6 - Authentication

9 listopada 2010
20:53

The public channel needs to be authenticated, it is important that we use just a small part of the secret key from QKD for authentication of the next one.

m - message. Using key K we generate MAC (message authentication code) with some block cipher encryption and transmit: $MAC = f_K(m)$

(m, MAC)

Someone possessing K can verify that indeed MAC is obtained from m.

Length of the key k $\quad p_E \sim 2^{-k}$ probability of E figuring out the key

If $\mathcal{H}$ ε-strongly two-universal class of functions: $A \to B$:

(i) for any $x_1 \in A$ and $y_1 \in B$, $|\{h \in \mathcal{H} : h(x_1) = y_1\}| = \frac{|\mathcal{H}|}{|B|}$

(ii) for any $x_1 \neq x_2 \in A$ and $y_1, y_2 \in B$

$$|\{h \in \mathcal{H},\ h(x_1) = y_1 \wedge h(x_2) = y_2\}| \leq \frac{\varepsilon |\mathcal{H}|}{|B|^2}$$

if $\varepsilon = 1$ (ii) $\Rightarrow$ (i)

"$\leq$" $\Rightarrow$ "$=$"

Intuition: different inputs yield different outputs (more trivial for $|B| < |A|$)

$MAC = h_K(m)$

m ← message

K ← key (determines which function from $\mathcal{H}$ to use)

Security: (for each message we use new secure key)

a) Impersonation probability $\leq \frac{1}{|B|}$ ← (after seeing n messages E creates not-1 message)

b) substitution probability $\leq \frac{\varepsilon}{|B|}$ ← (modifies with message)

Proof:

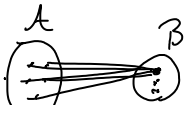
a) we transmit message $\{m, h_{K'}(m)\}$ with some $K' = 1 \ldots |\mathcal{H}|$

the true key is K. Probability that

$h_{K'}(m) = h_K(m) = MAC$ is equal to

$$\frac{|\{h \in \mathcal{H} : h(m) = MAC\}|}{|\mathcal{H}|} \leq \frac{1}{|B|}$$

{ for this we could have a very trivial class of constant functions with $|\mathcal{H}| = |B|$



6 - Authentication

9 listopada 2010
20:53

The public channel needs to be authenticated, it is important that we use just a small part of the secret key from QKD for authentication of the next one.

m - message. Using key K we generate MAC (message authentication code) with some block cipher encryption and transmit: $MAC = f_K(m)$

(m, MAC)

Someone possessing K can verify that indeed MAC is obtained from m.

Length of the key k $\quad p_E \sim 2^{-k}$ probability of E figuring out the key

If $\mathcal{H}$ ε-strongly two-universal class $\mathcal{H}$ of functions $h: A \to B$:

(i) for any $x_1 \in A$ and $y_1 \in B$, $|\{h \in \mathcal{H} : h(x_1) = y_1\}| = \frac{|\mathcal{H}|}{|B|}$

(ii) for any $x_1 \neq x_2 \in A$ and $y_1, y_2 \in B$

$$|\{h \in \mathcal{H}, h(x_1) = y_1 \wedge h(x_2) = y_2\}| \leq \frac{\varepsilon |\mathcal{H}|}{|B|^2}$$

if $\varepsilon = 1$ (ii) $\Rightarrow$ (i)

if $\varepsilon = 1$ (i) $\Rightarrow$ (ii)

Intuition: different inputs yield different outputs (more trivial for $|B| < |A|$)

$MAC = h_K(m)$

m — message

K — key (determines which function from $\mathcal{H}$ to use)

Security: (for each message we use new secure key)

a) Impersonation probability $\leq \frac{1}{|B|}$ (after seeing n messages E creates $n+1$ message)

b) substitution probability $\leq \frac{\varepsilon}{|B|}$ (modifies n-th message)

Proof:

a) we transmit message $\{m, h_{K'}(m)\}$ with some $K' = 1 \ldots |\mathcal{H}|$

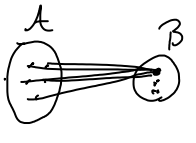
the true key is K. Probability that

$h_{K'}(m) = h_K(m) = MAC$ is equal to

$$\frac{|\{h \in \mathcal{H} : h(m) = MAC\}|}{|\mathcal{H}|} \leq \frac{1}{|B|}$$

For this we could have a very trivial class of constant functions with $|\mathcal{H}| = |B|$

We use k bits of K and have $\frac{1}{2^k}$ security. ok



b) We get $\{m, h_K(m)\}$ and want to substitute for $\{m', h_K(m')\}$ not knowing K. $(m' \neq m)$

probability that $h_{k'}(m') = h_k(m') = MAC'$ is

$$\frac{|\{h \in \mathcal{H} : h(m') = MAC' \wedge h(m) = MAC\}|}{|\{h \in \mathcal{H} : h(m) = MAC\}| \geq \frac{|\mathcal{H}|}{|\beta|}} \leq \frac{\frac{\varepsilon |\mathcal{H}|}{|\beta|^2}}{\frac{|\mathcal{H}|}{|\beta|}} = \frac{\varepsilon}{|\beta|}$$

In Practice

- Random binary matrices are strongly 2-universal

$b = M \cdot a + v$ ← rand. vector
↑ rand. Matrix

$|\mathcal{H}| = 2^{(a+1)\cdot b}$

require $k = (a+1)b$ bits of the key! (more than the message)

Proof:

(i) $\forall_{x_1, y_1}$ $|\{h : h(x_1) = y_1\}| \leq \frac{|\mathcal{H}|}{|\beta|}$

In our case $Mx_1 + v = y_1$ how many elements (M, v):

this gives $|\{h : h(x_1) = y_1\}| = 2^{a \cdot b} = \frac{2^{(a+1)b}}{2^b}$ ok —

(ii) $\forall_{x_1 \neq x_2} \forall_{y_1, y_2}$ $|\{h : h(x_1) = y_1 \wedge h(x_2) = y_2\}| \leq \frac{|\mathcal{H}|}{|\beta|^2}$ $(\varepsilon = 1)$

$Mx_1 + v = y_1$ $\quad M(\overbrace{x_1 - x_2}^{\neq 0}) = y_1 - y_2$

$Mx_2 + v = y_2$ $\quad$ there are $2^{(a+1)b}$ matrices

After choosing M, v is determined so

$|\mathcal{K}| = 2^{(a-1)b} = \frac{2^{(a+1)b}}{2^{2b}}$ ok

If there was no v we would have a problem.

- Toeplitz binary $a \times b$ matrices

Is it strongly 2-universal?

$T = b\left[\begin{matrix} 1 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 1 \end{matrix}\right]$ a $\quad T_{ij} = T_{i+k, j+k}$

y

$y = Tx + v$ ← random vector yes!
↑ Toeplitz

$k = a + b - 1 + b$ bits. $= a + 2b - 1$ bits

⌂ Proof

- There exist more efficient methods, see Series 5 ⌂ $\quad k \sim \log a$