Authentication in Digital World

1. Marking and tracing

2. Privacy preserving authentication

Rei Safavi-Naini
University of Calgary

7/12/07

"On the Internet, nobody knows you're a dog."

Two kinds of questions:

1. Who am I talking to?
   - Where is this message coming from?

2. Is this message authentic?
   - Modified?
   - Authentic or 'copy'?
   - Real or computer generated?

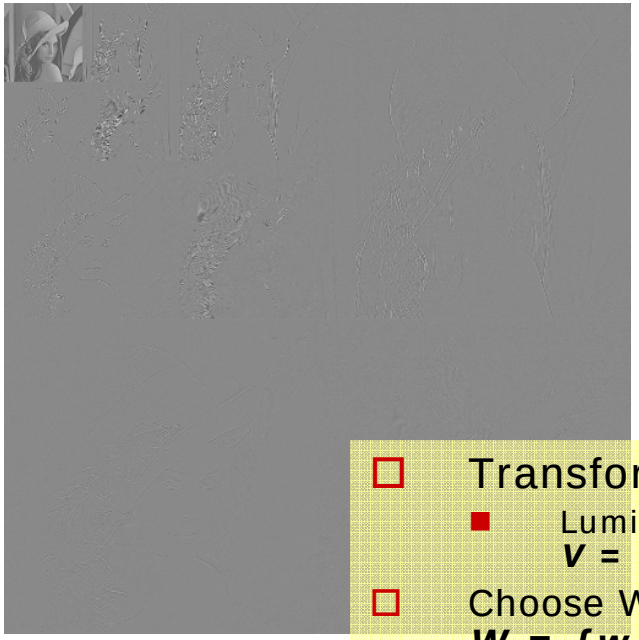
"On the Internet, nobody knows you're a dog."

This talk

1. Marking and tracing: *Codes for identification*
   - Related areas
     - Authentication codes
     - Other applications of codes for security *(not in this talk)*
       - Key pre-distribution
       - Key assignment for sensor networks
       - …

2. Ring authentication: *Privacy enhanced authentication*
   - Related topics *(not in this talk)*
     - Ring signature
     - Anonymous credential
     - Group signature

Marking objects



- Transform Image
  - Luminance Coefficients
    $V = \{v_1, v_2, \ldots, v_n\}$
- Choose Watermark
  $W = \{w_1, w_2, \ldots, w_n\}$, $w_i \in N(0,1)$
- Embed
  $V' = V + \alpha W$
- Extract
  $X = (V' - V) / \alpha$
  $S = X.W / ||X||$

Block-based Embedding

2			1
	2		
		1	
1		2	

Fingerprint:
2 1 3 1 1 2

Collusion Attack:

1			2
	3		
		2	
2		3	

2			1
	2		
		1	
1		2	

Pirate object

2			2
	3		
		1	
1		2	

Tracing Colluders: *Static Content*

- An *(l,n,m)* code is a set of n strings of length *l* over an alphabet of size *m* is a collection
- Example: *A={1,2,3},* a *(4,5,3)*-code

a1 = 3 1 1 2
a2 = 1 2 1 3
a3 = 2 2 2 2
a4 = 1 3 3 1
a5 = 3 3 2 1

- Codes for marking and tracing
  - Frame-proof codes
  - Codes with Identifiable Parent Property
  - c-secure codes
  - c-traceability codes
  - ..

Modeling Collusion

a1 = **3** 1 **1** 2
a2 = 1 **2** 1 **3**
a3 = 2 **2** 2 2

} parent words

3 2 1 3 → descendent word

- "Marking assumption"
  - How colluders construct the pirate object
- Other marking assumptions
  - Some marks are erased
  - Part of the string deleted

3 2 ? 3

3 2

Traceability Codes

(Staddon, Stinson, Wei 2000)

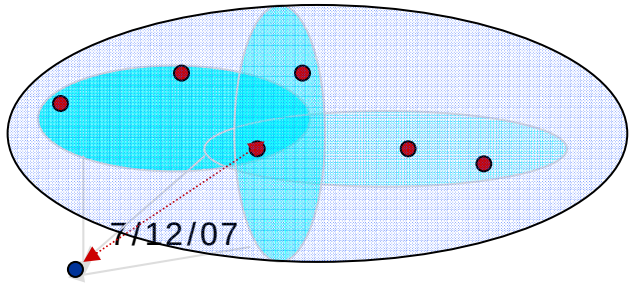
- A w-TA code is a code such that:

  Given a descendent of a set of up to w codewords , there exists a codeword that,

  - Has the smallest Hamming distance to this descendent
  - Belongs to every set of codewords of size up to w that could produce that descendent

  ➔ Given a descendent of a set of up to w codeword, at least one parent can be identified:

  find the codeword that is closest to the descendent



"Good" codes

- Codes with many codewords→ many users
- Small alphabet→ few bit embedding
- Efficient tracing

- Construction *approaches*
  - From scratch: an error correcting code with $d>(1-1/w^2)$ gives a w-traceability codes
  - Recursive construction: start from a small code and build on that

A Recursive Construction

(Safavi-Naini, Tonien 2006)

n, J are positive integers, $J > 1$,

An (n, J)-difference function family is a function family

$\Phi = \{\phi_{i,j} : i = 1, \ldots, n,\ j = 1, \ldots, J\}$ with nJ functions that map $[n] \rightarrow [n]$ and satisfies the following condition:

$$\begin{cases} \phi_{i_1,j_1}(x) = \phi_{i_2,j_1}(y) \\ \phi_{i_1,j_2}(x) = \phi_{i_2,j_2}(y) \\ j_1 \neq j_2 \end{cases} \longrightarrow \begin{cases} i_1 = i_2 \\ x = y \end{cases}$$

Explicit Constructions

An example:

Let $\Phi = \{\phi_{i,j}\} \subset [n]^{[n]}$ is a function family of size $n \times J$ with

$\phi_{i,j}(x) \equiv tjx + \mu(i) + \eta(j) + \xi(x) \pmod{n}$

- n, J, t be positive integers such that $J > 1$ and $\gcd(n, t) = \gcd(n, (J-1)!) = 1$
- η, ξ, μ are functions mapping $[n]$ into $\mathbf{Z}$; μ is one-to-one modulo n

Then Φ is an (n, J)-difference function family.

An Example

Choose $n = 5$, $J = 3$, $t = 1$, $s = 1$, $\eta = 0$, $\xi = 0$

$\phi_{i,j}(x) \equiv jx + i \pmod 5$

$$\Phi = \begin{matrix} \phi_{1,1} & \phi_{1,2} & \phi_{1,3} \\ \phi_{2,1} & \phi_{2,2} & \phi_{2,3} \\ \phi_{3,1} & \phi_{3,2} & \phi_{3,3} \\ \phi_{4,1} & \phi_{4,2} & \phi_{4,3} \\ \phi_{5,1} & \phi_{5,2} & \phi_{5,3} \end{matrix}$$

$\phi_{1,1}(x) = x + 1 \pmod 5$	$\phi_{1,2}(x) = 2x + 1 \pmod 5$
$1 \mapsto 2$	$1 \mapsto 3$
$2 \mapsto 3$	$2 \mapsto 5$
$3 \mapsto 4$	$3 \mapsto 2$
$4 \mapsto 5$	$4 \mapsto 4$
$5 \mapsto 1$	$5 \mapsto 1$

Recursive Construction

Γ has 5 codewords, represented as 5 rows. The matrix $\phi_{1,1}(\Gamma)$ is define as follows

$$\begin{array}{lll} \phi_{1,1}(x) = x + 1 \pmod 5 & \Gamma & \phi_{1,1}(\Gamma) \\ 1 \mapsto 2 & \Gamma_1 & \Gamma_2 \\ 2 \mapsto 3 & \Gamma_2 & \Gamma_3 \\ 3 \mapsto 4 & \Gamma_3 & \Gamma_4 \\ 4 \mapsto 5 & \Gamma_4 & \Gamma_5 \\ 5 \mapsto 1 & \Gamma_5 & \Gamma_1 \end{array}$$

$\phi_{1,1}(\Gamma)$ as the same size as Γ

The new code

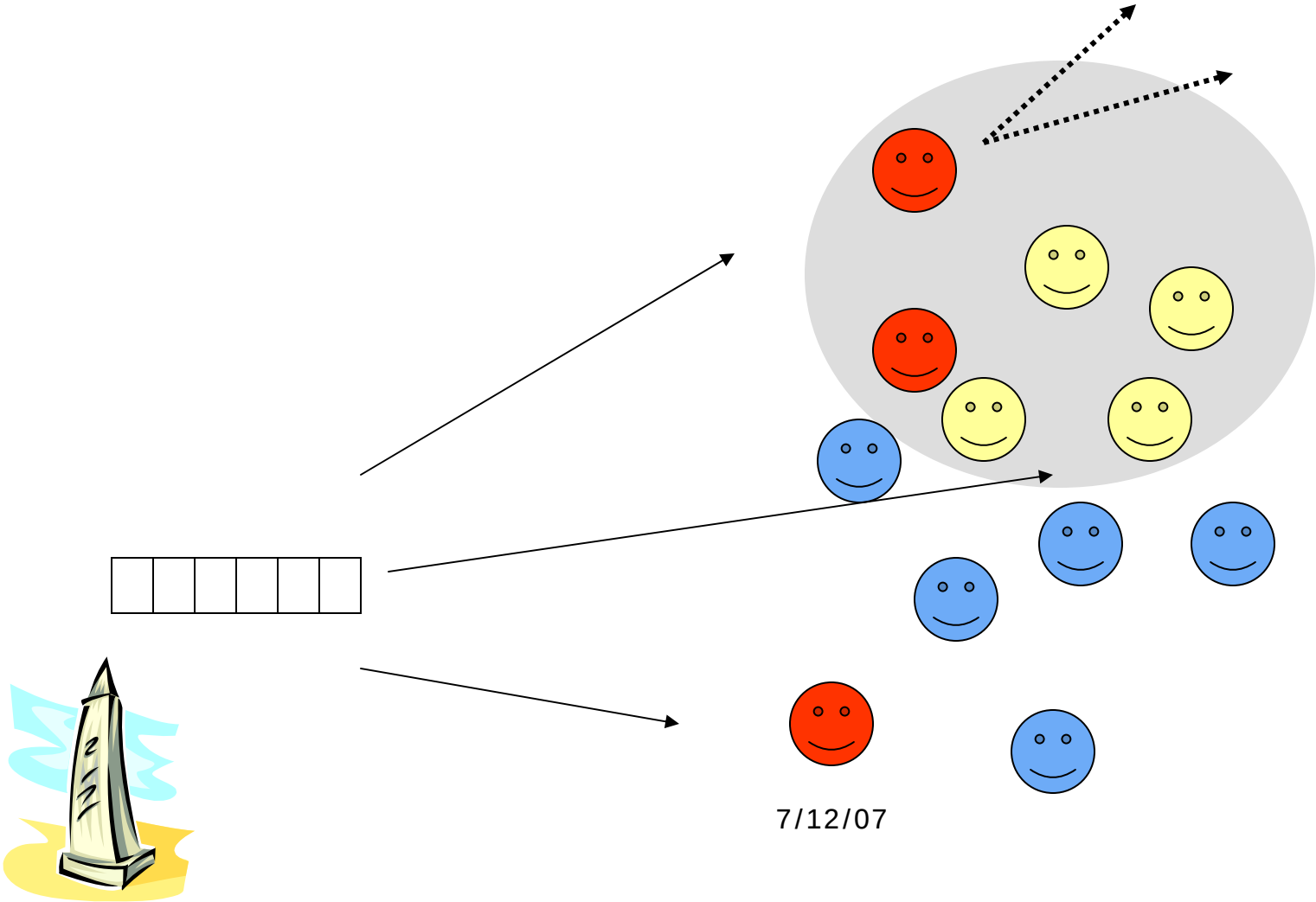
Putting all matrices $\phi_{i,j}(\Gamma)$ together as one matrix

$$\Phi(\Gamma) = \begin{matrix} \phi_{1,1}(\Gamma) & \phi_{1,2}(\Gamma) & \phi_{1,3}(\Gamma) \\ \phi_{2,1}(\Gamma) & \phi_{2,2}(\Gamma) & \phi_{2,3}(\Gamma) \\ \phi_{3,1}(\Gamma) & \phi_{3,2}(\Gamma) & \phi_{3,3}(\Gamma) \\ \phi_{4,1}(\Gamma) & \phi_{4,2}(\Gamma) & \phi_{4,3}(\Gamma) \\ \phi_{5,1}(\Gamma) & \phi_{5,2}(\Gamma) & \phi_{5,3}(\Gamma) \end{matrix}$$

Size of $\Phi(\Gamma)$:

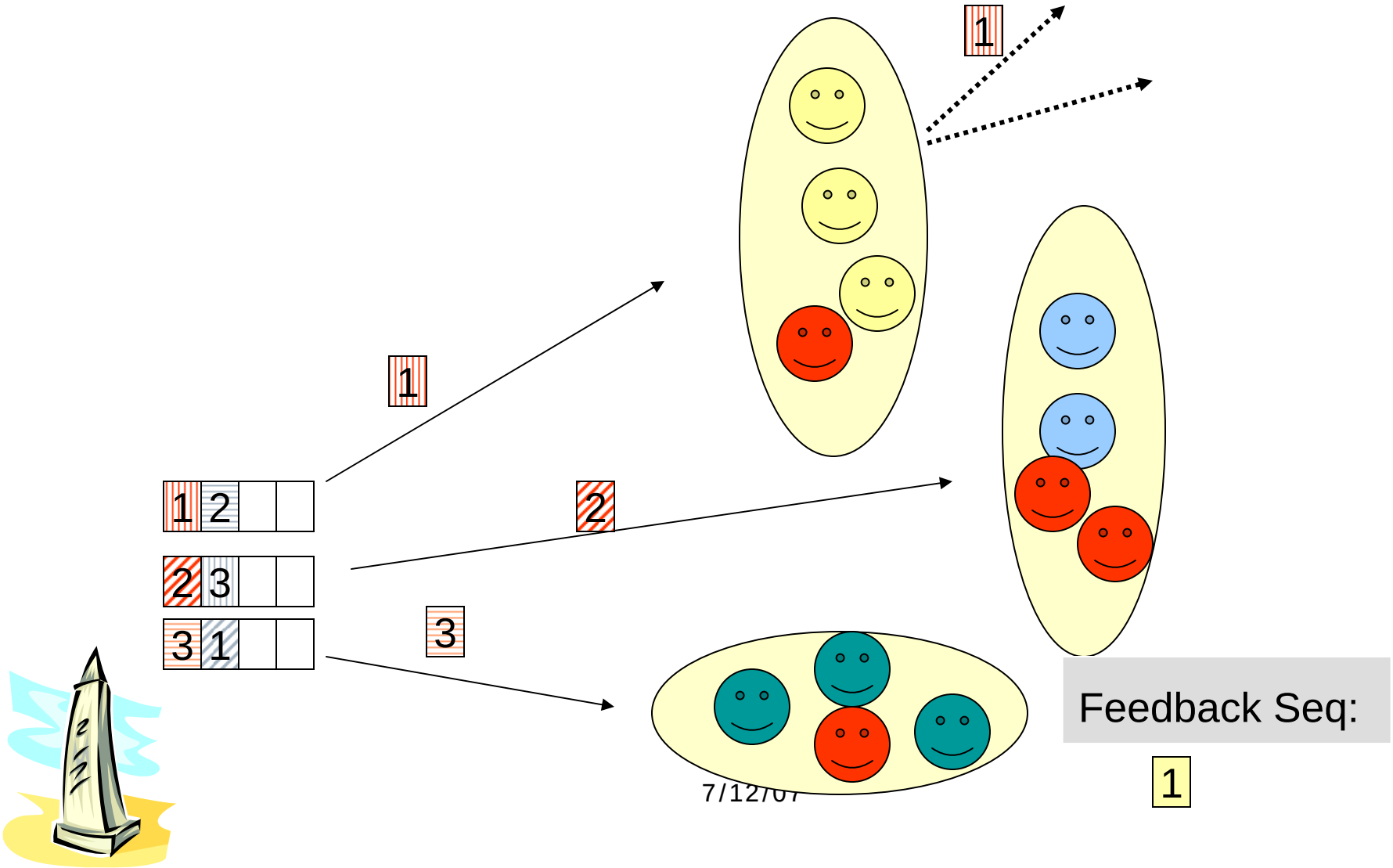
- Matrix form of Γ of size $n \times \ell$;
- Φ of size $n \times J \Rightarrow \Phi(\Gamma)$ is of size $n^2 \times \ell J$

Tracing Colluders: *Dynamic content:* ***Re-broadcast***

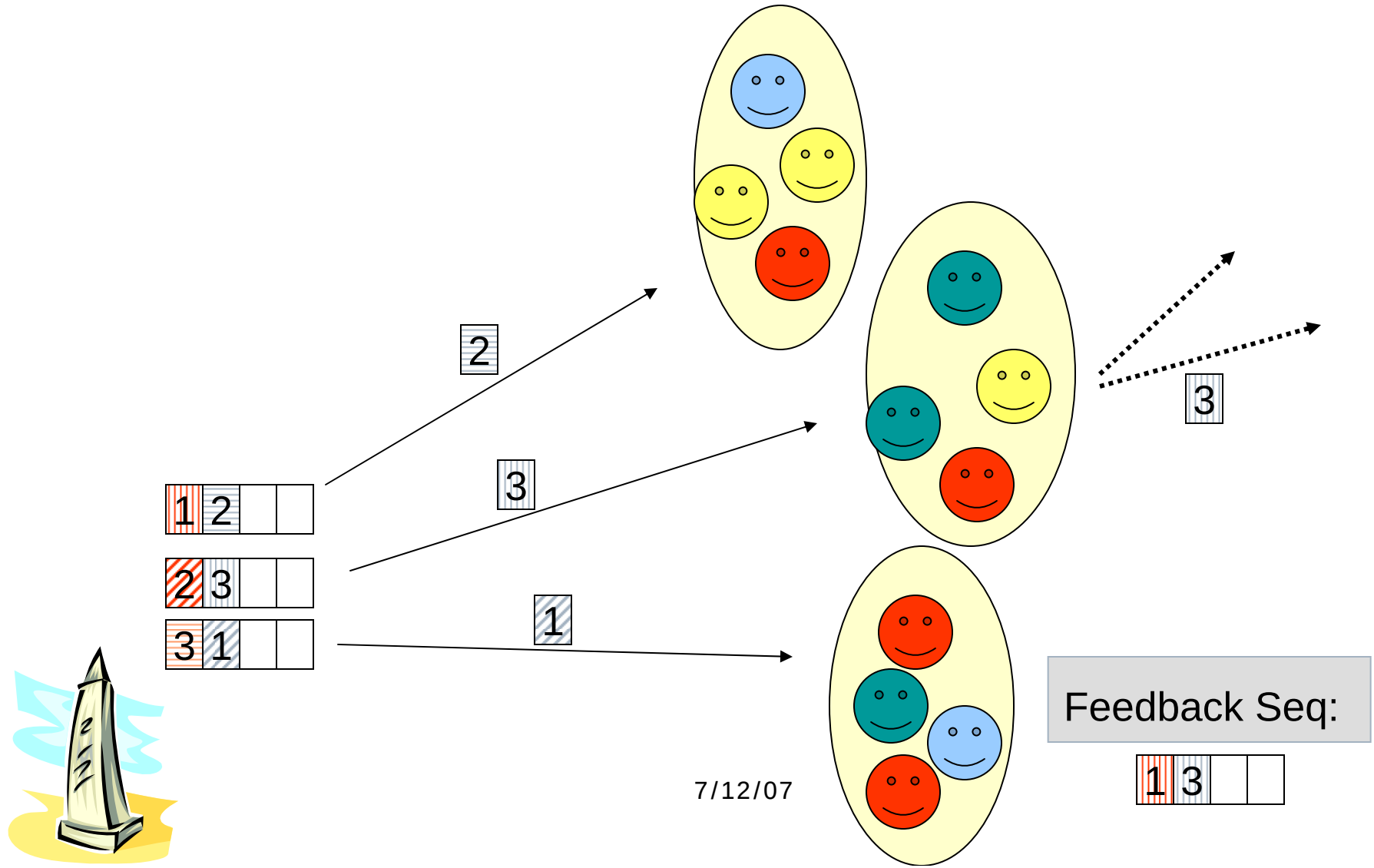


Sequential Tracing

(Safavi-Naini, Wang 2000)



Sequential Tracing



Mark Allocation Table

(1, 1):	1	2	3	4	5	6
(1, 2):	2	4	6	8	10	1
(1, 3):	3	6	9	1	4	7
(1, 4):	4	8	1	5	9	2
(1, 5):	5	10	4	9	3	8
(1, 6):	6	1	7	2	8	3
(1, 7):	7	3	10	6	2	9
(1, 8):	8	5	2	10	7	4
(1, 9):	9	7	5	3	1	10
(1, 10):	10	9	8	7	6	5

(2, 1):	1	3	4	5	6	7
(2, 2):	2	6	8	10	1	3
(2, 3):	3	9	1	4	7	10
(2, 4):	4	1	5	9	2	6
(2, 5):	5	4	9	3	8	2
(2, 6):	6	7	2	8	3	9
(2, 7):	7	10	6	2	9	5
(2, 8):	8	2	10	7	4	1
(2, 9):	9	5	3	1	10	8
(2, 10):	10	8	7	6	5	4

(3, 1):	1	4	5	6	7	8
(3, 2):	2	8	10	1	3	5
(3, 3):	3	1	4	7	10	2
(3, 4):	4	5	9	2	6	10
(3, 5):	5	9	3	8	2	7
(3, 6):	6	2	8	3	9	4
(3, 7):	7	6	2	9	5	1
(3, 8):	8	10	7	4	1	9
(3, 9):	9	3	1	10	8	6
(3, 10):	10	7	6	5	4	3

(4, 1):	1	5	6	7	8	9
(4, 2):	2	10	1	3	5	7
(4, 3):	3	4	7	10	2	5
(4, 4):	4	9	2	6	10	3
(4, 5):	5	3	8	2	7	1
(4, 6):	6	8	3	9	4	10
(4, 7):	7	2	9	5	1	8
(4, 8):	8	7	4	1	9	6
(4, 9):	9	1	10	8	6	4
(4, 10):	10	6	5	4	3	2

(5, 1):	1	6	7	8	9	10
(5, 2):	2	1	3	5	7	9
(5, 3):	3	7	10	2	5	8
(5, 4):	4	2	6	10	3	7
(5, 5):	5	8	2	7	1	6
(5, 6):	6	3	9	4	10	5
(5, 7):	7	9	5	1	8	4
(5, 8):	8	4	1	9	6	3
(5, 9):	9	10	8	6	4	2
(5, 10):	10	5	4	3	2	1

10	10	8	3	6	7
↓	↓	↓	↓	↓	↓
(1, 10)	(1, 5)	(1, 10)	(1, 9)	(1, 10)	(1, 3)
(2, 10)	(2, 7)	(2, 2)	(2, 5)	(2, 1)	(2, 1)
(3, 10)	(3, 8)	(3, 6)	(3, 6)	(3, 4)	(3, 5)
(4, 10)	(4, 2)	(4, 5)	(4, 2)	(4, 9)	(4, 2)
(5, 10)	(5, 9)	(5, 9)	(5, 10)	(5, 8)	(5, 4)

Colluders: (1,10), (4,2)

Feedback Seq: (10, 10, 8, 3, 6, 7)

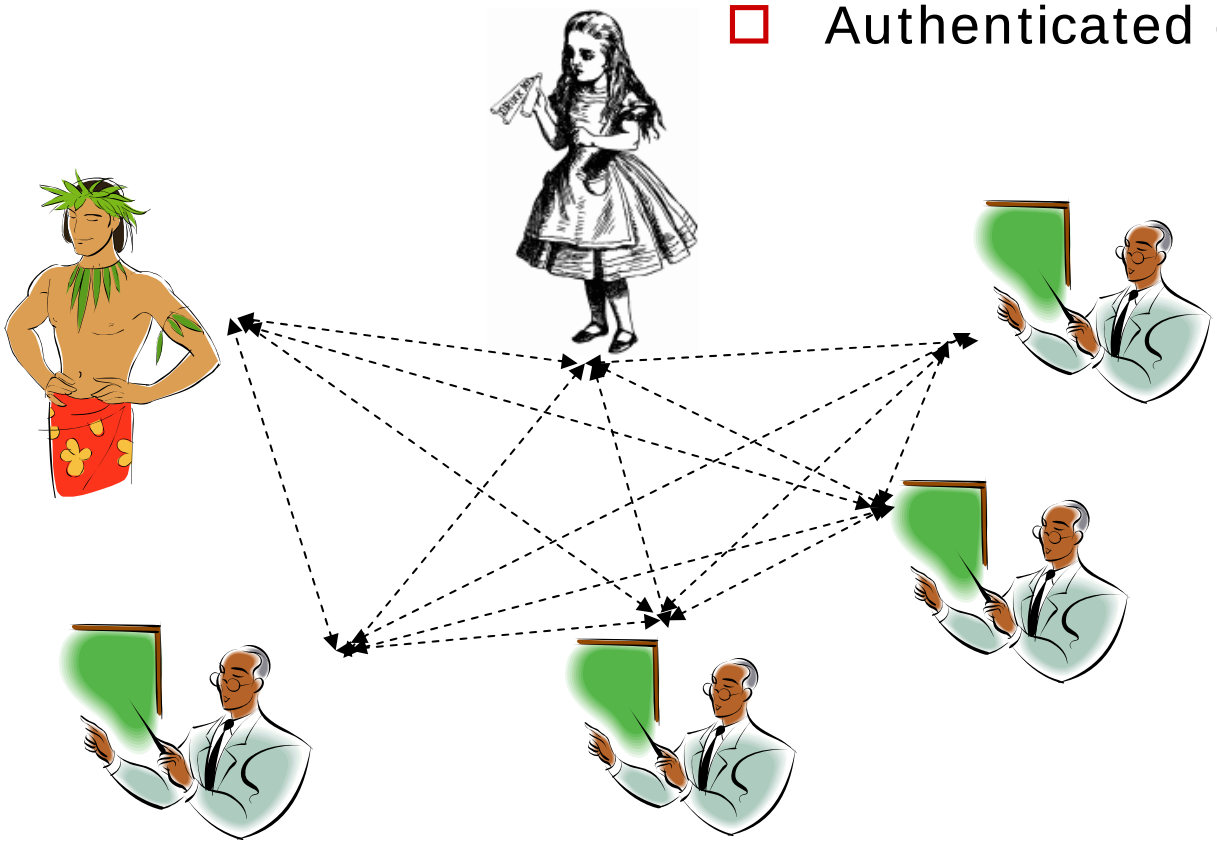
First Colluder after: $c^2+1=5$

- Sequential tracing can be used for ***static content***
  - Use each row of the table as a fingerprint sequence

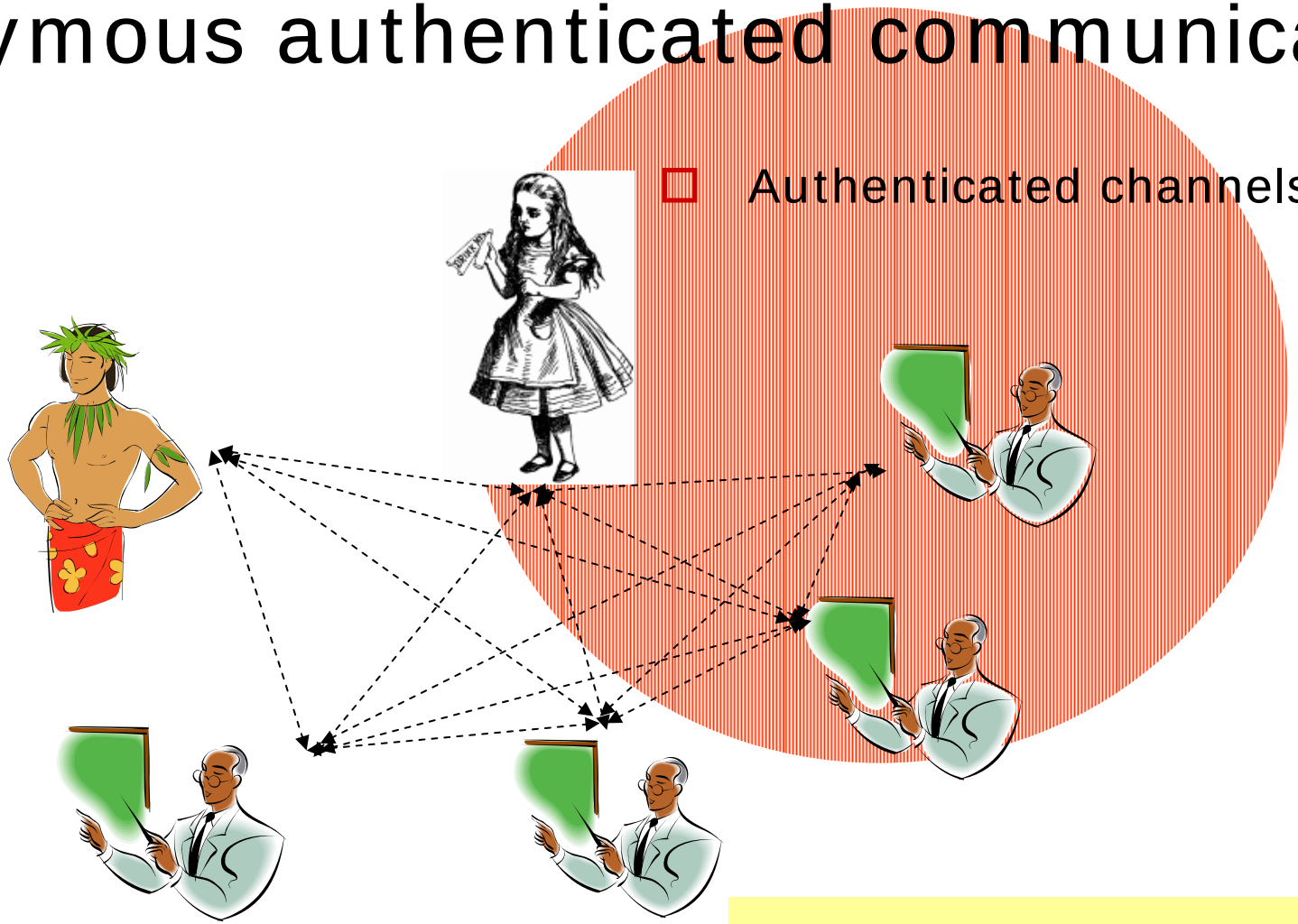
2. Privacy preserving authentication

- Privacy is the `right to be left alone'
- Control over one's personal information
  - Choice of whether to disclose information
  - Control over whom to share it with
  - Control over how it is used
    - purpose
- Anonymous = *'without a name'*
  - One aspect of privacy
- Degrees of anonymity
  - One of three suspects
  - Anonymous submission
  - Anonymous communications
    - Email, ftp, web surfing

Anonymous authenticated communication



Anonymous authenticated communication



User controlled anonymity

Ring authentication

Ring Signature (RST 2000)

- Alice chooses a set of *possible signers* = *ring*
  - *ring-sign(m; P_1; P_2; ... P_r; sk_A; PK_X)*
  - *ring-verify(m; σ)*
- *Properties*
  - Everyone can verify that message is from the group
  - *set-up free*

  But, the size grows linearly with the size of the ring
- RSA public key $P_i = (n; e_i)$
  - $f_i(x) = x^{ei} \pmod n$

Ring-sign(m; P_1,$P_{2\ 1}$, $sk_{\ 1}$, PK_X): $E_{H(m)}(E_{H(m)}(v+x_1^{e1}) +x_2^{e2})=v$

➔ *$u= x_1^{e1}$* ➔ *x_1*

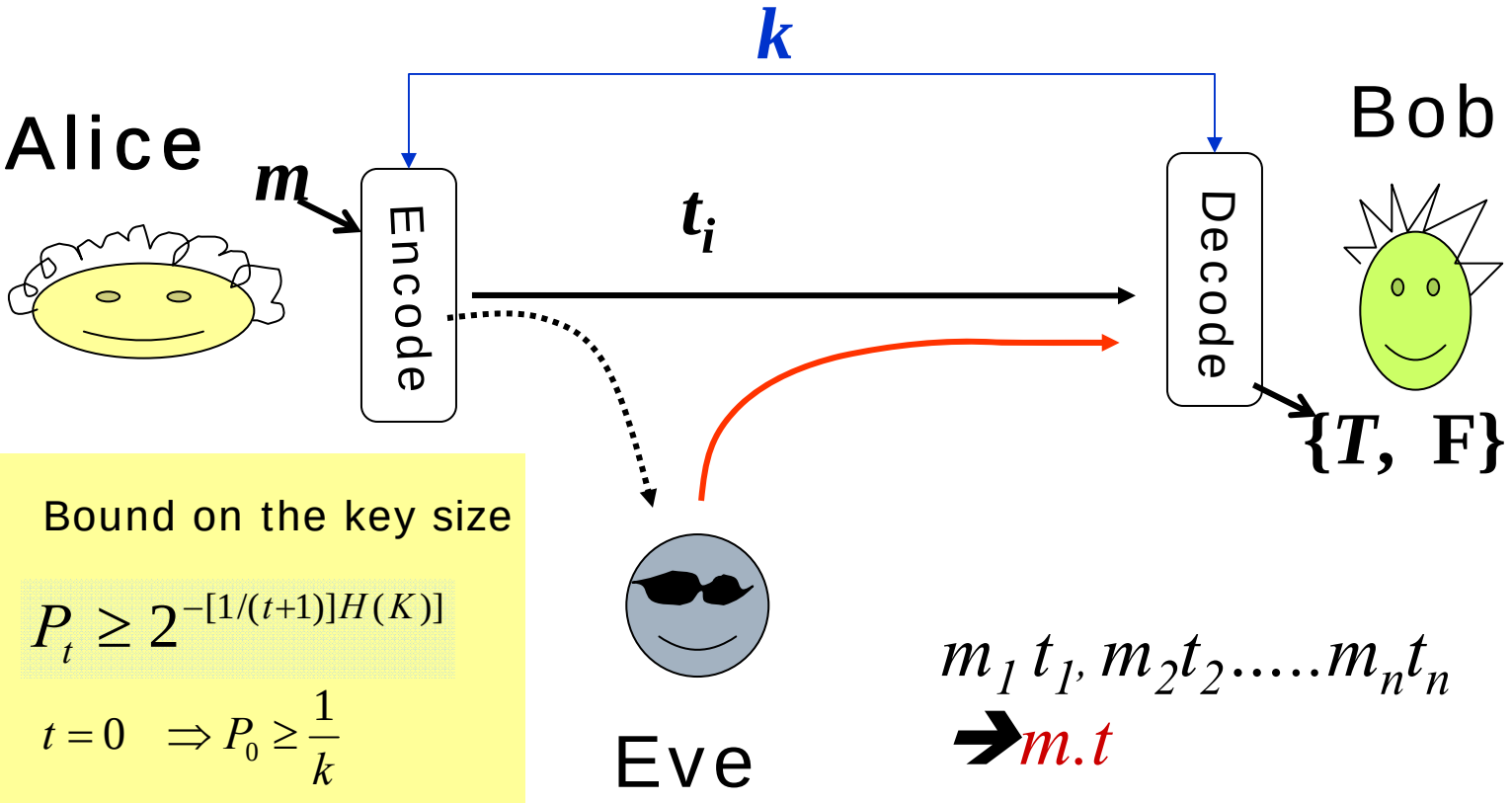
Ring-sign(m)= (m; P_1,P_2, x_1,x_2)

Limitations:

- Requires *PKI*
- a
- *Signatures can be forged if,*
  - RSA (or DL) problem is solved
  - More powerful computers can factorise the modulus Alice has used
  - Quantum computers can be built..
- Signatures are expensive
- Unconditionally secure anonymity
  - Dining cryptographer (Chaum 1980's)

Authentication Codes (A-codes)

(Simmons 1982, Gilbert, MacWilliams &Sloane 1974)



- Bound on the key size

$$P_t \geq 2^{-[1/(t+1)]H(K)]}$$

$$t=0 \quad \Rightarrow P_0 \geq \frac{1}{k}$$

$$t=1 \quad \Rightarrow P_1 \geq \frac{1}{\sqrt{k}}$$

$$t=2 \quad \Rightarrow P_2 \geq \frac{1}{\sqrt[3]{k}}$$

$m_1 t_1, m_2 t_2 \ldots\ldots m_n t_n$

➔ $m.t$

Unconditionally secure authentication systems are practical.

Wegman-Carter Construction:

ε-AU hash function+ encryption

US Ring Authentication: User controlled anonymity *(ASIACCS 2007)*

- Ring Authentication (RA)
  - Initialisation
  - $RTg: t \leftarrow RTg(k_{X'}, [X,j], m)$
  - $RVf(k_X, [X,j], m.t) \in \{0,1\}$
- Properties
  - Correctness
    $RVf(k_X, [X,j], m.RTg(k_X, [X,j], m)) = 1$
  - Security
    $P[\, RVf(k_X, [X,j], m.t)=1 \mid k_C, [X_1,j1], m_1.t_1, .. [X_u,j_u], m_u.t_u\ 1] < \varepsilon$
    $C \cap X' = \varnothing$

  ➔ Anonymity

  ➔Collusion tolerance
    - Collusion of up to size c cannot 'break' system's security
- Security
  - Anonymity
    - The chance of spoofing by an outsider is negligible
  - Authenticity/Accountability
    - An authenticated message could only be generated by a non group member

- A trivial system:
  - Give a shared key to all group members

  ➔ No accountability

US Ring Authentication

A generic construction:

1. A-code
2. Non-interactive conference key distribution

- Trusted initializer
  - Distributes initial secrets
- u_i calculates a common key k with a group $X=\{u_1, u_2 \ldots u_\omega\}$
- $C= \{u_{\omega+1} \ldots u_{\omega+c}\}$ cannot learn anything about k
- Perfect security $H(k_X|K_C)= H(k_X)$

- TI distributes keys
- u_j chooses a group X and finds $k[X,i]$
- For a message s, finds the tag
  - $RTag= Tg(s, k[X,i])$
- Verification:
  - Calculate the tag and compare
- Security statement (informally):

  The construction is secure if the authentication code and conference keys are secure

A concrete construction

1. **An A-code with perfect protection**

- $s \in GF(q)$, $k=(a,b)$, $a,b \in GF(q)$

  $Tg\ (k,s)= t= a \times m+b$ ➔ $m.t$

  $Ver(k, u.v)$: $au+b=v$

  $P_0=P_1= 1/q$

m_1

	$s_1=0$	$s_2=1$
$(0,0)$	$t_1=0$	$t_1=0$
$(1,0)$	$t_1=0$	$t_2=1$
$(1,1)$	$t_2=1$	$t_1=0$
$(0,1)$	$t_2=1$	$t_2=1$

m_2

2. An (ω,c)-NI Conference Key Distribution

- Symmetric polynomials: for any permutation σ
  $F(x_1 \ldots x_w) = F(x_{\sigma(1)} \ldots , x_{\sigma(w)})$
- Initialization:
  - Randomly chooses a degree c symmetric polynomial $F(x_1 \ldots x_w)$,
  - coefficients randomly chosen from a finite field GF(q)
- Key for User u_i : $F_i=F(i_1,\ldots x_w)$
- u_1 calculates a shared key with
  $X=\{u_2,..u_\omega\}$
  $k_X=F_1(2,\ldots \omega)$
- Security: $H(k_X|K_C)=1/q$

A ring authentication system

- Initialization:
  - TI randomly chooses two degree c symmetric polynomials
    $F(x_1....x_w)$, $G(x_1....x_w)$
  - Key for user u_i :
    $F(i, x_2,...x_w)$, $G(i, x_2,...x_w)$

- u_1 wants to send a message m to u_2,
  - Choose an anonymity set
    $X=\{u_1, u_3, . u_w\}$
  - Find
    $a= F_1(x_2..x_w)$, $b= G_1(x_2... x_w)$
    $t= a \times m+b$ ➔ $[X, u_2],m.t$

Security:

- The system is $(1/q)$-secure (w,c) USRA of order 2, with $w+c<N$

Ring authentication with computational security *(ASIACCS 2008)*

- Main idea:
  - The same:
    NICKDS+ MAC
- Challenges:
  - Adaptive security: adversary with access to REVEAL oracle
  - NICKDS is secure against passive adversary

  ➔ Define adaptive security for NICKD

  ➔Construct secure NICKDS

- Construction:

NICKS (passive sec)+ Hash
➔ NICDS (adaptive sec)

Other privacy enhanced systems

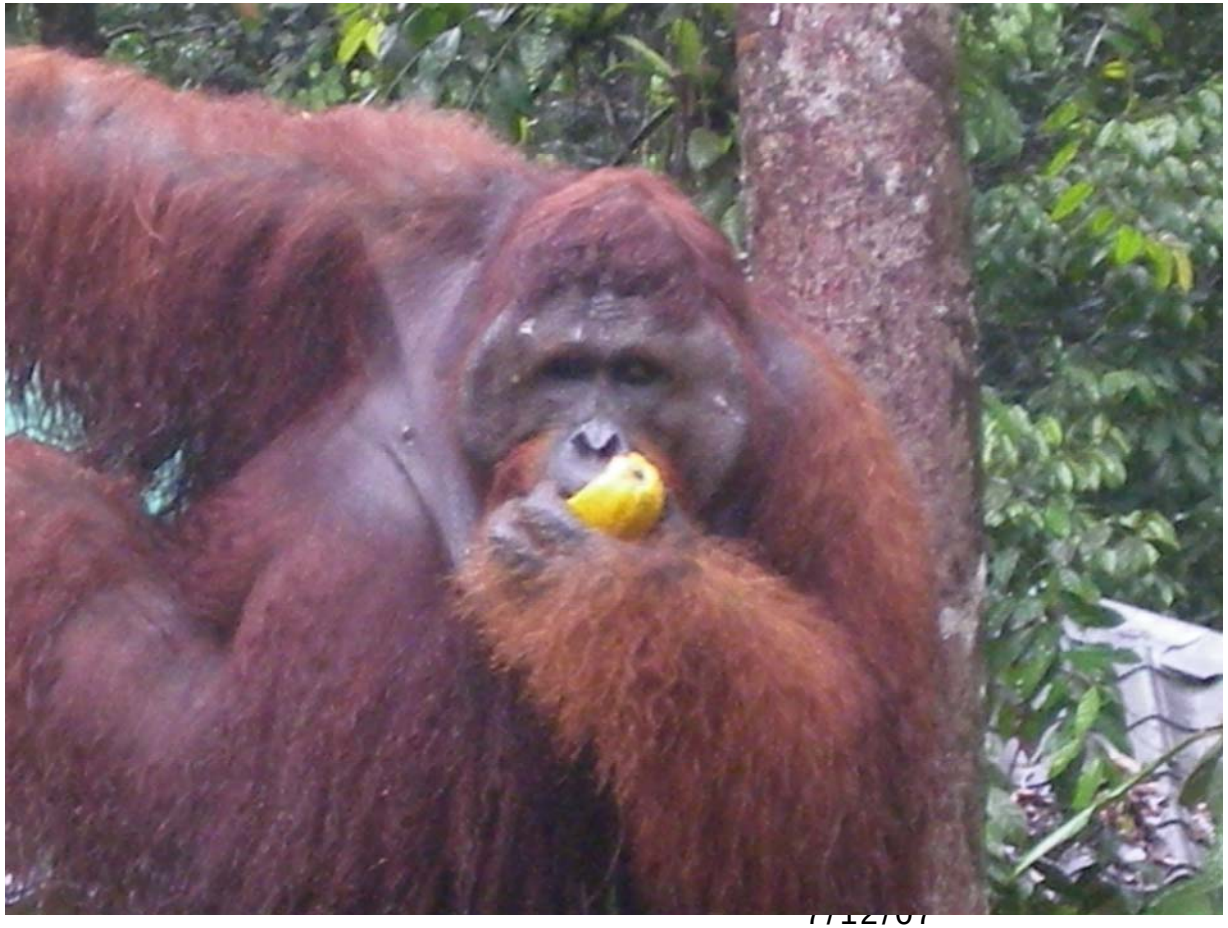
- Anonymous identification
  - Anonymous credential systems
    - Authorising without identifying
  - Ad hoc anonymous identification

- Anonymous authentication
  - Hiding the sender of a message while ensuring authenticity
    - Group signature
    - Ring signature
    - Ring authentication

Summary

- Privacy preserving security
- Codes and finite structures for security applications
- Security systems for content protection
- Other research at Calgary
  - Database privacy
  - Biometrics
  - Malicious software
  - Intelligent testing for softwares

Thank you!



George@Kuching.Malasya