not good PRPs

Commercial break



How to model primitives?

Ideal model

- Ideal model allows making p queries to the ideal cipher
- In practice, the ideal model is stronger than the standard model
  - Set $p = 0$ to recover standard model bound (without PRP term)
  - Primitive queries are important (capture real generic attacks)

⚠ Widespread confusion between *primitive model* and *access model*

What are the limits of information-theoretical security?

What are the limits of information-theoretical security?

- Information-theoretical security of real block ciphers $\approx$ none
- Weaker security notions?
- Randomess trap
  - Don't expect too much (often results in ignoring important aspects)
  - Not every idealization must be based on randomness (examples in cryptanalysis)

What are the limits of information-theoretical security?

Pointwise decorrelation

- Pointwise independence: for all x and y,

$$\Pr_{\boldsymbol{k}}\left[E_{\boldsymbol{k}}(x) = y\right] = \frac{1}{N}$$

- Example: $x \mapsto x + k$

- Nonetheless, does not hold for most block ciphers (barely enough randomness)
  cf. issues with definition of prp security

What are the limits of information-theoretical security?

Pairwise decorrelation (a.k.a. pairwise independence)

- Pairwise independence: for all $(x_1, x_2), (y_1, y_2)$ with $x_1 \neq x_2$ and $y_1 \neq y_2$,

$$\Pr_{\boldsymbol{k}}\left[(E_{\boldsymbol{k}}(x_1), E_{\boldsymbol{k}}(x_2)) = (y_1, y_2)\right] = \frac{1}{N} \times \frac{1}{N-1}$$

- Example: $x \mapsto k_1 \cdot x + k_2$ (exclude zero)
- Most block ciphers are not pairwise independent (not enough randomness)

Pairwise independence

- ε-pairwise indepencence: for all (x_1, x_2) with $x_1 \neq x_2$,

$$\frac{1}{2} \sum_{y_1 \neq y_2} \left| \Pr_{\boldsymbol{k}}\left[(E_{\boldsymbol{k}}(x_1), E_{\boldsymbol{k}}(x_2)) = (y_1, y_2)\right] - \frac{1}{N} \times \frac{1}{N-1} \right| \leq \varepsilon$$

- Example: $x \mapsto k_1 \cdot x + k_3$ is ε-pairwise independent with $\varepsilon = 1/2N$
- ε is large for most block ciphers (barely enough randomness)
- Key-alternating block ciphers with independent and uniform random rounds keys

Pairwise independence

- Round keys are not independent

Pairwise independence

- **Round keys are not independent**

Pairwise independence

- **Round keys are not independent**
- So, what is the point?

Pairwise independence

- **Round keys are not independent**
- So, what is the point?
- Actually, we don't even need keys for pairwise independence to be meaningful
- Pairwise independence rules out some cryptanalytic techniques
  - Differential cryptanalysis if quasidifferential trails with nonzero masks are ignored
  - Class of techiques can be defined in terms of trails (geometric approach)

Pairwise independence

AES with independent round keys

- Variant of the AES with r rounds and independent round keys
- Liu, Tessaro and Vaikuntanathan:

$$\varepsilon = (0.924)^r$$

- Need $r \geq 9168$ to get $\varepsilon \leq 2^{-128}$

Pairwise independence

AES with independent round keys

- Variant of the AES with r rounds and independent round keys
- Liu, Tessaro and Vaikuntanathan:

$$\varepsilon = (0.924)^r$$

- Need $r \geq 9168$ to get $\varepsilon \leq 2^{-128}$
- Recent joint work with Gregor Leander and Immo Schütt (ePrint 2025/1495):

$$\varepsilon = 2^{44} \cdot 2^{-30\lfloor \frac{r}{4} \rfloor}$$

- Need $r \geq 24$ to get $\varepsilon \leq 2^{-128}$
- These are preliminary results (large improvement in exponent still unpublished)

Pairwise independence

AES with independent round keys

- Proof: see ePrint 2025/1495 (only 5 pages!)
- Idea developed in 2021 to address a question from Rønjom (ePrint 2019/622)
- Application to pairwise independence:
  Master's thesis of Immo Schütt (Ruhr University Bochum, March 2025)
- Techniques used:
  - Essentially an application of the geometric approach to cryptanalysis
  - Truncated differentials and singular values of the difference-distribution matrix

Pairwise independence

AES with independent round keys

- Let D be the difference-distribution matrix of a *random cipher* $E_{\boldsymbol{k}}$ with whitening

$$D_{b,a} = \Pr_{\boldsymbol{k},\boldsymbol{x}}\left[E_{\boldsymbol{k}}(\boldsymbol{x} + a) = E_{\boldsymbol{k}}(\boldsymbol{x}) + b\right]$$

  (it doesn't matter what $\boldsymbol{x}$ is, you can take it either random or fixed)

- $E_{\boldsymbol{k}}$ is pairwise independent if and only if $\|D - U\|_\infty \leq 2\varepsilon$
- We show that $\|D - U\|_2 \leq 2^{-30}$ for four-round AES with independent round keys
- In several ways, $\|\cdot\|_2$ is actually better motivated than $\|\cdot\|_\infty$ (cf. power bounds)

Pairwise independence
AES with independent round keys

Activity patterns

- Familiar concept from cryptanalysis
- For $z \in \{0,1\}^n$, define $[z] = [z_1] \times [z_2] \times \cdots \times [z_n]$ with $[0] = \{0\}$ and $[1] = \mathbb{F}_q$
- Let $V = \mathrm{Span}\left\{\delta_{[z]} \mid z \in \{0,1\}^n\right\} \subset \mathbb{R}[\mathbb{F}_q^n]$, with $\delta_{[z]}$ the indicator of $[z]$

Trails and approximation maps

- Basis-free geometric approach for inner product spaces (Crypto 2021)
- Approximation maps $\pi_V D\, i_V$, $\pi_{V^\perp} D\, i_V$, $\pi_V D\, i_{V^\perp}$ and $\pi_{V^\perp} D\, i_{V^\perp}$

Pairwise independence

AES with independent round keys

- Trails determined by the decomposition $\mathbb{R} = V \oplus V^{\perp}$ give

$$\left\|D - U\right\|_2 \leq \left\| \begin{bmatrix} \|\pi_V \ (D-U) i_V\|_2 & \|\pi_V \ (D-U)\, i_V \ \|_2 \\ \|\pi_{V^\perp}(D-U)\, i_V\|_2 & \|\pi_{V^\perp}(D-U)\, i_{V^\perp}\|_2 \end{bmatrix} \right\|_2 .$$

- Term $\pi_V(D-U)i_V$: truncated differentials defined by activity patterns
  - Compute it numerically ($2^n \times 2^n$ matrix)
  - Closed-form formula based on Frobenius norm: $\|\pi_V(D-U)i_V\|_2 \leq (2/(\sqrt{q}-1))^n$
- Other terms: bound using $\sigma_3(D^S)$, easiest approach is Frobenius norm

Three questions about provable security

- How to define security?
  Indistinguishability as a basis, but don't forget what the end user needs
  Consider alternatives to advantage bounds (such as power bounds)

- How to model primitives?
  Prefer the ideal model over the standard model (primitive queries are important)
  In practice, the standard model is just another ideal model

- What are the limits of information-theoretical security?
  Don't fall into the randomness trap
  Not every idealization must be based on randomness (trails in cryptanalysis **!**)