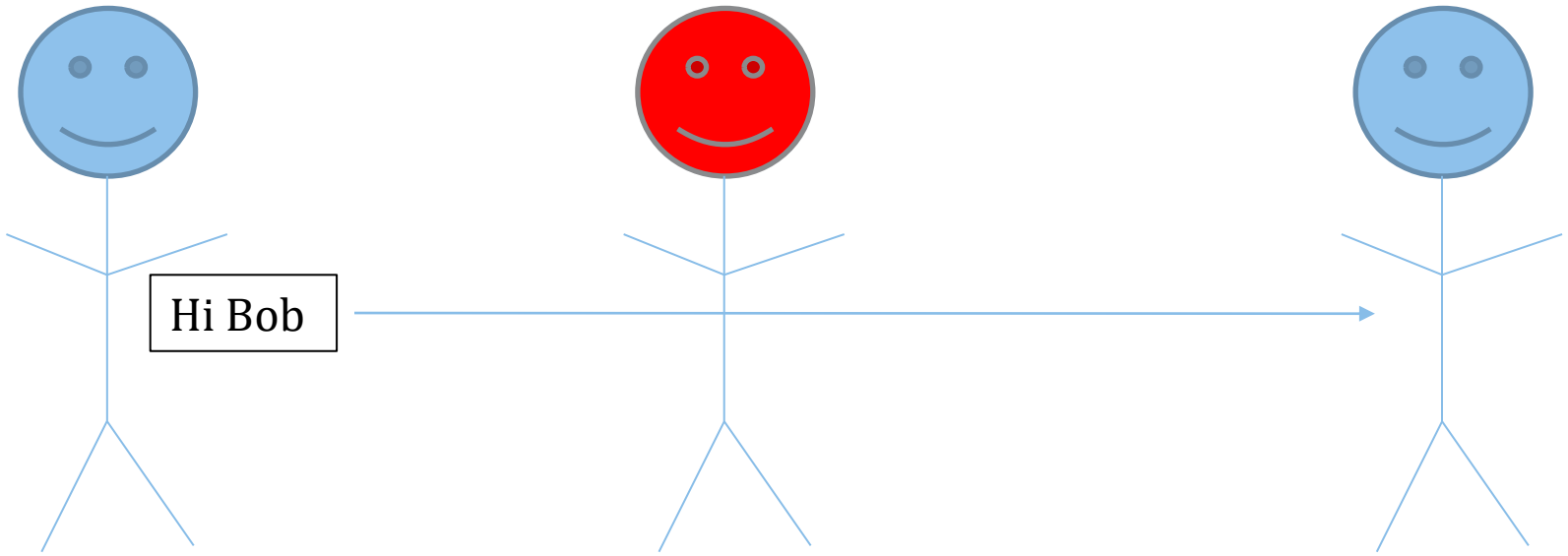
The McEliece Cryptosystem as a Solution to the Post-Quantum Cryptographic Problem

Isaac Hanna

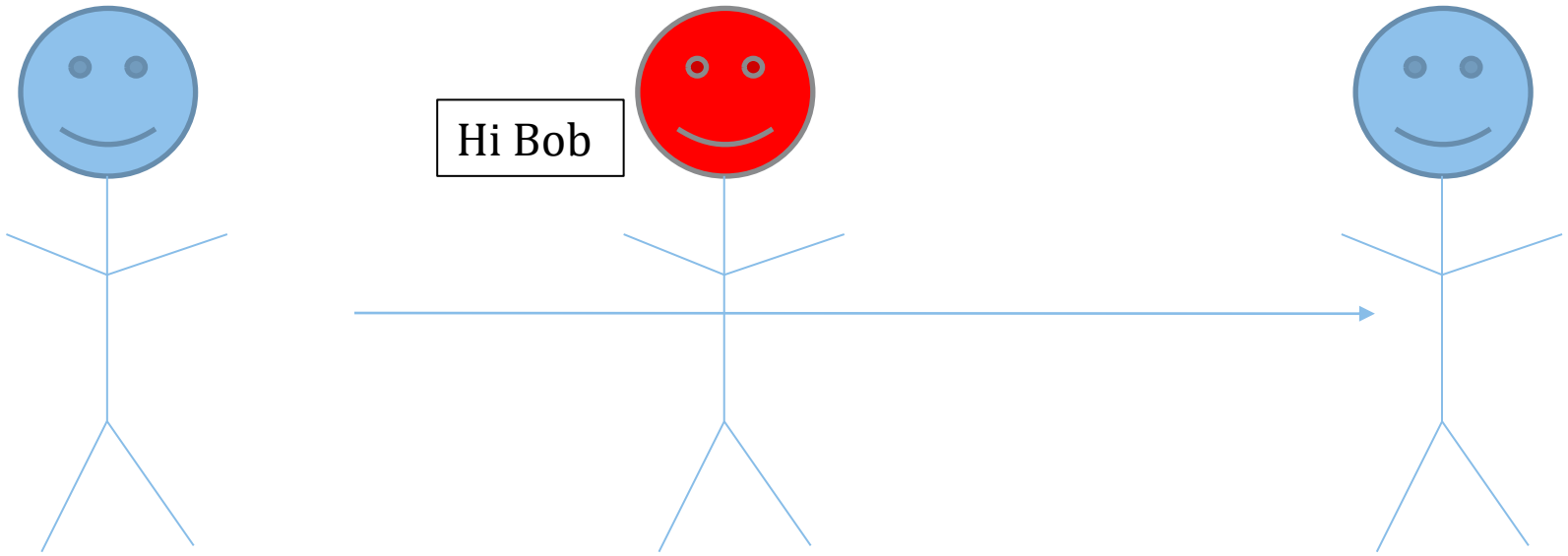
The McEliece Cryptosystem as a Solution to the Post-Quantum Cryptographic Problem

Isaac Hanna

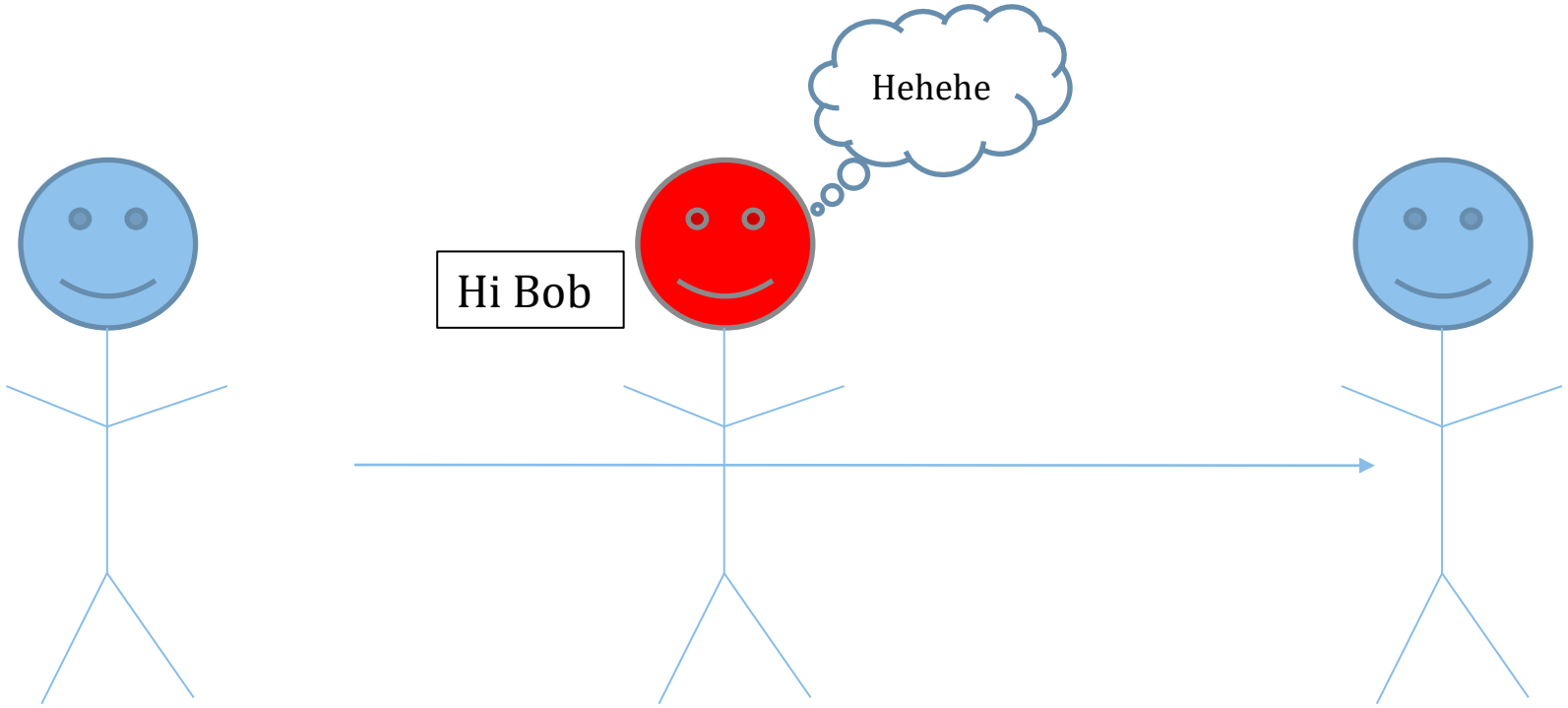
The Cryptographic Problem



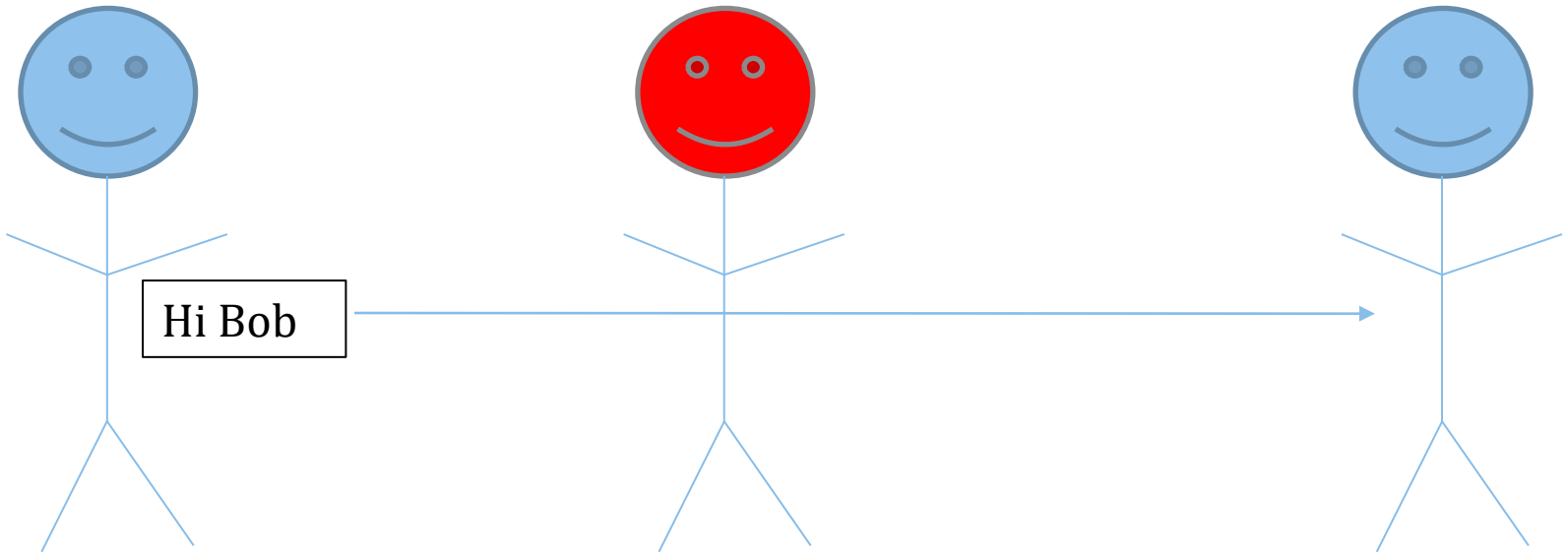
The Cryptographic Problem



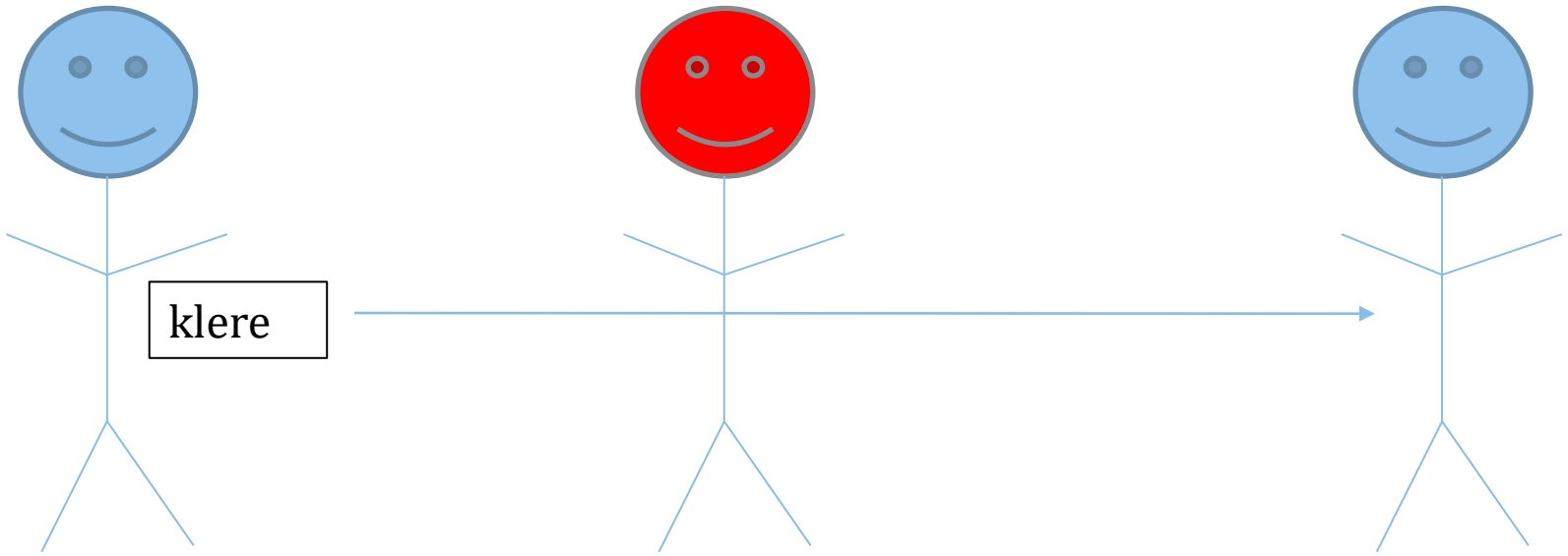
The Cryptographic Problem



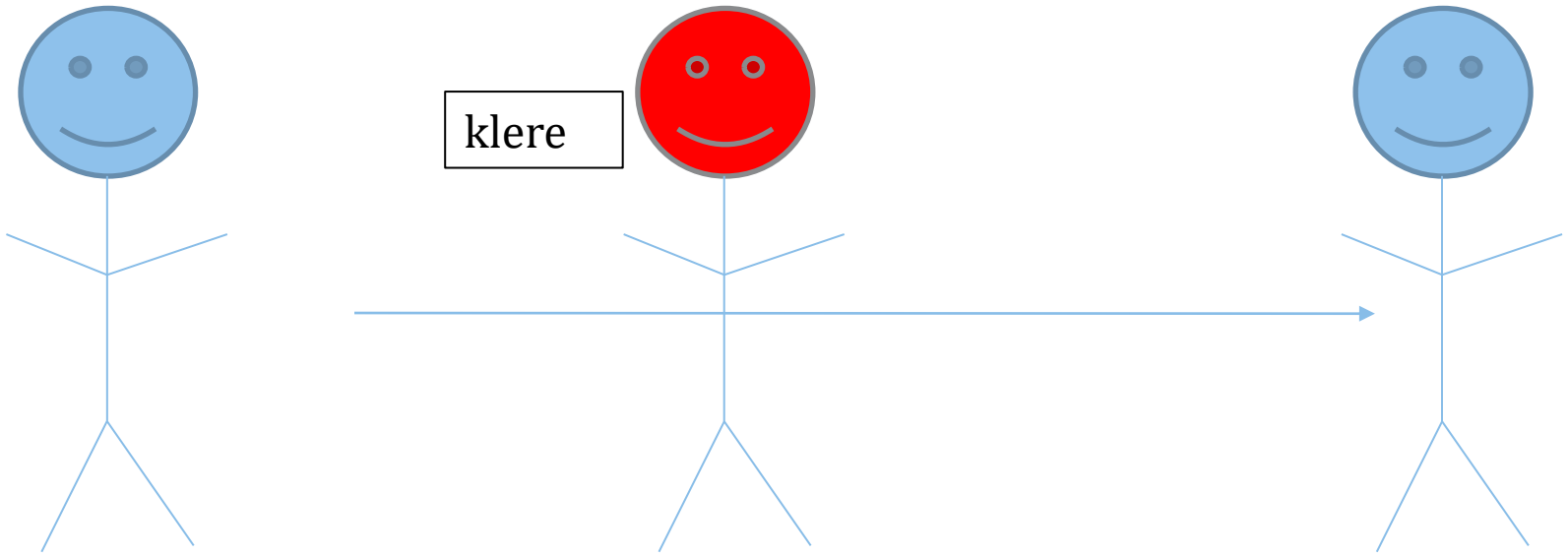
The Cryptographic Problem



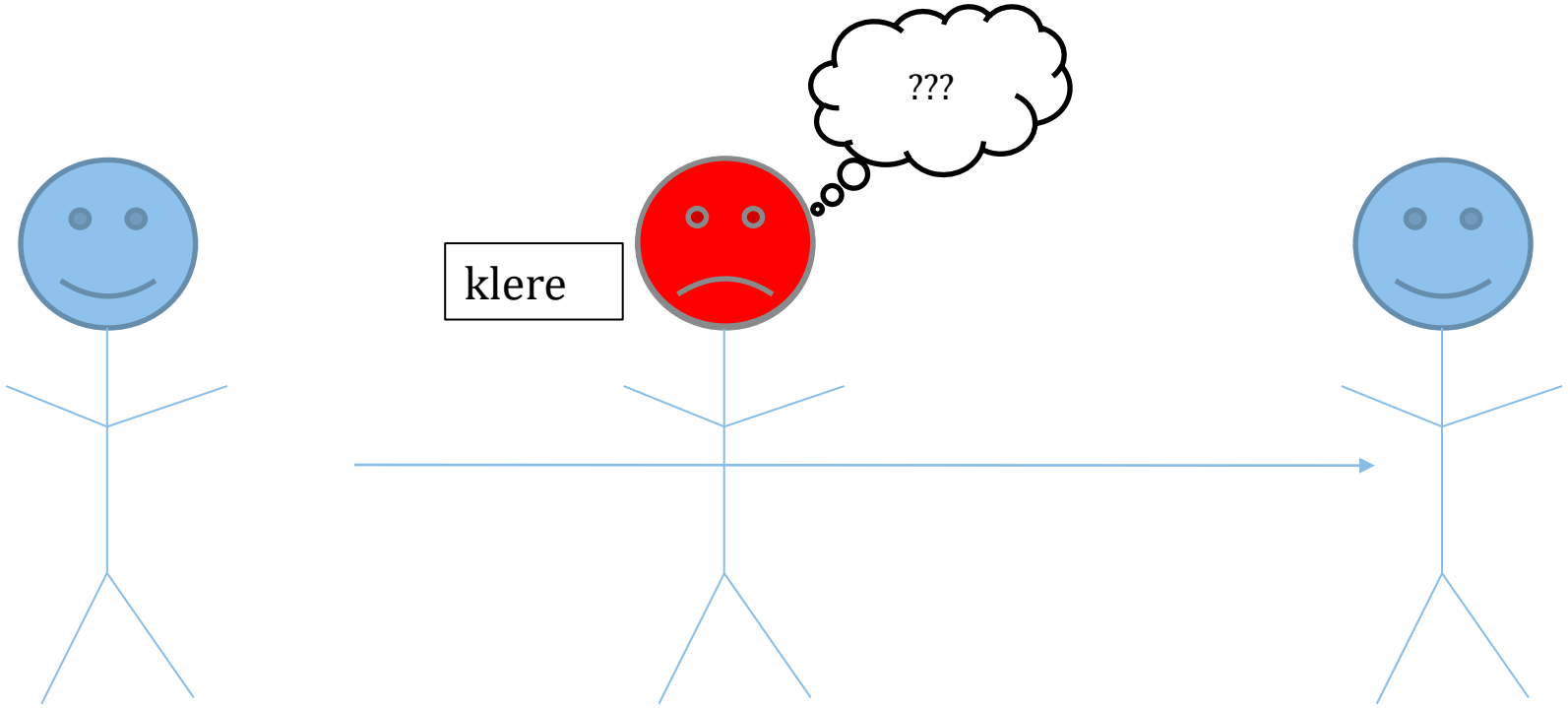
The Cryptographic Problem



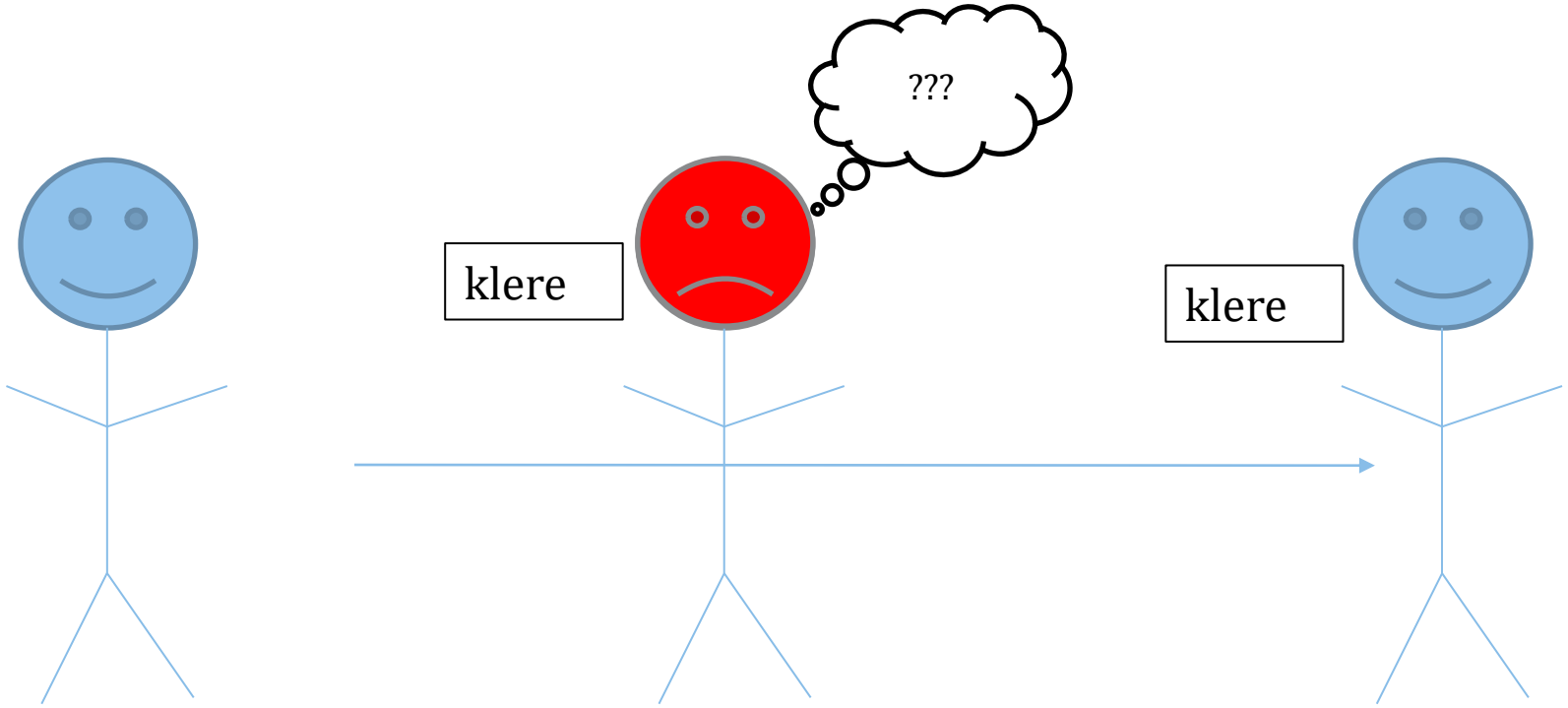
The Cryptographic Problem



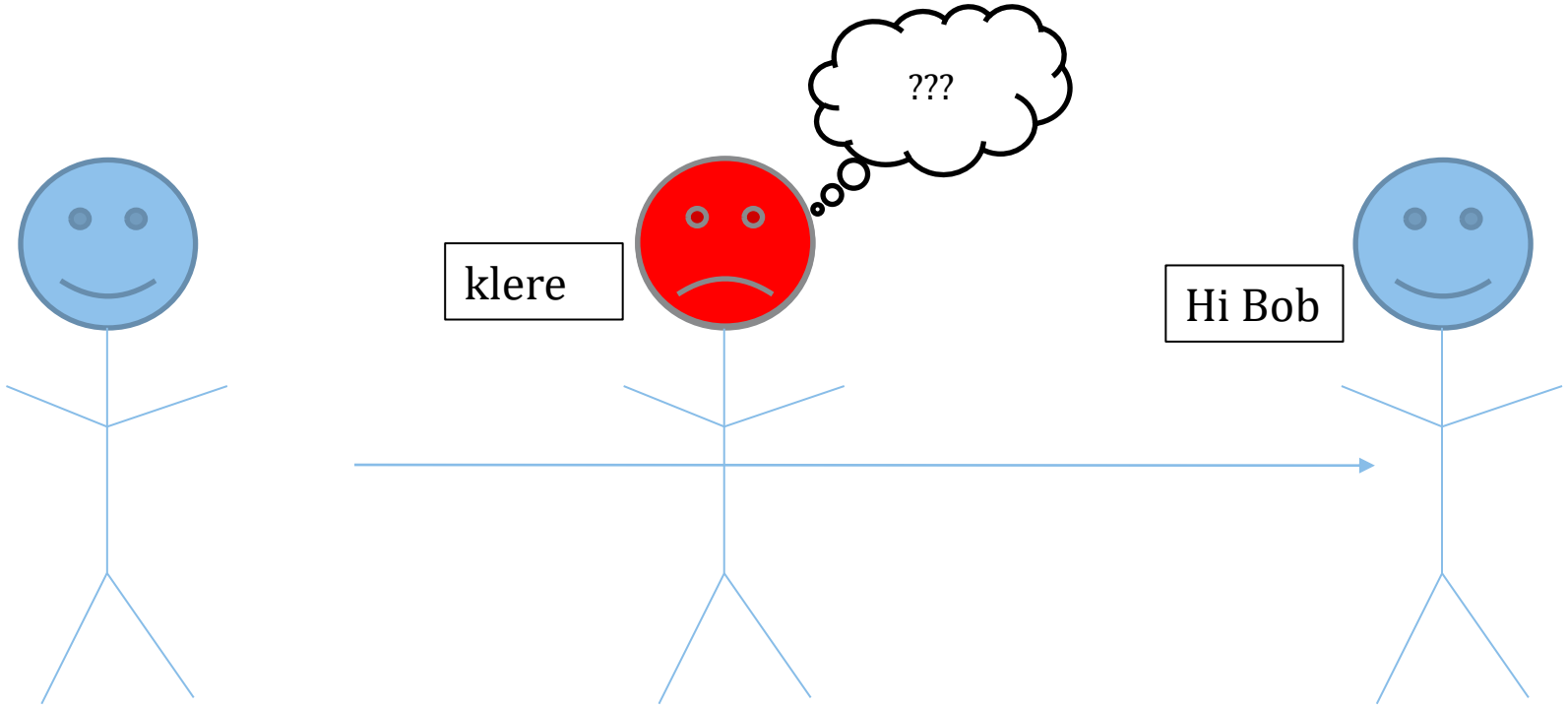
The Cryptographic Problem



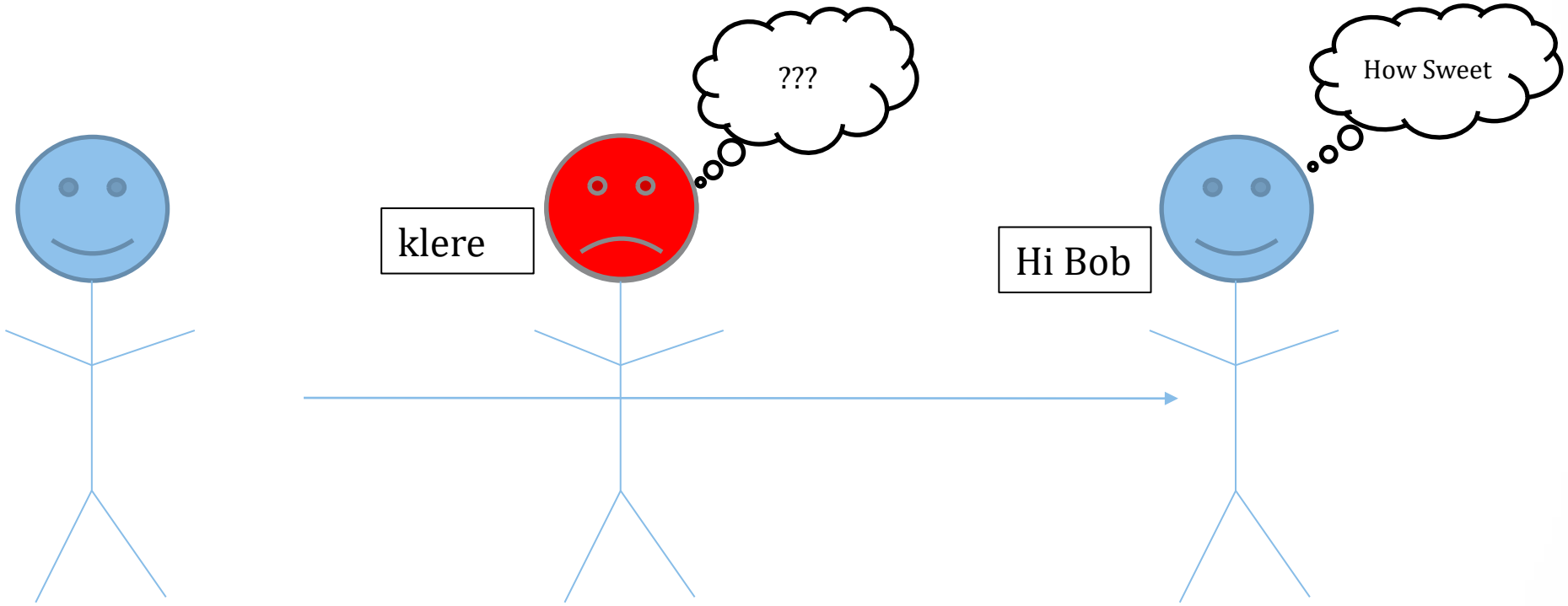
The Cryptographic Problem



The Cryptographic Problem



The Cryptographic Problem



Asymmetric Encryption

Asymmetric Encryption

- $D_k = E_k^{-1}$

Asymmetric Encryption

- $D_k = E_k^{-1}$
- E_k and D_k cannot be computed easily

Asymmetric Encryption

- $D_k = E_k^{-1}$
- E_k and D_k cannot be computed easily
- D_k cannot be feasibly derived from E_k

Asymmetric Encryption

- $D_k = E_k^{-1}$
- E_k and D_k cannot be computed easily
- D_k cannot be feasibly derived from E_k
- E_k and D_k can be computed from k

RSA Encryption

RSA Encryption

- Public Key: n, d

RSA Encryption

- Public Key: n, d
- Private Key: p, q, e

RSA Encryption

- Public Key: n, d
- Private Key: p, q, e
- $E_k(m) = m^d (mod\ n)$

RSA Encryption

- Public Key: n, d
- Private Key: p, q, e
- $E_k(m) = m^d (mod\ n)$
- $D_k(x) = x^e (mod\ n) = m$

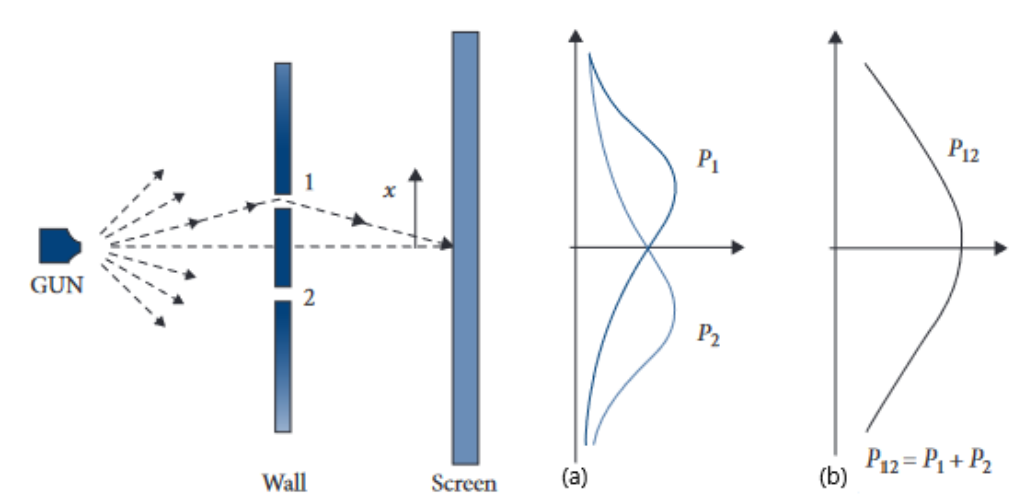
RSA Encryption

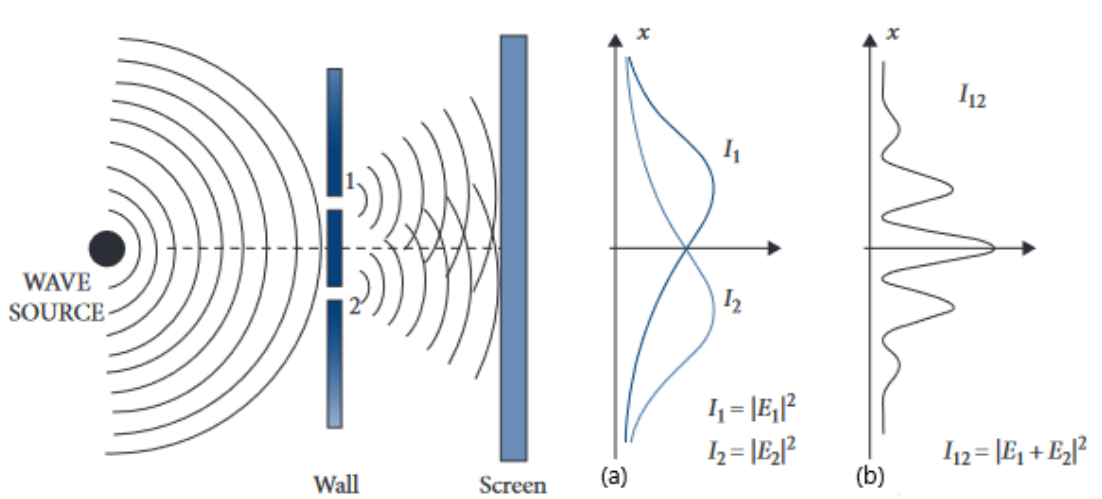
- Public Key: n, d
- Private Key: p, q, e
- $E_k(m) = m^d (mod\ n)$
- $D_k(x) = x^e (mod\ n) = m$
- Security rests upon difficulty of finding p and q to obtain e

RSA Encryption

- Public Key: n, d
- Private Key: p, q, e
- $E_k(m) = m^d (mod\ n)$
- $D_k(x) = x^e (mod\ n) = m$
- Security rests upon difficulty of finding p and q to obtain e
- Shor's Algorithm provides an exponential speedup

Double Slit Experiment





Quantum States and Superposition

Quantum States and Superposition

- $|a\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

Quantum States and Superposition

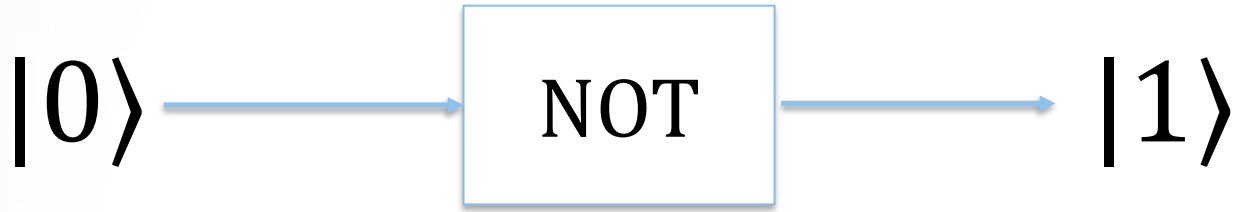
- $|a\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
- $|a\rangle = c_0|0\rangle + c_1|1\rangle$

Quantum States and Superposition

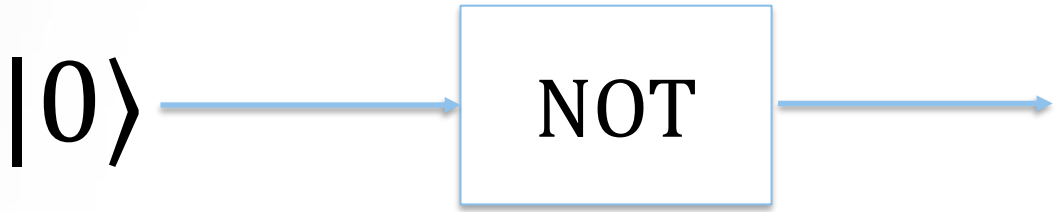
- $|a\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
- $|a\rangle = c_0|0\rangle + c_1|1\rangle$
- $|ab\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$

Quantum Gates

Quantum Gates

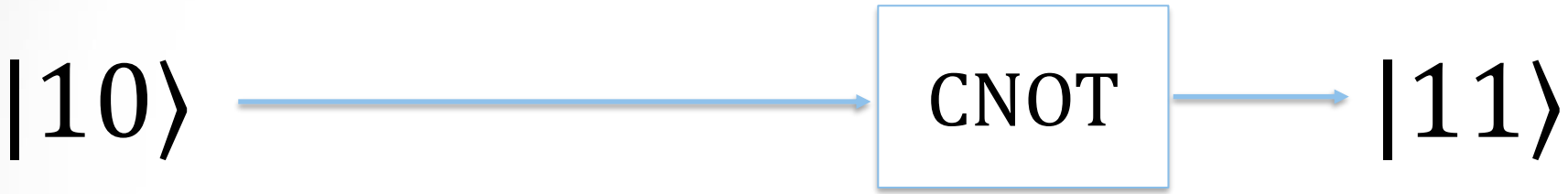


Quantum Gates



Multi-Qubit Gates

Multi-Qubit Gates



Multi-Qubit Gates

$|10\rangle$ → CNOT → $|11\rangle$

$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$ → CNOT → ???

Multi-Qubit Gates

$$|10\rangle \longrightarrow \boxed{\text{CNOT}} \longrightarrow |11\rangle$$

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle \longrightarrow \boxed{\text{CNOT}} \longrightarrow \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Entanglement

Entanglement

- Two particles are inextricably linked

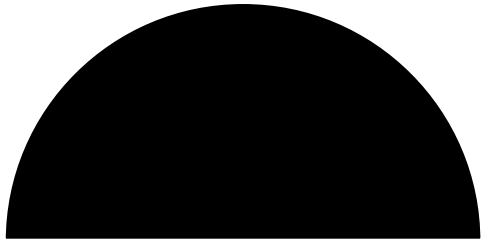
Entanglement

- Two particles are inextricably linked
- Finding information about one gives us information about the other

Phase Encoding

Phase Encoding

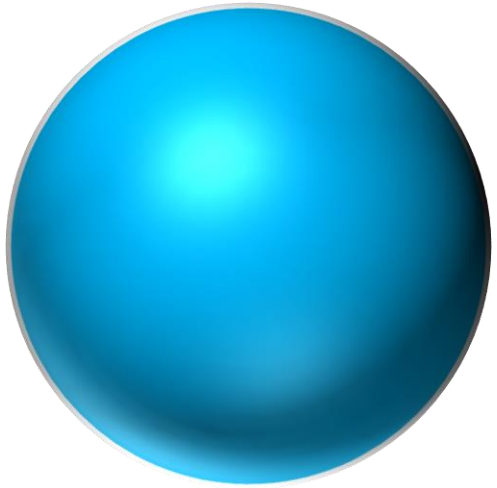
- Without Phase:



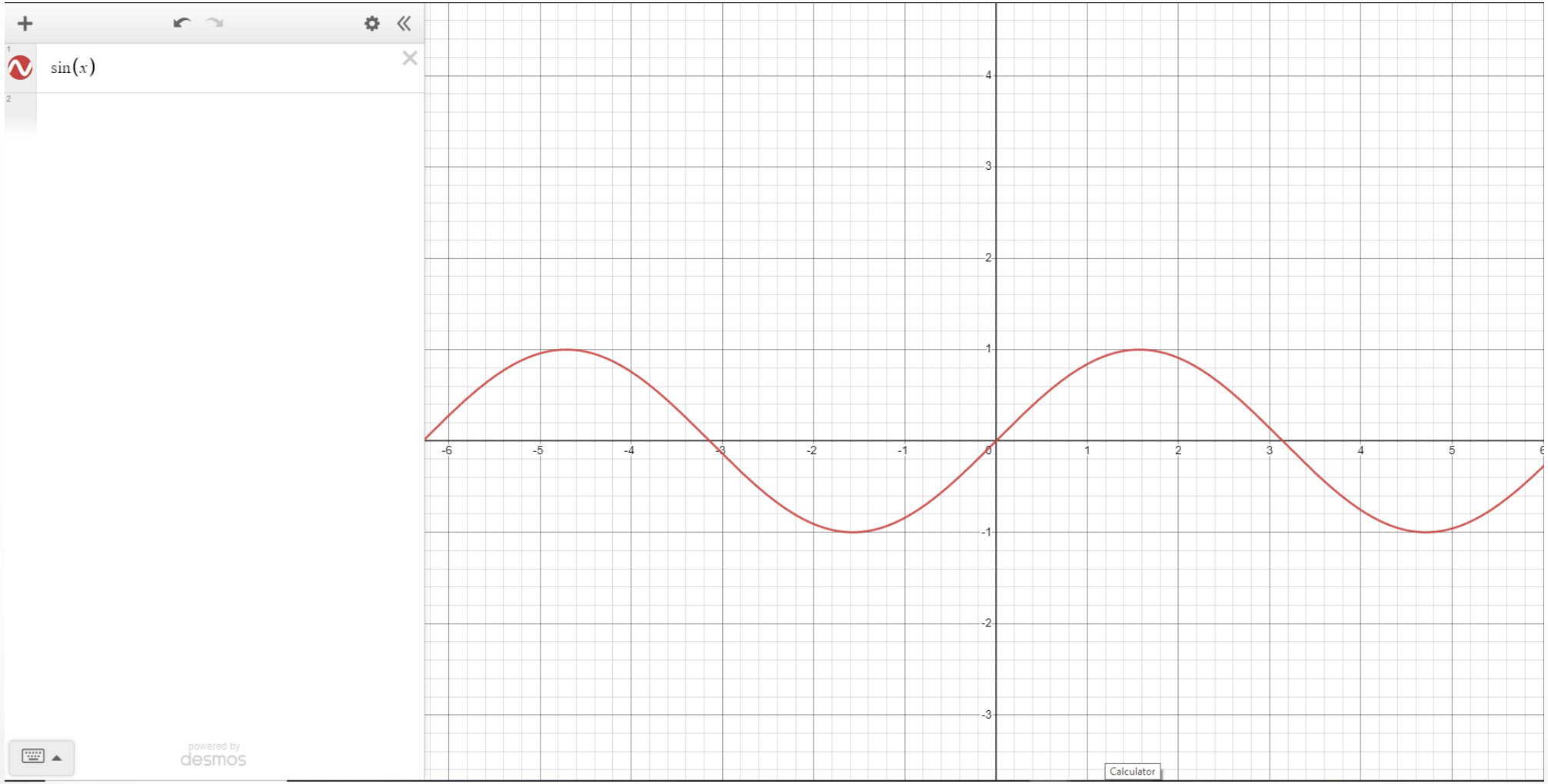
Phase Encoding

- Without Phase:

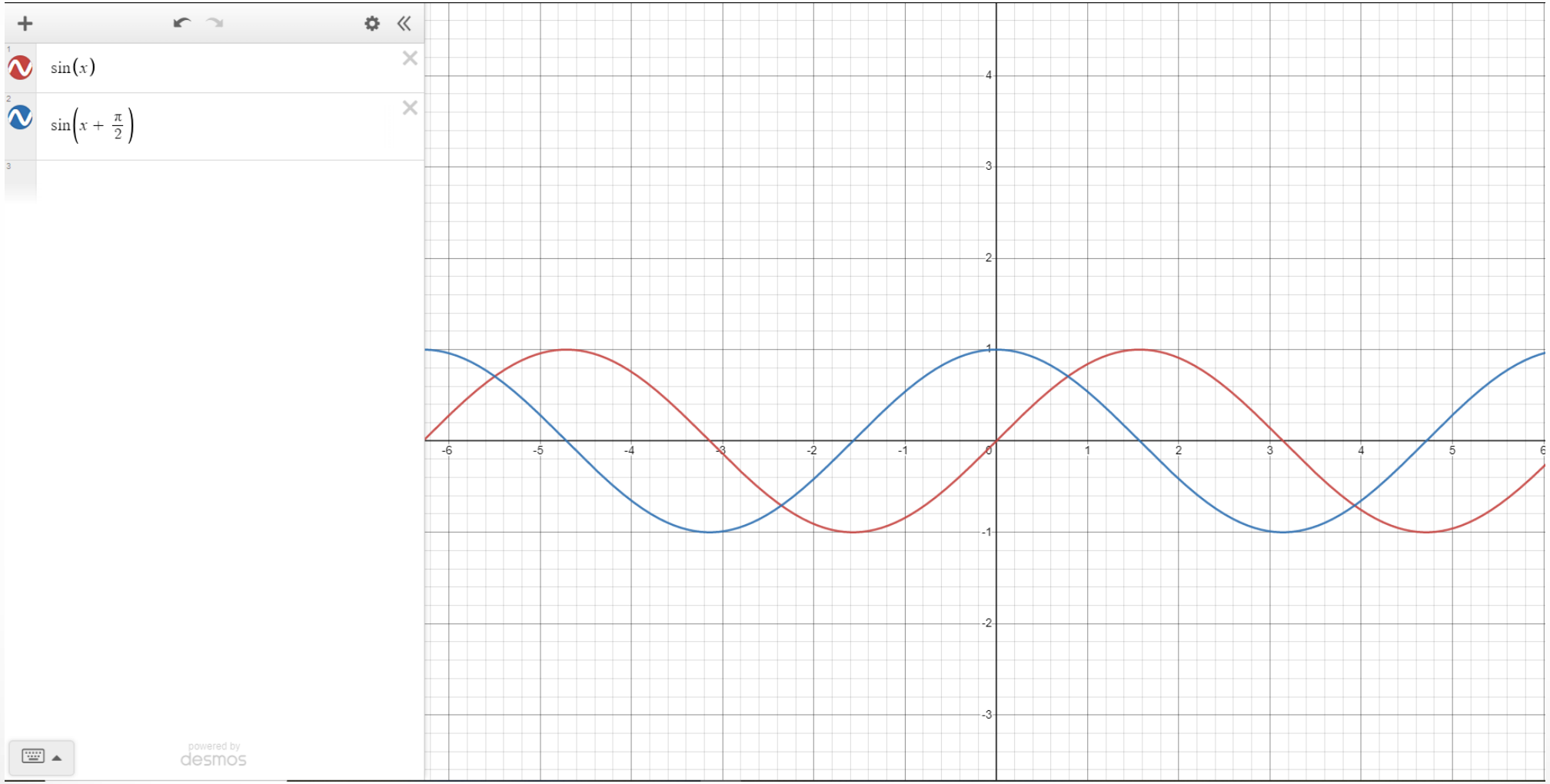
- With Phase:



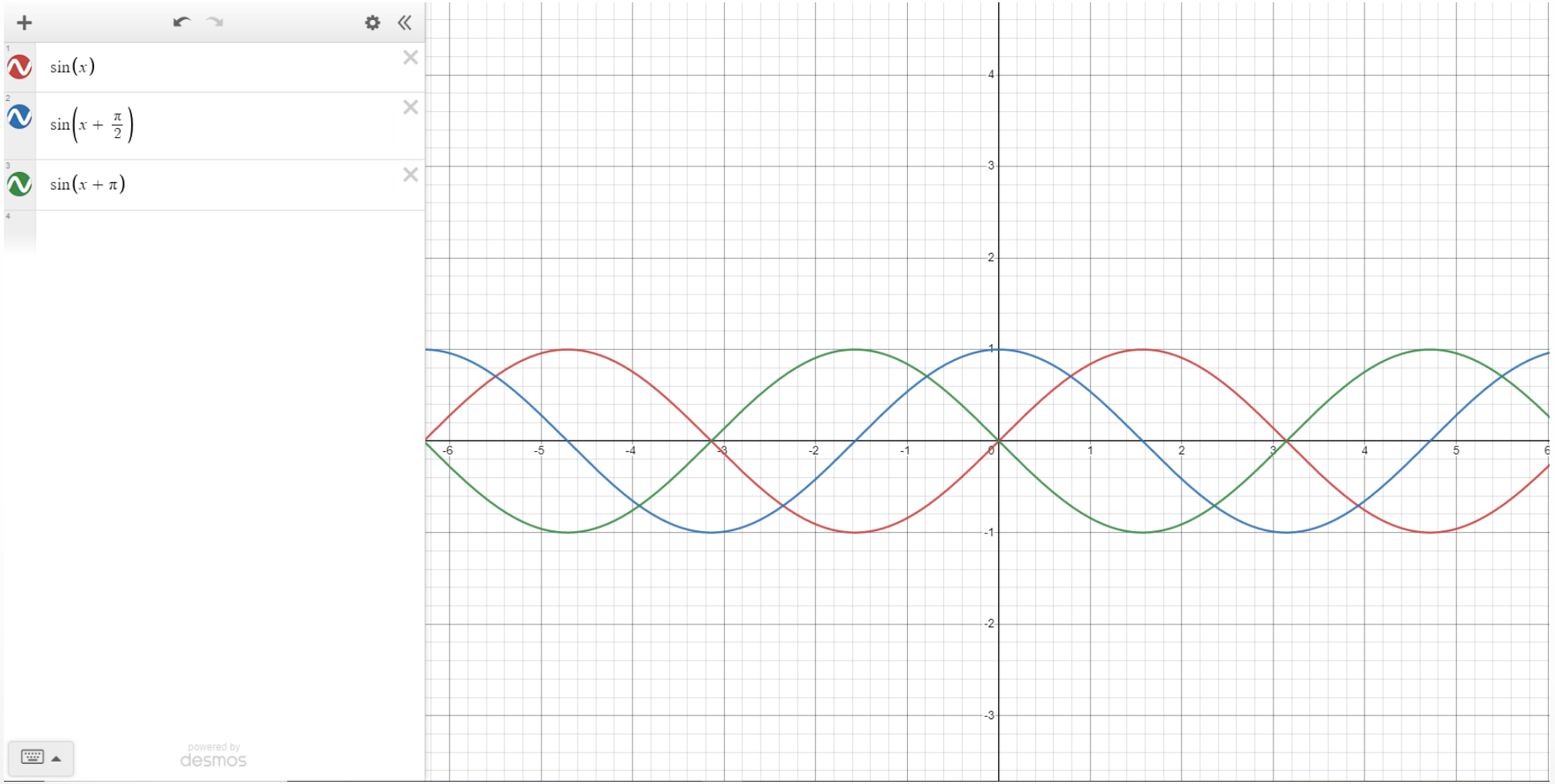
Phase Encoding



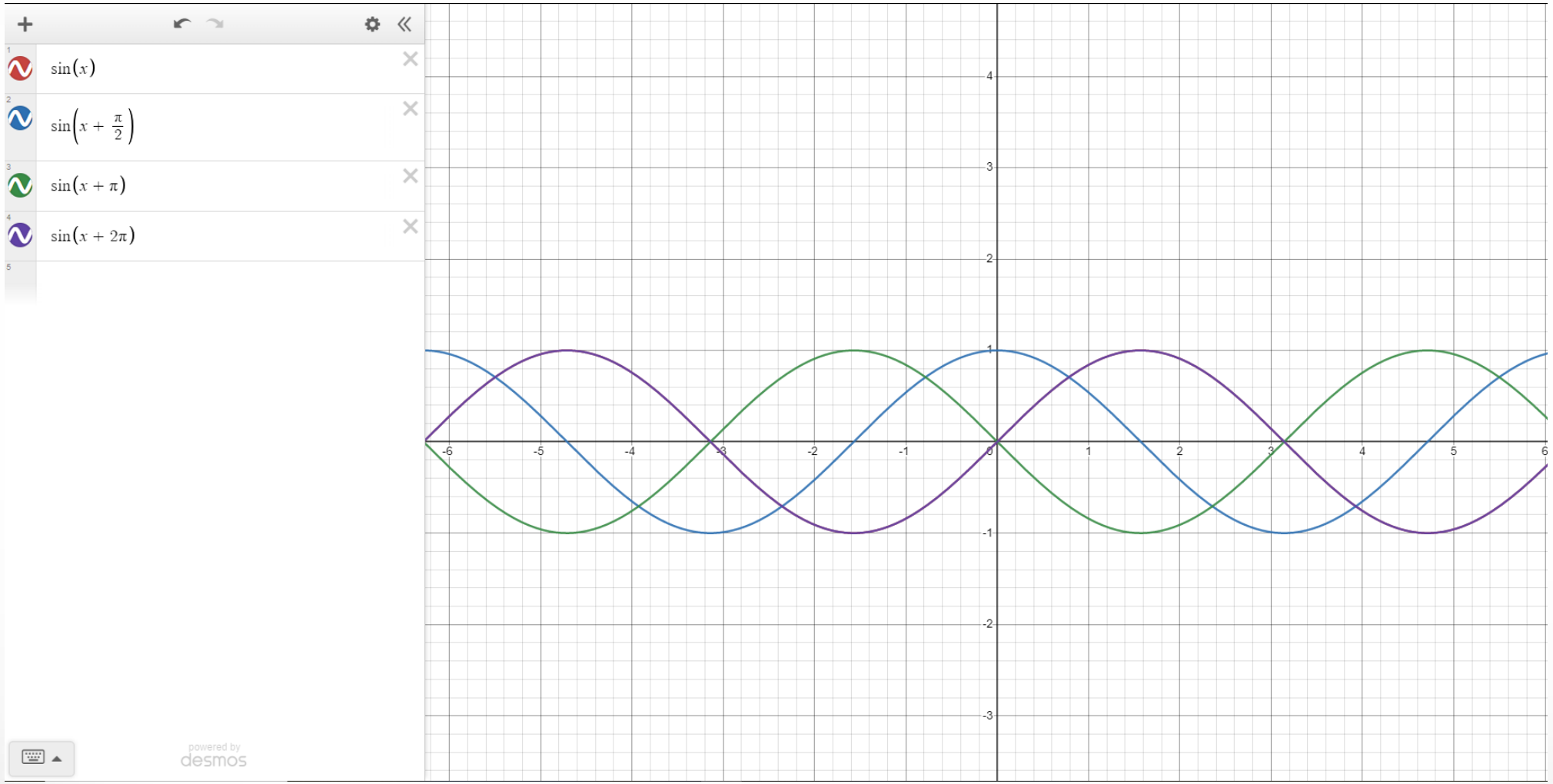
Phase Encoding



Phase Encoding



Phase Encoding



Shor’s Algorithm

Shor’s Algorithm

- Encode all values from 0 to q – 1 in a register

Shor's Algorithm

- Encode all values from 0 to q – 1 in a register

- Create an Entanglement with a second register by mapping a to $x^a \ (mod\ n)$

Shor's Algorithm

- Encode all values from 0 to q – 1 in a register
- Create an Entanglement with a second register by mapping a to $x^a \ (mod\ n)$
- Encode the values in the phase of the first register

Shor's Algorithm

- Encode all values from 0 to q – 1 in a register
- Create an Entanglement with a second register by mapping a to $x^a \ (mod\ n)$
- Encode the values in the phase of the first register
- Observe the value of the second register

McEliece

McEliece

- Binary Goppa Codes – Built upon a generator polynomial and corresponding matrix

McEliece

- Binary Goppa Codes – Built upon a generator polynomial and corresponding matrix

- Polynomial of degree s allows correcting up to s errors

McEliece (Encoding)

McEliece (Encoding)

- Split data into k-bit blocks

McEliece (Encoding)

- Split data into k-bit blocks
- Scramble the blocks with invertible matrix S

McEliece (Encoding)

- Split data into k-bit blocks
- Scramble the blocks with invertible matrix S
- Encode as n-bit codewords using generator matrix G

McEliece (Encoding)

- Split data into k-bit blocks
- Scramble the blocks with invertible matrix S
- Encode as n-bit codewords using generator matrix G
- Permute codewords using permutation matrix P

McEliece (Encoding)

- Split data into k-bit blocks
- Scramble the blocks with invertible matrix S
- Encode as n-bit codewords using generator matrix G
- Permute codewords using permutation matrix P
- Add t errors where t is the degree of the generator polynomial

McEliece

McEliece

- Private Key: $S, G, P, G(x)$

McEliece

- Private Key: $S, G, P, G(x)$
- Public Key: $G' = SGP$

McEliece

- Private Key: $S, G, P, G(x)$
- Public Key: $G' = SGP$
- Decoding

McEliece

- Private Key: $S, G, P, G(x)$
- Public Key: $G' = SGP$
- Decoding
  - Depermute using P^{-1}

McEliece

- Private Key: $S, G, P, G(x)$
- Public Key: $G' = SGP$
- Decoding
  - Depermute using P^{-1}
  - Correct errors

McEliece

- Private Key: $S, G, P, G(x)$
- Public Key: $G' = SGP$
- Decoding
  - Depermute using P^{-1}
  - Correct errors
  - Decode to k-bit vector

McEliece

- Private Key: $S, G, P, G(x)$
- Public Key: $G' = SGP$
- Decoding
  - Depermute using P^{-1}
  - Correct errors
  - Decode to k-bit vector
  - Unscramble using S^{-1}

Security and Cost

Security and Cost

- Security rests upon multiple difficult problems

Security and Cost

- Security rests upon multiple difficult problems
  - Crack a linear code with errors

Security and Cost

- Security rests upon multiple difficult problems
  - Crack a linear code with errors
  - Or Decode a matrix into three matrices

Security and Cost

- Security rests upon multiple difficult problems
  - Crack a linear code with errors
  - Or Decode a matrix into three matrices

- Cannot be reduced to the Hidden Subgroup Problem

Security and Cost

- Security rests upon multiple difficult problems
  - Crack a linear code with errors
  - Or Decode a matrix into three matrices
- Cannot be reduced to the Hidden Subgroup Problem
- The large keys make it much more expensive than current schemes

Conclusion

Conclusion

- Encryption is a key part of today's economy

Conclusion

- Encryption is a key part of today's economy
- Current encryption is based upon integer factorization

Conclusion

- Encryption is a key part of today's economy
- Current encryption is based upon integer factorization
- Shor's Algorithm takes advantage of superposition, entanglement, and phase encoding to provide an exponential speedup

Conclusion

- Encryption is a key part of today's economy
- Current encryption is based upon integer factorization
- Shor's Algorithm takes advantage of superposition, entanglement, and phase encoding to provide an exponential speedup
- The McEliece Cryptosystem is not currently susceptible to quantum attack

References

- Aspect, A., Dalibard, J., & Roger, G. (1982). Experimental Test of Bell's Inequalities Using Time- Varying Analyzers. Physical Review Letters, 49(25), 1804–1807
- Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644–654.
- Feynman, R., Leighton, R., & Sands, M. (1964). Feynman Lectures on Physics Vol 3 Feynman, Leighton and Sands (1964)
- Fry, E. S., & Thompson, R. C. (1976). Experimental Test of Local Hidden-Variable Theories
- Hallgren, S., Russell, A., & Ta-Shma, A. (2003). The Hidden Subgroup Problem and Quantum Computation Using Group Representations
- McEliece, R. (1977). Theory of Information and Coding
- McEliece, R. (1978). A Public-Key Cryptosystem Based on Algebraic Coding Theory, 3
- Patterson, N. (1975). The algebraic decoding of Goppa codes. IEEE Transactions on Information
- Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. 21(2), 7
- Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing, 26(5), 26.
- Stein, W. (2009). Elementary Number Theory: Primes, Congruences, and Secrets. Springer New York.
- Zubairy, M. S. (2020). Quantum Mechanics for Beginners: With Applications to Quantum Communication and Quantum Computing. Oxford University Press