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 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 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
Message collision: two messages cancel each other out
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]
- But they are not efficient.
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

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

Proof

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

$\sum_i x_i y_i = -x_1 x_2 - x_1 x_3 - x_1 x_4$

$+ x_2 x_1 - x_2 x_3 - x_2 x_4$

$+ x_3 x_1 + x_3 x_2 - x_3 x_4$

$+ x_4 x_1 + x_4 x_2 + x_4 x_3 = 0$. 

Feng Hao, Piotr Zieliński
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

<table>
<thead>
<tr>
<th>related work</th>
<th>pub year</th>
<th>round no</th>
<th>broadcast</th>
<th>priv chan</th>
<th>colli-sion</th>
<th>third party</th>
<th>collu-sion</th>
<th>system compl</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit Eval</td>
<td>1987</td>
<td>$O(1)$</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>half</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Chaum</td>
<td>1988</td>
<td>$\geq 2$</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>full</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Kiayias-Yung</td>
<td>2003</td>
<td>3</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>full</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Groth</td>
<td>2004</td>
<td>$n + 1$</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>full</td>
<td>$O(n)$</td>
</tr>
<tr>
<td>Brandt</td>
<td>2005</td>
<td>4</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>full</td>
<td>$O(n)$</td>
</tr>
<tr>
<td>AV-net</td>
<td>—</td>
<td>2</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>full</td>
<td>$O(n)$</td>
</tr>
</tbody>
</table>

Feng Hao, Piotr Zieliński  
A 2-Round Anonymous Veto Protocol
## Conclusion

<table>
<thead>
<tr>
<th>related work</th>
<th>pub year</th>
<th>round no</th>
<th>broadcast</th>
<th>priv chan</th>
<th>collision</th>
<th>third party</th>
<th>collusion</th>
<th>system compl</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit Eval</td>
<td>1987</td>
<td>$O(1)$</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>half</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Chaum</td>
<td>1988</td>
<td>$\geq 2$</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>full</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Kiayias-Yung</td>
<td>2003</td>
<td>3</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>full</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Groth</td>
<td>2004</td>
<td>$n + 1$</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>full</td>
<td>$O(n)$</td>
</tr>
<tr>
<td>Brandt</td>
<td>2005</td>
<td>4</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>full</td>
<td>$O(n)$</td>
</tr>
<tr>
<td>AV-net</td>
<td>—</td>
<td>2</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>full</td>
<td>$O(n)$</td>
</tr>
</tbody>
</table>

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