Protecting Circuits from Computationally-Bounded Leakage

Eran Tromer  
MIT

Joint work with

Sebastian Faust  
K.U. Leuven

Leo Reyzin  
Boston University
Motivation

The great tragedy of Crypto -
the slaying of a provably secure scheme
by an ugly side channel.
Engineering approach

- Try preventing leakage.

Imagine a list of
- all known side channel attacks
- all new attacks during the device's lifetime.

- Good luck.
Cryptographic approach

- Face the music: computational devices are not black-box.

- Leakage is a given, i.e., modeled by an adversarial observer. The device should protect itself against it.
Cryptographic Machinery

- Standard toolbox against polynomial-time adversaries (obfuscation, oblivious RAM, fully-homomorphic encryption).
  - Minimize assumptions on adversary's power.
  - Looks hard/impossible/expensive to realize.
  - Worth exploring!

- New tools for a new setting
  - Model the leakage more finely
    - What leaks
    - How much leaks
    - How is the leakage chosen
  - Devise ways to make specific functionality, or even arbitrary circuits, resilient to such leakage.
Related Work

[CDHKS00]: Canetti, Dodis, Halevi, Kushilevitz, Sahai: Exposure-Resilient Functions and All-Or-Nothing Transforms
[ISW03]: Ishai, Sahai, Wagner: Private Circuits: Securing Hardware against Probing Attacks
[MR04]: Micali, Reyzin: Physically Observable Cryptography
[GTR08]: Goldwasser, Tauman-Kalai, Rothblum: One-Time Programs
[DP08]: Dziembowski, Pietrzak: Leakage-Resilient Cryptography in the Standard Model
[Pie09]: Pietrzak: A leakage-resilient mode of operation
[AGV09]: Akavia, Goldwasser, Vaikuntanathan: Simultaneous Hardcore Bits and Cryptography against Memory Attacks
[ADW09]: Alwen, Dodis, Wichs: Leakage-Resilient Public-Key Cryptography in the Bounded Retrieval Model
[FKPR09]: Faust, Kiltz, Pietrzak, Rothblum: Leakage-Resilient Signatures
[DHT09]: Dodis, Lovett, Tauman-Kalai: On Cryptography with Auxiliary Input
[SMY09]: Standaert, Malkin, Yung: A Unified Framework for the Analysis of Side-Channel Key-Recovery Attacks

...
[Ishai Sahai Wagner '03]

Any boolean circuit

Circuit transformation

Transormed circuit

indistinguishable
Our goal

Allow much stronger leakage.

In particular, don’t assume spatial locality

- $t$ wires

- “Only computation leaks information”

[MR04][DP08][Pie09][FKPR09]
Our main construction

A transformation that makes **any circuit** resilient against

- **Global adaptive leakage**
  May depend on whole state and intermediate results, and chosen adaptively by a powerful on-line adversary.

- **Arbitrary total leakage**
  Bounded just per observation.  

But we must assume something:

- **Leakage function is computationally weak**  \([\in MR04]\)
- **A simple leak-free component**  \([\in MR04]\)
Computationally-weak leakage

can be powerful

"antennas are dumb"

computationally weak
Leak-free components

- **Secure memory**
  
  [MR04][DP08][Pie09][FKPR09]

- **Secure processor**
  
  [G89][GO95]

- Here: simple component that samples from a fixed distribution, e.g:

  **securely draw strings with parity 0.**
  
  - No stored secrets or state
  - No input
    
    $\rightarrow$ Consumable leak-free “tape roll”
  - Can be relaxed

- Large leak-free components may be **necessary** in this model (more later)
1. Computation model
2. Security model
3. Circuit transformation
4. Proof approach
5. Extensions
6. Necessity of leak-free components
Original circuit C of arbitrary functionality (e.g., crypto algorithms). Computes over a finite field $K$. Example: AES encryption with secret key $M$. $X \rightarrow C[M] \rightarrow Y$
Original circuit

Allowed gates in C:

- Multiply in $K$: \[ \cdot \]
- Add in $K$: \[ + \]
- Coin: \[ $ \]
- Const: \[ 1 \]
- Memory: \[ M \]
- Copy: \[ C \]

(Boolean circuits are easily implemented.)
Transformed circuit  [IW03]

Same underlying gates as in C, plus opaque gate (later).

Soundness: For any $X, M$: $C[M](X) = C'[M'](X)$
Model: single observation in leakage class $L$

$X$ \[\downarrow\text{wires}\] $f \in L$ $\downarrow f(\text{wires})$ $Y$
Model: adaptive observations

refresh state $\Rightarrow$ allows total leakage to be large!
Model: $L$-secure transformation

Adversary learns no more than by black-box access:

Simulation:

Real:
Motivating example

Problem: Adversary learns one bit of the state
Solution: Share each value over many wires [ISW03, generalized]

Every value encoded by a linear secret sharing scheme (Enc, Dec) with security parameter t:

**Enc:** $K \rightarrow K^t$ (probabilistic)

**Dec:** $K^t \rightarrow K$ (surjective, linear function)
Leakage: $L$-leakage-indistinguishability

$(Enc, Dec)$ is $L$-leakage-indistinguishable:
For all $x_0, x_1 \in K$:

\[
\begin{align*}
&\text{Enc}(x_0) \quad \text{Enc}(x_1) \\
b \in \{0, 1\} \\
f \in L \\
f(\text{Enc}(x_b)) \\
b' \leftarrow \\
\Pr[b' = b] - \frac{1}{2} \leq \text{negl}
\end{align*}
\]

Consequence:
Leakage functions in $L$ cannot decode
Main construction

For any linear encoding scheme that is $L$-leakage indistinguishable, we present an $L'$-secure transformation for any circuit and state.
Unconditional resilience against $\text{AC}^0$ leakage

Some known circuit lower bounds imply $L$-leakage-indistinguishability

Parity $\rightarrow$ hard for $\text{AC}^0$

Enc(x)

depth: 2
size: $O(t^2)$

const depth and poly size circuits

$\text{AC}^0$

Theorem

$\rightarrow$

$f'$

$f \in \text{AC}^0$
Transformation: high level

- The state is encoded: $M' = \text{Enc}(M)$
- Circuit topology is preserved
- Every wire is encoded
- Inputs are encoded; outputs are decoded
- Every gate is converted into a **gadget** operating on encodings
Computing on encodings

*first attempt*

\[ \tilde{a} = \text{Enc}(a) \]
\[ \tilde{b} = \text{Enc}(b) \]
\[ a = \text{Dec}(\tilde{a}) \]
\[ b = \text{Dec}(\tilde{b}) \]
\[ c \]
\[ \tilde{c} = \text{Enc}(c) \]

Notation: \( \tilde{x} = \text{Enc}(x) \)

Easy to attack
Computing on encodings
second attempt – use linearity

\[ \tilde{a} = \text{Enc}(a) \]
\[ \tilde{b} = \text{Enc}(b) \]

\[ \tilde{c} \]

\[ f(\text{wires}) \]

Works well for a single gate... but does not compose. Exponential security loss (for AC\(^0\)).
Intuition: wire simulation

Since $f$ can verify arbitrary gates in circuit, wires must be consistent with $X$ and $Y$.

**Problem:** simulator does not know state $M$

**Solution:** to fool the adversary, introduce **non-verifiable** atomic gate.
Opaque gate

Fool adversary: gate is non-verifiable by functions in \( L \).

**Opaque gate:**

- Samples from a fixed distribution.
- No inputs
- Can be realized by a leak-free "consumable tape"
Using the opaque gate

Full transformation for $+$ gate:

Wire’s simulator advantage: can change output of opaque without getting noticed ($L$-leakage-indistinguishable)

So we can simulate this independent of all others gates
Other gates

- Similar transformation for other gates.
- The challenging case is the non-linear gate, field \textit{multiplication}. Hard to make leak-resilient; standard MPC doesn’t work.

Trick: give wire simulator enough degrees of freedom.

\[
\begin{align*}
\text{Dec}(\vec{c}) &= \vec{r}^T(\vec{q} + \vec{o}) = \vec{r}^T((B+S)\vec{r} + \vec{o}) = \vec{r}^T((\vec{a}\vec{b}^T + S)\vec{r} + \vec{o}) \\
&= (\vec{r}^T\vec{a})(\vec{b}^T\vec{r}) + (\vec{r}^T S')\vec{r} + \vec{r}^T\vec{o} = ab + \vec{0}^T\vec{r} + 0 = ab
\end{align*}
\]
Proof technique: wire simulators

All of our gadgets have shallow wire simulators that are $L$-leakage indistinguishable from honest:
Wire simulator composability

This property (suitably defined)
composes!

If every gadget
has a (shallow) wire simulator
then the whole transformed circuit
has a (shallow) wire simulator.

Security for single round follows easily.

For multiple rounds there’s extra work due to adaptivity of the leakage and inputs.
Security proof: bottom line

- Loss in the reduction to leakage-indistinguishability of the encoding scheme: very small.
- Necessary since we prove security against low computational classes.
- This makes the computational-security proof very delicate.
Wire simulators redux

General proof technique. Theorem:

If every gadget has (shallow) wire simulators, then the transformation is (almost) as leakage-indistinguishable as the encoding.

Applications:

• Resilience against polynomial-time leakage using public-key encryption.
  – Assumes leak-free GenKey-Decrypt-Compute-Encrypt components.
  – Proof is extremely easy!

• Resilience against noisy leakage[Rabin Vaikuntanathan 2009]
  – Easy alternative proof.

• Theorem for hire!
Wire simulators strike again

Nested-composition theorem:
Can replace each leak-free gate with a gadget of the same I/O functionality (based on different gates), if the gadget has a wire simulator that is leakage-indistinguishable.

Example: reduce randomness in the $AC^0$ opaque gate.

- Can be implemented using $\text{polylog}(t)$ randomness + PRG. [Nis91]
- Can be implemented shallowly using any $\text{polylog}(t)$-independent source. [Bra09]
Summary of (positive) results

Public-key encryption + Gen+Dec+Enc gadgets with wire sim. → Any encoding + leakage class which can’t decode + gadgets with wire sim. → Noisy leakage + leak-free encoding gates (alt. proof of [RV09])

Linear encoding + leakage class which can’t decode + Enc(0) gadget with wire sim. → Linear encoding + leakage class which can’t decode + leak-free Enc(0) gates → AC^0 / ACC^0[q] leakage + leak-free 0-parity gates
Theorem: any sound transformation that has wire simulators fooling nontrivial leakage classes requires large leak-free components (grow with security parameter, which grows with circuit size).

Intuition: otherwise leakage functions \( f \in L \) can verify the simulated wire values, and thus force the wire simulator to honestly compute the function.

Then shallow circuits (wire simulators) can compute any function computable by polysize circuits!

- Impossible if the simulation (and encoding) are constant-depth.
- More generally, implies unlikely complexity-theoretic collapses, e.g., \( \text{NC} = \text{P/poly} \).

Conjecture: necessity holds for all circuit transformations which are secure against nontrivial leakage via a black-box reduction to the leakage-indistinguishability of encodings.
Conclusions

**Achieved**

- **New model** for side-channel leakage, which allows **global leakage** of unbounded total size
- Constructions for **generic** circuit transformation, for example, against all leakage in \( \text{AC}^0 \).
- Partial **impossibility** results.
- General **proof technique** + additional applications.

**Open problems**

- More leakage classes
- Smaller leak-free components
- Proof/falsify black-box necessity conjecture
- Circumvent necessity result (e.g., non-blackbox constructions)