Unconditionally secure chaffing and winnowing with short authentication tags

Douglas R. Stinson
David R. Cheriton School of Computer Science
University of Waterloo

Authentication vs. Encryption

- an secret-key encryption scheme uses a secret key K to transform a plaintext x into a ciphertext y
- the same key can be used to decrypt y, thereby obtaining x
- without knowledge of K, it should be infeasible to compute x from y
- a message authentication code (or, MAC) uses a secret key K to compute an authentication tag a for a plaintext x
- the message (x, a) is transmitted to a recipient who also knows the value of K
- knowledge of K allows the tag to be verified
- if an adversary, who does not know the value of K, creates a bogus new message (x', a'), then (with high probability) the tag a' will not be valid for the plaintext x'

Motivating Scenario

- chaffing-and-winnowing was suggested by Ron Rivest
- suppose that encryption schemes are outlawed, while message authentication codes remain legal
- the basic idea is to **use a MAC to provide confidentiality**
- a sender (Alice) and a receiver (Bob) share a secret key K
- Alice prepares a number of messages and sends them to Bob
- each message has the form $m = (x, a)$, where each x is a plaintext and a is an authentication tag
- Bob only accepts the message(s) having authentication tags that are valid under the key K
- a bad guy has no way to distinguish between valid and invalid authentication tags, so confidentiality is achieved

Unconditionally Secure Schemes

- Hanaoka *et al.* first studied chaffing-and-winnowing schemes in the setting of unconditional security (which is also known as information-theoretic security)
- they make use of authentication codes that are unconditionally secure against impersonation
- in their construction, the entropy of the authentication tag is the same as the entropy of the plaintext
- this means that **a tag (by itself, without any plaintext) already can provide perfect secrecy**
- we construct unconditionally secure chaffing-and-winnowing schemes with short (i.e., 1-bit) authentication tags

Unconditionally Secure Chaffing-and-Winnowing Scheme

An unconditionally secure chaffing-and-winnowing scheme is a 5-tuple $(\mathcal{X}, \mathcal{A}, \mathcal{K}, \mathcal{E}, \mathcal{F})$ is a chaffing-and-winnowing scheme.

- $\mathcal{X} = \{0, \ldots, n-1\}$ is the set of plaintexts,
- $\mathcal{A}$ is a set of authentication tags,
- $\mathcal{K}$ is a set of decryption keys,
- for any $K \in \mathcal{K}$ and any $x \in \mathcal{X}$, there is a set $\mathcal{E}(K, x)$ of encryption functions. For each $e \in \mathcal{E}(K, x)$, $e : \mathcal{X} \rightarrow \mathcal{A}$.
- $\mathcal{E} = \bigcup_{K \in \mathcal{K}, x \in \mathcal{X}} \mathcal{E}(K, x)$
- $\mathcal{F} = \{f_K : K \in \mathcal{K}\}$ is a set of authentication functions, where $f_K : \mathcal{X} \rightarrow \mathcal{A}$ for every $K \in \mathcal{K}$

The Protocol

Suppose $(\mathcal{X}, \mathcal{A}, \mathcal{K}, \mathcal{E}, \mathcal{F})$ is a chaffing-and-winnowing scheme.

Step 1. A decryption key $K \in \mathcal{K}$ is chosen randomly by Alice and communicated to the receiver, Bob, over a secure channel.

Step 2. Later, Alice wants to encrypt a plaintext $x \in \mathcal{X} = \{0, \ldots, n-1\}$ to send to Bob. Alice chooses an encryption function $e \in \mathcal{E}(K, x)$ uniformly at random. Then Alice computes $a_j = e(j)$ for all j, $0 \leq j \leq n-1$. The list of n ordered pairs,

$$y = ((0, a_0), \ldots, (n-1, a_{n-1})),$$

is sent to Bob; y is the ciphertext.

Step 3. Bob computes $b_j = f_K(j)$ for all j, $0 \leq j \leq n-1$. Bob decrypts y to the plaintext x if and only if $\{j : b_j = a_j\} = \{x\}$. (There must be **exactly one** ordered pair $m = (x, a)$ such that a is a valid authentication tag under the key K. The plaintext element x is the decryption of y.)

Perfect Secrecy

- in the setting of unconditional security, confidentiality means "perfect secrecy" as defined by Shannon
- a chaffing-and-winnowing scheme is said to provide $\boxed{\text{perfect secrecy}}$ if $\mathsf{Pr}[x|y] = \mathsf{Pr}[x]$ for all plaintexts x and all ciphertexts y
- that is, the **a priori** probability of plaintext x is the same as the **a posteriori** probability of x given that the ciphertext y is observed.
- we assume that $\mathsf{Pr}[x] > 0$ for all x, so we can apply Bayes' Theorem, which states that

$$\mathsf{Pr}[y|x] = \frac{\mathsf{Pr}[x|y] \times \mathsf{Pr}[y]}{\mathsf{Pr}[x]},$$

- it is easily seen that we have perfect secrecy if and only if $\mathsf{Pr}[y|x] = \mathsf{Pr}[y]$ for all plaintexts x and all ciphertexts y.

Example (Hanaoka *et al.*)

We describe a special case of the scheme of Hanaoka *et al.* Suppose that $\mathcal{X} = \mathcal{A} = \{0, \ldots, n-1\}$, $\mathcal{K} = \{K_0, \ldots, K_{n-1}\}$ and $f_{K_i}(j) = j - i \bmod n$ for all i and j.

For any i, x, there is one function in $\mathcal{E}(K_i, x)$, namely, $e_{i,x}$, where $e_{i,x}(j) = x - i$ for all j.

Then it is easy to see that a ciphertext has the form

$$y = ((0, x-t), (1, x-t), \ldots, (n-1, x-t)).$$

We illustrate with the case $n = 4$. First we present the four decryption functions and then we present the encryption function in each $\mathcal{E}(K_i, x)$. All encryption and decryption functions are written as 4-tuples.

Example (cont.)

K_i	f_{K_i}
K_0	$(0, 1, 2, 3)$
K_1	$(3, 0, 1, 2)$
K_2	$(2, 3, 0, 1)$
K_3	$(1, 2, 3, 0)$

i	$x = 0$	$x = 1$	$x = 2$	$x = 3$
0	$(0, 0, 0, 0)$	$(1, 1, 1, 1)$	$(2, 2, 2, 2)$	$(3, 3, 3, 3)$
1	$(3, 3, 3, 3)$	$(0, 0, 0, 0)$	$(1, 1, 1, 1)$	$(2, 2, 2, 2)$
2	$(2, 2, 2, 2)$	$(3, 3, 3, 3)$	$(0, 0, 0, 0)$	$(1, 1, 1, 1)$
3	$(1, 1, 1, 1)$	$(2, 2, 2, 2)$	$(3, 3, 3, 3)$	$(0, 0, 0, 0)$

Example (cont.)

Suppose $K = K_2 = (2, 3, 0, 1)$ and $x = 1$.

The ciphertext is $y = ((0, 3), (1, 3), (2, 3), (3, 3))$.

To decrypt y, compare K and the list of authenticators in y.

$(2, 3, 0, 1)$ and $(3, 3, 3, 3)$ agree in the second co-ordinate, so $x = 1$.

Critique

- this chaffing-and-winnowing scheme provides perfect secrecy
- a ciphertext consists of a list of all possible plaintexts, each one having the same authentication tag,
- it is clearly sufficient to transmit just the tag, since all the other information is redundant
- however, **the tag, by itself, provides perfect secrecy**: it can be uniquely decrypted by the recipient of the message, but no adversary has any information about the value of the plaintext
- that is, the underlying authentication scheme already provides perfect secrecy and hence it can be viewed as an encryption scheme

A New Scheme Based on 1-bit Authenticators

Suppose that $\mathcal{X} = \{0, \ldots, n-1\}$, $\mathcal{A} = \{0, 1\}$, $\mathcal{K} = \{0, 1\}^n$ and

$$f_K(j) = \kappa_j \bmod n$$

for all $K = (\kappa_0, \ldots, \kappa_{n-1})$ and all j.

For any K, x, there is one function in $\mathcal{E}(K, x)$, namely, $e_{K,x}$, where

$$e_{K,x}(j) = \begin{cases} \kappa_j & \text{if } j = x \\ 1 - \kappa_j & \text{if } j \neq x. \end{cases}$$

The authentication function f_K and the encryption function $e_{K,x}$ are "complements" of each other, except for the input x, where they agree.

An Improvement

- suppose we restrict the set of decryption keys to be

$$\mathcal{K}_E = \left\{ K = (\kappa_0, \ldots, \kappa_{n-1}) \in \{0,1\}^n, \sum_{i=0}^{n-1} \kappa_i = 0 \bmod 2 \right\}$$

- we reduce the number of decryption keys by a factor of two by only using keys with even hamming weight
- this modified scheme is denoted $\mathsf{CW}_E(n)$

Theorem 1

For any integer $k \geq 1$, the scheme $\mathsf{CW}_E(2^k)$ is an unconditionally secure chaffing-and-winnowing scheme for k-bit plaintexts, based on 1-bit authenticators, in which a decryption key consists of $2^k - 1$ bits and a ciphertext consists of 2^k bits.

Example

In the case $n = 4$, we present the sets $\mathcal{E}_E(K, x)$ in the scheme $(\mathcal{X}, \mathcal{A}, \mathcal{K}_E, \mathcal{E}_E, \mathcal{F})$:

K	$x = 0$	$x = 1$	$x = 2$	$x = 3$
$(0,0,0,0)$	$(0,1,1,1)$	$(1,0,1,1)$	$(1,1,0,1)$	$(1,1,1,0)$
$(0,0,1,1)$	$(0,1,0,0)$	$(1,0,0,0)$	$(1,1,1,0)$	$(1,1,0,1)$
$(0,1,0,1)$	$(0,0,1,0)$	$(1,1,1,0)$	$(1,0,0,0)$	$(1,0,1,1)$
$(0,1,1,0)$	$(0,0,0,1)$	$(1,1,0,1)$	$(1,0,1,1)$	$(1,0,0,0)$
$(1,0,0,1)$	$(1,1,1,0)$	$(0,0,1,0)$	$(0,1,0,0)$	$(0,1,1,1)$
$(1,0,1,0)$	$(1,1,0,1)$	$(0,0,0,1)$	$(0,1,1,1)$	$(0,1,0,0)$
$(1,1,0,0)$	$(1,0,1,1)$	$(0,1,1,1)$	$(0,0,0,1)$	$(0,0,1,0)$
$(1,1,1,1)$	$(1,0,0,0)$	$(0,1,0,0)$	$(0,0,1,0)$	$(0,0,0,1)$

Optimality

Lemma 2

Suppose $(\mathcal{X}, \mathcal{A}, \mathcal{K}, \mathcal{E}, \mathcal{F})$ *is any chaffing-and-winnowing scheme in which* $|\mathcal{X}| = n$ *and* $|\mathcal{A}| = 2$*. Suppose that* $K = (\kappa_0, \ldots, \kappa_{n-1}) \in \mathcal{K}$*,* $K' = (\kappa'_0, \ldots, \kappa'_{n-1})$ *and* $\mathsf{dist}(K, K') = 2$*, where* $\mathsf{dist}(\cdot, \cdot)$ *denotes the hamming distance between two vectors. Then* $K' \in \mathcal{K}$*.*

Theorem 3

Suppose $(\mathcal{X}, \mathcal{A}, \mathcal{K}, \mathcal{E}, \mathcal{F})$ *is any chaffing-and-winnowing scheme in which* $|\mathcal{X}| = n$ *and* $|\mathcal{A}| = 2$*. Then* $\mathcal{K}$ *must consist of all the binary* n*-tuples of even weight, all the binary* n*-tuples of odd weight, or all the binary* n*-tuples.*

Corollary 4

Suppose $(\mathcal{X}, \mathcal{A}, \mathcal{K}, \mathcal{E}, \mathcal{F})$ *is any chaffing-and-winnowing scheme in which* $|\mathcal{X}| = n$ *and* $|\mathcal{A}| = 2$*. Then* $|\mathcal{K}| \geq 2^{n-1}$*.*

A Hybrid Scheme

Suppose we have an ℓ-bit plaintext, where $\ell = rk$, and we break it into r blocks, each of which contains k bits. Each k-bit block is then encrypted using a scheme $\mathsf{CW}_E(2^k)$. In total, we have r independent schemes $\mathsf{CW}_E(2^k)$, each of which has an independently chosen key. Each possible ℓ-bit plaintext receives an r-bit authenticator, which is the concatenation of the 1-bit authenticators of each of the r blocks in the plaintext. This hybrid scheme, which will be denoted by $\mathsf{HCW}(r, k)$, has the following properties.

Theorem 5

For integers $k, r \geq 1$, the scheme $\mathsf{HCW}(r, k)$ is an unconditionally secure chaffing-and-winnowing scheme for rk-bit plaintexts, based on r-bit authenticators, in which a decryption key consists of $r(2^k - 1)$ bits and a ciphertext consists of $r\, 2^k$ bits.

References

- **G. Hanaoka, Y. Hanaoka, M. Hagiwara, H. Watanabe and H. Imai.**
  Unconditionally secure chaffing-and-winnowing: a relationship between encryption and authentication.
  Lecture Notes in Computer Science **3857** (2006), 154–162 (AAECC-16).

- **R.L. Rivest.**
  Chaffing and winnowing: confidentiality without encryption.
  CryptoBytes **4-1** (1998), 12–17.

- **D.R. Stinson.**
  Unconditionally secure chaffing and winnowing with short authentication tags.
  Advances in Mathematics of Communications **1** (2007), 269–280.