On the Power of Misbehaving Adversaries and Security Analysis of the Original EPOC

Marc Joye[1], Jean-Jacques Quisquater[2], and Moti Yung[3]

[1] Gemplus Card International, Gémenos, France
marc.joye@gemplus.com
[2] UCL Crypto Group, Louvain-la-Neuve, Belgium
jjq@dice.ucl.ac.be
[3] CertCo, New York NY, U.S.A.
moti@certo.com, moti@cs.columbia.edu

Abstract. Nowadays, since modern cryptography deals with careful modeling and careful proofs, there may be two levels of cryptanalysis. One, the traditional breaking or weakness demonstration in schemes which are not provably secure. The second level of cryptanalysis, geared towards provably secure schemes, has to do with refining models and showing that a model was either insufficient or somewhat unclear and vague when used in proving systems secure. The best techniques to perform this second type of investigation are still traditional cryptanalysis followed by corrections. In this work, we put forth the second type of cryptanalysis.

We demonstrate that in some of the recent works modeling chosen ciphertext security (non-malleability), the notion of validity of ciphertext was left vague. It led to systems where under the model as defined/understood, it was shown provably secure. Yet, under another (natural) behavior of the adversary, the "provably secure system" is totally broken, since key recovery attack is made possible. We show that this behavior of an adversary is possible and further there are settings (the context of escrowed public key cryptosystems) where it is even highly relevant.

We mount the attack against systems which are chosen-ciphertext secure and non-malleable (assuming the adversary probes with valid messages), yet they are "universally" insecure against this attack: namely, the trapdoor key gets known by the adversary (as in Rabin's system under chosen ciphertext attacks). Specifically, the attack works against EPOC which has been considered for standardization by IEEE P1363 (the authors have already been informed of the attack and our fix to it and will consider this issue in future works). This re-emphasizes that when proving chosen-ciphertext security, allowing invalid ciphertext probes increases the adversary's power and should be considered as part of the model and in proofs.

1 Introduction

Classifying the security of cryptosystems, based on the power of the attacking adversary, is a central subject in modern cryptography. After many years of work by many researchers, the notion of attacks on public key systems has been carefully presented in a unified way in [2,5]. In the attack modeling of chosen ciphertext attacks they only explicitly consider *valid ciphertexts* by the adversary, referring directly to the size of the ciphertexts used by the adversary. —In a later (final) versions they justify that: an adversary who sends "invalid ciphertexts" will know that the machine it probes will answer that the ciphertext is invalid as a justification for this model (this was published on the web, but since our results here were made known in Feb. 2000 (see [A7]), this was omitted, by now). In any case, the model (even in these careful elegant classification works) has left vague and has not directly treated how to deal with invalid ciphertext. Such vagueness is dangerous since at times it may lead to misinterpretations and potentially to false claims based on correct proofs (as we will show). Our purpose here is to demonstrate and thus to re-emphasize that it is, in fact, important to deal with invalid ciphertext probing by the adversary. We do this via cryptanalysis which employs such messages. Since our attack is against a scheme provably secure against attacker which only employs valid ciphertext, we demonstrate that this issue is not merely for completeness of modeling, but a central one which should be considered in proofs, when chosen-ciphertext attacks are allowed. In more general terms, the work demonstrates how important is the interaction between careful modeling and investigating (seemingly) extended settings and new scenarios in order to refine, better understand and eliminate vagueness in formal models.

Security Notions under Active Attacks. The notions of "chosen ciphertext security" [CCS] (in a non-adaptive [36] and an adaptive [43,16] fashion) and "non-malleability" [NM] [16] are security notions for cryptosystems when coping with an active probing by an adversary who tries to break a system (namely, understand a message [CCS] or modify it [NM]). The adversary can choose ciphertexts in a certain way and probe the device on these messages. The security implies that the attacker does not get any advantage in breaking the system due to the probing. These security notions are extensions of "semantic security" (or polynomial security) [25] which assures that the system is secure —hiding all partial information against a passive adversary (in the public key model a passive adversary can, by itself, mount a chosen message attack).

The first public encryption scheme provably secure against (non-adaptive) chosen ciphertext attacks was devised by Naor and Yung [36] in 1990. In [43], Rackoff and Simon generalized their results and realized the first scheme provably secure against adaptive attacks. In the same year (1991), Dwork, Dolev and Naor [16] gave another provably secure scheme. More practical constructions (some of which are heuristics and some are validated in idealized random hash models) were proposed by Damgård [12] (only secure against non-adaptive attacks [47]), Zheng and Seberry [47] (see also [3] and [33]), Lim and Lee [33] (cryptanalyzed in [19]), Bellare and Rogaway [3,4] and Shoup and Gennaro [45] (for threshold cryptography). Recent formal treatment of the issue was given by Bellare, Desai, Pointcheval and Rogaway and Bellare and Sahai [2,5]; they show, among other things that under adaptive chosen message attacks indistinguishability attack is equivalent to malleability one. Recently designed schemes which are practical and based on new assumption or hybrid encryption are given in [40, 23, 39, 41]. The security of these practical schemes holds in the idealized random oracle setting [3] and/or under non-standard assumptions. One notable exception is the Cramer-Shoup scheme [11] which remarkably achieves both provable security (under the decisional Diffie-Hellman assumption, namely in the standard model) and high level of practicality.

The Attack. We now define somewhat more formally our attack. Roughly speaking, it is a chosen ciphertext attack where the adversary has access to a "decryption oracle." It however emphasizes and explicitly allows the adversary to misbehave and repeatedly feed the decryption oracle with invalid ciphertexts. (Remark: we use "our attack", though, of course, we do not claim it is a new (see [6]), just that using it against provable systems and emphasizing it in contrast with the context which uses only valid messages are, as far as we know, new).

Definition 1 (The Attack). *Let k be a security parameter that generates matching encryption/decryption keys (e, d) for each user in the system. A* chosen-ciphertext attack *is a process which, on input 1^k and e, obtains*

- *either plaintexts (relatively to d) corresponding to ciphertexts of its choice; or*
- *an indication that the chosen ciphertexts are invalid,*

for polynomially (in k) many ciphertexts, and produces an history tape h.

To this attack corresponds a security notion, namely resistance against our attack which coincides with chosen ciphertext security. A probabilistic polynomial time machine, called "message finder", generates two messages m_1 and m_2 on input 1^k and an auxiliary tape (which may include h, e and other public information). Let c be the ciphertext corresponding to m_b where b is randomly drawn from $\{0, 1\}$. Then, given m_1, m_2, c, h and e, another probabilistic polynomial time algorithm, called "message distinguisher", outputs $b' \in \{0, 1\}$. The (non-adaptive) chosen ciphertext attack *succeeds* if $b = b'$. Similarly to [43], we can make the previous scenario stronger by assuming that the adversary may run a second chosen ciphertext attack upon receiving the challenge ciphertext c (the only restriction being that the adversary does not probe on c). Accordingly, this adaptive attack *succeeds* is $b = b'$.

We may even reduce the attacker's probing power by letting it know if the ciphertext corresponds to a valid message or not.

Definition 2 (Security). *An encryption scheme is* secure *if every (non-adaptive /adaptive) chosen ciphertext attack succeeds with probability at most negligibly greater than 1/2.*

Our Results. We first apply the attack model to break the EPOC systems [37, 38]. These are very interesting systems which are about three year old and which have a lot of insight behind them (i.e., they use new trapdoor). They are provably secure against adaptive chosen ciphertext attacks in the ideal hash model. So indeed, if the context is such that our adversary is excluded, these are high quality ciphers (they are under consideration for standardization in IEEE P1363a). Yet, we teach that there are extended situations (i.e., misbehaving adversaries) where more care is needed since the systems are broken in these cases. We then show that even interactive systems which are secure against traditional chosen ciphertext attacks, can fail against the extended setting. We then discuss measures for correcting the schemes in order to prevent the attacks (which demonstrates the importance of the original work on these schemes). Finally, we revisit the general implications of the attack on chosen ciphertext security. Finally, we comment that we have notified the authors of EPOC of the attacks and the vagueness of the definitions, and they took notice. The EPOC authors' reaction is presented in an Appendix.

An Application of the Model. How realistic is to allow explicit invalid ciphertext and how much one should care about these? One can argue that when attacking a server system to provide decryptions of ciphertexts, then if too many invalid ones are asked, the server may shuts itself up. This may lead to denial of service attacks. Even more so, the attack is always possible in the context of escrow public key systems (for the sake of law enforcement). See Section 4 for details.

2 The Attacks

The attack which can be called "chosen valid/invalid ciphertext attack" applies to a large variety of cryptosystems, including systems using the so-called "coset encryption" [42]. See [24] for an application to the 'RSA for paranoids' [44] and [29] for the NICE [27] and HJPT [28] systems.

The above are attacks on "raw algebraic versions" of trapdoor functions. Perhaps other purely algebraic trapdoors are susceptible to the attack. However, more interestingly and perhaps somewhat surprising, we actually illustrate in this section attacks on a public encryption system which already possesses very strong security properties. The scheme is the system by Okamoto, Uchiyama and Fujisaki, EPOC [38]. EPOC has two versions, EPOC-1 and EPOC-2, and uses the trapdoor function described in [37]. It presents the advantages of being secure and non-malleable under chosen-ciphertext attacks, which, following [2], represents the *highest* level of security. Moreover, we show that interactive protocols [17] aiming to transform a semantically secure system into a system secure against chosen-ciphertext attacks may also be susceptible to the attack.

2.1 The EPOC-1 System

Hereafter, we give a brief review of EPOC-1; we refer to [38] for details. The scheme is divided into three parts: system setup, encryption and decryption.

[System setup] For security parameter k, two k-bit primes p and q are chosen and $n = p^2 q$. Then an element $g \in (\mathbf{Z}/n\mathbf{Z})^\times$ such that $g_p = g^{p-1} \bmod p^2$ has order p is chosen randomly. Likewise $h_0 \in (\mathbf{Z}/n\mathbf{Z})^\times$ is chosen randomly (and independently from g) and $h = (h_0)^n \bmod n$. Finally, three integers p_{Len}, m_{Len} and r_{Len} such that $p_{\mathrm{Len}} = k$ and $m_{\mathrm{Len}} + r_{\mathrm{Len}} \leq p_{\mathrm{Len}} - 1$ and a public (hash) function H are defined.
The public parameters are $(n, g, h, p_{\mathrm{Len}}, m_{\mathrm{Len}}, r_{\mathrm{Len}}, H)$. The secret parameters are (p, g_p).

[Encryption] A message $M \in \{0,1\}^{m_{\mathrm{Len}}}$ is encrypted as

$$C = g^{(M\|R)} h^r \bmod n$$

where R is uniformly chosen in $\{0,1\}^{r_{\mathrm{Len}}}$ and $r = H(M\|R)$.

[Decryption] Given the ciphertext C, the decryption process runs as follows. Let

$$X = \frac{\mathrm{L}(C_p)}{\mathrm{L}(g_p)} \bmod p$$

where $C_p = C^{p-1} \bmod p^2$ and $\mathrm{L}(x) = (x-1)/p$. Then if $g^X h^{H(X)} \bmod n = C$ holds, the decrypted message is given by $[X]^{m_{\mathrm{Len}}}$ (that is, the m_{Len} most significant bits of X); otherwise the null string ε is output.

2.2 The Attack

The encryption process assumes that the message being encrypted is smaller than $2^{m_{\mathrm{Len}}}$, or more precisely that $(M\|R) < 2^{p_{\mathrm{Len}}-1}$. What happens if a larger message is encrypted?

Let $\hat{C}$ $(= g^{(\hat{M}\|R)} h^{H(\hat{M}\|R)} \bmod n)$ denote the ciphertext corresponding to a message $\hat{M}$. The decryption of $\hat{C}$ yields the intermediary value

$$X = \frac{\mathrm{L}(\hat{C}^{p-1} \bmod p^2)}{\mathrm{L}(g_p)} \bmod p \enspace .$$

Defining $\hat{X} = (\hat{M}\|R)$, we have $X = \hat{X} \bmod p$; or equivalently $\hat{X} = X + \alpha p$ with $\alpha = \lfloor \hat{X}/p \rfloor$. If $\hat{X} \geq p$ then $\hat{X} \neq X$ (i.e., $\alpha > 0$) and the test $g^X h^{H(X)} \bmod n \stackrel{?}{=} \hat{C}$ will fail. The decryption algorithm will thus output the null string ε. This can be exploited by an adversary as follows. Since the secret prime p is a p_{Len}-bit number, she knows that p lies in the interval $I_0 =]2^{p_{\mathrm{Len}}-1}, 2^{p_{\mathrm{Len}}}[$. So, she chooses a message $\hat{M}$ such that $\hat{X} = (\hat{M}\|R) \in I_0$ and computes the corresponding ciphertext $\hat{C}$. If $\hat{C}$ can be decrypted then she knows that $\hat{X} < p$; otherwise (i.e., if ε is returned) she knows that $\hat{X} \geq p$. She then reiterates the process with the interval $I_1 =]\hat{X}, 2^{p_{\mathrm{Len}}}[$ or $I_1 =]2^{p_{\mathrm{Len}}-1}, \hat{X}]$, respectively. And so on... until the interval becomes small enough to guess —by exhaustion or more elaborated techniques (e.g., [10, 8])— the correct value of p. Noting that each iteration of a standard binary search halves the interval containing p, an upper bound for the total number of probes is certainly $p_{\mathrm{Len}} - 1$. For example, with a 1024-bit modulus n, at most 340 ciphertexts are necessary to recover the whole secret key.

2.3 The EPOC-2 System

In EPOC-2, the system setup is broadly the same as in EPOC-1 except that two public (hash) functions H and G are defined together with a symmetric cryptosystem. We let $\mathrm{SymEnc}(K, X)$ (resp. $\mathrm{SymDec}(K, X)$) denote the encryption (resp. decryption) of X under the symmetric key K. A message $M \in \{0,1\}^{m_{\mathrm{Len}}}$ is encrypted as (C_1, C_2) with $C_1 = g^R h^{H(M\|R)} \bmod n$ and $C_2 = \mathrm{SymEnc}(G(R), M)$ where R is uniformly chosen in $\{0,1\}^{r_{\mathrm{Len}}}$. Given (C_1, C_2), the decryption algorithm computes $C_p = C_1^{p-1} \bmod p^2$, $R' = \frac{\mathrm{L}(C_p)}{\mathrm{L}(g_p)} \bmod p$ and $M' = \mathrm{SymDec}(G(R'), C_2)$. If $g^{R'} h^{H(M'\|R')} \equiv C_1 \pmod{n}$ then the plaintext is M'; otherwise the null string ε is output. So, the attack on EPOC-1 readily applies on EPOC-2. The adversary now guesses the value of the secret factor p according to $p > R$ if the decryption process is possible or $p \le R$ if ε is returned, from suitable values of R she chooses.

2.4 The Fischlin PPTK Protocol

In [17], R. Fischlin presents a generic technique to turn any semantically secure cryptosystem into an (interactive) scheme which is immune against chosen-ciphertext attacks. We will apply this technique to the (semantically secure) Okamoto-Uchiyama cryptosystem [37]. The resulting scheme is very similar to the EPOC-1 system. This is not too surprising if you know that the EPOC systems are derived from an application to the Okamoto-Uchiyama system of the generic techniques of [21] (see also [22]) to transform a semantically secure system into a system secure against chosen-ciphertext attacks.

[System setup] For security parameter k, the parameters p, q, n, g, g_p, h_0 and h are defined as in § 2.1. There are also two integers p_{Len} and m_{Len} such that $p_{\mathrm{Len}} = k$ and $2m_{\mathrm{Len}} \le p_{\mathrm{Len}} - 1$. The public parameters are $(n, g, h, p_{\mathrm{Len}}, m_{\mathrm{Len}})$. The secret parameters are (p, g_p).

[Commitment/Encryption] A sender commits to a message $M \in \{0,1\}^{m_{\mathrm{Len}}}$ by computing and sending

$$C = g^{(M\|R)} h^r \bmod n$$

where R is uniformly chosen in $\{0,1\}^{m_{\mathrm{Len}}}$ and r in $\{0,1\}^{2m_{\mathrm{Len}}}$. Note that C is the Okamoto-Uchiyama encryption of $(M\|R)$.

[Challenge] Upon receiving C, the receiver chooses a challenge $\lfloor p_{\mathrm{Len}}/2 \rfloor$-bit prime π which he sends to the sender.

[PPTK] The sender computes $X_\pi = (M\|R) \bmod \pi$ and sends it to the receiver as a proof of plaintext knowledge.

[Decryption] Given X_π, the receiver decrypts C as

$$X = \frac{\mathrm{L}(C_p)}{\mathrm{L}(g_p)} \bmod p$$

where $C_p = C^{p-1} \bmod p^2$. Then if $X \equiv X_\pi \pmod{\pi}$, he accepts the plaintext given by $[X]^{m_{\mathrm{Len}}}$ (that is, the m_{Len} most significant bits of X); otherwise the null string ε is output, i.e., the receiver rejects the encryption.

The idea behind Fischlin's technique is quite intuitive. To make a system immune against chosen-ciphertext attacks, the sender (interactively) provides a "proof of plaintext knowledge" (PPTK). Although this seems sound, the attack presented against EPOC-1 in § 2.2 still applies. If $(M\|R)$ is smaller than the secret prime p then the decryption of the commitment C, X, is equal to $(M\|R)$. Therefore, the relation $X \equiv (M\|R) \pmod{\pi}$ will be verified whatever the value of the challenge π is. On the contrary, if $(M\|R) \geq p$ then the verification will fail and the null string ε is returned. So as before, the adversary can recover the bits of p successively according to whether ε is returned or not from appropriately chosen values for M. (Remark: recently, the author has removed his paper [17] from the public library, yet we do not think that it is due to the attack since the scheme as a generic method may be sound once considering the issues raised in the current work and similar considerations, see our repair to the specific application below.)

3 Repairing the Schemes

Here we show how to repair the systems, thus showing the usefulness of the work on the original schemes (the standardization bodies have to take note of our fixes, though).

The attack, as presented in § 2.2, is easily avoidable. EPOC-1 requires that message M being encrypted is such that $X = (M\|R) < 2^{p_{\mathrm{Len}}-1}$. This condition can be explicitly checked at the decryption stage:

[Decryption] Given the ciphertext C, the decryption process runs as follows. Let

$$X = \frac{\mathrm{L}(C_p)}{\mathrm{L}(g_p)} \bmod p$$

where $C_p = C^{p-1} \bmod p^2$ and $\mathrm{L}(x) = (x-1)/p$. Then if $g^X h^{H(X)} \bmod n = C$ **and if $\boldsymbol{X < 2^{p_{\mathrm{Len}}-1}}$ holds**, the decrypted message is given by $[X]^{m_{\mathrm{Len}}}$ (that is, the m_{Len} most significant bits of X); otherwise the null string ε is output.

Now the attacker has no longer advantage to feed the decryption oracle with invalid ciphertexts $\hat{C}$ (i.e., corresponding to an $\hat{X} \geq 2^{p_{\mathrm{Len}}-1}$). Indeed, if $\hat{X} \in$

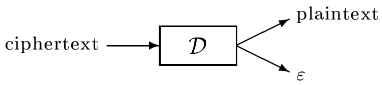

Fig. 1. Decryption algorithm.

$[2^{p_{\mathrm{Len}}-1}, p[$ then the decryption process yields an $X = \hat{X} \geq 2^{p_{\mathrm{Len}}-1}$ and so the null string ε is returned. If $\hat{X} \geq p$ then $X \neq \hat{X}$ (and thus $g^X h^{H(X)} \bmod n \neq \hat{C}$) and again ε is returned.

Likewise, EPOC-2 can be made robust against the attack of § 2.3 by further checking that $R' < 2^{r_{\mathrm{Len}}}$ $(< 2^{p_{\mathrm{Len}}-1})$ in the decryption stage. Finally, in Fischlin protocol, the receiver must also check that $X < 2^{p_{\mathrm{Len}}-1}$ in the decryption stage and reject the encryption if it is not the case.

4 Illustration: The "Policeman-in-the-middle Attack"

In this section, we present a detailed example in the context of escrowed public key cryptosystems. The attack is by misbehaving law enforcement which fakes ciphertexts repeatedly, and asks the escrow authorities to recover them (thus the proposed name of the attack: "the Policeman-in-the-middle Attack"). The attacker is allowed to misbehave and choose "invalid ciphertexts" (since, supposedly, they are what the wiretapping has recorded and this fact has to be reported).

The basic configuration of the system model (when concentrating on a single sender-receiver pair) is given in Fig. 2. It includes a sender (Alice) which employs the receiver's (Bob) public key to send messages. The receiver gets the ciphertext message and can decrypt it. In addition, the law enforcement (Police) gets the message and forwards it to the escrow agent (TTP). Police gets back a cleartext which is the valid decryption of the message or an indication of "invalid message" from TTP. (Typically, Police is authorized to decrypt messages in some time interval and based on this authorization by the court, TTP has to comply and serve as a "decryption oracle" say at some time interval.) The weaker probing capability where the trusted party only answers whether a ciphertext correspond to a valid or invalid message (which suffices for our attacks), is realistic in the context in which sporadic tests of compliance with the escrow system are performed by law enforcement and the TTP only validates correct usage.

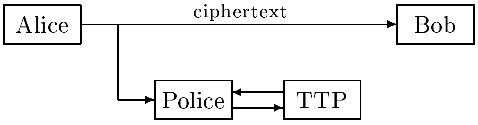

Fig. 2. Basic model.

Related Work on Escrow Systems.

Indeed, the notion of the attack makes sense in the context of the Police which tries to verify messages and the sender and the receiver may be bypassing the system. Therefore, the knowledge of "invalid message" is important (and should be supplied) to law enforcement. This is an interesting interplay between a protocol notion (escrowed encryption) and the relevant attack (chosen valid/invalid ciphertext attack). Let us review (only) some of the various escrow systems models which have been considered in the literature. A quite general framework to describe key escrow systems was proposed in [13] by Denning and Brandstad. Upon this, they classified the escrow mechanisms of complete systems as well as various design options, including the Escrow Encryption Standard (EES) and its Clipper implementation [1, 14] (see also [7, 35]), the fair cryptosystems [34, 31], the traceable ciphertexts [15, 32, 9], the Trusted Third Parties services [30], etc... (See also [18] for further discussions.) The model of Denning and Brandstad assumes that the sender (Alice) binds the ciphertext and the corresponding encryption key, normally by attaching a "data recovery field" (DRF) to the ciphertext. In our model, the DRF is merely an indication that the ciphertext was encrypted under Bob's public key. Variants on this model were considered in [20] by Frankel and Yung. They abstracted a public key based model where a message is sent to two receivers and where validation is added so that the line contains messages that have been validated as "messages available to both Bob and Police", then such systems are equivalent to "chosen ciphertext secure public-key systems," and furthermore, the reductions are very efficient (security wise).

5 Chosen Valid/Invalid Ciphertext Attacks

The scheme of Damgård [12] is semantically secure and has some other heuristic security properties, but a man-in-the-middle attack shows that this scheme is malleable [46, § 6]. EPOC is semantically secure and was "shown" to be non-malleable but is susceptible to a policeman-in-the-middle attack. This emphasizes the extended notion of chosen ciphertext security which considers security under "chosen **valid/invalid** ciphertext attacks." Certain security proofs assume that the adversary gets no credit for producing an invalid ciphertext. While this is true for most cryptosystems indeed, this is incorrect in general.

A particularity of Okamoto-Uchiyama primitive (as well as the other coset-based encryption primitives) is that the whole set of valid messages, $[0, p)$, is kept secret. Thus, to construct a cryptosystem thereof, one must work in a subset $[0, T)$ with $T < p$. This gives rise to two kinds of invalid ciphertexts: the invalid ciphertexts (i.e., those for which the null string ε is returned) and those for which a message is returned rather than a notification of invalidity. This shows the soundness of our repair (Section 3) since ε is returned for both types of invalid ciphertexts.

In many of the "generic constructions" there is a polynomial time algorithm so that when given a ciphertext it can verify (with overwhelming probability) that we have a "proper ciphertext" which implies that it is a valid plaintext which is encrypted correctly (e.g., the constructions that employ general non-interactive zero-knowledge as in [36, 43]). Thus implicitly, either one sends valid ciphertext or the ciphertext can be rejected in polynomial-time (namely, without the computational power of the decryption algorithm). In this case indeed "invalid ciphertexts" do not add power (the probing adversary can reject the invalid ciphertext itself). However, as demonstrated here this may not be the case with other schemes where there is no public verification of ciphertext validity.

Sometimes, considering only valid messages may be enough. For example, for the concrete schemes we attack (EPOC), it may still be very useful in cases where the tampering adversary attacks a centralized device (the device may stop on the first invalid message, or may record and limit such attacks). In this setting the security as was proved in [38] applies. However, in the protocol setting we identified, reporting "invalid ciphertext" is part of the actual task of the decryption entity (escrow authorities or TTP). We conclude that in these cases the systems have to be robust against the extended setting.

Acknowledgements

The authors are grateful to Jean-Sébastien Coron and David Pointcheval for some fruitful comments.

References

1. FIPS PUB 185. Escrowed encryption standard (EES). Federal Information Processing Standards Publication 185, U.S. Dept of Commerce, February 1994.
2. Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. Relations among notions of security for public-key encryption schemes. Full paper (30 pages), available at URL <http://www-cse.ucsd.edu/users/mihir/papers/pke.html>, February 1999. An extended abstract appears in H. Krawczyk, ed., *Advances in Cryptology – CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 26–45, Springer-Verlag, 1998.
3. Mihir Bellare and Phillip Rogaway. Random oracles are practical: a paradigm for designing efficient protocols. In *Proc. of the 1st ACM Conference on Computer and Communications Security*, pages 62–73, ACM Press, 1993.
4. ———. Optimal asymmetric encryption. In A. De Santis, ed., *Advances in Cryptology – EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pages 92–111, Springer-Verlag, 1995.
5. Mihir Bellare and Amit Sahai. Non-malleable encryption: Equivalence between two notions. In M. Wiener, ed., *Advances in Cryptology – CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 519–536, Springer-Verlag, 1999.
6. Daniel Bleichenbacher. A chosen ciphertext attack against protocols based on the RSA encryption standard PKCS#1. In H. Krawczyk, ed., *Advances in Cryptology – CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 1–12, Springer-Verlag, 1998.
7. Matt Blaze. Protocol failure in the escrowed encryption standard. In *Proc. of the 2nd ACM Conference on Computer and Communications Security*, pages 59–67, ACM Press, 1994.

8. Dan Boneh, Glenn Durfee, and Nick Howgrave-Graham. Factoring $N = p^r q$ for large r. In J. Stern, ed., *Advances in Cryptology – EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, Springer-Verlag, 1999.
9. Colin Boyd. Enforcing traceability in software. In Y. Han, T. Okamoto, and S. Qing, eds., *Information and Communications Security (ICICS '97)*, volume 1334 of *Lecture Notes in Computer Science*, pages 398–408, Springer-Verlag, 1997.
10. Don Coppersmith. Finding a small root of a bivariate integer equation; factoring with high bits known. In U. Maurer, ed., *Advances in Cryptology – EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 178–189, Springer-Verlag, 1996.
11. Ronald Cramer and Victor Shoup. A practical public-key cryptosystem provably secure against adaptive chosen ciphertext attack. In H. Krawczyk, ed., *Advances in Cryptology – CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 13–25, Springer-Verlag, 1998.
12. Ivan Damgård. Towards practical public key systems secure against chosen ciphertext attacks. In J. Feigenbaum, ed., *Advances in Cryptology – CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 445–456, Springer-Verlag, 1992.
13. Dorothy E. Denning and Dennis K. Brandstad. A taxonomy for key escrow encryption systems. *Communications of the ACM*, 39(3):34–40, 1996.
14. Dorothy E. Denning and Miles Smid. Key escrowing today. *IEEE Communications Magazine*, 32(9):58–68, 1994.
15. Yvo Desmedt. Securing traceability of ciphertexts: Towards a secure software key escrow system. In L. C. Guillou and J.-J. Quisquater, eds., *Advances in Cryptology – EUROCRYPT '95*, volume 921 of *Lecture Notes in Computer Science*, pages 147–157, Springer-Verlag, 1995.
16. Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography. Manuscript (51 pages), available at URL `<http://www.wisdom.weizmann.ac.il/~naor/onpub.html>`, To appear in *SIAM J. on Computing.* A preliminary version appears in *Proc. of the 23rd ACM Annual Symposium on the Theory of Computing (STOC '91)*, pages 542–552, ACM Press, 1991.
17. Roger Fischlin. Fast proof of plaintext-knowledge and deniable authentication based on Chinese remainder theorem. Theory of Cryptography Library, 99-06, available at URL `<http://philby.ucsd.edu/cryptolib/1999.html>`, March 1999.
18. Yair Frankel and Moti Yung. Escrow encryption systems visited: attacks, analysis and designs. In D. Coppersmith, ed., *Advances in Cryptology – CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*, pages 222–235, Springer-Verlag, 1995.
19. ———. Cryptanalysis of the immunized LL public key systems. In D. Coppersmith, ed., *Advances in Cryptology – CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*, pages 287–296, Springer-Verlag, 1995.
20. ———. On characterization of escrow encryption schemes. In P. Degano, R. Garriero, and A. Marchetti-Spaccamela, eds., *Automata, Languages, and Programming (ICALP '97)*, volume 1256 of *Lecture Notes in Computer Science*, pages 705–715, Springer-Verlag, 1997.
21. Eiichiro Fujisaki and Tatsuaki Okamoto. How to enhance the security of public-key encryption at minimum cost. In H. Imai and Y. Zheng, eds., *Public Key Cryptography*, volume 1560 of *Lecture Notes in Computer Science*, pages 53–68, Springer-Verlag, 1999.
22. ———. How to enhance the security of public-key encryption at minimum cost. *IEICE Transactions on Fundamentals*, E83-A(1): 24–32, 2000.

23. ———. Secure integration of asymmetric and symmetric encryption schemes. In M. Wiener, ed., *Advances in Cryptology – CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 537–554, Springer-Verlag, 1999.
24. Henri Gilbert, Dipankar Gupta, Andrew Odlyzko, and Jean-Jacques Quisquater. Attacks on Shamir's 'RSA for paranoids'. *Information Processing Letters*, 68: 197–199, 1998.
25. Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28:270-299, 1984.
26. Chris Hall, Ian Goldberg, and Bruce Schneier. Reaction attacks against several public-key cryptosystems. In V. Varadharajan and Yi Mu, eds., *Information and Communications Security*, volume 1726 of *Lecture Notes in Computer Science*, pages 2–12, Springer-Verlag, 1999.
27. Michael Hartmann, Sachar Paulus, and Tsuyoshi Takagi. NICE - New ideal coset encryption. In Ç. K. Koç and C. Paar, eds., *Cryptographic Hardware and Embedded Systems*, volume 1717 of *Lecture Notes in Computer Science*, pages 328–339, Springer-Verlag, 1999.
28. Detlef Hühnlein, Michael J. Jacobson Jr., Sachar Paulus, and Tsuyoshi Takagi. A cryptosystem based on non-maximal imaginary quadratic orders with fast decryption. In K. Nyberg, ed., *Advances in Cryptology – EUROCRYPT '98*, volume 1403 of *Lecture Notes in Computer Science*, pages 294–307. Springer-Verlag, 1998.
29. Éliane Jaulmes and Antoine Joux. A NICE cryptanalysis. In B. Preneel, ed., *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 382–391, Springer-Verlag, 2000.
30. Nigel Jefferies, Chris Mitchell, and Michael Walker. A proposed architecture for trusted third parties services. In E. Dawson and J. Golić, eds., *Cryptography: Policy and Algorithms*, volume 1029 of *Lecture Notes in Computer Science*, pages 98–104, Springer-Verlag, 1996.
31. Joe Kilian and Tom Leighton. Fair cryptosystems, revisited. In D. Coppersmith, ed., *Advances in Cryptology – CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*, pages 208–221, Springer-Verlag, 1995.
32. Lars R. Knudsen and Torben P. Pedersen. On the difficulty of software key escrow. In U. Maurer, ed., *Advances in Cryptology – EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 237–244, Springer-Verlag, 1996.
33. Chae Hoon Lim and Pil Joong Lee. Another method for attaining security against chosen ciphertext attacks. In D. R. Stinson, ed., *Advances in Cryptology – CRYPTO '93*, volume 773 of *Lecture Notes in Computer Science*, pages 420–434, Springer-Verlag, 1994.
34. Silvio Micali. Fair public-key cryptosystems. In E. F. Brickell, ed., *Advances in Cryptology – CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 113–138, Springer-Verlag, 1993.
35. Silvio Micali and Ray Sidney. A simple method for generating and sharing pseudorandom functions, with applications to Clipper-like key escrow systems. In D. Coppersmith, ed., *Advances in Cryptology – CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*, pages 185–196, Springer-Verlag, 1995.
36. Moni Naor and Moti Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *Proc. of the 22nd ACM Annual Symposium on the Theory of Computing (STOC '90)*, pages 427–437, ACM Press, 1990.
37. Tatsuaki Okamoto and Shigenori Uchiyama. A new public-key cryptosystem as secure as factoring. In K. Nyberg, ed., *Advances in Cryptology – EUROCRYPT '98*, volume 1403 of *Lecture Notes in Computer Science*, pages 308–318. Springer-Verlag, 1998.

38. Tatsuaki Okamoto, Shigenori Uchiyama, and Eiichiro Fujisaki. EPOC: Efficient probabilistic public-key encryption. Submission to P1363a, available at URL `<http://grouper.ieee.org/groups/1363/addendum.html>`, November 1998.
39. Pascal Paillier and David Pointcheval. Efficient public-key cryptosystem provably secure against active adversaries. In *Advances in Cryptology – ASIACRYPT '99*, volume of *Lecture Notes in Computer Science*, Springer-Verlag, 1999.
40. David Pointcheval. New public-key cryptosystem based on the dependent-RSA problem. In J. Stern, ed., *Advances in Cryptology – EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, Springer-Verlag, 1999.
41. ———. Chosen ciphertext security for any one-way cryptosystem. In H. Imai and Y. Zheng, eds., *Public Key Cryptography*, volume 1751 of *Lecture Notes in Computer Science*, pages 129–146, Springer-Verlag, 2000.
42. Sachar Paulus and Tsuyoshi Takagi. A generalization of the Diffie-Hellman problem and related cryptosystems allowing fast decryption. In *Proc. of the 1998 International Conference on Information Security and Cryptology (ICISC '98)*, Seoul, December 18–19, 1998.
43. Charles Rackoff and Daniel R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In J. Feigenbaum, ed., *Advances in Cryptology – CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 433–444, Springer-Verlag, 1992.
44. Adi Shamir. RSA for paranoids. *Cryptobytes*, 1(2):1–4, 1995.
45. Victor Shoup and Rosario Gennaro. Securing threshold cryptosystems against chosen ciphertext attack. IBM Research Report RZ 2974, Zurich Research Laboratory, Zurich, November 1997. An extended abstract appears in K. Nyberg, ed., *Advances in Cryptology – EUROCRYPT '98*, volume 1403 of *Lecture Notes in Computer Science*, pages 1–16, Springer-Verlag, 1998.
46. Yiannis Tsiounis and Moti Yung. On the security of ElGamal based encryption. In H. Imai and Y. Zheng, eds., *Public Key Cryptography*, volume 1431 of *Lecture Notes in Computer Science*, pages 117–134, Springer-Verlag, 1998.
47. Yuliang Zheng and Jennifer Seberry. Immunizing public-key cryptosystems against chosen ciphertext attacks. *IEEE Journal on Selected Areas in Communications*, 11(5):715–724, 1993.

Appendix: A Comment from EPOC Authors

As described in this manuscript and [A7], the initial version of EPOC [A5] had an error in the description; hence the current version of EPOC [A6] already includes the fix and so is proof against JQY attack.

The reason why the initial version was weak against chosen-ciphertext attack such as JQY attack is that it was not an exact implementation of [A1,22]. In other words, the weakness of the initial version is due to the gap between the implementation [A5] and the theoretical results [A1,A2].

In [A1,A2], we have shown two different conversions from an (arbitrary) asymmetric encryption scheme, which is secure in a weaker sense, into an asymmetric encryption scheme that is secure against adaptive chosen-ciphertext attacks in the random oracle model: For message $m \in \{0,1\}^{mlen}$, picking random string $r \in \{0,1\}^{rlen}$, the schemes obtained by the conversions are

$$\mathcal{E}^{\mathrm{FO1}}_{pk}(m;r) = \quad \mathcal{E}^{\mathrm{asym}}_{pk}((m||r);H(m,r)), \text{ and} \tag{1}$$

$$\mathcal{E}_{pk}^{\mathrm{FO2}}(m;r) = \quad \mathcal{E}_{pk}^{\mathrm{asym}}(r;H(m,r)) \quad || \quad m \oplus G(r), \tag{2}$$

respectively, where G, H denote hash functions such that $G : \{0,1\}^{rlen} \to \{0,1\}^{glen}$ and $H : \{0,1\}^{mlen} \times \{0,1\}^{rlen} \to \{0,1\}^{hlen}$. To appropriately quote from [A1,A2], the hash functions in the conversions must be carefully implemented. H in conversions, (1) and (2), should be considered as the different hash functions with the different domains. We denote by $\mathtt{MSP}$ the message space of the underlying encryption, $\mathcal{E}_{pk}^{\mathrm{asym}}$; that is, for $\mathcal{E}_{pk}^{\mathrm{asym}}(X;R)$, $X \in \mathtt{MSP}$. Following [A1,A2], it is required that $\mathtt{MSP}$ = '$\{0,1\}^{mlen} \times \{0,1\}^{rlen}$' in EPOC-1 and $\mathtt{MSP}$ = '$\{0,1\}^{rlen}$' [1] (The reader should not confuse $\mathtt{MSP}$ of $\mathcal{E}_{pk}^{\mathrm{asym}}$ with the *real* message space, $\{0,1\}^{mlen}$, of $\mathcal{E}_{pk}^{\mathrm{FO1}}$ and $\mathcal{E}_{pk}^{\mathrm{FO2}}$). The above requirement implies that the hash functions will halt if they take an element outside their domains (because the input is not defined!) and the decryption must abort (and output an *invalid* signal) if the hash functions invoked takes such an invalid element.

In the initial version of EPOC, H was described as a function in both conversions *carelessly* with an *inappropriate* domain such that $H : \{0,1\}^* \to \{0,1\}^{hlen}$. As mentioned later, the message space of the Okamoto-Uchiyama encryption scheme, which is used as the underlying encryption scheme in EPOC, is not equivalent to $\{0,1\}^*$: i.e., $\mathtt{MSP} \subsetneq \{0,1\}^*$. That is why the initial version was open to JQY attack — Actually, a knowledge extractor constructed by following [A1,A2] doesn't work on these wrong implementations; so the chosen-cipher security of these schemes is not guaranteed in general.

Recall the Okamoto-Uchiyama encryption scheme [A4]. For $x \in \{0,1\}^K$, picking a random string r from an appropriate domain, the encryption of x is

$$\mathcal{E}_{pk}^{\mathrm{asym}}(x;r) = \quad g^x h^r \bmod n. \tag{3}$$

Following [A1,A2], we must implement H so that $H : \{0,1\}^{mlen} \times \{0,1\}^{rlen} \to \{0,1\}^{hlen}$, where $K = mlen + rlen$ in EPOC-1 and $K = rlen$ in EPOC-2. In addition, as the Okamoto-Uchiyama scheme is an encryption scheme, we naturally get $K < |p|$, because an encryption scheme is required to satisfy the condition that, for any $x \in \mathtt{MSP}$ and $y \leftarrow E_{pk}^{\mathrm{asym}}(x)$, then $D_{sk}^{\mathrm{asym}}(y) = x$ (See [A1,A2]). If $|p| \leq K$, this condition does not hold.

As a result, an appropriate implementation wouldn't be open to any chosen-ciphertext attacks, not just JQY attack. Please refer to [A3,A6] for more details.

Finally, we would like to thank M. Joye, J.J. Quisquater, and M. Yung for giving us to place a comment in the appendix of their paper.

References

[A1] E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In M. Wiener, editor, *Advances in Cryptology — CRYPTO'99*, volume 1666 of *Lecture Notes in Computer Science*, pages 537–554. Springer-Verlag, 1999.

[1] This means that the encoding from $\mathtt{MSP}$ to '$\{0,1\}^{mlen} \times \{0,1\}^{rlen}$' is bijective in (1) and the encoding from $\mathtt{MSP}$ to '$\{0,1\}^{rlen}$' is bijective in (2).

[A2] E. Fujisaki and T. Okamoto. How to enhance the security of public-key encryption at minimum cost. *IEICE Transaction of Fundamentals of electronic Communications and Computer Science*, E83-A(1):24–32, January 2000.

[A3] E. Fujisaki and T. Okamoto. A Chosen-Cipher Secure Encryption Scheme Tightly As Secure As Factoring. *IEICE Transaction of Fundamentals of electronic Communications and Computer Science*, E84-A(1), To appear in January 2001.

[A4] T. Okamoto and S. Uchiyama. A new public-key cryptosystem as secure as factoring. In K. Nyberg, editor, *Advances in Cryptology — EUROCRYPT'98*, Lecture Notes in Computer Science, pages 308–318. Springer-Verlag, 1998.

[A5] T. Okamoto, S. Uchiyama, and E. Fujisaki. EPOC: Efficient probabilistic public-key encryption. Proposal to IEEE P1363a, November 1998.

[A6] T. Okamoto, S. Uchiyama, and E. Fujisaki. EPOC: Efficient probabilistic public-key encryption. Proposal to IEEE P1363a, ver. D6, Nov. 2000, available via: `http://grouper.ieee.org/groups/1363/P1363a/draft.html`

[A7] M. Joye, J.J. Quisquater, and M. Yung. On the power of misbehaving adversaries and security analysis of EPOC. Manuscript, February 2000.