CWI

An All-But-One Entropic Uncertainty Relation and Application to Password-based Identification

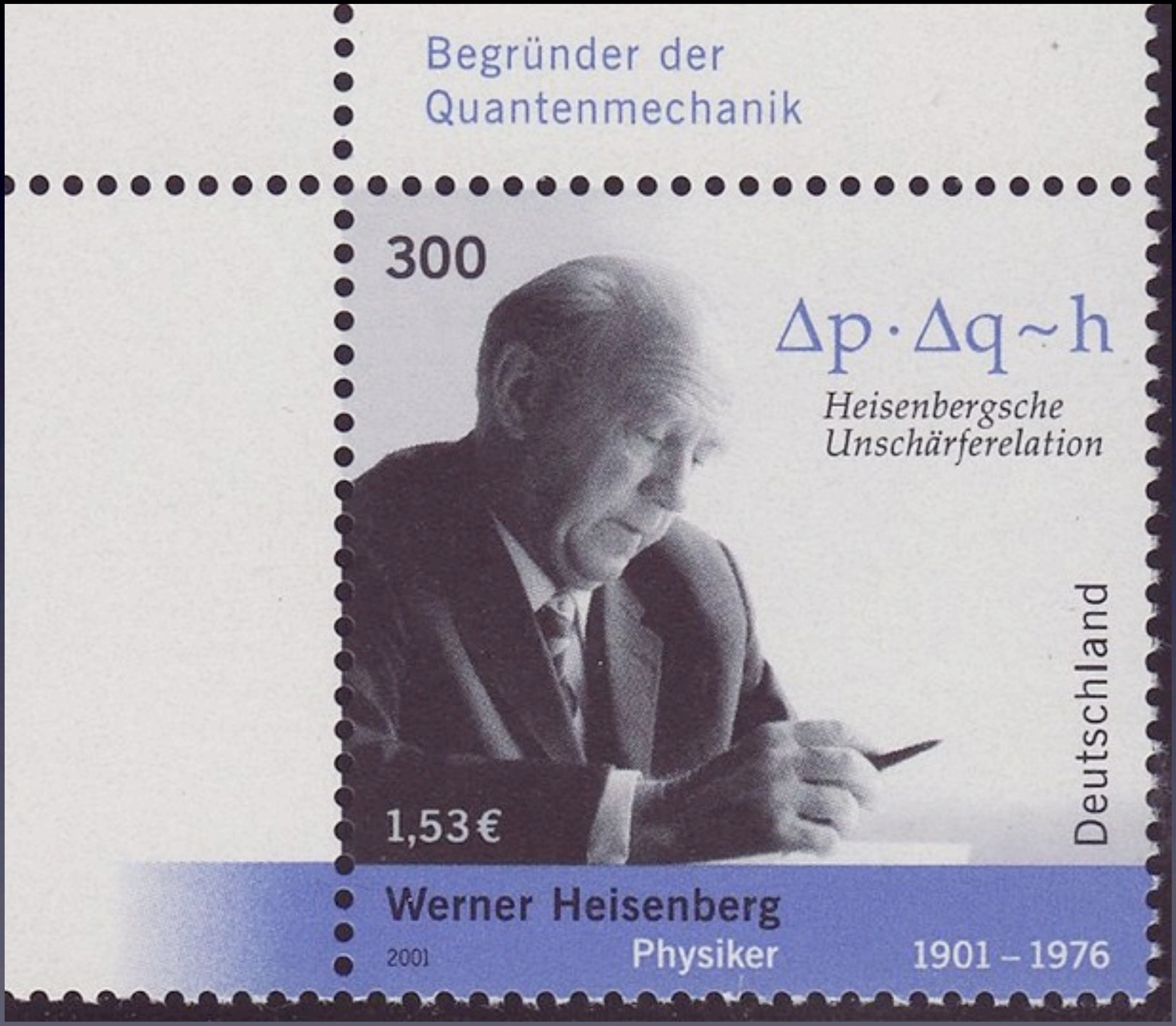
Niek J. Bouman, Serge Fehr, Carlos Gonzáles-Guillén, Christian Schaffner

Thu, Sept 15 / QCRYPT 2011 / ETH Zürich

University of Amsterdam

Instituto de Matemática Interdisciplinar

Uncertainty Relations



Uncertainty Relations

First *Entropic* Uncertainty Relation:
Isodore Hirschman (1957)

Uncertainty Relations

First *Entropic* Uncertainty Relation:
Isodore Hirschman (1957)

A more well-known entropic UR:
Maassen-Uffink (1988)

Definition

Let $\{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ be a family of orthonormal bases for an n-qubit Hilbert space. We define the **maximum overlap** of this family as the number

Definition

Let $\{\mathcal{B}_1,\ldots,\mathcal{B}_m\}$ be a family of orthonormal bases for an n-qubit Hilbert space. We define the maximum overlap of this family as the number

$$c := \max\{|\langle\phi|\psi\rangle| : |\phi\rangle \in \mathcal{B}_j, |\psi\rangle \in \mathcal{B}_k, 1 \leq j < k \leq m\}$$

Definition

Let $\{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ be a family of orthonormal bases for an n-qubit Hilbert space. We define the **maximum overlap** of this family as the number

$$c := \max\{|\langle\phi|\psi\rangle| : |\phi\rangle \in \mathcal{B}_j, |\psi\rangle \in \mathcal{B}_k, 1 \leq j < k \leq m\}$$

Example

For the family consisting of the computational and Hadamard basis on n qubits,

$$c = 2^{-n/2}$$

Definition

Let $\{\mathcal{B}_1,\ldots,\mathcal{B}_m\}$ be a family of orthonormal bases for an n-qubit Hilbert space. We define the maximum overlap of this family as the number

$$c := \max\{|\langle\phi|\psi\rangle| : |\phi\rangle \in \mathcal{B}_j, |\psi\rangle \in \mathcal{B}_k, 1 \leq j < k \leq m\}$$

Example

For the family consisting of the computational and Hadamard basis on n qubits,

$$c = 2^{-n/2}$$

Remark

For "good" families, $\lim_{n \to \infty} -\frac{1}{n} \log_2 c \in (0, \frac{1}{2}]$

$\{\mathcal{B}_1,\ldots,\mathcal{B}_m\}$ = family of bases for n-qubit space, with max. overlap c

$\{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ = family of bases for n-qubit space, with max. overlap c

Theorem (Maassen-Uffink)

For all n-qubit states ρ it holds that when measuring such a state either in basis $\mathcal{B}_j$ or $\mathcal{B}_k$

$$H(X \mid J = j) + H(X \mid J = k) \geq -2 \log(c)$$

$$\forall\, j \neq k \in [m]$$

where X is the outcome when measuring in $\mathcal{B}_J$

Applications of Uncert. Relations

Applications of Uncert. Relations

- They deepen our understanding of Quantum Mechanics

Applications of Uncert. Relations

- They deepen our understanding of Quantum Mechanics
- Entropic Uncertainty Relations that give a bound on the min-entropy are convenient proof-tools in quantum cryptography

$$H_{\min}(X) := -\log \max_x P_X(x)$$

Applications of Uncert. Relations

- They deepen our understanding of Quantum Mechanics
- Entropic Uncertainty Relations that give a bound on the min-entropy are convenient proof-tools in quantum cryptography

$$H_{\min}(X) := -\log \max_x P_X(x)$$

- ...

Contribution

Contribution

A new entropic uncertainty relation, with three key properties

Contribution

A new entropic uncertainty relation, with three key properties

1. Min-entropy as uncertainty measure

Contribution

A new entropic uncertainty relation, with three key properties

1. Min-entropy as uncertainty measure
2. Guarantees uncertainty in the measurement outcome for “all-but-one” measurements

Contribution

A new entropic uncertainty relation, with three key properties

1. Min-entropy as uncertainty measure
2. Guarantees uncertainty in the measurement outcome for "all-but-one" measurements
3. Compatible with single-qubit measurements, hence usable to prove the security of schemes that can be implemented with today's technology

Talk Plan

Talk Plan

1. State and explain the new uncertainty relation

Talk Plan

1. State and explain the new uncertainty relation
2. Discuss main application: Password-based Identification

Main Theorem

Main Theorem

Let $\{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ be a family of bases with maximum overlap c.

Main Theorem

Let $\{\mathcal{B}_1,\ldots,\mathcal{B}_m\}$ be a family of bases with maximum overlap c.

For all n-qubit states ρ and for all RVs J over $[m]$ (independent of ρ), there exists a RV J' over $[m]$ that is independent of J, such that:

Main Theorem

Let $\{\mathcal{B}_1,\ldots,\mathcal{B}_m\}$ be a family of bases with maximum overlap c.

For all n-qubit states ρ and for all RVs J over $[m]$ (independent of ρ), there exists a RV J' over $[m]$ that is independent of J, such that:

$$H_{\min}(X|J=j, J'=j') \gtrapprox -\log(c) \quad \forall j \neq j' \in [m]$$

Main Theorem

Let $\{\mathcal{B}_1,\ldots,\mathcal{B}_m\}$ be a family of bases with maximum overlap c.

For all n-qubit states ρ and for all RVs J over $[m]$ (independent of ρ), there exists a RV J' over $[m]$ that is independent of J, such that:

$$H_{\min}(X|J=j, J'=j') \gtrapprox -\log(c) \quad \forall j \neq j' \in [m]$$

where X is the outcome when measuring in $\mathcal{B}_J$.

Our Result Explained

Our Result Explained

Contribution

A new entropic uncertainty relation, with three key properties

1. Min-entropy as uncertainty measure
2. Guarantees uncertainty in the measurement outcome for "all-but-one" measurements
3. Compatible with single-qubit measurements, hence usable to prove the security of schemes that can be implemented with today's technology

Our Result Explained

Contribution

A new entropic uncertainty relation, with three key properties

1. ~~Min-entropy as uncertainty measure~~
2. Guarantees uncertainty in the measurement outcome for "all-but-one" measurements
3. Compatible with single-qubit measurements, hence usable to prove the security of schemes that can be implemented with today's technology

$\{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ = family of bases for n-qubit space, with max. overlap c

$\{\mathcal{B}_1,\ldots,\mathcal{B}_m\}$ = family of bases for n-qubit space, with max. overlap c

Theorem (Maassen-Uffink)

For all n-qubit states ρ it holds that when measuring such a state either in basis $\mathcal{B}_j$ or $\mathcal{B}_k$

$$H(X\,|\,J=j) + H(X\,|\,J=k) \geq -2\log(c)$$

$$\forall\, j \neq k \in [m]$$

where X is the outcome when measuring in $\mathcal{B}_J$

$\{\mathcal{B}_1,\ldots,\mathcal{B}_m\}$ = family of bases for n-qubit space, with max. overlap c

Theorem (Maassen-Uffink)

For all n-qubit states ρ it holds that when measuring such a state either in basis $\mathcal{B}_j$ or $\mathcal{B}_k$

$$H(X\,|\,J=j) + H(X\,|\,J=k) \geq -2\log(c)$$

$$\forall\, j \neq k \in [m]$$

where X is the outcome when measuring in $\mathcal{B}_J$

⇒ There exists at most one $j' \in [m]$ such that

$$H(X\,|\,J=j') < -\log(c)$$

$\{\mathcal{B}_1, \dots, \mathcal{B}_m\}$ = family of bases for n-qubit space, with max. overlap c

Theorem (Maassen-Uffink)

For all n-qubit states ρ it holds that when measuring such a state either in basis $\mathcal{B}_j$ or $\mathcal{B}_k$

$$H(X\,|\,J=j) + H(X\,|\,J=k) \geq -2\log(c)$$

$$\forall\, j \neq k \in [m]$$

where X is the outcome when measuring in $\mathcal{B}_J$

⇒ There exists at most one $j' \in [m]$ such that

$$H(X\,|\,J = j') < -\log(c)$$

All-but-One Shannon Entropy Uncert. Relation

$$H(X\,|\,J = j) \geq -\log(c) \qquad \forall\, j \neq j'$$

Comparison

All-but-One Shannon-Entr. UR (follows from Maassen Uffink)	New All-b.-One Min-Entropy UR
$H(X \mid J = j) \geq -\log(c)$ $\forall\, j \neq j'$	$H_{\min}(X \mid J{=}j,\ J'{=}j') \gtrsim -\log(c)$ $\forall\, j \neq j'$

Comparison

All-but-One Shannon-Entr. UR (follows from Maassen Uffink)	New All-b.-One Min-Entropy UR
$H(X \mid J = j) \geq -\log(c)$ $\forall j \neq j'$	$H_{\min}(X \mid J{=}j, J'{=}j') \gtrapprox -\log(c)$ $\forall j \neq j'$

Is this RV J' necessary?

Comparison

All-but-One Shannon-Entr. UR (follows from Maassen Uffink)	New All-b.-One Min-Entropy UR
$H(X \mid J = j) \geq -\log(c)$ $\forall\, j \neq j'$	$H_{\min}(X \mid J{=}j,\ J'{=}j') \gtrapprox -\log(c)$ $\forall\, j \neq j'$

Is this RV J' necessary?

Recall: For "good" families of bases on an n-qubit space, $-\log(c)$ is linear in n

Necessity of J'

Example with "good" family of bases,
for which $H_{\min}(X \mid J{=}j){=}1 \quad \forall j$

Necessity of J'

Example with "good" family of bases, for which $H_{\min}(X \mid J{=}j){=}1 \quad \forall j$

Let ρ be the n-qubit mixture:

$$\rho = \tfrac{1}{2}|0\cdots0\rangle\langle0\cdots0| + \tfrac{1}{2}|+\cdots+\rangle\langle+\cdots+|$$

Necessity of J'

Example with "good" family of bases,
for which $H_{\min}(X \mid J{=}j){=}1 \quad \forall j$

Let ρ be the n-qubit mixture:

$$\rho = \tfrac{1}{2}|0\cdots0\rangle\langle0\cdots0| + \tfrac{1}{2}|+\cdots+\rangle\langle+\cdots+|$$

equivalently:

$\rho = |0\cdots0\rangle\langle0\cdots0|$ with prob. ½

$\rho = |+\cdots+\rangle\langle+\cdots+|$ with prob. ½

Necessity of J'

Example with "good" family of bases,
for which $H_{\min}(X \mid J{=}j){=}1 \quad \forall j$

Let ρ be the n-qubit mixture:

$$\rho = \tfrac{1}{2}|0\cdots0\rangle\langle0\cdots0| + \tfrac{1}{2}|+\cdots+\rangle\langle+\cdots+|$$

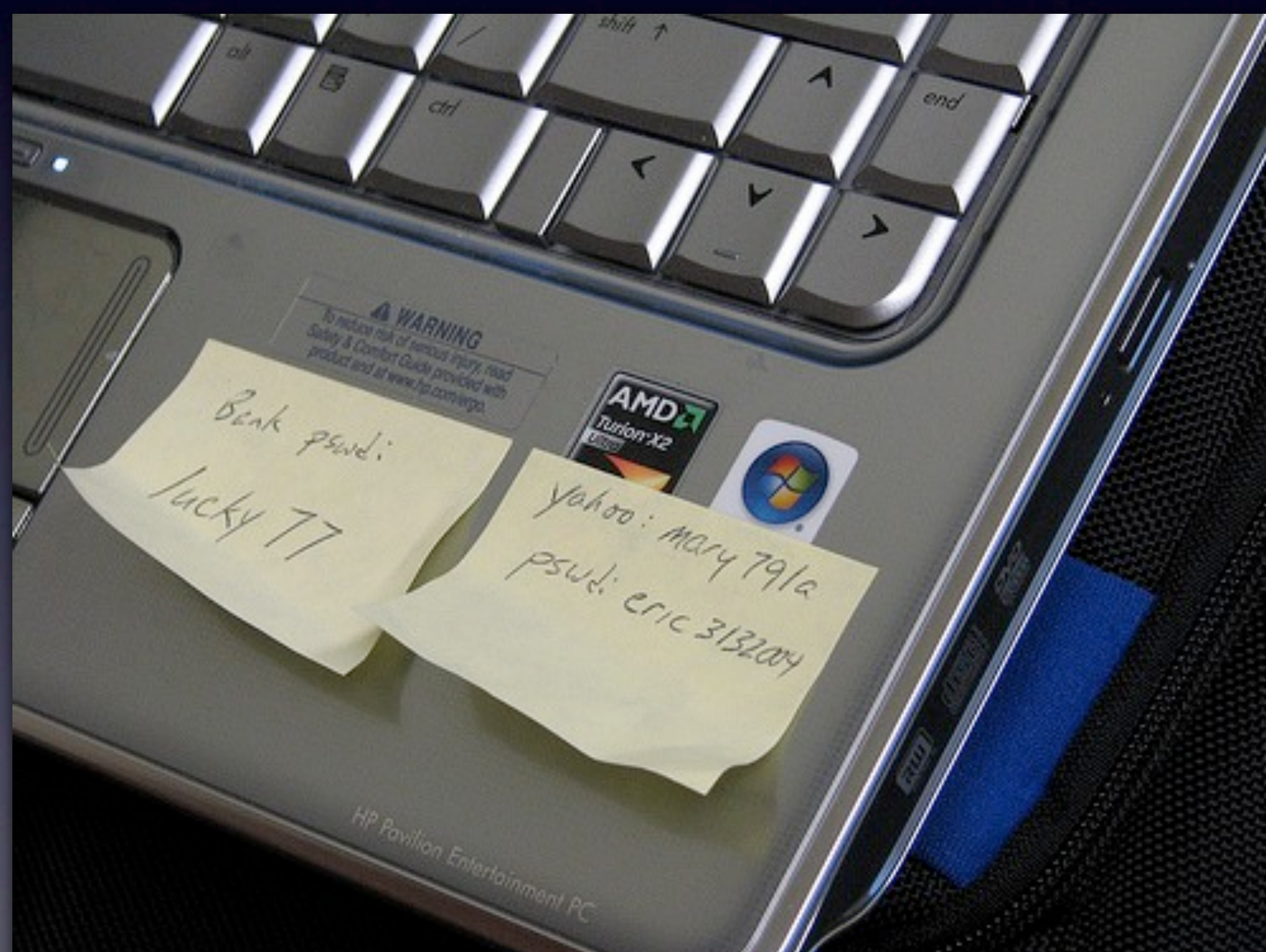
equivalently:

$\rho = |0\cdots0\rangle\langle0\cdots0|$ with prob. ½

$\rho = |+\cdots+\rangle\langle+\cdots+|$ with prob. ½

The family of (meas.) bases is $\{\mathrm{Comp}, \mathrm{Hadamard}\}$,
on n qubits for which $c = 2^{-n/2}$

Application: Password-Based Identification



Application: Password-Based Identification

User

Server

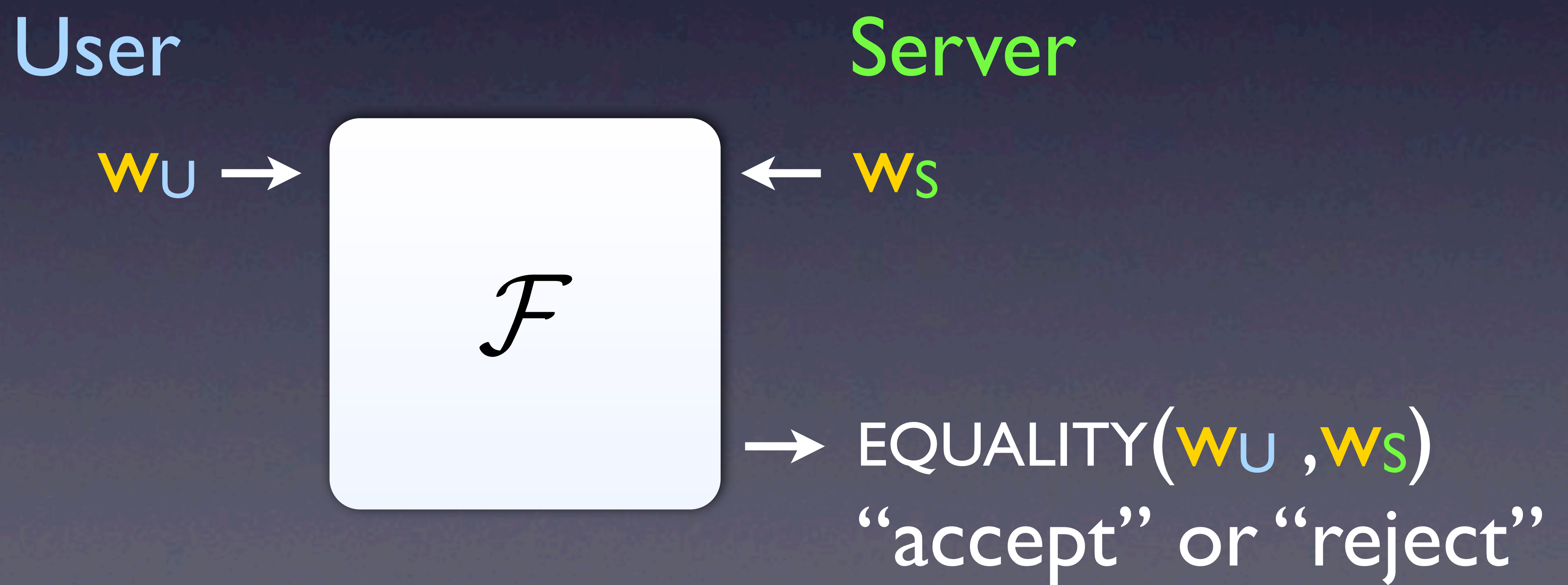
Application: Password-Based Identification

- User proves knowledge of password w to Server, such that a dishonest party learns (almost) no information about w

User Server

Application: Password-Based Identification

- User proves knowledge of password w to Server, such that a dishonest party learns (almost) no information about w



Impossibility Result [DFSS07]

Any quantum identification (QID) scheme can be broken by a malicious party with unbounded quantum storage and unbounded quantum computation

Impossibility Result [DFSS07]

Any quantum identification (QID) scheme can be broken by a malicious party with unbounded quantum storage and unbounded quantum computation

Circumventing the Impossibility Result

Impossibility Result [DFSS07]

Any quantum identification (QID) scheme can be broken by a malicious party with unbounded quantum storage and unbounded quantum computation

Circumventing the Impossibility Result

- bounded quantum storage + unbounded quantum computation (= "Bounded Quantum Storage Model")

Impossibility Result [DFSS07]

Any quantum identification (QID) scheme can be broken by a malicious party with unbounded quantum storage and unbounded quantum computation

Circumventing the Impossibility Result

- bounded quantum storage + unbounded quantum computation (= "Bounded Quantum Storage Model")
- unbounded quantum storage + bounded quantum computation ??

New: “Single-Qubit Operations Model” (SQOM)

- Malicious party has unbounded quantum storage,
- but is restricted to single-qubit operations and measurements

Existing QID Scheme

QID Scheme of Damgård et al. [DFSS07]

- Unconditionally secure against malicious user
- Secure against malicious server in the BQSM
- Security breaks down if malicious server can store all qubits (no quant. computation needed)

Existing QID Scheme

QID Scheme of Damgård et al. [DFSS07]

- Unconditionally secure against malicious user
- Secure against malicious server in the BQSM
- Security breaks down if malicious server can store all qubits (no quant. computation needed)

Our QID Scheme

- Unconditionally secure against malicious user
- Secure against malicious server in BQSM as well as in SQOM
- Some security left if malicious server can store all qubits (non-trivial quant. comp. needed to break it)

Our QID Scheme

- Unconditionally secure against malicious user
- Secure against malicious server in BQSM as well as in SQOM
- Some security left if malicious server can store all qubits (non-trivial quant. comp. needed to break it)

Remark

Security proof of new QID scheme in BQSM is based on our uncertainty relation

Thank You