

Network Coding in P2P-Systems

Christian Ortolf

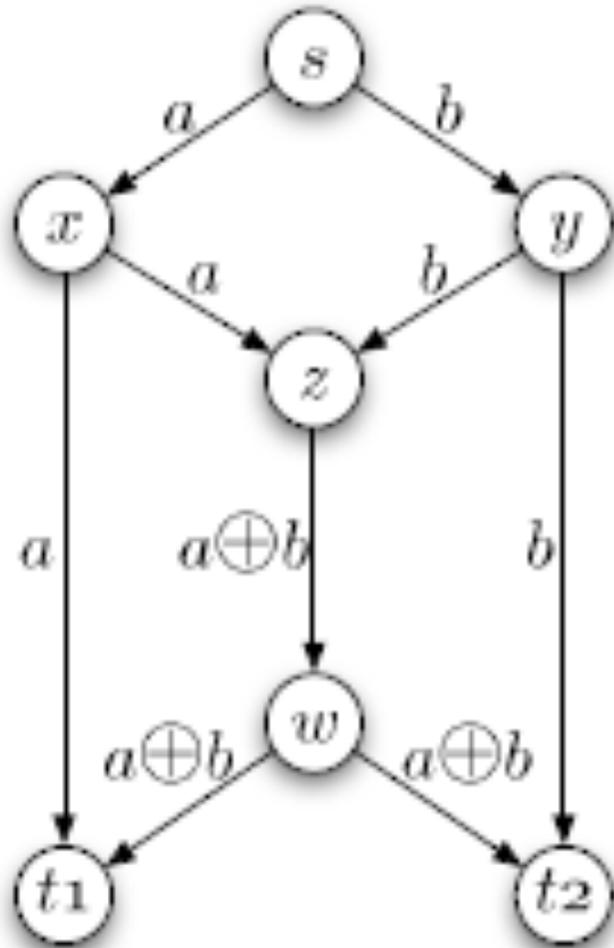
Overview

- Introduction
- Galois fields
- Encoding/Decoding of Files
- Gain
 - Coupon Collector's problem
- Problems
- Security
- Other fields where it can be used
- Research in Freiburg

Introduction - History

- 1999 first time used R.W.Yeung and Z. Zhang , "Distributed Source Coding for Satellite Communications"
- 2000 Definition of Network Coding, Max-Flow Min-Cut Theorem *in Ahlswede, R., Cai, N., Li, S.Y.R., Yeung, R.W.: Network information flow.*
- *2005 through Avalanche, Network Coding gets into the media, "Network Coding for Large Scale Content Distribution", C. Gkantsidis, P. Rodriguez*
- *Since 2000 more than 200 Papers dealing with Network Coding*

Introduction – Canonical Example



- Max-Flow – Min-Cut Theorem
- Max Flow can't be reached here without coding

Galois field – Évariste Galois



- * 25. Oktober 1811 in Bourg-la-Reine
- † 31. Mai 1832 in Paris

Galois field

- Field
- Notation

GF_{p^n} additional F_q

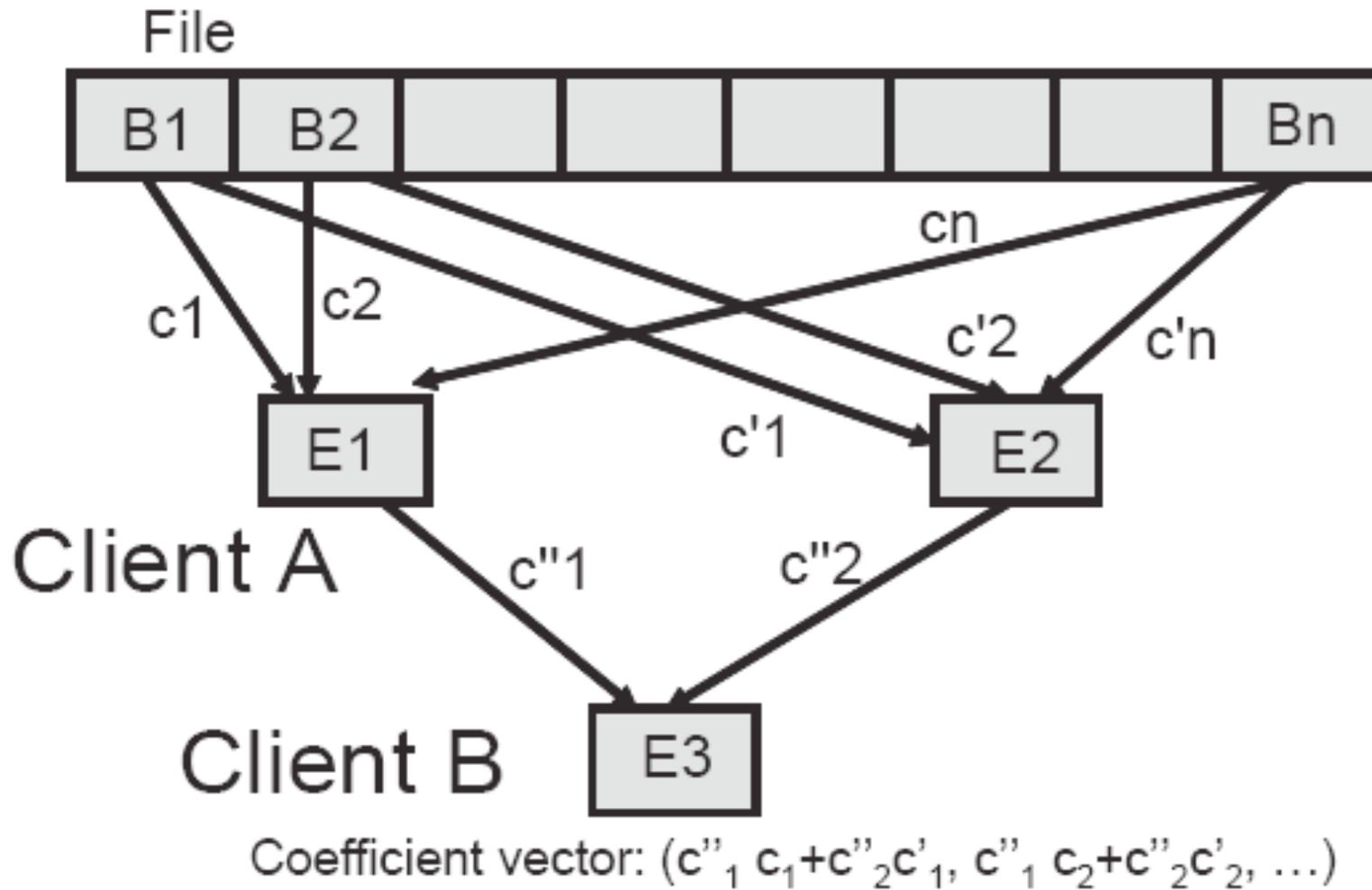
- Example: $M = \{0, 1\}$ with $+$ and $*$ defined as:

$+$		0	1		\cdot		0	1
---	+	---	---		---	+	---	---
0		0	1		0		0	0
1		1	0		1		0	1

- Construction: Irreducible Polynomials

Galois Field – Example

Encoding of files



- From "Network Coding for Large Scale Content Distribution", C. Gkantsidis, P. Rodriguez

Encoding - Example



Decoding of Files

- Check if Coefficient vector is Helpful

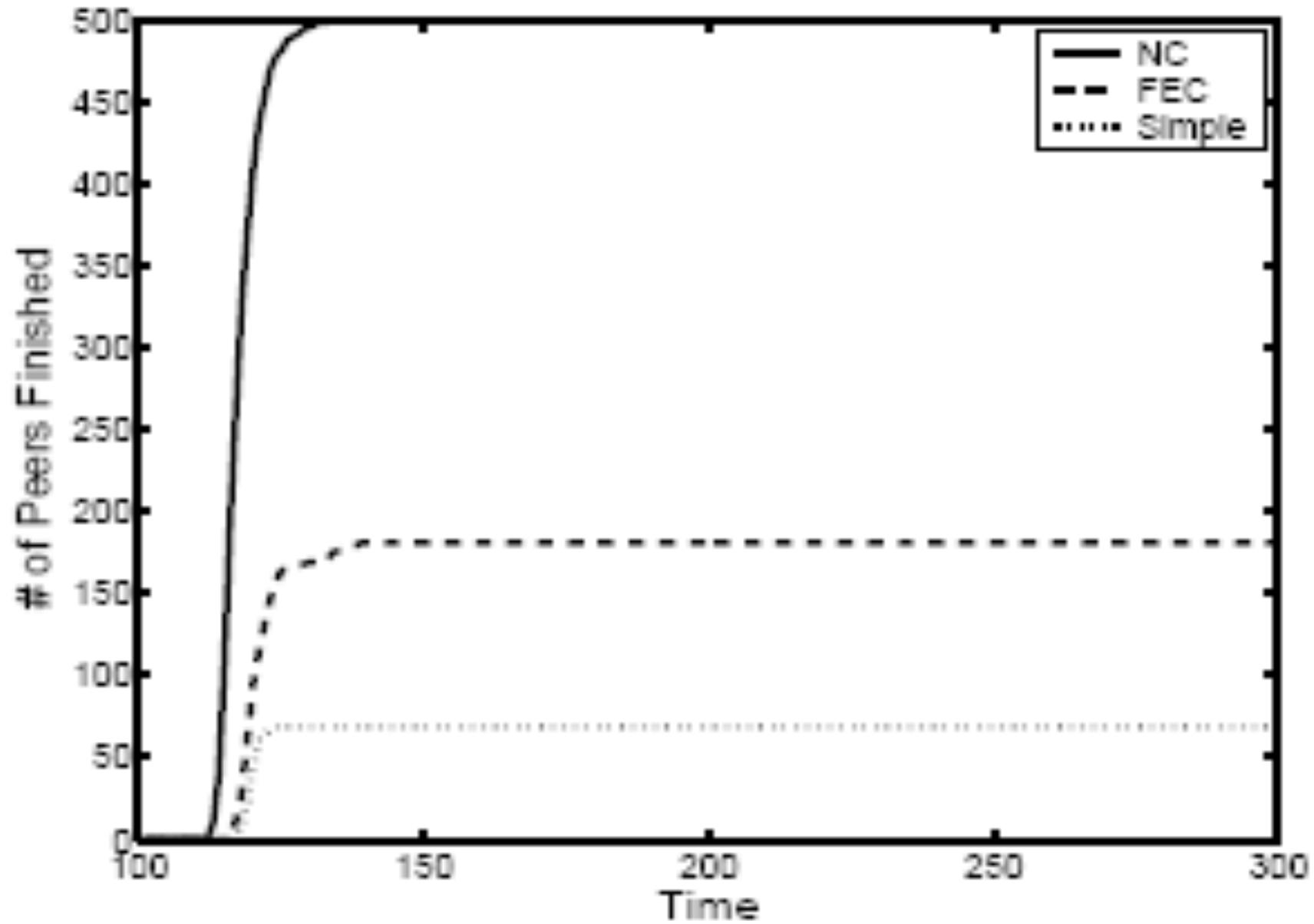
$$\begin{array}{cccccccccc} a_{11} & a_{12} & a_{13} & \text{---} & a_{1n} & z_{11} & z_{12} & 0 & \text{---} & 0 \\ 0 & a_{22} & a_{23} & \text{---} & a_{2n} & z_{21} & z_{22} & 0 & \text{---} & 0 \\ 0 & 0 & 0 & \text{---} & 0 & 0 & 0 & 1 & \text{---} & 0 \\ \text{---} & \text{---} & \text{---} & \text{---} & 0 & 0 & 0 & 0 & \text{---} & 0 \\ 0 & 0 & 0 & \text{---} & 0 & 0 & 0 & 0 & \text{---} & 1 \end{array}$$

- Download up to N Blocks
- Invert Matrix and Decode

Gain – Solves Coupon Collector's Problem

- Easier Protocol
 - Less Knowledge Exposed
 - Better Incentive mechanisms possible
- High Chance to finish File if source leaves

Gain

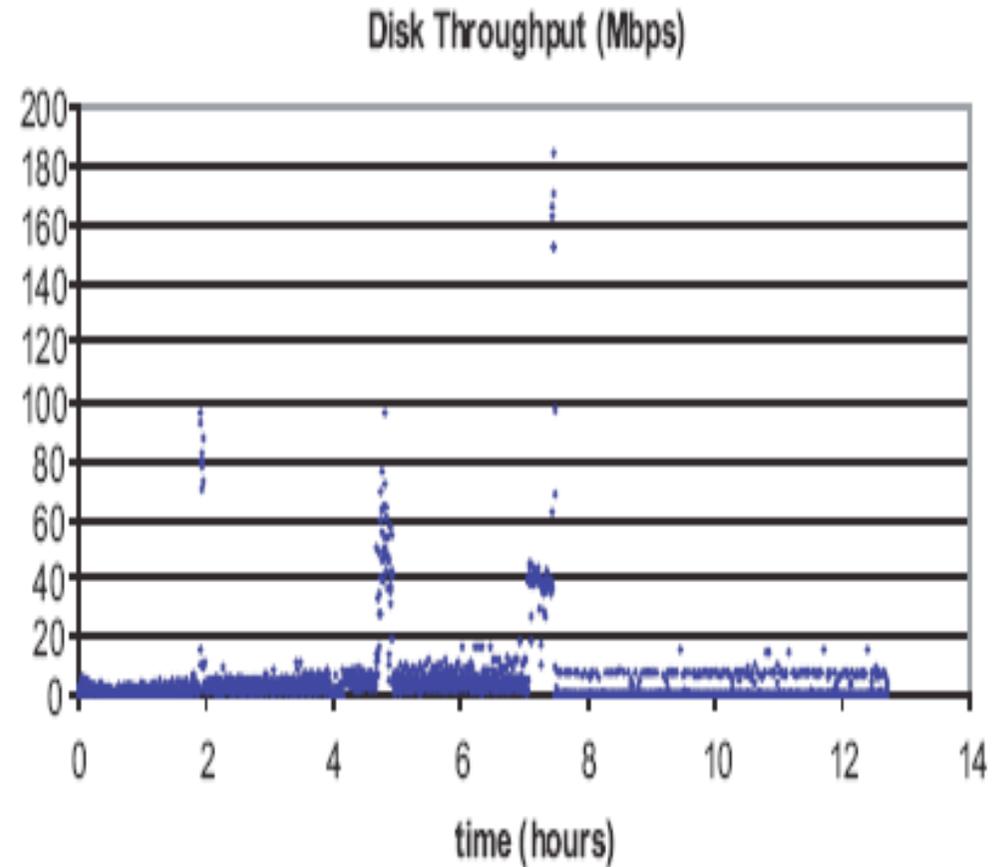
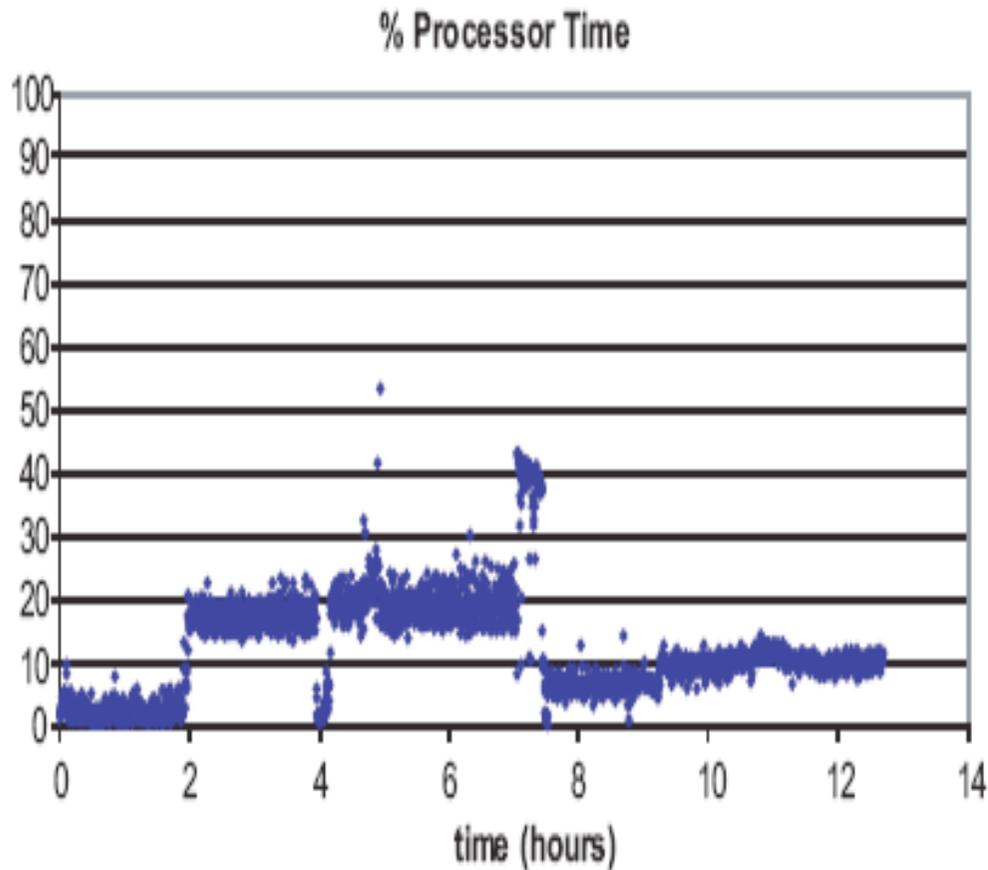


From "Modeling and Simulation of Peer-to-Peer Distributed Content Distribution" by G. Goumard, P. B. Debat

Problems

- Small Blocks make large Coefficient Vectors
 - 512KB blocks on 4GB file with $GF(2^8)$ makes 64MB
- CPU usage
 - Encoding of aBlock $O(n)$
 - Decoding $O(n^2)$
 - Inverting $O(n^3)$

Problems - CPU



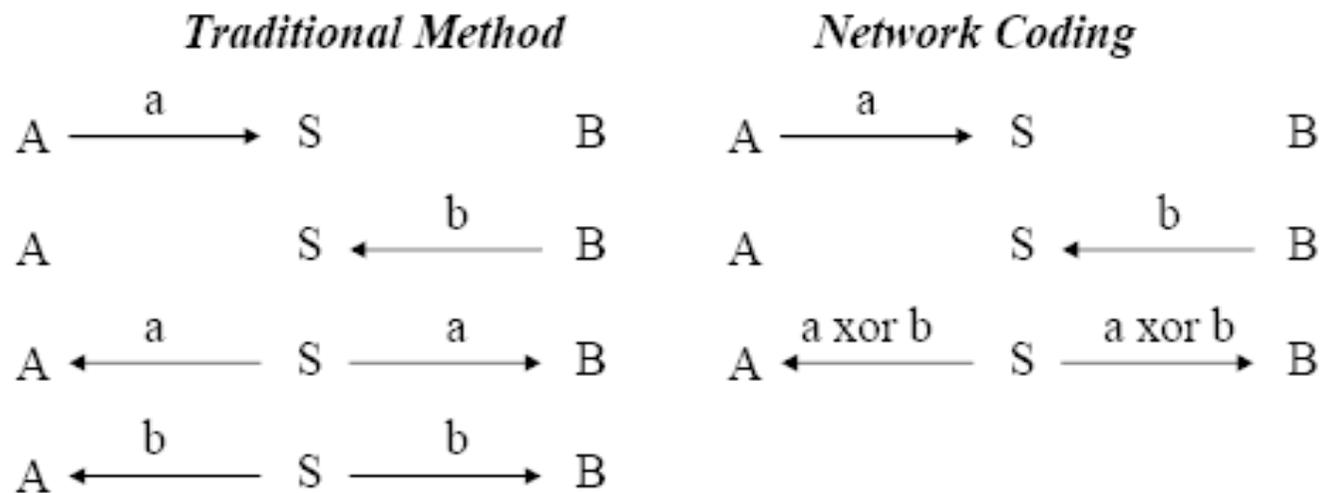
- *From Anatomy of a P2P Content Distribution system Gkantsidis et al*
- Average: 1.4Mbit down 300Kbit/s up

Security

- Usual Hashfunctions don't work
 - Homomorphic Hashfunctions as solution
 - Very slow
 - Cooperative hashing
 - Complex
 - Needs SRCs to protect against DoS
 - Bulk Hashing
 - Secure Randomn Checksums (SRCs)
- Harder to get info from a tapped wire
- Data injection even without Hashing nearly impossible

Other Fields where it can be used

- In Multicast Networks (example from NC Primer)



- Reduce Cost in WSN / Storage redundancy
- Network Tomography
- P2P - SAN

Research in Freiburg - TooFree

The screenshot shows the TooFree application window. The title bar reads "TooFree". The menu bar contains "File" and "Help". Below the menu bar are three buttons: "Create Token", "Publish File", and "Download". The main window displays a file named "Aktiv-Tutorialdivc.avi" with the following details:

- File: x.avi
- Filesize: 30,40 MB
- Blocksize: 256 KB
- #Blocks: 122
- RootHash: 4Y5BLU4SR8SLUH7NF0HFEBD3NDNH5M9Q25VED6CYQ

The "Current State" section shows:

- DecodedBlocks: 0
- Downloaded Blocks: 78
- Uploaded Blocks: 0
- RunningTransfers: 1
- CCs: 44

A progress bar is visible below the current state, and a "pause" button is located at the bottom left of the main area.

The central part of the interface is a grid of 122 colored blocks, each containing a number. The blocks are arranged in a roughly rectangular shape, with some missing in the bottom-left corner. The numbers range from 0 to 100, with some numbers appearing multiple times (e.g., 71, 10, 27, 34, 47, 53, 54, 69, 75, 80, 83, 91, 100). The colors of the blocks vary, including blue, green, red, purple, yellow, and grey.

At the bottom of the window, there is a table with the following columns: ID, Status, Block, and Ratio.

ID	Status	Block	Ratio
192.168.0.17	Downloaded 40,95 KB(16%)	(97,115)am-19bm124	-78

Finding solutions for the too large CPI cost

Thank you for
your Attention

Questions?