Measurable Security through Isotropic Channels

Micah Sherr, Eric Cronin, and Matt Blaze

Department of Computer and Information Science
University of Pennsylvania
{msherr,ecronin,blaze}@cis.upenn.edu

Abstract. This position paper proposes the use of special broadcast networks to achieve provable and measurable confidentiality of messages. We call these networks *isotropic channels*, broadcast channels in which receivers cannot reliably determine whether a given message originated from any particular sender and senders cannot prevent a message from reaching any particular receiver. As long as eavesdroppers cannot reliably (i.e., with probabilistic certainty) identify the sender of a message, honest parties can efficiently exchange messages with confidentiality that asymptotically approaches and in some cases reaches perfect secrecy. Even under incorrect assumptions regarding the degree of isotropism offered by a particular channel, a high measure of confidentiality can be efficiently achieved.

This position paper additionally makes the case that isotropic channels already exist, and are, in fact, often used in practice. By leveraging isotropic techniques, measurable information theoretic security can be practically achieved.

1 Introduction

Introductory network security courses teach that the correct approach for message confidentiality is to encrypt messages at their source and decrypt at their destinations. The end-points are the trusted parties, and no component or functionality of the network should be relied upon to adequately protect message content. The mechanisms of cryptography should be implemented at the end-points, and nowhere else.[1]

This paper promotes the opposite. Rather than relying on standard end-to-end cryptographic protocols, we explore the security guarantees offered by particular communication media. These channels behave approximately like a broadcast medium, in which eavesdroppers can receive (and possibly transmit), but with the constraint that receivers cannot reliably determine whether a given message originated from any particular sender and senders cannot prevent a message from reaching any particular receiver. We refer to such "directionless" media as *isotropic channels*[2] [1].

Isotropic channels have some interesting security properties. Even without the use of standard cryptographic techniques, the confidentiality of messages can be probabilistically guaranteed and *measured*. Unlike traditional (i.e., computational) cryptography, isotropic protocols do not rely on any standard assumptions or computational models.

[1] This is of course often relaxed due to practical considerations, e.g., in VPNs.

[2] Our use of the term "isotropic" is inspired by, but not identical to, the analogous concept in physics and communications theory.

A *perfect* isotropic channel (i.e., one in which Eve cannot discern any information concerning the sender or receiver of a packet) offers perfect information theoretic security (i.e., Shannon's perfect secrecy [2]), even in the case of a computationally unbounded and active adversary!

Perhaps more interestingly, the confidentiality provided by isotropic protocols scales gracefully with the degree of isotropism. That is, isotropism need not be a binary value. Isotropic protocols yield measurable probabilistic confidentiality as long as there is any uncertainty as to the source of messages. As we show below, Eve's ability to decipher bits of plaintext increases only logarithmically with a linear increase in her ability to determine sender information. Moreover, if the honest parties can bound Eve's ability to identify sender information, then simple privacy amplification techniques can be used to achieve confidentiality that exponentially approaches perfect secrecy.

In the remainder of this position paper, we investigate the security properties of isotropic protocols. We argue that due to their ability to scale gracefully with decreasing levels of isotropism, isotropic protocols represent a promising confidentiality technique under both correct and incorrect assumptions regarding the degree of sender anonymity in the channel. We conclude by proposing some practical applications for isotropic protocols that use existing network infrastructure.

2 Isotropic Channels

In this section, we briefly and somewhat informally describe isotropic channels and protocols. For a more detailed and formal treatment of isotropic channels, we refer the reader to our earlier work [1].

Typical communication channels often have some notion of *directionality*, and indeed it is usually seen as a prerequisite for authentication. Any party (including an eavesdropper) can identify the sender of a received message. However, it may be possible (and, as we show, useful) to design and implement communication networks in which messages convey little or no information concerning their true senders. These channels can be established using some physical property of the communication medium (e.g., the difficulty of locating the source of a wireless transmission when parties are mobile or move their transmitters [3], or intrinsic isotropism [4]), or they may be constructed using logical overlay networks such as anonymity networks [5,6,7,8]. As exotic and unpractical as such networks may at first seem, a common hubbed Ethernet is a simple example of a realizable isotropic network.

Formally, an isotropic channel is defined as follows:

Definition 1 *(Isotropic Channel) A communications channel is an* isotropic channel *if all messages are broadcast to all parties, an honest party cannot discern the sender of a message not from itself (although it may reason about a message's origins) and the probability that an eavesdropper E can correctly identify the sender of a message not originating from E is at most ρ, where $\frac{1}{n} \leq \rho < 1$ and n is the number of nodes in the channel, excluding the eavesdropper.*

Definition 2 *(Perfectly Isotropic Channel) A communications channel is a* perfectly isotropic channel *if it is an isotropic channel and $\rho = \frac{1}{n}$, where n is the number of nodes in the channel, excluding the eavesdropper.*

Definition 3 *(ρ-bounded Isotropic Channel) A communications channel is a ρ-*bounded isotropic channel *if it is an isotropic channel and $\rho < \frac{1}{n}$, where n is the number of nodes in the channel, excluding the eavesdropper.*

We assume that ρ represents the maximum probability that Eve learns the identity of the sender, taking into consideration possibilities such as multiple points of eavesdropping. Furthermore, ρ is a constant probability and does not vary over time.

In this paper, we consider three principals: Alice and Bob, who are honest participants without any *a priori* shared secrets, and Eve, a (potentially active) eavesdropper. If, in reality, there are multiple eavesdroppers, we assume that they are colluding and can combine their knowledge and capabilities, and we model them collectively as Eve.

In the following section, we describe a protocol for achieving perfect secrecy in perfectly isotropic channels. We conservatively assume that all eavesdroppers receive all messages (i.e., they experience no loss). Due to space constraints, we consider only passive eavesdroppers in this paper. However, we note that more complicated isotropic protocols are available that provably thwart active eavesdropping attempts [1].

3 Security Properties of Perfectly Isotropic Channels

Isotropic channels give honest parties an inherent advantage over even the most perceptive eavesdropper. For example, consider a perfectly isotropic channel with only three principals: Alice, Bob, and a passive or blocking adversary, Eve. If Alice broadcasts a message, she knows she is the originator of the message by virtue of having sent it. Since Eve lacks the ability to inject messages, Bob knows the message originated from Alice since he did not send it and Eve could not have sent it. Eve, on the other hand, cannot discern the source of a message since it could have been sent by either Alice or Bob.

The two honest parties can exploit this asymmetry to securely share messages. By conducting a number of *rounds* in which one bit is securely exchanged, Alice and Bob can exchange a k-bit secret. In a given round, Alice or Bob (but not both) broadcast. If Alice originated the broadcast, the next bit of the message is `0`; if Bob transmitted, the next bit is `1`. Note that in each round, Eve's ability to identify the source of a message is $\frac{1}{2}$, and therefore that is also her probability of guessing a bit. Once the k-bit secret is shared, Alice can employ a Vernam cipher [9] to encrypt her plaintext. Since Eve's *a posteriori* probability of knowing the plaintext equals her *a priori* probability, such a scheme achieves perfect secrecy.

Of course, for such a protocol to be realizable, Alice and Bob must *a priori* agree on an ordering of when to transmit, which would itself require k bits of shared secret. (Otherwise, neither or both parties may transmit during a round.) Thus, a slightly more complicated protocol is required.

The revised protocol consists of two phases. In the first phase, Alice broadcasts a sequence of random nonces, $\{r_{A1}, r_{A2}, ..., r_{Al}\}$, where $r_{Ai} \in_R [0, 2^{\alpha} - 1]$, $1 \leq i \leq l$, and $\in_R$ denotes choosing uniformly at random from a set. Each nonce is broadcast as a separate transmission (i.e., packet), and the time between transmissions is chosen according to a Poisson process with average rate λ. Simultaneously, Bob broadcasts a series of random nonces, $\{r_{B1}, r_{B2}, ..., r_{Bm}\}$, in an analogous manner: The value of α should be sufficiently large to prevent duplicate nonces.

The second phase of the protocol commences when Alice has broadcast at least k values and she has received at least k values from Bob. Alice selects k nonces at random from her sequence $\{r_{A1}, r_{A2}, ..., r_{Al}\}$. Let $\mathcal{A}$ represent the resultant set. She also selects k values at random from the set of nonces received from Bob (recall that Alice can identify Bob's nonces by virtue of having not sent them herself). We denote this set as $\mathcal{B}$. Alice then generates a string of nonces $s_1, s_2, ..., s_k$ in the following manner: For each $s_i, 1 \leq i \leq k$, with probability 0.5, Alice chooses $s_i \in_R \mathcal{A}$ and sets $\mathcal{A} \leftarrow \mathcal{A} - s_i$. With probability 0.5, she picks $s_i \in_R \mathcal{B}$ and sets $\mathcal{B} \leftarrow \mathcal{B} - s_i$. She then broadcasts her string of nonces, $s_1, s_2, ..., s_k$.

The string encodes the secret in the following manner. If s_i belongs to the set of nonces sent by Alice, s_i encodes a `0`. Otherwise, s_i encodes a `1`. Note that due to channel loss, collision[3], or blocking by an eavesdropper, Bob may not receive all tuples broadcast by Alice. In such a case, all "unknown" nonces in the string $s_1, s_2, ..., s_k$ must belong to Alice and can safely be decoded as `0`s.

Recall that the channel's isotropism prevents Eve from distinguishing Alice's transmissions from Bob's. Since the first phase of the protocol is symmetric with respect to Alice and Bob, Eve cannot use the content of messages to identify sender information. Each nonce in $s_1, s_2, ..., s_k$ therefore has equal probability of being originally broadcast by Alice or Bob, and hence the protocol guarantees perfect secrecy.

Note that the above protocol functions only when there are exactly two honest parties in the channel. The protocol can be trivially amended to support channel multiplexing among several sets of honest parties by prefixing all messages with *conversation identifiers*. A conversation identifier is used to identify a broadcast with a particular exchange between two parties. A party silently drops transmissions if it does not recognize the message's conversation identifier.

4 Graceful Degradation of Security with Imperfect Isotropism

The protocol described in the previous section is appropriate for perfectly isotropic channels. In a ρ-bounded isotropic channel, Eve can identify each bit with probability ρ (which may approach 1). Fortunately, privacy amplification techniques can be used to further enhance message confidentiality.

A simple (but somewhat inefficient) privacy amplification scheme makes use of exclusive-or (xor). To share a k-bit secret, Alice and Bob securely exchange $x \cdot k$ bits using the protocol previously described, where x is a tunable security parameter called the *privacy amplification parameter*. After the $x \cdot k$ bits are shared, they are evenly split into k bit strings, each of length x. The ith bit of secret is decoded by xor'ing all x bits in the ith string. To successfully decode a bit of the secret, Eve must therefore incorrectly interpret an even number of the x bits. In our previous work on isotropism [1], we prove that this privacy amplification scheme results in confidentiality that exponentially reaches perfect secrecy at the expense of a linear number of communicated bits.

[3] We assume that collision results in message loss. Message corruption can be prevented through the use of CRCs.

If the honest parties can correctly and efficiently measure ρ, then they can achieve their desired level of confidentiality by adjusting the privacy amplification parameter. Let c represent the *desired* level of confidentiality, or more precisely, the *desired* maximum probability that Eve can identify a bit in the secret. Note that $c \geq 0.5$, since Eve can do no worse than random guessing. Using the proof of Theorem 9 in our introduction to isotropism [1], we have

$$c = \frac{1 + (2\rho - 1)^x}{2} \tag{1}$$

If the honest parties want to limit Eve's probability of learning each bit to at most c, they will select a corresponding privacy amplification factor. Solving for x yields

$$x = \lceil \frac{\lg(2c - 1)}{\lg(2\rho - 1)} \rceil \tag{2}$$

We now explore the confidentiality of exchanged secrets when Alice and Bob underestimate ρ. We let ρ' denote Alice's and Bob's estimation of ρ. (We leave as future work how Alice and Bob agree on ρ'.)

If Alice and Bob wish to bound Eve's probability of learning bits to c, they will choose a privacy factor x' according to Equation 2, and therefore $x' = \lceil \frac{\lg(2c-1)}{\lg(2\rho'-1)} \rceil$. If Alice and Bob use x' as their privacy amplification parameter, Eve's true probability of learning a given bit of secret is:

$$c' = \frac{1 + (2\rho - 1)^{\lceil \frac{\lg(2c-1)}{\lg(2\rho'-1)} \rceil}}{2} \tag{3}$$

The graphs in Figure 1 depict the degradation of security with incorrect estimates of ρ, calculated using Equation 3. The honest parties' desired measure of confidentiality (c) is shown on the x-axis of each plot, while the actual achieved measure of confidentiality (c') is plotted on the y-axis. Each graph uses a particular level of isotropism (ρ), from very isotropic ($\rho = 0.65$) to poorly isotropic ($\rho = 0.95$). Within each graph, the effects of several incorrect estimates of isotropism (ρ') are shown. Note that when $\rho' = \rho$, the resultant curve is the identity function.

Under some conditions, minor differences between ρ and ρ' may be tolerated, resulting in less than desired (but not broken) confidentiality. However, the honest parties can hedge their bets by multiplying the privacy amplification parameter by a multiplier z. If we let δ represent the difference between the desired confidentiality (again, measured as the maximum probability that Eve correctly identifies a bit of secret), then we have:

$$\delta = c - c' = \frac{1 + (2\rho - 1)^{\lceil \frac{\lg(2c-1)}{\lg(2\rho-1)} \rceil}}{2} - \frac{1 + (2\rho - 1)^{z \lceil \frac{\lg(2c-1)}{\lg(2\rho'-1)} \rceil}}{2} \tag{4}$$

Thus, a linear increase in z results in an exponential decrease in δ. Even if Alice and Bob grossly misjudge the isotropism of the channel, they can pick a small value of z and likely reach ($\delta = 0$) or succeed ($\delta < 0$) their desired level of confidentiality.

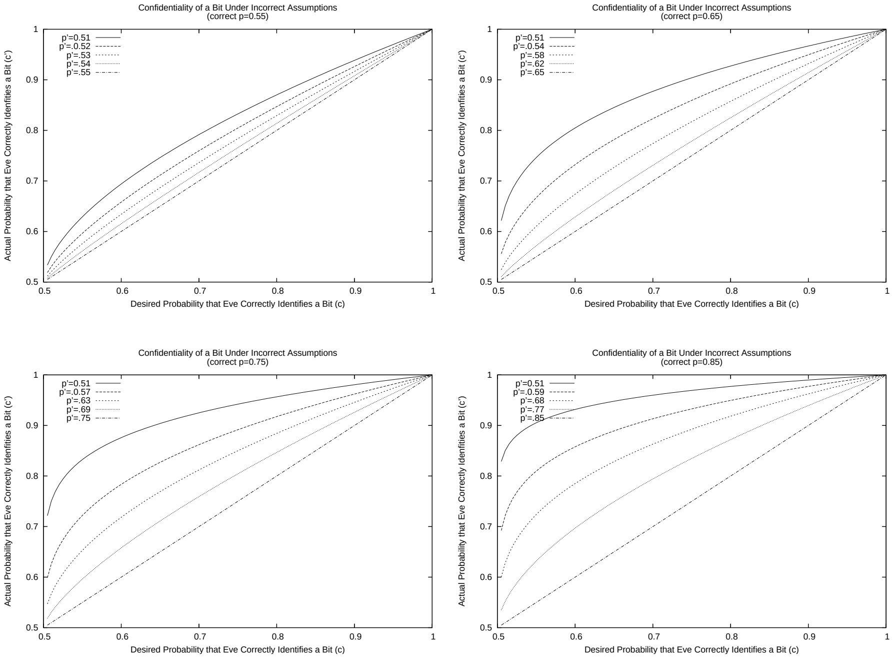

Fig. 1. Degradation of Security with Incorrect Estimates of ρ

5 Some Practical Applications for Isotropic Communication

Key Agreement in Wireless Networks A particularly powerful motivation for isotropic communication is key exchange between clients and unknown wireless access points (WAPs). Because of the broadcast nature of wireless communications, secure WAPs almost always employ link-layer encryption to prevent eavesdropping by nearby receivers. Standard link layer encryption schemes such as WEP and WPA [10,11] rely on pre-shared keys (either per-WAP or per-client) and are therefore inappropriate for certain environments, e.g., Internet cafes, in which pre-agreement on keys is problematic. Additionally, both WEP and WPA in PSK mode only protect from eavesdropping by outsiders; other clients of the same WAP (e.g. other customers of the Internet cafe) share the same key and can see all clients' traffic.

The ability to detect MitM attacks while offering exponentially close to perfect secrecy [1] makes isotropic protocols ideal for wireless networks. Although wireless networks are not perfectly isotropic (Eve can conduct a direction-finding attack against isotropism), there will always be some uncertainty associated with Eve's ability to identify the sources of messages, especially if some countermeasure is employed [3].

The communication overhead associated with isotropic protocols may be significant, so isotropism is perhaps most useful for key exchange. Upon entering a wireless hotspot, a client broadcasts its desire to associate with a particular wireless network, e.g., one operated by a ubiquitous coffee shop company. It then exchanges a key with the access point using an isotropic protocol that ensures the detection of active adversaries. Note that the client and the base-station should choose zero-valued MAC addresses for their transmissions so that link layer packet headers do not reveal sender information. If the client did not detect an active Eve and it has received verification via a notification protocol that the base-station did not perceive Eve, then the client accepts the key.

Once the client and the base-station have successfully shared a key, that key is then used to encrypt subsequent transmissions using a standard computational cryptographic algorithm.

Mobile Ad-hoc Wireless Sensor Networks The mobility of ubiquitous sensors makes direction finding difficult [12]. While Eve may employ some physical (layer 1) technique to discern sender information for a stationary object, the frequent movement of the sensor nodes requires Eve to constantly reconfigure her eavesdropping apparatus. Unless Eve can visually monitor the sensors and quickly adapt to changes in their locations, her ability to distinguish sender information is perturbed.

Using the isotropic key exchange mechanism previously described, sensor nodes can securely share keys and use standard cryptographic techniques to protect their messages. Or, since sensor messages are typically short, isotropic protocols may be used directly to provide information theoretic guarantees as to message confidentiality.

Hubbed Ethernet An Ethernet hub acts as a layer-1 *normalizer*, standardizing the physical characteristics of transmissions (e.g., voltage) that might otherwise be used to distinguish senders. Thus, a hub provides a perfectly isotropic channel. If Alice, Bob, and Eve each has access to a separate port on the hub, Alice and Bob can communicate with perfect secrecy.

Anonymous Overlay Networks The anonymity provided by anonymous overlay networks [7,8,13] is a promising source of isotropism. Some information theoretic anonymity networks, e.g., DC-Nets [5], seem readily amenable to isotropic protocols due to their use of broadcast as the underlying communication mechanism. However, many of the widely deployed anonymity networks (e.g., Tor [6]) do not currently support broadcast. Enhancing these networks to support broadcast or multicast communication while still preserving anonymity represents a significant research problem, and is left as future work.

6 Conclusion

This position paper has argued that isotropic protocols represent an effective means of achieving measurable and unconditional security. Even under broken assumptions regarding the level of isotropism in a channel, honest parties can communicate with some degree of confidentiality. Moreover, isotropism exists in many already deployed networks, offering exciting opportunities to investigate the practicality of these information theoretic techniques.

References

1. Anand, M., Cronin, E., Sherr, M., Blaze, M., Kannan, S.: Security protocols with isotropic channels. Technical Report CIS-06-18, University of Pennsylvania, Department of Computer and Information Science (Nov 2006) Available at `http://micah.cis.upenn.edu/papers/isotropism-tr-cis-06-18.pdf`.
2. Shannon, C.E.: A mathematical theory of communication. Bell System Technical Journal **27** (1948) 379–423, 623–656
3. Castelluccia, C., Mutaf, P.: Shake them up!: A movement-based pairing protocol for CPU-constrained devices. In: MobiSys '05: Proceedings of the 3rd international conference on Mobile systems, applications, and services, New York, NY, USA, ACM Press (2005) 51–64
4. Scheuer, J., Yariv, A.: Giant fiber lasers: A new paradigm for secure key distribution. Physical Review Letters **97**(14) (Oct 2006)
5. Chaum, D.: The dining cryptographers problem: Unconditional sender and recipient untraceability. Journal of Cryptology **1** (1988) 65–75
6. Dingledine, R., Mathewson, N., Syverson, P.: Tor: The second-generation onion router. In: Proc. of the 13th Usenix Security Symposium. (2004) 303–320
7. Syverson, P.F., Goldschlag, D.M., Reed, M.G.: Anonymous connections and onion routing. IEEE Journal on Selected Areas in Communications **16**(4) (May 1998) 482–494
8. Shields, C., Levine, B.N.: Hordes: a multicast based protocol for anonymity. Journal of Computer Security **10**(3) (2002) 213–240
9. Vernam, G.S.: Cipher printing telegraph systems for secret wire and radio telegraphic communications. Journal of the American Institute of Electrical Engineers **55** (1926) 109–115
10. LAN/MAN Standards Committee: Wireless LAN medium access control (MAC) and physical layer (PHY). IEEE Standard 802.11, IEEE Computer Society (1999)
11. LAN/MAN Standards Committee: Wireless LAN medium access control (MAC) and physical layer (PHY) amendment 6: Medium access control (MAC) security enhancements. IEEE Standard 802.11i, IEEE Computer Society (2004)
12. Castelluccia, C., Avoine, G.: Noisy tags: A pretty good key exchange protocol for RFID tags. In: Seventh Smart Card Research and Advanced Application IFIP Conference. (Apr 2006)
13. Reiter, M.K., Rubin, A.D.: Crowds: Anonymity for web transactions. In: ACM Transactions on Information and System Security. (1998)