

---

# TEST OF TIME AWARD



---

Kleene Award:

The Identity Problem in the special affine group of  $\mathbb{Z}^2$   
Ruiwen Dong

---

*For solving the identity problem for  $SA(2, \mathbb{Z})$ .*

*The paper makes significant progress on a well-known open problem,  $SL(3, \mathbb{Z})$ , using an impressive catalog of methods from linear algebra, geometry, and group theory.*

---

---

# Test-of-Time Award

18th Annual IEEE Symposium on Logic in Computer Science  
Ottawa, Canada, 2003



Nathalie Bertrand, Phokion G. Kolaitis (chair), John Mitchell

---

---

# Tractable conservative Constraint Satisfaction Problems,

## Andrei A. Bulatov

---

*Constraint satisfaction problems constitute a large family of ubiquitous algorithmic problems that contain Boolean satisfiability and graph colorability as special cases. In 1993, Tomas Feder and Moshe Vardi conjectured that for every relational structure  $B$ , the associated constraint satisfaction problem  $CSP(B)$  is either NP-complete or solvable in polynomial time.*

*The Feder-Vardi conjecture became the catalyst for numerous subsequent investigations aiming to classify the complexity of constraint satisfaction problems. Andrei Bulatov's paper confirmed the Feder-Vardi conjecture for the case of conservative constraint satisfaction problems, which are the  $CSP(B)$  problems in which the relations in  $B$  include all subsets of the universe of  $B$ .*

*This paper remained the strongest positive partial result towards the Feder-Vardi conjecture until the conjecture was finally proved independently by Andrei Bulatov and Dmitriy Zhuk in 2017 using methods and techniques from universal algebra.*

---

---

An NP Decision Procedure for Protocol Insecurity with XOR  
Yannick Chevalier, Ralf Küsters, Michaël Rusinowitch, and Mathieu Turuani

---

Intruder Deductions, Constraint Solving and Insecurity Decision in  
Presence of Exclusive OR

Hubert Comon-Lundh and Vitaly Shmatikov

---

*Cryptographic protocols rely on cryptographic primitives to achieve goals such as data privacy and data authenticity in the presence of an attacker. Their use in important applications such as communications over the Internet or credit card payments calls for the automated verification of their security.*

*These two papers made important progress on algorithmic aspects of protocol verification with additional operators, including XOR which is widely used in real-life applications. Specifically, these papers establish the decidability of insecurity of cryptographic protocols with XOR and other equational theories.*

*Chevalier et al. prove membership in NP when restricted to XOR, while Comon and Shmatikov prove decidability in a broader setting. In addition to definitively settling the complexity question for these cases, the lasting value of this line of work is demonstrated by mature verification tools such as ProVerif, Tamarin, Maude-NPA, and CPSA.*

---