CBMC-GC:
Secure Two-Party Computations in ANSI C

Stefan Katzenbeisser
Security Engineering Group
Technische Universität Darmstadt & CASED
skatzenbeisser@acm.org

Joint work with:
Martin Franz (CASED), **Andreas Holzer** (TU Wien), **Helmut Veith** (TU Wien)

Data Privacy — The Traditional Approach

TECHNISCHE UNIVERSITÄT DARMSTADT

Data privacy relies on several technical and administrative approaches:

- Legal requirements
- Policies
- Audits
- Training
- Technical means (access control, network security, intrusion detection)
- Physical security

Does it work?

TECHNISCHE UNIVERSITÄT DARMSTADT

Restaurant chain customers' credit card data stolen

The Boston Globe

By Bruce Mohl, Globe Staff | October

Not Your Average Joe's, a Massachusett
yesterday that thieves have stolen credit
customers.

The Dartmouth-based chain estimated le
than 3,500 of the 350,000 customers it
served in August and September had the
credit card information stolen. The 14-
restaurant chain said it is working with th
US Secret Service and major credit card
companies to determine how the data the
occurred and precisely how many custon
were affected.

Today, the chain plans to post on its web
a notice to customers about the security
breach.

Diana Pisciotta, a spokeswoman for Not
Your Average Joe's, said the chain decid
could check their credit card statements
companies about any suspicious charges
not responsible for fraudulent activity on

"We're doing this out of an abundance of
and forthright with our customers," she s

Stolen computer contained info from 88,000 patients at Staten Island hospital

by Staten Island Advance

Wednesday April 30, 2008, 4:37 PM

Computer equipment stolen from an administrative office in Clifton in December contained personal information from 88,000 patients that have been treated at Staten Island University Hospital.

After four months with no arrests, hospital administrators are just now beginning the process of sending out letters to patients whose names, Social Security and health insurance numbers were contained in computer files on a desktop computer and a backup hard drive stolen Dec. 29 from the hospital's finance office at 1 Edgewater Plaza.

"The hospital is in the process of issuin
patient involved in which one year of fi
a hospital statement, released by spoke
said.

News Site of the Year | The 2008 Newspaper Awards

TIMESONLINE

NEWS | COMMENT | BUSINESS | SPORT | LIFE & STYLE | ARTS & ENTERTAINMENT | RICH LI

UK NEWS | WORLD NEWS | POLITICS | ENVIRONMENT | WEATHER | TECH & WEB NEWS | RELATED R

Where am I? › Home › News › Politics

From The Times

January 19, 2008

Personal data of 600,000 on lost laptop

Michael Evans, Defence Editor

A junior Royal Navy officer is facing a court martial after a laptop containing the personal data of 600,000 people, including serving personnel and thousands of people who have shown an interest in a military career, was stolen from his car.

The loss of the laptop was considered to be so serious that Des Browne, the Defence Secretary, will make a statement to the Commons early next week.

TIMES RECOMMENDS

- MPs back creation of human-animal embryos
- Bank Holiday plan to celebrate Armed Forces
- Wanted: criminal law expert to be new DPP

EXCLUSIVE EXTRACTS

Cherie autobiography

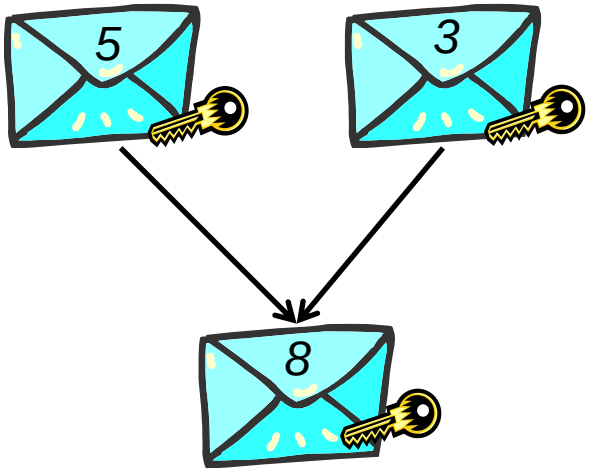
Full coverage and exclusive interviews and extracts from a decade in power

Privacy-Enhancing Technologies (PETs)

TECHNISCHE UNIVERSITÄT DARMSTADT

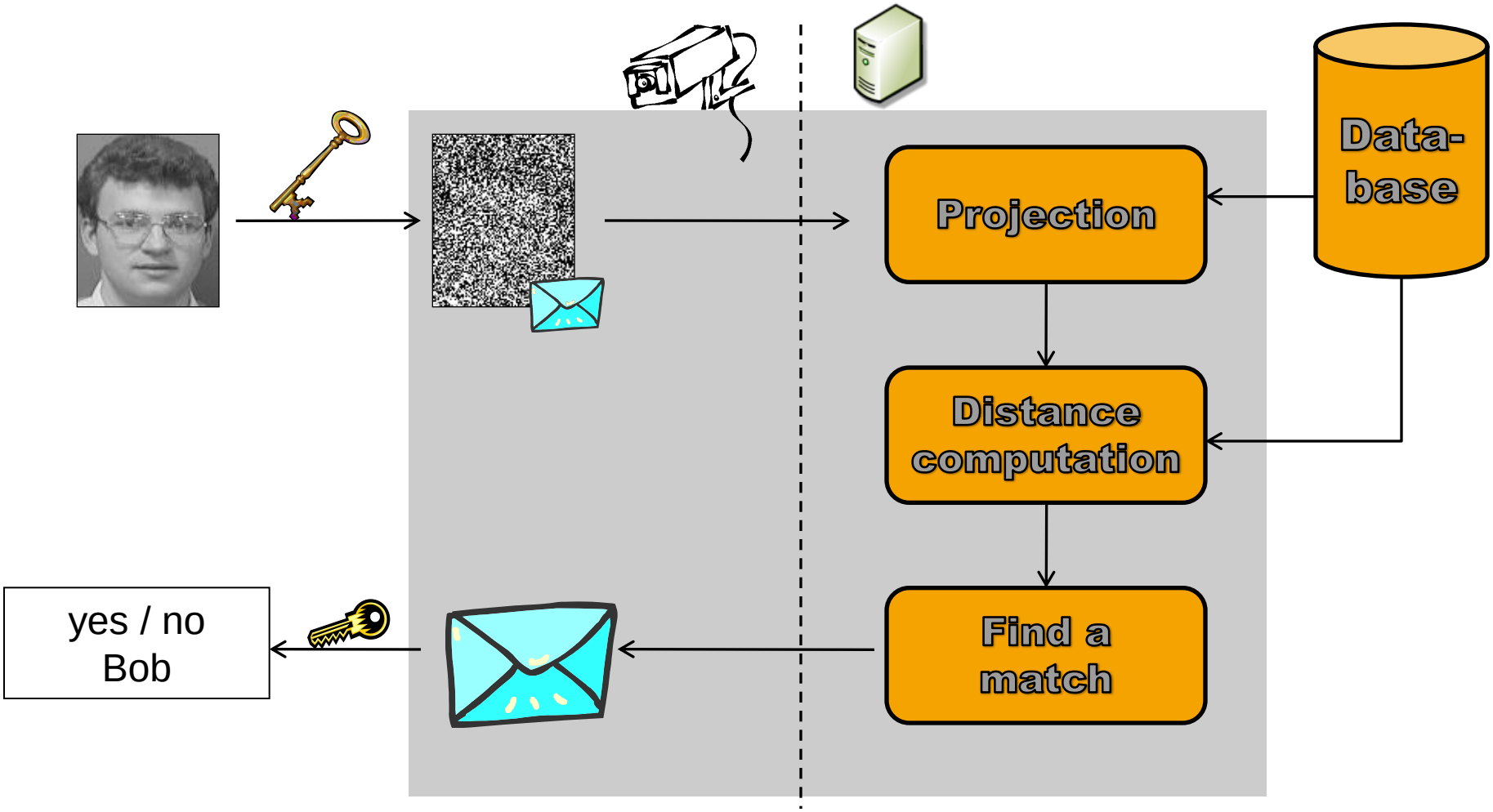
- Strike a balance between data availability and privacy
- **Paradigm:** keep data encrypted, PETs **compute with encrypted data**
- **Privacy By Design**:
  Cryptographic protocols precisely limit amount of information available

- Cryptographic tools are available!
  - Homomorphic encryption
  - Yao's Garbled circuits
  - Customized protocols
    (private set intersection, ...)



Example:
Private Face Detection

TECHNISCHE UNIVERSITÄT DARMSTADT



Example:
Private Processing of Genome Data

TECHNISCHE UNIVERSITÄT DARMSTADT

Physician

Bioinformatics Institute

Two-Party Computation

Medical Test

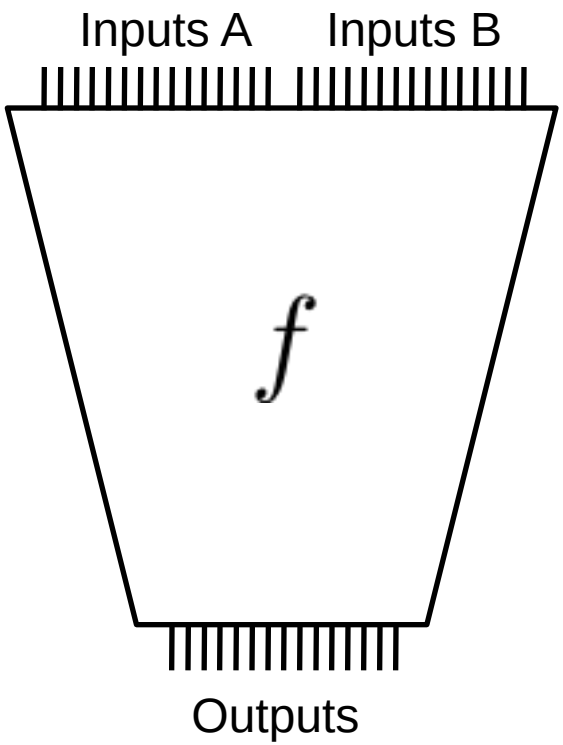
Nice approach, but is it ready for practice?

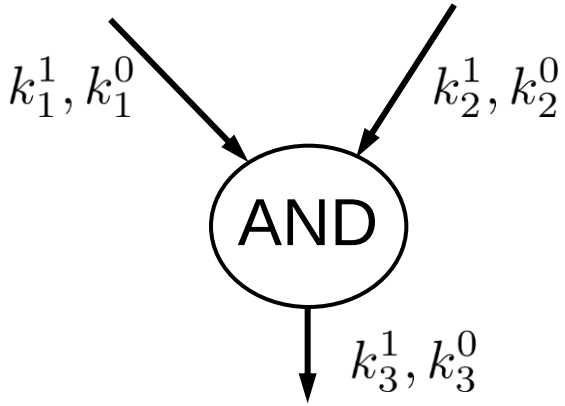
TECHNISCHE UNIVERSITÄT DARMSTADT

- Cryptographic protocols are ready, **but tedious to use**
- Lack of a good tool chain that a programmer can use
- Research prototypes are available:
  - Fairplay, FairplayMP, Sharemind, Tasty
  - Fast GC frameworks (implementation support for Java)
- We need “usable” **compilers** that helps a programmer implement PETs!

Recap:
Yao's garbled circuits

TECHNISCHE UNIVERSITÄT DARMSTADT





$\wedge$	$x=1$	$x=0$
$y=1$	1	0
$y=0$	0	0

	$x=1$	$x=0$
$y=1$	$E(k_1^1, E(k_2^1, k_3^1))$	$E(k_1^1, E(k_2^0, k_3^0))$
$y=0$	$E(k_1^0, E(k_2^1, k_3^0))$	$E(k_1^0, E(k_2^0, k_3^0))$

Our choice as basis: Bit-precise Model Checker CBMC

TECHNISCHE UNIVERSITÄT DARMSTADT

- Transforms C program into a Boolean formula
- Transformation is “bit precise”
  ➔ models evolution of program memory

http://www.cprover.org

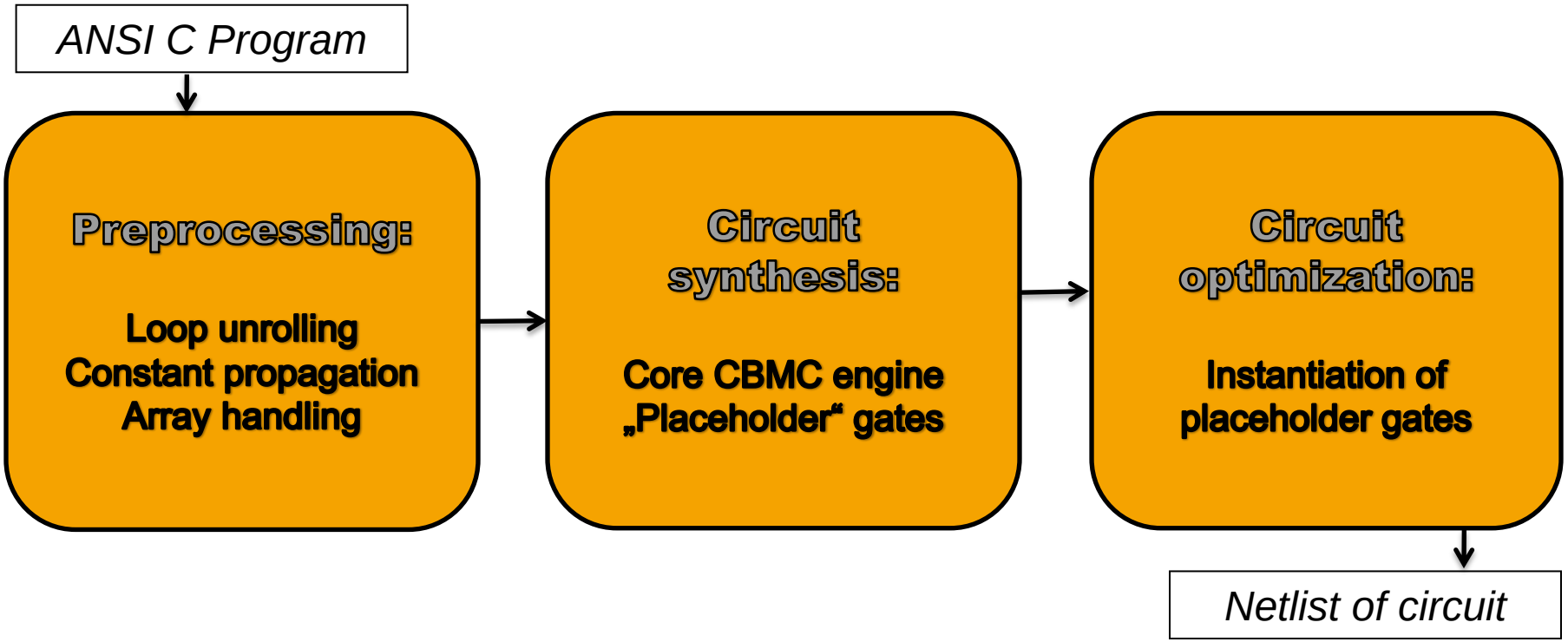
- **Bounded model checker:**
  - Unrolls program up to a fixed number of loop iterations
  - Heuristics on how much unrolling is needed

- Boolean formula consists of program model and negated property
- SAT solver checks for solution

CBMC-GC

TECHNISCHE UNIVERSITÄT DARMSTADT

Central idea: use transformation from C code to SAT formula provided by CBMC for secure computing



CBMC-GC: Example, Yao's Millionaires

TECHNISCHE UNIVERSITÄT DARMSTADT

```
void millionaires() {
int INPUT_A_mila;
int INPUT_B_milb;
int OUTPUT_res;

if (INPUT_A_mila > INPUT_B_milb)
   OUTPUT_res = 1;
else
   OUTPUT_res = 0;
}
```

Local variables code inputs and outputs

Computations specified as C program

CBMC-GC: A bigger example
Matrix multiplication

TECHNISCHE UNIVERSITÄT DARMSTADT

```
#define S 8 // size of matrices
int INPUT_A_a[S][S];
int INPUT_B_b[S][S];
int OUTPUT_c[S][S];
void multiply()
{
  int i, j, k;
  for (i = 0; i < S; i++)
    for (j = 0; j < S; j++)
      for (k = 0; k < S; k++)
        OUTPUT_c[i][j] += INPUT_A_a[i][k] * INPUT_B_b[k][j];
}
```

More complex data types like arrays, structs, enums

(Limited) support for pointer arithmetic

Limitations

TECHNISCHE UNIVERSITÄT DARMSTADT

CBMC-GC inherits limits from CBMC:

- **Bounded programs**: bounds for all loops must be known
  ➔ in practice no problem
- No support for **floating point arithmetic**
- No support for **library functions** (yet)
- Limited **pointer arithmetic**
- **Integer data types** of fixed size
  ➔ limits efficiency in secure computations

CBMC-GC: More examples
Bubblesort

TECHNISCHE UNIVERSITÄT DARMSTADT

```
#define K 11 // length of array
#define MEDIAN 5 // position of median
int INPUT_A_a[K];
int OUTPUT_median;
void median_bubblesort() {
  int i, j, tmp, tmp1, tmp2;
  for (i = K - 1; i > 0; i--) {
    for (j = 0; j < i; j++) {
      tmp1 = INPUT_A_a[j]; tmp2 = INPUT_A_a[j + 1];
      if (tmp1 > tmp2) {
        INPUT_A_a[j] = tmp2; INPUT_A_a[j + 1] = tmp1;
      }
    }
  }
  OUTPUT_median = INPUT_A_a[MEDIAN];
}
```

CBMC can determine loop bounds by static analysis

CBMC-GC supports recursion
Example: Mergesort

TECHNISCHE UNIVERSITÄT DARMSTADT

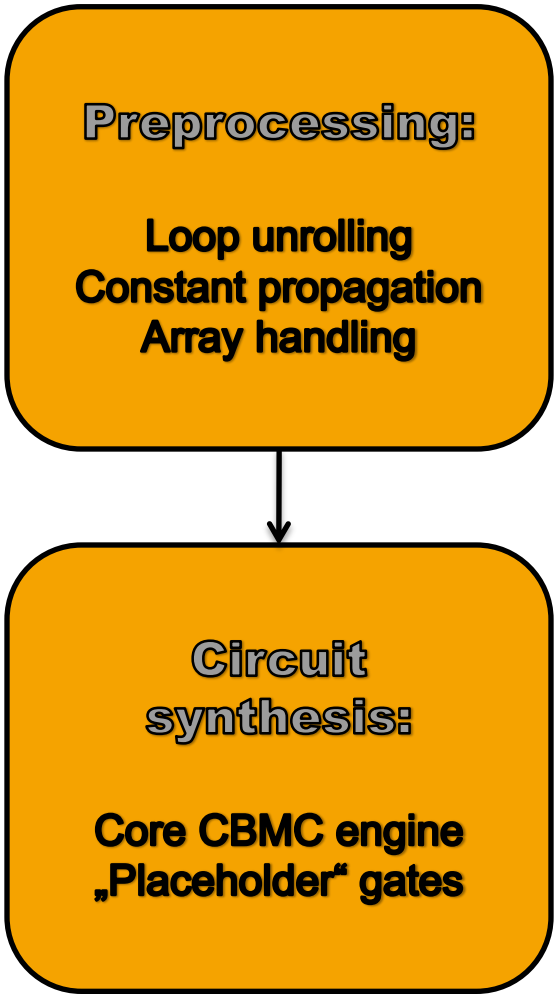
```
int b[K]; // temporary array for mergesort
void mergesort(int l, int r) {
  int i, j, k, m;
  if (r > l) {
    m = (r + l)/2; mergesort(l, m); mergesort(m + 1, r);
    for (i = m + 1; i > l; i--)
      b[i - 1] = INPUT_A_a[i - 1];
    for (j = m; j < r; j++)
      b[r + m - j] = INPUT_A_a[j + 1];
    for (k = l; k <= r; k++) {
      if (b[i] < b[j])
        INPUT_A_a[k] = b[i]; i++;
      else
        INPUT_A_a[k] = b[j]; j--;
    }
  }
}
```

Recursion; CBMC can determine bounds by static analysis

CBMC-GC: Optimizations

TECHNISCHE UNIVERSITÄT DARMSTADT

- Array access are slow
  - ➔ requires evaluation of a MUX circuit
  - ➔ remove some by static analysis
- CBMC is optimized for SAT performance
  - ➔ introduce placeholder gates
  - ➔ later instantiation with optimized circuits
- Optimization engine extensible



Experimental results

TECHNISCHE UNIVERSITÄT DARMSTADT

We used CBMC-GC in conjunction with framework for execution of garbled circuits by Huang et al (USENIX 2011)

Experiment	Number of gates	Execution time, preprocessing	Execution time, circuit evaluation
3000 random arithmetic operations	2,298,441 (608,668)	970 ms	9,774 ms
8x8 matrix multiplication	3,257,345 (905,728)	680 ms	18,173 ms
Median, bubble sort, 31 elements	149,040 (45,120)	733 ms	1,644 ms
Median, merge sort, 31 elements	1,339,084 (436,916)	660 ms	3,790 ms

Conclusions

TECHNISCHE UNIVERSITÄT DARMSTADT

- Automatic compilation of two-party protocols is indeed possible
- Not as fast as hand-written code, but nevertheless usable in practice
- Will hopefully stimulate research in optimization issues, separates crypto functionality from compiler design
- Future research: other basic tools, other languages, optimizations, overcoming current limitations of CBMC-GC, ...

To come:
http://forsyte.at/software/cbmc-gc/