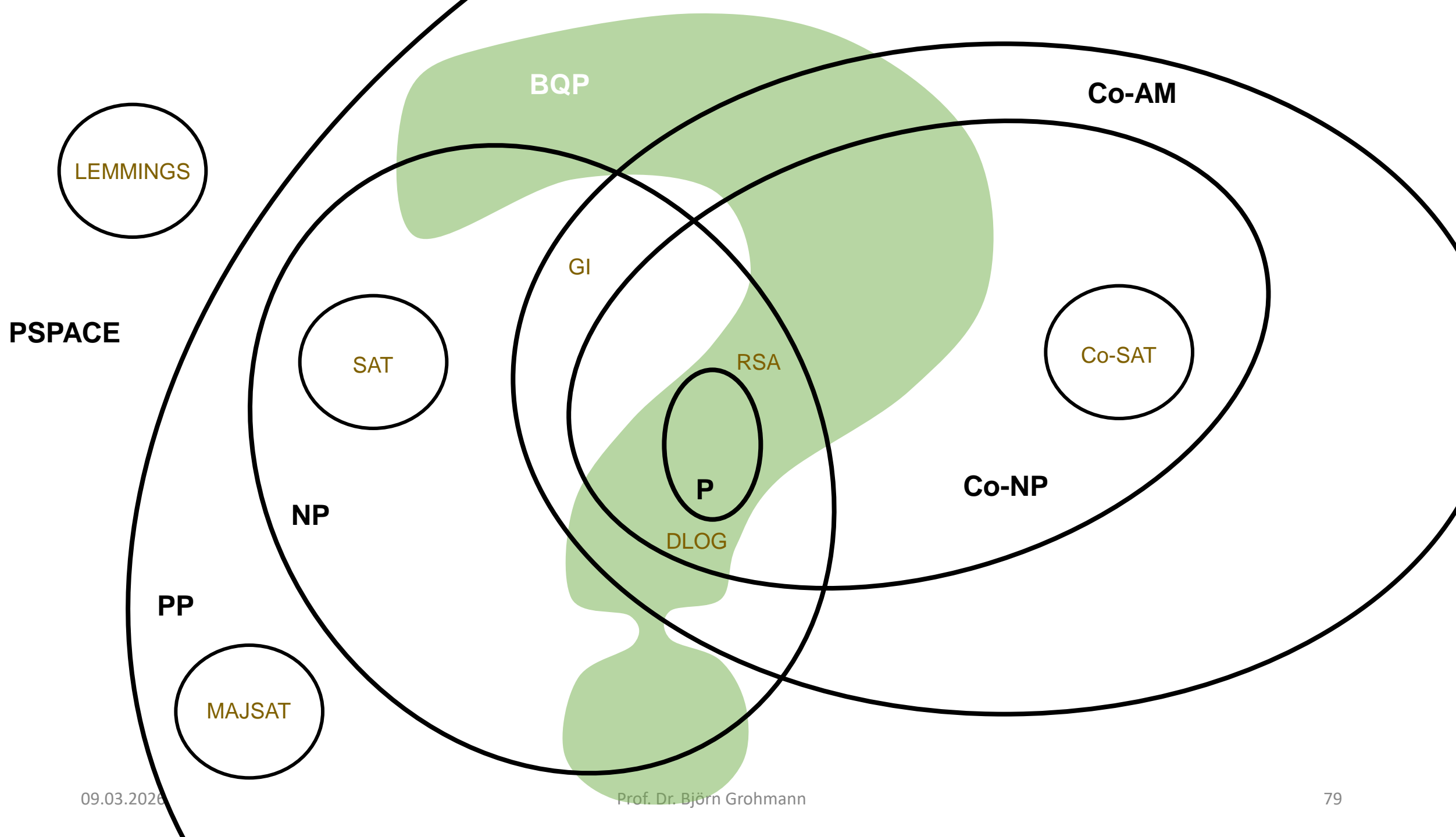




Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Kryptographie

Prof. Dr. Björn Grohmann



PQC STRATEGIES



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

- Lattice-based
- Code-based
- Multivariate polynomials
- Isogenies
- Hash-based
- Trotziges Kind
- MPC in the Head
- ...

PQC STRATEGIES



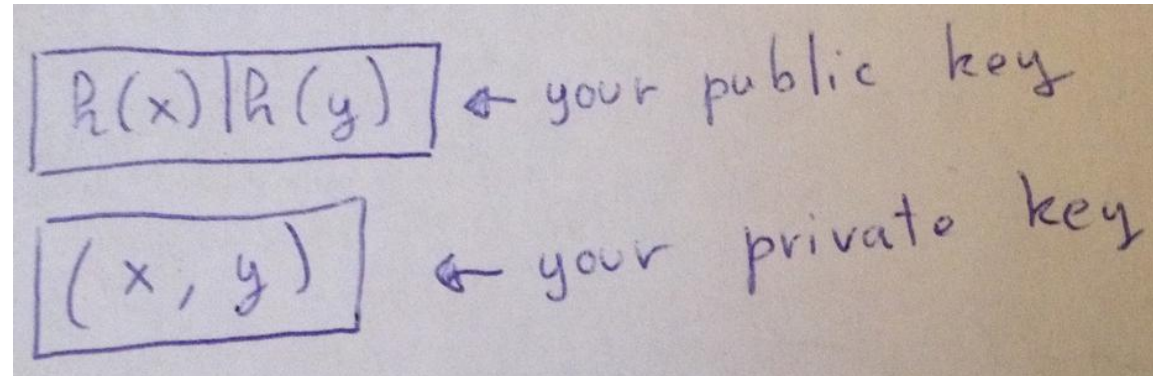
PQ-RSA: RSA with a modulus of size about 1 TB as a product of 4096-bit primes.

Cost quantum attacker: $\sim 2^{100}$

Cost secr.-key owner: $\sim 2^{50}$

- Trotziges Kind

PQC STRATEGIES

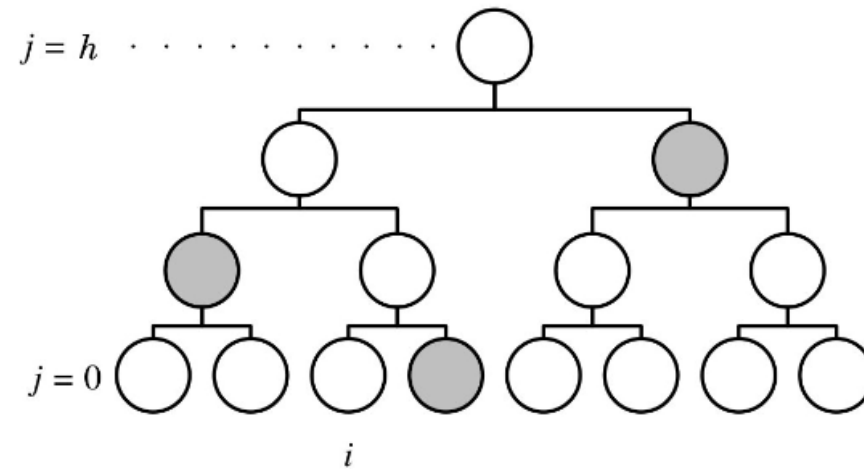


- Hash-based

PQC STRATEGIES



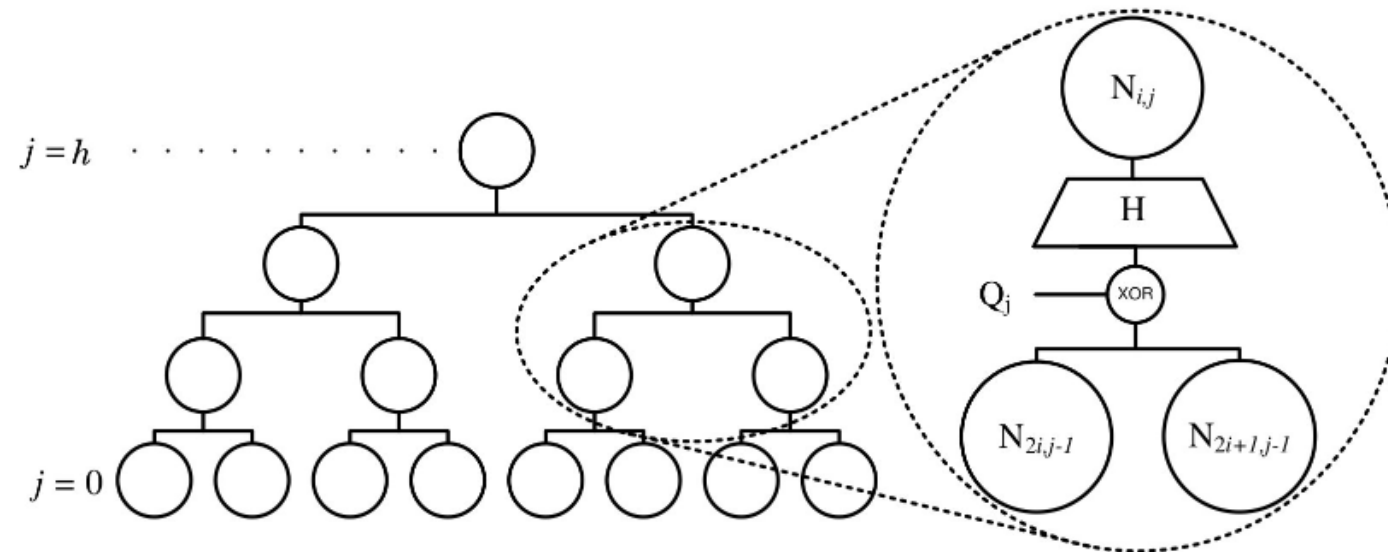
- Hash-based



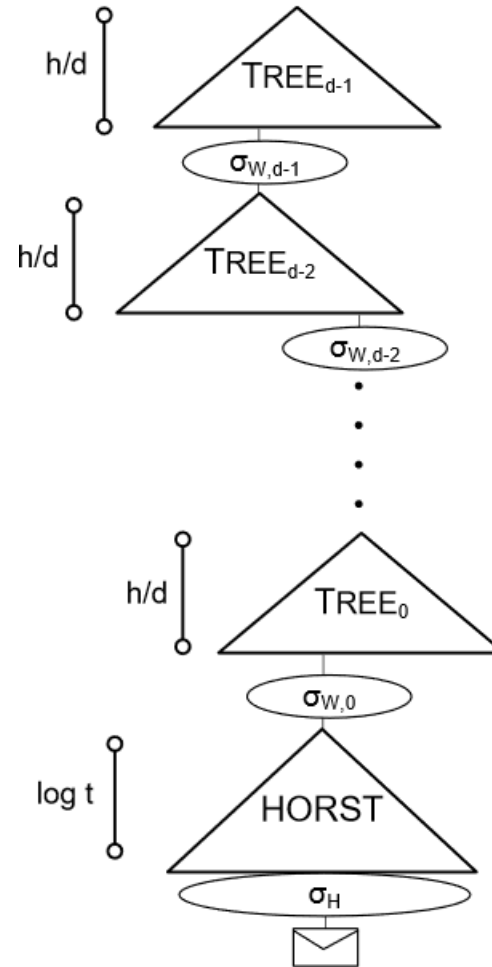
PQC STRATEGIES



- Hash-based



PQC STRATEGIES

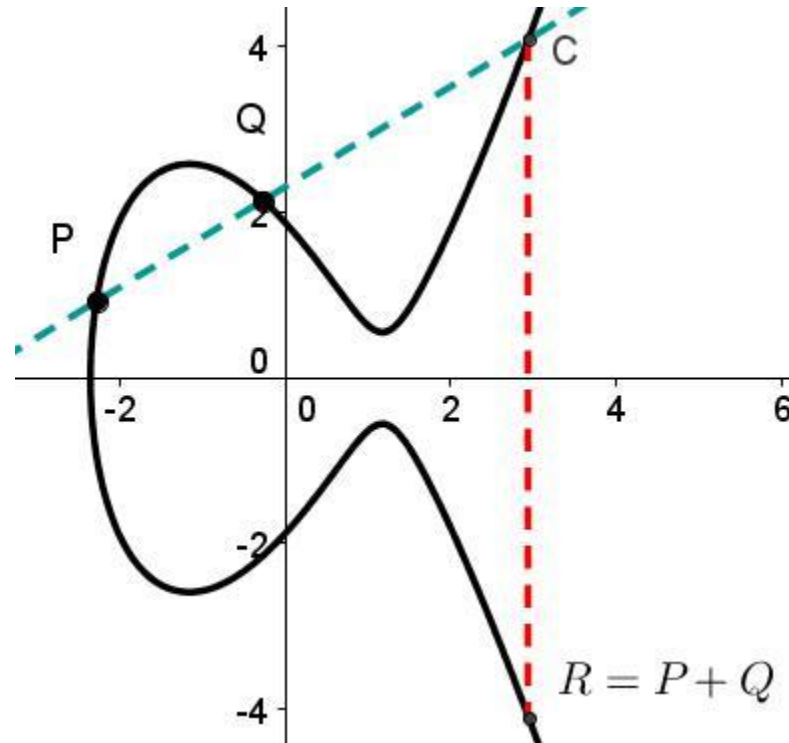


- Hash-based

PQC STRATEGIES



- Isogenies



PQC STRATEGIES



$$[n] : E \rightarrow E$$
$$[n]P = \underbrace{P + \dots + P}_{n \text{ times}}$$

- Isogenies

Let $E : y^2 = x^3 + x$. Then the map $[2] : E \rightarrow E$ is given by the rational function

$$[2](x, y) = \left(\frac{(x^2 - 1)^2}{4(x^3 + x)}, \frac{y(x^6 + 5x^4 - 5x^2 - 1)}{8(x^3 + x)^2} \right).$$

PQC STRATEGIES

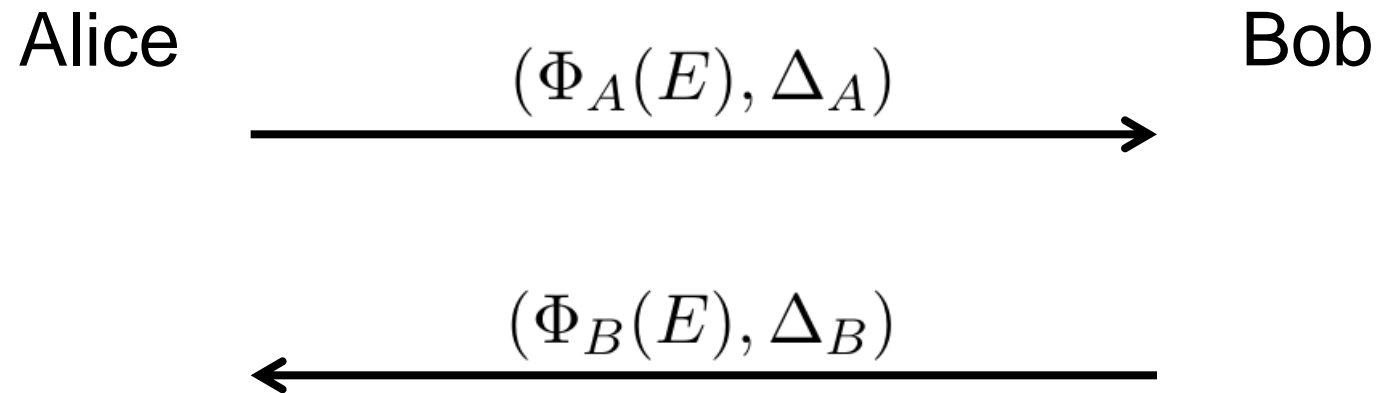


- Isogenies

$$\phi : E \rightarrow E'$$

$$\phi(x, y) = \left(\frac{f_1(x, y)}{g_1(x, y)}, \frac{f_2(x, y)}{g_2(x, y)} \right)$$

PQC STRATEGIES



- Isogenies

$$j(\Phi'_A(\Phi_B(E))) = k = j(\Phi'_B(\Phi_A(E)))$$

PQC STRATEGIES



- Multivariate polynomials



Hilbert

Eine *D i o p h a n t i s c h e* Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden. läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

PQC STRATEGIES



- Multivariate polynomials

$$p^{(1)}(x_1, \dots, x_n) = 0$$

$$p^{(2)}(x_1, \dots, x_n) = 0$$

$$\vdots$$

$$p^{(m)}(x_1, \dots, x_n) = 0,$$

$$p^{(k)}(x_1, \dots, x_n) := \sum_{1 \leq i \leq j \leq n} \gamma_{ij}^{(k)} x_i x_j + \sum_{1 \leq i \leq n} \beta_i^{(k)} x_i + \alpha^{(k)}.$$

MQ Problem. Given a quadratic polynomial map $\mathcal{P} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ over a finite field \mathbb{F}_q , find $\mathbf{x} \in \mathbb{F}_q^n$ that satisfies $\mathcal{P}(\mathbf{x}) = \mathbf{0}$.

PQC STRATEGIES



$$\mathcal{P}(\mathbf{x}) = h(\mathbf{m})$$

- Multivariate polynomials

$$\mathcal{P} = T \circ Q \circ S$$

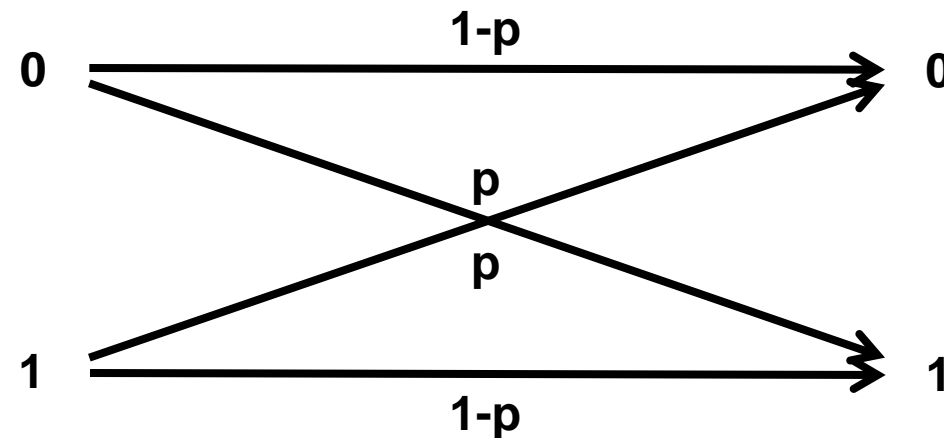
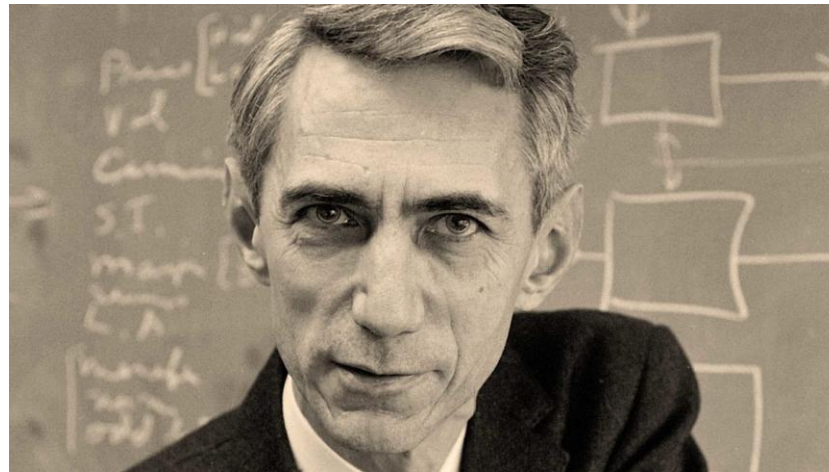
$$q^{(k)}(\mathbf{x}) = \sum_{i=1}^v \sum_{j=1}^n \gamma_{ij}^{(k)} x_i x_j + \sum_{i=1}^n \beta_i^{(k)} x_i + \alpha^{(k)}$$



PQC STRATEGIES



- Code-based



PQC STRATEGIES



- Code-based

$$\mathbf{c} \in \mathcal{C} \subseteq \mathbb{F}_2^n \iff \mathbf{c}H = 0$$

$$(\mathbf{c} + \mathbf{e})H = \mathbf{c}H + \mathbf{e}H = \mathbf{e}H =: \mathbf{s}$$

Coset Weights: Gegeben \mathbf{s} und H . Finde \mathbf{x} , mit $\nu(\mathbf{x}) \leq t$ und $\mathbf{x}H = \mathbf{s}$.

PQC STRATEGIES



- Code-based

$$H^* = PHS$$

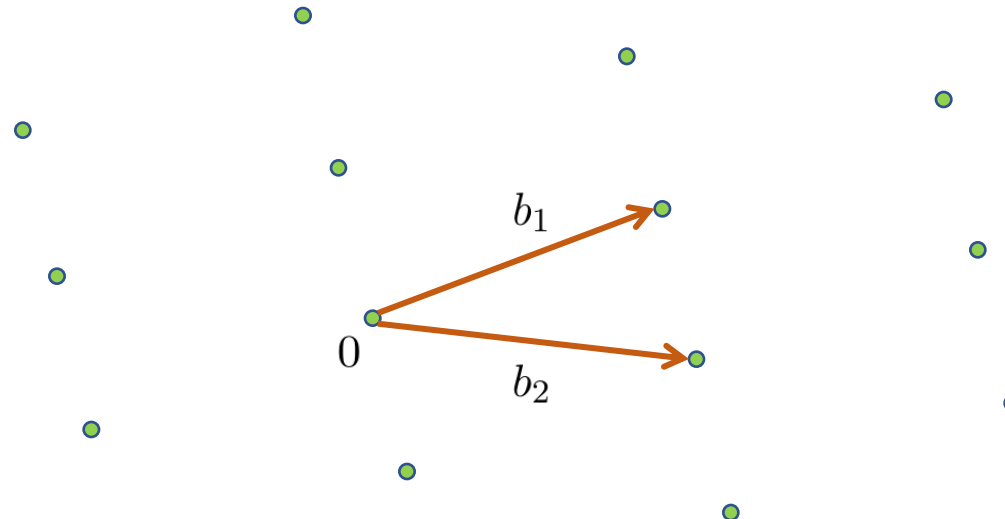
$$\text{Encode: } \mathbf{c} = \mathbf{m}H^*$$

$$\text{Decode: } \mathbf{m} = \delta_H(\mathbf{c}S^{-1})P^{-1}$$

PQC STRATEGIES



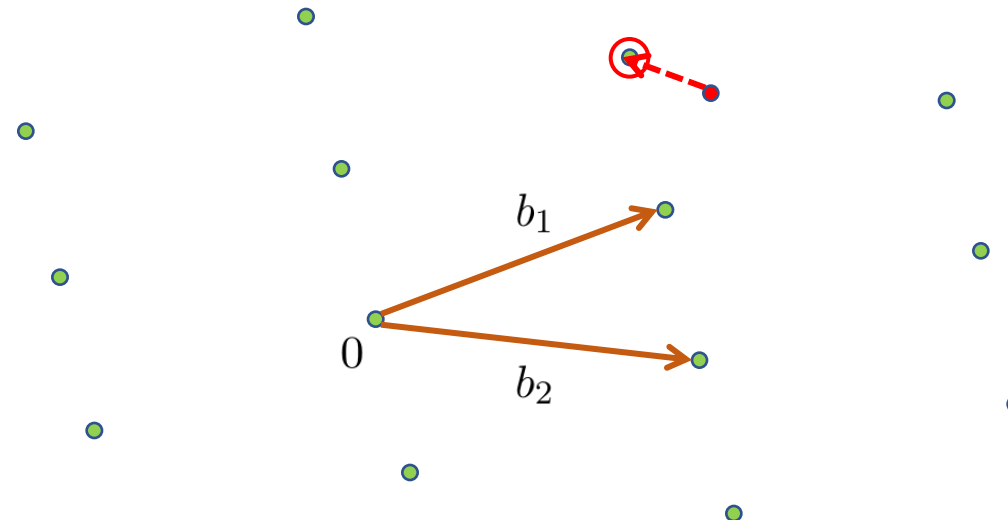
- Lattice-based



PQC STRATEGIES



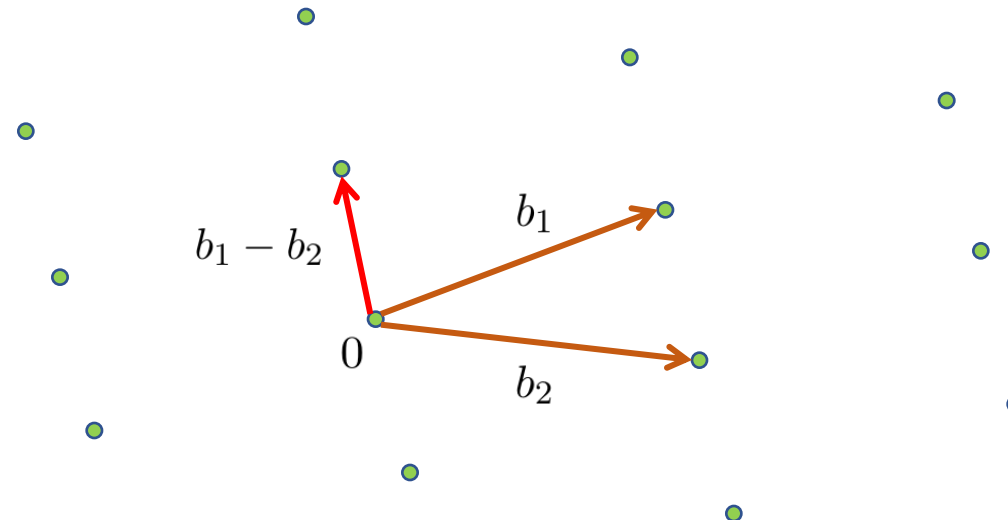
- Lattice-based



PQC STRATEGIES



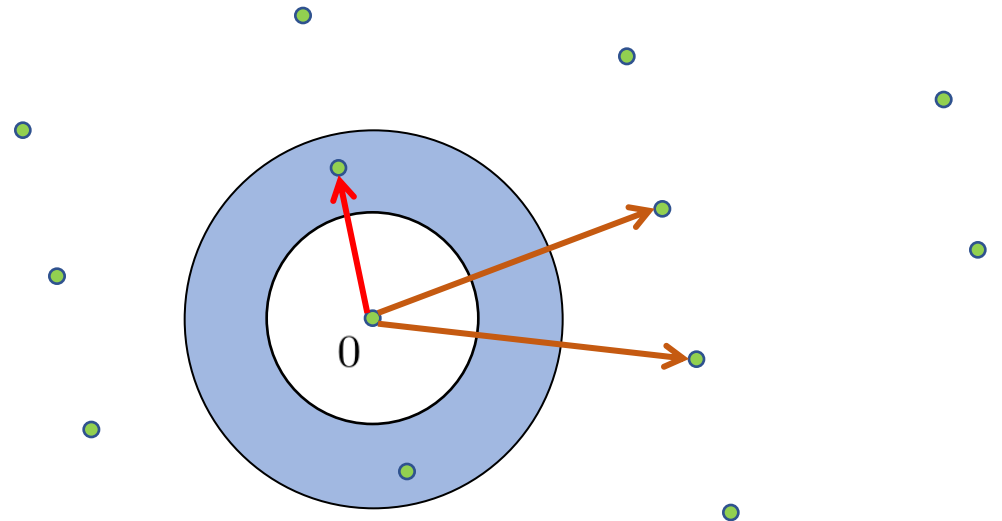
- Lattice-based



PQC STRATEGIES



- Lattice-based



PQC STRATEGIES

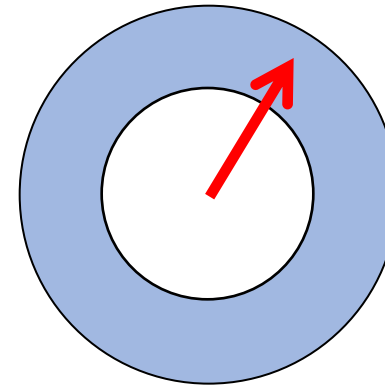


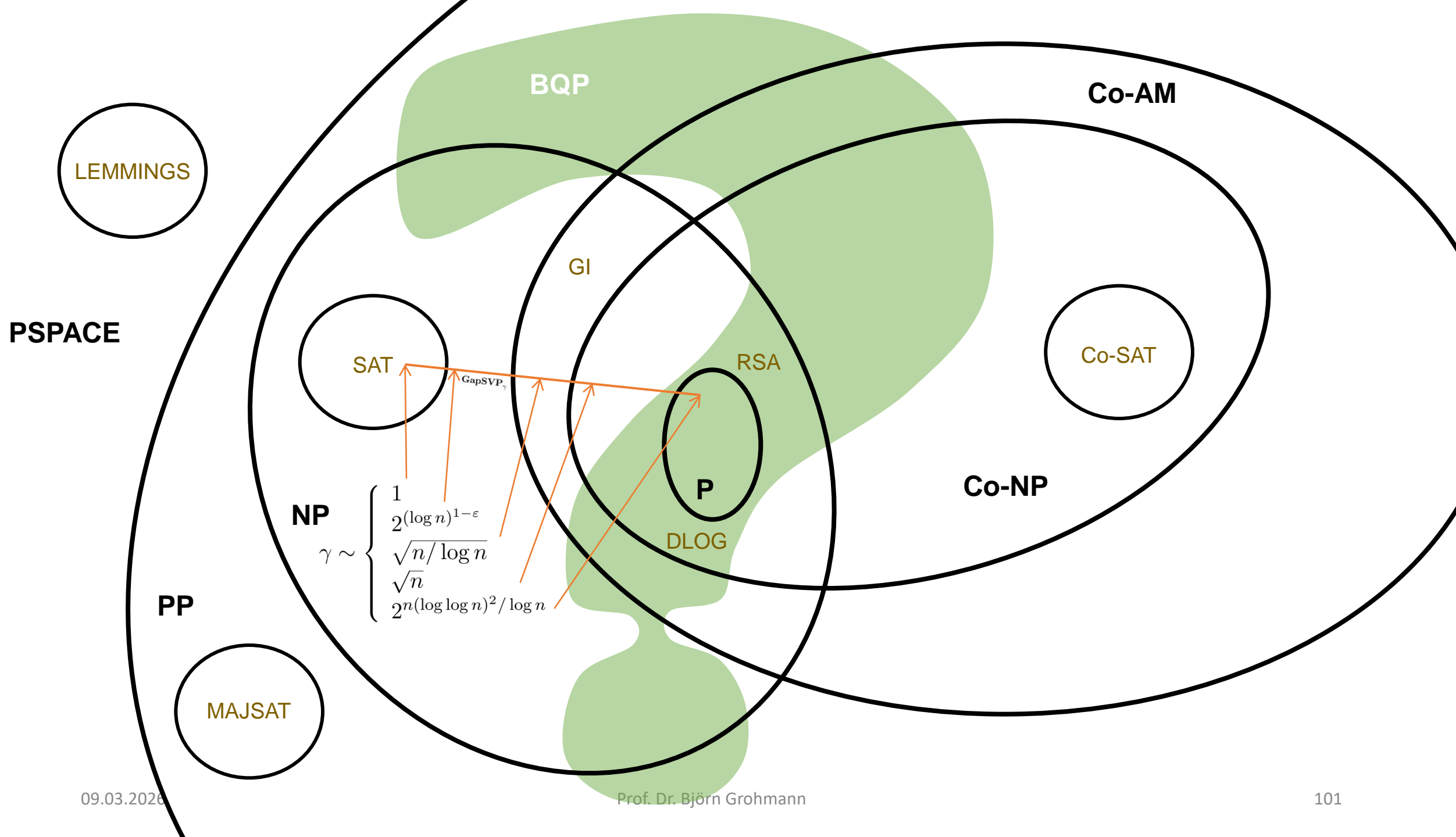
- Lattice-based

GapSVP _{γ}

Input: **B**, d .

Output: **Yes**, if $\lambda(\mathbf{B}) \leq d$.
No, if $\lambda(\mathbf{B}) > \gamma d$.
(else, don't care)





PQC STRATEGIES



- Lattice-based

Worst-Case vs Average-Case

There exist worst-case to average-case reductions from GapSVP_γ
to some other problems (**LWE**, **SIS**)
for $\gamma = \text{poly}(n)$

PQC STRATEGIES



- Lattice-based

Beispiel: Regev's public-key cryptosystem (based on LWE)

- **Private key:** Private key is an $\mathbf{s} \in \mathbb{Z}_q^n$ chosen uniformly at random.
- **Public key:** Choose m vectors $\mathbf{a}_1, \dots, \mathbf{a}_m \in \mathbb{Z}_q^n$ uniformly and independently. Choose error offsets $e_1, \dots, e_m \in \mathbb{T}$ independently according to χ . The public key consists of $(\mathbf{a}_i, b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle / q + e_i)_{i=1}^m$
- **Encryption:** The encryption of a bit $x \in \{0, 1\}$ is done by choosing a random subset S of $[m]$ and then defining $\text{Enc}(x)$ as

$$\left(\sum_{i \in S} \mathbf{a}_i, \frac{x}{2} + \sum_{i \in S} b_i \right)$$

- **Decryption:** The decryption of (\mathbf{a}, b) is 0 if $b - \langle \mathbf{a}, \mathbf{s} \rangle / q$ is closer to 0 than to $\frac{1}{2}$, and 1 otherwise.

das LWE-
Problem lautet:
bestimme "s"

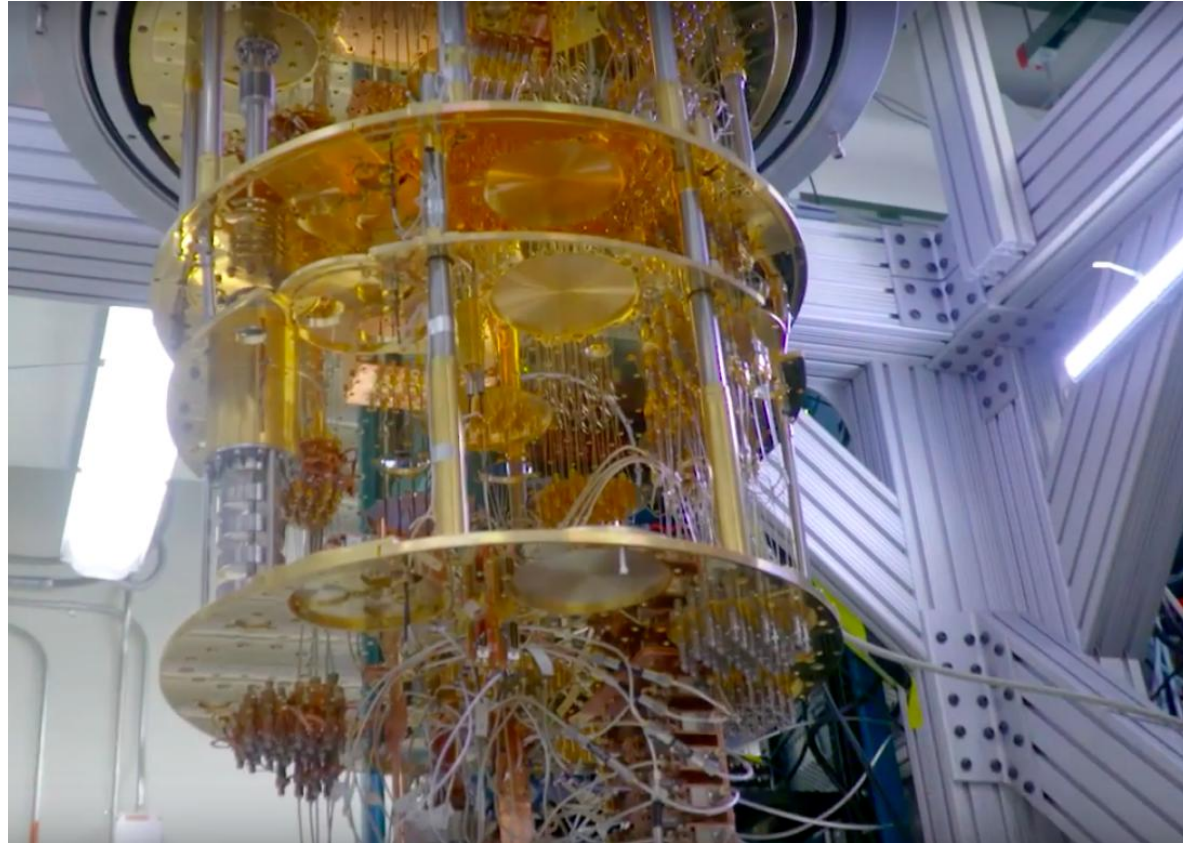
eine bestimmte
Verteilung

$$\mathbb{T} = \mathbb{R}/\mathbb{Z}$$

HOW SOON DO WE NEED TO WORRY?



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



HOW SOON DO WE NEED TO WORRY?



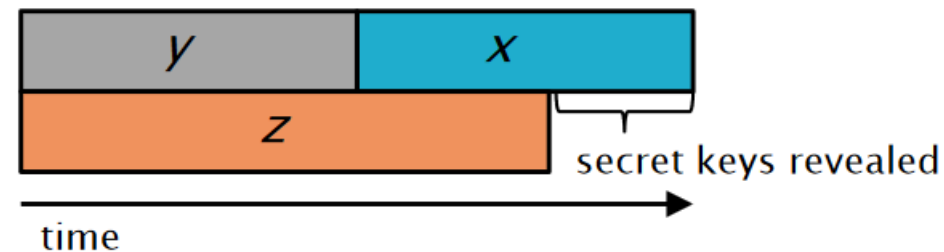
Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

How long does encryption need to be secure (x years)

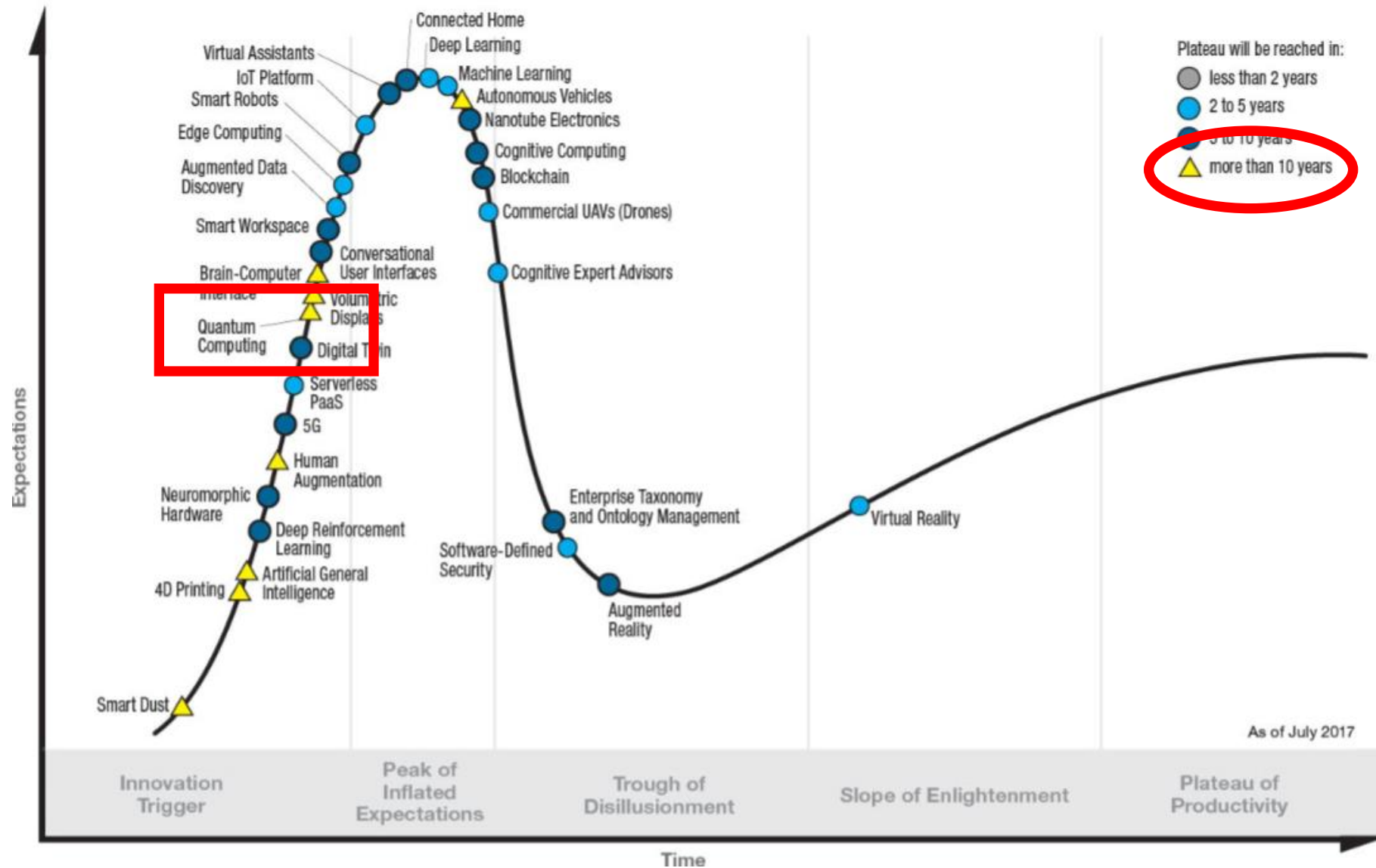
How long to re-tool existing infrastructure with quantum safe solution (y years)

How long until large-scale quantum computer is built (z years)

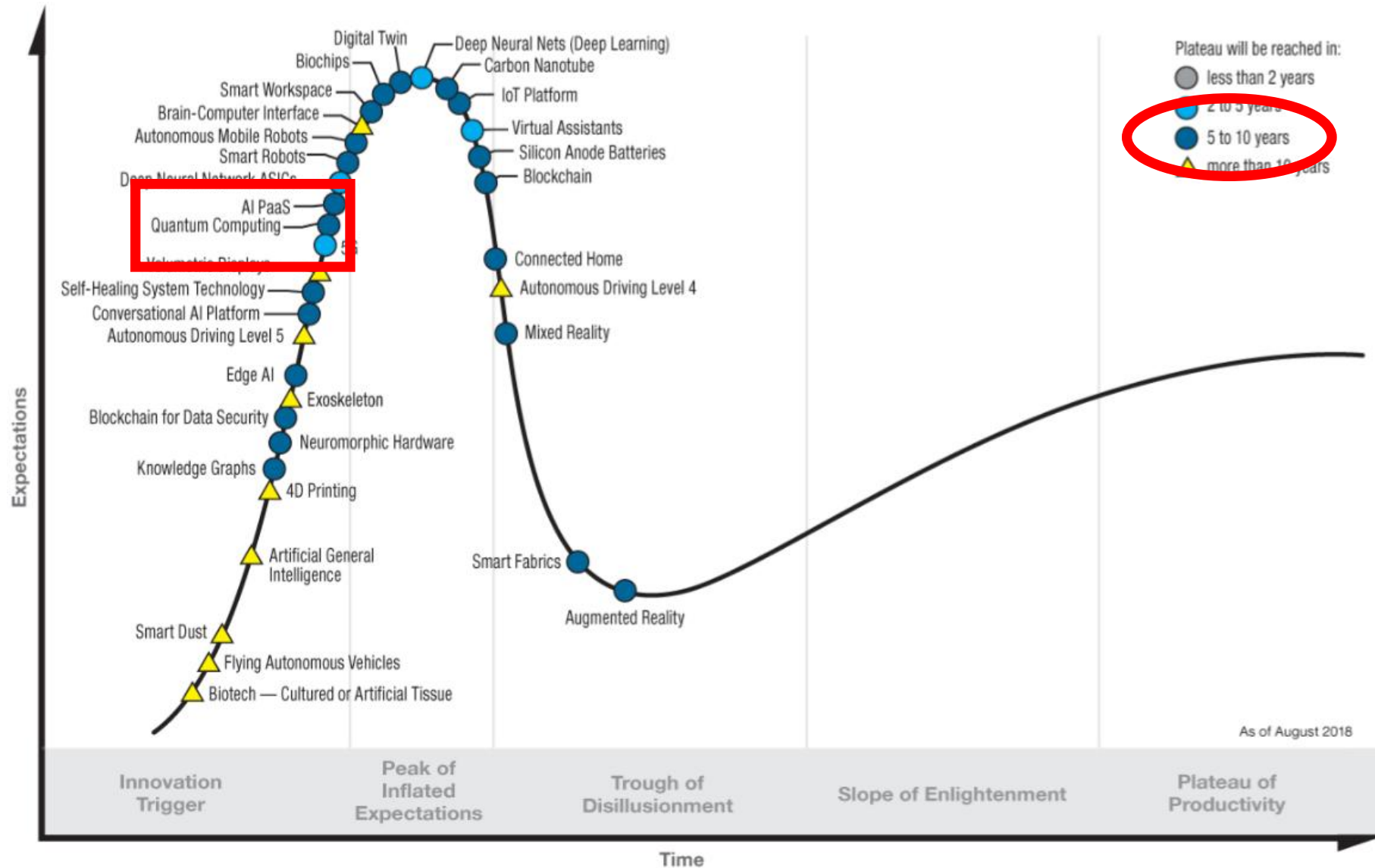
Theorem (Mosca): If $x + y > z$, then worry



Gartner Hype Cycle for Emerging Technologies, 2017



Hype Cycle for Emerging Technologies, 2018



NIST Competition PQC Standardization

- 1. Round, Nov 2017, with 69 candidates
- Selected Algorithms 2022:
 - CRYSTAL-Kyber (KEM)
 - CRYSTAL-Dilithium (DSA)
 - Falcon (DSA)
 - Sphincs+ (DSA)
- 2022-24 Draft of standard available



SPHINCS⁺



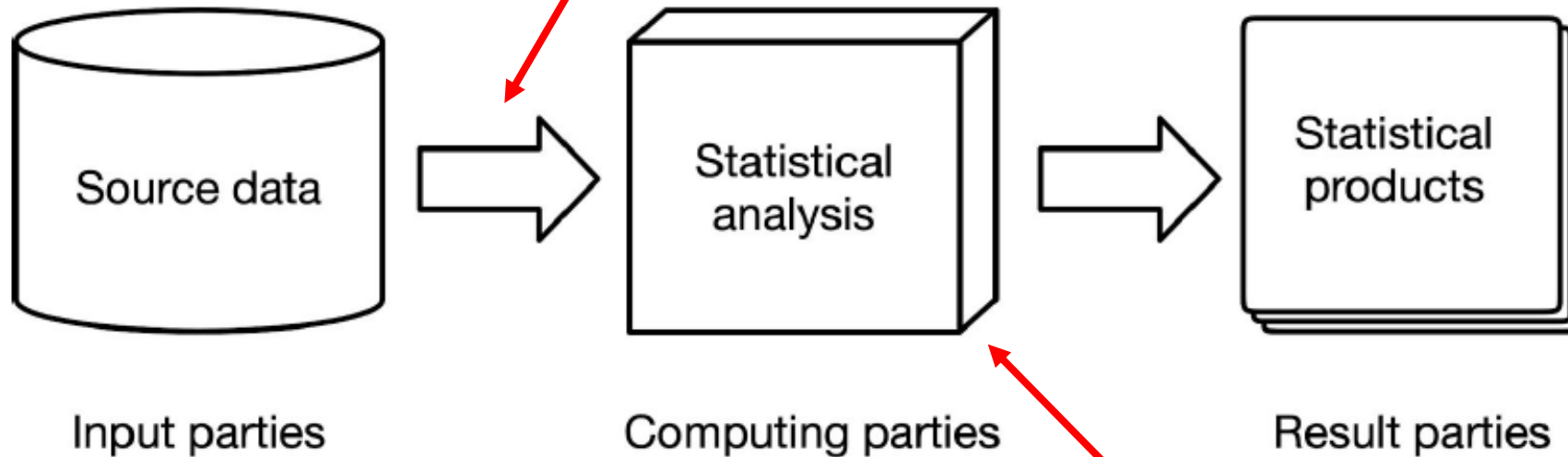
THREE DIMENSIONS

Data in transit

- Confidentiality
- Integrity
- Authenticity
- ...



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



Data at rest

- Confidentiality
- Integrity
- ...

Data in use

- Confidentiality
- ...

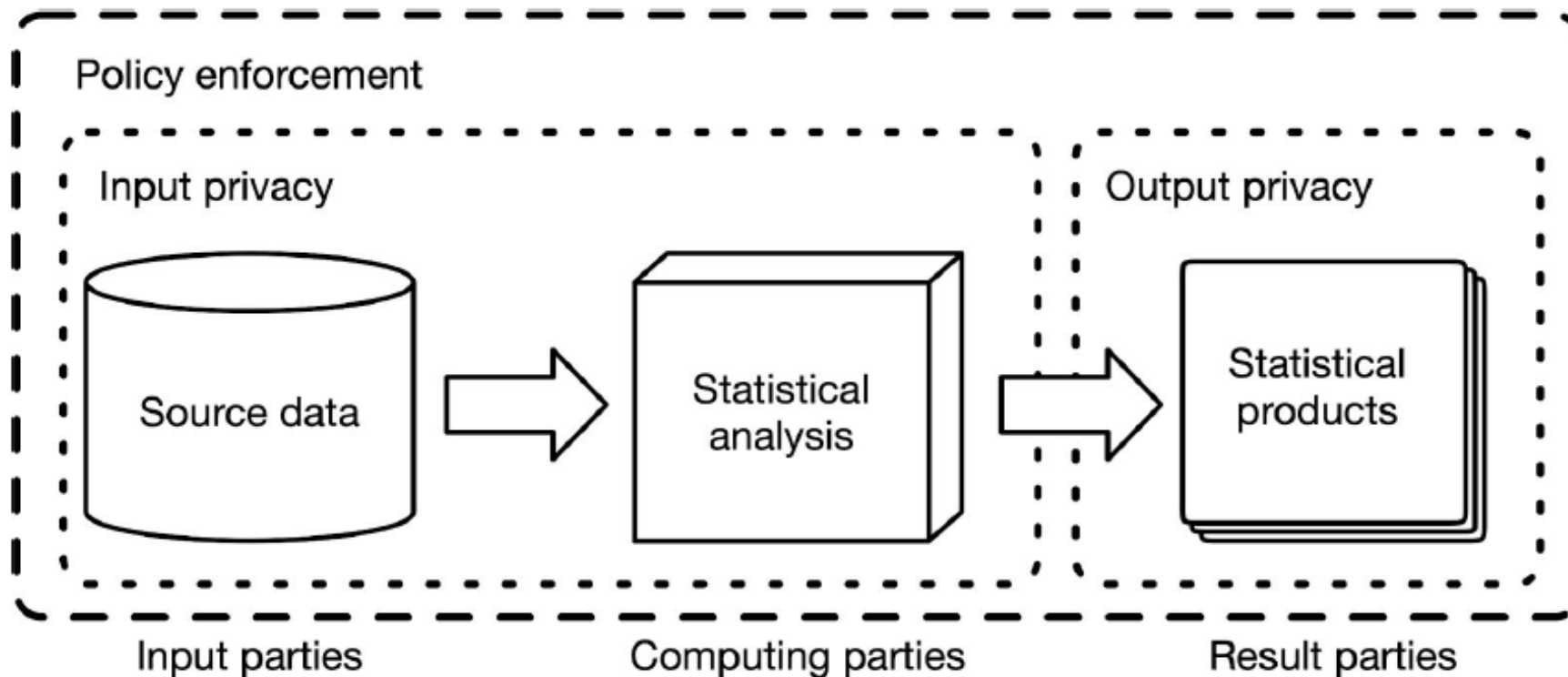
WEITERE SCHUTZZIELE



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

- Input Privacy
- Output Privacy
- Policy Enforcement
- Weitere?!

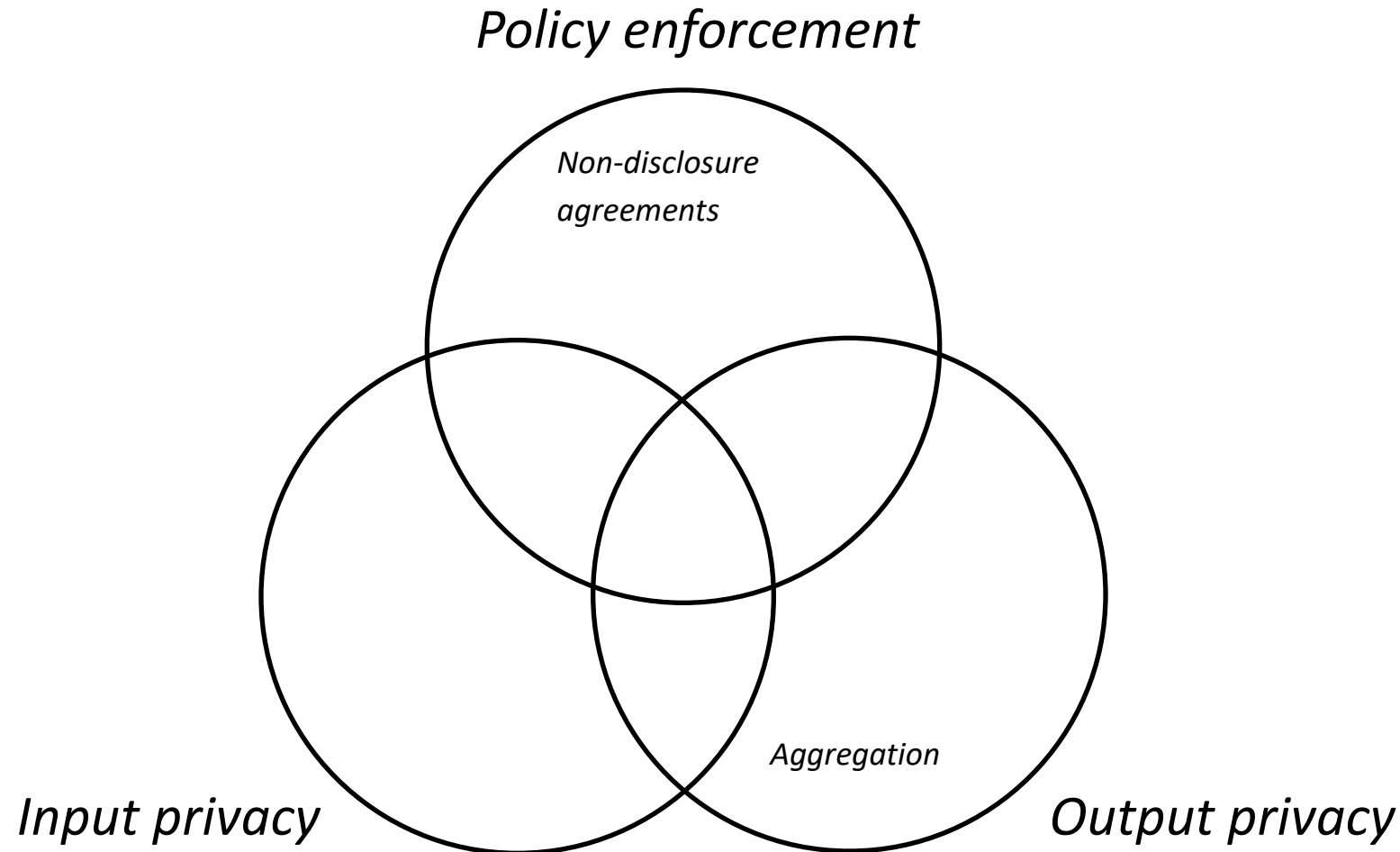
PRIVACY GOALS



PRIVACY GOALS AND TECHNOLOGIES



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



HOMOMORPHIC ENCRYPTION



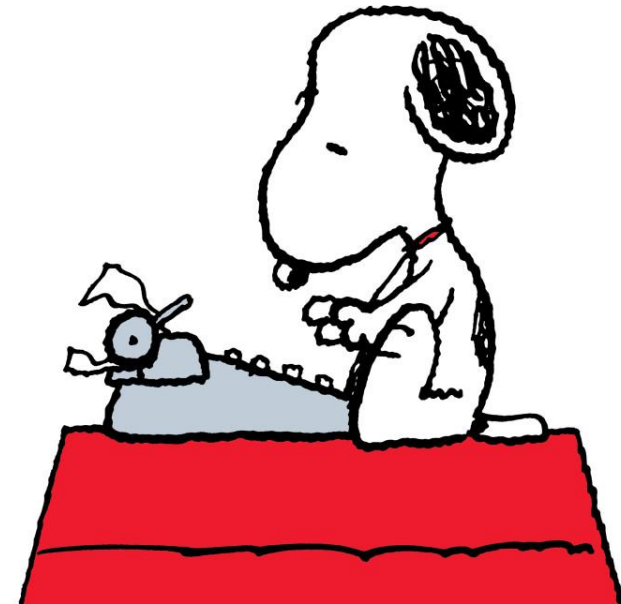
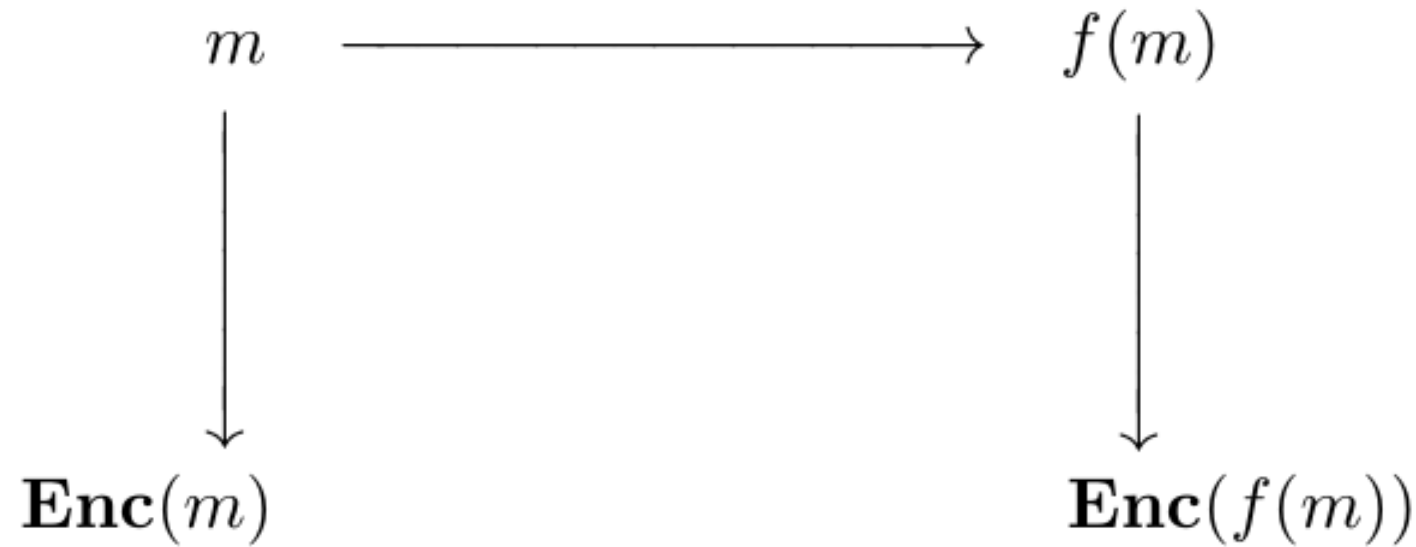
Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



HOMOMORPHIC ENCRYPTION



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



HOMOMORPHIC ENCRYPTION



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

„Kann man nicht auch auf verschlüsselten
Daten rechnen?“



HOMOMORPHIC ENCRYPTION

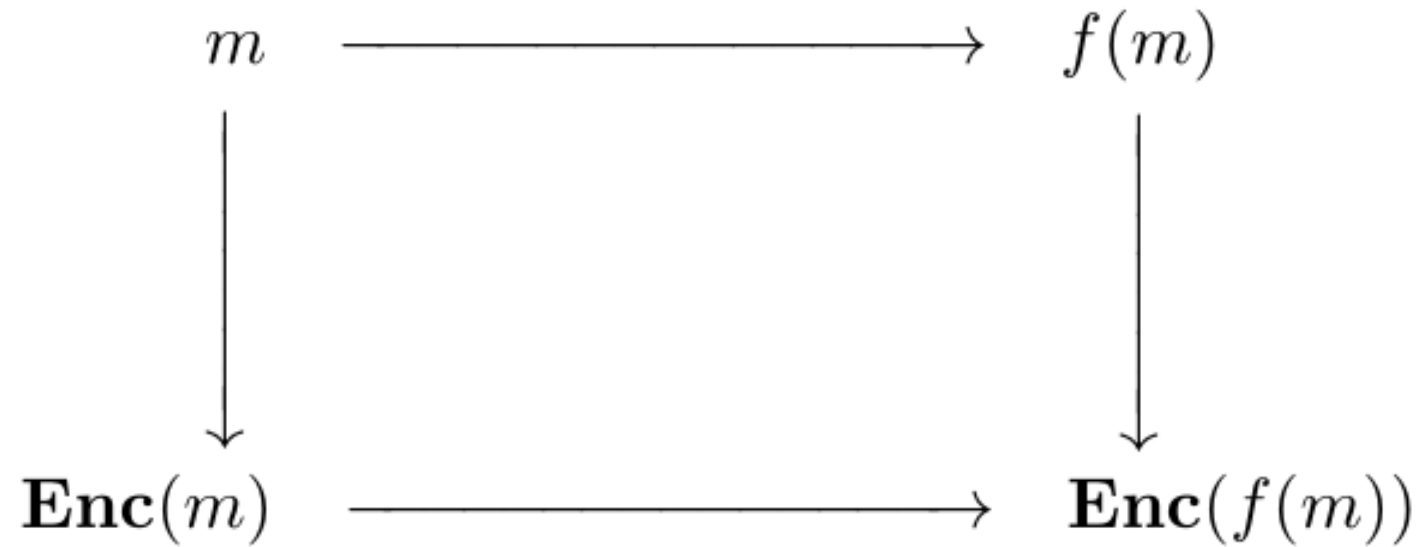


Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

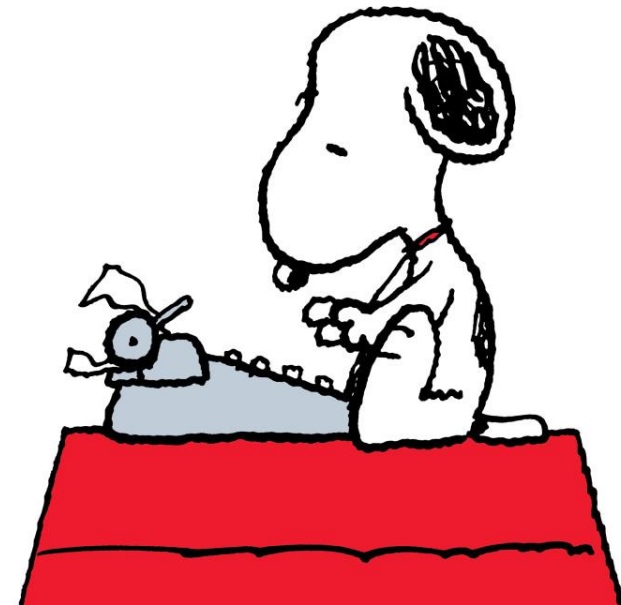
$$\mathbf{Enc}(m_1) \star \mathbf{Enc}(m_2) = \mathbf{Enc}(m_1 \circ m_2)$$



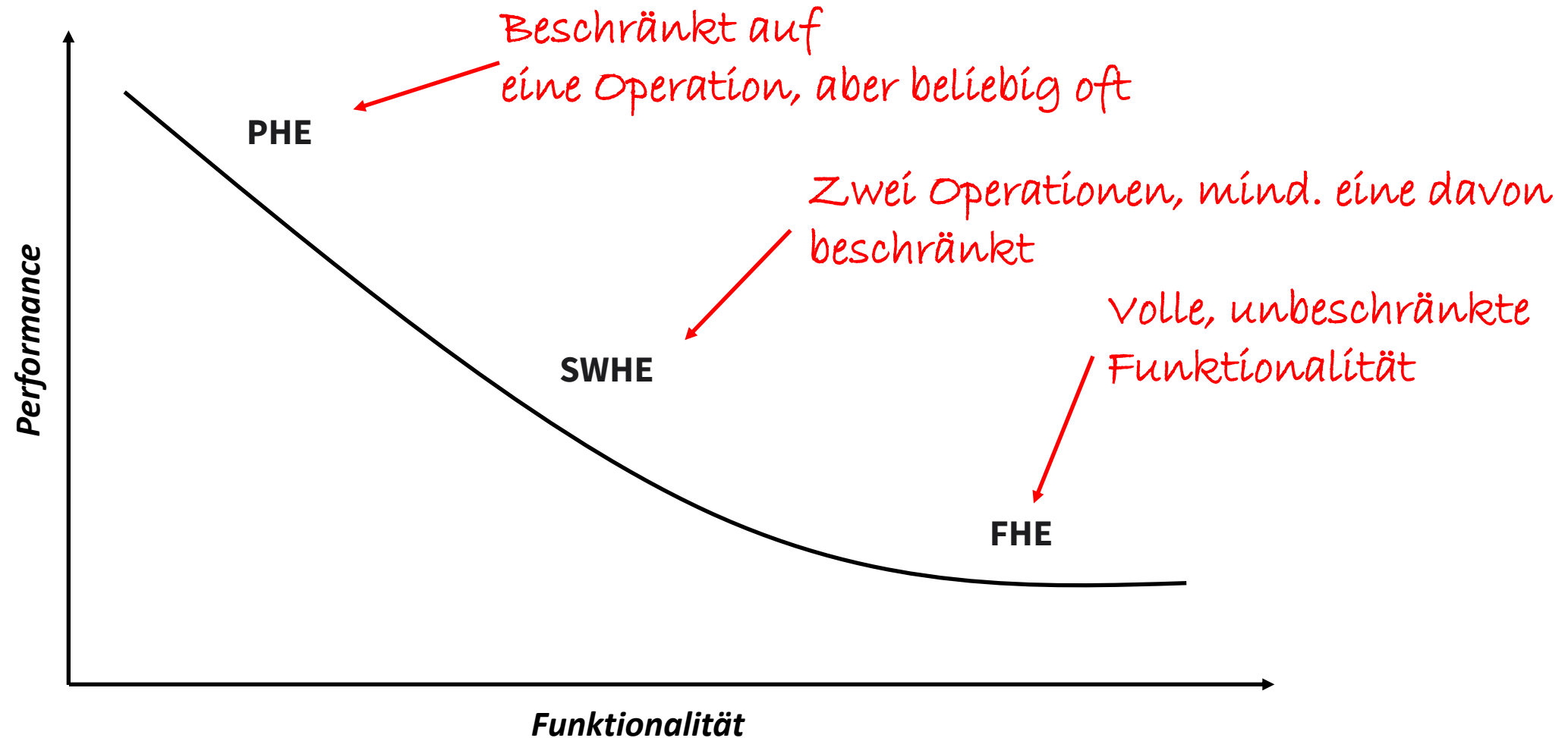
HOMOMORPHIC ENCRYPTION



Homomorphic Encryption
macht diesen Pfeil möglich



HE -- PERFORMANCE vs FUNKTIONALITÄT



HE -- BEISPIEL: RSA



RSA Algorithm

Key Generation

Select p, q	p and q both prime; $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption

Plaintext:	C
Ciphertext:	$M = C^d \bmod n$

Denn
 $E(M_1) * E(M_2) = E(M_1 * M_2),$

d.h. das Produkt von zwei
Chiffretexten, entspricht dem
Produkt der Klartexte.

HE -- BEISPIEL: PAILLER



$g = n + 1$, $\lambda = \varphi(n)$, and $\mu = \varphi(n)^{-1} \bmod n$, where $\varphi(n) = (p - 1)(q - 1)$

Handwritten red note: $n = p * q$ with an arrow pointing to n in the equation above.

Encryption [\[edit \]](#)

1. Let m be a message to be encrypted where $0 \leq m < n$
2. Select random r where $0 < r < n$ and $\gcd(r, n) = 1$
3. Compute ciphertext as: $c = g^m \cdot r^n \bmod n^2$

Decryption [\[edit \]](#)

1. Let c be the ciphertext to decrypt, where $c \in \mathbb{Z}_{n^2}^*$
2. Compute the plaintext message as: $m = L(c^\lambda \bmod n^2) \cdot \mu \bmod n$

$$L(x) = \frac{x - 1}{n}$$

Handwritten red note: An arrow points from the c^λ term in the decryption step 2 to the x in the $L(x)$ function.

HE -- BEISPIEL: PAILLER



$$D(E(m_1, r_1) \cdot E(m_2, r_2) \bmod n^2) = m_1 + m_2 \bmod n$$

Das Produkt von
zwei Chiffretexten entspricht
also der Summe der Klartexte

HE -- BEISPIEL: SWHE



Das Nachrichten-Bit

Random Werte

Geheime Primzahl

Chiffre

$$c_1 = b_1 + 2r_1 + r_2p$$

Zum Dechiffrieren erst „modulo p“, dann „modulo 2“

HE -- BEISPIEL: SWHE



$$c_1 = b_1 + 2r_1 + r_2p$$

$$c_2 = b_2 + 2s_1 + s_2p$$

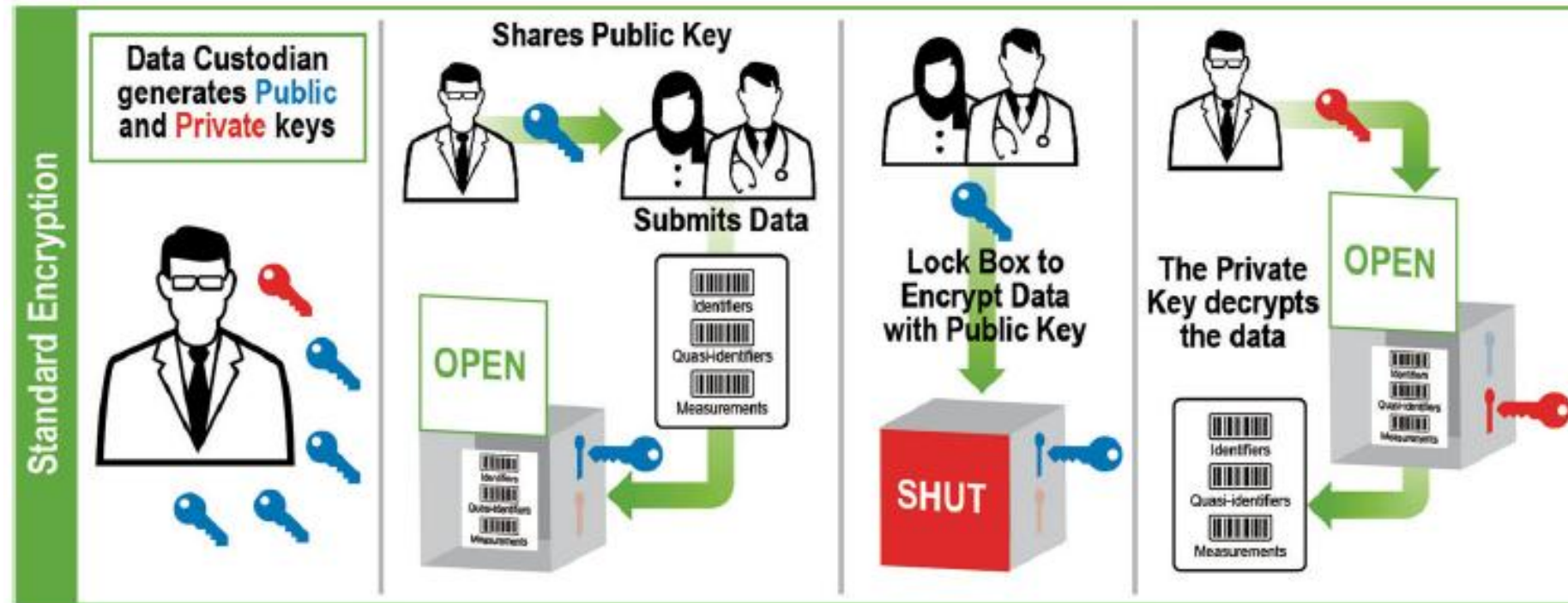
Rechnung in $GF(2)$

$$c_1 + c_2 = b_1 + b_2 + 2(r_1 + s_1) + p(r_2 + s_2)$$

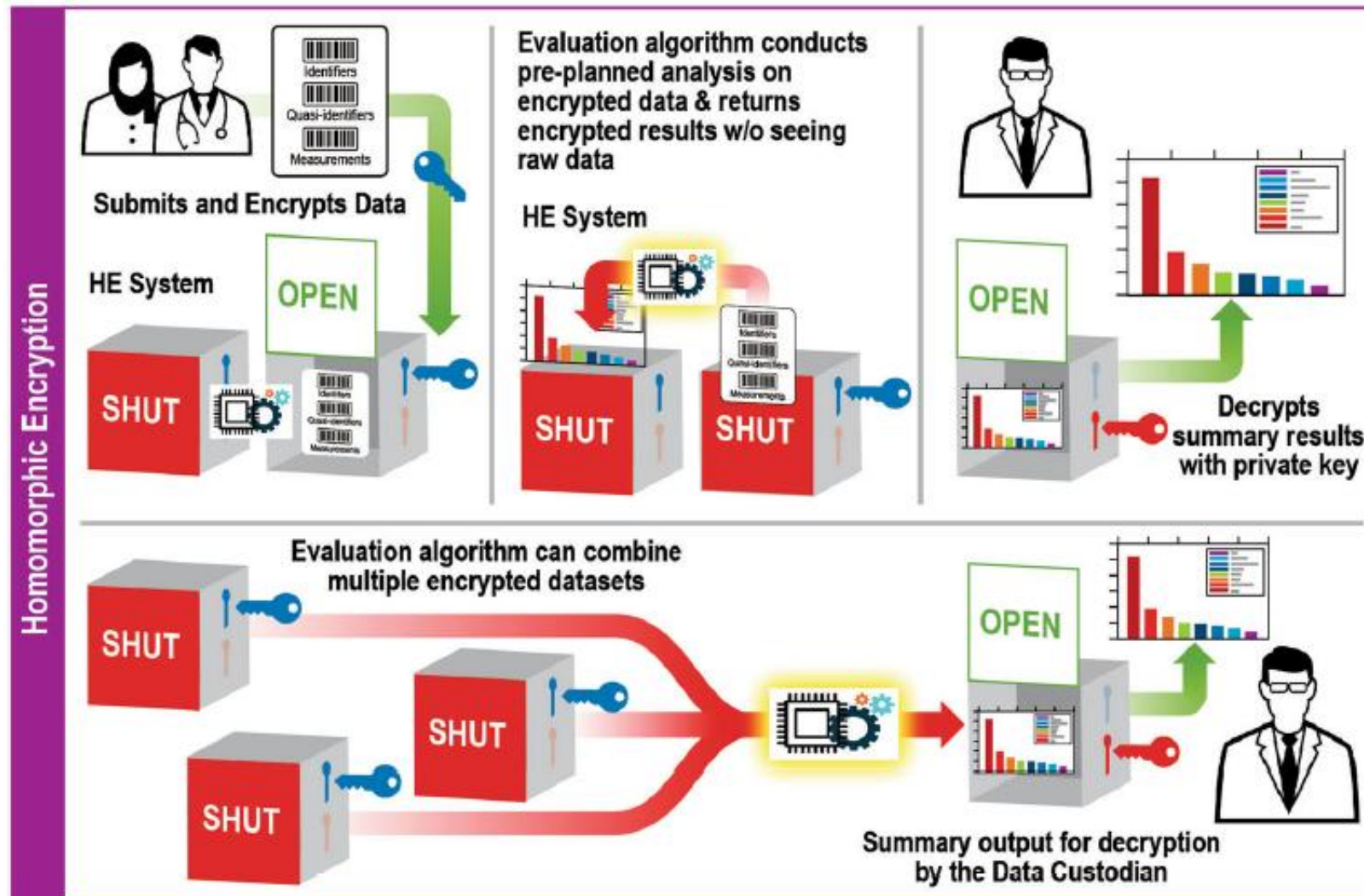
$$c_1 c_2 = b_1 b_2 + 2(b_2 r_1 + b_1 s_1 + 2r_1 s_1) + p(b_2 r_2 + b_1 s_2 + 2r_1 s_2 + 2s_1 r_2 + p r_2 s_2)$$

Anforderungen an die Intervalle der r 's und s 's

HE vs CLASSICAL APPROACH



HE vs CLASSICAL APPROACH



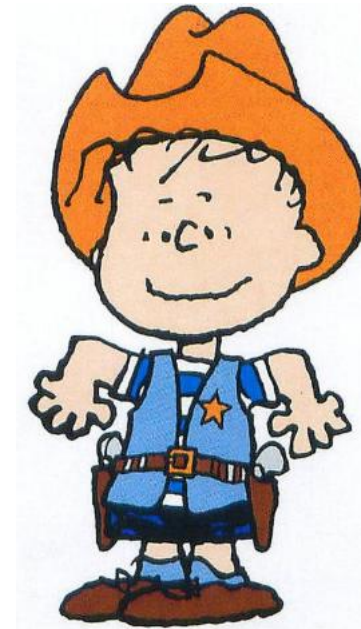
MULTI-PARTY-COMPUTATION



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



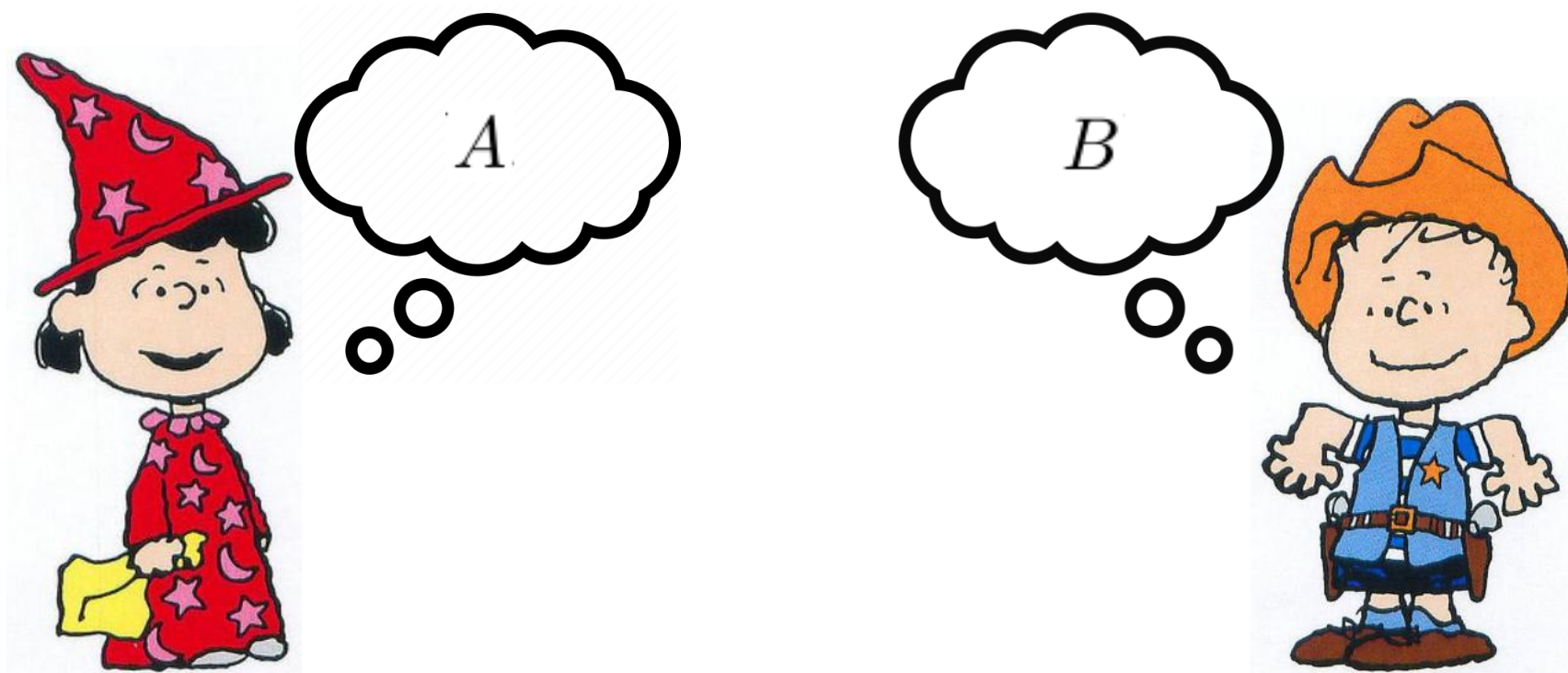
„Wie können Lucy und Linus
herausfinden, wer von beiden mehr
Bonbons besitzt, ohne die
Anzahl ihrer Bonbons
preiszugeben?“



MULTI-PARTY-COMPUTATION



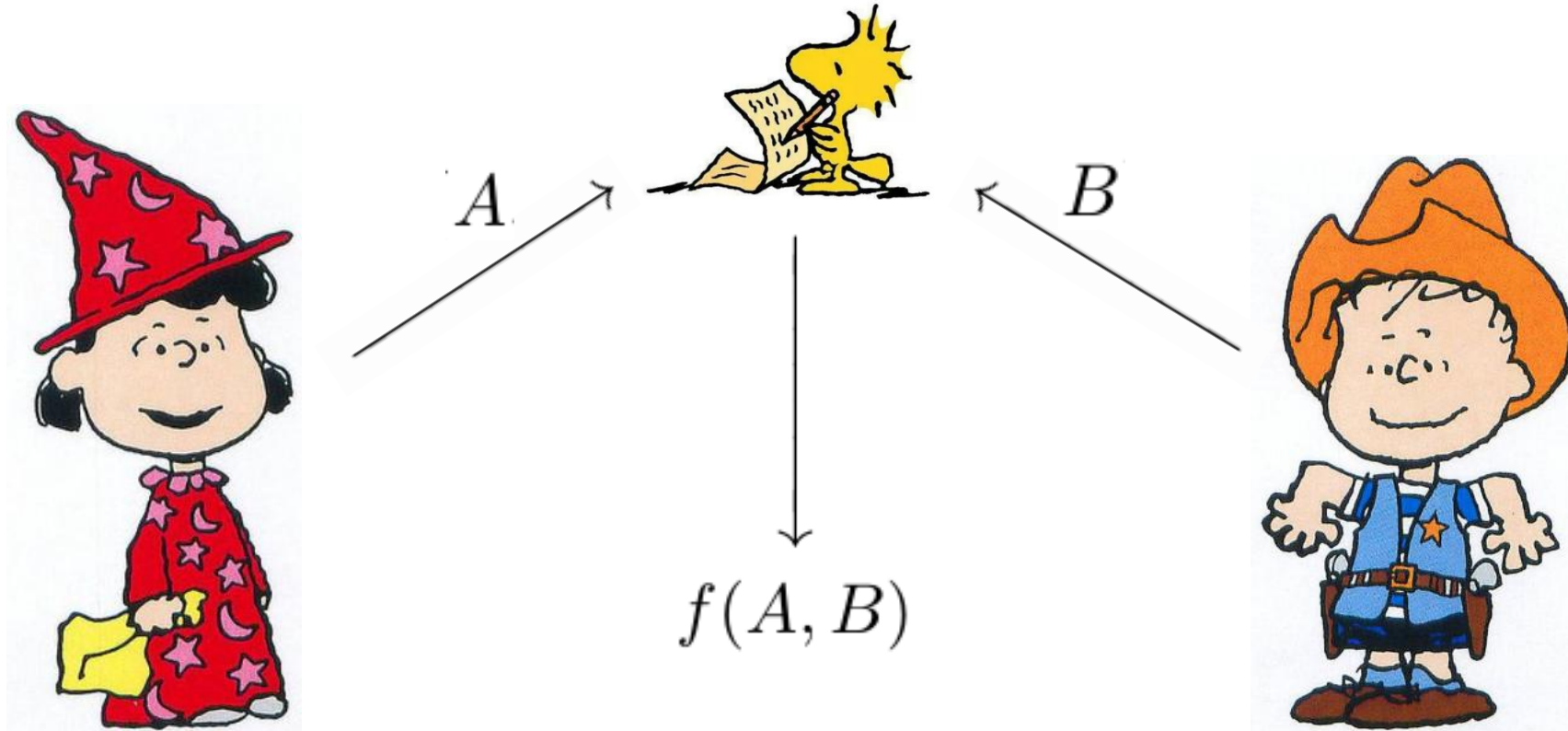
Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



MULTI-PARTY-COMPUTATION



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



MULTI-PARTY-COMPUTATION

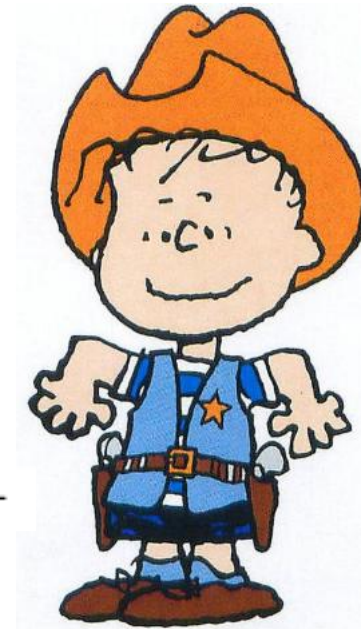


Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



„Geht das auch
ohne vertrauenswürdige
dritte Partei?“

$$\xrightarrow{A} f(A, B) \xleftarrow{B}$$



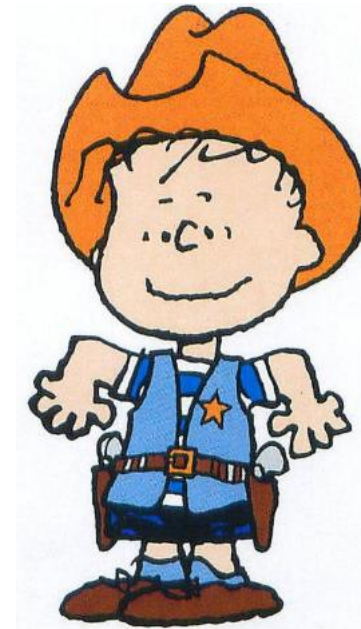
MULTI-PARTY-COMPUTATION



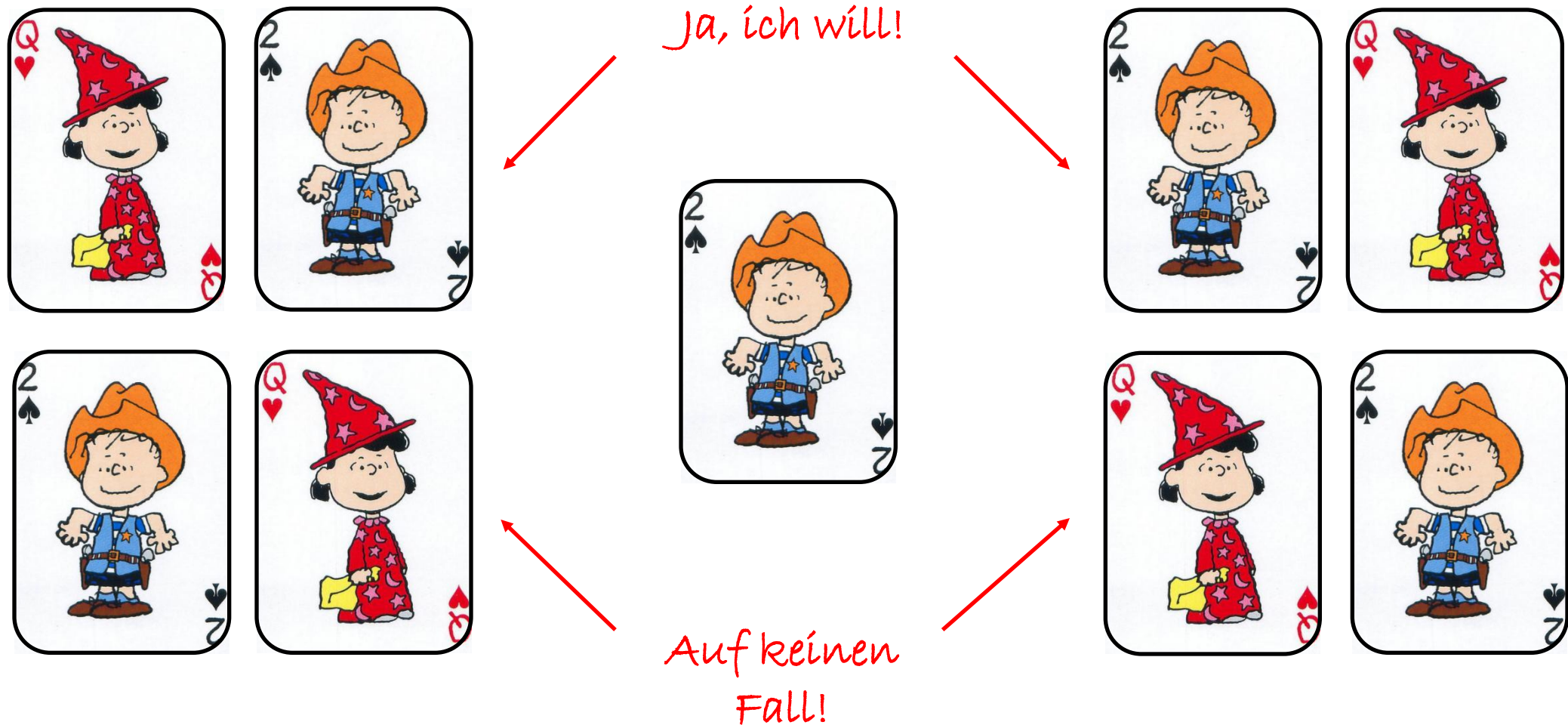
Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



„Wie können Lucy und Linus
herausfinden, ob beide zusammen
zum Fasching gehen wollen, ohne
sich „einen Korb“ zu holen?“



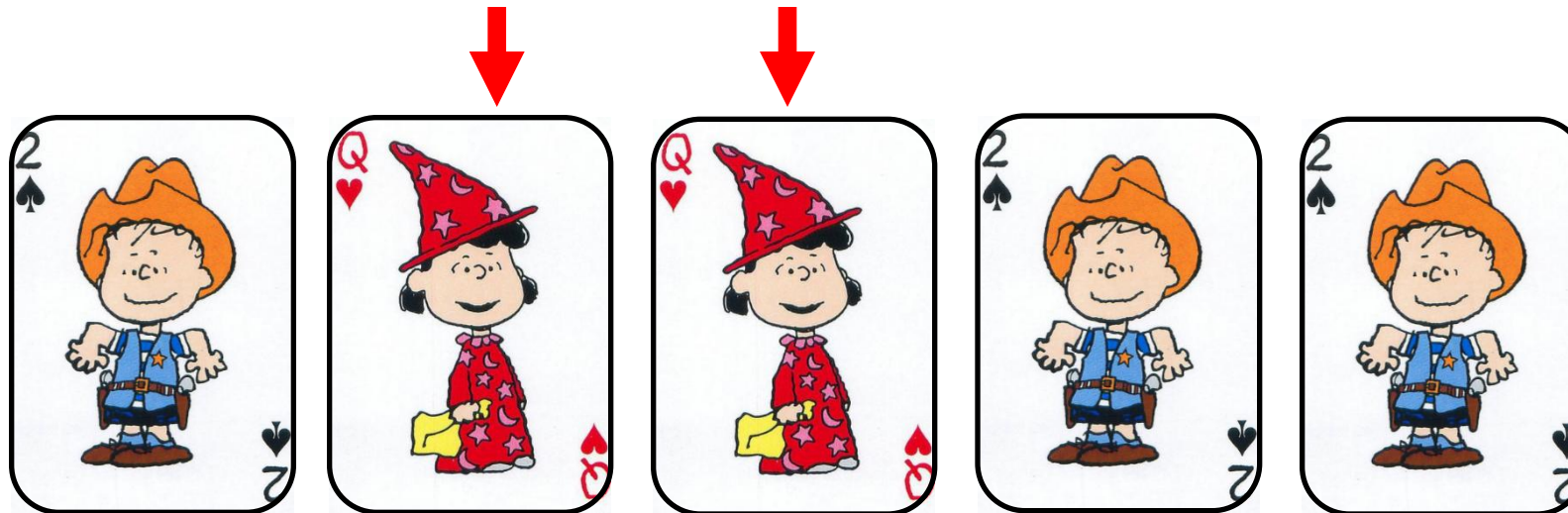
MULTI-PARTY-COMPUTATION



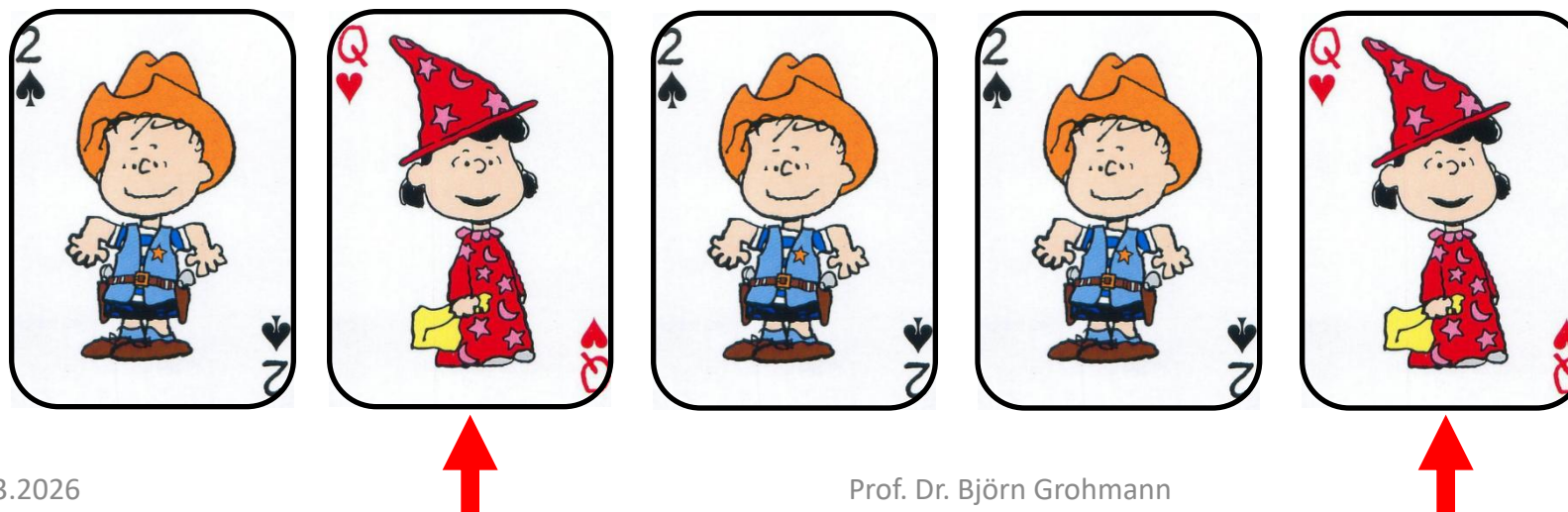
MULTI-PARTY-COMPUTATION



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



Lass uns
zusammen gehen



Danke, und
nichts für ungut



OBLIVIOUS TRANSFER (RABIN 1981)

We refer to this mode of transferring
information, where the sender does not know whether
the recipient actually received the information,
as an oblivious
transfer.

OBLIVIOUS TRANSFER



Definition 1: (O.T.)

- Alice knows one bit b .
- Bob gets bit b from Alice with probability $\frac{1}{2}$.
- Bob knows whether he got b or not.
- Alice does not know whether Bob got b or not.

Definition 2: (one-out-of-two O.T.)

- Alice knows two bits b_0 and b_1 .
- Bob gets bit b_k and not $b_{\bar{k}}$ with $Pr(k=0) = Pr(k=1) = \frac{1}{2}$
- Bob knows which of b_0 or b_1 he got.
- Alice does not know which b_k Bob got.

OBLIVIOUS TRANSFER



Definition 3: (p -O.T.)

- Alice knows one bit b .
- Bob gets bit b from Alice with probability p .
- Bob knows whether he got b or not.
- Alice does not know whether Bob got b or not.

OBLIVIOUS TRANSFER



Assume Alice owns b_0, b_1 two secret bits. To disclose one of them to Bob without knowing which one Bob gets, they can do the following for $p \leq \frac{3}{4}$:

Protocol for one-out-of-two O.T.

Alice and Bob agree on a security parameter s .

Alice chooses at random Ks bits r_1, r_2, \dots, r_{Ks} for some constant K to be later determined.

For each of these Ks bits Alice uses the p -O.T. protocol to disclose the bit r_i to Bob with probability p .

Bob selects $U = \{i_1, i_2, \dots, i_{\alpha_s}\}$ and $V = \{i_{\alpha_s+1}, i_{\alpha_s+2}, \dots, i_{2\alpha_s}\}$ where $\alpha_s = \left\lceil \frac{2Kps}{3} \right\rceil$

with $U \cap V = \emptyset$ and such that he knows r_{i_j} for each $i_j \in U$.

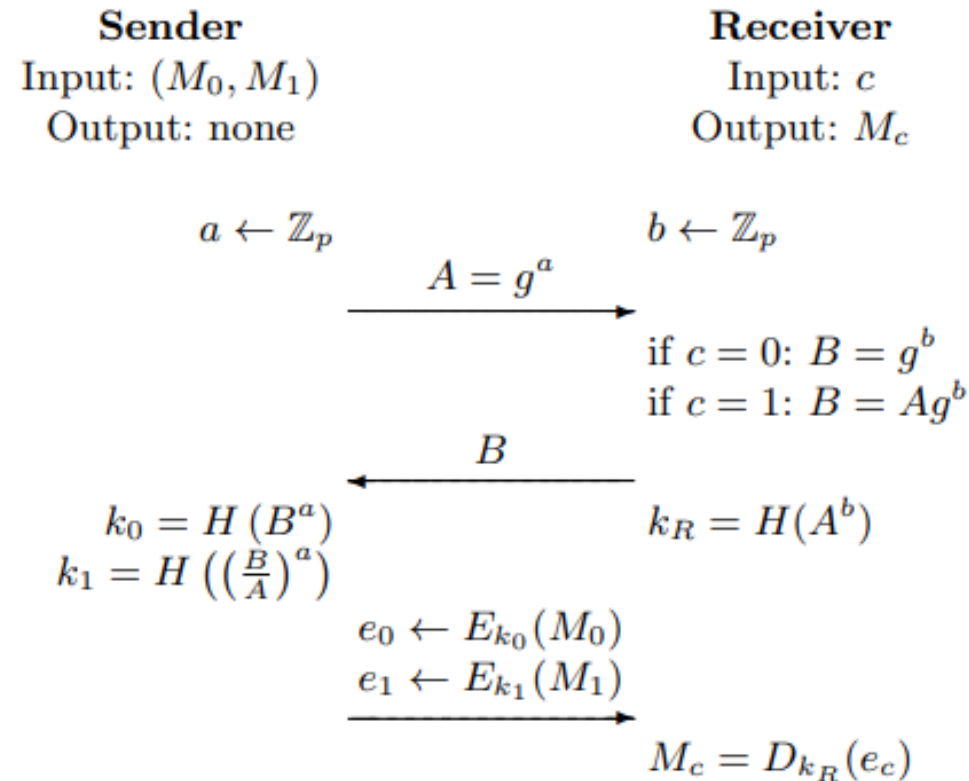
Bob sends $(X, Y) = (U, V)$ or $(X, Y) = (V, U)$ to Alice at random.

Alice computes $m_0 = \bigoplus_{x \in X} r_x$ and $m_1 = \bigoplus_{y \in Y} r_y$.

Alice returns to Bob k , $b_k \oplus m_0$ and $b_{\bar{k}} \oplus m_1$ for a random bit k .

Bob computes $\bigoplus_{u \in U} r_u \in \{m_0, m_1\}$ and uses it to get his secret bit.

OBLIVIOUS TRANSFER



OBLIVIOUS TRANSFER



The Implementation of OT_2^1

protocol $OT_2^1(S, R, M_0, M_1)$

- (1) S chooses, randomly, one instance of the PKCS, (E_x, D_x) ;
 S chooses, randomly, two messages, m_0 and m_1 , from \mathcal{M}_x (the message space of the above PKCS instance);
 S transmits E_x , m_0 , and m_1 , to R ;
- (2) R chooses, randomly, $r \in \{0, 1\}$;
 R chooses, randomly, a message $k \in \mathcal{M}_x$;
 R transmits $q = E_x(k) \oplus m_r$ to S ;
- (3) S computes $k'_i = D_x(q \oplus m_i)$, for $0 \leq i \leq 1$;
 S chooses, randomly, $s \in \{0, 1\}$;
 S transmits $(M_0 \oplus k'_s, M_1 \oplus k'_{s \oplus 1}, s)$ to R ,
(Comment: \oplus denotes addition modulo 2.)

Hier wird angenommen,
dass ein Chiffretext
nicht von einem Nicht-
Chiffretext
unterschieden werden
kann

OBLIVIOUS TRANSFER



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

À quoi bon l'enfant qui vient de naître?

Benjamin Franklin¹ (1783)