PEQUEÑA INTRODUCCIÓN DE LA TAXONOMÍA

En la siguiente gráfica se mostrará como es organizada la clasificación según este survey. Por un lado se tiene el ataque a la criptografía clásica simétrica y por otro lado a la parte asimétrica, así como también la subclasificación del algoritmo Grover y el algoritmo Shor respectivamente.

caption del grafico:
Representación gráfica de la taxonomía

CORRECION DE LA CONCLUSION:

Según lo revisado, se concluye que la criptografía cuántica es un campo que recientemente está emergiendo y de manera rápida y por tal motivo muchas compañías alrededor del mundo invierten recursos para aumentar el conocimiento y las prácticas que se tiene actualmente con respecto a la seguridad post cuántica. Los avances adicionales en la tecnología basada en la mecánica cuántica podrían conducir a una expansión de estas capacidades, lo que daría como resultado formas mejores y más eficientes de implementar criptosistemas simétricos, Además, siempre que la criptografía simétrica no se implemente con oráculos cuánticos, están a salvo de los ataques cuánticos.

Hoy en día nuestros datos clásicos actuales están seguros, sin embargo, usando computación clásica podemos romper dicha seguridad, y para lograrlo existen algoritmos con un tiempo de ejecución exponencial, lo que disminuye la probabilidad que puedan ser vulnerados. Sin embargo con los avances en computación cuántica se consiguió diseñar e implementar algoritmos que pueden lograr el mismo objetivo en tiempo polinomial, la única limitante sería que no se dispone aún con la cantidad de qubits necesarios para romper un metodo de cifrado simetrico o asimetrico de 2048 bits; cabe resaltar que los avances en computación cuántica son rápidos y que para contrarrestar posibles ataques cuánticos se hace uso de la criptografía post-cuántica.