TeleTrusT
Pioneers in IT security.

TeleTrusT-Informationstag "Elektronische Signatur und Vertrauensdienste" 2019

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Berlin, 24.09.2019

Post-Quantum-Signaturen – anschaulich erklärt

Klaus Schmeh, cryptovision

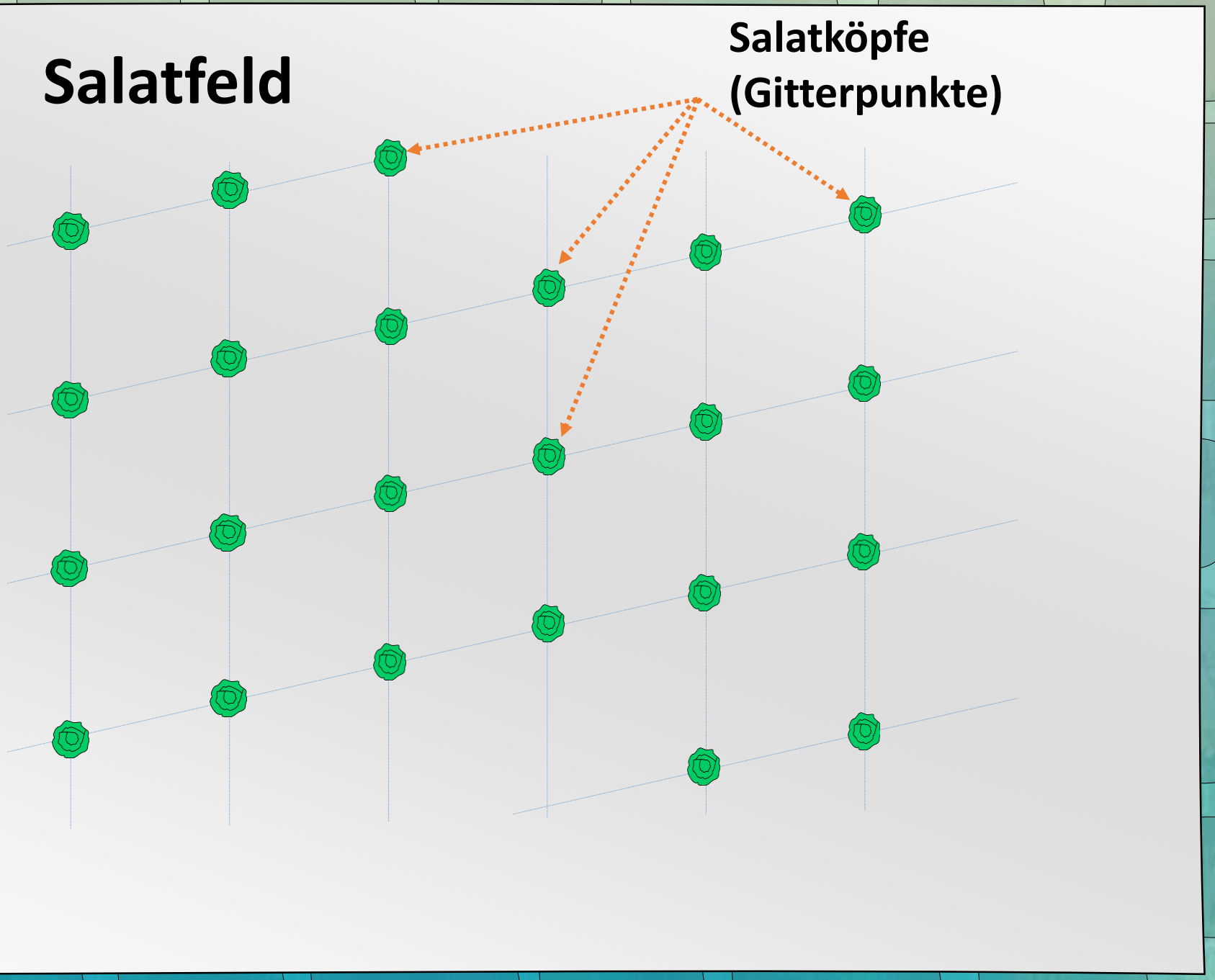

Gestatten,
Klaus Schmeh.
Berater bei
cryptovision in
Gelsenkirchen.
TeleTrusT
Pioneers in IT security.
cryptoVision

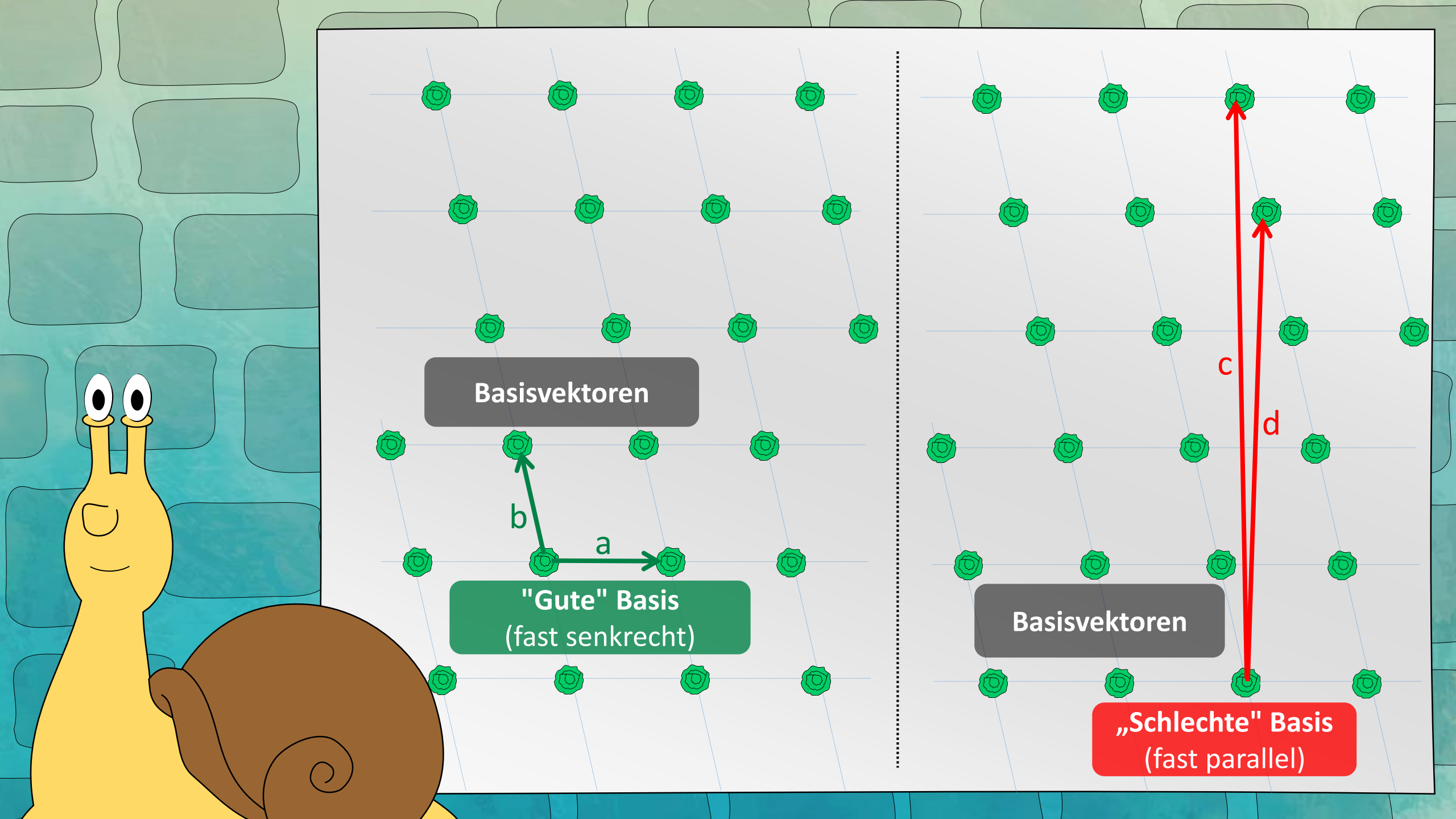

Sie haben sicherlich schon von Quantencomputern gehört.
TeleTrusT
Pioneers in IT security.
RSA und viele andere lassen sich damit knacken.
Zwei quantensichere Verfahren werde ich vorstellen.
cryptoVision


Guten Tag,
Herr Schnecke!
TeleTrusT
Pioneers in IT security.
cryptoVision

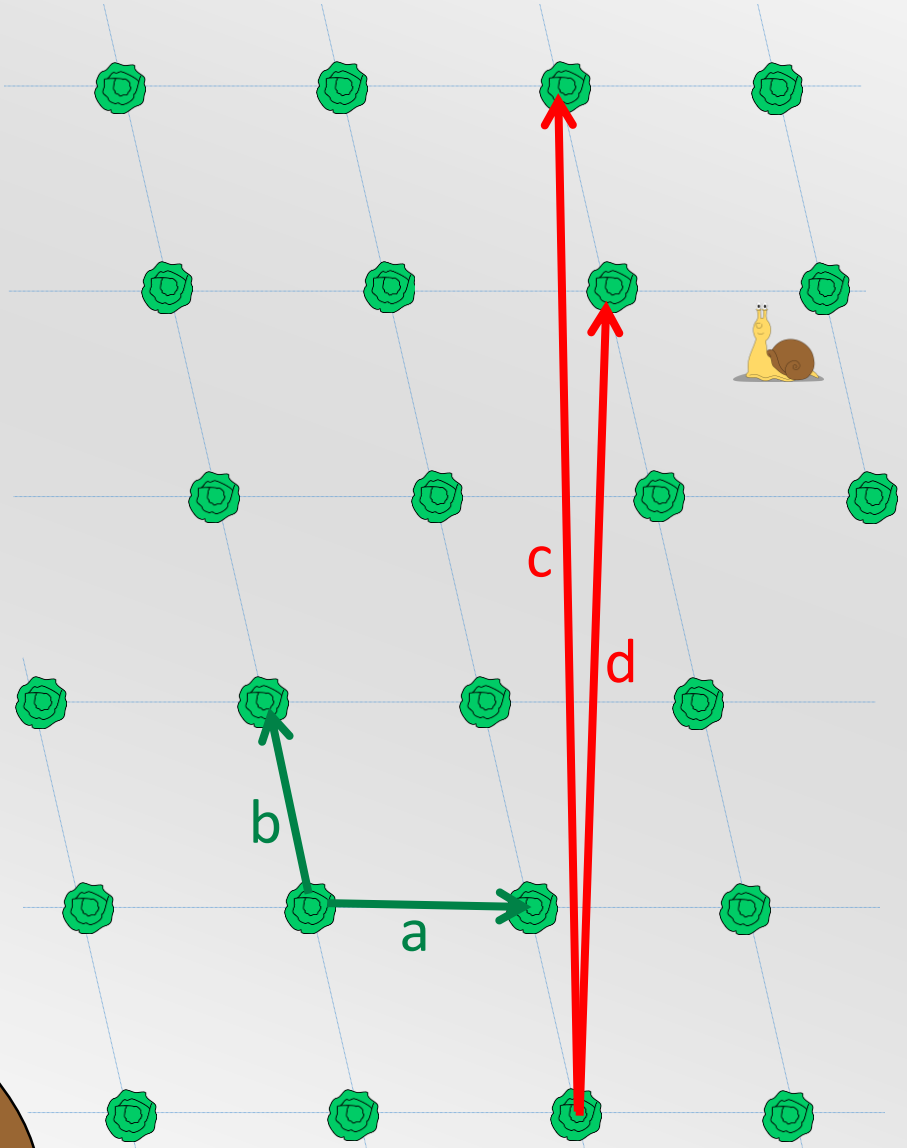

Können Sie uns Gitter-basierte Kryptografie erklären?
Gerne.
TeleTrusT
Pioneers in IT security.
cryptoVision

Salatfeld: in der Mathematik als Gitter bekannt.




Basisvektoren
b
a
"Gute" Basis
(fast senkrecht)
c
d
Basisvektoren
„Schlechte" Basis
(fast parallel)

Das Schnecke-im-Salat-Problem



Welcher Salat ist für die Schnecke der nächste?

Im Zweidimensionalen einfach zu beantworten

Aber im 250-dimensionalen?

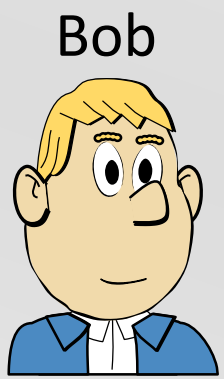
Einfach zu beantworten, wenn gute Basis bekannt

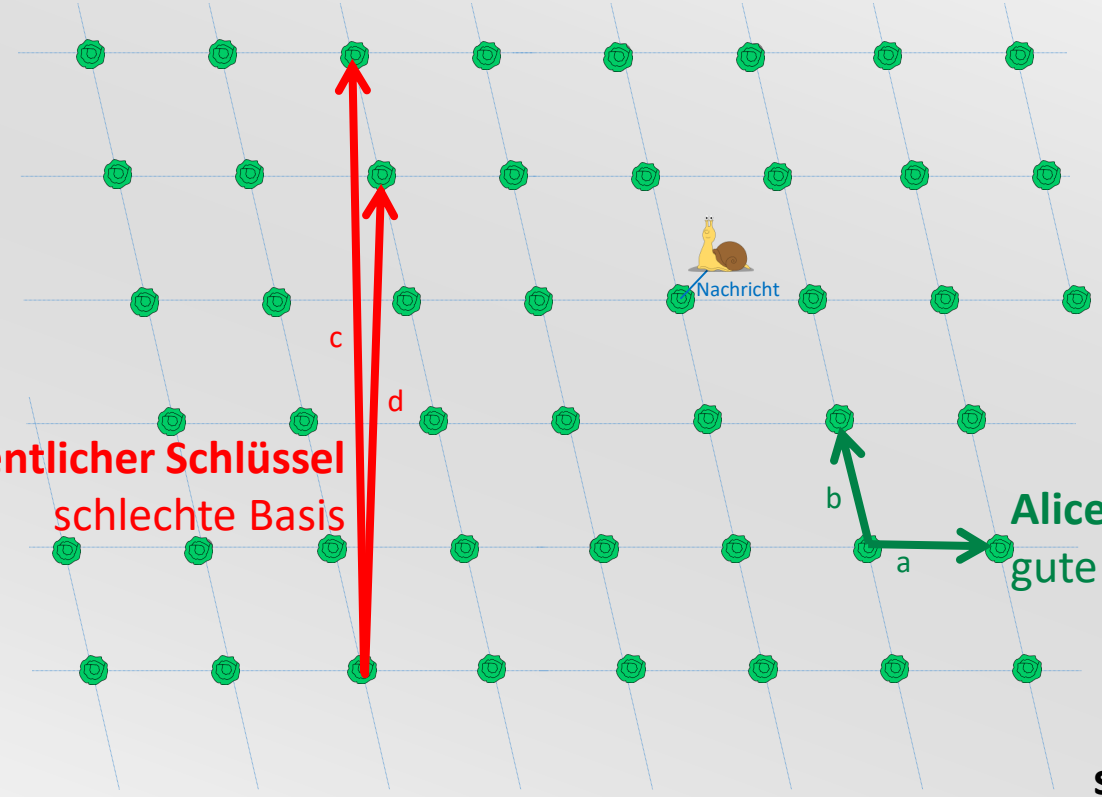
Schwer zu beantworten, wenn nur schlechte Basis bekannt

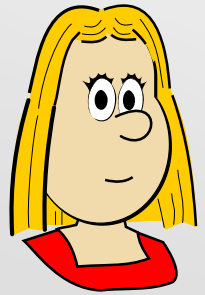
Gitter-basierte Verschlüsselung

Verschlüsselung nach Goldreich–Goldwasser–Halevi (GGH)

Bob







Alices öffentlicher Schlüssel
schlechte Basis

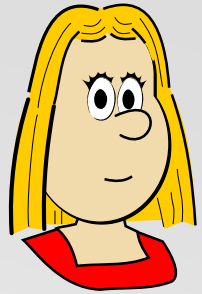
Alices privater Schlüssel
gute Basis

Alice kann entschlüsseln, weil sie gute Basis kennt

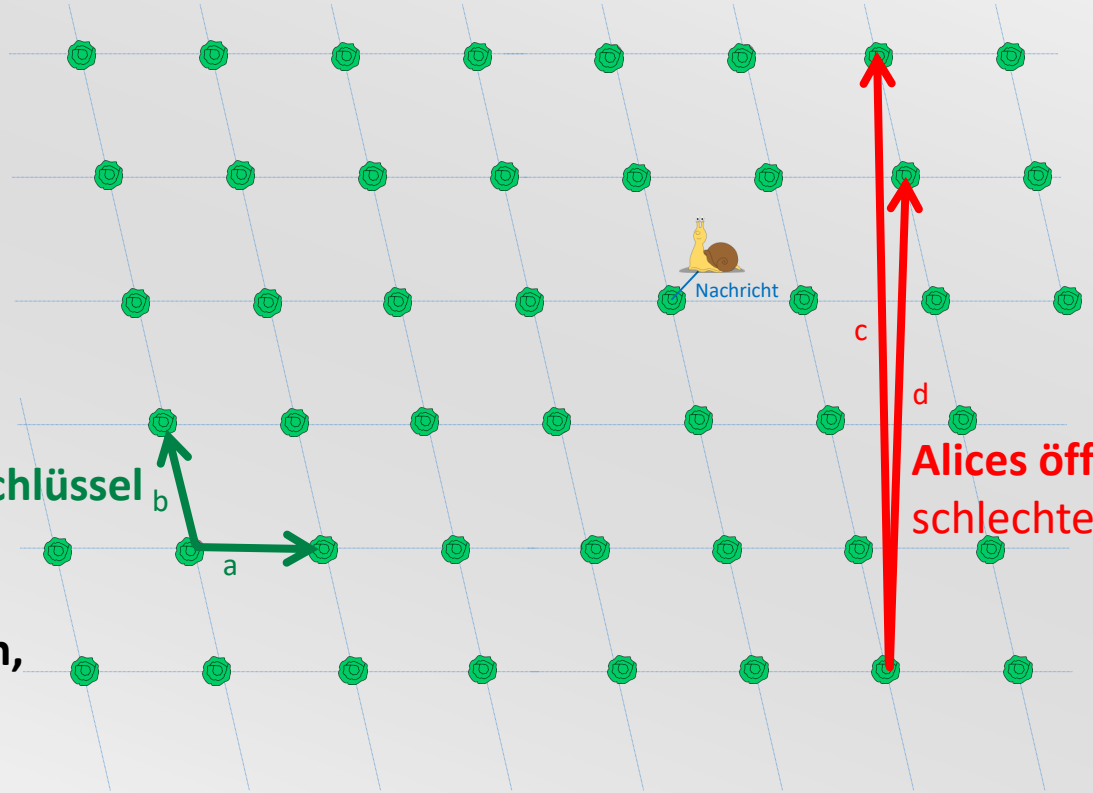
Angreifer kann nicht entschlüsseln, weil er nur schlechte Basis kennt

Gitter-basierte Signatur

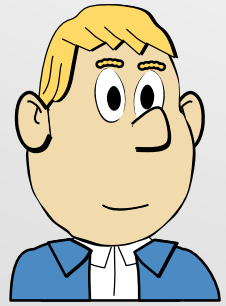
Signatur nach Goldreich–Goldwasser–Halevi (GGH)



Alices privater Schlüssel
gute Basis



Bob



Alices öffentlicher Schlüssel
schlechte Basis

Alice kann signieren, weil sie gute Basis kennt

Angreifer kann nicht signieren, weil er nur schlechte Basis kennt

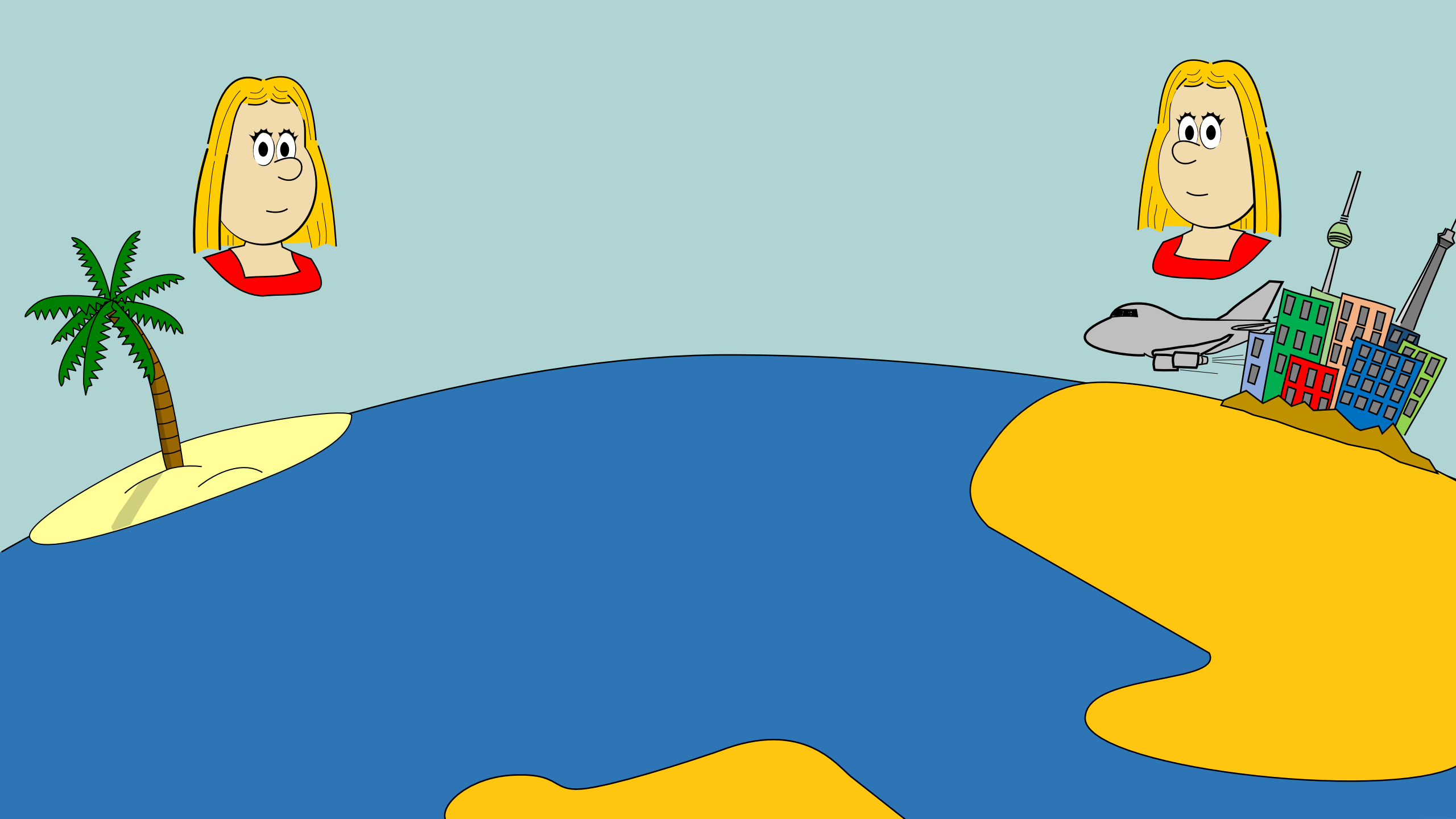

GGH wurde geknackt.
Ja, aber es gibt andere Gitter-Verfahren.
Zum Beispiel NTRU, (R)LWE, New Hope.
TrusT
Pioneers in IT security.

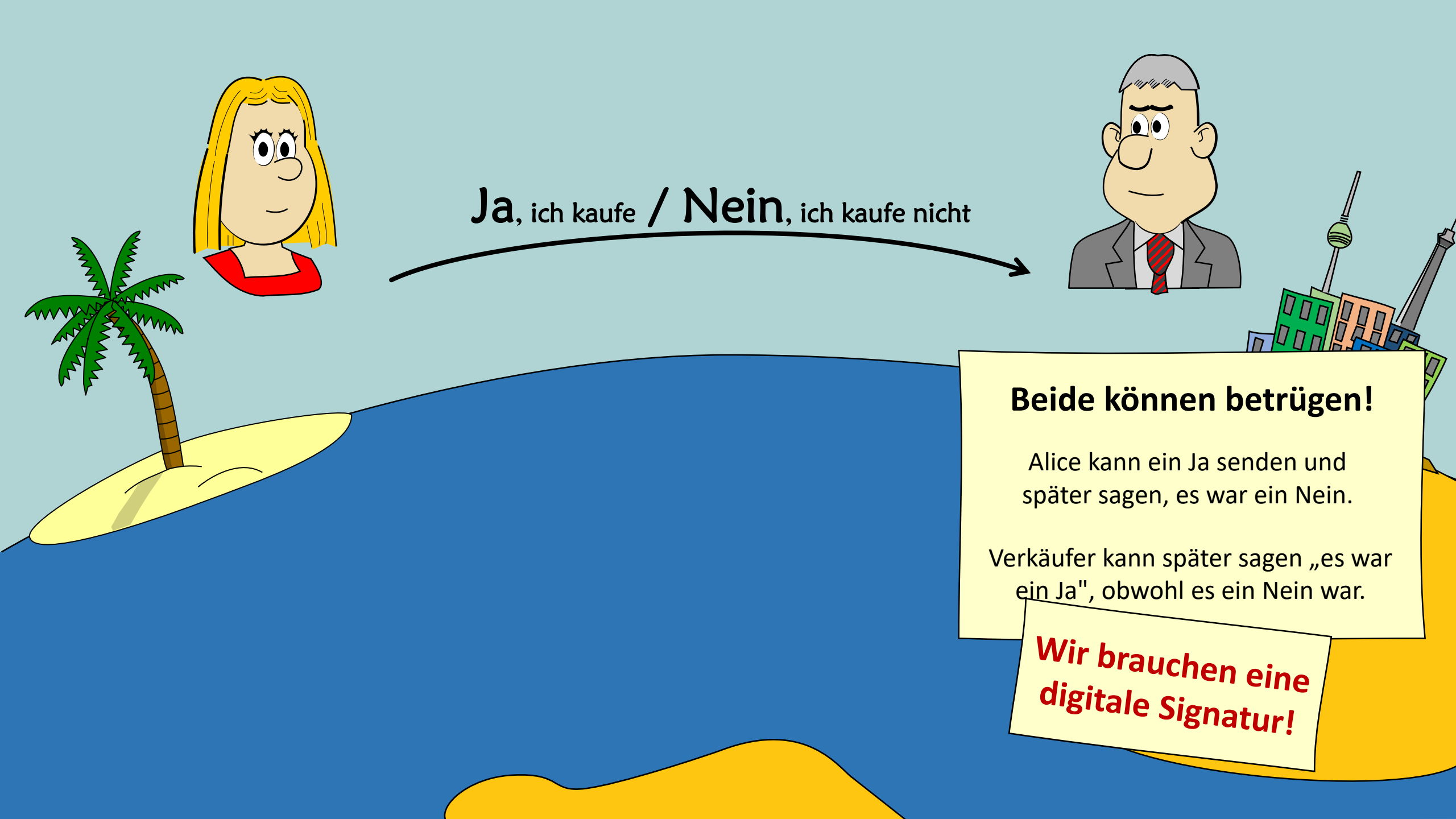

Danke Herr Schnecke!
TeleTrusT
Pioneers in IT security.
cryptoVision

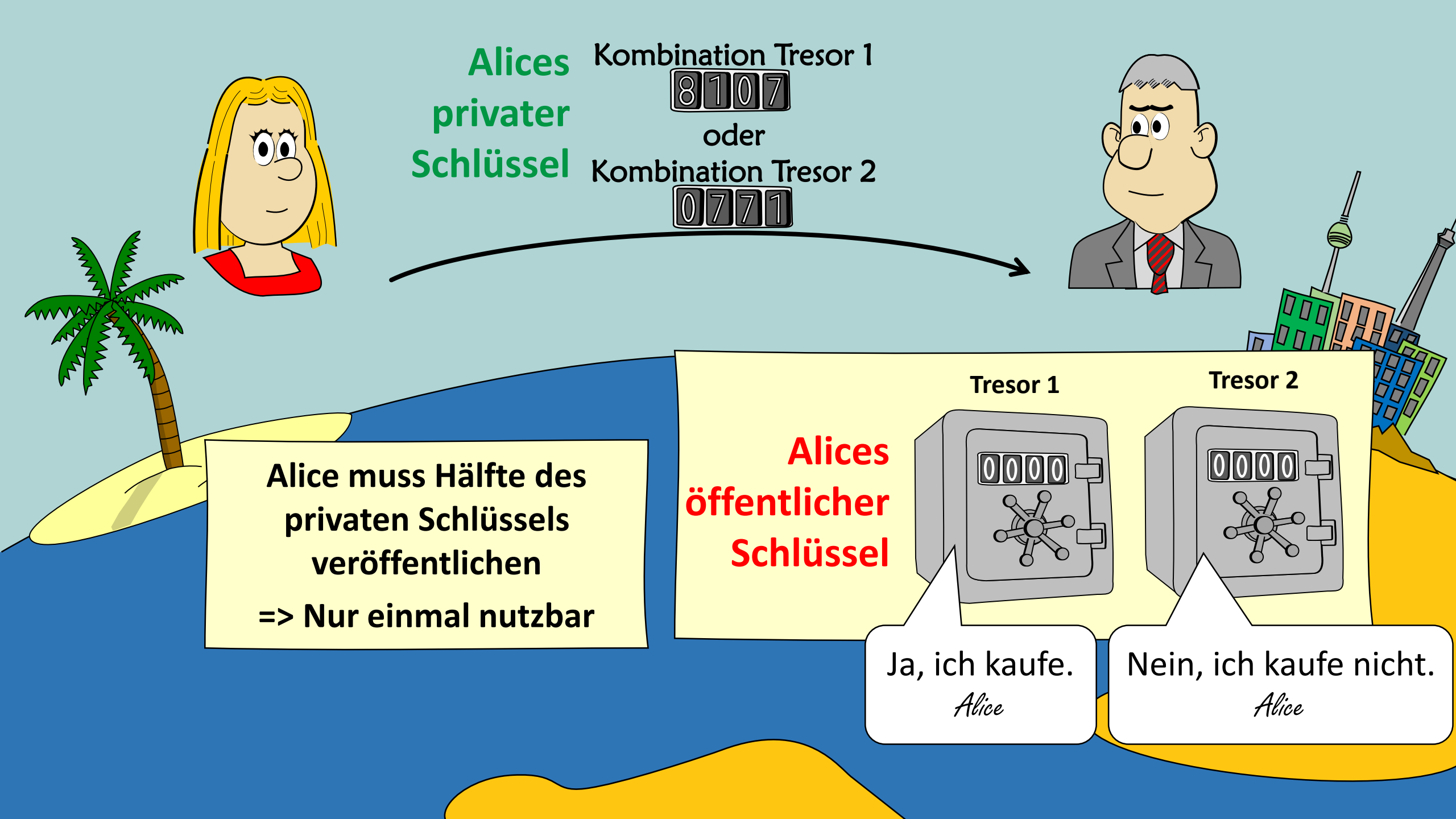

Nächster Gast: ein Inselverkäufer!
Hallo!
$15000
cryptoVision


Erzählen Sie uns von Ihrer Arbeit.
$15000
cryptoVision


$10000
$15000
Wollen Sie eine Insel kaufen?
Ja. Ich möchte sie aber erst ansehen.

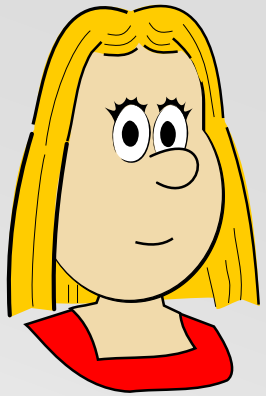



Ja, ich kaufe / Nein, ich kaufe nicht
Beide können betrügen!
Alice kann ein Ja senden und später sagen, es war ein Nein.
Verkäufer kann später sagen „es war ein Ja", obwohl es ein Nein war.
Wir brauchen eine digitale Signatur!

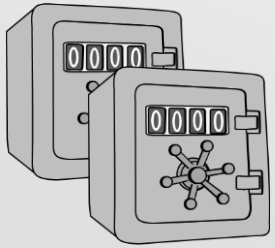

Alices privater Schlüssel
Kombination Tresor 1
8107
oder
Kombination Tresor 2
0771
Alice muss Hälfte des privaten Schlüssels veröffentlichen
=> Nur einmal nutzbar
Alices öffentlicher Schlüssel
Tresor 1
Tresor 2
0000
0000
Ja, ich kaufe.
Alice
Nein, ich kaufe nicht.
Alice

Hash-basierte Signaturen

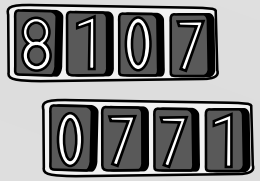
Methode lässt sich auch digital nutzen.



Schlüssel sind nur einmal nutzbar.

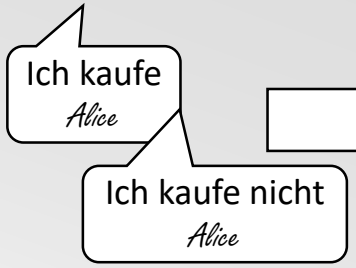


Hash-Funktion
(e.g., SHA-2)



Zufallszahl 1
Zufallszahl 2

Alices privater Schlüssel



Hashwert von Zufallszahl 1

Hashwert von Zufallszahl 2

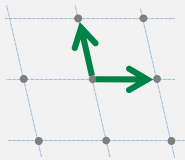
Alices öffentlicher Schlüssel

Um ein Bit zu signieren, veröffentlicht Alice Nachricht 1 oder Nachricht 2

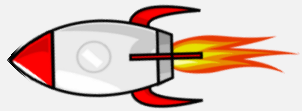

Das sieht aber aufwendig aus.
Und das alles für ein Bit
Es gibt Möglichkeiten, das Verfahren zu verbessern.
Trotzdem: lange Schlüssel, lange Signaturen, aufwendige Generierung
Vorteil: beweisbar sicher


Danke, Herr Inselverkäufer.
$15000
cryptoVision

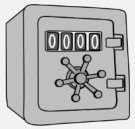
Auch andere Post-Quanten-Verfahren kann man anschaulich erklären.



Gitter-basiert

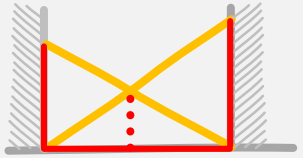


Code-basiert



Hash-basiert

Nichtkommutativ



Multivariat

Isogenie-basiert

cryptoVision

Post-Quantum-Kryptografie anschaulich erklärt

Die Schnecke im Salatfeld

Klaus Schmeh

Für Laien ist die komplexe Mathematik hinter Post-Quantum-Kryptografie kaum nachvollziehbar. Einfache Analogien können jedoch den Zugang enorm erleichtern.

Trotz aller Fortschritte in der Informationstechnik seit Pionieren wie Konrad Zuse oder Alan Turing hat sich eines nie geändert: Computer arbeiten mit Nullen und Einsen – und damit mit Speicherbausteinen, die stets den einen oder anderen Wert annehmen. Das muss aber nicht unbedingt so bleiben, denn es gibt eine Technik, die dieses Konzept verändern könnte. Sie arbeitet auch mit binären Speicherbausteinen, die jedoch im Gegensatz zu herkömmlichen Bits die Werte null und eins gleichzeitig annehmen können. Die Rede ist von sogenannten Quantencomputern.

Dabei handelt es sich um Rechner, die nach den Prinzipien der Quantenphysik arbeiten. Eine davon wird oft mit Schrödingers Katze veranschaulicht, die gleichzeitig tot und lebendig ist – so lange, bis man nachschaut. Ähnlich verhält es sich mit einem Quanten-Speicherbaustein. Ein solcher hat gleichzeitig den Wert null und eins – so lange, bis man ihn ausliest. Durch diese spezielle Eigenschaft können Quantencomputer mühelos Aufgaben lösen, für die herkömmliche Rechner astronomische Zeiträume benötigen würden. Insbesondere für das Knacken asymmetrischer Kryptoverfahren wären Quantencomputer äußerst nützlich. Praktisch alle eingesetzten Algorithmen dieser Art – inklusive

iX-TRACT

- Asymmetrische und gegenüber Quantencomputern nicht anfällige Kryptomethoden (Post-Quanten-Verfahren) sind mathematisch anspruchsvoll.
- Mithilfe einiger Analogien und Vereinfachungen können auch Nichtmathematiker Post-Quanten-Verfahren

iX Spezial 2019


Auf Wiedersehen!
TeleTrusT
Pioneers in IT security.
cryptoVision
www.cryptovision.com