Einführung in die Quantenkryptographie

Irene Diener, Toni Roob, Jarod A. M. Békési

30. September 2025

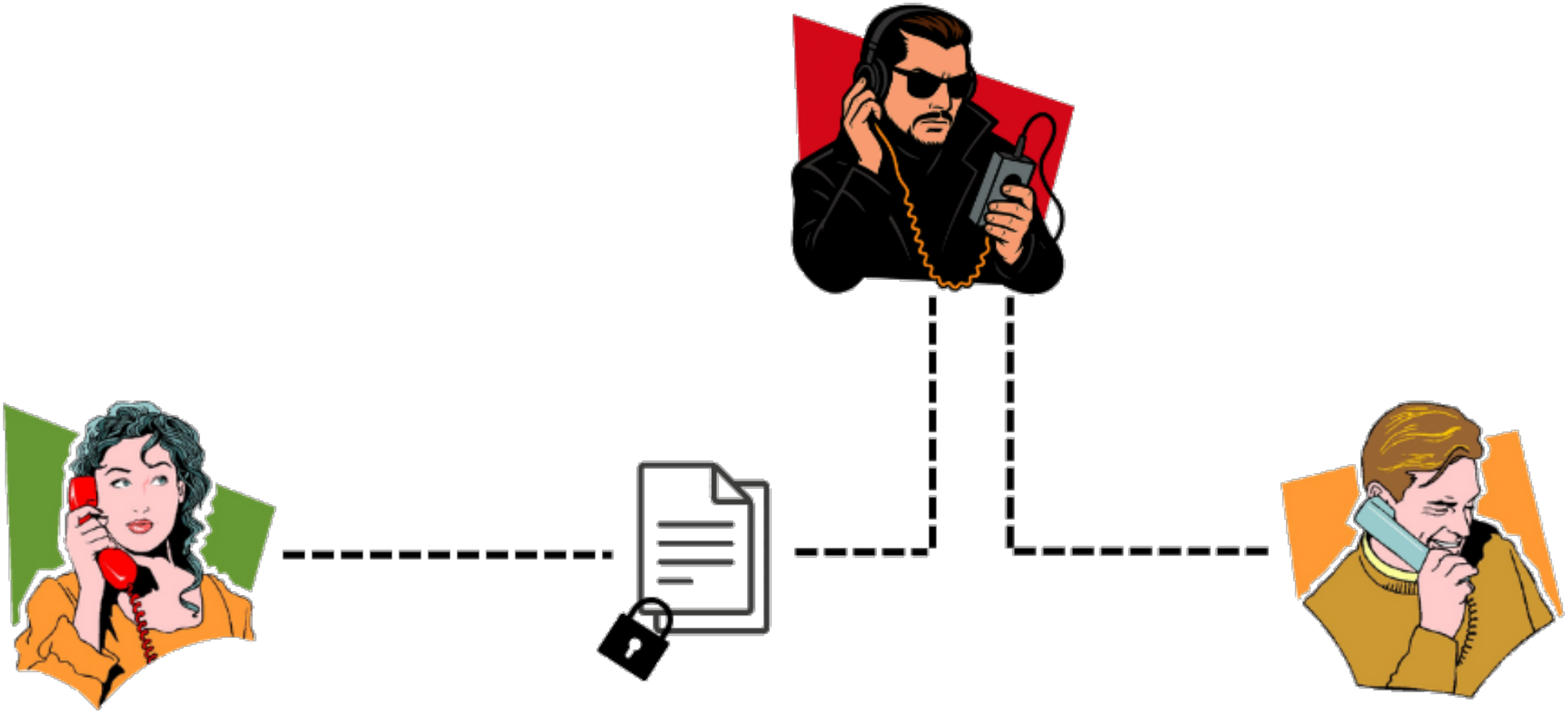
Inhaltsverzeichnis I

1. Quantum Key Distribution
   - BB84
   - B92
   - E91
2. Gitterbasierte Kryptografie
   - GGH Verschlüssung[1]
3. Quellenverzeichnis

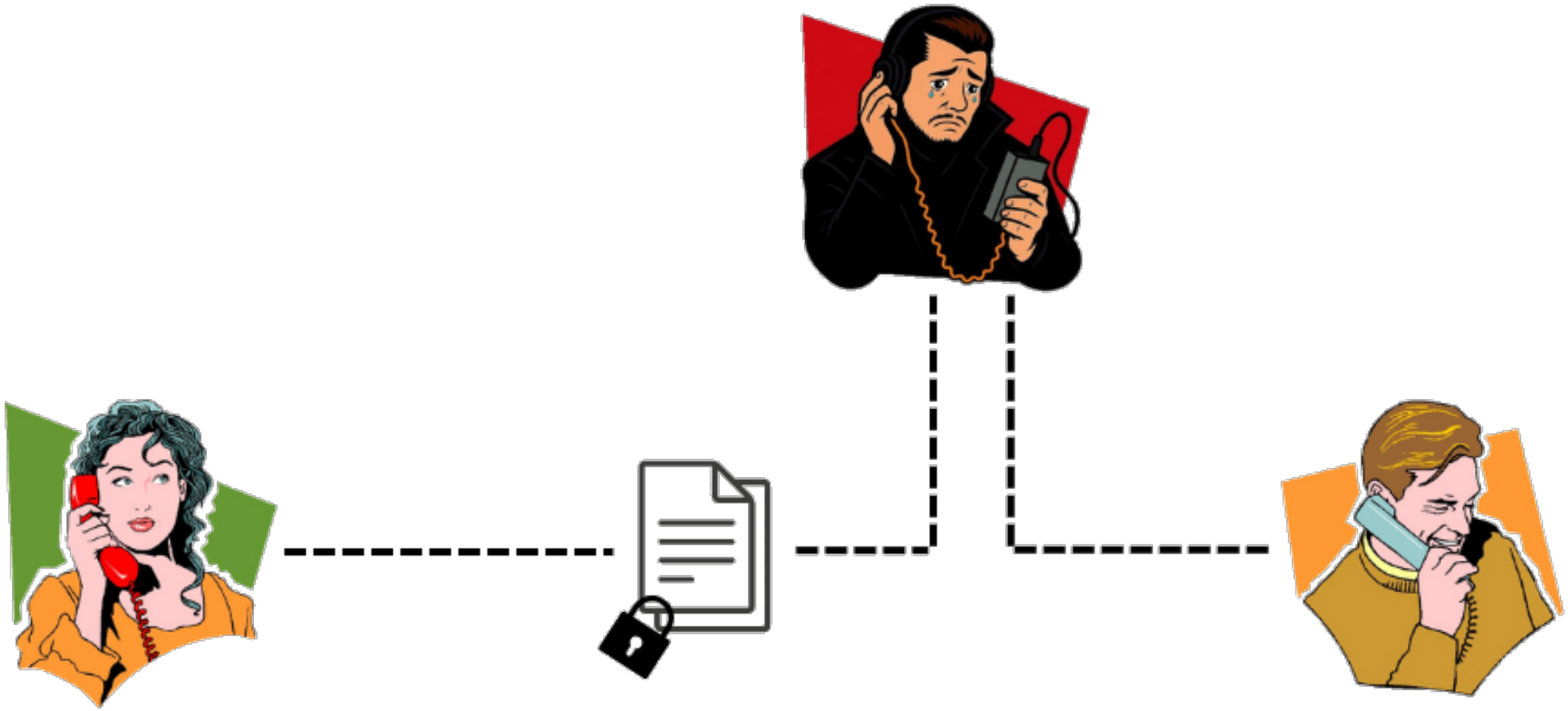
DHSN DUALE HOCHSCHULE SACHSEN

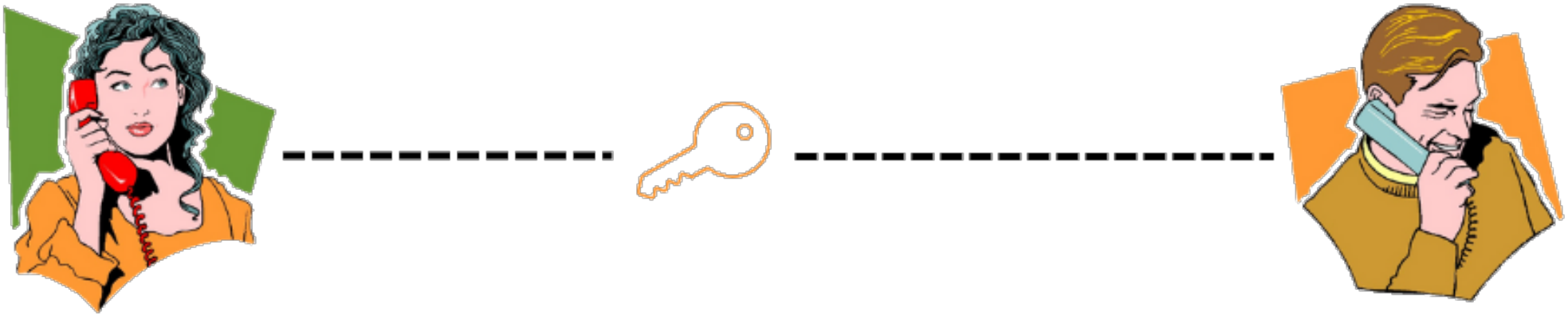
DUALE HOCHSCHULE SACHSEN

DUALE HOCHSCHULE SACHSEN



DUALE HOCHSCHULE SACHSEN





DUALE HOCHSCHULE SACHSEN

DHSN
DUALE HOCHSCHULE
SACHSEN

DHSN
DUALE HOCHSCHULE SACHSEN

BB84

- Entwickelt durch Charles Bennett und Gilles Brassard im Jahr 1984
- Lässt sich mit jedem quantenmechanischen Zwei-Zustandssystem durchführen
- Keine Verschränkung notwendig
- Meistens die Verwendung der linearen Polarisationszustände von Photonen

DHSN DUALE HOCHSCHULE SACHSEN

Polarisationsrichtungen[1]

H ,V ,D ,A

Basen (Photonenzustände):

Orthogonal: H/V – Z-Basis

H, 0°: horizontal →

V, 90°: vertikal ↑

Schräg: +/− – X-Basis

+, 45°: diagonal ↗

−, −45°: antidiagonal ↖

[1] lineare Polarisation

Alice

Photon	1	2	3	4	5	6	7	8	9	10
Basis	$+/-$	$+/-$	h/v	$+/-$	h/v	h/v	h/v	$+/-$	$+/-$	h/v
Zustand	$+$	$-$	h	$+$	h	h	h	$-$	$+$	h
Bit	1	0	0	1	0	0	0	0	1	0

DUALE HOCHSCHULE SACHSEN

Bob

Photon	1	2	3	4	5	6	7	8	9	10
Basis	$+/-$	$+/-$	h/v	h/v	$+/-$	$+/-$	h/v	h/v	$+/-$	h/v
Zustand	$+$	$-$	h	$+$	h	h	h	$-$	$+$	h
Bit	1	0	0	0	1	0	0	0	1	0

DUALE HOCHSCHULE SACHSEN

Basis-Austausch

Photon	1	2	3	4	5	6	7	8	9	10
Alice Basis	$+/-$	$+/-$	h/v	$+/-$	h/v	h/v	h/v	$+/-$	$+/-$	h/v
Bit	1	0	0	1	0	0	0	0	1	0
Bob Basis	$+/-$	$+/-$	h/v	h/v	$+/-$	$+/-$	h/v	h/v	$+/-$	h/v
Bit	1	0	0	0	1	0	0	0	1	0
Key	1	0	0	-	-	-	0	-	1	0

DUALE HOCHSCHULE SACHSEN

Eve

Photon	1	2	3	$\underline{4}$	$\underline{5}$	6	$\underline{7}$	8	9	10
Basis	h/v	h/v	$+/-$	$+/-$	h/v	$+/-$	h/v	h/v	h/v	$+/-$
Zustand	v	v	$-$	$+$	h	$-$	h	v	h	$-$
Bit	1	1	0	1	0	0	0	1	0	0

Photon	1	2	3	4	5	6	7	8	9	10
Alice Basis	$+/-$	$+/-$	h/v	$+/-$	h/v	h/v	h/v	$+/-$	$+/-$	h/v
Bit	1	0	0	1	0	0	0	0	1	0
Bob Basis[1]	$+/-$	$+/-$	h/v	h/v	$+/-$	$+/-$	h/v	h/v	$+/-$	h/v
Bit	1	0	0	0	1	0	0	0	1	0
Eve Basis	h/v	h/v	$+/-$	$+/-$	h/v	$+/-$	h/v	h/v	h/v	$+/-$
Bit	1	1	0	1	0	0	0	1	0	0
Bob Basis[2]	$+/-$	$+/-$	h/v	h/v	$+/-$	$+/-$	h/v	h/v	$+/-$	h/v
Bit	1	1	0	0	1	0	0	1	1	1

[1]: Ohne Eve; [2]: mit Eve

DHSN DUALE HOCHSCHULE SACHSEN

Übung[1]

Frage

Weshalb sollte Bob die Orientierungen bei seinen Messungen zufällig wählen?
Welche Gefahr besteht, wenn er für die Orientierungen beispielsweise abwechselnd h/v und $+/-$ wählt?

[1] Quelle [Fil23]

Übung[1]

Antwort

Die Gefahr besteht darin, dass Eve diese Vorliebe von Bob kennt.
In diesem Fall wählt sie dieselben Orientierungen bei den Messungen wie Bob. Wenn Alice und Bob später ihre gewählten Basissysteme vergleichen, erhalten sie dieselben Übereinstimmungen wie Alice und Eve. Bei den Photonen, bei denen die Orientierungen von Eve und Bob sich von denen von Alice unterscheiden, können die Messwerte verschieden sein, doch diese Bits werden verworfen. Bei den Bits, die behalten werden, stimmen Eve, Bob und Alice überein. Alice und Bob werden also nicht bemerken, dass sie belauscht wurden.

DHSN DUALE HOCHSCHULE SACHSEN

[1] Quelle [Fil23]

B92

– Zwei beliebige nicht orthogonale Zustände
– Unterscheidung der Zustände per Phase

Beispiel:

$|\alpha\rangle = 0$ und $|-\alpha\rangle = 1$

Bob misst per Homodyn-Detektion den Wert von q.

$\Rightarrow$ Wenn q:
- – größer als rechte Linie war es $|\alpha\rangle$
- – kleiner als linke Linie war es $|-\alpha\rangle$
- – Ergebnis ungültig

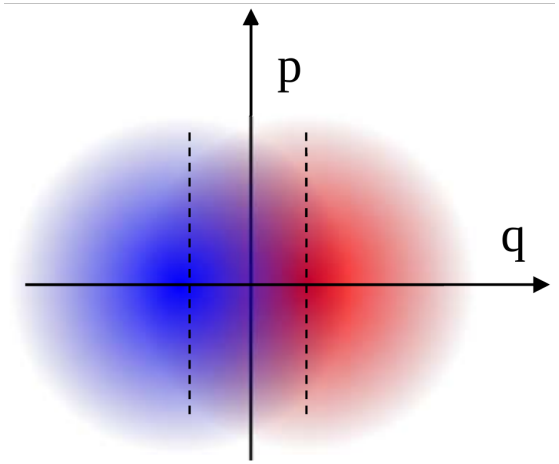


Figure: Visualisierung des B92-Protokolls

Beispiel[1]

Gesendet wird	0° (1)	0° (1)	45° (0)	45°(0)
Gemessen wird mit	90° (0)	135° (1)	90° (0)	135° (1
Detektion des Photons?	Nein	Vielleicht (1)	Vielleicht (0)	Nein

[1] Aus [SchkA]

E91

- Entwickelt durch Artur Ekert im Jahr 1991
- Verwendung von Bell States
- Auswahl zufälliger Polarisationsbasen
- Bob nutzt die inverse Interpretation von Alice (unter Verwendung von $|\Psi^{(-)}\rangle$)

Basis	H	V	D	A
Alice	0	1	0	1
Bob	1	0	1	0

DHSN DUALE HOCHSCHULE SACHSEN

Mathematischer Beweis[1] I

$$|\Psi^{(-)}\rangle = \frac{1}{\sqrt{2}}\{|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B\} \tag{1}$$

Übergang zur diagonalen Basis:

$$|H\rangle_A = a_H^+|0\rangle = \frac{1}{\sqrt{2}}(a_D^+ + a_A^+)|0\rangle = \frac{1}{\sqrt{2}}(|D\rangle_A + |A\rangle_A)$$

$$|V\rangle_A = a_H^+|0\rangle = \frac{1}{\sqrt{2}}(a_D^+ - a_A^+)|0\rangle = \frac{1}{\sqrt{2}}(|D\rangle_A - |A\rangle_A)$$

DHSN DUALE HOCHSCHULE SACHSEN

[1] Aus [Gro18] übernommen

Mathematischer Beweis[1] II

Photon B

$$|\Psi^{(-)}\rangle = \frac{1}{2\sqrt{2}}\{(|D\rangle_A + |A\rangle_A)(|D\rangle_B - |A\rangle_B) - (|D\rangle_A + |A\rangle_A)(|D\rangle_B - |A\rangle_B)\}$$
$$= \frac{1}{2\sqrt{2}}\{|A\rangle_A|D\rangle_B - |D\rangle_A|A\rangle_B)\}$$

[1] Aus [Gro18] übernommen

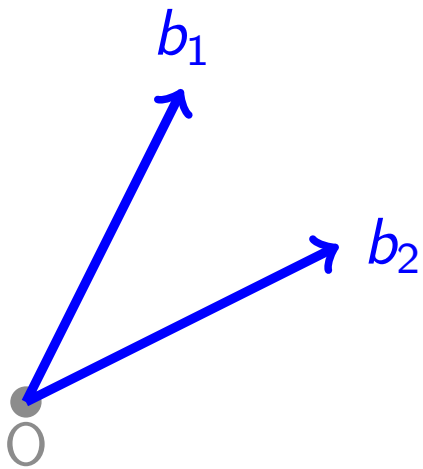
Inhaltsverzeichnis I

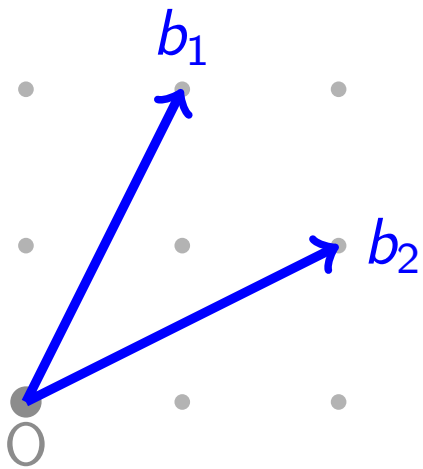
1 Quantum Key Distribution
- BB84
- B92
- E91

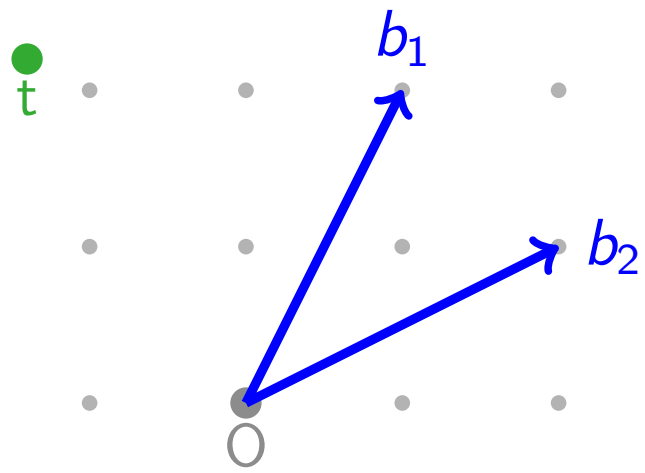
2 Gitterbasierte Kryptografie
- GGH Verschlüssung[1]

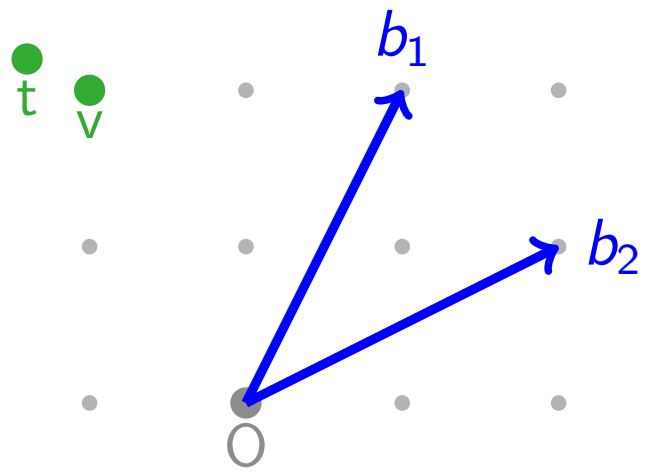
3 Quellenverzeichnis

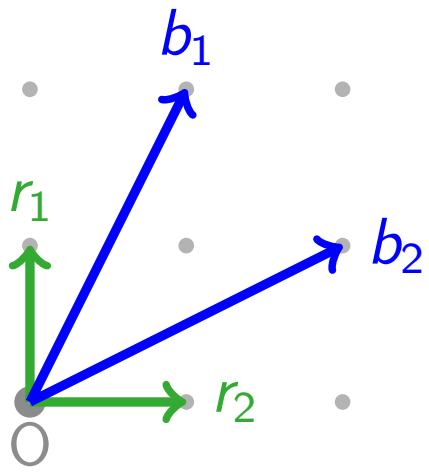
DHSN DUALE HOCHSCHULE SACHSEN

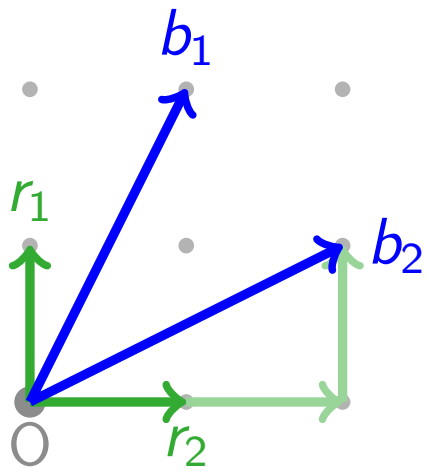

b_1
b_2
0

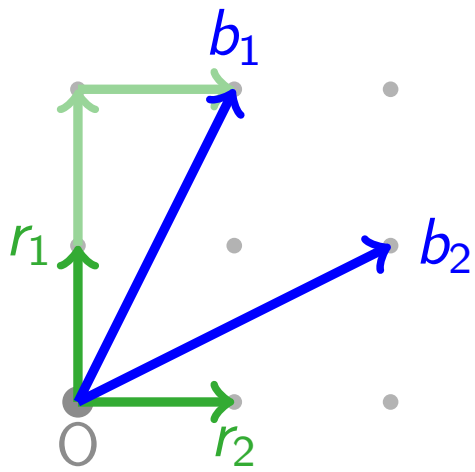

b_1
b_2
0


t
b_1
b_2
0


t
v
b_1
b_2
0


b_1
r_1
b_2
r_2
O


b_1
r_1
b_2
O
r_2


b_1
b_2
r_1
r_2
O

GGH Verschlüssung

Private key: $R = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix}$

Encrypt $\mathbf{m}$:

$\mathbf{v} = \mathbf{m}B$

$\mathbf{c} = \mathbf{v} + \mathbf{e}$

Decrypt $\mathbf{c}$:

$\mathbf{v}' = \lfloor \mathbf{c}R^{-1} \rceil R$

$\mathbf{m}' = \mathbf{v}'B^{-1}$

[1] Basierend auf [Thi15]

Private key: $R = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix}$

Encrypt $\mathbf{m}$:

$\mathbf{v} = \mathbf{m}B$

$\mathbf{c} = \mathbf{v} + \mathbf{e}$

Decrypt $\mathbf{c}$:

$\mathbf{v}' = \lfloor \mathbf{c}R^{-1} \rceil R$

$\mathbf{m}' = \mathbf{v}'B^{-1}$

[1] Basierend auf [Thi15]

Private key: $R = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix}$

Encrypt $\mathbf{m}$:

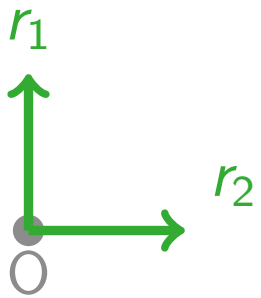
$\mathbf{v} = \mathbf{m}B$

$\mathbf{c} = \mathbf{v} + \mathbf{e}$

Decrypt $\mathbf{c}$:

$\mathbf{v}' = \lfloor \mathbf{c}R^{-1} \rceil R$

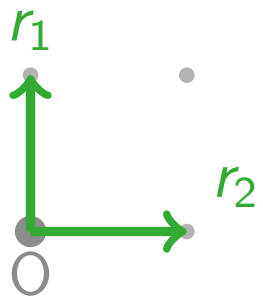
$\mathbf{m}' = \mathbf{v}'B^{-1}$



[1] Basierend auf [Thi15]

Private key: $R = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix}$



Encrypt $\mathbf{m}$:

$\mathbf{v} = \mathbf{m}B$

$\mathbf{c} = \mathbf{v} + \mathbf{e}$

Decrypt $\mathbf{c}$:

$\mathbf{v}' = \lfloor \mathbf{c}R^{-1} \rceil R$

$\mathbf{m}' = \mathbf{v}'B^{-1}$

[1] Basierend auf [Thi15]

Private key: $R = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix}$

Encrypt $\mathbf{m}$:

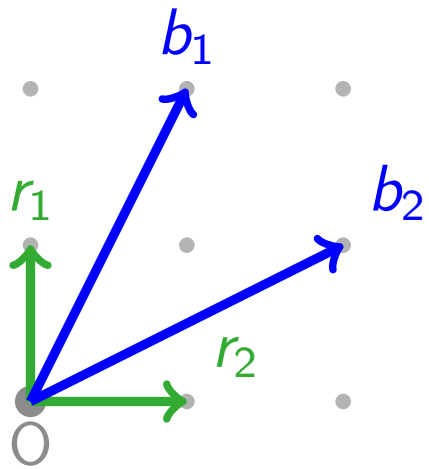
$\mathbf{v} = \mathbf{m}B$

$\mathbf{c} = \mathbf{v} + \mathbf{e}$

Decrypt $\mathbf{c}$:

$\mathbf{v}' = \lfloor \mathbf{c}R^{-1} \rceil R$

$\mathbf{m}' = \mathbf{v}'B^{-1}$



[1] Basierend auf [Thi15]

Private key: $R = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix}$

Encrypt $\mathbf{m}$:

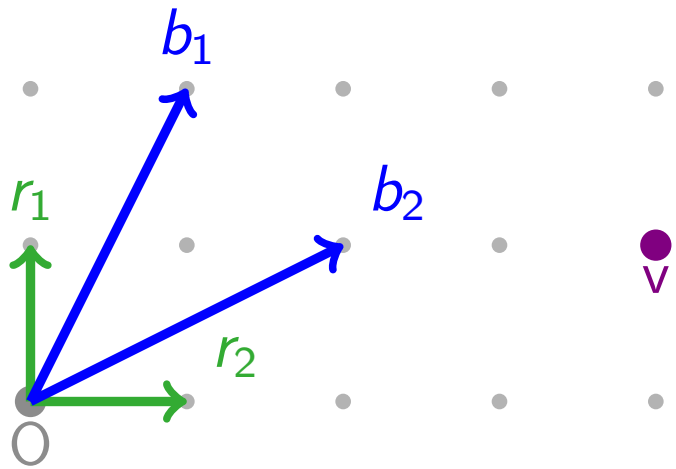
$\mathbf{v} = \mathbf{m}B$

$\mathbf{c} = \mathbf{v} + \mathbf{e}$

Decrypt $\mathbf{c}$:

$\mathbf{v}' = \lfloor \mathbf{c}R^{-1} \rceil R$

$\mathbf{m}' = \mathbf{v}'B^{-1}$



[1] Basierend auf [Thi15]

Private key: $R = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix}$

Encrypt $\mathbf{m}$:

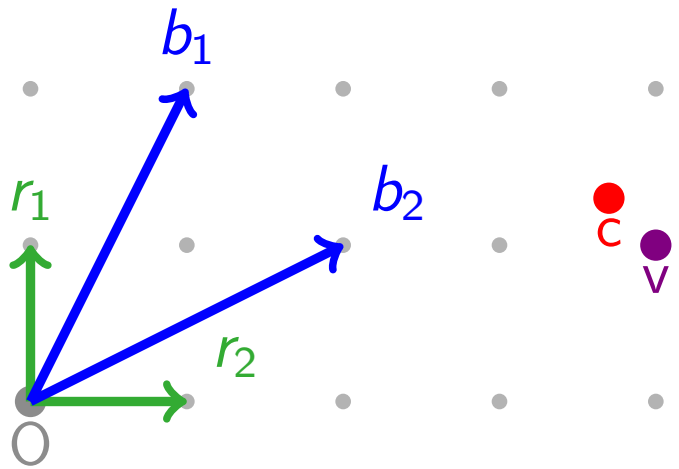
$\mathbf{v} = \mathbf{m}B$

$\mathbf{c} = \mathbf{v} + \mathbf{e}$

Decrypt $\mathbf{c}$:

$\mathbf{v}' = \lfloor \mathbf{c}R^{-1} \rceil R$

$\mathbf{m}' = \mathbf{v}'B^{-1}$



[1] Basierend auf [Thi15]

Private key: $R = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix}$

Encrypt $\mathbf{m}$:

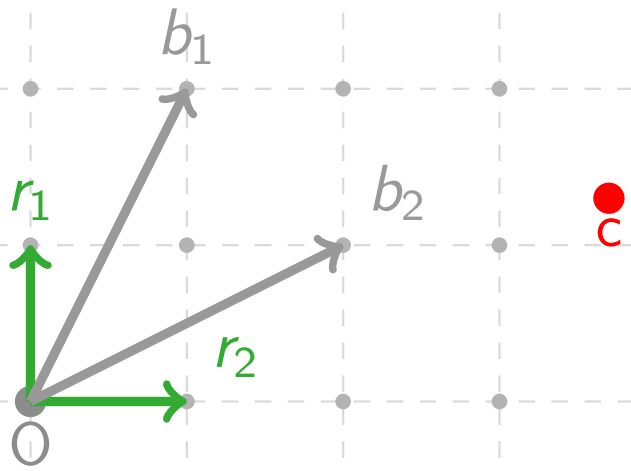
$\mathbf{v} = \mathbf{m}B$

$\mathbf{c} = \mathbf{v} + \mathbf{e}$

Decrypt $\mathbf{c}$:

$\mathbf{v}' = \lfloor \mathbf{c}R^{-1} \rceil R$

$\mathbf{m}' = \mathbf{v}'B^{-1}$



[1] Basierend auf [Thi15]

Private key: $R = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix}$

Encrypt $\mathbf{m}$:

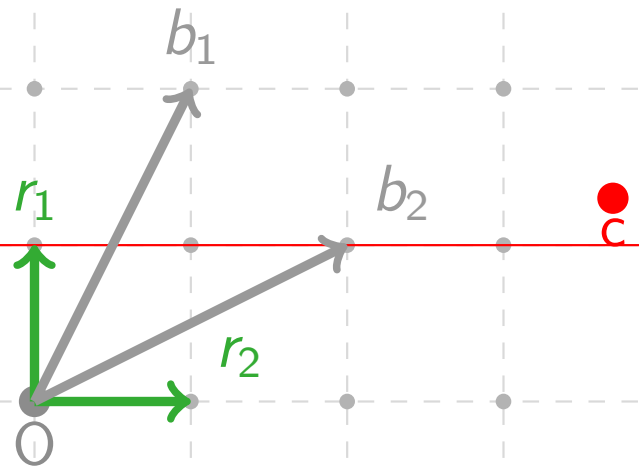
$\mathbf{v} = \mathbf{m}B$

$\mathbf{c} = \mathbf{v} + \mathbf{e}$

Decrypt $\mathbf{c}$:

$\mathbf{v}' = \lfloor \mathbf{c}R^{-1} \rceil R$

$\mathbf{m}' = \mathbf{v}'B^{-1}$



[1] Basierend auf [Thi15]

Private key: $R = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix}$

Encrypt $\mathbf{m}$:

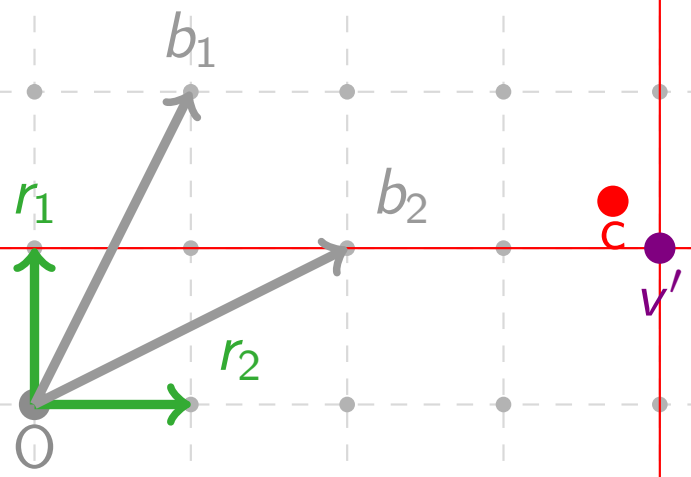
$\mathbf{v} = \mathbf{m}B$

$\mathbf{c} = \mathbf{v} + \mathbf{e}$

Decrypt $\mathbf{c}$:

$\mathbf{v}' = \lfloor \mathbf{c}R^{-1} \rceil R$

$\mathbf{m}' = \mathbf{v}'B^{-1}$



[1] Basierend auf [Thi15]

Private key: $R = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix}$

Encrypt $\mathbf{m}$:

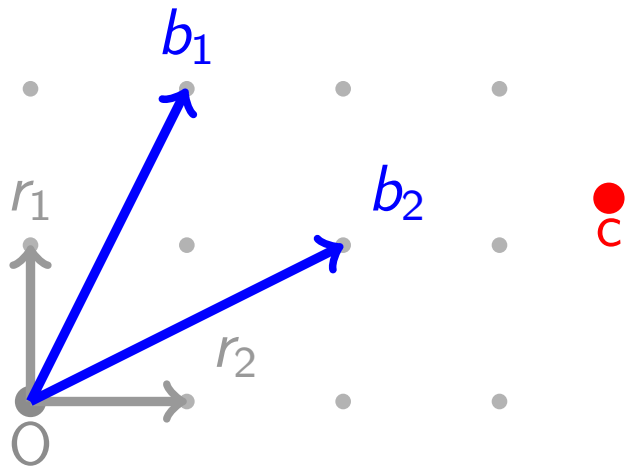
$\mathbf{v} = \mathbf{m}B$

$\mathbf{c} = \mathbf{v} + \mathbf{e}$

Decrypt $\mathbf{c}$:

$\mathbf{v}' = \lfloor \mathbf{c}R^{-1} \rceil R$

$\mathbf{m}' = \mathbf{v}'B^{-1}$



[1] Basierend auf [Thi15]

Private key: $R = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix}$

Encrypt $\mathbf{m}$:

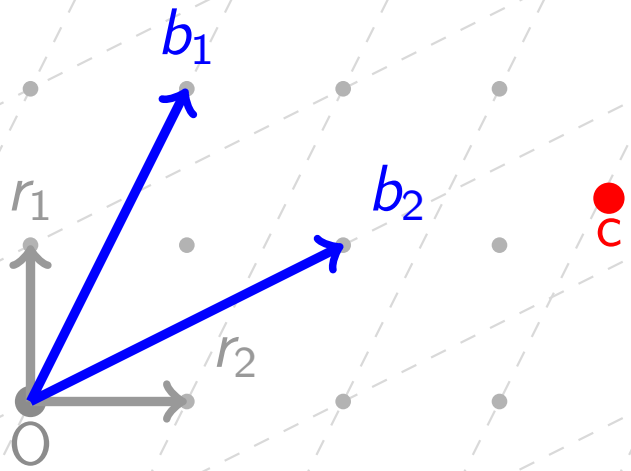
$\mathbf{v} = \mathbf{m}B$

$\mathbf{c} = \mathbf{v} + \mathbf{e}$

Decrypt $\mathbf{c}$:

$\mathbf{v}' = \lfloor \mathbf{c}R^{-1} \rceil R$

$\mathbf{m}' = \mathbf{v}'B^{-1}$



[1] Basierend auf [Thi15]

Private key: $R = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix}$

Encrypt $\mathbf{m}$:

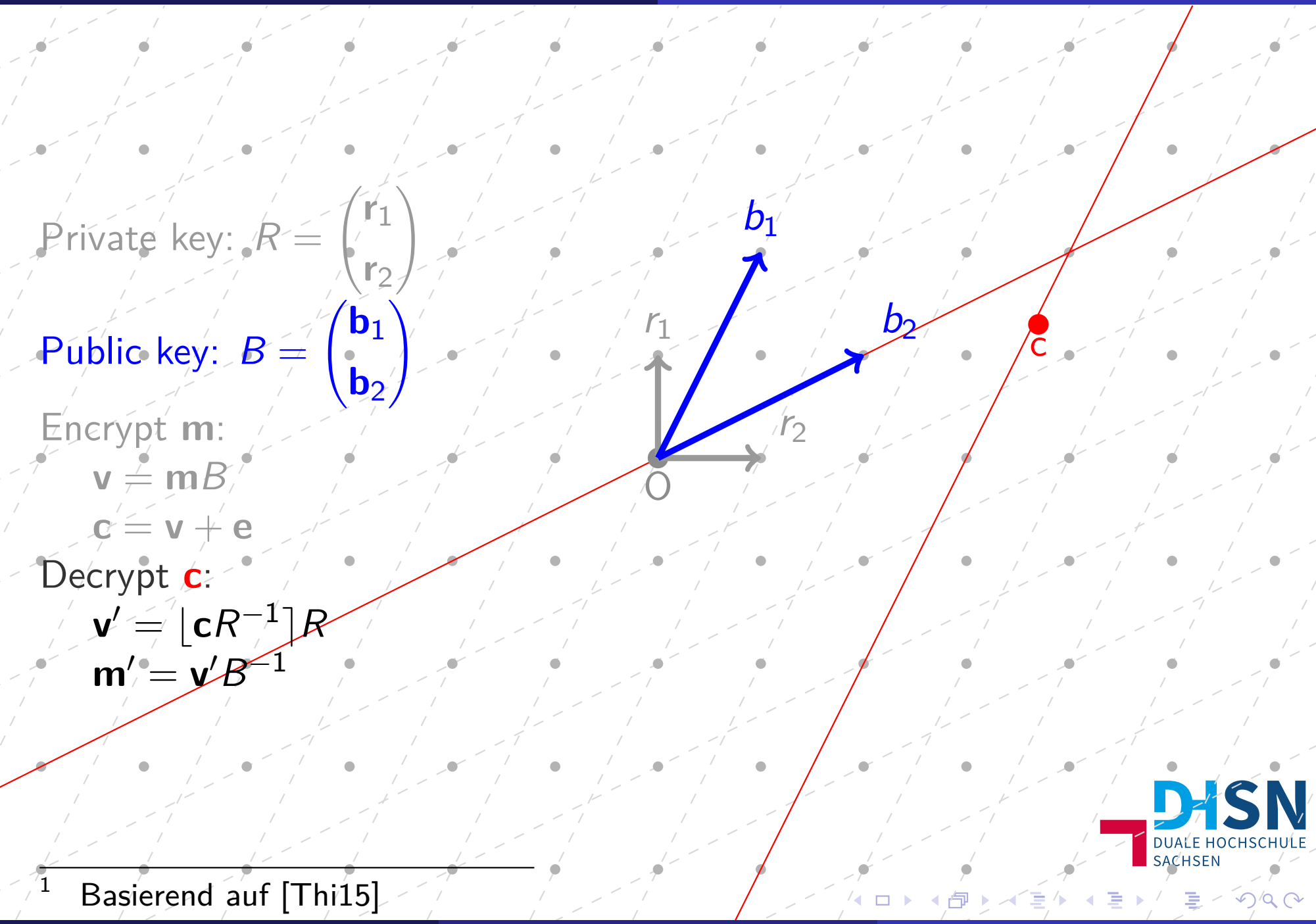
$\mathbf{v} = \mathbf{m}B$

$\mathbf{c} = \mathbf{v} + \mathbf{e}$

Decrypt $\mathbf{c}$:

$\mathbf{v}' = \lfloor \mathbf{c}R^{-1} \rceil R$

$\mathbf{m}' = \mathbf{v}'B^{-1}$



[1] Basierend auf [Thi15]

Private key: $R = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix}$

Encrypt $\mathbf{m}$:

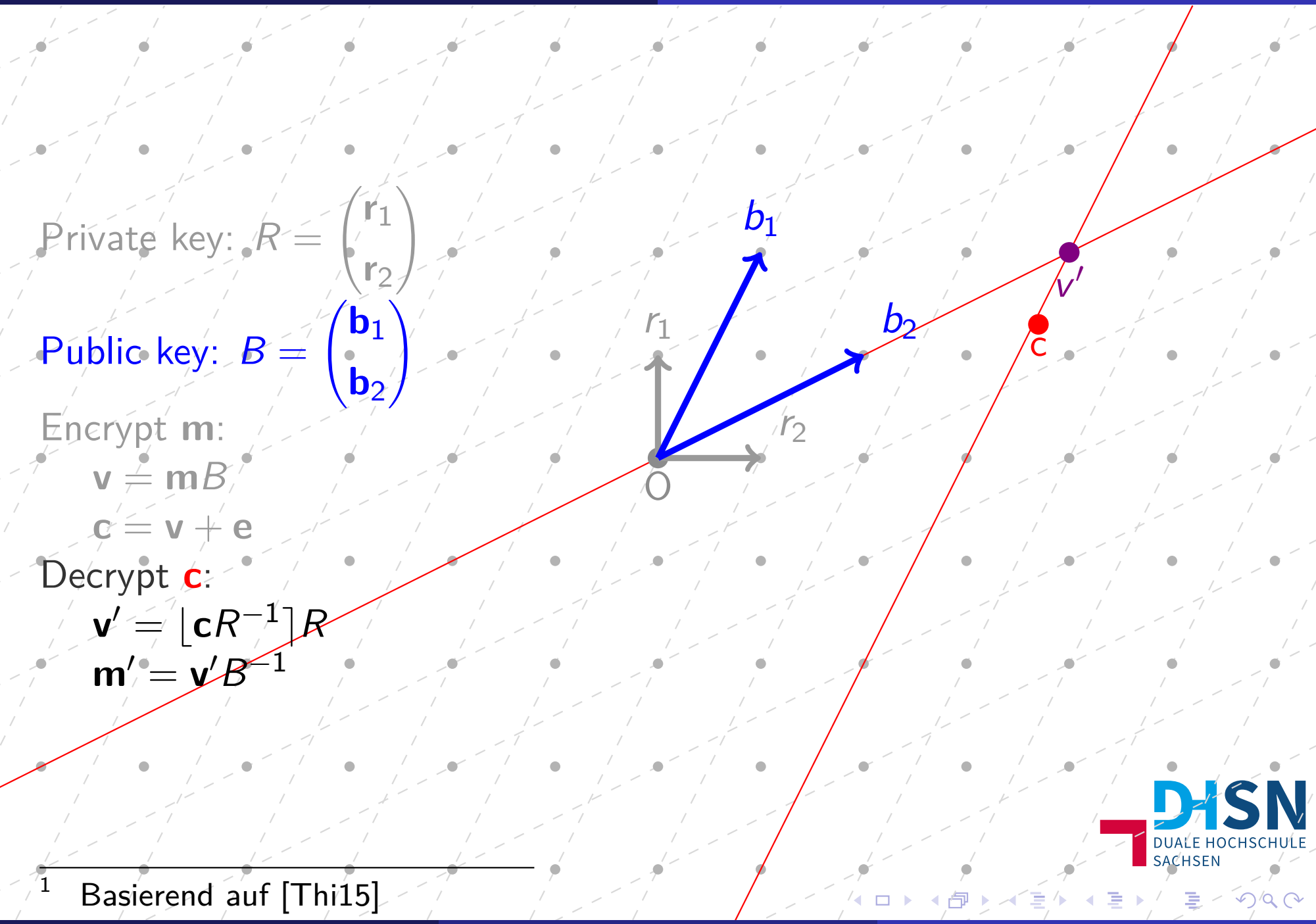
$\mathbf{v} = \mathbf{m}B$

$\mathbf{c} = \mathbf{v} + \mathbf{e}$

Decrypt $\mathbf{c}$:

$\mathbf{v}' = \lfloor \mathbf{c}R^{-1} \rceil R$

$\mathbf{m}' = \mathbf{v}'B^{-1}$



[1] Basierend auf [Thi15]

Private key: $R = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix}$

Encrypt $\mathbf{m}$:

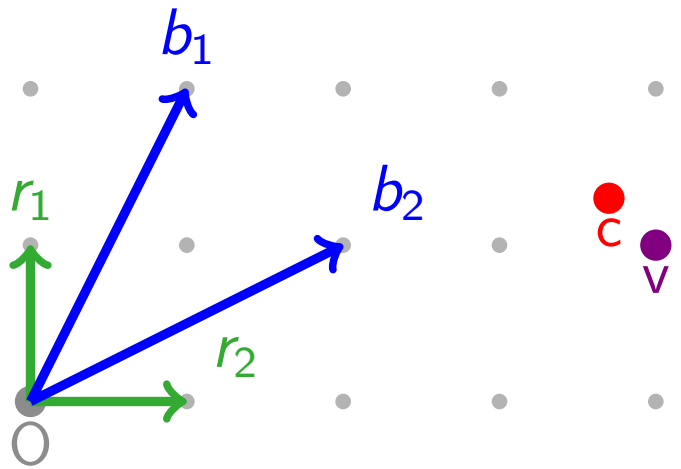
$\mathbf{v} = \mathbf{m}B$

$\mathbf{c} = \mathbf{v} + \mathbf{e}$

Decrypt $\mathbf{c}$:

$\mathbf{v}' = \lfloor \mathbf{c}R^{-1} \rceil R$

$\mathbf{m}' = \mathbf{v}'B^{-1}$



[1] Basierend auf [Thi15]

Inhaltsverzeichnis I

1. Quantum Key Distribution
   - BB84
   - B92
   - E91
2. Gitterbasierte Kryptografie
   - GGH Verschlüssung[1]
3. Quellenverzeichnis

Quellenverzeichnis I

Filk, Thomas:
BB48 – Quantenkryptographie.
https://physikdidaktik.uni-freiburg.de/wp-content/uploads/2023/06/BB84-Quantenkryptographie.pdf.
Version: Juni 2023, Abruf: 17.09.2025

Group, Chekhova R.:
Lecture 12: Quantum key distribution.
https://mpl.mpg.de/fileadmin/user_upload/Chekhova_Research_Group/Lecture_4_12.pdf, 2018. –
Lecture on Polarization of Light in Classical, Nonlinear, and Quantum Optics

DHSN DUALE HOCHSCHULE SACHSEN

Quellenverzeichnis II

Schmidt, Martin:
Quantenkryptographie.
https://gocs.de/pages/quanten/report/quantenkryptologie.pdf, k.A.

Thijs, L.:
Lattice Cryptography and Lattice Cryptanalysis.
https://ve42.co/Thijs2015, 2015. – TU Eindhoven

DHSN DUALE HOCHSCHULE SACHSEN