

## 11 Additional Proofs

The following is the complete proof that the Vernam Cipher and OTP can be extended from binary to N-ary values without loss of secrecy.

**Lemma 1.** *If the selection of  $\mathbf{k}_m$  is purely random, then*

$$p(\mathbf{c}_m[i]=z|\mathbf{m}_m[i]=x)=p(\mathbf{c}_m[i]=z), \forall x \in M_m, \forall z \in C_m, \forall i \quad (17)$$

*Proof.* Starting from the left-hand part in (17), by Bayes' formula we get

$$p(\mathbf{m}_m[i]=x|\mathbf{c}_m[i]=z)=\frac{p(\mathbf{m}_m[i]=x \wedge \mathbf{c}_m[i]=z)}{p(\mathbf{c}_m[i]=z)}, \forall x \in M_m, \forall z \in C_m \quad (18)$$

The encryption function in the numerator in (18) can be expanded to produce the following equivalence

$$p(\mathbf{m}_m[i]=x \wedge \mathbf{c}_m[i]=z)=p(\mathbf{m}_m[i]=x \wedge \mathbf{k}_m[i]=(z-x) \bmod \phi) \quad (19a)$$

Since the *a priori* probability of the key selection is independent from that of the plaintext magnitudes, the right-hand part of (19a) can be expressed as

$$p(\mathbf{m}_m[i]=x) \times (\mathbf{k}_m[i]=(z-x) \bmod \phi) \quad (19b)$$

and since the selection of  $\mathbf{k}_m[i]$  is chosen uniformly on the range  $[0, \phi]$ , (19b) can be reduced to

$$p(\mathbf{m}_m[i]=x) \times \frac{1}{L} \quad (19c)$$

where  $L$  is the discrete number of levels in the range  $[0, \phi]$ .

The following equivalence can be applied to the denominator in (18)

$$p(\mathbf{c}_m[i]=z)=\sum_X p(\mathbf{m}_m[i]=x \wedge \mathbf{c}_m[i]=z)=\sum_X p(\mathbf{m}_m[i]=x) \times \frac{1}{L}=\frac{1}{L}$$

In other words, we can deduce from the denominator in (18) that each cryptogram magnitude  $z$  is equally likely to occur. Therefore, from Bayes' theorem in (17) it can be shown that

$$p(\mathbf{m}_m[i]=x|\mathbf{c}_m[i]=z)=\frac{p(\mathbf{m}_m[i]=x) \times \frac{1}{L}}{\frac{1}{L}}=p(\mathbf{m}_m[i]=x), \forall x \in M_m, \forall z \in C_m, \forall i \quad (20)$$

**Lemma 2.** *If the selection of  $\mathbf{k}_a$  is purely random, then*

$$p(\mathbf{m}_a[i]=x|\mathbf{c}_a[i]=z)=p(\mathbf{m}_a[i]=x), \forall x \in M_a, \forall z \in C_a, \forall i \quad (21)$$

*Proof.* Following (18), similarly to (19a), (21) can be presented as

$$p(\mathbf{m}_a[i]=x \wedge \mathbf{c}_a[i]=z)=p(\mathbf{m}_a[i]=x \wedge \mathbf{k}_a[i]=(z-x)) \quad (22)$$

Since the selection of  $\mathbf{k}_a[i]$  is chosen uniformly on the range  $[-\pi, \pi]$ , and following (19b), (22) can be reduced to

$$p(\mathbf{m}_a[i]=x) \times \frac{1}{L} \quad (23)$$

where  $L$  is the discrete number of levels in the range  $[-\pi, \pi]$ .

Therefore, by (20), applying Bayes' theorem as in (21) results in

$$p(\mathbf{m}_a[i]=x|\mathbf{c}_a[i]=z)=\frac{p(\mathbf{m}_a[i]=x) \times \frac{1}{L}}{\frac{1}{L}}=p(\mathbf{m}_a[i]=x), \forall x \in M_a, \forall z \in C_a, \forall i$$

**Theorem 1.** *If the selection of  $\mathbf{k}=(\mathbf{k}_m, \mathbf{k}_a)$  is purely random, then the VPSC is unconditionally secure (unbreakable).*

*Proof.* According to Claude Shannon's work in [21], given a plaintext message  $m_1$  and cryptogram  $c_1$ ,

$$p(C=c_1|M=m_1)=p(C=c_1), \quad (24)$$

Therefore, the VPSC is unconditionally secure if

$$p(\mathbf{c}[i]=z|\mathbf{m}[i]=x)=p(\mathbf{c}[i]=z), \forall x \in M, \forall z \in C, \forall i \quad (25)$$

In other words, the VPSC's encrypted channel must provide no equivocation. No amount of cryptograms  $\mathbf{c}_m[i]$  may provide any information about the original plaintext  $\mathbf{m}[i]$ . By Bayes' theorem, (25) is equivalent to

$$p(\mathbf{m}[i]=x|\mathbf{c}[i]=z)=p(\mathbf{m}[i]=x), \forall x \in M, \forall z \in C, \forall i \quad (26)$$

By expanding the magnitude and angle components of  $x \in M, z \in C$ , (26) is equivalent to

$$p(\mathbf{m}[i]=(x_m, x_a)|\mathbf{c}[i]=(z_m, z_a))=p(\mathbf{m}[i]=(x_m, x_a)), \forall x_m, z_m \in M, \forall x_a, z_a \in C, \forall i \quad (27a)$$

In other words, the left-hand part of (27a) can be expressed as

$$p(\mathbf{m}_m[i]=x_m \wedge \mathbf{m}_a[i]=x_a | \mathbf{c}_m[i]=z_m \wedge \mathbf{c}_a[i]=z_a) \quad (27b)$$

For truly random  $\mathbf{k}_m, \mathbf{k}_a$ , the angle and magnitude components of both message and ciphertext are independent, therefore (27b) is equivalent to

$$p(\mathbf{m}_m[i]=x_m | \mathbf{c}_m[i]=z_m) \times p(\mathbf{m}_a[i]=x_a | \mathbf{c}_a[i]=z_a) \quad (27c)$$

By lemmas 1 and 2, and using (27c), (27a) reduces to

$$p(\mathbf{m}[i]=(x_m, x_a))=p(\mathbf{m}[i]=(x_m, x_a)), \forall x_m, z_m \in M, \forall x_a, z_a \in C, \forall i \quad (28)$$

Which is trivially true, therefore we have proven the equivalence in (25). This means that the encryption of the channel provides no equivocation, by Shannon's theorem of Theoretical Secrecy [21].

The following is a proof that knowledge of the system's parameter  $\phi$  does not affect the system's secrecy.

**Theorem 2.** *For any plaintext value  $m$  of magnitude  $m_m$ , and for all  $\phi=\varphi$  s.t.  $\varphi_i \geq m_m$ , if  $m_m$  is encrypted using a purely random key  $k_m$ , the encrypted value  $c$  provides no equivocation over  $m$ .*

*Proof.* We will prove this theorem by contradiction. Let us assume that there is some  $\phi=\varphi_i$  s.t.

$$p(m=(x_m, x_a)|c=(z_m, z_a)) \neq p(m=(x_m, x_a)) \quad (29)$$

Following (27c), (29) is equivalent to

$$p(m_m=x_m | c_m=z_m) \neq p(m_m=x_m) \quad (30)$$

By expansion of the encryption operation, and since the *a priori* probability of the key selection is independent from that of the plaintext

$$p(m_m=x_m \wedge c_m=z_m)=p(m_m=x \wedge k_m=(z-x) \bmod \varphi) \quad (31)$$

However, that is in violation of theorem 1 which we have proven by (19a) to be valid for all values of  $\phi$  within the domain defined in the encryption function.