Searching for Optimal Generalized Winnow Protocol

DONNY KOK-ANN TEO (DSO NATIONAL LABORATORIES)

KHOONGMING KHOO (DSO NATIONAL LABORATORIES)

Information Reconciliation

- In Quantum Key Distribution, there may be errors in the secret shared by Alice and Bob due to:
  - Quantum noise
  - Eavesdropping by the adversary Eve
- Thus need to do information reconciliation to correct shared secret
- A well known reconciliation protocol is the Winnow protocol

Winnow IR Protocol

1. Shared secret is divided into 7-bit segments
2. A single parity bit from each segment is sent for error detection
3. If parity does not match, 3-bit syndrome of Hamming[7,4,3] code is sent for error correction
4. Shared secret is permuted and steps 2 to 3 is repeated over several passes

Generalized Winnow IR Protocol

- We generalize the Winnow Protocol as follows:
- We replace the Hamming[7,4,3] code with [n,k,d] error correction code.
- We divide the secret string into n-bit segments.
- For each n-bit segment, we replace single-bit parity check with different CRC codes to detect errors before doing error correction.

Generalized Winnow IR Protocol

- We replace the single parity check CRC($1+x$) with other error detection codes:
  - CRC($1+x$), CRC($1+x+x^2$), CRC($1+x^2+x^3+x^4$)

- We replace Hamming[7,4,3] with other error correction codes:
  - 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 $3\times 8=24$ combinations of above detection/correction codes.

Simulation Set-Up

- We correct secret strings of length 8192 bits.
- We repeat the IR experiments 1000 times for each BER between 3% to 9%.
- We look for detection/correction codes that can correct all 8192 bits for ≥ 999 out of 1000 experiments.
- For each BER, we look for optimal codes that
  - Leak the least parity bits
  - Use the least pass

Generalized Winnow Leaking Least Bits

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

Generalized Winnow Using Least Passes

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

Conclusion

- Hamming (15,11,3) with CRC 1+x is the combination to give the least bit leakage for majority (4/7) of the qBERs.
- Hamming (7,4,3) with CRC 1+x is the combination to give the least number of passes for majority (4/7) of the qBERs.
- Since the number of passes is always low(<8), Hamming (15,11,3) with CRC 1+x has the best tradeoff (low leakage, small number of passes) amongst the combinations under test.