Searching for Optimal Generalized Winnow Protocol

Donny Kok-Ann Teo and Khoongming Khoo, DSO National Laboratories

In Quantum Key Distribution, there may be errors in the secret shared by Alice and Bob due to quantum noise and eavesdropping by the adversary Eve. Therefore Alice and Bob need to do information reconciliation (IR) to correct the shared secret. A well-known IR protocol is the Winnow protocol based on single-bit parity check and Hamming[7,4,3] error correction code. Alice and Bob divide their N-bit secret into blocks of length 7. Then Alice sends 1-bit parity of each block for Bob to do error detection. When Bob indicates an error in a block, Alice will send the 3-bit Hamming code syndrome of the block to Bob, from which Bob can do error correction. Because not all errors can be corrected in one pass, a permutation is applied to the shared secret and this process is repeated over several passes until all errors are corrected.

We generalize the Winnow protocol by replacing the single-bit parity check and Hamming[7,4,3] code with other error detection and error correction code. And apply our variant scheme on 8192-bit secret strings to see if decoding performance can be improved. We look for codes which can achieve block-decoding error probability of less than 0.001 (i.e. correct more than 999 secret strings of length 8192-bit out of 1000 experiments) by leaking less bits or by using less passes. In the spirit of the Winnow protocol, we will restrict ourselves to small cyclic redundancy code (CRC) for error detection and small [n,k,d]-linear code for error correction (as listed below).

Error Detection: CRC(1+x) [single-bit parity check], CRC($1+x+x^2$), CRC($1+x^2+x^3+x^4$)
Error Correction Code: Hamming[7,4,3], Hamming[15,11,3], Hamming[31,26,3], Golay[23,12,7], BCH[15,5,7], BCH[15,7,5], BCH[31,11,11], BCH[31,16,7]

We simulate generalized winnow for all 3×8=24 combinations for the error detection/correction codes listed above. In the following two tables, we identify for each QBER between 3%-9%, the generalized winnow combination that achieve block-decoding error probability of less than 0.001 by **(a) Leaking the least number of bits** or **(b) Using the least number of passes.**

QBER (%)	Best combination optimizing least leakage		Leakage (%) [Least]	Number of Passes
	Linear Code	CRC type		
3	Hamming[31,26,3]	1+x	37	6
4	Hamming[31,26,3]	1+x	48	7
5	Hamming[15,11,3]	1+x	55	5
6	Hamming[15,11,3]	1+x	67	6
7	Hamming[15,11,3]	1+x	74	6
8	Hamming[7,4,3]	1+x	83	4
9	Hamming[15,11,3]	1+x	95	7
QBER (%)	Best combination optimizing least passes		Leakage (%)	Number of Passes [Least]
	Linear Code	CRC type		
3	Hamming[7,4,3]	1+x	52	3
4	BCH[31,16,7]	$1+x^2+x^3+x^4$	83	3
5	Golay[23,12,7]	$1+x^2+x^3+x^4$	94	3
6	Hamming[7,4,3]	1+x	75	4
7	Hamming[7,4,3]	1+x	79	4
8	Hamming[7,4,3]	1+x	83	4
9	Hamming[15,11,3]	1+x	95	7