sharemind & secrec

a secure algorithm development platform

http://research.cyber.ee/sharemind/

Dan Bogdanov

researcher
dan@cyber.ee

CYBERNETICA

stacc

UNIVERSITY OF TARTU
1632

Separation of public and private

PLAGE PUBLIQUE
DU RUHL
BAIGNADE NON SURVEILLEE
RATIQUEE AUX RISQUES ET PERILS DES INTERESSES
UPERVISED BATHE
BALNEAZIONE NON SORVEGLIATA
DRAPEAUX
BEAU RIVAGE
CENTENAIRE
PONCHETTES
FORUM
LIDO
MAGNAN
POINCARE
BAMBIN
STE HELENE
CARRAS
BAIE DES ANGES
LEGENDE
Autorisation
Véhicules nautiques à moteur et engins motorisés
Scooter des mers et Jet ski
Véhicules nautiques sans moteur
LISTE DES PLAGES PUBLIQUES

Separation of public and private

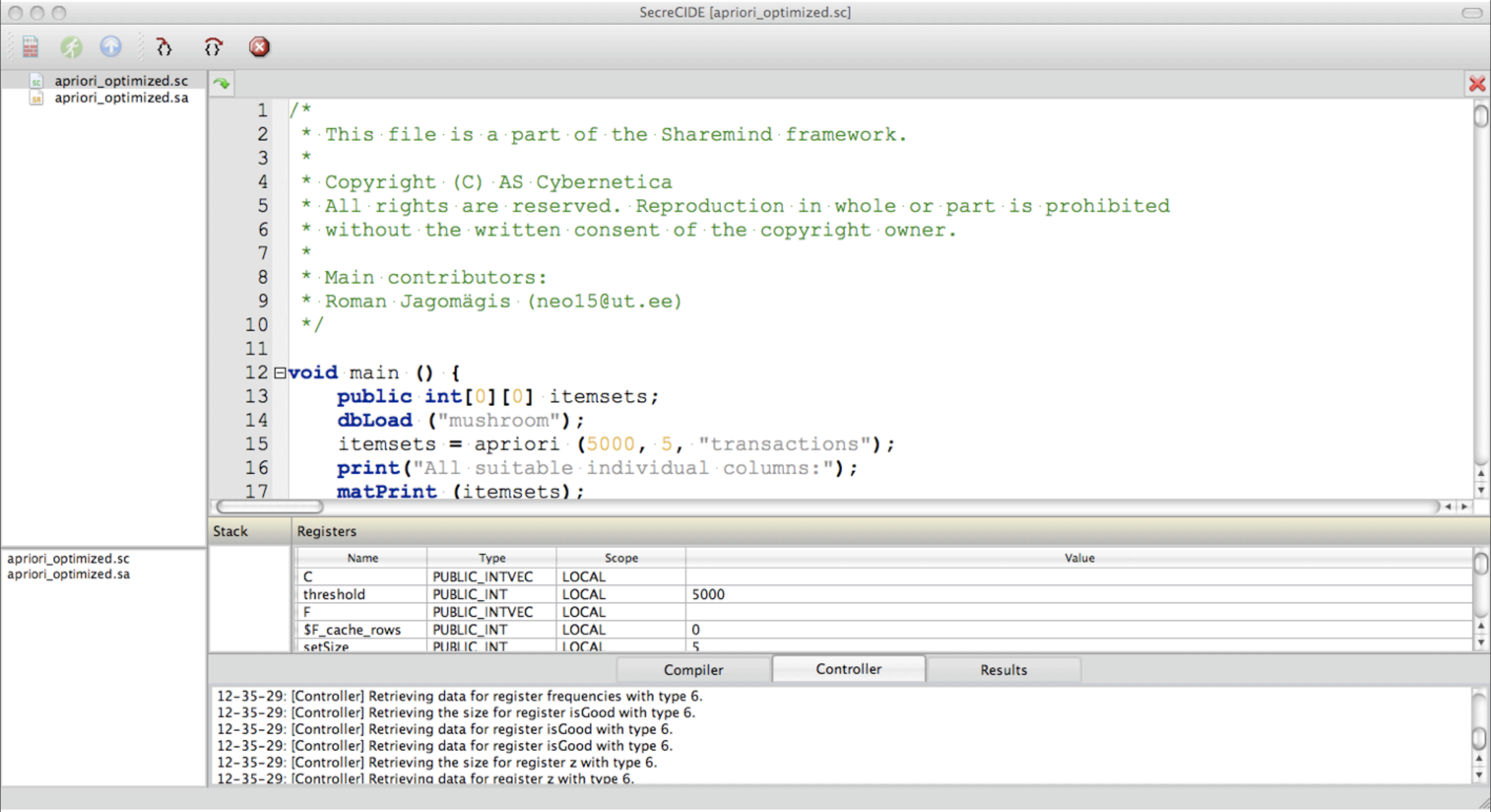
Algorithm language that separates private and public data.

```
public bool whoIsRicher
    (private int alice, private int bob)
{
    private bool winner;
    winner = (alice > bob);
    return declassify (winner);
}
```

A whole development environment

- **sharemind** is a virtual machine based on MPC
- **sharemind** performs private computations
- **sharemind** can also securely store data
- **secrec** is compiled to **sharemind** assembly
- the assembly code is executed by **sharemind**
- we have built an IDE to help developers

A whole development environment



```
/*
 * This file is a part of the Sharemind framework.
 *
 * Copyright (C) AS Cybernetica
 * All rights are reserved. Reproduction in whole or part is prohibited
 * without the written consent of the copyright owner.
 *
 * Main contributors:
 * Roman Jagomägis (neo15@ut.ee)
 */

void main () {
    public int[0][0] itemsets;
    dbLoad ("mushroom");
    itemsets = apriori (5000, 5, "transactions");
    print("All suitable individual columns:");
    matPrint (itemsets);
```

Name	Type	Scope	Value
C	PUBLIC_INTVEC	LOCAL	
threshold	PUBLIC_INT	LOCAL	5000
F	PUBLIC_INTVEC	LOCAL	
$F_cache_rows	PUBLIC_INT	LOCAL	0
setSize	PUBLIC_INT	LOCAL	5

```
12-35-29: [Controller] Retrieving data for register frequencies with type 6.
12-35-29: [Controller] Retrieving the size for register isGood with type 6.
12-35-29: [Controller] Retrieving data for register isGood with type 6.
12-35-29: [Controller] Retrieving data for register isGood with type 6.
12-35-29: [Controller] Retrieving the size for register z with type 6.
12-35-29: [Controller] Retrieving data for register z with type 6.
```

We are looking for collaborations

- We are interested in:
  - using **secrec** to implement private algorithms
  - porting **secrec** to new secure machines
  - developing the **sharemind** virtual machine
- Please contact us by e-mail or in person

Thank you!

sharemind

http://research.cyber.ee/sharemind/

Dan Bogdanov

dan@cyber.ee