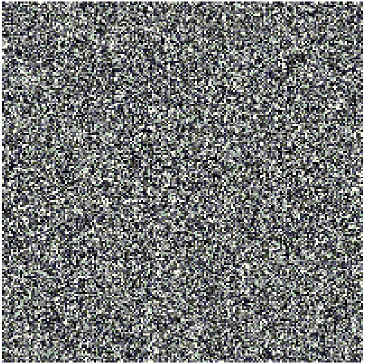
Hiding Signals in Quantum Random Noise

Michael Stephen Fiske
HICSS-58

Aemea Institute

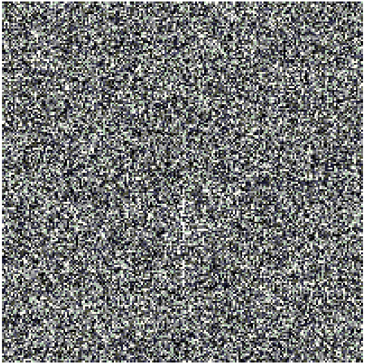
January 9, 2025

A Signal Hidden in Quantum Random Noise



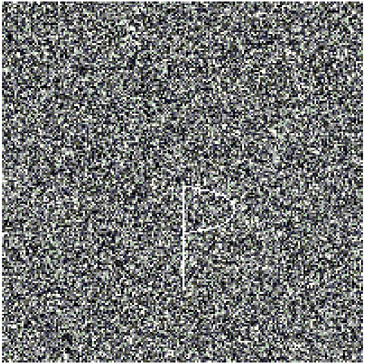
The signal and noise probability distributions are identical.

A Partially Hidden Signal



The signal and noise probability distributions are slightly different.

A Detectable Signal



The signal and noise probability distributions are quite different.

Primary Contributions

Quantum random bits x_i. Heisenberg uncertainty principle.

Axiom 1: *No bias.* $P(x_i = 0) = P(x_i = 1) = \frac{1}{2}$.

Axiom 2: *Independence.* Event $H_i = \{x_1 = b_1, \ldots, x_i = b_i\}$.
Every b_j in $\{0, 1\}$. $P(x_{i+1} = 0 \mid H_i) = P(x_{i+1} = 1 \mid H_i) = \frac{1}{2}$.

- Hiding procedure: $O(n)$ fast, inexpensive, post-quantum.
- If m signal and ρ noise bits satisfy axioms 1 & 2, the signal can be hidden arbitrarily close to perfect secrecy ($\rho \to \infty$).
- A post-quantum key exchange with much smaller key sizes.
- Easy for signal to satisfy axioms 1 & 2. Random keys satisfy axioms 1 & 2. Plaintext: encrypt before hiding or embed signal in higher dimensional Hamming space.

Favorable Properties

- Hiding public keys hinders Mallory-in-the-middle (MITM) attacks that can attack a Diffie-Hellman exchange.
- Search complexity for hidden, public keys substantially exceeds the conjectured complexity of a public key.
- Quantum complexity is comparable to Grover's algorithm. Post-quantum Internet of Things! Less than \$1.00 per device.
- Implementable with TCP/IP infrastructure & an off-the-shelf quantum random number generator (QRNG flip-flop).
- QRNG flip-flops can generate 3.3 Gigabits per second.
- Decentralization. Alice and Bob have their own QRNGs.

Related Work

- In 1550, Cardano proposed a rectangular grid for writing hidden messages. Protection was not adequate.
- Quantum cryptography (Weisner, BB84) relies on the uncertainty principle. When Eve measures a photon's polarization, it destroys the other orthogonal component. Requires polarized photons and special infrastructure to transmit polarized photons. Alice and Bob require a shared authentication secret to stop Mallory interfering with the public channel.
- Quantum secure direct communication (QSDC). QSDC claims advantages over BB84: QSDC is deterministic; every photon contributes a key bit so QSDC is more efficient; QSDC requires expensive quantum hardware and a new physical infrastructure when feasible.

A Simple Hiding Example

Signal $k_1 k_2 k_3 = 001$. $m = 3$.

Noise $r_1 r_2 r_3 r_4 r_5 r_6 r_7 = 10\ 01\ 010$. $\rho = 7$.

Map $(l_1\ \ l_2\ \ l_3) = (8\ 3\ 6)$. $n = 10$. $n = m + \rho$ always holds.

Bit $k_1 = 0$ is hidden at location 8.

Bit $k_2 = 0$ is hidden at location 3.

Bit $k_3 = 1$ is hidden at location 6.

Hidden signal $\mathcal{S}(k_1 k_2 k_3,\ r_1 r_2 r_3 r_4 r_5 r_6 r_7) = 10\ 0\ 01\ 1\ 0\ 0\ 10$.

Creating a Quantum Random Scatter Map

`Input:` n

`Variables:` $n,\ j,\ r,\ t,\ l_1, l_2, \ldots l_n$.

$l_1 := 1 \quad l_2 := 2 \quad \ldots \quad l_n := n \qquad j := n$

`while` $j \geq 2 \quad \{$

`A QRNG randomly chooses` r `in` $\{1, 2, \ldots, j\}$.

$t := l_r$

$l_r := l_j$

$l_j := t$

$j := j - 1$

$\}$

`Output:` $\pi = \left(l_1 \ l_2 \ \ldots \ l_n \right)$

Scatter Map Definitions

Map $\pi = (l_1 \ l_2 \ldots l_n)$. Signal $k_1 \ldots k_m$. Noise $r_1, r_2, \ldots r_\rho$.

Signal Locations $\{l_1 \ l_2 \ \ldots \ l_m\}$.

Noise Locations $\mathcal{N}(l_1 \ l_2 \ \ldots \ l_m) = \{1, \ldots, n\} - \{l_1, l_2, \ldots, l_m\}$.

Define scatter function $\mathcal{S} : \{0,1\}^m \times \{0,1\}^\rho \to \{0,1\}^n$.

$\mathcal{S}(k_1, \ldots, k_m, \ r_1, r_2 \ldots r_\rho) = (s_1, \ldots s_n)$.

Signal bits $s_{l_1} := k_1; \quad s_{l_2} := k_2; \quad \ldots \quad s_{l_m} := k_m$.

Noise bits $s_{i_k} := r_k$. $\ i_k$ is kth smallest number in $\mathcal{N}(l_1 \ldots l_m)$.

Hide a Signal with Scatter Map π

`Input: Signal` $k_1\ k_2\ \ldots\ k_m$. `Map` $\pi = (l_1\ l_2 \ldots l_n)$.

`Alice's QRNG creates noise` $r_1\ r_2\ \ldots\ r_\rho$. $\rho = n - m$.

`Alice's map` π `sets` $s_{l_1} = k_1\ \ldots\ s_{l_m} = k_m$.

`Per` $\mathcal{S}(k_1, \ldots, k_m, r_1, r_2 \ldots r_\rho)$, `Alice fills in` $\mathcal{S} = (s_1 \ldots s_n)$.

`Alice sends` $\mathcal{S}$ `to Bob.`

`Output: Bob's` π `extracts` $k_1\ \ldots\ k_m$ `from` $\mathcal{S}$.

A Random Hidden Nonce Makes π Reusable

- Alice and Bob share π.
- Each transmission uses a distinct hiding map σ.
- Each time Alice's QRNG generates a new random nonce $\mathcal{N}$.
- Alice executes procedure 3 to derive σ from $\mathcal{N}$ & π.
- Alice hides her signal with map σ.
- Alice hides nonce $\mathcal{N}$, using part of π.
- Bob uses part of π to extract nonce $\mathcal{N}$ from the noise.
- Bob executes procedure 3 to derive σ from $\mathcal{N}$ & π.
- Bob uses σ to extracts Alice's signal from the noise.

Procedure 3: Randomly Generating σ

`Inputs:` m, n. $\pi = (l_1 l_2 \dots l_n)$. κ, $\mathcal{N}$, j_0. Ψ is SHA-512.

$q_1 := l_1 \quad q_2 := l_2 \quad \dots \quad q_n := l_n \qquad j := j_0$.

`while` $j \geq 2 \quad \{$

$\quad \kappa := \Psi(\kappa) \oplus \mathcal{R}(\kappa, 8)$

$\quad \mathcal{N} := \Psi(\kappa\, \mathcal{N}) \oplus \mathcal{R}(\mathcal{N}, 8)$

$\quad r := (\mathcal{N} \mod j) + 1$

$\quad t := q_r$

$\quad q_r := q_j$

$\quad q_j := t$

$\quad j := j - 1$

$\}$

`Output:` $\sigma = \big(q_1\ q_2\ \dots\ q_m\big)$.

Procedure 3 Explained at HICSS-58

Mathematical Analysis of a Single Transmission

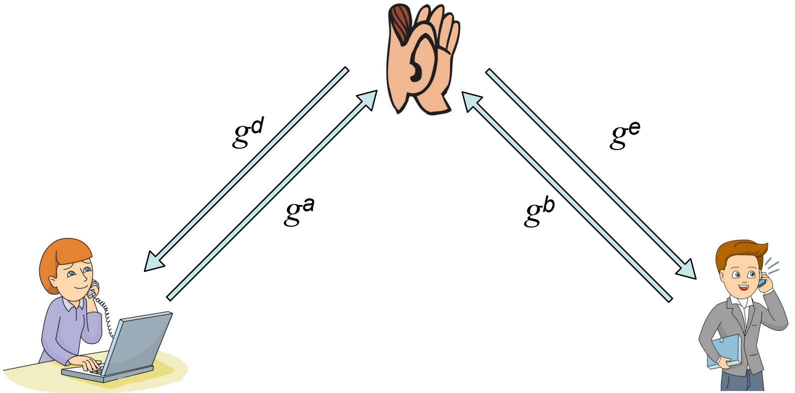
- If an m-bit signal & ρ bits of noise satisfy axiom 1 (unbiased) & axiom 2 (independence), our math proofs show that a one-time transmission $\mathcal{S}$ from Alice to Bob approaches perfect secrecy as ρ increases.
- Perfect secrecy: the probability that a signal $= k_1, k_2, \dots k_m$ before Eve sees $\mathcal{S}$ remains unchanged after Eve sees $\mathcal{S}$.
- If necessary, transform the signal so it satisfies axioms 1 & 2. Good keys automatically satisfy axioms 1 & 2.
- Our proofs rely on the standard normal curve's geometry. A binomial distribution approaches the standard normal curve as $n = m + \rho$ increases. (Central Limit Theorem.)

Hiding Public Keys in Noise

- A new key exchange can hide public keys in noise.
- Hinders MITM attack on a Public Key Exchange. Complexity is too high for Eve.
- Implemented with the 25519 elliptic curve.[1]
- Mallory's complexity is 10^{37} for a naked 25519 public key P. If no auxiliary information, Mallory has no halting criteria.
- Post-quantum. Reduces key sizes. A quantum computer can break naked 25519 public keys in $O(n^2)$ or $O(n^3)$ steps.

[1] D.Bernstein.(2006) "Curve25519: new Diffie-Hellman speed records." *Public Key Cryptography*.LNCS 3958. Springer. 207–228.

Hiding Hinders Mallory in the Middle Attacks



Eve and Alice share secret g^{ad}. Eve and Bob share secret g^{be}.

A Hidden 25519 Elliptic Public Key P

Alice's hidden public key P = 119 179 68 170 227 9 166 162 231 42 145 129 112 181 218 237 103 207 26 200 158 198 149 143 41 87 194 114 11 1 214 24

$\sigma(0) = 1993$. $\sigma(1) = 725$. $\sigma(2) = 405$. $\sigma(3) = 138$. $\sigma(4) = 1825$. $\sigma(5) = 1553$. $\sigma(6) = 213$. $\sigma(7) = 858$.

$n = 2048$. $m = 255$. All signal bits are blue, except first 8 bits are orange. Decimal 119 = 0111 0111

000010100100011111011010101001101000011100100101001010111111011001000101110100001000000100101100010010
1001111111110010000000101000010110111001000000101111001001101110110001111001011010110101101001010111 01
1111001011000101110011011001110011100100101000111111101100101010111101011000011101010011111110110111
0011011100100001001100011111011000101101000110011011110011000100011101101011110011011000101001101001
0100010001001100101111110010111001000111111110011001011111111010010000111000111010110110011100111 1001
0000110000100100010011101100101101011101000011001000000110010110100010100000100100000111111001000101
1010001111111010100100110000010111011101110001110010011011111100000001000100010010110111001111100110
0110101010101011011100011110100000110000111110000111101111101111101110011011110111100011111101110011
1111001001111110101111110001010001101010111111000111000110100010111000100011001111011011011010000010
0100110100110001010001001000111110101111011010100101101010110011000000001011100101101101000111001110

10101101111011000000110010111001110101010000010010010011101110110010000000110111010010100001110000
1011111100100111010000010001110101110111111001101110100000000001001100111001111000100110100010100001 11
0101010110100010100111011000001001111000110111001001100011100001011100111111010110000010001000010 10
0010111111111100111000001010110101011011100100100010110011001111010001001001110101011110111111100110
1101010100100101110011000010001101110110000111011100101100011011101000100111001000111100000000111010 1
1111101101100111011111100111100000001111111100101110111101101100101111111000001001101110010100010 10
0010000001001010110100110010000100000110101111111111011101111101110110111011110000110011101100011001
111001100110000000000010111000001100001100101110000111100110110000111101001111000000111100110101 1001
01100001011010110110010001000100100010111111010111011000000110111111010111100001000011111110000001 10
1100110100100001011010110010000001001001110101110011111101110101100010101100100011001001101111001110
11001111111100110011110110101110010010100010 1110

Complexity of Finding a 25519 Elliptic Public Key P

σ determines where P is hidden.

A random nonce hidden in the noise unpredictably changes σ each time. (Entropy Invariance.)

Every possible σ is uniformly reachable from π, based on Diehard testing of Procedure 3.

Eve knowing where P was hidden in a prior hidden transmission reveals nothing about the location of the new P.

Since there are more than 255 0s and 1s of noise, every public key P in $\{0,1\}^{255}$ is possible.

Stops MITM attack: If Eve doesn't know π, Eve must test every possible P. That won't work.

Statistical Testing of 25519 Public Keys & QR Noise

Statistical testing helps verify 25519 public keys (signal) and quantum random noise satisfy axioms 1 & 2.

do 80 million times {

a QRNG creates a 25519 private key κ.

compute public 25519 key $\mathcal{P}$ from κ.

write κ to noise_control_file.txt

for each bit b_i in byte j of $\mathcal{P}$

write bit b_i in byte_j_bit_i.txt }

Diehard tests on byte_j_bit_i.txt look for statistical anomalies in the ith bit of the jth byte of 25519 public keys.

Every file byte_j_bit_i.txt passed all 13 Diehard tests.

Relevance to Quantum Computing

- N unsorted databased items. Classical algorithm $O(\frac{N}{2})$ steps.
- Grover's quantum algorithm takes $O(\sqrt{N})$ steps.
- Grover's algorithm requires a terminating condition.
- Scatter maps in $\mathcal{L}_{(m,n)}$ correspond to N database items.
- Eve has a terminating condition for scatter maps only if Eve has auxiliary information about σ after the scatter.
- Conjectured complexity is $O\left(\sqrt{\frac{n!}{(n-m)!}}\right)$ if Eve has a terminating condition.
- $\sqrt{\frac{8192!}{(8192-255)!}} > 10^{498}$ for $m = 255$ & $n = 8192$.

Research Summary

- A procedure hides a signal in quantum random noise.
- The locations of the signal bits randomly change each time.
- Security of the hidden signal can be made arbitrarily close to perfect secrecy.
- A new key exchange hides public keys in noise.
- Diehard tests verified that the probability distribution of 25519 public keys satisfy axioms 1 & 2.
- Our hiding procedure can be implemented with TCP/IP infrastructure and an inexpensive, off-the-shelf QRNG.
- If a quantum computer can solve *NP* hard lattice problems in $O(n^2)$ or $O(n^3)$, some of NIST's crypto is vulnerable.

Factorial Growth vs. Exponential Growth

Set $r(n) = \frac{n!}{2^n}$.

$$\log(r(n)) = \log(n!) - \log(2^n) = \sum_{k=2}^{n} \log(k) - n\log(2).$$

```
[julia> factorial(4)
24

[julia> 2^4
16

[julia> function r(n)
[       r = factorial(big(n) ) / 2^(big(n))
[       return r
[       end
r (generic function with 1 method)

[julia> r(4)
1.5

[julia> factorial(4) / 2^4
1.5

[julia> r(100)
7.362140279596095642145348079335098603605904786041407178165622553205507320042596e+127

[julia> r(1000)
3.755333903791443599585571559542306426775894026657514769644025241443938219420678e+2266
```

Future Work & Research

Future work should explore an Internet of Things (IoT) implementation due to being low cost and post-quantum.

Based on Grover's algorithm, we anticipate Eve's quantum complexity is $O\left(\sqrt{\frac{n!}{(n-m)!}}\right)$ when m signal bits are hidden in $n-m$ noise bits and signal and noise satisfy axioms 1 & 2.

Future research should explore variations of Grover's algorithm to further analyze the quantum complexity of our key exchange hidden in noise.