# Hiding Signals in Quantum Random Noise

Michael Stephen Fiske
Aemea Institute
mf@aemea.org

## Abstract

*An $O(n)$ procedure for hiding $m$ bits of signal inside of $n - m$ bits of quantum random noise is introduced. When a signal and quantum noise have a uniform probability distribution, and the signal size is fixed, the security of one hidden signal transmission can be made arbitrarily close to perfect secrecy. Our hiding procedures are implemented with commercially available quantum random number generators, and current TCP/IP infrastructure. A random nonce unpredictably changes bit locations of the signal: a prior hidden signal transmission does not reveal information to Eve on where the current signal is hidden. This security property enables a new key exchange that hides public keys in quantum randomness; introduces a post-quantum key exchange with substantially smaller key sizes; offers a substantially greater classical complexity than the underlying public keys; and provides quantum complexity that is comparable to Grover's quantum computing algorithm.*

**Keywords:** Grover's algorithm, hide, key exchange, perfect secrecy, quantum complexity, quantum random.

## 1. Introduction

In information security, a fundamental problem is for a sender, Alice, to securely transmit a message $M$ to a receiver, Bob, so that the adversary, Eve, receives no information about the message. In Shannon's seminal paper (Shannon, 1949), his model assumes that Eve has complete access to a public, noiseless channel: Eve sees an identical copy of ciphertext $C$ that Bob receives, where $C(M, K)$ is a function of message $M$ lying in message space $\mathcal{M}$ and secret key $K$ lying in key space $\mathcal{K}$. Expressed as conditional probabilities, Shannon defined a cryptographic method to be perfectly secret if probablity $P(M) = P(M \mid \texttt{Eve sees ciphertext } C)$ for every cipher text $C$ and for every message $M$ in a message space $\mathcal{M}$. In other words, Eve has no more information about message $M$ after Eve sees ciphertext $C$ pass through the public channel. For a noiseless, public channel, Shannon proved the entropy of the keyspace $\mathcal{K}$ must be at least as large as message space $\mathcal{M}$ to achieve perfect secrecy with his cryptographic model.

A scatter map procedure is introduced that hides a signal inside of noise, created by a quantum random number generator (QRNG) (Herrero, 2017). A QRNG's randomness relies upon the Heisenberg uncertainty principle (Heisenberg, 1927). Our methods assume the QRNG obeys randomness axioms 1 and 2. Most, if not all, of the QRNGs in (Herrero, 2017), passed statistical tests that validate axioms 1 and 2.

**Axiom 1.** *No bias.* For each $i$, outcome $x_i$ of bit sequence $(x_1x_2x_3\dots)$, measured and created by a source of randomness, has probabilities $P(x_i = 1) = P(x_i = 0) = \frac{1}{2}$.

**Axiom 2.** *Independence.* For each $i$, outcome $x_i$ is independent of its history. No correlation exists between distinct outcomes. Conditional probability $P(x_i = a \mid x_1 = b_1, \dots, x_{i-1} = b_{i-1}) = \frac{1}{2}$ for all $a, b_j$ in $\{0, 1\}$.

A fundamental contribution proves that if an $m$-bit signal and $\rho$ bits of noise satisfy axioms 1 and 2, the signal can be hidden arbitrarily close to perfect secrecy, as $\rho \to \infty$. The closeness to perfect secrecy can be efficiently computed. Another contribution is a post-quantum key exchange with much smaller key sizes.

If the signal is plaintext $M$, then encrypt $M$ before hiding so that the encrypted plaintext has a uniform probability distribution on message space $\mathcal{M}$. If the signal is a cryptography key $K$, then transforming $K$ should not be necessary because choosing $K$ from keyspace $\mathcal{K}$ should already satisfy axioms 1 and 2.

Our methods offer the following advantages:

- Our hiding procedure takes on the order of $n$ computational steps, where $m$ signal bits are stored in memory, and $\rho = n - m$ noise bits are generated by a QRNG and stored in memory. Some QRNGs generate random bits at rates that exceed three gigabits per second (Keshavarzian, 2023).

URI: https://hdl.handle.net/10125/109705
978-0-9981331-8-8

• A scatter map can be reused when a signal and noise obey axioms 1 & 2; and for each transmission, new noise, a new signal and a new nonce are used. A practical method of hiding public keys hinders man-in-the-middle (MITM) attacks during a Diffie-Hellman (Diffie, 1976) exchange of public keys (Merkle, 1975). Our hidden key exchange can be complemented with a short authentication string (SAS) (Vaudenay, 2005) so that Alice and Bob can detect a MITM. For large $\rho$, the complexity of searching for hidden, public keys can substantially exceed the conjectured computational complexity of a public key. The quantum complexity is comparable to Grover's quantum algorithm that performs database search (Grover, 1996).

• A noiseless, public channel is used that can be implemented with TCP/IP infrastructure, and commercially available QRNGs. Quantum random flip-flop circuits (Keshavarzian, 2023), that generate 3.3 gigabits per second, can be manufactured in high volume for substantially less than one US dollar. In contrast, quantum hardware that performs BB84 (Bennett, 1984) requires an expensive, special fiber optics infrastructure and endpoint devices that create polarized photons. An endpoint device (Lowndes, 2021) with short range, that is too large for an Iphone or an IoT device (Greengard, 2021), costs over $600. Traditional fiber optics cable costs $15k to $60k per mile for underground installation and $10k to $25k per mile for aerial installation (Foster, 2024).

• Alice and Bob possess their own QRNGs. Decentralization eliminates single points of failure in quantum hardware (Jain, 2014) that Alice and Bob do not control.

## 2. Related Work

Cardano (Cardano, 1550) proposed a rectangular grid for writing hidden messages. Apertures in a grille reveal the hidden message. Various implementations have not provided adequate protection due to inadequate sources of randomness and *not using identical probability distributions for the signal and noise*.

Conceived by Weisner (Weisner, 1969), quantum cryptography is based on the uncertainty principle, and was eventually published in (Bennett, 1984) (BB84). By measuring one component of a photon's polarization, Eve irreversibly loses the ability to measure the orthogonal component of the polarization. The irreversibility of Eve's observation and the attainment of perfect secrecy is quite elegant. Alice and Bob must share a preestablished authentication secret to assure that Mallory cannot corrupt messages about the polarization bases, communicated on a public channel. Quantum cryptography requires an expensive physical infrastructure built across vast distances (Townsend, 1993).

In (Bennett, 1988), an unconditionally secure secret key agreement uses noise, and builds upon BB84. A more general information-theoretic model is introduced in (Maurer, 1993) that suggests how to build provably secure cryptographic systems. Alice and Bob establish a secret key across a noisy channel, modelled by probability distributions for Alice, Bob, and Eve. Eve can listen as a passive eavesdropper. When Mallory is tampering with the public channel, Alice and Bob must share a preestablished authentication key to address an active attack. An implementation is not specified.

Quantum secure direct communication (QSDC) (Deng, 2004) was introduced in (Beige, 2001). QSDC claims some advantages over BB84: QSDC is deterministic; every photon contributes a key bit so QSDC is more efficient; and no information is revealed to a potential eavesdropper. QSDC will require expensive quantum hardware and a new physical infrastructure, when feasible.

## 3. Math Notation & Definitions

$\mathbb{N}$, $\mathbb{N}^+$, and $\mathbb{Z}$ are the natural numbers $\{0, 1, 2, \dots\}$, positive natural numbers, and integers, respectively. If $A \subset X$, define $X - A = \{x \texttt{ in } X : x \texttt{ is not in } A\}$. $f : X \to Y$ is a function with domain $X$ and range $Y$. For $f : \mathbb{N} \to \mathbb{N}$ and input $n$ in $\mathbb{N}$, a procedure $\mathcal{A}$ is called $O\big(f(n)\big)$ if there exist constants $C$ and $M$ such that $\mathcal{A}$'s number of computational steps is $\leq Cf(n)$ whenever $n \geq M$. Factorial $! : \mathbb{N} \to \mathbb{N}^+$ is $0! = 1$ and for $n \in \mathbb{N}^+$, $n! = n * (n-1)!$. If $n \geq m$, $\binom{n}{m} = \frac{n!}{m!\,(n-m)!}$. Define $\lfloor x \rfloor = \sup\{n \in \mathbb{Z} : n \leq x\}$.

$\kappa\mathcal{N}$ concatenates bit strings $\kappa$ and $\mathcal{N}$. $A \oplus B$ is bitwise exclusive-or between $A$ and $B$; if necessary, trailing 0's are concatenated to the shorter string. If $A = a_n\ a_{n-1} \dots a_2\ a_1$, then $|A| = n$. $\mathcal{R}(A, 8)$ rotates $A$ by 8 bits to the right, so $\mathcal{R}(A, 8) = a_8\ a_7 \dots a_1\ a_n\ a_{n-1} \dots a_9$. $\{0,1\}^n$ is the set of all bit strings of length $n$. $|A|$ is the number of elements in set $A$. $|\{0,1\}^n| = 2^n$. The number of 1's in bit string $b_1 \dots b_k$ is $\eta_1(b_1 \dots b_k)$. For example, $\eta_1(0101) = 2$.

Probability distribution $P$ is uniform on $\{0,1\}^n$ if and only if $P(\{b_1 \dots b_n\}) = \frac{1}{2^n}$ for all bit strings $b_1 \dots b_n$. $P(A \mid B)$ is the conditional probability that event $A$ occurs given that it is known that event $B$ occurred. $P(A \mid B) = \frac{P(A \cap B)}{P(B)}$. Events $A$ and $B$ are independent if and only if $P(A \cap B) = P(A)\ P(B)$.

## 4. Scatter Map Hiding

A scatter map stores each bit of signal at a distinct location inside the noise. A location space is defined.

**Definition 1.** *Let $m, n \in \mathbb{N}$, where $m \leq n$. Define an $(m, n)$ location space as* $\mathcal{L}_{m,n} = \{(l_1\ l_2\ \ldots\ l_m)\ \texttt{in}\ \{1, 2, \ldots, n-1, n\}^m : l_j \neq l_k\ \texttt{if}\ j \neq k\}$.

**Remark 1.** $|\mathcal{L}_{m,n}| = \frac{n!}{(n-m)!}$ elements.

**Definition 2.** *Let $(l_1\ l_2\ \ldots\ l_m)$ be in $\mathcal{L}_{m,n}$. Define $(l_1\ l_2\ \ldots\ l_m)$'s noise locations as* $\mathcal{N}(l_1\ l_2\ \ldots\ l_m) = \{1, 2, \ldots, n-1, n\} - \{l_i : 1 \leq i \leq m\}$.

**Definition 3.** *Scatter Map*
*Let $(l_1\ \ldots\ l_n)$ be in $\mathcal{L}_{n,n}$. Thus, $(l_1 \ldots l_m)$ is in $\mathcal{L}_{m,n}$. Define scatter map $\mathcal{S} : \{0,1\}^m \times \{0,1\}^{n-m} \to \{0,1\}^n$ as $\mathcal{S}(k_1, \ldots, k_m,\ r_1, r_2 \ldots r_{n-m}) = (s_1, \ldots s_n)$ with signal locations $s_{l_1} = k_1;\ s_{l_2} = k_2;\ \ldots\ s_{l_m} = k_m$. For each $k$ in $1 \leq k \leq n-m$, set $s_{i_k} = r_k$ such that $i_k$ is the $k$th smallest number in $\mathcal{N}(l_1 \ldots l_m)$.*

**Example 1.** Signal $k_1k_2k_3 = 001$. $m = 3$. Noise $r_1 \ldots r_7 = 1001010$. $(l_1l_2l_3) = (8\ 3\ 6)$. $n = 10$. 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. Scatter map $\mathcal{S}(k_1k_2k_3, r_1r_2r_3r_4r_5r_6r_7) = 1000110010$.

An initial scatter map $\pi$ is generated by procedure 1.

**Procedure 1.** *Quantum Random Scatter Map $\pi$*

Inputs: $m, n$ with $m \leq n$.
Variables: $j, r, t,\ l_1, l_2, \ldots l_n$.
$l_1 := 1 \quad l_2 := 2 \quad \ldots \quad l_n := n \qquad j := n$
while $j \geq 2$ {
  a QRNG randomly chooses $r$ in $\{1, 2, \ldots, j\}$
  $t := l_r$
  $l_r := l_j$
  $l_j := t$
  $j := j - 1$
}
Output: $\pi = (l_1\ l_2\ \ldots\ l_n)$ in $\mathcal{L}_{n,n}$.

**Procedure 2.** *Hiding a Signal with Scatter Map $\pi$*

Input: Signal $k_1\ k_2 \ldots k_m$. Scatter map $\pi$
Alice's QRNG creates noise $r_1\ r_2 \ldots r_\rho$.
Alice's map $\pi$ sets $s_{l_1} = k_1\ \ldots\ s_{l_m} = k_m$.
Per defn. 3, Alice fills in $\mathcal{S} = (s_1 \ldots s_n)$.
Alice sends $\mathcal{S}$ to Bob.
Output: Bob's $\pi$ extracts $k_1 \ldots k_m$ from $\mathcal{S}$.

Procedure 3 enhances procedure 2, by creating a dynamic hidden channel $\sigma$ for Alice to hide her signals.

**Procedure 3.** *Random Hidden Nonce Scatter Map*

Inputs: $m, n$ & $m \leq n$. $\pi = (l_1l_2 \ldots l_n)$. $\kappa$, $\mathcal{N}$, $j_0$.
$q_1 := l_1 \quad q_2 := l_2 \quad \ldots \quad q_n := l_n \qquad j := j_0$.
while $j \geq 2$ {
  $\kappa := \Psi(\kappa) \oplus \mathcal{R}(\kappa, 8)$
  $\mathcal{N} := \Psi(\kappa\, \mathcal{N}) \oplus \mathcal{R}(\mathcal{N}, 8)$
  $r := (\mathcal{N} \mod j) + 1$
  $t := q_r$
  $q_r := q_j$
  $q_j := t$
  $j := j - 1$
}
Output: $\sigma = (q_1\ q_2 \ldots q_m)$.

$\sigma$ is created from authentication key $\kappa$, nonce $\mathcal{N}$ initial map $\pi = (l_1l_2 \ldots l_n)$, and $j_0 = n - |\mathcal{N}|$. Alice and Bob share $\mathcal{N}$, $\pi$, and $\kappa$. $\Psi$ is a one-way hash function, e.g. SHA-512 (Lilly, 2004). Procedure 3 is similar to procedure 1, except index $r$ is selected by the first 3 steps in the while loop, and the initial permutation is $\pi$. For $M = \min\{|\psi(\kappa\mathcal{N})|, |\mathcal{N}|\}$, $n < 2^M$ is recommended.

Procedure 3 makes procedure 4 powerful because nonce $\mathcal{N}$ is hidden from Eve and $\sigma$ randomly changes each time Alice executes procedure 4. Hence, procedure 4 is reusable. Alice and Bob share $\pi = (l_1l_2 \ldots l_n)$, created by procedure 1. Alice computes $\sigma$ from $\mathcal{N}$, key $\kappa$, and $\pi$. $\sigma$ hides Alice's $m$-bit signal. Alice's $\pi$ hides $\mathcal{N}$ at bit locations $l_{n-|\mathcal{N}|+1}, \ldots l_n$ .

**Procedure 4.** *Hiding a Signal with Random Map $\sigma$*

Input: Signal $k_1 \ldots k_m$. Map $\pi$. Key $\kappa$.
Alice's QRNG creates noise $r_1\ r_2 \ldots r_\rho$.
Alice's QRNG creates random nonce $\mathcal{N}$.
Procedure 3 computes $\sigma$ on $\pi, \mathcal{N}, \kappa, j_0 = n - |\mathcal{N}|$.
Alice's $\sigma$ hides $k_1, \ldots k_m$ at $s_{q_1}, s_{q_2}, \ldots s_{q_m}$.
Alice's $\pi$ hides $\mathcal{N}$ at $l_{n-|\mathcal{N}|+1}, \ldots l_n$.

Alice stores $r_1 \ldots r_\rho$ in $\mathcal{S} = (s_1 \ldots s_n)$.
Alice sends $\mathcal{S}$ to Bob.
Bob receives $\mathcal{S}$ from Alice.
Bob's $\pi$ extracts $\mathcal{N}$ at $l_{n-|\mathcal{N}|+1}, \ldots l_n$.

Procedure 3 computes $\sigma$ on $\pi, \mathcal{N}, \kappa, j_0 = n - |\mathcal{N}|$.
Bob extracts $k_1 \ldots k_m$ from $\mathcal{S}$ with $\sigma$.

The algorithms in procedures 1, 2, 3, and 4 are $O(n)$. Alice and Bob can also establish the signal size as a shared secret. Section 5 assumes Eve knows $m$.

In regard to analyzing procedure 4, sections 5 and 8 address: *What can Eve infer about a hidden signal after seeing one transmission?* Theorem 4 and section 8 cover: *What can Eve infer about $\pi$ after seeing multiple transmissions where a distinct $\sigma$ hides each signal?*[1]

[1] Theorem 4 uses conditional entropy to answer this question.

## 5. Math Analysis of One Transmission

Assuming that Eve has no information about map $\pi$, we analyze how much Eve can infer about a signal after Eve sees $\mathcal{S} = (s_1, \ldots, s_n)$. If Alice hides an $m$-bit signal in $\rho$ bits of noise, before Eve sees $\mathcal{S}$, all $m$-bit signals are equally likely: $P(k_1 = b_1, \ldots, k_m = b_m) = \frac{1}{2^m}$ for all $(b_1, \ldots b_m)$ in $\{0,1\}^m$. After Eve sees $\mathcal{S}$, conditional probability $P(k_1 = b_1, \ldots, k_m = b_m \mid \texttt{Eve sees } \mathcal{S})$ can be distinct from $\frac{1}{2^m}$.

Overall, our results follow from the geometry of a uniform binomial distribution. For $n$ fair Bernoulli trials, the standard deviation equals $\frac{\sqrt{n}}{2}$. For a constant signal size $m$ and any constant $c > 0$, the central limit theorem (Feller, 1958) implies the middle section of the binomial distribution, that approaches the normal curve on the interval $[\frac{n}{2} - \frac{c\sqrt{n}}{2}, \frac{n}{2} + \frac{c\sqrt{n}}{2}]$, flattens and spreads out as the noise size $\rho$ increases. Due to this geometric effect, after Eve observes $\mathcal{S} = (s_1, \ldots, s_n)$, her conditional probabilities, with respect to Alice's $m$-bit hidden signal hidden in noise, approach $\frac{1}{2^m}$ as $\rho \to \infty$.

Define $E_{i,n} = \{w \in \{0,1\}^n : \eta_1(w) = i\}$, where $0 \le i \le n$. $E_{0,4} = \{0000\}$, $E_{1,4} = \{0001, 0010, 0100, 1000\}$, $E_{2,4} = \{0011, 0101, 0110, 1001, 1010, 1100\}$, $E_{3,4} = \{0111, 1011, 1101, 1110\}$ and $E_{4,4} = \{1111\}$. Hence, $|E_{k,n}| = \binom{n}{k}$.

The *ith element* of $E_{k,n}$ refers to ordering set $E_{k,n}$ according to an increasing sequence of natural numbers that each bit string represents and selecting the $i$th element. The 3rd element of $E_{2,4}$ is 0110.

In table 1, $k_i$ and $r_i$ are the $i$th bits of the signal and noise, respectively. Signal event $B_{i,j}$ is the $i$th element in $E_{j,m}$. Noise event $R_i$ is the set of noise elements containing $i$ ones with noise size $\rho = n - m$. Event $A_i$ is a scatter $(s_1 \ldots s_n)$ that contains $i$ ones.

Table 1: Eve sees $(m, n)$ scatter $\mathcal{S} = (s_1 \ldots s_n)$

| Event | Probability | Description |
|---|---|---|
| $B_{i,j}$ | $\frac{1}{2^m}$ | $i$th $k_1 k_2 \ldots k_m$ in $E_{j,m}$ |
| $R_i$ | $\frac{\binom{\rho}{i}}{2^\rho}$ | $\eta_1(r_1 r_2 \ldots r_\rho) = i$ |
| $A_i$ | $\frac{\binom{n}{i}}{2^n}$ | $\eta_1(s_1 \ldots s_n) = i$ |

$R_k$ refers to noise and $B_{l,j}$ refers to signal, so $R_k$ and $B_{l,j}$ are independent. If $0 \le k \le \rho$, $0 \le j \le m$ and $1 \le l \le \binom{m}{j}$, then $P(R_k \cap B_{l,j}) = P(R_k) \cap P(B_{l,j})$. If $0 \le j \le \min\{k, m\}$ and $1 \le l \le \binom{m}{j}$, $P(A_k | B_{l,j}) = P(R_{k-j}) = \frac{\binom{\rho}{k-j}}{2^\rho}$. The prior equation follows from table 1; $\eta_1(s_1 \ldots s_n) = \eta_1(r_1 \ldots r_\rho) + \eta_1(k_1 \ldots k_m)$; and the definition of conditional probability.

A finite sample space and $P(\bigcup_{j=0}^{m} \bigcup_{l=1}^{|E_{j,m}|} B_{l,j}) = 1$ imply that each event $A_k \subset \bigcup_{j=0}^{m} \bigcup_{l=1}^{|E_{j,m}|} B_{l,j}$. Also, $B_{l_1,j_1} \cap B_{l_2,j_2} = \emptyset$ whenever $l_1 \ne l_2$ or $j_1 \ne j_2$ such that $0 \le j_1, j_2 \le m$ and $1 \le l_1 \le E_{j_1,m}$ and $1 \le l_2 \le E_{j_2,m}$. A derivation of equation (5.1), that uses Bayes law (Bayes, 1764), precedes definition 4.

Whenever $0 \le j \le \min\{k, m\}$ and $1 \le l \le \binom{m}{j}$,

$$P(B_{l,j} | A_k) = \frac{\binom{\rho}{k-j}}{\sum_{b=0}^{\min\{k,m\}} \binom{m}{b}\binom{\rho}{k-b}}. \tag{5.1}$$

$$\begin{aligned} P(B_{l,j} | A_k) &= \frac{P(B_{l,j}) P(A_k | B_{l,j})}{\sum_{b=0}^{\min\{k,m\}} \sum_{a=1}^{|E_{b,m}|} P(B_{a,b}) P(A_k | B_{a,b})} \\ &= \frac{P(A_k | B_{l,j})}{\sum_{b=0}^{\min\{k,m\}} \sum_{a=1}^{|E_{b,m}|} P(A_k | B_{a,b})} \\ &= \frac{\binom{\rho}{k-j} 2^{-\rho}}{\sum_{b=0}^{\min\{k,m\}} |E_{b,m}| \binom{\rho}{k-b} 2^{-\rho}}. \end{aligned}$$

**Definition 4.** *Let $c$ be a positive integer. $\sigma : \mathbb{N} \to \mathbb{N}$ is called a $c$-standard deviations function if there exists $N_\sigma \in \mathbb{N}$ such that $\rho \ge N_\sigma$ implies $|\sigma(\rho) - \frac{\rho}{2}| \le c\frac{\sqrt{\rho}}{2}$*

Define function $h_c(\rho) = \max\{0, \frac{\rho}{2} - \lfloor c\frac{\sqrt{\rho}}{2} \rfloor\}$. Then $h_c$ is a $c$-standard deviations function. Lemmas 1 and 2 help to prove theorem 1. In the proofs, math expressions assume $\rho$ is larger than $N_\sigma$ in definition 4.

**Lemma 1.** Let $\sigma : \mathbb{N} \to \mathbb{N}$ be a $c$-standard deviations function. Then $\lim_{\rho \to \infty} \frac{\binom{\rho}{\sigma(\rho)-1}}{\binom{\rho}{\sigma(\rho)}} = 1$.

PROOF. $\frac{\binom{\rho}{\sigma(\rho)-1}}{\binom{\rho}{\sigma(\rho)}} = \frac{\sigma(\rho)}{\rho - \sigma(\rho) + 1}$. $\sigma(\rho)$ is a $c$-standard deviations function, so $\frac{\rho}{2} - \frac{c\sqrt{\rho}}{2} \le \sigma(\rho) \le \frac{\rho}{2} + \frac{c\sqrt{\rho}}{2}$. Thus, $\frac{\rho}{2} + \frac{c\sqrt{\rho}}{2} + 1 \ge \rho - \sigma(\rho) + 1 \ge \frac{\rho}{2} - \frac{c\sqrt{\rho}}{2}$.

Divide corresponding expressions.[2] Hence,

$$\frac{\frac{\rho}{2} - \frac{c\sqrt{\rho}}{2}}{\frac{\rho}{2} + \frac{c\sqrt{\rho}}{2} + 1} \le \frac{\binom{\rho}{\sigma(\rho)-1}}{\binom{\rho}{\sigma(\rho)}} \le \frac{\frac{\rho}{2} + \frac{c\sqrt{\rho}}{2}}{\frac{\rho}{2} - \frac{c\sqrt{\rho}}{2}}. \tag{5.2}$$

[2] $\sqrt{\rho} > c$ must hold to assure $\frac{\rho}{2} - \frac{c\sqrt{\rho}}{2} > 0$. For a fixed $c$, eventually $\sqrt{\rho} > c$ holds as $\rho \to \infty$.

Apply the squeeze theorem to the previous inequalities since $\lim_{\rho\to\infty} \frac{\frac{\rho}{2}-\frac{c\sqrt{\rho}}{2}}{\frac{\rho}{2}+\frac{c\sqrt{\rho}}{2}+1} = \lim_{\rho\to\infty} \frac{\frac{\rho}{2}+\frac{c\sqrt{\rho}}{2}}{\frac{\rho}{2}-\frac{c\sqrt{\rho}}{2}} = 1.$ ■

Lemma 1 helps to prove lemma 2.

**Lemma 2.** Fix $m \in \mathbb{N}$. Let $\sigma : \mathbb{N} \to \mathbb{N}$ be a $c$-standard deviations function. For any $b, j$ such that $0 \le b, j \le m$, then $\lim_{\rho\to\infty} \frac{\binom{\rho}{\sigma(\rho)-j}}{\binom{\rho}{\sigma(\rho)-b}} = 1$.

PROOF. For $c+1$ standard deviations, carry out a similar computation as the inequalities, labeled (5.2). For a large enough $\rho$, $\sigma(\rho)-b$ and $\sigma(\rho)-j$ lie within $c+1$ standard deviations. If $i$ satisfies $0 \le i \le m$, then $\lim_{\rho\to\infty} \frac{\binom{\rho}{\sigma(\rho)-i-1}}{\binom{\rho}{\sigma(\rho)-i}} = 1$. WLOG, suppose $j < b$. Hence, $\lim_{\rho\to\infty} \frac{\binom{\rho}{\sigma(\rho)-j}}{\binom{\rho}{\sigma(\rho)-b}} = \lim_{\rho\to\infty} \frac{\binom{\rho}{\sigma(\rho)-j}}{\binom{\rho}{\sigma(\rho)-(j+1)}} \lim_{\rho\to\infty} \frac{\binom{\rho}{\sigma(\rho)-(j+1)}}{\binom{\rho}{\sigma(\rho)-(j+2)}} \cdots \lim_{\rho\to\infty} \frac{\binom{\rho}{\sigma(\rho)-(b-2)}}{\binom{\rho}{\sigma(\rho)-(b-1)}} \lim_{\rho\to\infty} \frac{\binom{\rho}{\sigma(\rho)-(b-1)}}{\binom{\rho}{\sigma(\rho)-b}} = 1.$ ■

**Theorem 1.** Fix signal size $m \in \mathbb{N}$. Let $c \in \mathbb{N}$. Let $\sigma : \mathbb{N} \to \mathbb{N}$ be a $c$-standard deviations function. Then $\lim_{\rho\to\infty} P(B_{l,j} \mid A_{\sigma(\rho)}) = \frac{1}{2^m}$.

PROOF. From equation (5.1), $\lim_{\rho\to\infty} P(B_{l,j} \mid A_{\sigma(\rho)}) = \lim_{\rho\to\infty} \frac{\binom{\rho}{\sigma(\rho)-j}}{\sum_{b=0}^{\min\{\sigma(\rho),m\}} \binom{m}{b}\binom{\rho}{\sigma(\rho)-b}} = \lim_{\rho\to\infty} \frac{\binom{\rho}{\sigma(\rho)-j}}{\sum_{b=0}^{m} \binom{m}{b}\binom{\rho}{\sigma(\rho)-b}}$ since $m$ is fixed and $\rho \to \infty$ implies $\sigma(\rho) > m$. Lastly, $\lim_{\rho\to\infty} \frac{\binom{\rho}{\sigma(\rho)-j}}{\sum_{b=0}^{m} \binom{m}{b}\binom{\rho}{\sigma(\rho)-b}} = \frac{1}{2^m}$ is derived from the binomial identity $\sum_{b=0}^{m} \binom{m}{b} = 2^m$ and lemma 2. ■

**Remark 2.** Theorem 1 is not applicable when a function of $\rho$ stays on or near the boundary of Pascal's triangle. Consider $\lim_{\rho\to\infty} \frac{\binom{\rho}{0}}{\binom{\rho}{1}} = 0$ or $\lim_{\rho\to\infty} \frac{\binom{\rho}{1}}{\binom{\rho}{2}} = 0$. The math validates common sense: if Eve sees event $A_0$, then Eve knows that Alice's signal is all 0s. Fortunately, a practical and large enough noise size enables procedures 2 and 4 to effectively hide the signal transmission so that outliers such as $A_0, A_1$ are extremely unlikely. For example, when $n = 2048$, $P(A_0) = 2^{-2048}$ and $P(A_1) = 2^{-2037}$. Note $2^{2048} > 10^{500}$; this event won't happen in our lifetime. If an outlier event occurs, Alice can generate new random noise and hide the signal in that second generation of noise.

Definitions 5, 7 and theorems 2, 3 provide a basis for calculating how big the noise size should be in order to establish an extremely low probability that Eve will see outlier events such as $A_0$.

**Definition 5.** *$f : \mathbb{N} \to \mathbb{N}$ is an binomial $\epsilon$-tail function if there exists $N \in \mathbb{N}$ such that $n \ge N$ implies that* $2^{-n}\left(\sum_{k=0}^{f(n)} \binom{n}{k} + \sum_{k=n-f(n)}^{n} \binom{n}{k}\right) < \epsilon$.

The area under the standard normal curve from $-\infty$ to $x$ is expressed as $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{1}{2}t^2} dt$.

**Theorem 2.** For each $c \in \mathbb{N}$, set $\epsilon_c = 4\Phi(-c)$. The function $g_c(n) = \max\{0, \lfloor \frac{n}{2} - c\frac{\sqrt{n}}{2} \rfloor\}$ is a binomial $\epsilon_c$-tail function.

PROOF. This is an immediate consequence of the central limit theorem, applied to the binomial distribution. Some details are provided below.

Define $B_n(x) = 2^{-n} \sum_{k=0}^{\lfloor x \rfloor} \binom{n}{k}$. In (Moivre, 1738), de Moivre proved for each fixed $x$ that $\lim_{n\to\infty} B_n(\frac{n}{2} + x\frac{\sqrt{n}}{2}) = \Phi(x)$. Thus, $\lim_{n\to\infty} 2^{-n} \sum_{k=0}^{g_c(n)} \binom{n}{k} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{-c} e^{-\frac{1}{2}t^2} dt$. Now $\epsilon_c$ is four times the value of $\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{-c} e^{-\frac{1}{2}t^2} dt$, which verifies that $g_c$ is a binomial $\epsilon_c$-tail function. ■

Definition 6 helps to analyze example 2.

**Definition 6.** *Let $m$ be the signal size. The secrecy ratio of conditional probability $P(B_{l,j} \mid A_k)$ is defined as $\frac{P(B_{l,j} \mid A_k)}{2^{-m}}$. When Eve's conditional probability $P(B_{l,j} \mid A_k)$ equals $2^{-m}$, the secrecy ratio = 1.*

**Example 2.** This example provides some perspective on some $\epsilon$-tails and Eve's conditional probabilities. For $n = 2500$, the scatter mean $\mu$ is 1250 and the standard deviation $\sigma = \frac{\sqrt{2500}}{2} = 25$. Set $c = 20$, so $\mu - c\sigma = 750$. A calculation shows that $2^{-2500} \sum_{j=0}^{750} \binom{2500}{j} < 10^{-91}$. For $n = 4096$, the scatter mean is 2048 and the standard deviation $\sigma = 32$. Set $c = 50$ standard deviations, so $\mu - c\sigma = 448$. A calculation shows that $2^{-4096} \sum_{j=0}^{448} \binom{4096}{j} < 10^{-621}$.

Some of Eve's conditional probabilities are calculated for $n = 2500$ and signal size $m = 576$. The

average number of 1's in a signal is $\mu_m = 288$ and the standard deviation $\sigma_m = 12$.

A typical case is when $j = 300$ and $k = 1275$, which are both one standard deviation to the right of the signal mean and scatter mean, respectively. From equation (5.1), a computer calculation shows that the secrecy ratio is $\frac{P(B_{l,300} \mid A_{1275})}{2^{-576}} \approx 1.576$, so $2^{-576} < P(B_{l,300} \mid A_{1275}) < 2^{-575}$.

A rare event is when $j = 228$ and $k = 1225$. That is, $j = 228$ is five standard deviations to the left of $\mu_m$ and $k = 1225$ is one standard deviation to the left of the scatter mean. A calculation shows that secrecy ratio $\frac{P(B_{l,228} \mid A_{1225})}{2^{-576}} \approx 0.526$. Thus, $2^{-577} < P(B_{l,228} \mid A_{1225}) < 2^{-576}$.

A rare event occurs when $j = 228$ and $k = 1125$. Event $A_{1125}$ is four standard deviations to the left. Secrecy ratio $\frac{P(B_{l,228} \mid A_{1125})}{2^{-576}} \approx 3840$. Thus, $2^{-565} < P(B_{l,228} \mid A_{1125}) < 2^{-564}$. While a secrecy ratio of 3840 is quite skew, it still means that even if Eve sees a scatter transmission four standard deviations to the left, there is still a probability in the interval $[2^{-565}, 2^{-564}]$ of Alice's signal being the event $B_{l,228}$. These secrecy ratio calculations motivate definition 7.

**Definition 7.** *Let $\epsilon > 0$. Eve's conditional probabilities $P(B_{l,j} \mid A_{\sigma(\rho)})$ are $\epsilon$-close to perfect secrecy if there exists a binomial $\epsilon$-tail function $f$ such that for any function $\sigma : \mathbb{N} \to \mathbb{N}$ satisfying $f(\rho) \leq \sigma(\rho) \leq \rho - f(\rho)$, then $\lim_{\rho \to \infty} P(B_{l,j} \mid A_{\sigma(\rho)}) = 2^{-m}$.*

**Theorem 3.** For any $\epsilon > 0$, there exists $M \in \mathbb{N}$ such that $\epsilon_c < \epsilon$ for all $c \geq M$ and $c \in \mathbb{N}$. Furthermore, function $g_c$ is a binomial $\epsilon_c$-tail function that makes Eve's conditional probabilities $P(B_{l,j} \mid A_{\sigma(\rho)})$ $\epsilon_c$-close to perfect secrecy, where $g_c(\rho) \leq \sigma(\rho) \leq \rho - g_c(\rho)$.

PROOF. Since $\lim_{x \to \infty} \Phi(-x) = 0$, there exists $M \in \mathbb{N}$ such that $\epsilon_c < \epsilon$ for all $c \geq M$. Recall that $h_c(\rho) = \max\{0, \frac{\rho}{2} - \lfloor c\frac{\sqrt{\rho}}{2} \rfloor\}$. For all $\rho \in \mathbb{N}$, $|g_c(\rho) - h_c(\rho)| \leq 1$ and $g_c(4\rho^2) - h_c(4\rho^2) = 0$. This fact and $h_c$ is a $c$-standard deviations function together imply that lemma 2 and theorem 1 also hold for function $g_c$. That is, $\lim_{\rho \to \infty} P(B_{l,j} \mid A_{g_c(\rho)}) = 2^{-m}$. Whenever function $\sigma$ satisfies $g_c(\rho) \leq \sigma(\rho) \leq \rho - g_c(\rho)$, this implies $\sigma$ is a $c + 1$-standard deviations function. Thus, theorem 3 follows from theorems 1, 2 and from definition 7. ■

## 6. Visual Intuition of Effective Hiding

A critical assumption in section 5 motivates the following. When Eve has no information about scatter map $\pi$ and after Eve observes multiple hidden signal transmissions, a key goal is to determine what Eve can learn about $\pi$. A hiding procedure's effectiveness depends upon an observation: When Eve *executes an algorithm to search for a signal in the noise*, how can her search algorithm know if it found a signal?

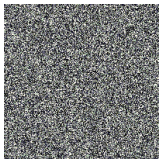

**Fig. 1.** A Hidden Signal in Random Noise

The pixels of the secret signal are hidden in the noise of the visual image such that the probabilities of the pixel values satisfy the two randomness axioms: this explains why the secret signal in Fig. 1 is undetectable by the human eye.

Suppose Eve performs a brute-force search over all $\frac{n!}{(n-m)!}$ possibilities for scatter map $\pi$. Even if Eve's search method stumbles upon the correct sequence of bit locations, Eve's method has no basis for distinguishing the signal from the noise because the signal and noise probability distributions are equal.

Unless Eve obtains useful auxiliary information about $\pi$, Eve does not have a terminating condition for halting with a sequence of bit locations hiding the signal despite that $\pi$ is a linear map from $m$ bits of signal and $n - m$ bits of noise onto $\{0,1\}^n$. (A permutation of $m$ bits of signal and $n - m$ bits of noise onto $\{0,1\}^n$ can be represented by an $n \times n$ matrix of 0's and 1's.)

**Fig. 2.** Two Biased Hidden Signals

In Fig. 2, Eve can obtain some bit locations of the secret signal because the probability distribution of the signal (foreground) is not the same as the noise (background). Eve can determine the signal is located in a 'P' shape, because the probability distribution of the pixel values is not uniform.

## 7. Hiding Public Keys in Noise

A Diffie-Hellman exchange is vulnerable to man-in-the-middle (MITM) attacks (Geary, 2009). To address MITM attacks and increase computational complexity, procedures 5 and 6 hide public keys during a key exchange between Alice and Bob. We assume Alice and Bob have previously established secret scatter map $\pi = (l_1, l_2 \ldots l_n)$ and authentication key $\kappa$. Alice and Bob may establish $\pi$ and $\kappa$ with a prior (distinct) Diffie-Hellman exchange, where their public keys are signed in a secure computing environment; or they establish $\pi$ and $\kappa$ via a private channel or a one-time use of QSDC when it is commercially available.

Let $h_\kappa$ be a MAC function – e.g., HMAC (Bellare, 1996) or (Wegman, 1981) – implemented with SHA-512. $h_\kappa$ is used to authenticate a scattered transmission. $h_\kappa$ hinders the following attack by Eve: An active Eve (Mallory) can flip a bit at location $l$ in a scattered transmission. If Alice and Bob don't authenticate, then Eve gains information about bit location $l$ when Alice resends a scattered transmission.

**Procedure 5.** *Hide a Public Key with a Public Nonce*

Alice's QRNG creates private key $K$.
Alice computes public key $P = p_1 \ldots p_m$.
Alice's QRNG creates noise $r_1\, r_2 \ldots r_\rho$.
Alice's QRNG creates a random nonce $\mathcal{N}$.
Procedure 3 computes $\sigma$ on $\pi$, $\kappa$, $\mathcal{N}$, $j_0 = n$.
Alice sets $s_{q_1} = p_1 \ldots s_{q_m} = p_m$ with $\sigma$.
Alice fills in $\mathcal{S} = (s_1 \ldots s_n)$ with $r_1 \ldots r_\rho$.
Alice sends $\mathcal{S}, \mathcal{N}$ and $h_\kappa(\mathcal{NS})$ to Bob.
Bob receives $\mathcal{S}', \mathcal{N}'$ and $h_\kappa(\mathcal{NS})$ from Alice.
Bob compares $h_\kappa(\mathcal{N}'\mathcal{S}')$ and $h_\kappa(\mathcal{NS})$.

if $h_\kappa(\mathcal{N}'\mathcal{S}')$ is valid {
  Procedure 3 computes $\sigma$ on $\pi$, $\kappa$, $\mathcal{N}$, $j_0 = n$.
  Bob extracts $p_1 \ldots p_m$ with $\sigma$. }
else { Bob rejects $\mathcal{S}'$.
  Alice resends $\mathcal{S}, \mathcal{N}$ and $h_\kappa(\mathcal{NS})$. }

In procedure 5, Alice hides her public key using random nonce $\mathcal{N}$. When Bob sends his public key to Alice, their roles are swapped in procedures 3 and 5. Bob executes the same steps as Alice and Alice executes the same steps as Bob. For example, Bob creates a random nonce instead of Alice before sending his nonce.

**Procedure 6.** *Hide a Public Key with a Hidden Nonce*
Procedure 6 is similar to procedure 5. The main difference is that Alice executes procedure 4, where Alice's public key $P$ is her signal, and $m = |P|$. Also, when Bob authenticates the scattered transmission $\mathcal{S}'$ received from Alice, he compares $h_\kappa(\mathcal{S}')$ and $h_\kappa(\mathcal{S})$ instead of comparing $h_\kappa(\mathcal{N}'\mathcal{S}')$ and $h_\kappa(\mathcal{NS})$. ■

Let $(X, P)$ be a probability space, $P(X) = 1$. If event $A = \{a_1, \ldots a_N\} \subset X$ is a finite set, $A$'s entropy is defined $H(A) = -\sum_{i=1}^{N} P(a_i) \log_2 P(a_i)$. If event $B = \{b_1, \ldots b_M\}$, define conditional entropy $H(B \mid a_i) = -\sum_{j=1}^{M} P(b_j \mid a_i) \log_2 P(b_j \mid a_i)$. Define conditional entropy $H(B \mid A) = \sum_{i=1}^{N} P(a_i)\, H(B \mid a_i)$.

**Theorem 4.** *Entropy Invariance of Procedure 4*
Suppose a QRNG generating the noise and random nonce $\mathcal{N}$ and the signal satisfy axioms 1 and 2. Suppose $\mathcal{N}$ is hidden with procedure 4, and $\pi = (l_1 \ldots l_m\ l_{m+1} \ldots l_n)$. If the first 3 steps inside the while loop in procedure 3 randomly select $r$ with a uniform distribution on $\{1, 2, \ldots, j\}$ for each $j$ where $1 \le j \le n$, then $H(\pi) = H(\pi \mid$ Eve sees $\mathcal{S}(1), \ldots, \mathcal{S}(k))$.

PROOF Outline. Since $r$'s selection is uniformly distributed, based on $\kappa$ and $\mathcal{N}$, $\sigma$ is randomly selected by procedure 3, with a uniform distribution. (Section 8 discusses Diehard tests on index $r$'s distribution.) For each scattered transmission $\mathcal{S}(k)$ seen by Eve, $\mathcal{N}$ is randomly generated and hidden from Eve. Eve gains no information about $\pi$ as every $\sigma$, in a space isomorphic to $\mathcal{L}_{m,n-|\mathcal{N}|}$, is uniformly reachable. ■

In a software implementation of procedures 5 and 6, public keys are generated from elliptic curve 25519 (Bernstein, 2006). Some definitions are needed. A byte is in $\{0, 1, \ldots, 255\}$. For $c$ in $\{0, 1, \ldots, 2^{256}-1\}$, $c \to \underline{c}$ is a little-endian bijection $\underline{c} = (c \bmod 256, \lfloor \frac{c}{256} \rfloor \bmod 256, \ldots, \lfloor \frac{c}{256^{31}} \rfloor \bmod 256)$ (a 32-byte string). Public 25519 keys are defined as $\mathcal{P}_{25519} = \{0, 1, \ldots, 255\}^{32}$. In procedure 5 or 6, $m = 255$ and the first 8 bits $p_1 \ldots p_8$ in $\mathcal{P}$ correspond to the first byte in $\{0, 1, \ldots, 255\}^{32}$; bits $p_9 \ldots p_{16}$ in $\mathcal{P}$ correspond to the second byte in $\{0, 1, \ldots, 255\}^{32}$; and so on. The most significant bit is not hidden since the last byte is in $\{0, 1, \ldots, 127\}$.

A scattered transmission has size $n = 8192$ bits. $m = 255$ bits is the signal size. Noise size $\rho = n - m = 7937$. Per $\sigma = (q_1, q_2 \ldots q_m)$ in procedure 5, the $k$th bit of $\mathcal{P}$ is stored in bit location $q_k$. Private 25519 keys are randomly selected from $S_{25519} = \{0, 8, 16, \ldots 248\} \times \{0, 1, \ldots 255\}^{30} \times \{64, 65, \ldots, 127\}$. $|S_{25519}| = 2^{251}$. Algorithm $\mathcal{A}$ computes $\mathcal{A} : S_{25519} \times \mathcal{P}_{25519} \to \mathcal{P}_{25519}$.

Procedures 5 and 6 have a useful property. Alice and Bob can communicate a SAS (Vaudenay, 2005) before a subsequent encrypted communication via a different channel. For example, Alice and Bob can verify a 4 to 5 word SAS with a phone speaker. By sending a SAS on a different channel, Alice and Bob can detect if Eve

knows $\pi$.

Let $a$ be Alice's private key and $b$ be Bob's private key. Let $e_1, e_2$ be Eve's private keys. During a MITM, Eve computes $\mathcal{A}\big(e_1, \mathcal{A}(a,9)\big)$ with Alice. Eve computes $\mathcal{A}\big(e_2, \mathcal{A}(b,9)\big)$ with Bob. When Alice and Bob verify their SAS, $\mathcal{A}\big(e_1, \mathcal{A}(a,9)\big) \neq \mathcal{A}\big(e_2, \mathcal{A}(b,9)\big)$ holds with high probability. Consequently, $h_\kappa(\mathcal{A}\big(e_1, \mathcal{A}(a,9)\big)) \neq h_\kappa(\mathcal{A}\big(e_2, \mathcal{A}(b,9)\big))$ holds with high probability. Section 9 shows that if Eve doesn't know $\pi$, her complexity is much greater than a 25519 public key's conjectured complexity (Bernstein, 2006), which is $2^{128}$.

If a SAS helps to detect a MITM on a Diffie-Hellman exchange, why hide the public keys in noise? SAS and *hiding public keys in random noise* are complementary. SAS isn't effective if Eve uses unforeseen techniques: the security of a standard Diffie-Hellman exchange relies upon an abelian group's complexity. For example, a quantum algorithm (Proos, 2003) can break the 25519 curve in time O($n^2$) or O($n^3$), depending on the quantum hardware. They estimate a 1000 qubit computer can break a 160 bit elliptic curve.

## 8. Statistical Testing of Public 25519 Keys

Diehard tests (Marsaglia, 1995) were performed on random public 25519 keys to assure that the math theory in section 5 covers procedures 5 and 6. A public key is computed by applying algorithm $\mathcal{A}$ to a randomly generated 25519 private key. Diehard tests determine if a public key's bits statistically satisfy axioms 1 and 2.

The following steps generated 255 files of test data.

```
do 80 million times  {
  randomly generate a 25519 private key κ.
  compute public 25519 key P from κ.
  for each bit b_i in byte  k of P
     write bit b_i in byte_k_bit_i.txt   }
```

Each of these 255 files (e.g., `byte_31_bit_5.txt`) contains 10 million bytes of data. For each test file, every random 25519 private key, was created by a QRNG (Stipčević, 2016), called by C function `int qrng(uchar* private_key, int num_bytes)`.

Our tests also generated 10 MB control files, by calling function `qrng(private_key, 32)` 312,500 times and writing each 32 byte private key to a file.

Thirteen Diehard tests were applied to each of the 255 test files with filenames `byte_k_bit_i.txt`, where $0 \leq k \leq 31$ and $0 \leq i \leq 7$, excluding $k = 31$ and $i = 7$. The 13 Diehard tests are (1) Birthday Spacings. (2) Ranks of 31×31 and 32×32 Matrices. (3) Ranks of 6×8 Matrices. (4) Monkey Tests on 20-bit Words. (5) Monkey Tests OPSO, OQSO, DNA. (6) Count the 1's in a Stream of Bytes. (7) Count the 1's in Specific Bytes. (8) Parking Lot Test. (9) Minimum Distance Test. (10) Random Spheres Test. (11) Squeeze Test. (12) Runs Test. (13) Craps Test. The Overlapping Permutations and Overlapping Sums tests were omitted: physicist Robert Brown observed that overlapping bit sequences are not independent and the weak inverses of covariance matrices have implementation errors (Brown, 2015).

Diehard tests on file `byte_k_bit_i.txt` look for statistical anomalies in the ith bit of the kth byte of 25519 public keys. The control files and the 255 files passed the 13 Diehard tests. The Diehard tests did not find any statistically significant differences between the control files and each of the 255 files `byte_k_bit_i.txt`. For $\Psi$ = SHA-512, Diehard tests on the first 3 steps inside the while loop of procedure 3 showed a uniform distribution of index $r$ on $\{1, 2, \ldots, n\}$ for $n = 8192$ with nonce sizes $|\mathcal{N}| = \{128,\ 256,\ 512,\ 1024,\ 2048,\ 4096, 8192\}$. (For $n = 8192$, nonce size $|\mathcal{N}| \geq 512$ is recommended.)

## 9. Discussion of Testing and Complexity

Two assumptions below help assure that information is not unnecessarily leaked to Eve.

**Assumption 1.** *New Noise and New Signal*

For each scattered transmission, it is assumed that Alice creates a new signal $k_1 \ldots k_m$ and new noise $r_1 \ldots r_{n-m}$ from a QRNG that both satisfy randomness axioms 1 and 2.

**Assumption 2.** *No Auxiliary Information*

During the $k$th scattered transmission $\mathcal{S}(k)$, it is assumed that Eve only observes $\mathcal{S}(k)$. Eve receives no auxiliary information from Alice or Bob.

Suppose 255 bits of the 25519 public key $\mathcal{P}$ are hidden inside of 7937 bits of noise. (Byte 31's most significant bit is always 0, so 255 bits are hidden.) Then the scatter size $n = 8192$ bits. There are 8192 possible locations to hide the first bit of $\mathcal{P}$; 8191 locations to hide the second bit of $\mathcal{P}$; ...; and 7938 locations to hide the 255th bit of $\mathcal{P}$. Hence, the scatter map complexity is $|\mathcal{L}_{255,8192}| > 10^{997}$. The brute-force complexity of a 25519 private key is $2^{254} \approx 10^{77}$. The complexity of hiding 255 bits of public key in 7937 bits of noise exceeds the complexity of a 25519 private key by more than 919 orders of magnitude.

If Eve does not receive any auxiliary information, Diehard tests show that it is extremely unlikely that Eve can extract any information about the bit locations even after observing 80 million public keys. For Eve to launch a MITM attack on the key exchange in procedure 5 or procedure 6, she must know $\sigma$ in $\mathcal{L}_{255,8192}$.

If Alice and Bob encrypt their subsequent

communication with symmetric cryptography in a distinct channel that Eve does not have access to, then the statistics from the Diehard tests suggest that Eve will never be able to find any of the bit locations of $\sigma \in \mathcal{L}_{255,8192}$. Even if Eve has enough computing power to brute-force search[3] each element $\sigma \in \mathcal{L}_{255,8192}$ and subsequently find public key $\mathcal{P}$, Eve still has no way of knowing if this particular $\sigma$ is the scatter map that Alice and Bob used. If there are at least 255 ones and 255 zeroes in the scattered transmission $\mathcal{S}(k)$, every possible public key can be hidden in $\mathcal{S}(k)$.

Eve requires auxiliary information to execute an attack on this hidden key exchange. In many practical cases, Alice and Bob use the same channel to perform their encrypted communication so Eve will be able to observe this encrypted communication. We examine what Eve can accomplish when assumption 2 is violated.

Following Kerckhoff's principle, assume that Eve knows Alice and Bob's symmetric cryptography algorithms and the algorithm that derives the symmetric key(s) from the key exchange in procedure 5. Assume that Eve can break the symmetric cryptography algorithms and find the symmetric key $s$ used for that particular encrypted communication between Alice and Bob. After this, Eve must also search for Alice's private key $a$ and Bob's private key $b$ such that $\mathcal{A}\big(b, \mathcal{A}(a, 9)\big) = s$. This search has a complexity of at least $2^{251}$ because the size of private key space $S_{25519} = 2^{251}$; for each public key $\mathcal{P} \in \mathcal{P}_{25519}$, the map $\mathcal{A}(x, \mathcal{P})$ is 1-to-1 on $S_{25519}$; and $s$ is a constant for this search. If SHA-512 derives the symmetric cryptography key(s) from the shared secret established by procedure 5 then Eve must also execute a preimage attack on SHA-512.

Our complexity estimate is simplified by assuming that Eve knows public key $\mathcal{P}$ hidden in the noise. A simplified complexity $\mathcal{C}$ for Eve assumes that she can directly eliminate possibilities from $\mathcal{L}_{(m,n)}$.[4]

Let $\mathcal{S}(k)$ be the $k$th transmission that hides public key $\mathcal{P}$. Let $m_0$ be the number of 0's in $\mathcal{P}$ that Eve knows. Let $m_1$ be the number of 1's in $\mathcal{P}$. Let $\eta_0$ be the number of 0's in $\mathcal{S}(k)$. Let $\eta_1$ be the number of 1's in $\mathcal{S}(k)$. $m = m_0 + m_1$ and $n = \eta_0 + \eta_1$. Then Eve reduces her simplified complexity $\mathcal{C}$ from $|\mathcal{L}_{(m,n)}|$ to $\frac{\eta_0!}{(\eta_0 - m_0)!}$ $\frac{\eta_1!}{(\eta_1 - m_1)!}$. If $\eta_0 = 0$ or $\eta_1 = 0$, then $\mathcal{C} = |\mathcal{L}_{(m,n)}|$.

Consider outlier event $\mathcal{S}(k)$ containing 8192 zeroes. (In practice this will not happen.) Eve knows Alice's public key, but Eve obtains no additional information about $\sigma$ and hence none about $\pi$. Thus, $\mathcal{C} = |\mathcal{L}_{(m,n)}|$.

[3]Quantum computing is currently unrealistic as $\frac{8192!}{7937!} > 10^{997}$.

[4]This assumption is conservative. Eve's elimination of elements in $\mathcal{L}_{m,n}$ is not expected to be effective against procedures 4, 5 and 6 because in each transmission a new nonce $\mathcal{N}$ randomly changes $\sigma$.

At the other extreme, assume that the $2i$ (even) bits in $\mathcal{S}(k)$ are 0 and the $2i - 1$ (odd) bits are 1, where $1 \leq i \leq 4096$. Assume that all the bits in public key $\mathcal{P}$ are 1, which minimizes Eve's complexity. When Eve knows $P = 1^{255}$, this implies $\mathcal{C}(\mathcal{P}) = \frac{4096!}{3841!}$.[5]

Even after Eve's overcomes the complexity of capturing symmetric cryptography key $s$ and the search complexity of private key space $S_{25519}$, a lower bound for Eve's complexity $\mathcal{C}$, to achieve a MITM, is $\frac{4096!}{3841!} > 10^{917}$. If Eve uses auxiliary information for $n = 8192$, Eve's complexity to obtain $\pi$ substantially exceeds the conjectured complexity of a 25519 public key.

## 10. Relevance to Quantum Computing

Eve's goal of searching for bit locations of a hidden signal is related to Grover's goal of using a quantum computer to speed up database search. In (Grover, 1996), Grover states: "The problem is this: there is an unsorted database containing $N$ items out of which just one item satisfies a given condition - that one item has to be retrieved. Once an item is examined it is possible to tell whether or not it satisfies the condition in one step. However, there does not exist any sorting on the database that would aid its selection. The most efficient classical algorithm for this is to examine the items in the database one by one. If an item satisfies the required condition stop; if it does not, keep track of this item so that it is not examined again."

One item in Grover's database corresponds to one scatter map in $\mathcal{L}_{m,n}$. That is, $N$ database items correspond to $\frac{n!}{(n-m)!}$ scatter maps. Grover states that his algorithm has to tell whether a database item satisfies a condition. Section 6 observed that without auxiliary information Eve has no way of determining whether a sequence of bit locations is $\pi$. A quantum algorithm search requires auxiliary information so that it can test for a condition on each prospective scatter map.

Grover's algorithm has a quantum complexity of $O(\sqrt{N})$, when there are $N$ items in the database. Classical Turing machine algorithms have a database search complexity of $O(\frac{N}{2})$. Based on the correspondence between scatter map and database search, we propose: If Eve's quantum search algorithm has an adequate terminating condition that does not compromise a scatter map's bit locations, then Eve's conjectured quantum complexity is $O\big(\sqrt{\frac{n!}{(n-m)!}}\big)$. If $(m, n) = (255, 8192)$, then Eve's conjectured quantum complexity is $\sqrt{\frac{8192!}{(8192-255)!}} > 10^{498}$.

[5] $\frac{4096!}{3841!}$ is the number of possible ways to hide $\mathcal{P} = 1^{255}$ in $\mathcal{S}(k)$.

## 11. Summary & Future Research

A procedure that hides a signal in quantum random noise was introduced. We proved that when the signal and noise satisfy axioms 1 and 2 the security of the hidden signal can be made arbitrarily close to perfect secrecy, by increasing the noise size. A key exchange was proposed that hides public keys in noise. Diehard tests verified that the probability distribution of the public keys validated axioms 1 and 2. Our hiding methods can be implemented with TCP/IP infrastructure and an inexpensive, off-the-shelf QRNG.

Based on a correspondence with Grover's quantum algorithm, if Eve has a terminating condition for finding a secret scatter map in $\mathcal{L}_{m,n}$, our conjecture is that Eve's quantum complexity is $O\left(\sqrt{\frac{n!}{(n-m)!}}\right)$, where $n-m$ is the noise size and $m$ is the signal size. Future research should explore variations of Grover's algorithm to further analyze the quantum complexity of our key exchange hidden in noise.

## Acknowledgments

We thank the peer reviewers for their helpful comments. We thank Joanne Mary Gomez. We thank Mario Stipčević for generating random data from his quantum random flip-flop.

## References

S.M. Barnett. (2011) *Quantum Information*. Oxford Press.

T. Bayes. (1764) "An Essay towards solving a Problem in the Doctrine of Chances." *Philosophical Transactions of the Royal Society of London*. 53, 370–418.

A. Beige, et. al. (2001, November 20) "Secure communication with a publicly known key." *arXiv:quant-ph*/0111106.

M. Bellare, et. al. (1996) "Keying Hash Functions for Message Authentication." *Crypto 96*. 1109, Springer.

C.H. Bennett, & G. Brassard. (1984) "Quantum cryptography: Public key distribution and coin tossing." *Proc. IEEE Intl. Conf. Computers, Systems & Signal Proc. 175–179.*

C.H. Bennett, et. al. (1988, April) "Privacy Amplification by Public Discussion." *SIAM J. Computing*. 17(2), 210–229.

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

R.G. Brown, D. Eddelbuettel, & D. Bauer. (2015) "Dieharder: A Random Number Test Suite." *Duke University*.

G. Cardano. (1550) "De subtilitate rerum." *Nuremberg*.

F.G. Deng & G.L. Long. (2004, May 28) "Secure Direct Communication with a Quantum One-Time-Pad." *arXiv:quant-ph*/0405177.

W. Diffie & M. Hellman. (1976, November) "New directions in cryptography." *IEEE Trans. on Info. Theory*. 22, 644–654.

R. Durstenfeld. (1964, July) "Algorithm 235: Random Permutation." *Communications of the ACM*. 7(7), 420.

W. Feller. (1958, 1966) *An Introduction to Probability Theory and Its Applications*. Vol. I, II. John Wiley.

S. Foster. (2024, May 21) "How Much Does Fiber Optic Cable Cost Per Mile." *PulseWires*.

A.C. Geary. (2009) *Analysis of a Man-In-The-Middle-Attack on the Diffie-Hellman Key Exchange Protocol*. M.S. Thesis. Naval Postgraduate School.

S. Greengard. (2021) *The Internet of Things.* MIT Press.

L.K. Grover. (1996) "A fast quantum mechanical algorithm for database search." *Proceedings STOC*. 212–219.

W. Heisenberg. (1927) "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik." *Zeitschrift für Physik*. 43(3-4), 172–198.

M. Herrero-Collantes, & J.C. Garcia-Escartin. (2017, Feb. 22) "Quantum random number generators." *Reviews of Modern Physics*. 89(1), 015004, APS.

N. Jain, et al. (2014, June 23) "Trojan-horse attacks threaten the security of practical quantum cryptography." *New Journal of Physics*. 16, 123030.

P. Keshavarzian, et al. (2023, September) "A 3.3-Gb/s SPAD-Based Quantum Random Number Generator." *IEEE Journal of Solid-State Circuits.* 58(9).

G.M. Lilly. (2004, December 7) "Device for and Method of One-Way Cryptographic Hashing." *U.S. Patent* 6,829,235.

D. Lowndes, et. al. (2021, May 26) "A low cost, short range quantum key distribution system." *EPJ Quantum Technology*. 8(15), Springer.

G. Marsaglia. (1995) "The Marsaglia Diehard Battery of Tests of Randomness." *Florida State University*.

U.M. Maurer. (1993, May) "Secret Key Agreement by Public Discussion from Common Information." *IEEE Transactions on Information Theory*. 39(3), 733–742.

R.C. Merkle. (1975) "Secure Communications over Insecure Channels." *Communications of the ACM*. 21(4), 294–299. https://aemea.org/cs/Merkle_Puzzles.pdf

A. de Moivre. (1738) *Doctrine of Chances: A Method of Calculating Probabilities of Events in Play*. Woodfall.

J. Proos, & C. Zalka. (2003, January 25) "Shor's discrete logarithm quantum algorithm for elliptic curves." *Quantum Information & Computation.* 3(4), 317–344.

C. Shannon. (1949) "Communication Theory of Secrecy Systems." *Bell Technical Journal.* 28(4), 656–715.

M. Stipčević. (2016, March 16) "Quantum random flip-flop and its applications in random frequency synthesis and true random number generation." *Rev. Sci. Inst.* 87, 035113.

P.D. Townsend, J.G. Rarity & P. Tapster. (1993, April 1) "Single photon interference in a 10km long optical fibre interferometer." *Electronic Letters*. 29(7), 634–635.

S. Vaudenay. (2005, August 14) "Secure Communications over Insecure Channels Based on Short Authenticated Strings." *Crypto 2005. Advances in Cryptology*. 309–326.

M. Wegman, & J.L. Carter. (1981, June) "New Hash Functions and Their Use in Authentication and Set Equality." *Journal of Computer and System Sciences*. 22, 265–279.

S. Weisner. (1969) "Conjugate Coding." *Columbia University*. 78–88. https://aemea.org/physics/Conjugate_Coding.pdf