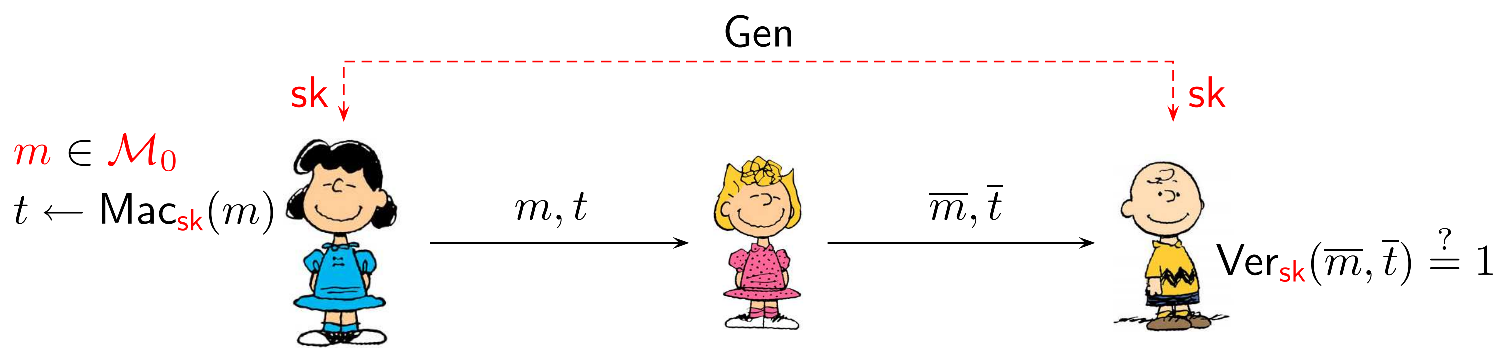
Message authentication

Sven Laur
swen@math.ut.ee

University of Tartu

Formal Syntax

Symmetric message authentication



- ▷ A randomised key generation algorithm outputs a secret key $\mathsf{sk} \in \mathcal{K}$ that must be transferred privately to the sender and to the receiver.
- ▷ A keyed hash function $\mathsf{Mac}_{\mathsf{sk}} : \mathcal{M} \rightarrow \mathcal{T}$ takes in a plaintext and outputs a corresponding digest (also known as hash value or tag).
- ▷ A verification algorithm $\mathsf{Ver}_{\mathsf{sk}} : \mathcal{M} \times \mathcal{C} \rightarrow \{0, 1\}$ tries to distinguish between altered and original message pairs.
- ▷ The authentication primitive is functional if for all $\mathsf{sk} \leftarrow \mathsf{Gen}$ and $m \in \mathcal{M}$:

$$\mathsf{Ver}_{\mathsf{sk}}(m, \mathsf{Mac}_{\mathsf{sk}}(m)) = 1$$

Two main attack types

▷ **Substitution attacks.** An adversary substitutes (m, t) with a different message pair $(\overline{m}, \bar{t})$. An adversary succeeds in deception if

$$\mathsf{Ver}_{\mathsf{sk}}(\overline{m}, \bar{t}) = 1 \qquad \text{and} \qquad m \neq \overline{m} \enspace .$$

▷ **Impersonation attacks.** An adversary tries to create a valid message pair $(\overline{m}, \bar{t})$ without seeing any messages from the sender. An adversary succeeds in deception if

$$\mathsf{Ver}_{\mathsf{sk}}(\overline{m}, \bar{t}) = 1 \enspace .$$

Maximal resistance against substitutions

For clarity, assume that $\mathcal{M} = \{0, 1\}$ and $\mathcal{K} = \{0, 1, 2, 3\}$. Then we can express the keyed hash function as a table

	0	1	2	3
0	a	b	c	d
1	e	f	g	h

For simplicity, assume that sk is chosen uniformly from $\mathcal{K}$. Now a, b, c and d are all different then the pair $(0, t)$ reveals the key sk. Hence, the optimal layout is following.

	0	1	2	3
0	a	a	b	b
1	a	b	a	b

Maximal resistance against impersonation

For clarity, assume that $\mathcal{M} = \{0,1\}$ and $\mathcal{K} = \{0,1,2,3\}$. Then the following keyed hash function achieves maximal impersonation resistance.

	0	1	2	3
0	a	b	c	d
1	a	b	c	d

However, this keyed hash function is insecure against substitution attacks.

Conclusion. Security against substitution attacks and security against impersonation attacks are contradicting requirements.

Information theoretical security

Authentication as hypothesis testing

The procedure $\mathsf{Ver}_{\mathsf{sk}}$ must distinguish between two hypotheses.

$\mathcal{H}_0$: The pair $c = (m, t)$ is created by the sender.

$\mathcal{H}_1$: The pair $c = (\overline{m}, \overline{t})$ is created by the adversary $\mathcal{A}$.

Let $\mathcal{C}_0$ and $\mathcal{C}_1$ be the corresponding distributions of messages.

Since the ratio of false negatives $\Pr[\mathsf{Ver}_{\mathsf{sk}}(m,t) = 0]$ must be zero, the optimal verification strategy is the following

$$\mathsf{Ver}_{\mathsf{sk}}(c) = 1 \quad \Leftrightarrow \quad c \in \mathrm{supp}(\mathcal{C}_0)$$

To defeat the message authentication primitive, the adversary $\mathcal{A}$ must chose the distribution $\mathcal{C}_1$ such that the ratio of false positives is maximal.

Kullback-Leibler divergence

Let $(p_x)_{x\in\{0,1\}^*}$ and $(q_x)_{x\in\{0,1\}^*}$ be two probability distributions. Then the Kullback-Leibler divergence is defined as

$$d(p\|q) \doteq \sum_{x:p_x>0} p_x \cdot \log_2 \frac{p_x}{q_x} \quad ,$$

Note that the Jensen's inequality assures

$$-d(p\|q) = \sum_{x:p_x>0} p_x \cdot \log_2 \frac{q_x}{p_x} \leq \log_2 \left(\sum_{x:p_x>0} q_x \right)$$

and consequently

$$\sum_{x:p_x>0} q_x \geq 2^{-d(p\|q)} \quad .$$

Lower bound on false positives

Fix a target message $\overline{m}$. Then by construction

$$\Pr\left[\mathsf{Ver}_{\mathsf{sk}}(\overline{m},\bar{t})=1\right]=\sum_{p_{t,\mathsf{sk}}>0} q_{t,\mathsf{sk}} \geq 2^{-d(p\|q)}$$

where

$$p_{t,\mathsf{sk}} = \Pr\left[\mathsf{sk} \leftarrow \mathsf{Gen} : \mathsf{sk} \wedge \text{The sender creates } t \text{ for } \overline{m}\right]$$
$$q_{t,\mathsf{sk}} = \Pr\left[\mathsf{sk} \leftarrow \mathsf{Gen} : \mathsf{sk} \wedge \text{The adversary creates } t \text{ for } \overline{m}\right]$$

Simplest impersonation attack

Consider the following attack

$$\mathcal{A}_{\overline{m}}\left[\begin{array}{l}\overline{\mathsf{sk}} \leftarrow \mathsf{Gen} \\ \bar{t} \leftarrow \mathsf{Mac}_{\overline{\mathsf{sk}}}(\overline{m}) \\ \text{return } (\overline{m}, \bar{t})\end{array}\right.$$

Then obviously

$$\Pr\left[\,\bar{t}\,\right] = \sum_{\overline{\mathsf{sk}}} \Pr\left[\mathsf{sk} \leftarrow \mathsf{Gen} : \mathsf{sk} = \overline{\mathsf{sk}}\right] \cdot \Pr\left[\bar{t} \leftarrow \mathsf{Mac}_{\overline{\mathsf{sk}}}(\overline{m})\right]$$

is a marginal distribution of $\bar{t}$ generated by the sender.

Success probability

Let us now compute the corresponding Kullback-Leibler divergence

$$\begin{aligned} d(p\|q) &= \sum_{\mathsf{sk},t} p_{t,\mathsf{sk}} \cdot \log_2 \frac{p_{t,\mathsf{sk}}}{p_{\mathsf{sk}} \cdot p_t} \\ &= \sum_{\mathsf{sk},t} p_{t,\mathsf{sk}} \cdot \log_2 p_{t,\mathsf{sk}} - \sum_{\mathsf{sk},t} p_{t,\mathsf{sk}} \log_2 p_{\mathsf{sk}} - \sum_{\mathsf{sk},t} p_{t,\mathsf{sk}} \cdot \log_2 p_t \\ &= -H(\mathsf{sk}, t) + H(\mathsf{sk}) + H(t) \end{aligned}$$

and thus

$$\Pr\left[\text{Successful impersonation}\right] \geq 2^{H(\mathsf{sk},t)-H(\mathsf{sk})-H(t)} = 2^{-I(\mathsf{sk}:t)}$$

for a fixed target message $\overline{m}$.

An obvious substitution attack

To replace m with $\overline{m}$, we can use the following strategy:

$$\mathcal{A}(m, t, \overline{m})$$
$$\left[\begin{array}{l}\mathsf{sk}_* \leftarrow \operatorname*{argmax}_{\overline{\mathsf{sk}}} \Pr\left[\mathsf{sk} \leftarrow \mathsf{Gen} : \mathsf{sk} = \overline{\mathsf{sk}} | m, t\right] \\ \overline{t} \leftarrow \mathsf{Mac}_{\mathsf{sk}_*}(\overline{m}) \\ \mathsf{return}\ (\overline{m}, \overline{t})\end{array}\right.$$

Obviously, the adversary $\mathcal{A}$ succeeds if it guesses the key sk

$$\begin{aligned}\Pr\left[\text{Success}\right] &\geq \Pr\left[\mathsf{sk} \leftarrow \mathsf{Gen} : \mathsf{sk} = \mathsf{sk}_*\right] \\ &\geq \sum_t \Pr\left[t = \mathsf{Mac}_{\mathsf{sk}}(m)\right] \cdot \max_{\overline{\mathsf{sk}}} \Pr\left[\mathsf{sk} = \overline{\mathsf{sk}} | t\right] \quad .\end{aligned}$$

Properties of conditional entropy

Note that for any distribution $(p_x)_{x\in\{0,1\}^*}$

$$H_\infty(X) = -\log_2\left(\max_{x:p_x>0} p_x\right) = \min_{x:p_x>0}(-\log_2 p_x)$$
$$\leq \sum_{x:p_x>0} p_x\cdot(-\log_2 p_x) = H(X) \enspace .$$

Now for two variables

$$\sum_y \Pr[y]\cdot\max_x \Pr[x|y] = \sum_y \Pr[y]\cdot 2^{-H_\infty(X|y)} \geq \sum_y \Pr[y]\cdot 2^{-H(X|y)}$$
$$\geq 2^{\sum_y \Pr[y]\cdot(-H(X|y))} = 2^{-H(X|Y)} \enspace ,$$

where the second inequality follows from Jensen's inequality.

Lower bound on success probability

As the success probability of our impersonation attack is

$$\begin{aligned}\Pr[\text{Success}] &= \Pr[\mathsf{sk} \leftarrow \mathsf{Gen} : \mathsf{sk} = \mathsf{sk}_*] \\ &= \sum_t \Pr[t = \mathsf{Mac}_{\mathsf{sk}}(m)] \cdot \max_{\overline{\mathsf{sk}}} \Pr\left[\mathsf{sk} = \overline{\mathsf{sk}} | t\right] \quad ,\end{aligned}$$

we can rewrite in terms of conditional entropy

$$\Pr[\text{Success}] \geq 2^{-H(\mathsf{sk}|t)} \quad .$$

Simmons's lower bounds

For any message authentication primitive

$$\Pr\left[\textsf{Successful impersonation}\right] \geq \max_{m\in\mathcal{M}} \left\{2^{-I(\textsf{sk}:t)}\right\}$$

$$\Pr\left[\textsf{Successful substitution}\right] \geq \max_{m\in\mathcal{M}} \left\{2^{-H(\textsf{sk}|t)}\right\}$$

and thus

$$\Pr\left[\textsf{Successful attack}\right] \geq \max_{m\in\mathcal{M}} \left\{2^{-\min\{I(\textsf{sk}:t),H(\textsf{sk}|t)\}}\right\} \geq \max_{m\in\mathcal{M}} \left\{2^{-\frac{H(\textsf{sk})}{2}}\right\}$$

since $I(\textsf{sk}:t) = H(\textsf{sk}) + H(t) - H(\textsf{sk},t) = H(\textsf{sk}) - H(\textsf{sk}|t)$.

Examples

Universal hash functions

A universal hash function $h : \mathcal{M} \times \mathcal{K} \to \mathcal{T}$ is a keyed hash function such that for any two different inputs $m_0 \neq m_1$, the corresponding hash values $h(m_0, k)$ and $h(m_1, k)$ are independent and have a uniform distribution over $\mathcal{T}$ when k is chosen uniformly from $\mathcal{K}$.

Corollary. An authentication protocol that uses a universal hash function h achieves maximal security against impersonation and substitution attacks

$$\Pr\left[\text{Successful deception}\right] \leq \frac{1}{|\mathcal{T}|}$$

Example. A function $h(m, k_0\|k_1) = k_1 \cdot m + k_0$ is a universal hash function if $\mathcal{M} = \mathsf{GF}(2^n)$, $\mathcal{K} = \mathsf{GF}(2^n) \times \mathsf{GF}(2^n)$ and operations are done in $\mathsf{GF}(2^n)$.

Polynomial message authentication code

Let $m_1, m_2, \ldots, m_\ell$ be n-bit blocks of the message and $k_0, k_1 \in \mathsf{GF}(2^n)$ sub-keys for the hash function. Then we can consider a polynomial

$$f(x) = m_\ell \cdot x^\ell + m_{\ell-1} \cdot x^{\ell-1} + \cdots + m_1 \cdot x$$

over $\mathsf{GF}(2^n)$ and define the hash value as

$$h(m, k) = f(k_1) + k_0 \enspace .$$

If k_0 is chosen uniformly over $\mathsf{GF}(2^n)$ then the hash value $h(m, k)$ is also uniformly distributed over $\mathsf{GF}(2^n)$:

$$\Pr\left[\text{Successful impersonation}\right] \leq 2^{-n} \enspace .$$

Security against substitution attacks

Let $\mathcal{A}$ be the best substitution strategy. W.l.o.g. we can assume that $\mathcal{A}$ is a deterministic strategy. Consequently, we have to bound the probability

$$\max_{m\in\mathcal{M}} \Pr\left[k \leftarrow \mathcal{K}, (\overline{m}, \overline{t}) \leftarrow \mathcal{A}(m, h(m,k)) : h(\overline{m}, k) = \overline{t} \wedge m \neq \overline{m}\right] \quad .$$

Since $\mathcal{A}$ outputs always the same reply for $k \in \mathcal{K}$ such that $h(m,k) = t$, we must find cardinalities of the following sets:

- ▷ a set of all relevant keys $\mathcal{K}_{\mathrm{all}} = \{k \in \mathcal{K} : h(m,k) = t\}$
- ▷ a set of good keys $\mathcal{K}_{\mathrm{good}} = \left\{k \in \mathcal{K} : h(m,k) = t \wedge h(\overline{m}, k) = \overline{t}\right\}$.

Some algebraic properties

For each m, t and k_1, there exists one and only one value of k_0 such that $h(m,k) = t$. Therefore, $|\mathcal{K}_{\mathrm{all}}| = 2^\ell$ for any m and t.

If $h(m,k) = t$ and $h(\overline{m},k) = \overline{t}$ then

$$h(m,k) - h(\overline{m},k) - t + \overline{t} = 0$$
$$\Updownarrow$$
$$f_m(k_1) - f_{\overline{m}}(k_1) - t + \overline{t} = 0$$
$$\Updownarrow$$
$$f_{m-\overline{m}}(k_1) - t + \overline{t} = 0$$

This equation has at most ℓ solutions $k_1 \in \mathsf{GF}(2^n)$, since degree of $f_{m-\overline{m}}(x)$ is at most ℓ. Since k_1, m, t uniquely determine k_0, we get $|\mathcal{K}_{\mathrm{good}}| \leq \ell$.

The corresponding bounds

Hence, we have obtained

$$\Pr\left[k \leftarrow \mathcal{K} : h(\overline{m}, k) = \bar{t} | m \neq \overline{m}, t\right] = \frac{|\mathcal{K}_{\mathrm{good}}|}{|\mathcal{K}_{\mathrm{all}}|} \leq \frac{\ell}{2^n} \enspace .$$

Since

$$\begin{aligned}
&\Pr\left[k \leftarrow \mathcal{K}, (\overline{m}, \bar{t}) \leftarrow \mathcal{A}(m, h(m,k)) : h(\overline{m}, k) = \bar{t} \wedge m \neq \overline{m}\right] \\
&\leq \sum_t \Pr\left[k \leftarrow \mathcal{K} : h(m,k) = t\right] \cdot \max_{\substack{\overline{m} \neq m \\ \bar{t} \in \mathcal{T}}} \Pr\left[h(\overline{m}, k) = \bar{t} | m \neq \overline{m}, t\right] \\
&\leq \sum_t \Pr\left[k \leftarrow \mathcal{K} : h(m,k) = t\right] \cdot \frac{\ell}{2^n} \leq \frac{\ell}{2^n} \enspace ,
\end{aligned}$$

we also have a success bound on substitution attacks.

Computational security

Authentication with pseudorandom functions

Consider following authentication primitive:

- ▷ secret key $f \xleftarrow[u]{} \mathcal{F}_{\mathrm{all}}$ where $\mathcal{F}_{\mathrm{all}} = \{f : \mathcal{M} \to \mathcal{T}\}$;
- ▷ authentication code $\mathsf{Mac}_f(m) = f(m)$
- ▷ verification procedure $\mathsf{Ver}_f(m, t) = 1 \Leftrightarrow f(m) = t$.

This authentication primitive is $\frac{1}{|\mathcal{T}|}$ secure against impersonation and substitution attacks, since Mac is a universal hash function.

As this construction is practically uninstantiable, we must use (t, q, ε)-pseudorandom function family $\mathcal{F}$ instead of $\mathcal{F}_{\mathrm{all}}$. As a result

$$\Pr\left[\text{Successful attack}\right] \leq \frac{1}{|\mathcal{T}|} + \varepsilon$$

against all t-time adversaries if $q \geq 1$.

Formal security definition

A keyed hash function $h : \mathcal{M} \times \mathcal{K} \to \mathcal{T}$ is a (t, q, ε)-secure message authentication code if any t-time adversary $\mathcal{A}$:

$$\mathsf{Adv}_h^{\mathsf{mac}}(\mathcal{A}) = \Pr\left[\mathcal{G}^{\mathcal{A}} = 1\right] \leq \varepsilon \enspace ,$$

where the security game is following

$$\begin{array}{l}
\mathcal{G}^{\mathcal{A}} \\
\left[\begin{array}{l}
k \xleftarrow[u]{} \mathcal{K} \\
\quad \text{For } i \in \{1, \ldots, q\} \text{ do} \\
\quad \left[\ \text{Given } m_i \leftarrow \mathcal{A} \text{ send } t_i \leftarrow h(m_i, k) \text{ back to } \mathcal{A}\right. \\
(m, t) \leftarrow \mathcal{A} \\
\text{return } [t \stackrel{?}{=} h(m, k)] \wedge [(m, t) \notin \{(m_1, t_1), \ldots, (m_q, t_q)\}]
\end{array}\right.
\end{array}$$

Problems with multiple sessions

All authentication primitives we have considered so far guarantee security if they are used only once. A proper message authentication protocol can handle many messages. Therefore, we use additional mechanisms besides the authentication primitive to assure:

- ▷ security against reflection attacks
- ▷ message reordering
- ▷ interleaving attacks

Corresponding enhancement techniques

- ▷ Use nonces to defeat reflection attacks.
- ▷ Use message numbering against reordering.
- ▷ Stretch secret key using pseudorandom generator.