Ο Σοβιετικός Κρυπταλγόριθμος GOST

Στην παρούσα εργασία παρουσιάζεται η υλοποίηση του Σοβιετικού κρυπταλγορίθμου GOST για την πλατφόρμα επεξεργαστή-συνεπεξεργαστή(αναδιατασσόμενης λογικής) Stretch.

"Ενσωματωμένα Συστήματα Μικροεπεξεργαστών" , χειμερινό εξάμηνο 2006.

Πολυτεχνείο Κρήτης,
19 Δεκεμβρίου 2006

Ι.Αγαδάκος
Κ.Θεοχαρούλης
Ν. Παπουλιας

Περι τίνος πρόκειται ?

ГОСУДАРСТВЕННЫЙ СТАНДАРТ СОЮЗА ССР

ДУГОВАЯ СВАРКА В ЗАЩИТНОМ ГАЗЕ

СОЕДИНЕНИЯ СВАРНЫЕ

ОСНОВНЫЕ ТИПЫ, КОНСТРУКТИВНЫЕ ЭЛЕМЕНТЫ И РАЗМЕРЫ

ГОСТ 14771—76

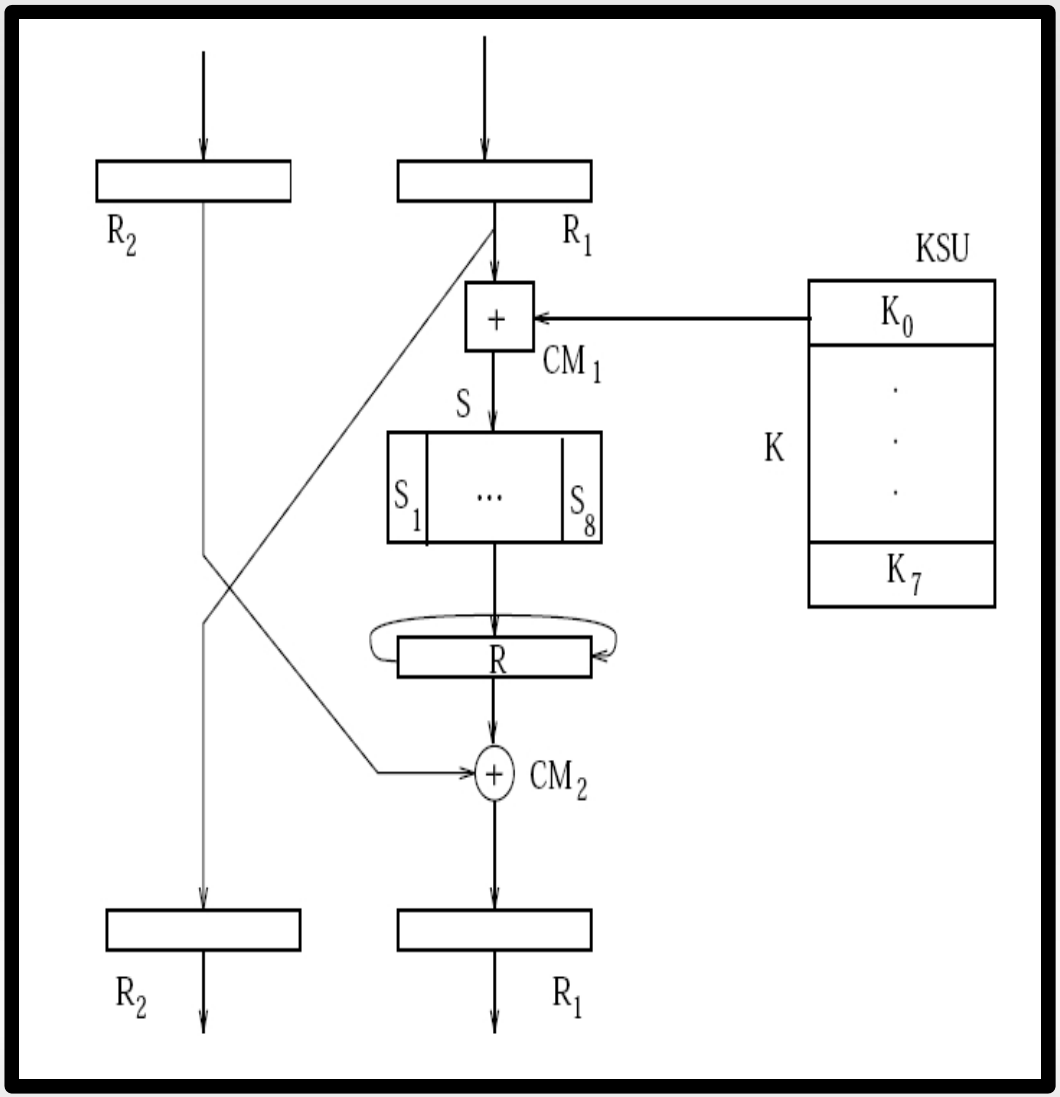
Издание официальное

Ο κρυπταλγόριθμος GOST, αναπτύχθηκε στην Σοβιετική Ένωση κατα την δεκαετία του 1970 και χρησιμοποιήθηκε σαν εναλλακτική λύση κρυπτογράφησης, έναντι του δημοφιλούς προτύπου των Η.Π.Α D.E.S.

Χαρακτηριστικά του GOST

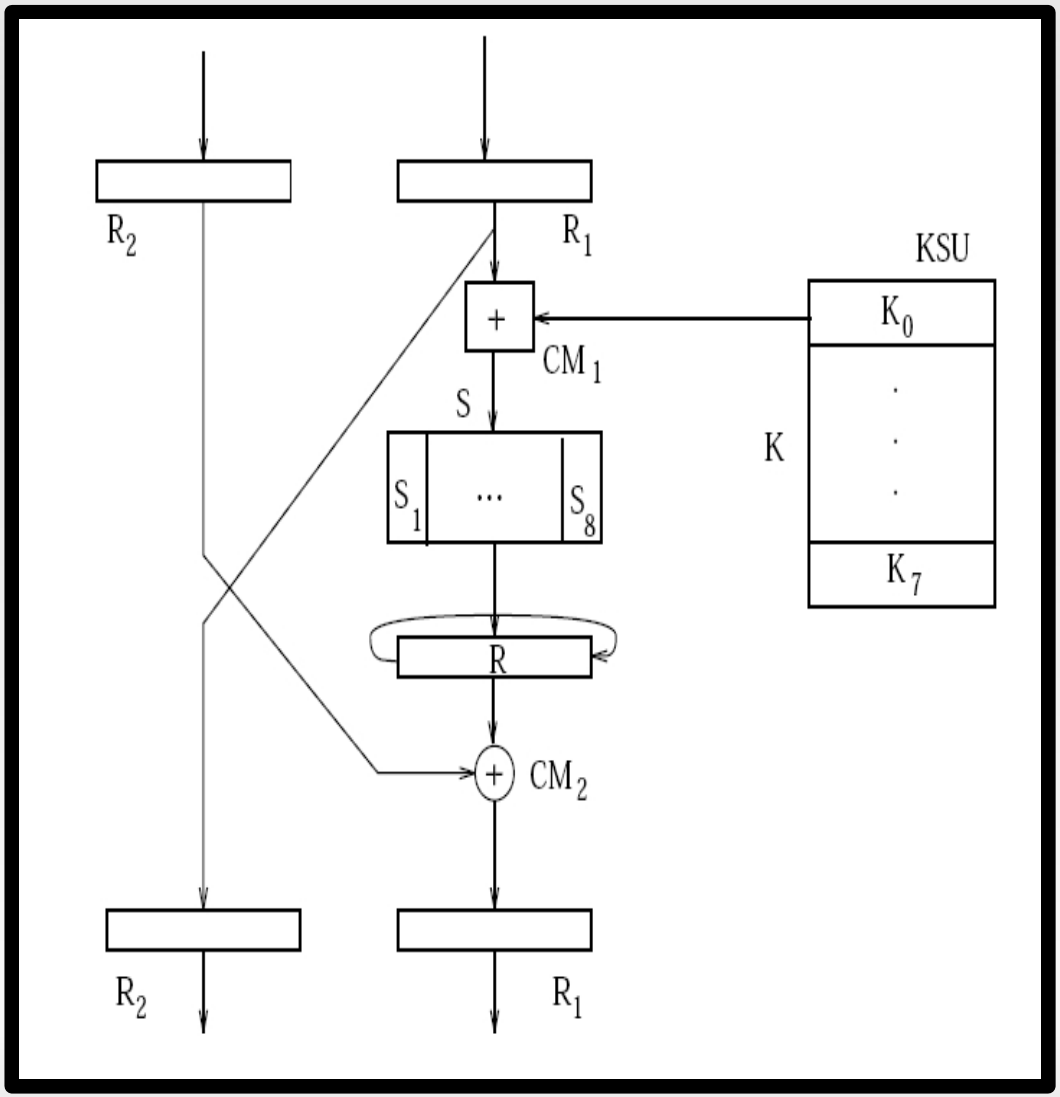
- κρυπταλγόριθμος τμήματος 64bit
- αρχιτεκτονικής δικτύου Feistel 32 γύρων
- μέγεθος κλειδιού 256bit
- “προαιρετικά κρυφό” κομμάτι Δικτύου Αντικατάστασης (S-boxes)

Δομή του κρυπταλγορίθμου



- Χωρισμός της εισόδου σε 2 τμήματα των 32bits
- Πρόσθεση mod 2^32 του δεξιού τμήματος με 32bit ποσότητα του κλειδιού σύμφωνα με το key-schedule
- 4bit αντικατασταση 8 κουτιών (S-boxes) του αποτελέσματος

Δομή του κρυπταλγορίθμου(συνέχεια)



- Αριστερή Κυκλική Ολίσθηση κατά 11bits
- Exclusive-OR του αποτελέσματος με το αριστερό τμήμα της εισόδου
- Εναλλαγή τμημάτων εισόδου

Gost vs D.E.S

- Ο Gost έχει μέγεθος κλειδιού 256bit, έναντι μόλις 56bit του D.E.S.
- Εάν προσθεθεί η δυνατότητα “κρυφού” κομματιού αντικαταστάσεων, έχουμε συνολικά 610bit κρυφής πληροφορίας.
- Ο Gost έχει 32 γύρους κρυπτογράφησης, έναντι μόλις 16 γύρων στον D.E.S
- Ο Gost επιτυγχάνει την ικανοποίηση ισχυρών κριτηρίων κρυπτογράφης (strict avalanche effect) με συγκριτικά πολύ απλούστερη υλοποίηση τόσο σε λογισμικό όσο και σε hardware
- *Πηγή: Applied Cryptography, 2nd Edition*

Υλοποίηση σε P.C - Verification

- Υλοποίηση σε περιβάλλον Windows - GCC.
- Συγγραφή ξεχωριστού λογισμικού αυτόματης επαλήθευσης
- Μέγεθος εισόδου 700MB (εξωτερικό αρχείο)
- Διαδικασία κρυπτογράφης – αποκρυπτογράφης και επαλήθευσης αρχικού κειμένου με αποκρυπτογραφημένο κείμενο
- Μέσος χρόνος κρυπτογράφης (εισόδου 700MB) , περίπου 6λεπτά

Υλοποίηση σε Stretch IDE - Verification

- Ταυτόσημη υλοποίηση με αυτήν σε PC (Windows-GCC) με προσεκτική χρήση της Standard C Library
- Χρήση ξεχωριστού λογισμικού αυτόματης επαλήθευσης
- Μέγεθος εισόδου 4Kb (verification) , 278bytes profiling (εξωτερικό αρχείο)
- Διαδικασία κρυπτογράφης – αποκρυπτογράφης και επαλήθευσης αρχικού κειμένου με αποκρυπτογραφημένο κείμενο
- **Total Cycles: 604126 or 0,002 sec**
- **Dcache Misses: 2491**

Profiling - Αποδόμηση

(Gprof Profile) ☐ Show All

%	Cumulative Cycles	Self Cycles	Calls	Self Cycles/call	Total Cycles/call	Name	Graph
79.27	479563.00	479563.00	1120	428.18	428.18	s_box	
13.20	559435.00	79872.00	35	2282.06	15983.86	gost_block_encrypt	
3.40	579982.00	20547.00	??	??	??	ResetH	

- 79,27% του χρόνου εκτέλεσης στην συνάρτηση που υλοποιεί τα S-Boxes
- 13,20% στην συνάρτηση που υλοποιεί τους 32 γύρους κρυπτογράφησης
- Λοιπός χρόνος εκτέλεσης σε εσωτερικές συναρτήσεις της πλατφόρμας

Profiling – Αποδόμηση (συνέχεια)

- Συνολικά 92,47% του χρόνου εκτέλεσης στην συνάρτηση κρυπτογράφησης των 32 επαναλήψεων
- Επιλογή του κύριου κύκλου κρυπτογράφησης για την υλοποίηση στο αναδιατασσόμενο κομμάτι (ανα block 64bit χωρίς παραλληλισμό)
- Βρόγχος προς βελτιστοποίηση: 15946 κύκλοι
- Αποτελέσματα:
- Total Cycles: 123321 or 0,0004 , Opt: 79,58%
- Loop Cycles: 2433 , Opt: 86,09%
- Dcache Misses: 2217
- Successfull Data verification

Optimization - Παραλληλισμός

- Παράλληλη κρυπτογράφη 4 block των 64bit (έναντι ενός) στο αναδιατασσόμενο κομμάτι
- Αποτελέσματα:
- Total Cycles: 74108 , Opt: 87,73%
- Loop Cycles: 3084 , Opt: 80,65%
- Dcache Misses: 2439
- Successfull Data verification

Optimization – Man Loop Unrolling

- Βέλτιστο Unrolling για 8 κλήσεις της αναδιατασσόμενης συνάρτησης ανά επανάληψη
- Αποτελέσματα:
- Total Cycles: 72430 , Opt: 88,01%
- Loop Cycles: 2834 , Opt: 82,22%
- Dcache Misses: 2468
- Successfull Data verification

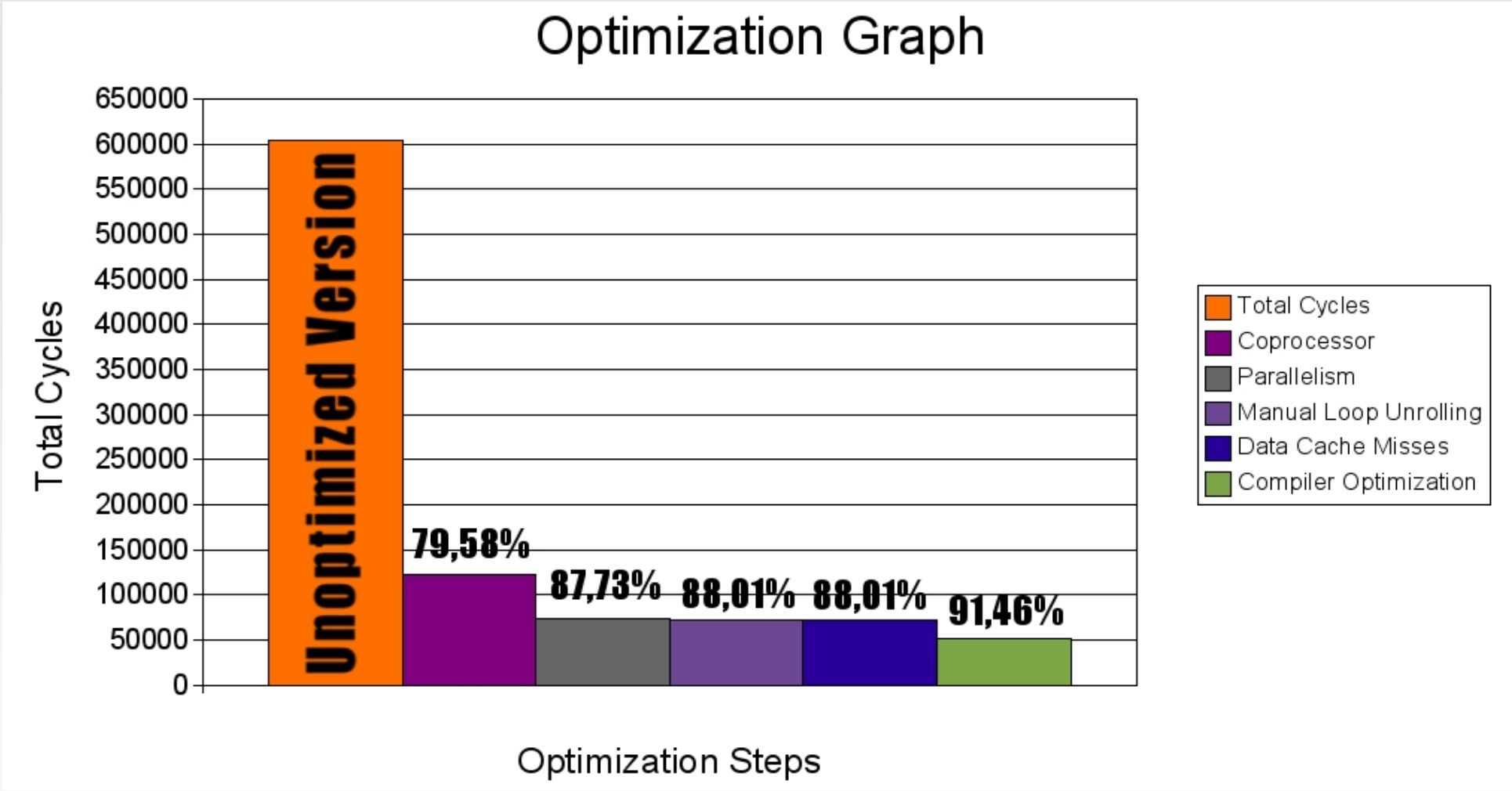
Optimization – Dcache Misses

- Τοποθέτηση όλων των global δεδομένων (key,key_schedule,sboxes) στην dcache του ίδιου του επεξεργαστή
- Αποτελέσματα:
- Total Cycles: 72391 , Opt: 88,01%
- Loop Cycles: 2834 , Opt: 84,76%
- Dcache Misses: 2430
- Successfull Data verification

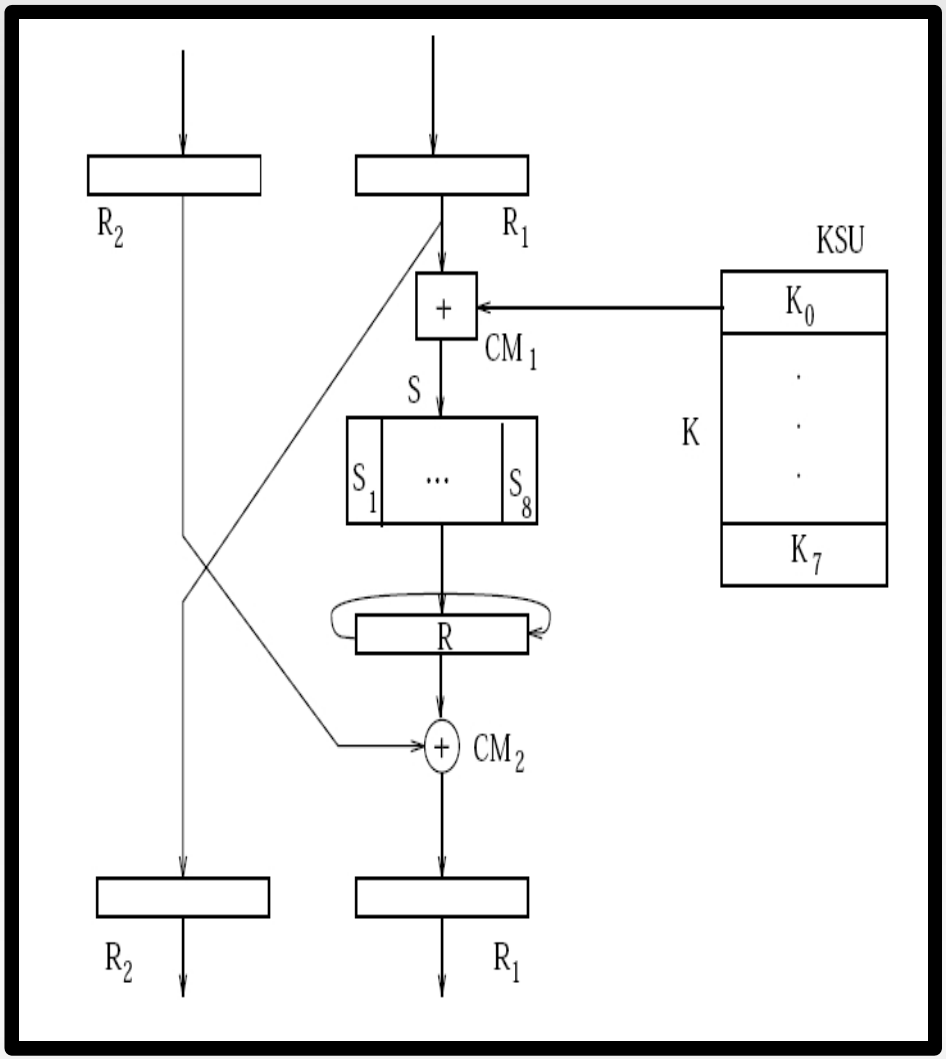
Final results :Optimization through compilation

- Αποτελέσματα:
- Total Cycles: 51540 or 0,0001sec
- Opt: 91,46%
- Loop Cycles: 880 , Opt: 94,48%
- Dcache Misses: 2355
- Successfull Data verification

Optimization Graph



Future Work



- Επανεξέταση των τεχνικών του key management
- Μετατροπή των Sboxes από 4bit σε 8bit για την ελαχιστοποίηση των προσβάσεων μνήμης
- Επαναξέταση των θέσεων ολίσθησης για την μείωση των συνολικών bit που ολισθαίνουν
- Σύγκριση througput Mb/s μεταξύ PC και Stretch
- Σύγκριση απόδοσης με άλλες υλοποιήσεις του αλγορίθμου
- Μεταφορά της υλοποίησης στο Stretch Board