A 2-Round Anonymous Veto Protocol

A new solution to the dining cryptographers problem

Speaker: Feng Hao

Computer Laboratory
University of Cambridge

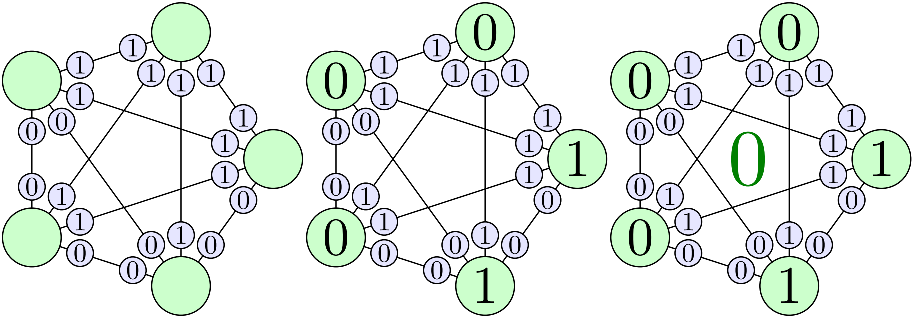
Joint work with Piotr Zieliński

Security Protocols Workshop '06

A crypto puzzle

The Galactic Security Council must decide whether to invade an enemy planet. Some delegates wish to veto the measure, but worry about sanctions from the pro-war faction. This presents a dilemma: how can they anonymously veto the decision?

Dining Cryptographers



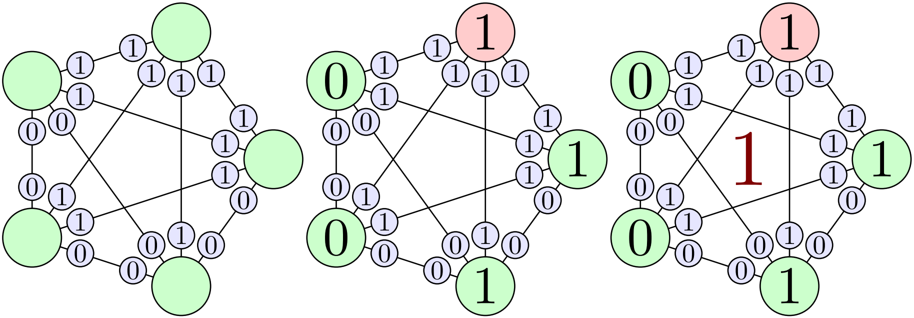
Dining Cryptographers Problem

- How to determine OR – essentially a veto problem

Solution: DC-net [Chaum, 1988]

1. set up pairwise keys through private channels
2. broadcast **xor** of the shared keys or the opposite
3. compute **xor** of the broadcast values

Dining Cryptographers



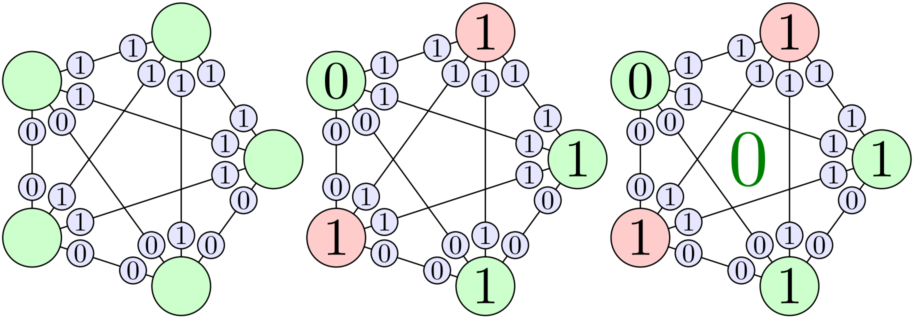
Dining Cryptographers Problem

- How to determine OR – essentially a veto problem

Solution: DC-net [Chaum, 1988]

1. set up pairwise keys through private channels
2. broadcast **xor** of the shared keys or the opposite
3. compute **xor** of the broadcast values

Dining Cryptographers



Message collision: two messages cancel each other out

Dining Cryptographers

Summary of DC-net Weaknesses

- Message collisions
- Complex key setup
- Subject to disruptions

There are other solutions

- Circuit evaluation by Goldreich, Micali and Wigderson [1987]
- Anonymous veto protocols by Kiayias-Yung [2003], Groth [2004] and Brandt [2005].
- But they are not efficient.

Our solution

Our solution: Anonymous Veto Network (AV-net)

- Overcomes all the major limitations in DC-net
- No secret channels, third parties and collisions
- Efficient in many aspects: rounds, computation load and bandwidth usage

Anonymous Veto Network protocol

Round 1: (for every participant $P_i \in \{P_1, \ldots, P_n\}$)

1. broadcast g^{x_i} and a knowledge proof for x_i.
2. compute

$$g^{y_i} = \prod_{j=1}^{i-1} g^{x_j} \Bigg/ \prod_{j=i+1}^{n} g^{x_j}$$

Round 2:

1. broadcast $g^{c_i y_i}$ and a knowledge proof for c_i

$$g^{c_i y_i} = \begin{cases} g^{x_i y_i} & \text{if } P_i \text{ sends `0' (no veto)} \\ g^{r_i y_i} & \text{if } P_i \text{ sends `1' (veto), where } r_i \text{ is random} \end{cases}$$

2. the following holds iff nobody vetoed:

$$\prod_i g^{c_i y_i} = 1$$

Correctness of AV-net

Theorem

$$\text{No veto} \iff \prod_i g^{x_i y_i} = 1 \iff \sum_i x_i y_i = 0$$

Proof

$$g^{y_i} = \prod_{j=1}^{i-1} g^{x_j} \Big/ \prod_{j=i+1}^{n} g^{x_j} \iff y_i = \sum_{j=1}^{i-1} x_j - \sum_{j=i+1}^{n} x_j$$

$$\begin{aligned}\sum_i x_i y_i = \quad & - x_1x_2 - x_1x_3 - x_1x_4 \\ & + x_2x_1 - x_2x_3 - x_2x_4 \\ & + x_3x_1 + x_3x_2 - x_3x_4 \\ & + x_4x_1 + x_4x_2 + x_4x_3 \qquad = 0.\end{aligned}$$

Security analysis

- The two ciphertexts, ‘0’ and ‘1’, are indistinguishable
- Only compromised under full-collusion
- Resistance to disruptions — veto cannot be suppressed

Efficiency of AV-net

related work	pub year	round no	broad-cast	priv chan	colli-sion	third party	collu-sion	system compl
Circuit Eval	1987	$O(1)$	yes	yes	no	no	half	$O(n^2)$
Chaum	1988	≥ 2	yes	yes	yes	no	full	$O(n^2)$
Kiayias-Yung	2003	3	yes	no	no	yes	full	$O(n^2)$
Groth	2004	$n+1$	yes	no	no	yes	full	$O(n)$
Brandt	2005	4	yes	no	no	no	full	$O(n)$
AV-net	—	2	yes	no	no	no	full	$O(n)$

Conclusion

related work	pub year	round no	broad-cast	priv chan	colli-sion	third party	collu-sion	system compl
Circuit Eval	1987	$O(1)$	yes	yes	no	no	half	$O(n^2)$
Chaum	1988	≥ 2	yes	yes	yes	no	full	$O(n^2)$
Kiayias-Yung	2003	3	yes	no	no	yes	full	$O(n^2)$
Groth	2004	$n+1$	yes	no	no	yes	full	$O(n)$
Brandt	2005	4	yes	no	no	no	full	$O(n)$
AV-net	—	2	yes	no	no	no	full	$O(n)$

We propose the Anonymous Veto Network (AV-net)

- No secret channels, third parties and collisions
- Provably secure under Decision Diffie-Hellman
- Efficient in rounds, computation load and bandwidth usage
- Very little room left for improvement in efficiency