Doctoral Thesis

Photonics for THz quantum cascade lasers

Author(s):
Amanti, Maria I.

Publication Date:
2010

Permanent Link:

https://doi.org/10.3929/ethz-a-006213928 →

Diss. ETH No. 19204

Computational Indistinguishability Amplification

A dissertation submitted to

ETH ZURICH

for the degree of
Doctor of Sciences

presented by

Stefano Tessaro
MSc ETH CS, ETH Zurich

born July 4, 1981
citizen of Coldrerio, TI, Switzerland

accepted on the recommendation of

Prof. Dr. Ueli Maurer, examiner
Prof. Dr. Thomas Holenstein, co-examiner
Prof. Dr. Salil Vadhan, co-examiner

2010

Abstract

Computational security of cryptographic schemes is always shown under the (unproven) assumption that some underlying primitive is secure. In several important examples, the security of these primitives is defined in terms of *computational indistinguishability*, the property that two systems, despite possibly being very different, exhibit essentially the same behavior in the eyes of a computationally bounded observer. The most prominent example is a pseudorandom generator (PRG), an efficiently computable function stretching a short random secret seed into a longer string which is computationally indistinguishable from an equally long random string. Further examples are pseudorandom functions (PRFs) and permutations (PRPs), keyed functions and permutations which, under a random secret key, behave as a uniformly chosen function and permutation, respectively. Pseudorandom systems underlie essentially all efficient secret-key cryptographic schemes, and are frequent important components in public-key schemes and cryptographic protocols. Also, it is common to assume that block ciphers, such as the Advanced Encryption Standard (AES), are secure PRPs.

Yet computational indistinguishability is a strong requirement, and continuous progress in the development of cryptanalytic techniques casts some doubt as to whether such assumptions are any longer justified for existing designs. To this end, this dissertation addresses the fundamental question of basing efficient cryptography on primitives satisfying substantially weaker forms of computational indistinguishability. In particular, we refer to *computational indistinguishability amplification* as the problem of strengthening such primitives, and consider, throughout this work, two main axes along which amplification is achieved.

The first and main part of this thesis addresses the case where the observer is allowed to achieve some non-negligible (albeit quantitatively bounded) advantage over random guessing in distinguishing the two systems. By means of a series of general theorems, we undertake an in-depth investigation of the behavior of the computational distinguishing advantage under different forms of system composition, with the aim of finding efficient combination operations reducing the computational distinguishing advantage. All these results apply to the general class of systems whose state does not depend on the interaction, which comprises most cryptographic systems of interest. Our most important application is an exact characterization of the security amplification achieved by the cascade (i.e., sequential composition) of PRPs with respect to the distin-

guishing advantage, a long-standing open problem. (Even stronger amplification is shown under a minimal modification of the cascade.) Also, we provide a construction for security amplification of weak PRGs with optimal output length, as well as tighter and / or simpler proofs for all existing results in the literature in the context of advantage amplification.

A key technique is the generalization of complexity-theoretic results, such as Yao's XOR Lemma and Impagliazzo's Hardcore Lemma, to the setting of interactive systems, which is of independent interest. Also, most of our results can be interpreted as computational analogues of information-theoretic results, and help providing a better understanding of the intrinsic relationship between information-theoretic and computational security.

In contrast, the final part of this thesis is devoted to a weaker form of computational indistinguishability where the observer is only granted restricted access to the given system. In particular, we consider PRFs where computational indistinguishability only holds for observers which are allowed a bounded number (e.g., a constant as low as two) of random (but known) queries. We provide constructions of fully secure PRFs from such weaker PRFs that even improve on the efficiency of existing constructions in the literature based on the stronger assumption where observers are allowed any number of random queries. Our results yield efficient encryption schemes from block ciphers, and efficient message authentication codes from hash functions, both under such very weak pseudorandomness assumptions on the underlying primitives.

Riassunto

Ogni dimostrazione della sicurezza computazionale di uno schema crittografico si basa sull'assunzione, non dimostrata, che una primitiva, impiegata come componente, soddisfi a sua volta dei requisiti di sicurezza computazionale. La sicurezza di tali primitive viene spesso definita tramite il concetto di *indistinguibilità computazionale*, ossia la proprietà secondo la quale due sistemi crittografici, sebbene sostanzialmente diversi, presentino un comportamento pressoché identico nei confronti di osservatori la cui potenza di calcolo è limitata. L'esempio più comune è rappresentato dai cosiddetti *generatori pseudocasuali* (PRG), funzioni efficienti il cui output, dato un input segreto distribuito uniformemente, è computazionalmente indistinguibile da una stringa distribuita uniformemente e di lunghezza maggiore dell'input. Ulteriori esempi sono le *funzioni pseudocasuali* (PRF) e le *permutazioni pseudocasuali* (PRP), funzioni (e rispettivamente permutazioni), indicizzate da una chiave segreta, che sono indistinguibili da una funzione (o permutazione) scelta uniformemente dall'insieme di funzioni (o permutazioni) con il medesimo dominio. I sistemi pseudocasuali sono alla base di quasi tutti gli schemi efficienti in crittografia simmetrica, come pure di molti schemi nella crittografia a chiave pubblica e in protocolli crittografici. È inoltre comune assumere che i cosiddetti *block ciphers*, come l'Advanced Encryption Standard (AES), sono delle PRP.

L'indistinguibilità computazionale rimane tuttavia una properietà di sicurezza molto forte, e i continui progressi nello sviluppo di tecniche crittanalitiche mettono sempre più in dubbio la validità dell'assunzione che l'AES è una PRP. Pertanto, l'obbiettivo primario di questa dissertazione è uno studio dettagliato di soluzioni crittografiche efficienti basate su primitive che soddisfano unicamente forme ben più deboli di indistinguibilità computazionale. In particolar modo, studieremo il problema dell'amplificazione dell'indistinguibilità computazionale (*computational indistinguishability amplification*), ossia il problema di incrementare la sicurezza di queste primitive.

La prima (e maggior) parte di questa tesi si propone di studiare il caso dove è permesso all'osservatore, confrontato con il compito di distinguere due sistemi, raggiungere un *vantaggio* sostanziale (sebbene limitato quantitativamente) rispetto a una semplice scelta casuale. Attraverso una serie di teoremi generali, affronteremo un'analisi quantitativa del comportamento del vantaggio nel caso di diversi tipi di operazioni di composizione di sistemi: l'obbiettivo è di individuare esempi efficienti

di operazioni in grado di ridurre sostanzialmente tale vantaggio. Questi risultati sono applicabili a una classe generale di sistemi con uno stato iniziale arbitrario, che non viene però aggiornato nel corso dell'interazione, la quale comprende la maggior parte dei sistemi crittografici d'interesse. L'applicazione principale di questi risultati è una caratterizzazione esatta dell'amplificazione della sicurezza raggiunta dalla cascata (o composizione sequenziale) di PRP, un problema finora irrisolto. Inoltre, una minima modifica della cascata raggiunge un'amplificazione ottimale. Ulteriori applicazioni consistono in un nuovo metodo per incrementare la sicurezza di PRG deboli con un output di lunghezza ottimale, come pure analisi semplificate di tutti i risultati precedenti nel contesto dell'amplificazione del vantaggio.

Una tecnica chiave nello sviluppo di questi risultati, di interesse indipendente, consiste nella generalizzazione al contesto dei sistemi interattivi di risultati fondamentali come l'*XOR Lemma* di Yao e l'*Hardcore Lemma* di Impagliazzo. Inoltre, molti risultati di questa tesi sono interpretatabili come analoghi computazionali di teoremi precedentemente dimostrati nel contesto della sicurezza incondizionata (basata sulla teoria dell'informazione), e contribuiscono pertanto a una migliore comprensione della relazione fra i due tipi di sicurezza.

La seconda parte della tesi considera un indebolimento dell'indistinguibilità computazionale attraverso la limitazione dell'accesso. In modo particolare, studieremo funzioni pseudocasuali dove all'osservatore è unicamente permessa la valutazione presso un numero limitato (che può essere addirittura una costante maggiore o uguale a due) di input casuali. Il risultato principale di quest'ultima parte consiste in nuove costruzioni di PRF (per osservatori con valutazioni arbitrarie) da queste varianti di PRF deboli, la cui efficienza è addirittura superiore a quella di precedenti costruzioni richiedenti un'assunzione ben più forte dove il numero di valutazioni a input casuali non è limitato. Due conseguenze dirette sono un nuovo sistema di cifratura basato su *block ciphers*, come pure un nuovo metodo di autentificazione di messaggi a partire da funzioni di *hash*, entrambi basati unicamente su tali deboli assunzioni pseudocasuali.