Public Key Cryptosystems with Partial Secrecy

Judy Goldsmith[1] and Andrew Klapper[2]
Department of Computer Science
University of Kentucky
Lexington, KY 40506-0046
{goldsmit,klapper}@cs.engr.uky.edu

February 6, 1996

[1]Project sponsored in part by NSERC operating grant OGP0121527, and NSF grant CCR-9315354.

[2]Project sponsored in part by NSERC operating grant OGP0121648, the National Security Agency under Grant Number MDA904-91-H-0012, and the National Science Foundation under grant number NCR-9400762. The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation hereon.

Abstract

Yamamota's notion of partial secrecy is extended to Public Key Cryptosystems: the security of a cryptosystem depends on keeping some function of the original record secret, while sending the relevant message (also a function of the original record). Notions of security and semantic security are introduced and compared for such cryptosystems, and security-preserving reductions between such systems are described.

1 Introduction

A cryptosystem is generally considered secure if a sender can transmit messages across an insecure channel and expect that the intended receiver will decode them, but no eavesdropper can recover them. A cryptosystem is called *semantically secure* if an eavesdropper can't use the encrypted messages to compute anything about the original messages any better than she could without the encryption.

In reality, most messages that are encrypted contain some information that is important to hide from eavesdroppers, and some that is common knowledge. It is possible that a cryptosystem may be considered secure, yet may give away partial information about the messages sent – even crucial information. The standard (nonsemantic) notions of security are too weak to protect against this. Semantic security is, in different senses, both too strong and too weak. On the one hand it attempts to protect confidentiality of *all* partial information about a message. On the other hand it only guarantees that no eavesdropper can do significantly better than an adversary who does not see the cipher text – calling a system secure if it gives away information to such an oblivious adversary.

In order to discuss the notion that *certain* information about a message may be crucial to hide from eavesdroppers, we introduce a function, f, the *secret function.* If we assume that $s = f(m)$ is the information about the message that we need to keep secret, we can then begin to design cryptosystems that specifically protect that information. In this paper, we consider public key encryption of messages, where the encryption is considered secure if no eavesdropper can deduce the associated secrets.

Diffie and Hellman introduced the notion of public key cryptography in 1976, to allow encryption using shorter keys than are possible with private key cryptography [3]. More recently, Yamamoto showed that some of the information-theoretic bounds on the length of the key for private key cryptography could be overcome by considering cryptosystems that only depended on keeping certain information secret, rather than entire messages [9]. We extend Yamamoto's idea to public key cryptography.

Several authors have classified levels of security for public key cryptosystems (PKCSs). For example, Goldwasser and Micali [5] defined the notions of semantic security and probabilistic encryption. Micali, Rackoff, and Sloan [7] and Goldreich [4] then showed that semantic security was equivalent to indistinguishability. Naor and Yung [8] used noninteractive zero knowledge proofs [1] to transform secure PKCSs into PKCSs secure against chosen plaintext attack.

Currently, all known public key cryptosystems depend on the intractibility of particular problems. For example, Blum and Goldwasser [2] described a probabilistic encryption scheme which is secure if factoring is hard. We hope that, by relaxing the requirement that the encryption hide all information about the message, researchers may find provably secure public key cryptosystems, or cryptosystems whose security depends on weaker assumptions. Further, we define security-preserving reductions between cryptosystems. This allows *classes* of cryptosystems, rather than individual cryptosystems, to be proved secure or insecure, relative to various measures of security.

The model we actually consider is a further generalization of the original model of public key cryptosystems. We assume that the sender has a collection of *records,* and associated with each record is the information that the sender wishes to transmit, the *message,* and the information that the sender wishes to keep hidden from eavesdroppers, the *secret.* Our model thus has three sets, R, M, and S, and functions $f : R \to S$ and $g : R \to M$, mapping records to their respective secrets and messages. We call the tuple of (R, M, S, f, g) a *secrecy system.*

One simple example is a record space consisting of bank account histories. The message (sent to instant teller machines) is the name and current status of an account, the secret might be the entire transaction history. Another example is the record space of student records. The messages may be transcripts, and the secrets payment history, library fines, or misdemeanor records.

In this paper, we

1. propose a model of public key cryptography, based on secrecy systems;
2. define and contrast various notions of security;
3. define security-preserving reductions between secrecy systems, so that results about one system may be applied to entire classes of systems;
4. give a variety of examples of secrecy systems for which secure public key cryptosystems exist, or don't exist, for various types of security; and
5. show that the classical secrecy system (messages = records = secrets) is not "complete" relative to reductions preserving standard security, but is complete relative to reductions preserving semantic security.

We precisely characterize several notions of security for secrecy systems, depending in part on the size of the set of records on which an adversary must be successful, in order to consider the security cracked. We generally assume that records are generated according to a distribution in terms of which we measure the sizes of sets of records, and that the size of the record (or the security parameter) in question is efficiently computable by the receiver and eavesdropper.

The types of security include weak security, in which the adversary must succeed on all records; weak polynomial fractional security, in which the adversary must succeed on a polynomial fraction of the records for each key; and polynomial fractional security in which the adversary must succeed on a polynomial fraction of the keys and records. We also consider both deterministic and probabilistic encryption, and both standard security and semantic security.

In Section 3 we investigate the relative security of secrecy systems. Our basic tool is a notion of reduction between secrecy systems, a triple of functions mapping records to records, secrets to secrets, and messages to messages. We show that for a certain class of reductions, the security of one system implies the security of another. This provides a framework for constructing secure PKCSs for many secrecy systems, given a secure PKCS for one. We have results of this type for both standard and semantic security, although the notions of reductions are slightly different. In the case of semantic security, we conclude that if the "classical" secrecy system has a secure PKCS, then all secrecy systems do – a type of completeness result.

In Section 4 we give several examples of the existence and nonexistence of secure PKCSs. For example, if the secret function is constant on a P-printable set, and one-to-one elsewhere, then weak security is impossible. We also give examples of (1) a PKCS which is secure but not semantically secure; (2) a PKCS which is semantically secure but not secure; and (3) a secrecy system that cannot reduce to the classical secrecy system, showing that the classical system is not complete under this reduction. Finally, we observe that two secrecy systems are secure if and only if their join is.

2 Definitions

In this section we describe the structures – secrecy systems – whose security we study. We define several notions of security for these systems. In what follows, an ensemble, X, is a family of finite sets of strings $\{X_n\}$ indexed by a positive integer n. (The finite sets may be distinguished by the size of their elements, or by the level of security required in the transmission of their elements; n is called the *security parameter*.) A function $f : X \to Y$ between ensembles is a family of functions $f_n : X_n \to Y_n$. It is p-time computable if there is a p-time transducer T which on input $\langle x, 1^n \rangle$, $x \in X_n$, computes $f_n(x)$.

Definition 2.1 *A* secrecy system *is a 5-tuple (R, S, M, f, g) where R, S, and M are ensembles (records, secrets, and messages), and $f : R \to S$ and $g : R \to M$ are p-time computable.*

A user has a set of records. Each record $r \in R$ has an associated secret $f(r) \in S$. The user wants to send messsage $g(r) \in M$ without revealing $f(r)$ to an eavesdropper.

Definition 2.2 *A* public key cryptosystem (PKCS) *for (R, S, M, f, g) consists of*

1. *a key source, G, which generates key pairs (k_1, k_2) in an ensemble $K \subset K^1 \times K^2$, the key set;*
2. *the cipher set, C, an ensemble;*
3. *the encryption algorithm, $E : R \times K^1 \to C$;*
4. *the decryption algorithm, $D : C \times K^2 \to M$.*

The key source, G, is a probabilistic p-time algorithm which on input 1^n generates elements of K_n uniformly at random. Any pair (k_1, k_2) in K is called a valid key pair. If (k_1, k_2) is a valid key pair, k_1 is the public key and k_2 is the private key. The encryption algorithm, E, is a p-time computable encryption algorithm, which may be deterministic or probabilistic (i.e., $E : X \times R \times K^1 \rightarrow C$ for some ensemble, X, of random strings). The decryption algorithm, D, is a p-time computable deterministic algorithm. If $(k_1, k_2) \in K_n$ is a key pair, and $r \in R_n$ is a record, then r, encrypted by k_1, must give $g(r)$ when decrypted with k_2. I.e., $D(E(r, k_1), k_2) = g(r)$. If E is probabilistic, this should hold for all random strings.

2.1 Security

A secrecy system is insecure when an adversary or eavesdropper can compute the associated secrets for many, most, or all messages (depending on the desired type of security). We define the notions of "many" and "most" according to the following parameters.

The sizes of the sets of records and keys on which an adversary must succeed can be varied. Records may be generated by a source according to a distribution δ. That is, for each security parameter n, there is a probability distribution δ_n on R_n. A system may be secure relative to a particular distribution or to all distributions in some set. When r is chosen according to distribution δ we write $r \in_\delta R$. We let π be the uniform distribution on any ensemble. The set of security parameters n on which a successful adversary must crack the system can be varied. With almost everywhere (a.e.) security, the adversary must succeed for all but finitely many n. With infinitely often (i.o.) security, the adversary need only succeed for infinitely many n. All results apply to both a.e. or i.o. security unless otherwise stated. In practice, we expect that the size of R_n is exponential in n.

Definition 2.3 *Let $\mathbf{P} = (C, K, E, D, G)$ be a PKCS for $\mathbf{R} = (R, S, M, f, g)$. Let $B : C \times K^1 \rightarrow S$. Then B* cracks $\mathbf{P}$ *at $r \in R$, $k = (k_1, k_2) \in K$ if $B(E(r, k_1), k_1) = f(r)$. If E is probabilistic with random strings X, B may be probabilistic with random strings Y, so $B : Y \times C \times K^1 \rightarrow S$. Then B* cracks $\mathbf{P}$ at *y, x, r, k if $B(y, E(x, r, k_1), k_1) = f(r)$. If δ is a distribution on R, then*

1. *B* strongly cracks $\mathbf{P}$ *if $\forall r \in R_n, k \in K_n : B$ cracks $\mathbf{P}$ at r, k.*

2. *B* strongly polynomial fractionally cracks $\mathbf{P}$ relative to *δ if there is a polynomial $p(n)$ such that $\forall k \in K_n : Prob\{B$ cracks $\mathbf{P}$ at $k\} > 1/p(n)$. The probability is over $r \in_\delta R_n$ if B is deterministic, and over $y \in_\pi Y_n$, $x \in_\pi X_n$, and $r \in_\delta R_n$ if B is probabilistic.*

3. *B* polynomial fractionally cracks $\mathbf{P}$ relative to *δ if there is a polynomial $p(n)$ such that $Prob\{B$ cracks $\mathbf{P}\} > 1/p(n)$. The probability is over $k \in_\pi K_n$ and $r \in_\delta R_n$ if B is deterministic, and over $y \in_\pi Y_n$, $x \in_\pi X_n$, $k \in_\pi K_n$, and $r \in_\delta R_n$ if B is probabilistic.*

4. B non-sparsely cracks $\mathbf{P}$ *if for every polynomial* $p(n)$, $\exists N \forall n > N \forall k \in K_n |\{r \in R_n : B \text{ cracks } \mathbf{P} \text{ at } r, k\}| > p(n)$.

In each case, n is a.e. or i.o., as appropriate.

Note that for any $\mathbf{P}$ and polynomial $q(n)$ there is a B that, for every k, cracks $\mathbf{P}$ on a set of size at least $q(n)$. Specifically,

B: input $c \in C_n$, $k_1 \in K_n^1$
  for each of the lexicographically first $q(n)$ elements r of R_n do
    if $E(r, k_1) = c$ then
      output $f(r)$ and halt
  od

This is a generalization of an attack due to Grollmann and Selman [6]. Thus resistance to non-sparse cracking is the most we can hope for.

Security can now be defined in terms of resistance to these attacks.

Definition 2.4 *Let* $\mathbf{R} = (R, S, M, f, g)$ *be a secrecy system, let* $\mathbf{P} = (C, K, E, D, G)$ *be a PKCS for* $\mathbf{R}$, *and let* Δ *be a set of distributions on* R.

1. $\mathbf{P}$ *is* weakly secure *if there is no p-time computable function B that strongly cracks* $\mathbf{P}$.

2. $\mathbf{P}$ *is* weakly polynomial fractionally secure relative to Δ *if there is no p-time computable B that strongly polynomial fractionally cracks* $\mathbf{P}$ *for any* $\delta \in \Delta$.

3. $\mathbf{P}$ *is* polynomial fractionally secure relative to Δ *if there is no p-time computable B that polynomial fractionally cracks* $\mathbf{P}$ *for any* $\delta \in \Delta$.

4. $\mathbf{P}$ *is* sparsely secure *if there is no p-time computable B that non-sparsely cracks* $\mathbf{P}$.

Observe that weak security can always be achieved if there are $r, r' \in R_n$ such that $g(r) = g(r')$ and $f(r) \neq f(r')$ (for infinitely many n in the case of i.o. security, for all but finitely many n in the case of a.e. security). This is done by letting $E(r, k_1) = g(r)$. An adversary is then unable to choose between $f(r)$ and $f(r')$. (Remember that, in this model, the receiver gets $g(r)$, and is not required to compute r.)

Now consider the case of weak polynomial fractional security. For a given distribution δ, subensemble W will be called a *polynomial fraction* of R if there is a polynomial q such that for all n $\delta(W_n) \geq 1/q(n)$. Encrypting by simply sending $g(r)$ is guaranteed to be secure in this way if for each $\delta \in \Delta$ and every polynomial fraction W of R, there are n and $r, r' \in W_n$ such that $g(r) = g(r')$ and $f(r) \neq f(r')$.

2.2 Semantic Security

The notions of security discussed here so far require an adversary to determine an entire secret in order to succeed. Goldwasser and Micali [5] considered semantic security, in which the adversary is successful if she can determine any partial information about a message with significantly greater probability (relative to any distribution), given a cipher, than without the cipher. We can adapt this concept of security to our setting.

Definition 2.5 *Let* $\mathbf{P} = (C, E, D, K, G)$ *be a p-time PKCS for* $\mathbf{R} = (R, S, M, f, g)$*, and let* δ *be a distribution on* R*. Let* V *be an ensemble, and* $\mathcal{F} = \{h_k : S_n \to V_n : k \in K_n\}$ *be a set of functions (partial information about the secrets). Let* $p_k(n) = \max_{v \in V_n}(\delta\{r \in R_n : h_k(f(r)) = v\})$ *(the best an adversary can do without a cipher). A p-time machine* B polynomial fractionally computes $\mathcal{F}$ *if there are polynomials* $q_1(n)$ *and* $q_2(n)$ *such that*

$$Prob\left\{k = (k_1, k_2) \in K_n : Prob\left(B(k_1, E(r, k_1)) = h_k \circ f(r)\right) > p_k(n) + \frac{1}{q_1(n)}\right\} > \frac{1}{q_2(n)}.$$

The outer probability is relative to the uniform distribution π *on* K*, and the inner is relative to* δ *on* R *and* π *on the random choices of* E *and* B*.* $\mathbf{P}$ *is* semantically secure relative to δ *if for all* $\mathcal{F}$*, there is no p-time* B *that polynomial fractionally computes* $\mathcal{F}$*.* $\mathbf{P}$ *is* semantically secure relative to a set of distributions Δ *if it is semantically secure relative to every* $\delta \in \Delta$*.*

Semantic security seems similar to the preceding notions of security, but there are several major differences. Whereas polynomial fractional and weak polynomial fractional security seek to protect a particular secret function, semantic security seeks to protect *all* secret functions. In this sense, semantic security is a stronger notion. In another sense, semantic security is a weaker notion than polynomial fractional or weak polynomial fractional security. A system is semantically secure, for example, if the adversary can guess the secret *without the encryption.* A system is polynomial fractionally or weakly polynomial fractionally secure only if the adversary has no way at all to obtain the secret (just doesn't get it). The other major difference is that "getting it," in our system, depends on a message, rather than the original record. It is shown in Section 4 that polynomial fractional and weak polynomial fractional security are independent of semantic security.

2.3 Complexity Theory and Security

In the classical case, there is a secure PKCS only if a one-way function exists. A similar result holds for secrecy systems. Generalizations of one-to-one and one-way functions can be described using the concept of one partial function dividing another.

Definition 2.6 *A function* h *is a* (p-time) divisor *of* f *if there is a (p-time) function* h' *such that* $h' \circ h = f$*.*

Thus, h divides the identity function if and only if it is invertible on the left. If so, it is one-to-one; otherwise, it is one-way.

Definition 2.7 *A partial function f' to be the* lift *of f if f' is a partial function of the form $f'(r,k) = (f(r),k)$ such that for each $r \in dom(f)$, there is at least one $(r,k) \in dom(f')$.*

Theorem 2.8 *If $\mathbf{R} = (R,S,M,f,g)$ has a weakly secure PKCS, then there is a pair of lifts f' and g' of f and g with $dom(f') = dom(g')$, and a p-time computable function which p-time divides g' and does not p-time divide f'.*

Proof: If $\mathbf{P} = (C,E,D,K,G)$ is a secure PKCS for $\mathbf{R}$, then the functions $f'(r,k) = (f(r),k)$, $g'(r,k) = (g(r),k)$, and $E'(r,k) = (E(r,k),k)$ (whenever $r \in R_n$ and k is the first element of a valid key pair) satisfy the requirements of the theorem. □

If we modify the concept of divisibility to divisibility on a polynomial fraction or on a non-sparse set, then the same theorem applies to polynomial fractional or sparse security.

The functions f' and g' are partial functions since not all keys are valid keys, and the set of valid keys might not be in P. If f and g are the identity, the conclusion of the theorem reduces to Grollmann and Selman's result that weak one-way functions exist if there is a secure PKCS for the classical secrecy system. They further showed that weak one-way functions exist if and only if NP contains P-inseparable sets. We generalize this in Proposition 2.9. We also observe that the p-time divisibility relation on functions defines a partial order on pairs of functions. In Section 4, we begin to explore the structure of this order, but many questions remain open if one-way functions exist.

Recall that two sets, A_1 and A_2, are P-inseparable if there is no set L in P such that $A_1 \subseteq L$ and $A_2 \subseteq \bar{L}$. In our case we can say that if a weakly secure PKCS exists then a particular pair of NP sets is P-inseparable.

Proposition 2.9 *Let $\mathbf{P} = (C,K,E,D,G)$ be a weakly secure PKCS for $\mathbf{R} = (R,S,M,f,g)$. Assume that g is honest (i.e., g^{-1} is polynomially length-bounded). Then the sets*

$$A_1 = \{(s,c,k_1) \in S \times C : \exists r \in R : E(g(r),k_1) = c \textit{ and } f(r) \leq s\}$$

and

$$A_2 = \{(s,c,k_1) \in S \times C : \exists r \in R : E(g(r),k_1) = c \textit{ and } f(r) > s\}$$

are disjoint and P-inseparable.

Proof: Suppose there were a set $L \in P$ with $A_1 \subseteq L$ and $A_2 \subseteq \bar{L}$. Consider the algorithm B which, on input c, k_1, finds the largest s such that $(s,c,k_1) \in L$ and outputs s. This can be done in polynomial time by performing binary search. The honesty of g allows us to find an upper bound for s so the binary search can be begun. It follows that B strongly cracks $\mathbf{P}$, a contradiction. □

In Section 4, Example 4, we show that there are PKCSs that are incomparable to the classical PKCS. Thus Proposition 2.9 gives additional conditions under which disjoint P-inseparable sets exist.

$$\begin{tikzcd} S' & R' \arrow[l, "f'"'] \arrow[r, "g'"] & M' \arrow[d, "\mu"] \\ S \arrow[u, "\sigma"] & R \arrow[l, "f"'] \arrow[r, "g"] \arrow[u, "\rho"] & M \end{tikzcd}$$

Figure 1: A reduction between security systems.

3 Reductions Between Security Systems

We next consider a partial order on secrecy systems. Given $\mathbf{R}$ and $\mathbf{R}'$, and a secure PKCS for $\mathbf{R}'$, is there necessarily a secure PKCS for R? This is possible if a PKCS for $\mathbf{R}'$ can be transformed into one for $\mathbf{R}$ as follows.

1. Given a record r in R, map r to a record r' in R'.
2. Encrypt r' and send the resulting cipher c'.
3. To decipher c', decipher it to a message in M', then map the result to M.

The security of the original PKCS will imply the security of the newly constructed PKCS if we can map secrets in S to secrets in S'. This gives rise to the following notions of reduction between secrecy systems (see Figure 1).

Definition 3.1 *A reduction from* $\mathbf{R} = (R, S, M, f, g)$ *to* $\mathbf{R}' = (R', S', M', f', g')$ *consists of:*

1. *A polynomial q giving a correspondence between security levels of* $\mathbf{R}$ *and* $\mathbf{R}'$*;*
2. *An honest deterministic or probabilistic p-time computable* $\rho : R_n \to R'_{q(n)}$*;*
3. *A p-time computable function* $\sigma : S_n \to S'_{q(n)}$*;*
4. *A p-time computable function* $\mu : M'_{q(n)} \to M_n$

such that $\forall r \in R_n : \mu \circ g' \circ \rho(r) = g(r)$ *and* $f' \circ \rho(r) = \sigma \circ f(r)$*. If ρ is probabilistic, this should hold for all random strings of ρ. (There is no gain in making σ and μ probabilistic.)*

Let $\mathbf{P}' = (C', K', E', D', G')$ be a PKCS for $\mathbf{R}'$ and suppose $\mathbf{R}$ reduces to $\mathbf{R}'$ by $H = (q, \rho, \sigma, \mu)$. Then we can construct a PKCS for $\mathbf{R}$ as follows:

a. For any n, $K_n = K'_{q(n)}$ and $G(1^n) = G'(1^{q(n)})$.
b. For any n, $C_n = C'_{q(n)}$ and for any $r \in R_n$ and $k_1 \in K^1_n$, $E(r, k_1) = E'(\rho(r), k_1)$.
c. For any n, $c \in C_n$ and $k_1 \in K^1_n$, $D(c, k_2) = \mu(D'(c, k_2))$.

It can be seen that if $(k_1, k_2) \in K_n$, and $r \in R_n$, then $D(E(r, k_1), k_2) = r$. If E', D' and G' are p-time computable, then so are E, D, and G. Thus $H(\mathbf{P}') = (C, K, E, D, G)$ is a p-time PKCS for $\mathbf{R}$. The honesty of ρ serves to ensure that $H(\mathbf{P}')$ is secure when $\mathbf{P}'$ is. In addition, ρ must map dense sets to dense sets, where the notion of density depends on the degree of security.

Definition 3.2 *Let U and V be ensembles with distributions δ and γ respectively. A function $\rho : U \to V$ is* polynomial fractional preserving (PFP) *relative to (δ, γ) if whenever W is a polynomial fraction of U (i.e., there is a polynomial $p(n)$ such that for each n, $\delta(W_n) > 1/p(n)$), $\rho(W)$ is a polynomial fraction of V. If Δ is a set of distributions, then ρ is PFP relative to Δ if for all $\delta \in \Delta$, a distribution on U, there is a $\gamma \in \Delta$, a distribution on V, such that ρ is PFP relative to (δ, γ).*

Definition 3.3 *Let $H = (q, \rho, \sigma, \mu)$ reduce $\mathbf{R}$ to $\mathbf{R}'$ and Δ be a set of distributions.*

1. *If ρ is onto, then H is a* strong reduction.
2. *If ρ maps non-sparse sets to non-sparse sets, then H is a* non-sparse preserving reduction.
3. *If ρ is polynomial fraction preserving relative to Δ, then H is a* polynomial fractional reduction *relative to Δ.*
4. *If ρ is probabilistic and polynomial fraction preserving relative to Δ, then H is a* probabilistic polynomial fractional reduction *relative to Δ.*

We next describe conditions under which security is preserved by reductions. To do so, we need two propositions on polynomial fractional preserving functions.

Proposition 3.4 *Let $\rho : U \to V$ be PFP relative to (δ, γ), and let $p(n)$ be any polynomial. There is a polynomial $p'(n)$ such that for all n, if W_n is any subset of U_n satisfying $\delta(W_n) > 1/p(n)$, then $\gamma(\rho(W_n)) > 1/p'(n)$.*

Proof: For each n, let $Z_n \subseteq U_n$ be a set with $\delta(Z_n) \geq 1/p(n)$, such that $\gamma(\rho(Z_n))$ is minimized. (Since U_n is finite, this is well-defined.) Let $Z = \{Z_n\}$. Then Z is a polynomial fraction of U. Therefore, there is a polynomial $p'(n)$ such that $\gamma(\rho(Z_n)) > 1/p'(n)$. Let W be any other subset of U such that for each n, $\delta(W_n) > 1/p(n)$. Then $\gamma(\rho(W_n)) > \gamma(\rho(Z_n)) > 1/p'(n)$. □

Thus, PFP functions are, in a measure-theoretic sense, uniform on their domains.

Proposition 3.5 *Let $\rho : U \to V$ be PFP relative to (δ, γ), and Z have distribution ϵ. Then $\rho \times id_Z : U \times Z \to V \times Z$ is PFP relative to $(\delta \times \epsilon, \gamma \times \epsilon)$.*

Proof: Let $W \subseteq U \times Z$ be a polynomial fraction, with $(\delta \times \epsilon)(W_n) > 1/p(n)$ for some polynomial p. For $z \in Z_n$, let $A_n = \{z : \delta\{u : (u, z) \in W_n\} \geq 1/(2p(n))\}$. Suppose that, for some n, $\epsilon(A_n) < 1/(2p(n))$. Then

$$\begin{aligned}
(\delta \times \epsilon)(W_n) &= \sum_{z \in A_n} \delta\{u : (u, z) \in W_n\} \cdot \epsilon(z) + \sum_{z \notin A_n} \delta\{u : (u, z) \in W_n\} \cdot \epsilon(z) \\
&< \sum_{z \in A_n} \epsilon(z) + \sum_{z \notin A_n} \frac{1}{2p(n)} \cdot \epsilon(z) \\
&< \frac{1}{p(n)},
\end{aligned}$$

contradicting our original assumption. Thus $\epsilon(A_n) \geq 1/2p(n)$. By Proposition 3.4, there is a polynomial $p'(n)$ such that whenever Y is a polynomial fraction of U of size at least $1/(2p(n))$, $\rho(Y)$ is a polynomial fraction of V of size at least $1/p'(n)$. Each set of the form $\{u : (u,z) \in W_n\}$ with $z \in A_n$ belongs to some polynomial fraction of U of size at least $1/(2p(n))$. Thus,

$$\begin{aligned}
(\gamma \times \epsilon)(\rho(W_n)) &\geq \sum_{z \in A_n} \gamma(\rho(\{u : (u,z) \in W_n\})) \cdot \epsilon(z) \\
&\geq \frac{\epsilon(A_n)}{p'(n)} \\
&\geq \frac{1}{2p(n)p'(n)}.
\end{aligned}$$

□

Theorem 3.6 *Let* $\mathbf{R} = (R, S, M, f, g)$ *and* $\mathbf{R}' = (R', S', M', f', g')$ *be secrecy systems,* $H = (q, \rho, \sigma, \mu)$ *reduce* $\mathbf{R}$ *to* $\mathbf{R}'$*, and* $\mathbf{P}' = (C', K', E', D', G')$ *be a PKCS for* $\mathbf{R}'$.

1. *If* H *is a strong reduction and* $\mathbf{P}'$ *is weakly secure, then* $H(\mathbf{P}')$ *is weakly secure.*
2. *If* H *is a non-sparse preserving reduction and* $\mathbf{P}'$ *is sparsely secure, then* $H(\mathbf{P}')$ *is sparsely secure.*
3. *If* $\mathbf{P}'$ *is deterministic,* H *is a polynomial fractional reduction relative to* Δ*, and* $\mathbf{P}'$ *is polynomial fractionally secure relative to* Δ*, then* $H(\mathbf{P}')$ *is polynomial fractionally secure relative to* Δ.
4. *If* $\mathbf{P}'$ *is deterministic,* H *is a polynomial fractional reduction relative to* Δ*, and* $\mathbf{P}'$ *is weakly polynomial fractionally secure relative to* Δ*, then* $H(\mathbf{P}')$ *is weakly polynomial fractionally secure relative to* Δ.
5. *If* $\mathbf{P}'$ *is probabilistic,* H *is a probabilistic polynomial fractional reduction relative to* Δ*, and* $\mathbf{P}'$ *is polynomial fractionally secure relative to* Δ*, then* $H(\mathbf{P}')$ *is polynomial fractionally secure relative to* Δ.

These results hold for i.o. security. Moreover, if $q(n)$ *is onto, then they hold for a.e. security.*

Proof: Let $B : Y \times C \to S$. (Here, Y is an ensemble of random strings, or a singleton set in the deterministic case.) We define $B'(y, c, k_1) = \sigma(B(y, c, k_1))$. We show that whenever B cracks $H(\mathbf{P}')$ for security parameter n, B' cracks $\mathbf{P}'$ for security parameter $q(n)$. Thus if B cracks i.o., then B' cracks i.o., and if q is onto and B cracks a.e., then B' cracks a.e. Throughout the proof, note that E, B, and ρ may be probabilistic, and thus each carries an extra parameter (x, y, and z, respectively). The definition of E is modified accordingly: $E'(x, \rho(z, r), k) = E((x, z), r, k)$.

Suppose B cracks $\mathbf{P}$ at $y \in Y_n \stackrel{def}{=} Y'_{q(n)}$, $x \in X_n \stackrel{def}{=} X'_{q(n)}$, $r \in R_n$, and $(k_1, k_2) \in K_n = K'_{q(n)}$. Let $r' = \rho(z, r)$. For any z we have

$$\begin{aligned} B'(y, E'(x, \rho(z, r), k_1), k_1) &= \sigma \circ B(y, E((x, z), r, k_1), k_1) \\ &= \sigma \circ f(r') \text{ (because } B \text{ cracks } \mathbf{P} \text{ here)} \\ &= f' \circ \rho(z, r), \end{aligned}$$

so B' cracks $\mathbf{P}'$ at y, x, $r' = \rho(z, r)$, (k_1, k_2).

In the deterministic case, if ρ is onto, this happens for every $r' \in R_{q(n)}$. Thus, if B cracks $H(\mathbf{P}')$ strongly, then B' cracks $\mathbf{P}'$ strongly. That is, if $\mathbf{P}'$ is weakly secure, then $H(\mathbf{P}')$ is weakly secure.

Suppose ρ is PFP relative to Δ. Let $\delta \in \Delta$ be a distribution on R. There is a distribution $\delta' \in \Delta$ on R' such that ρ is PFP relative to (δ, δ'). Suppose B strongly polynomial fractionally cracks $H(\mathbf{P}')$. Then there is a polynomial $p(n)$ such that for every k, the probability that B cracks is at least $1/p(n)$. By Propositions 3.4 and 3.5, there is a polynomial $p'(n)$ such that the image under $id_{Y \times X} \times \rho$ of any subset of $Y_n \times X_{q(n)} \times Z_n \times R_n$ of probability at least $1/p(n)$ has probability at least $1/p'(n)$ in $Y_n \times X_{q(n)} \times R'_{q(n)}$ where probabilities are taken relative to δ on R, δ' on R', and the uniform distribution on X, Y, and Z. Thus, for any (k_1, k_2), the probability that B' cracks at (k_1, k_2) is at least $1/p'(n) \geq 1/p'(q(n))$ (we may assume that $p'(n) \leq p'(q(n))$). It follows that B' strongly polynomial fractionally cracks $\mathbf{P}'$.

The remaining cases are similar. □

A "classical" secrecy system is one for which the record ensemble, secret ensemble, and message ensemble coincide, and the secret function and message function are the identity. We can almost characterize those secrecy systems which reduce to a classical system.

Proposition 3.7 *Let $\mathbf{R} = (R, S, M, f, g)$ be a secrecy system.*

1. *If $\mathbf{R}$ reduces or polynomial fractionally reduces to a secrecy system of the form*

$$\mathbf{R}' = (R', R', R', id, id),$$

then f divides g (that is, there is a function h such that $g = h \circ f$).

2. *If f divides g and either f or g is onto, then $\mathbf{R}$ reduces to a secrecy system of the form $\mathbf{R}' = (R', R', R', id, id)$.*

3. *If f divides g and either f or g is PFP, then $\mathbf{R}$ polynomial fractionally reduces to a secrecy system of the form $\mathbf{R}' = (R', R', R', id, id)$.*

Proof: In the first case suppose $H = (q, \rho, \sigma, \mu)$ reduces $\mathbf{R}$ to $\mathbf{R}'$. Then $\rho = \sigma \circ f$, and $g = \mu \circ \rho$. It follows that $g = \mu \circ \sigma \circ f$.

In the second case, suppose $g = h \circ f$. We can let $H = (n, f, id, h)$ if f is onto (resp., PFP), or $H = (n, g, h, id)$ if g is onto (resp., PFP). □

If the compression of records by ρ is fairly uniform, we can identify PFPness by a simpler condition.

Proposition 3.8 *Let $\mathbf{R}$ and $\mathbf{R}'$ be secrecy systems with distributions δ and δ', respectively. Let ρ be a probabilistic polynomial time computable function (i.e., $\rho : Z \times R \to R'$ for some Z), and let $b_1(n)$ and $b_2(n)$ be functions such that for every $r' \in Im(\rho)$ (the image of ρ),*

$$b_1(n) \leq \frac{(\pi \times \delta)(\rho^{-1}(r'))}{\delta'(r')} \leq b_2(n).$$

If ρ is PFP relative to (δ, δ'), then $b_1(n)$ is bounded by a polynomial. If $b_2(n)$ is bounded by a polynomial, then ρ is PFP relative to (δ, δ').

Proof: (1): Assume that ρ is PFP relative to (δ, δ'). Then there is a polynomial $p(n)$ such that $\delta'(Im(\rho)) > 1/p(n)$. The hypotheses imply

$$\begin{aligned} 1 &= \sum_{r' \in Im(\rho)} (\pi \times \delta)(\rho^{-1}(r')) \\ &\geq b_1(n) \sum_{r' \in Im(\rho)} \delta'(r') \\ &= b_1(n)\delta'(Im(\rho)) \\ &\geq \frac{b_1(n)}{p(n)}. \end{aligned}$$

This implies that $p(n) \geq b_1(n)$.

(2): Assume that $b_2(n)$ is bounded by a polynomial $q(n)$. Let W be a subset of $Z \times R$ and $t(n)$ be a polynomial such that for every n, $(\pi \times \delta)(W_n) > 1/t(n)$. Then

$$\begin{aligned} (\pi \times \delta)(W_n) &\leq (\pi \times \delta)(\rho^{-1}(\rho(W_n))) \\ &= \sum_{r' \in \rho(W_n)} (\pi \times \delta)(\rho^{-1}(r')) \\ &\leq \sum_{r' \in \rho(W_n)} q(n)\delta'(r') \\ &= q(n)\delta'(\rho(W_n)). \end{aligned}$$

Thus $\delta'(\rho(W_n)) \geq (\pi \times \delta)(W_n)/q(n) > 1/(q(n)t(n))$, as required. □

Corollary 3.9 *Suppose there is a function $b(n)$ such that for every $r' \in Im(\rho)$, $(\pi \times \delta)(\rho^{-1}(r')) = b(n)\delta'(r')$. Then ρ is PFP relative to (δ, δ') if and only if $b(n)$ is bounded by a polynomial.*

In the case of semantic security we need a slightly different notion of reduction between secrecy systems.

Definition 3.10 *A* semantic reduction *from* $\mathbf{R} = (R, S, M, f, g)$ *to* $\mathbf{R}' = (R', S', M', f', g')$ *consists of:*

1. *A polynomial* q *giving a correspondence between security levels of* $\mathbf{R}$ *and* $\mathbf{R}'$*;*
2. *An honest probabilistic p-time computable* $\rho : R_n \to R'_{q(n)}$ *with random strings* Z*;*
3. *A p-time computable function* $\sigma : S'_{q(n)} \to S_n$*;*
4. *A p-time computable function* $\mu : M'_{q(n)} \to M_n$

such that for all $r \in R_n$, $\mu \circ g' \circ \rho(r) = g(r)$, *and* $\sigma \circ f' \circ \rho(r) = f(r)$. *This should hold for all random strings of* ρ. *(There is no gain from allowing* σ *and* μ *to be probabilistic.)*

The difference between this and our earlier notion of reduction is the direction of the map σ. As before, if $\mathbf{P}' = (C', E', D', K', G')$ is a PKCS for $\mathbf{R}'$, then there is an induced PKCS $H(\mathbf{P})$ on $\mathbf{R}$.

If δ is a distribution on R and $\rho : R \to R'$ is probabilistic with random strings Z, then the distribution δ' induced on R' is defined by $\delta'(r') = (\pi \times \delta)\{(z, r) : \rho(z, r) = r'\}$, where π is the uniform distribution on Z. Note that ρ is always PFP relative to (δ, δ') since for any W, $\delta'(\rho(W)) = \delta(\rho^{-1}(\rho(W))) \geq \delta(W)$.

Theorem 3.11 *Let* $\mathbf{R} = (R, S, M, f, g)$ *and* $\mathbf{R}' = (R', S', M', f', g')$ *be secrecy systems, let* $H = (q, \rho, \sigma, \mu)$ *be a semantic reduction from* $\mathbf{R}$ *to* $\mathbf{R}'$*, let* δ *be a distribution on* R*, and let* δ' *be the induced distribution on* R'*. If* $\mathbf{P}' = (C', E', D', K', G')$ *is a semantically secure PKCS for* $\mathbf{R}'$ *relative to* δ'*, then* $H(\mathbf{P}')$ *is semantically secure for* $\mathbf{R}$ *relative to* δ*.*

Proof: Let $H(\mathbf{P}) = \mathbf{P}' = (C, E, D, K, G)$. Suppose that, contrary to the assertion of the theorem, $\mathcal{F} = \{h_k : S_n \to V_n : k \in K_n\}$ is a set of functions and $p(n)$ and $t(n)$ are polynomials such that $Prob\{k = (k_1, k_2) \in K_n : Prob(B(k_1, E(r, k_1)) = h_k \circ f(r)) > p_k + 1/t(n)\} > 1/p(n)$ relative to δ for some probabilistic p-time B. For each k, let $h'_k = h_k \circ \sigma$ and $\mathcal{F}' = \{h'_k\}$. We claim that B polynomial fractionally computes $\mathcal{F}'$ for $\mathbf{R}'$ relative to δ' for each security parameter in the image of q.

We have, for any $v \in V_n$ and $k \in K_n = K'_{q(n)}$,

$$\begin{aligned}
\delta'\{r' \in R'_{q(n)} : h'_k \circ f'(r') = v\} &= (\pi \times \delta)\{(x, r) \in X_n \times R_n : h_k \circ \sigma \circ f' \circ \rho(x, r) = v\} \\
&= (\pi \times \delta)\{(x, r) \in X_n \times R_n : h_k \circ f(r) = v\} \\
&= \delta\{r \in R_n : h_k \circ f(r) = v\}.
\end{aligned}$$

Thus $\max_{v\in V_n} \delta'\{r' \in R'_{q(n)} : h'_k\circ f'(r') = v\} = \max_{v\in V_n} \delta\{r \in R_n : h_k\circ f(r) = v\}$. Similarly,

$$\begin{aligned} &Prob(B(k_1, E'(r', k_1)) = h'_k\circ f'(r')) \\ &= (\pi \times \delta')\{(y, z, r') : B(y, k_1, E'(z, r', k_1)) = h_k\circ\sigma\circ f'(r')\} \\ &= (\pi \times \delta)\{(y, z, x, r) : B(y, k_1, E'(z, \rho(x, r), k_1)) = h_k\circ\sigma\circ f'\circ\rho(x, r)\} \\ &= (\pi \times \delta)\{(y, z, x, r) : B(y, k_1, E(z, x, r, k_1)) = h_k\circ f(r)\} \\ &= Prob(B(k_1, E(r, k_1)) = h_k\circ f(r)). \end{aligned}$$

The fact that B polynomial fractionally computes $\mathcal{F}$ for $\mathbf{R}$ relative to δ for security parameter n thus implies that B polynomial fractionally computes $\mathcal{F}'$ for $\mathbf{R}'$ relative to δ' for security parameter $q(n)$. □

If Δ is a class of distributions, and $\rho : R \to R'$ a map, then we say ρ preserves Δ if whenever $\delta \in \Delta$ is a distribution on R, the induced distribution δ' on R' is in Δ.

Corollary 3.12 *Let $\mathbf{R} = (R, S, M, f, g)$ and $\mathbf{R}' = (R', S', M', f', g')$ be secrecy systems, let $H = (q, \rho, \sigma, \mu)$ be a semantic reduction from $\mathbf{R}$ to $\mathbf{R}'$ and let Δ be a class of distributions. Suppose ρ preserves Δ. If $\mathbf{P}' = (C', E', D', K', G')$ is a semantically secure PKCS for $\mathbf{R}'$ relative to Δ, then $H(\mathbf{P}')$ is a semantically secure for $\mathbf{R}$ with respect to Δ.*

Corollary 3.13 *Let $\mathbf{R} = (R, S, M, f, g)$ be a secrecy system with a semantically secure PKCS $\mathbf{P} = (C, E, D, K, G)$ relative to δ on R. Let $f' : S \to S'$ and $g' : M \to M'$. Then $(C', E, g'\circ D, K, G)$ is a semantically secure PKCS for $(R, S, M, f'\circ f, g'\circ g)$.*

Corollary 3.14 *Let R be an ensemble with a distribution δ. If (R, R, R, id_R, id_R) (the "classical" secrecy system) has a semantically secure PKCS relative to δ, then for every $f : R \to S$ and $g : R \to M$, the secrecy system $\mathbf{R} = (R, S, M, f, g)$ has a semantically secure PKCS.*

Thus, if Δ is the class of all distributions, then every secrecy system with a fixed ensemble of records reduces to the classical secrecy system with respect to Δ. In a sense, this says that the classical secrecy system is complete for semantic security. This is not the case for polynomial fractional security, as is shown in the following section.

4 Existence and Nonexistence

Under some conditions we can say with certainty that a secure PKCS does or does not exist. These include both purely set theoretic and complexity theoretic conditions. We first see that if one secret is associated with enough messages, then the system can always be cracked.

Proposition 4.1 *Let $\mathbf{R} = (R, S, M, f, g)$ be a secrecy system and δ a distribution on R. If there is a polynomial fraction W in S such that f is a (not necessarily computable) constant on each W_n, then there is no PKCS for $\mathbf{R}$ which is weakly polynomial fractionally secure relative to δ.*

Proof: Suppose f is constant on W and $\delta(W_n) > 1/p(n)$ for some polynomial $p(n)$. Fix a PKCS $\mathbf{P}$ with ciphers C. Let B be the algorithm which, on input $c \in C_n$, randomly chooses $r \in_\delta R_n$ and outputs $f(r)$. Then B cracks $\mathbf{P}$ if $r \in W_n$ and c is the encryption of a record in W_n. Each of these events occurs with probability $\delta(W_n) > 1/p(n)$, so B cracks $\mathbf{P}$ with probability at least $1/p(n)^2$.

Note that if the constant value of f on W_n is p-time computable, then the error can be improved to $1/p(n)$ by always outputting the constant. □

A W such that each W_n contains a single element is called a singleton ensemble. In general we assume R contains no singleton ensemble whose probability is a polynomial fraction.

Proposition 4.2 *Let $\mathbf{R} = (R, S, M, f, g)$ be a secrecy system. Suppose there is a P-printable set $L \subseteq R$ such that the restriction of f to $R_n - L_n$ is a constant and if $x \in L_n$, $y \in R_n$, then $g(x) \neq g(y)$. Then there is no weakly secure PKCS for $\mathbf{R}$.*

Proof: Let $L_n = \{x_1, \cdots, x_t\}$ and let $u \in R_n - L_n$ (computable, say, as the lexicographically first element of $R_n - L_n$). To crack a PKCS for $\mathbf{R}$, on input c, find an i such that $c = E(x_i, k_1)$. The P-printability of L allows us to perform all these encryptions in polynomial time. If such an i is found, output $f(x_i)$, otherwise output $f(u)$. □

Proposition 4.3 *Let $\mathbf{R} = (R, S, M, f, g)$ be a secrecy system. Suppose $R = S \times M$, and f and g are projections on the first and second coordinates. Then the PKCS with $E(s, m) = g(s, m)$ is polynomial fractionally secure relative to any product distribution on R relative to which S contains no polynomial fractional singleton, and is semantically secure relative to any product distribution on R.*

Proof: Let $\delta = \gamma \times \epsilon$ be a product distributions on R. Suppose B is a probabilistic p-time function that polynomial fractionally cracks this PKCS. Then B is a function from M to S, and is successful on $\{(B(m), m) \in R\}$. This set has probability

$$\begin{aligned} \sum_{m \in M_n} \gamma(B(m))\epsilon(m) &\leq \sum_{m \in M_n} \max_{m'}\{\gamma(B(m'))\}\epsilon(m) \\ &= \max_{m'}\{\gamma(B(m'))\}. \end{aligned}$$

However, by hypothesis this set must be a polynomial fraction, so

$$\max_{m'}\{\gamma(B(m'))\} \geq \frac{1}{p(n)}$$

for some polynomial $p(n)$. This maximum must be achieved at some m, so S contains a polynomial fractional singleton.

Now suppose V is an ensemble, and $\mathcal{F} = \{h : S_n \to V_n\}$ is a set of functions. Let $t = \max_{v \in V_n} \gamma\{s \in S_n : h(s) = v\}$. Then

$$\begin{aligned}(\pi \times \delta)\{(x, s, m) : B(x, m) = h(s)\} &= \sum_{x,m} (\pi \times \epsilon)(x, m) \cdot \gamma\{s : B(x, m) = h(s)\} \\ &\leq \sum_{x,m} (\pi \times \epsilon)(x, m) \cdot t \\ &= t.\end{aligned}$$

Thus $\mathbf{P}$ is semantically secure relative to δ. □

Furthermore, we have:

Proposition 4.4 *Let $\mathbf{R} = (R, S, M, f, g)$ be a secrecy system and δ a distribution on R. If f and g are independent as random variables, then the PKCS which always sends $g(r)$ is semantically secure.*

Proof: The independence of f and g means that for any $s \in S$ and $m \in M$,

$$\delta\{r \in R : f(r) = s \text{ and } g(r) = m\} = \delta\{r \in R : f(r) = s\} \cdot \delta\{r \in R : g(r) = m\}.$$

It follows that if $\rho = f \times g : R \to S \times M$, then the distribution induced by ρ on $S \times M$ is the product of the distributions induced by f and g on S and M respectively. Let $\mathbf{R}'$ be the secrecy system $(S \times M, S, M, pr_1, pr_2)$ (where pr_i is projection on the ith component). By Proposition 4.3, the PKCS which, given (s, m), sends m is semantically secure relative to the product of the distributions induced by f and g on S and M respectively. Moreover (ρ, id, id) is a semantic reduction from $\mathbf{R}$ to $\mathbf{R}'$. The proposition follows from Theorem 3.11. □

4.1 Independence of Different Security Notions

In the following, we give: a secure PKCS; a secure but not semantically secure PKCS; a semantically secure and not secure PKCS; and secrecy systems that are incomparable to the classical secrecy system, with and without secure PKCSs.

Example 1: Let $g : R \to M$ be a weak one-way function (i.e., g is one-to-one, p-time computable, and honest, and there is no p-time computable function h such that for all $r \in R$, $h(g(r)) = r$). Then the secrecy system (R, R, M, id_R, g) has the (keyless) weakly secure PKCS $\mathbf{P}$ with $E(r) = g(r)$, and $D(m) = m$. If, moreover, g is *one-way relative to a distribution δ* in the sense that no p-time h can invert g on a polynomial fraction of R, then $\mathbf{P}$ is polynomial fractionally secure relative to δ.

Example 2: Let $g' : U \to W$ be a one-way function relative to γ on U. Let $R = \{0, 1\} \times U$, $M = \{0, 1\} \times W$, $g(ax) = ag'(x)$, and $f = id_R$, so $\mathbf{R} = (R, R, M, id_R, g)$. For $x \in U$, define $\delta(ax) = \gamma(x)/2$. The function g is still a one-way function, so the PKCS $\mathbf{P}$ with $E(y) = g(y)$

and $D = id_M$ is secure for $\mathbf{R}$. However, if $V_n = \{0,1\}$, $\mathcal{F} = \{h : h(ax) = a\}$, and $B(ay) = a$, then for $a \in W$, $p = \delta\{r \in R_n : h(id_R(r)) = a\} = 1/2$, while $Prob(B(E(ax)) = h(id_R(ax))) = 1$, so B polynomial fractionally computes $\mathcal{F}$ and $\mathbf{P}$ is not semantically secure, despite being secure.

Example 3: Let $\mathbf{R}$ be any secrecy system with the secret function f constant on R_n for each n. Then $\mathbf{R}$ can have no weakly secure PKCS – an adversary can simply choose an $r \in R_n$ and output $f(r)$. On the other hand, for any message function g, if we encrypt by sending $g(r)$ on input r, then we have semantic security, since no adversary can do better than the oblivious adversary.

Example 4: In this example we consider secrecy systems which are incomparable (under weak polynomial fractional reductions) to the classical secrecy system. Suppose (1) g is $m(n)$-to-one, where $m(n)$ is larger than any polynomial for n sufficiently large, and (2) for every n there are $r, r' \in R_n$ such that $f(r) = f(r')$ and $g(r) \neq g(r')$. By Proposition 3.7, $\mathbf{R}$ does not reduce to the classical secrecy system. Further, if the classical PKCS reduces to $\mathbf{R}$, then we would have $\mu \circ g \circ \rho = id$, with ρ PFP. Thus g would be one-to-one on a polynomial fraction of R, which is impossible by the assumption on $m(n)$. We can achieve these conditions, for example, by letting $R_n = R'_n \times R''_n \times R'''_n$, $g(r', r'', r''') = g'(r', r'')$ for some one-to-one function g', and $f(r', r'', r''') = (r', r''')$.

Suppose $|R'|$ and $|R'''|$ are bounded by polynomials in n, and $R'' = \Sigma^n$. Then f is constant on a polynomial fraction of R. By Proposition 4.1, $\mathbf{R}$ has no weakly polynomial fractionally secure PKCS. Thus we have an example of a secrecy system which is incomparable to the classical secrecy system and can have no weakly polynomial fractionally secure PKCS.

Suppose on the other hand that $R' = \Sigma^n$, $R'' = R''' = \{0,1\}$, and $g'(r', r'') = (g''(r'), r'')$ where g'' is a one-way function in the sense that it cannot be inverted on any polynomial fraction of its domain. Then the resulting secrecy system has a weakly polynomial fractionally secure PKCS, but again is incomparable with the classical secrecy system.

4.2 Combining PKCSs

We conclude by observing that there are polynomial fractionally (resp., weakly polynomial fractionally) secure PKCSs for both $\mathbf{R}_1$ and $\mathbf{R}_2$ if and only if there is a polynomial fractionally (resp., weakly polynomial fractionally) secure PKCS for their join. Remember that if A and B are sets, $A \oplus B = \{0x : x \in A\} \cup \{1y : y \in B\}$; if X and Y are ensembles, $(X \oplus Y)_n = X_n \oplus Y_n$. If $\mathbf{R}_i = (R^i, S^i, M^i, f^i, g^i)$, $i = 1, 2$, are two secrecy systems, let

$$\mathbf{R}_1 \oplus \mathbf{R}_2 = (R^1 \oplus R^2, S^1 \oplus S^2, M^1 \oplus M^2, f^1 \oplus f^2, g^1 \oplus g^2).$$

Let δ^i be a distribution on R^i, and for each n, let ϵ_n be a distribution on $\{0,1\}$ and $p(n)$ be a polynomial such that $\epsilon_n(0) > 1/p(n)$ and $\epsilon_n(1) > 1/p(n)$. Let $\delta_n(0x) = \epsilon_n(0) \cdot \delta^1_n(x)$ and $\delta_n(1x) = \epsilon_n(1) \cdot \delta^1_n(x)$.

Proposition 4.5 *Suppose that, for $i = 1, 2$, in polynomial time in n we can generate some $r \in R^i$. Then $\mathbf{R}_1 \oplus \mathbf{R}_2$ has a weakly polynomial fractionally (respectively, polynomial fractionally) secure PKCS with respect to δ if and only if $\mathbf{R}_1$ and $\mathbf{R}_2$ both have weakly polynomial fractionally (resp., polynomial fractionally) secure PKCSs relative to δ^1 and δ^2.*

Proof: Let $\mathbf{P} = (C, K, E, D, G)$ be a PKCS for $\mathbf{R}_1 \oplus \mathbf{R}_2$. Then $\mathbf{P}_1 = (C, K, E_1, D_1, G)$, where $E_1(r_1, k_1) = E(0r_1, k_1)$ and $D_1(c, k_2) = y$ when $D(c, k_2) = 0y$, and is arbitrary otherwise, is a PKCS for $\mathbf{R}_1$. If for all k, $\mathbf{P}_1$ can be cracked on a polynomial fraction W of R^1, then $\mathbf{P}$ can be cracked on the image of W in $R^1 \oplus R^2$, which is a polynomial fraction. Thus $\mathbf{P}_1$ is weakly polynomial fractionally secure if $\mathbf{P}$ is. If $\mathbf{P}_1$ can be cracked on a polynomial fraction W of $R^1 \times K$, then $\mathbf{P}$ can be cracked on the image of W in $(R^1 \oplus R^2) \times K$, which is a polynomial fraction. Thus $\mathbf{P}_1$ is polynomial fractionally secure if $\mathbf{P}$ is. Similarly we can construct a secure PKCS for $\mathbf{R}_2$.

Conversely, suppose $\mathbf{P}_i = (C^i, K^i, E_i, D_i, G_i)$ is a PKCS for $\mathbf{R}_i$, $i = 1, 2$. Let

$$\mathbf{P} = (C^1 \oplus C^2, K^1 \times K^2, E, D, G_1 \times G_2)$$

where $E(0r, (k_1^1, k_1^2)) = 0E_1(r, k_1^1)$, $E(1r, (k_1^1, k_1^2)) = 1E_2(r, k_1^2)$, $D(0c, (k_2^1, k_2^2)) = 0D_1(c, k_2^1)$, and $D(1c, (k_2^1, k_2^2)) = 1D_2(c, k_2^2)$. Any polynomial fraction of $R^1 \oplus R^2$ must contain a polynomial fraction of the image of either R^1 or R^2. Thus if $\mathbf{P}$ can be infinitely often cracked on a polynomial fraction, then so can either $\mathbf{P}_1$ or $\mathbf{P}_2$. □

5 Conclusions

We have presented a new model for public key cryptosystems, generalizing the classical model. Rather then simply sending a message which must be kept secret, we are concerned with sending a message while keeping some related information secret. In this paper we have explored several notions of security for this model. We have also developed notions of reductions between secrecy systems that preserve security. Thus security for large classes of systems may be demonstrated by demonstrating the security of a single system.

The most important contributions of this paper are the notion of secrecy systems, which models many real-world security needs better than the classic PKCS; the definitions of reductions between secrecy systems, as tools for proving security or relative security of secrecy systems; and the comparison of weak security, PFP security, and semantic security.

Many interesting questions remain. We would like to find examples of secure PKCSs for secrecy systems (possibly depending on complexity theoretic assumptions) that are incomparable to the classical secrecy system. All existing PKCSs rely on unproven complexity theoretic assumptions for their security. We would like to find PKCSs for nonclassical secrecy systems whose security relies on weaker assumptions. This would provide examples of systems that are more likely to be secure than classical PKCSs.

In our model one can also study questions such as: "given a secret, what messages can safely be sent?" or "given a message, what secrets can be kept when we send it?" The first amounts to fixing a secret function f and asking for which message functions g do we have a secure PKCS. The second amounts to fixing g and asking for which f we have a secure PKCS. In both cases we have an induced notion of partial order on p-time functions, and this leads to questions about the structure of these partial orders.

6 Acknowledgements

The authors thank Hugh Williams for several valuable comments on the manuscript.

References

[1] M. Blum, P. Feldman, and S. Micali, *Noninteractive zero-knowledge proof systems,* Proc. 20th Annual Symp. Thy. Comp., Chicago, May, 1988, pp. 103-112.

[2] M. Blum and S. Goldwasser, *An efficient probabilistic public-key encryption that hides all partial information,* Proc. of Crypto 84, Santa Barbara, USA, August 1984, pp. 289-299.

[3] W. Diffie and M. Hellman. *New directions in cryptography*, IEEE Trans. Inf. Thy. IT-22 (1976) pp. 644-654.

[4] O. Goldreich, *A uniform complexity encryption and zero-knowledge,* Technion CS-TR 570, June 1989.

[5] S. Goldwasser and S. Micali, *Probabilistic encryption,* J. Com. Sys. Sci. 28 (1984) pp. 270-299.

[6] J. Grollmann and A. Selman. *Complexity measures for public- key cryptosystems*, SIAM J. Comput. 17 (1988) pp. 309-335.

[7] S. Micali, C. Rackoff, R. Sloan, *Notions of security of public key cryptosystems,* SIAM J. on Computing 17(2) (1988) pp. 412-426.

[8] M. Naor and M. Yung, *Public-key cryptosystems provably secure against chosen ciphertext attacks,* in Proc. 22nd Annual Symp. on Thy. of Comp., Baltimore, USA, May 1990, pp. 427-437.

[9] H. Yamamoto, *Shannon's cipher system with correlated source outputs,* in Proceedings of the 1990 Int. Symp. on Info. Thy. and its Applic. (ISITA '90), Hawaii, USA, Nov. 1990.