Securing Circuits Against Constant-Rate Tampering

Dana Dachman-Soled Yael Tauman Kalai

Microsoft Research

Tamper-Resilient Circuits

[Ishai-Prabhakaran-Sahai-Wagner06]

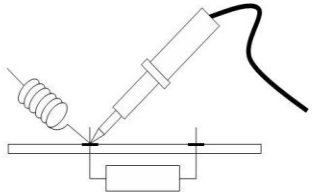
[IPSW06]: 1/size tampering rate

Our work: 1/const tampering rate

Physical Attacks

Cold-boot attack

[Halderman-Schoen-Heninger-Clarkson-Calandrino-Feldman-Appelbaum –Felten08]

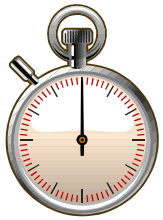


Fault attacks

[Boneh-DeMillo-Lipton97, Biham-Shamir98, …]

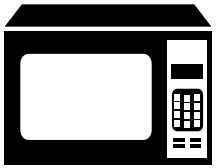
Timing attacks

[Kocher96,…]



Power attacks

[Kocher-Jaffe-Jun99,…]



Acoustic attacks

[Shamir-Tromer]

Radiation Attacks

[Agrawal-Archambeault-Rao-Rohatgi02]

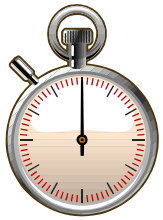
Leakage attacks

Cold-boot attack

[Halderman-Schoen-Heninger-Clarkson-Calandrino-Feldman-Appelbaum –Felten08]

Timing attacks

[Kocher96,…]



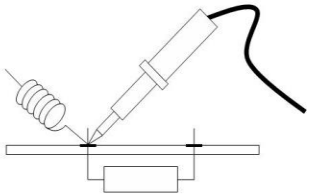
Power attacks

[Kocher-Jaffe-Jun99,…]

Acoustic attacks

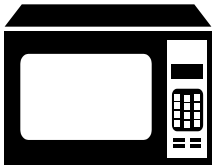
[Shamir-Tromer]

Tampering attacks



Fault attacks

[Boneh-DeMillo-Lipton97, Biham-Shamir98, …]



Radiation Attacks

[Agrawal-Archambeault-Rao-Rohatgi02]

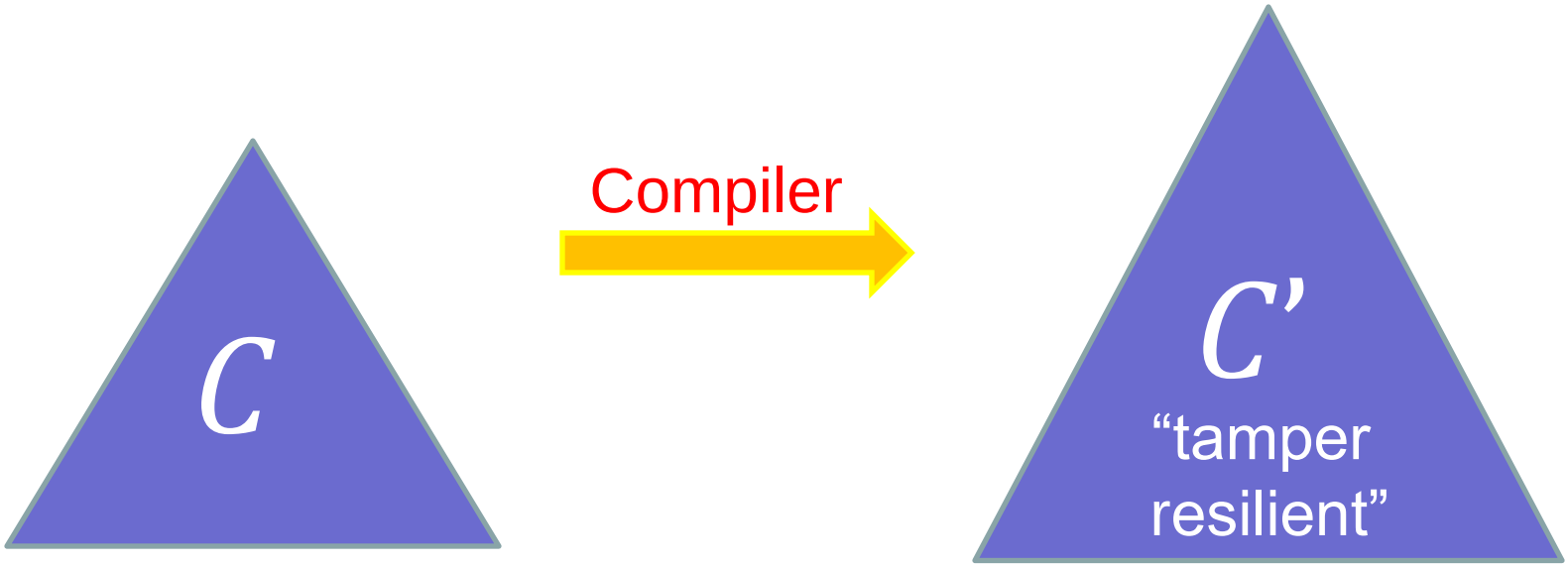
Leakage attacks

[Rivest1997, Boyko1999, Canetti-Dodis-Halevi-Kushilevitz-Sahai2000, Ishai-Sahai-Wagner2003, Micali-Reyzin2004, Ishai-Prabhakaran-Sahai-Wagner2006, Dziembowski-Pietrzak2008, Pietrzak2009 , Akavia-Goldwasser-Vaikuntanathan2009, Dodis-K-Lovett2009, Naor-Segev2009, Katz-Vaikuntanathan2009, Alwen-Dodis-Wichs2009, Alwen-Dodis-Naor-Segev-Walfish-Wichs2009, Faust-Kiltz-Pietrzak-Rothblum2009, Faust-Rabin-Reyzin-Tromer-Vaikuntanathan2010, Dodis-Goldwasser-K-Peikert-Vaikuntanathan2010, Goldwasser-K-Peikert-Vaikuntanathan2010, Juma-Vahlis2010, Goldwasswer-Rothblum2010, Canetti-K-Mayank-Wichs2010, Dodis-Haralambiev-LopezAlt-Wichs2010, Brakerski-K-Katz-Vaikuntanathan2010, Boyle-Segev-Wichs2010, Dodis-Pietrzak2010, Braverman-Hassidim-K2010, Lewko-Waters2010, Lewko-Rouselakis-Waters2011, Lewko-Lewko-Waters2011, Jain-Pietrzak2011, Bitansky-Canetti-Halevi-Goldwasser-K-Rothblum2011, Bitansky-Canetti-Halevi2011, Garg-Jain-Sahai2011, Brakerski-K2011, Dodis-Lewko-Waters-

Tampering attacks

[Bellare-Kohno2003, Gennaro-Lysyanskaya-Malkin-Micali-Rabin2004, Ishai-Prabhakaran-Sahai-Wagner2006, Applebaum-Harnik-Ishai2010, Dziembowski-Pietrzak-Wichs2010, Kalai-kanakhurthi-Sahai2011, , Choi-Kiayias-Malkin11, Kalai-Lewko-Rao2011, Liu-Lysyanskaya12]

Our Results



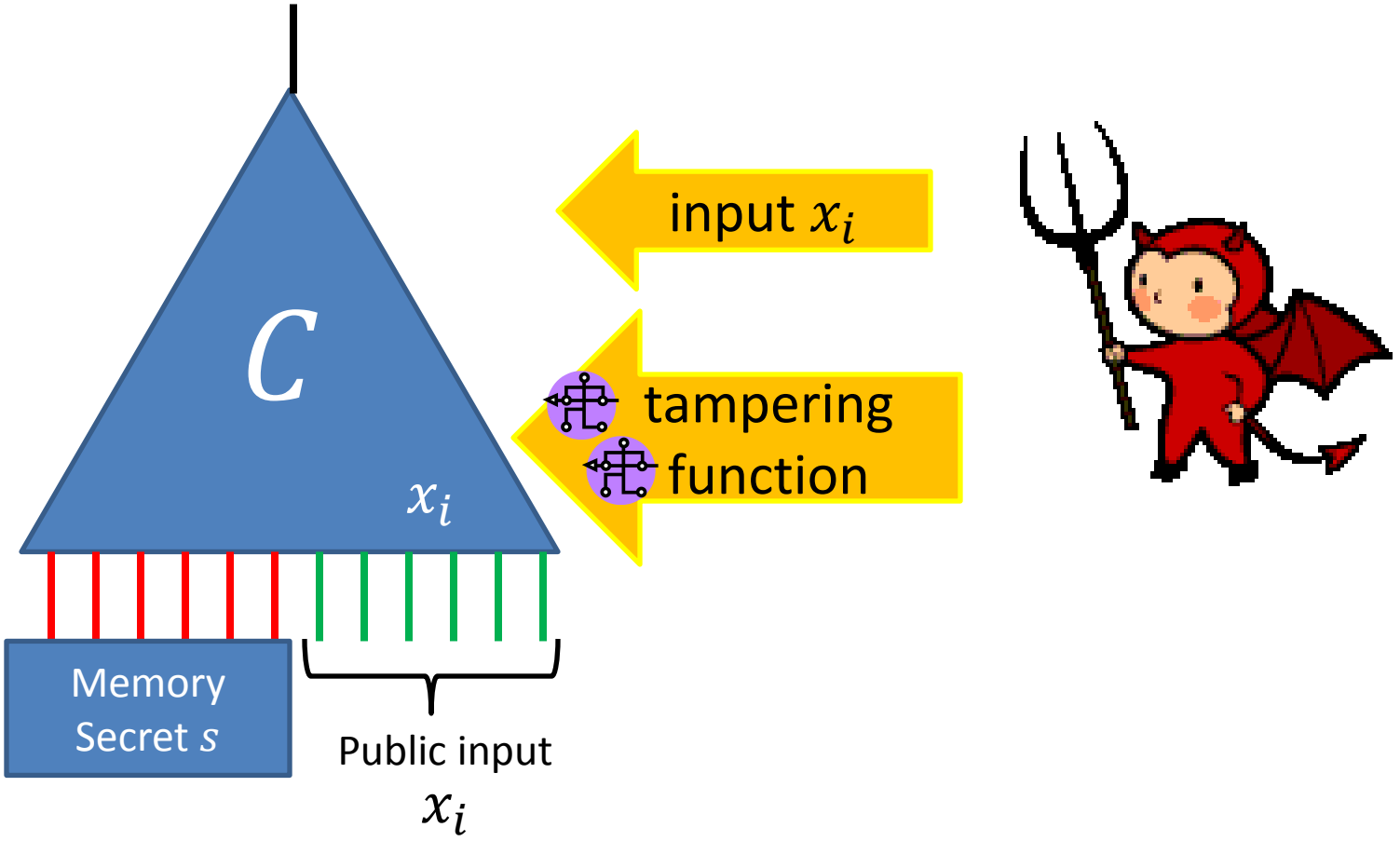
Need to define:

1. Tampering model
2. Security guarantee

Theoretical Result

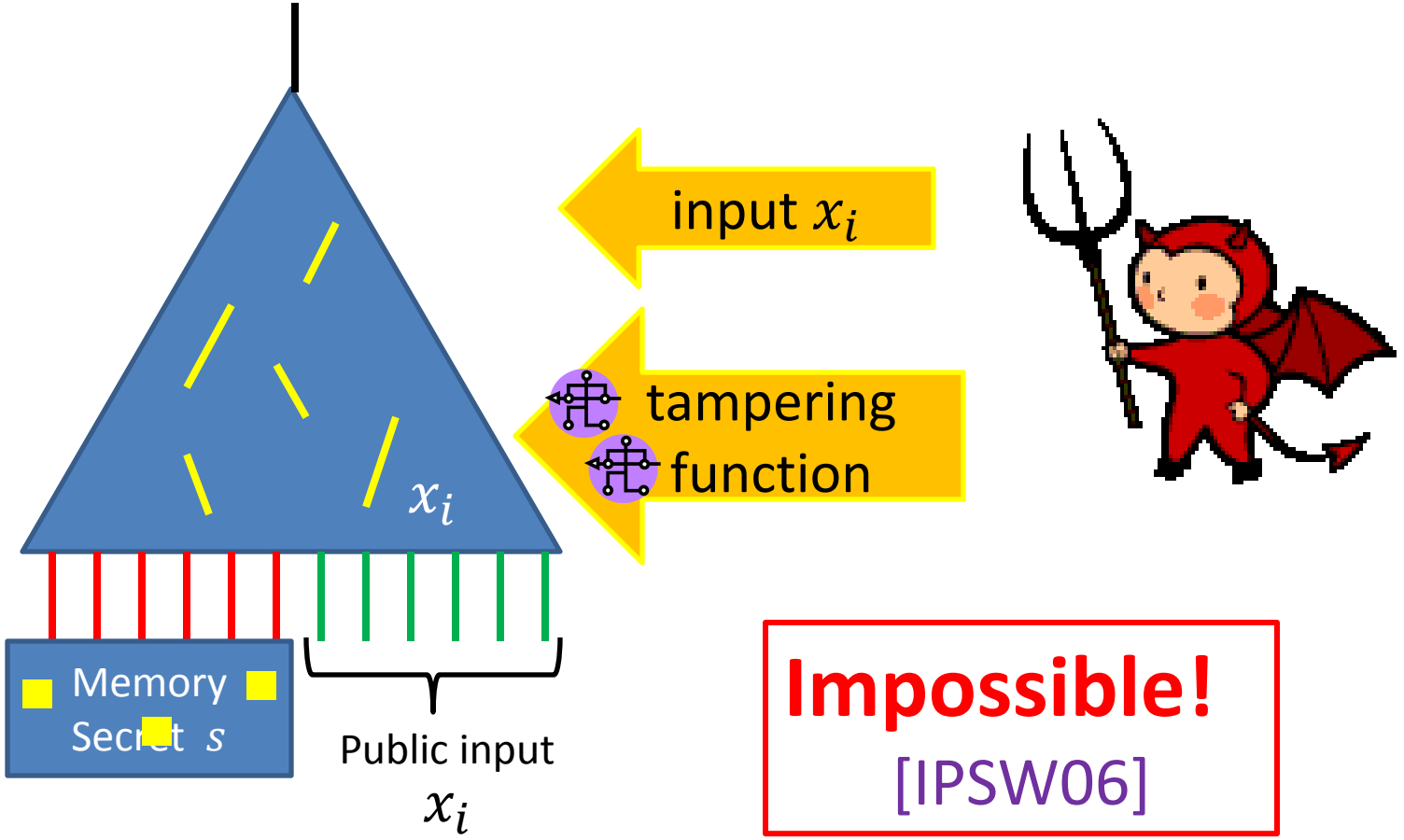
Tampering Model
(tampering with individual wires)

Inspired by [Ishai-Prabhakaran-Sahai-Wagner2006]



Tampering Model
(tampering with individual wires)

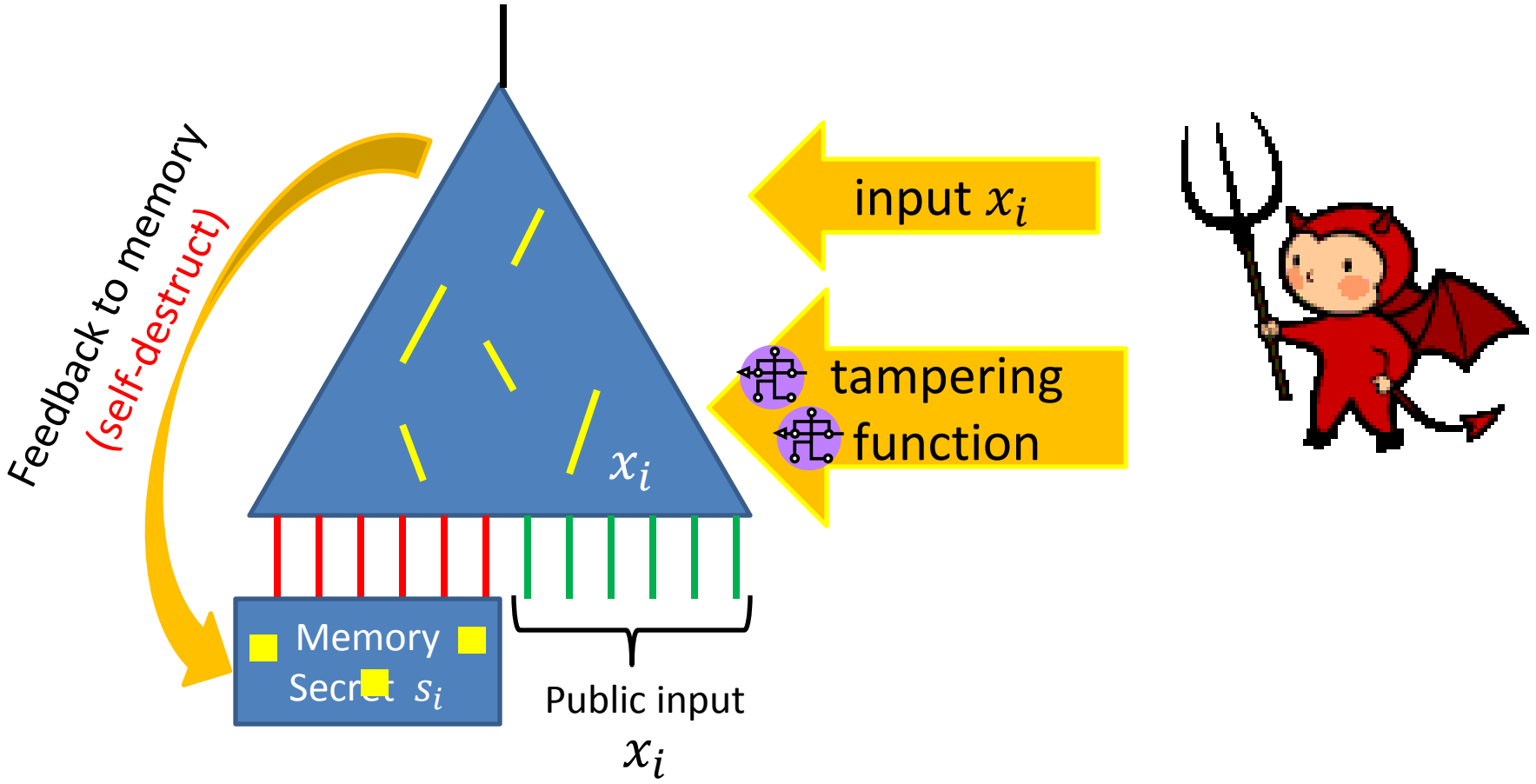
Inspired by [Ishai-Prabhakaran-Sahai-Wagner2006]



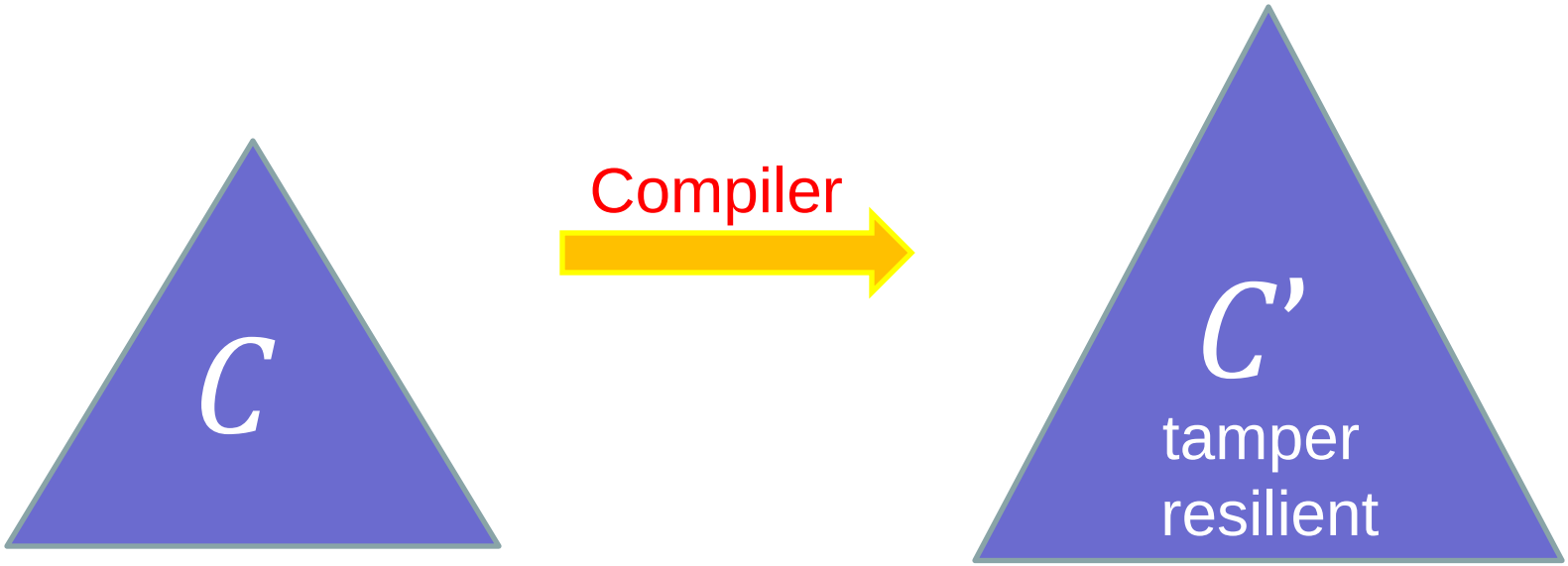
Impossible!
[IPSW06]

Tampering Model
(tampering with individual wires)

Inspired by [Ishai-Prabhakaran-Sahai-Wagner2006]



Our Results



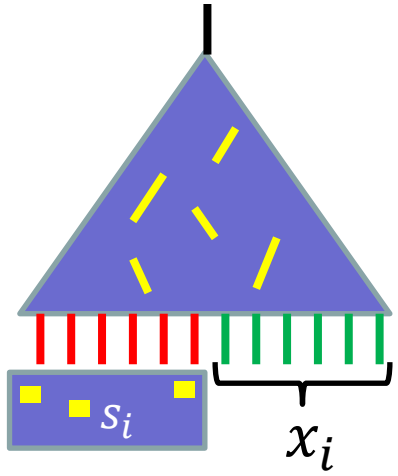
Need to define:

1. Tampering model ✓
2. Security guarantee

Security Guarantee

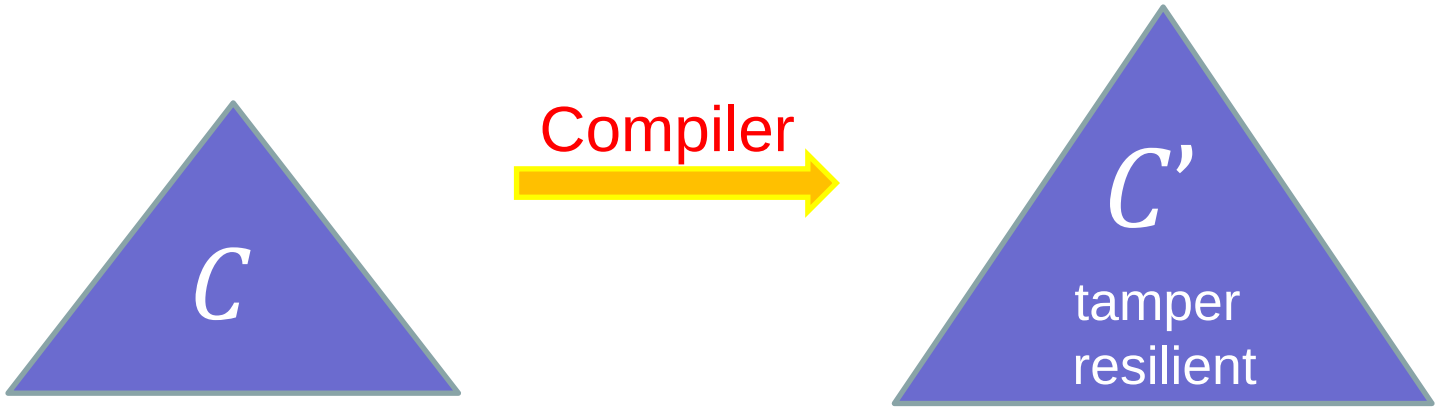
For every  there exists simulator Sim s.t.

$$Sim^{C,\,L(s)} \approx$$



When did self-destruct occur

Our Results



- Resilient to constant tampering rate.
- Information theoretic

Comparison with [IPSW06]

[IPSW06]	Our Work
Tampering rate $< \frac{1}{k}$	Tampering rate is **const**.
Uses randomness gates or relies on computational assumptions	Information theoretic no need for randomness
No leakage	log bits of leakage
Persistent faults	Non-persistent faults

Other Related Work

- Fault-tolerant computation

  [VonNeumann56, . . ., KLM94, GZ95, KRL12]

- Tampering only with the memory gates.

  [Gennaro-Lysyanskaya-Malkin-Micali-Rabin2004, Applebaum-Harnik-Ishai2010, Dziembowski-Pietrzak-Wichs2010, Kalai-Kanakhurthi-Sahai2011 , Choi-Kiayias-Malkin11, Liu-Lysyanskaya12]

- Tampering with the entire circuit:

  [IPSW06, Faust-Pietrzak-Venturi11]

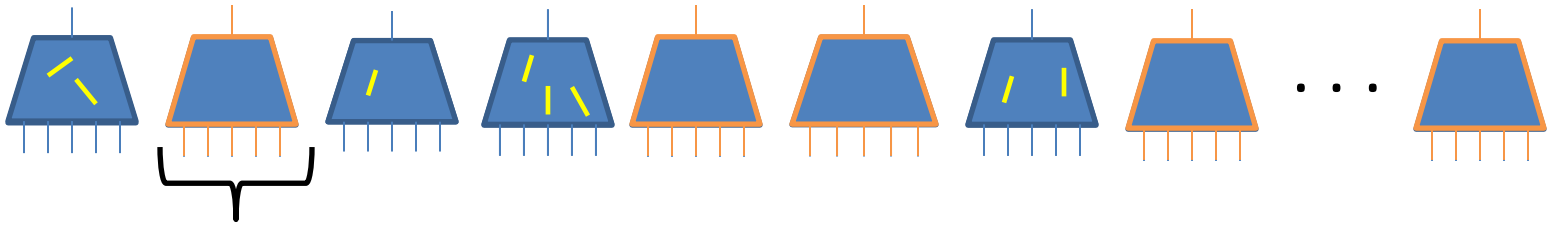
  - [FPV11] logarithmic leakage.
  - [FPV11] tamper with wires, but random errors

Overview of our Construction

Starting point [IPSW06]: tamper-resilient

Add tamper-detection component that erases memory if tampering is detected.

Key: Tamper-detection component in NC^0



circuit of constant size

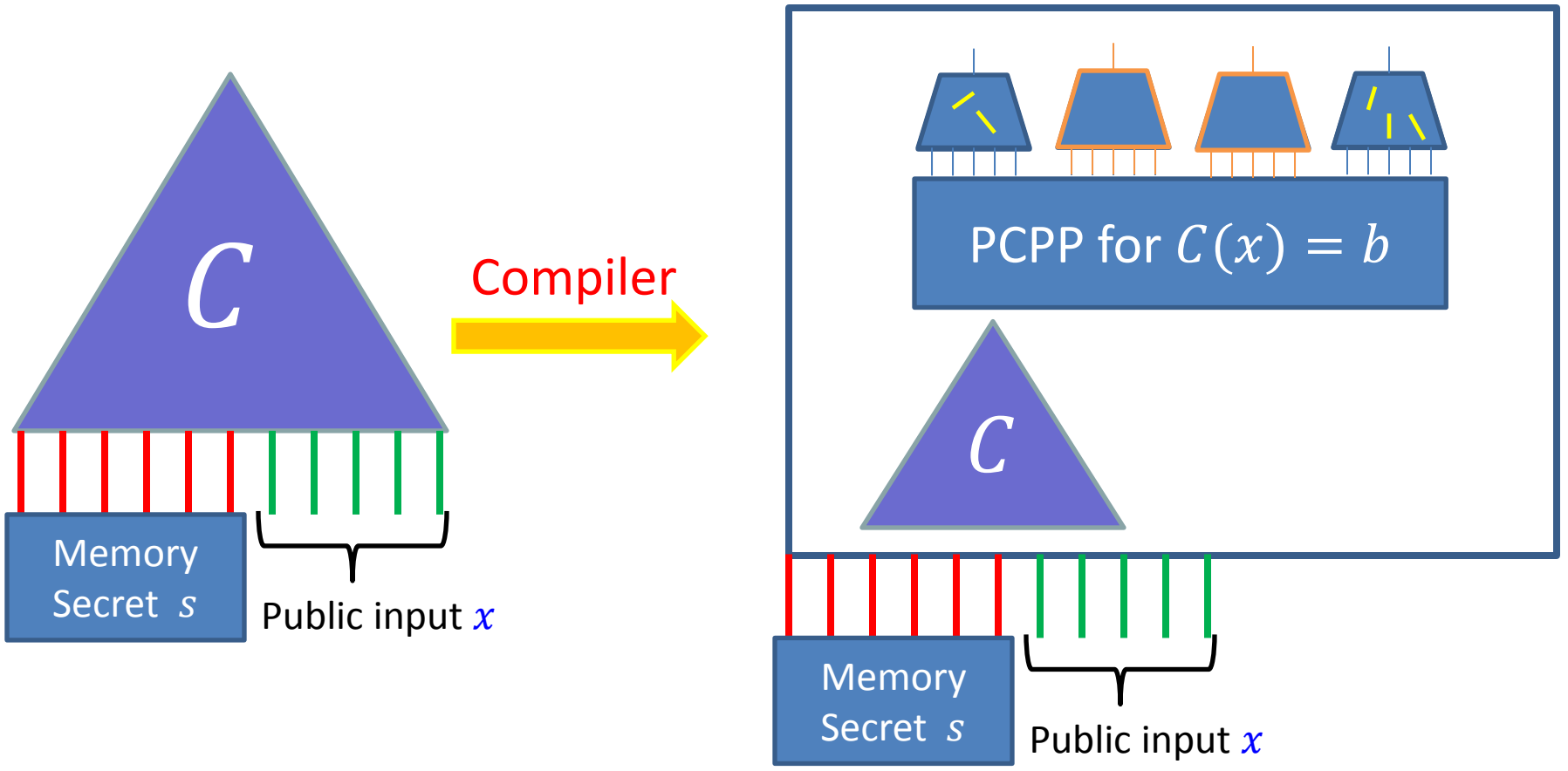
Tool: PCP of Proximity

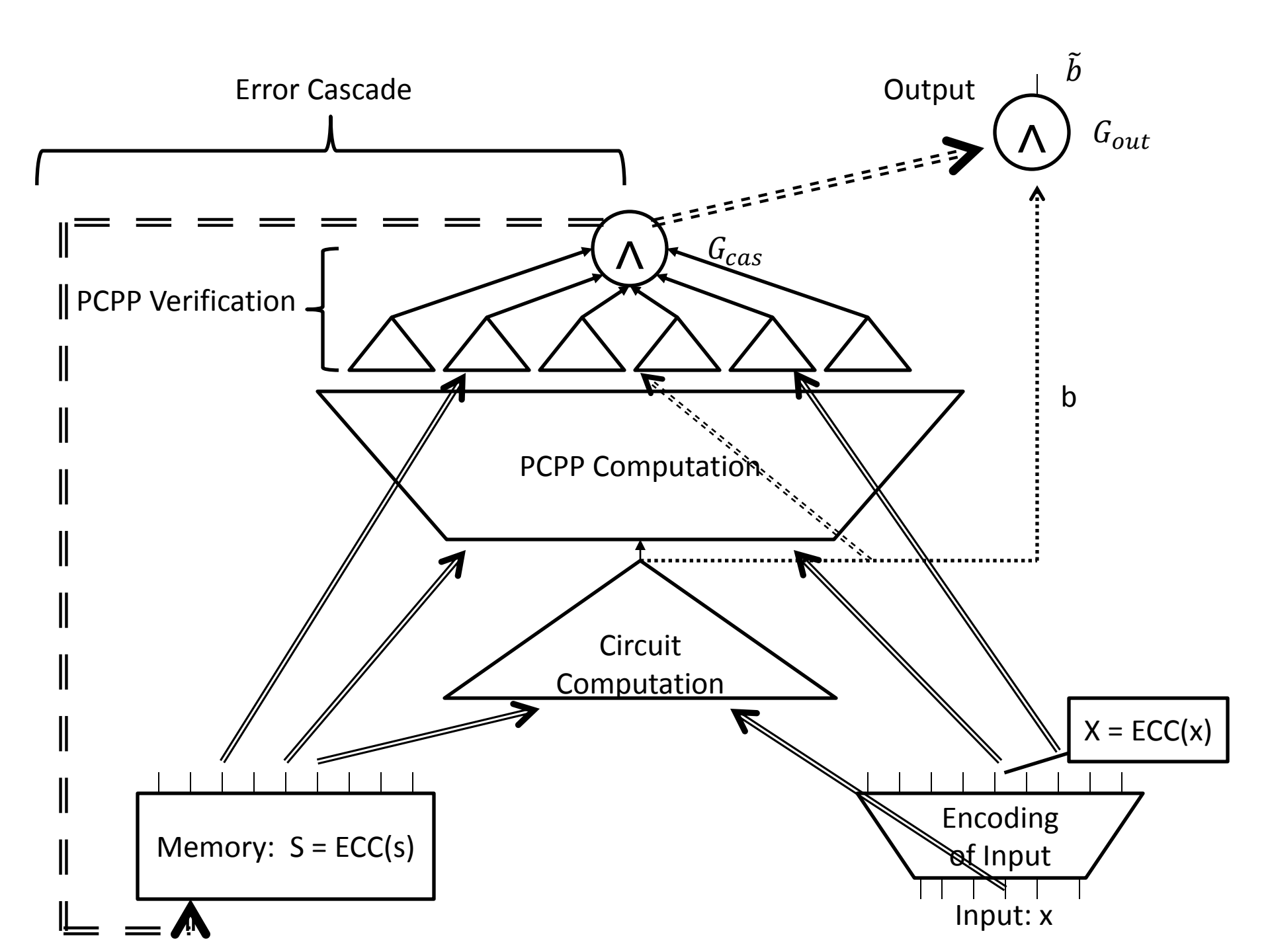
[Ben-Sasson-Goldreich-Harsha-Sudan-Vadhan06]

Overview of our Construction (Cont.)

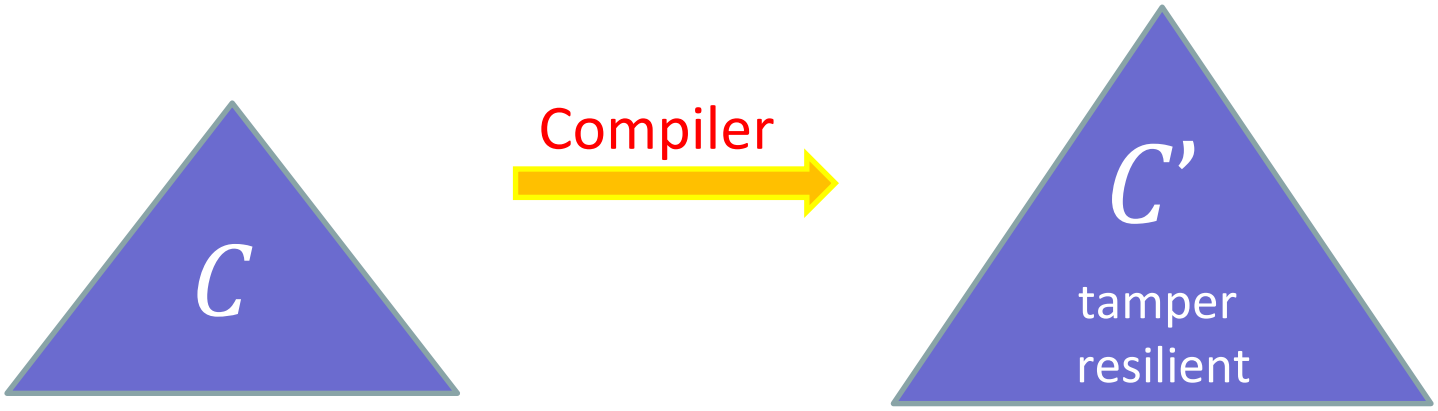
Tool: PCP of Proximity

[Ben-Sasson-Goldreich-Harsha-Sudan-Vadhan06]




Error Cascade
Output
$\tilde{b}$
G_{out}
G_{cas}
PCPP Verification
b
PCPP Computation
Circuit
Computation
X = ECC(x)
Memory: S = ECC(s)
Encoding
of Input
Input: x

Summary



- Resilient to constant tampering rate.
- Information theoretic
- Extend to leakage + tampering (in the paper)

Thank you!