Message Integrity

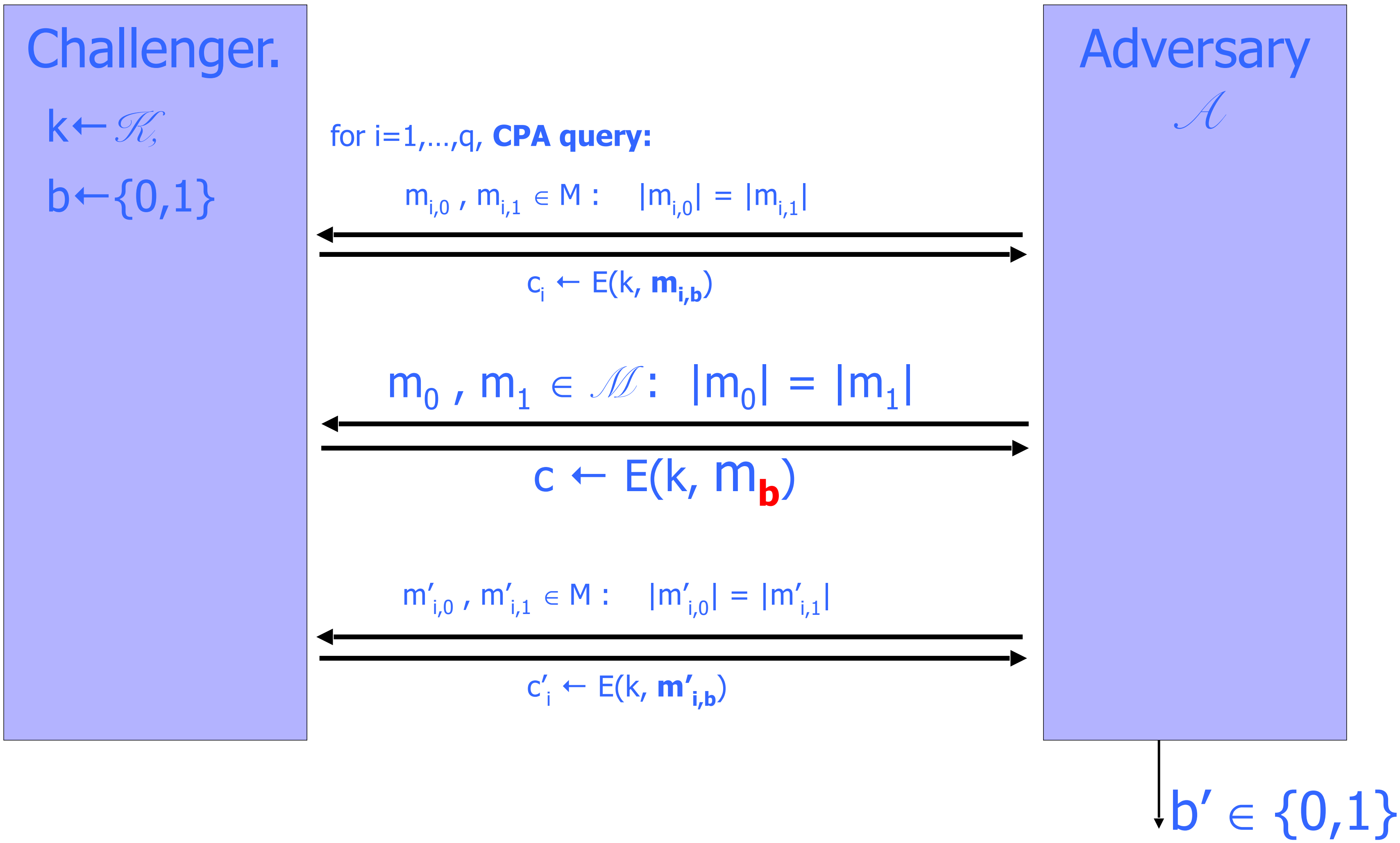
Yan Huang

CPA Recap

1. k←KeyGen(1^n). b←{0,1}. Give Enc(k, ·) to $\mathscr{A}$.
2. $\mathscr{A}$ chooses as many plaintexts as he wants, and receives the corresponding ciphertexts via Enc(k, ·).
3. $\mathscr{A}$ picks two plaintexts M_0 and M_1. (Picking plaintexts for which A previously learned ciphertexts is allowed!)
4. $\mathscr{A}$ receives the ciphertext of M_b, and continues to have accesses to Enc(k, ·).
5. $\mathscr{A}$ outputs b'.

$\mathscr{A}$ wins if b'=b.

CPA Recap



For all efficient adversary 𝒜,

| Pr[b=b'] - 1/2 | is "negligible".

Motivating Example

Is the request indeed coming from Alice?

Elec. Fund Transfer:

```
From: Alice
To: Bob
Amount: $100
```

Does Encryption Solve the Problem?

Enc(

Elec. Fund Transfer:
From: Alice
To: Bob
Amount: $100

)

A Simple Solution using MAC

(KeyGen, Mac, Vrfy)

k

k

Elec. Fund Transfer:

```
From: Alice
To: Bob
Amount: $100
```

```
tag ← Mac(k, m)
```

```
Vrfy(k, tag)
```

↓

1

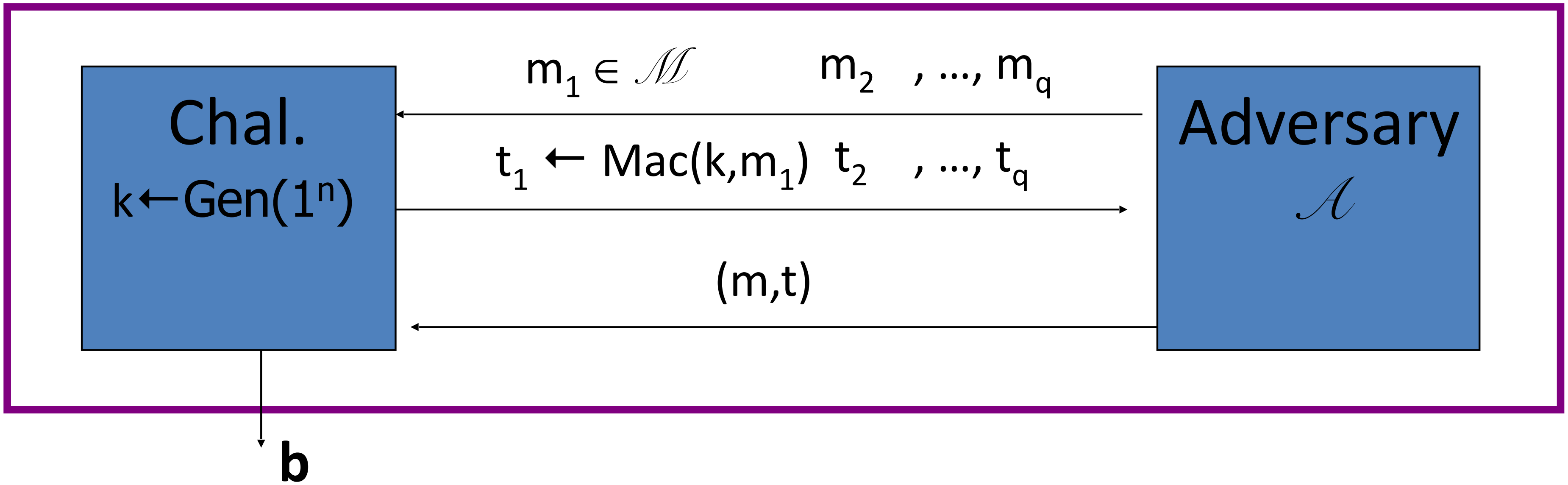
Message Integrity Game

1. $\mathtt{k} \leftarrow \mathtt{Gen}(1^n)$.
2. $\mathcal{A}$ is given polynomial time and an oracle access to query $\mathtt{Mac}(k, \cdot)$. Let $t_i = \mathtt{Mac}(k,\ m_i)$ and $Q = \{(m_1,\ t_1),\ \ldots,\ (m_q,\ t_q)\}$.
3. $\mathcal{A}$ outputs (m, t).

$\mathcal{A}$ wins the game if $\mathtt{Vrfy}(m,\ t)=1$ and $(m,t) \notin Q$.

Message Integrity

(Gen, Mac, Vrfy) --- a message authentication code scheme.



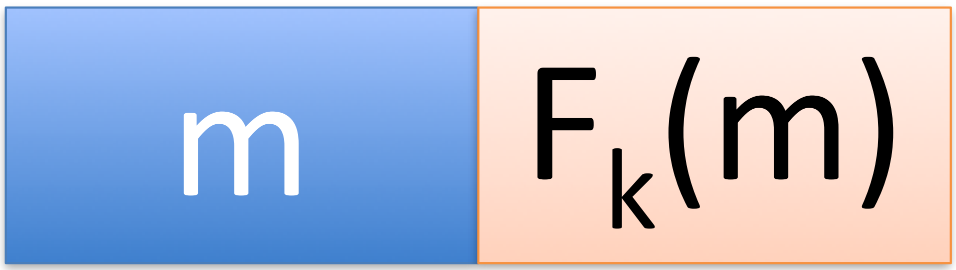
$$\mathbf{b} = \begin{cases} 1 & \text{if } \mathrm{Vrfy}(k,m,t) = 1 \text{ and } (m,t) \notin \{(m_1, t_1), \ldots, (m_q, t_q)\} \\ 0 & \text{otherwise} \end{cases}$$

Def: (Gen, Mac, Vrfy) is a **<u>Secure Message Authentication Code</u>** if for all "efficient" $\mathcal{A}$:

$\mathrm{Adv}_{\mathrm{Mac}}[\mathcal{A}]$ = Pr[Chal. outputs 1] is "negligible."

One block message

Let F be a secure block cipher (i.e., AES).




```
Mac(k,m)   = F(k,m)

Vrfy(k,m||t) = 1 iff F(k,m)=t
```

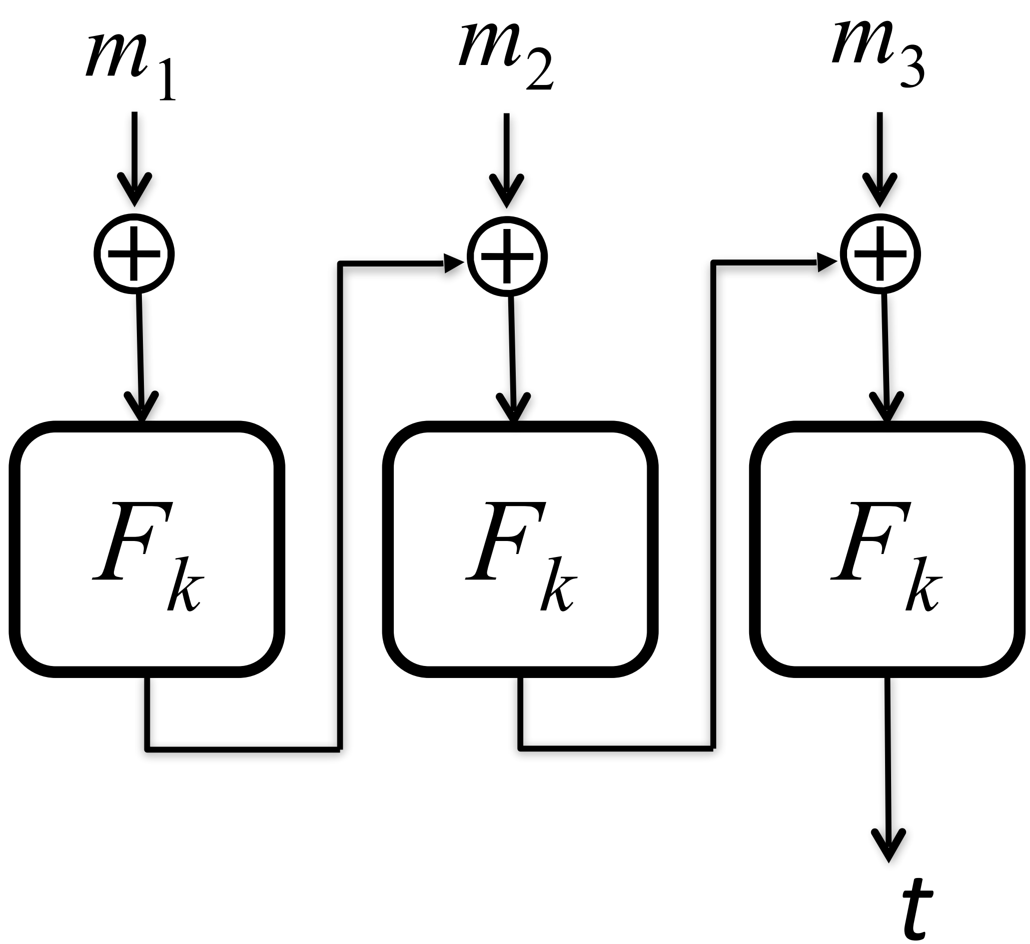
MAC arbitrary number of blocks

Does this work?

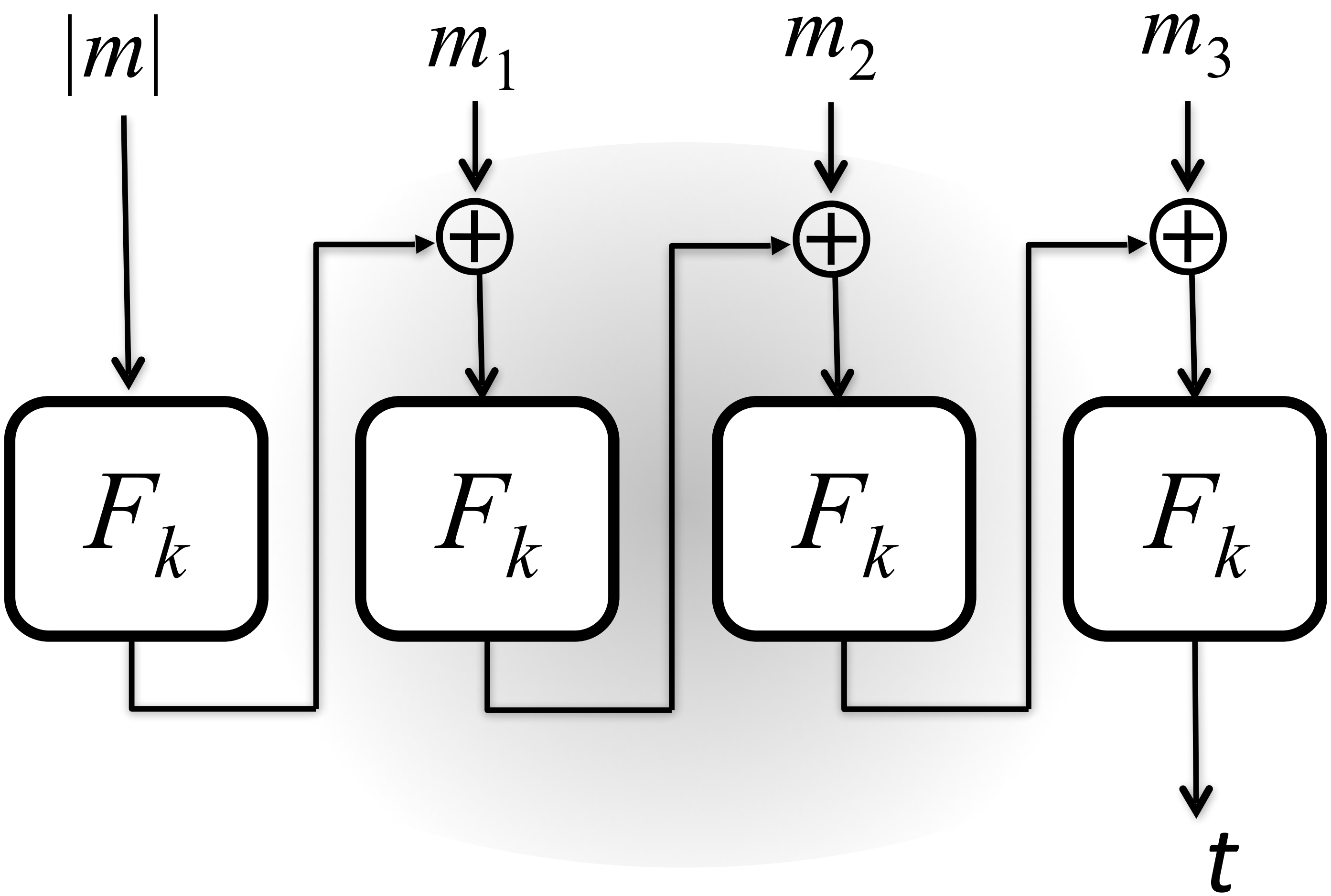
Let F be a secure block cipher (i.e., AES).

$$\texttt{Mac}(k,m) = F_k(m_1), F_k(m_2), F_k(m_3)$$

MAC arbitrary number of blocks
Is CBC a good MAC?

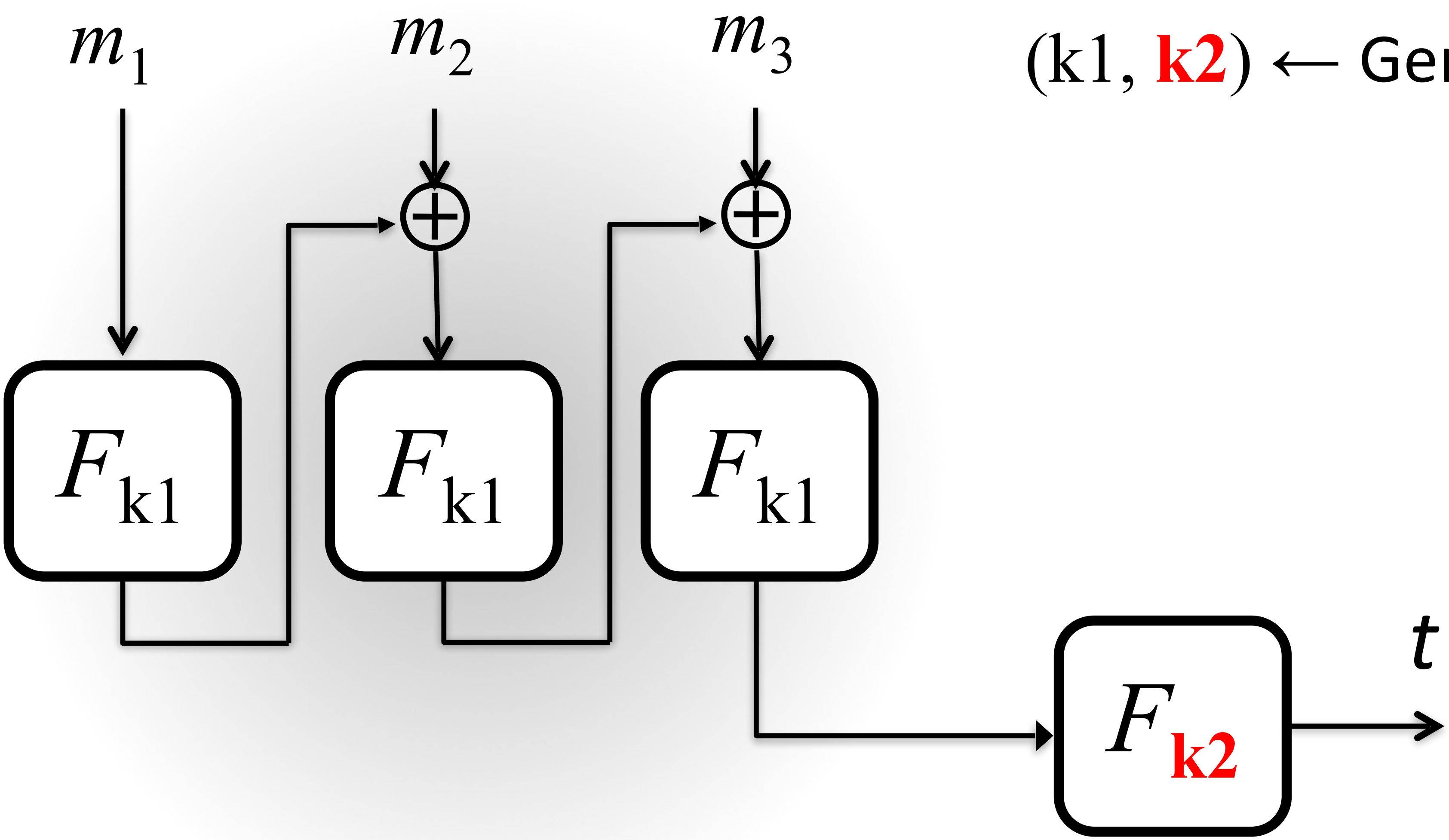


MAC arbitrary number of blocks
Scheme I



MAC arbitrary number of blocks
Scheme II

$(k1, k2) \leftarrow Gen(1^n)$



No need to know the length of the message in advance.

Warning!

Even harmless-looking modifications to cryptographic constructions can render them insecure!