Lecture 12

Authentication and integrity protection

Nicola Laurenti November 6, 2020

Lecture 12— Contents

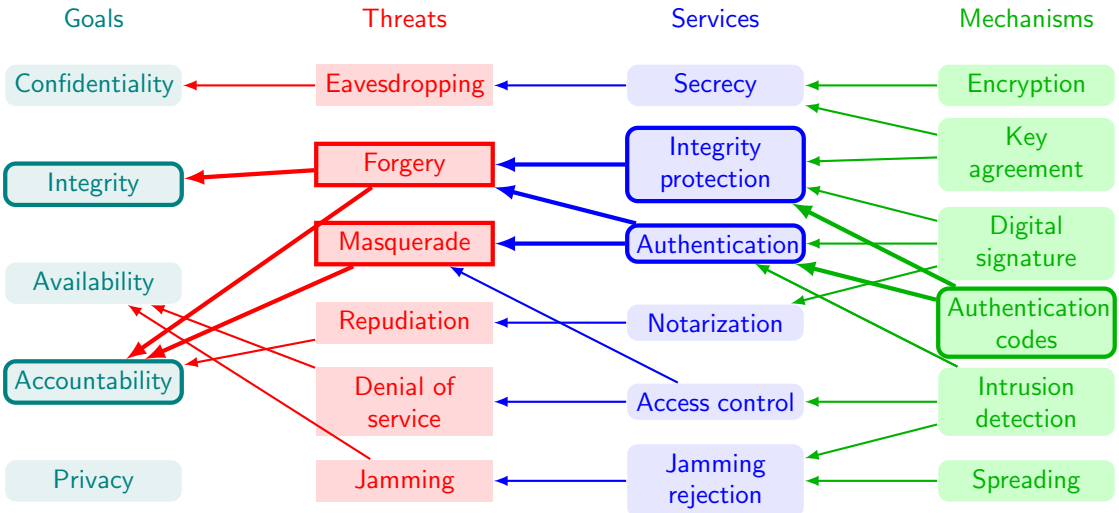
General model for authentication and integrity protection

Unconditionally secure authentication and integrity protection

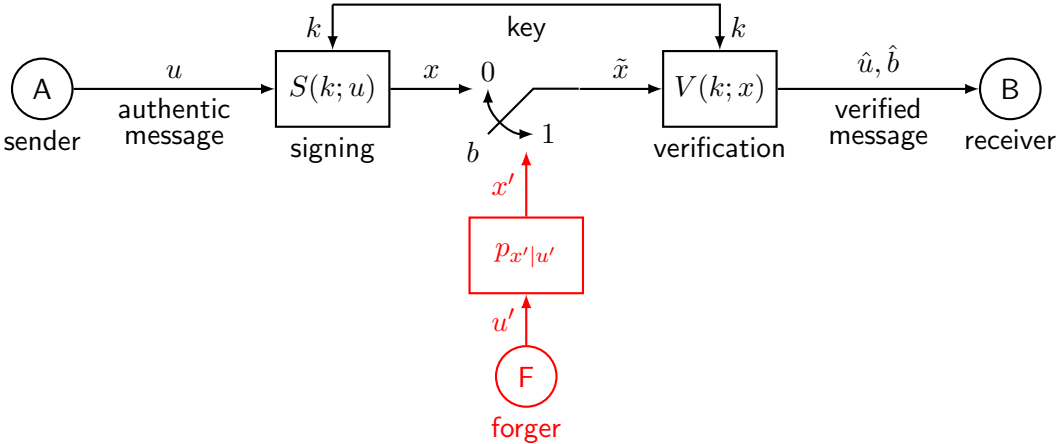
Universal hashing

Lower bounds on key entropy

Security goals, threats, services and mechanisms



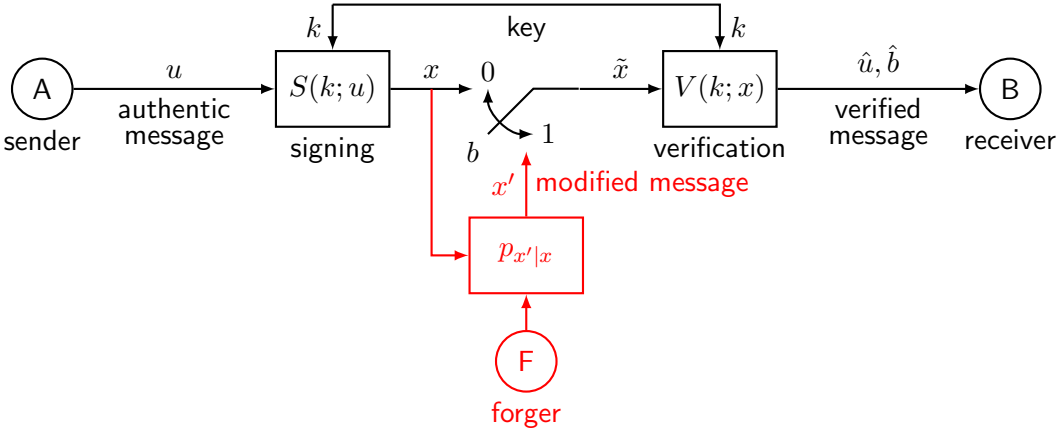
General model of the authentication problem



Forging attack

F wants to build x' so that $\hat{u} = u'$ and $\hat{b} = 0$ (i.e., u' is accepted)

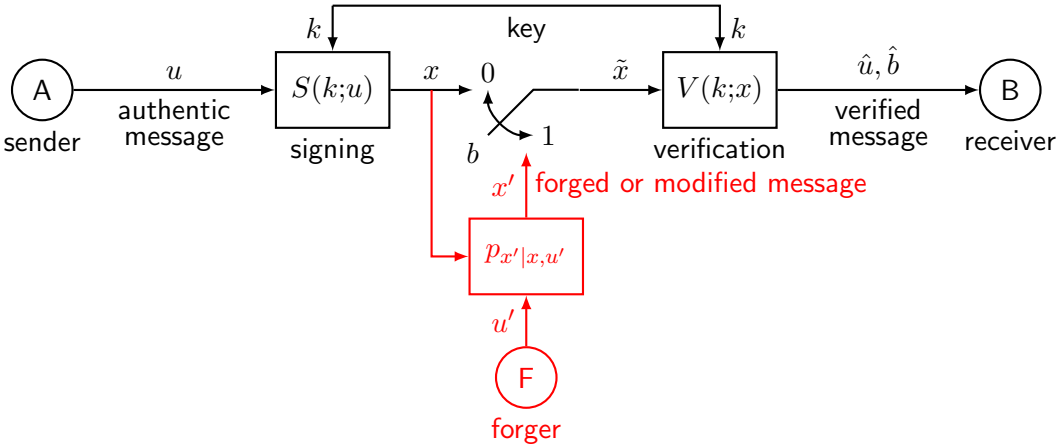
General model of the integrity protection problem



Illegitimate modification (alteration) attack

F can block x and wants to replace it with x' such that $\hat{u} \neq u$ and $\hat{b} = 0$

Authentication + integrity protection system



Authentication tags

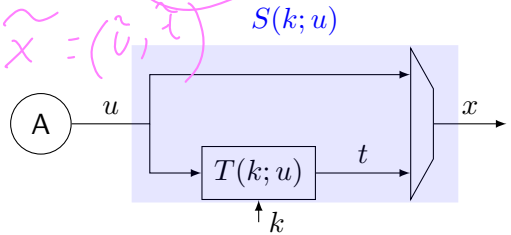
A typical solution for signing is to append a tag to the message

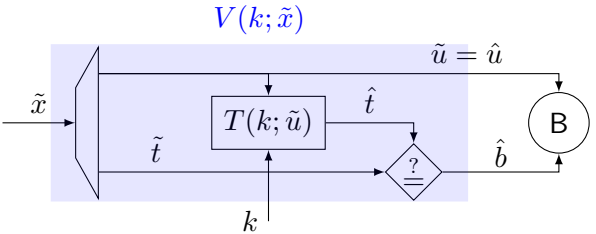
$$x = (u, t) \quad , \quad t = T(k, u)$$

The tag depends on both the key and the message

The corresponding verification splits the received signal into message and tag, computes the correct tag on the received message and checks it against the received tag

$$\tilde{x} = (\tilde{u}, \tilde{t}) \quad , \quad \hat{t} = T(k, \tilde{u}) \quad , \quad \hat{u} = \tilde{u} \quad , \quad \hat{b} = \begin{cases} 0 & , \text{ if } \tilde{t} = \hat{t} \\ 1 & , \text{ if } \tilde{t} \neq \hat{t} \end{cases}$$





Glossary and notation

authentic message	$u \in \mathcal{M}$	message space
false message	$u' \in \mathcal{M}$	
decoded message	$\tilde{u} \in \mathcal{M}$	
authenticated/signed message	$x \in \mathcal{X}$	signed message space
forged/modified message	$x' \in \mathcal{X}$	
received message	$\tilde{x} \in \mathcal{X}$	
authentication tag	$t \in \mathcal{T}$	tag space
forged/modified tag	$t' \in \mathcal{T}$	
received tag	$\tilde{t} \in \mathcal{T}$	
verification tag	$\hat{t} \in \mathcal{T}$	
authentication key	$k \in \mathcal{K}$	key space

Glossary and notation

signing map $S : \mathcal{K} \times \mathcal{M} \mapsto \mathcal{X}$

$S_k : \mathcal{M} \mapsto \mathcal{X} \quad S_k(u) \doteq S(k, u)$

verification map $V : \mathcal{K} \times \mathcal{X} \mapsto \mathcal{M} \times \{0, 1\}$

$V_k : \mathcal{X} \mapsto \mathcal{M} \times \{0, 1\} \quad V_k(x) \doteq V(k, x)$

tag computation map $T : \mathcal{K} \times \mathcal{M} \mapsto \mathcal{T}$

$T_k : \mathcal{M} \mapsto \mathcal{T} \quad T_k(u) \doteq T(k, u)$

The authentication and integrity protection system is completely specified as:

$$\mathcal{S} = (\mathcal{M}, \mathcal{X}, \mathcal{K}, S, V, p_u, p_k)$$

or, with the appended tag solution, as:

$$\mathcal{S} = (\mathcal{M}, \mathcal{T}, \mathcal{K}, T, p_u, p_k)$$

General assumptions

- (correctness) The receiver must be able to recover and accept any authentic message

$$V_k(S_k(u)) = (u, 0) \quad \forall k \in \mathcal{K}, u \in \mathcal{M}$$

- (Kerchoff-like assumption) The forger F knows the system $\mathcal{S}$ (in particular the maps $S(\cdot,\cdot)$ and $V(\cdot,\cdot)$, or $T(\cdot,\cdot)$)

Where does authenticity come from?

Non forgeability of x is only based on the fact that the attacker does not know the actual realization of k and hence the particular $S_k(\cdot)$, $V_k(\cdot)$, or $T_k(\cdot)$ used

Attack classes

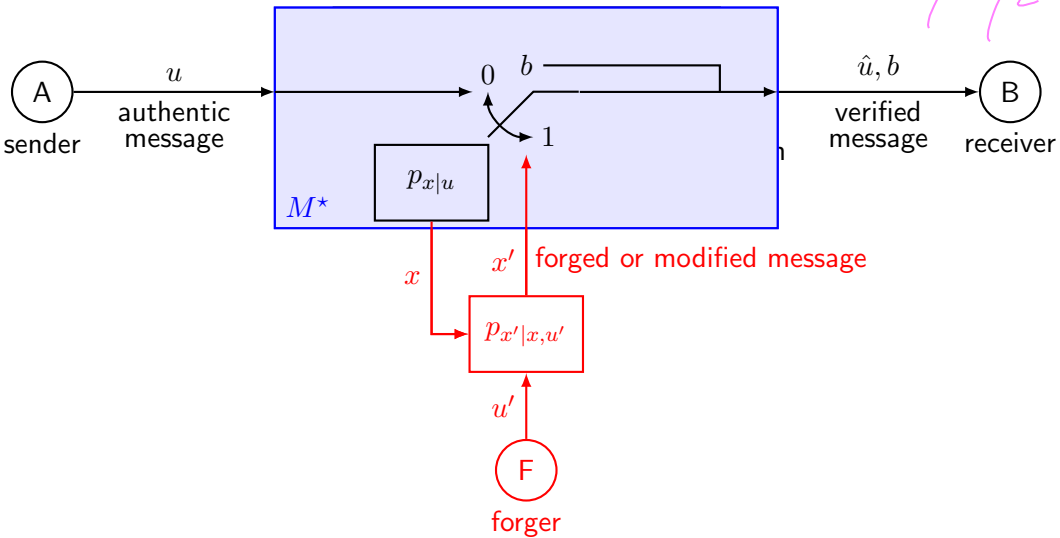
The class $\mathcal{A}_{\mathsf{f}}$ of forging attacks

- the attacker cannot block signed messages
- has a particular target message u'
- probabilistic forging strategy represented by the conditional pmd $p_{x'|u'}(\cdot|\cdot)$, or the joint pmd $p_{u'x'}(\cdot,\cdot)$
- success event $S_{\mathsf{f}} = \{\hat{u} = u'\} \cap \{\hat{b} = 0\}$

The class $\mathcal{A}_{\mathsf{m}}$ of modification attacks

- the attacker can block signed messages and replace them
- does not target a particular message
- probabilistic modification strategy represented by the conditional pmd $p_{x'|x}(\cdot|\cdot)$
- success event $S_{\mathsf{m}} = \{\hat{u} \neq u\} \cap \{\hat{b} = 0\}$

Ideal world model



Unconditionally secure authentication + integrity protection

In terms of distinguishability from the ideal counterpart

$$
\begin{aligned}
d(M, M^\star) &= d_{\mathsf{V}}(p_{\hat{u}\hat{b}|ux'b}, p_{\hat{u}^\star\hat{b}^\star|ux'b}) \\
&\leq d_{\mathsf{V}}(p_{\hat{u}\hat{b}|ux'b}, p_{\hat{u}^\star\hat{b}|ux'b}) + d_{\mathsf{V}}(p_{\hat{u}^\star\hat{b}|ux'b}, p_{\hat{u}^\star\hat{b}^\star|ux'b}) \\
&\leq \max_a \mathrm{P}\left[\hat{u} \neq a | u = a, b = 0\right] + \max\left\{p_{\hat{b}|b}(1|0), p_{\hat{b}|b}(0|1)\right\} \\
&= p_{\mathsf{e}} + \max\left\{p_{\mathsf{FA}}, p_{\mathsf{MD}}\right\}
\end{aligned}
$$

One time pad authentication

We aim for ε-unconditionally secure authentication against forging, i.e.

$$\mathrm{P}\left[S_{\mathsf{f}}; M, A\right] \leq \varepsilon \quad , \quad \forall A \in \mathcal{A}_{\mathsf{f}}$$

A possible solution is a mechanism M of the tag appending type, described by

$$\begin{aligned}
&\text{equal tag and key spaces } \mathcal{T} = \mathcal{K} \\
&\text{uniform distributed key } \; k \sim \mathcal{U}(\mathcal{K}) \quad \Leftrightarrow \quad p_k(a) = \frac{1}{|\mathcal{K}|} \, \forall a \in \mathcal{K} \\
&\text{sign by appending the key } \; t = T(k,u) = k \quad , \quad x = (u,k) \\
&\text{verify by checking the key } \; \hat{b} = \begin{cases} 0 & , \text{ if } \tilde{t} = k \\ 1 & , \text{ if } \tilde{t} \neq k \end{cases}
\end{aligned}$$

One time pad authentication

Correctness

Trivially, $b = 0 \quad \Rightarrow \quad \tilde{x} = x = (u, k) \quad \Rightarrow \quad \tilde{t} = k \quad \Rightarrow \quad \hat{b} = 0$

Security

Consider the class $\mathcal{A}_{\mathsf{f}}$ of forging attacks, where x' is independent of k and observe that

$$S_{\mathsf{f}} = \left\{\hat{u} = u', \hat{b} = 0\right\} = \left\{t' = k\right\}$$

$$\text{so that} \quad \mathrm{P}\left[S_{\mathsf{f}}\right] = \mathrm{P}\left[t' = k\right] = \sum_{a \in \mathcal{K}} \mathrm{P}\left[t' = a, k = a\right]$$

$$\text{(by independence)} \quad = \sum_{a \in \mathcal{K}} p_{t'}(a) p_k(a) = \sum_{a \in \mathcal{K}} p_{t'}(a) \frac{1}{|\mathcal{K}|} = \frac{1}{|\mathcal{K}|}$$

yielding ε-unconditional security, for $\varepsilon \geq 1/|\mathcal{K}|$, that is, if $H(k) \geq \log_{1/2} \varepsilon$

Universal hashing

OTP authentication cannot offer integrity protection

Trivial attack: F blocks $x = (u, k)$, replaces u with u', transmists $x' = (u', k)$
B verifies that $t' = k$ and accepts u'

Need $\{T_k(u)\}_{k \in \mathcal{K}}$ to be a ε-almost strongly universal$_2$ family of hashing functions for some parameter $\varepsilon \in (0, 1)$, that is

1. $T_k : \mathcal{M} \to \mathcal{T}$, $\forall k \in \mathcal{K}$
2. (uniform mapping) $\forall u \in \mathcal{M}, t \in \mathcal{T}$, it must be $|\mathcal{K}_{u \to t}| \leq \varepsilon |\mathcal{K}|$, where

$$\mathcal{K}_{u \to t} = \{k \in \mathcal{K} : T_k(u) = t\}$$

3. (uniform collisions) $\forall u_1 \neq u_2 \in \mathcal{M}$, it must be $|\mathcal{K}_{u_1 u_2}| \leq \varepsilon |\mathcal{K}|$, where

$$\mathcal{K}_{u_1 u_2} = \{k \in \mathcal{K} : T_k(u_1) = T_k(u_2)\}$$

Strongly universal families

What is the lowest (tightest) possible value for ε ?

for uniform mapping

Since, for any fixed u, the sets $\{\mathcal{K}_{u\to t}, t \in \mathcal{T}\}$ make up a partition of $\mathcal{K}$, we have

$$\mathcal{K} = \bigcup_{t\in\mathcal{T}} \mathcal{K}_{u\to t}$$

$$|\mathcal{K}| = \sum_{t\in\mathcal{T}} |\mathcal{K}_{u\to t}|$$

$$|\mathcal{K}| \leq \sum_{t\in\mathcal{T}} \varepsilon\,|\mathcal{K}| = |\mathcal{T}|\,\varepsilon\,|\mathcal{K}|$$

$$\varepsilon \geq \frac{1}{|\mathcal{T}|}$$

for uniform collisions

If $|\mathcal{M}| \leq |\mathcal{T}|$ there may be no collisions at all, so it can be $\varepsilon = 0$
On the other hand, if $|\mathcal{M}| \gg |\mathcal{T}|$

$$\varepsilon \geq \frac{1}{|\mathcal{T}|}\,\frac{|\mathcal{M}| - |\mathcal{T}|}{|\mathcal{M}| - 1}$$

$$\varepsilon \gtrsim \frac{1}{|\mathcal{T}|} \quad (\text{if } |\mathcal{M}| \gg |\mathcal{T}|\,)$$

An ε-almost strongly universal$_2$ family where $\varepsilon = 1/|\mathcal{T}|$ is called strongly universal$_2$

Classes of strongly universal$_2$ hashing functions

Example (All the functions)

The class of all the functions mapping $\mathcal{M}$ to $\mathcal{T}$ is strongly universal$_2$. Its cardinality is $|\mathcal{K}| = |\mathcal{T}|^{|\mathcal{M}|}$, and $H(k) = |\mathcal{M}| \log_2 |\mathcal{T}|$.

Example (All the linear functions, i.e. matrices)

If $\mathcal{M} = \mathbb{F}^{\ell_u}$, $\mathcal{T} = \mathbb{F}^{\ell_t}$, with $\mathbb{F}$ a finite field, the class of all the matrices $\mathbb{F}^{\ell_t \times \ell_u}$ is ε-universal$_2$ with $\varepsilon = 1/|\mathcal{T}|$. Its cardinality is $|\mathcal{K}| = |\mathbb{F}|^{\ell_t \ell_u} = |\mathcal{T}|^{\ell_u}$, and $H(k) = \ell_t \ell_u \log_2 |\mathbb{F}|$.

Example (All the Toeplitz matrices)

If $\mathcal{M} = \mathbb{F}^{\ell_u}$, $\mathcal{T} = \mathbb{F}^{\ell_t}$, with $\mathbb{F}$ a finite field, the class of all the Toeplitz matrices in $\mathbb{F}^{\ell_t \times \ell_u}$ is ε-universal$_2$ with $\varepsilon = 1/|\mathcal{T}|$. Its cardinality is $|\mathcal{K}| = |\mathbb{F}|^{\ell_t + \ell_u - 1} = |\mathcal{T}| \cdot |\mathcal{M}| / |\mathbb{F}|$, and $H(k) = (\ell_u + \ell_t - 1) \log_2 |\mathbb{F}|$.

Unconditional security of universal$_2$ hashing functions

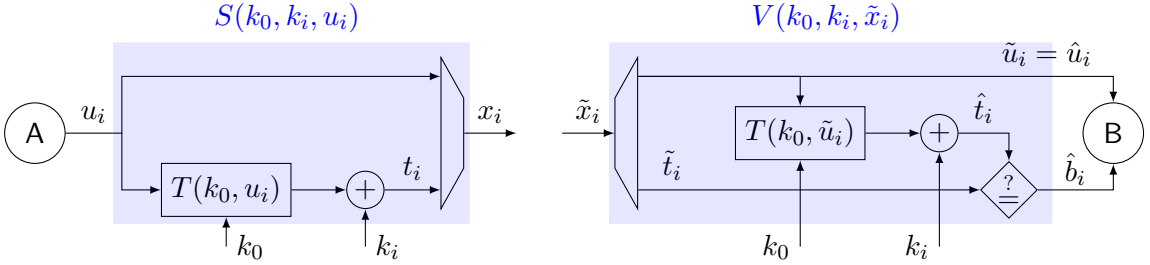
If the class of tag computation functions is ε-universal$_2$ for some $\varepsilon > 0$, the A+IP mechanism is ε-unconditionally secure against forging and modification attacks.

Unconditionally secure A+IP for multiple messages

Unconditionally secure authentication + integrity protection for a sequence of messages $u_1, \ldots, u_L$ can be obtained with universal hashing + one time pads

$$x_i = (u_i, t_i) \quad , \quad t_i = T(k_0, u) + k_i \quad , \quad i = 1, \ldots, L$$

This uses the same key k_0 for integrity protection of all messages and one key k_i for authentication of each message



Kullback-Leibler divergence for discrete rvs

Definition

Given two discrete rvs, x, y with alphabets $\mathcal{A}_x \subset \mathcal{A}_y$ and pmds p_x, p_y, their Kullback-Leibler divergence is

$$\mathrm{D}\left(p_x \| p_y\right) = \mathrm{E}\left[\log_2 \frac{p_x(x)}{p_y(x)}\right] = \sum_{a \in \mathcal{A}_x} p_x(a) \log_2 \frac{p_x(a)}{p_y(a)}$$

Example: Binary rvs

For binary rvs, with $\mathcal{A} = \{0, 1\}$,

$$\mathrm{D}\left(p_x \| p_y\right) = p_x(0) \log_2 \frac{p_x(0)}{p_y(0)} + p_x(1) \log_2 \frac{p_x(1)}{p_y(1)}$$

The KLD definition can be extended to the case $\mathcal{A}_x \not\subset \mathcal{A}_y$ (i.e. $p_y(a) = 0$ for some $a \in \mathcal{A}_x$), by letting $\mathrm{D}\left(p_x \| p_y\right) = \infty$ in that case

Kullback-Leibler divergence (cont.)

The KLD is a measure of statistical distance between rvs. It is related to their distinguishability

Properties

1. (positivity) $\mathrm{D}\left(p_x \| p_y\right) \geq 0$, $\forall p_x, p_y$
   and $\mathrm{D}\left(p_x \| p_y\right) = 0$ if and only if $p_x \equiv p_y$
2. (asymmetry) $\mathrm{D}\left(p_x \| p_y\right) \neq \mathrm{D}\left(p_y \| p_x\right)$, in general
3. (relation with entropy) If x, y are discrete and $y \sim \mathcal{U}(\mathcal{A}_x)$, $\mathrm{D}\left(p_x \| p_y\right) = H(y) - H(x)$.
4. (relation with mutual information) Let x, y have joint pmd p_{xy} and let x', y' be independent rvs with $p_{x'} = p_x$ and $p_{y'} = p_y$. Then,

$$\begin{aligned}\mathrm{D}\left(p_{xy} \| p_{x'y'}\right) &= \mathrm{E}\left[\log_2 \frac{p_{xy}(x,y)}{p_{x'y'}(x,y)}\right] = \mathrm{E}\left[\log_2 \frac{p_{xy}(x,y)}{p_{x'}(x) p_{y'}(y)}\right] \\ &= \mathrm{E}\left[\log_2 \frac{p_{xy}(x,y)}{p_x(x) p_y(y)}\right] = I(x,y) \quad \left(\text{aka } \mathrm{D}\left(p_{xy} \| p_x p_y\right)\right)\end{aligned}$$

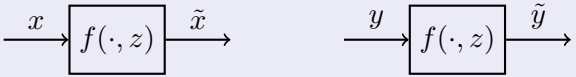
Kullback-Leibler divergence (cont.)

Properties (cont.)

5. (independent lower bound) Let x, y have joint pmd p_{xy}. For any x' independent of y, $\mathrm{D}\left(p_{xy} \| p_{x'y}\right) \geq I(x, y)$. Proof:

$$\begin{aligned}
\mathrm{D}\left(p_{xy} \| p_{x'y}\right) &= \mathrm{E}\left[\log_2 \frac{p_{xy}(x,y)}{p_{x'}(x)p_y(y)}\right] = \mathrm{E}\left[\log_2 \left(\frac{p_{xy}(x,y)}{p_x(x)p_y(y)} \frac{p_x(x)}{p_{x'}(x)}\right)\right] \\
&= \mathrm{E}\left[\log_2 \frac{p_{xy}(x,y)}{p_x(x)p_y(y)}\right] + \mathrm{E}\left[\log_2 \frac{p_x(x)}{p_{x'}(x)}\right] \\
&= I(x;y) + \mathrm{D}\left(p_x \| p'_x\right) \geq I(x;y)
\end{aligned}$$

6. (data processing inequality) If $\tilde{x} = f(x, z)$ and $\tilde{y} = f(y, z)$ for some function f and rv z independent of x, y, then $\mathrm{D}\left(p_x \| p_y\right) \geq \mathrm{D}\left(p_{\tilde{x}} \| p_{\tilde{y}}\right)$



Authentication as binary hypothesis testing

The authentication problem can be seen as a special case of binary hypothesis testing

Problem

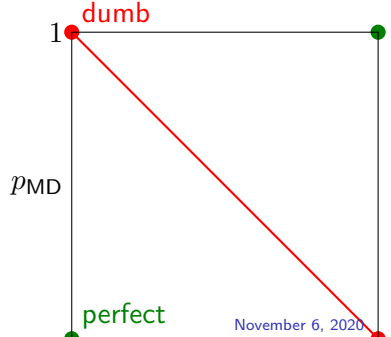
Given the observations $(\tilde{x}, k)$, the verifier must choose between hypotheses

$$\text{authentic message } \mathcal{H}_0 : \tilde{x} = x$$
$$\text{forged message } \mathcal{H}_1 : \tilde{x} = x'$$

Performance measures

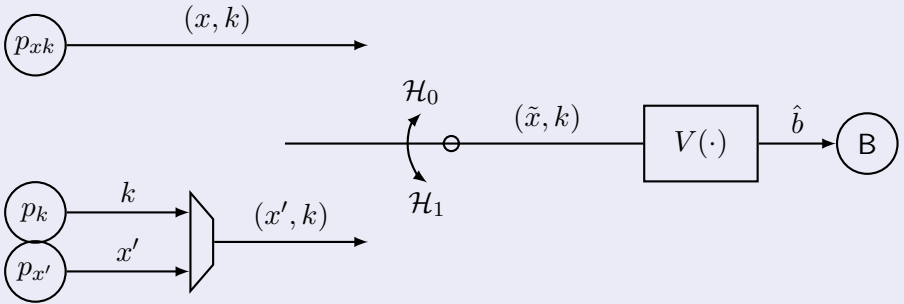
The performance of a verifier $\hat{b} = V(k, \tilde{x})$ is given by the pair of error probabilities

$$\text{false alarm } p_{\text{FA}} = p_{\hat{b}|b}(1|0)$$
$$\text{missed detection } p_{\text{MD}} = p_{\hat{b}|b}(0|1)$$



Outer bound on error probabilities

Simplified model



For any verifier (even probabilistic), the data processing inequality holds

$$\mathrm{D}\left(p_{\hat{b}|\mathcal{H}_0} \| p_{\hat{b}|\mathcal{H}_1}\right) \leq \mathrm{D}\left(p_{\tilde{x}k|\mathcal{H}_0} \| p_{\tilde{x}k|\mathcal{H}_1}\right)$$

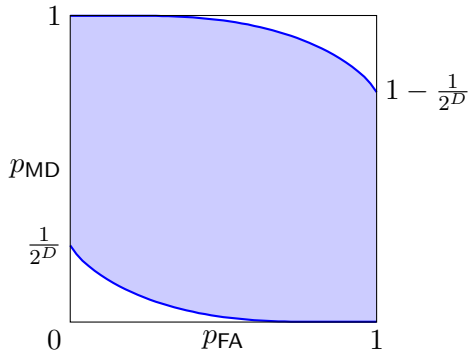
$$(1 - p_{\mathsf{FA}}) \log_2 \frac{1 - p_{\mathsf{FA}}}{p_{\mathsf{MD}}} + p_{\mathsf{FA}} \log_2 \frac{p_{\mathsf{FA}}}{1 - p_{\mathsf{MD}}} \leq \mathrm{D}\left(p_{xk} \| p_{x'k}\right)$$

Outer bound on error probabilities

Rewrite the above inequality as

$$f(p_{\mathsf{FA}}, p_{\mathsf{MD}}) \leq \mathrm{D}\left(p_{xk} \| p_{x'k}\right)$$

This limits the region of achievable $(p_{\mathsf{FA}}, p_{\mathsf{MD}})$ values, depending on $\mathrm{D}\left(p_{xk} \| p_{x'k}\right)$.
Observe that x' must be independent of k, hence $p_{x'k}(a, c) = p_{x'}(a) p_k(c)$



- p_{xk} and p_k depend on the signing mechanism; the signer wants to enlarge the achievable region, by making D as large as possible
- $p_{x'}$ depends on the attack strategy; the attacker wants to narrow the achievable region, by making D as small as possible

Lower bound on key entropy

By the independent lower bound for KLD, the attacker should choose $p_{x'} = p_x$ to minimize D, and hence $D = I(x, k)$.
Then, if we want to have $p_{\mathsf{FA}} = 0$ (correctness), we must accept $p_{\mathsf{MD}} \geq 1/2^{I(x,k)}$.
For an authentication mechanism with

$$\begin{cases} p_{\mathsf{FA}} = 0 \\ p_{\mathsf{MD}} \leq \varepsilon \end{cases}$$

a necessary condition is

$$\log_{1/2} \varepsilon \leq I(k, x) \leq H(k)$$

Lower bound on modification success probability

We derive a lower bound on the best attack, by considering a particular attack:

Key guessing attack

1. F intecepts authentic x
2. guesses $\hat{k} = g(x)$ with optimal strategy $g(c) = \arg\max_{a \in \mathcal{K}} p_{k|x}(a|c)$
3. chooses any $u' \neq u$
4. signs $x' = S(\hat{k}, u')$
5. transmits x' to B

Success event $S_{\mathcal{M}} \supset \left\{ \hat{k} = k \right\}$

Success probability

$$
\begin{aligned}
\mathrm{P}\left[S_{\mathcal{M}}\right] &\geq \mathrm{P}\left[\hat{k} = k\right] \\
&= \mathrm{P}\left[g(x) = k\right] \\
&= \sum_{c \in \mathcal{X}} \mathrm{P}\left[g(c) = k, x = c\right] \\
&= \sum_{c \in \mathcal{X}} p_{k|x}(g(c)|c) p_x(c) \\
&= \sum_{c \in \mathcal{X}} p_{k|x}(g(c)|c) \sum_{a \in \mathcal{K}} p_{kx}(a, c) \\
&\geq \sum_{c \in \mathcal{X}} \sum_{a \in \mathcal{K}} p_{k|x}(a|c) p_{kx}(a, c) \\
&= \mathrm{E}\left[p_{k|x}(k|x)\right]
\end{aligned}
$$

Lower bound on key entropy

By Jensen inequality we get

$$\mathrm{P}\left[S_{\mathcal{M}}\right] \geq \mathrm{E}\left[p_{k|x}(k|x)\right] = \mathrm{E}\left[1/2^{i_{k|x}(k|x)}\right] \geq 1/2^{\mathrm{E}\left[i_{k|x}(k|x)\right]} = 1/2^{H(k|x)}$$

For an integrity protection mechanism to guarantee $p_{\mathsf{MD}} \leq \varepsilon$ a necessary condition is

$$\log_{1/2} \varepsilon \leq H(k|x) \leq H(k)$$

For both authentication and integrity protection

Necessary condition

$$H(k) = H(k|x) + I(k,x) \geq 2 \log_{1/2} \varepsilon$$

Key entropy for multiple messages

Suppose we want to authenticate and protect the integrity of L consecutive messages $u_1, \ldots, u_L$. signed with the same key as

$$x_i = S(k, u_i) \quad , \quad i = 1, \ldots, L$$

and consider the attacks

Forging attack

F observes $x_1, \ldots, x_{i-1}$ and forges x'_i.
For ε-secure authentication we need

$$I(k, x_i | x_1, \ldots, x_{i-1}) \geq \log_{1/2} \varepsilon$$

Modification attack

F observes $x_1, \ldots, x_i$, blocks x_i, guesses $\hat{k}$, transmits $x'_i = S(\hat{k}, u'_i)$.
For ε-secure integrity we need

$$H(k | x_1, \ldots, x_i) \geq \log_{1/2} \varepsilon$$

Key entropy for multiple messages

By the chain rules for entropy and mutual information

$$\begin{aligned} H(k) &= H(k|x_1) + I(k, x_1) \\ &= H(k|x_1, x_2) + I(k, x_2|x_1) + I(k, x_1) \\ &= \cdots \\ &= H(k|x_1, \ldots, x_L) + \sum_{i=1}^{L} I(k, x_i|x_1, \ldots, x_{i-1}) \end{aligned}$$

and since each term must be $\geq \log_{1/2} \varepsilon$:

for both authentication and integrity protection

Necessary condition

$$H(k) \geq (L + 1) \log_{1/2} \varepsilon$$