SECURE RISK PROPAGATION

Banks	Customer	Bank account	Initial cash ratios
Yellow bank	Charlie	NL64ABNC04	0.1
Green Bank	Sam	NL06SNSB01	0.1
Purple Bank	Esme	NL54RABO03	0.6
Purple Bank	George	NL38RABO08	0.8

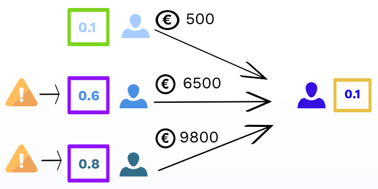
0.1 = Cash ratio of Charlies account , customer of Yellow bank

0.1 = Cash ratio of Sam's account , customer of Green bank

0.6 = Cash ratio of Esme's account , customer of Purple bank

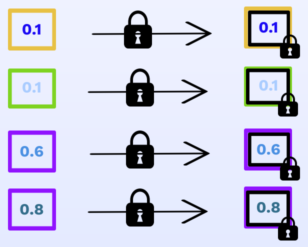
0.8 = Cash ratio of George's account , customer of Purple bank

Problem statement



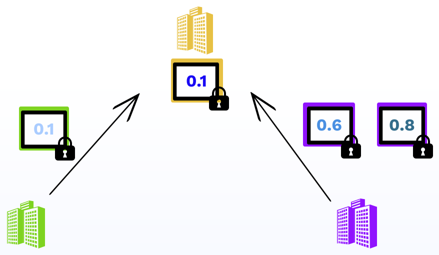
Esme and George from Purple bank have received suspicious money due to recent cash deposits, cryptocurrencies or amounts from high risk geographies. Charlie, customer of Yellow bank, receives a total of three transactions over the last period. Yellow bank, however, is unaware of the riskiness of Esme's and George's activities. None of the banks actually oversees the complete picture depicted above but only parts of it.
The starting point for the collaborating banks is to determine the initial cash ratio for its own customer's bank accounts.

Phase 1: Encryption



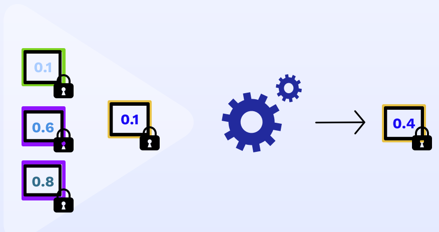
The parties encrypt the cash ratio of their customers using homomorphic encryption. Homomorphic encryption is a special type of encryption that allows the parties to perform meaningful computations on the data while that data stays encrypted through the entire operation. While encrypting, no communication takes place yet.

Phase 2a: Banks communicating the encrypted cash ratio



Once the data is encrypted locally, the distributed propagation (computation) over the encrypted data takes place. During this computation the data remains encrypted, the parties communicate intermediate encrypted results directly with each other, and there is no central party.

Phase 2b: Secure computation



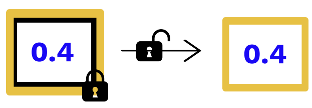
A calculation is performed by homomorphic encryption with the encrypted cash ratios of the accounts. Homomorphic encryption is a special type of encryption that allows the parties to perform meaningful computations on the data while data stays encrypted through the entire operation. The new encrypted cash ratios of Charlies account is computed by taking the average of the previous cash ratio of Charlies account and the average cash ratios from incoming transaction weighted with the transaction amount. *

After an iteration, the computation repeats (going to phase 2a) for another iteration or continues to the decryption (going to phase 3).

** In this example, the new encrypted cash ratio can be computed as follows, where the notation [2] means an encryption of 2.*

$$\frac{[0.1] \text{ x } 500 + [0.6] \text{ x } 6500 + [0.8] \text{ x } 9800}{(500 + 6500 + 9800) \text{ x } 2} + \frac{[0.1]}{2} = \frac{[0.7] + [0.1]}{2} = [0.4]$$

Phase 3: Joint decryption

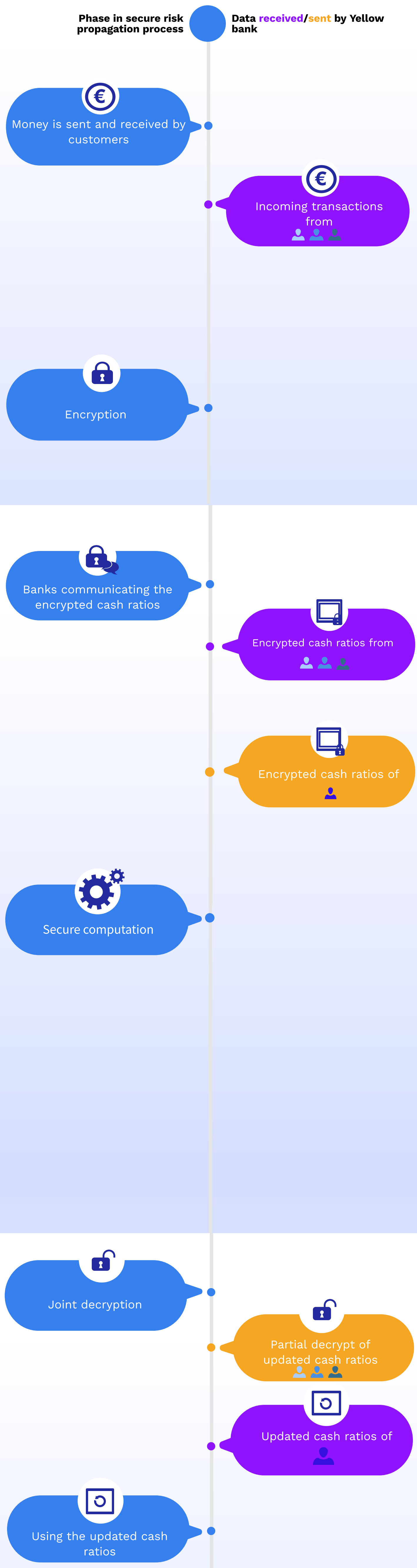


Each bank will need to perform a partial decrypt so that the updated cash ratio of Charlies account can be revealed to the Yellow bank.

Phase 4: Using the updated cash ratios

The updated cash ratios of Charlies accounts is used as additional feature in Yellow bank's monitoring and detection system for AML purposes. This results in improved detection and more accurate risks. In this example, it might be worthwhile to further investigate why Charlie has an increased cash ratio.

Start timeline


Phase in secure risk propagation process
Data received/sent by Yellow bank
Money is sent and received by customers
Incoming transactions from
Encryption
Banks communicating the encrypted cash ratios
Encrypted cash ratios from
Encrypted cash ratios of
Secure computation
Joint decryption
Partial decrypt of updated cash ratios
Updated cash ratios of
Using the updated cash ratios