

A Study on the Security of Privacy Homomorphism

Yu Yu, Jussipekka Leiwo, Benjamin Premkumar
Nanyang Technological University, School of Computer Engineering
Block N4, Nanyang Avenue, Singapore 639798

Abstract

Informally, Privacy Homomorphism (PH) refers to encryption schemes with a homomorphic property allowing to obtain $E_k(a + b)$ or $E_k(a \times b)$ from ciphertexts $E_k(a)$ and $E_k(b)$ without the knowledge of the decryption key. PH has a wide range of applications in information security due to its homomorphic property, but the best achievable security of them is yet unknown. In this paper, we discuss the security of PH in the black-box model and find that any PH is at most semantically secure under non-adaptive chosen-ciphertext attacks (i.e. IND-CCA1 secure). We also show that the IND-CCA1 security can be achieved with a small amount of hardware, namely, we offer a hardware-based solution to construct PH with provable security.

Keywords: privacy homomorphism, private computation, semantic security, chosen-ciphertext attacks, information security

1. Introduction

Privacy homomorphism (hereafter referred to as PH) is first introduced by Rivest et al. [19] as a tool for processing encrypted data. Basically, an additive PH is a tuple (G, E, D, \boxplus) of polynomial-time algorithms satisfying the following conditions:

1. On input 1^n , probabilistic key generator G outputs a pair of strings (e, d) , where n is the security parameter, e is the encryption key and d is the decryption key.
2. There exists a polynomially bounded function $\ell : \mathbb{N} \rightarrow \mathbb{N}$, called the block length, such that for every pair (e, d) produced by $G(1^n)$ and for every $x, y \in \{0,1\}^{\ell(n)}$, encryption algorithm E and decryption algorithm D satisfy

$$\Pr[D(d, E(e, x)) = x] = 1 \quad (1)$$

$$\Pr[D(d, \boxplus(E(e, x), E(e, y))) = x + y] = 1 \quad (2)$$

where "+" denotes addition over the plaintext space and the probability is taken over the internal coin tosses of E (note that D is deterministic).

The above definition does not distinguish between private-key block ciphers and public-key ones. In private-key schemes, e and d can be inferred from each other. Thus, for simplicity, we assume that $e=d=k$ and that k is kept secret. In public-key schemes, e is publicly known and it is computationally infeasible to infer d from e . In the rest of this paper, we write $E_e(x)$ instead of $E(e, x)$ and $D_d(c)$ instead of $D(d, c)$. Equations (1) and (2) are written in terms of probability since we do not distinguish probabilistic ciphers from deterministic ones. Analogously, we can define a multiplicative PH, (G, E, D, \boxtimes) , using almost the same definition as the additive PH except that (2) is replaced by (3)

$$\Pr[D_d(\boxtimes(E_e(x), E_e(y))) = x \times y] = 1 \quad (3)$$

where " \times " denotes multiplication over the plaintext space. If a PH, $(G, E, D, \boxplus, \boxtimes)$, is both additive and multiplicative (i.e., satisfies (1), (2) and (3)), it is called an algebraic PH.

PH would be useful in a number of applications such as secret sharing schemes, software protection, multiparty computation and electronic voting (e.g. [3, 20, 9, 8, 15]). Rivest et al. [19] have presented four basic PHs, which are later shown to be vulnerable to either ciphertext-only attacks or known-plaintext attacks [6]. Goldwasser and Micali [14] present a probabilistic additive PH (the GM crypto-system) with the block length $\ell(n)=1$ (i.e. regardless of the security parameter n) and it is semantically secure if the Quadratic Residuosity Assumption holds. More efficient GM crypto-system variants are proposed in [22, 4]. There are also other semantically secure additive PHs (e.g. [17, 18]) whose " \boxplus " simply takes as input two ciphertexts and outputs the product of them. Domingo-Ferrer [10, 11] proposed two algebraic PHs targeted at combating known-plaintext attacks and the corresponding cryptanalysis is given in [7, 2, 21].

Feigenbaum and Merritt [12] doubt the existence of secure algebraic PH. Ahituv et al. [1] show that any additive PH whose \boxplus is a simple addition function is insecure

under chosen-plaintext attacks and this result is sometimes mistakenly considered as the proof that no additive PH can be secure against chosen-plaintext attacks. Boneh and Lipton [5] show that any deterministic algebraic PH can be broken in sub-exponential time under a reasonable assumption. We stress that this result is not surprising since it is well-known that stateless deterministic encryption schemes are not secure under the standard privacy notion. Therefore, in spite of those negative results, the best achievable security of PH remains an open question.

In this paper, we explore the best achievable security of PH in the black-box model where only oracle access is allowed to the homomorphic functions \boxplus and \boxtimes . As shown in Figure 1, this can be achieved by implementing \boxplus and \boxtimes using a portable weak power device (e.g. a smart card) and thus it offers a hardware-based solution to construct secure PH. We show that the best achievable security of the resulting PH is semantic security under non-adaptive chosen-ciphertext attacks (IND-CCA1 security). Consequently, any PH (either hardware-based or algorithm-based) is at most IND-CCA1 secure.

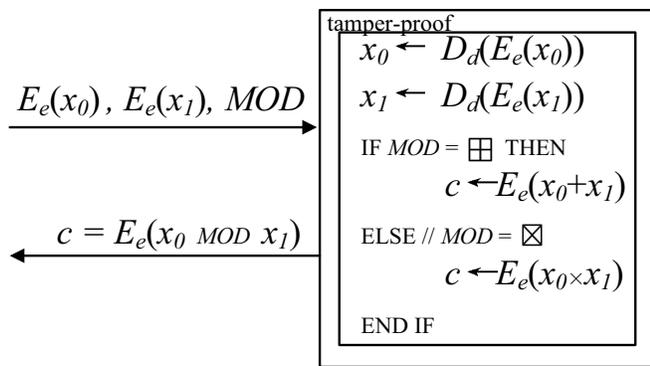


Figure 1. The oracle access to \boxplus (resp., \boxtimes) can be emulated by a tamper-proof device that takes $E_e(x_0)$ and $E_e(x_1)$ as argument, decrypts them and outputs the encrypted sum (resp., product) of x_0 and x_1 .

2. IND-CCA1 Secure Block Ciphers

In this section, we introduce the notion of IND-CCA1 security and point out that block ciphers of this type exist under reasonable assumptions.

Informally, a block cipher is IND-CCA1 secure if and only if it has indistinguishable encryptions¹ (i.e. IND) and it is secure under nonadaptive chosen-ciphertext attacks

¹In most cases, indistinguishability of encryptions is equivalent to semantic security. Thus, we use IND as the shorthand for semantic security.

(i.e. CCA). IND-CCA1 security can be described using a "guess" game between an adversary Malice and an oracle \mathcal{O} [16, Protocol 14.1]:

- Game 1.**
1. \mathcal{O} and Malice agree on a target (G, E, D) and \mathcal{O} chooses a pair of keys by $(e, d) \leftarrow G(1^n)$, where the encryption key e is revealed to Malice if (G, E, D) is a public-key encryption scheme.
 2. \mathcal{O} allows Malice to have oracle access to E_e and D_d . After several rounds, they proceed to the next step.
 3. Based on the information achieved, Malice selects two distinct messages x_0 and x_1 of the same length and sends them to \mathcal{O} .
 4. \mathcal{O} tosses a fair coin $b \in_U \{0, 1\}$ and selects a value c^* from the distribution of $E_e(x_b)$.
 5. After receiving c^* , Malice can only have oracle access to E_e . Then, Malice guesses b by answering either 0 or 1.

If Malice has no strategy to win Game 1 better than random guessing, then (G, E, D) is IND-CCA1 secure for any single message. We stress that the single-message IND-CCA1 security is equivalent to the multiple-message one in which multiple messages are encrypted [13, Section 5.4.4.1]. The rigorous definition for IND-CCA1 is given by Goldreich as follows [13, Definition 5.4.14]:

Definition 1. (indistinguishability of encryptions under non-adaptive chosen-ciphertext attacks):

For public-key schemes: A public-key block cipher, (G, E, D) , is said to be **IND-CCA1 secure** if for every pair of probabilistic polynomial oracle machines, A_1 and A_2 , for every positive polynomial p , and all sufficiently large n and $z \in \{0, 1\}^{\text{poly}(n)}$ it holds that

$$|p_{n,z}^{(0)} - p_{n,z}^{(1)}| < \frac{1}{p(n)}$$

where

$$p_{n,z}^{(i)} \stackrel{\text{def}}{=} \Pr \left[\begin{array}{l} v = 0, \text{ where} \\ ((x_0, x_1), \sigma) \leftarrow A_1^{E_e, D_d}(e, z) \\ c^* \leftarrow E_e(x_i) \\ v \leftarrow A_2^{E_e}(\sigma, c^*) \end{array} \right]$$

$(e, d) \leftarrow G(1^n)$, $|x_0| = |x_1| = n$ and the probability is taken over the internal coin tosses of G , E_e , A_1 and A_2 .

For private-key schemes: The definition is identical except that A_1 gets the security parameter 1^n instead of the encryption key e .

In the above definition, adversary Malice is decoupled into a pair of oracle machines $(A_1^{E_e, D_d}, A_2^{E_e})$. That is, A_1 has oracle access to both E_e and D_d (see the step 2 of Game 1) while A_2 is restricted to E_e (step 5). In the joint work of A_1 and A_2 , σ denotes the state information A_1 passes to A_2 . Since we use non-uniform formulations z is a non-uniform auxiliary input of A_1 (A_2 's counterpart is included in σ). Finally, A_2 outputs v as its guess.

We can construct block ciphers that is IND-CCA1 secure under reasonable assumptions, e.g., the private-key IND-CCA1 secure block cipher in [13, Construction 5.4.19] and the public-key one in [13, Construction 5.4.23]. In both cases, the encryption function E_e is probabilistic (or stateful deterministic), namely, if we invoke E_e on the same input x polynomially (in n) many times, its outputs will be different from each other with an overwhelming probability. Otherwise, Malice can win Game 1 with ease. In practice, \boxplus (resp., \boxtimes) can be emulated by tamper-proof hardware that takes as input two ciphertexts $E_e(m_1)$ and $E_e(m_2)$ and outputs $E_e(m_1+m_2)$ (resp., $E_e(m_1 \times m_2)$) by invoking E_e and D_d . Such hardware can be smart cards as some smart cards can do both private-key encryptions and public-key encryptions with the help of cryptographic co-processors.

3. IND-CCA1 Secure PH

In this section, we assume an IND-CCA1 secure block cipher (G, E, D) having oracle access to \boxplus and \boxtimes and prove that the resulting PH, $(G, E, D, \boxplus, \boxtimes)$, preserves IND-CCA1 security. Analogously, the IND-CCA1 security for PH $(G, E, D, \boxplus, \boxtimes)$ can be modeled with Game 2:

Game 2. 1. \mathcal{O} and Malice agree on a target $(G, E, D, \boxplus, \boxtimes)$ and \mathcal{O} chooses a pair of keys by $(e, d) \leftarrow G(1^n)$, where the encryption key e is revealed to Malice if (G, E, D) is a public-key encryption scheme.

2. \mathcal{O} allows Malice to have oracle access to E_e, D_d, \boxplus and \boxtimes . After several rounds, they proceed to the next step.
3. Based on the information achieved, Malice selects two distinct messages x_0 and x_1 of the same length and sends them to \mathcal{O} .
4. \mathcal{O} tosses a fair coin $b \in_U \{0, 1\}$ and selects a value c^* from the distribution of $E_e(x_b)$.
5. After receiving c^* , Malice is only allowed to have oracle access to E_e, \boxplus and \boxtimes . After that, Malice guesses b by answering either 0 or 1.

Thus, the formal definition of IND-CCA1 security for $(G, E, D, \boxplus, \boxtimes)$ is almost same as Definition 1 except

that the pair of oracle machines is $(A_1^{E_e, D_d, \boxplus, \boxtimes}, A_2^{E_e, \boxplus, \boxtimes})$ instead of $(A_1^{E_e, D_d}, A_2^{E_e})$.

We proceed to proving that an IND-CCA1 secure (G, E, D) preserves the same security when we allow adversaries to have additional oracle access to \boxplus and \boxtimes . Before presenting the formal proof, we sketch it informally in Figure 2. By definition, (G, E, D) is IND-CCA1 secure iff no polynomial-time adversary can win Game 1 better than random guessing. Note that the only difference between Game 1 and Game 2 is that in the latter case Malice can have oracle access to \boxplus and \boxtimes (see step 2 and step 5). We will show that the oracle access to $(E_e, D_d, \boxplus, \boxtimes)$ in step 2 is equivalent to accessing only (E_e, D_d) . In addition, the oracle access to $(E_e, \boxplus, \boxtimes)$ can be made computationally indistinguishable to accessing only E_e by emulating \boxplus and \boxtimes with E_e . Recall that the indistinguishable property (i.e. IND) implies that any polynomial-time adversary is unable to distinguish between any pair of distinct ciphertexts, e.g., $E_e(t_n)$ and $E_e(0)$.

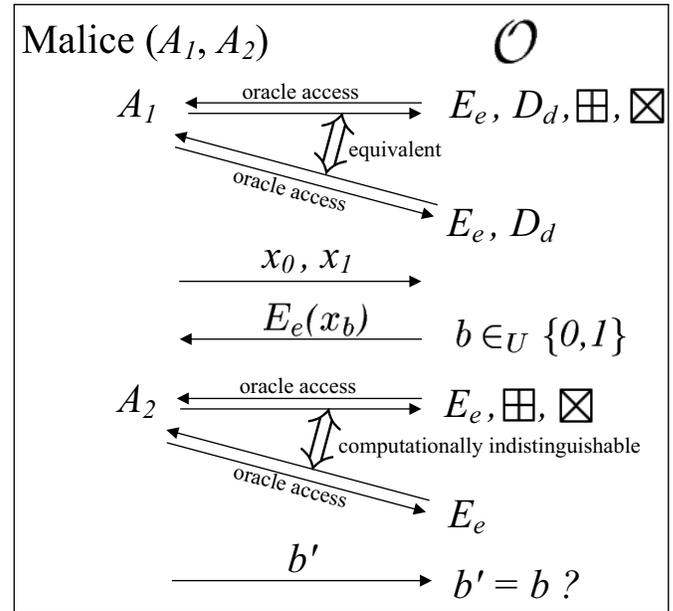


Figure 2. The proof sketch.

Lemma 1. (Indistinguishability between $E_e(t_n)$ and $E_e(0)$):

For public-key schemes: Let (G, E, D) be an IND-CCA1 secure public-key (resp., private-key) block cipher, then for every plaintext $t_n \in \{0, 1\}^n$, for every pair of probabilistic polynomial oracle machines A_1 and A_2 , every positive polynomial p , all sufficiently large n 's and $z \in \{0, 1\}^{poly(n)}$, it holds that

$$|p_{n,z}^{(0)} - p_{n,z}^{(1)}| < \frac{1}{p(n)}$$

where

$$p_{n,z}^{(i)} \stackrel{\text{def}}{=} \Pr \left[\begin{array}{l} v = 0, \text{ where} \\ \sigma \leftarrow A_1^{E_e, D_d}(e, z) \\ c^* \leftarrow \begin{cases} E_e(0), & i = 0 \\ E_e(t_n), & i = 1 \end{cases} \\ v \leftarrow A_2^{E_e}(\sigma, c^*) \end{array} \right]$$

$(e, d) \leftarrow G(1^n)$ and the probability is taken over the internal coin tosses of G, E_e, A_1 and A_2 .

For private-key schemes: The indistinguishability also holds except that A_1 gets the security parameter 1^n instead of the encryption key e .

Proof sketch. For the sake of contradiction, we assume that $E_e(t_n)$ and $E_e(0)$ are distinguishable by $A_2^{E_e}$ within polynomial time. It follows that Definition 1 does not hold in case that $x_0=0$ and $x_1=t_n$, which contradicts the fact that (G, E, D) is IND-CCA1 secure. \square

Theorem 1. (IND-CCA1 secure PH): Let (G, E, D) be an IND-CCA1 secure block cipher, let \boxplus and \boxtimes be as in (2) and (3) respectively and assume that only oracle access is allowed to \boxplus and \boxtimes , then the PH $(G, E, D, \boxplus, \boxtimes)$ is also IND-CCA1 secure.

Proof. As discussed, we only need to prove that Definition 1 still holds if we replace $(A_1^{E_e, D_d}, A_2^{E_e})$ by the corresponding $(A_1^{E_e, D_d, \boxplus, \boxtimes}, A_2^{E_e, \boxplus, \boxtimes})$. The equivalence of $A_1^{E_e, D_d}$ and $A_1^{E_e, D_d, \boxplus, \boxtimes}$ is quite straightforward since either \boxplus or \boxtimes is implied by E_e and D_d . In other words, \mathcal{O} can efficiently emulate \boxplus (resp., \boxtimes) by decrypting the input ciphertexts, computing the sum (resp., product) of the corresponding plaintexts and encrypting the result. The remaining difficulty is the reduction from $A_2^{E_e, \boxplus, \boxtimes}$ to $A_2^{E_e}$. Obviously, the input-output behaviors of \boxplus and \boxtimes cannot be emulated using only E_e , but \mathcal{O} can implement a function $\mathcal{O}^{+, \times}$ using E_e such that their input-output behaviors are computationally indistinguishable to those of \boxplus and \boxtimes . For example, we can let $\mathcal{O}^{+, \times}$ be as follow:

$$\mathcal{O}^{+, \times}(E_e(x_0), E_e(x_1)) \{ \\ \text{return } E_e(0); \\ \}$$

By the definition of \boxplus and \boxtimes , it holds that

$$\boxplus(E_e(x_0), E_e(x_1)) \{ \\ \text{return } E_e(x_0 + x_1); \\ \}$$

$$\boxtimes(E_e(x_0), E_e(x_1)) \{ \\ \text{return } E_e(x_0 \times x_1); \\ \}$$

By Lemma 1, $A_2^{E_e}$ cannot distinguish between $E_e(0)$ and $E_e(x_0 + x_1)$ (or $E_e(x_0 \times x_1)$), namely, whatever can be efficiently computed from the oracle access to \boxplus and \boxtimes can also efficiently computed from scratch. Thus, replacing (\boxplus, \boxtimes) by $\mathcal{O}^{+, \times}$ has no effect on the decision of A_2 and as a result, $A_2^{E_e, \boxplus, \boxtimes}$ and $A_2^{E_e, \mathcal{O}^{+, \times}}$ compute almost the same function (with a negligible difference). Therefore, it suffices that $A_2^{E_e, \mathcal{O}^{+, \times}}$ can be reduced to $A_2^{E_e}$ in a computational sense and the conclusion immediately follows. \square

In the above proof, we make use of the simulation paradigm, namely, if the view of an adversary can be efficiently simulated by a PPT from scratch (or what the adversary already knows), then the adversary gain nothing substantial from his view. The knowledge of \boxplus and \boxtimes only allows him to produce semantically correlated ciphertext triplets $(E_e(x_0), E_e(x_1), E_e(x_0 + x_1))$ and $(E_e(x_0), E_e(x_1), E_e(x_0 \times x_1))$, but does not help to distinguish between $E_e(x_0)$ and $E_e(x_1)$ for any distinct x_0 and x_1 . In addition, we note that E_e is probabilistic and hence Malice cannot even distinguish between the two instances of $E_e(x)$, where x is an arbitrary plaintext. Thus, Malice cannot tell whether two ciphertexts have the same semantics.

4. Beyond IND-CCA1 Security

We have shown that it is possible to obtain IND-CCA1 secure PH given only oracle access to \boxplus and \boxtimes . In this section, we show that IND-CCA1 is the best achievable security for any PH, namely, any security beyond IND-CCA1 is not attainable.

4.1. Non-Malleable Security

Informally, IND security against some-type attacks requires that the ciphertexts reveal nothing to passive adversaries conducting the some-type attacks, where "some-type" can be ciphertext-only, chosen-plaintext, chosen-ciphertext, etc. This notion is enough in most cases where the adversary only hopes to gain the information from ciphertexts, but it does not prevent Malice from replacing the ciphertext with a semantically related one. Let us consider the well-known private key encryption of the one-time pad (Vernam cipher). Given an n -bit message $m=m_1 \cdots m_n$, the key generator outputs an n -bit key $k=k_1 \cdots k_n$ uniformly chosen from $\{0,1\}^n$. The encryption is done by bitwise XORing m_i with k_i , that is, for $1 \leq i \leq n$, $c_i = m_i \oplus k_i$. It is well-known that this cipher is unconditionally secure in that ciphertexts disclose nothing (except the length n) in an information-theoretic sense. However, the cipher is malleable. Malice is able to flip each c_i by replacing c_i with $c'_i = c_i \oplus 1$ such that the one that decrypts c'_i will get the com-

plement of m_i . In this way, Malice can flip the semantics of each ciphertext.

$(G, E, D, \boxplus, \boxtimes)$ is also malleable. Given any plaintext-ciphertext pair $(a, E_e(a))$ with $a \neq 0$ (resp., $a \neq 1$), Malice is able to increment (resp., multiply) by a the semantics of any ciphertext c by replacing c with c' , where $c' \leftarrow \boxplus(c, E_e(a))$ (resp., $c' \leftarrow \boxtimes(c, E_e(a))$). Therefore, non-malleable (NM) security is not achievable for any PH. Although there are techniques (e.g. message authentication code) that prevents active adversaries from faking any valid ciphertext, these techniques contradict the definition of PH by which any party is allowed to create valid ciphertext using existing ciphertexts and \boxplus (or \boxtimes).

4.2. Security under Adaptive Chosen-Ciphertext Attacks

So far, we know that $(G, E, D, \boxplus, \boxtimes)$ cannot have NM security. That is, it is at most IND secure against some-type attacks and this "some-type" can be CCA. However, can this "some-type" be something more advanced? In other words, can $(G, E, D, \boxplus, \boxtimes)$ be IND secure under adaptive chosen-ciphertext attacks (CCA2)? To answer this question, we first model the notion of IND-CCA2 security for PH with the following game:

Game 3. 1. \mathcal{O} and Malice agree on a target $(G, E, D, \boxplus, \boxtimes)$ and \mathcal{O} chooses a pair of keys by $(e, d) \leftarrow G(1^n)$, where the encryption key e is revealed to Malice if (G, E, D) is a public-key encryption scheme.

2. \mathcal{O} allows Malice to have oracle access to E_e , D_d , \boxplus and \boxtimes . After several rounds, they proceed to the next step.
3. Based on the information achieved, Malice selects two distinct messages x_0 and x_1 of the same length and sends them to \mathcal{O} .
4. \mathcal{O} tosses a fair coin $b \in_U \{0, 1\}$ and selects a value c^* from the distribution of $E_e(x_b)$.
5. Upon receiving c^* , Malice is only allowed to have oracle access to E_e , D_d , \boxplus and \boxtimes with the exception that the decryption query of c^* will be denied. Then, Malice guesses b by answering either 0 or 1.

Now we show that Malice can always win Game 3 efficiently. For any c^* , Malice decrypts it using \boxplus (or \boxtimes) to obtain b with the following steps:

1. Malice queries E_e with 0 (resp., 1) to receive $E_e(0)$ (resp., $E_e(1)$).
2. Malice queries \boxplus (resp., \boxtimes) with c^* and $E_e(0)$ (resp., $E_e(1)$) to obtain c^{**} .

3. Malice queries D_d with c^{**} to obtain x_b .
4. Malice determines b by looking up x_b in (x_0, x_1) .

To conclude, no matter how secure (G, E, D) is, the homomorphic property of \boxplus or \boxtimes will make the PH vulnerable under CCA2. Thus, the best achievable security of PH is no more than IND-CCA1 security.

5. Concluding Remarks

We have shown that any PH (additive or multiplicative or both) can be at most IND-CCA1 secure in the black-box model, but it still remains an open question whether IND-CCA1 security is a tight upper bound for algorithm-based PH. Nevertheless, we can construct IND-CCA1 secure hardware-based PH using low-cost portable devices (e.g. smart cards with cryptographic co-processors) and they might be useful in applications where no algorithm-based solution is available. For example, in software protection, most algorithm-based solutions are heuristic and have no complexity-theoretic foundations. Thus, with hardware-based PH, we can use a small amount of hardware to achieve provable security.

References

- [1] N. Ahituv, Y. Lapid, and S. Neumann. Processing encrypted data. *Communications of the ACM (CACM)*, 30(9):777–780, 1987.
- [2] F. Bao. Cryptanalysis of a provable secure additive and multiplicative privacy homomorphism. In *Proceedings of the International Workshop on Coding and Cryptography (WCC 2003)*, pages 43–50, 2003.
- [3] J. C. Benaloh. Secret sharing homomorphisms: Keeping shares of a secret sharing. In *Advances in Cryptology - CRYPTO '1986*, pages 251–260. Springer-Verlag, 1986.
- [4] M. Blum and S. Goldwasser. An efficient probabilistic public-key encryption scheme which hides all partial information. In *Advances in Cryptology - CRYPTO '1984*, pages 289–302. Springer-Verlag, 1984.
- [5] D. Boneh and R. J. Lipton. Algorithms for black-box fields and their application to cryptography (extended abstract). In *Advances in Cryptology - CRYPTO 1996*, pages 283–297. Springer-Verlag, 1996.
- [6] E. F. Brickell and Y. Yacobi. On privacy homomorphisms (extended abstract). In *Advances in Cryptology - EUROCRYPT '1987*, pages 117–125. Springer-Verlag, 1987.
- [7] J. H. Cheon and H. S. Nam. A cryptanalysis of the original domingo-ferrer's algebraic privacy homomorphism. Cryptology ePrint Archive, Report 2003/221, 2003. <http://eprint.iacr.org/>.
- [8] R. Cramer, I. Damgård, and J. B. Nielsen. Multiparty computation from threshold homomorphic encryption. In *Advances in Cryptology - EUROCRYPT '2001*, pages 280–299. Springer-Verlag, 2001.

- [9] R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multi-authority election scheme. In *Advances in Cryptology - EUROCRYPT '1997*, pages 103–118. Springer-Verlag, 1997.
- [10] J. Domingo-Ferrer. A new privacy homomorphism and applications. *Information Processing Letters*, 60(5):277–282, 1996.
- [11] J. Domingo-Ferrer. A provably secure additive and multiplicative privacy homomorphism. In *Proceedings of the 5th International Conference on Information Security (ISC 2002)*, pages 471–483. Springer-Verlag, 2002.
- [12] J. Feigenbaum and M. Merritt. Open questions, talk abstracts, and summary of discussions. In *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, volume 2, pages 1–45, 1991.
- [13] O. Goldreich. *Foundations of Cryptography: Basic Applications*, volume 2. Cambridge University Press, 2004.
- [14] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.
- [15] A. Kiayias and M. Yung. The vector-ballot e-voting approach. In *Financial Cryptography (FC 2004)*, pages 72–89. Springer-Verlag, 2004.
- [16] W. Mao. *Modern Cryptography: Theory and Practice*. Prentice Hall PTR, 2004.
- [17] T. Okamoto and S. Uchiyama. A new public-key cryptosystem as secure as factoring. In *Advances in Cryptology - EUROCRYPT '1998*, pages 308–318. Springer-Verlag, 1998.
- [18] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Advances in Cryptology - EUROCRYPT 1999*, pages 223–238. Springer-Verlag, 1999.
- [19] R. L. Rivest, L. M. Adleman, and M. L. Dertouzos. On data banks and privacy homomorphisms. *Foundations of Secure Computation*, pages 169–180, 1978.
- [20] T. Sander and C. F. Tschudin. Towards mobile cryptography. In *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE CS Press, 1998.
- [21] D. Wagner. Cryptanalysis of an algebraic privacy homomorphism. In *Proceedings of the 5th International Conference on Information Security (ISC 2003)*, pages 234–239. Springer-Verlag, 2003.
- [22] A. C. Yao. Theory and applications of trapdoor functions. In *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (FOCS 1982)*, pages 80–91. IEEE CS Press, 1982.