

Bounds on Authentication Systems in Query Model

Rei Safavi-Naini

Univ of Wollongong, Australia

Joint work with, Peter Wild, Royal Holloway University of London

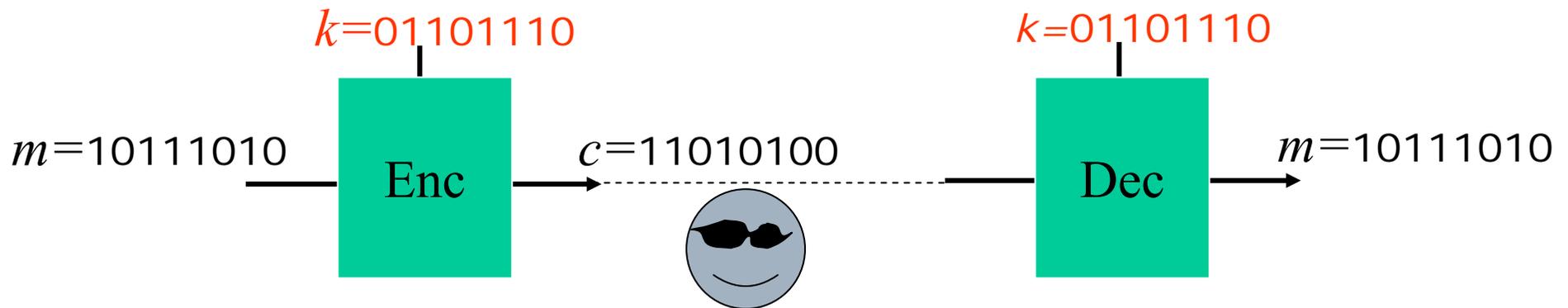
Motivation:
Information Theoretic Security:
Secrecy

– Shannon 1949

- Perfect secrecy: $H(m/c)=H(m)$
 - One-time pad

– Perfect secrecy is impractical

- ‘One-time’ random string $\rightarrow H(K) \geq H(M)$



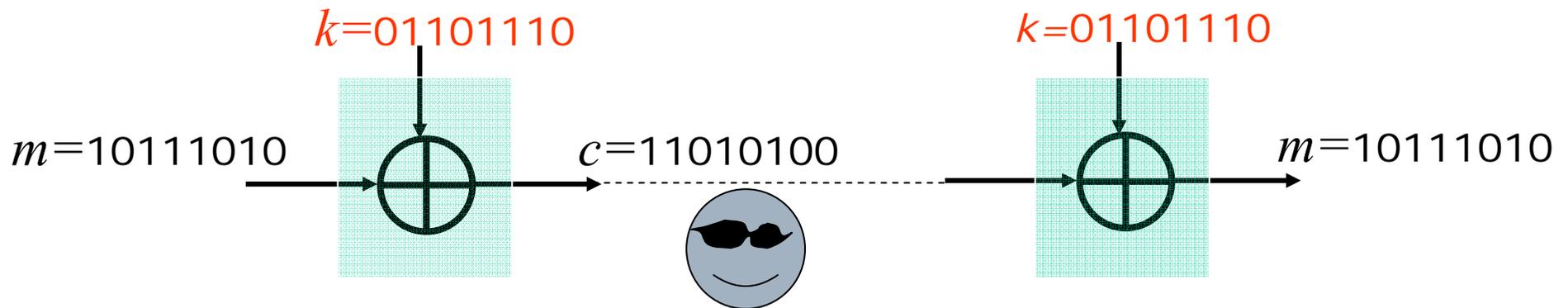
Motivation:
Information Theoretic Security:
Secrecy

– Shannon's 1949

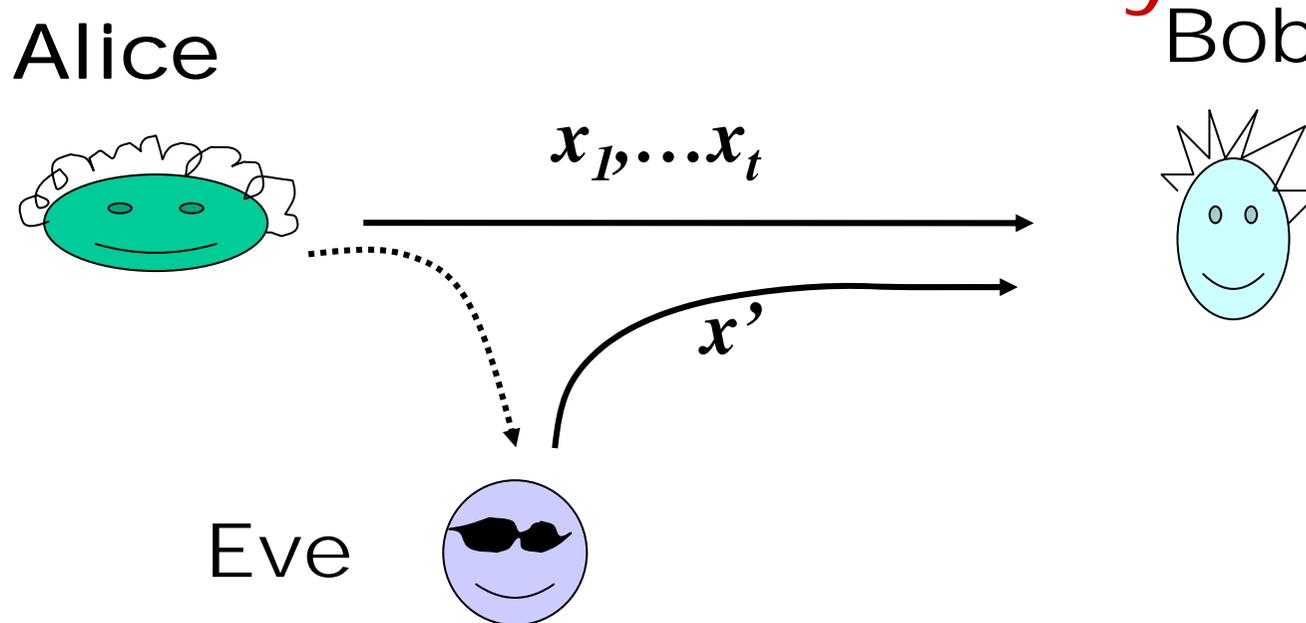
- Perfect secrecy: $H(m/c)=H(m)$
 - One-time pad

– Perfect secrecy is impractical

- 'One-time' random string $\rightarrow H(K) \geq H(M)$



Motivation:
Information Theoretic Security:
Authenticity



- Authentication Scenario
 - Sender and receiver trusted
 - Eve has **unlimited power**
 - Goals:
 - Detect fraudulent messages
 - Bound adversary's success

Authentication codes

- **Unconditionally Secure Authentication**

- *Gilbert MacWilliams and Sloane* 1974

- 2 party without secrecy

- **Authentication codes (A-codes)**

- *Simmons* 1982

- General model
- information theoretic bound

- **Extensions**

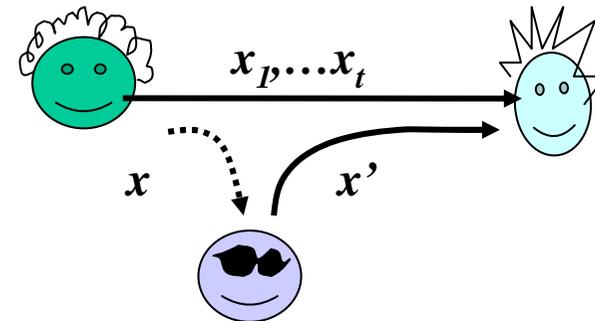
- Distributed systems
 - Multireceiver, shared generation of authenticator
- Un trusted participants

Brickel, Stinson, Johansson, Yung, Desmedt, Kurosawa, Martin, Safavi-Naini, Smeets, Wang, Pei, Rosenbaum, Wild, Walker

- **Adversary Model**

- **Non-interactive**

- Spoofing of order t



Authentication codes

- **Unconditionally Secure Authentication**
 - *Gilbert MacWilliams and Sloane 1974*
 - 2 party without secrecy
- **Authentication codes (A-codes)**
 - *Simmons 1982*
 - General model
 - information theoretic bound
 - **Extensions**
 - **Distributed systems**
 - Multireceiver, shared generation of authenticator
 - **Untrusted participants**
Brickell, Stinson, Johansson, Yung, Desmedt, Kurosawa, Martin, Safavi-Naini, Smeets, Wang, Pei, Rosenbaum, Wild, Walker
- **Adversary Model**
 - **Non-interactive**
 - Spoofing of order t

Authentication codes

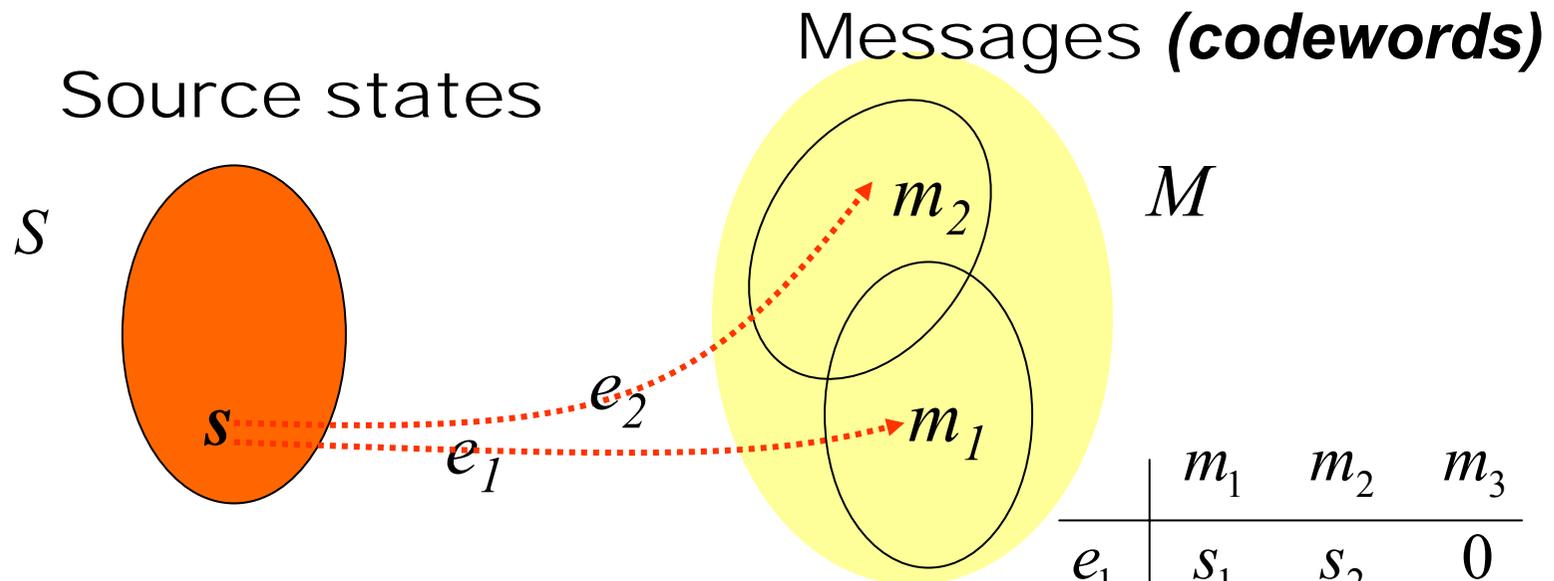
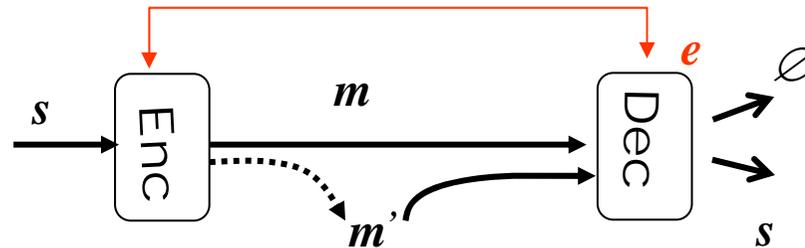
- **Unconditionally Secure Authentication**
 - *Gilbert MacWilliams and Sloane 1974*
 - 2 party without secrecy
- **Authentication codes (A-codes)**
 - *Simmons 1982*
 - General model
 - information theoretic bound
 - **Extensions**
 - Distributed systems
 - Multireceiver, shared generation of authenticator
 - Un trusted participants

Brickel, Stinson, Johansson, Yung, Desmedt, Kurosawa, Martin, Safavi-Naini, Smeets, Wang, Pei, Rosenbaum, Wild, Walker
- **Adversary Model**
 - **Non-interactive**
 - Spoofing of order t

This talk

- **Adaptive adversary**
 - **Oracle access**
 - Authentication
 - Verification
- **Optimal strategy**
- **Information theoretic bound**
- **When should adversary spoof?**
 - Stop querying
- **Bound on key size for adversary with access to authentication query**
- **Concluding remarks**

A-codes

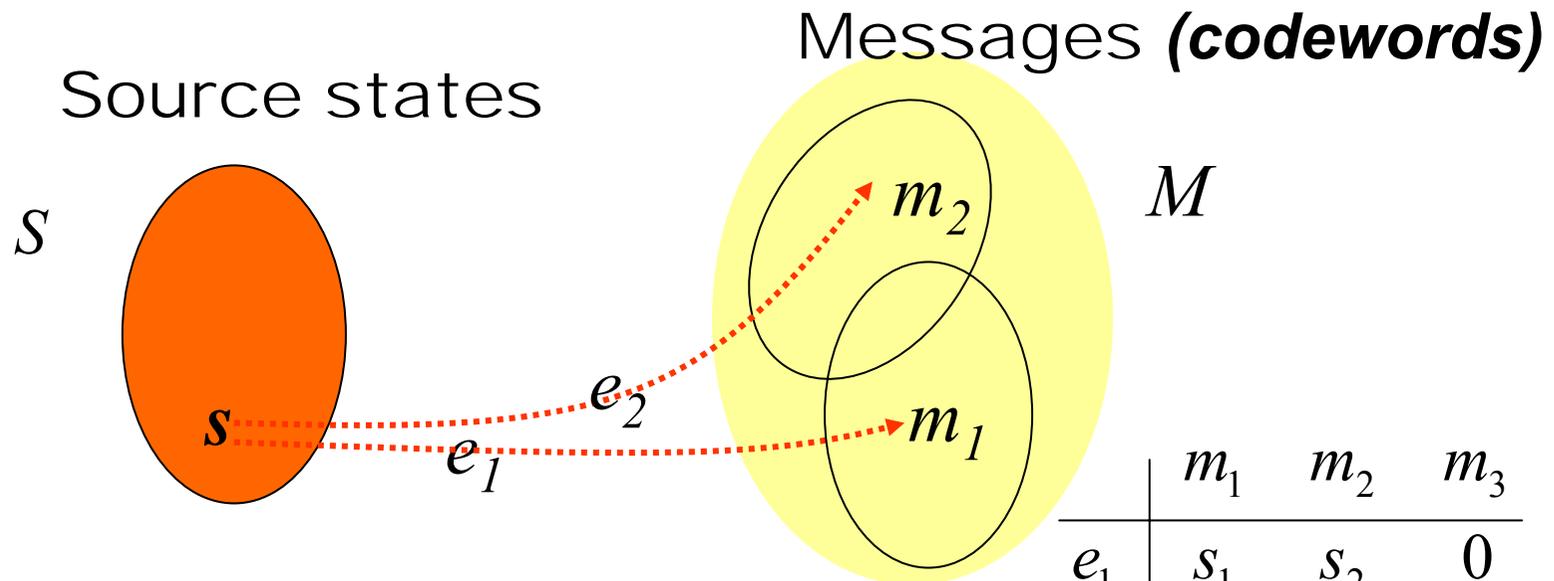
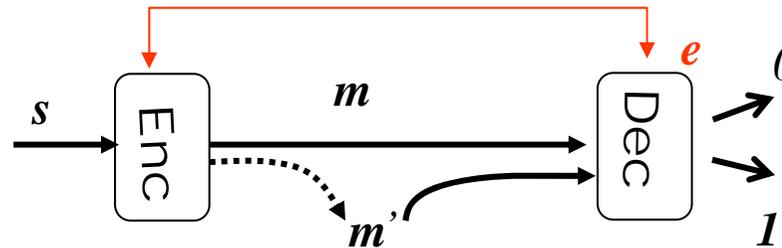


Authentication: $Auth = f(e, s)$
 Verification: $Ver(e, m) = \{s, \emptyset\}$

	m_1	m_2	m_3
e_1	s_1	s_2	0
e_2	0	s_1	s_2
e_3	s_1	0	s_2
e_4	0	s_1	s_2

Key entropy provides secrecy and authenticity.

A-codes



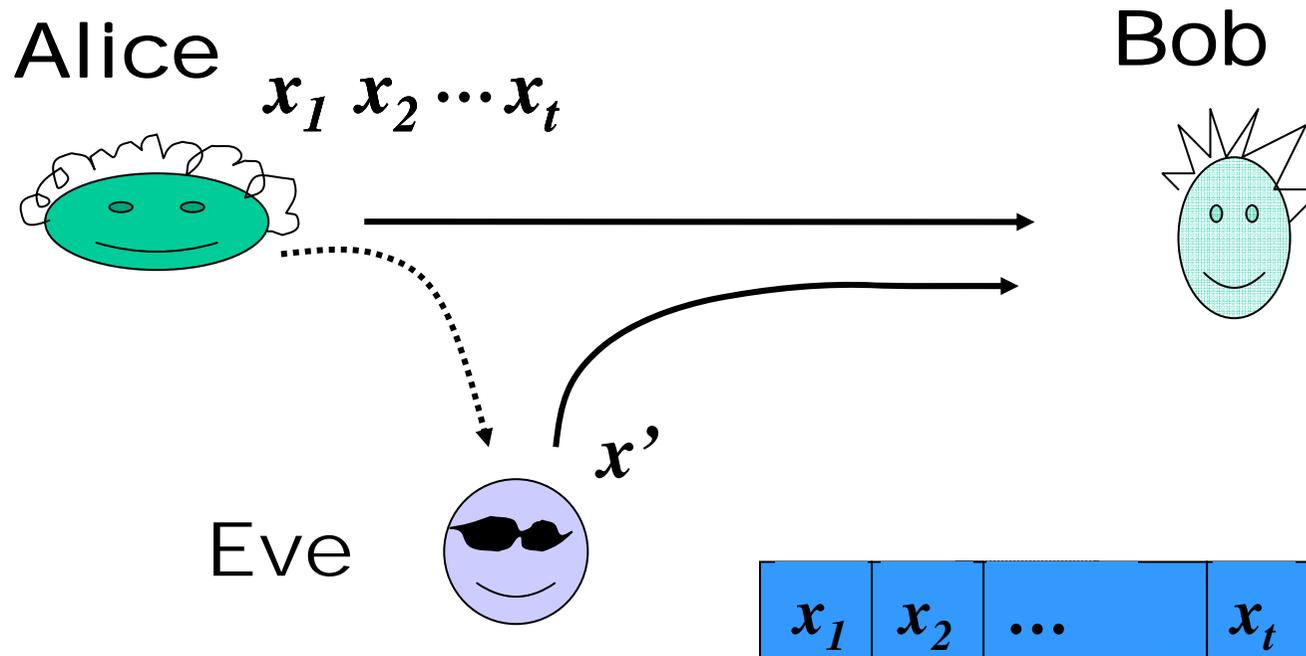
Authentication: $Auth = f(e, s)$
 Verification: $Ver(e, m) = \{s, \emptyset\}$

	m_1	m_2	m_3
e_1	s_1	s_2	0
e_2	0	s_1	s_2
e_3	s_1	0	s_2
e_4	0	s_1	s_2

Key entropy provides secrecy and authenticity.

Adversary Model

- **Spoofting of order t**
 - *Success probability P_t*



Representing A-code

Authentic messages

	m_1	m_2	m_3
e_1	s_1	s_2	0
e_2	0	s_1	s_2
e_3	s_1	0	s_2
e_4	0	s_1	s_2

Valid messages

	m_1	m_2	m_3
e_1	1	1	0
e_2	0	1	1
e_3	1	0	1
e_4	0	1	1

Spoofing:

$i=0$: *impersonation*

$i=1$: *substitution*

Success probability P_0

- Success chance
- m_1
 - $P(m_1)=1/2$

	m_1	m_2	m_3
e_1	1	1	0
e_2	0	1	1
e_3	1	0	1
e_4	0	1	1

Success probability P_0

- Success chance
- m_1
 - $P(m_1)=1/2$
- m_2
 - $P(m_2)=3/4$

	m_1	m_2	m_3
e_1	1	1	0
e_2	0	1	1
e_3	1	0	1
e_4	0	1	1

Success probability P_0

- Success chance
- m_1
 - $P(m_1)=1/2$
- m_2
 - $P(m_2)=3/4$
- m_3
 - $P(m_3)=3/4$

	m_1	m_2	m_3
e_1	1	1	0
e_2	0	1	1
e_3	1	0	1
e_4	0	1	1

Success probability P_0

- Success chance

- m_1

- $P(m_1)=1/2$

- m_2

- $P(m_2)=3/4$

- m_3

- $P(m_3)=3/4$

	m_1	m_2	m_3
e_1	1	1	0
e_2	0	1	1
e_3	1	0	1
e_4	0	1	1

→ $P_0=3/4$

Best strategy: Choose m_2 or m_3

Success probability P_1

- Observing m_1
 - $P(m_2|m_1)=1/2$
 - $P(m_3|m_1)=1/2 \rightarrow P(m_1)=1/2$
- Observing m_2
 - $P(m_1|m_2)=1/3$
 - $P(m_3|m_2)=2/3$
- Observing m_3
 - $P(m_1|m_3)=1/3$
 - $P(m_3|m_3)=2/3$

	m_1	m_2	m_3
e_1	1	1	0
e_2	0	1	1
e_3	1	0	1
e_4	0	1	1

Success probability P_1

- Observing m_1
 - $P(m_2|m_1)=1/2$
 - $P(m_3|m_1)=1/2 \rightarrow P(m_1)=1/2$
- Observing m_2
 - $P(m_1|m_2)=1/3$
 - $P(m_3|m_2)=2/3 \rightarrow P(m_2)=3/4$
- Observing m_3
 - $P(m_1|m_3)=1/3$
 - $P(m_3|m_3)=2/3$

	m_1	m_2	m_3
e_1	1	1	0
e_2	0	1	1
e_3	1	0	1
e_4	0	1	1

Success probability P_1

- Observing m_1
 - $P(m_2|m_1)=1/2$
 - $P(m_3|m_1)=1/2 \rightarrow P(m_1)=1/2$
- Observing m_2
 - $P(m_1|m_2)=1/3$
 - $P(m_3|m_2)=2/3 \rightarrow P(m_2)=3/4$
- Observing m_3
 - $P(m_1|m_3)=1/3$
 - $P(m_2|m_3)=2/3 \rightarrow P(m_3)=2/3$

	m_1	m_2	m_3
e_1	1	1	0
e_2	0	1	1
e_3	1	0	1
e_4	0	1	1

Success probability P_1

- Observing m_1
 - $P(m_2|m_1)=1/2$
 - $P(m_3|m_1)=1/2$
- Observing m_2
 - $P(m_1|m_2)=1/3$
 - $P(m_3|m_2)=2/3$
- Observing m_3
 - $P(m_1|m_3)=1/3$
 - $P(m_2|m_3)=2/3 \rightarrow P(m_3)=2/3$

	m_1	m_2	m_3
e_1	1	1	0
e_2	0	1	1
e_3	1	0	1
e_4	0	1	1

$$P_1 = \sum p(m_j) P(m_j)$$

$$P_1 = 1/3(1/2 + 2/3 + 2/3) = 11/18$$

Choosing the best game

- **Choose the game with the highest success probability**

- **Example**
 - **Impersonation or substitution**

$$P_0 = 3/4 = .75$$

$$P_1 = 11/18 = .61$$

	m_1	m_2	m_3
e_1	1	1	0
e_2	0	1	1
e_3	1	0	1
e_4	0	1	1

Observing a message may **reduce** success chance.

Authentication without secrecy

- **Message authentication codes**

$$m = s.t \quad t = \text{Auth}(e, s)$$

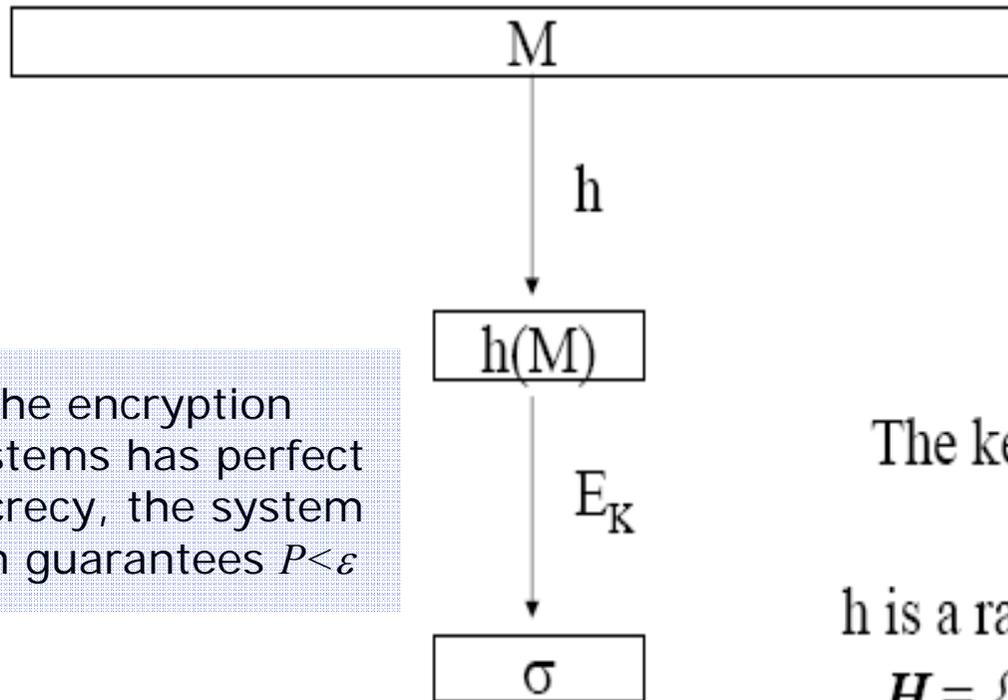
- **Construction for repeated authentication**

- **Carter and Wegman construction**

- Authentication without secrecy
- Efficient repeated authentication

- t bit key for a message s , $\text{len}(e) \ll \text{len}(s)$

Unconditionally secure authentication systems are practical



**Carter-Wegman
paradigm**

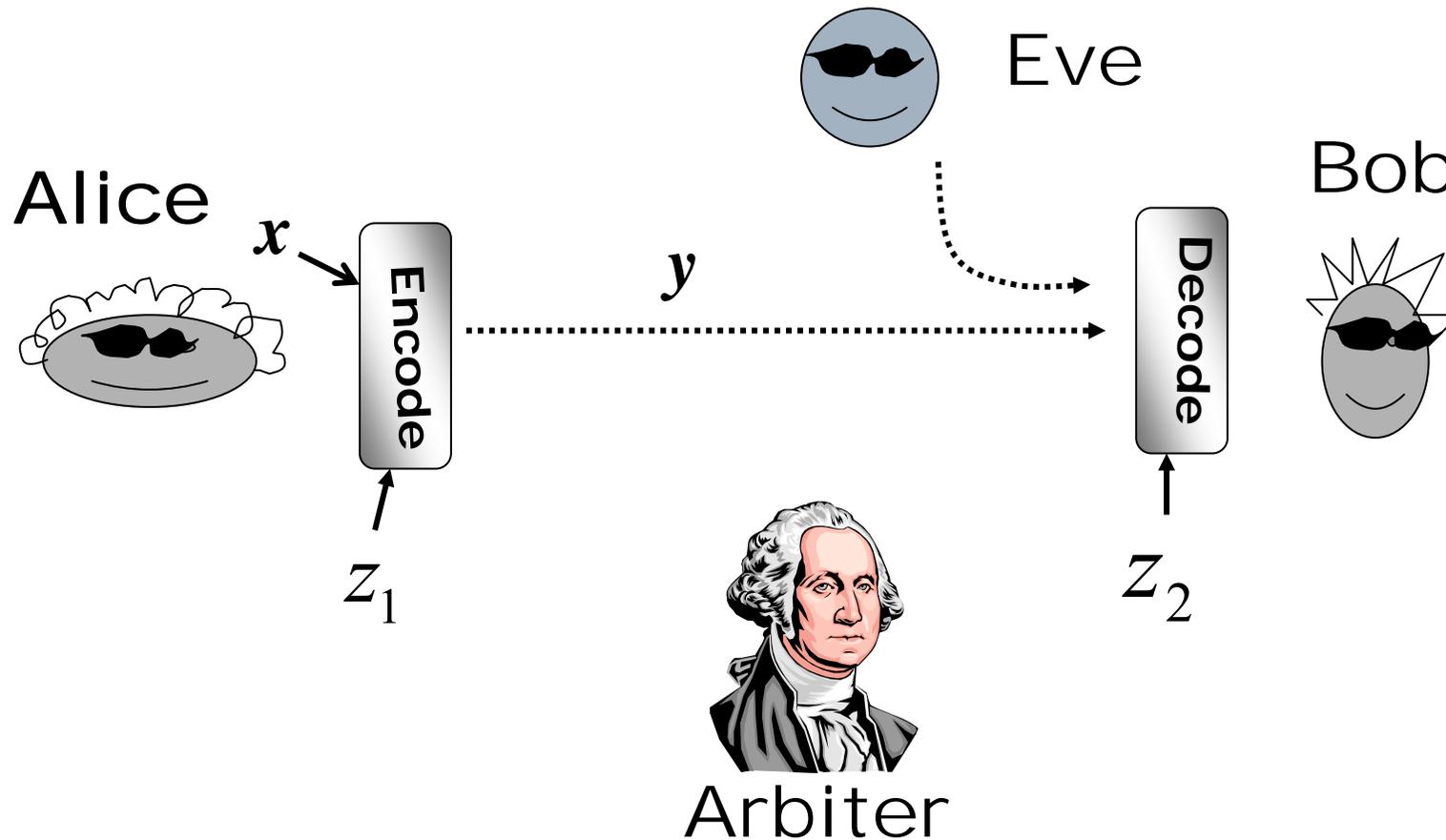
If the encryption systems has perfect secrecy, the system can guarantees $P < \varepsilon$

The key for the MAC is (h, K)

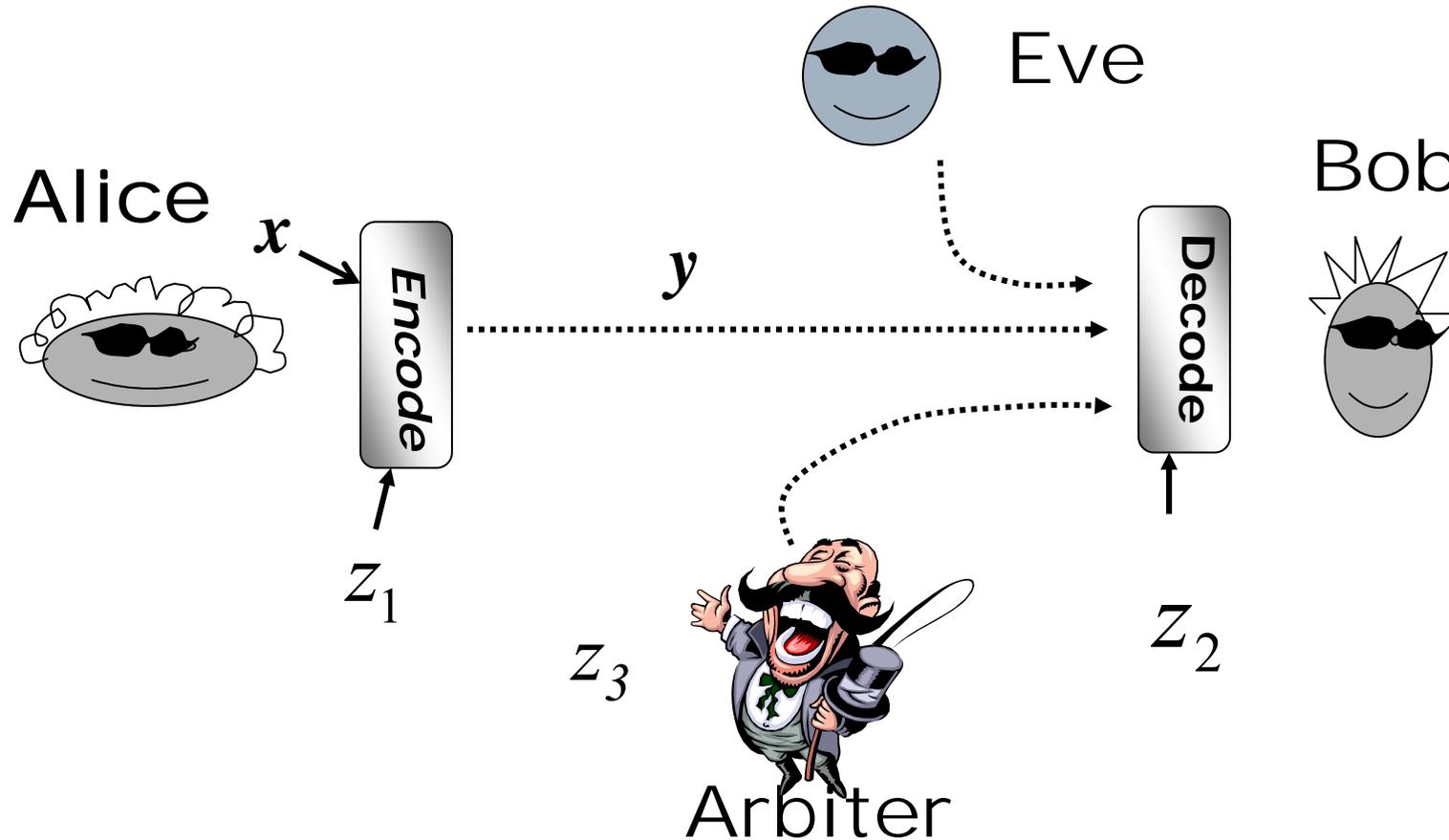
h is a random element of
 $H = \{h: M \rightarrow \{0,1\}^n\}$

Def: Family of hash functions $H = \{h: M \rightarrow \{0,1\}^n\}$
is ε -**AU** (almost universal) if for all $M, M' \in M, M \neq M'$,
 $\Pr_h [h(M) = h(M')] \leq \varepsilon$

Authentication with arbiter: A^2 -codes

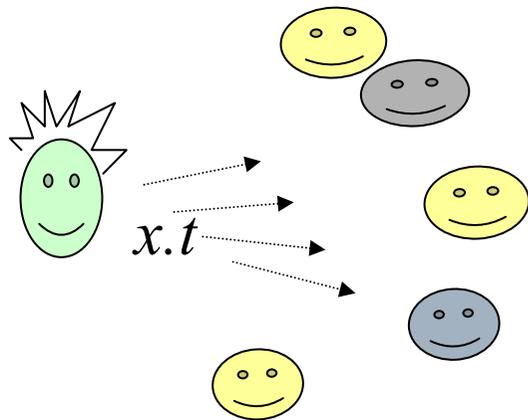


Authentication with arbiter: A^3 -codes

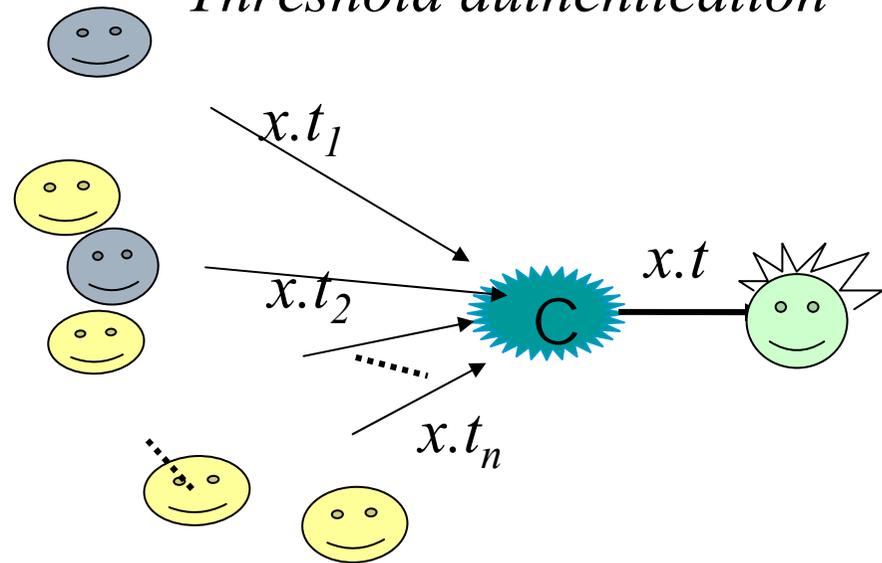


Authentication in groups

Multireceiver systems



Threshold authentication



Also, systems for dynamic sender: anyone can be a sender!

Security and efficiency

- **Security: Success probability of an adversary using his best strategy**
 - Spoofing of order i
- **Information theoretic bound (Simmons 82, Rosenbaum 93)**

$$P_i \geq 2^{-I(M;E|M^i)}$$

- **Relating the key with success chance** $P_d \geq 2^{\frac{-H(E)}{i+1}}$
 - For equi-probable keys and $i=1$

→ *Adversary's success chance increases with observing more messages.*

$$P_1 \geq \frac{1}{\sqrt{E}}$$

Choosing the best game

- Choose the game with the highest success probability

- **Example**

- Impersonation or substitution

$$P_0 = 3/4 = .75$$

$$P_1 = 11/18 = .61$$

	m_1	m_2	m_3
e_1	1	1	0
e_2	0	1	1
e_3	1	0	1
e_4	0	1	1

Observing a message may **reduce** success chance.

- *Information theoretic bound*

- $P(s_1) = 1/4, p(s_2) = 3/4 \rightarrow I(M;E) = 1.26, P_0 \geq 0.42$

- $P(s_1) = 1/2, p(s_2) = 1/2 \quad P_0 \geq 0.33$

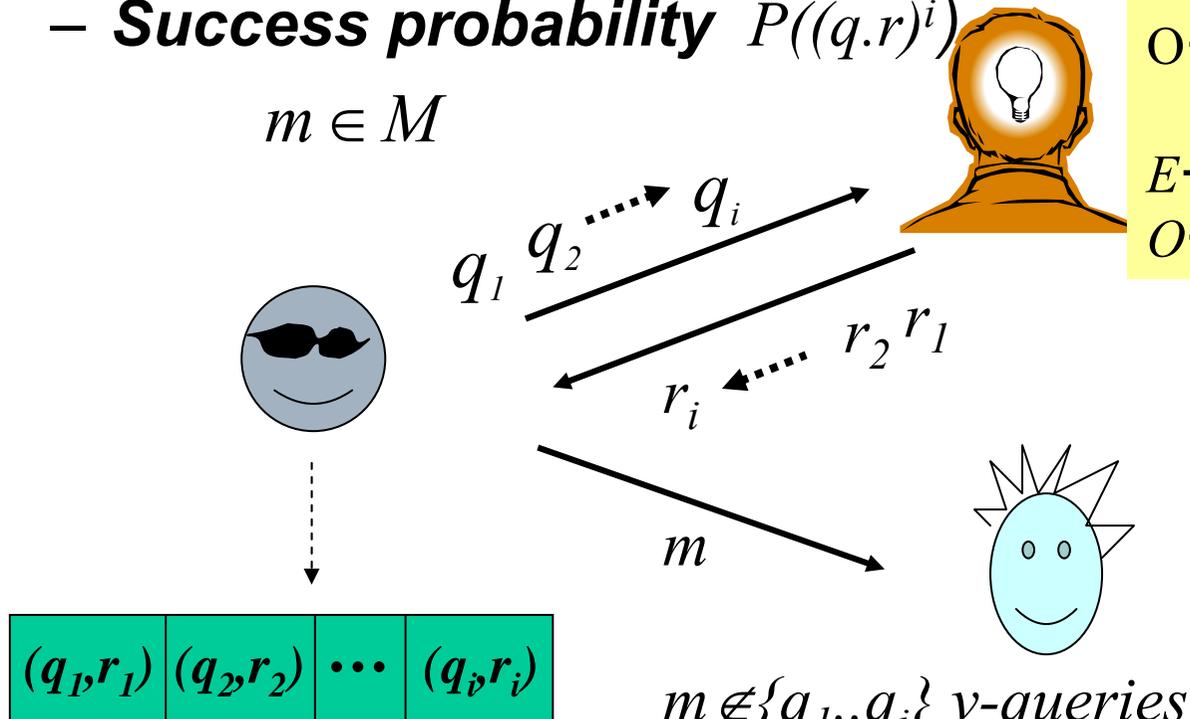
Adaptive Adversary: Oracle Queries

(SMY 04)

- **t queries**

- **Success probability** $P((q.r)^i)$

$m \in M$



Oracle can answer queries:

$E \rightarrow O: q = m$

$O \rightarrow E: r = Ver(e, m) \in \{0, 1\}$

$E \rightarrow O: q = s$

$O \rightarrow E: r = Auth(e, s) = m$

$m \notin \{q_1..q_i\}$ v-queries

$m \notin \{r_1..r_i\}$ A-queries

Adaptive Game

- **Communicants' strategy**
 - A distribution on keys: $p(e)$
- **Adversary's strategy**
 1. A sequence of probability distributions for selecting queries
 - One probability distribution for a sequence $(q,r)^i$ of query and response
 2. A probability distribution for spoofing messages

$$\tau(m), \tau_{(q,r)}(m), \tau_{(q,r)^2}(m), \tau_{(q,r)^3}(m) \cdots \tau_{(q,r)^{i-1}}(m), \tau_{(q,r)^i}(m)$$

Authentication & Verification queries

Authentication Queries

Experiment $\text{Exp}_{\Pi, F_a, \tau}(i, 1)$

$e \leftarrow \mathcal{E}$

If after asking *exactly* i queries s^i of $\text{Auth}(e, \cdot)$ and receiving corresponding responses \mathbf{m}^i

$F_{a, \tau}^{\text{Auth}(e, \cdot), \text{Ver}(e, \cdot)}$ makes a query m to the oracle $\text{Ver}(e, \cdot)$ such that the return

$\text{Ver}(e, m) = 1$, and

m had never been returned by

the oracle $\text{Auth}(e, \cdot)$

then return 1 **else** return 0

Verification Queries

Experiment $\text{Exp}_{\Pi, F_v, \tau}(i+1)$

$e \leftarrow \mathcal{E}$

If after asking *exactly* i queries \mathbf{m}^i of $\text{Ver}(e, \cdot)$ and receiving corresponding responses b^i

$F_{v, \tau}^{\text{Ver}(e, \cdot)}$ makes a query m to

the oracle $\text{Ver}(e, \cdot)$ such that the return

$\text{Ver}(e, m) = 1$, and

m was never asked of

the oracle $\text{Ver}(e, \cdot)$

then return 1 **else** return 0

Advantage of the forger

$$\text{Adv}_{\Pi, F_a, \tau}(i, 1) = P_T[\text{Exp}_{\Pi, F_a, \tau}(i, 1) = 1]$$

$$\text{Adv}_{\Pi, F_v, \tau}(i+1) = P_T[\text{Exp}_{\Pi, F_v, \tau}(i+1) = 1]$$

$$P_i^T = \sum_{q_1 \in Q} \tau(q_1) \sum_{r_1 \in \mathcal{R}} p(r_1 | q_1) \sum_{q_2 \in Q} \tau_{(\mathbf{q}, \mathbf{r})^1}(q_2) \sum_{r_2 \in \mathcal{R}} p(r_2 | q_2, (\mathbf{q}, \mathbf{r})^1) \dots$$

$$\sum_{q_i \in Q} \tau_{(\mathbf{q}, \mathbf{r})^{i-1}}(q_i) \sum_{r_i \in \mathcal{R}} p(r_i | q_i, (\mathbf{q}, \mathbf{r})^{i-1}) \sum_{m \in \mathcal{M}} \tau_{(\mathbf{q}, \mathbf{r})^i}(m) \sum_{e \in \mathcal{E}, \text{Ver}(e, m)=1} p(e | m, (\mathbf{q}, \mathbf{r})^i)$$

Success probability for strategy τ

$$P_i^\tau = \sum_{(\mathbf{q}, \mathbf{r})^i} p_i^\tau((\mathbf{q}, \mathbf{r})^i) P_i^\tau((\mathbf{q}, \mathbf{r})^i)$$

$$P_i^\tau((\mathbf{q}, \mathbf{r})^i) = \sum_{m \in \mathcal{M}} \tau_{(\mathbf{q}, \mathbf{r})^i}(m) P_i^\tau((\mathbf{q}, \mathbf{r})^i, (m, 1))$$

$$P_i^\tau((\mathbf{q}, \mathbf{r})^i, (m, 1)) = \sum_{e \in \mathcal{E}((\mathbf{q}, \mathbf{r})^i)} p(e | (\mathbf{q}, \mathbf{r})^i) \gamma(e, m, (\mathbf{q}, \mathbf{r})^i)$$

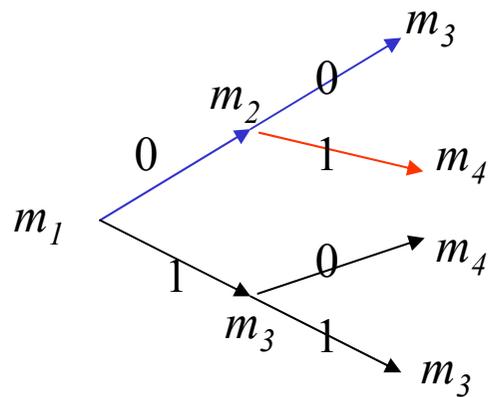
$$p_i^\tau((\mathbf{q}, \mathbf{r})^j) = p_i^\tau((\mathbf{q}, \mathbf{r})^{j-1}) \tau_{(\mathbf{q}, \mathbf{r})^{j-1}}(q_j) p(r_j | q_j, (\mathbf{q}, \mathbf{r})^{j-1})$$

Adversary's best success chance $P_i = \max_{\tau} P_i^\tau$

Pure strategies

τ is *pure* if $\tau_{(q,r)^i}$ is zero everywhere except a single query

- A pure strategy for the game can be represented by a tree

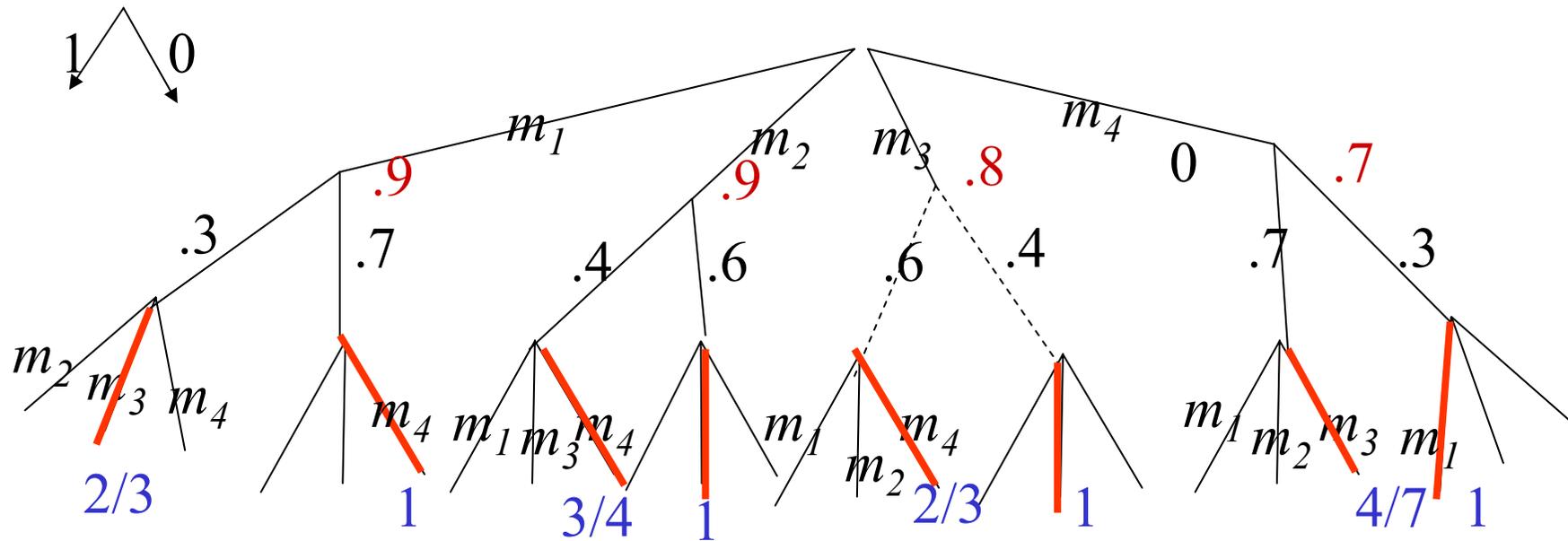


	m_1	m_2	m_3	m_4	m_5
e_1	1	1	0	0	0
e_2	1	0	1	0	0
e_3	0	1	0	0	1
e_4	0	0	0	1	1
e_5	0	1	0	1	0

Theorem: *There is always a pure optimal strategy.*

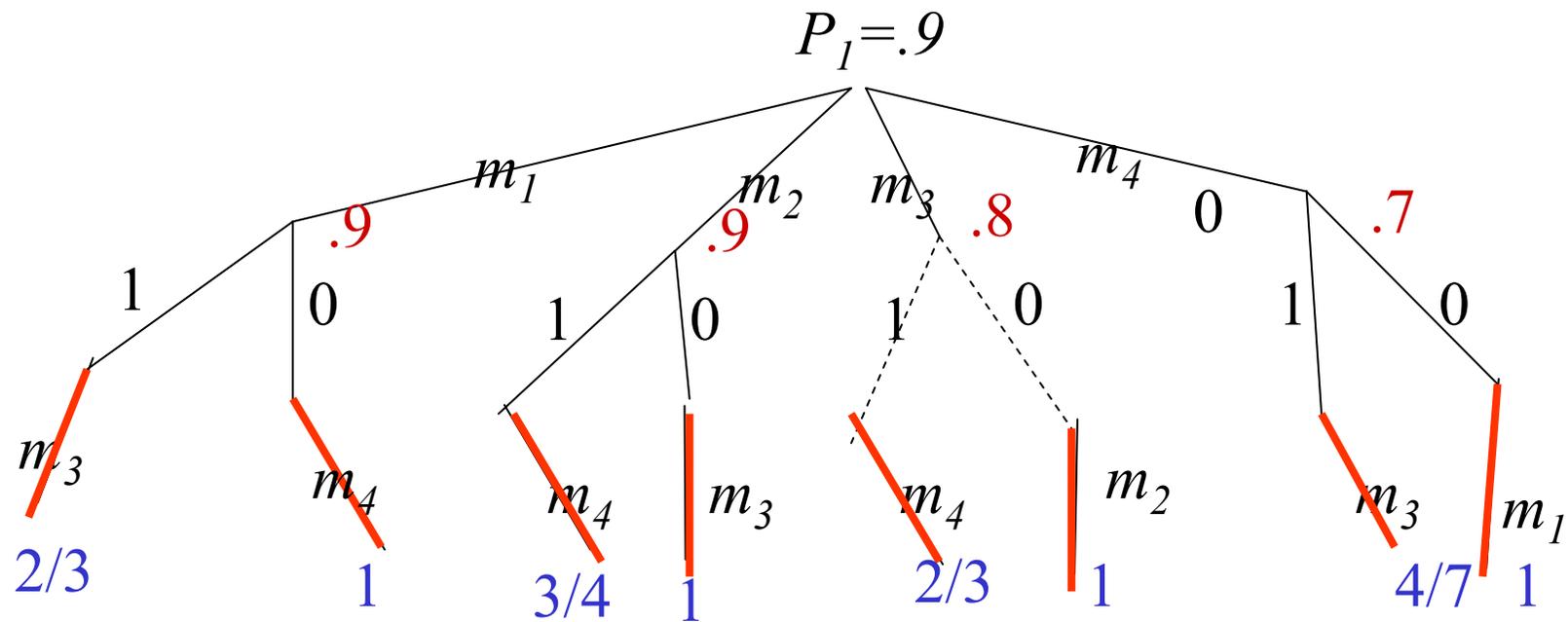
Finding pure optimal strategy

		m_1	m_2	m_3	m_4	
$i=1$	0.1	e_1	1	1	0	0
	0.2	e_2	1	0	1	0
	0.3	e_3	0	1	0	1
	0.4	e_4	0	0	1	1



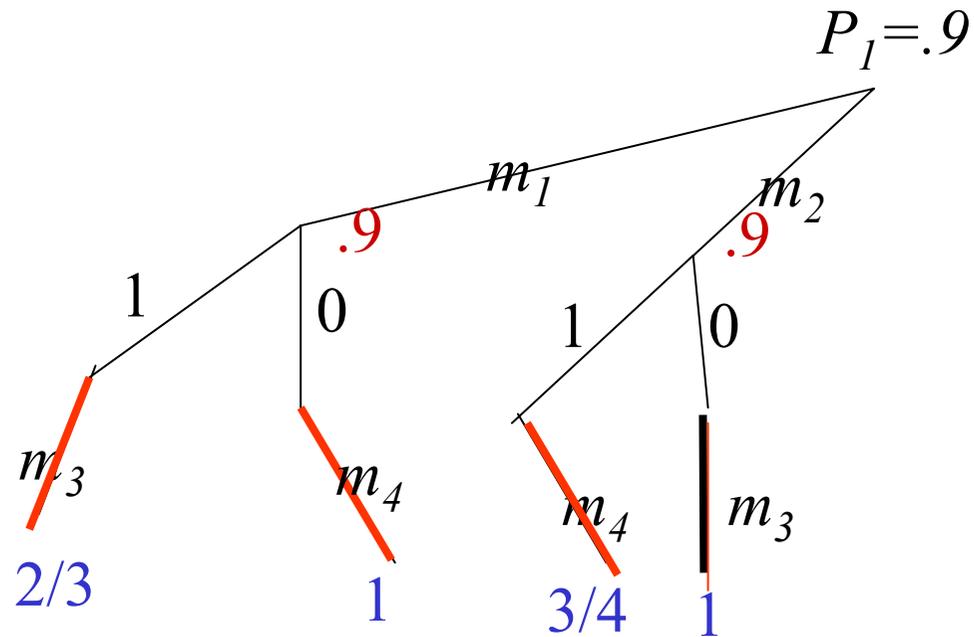
Finding pure optimal strategy

		m_1	m_2	m_3	m_4
01	e_1	1	1	0	0
02	e_2	1	0	1	0
0.3	e_3	0	1	0	1
0.4	e_4	0	0	1	1

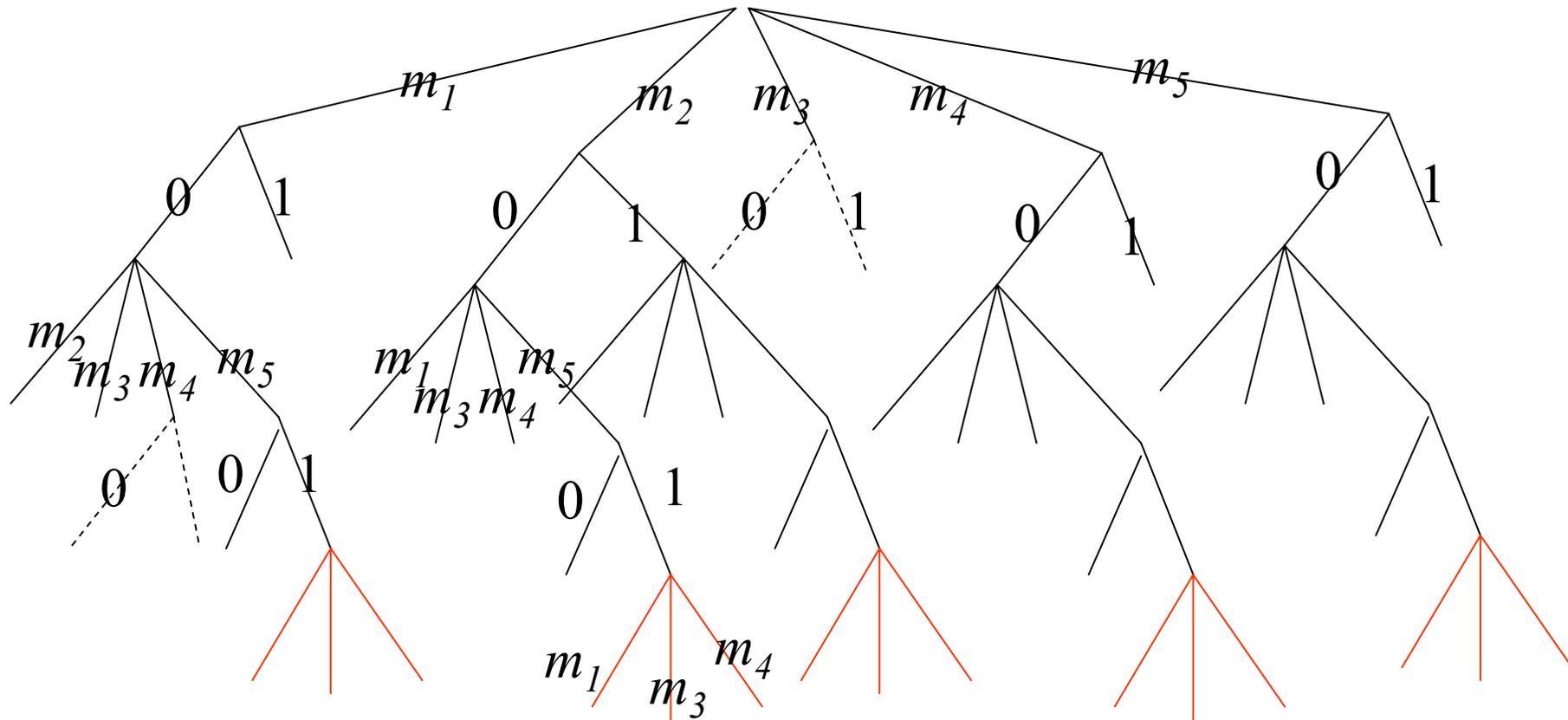


Finding pure optimal strategy

		m_1	m_2	m_3	m_4
01	e_1	1	1	0	0
02	e_2	1	0	1	0
0.3	e_3	0	1	0	1
0.4	e_4	0	0	1	1



Pure optimal strategy



Information Theoretic Bound

Theorem: Let Π be an authentication system and P_i^τ be the success probability of an adversary who makes i oracle queries using strategy τ , and then spoofs optimally after. Then

$$P_i^\tau \geq 2^{H(E|M, (Q^\tau, R^\tau)^i) - H(E|(Q^\tau, R^\tau)^i)} = 2^{-I(E; M | (Q^\tau, R^\tau)^i)}$$

Compared with message observing: $P_i \geq 2^{-I(M; E | M^i)}$

Adaptive adversary can change the bound!

Authentication queries

Theorem

$$P_i^{\tau} \geq 2^{H(E|M^*, (S^{\tau}, M^{\tau})^i) - H(E|(S^{\tau}, M^{\tau})^i)} = 2^{-I(E; M^* | (S^{\tau}, M^{\tau})^i)}$$

For an authentication system

$$\prod_{j=0}^i P_j \geq 2^{-H(E)}$$

$$\rightarrow P_d \geq 2^{-\frac{H(E)}{i+1}}$$

Number of queries

- **Suppose adversary can ask up to i queries:**
 - When should he stop querying and spoof?
- **For a message observing adversary: observing more messages may reduce success chance.**

Theorem:

Asking ‘good queries’ does not reduce success probability.

- **For V-queries, q is a good query if, :**
 - distinct from previous queries
 - If strategy τ has a unique optimal spoofing message m , then $q \neq m$

Two verification games

Game 1: Offline Game

- S1
 - adaptively asks i queries
 $q_i = q_1 \dots q_i$
 - observes responses
 $r_1 = r_1 \dots, r_i$
- S2
 - constructs a spoofing message
 $m \in M$

Adversary wins if the verifier accepts the message.

Game 2: On-line Game

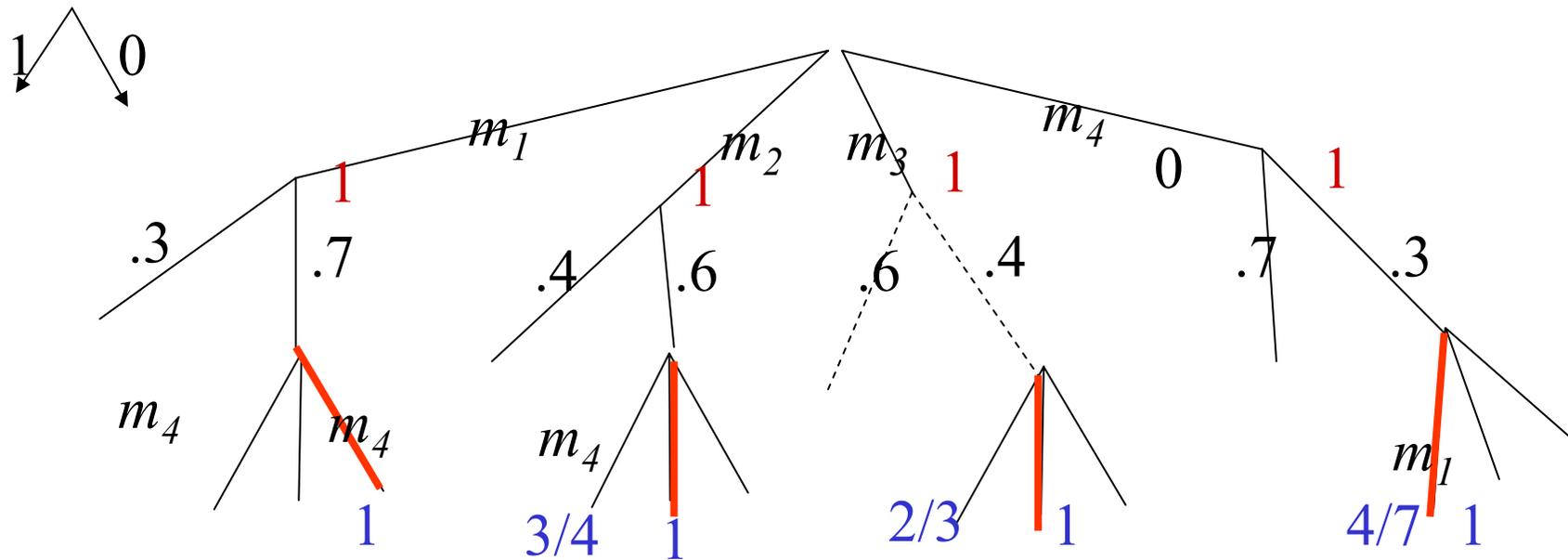
- S1
 - adaptively sends **up to $i+1$ queries**
 $q_i = q_1 \dots q_i$
 - observes responses
 $r_1 = r_1 \dots, r_i$

Adversary wins **as soon as** the verifier accepts a message.

- similar to computational model.

Finding pure optimal strategy

		m_1	m_2	m_3	m_4
01	e_1	1	1	0	0
02	e_2	1	0	1	0
0.3	e_3	0	1	0	1
0.4	e_4	0	0	1	1



'Power of verification queries'

- **'Folklore' in computational security**

$$P_v < 1/v P_1$$

- **Same result can be proven for on-line games**

For three queries:

$$\begin{aligned} P_3 &= p(m_1, 1) + p(m_1, 0)p((m_2, 1)|(m_1, 0)) + p((m_1, 0)(m_2, 0)) p((m_3, 1)|(m_1, 0)(m_2, 0)) \\ &= p(m_1, 1) + p((m_2, 1)(m_1, 0)) + p((m_3, 1)(m_1, 0)(m_2, 0)) \\ &\leq p(m_1, 1) + p(m_2, 1) + p(m_3, 1) \leq 3P_1 \end{aligned}$$

$$m_1 \xrightarrow{0} m_2 \xrightarrow{0} m_3$$

Concluding Remarks

- **Similar analysis for**
 - **Combined A-queries and V-queries**
 - **Success chance depends on the order of queries**
 - **Best strategy determines the order**
- **Open Questions**
 - **Distributed systems**
 - **Signature (Asymmetric) systems**