Rapid Mixing and Security of Chaum's Electronic Voting

Marcin Gomułkiewicz (TU Wrocław)

Marek Klonowski (TU Wrocław)

Mirek Kutyłowski (TU Wrocław and CC Signet)

How do we spend next 18 minutes (more or less) ?

- electronic voting
- David Chaum's voting scheme
- Randomized Partial Checking – method of Markus Jakobsson Ari Jules and Ronald R. Rivest
- our result that relates to Chaum's scheme

Electronic Voting

What is expected ?

- anonymity of voters
- verifiability
- no vote selling
- low cost and efficiency

Chaum's Electronic Voting Scheme - user's point of view

Combines Visual Cryptography and digital processing

- At polling place voter gets "receipts"
- Votes are processed
- At the end of the protocol voter can easy check if the vote is included in the final tally.

Chaum's Electronic Voting Scheme

It has many advantages:

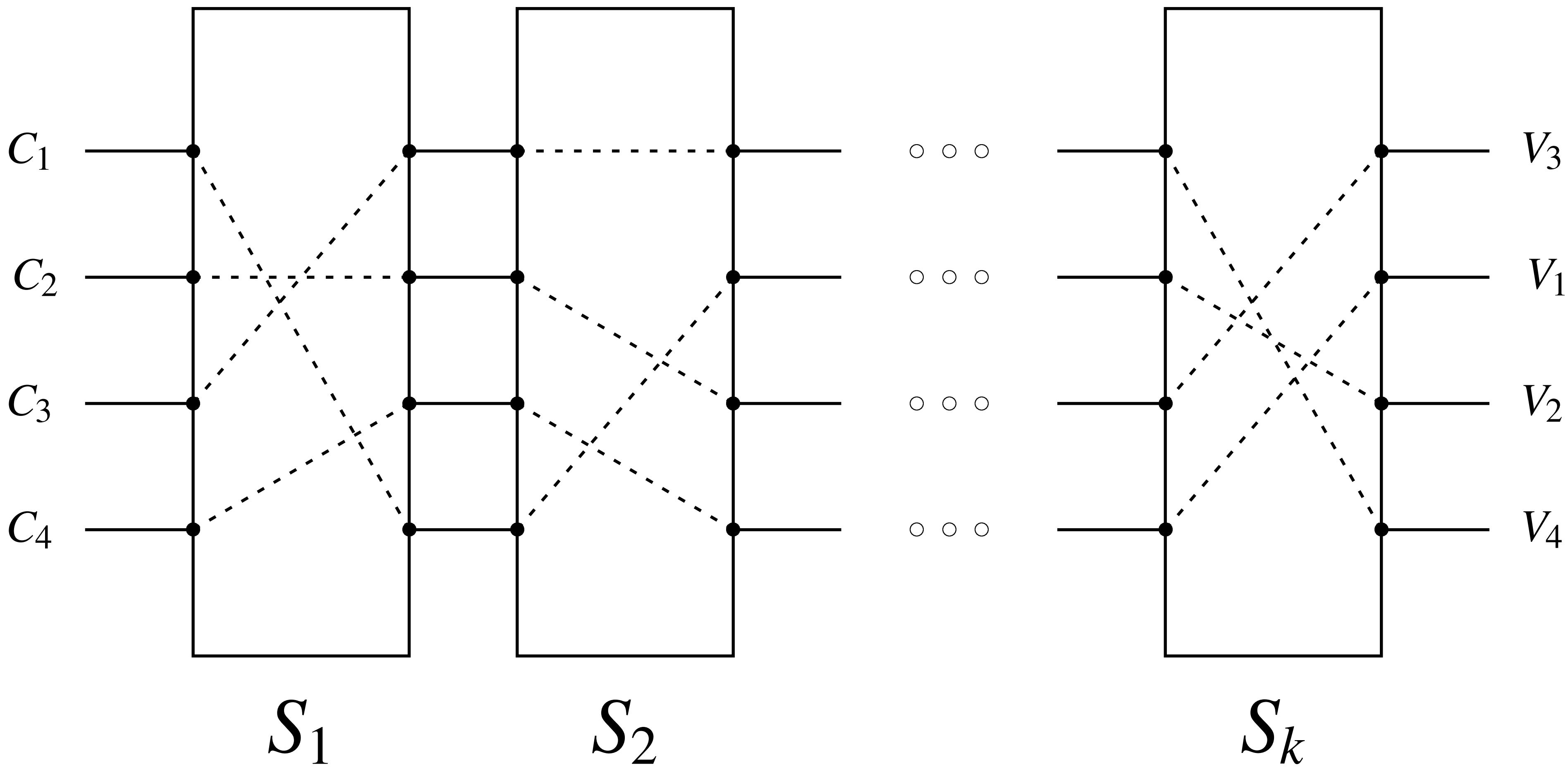
- fairly practical
- verifiable
- "receipts" for voters - no trust in electronic devices required
- no selling votes
- ...it seems that voter obtain anonymity, too

Our aim: Rigid mathematical proof of anonymity.

Electronic processing

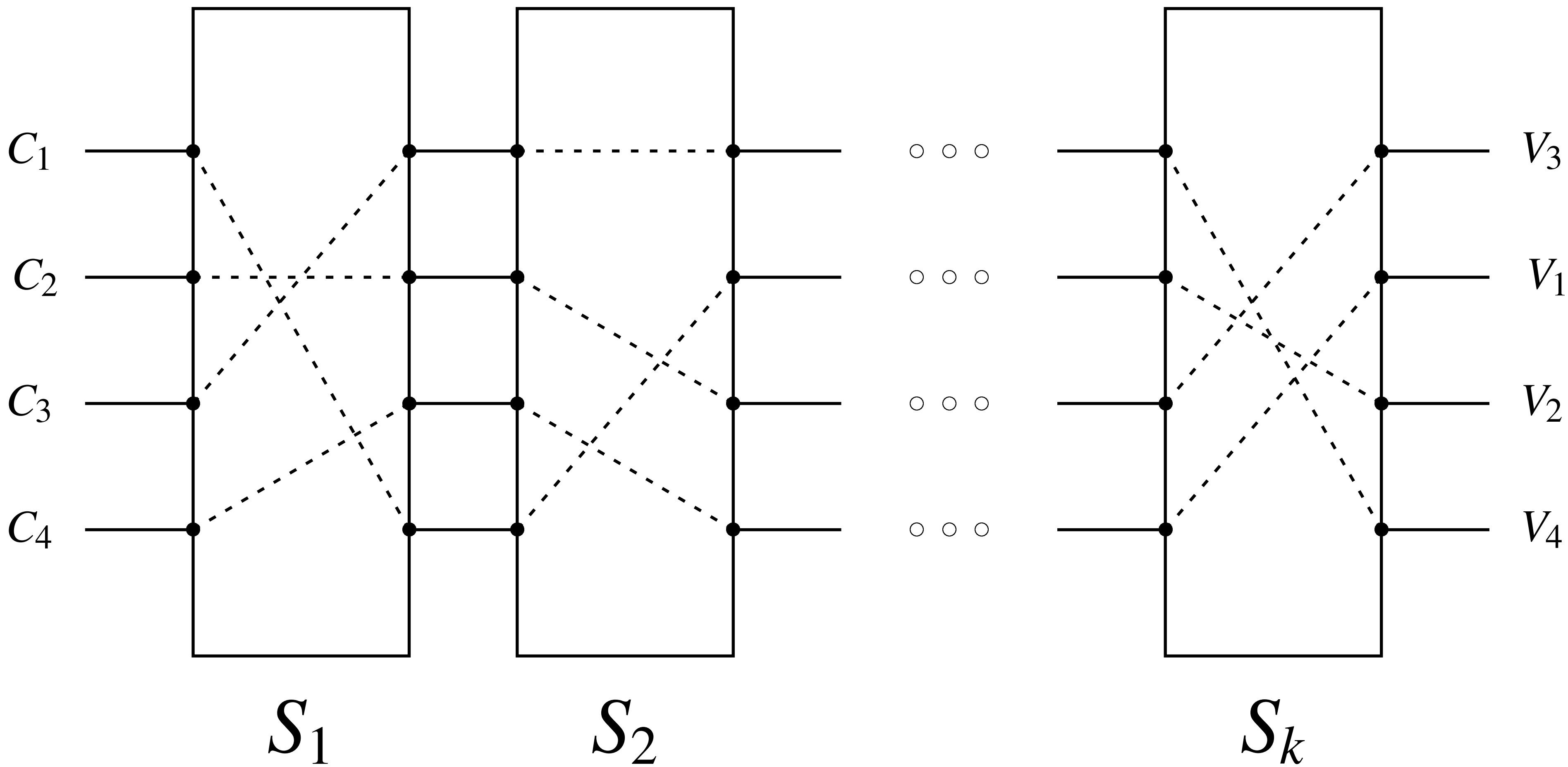
- Based on onion-routing
- k MIX-servers $S_1, S_2, ..., S_k$ with encryption and decryption algorithms E_i,D_i
- V-vote is encoded as $C = E_1(E_2(\ldots E_k(V)\ldots))$
- ...and decoded as $V = E_k(E_{k-1}(\ldots E_1(V)\ldots))$
- Each MIX-server peels off one encryption layer and mixes randomly all ballots.

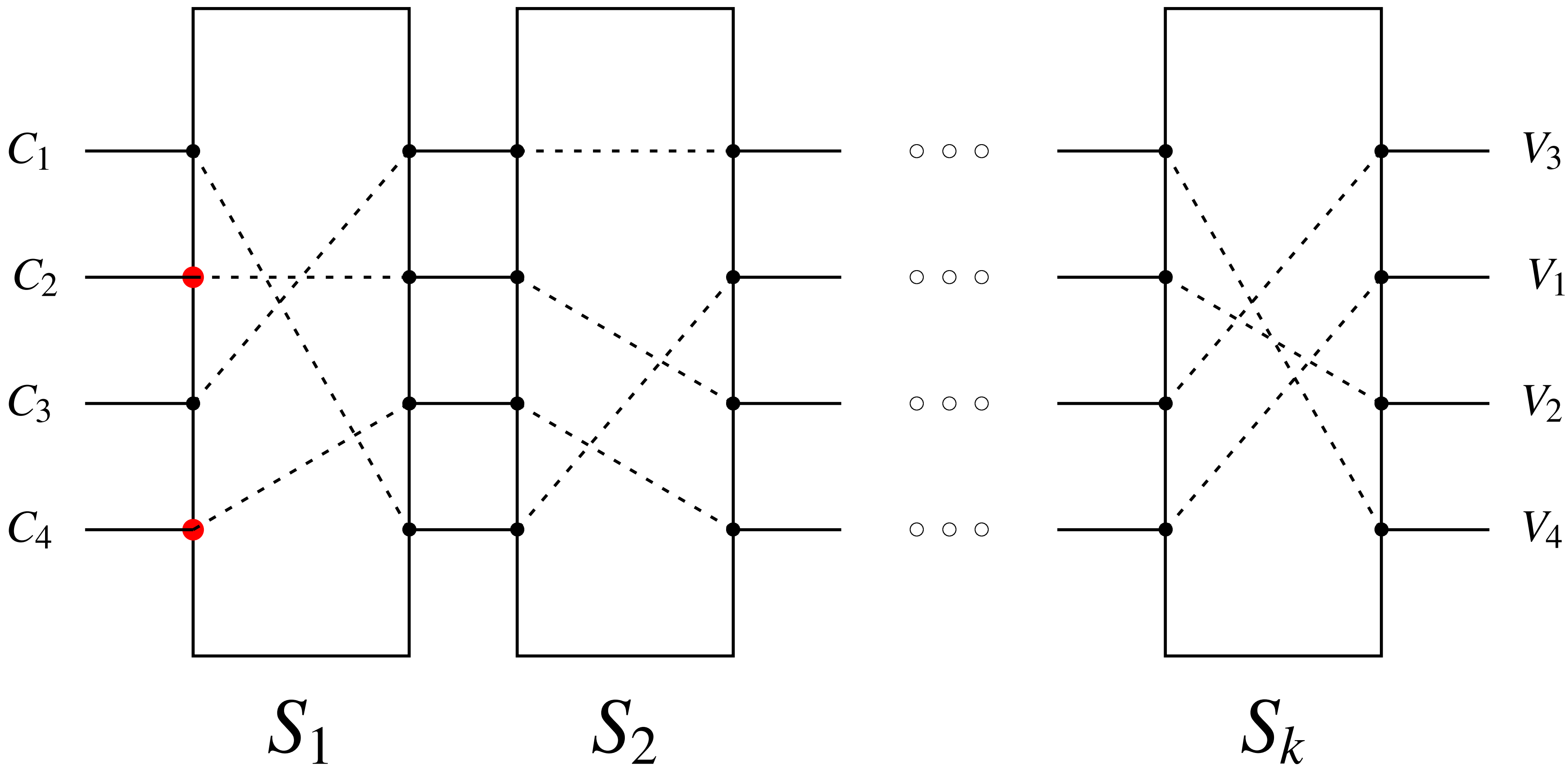
Full anonymity but no verifiability.

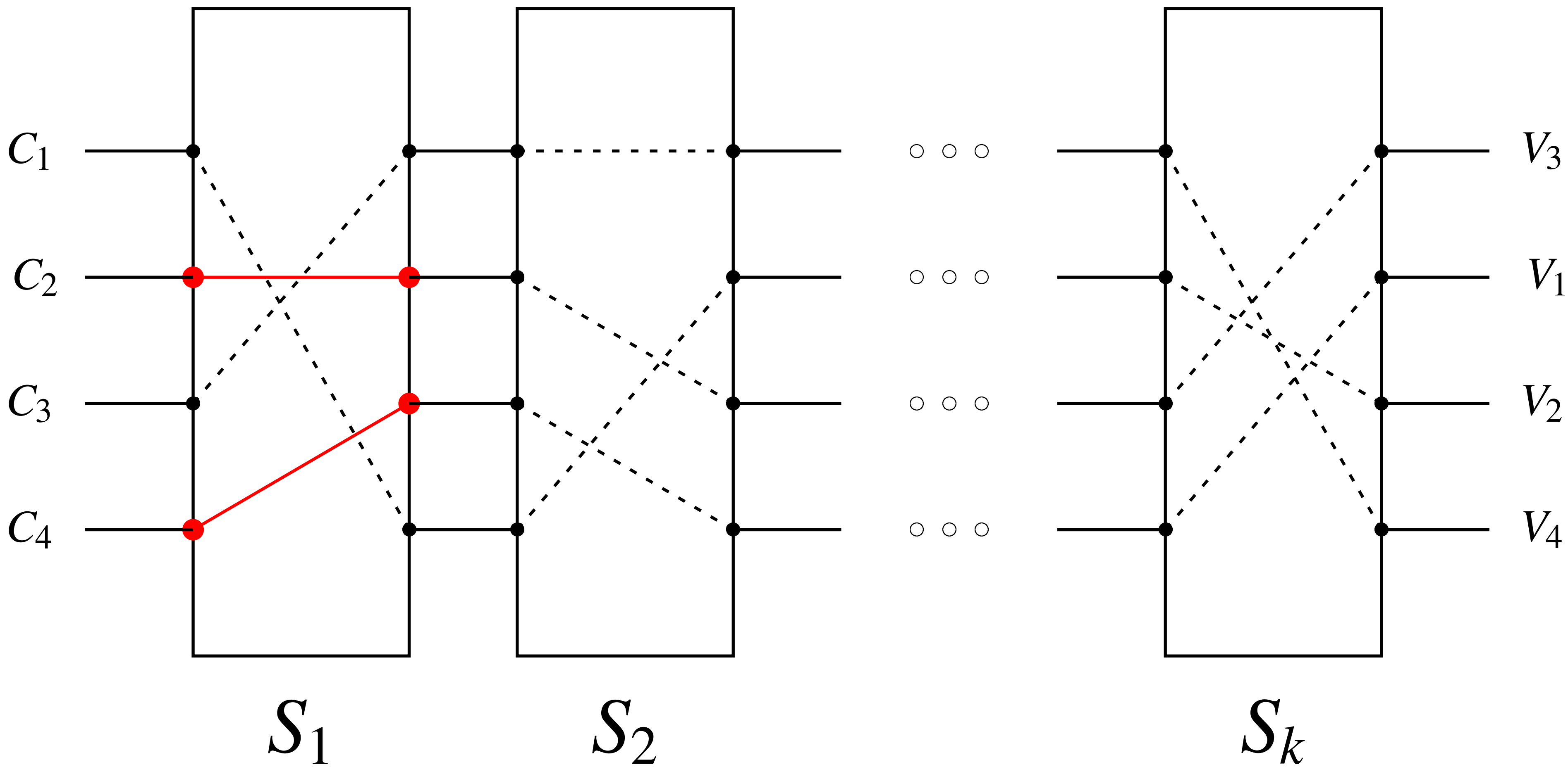

C_1
C_2
C_3
C_4
V_3
V_1
V_2
V_4
S_1
S_2
S_k

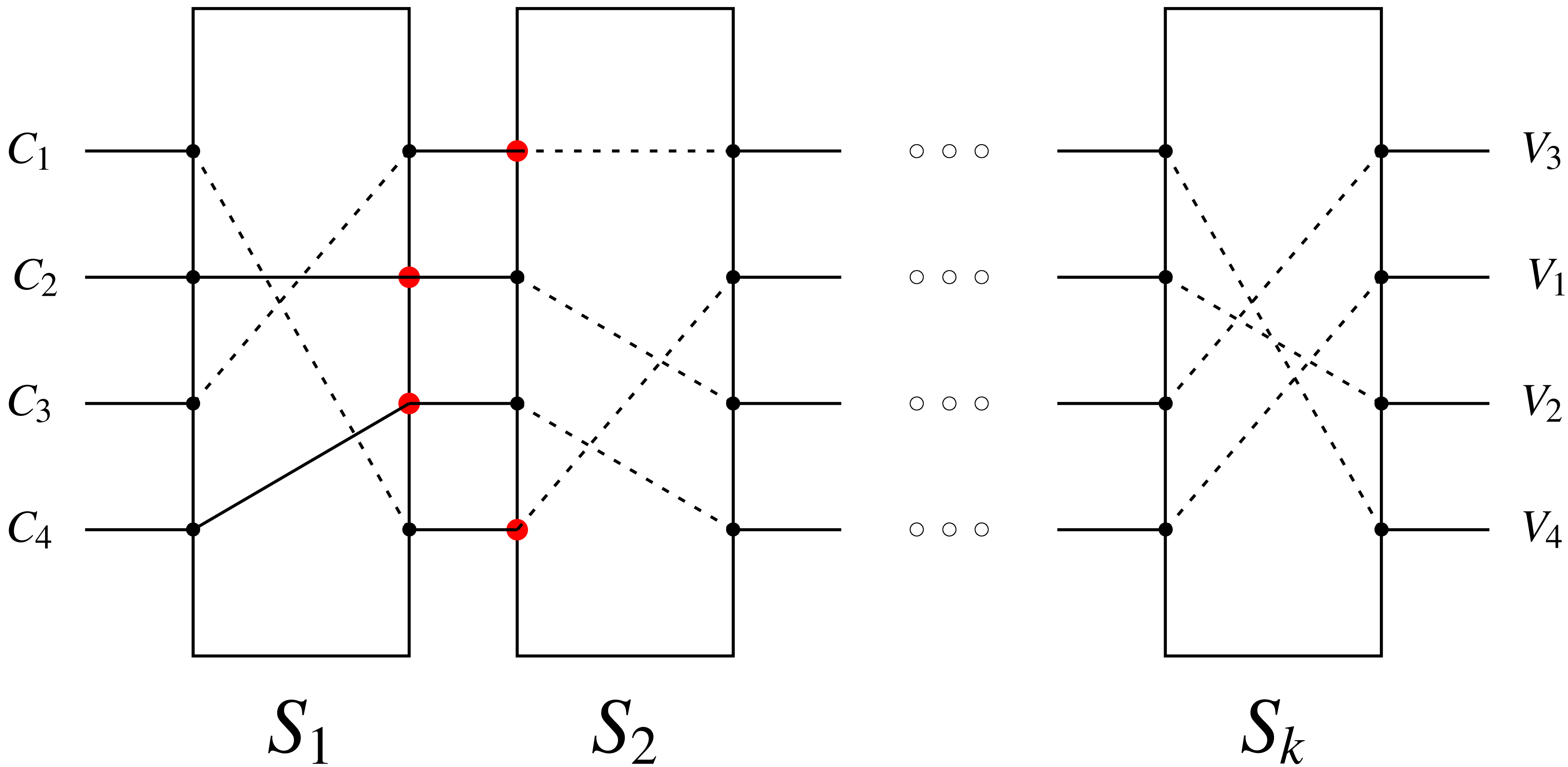
Randomized Partial Checking

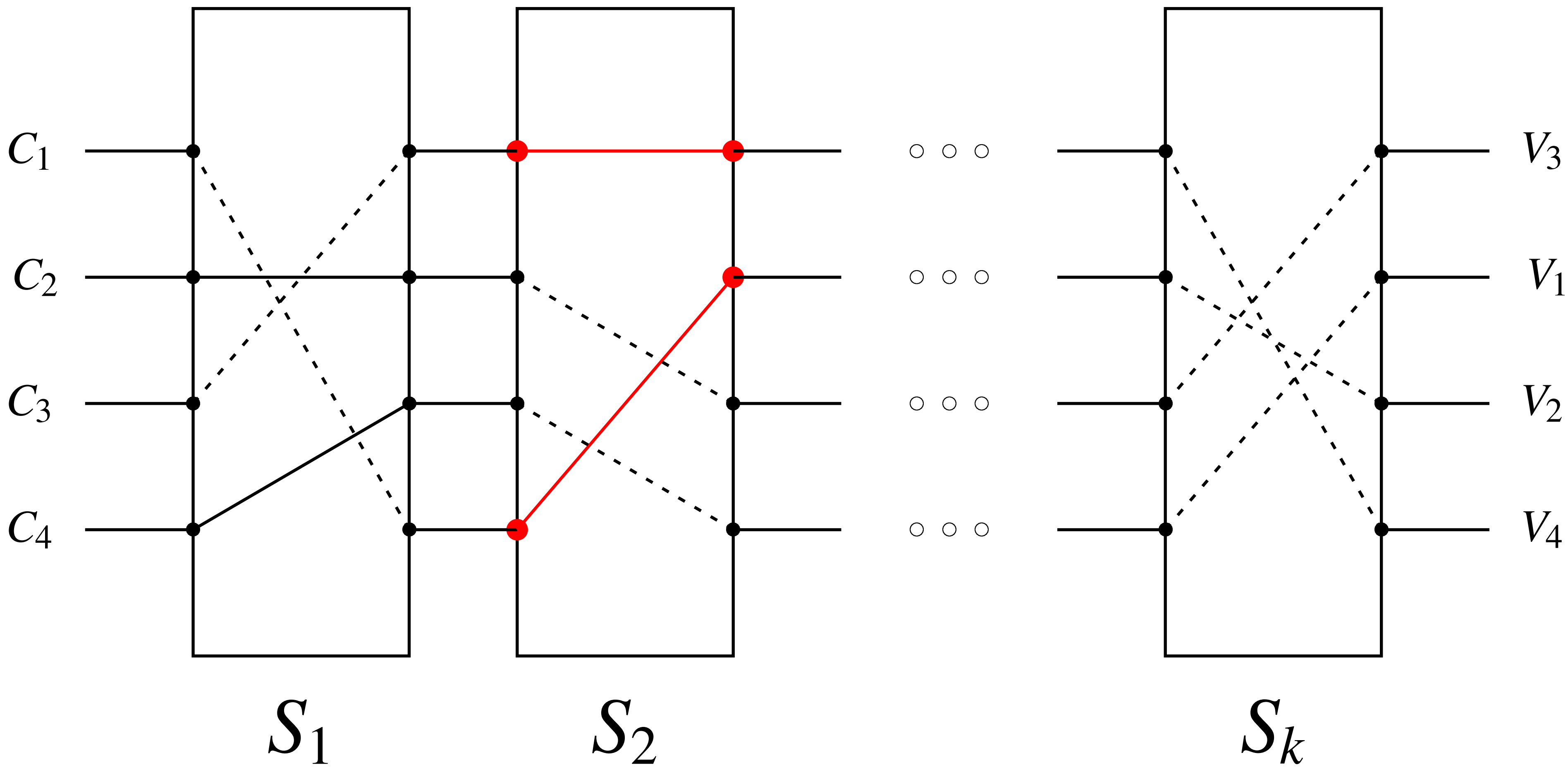
- M.Jakobsson, A.Juels, R.R.Rivest "Making Mix Nets Robust for Electronic Voting by Randomized Partial Checking" http://www.rsasecurity.com/rsalabs/staff/bios/mjakobsson/rpcmix/rpcmix.pdf

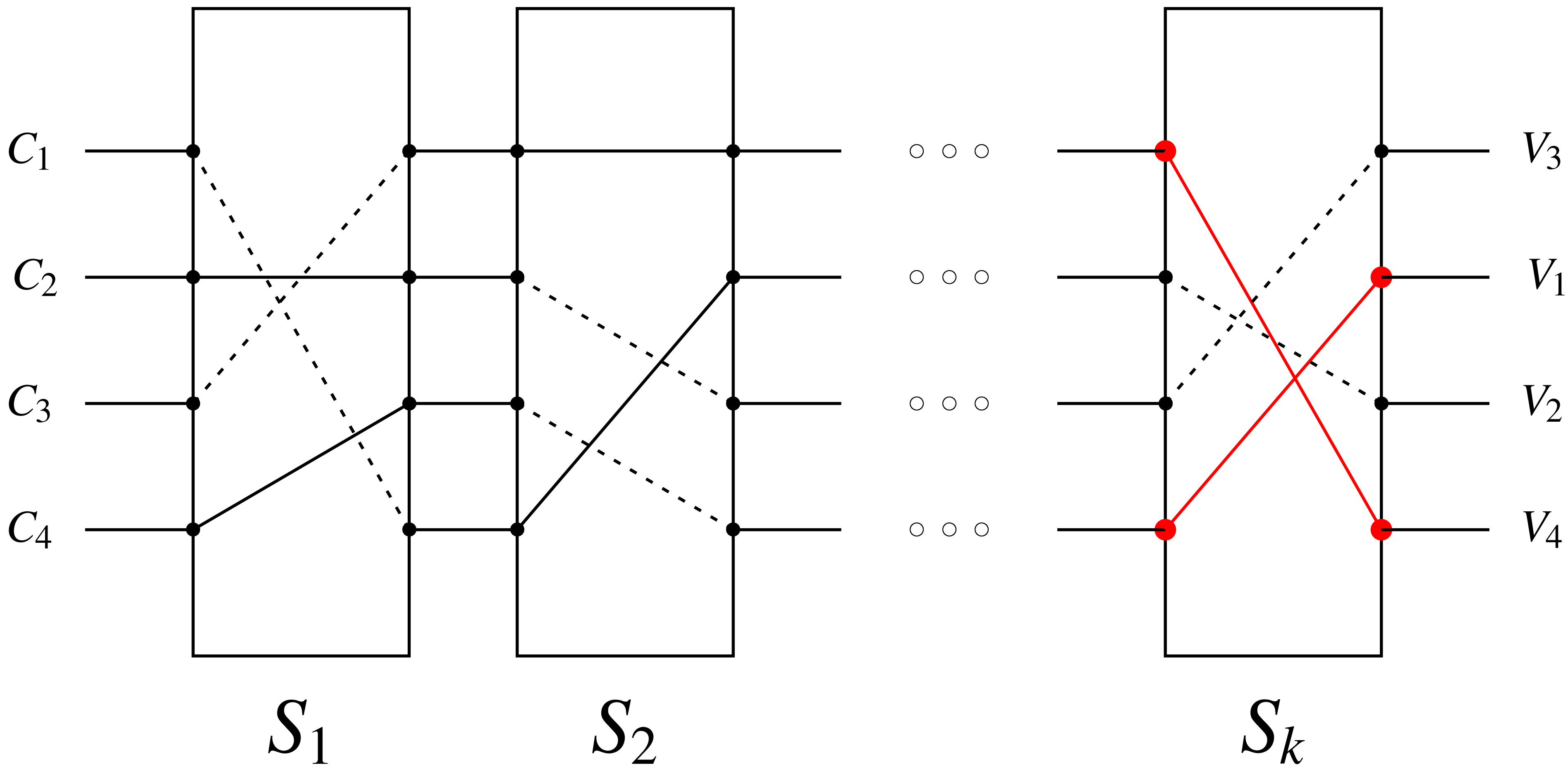

C1
C2
C3
C4
V3
V1
V2
V4
S1
S2
Sk

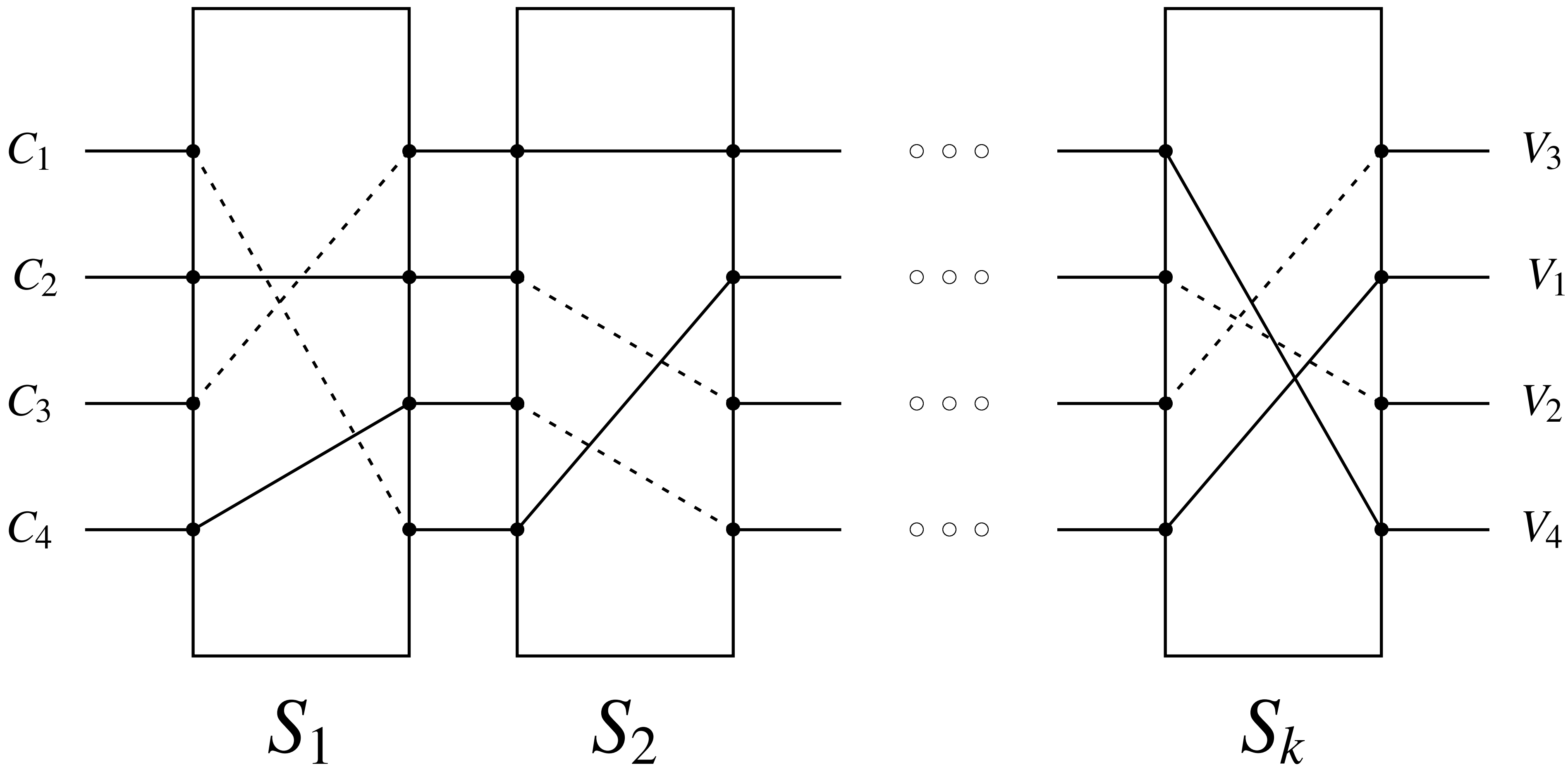

C1
C2
C3
C4
S1
S2
Sk
V3
V1
V2
V4


C_1
C_2
C_3
C_4
V_3
V_1
V_2
V_4
S_1
S_2
S_k


C_1
C_2
C_3
C_4
V_3
V_1
V_2
V_4
S_1
S_2
S_k


C_1
C_2
C_3
C_4
V_3
V_1
V_2
V_4
S_1
S_2
S_k


C1
C2
C3
C4
S1
S2
Sk
V3
V1
V2
V4


C1
C2
C3
C4
V3
V1
V2
V4
S1
S2
Sk

What is anonymity ?

- Voters are perfectly anonymous iff from the point of view of a passive adversary: **Each permutation between plaintexts at the end and ciphertexts at the beginning of MIX-cascade is equally probable.**
- Π_i - random variable that represents permutation of votes leaving the i–th MIX-server. For perfect anonymity we want Π_k to have the uniform distribution.

Total Variation Distance

For μ_1 and μ_2 over a finite space Ω *total variation distance* defines distance between μ_1 and μ_2.

$$\|\mu_1 - \mu_2\| = \frac{1}{2} \sum_{y \in \Omega} |\mu_1(y) - \mu_2(y)| \ .$$

Main Result

Let n be a number o voters, then

There exists $T = O(1)$ such that the variation distance between distribution of Π_T and the uniform distribution is $O\left(\frac{1}{n}\right)$.

Technicalities

- We treat $\{\Pi_i\}_{i \in \mathbb{N}}$ as a Markov chain.
- This process converges to uniform distributions.
- We need to estimate the rate of convergence.

Coupling

- $\mathcal{L}(\Pi_t)$ - probability distribution of Π_t
- μ -uniform distribution over $\mathbb{S}_n$
- *Coupling* is a stochastic process $(\Pi_t, \Pi_t^\star)$ on the space $\mathbb{S}_n \times \mathbb{S}_n$ such that $\mathcal{L}(\Pi_t^\star)$=$\mathcal{L}(\Pi_t)$
- Coupling Lemma (e.g. in D. Aldous "Random Walks of Finite Groups and Rapidly Mixing" 1983)

$$\|\mathcal{L}(\Pi_t) - \mu\| \leq \mathbf{Pr}[\Pi_t \neq \Pi_t^\star]$$

- We obtain estimation of converging rate by constructing proper coupling.

Path Coupling Method

- extension of well-known *Coupling*
- invented by Russ Bubley and Martin Dyer ("Path Coupling: A Technique for Proving Rapid Mixing in Markov Chains")
- Consist in building copies of stochastic process that differs slightly.
- We consider coupling only for a particular subset of $\mathbb{S}_n \times \mathbb{S}_n$
- Standard tools give $T = O(log(n))$ bound.

Grouping MIX-servers into pairs is important

If halves were chosen independently for all MIX-servers we would obtain $O(log(n))$ only.

Conclusions

- Using Chaum's Scheme we obtain **provable** anonymity
- We can use **constant** number of MIX-servers. Security does not depend on number of voters.
- We can divide mix-cascade into batches of two without loosing anonymity.