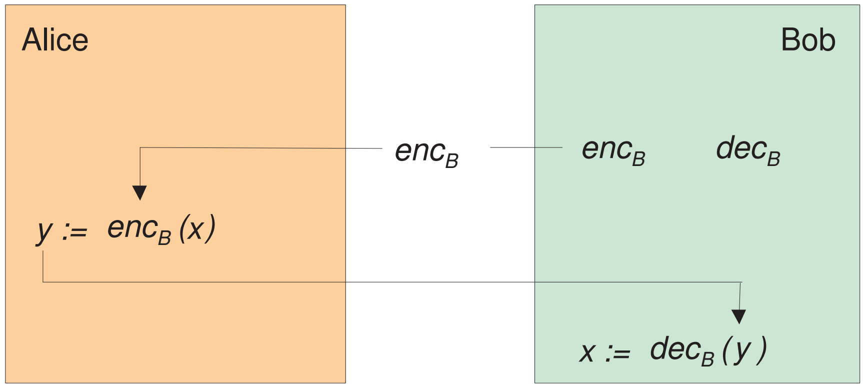
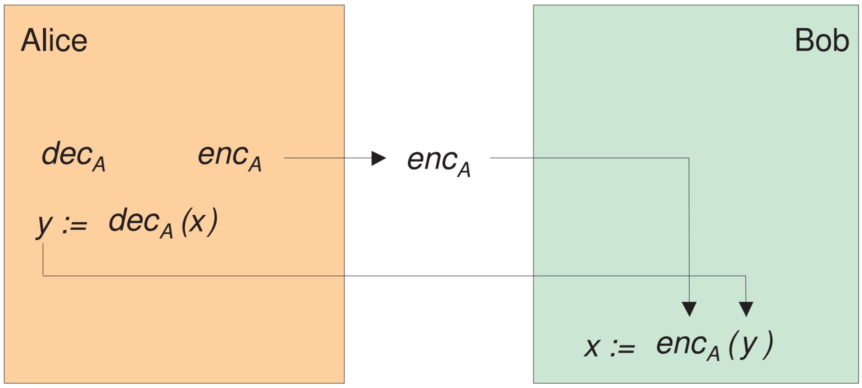
Bezahlen im Internet:
ecash + Geldkarte

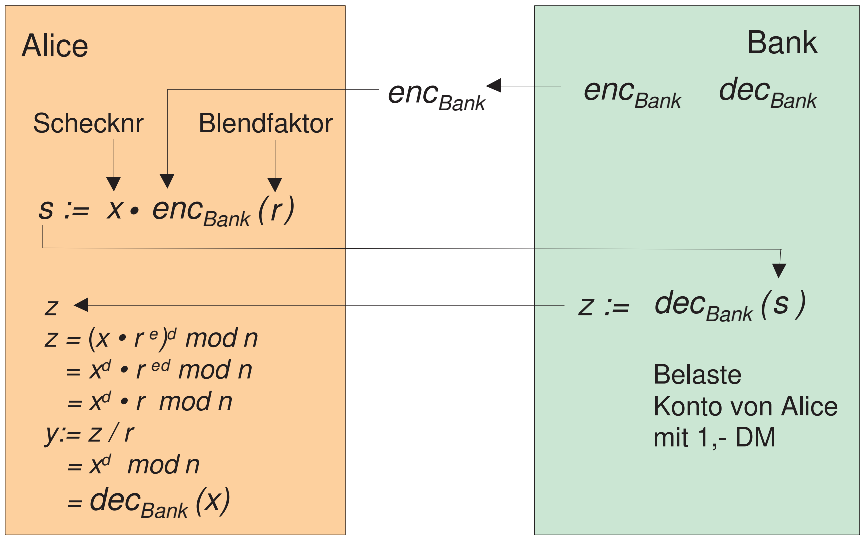
Oliver Vornberger
Fachbereich Mathematik/Informatik, Universität Osnabrück



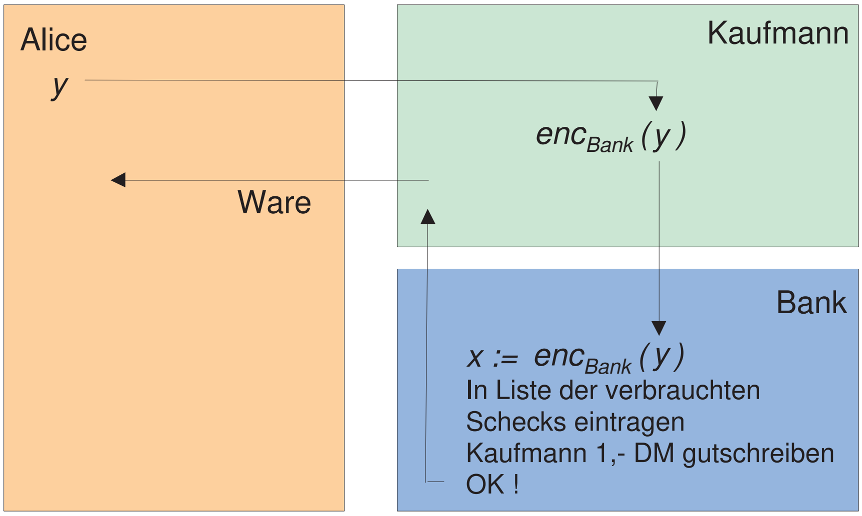
Nachricht verschlüsseln



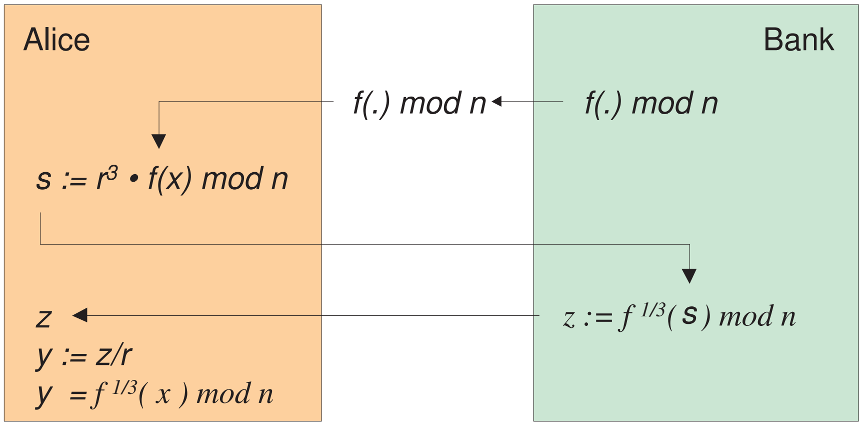
Nachricht signieren



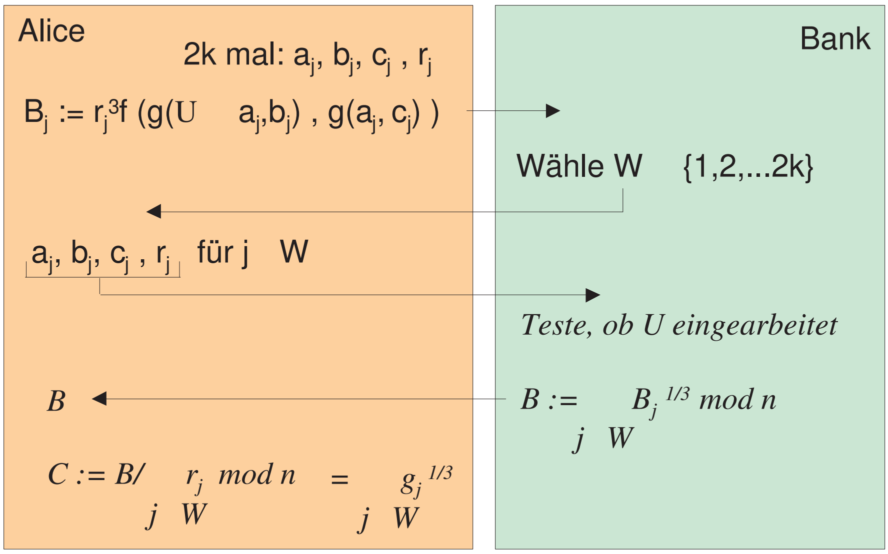
Münzen erzeugen mit blinder Signatur



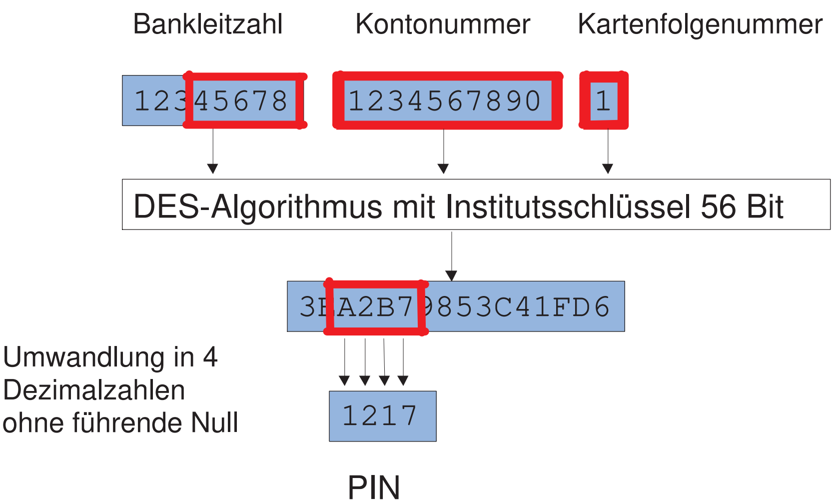
Münzen ausgeben



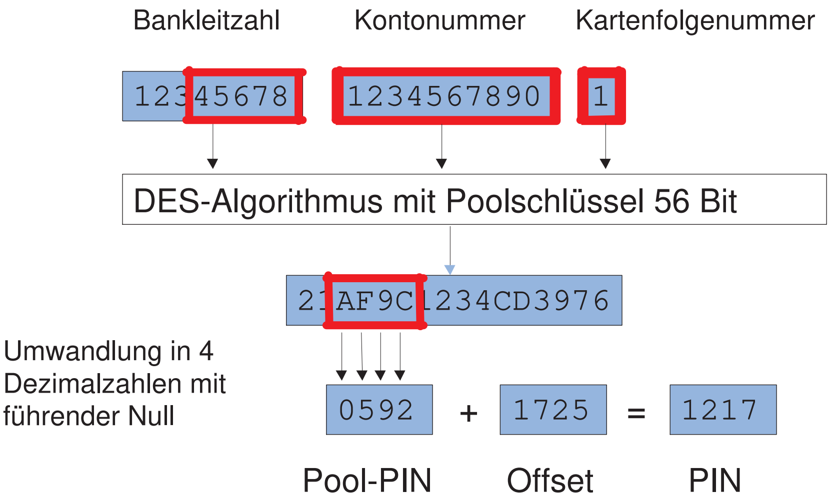
Blinde Signatur mit Einwegfunktion



Münzen erzeugen für Offline ecash scale



Altes EC-PIN-Verfahren (eigenes Institut)



Altes EC-PIN-Verfahren (fremdes Institut)

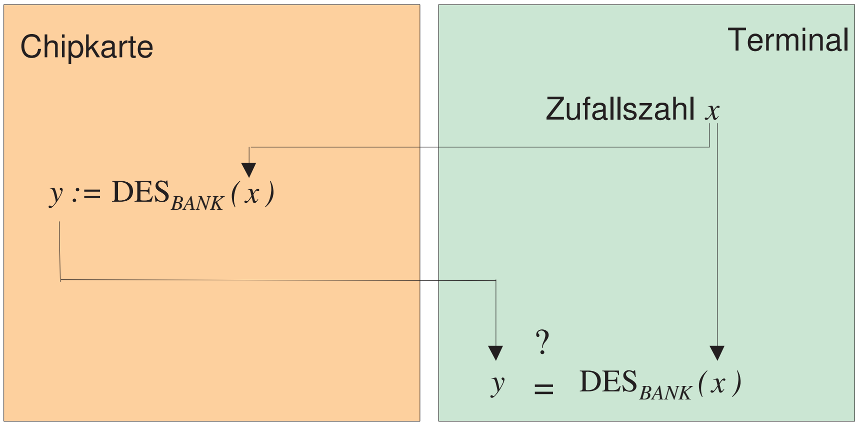
Erstes Zeichen:

Hex-Symbol	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
PIN-Ziffer	1	1	2	3	4	5	6	7	8	9	1	1	2	3	4	5

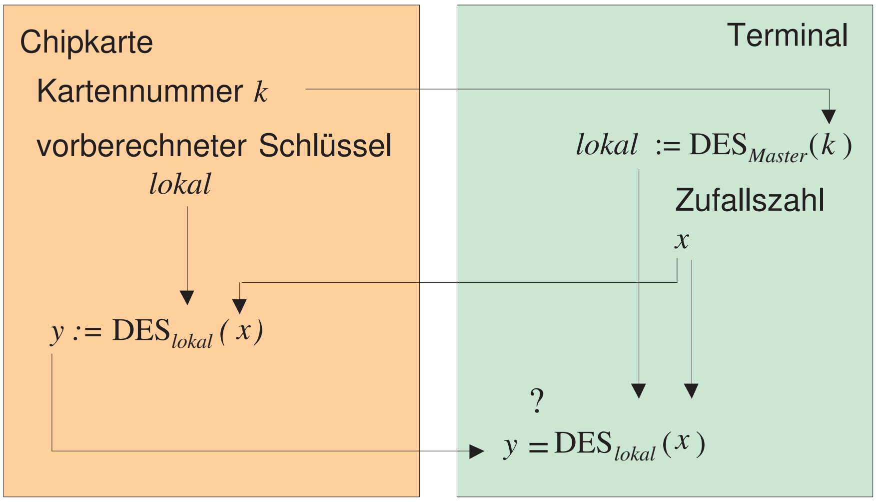
Zweites, drittes, viertes Zeichen:

Hex-Symbol	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
PIN-Ziffer	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5

Verteilung der PIN-Ziffern



Challenge Response mit globalem Schlüssel



Challenge Response mit lokalem Schlüssel