# New Limits of Provable Security and Applications to ElGamal Encryption

Sven Schäge
Eindhoven University of Technology

# ElGamal PKE (1984)

$$\mathsf{KeyGen}(1^\kappa) \rightarrow (sk,\ pk = g^{sk})$$
$$\mathsf{Enc}(pk, m; r) = (g^r,\ pk^r \cdot m) = (c_1, c_2) = c$$
$$\mathsf{Dec}(sk, c) = (c_1)^{sk}/c_2 = m$$

- Important PKE scheme that inspired many extensions/variants: IBE, ECIES, lattice-based PKE schemes
- Provably IND-CPA secure under DDH asssumption
- Provably not IND-CCA2 secure due to malleability of ciphertexts (unconditional impossibility)
- Long-standing open problem:

*Is ElGamal PKE provably IND-CCA1 secure (against lunchtime attacks)?*

The CCA1 security of ElGamal is a big open question. There are no attacks known, but standard reductions don't seem to work.

Yehuda Lindell
28k 1 67 85

https://crypto.stackexchange.com/questions/26867/is-elgamal-ind-cca1

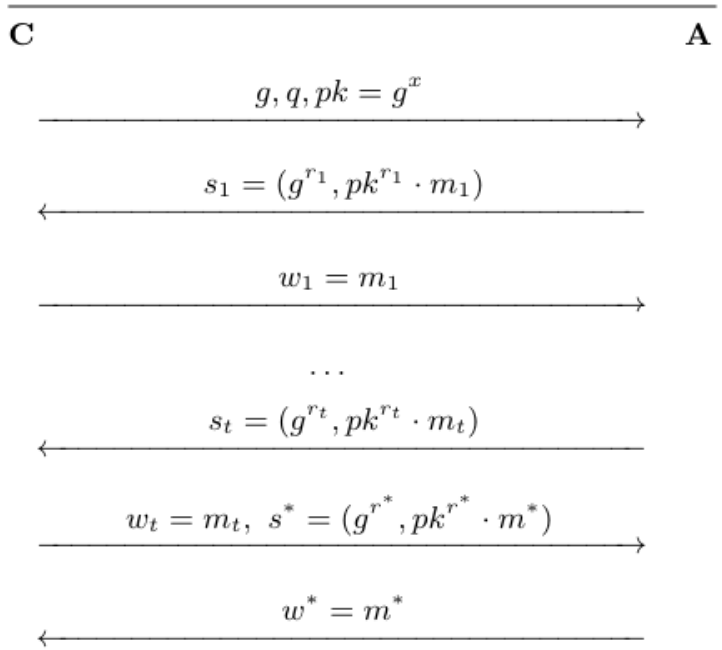
However, Elgamal's CCA1-security is a well-known open problem.

Helger Lipmaa, ``On the CCA-1 Security of Elgamal and Damgard's Elgamal", ISC 2011

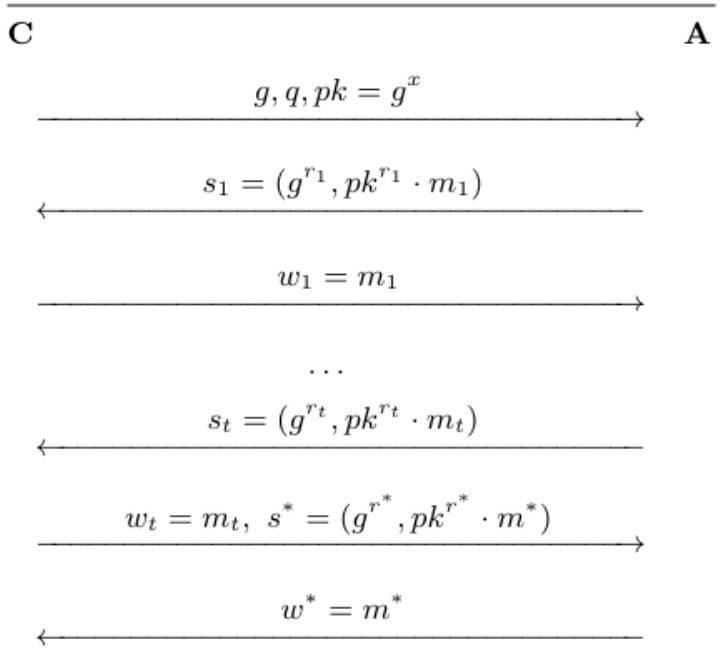
# Even harder question:
# Is ElGamal Provably PKE OW-CCA1 Secure?

IND-CCA1 security => OW-CCA1 security

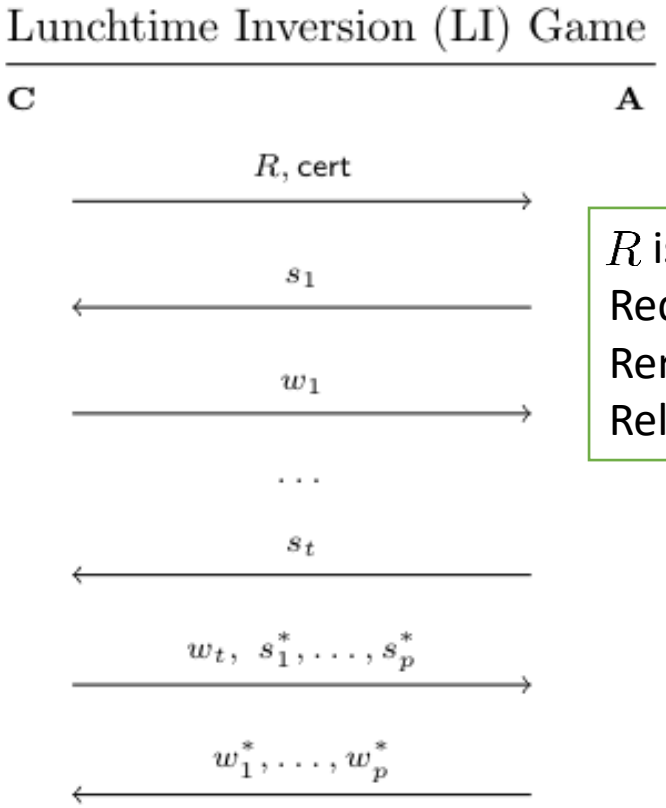
⇔ no provable OW-CCA1 security => no provable IND-CCA1 security



# Generalizing the Problem




generalize




$R$ is a Random Self-Reducible and Rerandomizable Relation (RRR)!

relation R, statement s, and witness w

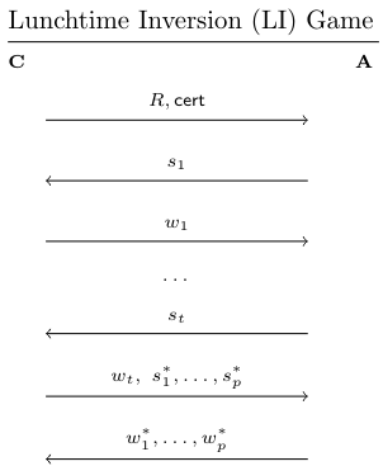
# Scope of RRRs

statement s: ciphertext
witness w: plaintext

ElGamal PKE — generalize →
Paillier PKE — generalize →
Damgård-Jurik PKE — generalize →
Linear Encryption & Generalization from MDDH — generalize →

Certified Semi-Homomorphic PKE — generalize →

$R$ is a Random Self-Reducible and Rerandomizable Relation (RRR)!




← generalize — Certified Homomorphic One-Way Bijection (CHOWB)

statement s: output CHOWB(x)
witness w: input x

← generalize — RSA
← generalize — Discrete Expon.

…

…

# Results

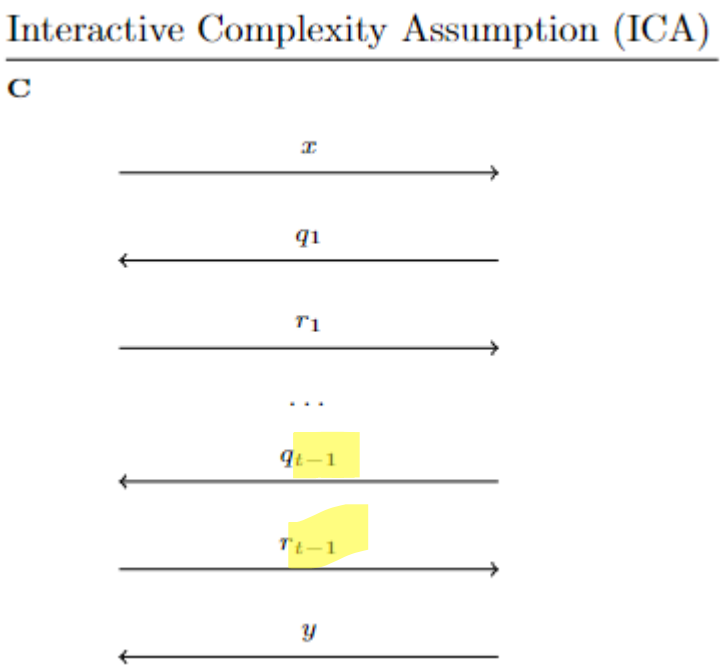
$R$ is a Random Self-Reducible and Rerandomizable Relation (RRR)!

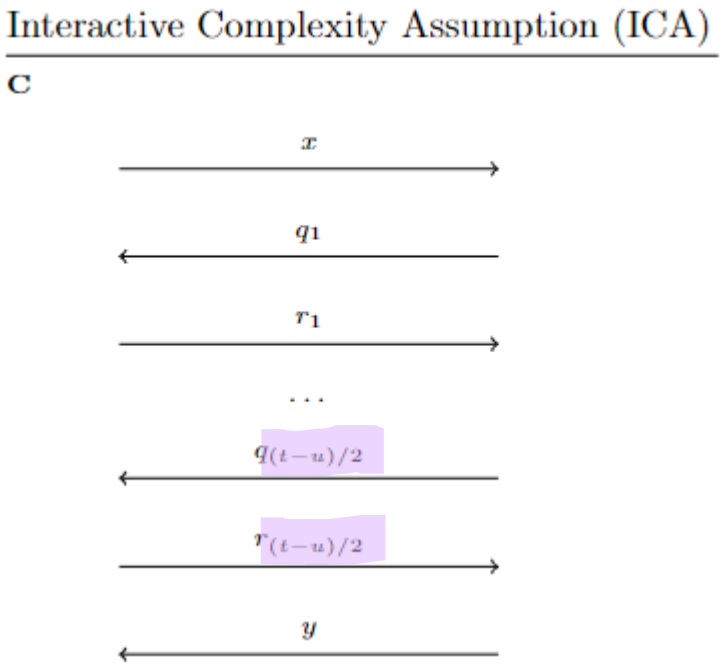
single instance, no rewinding

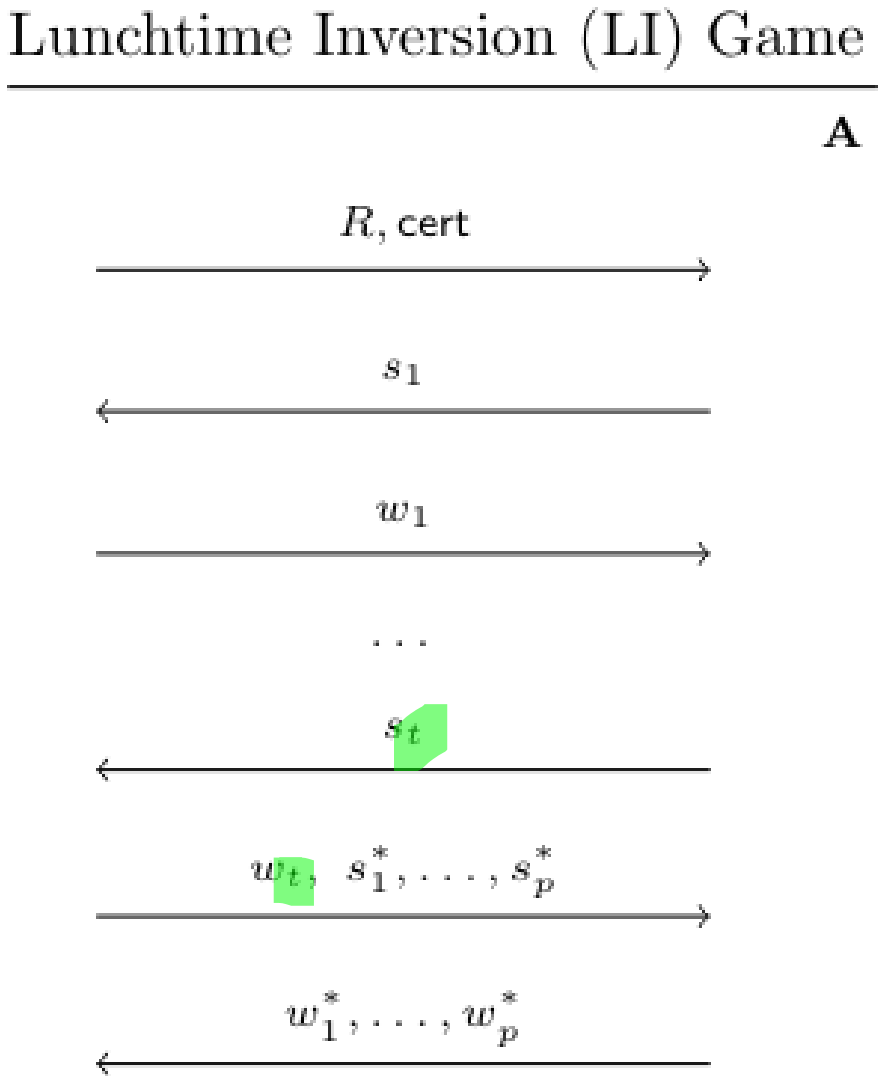
Simple Reduction

Turing Reduction

$u$: number of attacker instances create by reduction



# Result 1: Proof Idea Ideal Attacker

$R$ is a Random Self-Reducible and Rerandomizable Relation (RRR)!

**Interactive Complexity Assumption (ICA)**

**C**

$x$ →

← $q_1$

$r_1$ →

$\ldots$

← $q_{t-1}$

$r_{t-1}$ →

← $y$

Simple Reduction

**Lunchtime Inversion (LI) Game**

**A**

$R$, cert →

← $s_1$

$w_1$ →

$\ldots$

← $s_t$

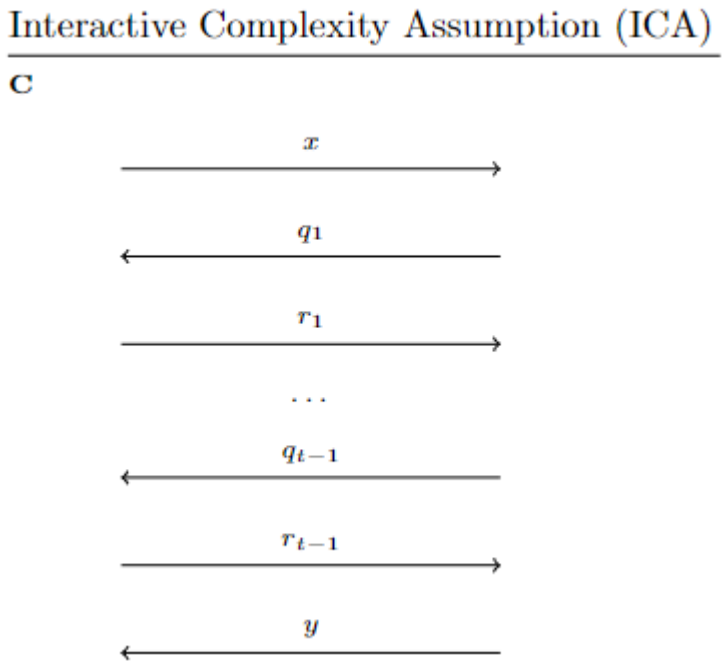
$w_t, \ s_1^*, \ldots, s_p^*$ →

brute-force computation

← $w_1^*, \ldots, w_p^*$

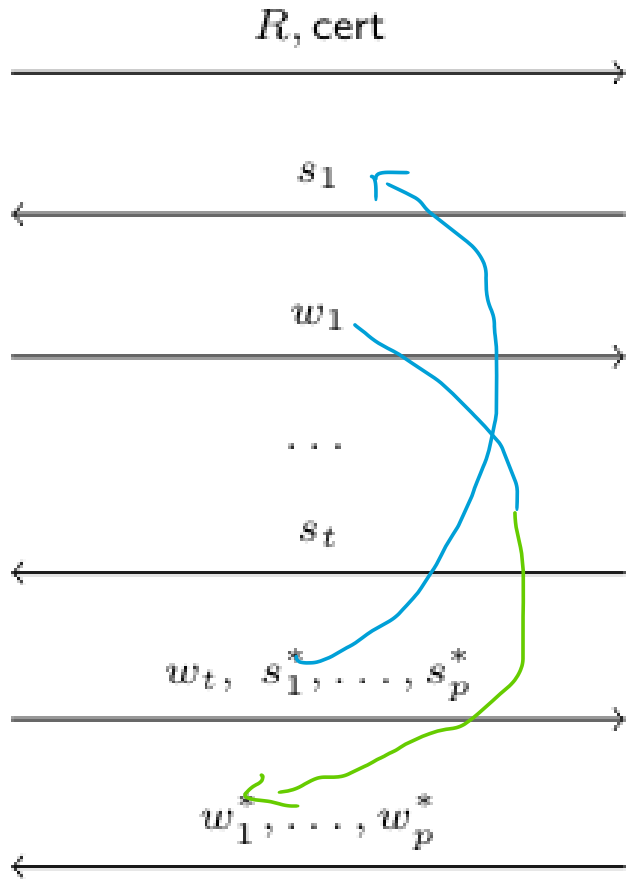
# Result 1: Proof Idea Meta-Reduction

$R$ is a Random Self-Reducible and Rerandomizable Relation (RRR)!


Simple Reduction

at least one LI query does not invoke a new ICA query




1) derive statements from challenge
2) rewind
3) query derived statements
4) compute witness to challenge from response
5) rerandomize witness

random self-reducibility and rerandomizability guarantee that derived statements are distributed as for ideal attacker

Simple Reduction responds with non-negligible prob correctly to all queries

# Dealing with General Reductions

- Problem 1: reduction might first send incorrect responses. Only if the attacker aborts it will rewind the attacker and send a correct response instead
  - Ideal attackers do always recognize incorrect responses
  - Meta-reduction may not be able to recognize incorrect responses after rewinding (e.g. when using RRRs based on Semi-Homomorphic PKE)
- Problem 2: reduction might generate $u$ instances of the attacker, run them concurrently, and make their behavior depend on each other
  - Can lead to exponential blow-up of runtime of meta-reduction

- Solution 1: use homomorphic MACs to help the meta-reduction recognize incorrect responses
- Solution 2: account for additive factor of -$u$ when bounding the number of queries in interactive complexity assumption

# Corollaries

- OW-CCA1 (IND-CCA1) security of ElGamal PKE (as well as any other Semi-Homomorphic PKE) forms hierarchy based on number of queries
- Similarly, the lunchtime security of Certified Homomorphic One-Way Bijections forms a hierarchy based on number of queries
  - Improves separation results for many one-more problems like one-more DLOG since challenges can now be decided on at the end of the security game!
- …

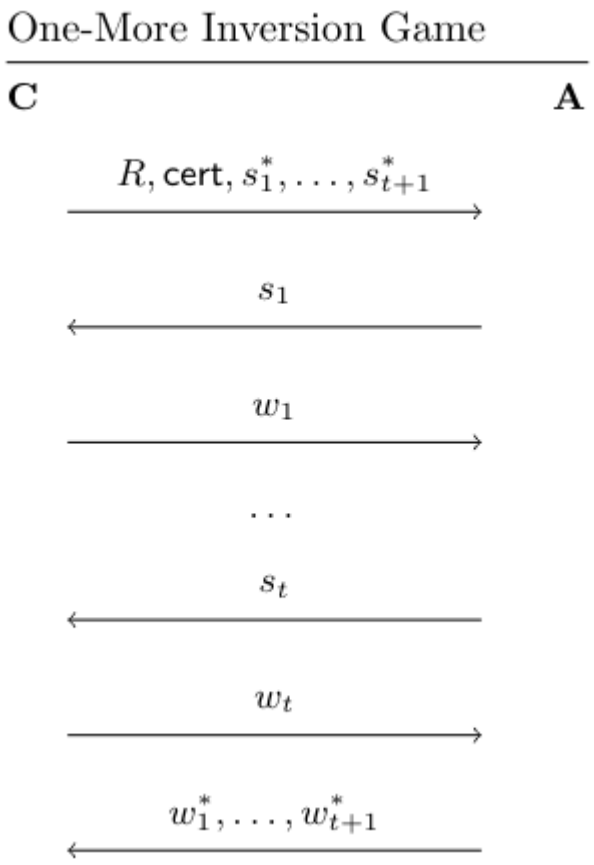
# Conclusion

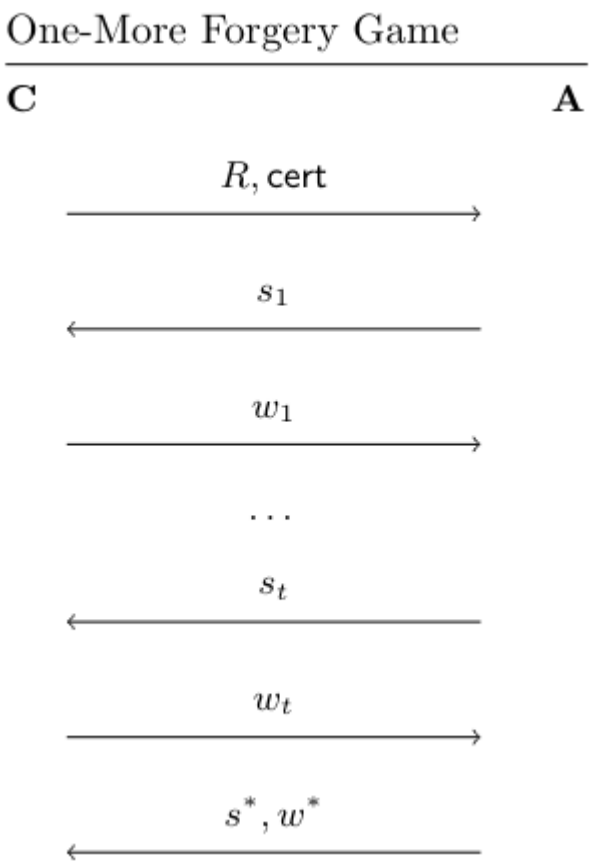
- Very broad impossibility result that has a plethora of applications in cryptography
- Results hold under the following mild conditions:
  - reduction treats inefficient attackers as black-box (but the attacker is unrestricted)
  - no use of idealized (non-committing) primitives like Programmable ROM
- Random self-reducibility is a double-edged sword in security proofs (often exploited for tighter security reductions)

# Thank you very much for your attention!

- Full paper: https://eprint.iacr.org/2024/795

# Previous Work




relation R (not necessarily RRR), statement s, and witness w