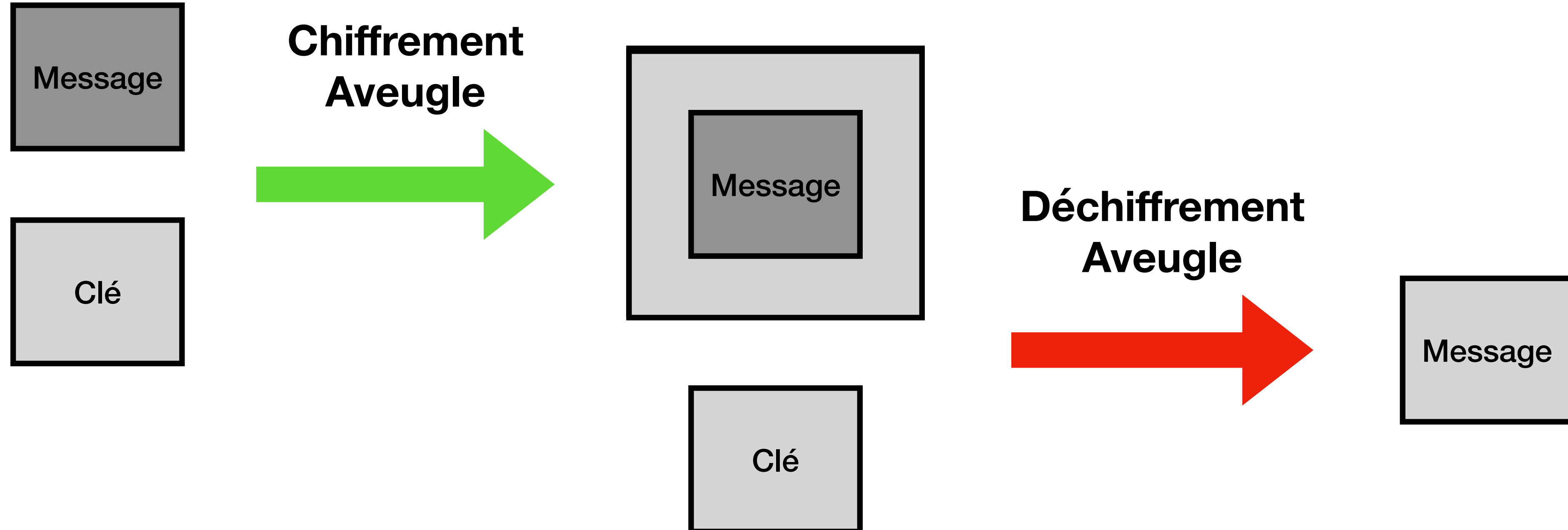


Bootstrapping

Procédure finale: Re-chiffrement et rafraichissement du bruit



Conclusion

Applications, limitations, ouverture

- Le premier schéma que Gentry a proposé
 - Basé sur les idéaux d'anneaux et les réseaux euclidiens, pas efficace
 - Mais le bootstrapping a mené à de nouvelles générations de schémas
- L'inefficacité des schémas existants pose encore frein à leur adoption