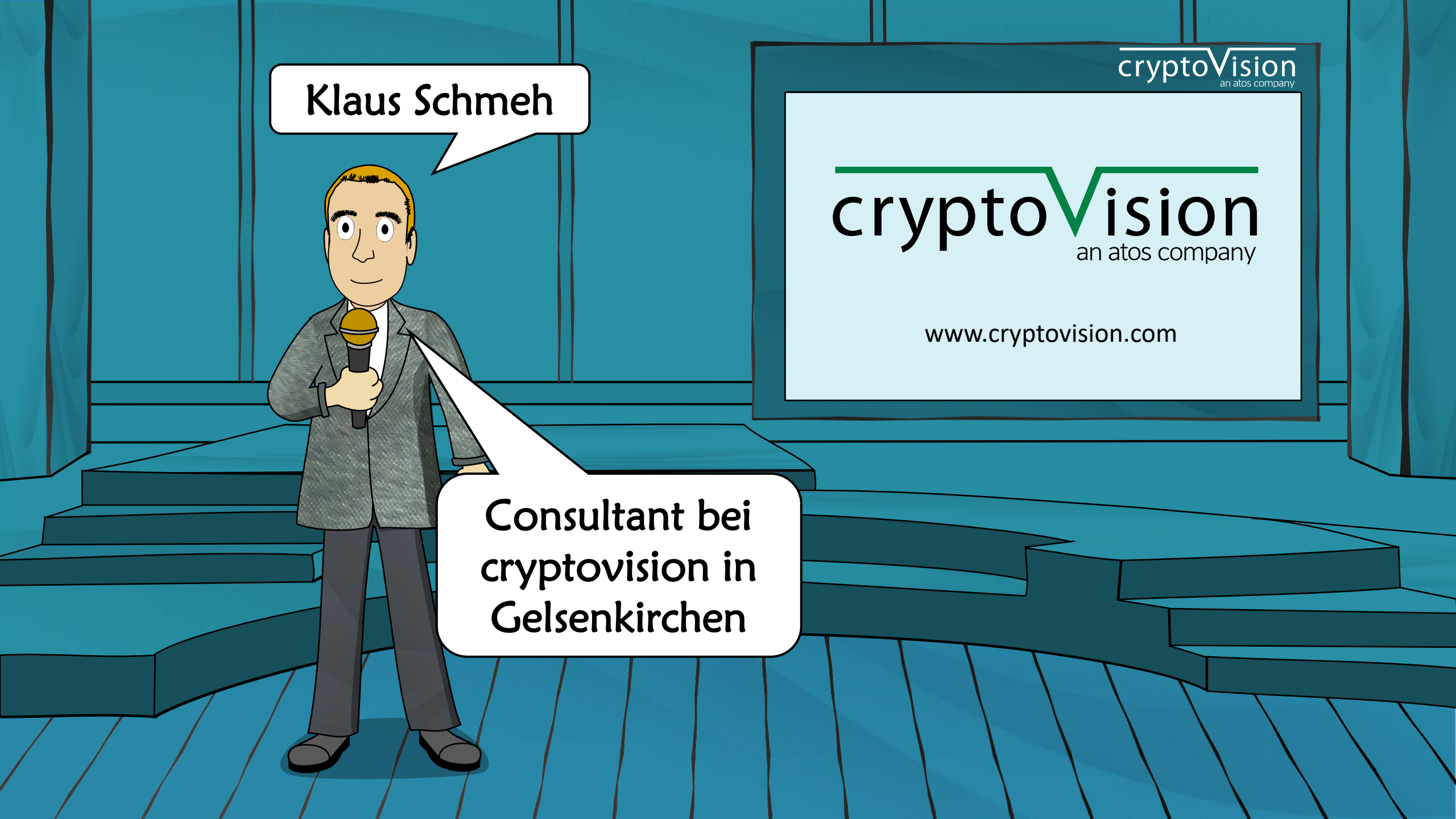
TeleTrusT/VOI-Informationstag "Elektronische Signatur und Vertrauensdienste"

Berlin, 23.09.2021

Die drei wichtigsten Post-Quantum-Signatur-Verfahren anschaulich erklärt

Klaus Schmeh, cryptovision (an Atos company)


Klaus Schmeh
Consultant bei cryptovision in Gelsenkirchen
cryptoVision
an atos company
cryptoVision
an atos company
www.cryptovision.com


Eine Einführung in die Post-Quanten-Kryptografie ...
... werde ich heute nicht geben.
crypto vision
an atos company

Es gibt Dutzende von Post-Quanten-Signatur-Verfahren.

Fünf davon sind besonders wichtig!

Man kann sie in drei Gruppen einteilen.

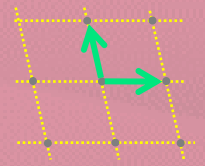
cryptoVision
an atos company

NIST-Wettbewerb

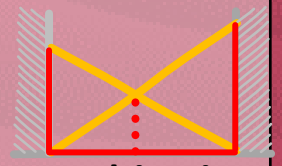
CRYSTALS-DILITHIUM

FALCON

Rainbow



gitterbasiert

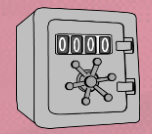


multivariat

RFC-Standard

XMSS

Leighton-Micali

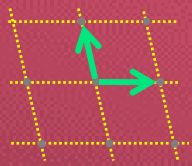


Hash-basiert


Mein erster Gast ist Herr Schnecke.
cryptoVision
an atos company

Herr Schnecke, können Sie uns gitterbasierte Signaturen erklären?

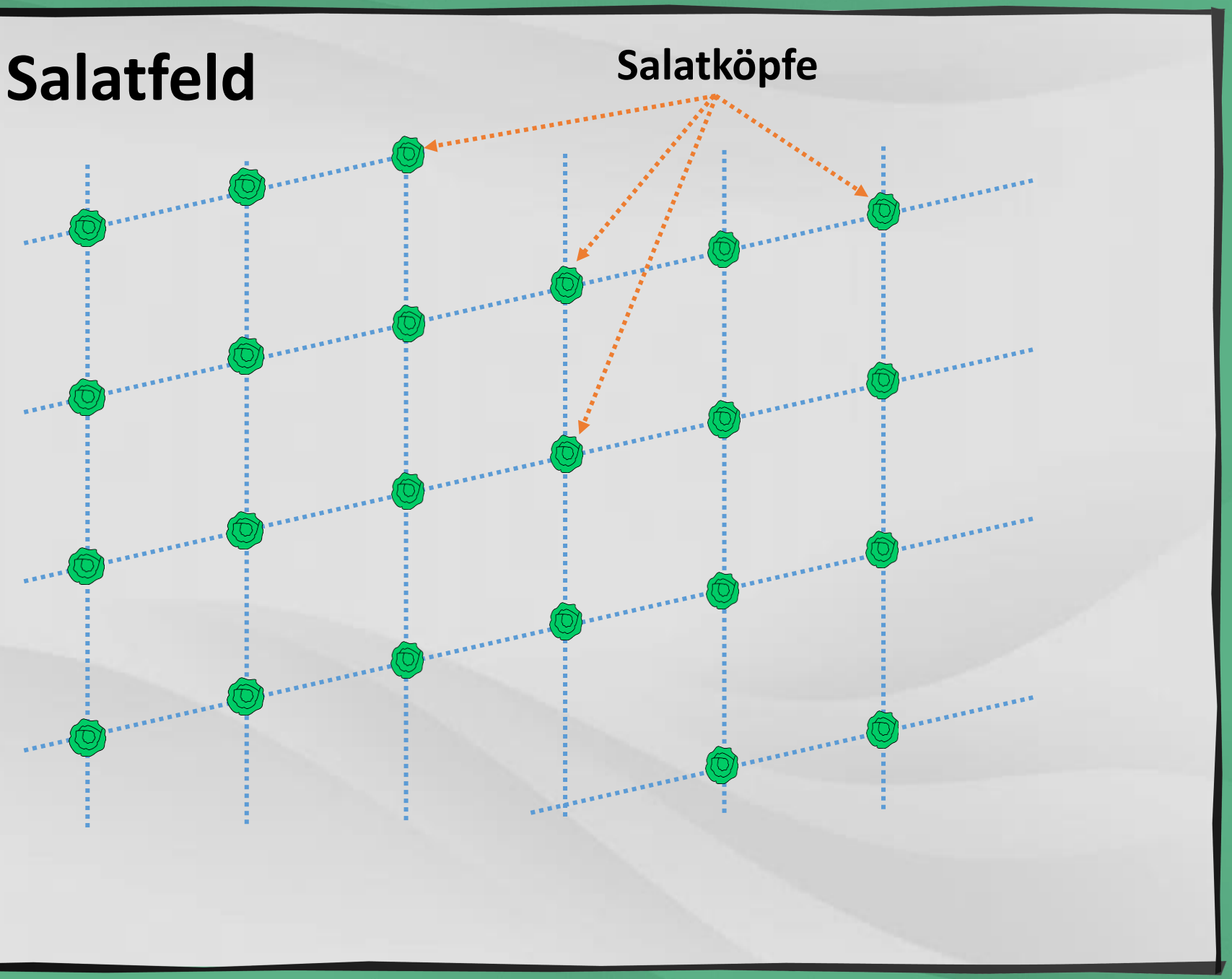
cryptoVision
an atos company

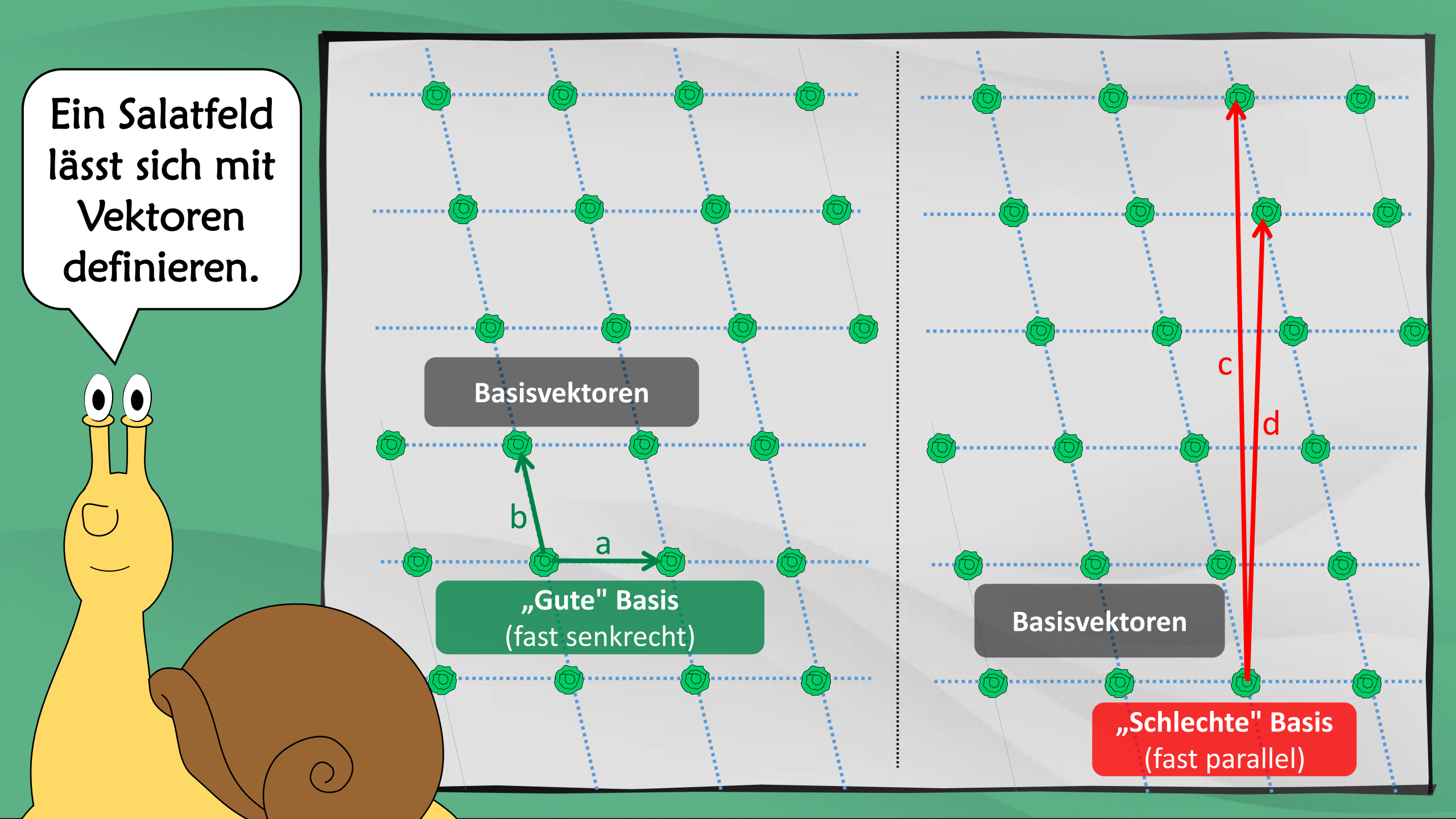


Gitter

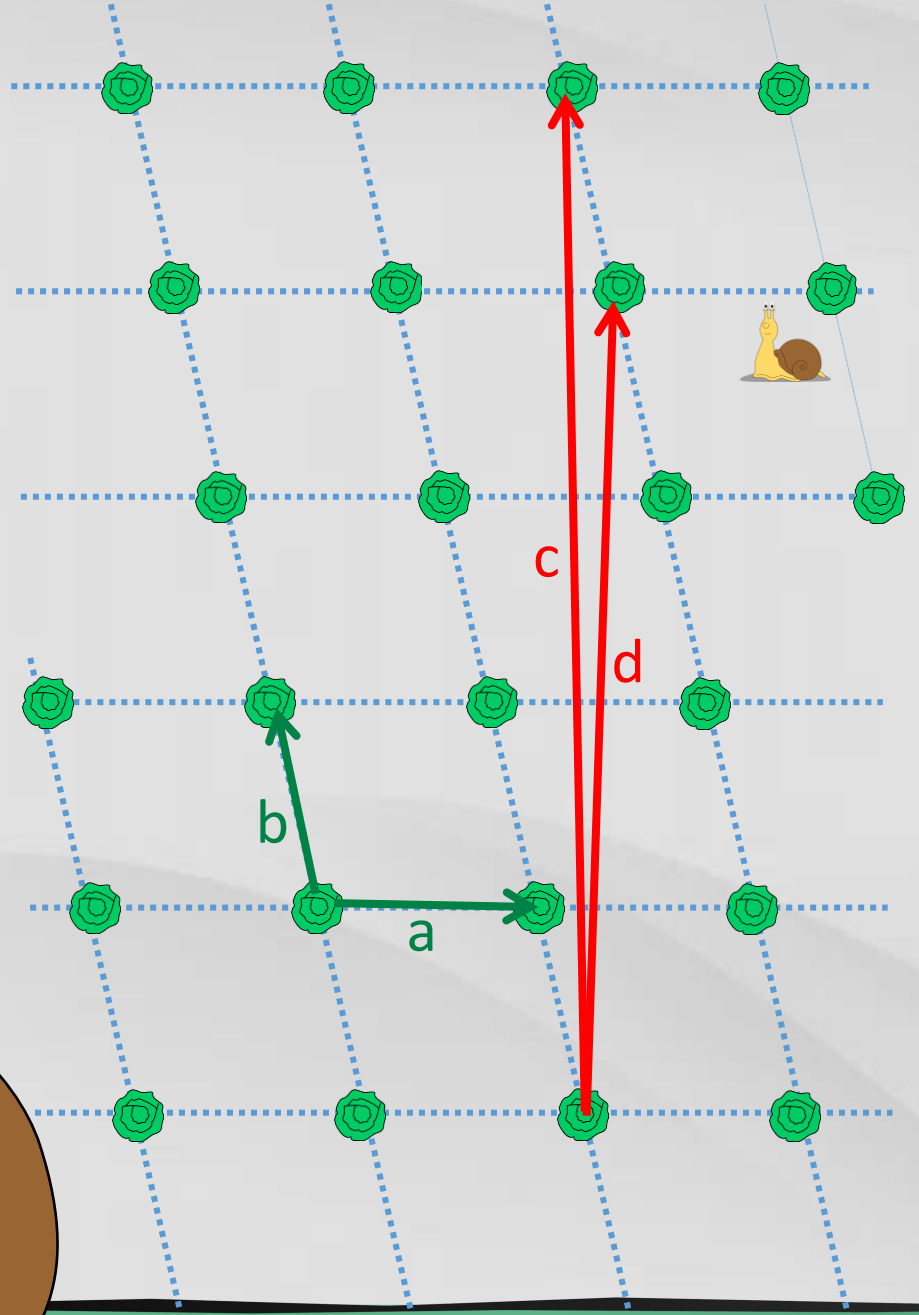
Mit Vergnügen!

Ein Gitter ist für mich ein Salatfeld.




Ein Salatfeld lässt sich mit Vektoren definieren.
Basisvektoren
b
a
„Gute" Basis
(fast senkrecht)
c
d
Basisvektoren
„Schlechte" Basis
(fast parallel)

Schnecke-im-Salat-Problem



Welcher Salatkopf ist der nächste?

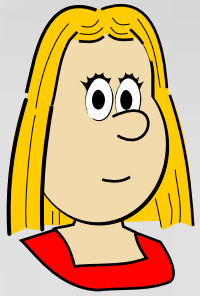
Im zweidimensionalen Raum einfach zu beantworten

Aber im 250-dimensionalenRaum?

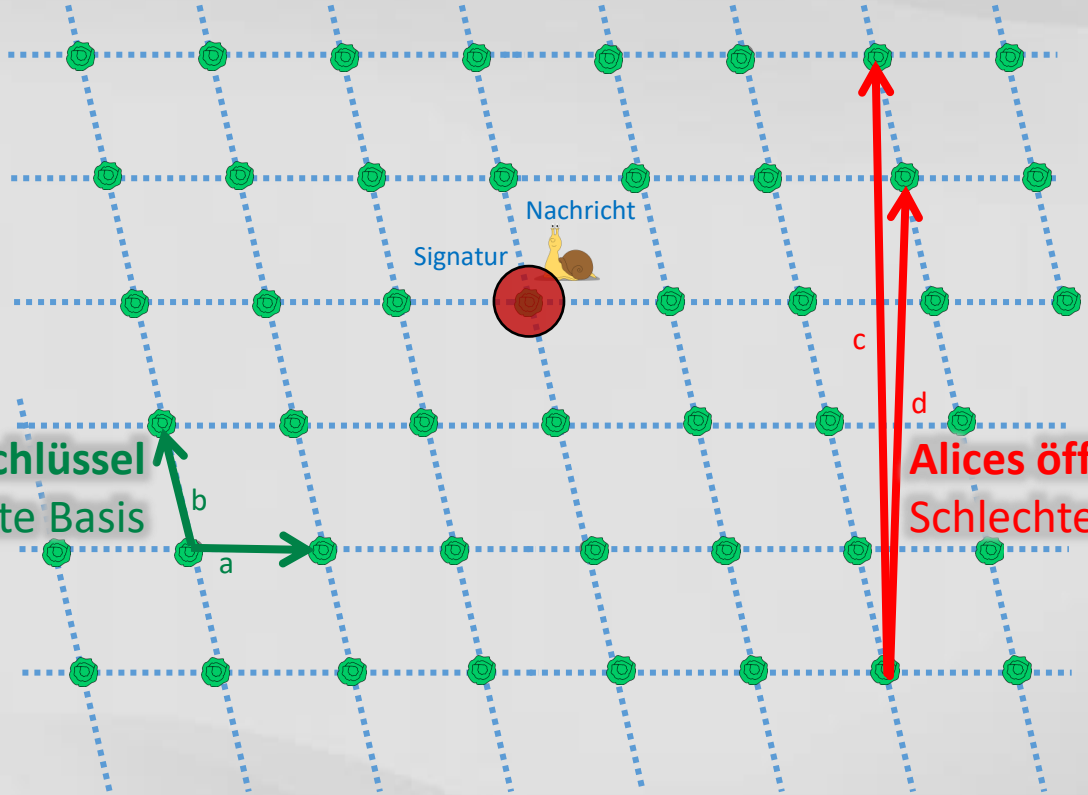
Einfach zu finden, wenn gute Basis bekannt ist

Schwer zu finden, wenn nur schlechte Basis bekannt ist

FALCON-Signatur-verfahren

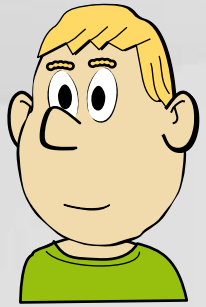


Alice



Alices privater Schlüssel
gute Basis

Alices öffentlicher Schlüssel
Schlechte Basis



Bob

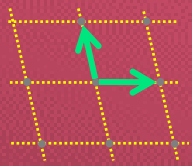
Signatur: aus Sicht der Schnecke nächster Salatkopf

Verifikation: Angreifer prüft, ob Abstand klein ist

Und was ist mit CRYSTALS-DILITHIUM?

Ähnliches Prinzip

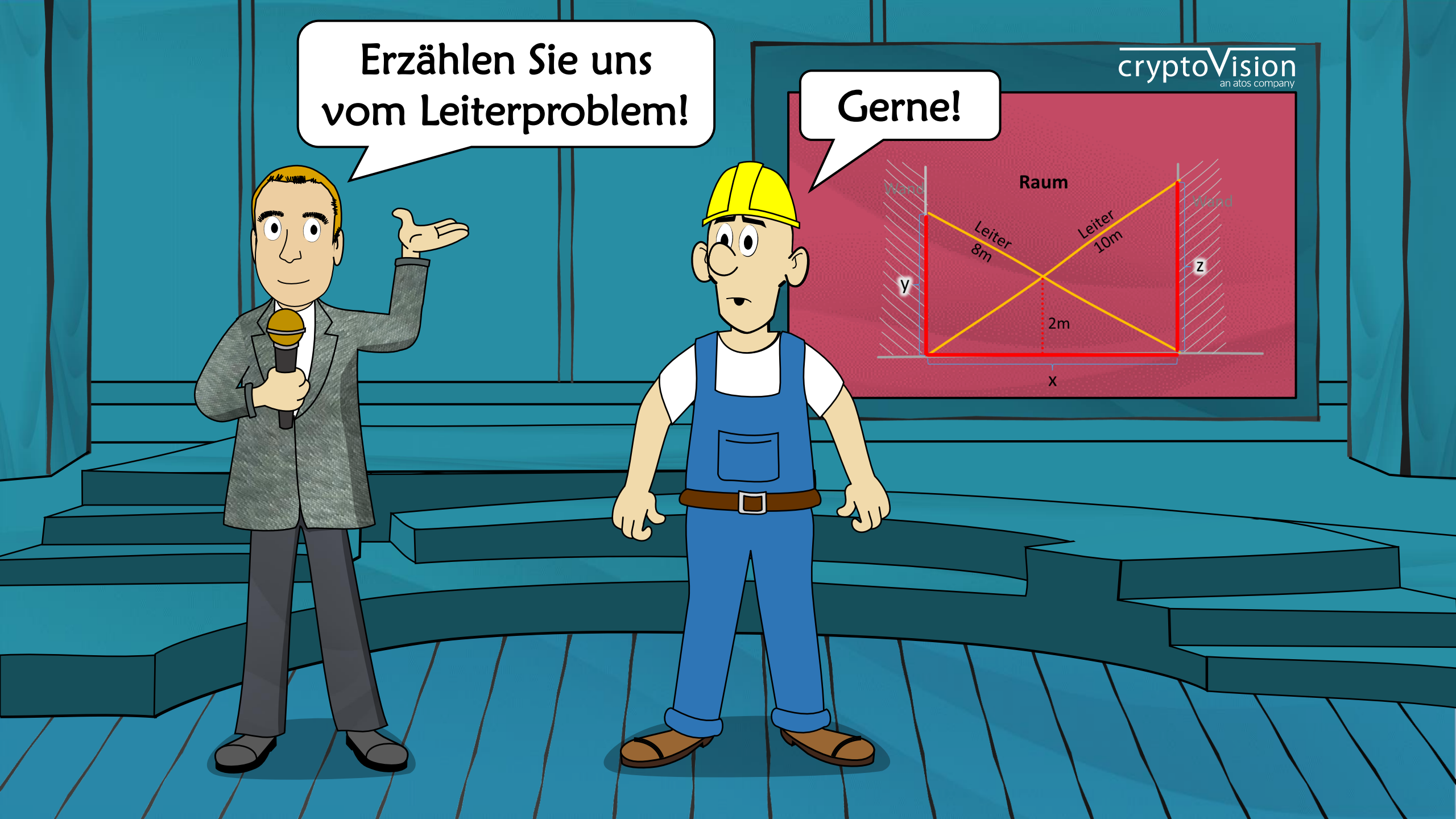
cryptoVision
an atos company



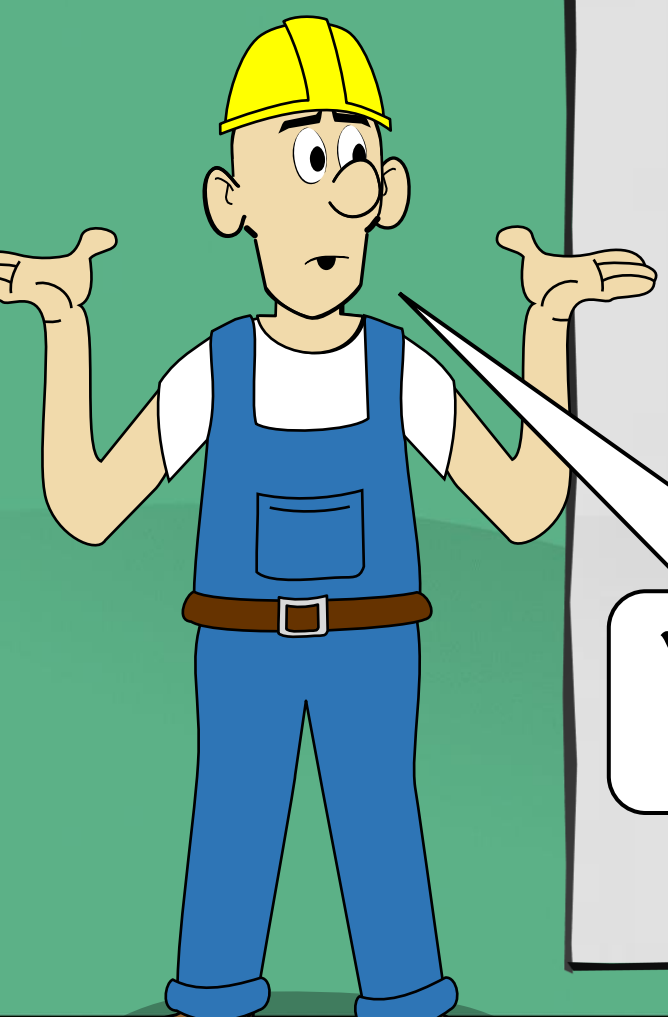
Gitter


Danke, Herr Schnecke!
cryptoVision
an atos company

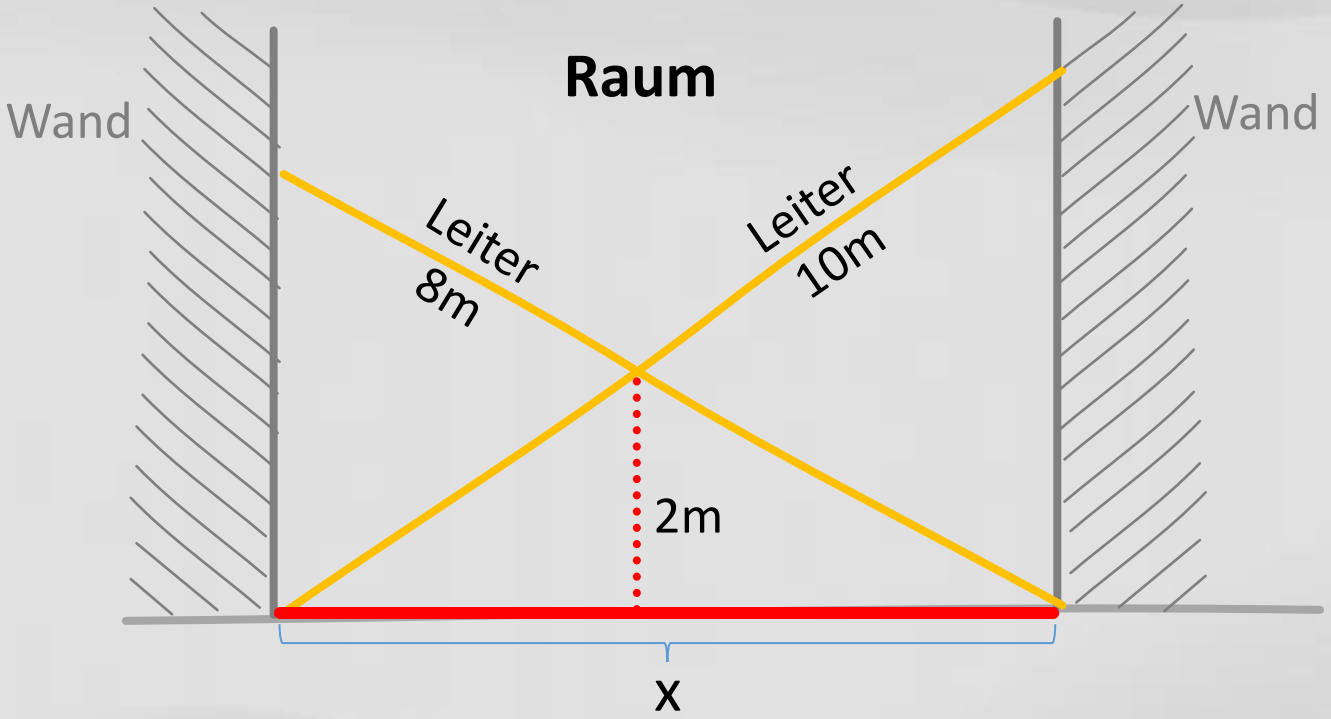

Unser nächster Gast ist ein Handwerker!
Hallo!
cryptoVision
an atos company

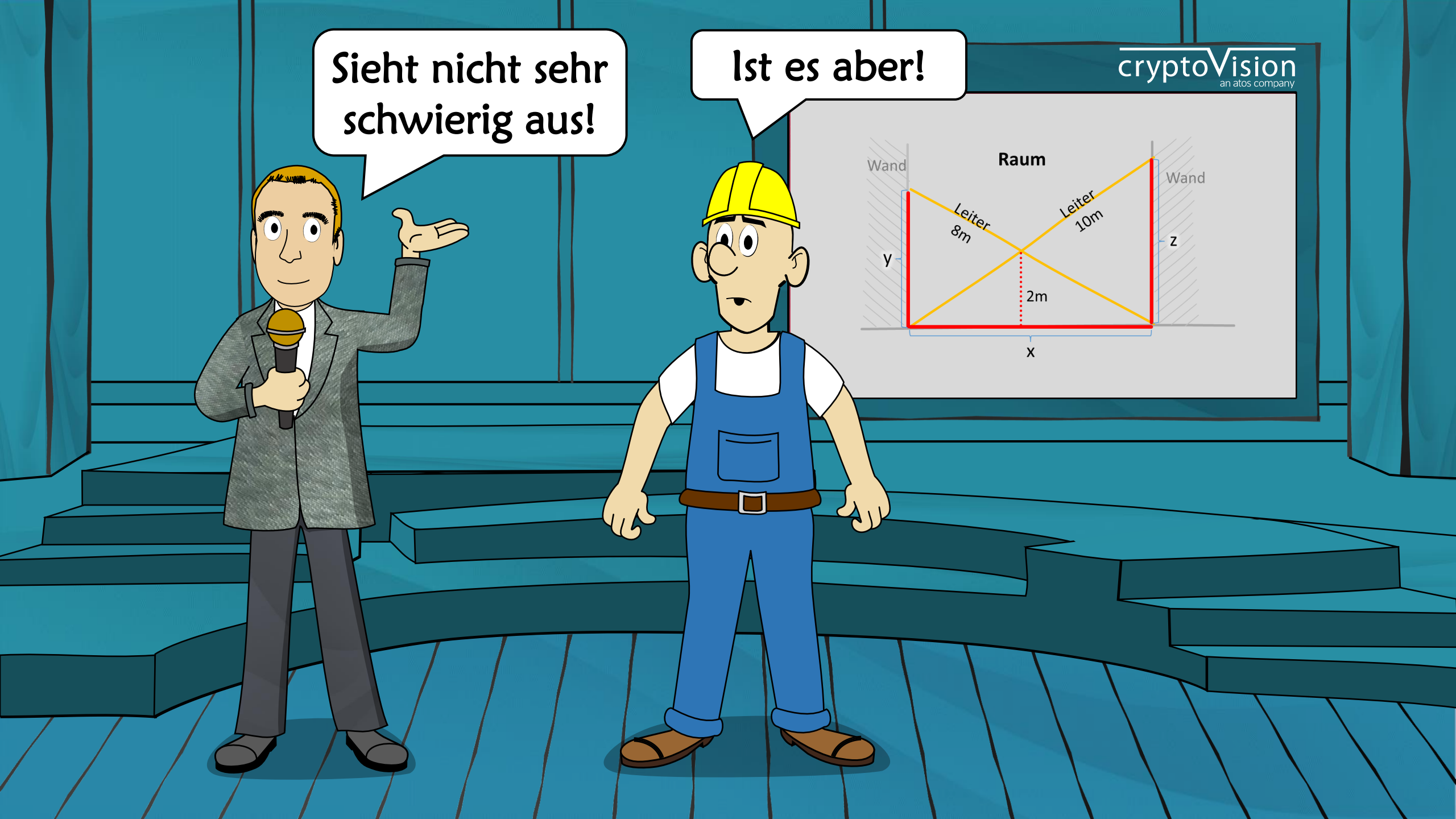

Erzählen Sie uns vom Leiterproblem!
Gerne!
cryptoVision
an atos company
Raum
Wand
Wand
Leiter 8m
Leiter 10m
y
z
2m
x

Das Leiterproblem



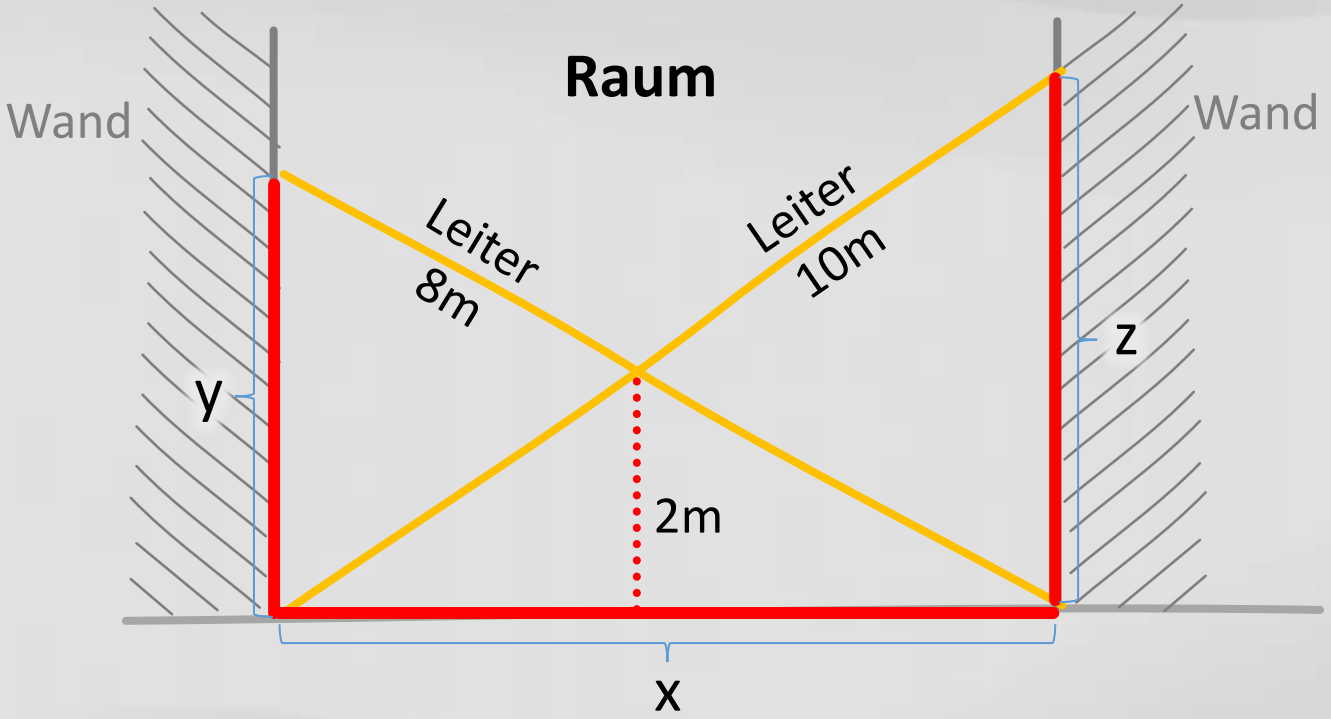
Wie breit ist der Raum?




Sieht nicht sehr schwierig aus!
Ist es aber!
cryptoVision
an atos company
Raum
Wand
Wand
Leiter
8m
Leiter
10m
y
z
2m
x

Man benötigt ein Gleichungssystem.

Ist schwer zu lösen.

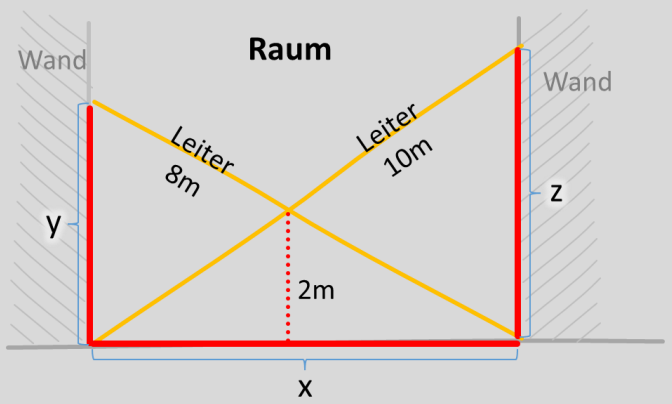


$$x^2+y^2=64$$

$$x^2+z^2=100$$

$$xy=16$$

Was hat das mit digitalen Signaturen zu tun?

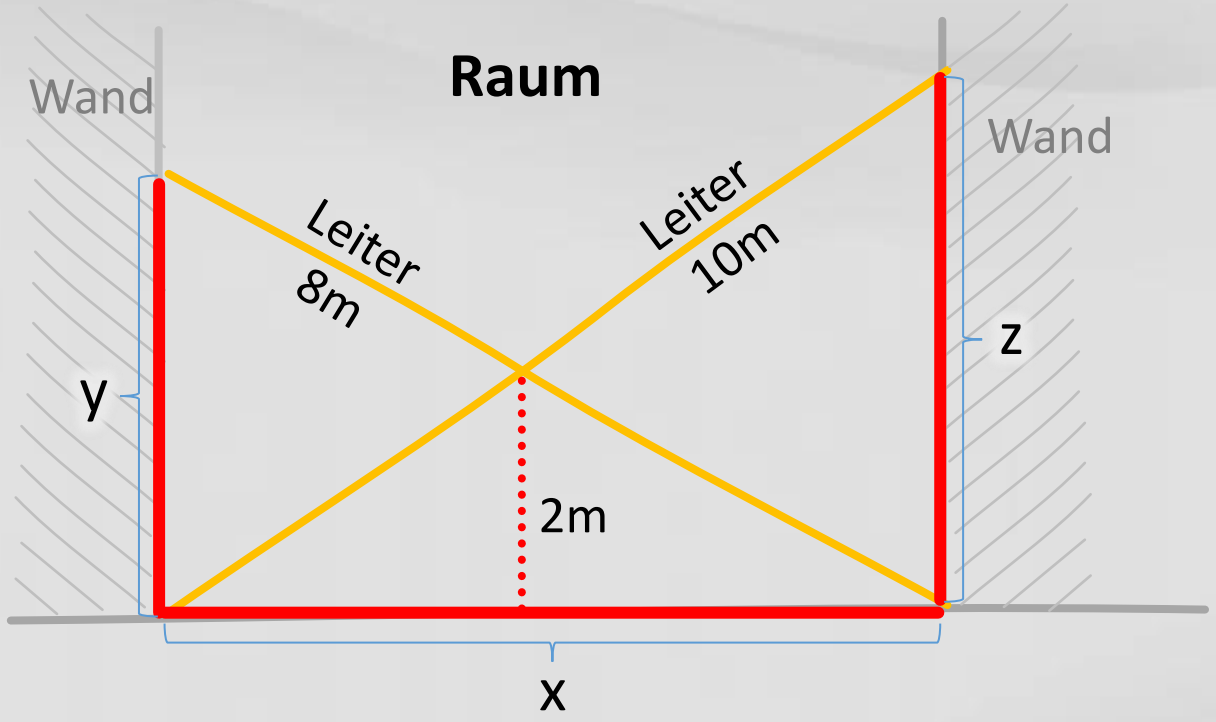


Ich zeig‘s Ihnen!

cryptoVision
an atos company

Das ist die zu signierende Nachricht.

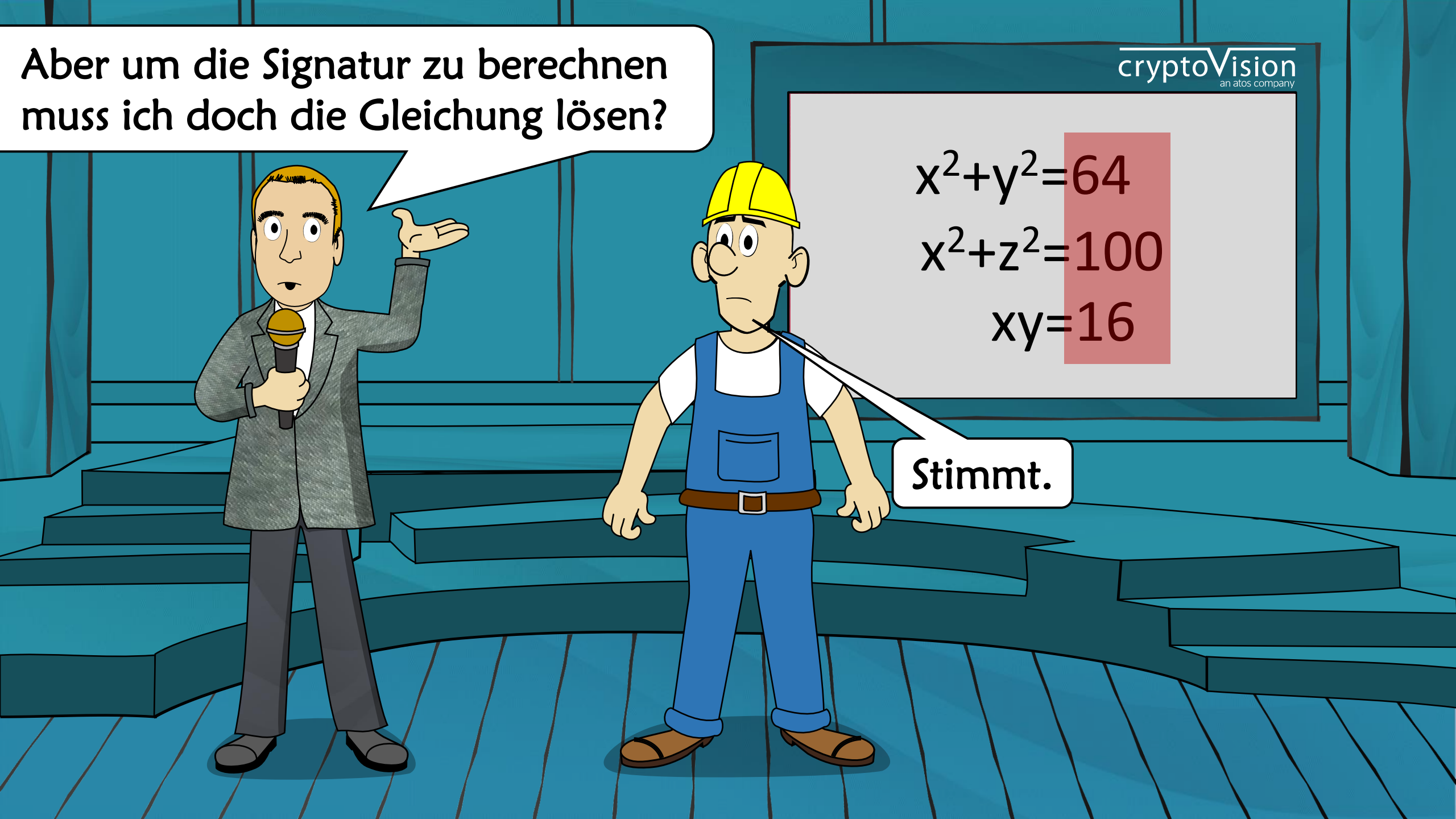
x, y und z bilden die Signatur.

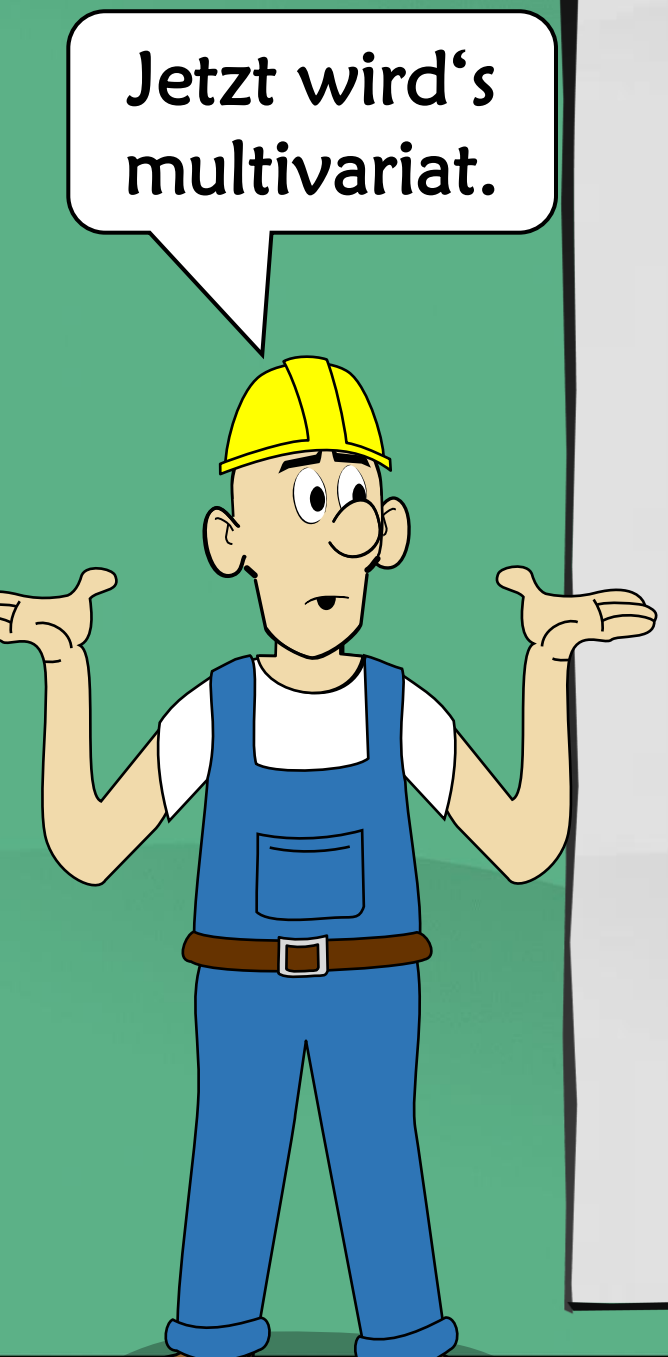


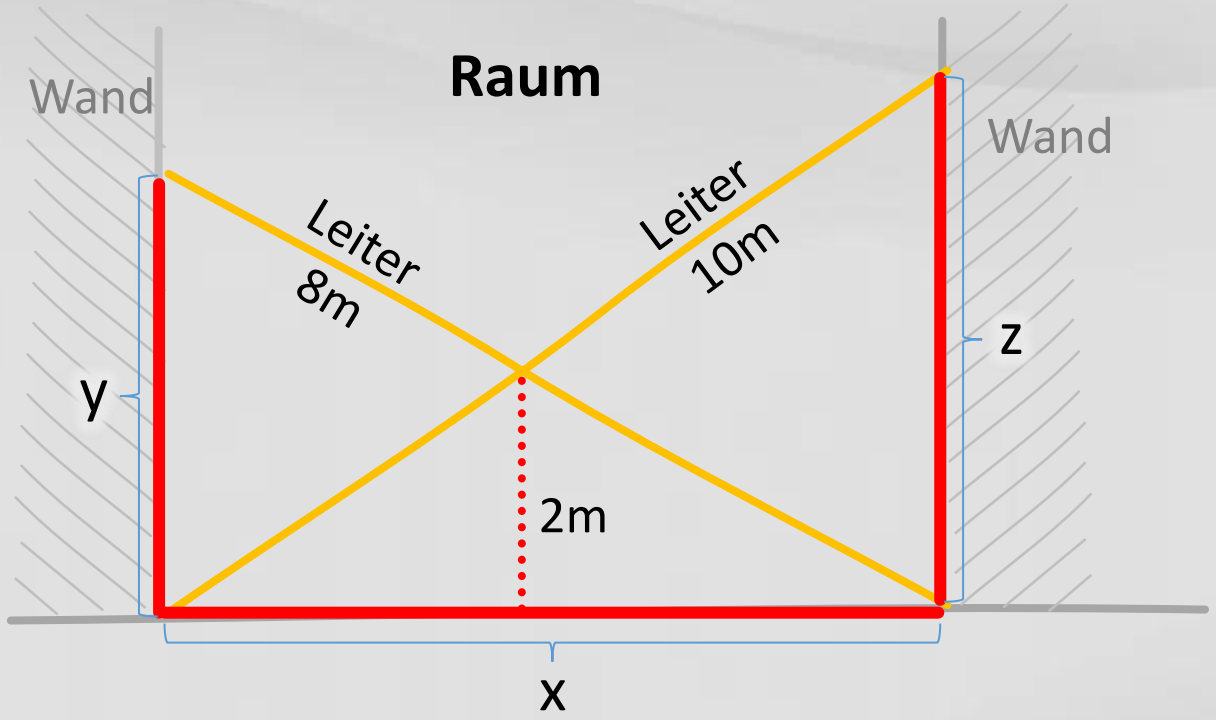
$$x^2+y^2=64$$

$$x^2+z^2=100$$

$$xy=16$$


Aber um die Signatur zu berechnen muss ich doch die Gleichung lösen?
cryptoVision
an atos company
$x^2+y^2=64$
$x^2+z^2=100$
$xy=16$
Stimmt.





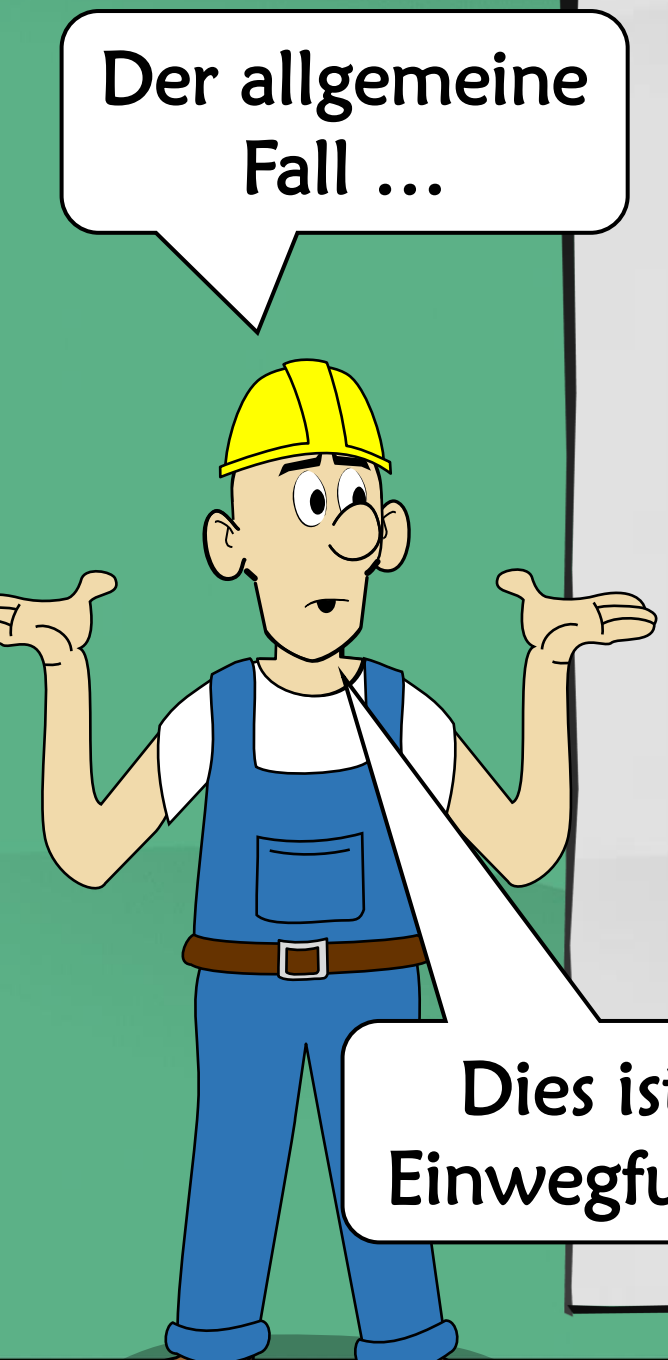
Multivariate Polynome

$x^2+y^2=64$

$x^2+z^2=100$

$xy=16$

Multivariates Gleichungssystem



Allgemeiner Fall eines multivariaten Gleichungssystems

$$2x^2 + 3y^2 + 5z^2 + 6xy + 4xz + 3yz + 5x + 8y + 3z + 7 = 44 \pmod{13}$$
$$3x^2 + 7y^2 + 8z^2 + 2xy + 2xz + 6yz + 7x + 4y + 8z + 3 = 34 \pmod{13}$$
$$6x^2 + 3y^2 + 3z^2 + 7xy + 3xz + 2yz + 4x + 3y + 2z + 2 = 13 \pmod{13}$$

Einfach zu generieren

Schwer zu lösen

Nicht ganz allgemeiner Fall eines multivariaten Gleichungssystems

$$2x^2 + 3y^2 + 5z^2 + 6xy + 4xz + 3yz + 5x + 8y + 3z + 7 = 44 \pmod{13}$$

$$3x^2 + 7y^2 + 8z^2 + 2xy + 2xz + 6yz + 7x + 4y + 8z + 3 = 34 \pmod{13}$$

$$6x^2 + 3y^2 + 3z^2 + 7xy + 3xz + 2yz + 4x + 3y + 2z + 2 = 13 \pmod{13}$$

Essigvariable

z

Ölvariablen

x,y

„Gutes“ Gleichungssystem

$$2x^2 + 3y^2 + 5z^2 + 6xy + 4xz + 3yz + 5x + 8y + 3z + 7 = 44 \pmod{13}$$
$$3x^2 + 7y^2 + 8z^2 + 2xy + 2xz + 6yz + 7x + 4y + 8z + 3 = 34 \pmod{13}$$
$$6x^2 + 3y^2 + 3z^2 + 7xy + 3xz + 2yz + 4x + 3y + 2z + 2 = 13 \pmod{13}$$

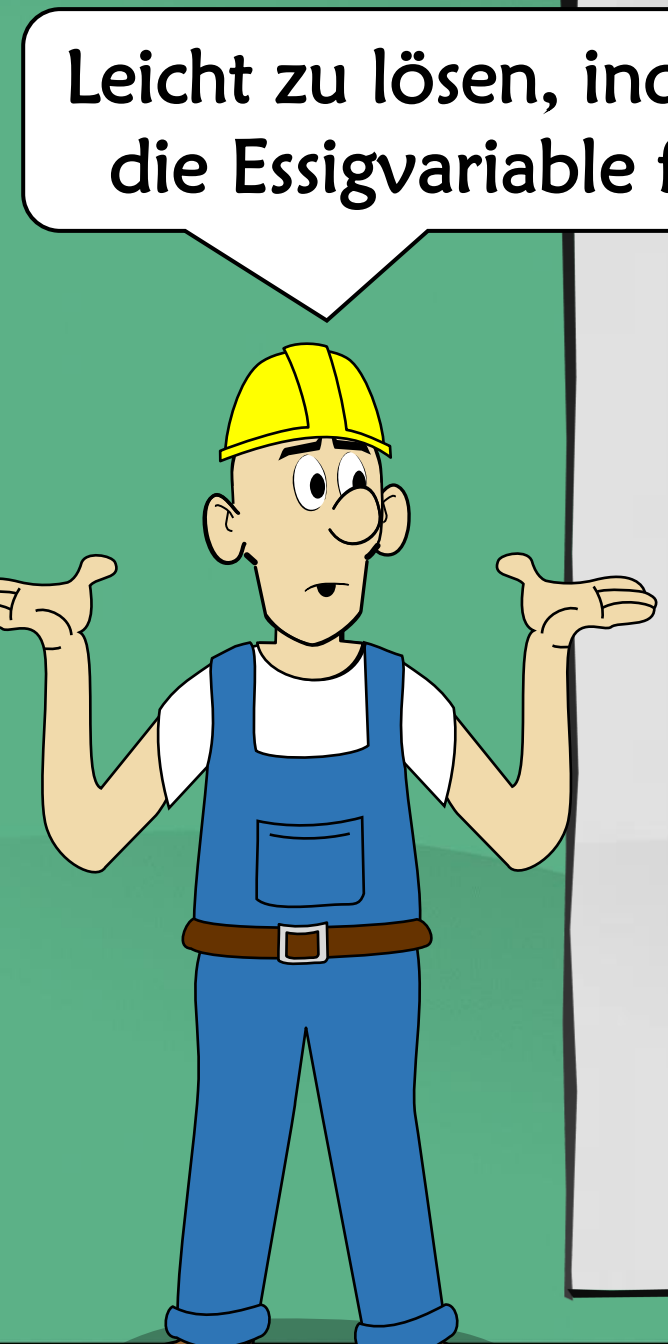
Essigvariable

z

Ölvariablen

x,y

Ölvariablen werden nicht untereinander multipliziert.



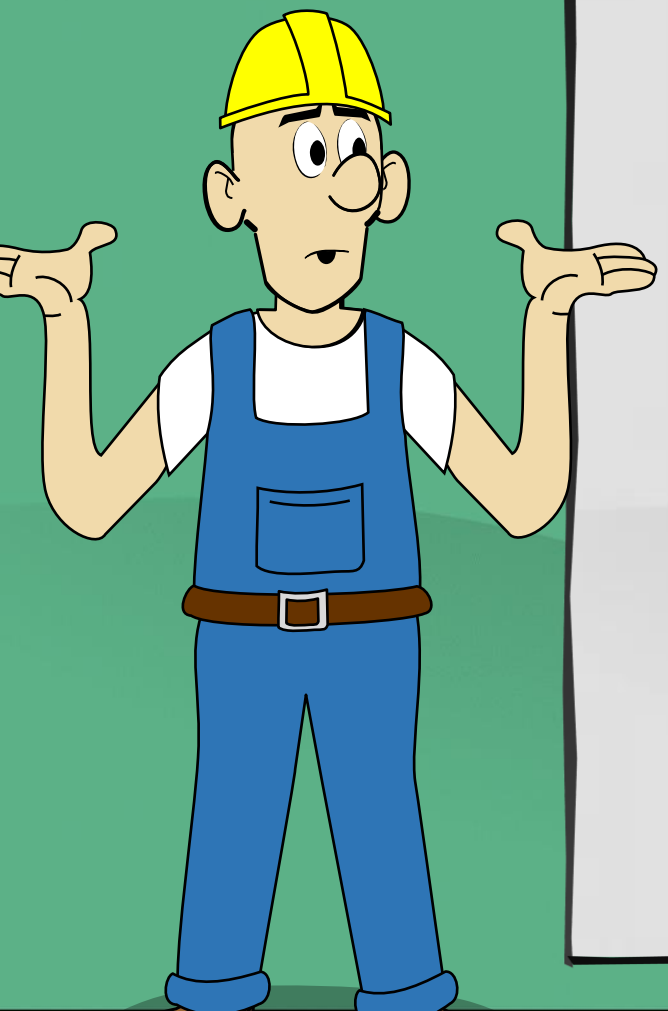
„Gutes Gleichungssystem“

$$5z^2 + 4xz + 3yz + 5x + 8y + 3z + 7 = 44 \pmod{13}$$
$$8z^2 + 2xz + 6yz + 7x + 4y + 8z + 3 = 34 \pmod{13}$$
$$3z^2 + 3xz + 2yz + 4x + 3y + 2z + 2 = 13 \pmod{13}$$

Sei z=1

$$5 + 4x + 3y + 5x + 8y + 3 + 7 = 44 \pmod{13}$$
$$8 + 2x + 6y + 7x + 4y + 8 + 3 = 34 \pmod{13}$$
$$3 + 3x + 2y + 4x + 3y + 2 + 2 = 13 \pmod{13}$$

„Gutes Gleichungssystem“

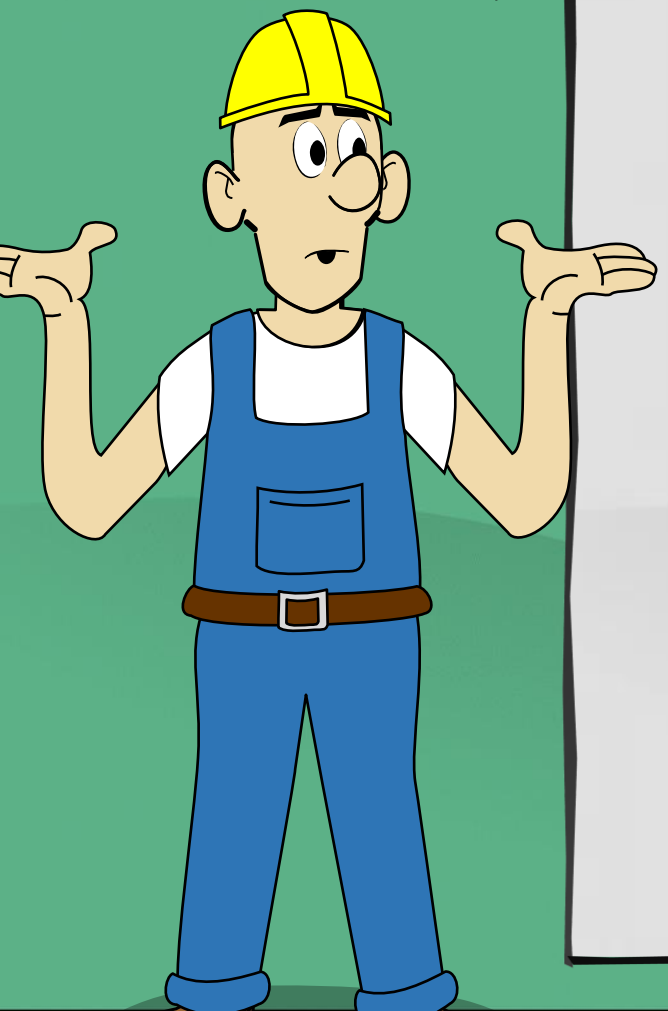


$$5z^2 + 4xz + 3yz + 5x + 8y + 3z + 7 = 44 \pmod{13}$$
$$8z^2 + 2xz + 6yz + 7x + 4y + 8z + 3 = 34 \pmod{13}$$
$$3z^2 + 3xz + 2yz + 4x + 3y + 2z + 2 = 13 \pmod{13}$$

Sei z=1

$$9x + 11y = 29$$
$$9x + 10y = 25$$
$$7x + 5y = 6$$

Gutes Gleichungssystem lässt sich in schlechtes umwandeln.



„Gutes Gleichungssystem“

$$5z^2 + 4xz + 3yz + 5x + 8y + 3z + 7 = 44 \pmod{13}$$
$$8z^2 + 2xz + 6yz + 7x + 4y + 8z + 3 = 34 \pmod{13}$$
$$3z^2 + 3xz + 2yz + 4x + 3y + 2z + 2 = 13 \pmod{13}$$

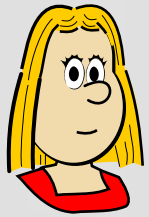
Einsetzen

$$z = x + 2$$

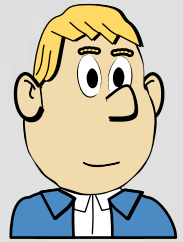
$$\Rightarrow z^2 = x^2 + 2xy + 4$$

Rainbow-Signatur

Alice



Bob



Gutes Gleichungssystem
Öffentlicher Schlüssel

$z^2 + 4xz + 3xz + 5x + 8y + 3z + 7 = ?$

$8z^2 + 2xz + 6xz + 7x + 4y + 8z + 3 = ?$

$3z^2 + 3xz + 2xz + 4x + 3y + 2z + 2 = ?$

Schlechtes Gleichungssystem
Privater Schlüssel

$x^2 + z^2 + 4xz + 3xz + 5x + 8y + 3z + 7 = ?$

$8z^2 + 2xy + 2xz + 6xz + 7x + 4y + 8z + 3 = ?$

$2z^2 + 3z^2 + 3xz + 2xz + 4x + 3y + 2z + 2 = ?$

Nachricht

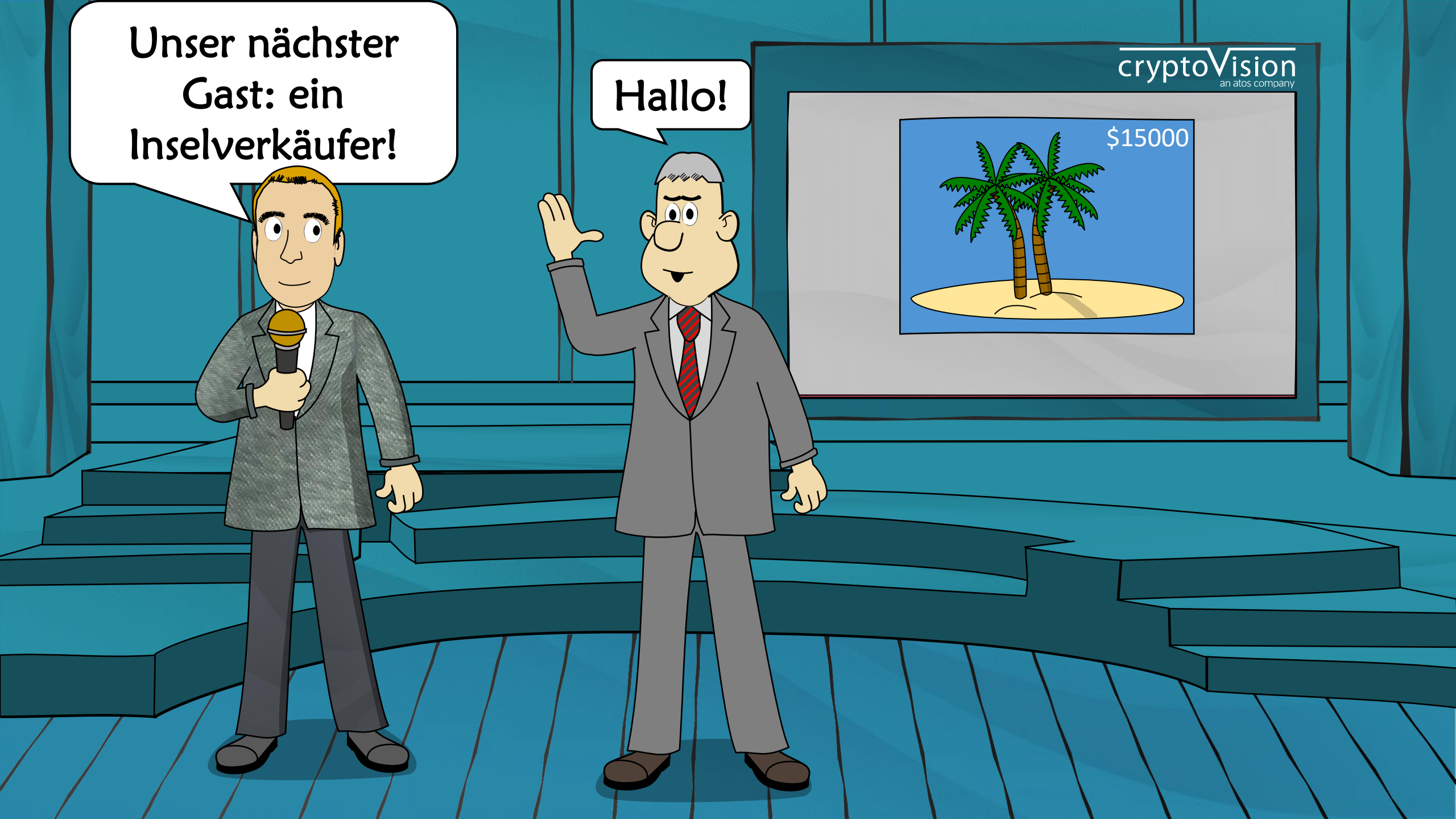
x,y,z: Signatur

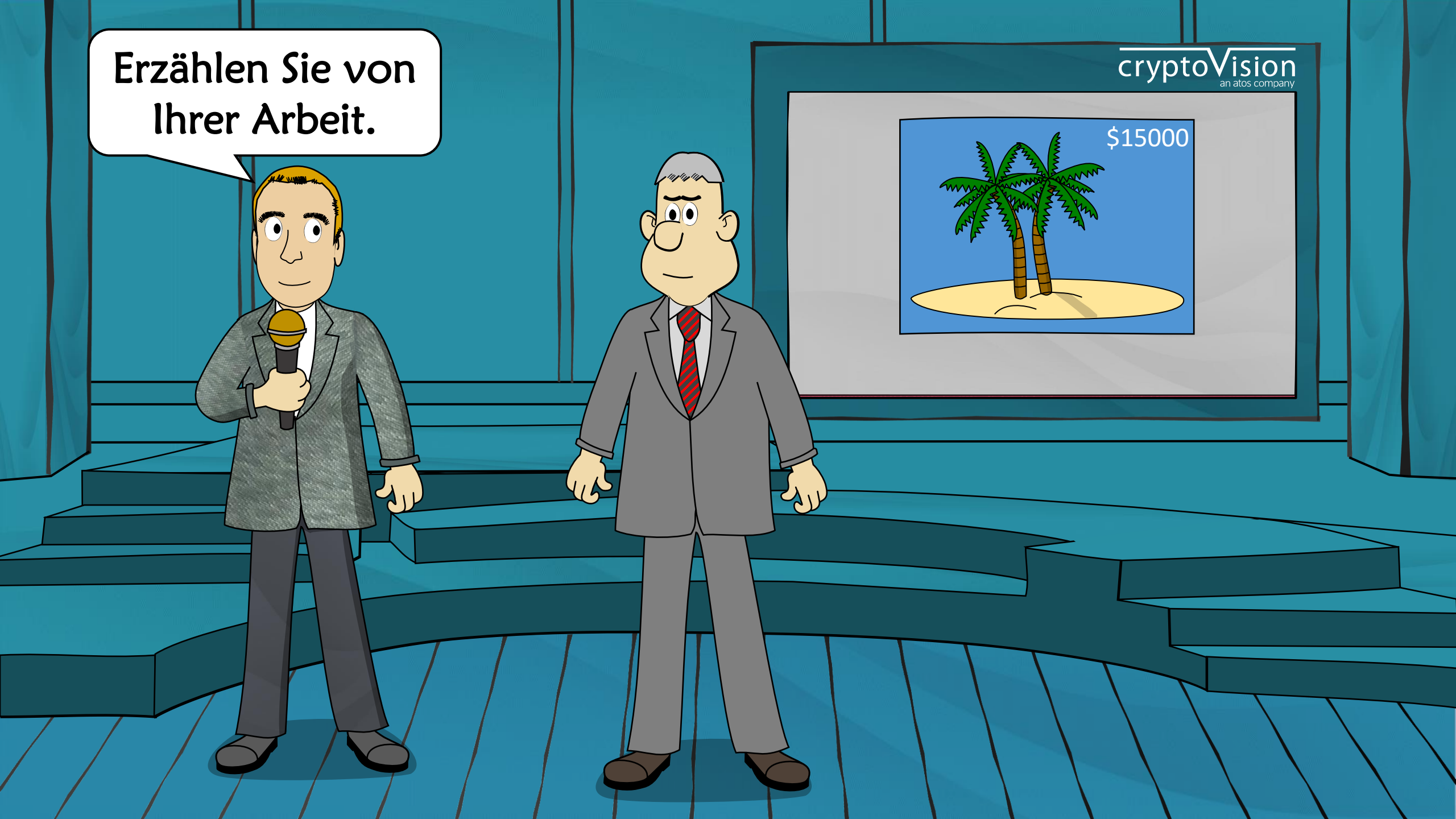
Typische Parameter

12 Variablen und Gleichungen

Länge des öffentlichen Schlüssels: 40 KB
Länge des privaten Schlüssels: : 5 KB

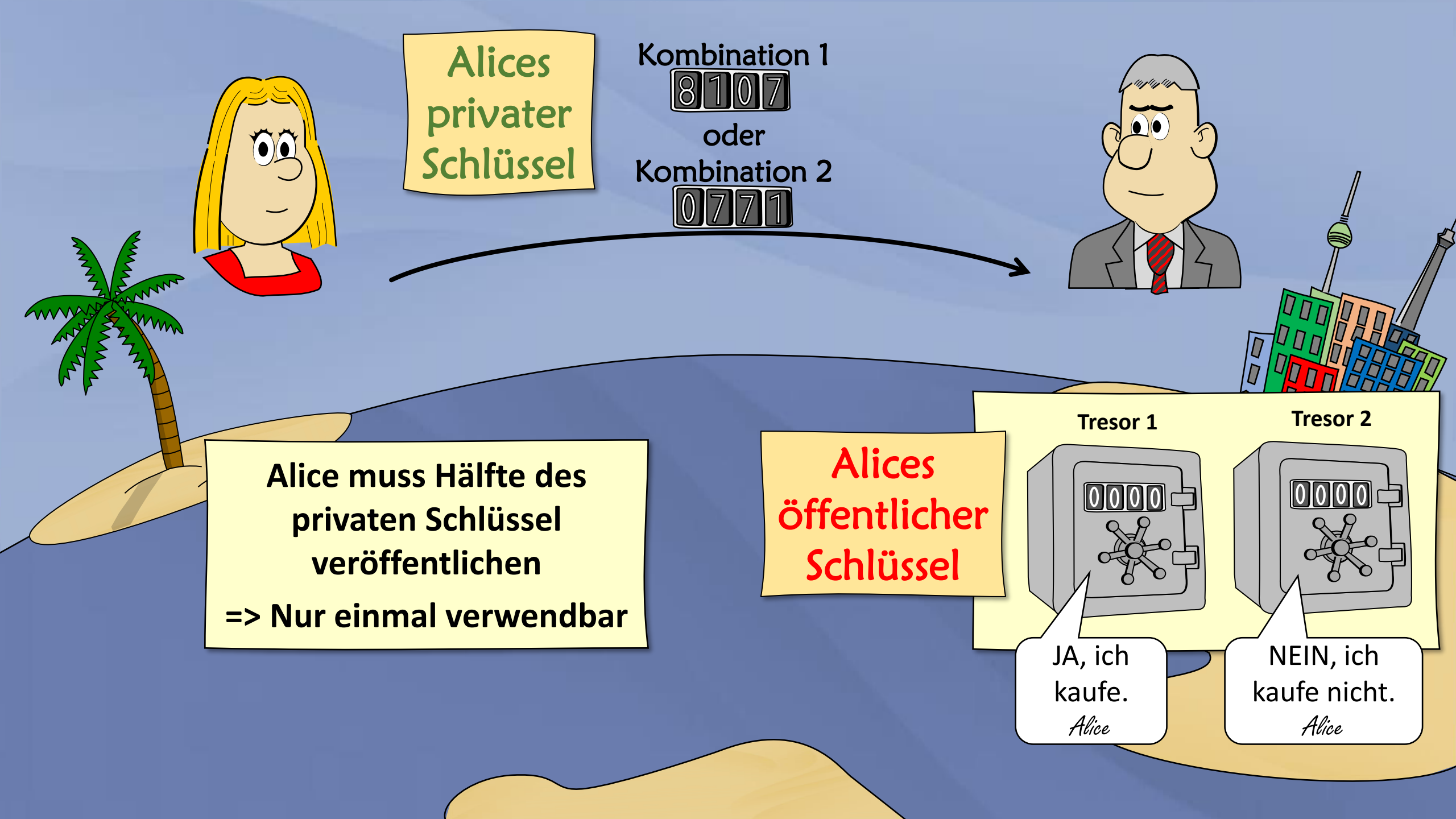

Danke, Herr Handwerker!
cryptoVision
an atos company
Wiedersehen!

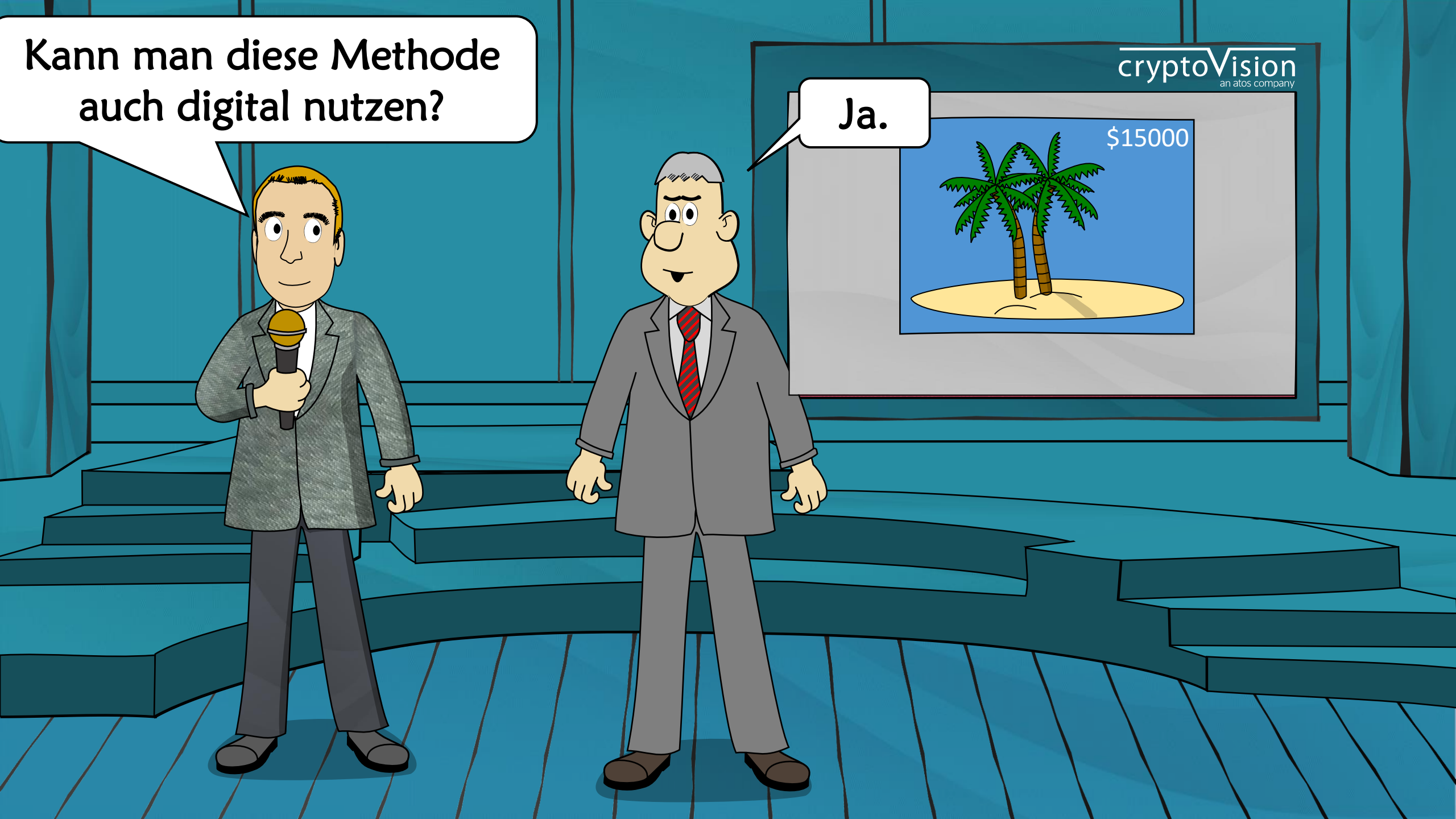

Unser nächster Gast: ein Inselverkäufer!
Hallo!
cryptoVision
an atos company
$15000


Erzählen Sie von Ihrer Arbeit.
cryptoVision
an atos company
$15000

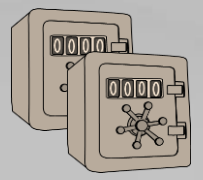

$10,000
$15,000
Wollen Sie eine Insel kaufen?
Ja, ich will sie aber erst sehen.

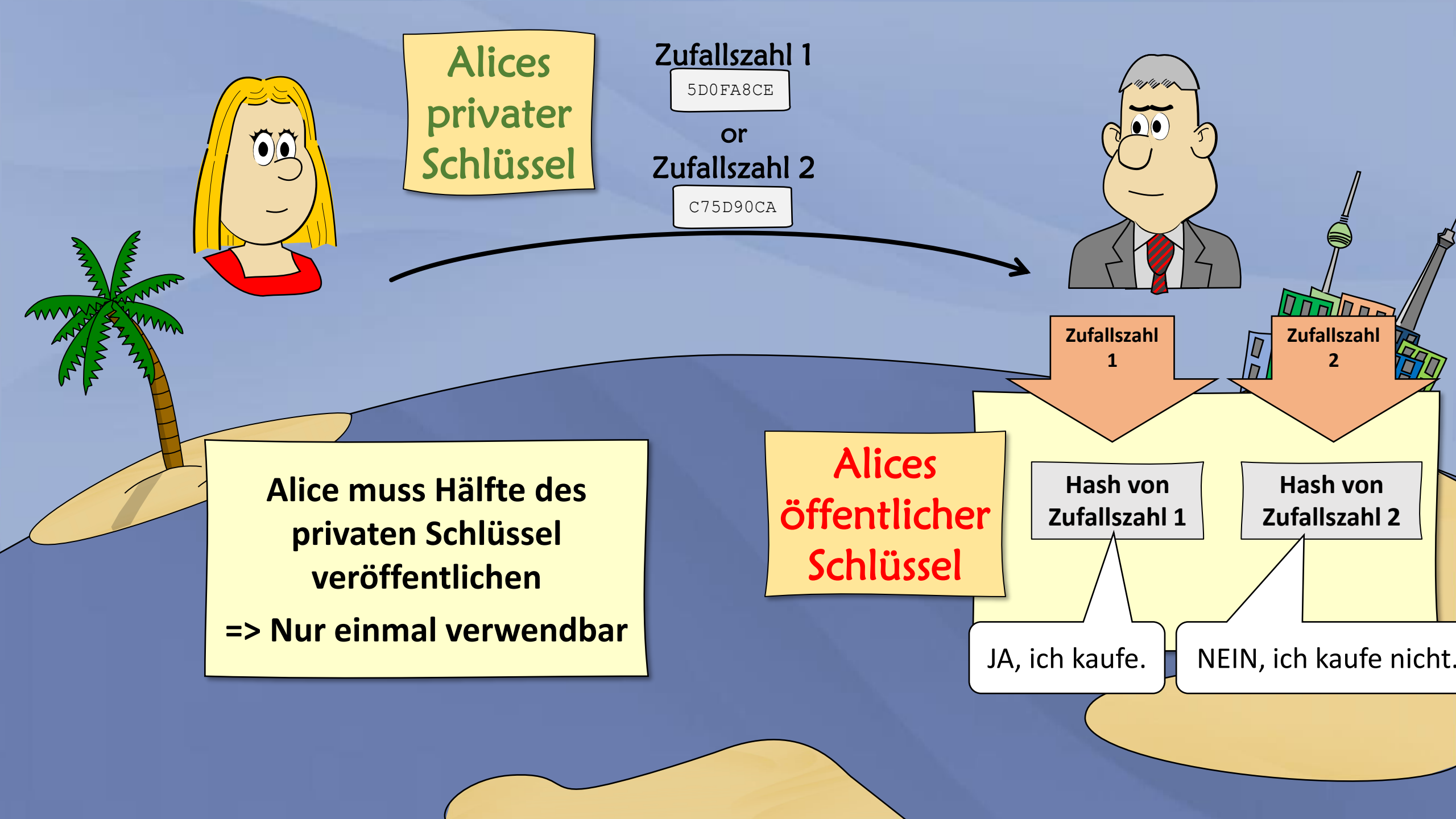

JA, ich kaufe / Nein, ich kaufe nicht
Beide können betrügen!
Alice kann JA senden und und später sagen, es war ein NEIN
Verkäufer kann sagen, es war JA, obwohl es ein NEIN war
Digitale Signatur notwendig!


Alices privater Schlüssel
Kombination 1
8107
oder
Kombination 2
0771
Alice muss Hälfte des privaten Schlüssel veröffentlichen
=> Nur einmal verwendbar
Alices öffentlicher Schlüssel
Tresor 1
Tresor 2
0000
0000
JA, ich kaufe.
Alice
NEIN, ich kaufe nicht.
Alice


Kann man diese Methode auch digital nutzen?
Ja.
$15000
cryptoVision
an atos company

Hash-basierte Signaturen

		Hash-Function (z.B. SHA-2)
Alices privater Schlüssel		Zufallszahl 1 Zufallszahl 2
Alices öffentlicher Schlüssel		Hash von Zufallszahl 1 Hash von Zufallszahl 2
Signatur	Kombination 1 oder 2	Zufallszahl 1 oder 2


Alices privater Schlüssel
Zufallszahl 1
5D0FA8CE
or
Zufallszahl 2
C75D90CA
Zufallszahl 1
Zufallszahl 2
Alice muss Hälfte des privaten Schlüssel veröffentlichen
=> Nur einmal verwendbar
Alices öffentlicher Schlüssel
Hash von Zufallszahl 1
Hash von Zufallszahl 2
JA, ich kaufe.
NEIN, ich kaufe nicht.

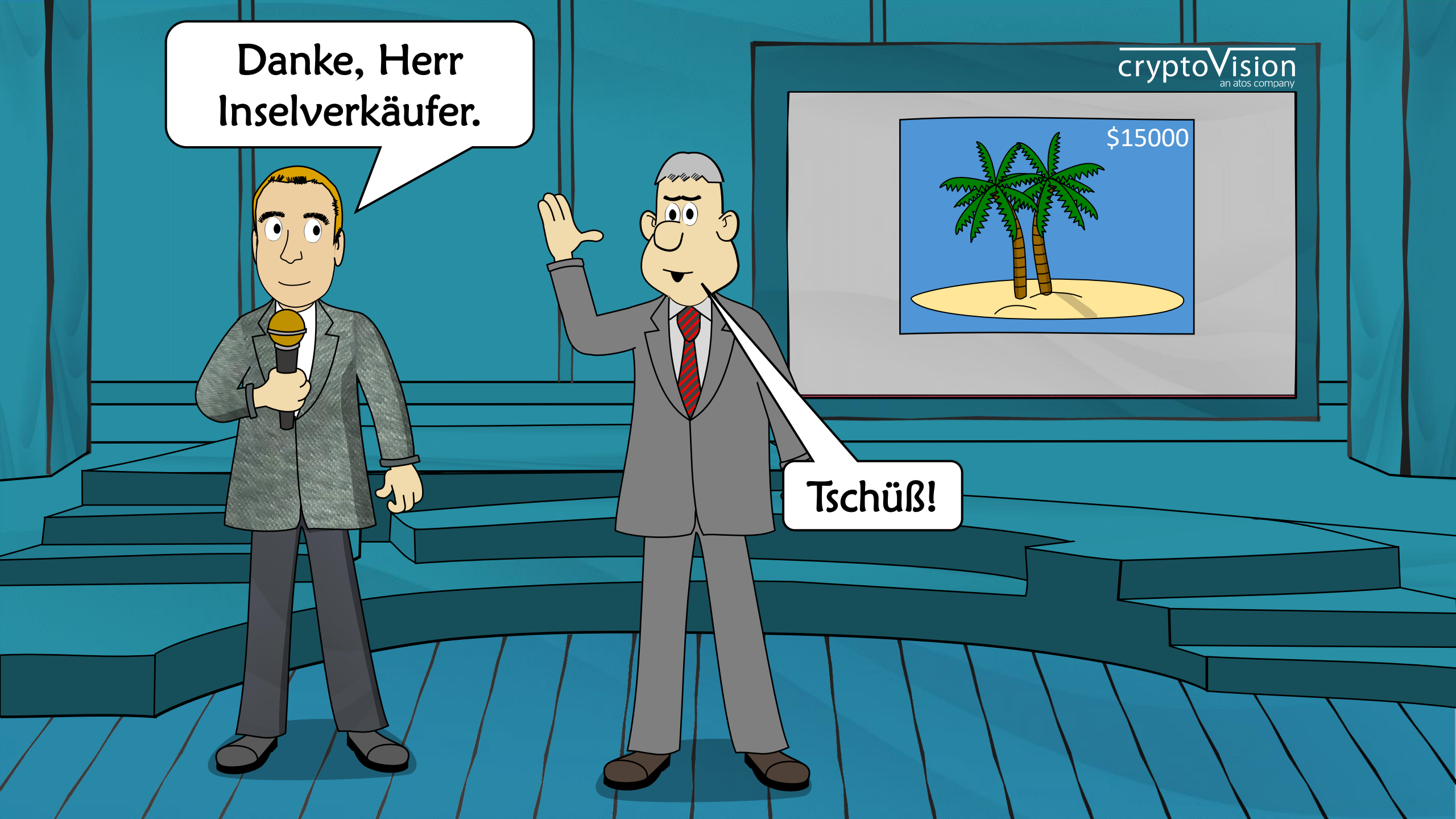

Ziemlich aufwendig für nur ein Bit.
Die Methode lässt sich verbessern.
Aber: Hash-basierte Signaturen sind immer aufwendig.
Aber sie sind beweisbar sicher.
cryptoVision
an atos company

Internet Research Task Force (IRTF)
Request for Comments: 8391
Category: Informational
ISSN: 2070-1721

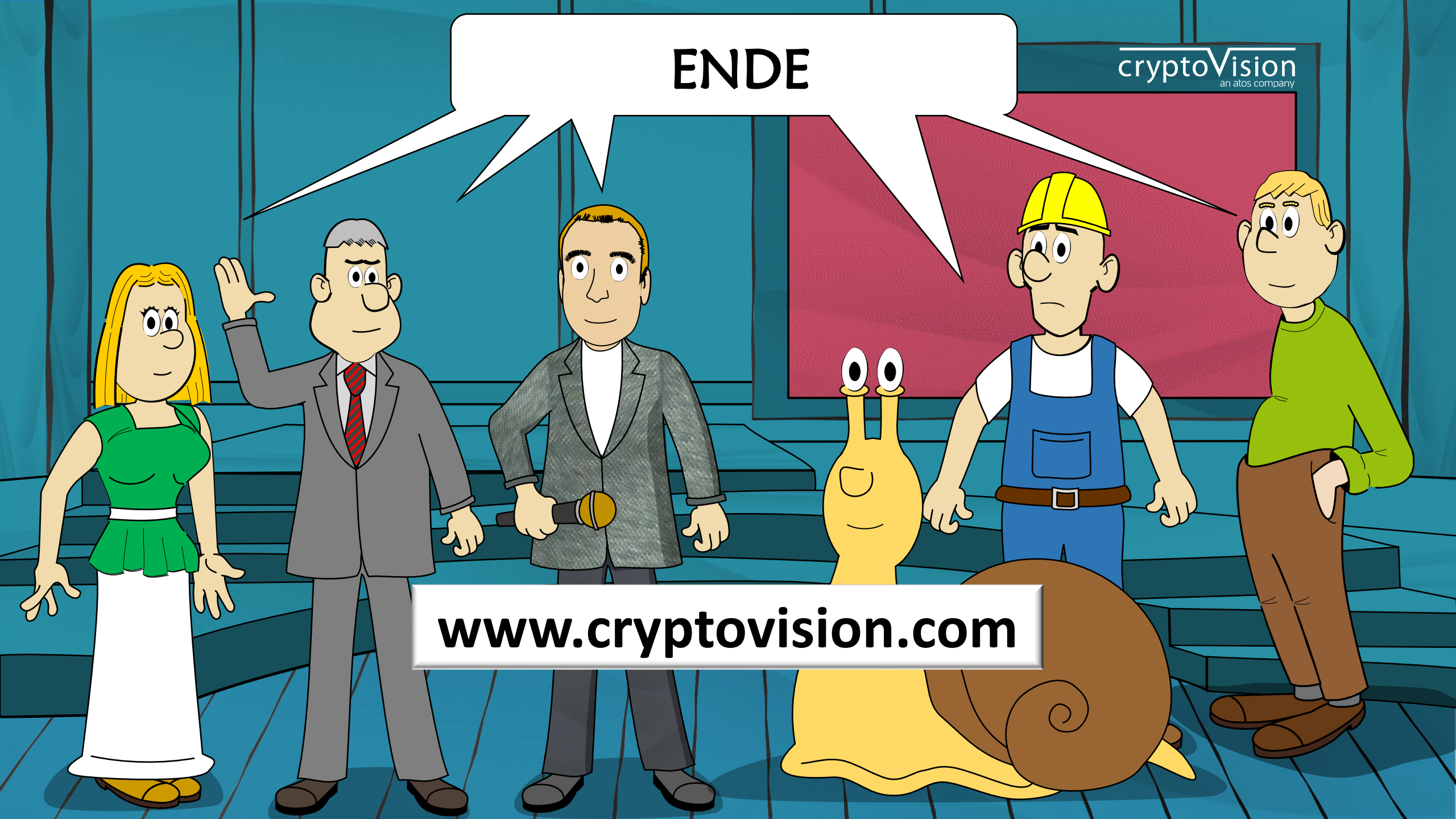
A. Huelsing
TU Eindhoven
D. Butin
TU Darmstadt
S. Gazdag
genua GmbH
J. Rijneveld
Radboud University
A. Mohaisen
University of Central Florida

May 2018

XMSS: eXtended Merkle Signature Scheme


Danke, Herr Inselverkäufer.
cryptoVision
an atos company
$15000
Tschüß!


Wenn Sie mehr wissen wollen ....
cryptoVision
an atos company
cryptoVision
Post-Quanten-Kryptografie
Vertrauliche Daten auch für die Zukunft schützen
cryptovision.com/post-quantum


ENDE
cryptoVision
an atos company
www.cryptovision.com