Companion to "Provably Secure Steganography"

Nicholas J. Hopper, John Langford, and Luis von Ahn

Carnegie Mellon University
{hopper,jcl,biglou}@cs.cmu.edu

Abstract. We point out and correct a flaw in our paper "Provably Secure Steganography", which appeared in the proceedings of CRYPTO 2002. The claims of the paper remain correct, but small changes need to be made in one of our protocols.

1 Introduction

Lea Kissner, Tal Malkin and Omer Reingold have pointed out a small flaw in our paper "Provably Secure Steganography". The flaw has to do with Construction 1 in Section 3.1. In this construction, RS samples the channel oracle $|K|$ times. As Kissner, Malkin and Reingold point out, this construction, as stated, is insecure. Luckily, the construction remains secure if RS samples from the oracle only twice. Hence, the construction should be changed to the following:

Construction 1 *(Steganographic Secrecy)*

Procedure `S1.Encode`:
Input: key K, hiddentext m', history h
Let $m = Enc(m')$
Parse m as $m_1^1||m_2^1||\cdots||m_l^1$
for $i = 1 \ldots l$ do
  $c_i \leftarrow RS^{M(h),F_K(N,\cdot)}(m_i, 2)$
  set $h = h||c_i$
  increment N
Output: $c_1||c_2||\ldots||c_l$

Procedure `S1.Decode`:
Input: key K, Stegotext c
Parse c as $c_1^b||c_2^b||\ldots||c_l^b$
for $i = 1 \ldots l$ do
  set $m_i = F_K(N, c_i)$
  increment N
let $m = m_1||m_2||\cdots||m_l$
Output: $Dec(m)$

The following section (in conjunction with our paper) should prove the correctness of this construction.

2 Correctness

Notation

Assume the channel has symbols $\{S_1, ..., S_k\}$ with probabilities $p_1, ..., p_k$. Assume f is a random function from $\{S_1, ..., S_k\}$ to $\{0, 1\}$. Consider the following experiment:

> Draw from the channel to get a symbol S. If $f(S) = 0$ output S. Otherwise draw again from the channel and output the result.

Denote the outcome of this experiment by S_E.

Let D be the event that after drawing twice from the channel you get a different symbol (a non-collision). Let $\overline{D}$ denote the event that after drawing twice from the channel you get the same symbol.

Lemmas

We need to show that drawing from the channel with replacement twice doesn't change the distribution. In other words:

Lemma 1.

$$\Pr_{f,\mathcal{C}}[S_E = S_i] = p_i$$

Proof.

$$\begin{aligned}\Pr_{f,\mathcal{C}}[S_E = S_i] &= p_i/2 + \frac{p_i}{4}\sum_{j\neq i} p_j + \frac{p_i}{4}\sum_{j\neq i} p_j + p_i^2/2 \\ &= p_i/2 + p_i(1-p_i)/2 + p_i^2/2 \\ &= p_i\end{aligned}$$

The first line is true because the probability of getting symbol S_i is the sum of the probabilities of the following disjoint events:

- The first draw from the channel results in S_i and $f(S_i) = 0$.
- The first draw from the channel is S_j for $i \neq j$ and $f(S_j) = 1$ and the second draw from the channel is S_i and $f(S_i) = 0$.
- The first draw from the channel is S_j for $i \neq j$ and $f(S_j) = 1$ and the second draw from the channel is S_i and $f(S_i) = 1$.
- The first draw from the channel is S_i and $f(S_i) = 1$ and the second draw from the channel is S_i.

Next we need to show that drawing twice from the channel results in a symbol that maps to the correct bit with a probability bounded away from 1/2:

Lemma 2.

$$\Pr_{f,\mathcal{C}}[f(S_E) = 0] > 5/8$$

Proof. First, note that:

$$\Pr_{f,\mathcal{C}}[f(S_E) = 0] = \frac{1}{2} + \frac{1}{4}\Pr_{f,\mathcal{C}}[D]$$

The right side is the sum of the probabilities of the following disjoint events:

- The first draw results in a symbol that maps to zero.
- The first draw results in a symbol that maps to 1 and the second draw results in a *different* symbol that maps to 0.

Let S_i be a symbol with highest probability ($p_i \geq p_j$ for all j), then

$$\Pr_{f,\mathcal{C}}[\overline{D}] = p_1^2 + \ldots + p_k^2 \leq p_i(p_1 + \ldots + p_k)$$

So $\Pr_{f,\mathcal{C}}[D] \geq (1 - p_i)$, and we have that

$$\begin{aligned}\Pr_{f,\mathcal{C}}[f(S_E) = 0] &\geq \frac{1}{2} + \frac{1}{4}(1 - p_i) \\ &> \frac{1}{2} + \frac{1}{8}\end{aligned}$$

(since we are assuming that $H_\infty(\mathcal{C}) > 1$).

Acknowledgments We are greatful to Lea Kissner, Tal Malkin and Omer Reingold for pointing out the flaw in our paper.

References

1. Nicholas J. Hopper, John Langford and Luis von Ahn. Provably Secure Steganography. In *Proceedings of CRYPTO 2002*.