SafeVanish: An Improved Data Self-Destruction for Protecting Data Privacy

Lingfang Zeng, Zhan Shi, Shengjie Xu, Dan Feng

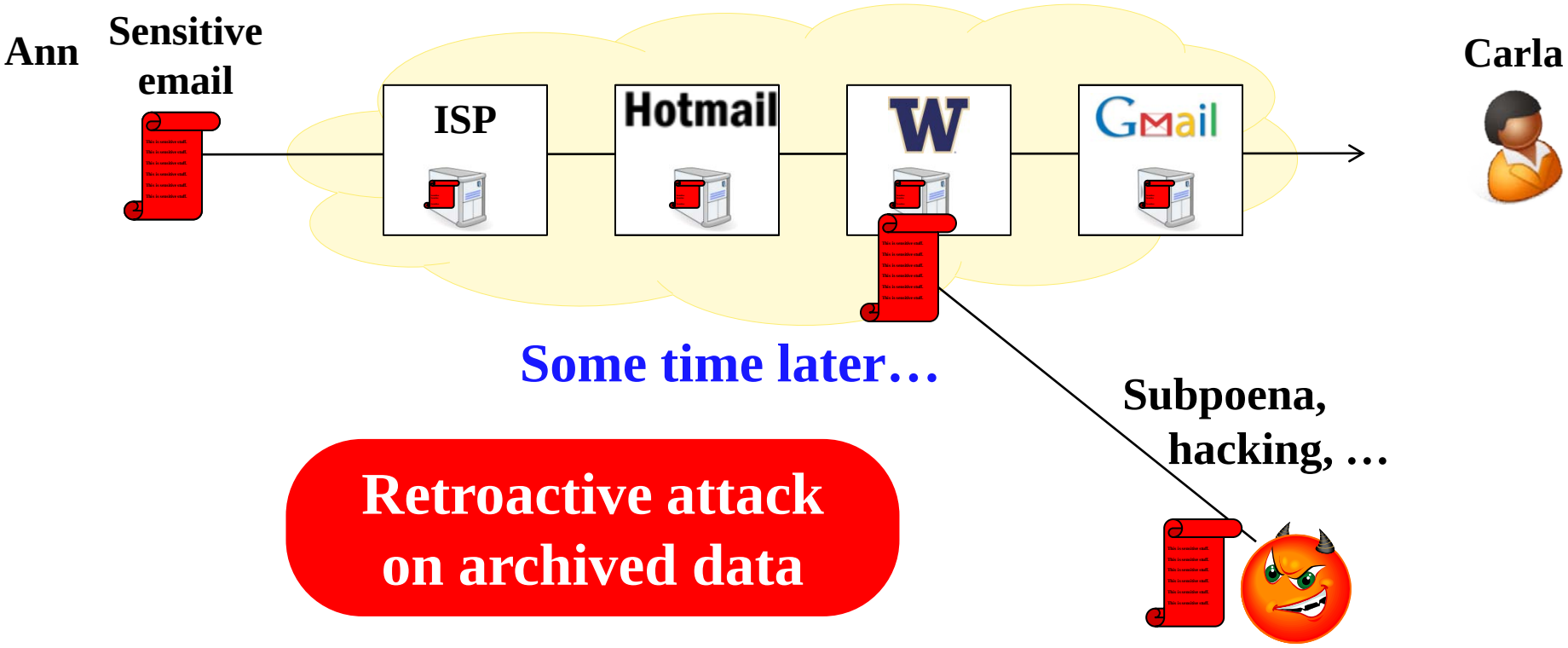
School of Computer Science and Technology, Huazhong University of Science and Technology
Information Storage Division, Wuhan National Laboratory for Optoelectronics

華中科技大學

Outline

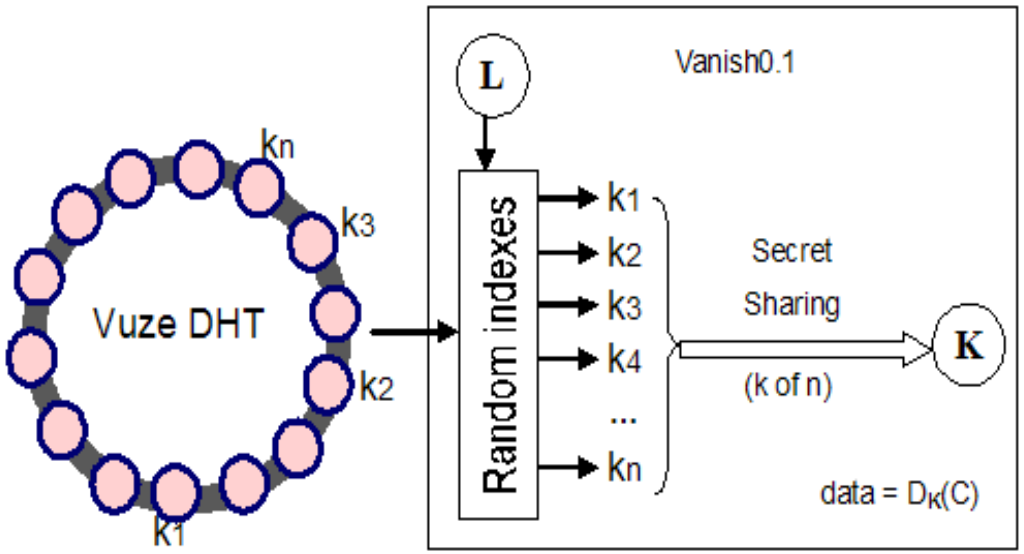
- Related work and motivation
- Solution for the hopping attack
- Solution for the sniffing attack
- Conclusion

Motivation: **Data Lives Forever (1/2)**



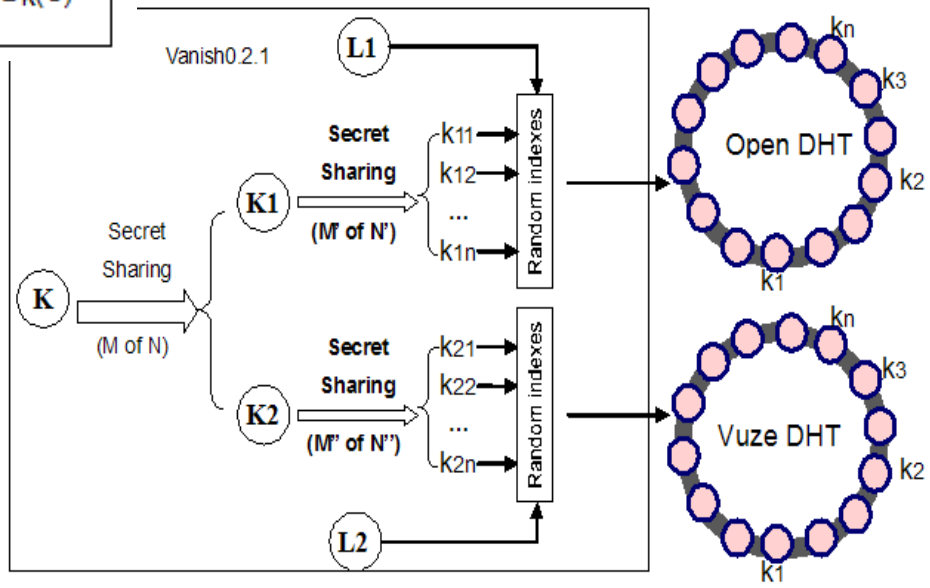
Reference: Roxana Geambasu, Tadayoshi Kohno, Amit Levy, Henry M. Levy. "Vanish: Increasing Data Privacy with Self-Destructing Data." In Proceedings of the 18th USENIX Security Symposium, Montreal, Canada, August 2009.

Motivation : **Data Lives Forever (2/2)**

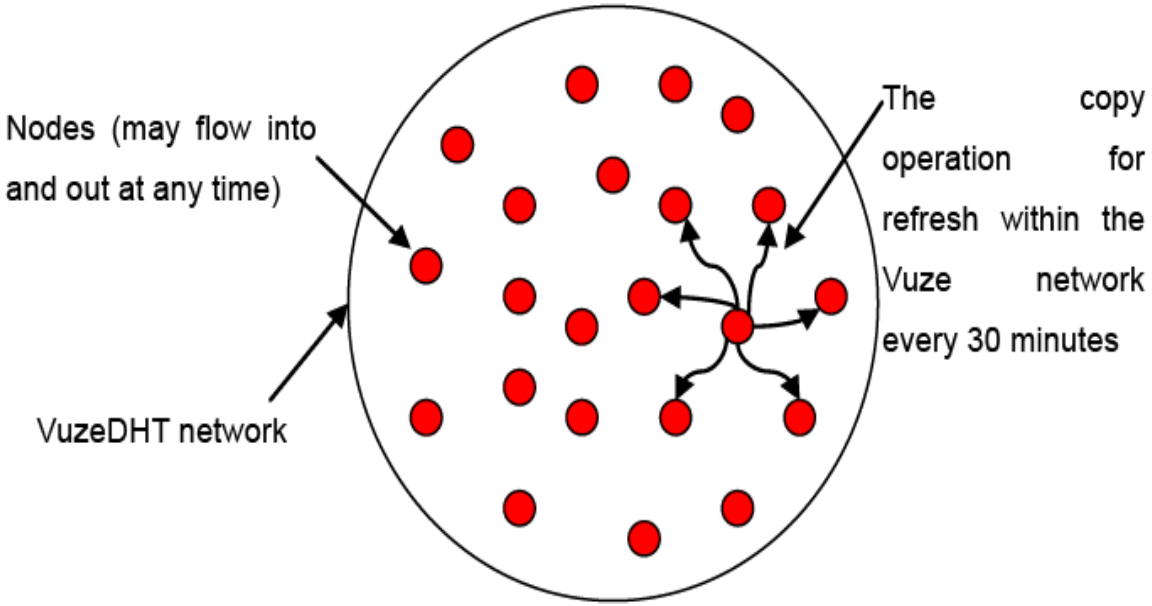


The decapsulation process by compose the encryption key for Vanish0.1.

The improved architecture of Vanish0.2.1.

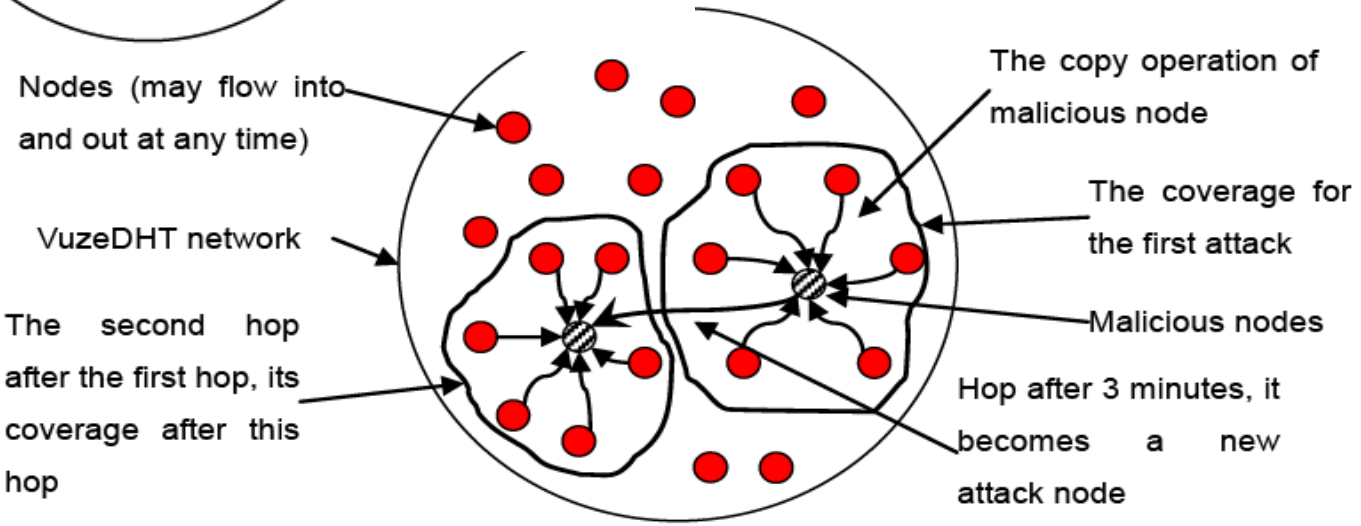


Motivation: **Hopping attack**

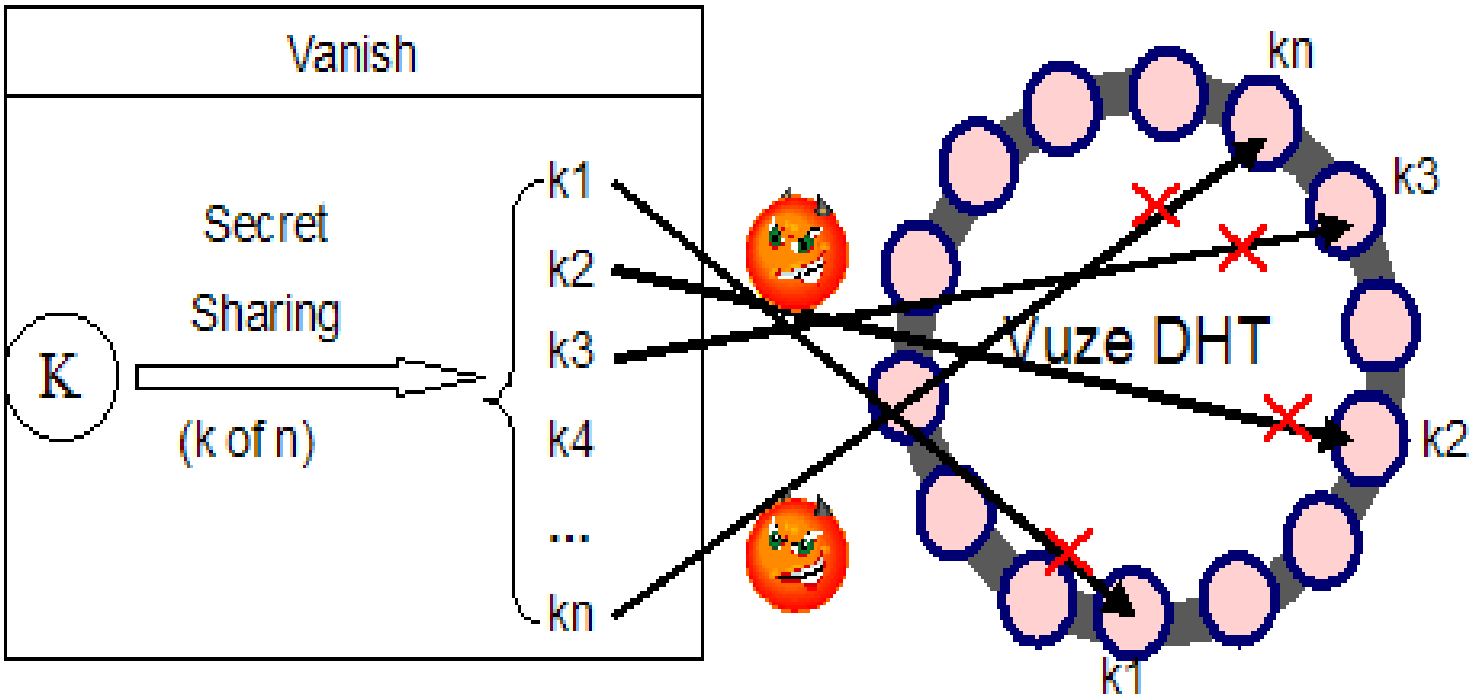


The push operation in the VuzeDHT network.

The hopping process of the malicious nodes in hopping attack.



Motivation: **Sniffing**

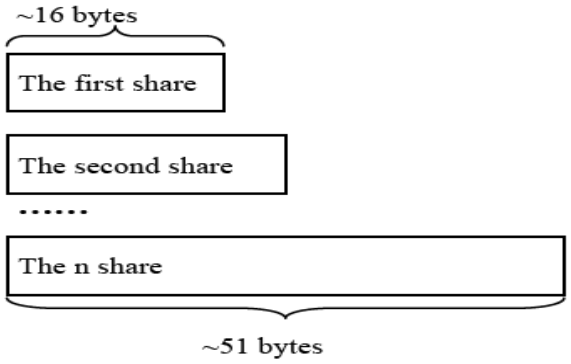


In addition, it's very dangerous for Vanish to transmit key shares that exposed to the network.

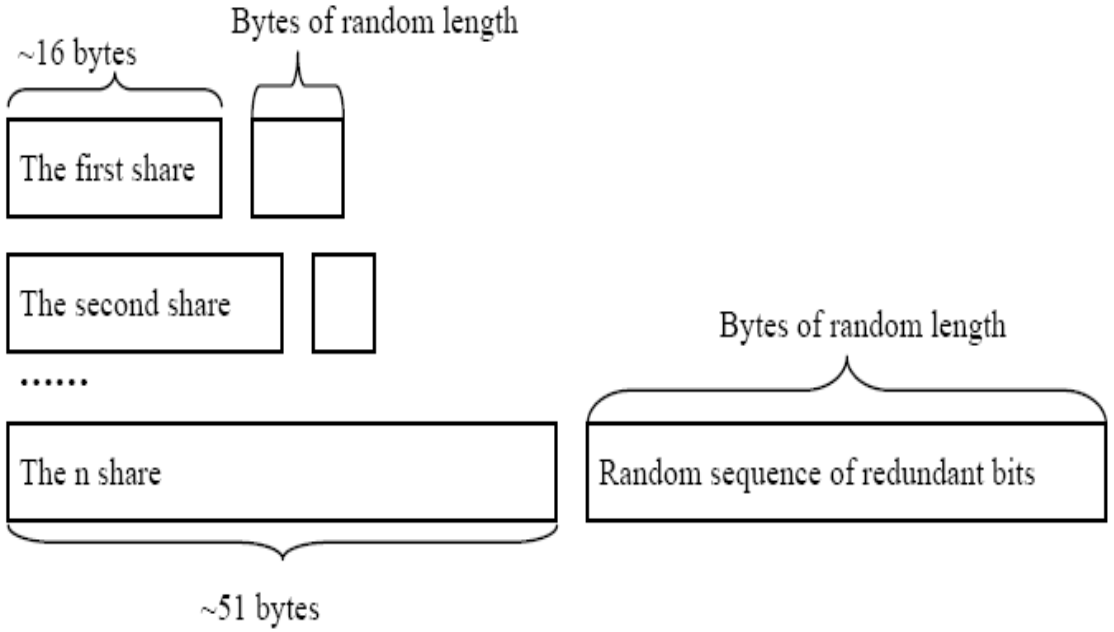
Existing approaches and their shortcomings

- **Increase the Vanish threshold *k* for composing the encryption key**
- **Switching Vanish to a privately hosted DHT**
- **Detect the attacker**
- **Limit the ID distribution mechanism of Vuze**

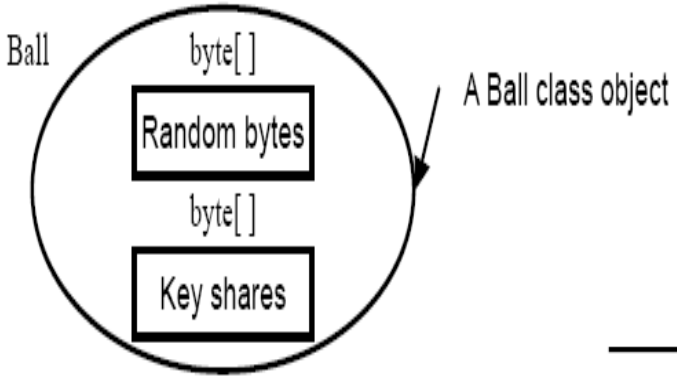
Solution for the hopping attack

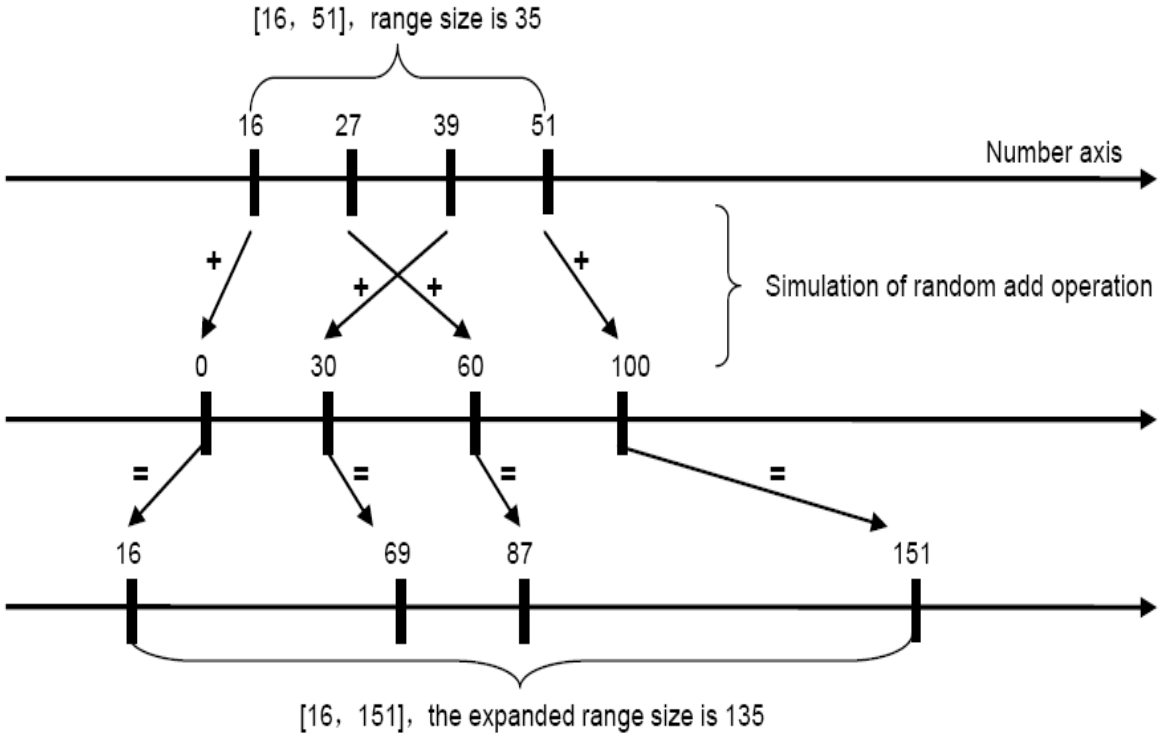


Increasing the length of range of key shares

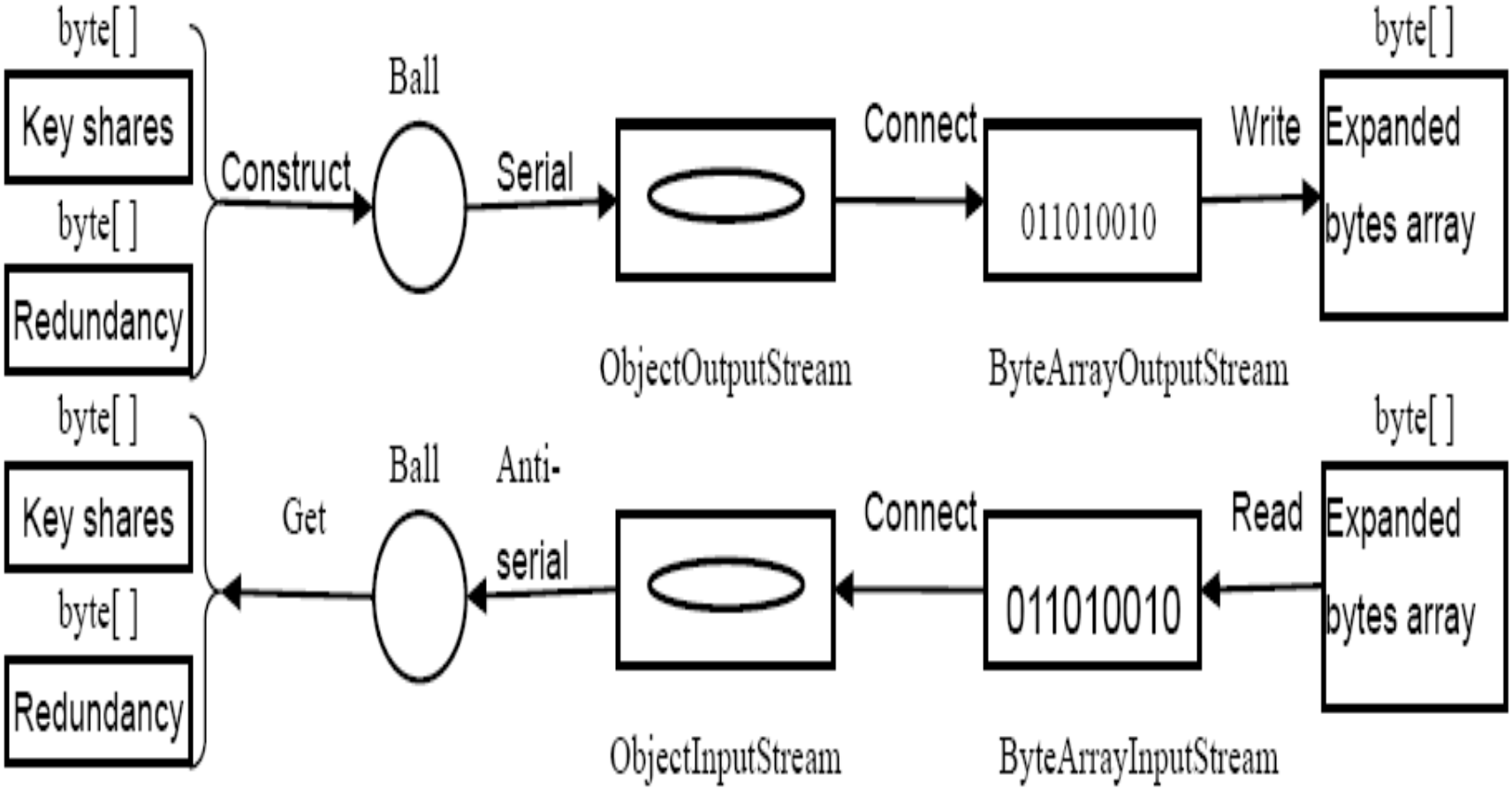


The expanded length range of key shares(1/2)

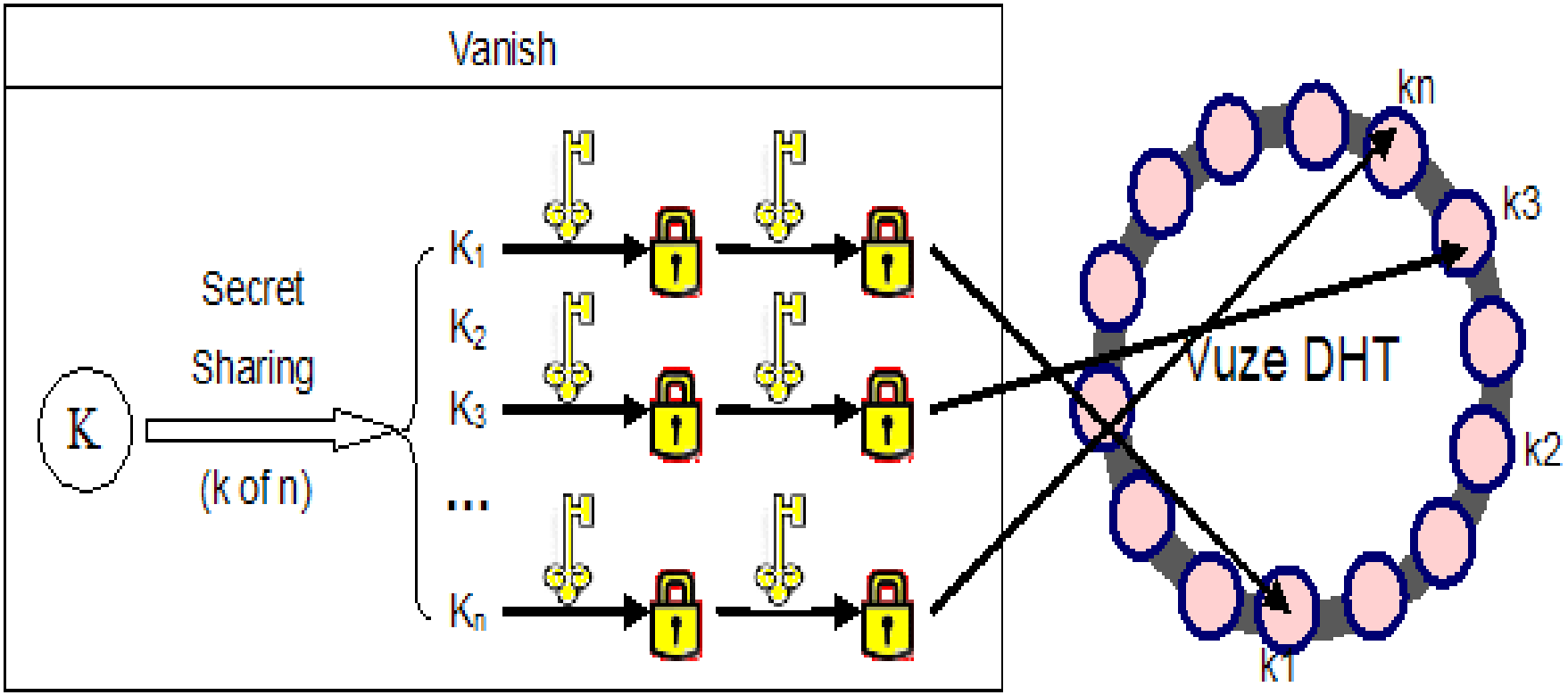




The expanded length range of key shares(2/2)



Solution for the sniffing attack



Using the RSA encryption algorithm

Conclusion

- **Discuss the existing state-of-the-art self-destructing data schemes (Vanish) exhibit fragile for hopping attack and sniffing attack in realistic application.**
- **Propose a new scheme called SafeVanish.**


Thanks!