BRICS

Basic Research in Computer Science

BRICS RS-01-43 Damgård & Nielsen: From Known-Plaintext Security to Chosen-Plaintext Security

From Known-Plaintext Security to Chosen-Plaintext Security

Ivan B. Damgård
Jesper Buus Nielsen

BRICS Report Series RS-01-43

ISSN 0909-0878 November 2001

See back inner page for a list of recent BRICS Report Series publications. Copies may be obtained by contacting:

BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK–8000 Aarhus C
Denmark

Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@brics.dk

BRICS publications are in general accessible through the World Wide Web and anonymous FTP through these URLs:

`http://www.brics.dk`
`ftp://ftp.brics.dk`
This document in subdirectory `RS/01/43/`

From Known-Plaintext Security to Chosen-Plaintext Security

Ivan Damgård   Jesper B. Nielsen*

November, 2001

Abstract

We present a new encryption mode for block ciphers. The mode is efficient and is secure against chosen-plaintext attack (CPA) already if the underlying symmetric cipher is secure against known-plaintext attack (KPA). We prove that known (and widely used) encryption modes as CBC mode and counter mode do not have this property. In particular, we prove that CBC mode using a KPA secure cipher is KPA secure, but need not be CPA secure, and we prove that counter mode using a KPA secure cipher need not be even KPA secure. The analysis is done in a concrete security framework.

1 Introduction

Which techniques can be applied to build encryption modes that are more secure than the underlying block cipher? In particular, how can we go from a KPA secure block cipher to a CPA secure encryption mode?

One motivation for looking at this problem is that even though a block cipher was designed to be CPA secure, using it in a way relying only on the KPA security of the block cipher gives an additional protection — security should generally be relative to the weakest possible assumption. Also, w.r.t. the concrete security framework, the KPA security of a scheme might be better than the CPA security. This is indeed the case for most ciphers if the security is measured by the cipher's resistance to common cryptanalytic techniques such as linear and differential cryptanalysis. Finally, we also find the question interesting from a theoretical point of view.

One idea that comes to mind is to try to build a pseudo-random function F_K (with K being the key) from the block cipher, and let the ciphertext for M be $(R, F_K(R) \oplus M)$, where R is a random string. For such an encryption

*{ivan,buus}@brics.dk.

algorithm, a CPA is equivalent to a KPA since both attacks simply imply that the adversary gets to see $(R, F_K(R))$. Note that, although we could in principle use the block cipher itself as F_K, this would be much too inefficient: we must have a function that expands significantly its input, to keep usage of random bits and ciphertext expansion low.

Building such a pseudo-random function is straightforward if the block cipher is secure under a CPA: choose a random block R, apply the cipher to $R, R+1, R+2, \ldots$ and define the sequence of cipher blocks to be the output. This is just the well known counter mode of encryption. Unfortunately, the proof that this is secure relies on the assumption that the block cipher is CPA secure, and does not work assuming only KPA security. Indeed we will in Section 4 prove that counter mode based on a KPA secure block cipher is not necessarily even KPA secure.

Despite this problem, we can give some intuitive arguments indicating that the pseudo-random function idea is essentially the only hope if we want an efficient solution.

We will restrict ourselves to what we call *known I/O modes*, that is, encryption modes where, given corresponding plaintext and ciphertext, one can easily compute the input and output of all encryption operations done when producing the ciphertext. CBC mode is such a mode, like most other known modes. Cipher feedback mode (CFB) is only known I/O in some variants, but this is due to the fact that only small parts of the output is used, leading to loss of efficiency. Also modes that use iterated encryption such as triple-DES are not strictly speaking known I/O, but in such cases it seems more reasonable to treat the entire iterated encryption as a block cipher, that is, to treat triple-DES as a single block cipher, for instance.

So an encryption mode can be thought of as a function that takes n blocks of plaintext as input and returns a random string R and n' blocks of ciphertext. It would be unreasonable if the mode could be be secure without doing at least n encryptions, so a CPA on the mode leads, by the known I/O assumption, to a KPA on the block cipher used, involving at least n blocks. Let M be the sequence of plaintext blocks, and M' the sequence of blocks that go into the block cipher. If the adversary fixes M, the entropy of the distribution of M' is at most the entropy of R.

Let us assume that the block cipher is KPA secure w.r.t. the uniform distribution of plaintext blocks. Then we may argue that the KPA on the block cipher that the adversary obtains through the encryption mode is harmless, provided that all $n' \geq n$ blocks in M' are uniformly distributed. But this would require that the length (entropy) of R is at least n blocks, and this is hardly interesting in practice. On the other hand, if R is shorter than M', we may still have a chance if the adversary cannot distinguish M' from a random string. But this means that the encryption mode in fact implements a pseudo-random function of precisely the type we asked for above!

So we may as well try directly to construct such a function, and in Section 3 we do exactly that. We construct a new mode for generating a pseudo-random string using a block cipher. The mode, called Pseudo-Random Tree (PRT) mode, is efficient and can be based on any secure pseudo-random function family, in particular any KPA secure block cipher. It only requires the communicating parties to store one key of the underlying function family and uses a number of random bits comparable to the widely used CBC mode and counter (CTR) mode. In Section 3 we analyse the security of PRT mode in a framework for concrete security from [BDJR97].

In [BDJR97] notions of CPA security and CCA security of block ciphers and symmetric encryption are developed in a concrete security framework, and the security of three well-known encryption modes, CBC mode and CTR mode (in its deterministic and probabilistic variants), are analysed. We extend this work. In Section 2 we give a definition of KPA security within their framework, and in Section 4 we analyse the KPA security of CBC mode and CTR mode, and compare the security of these modes with that of PRT mode.

Our results can be summaries as follows.

1. KPA security of the permutation family P implies KPA security of CBC mode based on P.

2. KPA security of the permutation family P does not imply CPA security of CBC mode based on P.

3. KPA security of the function family F does not imply even KPA security of CTR mode based on F.

4. KPA security of the function family F implies CPA security of PRT mode based on F.

In Section 5 we give a short discussion of the possibility of basing Chosen-Ciphertext Attack (CCA) secure encryption on KPA secure primitives.

2 Notions of Security

The following definitions are straightforward extensions of definitions from [BDJR97, Des00] to consider also KPA security. Of the four notions of security considered in [BDJR97] we have chosen real-or-random (ROR) indistinguishability, as it is proven to be the strongest notion.

A symmetric encryption scheme $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ consists of three randomized algorithms. The key generation algorithm $\mathcal{K}$ returns a key K; we write $K \leftarrow \mathcal{K}$. The encryption algorithm $\mathcal{E}$ takes as input the key K and a plaintext

M and returns a ciphertext C; we write $C \leftarrow \mathcal{E}_K(M)$. The decryption algorithm $\mathcal{D}$ takes as input the key K and a string C and returns a unique plaintext M or $\perp$; we write $x \leftarrow \mathcal{D}_K(C)$. We require that $\mathcal{D}_K(\mathcal{E}_K(M)) = M$ for all $M \in \{0,1\}^*$.

Definition 1 (ROR-KPA, ROR-CPA) *Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a symmetric encryption scheme. Let $b \in \{0,1\}$. Let A be an adversary that has access to an oracle. Let $\mathcal{R}_{K,b}$ be the oracle which on input $l \in \boldsymbol{N}$, if $b = 1$, outputs $(x, \mathcal{E}_K(x))$ for uniformly random $x \in \{0,1\}^l$, and, if $b = 0$, outputs $(x, \mathcal{E}_K(r))$ for uniformly random $x, r \in \{0,1\}^l$. Let $\mathcal{O}_{K,b}$ be the oracle which on input $x \in \{0,1\}^*$, if $b = 1$, outputs $\mathcal{E}_K(x)$, and, if $b = 0$, outputs $\mathcal{E}_K(r)$ for uniformly random r of the same length x. Now consider the following experiments:*

$$
\begin{array}{ll}
\underline{\textbf{proc}}\ \mathbf{Exp}^{\text{ror-kpa-}b}_{\mathcal{SE},A} \equiv & \qquad \underline{\textbf{proc}}\ \mathbf{Exp}^{\text{ror-cpa-}b}_{\mathcal{SE},A} \equiv \\
\quad K \leftarrow \mathcal{K} & \qquad\quad K \leftarrow \mathcal{K} \\
\quad d \leftarrow A^{\mathcal{R}_{K,b}} & \qquad\quad d \leftarrow A^{\mathcal{O}_{K,b}} \\
\quad \underline{\textbf{return}}\ d & \qquad\quad \underline{\textbf{return}}\ d
\end{array}
$$

We define the advantage *of the adversary via*

$$
\begin{aligned}
\mathbf{Adv}^{\text{ror-kpa}}_{\mathcal{SE},A} &= \Pr[\mathbf{Exp}^{\text{ror-kpa-}1}_{\mathcal{SE},A} = 1] - \Pr[\mathbf{Exp}^{\text{ror-kpa-}0}_{\mathcal{SE},A} = 1] \\
\mathbf{Adv}^{\text{ror-cpa}}_{\mathcal{SE},A} &= \Pr[\mathbf{Exp}^{\text{ror-cpa-}1}_{\mathcal{SE},A} = 1] - \Pr[\mathbf{Exp}^{\text{ror-cpa-}0}_{\mathcal{SE},A} = 1] \ .
\end{aligned}
$$

We define the advantage function of the scheme *as follows. For any integers t, q, μ,*

$$
\begin{aligned}
\mathbf{Adv}^{\text{ror-kpa}}_{\mathcal{SE}}(t,q,\mu) &= \max_A \left\{ \mathbf{Adv}^{\text{ror-kpa}}_{\mathcal{SE},A} \right\} \\
\mathbf{Adv}^{\text{ror-cpa}}_{\mathcal{SE}}(t,q,\mu) &= \max_A \left\{ \mathbf{Adv}^{\text{ror-cpa}}_{\mathcal{SE},A} \right\} \ ,
\end{aligned}
$$

where the maximum is over all A with "time complexity" t, making at most q queries to the oracle, these totaling at most μ bits.

By the "time complexity" we mean the worst case total running time of the experiment with $b = 1$, plus the size of the code of the adversary, in some fixed RAM model of computation. We stress that the total execution time of the experiment includes the time of *all* operations in the experiment, including the time for key generation and the encryptions done by the oracle. For a discussion of this time complexity, see [Des00].

A function family with key-space $\mathcal{K}$, input-length l, and output-length L is a map $F : \mathcal{K} \times \{0,1\}^l \to \{0,1\}^L$. For each key $K \in \mathcal{K}$ we define a map $F_K : \{0,1\}^l \to \{0,1\}^L$ by $F_K(\cdot) = F(K, \cdot)$. We write $f \stackrel{R}{\leftarrow} F$ for the operation $K \stackrel{R}{\leftarrow} \mathcal{K};\ f \leftarrow F_K$. We call F a family of permutations if for all $K \in \mathcal{K}$,

F_K is a permutation. We use $\mathrm{Rand}^{l \to L}$ to denote the family of all functions $\{0,1\}^l \to \{0,1\}^L$.

If a random function from the function family looks as a random function from $\mathrm{Rand}^{l \to L}$, we call the family a pseudo-random function family. We define this notion formally for KPAs. The definitions for CPAs and CCAs can be found in [BDJR97], but will not be used in the present paper. The security of permutation families is also defined relative to $\mathrm{Rand}^{l \to L}$ and not relative to random permutations. W.r.t. asymptotic security this makes no difference, where as there is a small difference w.r.t. concrete security. For a discussion of this see [BDJR97].

Definition 2 (PRF-KPA) *Let F be a function family with input-length l and output-length L. Let $b \in \{0,1\}$. Let D be a distinguisher that has access to an oracle. Let $\mathcal{R}_f$ be the oracle which on input* gen *generates a uniformly random $s \in \{0,1\}^l$ and outputs $(s, f(s))$. Now consider the following experiment:*

$$\begin{aligned} &\underline{\mathbf{proc}}\ \mathbf{Exp}_{F,D}^{\text{prf-kpa-}b} \equiv \\ &\quad f_0 \stackrel{R}{\leftarrow} \mathrm{Rand}^{l \to L};\ f_1 \stackrel{R}{\leftarrow} F \\ &\quad d \leftarrow D^{\mathcal{R}_{f_b}} \\ &\quad \underline{\mathbf{return}}\ d \end{aligned}$$

We define the advantage *of the distinguisher via*

$$\mathbf{Adv}_{F,D}^{\text{prf-kpa}} = \Pr[\mathbf{Exp}_{F,D}^{\text{prf-kpa-}1} = 1] - \Pr[\mathbf{Exp}_{F,D}^{\text{prf-kpa-}0} = 1] \ .$$

We define the advantage function of the function family *as follows. For any t, q,*

$$\mathbf{Adv}_{F}^{\text{prf-kpa}}(t,q) = \max_{D} \left\{ \mathbf{Adv}_{F,D}^{\text{prf-kpa}} \right\} \ .$$

where the maximum is over all D with time complexity t, making at most q queries to the oracle.

A variable-length output function family with key-space $\mathcal{K}$ and input-length l is a map $F : \mathcal{K} \times \boldsymbol{N} \times \{0,1\}^l \to \{0,1\}^*$. For each key $K \in \mathcal{K}$ we define a map $F_K : \boldsymbol{N} \times \{0,1\}^l \to \{0,1\}^*$ by $F_K(\cdot,\cdot) = F(K,\cdot,\cdot)$. We require that $|F(\cdot, L, \cdot)| = L$ for all inputs. We use VO-Rand^l to denote the following variable-length output function family. The key-space is $\{0,1\}^l \to \{0,1\}^*$ and for key f, $r \in \{0,1\}^l$, and $L \in \boldsymbol{N}$ we set $F(f, L, r)$ to be the first L bits of $f(r)$.

Definition 3 (VO-PRF-KPA) *Let F be a variable-length output function family with input-length l. Let $b \in \{0,1\}$. Let D be a distinguisher that has access to an oracle. Let $\mathcal{R}_f$ be the oracle which on input $L \in \boldsymbol{N}$ generates a uniformly random $r \in \{0,1\}^l$ and outputs $(r, f(L,r))$. Now consider the following experiment:*

$$
\begin{array}{l}
\underline{\textbf{proc}}\ \textbf{Exp}_{F,D}^{\text{vo-prf-kpa-}b} \equiv \\
\quad f_0 \stackrel{R}{\leftarrow} \text{VO-Rand}^l;\ f_1 \stackrel{R}{\leftarrow} F \\
\quad d \leftarrow D^{\mathcal{R}_{f_b}} \\
\quad \underline{\textbf{return}}\ d
\end{array}
$$

We define the advantage *of the distinguisher via*

$$\textbf{Adv}_{F,D}^{\text{vo-prf-kpa}} = \Pr[\textbf{Exp}_{F,D}^{\text{vo-prf-kpa-}1} = 1] - \Pr[\textbf{Exp}_{F,D}^{\text{vo-prf-kpa-}0} = 1] \ .$$

We define the advantage function of the function family *as follows. For any t, q, μ,*

$$\textbf{Adv}_{F}^{\text{vo-prf-kpa}}(t, q, \mu) = \max_{D} \left\{ \textbf{Adv}_{F,D}^{\text{vo-prf-kpa}} \right\} \ .$$

where the maximum is over all D with time complexity t, making at most q queries to the oracle, these totaling at most μ bits.

3 PRT Mode

In this section we describe the PRT encryption mode.

3.1 Variable-Length Output Pseudo-Random Function Encryption

Actually PRT mode is rather a construction of a VO-PRF-KPA secure variable-length output function family from a PRF-KPA secure function family. The encryption will then be done using the variable-length output function family as

$$\text{VO-PRF-ENC}[F]_K(M) = (r, F_K(r, |M|) \oplus M) \ ,$$

where r is uniformly random in $\{0,1\}^l$. We start by relating the ROR-CPA security of VO-PRF-ENC$[F]$ to the VO-PRF-KPA security of F.

Theorem 1 *Suppose F is a variable-length output function family. If F is VO-PRF-KPA secure, then* VO-PRF-ENC$[F]$ *is ROR-CPA secure.*[1] *Specifically, for any t, q, μ,*

$$\textbf{Adv}_{\text{VO-PRF-ENC}[F]}^{\text{ror-cpa}}(t, q, \mu) \leq \textbf{Adv}_{F}^{\text{vo-prf-kpa}}(t, q, \mu) + \frac{q(q-1)}{2^{l+1}} \ .$$

[1] Actually, we have not assigned a meaning to the claim that VO-PRF-ENC$[F]$ is ROR-CPA secure if F is VO-PRF-KPA secure, as we have no definition of security: In this paper we consider a concrete security framework without a security parameter. If, however, we introduced a security parameter k, then in the asymptotic security framework, all of t, q, μ, l, and L would be polynomial in k and typically $l = \Theta(k)$. We would then define security by requiring that the advantage of all probabilistic polynomial time (in k) adversaries is negligible (in k). The claim would then follow from the specific bound on $\textbf{Adv}_{\text{VO-PRF-ENC}[F]}^{\text{ror-cpa}}(t, q, \mu)$ given by the theorem. In the following we will use the term "secure" in this rather colloquial way.

$$
\begin{array}{l}
\underline{\textbf{proc}}\ \mathrm{PRT}_{\gamma_1,\ldots,\gamma_d}[F]_{K_0^1,\ldots,K_{\gamma_1-1}^1,K_0^2,\ldots,K_{\gamma_d-1}^d}(R_0^1) \ \equiv \\
\quad w_1 \leftarrow 1 \\
\quad \underline{\textbf{for}}\ i = 1\ \underline{\textbf{to}}\ d\ \underline{\textbf{do}} \\
\qquad \underline{\textbf{for}}\ j = 0\ \underline{\textbf{to}}\ \gamma_i - 1\ \underline{\textbf{do}}\ f_{i,j} \leftarrow F_{K_j^i}\ \underline{\textbf{od}} \\
\qquad w_{i+1} \leftarrow w_i \gamma_i \\
\qquad \underline{\textbf{for}}\ j = 0\ \underline{\textbf{to}}\ w_{i+1} - 1\ \underline{\textbf{do}}\ R_j^{i+1} \leftarrow f_{i,(j \bmod \gamma_i)}(R^i_{j \operatorname{div} \gamma_i})\ \underline{\textbf{od}} \\
\quad \underline{\textbf{od}} \\
\quad \underline{\textbf{return}}\ R_0^2 \ldots R_{w_2-1}^2 R_0^3 \ldots R_{w_{d+1}-1}^{d+1}
\end{array}
$$

Figure 1: Fixed-length PRT mode.

Proof: We prove the specific bound. Consider an ROR-CPA distinguisher $\overline{D}$ expecting access to an oracle $\mathcal{R}_{K,b}$ for the VO-PRF-ENC$[F]$ scheme. We construct a distinguisher D having access to a VO-PRF-KPA oracle $\mathcal{R}_f$ for the variable-length output function family F as follows. The distinguisher D runs the code of $\overline{D}$. Each time D request an encryption of message M, request a pair (r, R), where r is uniformly random in $\{0,1\}^l$ and $R = f(|M|, r)$. Then return $c = (r, M \oplus R)$. When D returns with some value d, return d.

If $b = 1$, then f is a random function from F and the values c are distributed exactly as values from $\mathcal{R}_{K,1}$. This implies that

$$
\Pr[\mathbf{Exp}_{F,D}^{\text{vo-prf-kpa-}1} = 1] = \Pr[\mathbf{Exp}_{\text{VO-PRF-ENC}[F],\overline{D}}^{\text{ror-cpa-}1} = 1] \ . \qquad (1)
$$

If on the other hand $b = 0$, then f is a uniformly random function from VO-Rand^l. In that case the values c are distributed as values from $\mathcal{R}_{K,0}$, as long as there are no collisions among the r-values returned by $\mathcal{R}_f$. Let C denote the event that there are such collisions. We then have that

$$
\Pr[\mathbf{Exp}_{F,D}^{\text{vo-prf-kpa-}0} = 1 | \neg C] = \Pr[\mathbf{Exp}_{\text{VO-PRF-ENC}[F],\overline{D}}^{\text{ror-cpa-}0} = 1 | \neg C] \ .
$$

Using that $\Pr[C] \leq \frac{q(q-1)}{2^{l+1}}$, we then have that

$$
\Pr[\mathbf{Exp}_{\text{VO-PRF-ENC}[F],\overline{D}}^{\text{ror-cpa-}0} = 1] \geq \Pr[\mathbf{Exp}_{F,D}^{\text{vo-prf-kpa-}0} = 1] - \frac{q(q-1)}{2^{l+1}} \ . \qquad (2)
$$

The theorem easily follows from (1) and (2). ■

3.2 Fixed-Length PRT Mode

We first describe a fixed-length version of PRT mode, which we will denote by $\mathrm{PRT}_{\gamma_1,\ldots,\gamma_d}[F]$. For notational convenience, we describe the mode for the case,

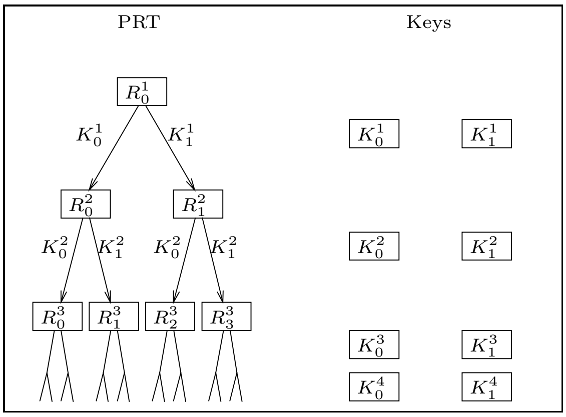

Figure 2: The mode $\mathrm{PRT}_{2,2,2,2}[F]$.

where the input-length and the output-length of the function family F are the same. The construction and analysis generalize in a straightforward manner to consider the more general case, where the input-length is smaller or even larger than the output-length. We call d the depth of the pseudo-random tree and require that $d > 0$. We call γ_i the branching of level i and require that $\gamma_i > 0$. PRT mode with parameters $\gamma_1, \ldots, \gamma_d$ is described in Fig. 1. The mode $\mathrm{PRT}_{2,2,2,2}[F]$ is sketched in Fig. 2.

We introduce some terminology, which will be used throughout the paper. We call the value w_i computed during the evaluation the width of level i, we call the value $(R_0^i, \ldots, R_{w_i-1}^i) \in (\{0,1\}^l)^{w_i}$ the blocks of level i, and we call the value $(K_0^i, \ldots, K_{\gamma_i-1}^i)$ the keys of level i. We let $\gamma = \sum_{i=1}^d \gamma_i$. If we consider q trees, then by level i in the forest, we mean level i of all the q trees. By a collision at level i (in the forest), we mean two identical blocks at level i (in the forest), and by a collision (in the forest), we mean two identical blocks positioned at the same level (in the forest). Finally, we call the levels indexed i, where $i \leq d$, the internal levels. Let $w = \sum_{i=1}^{d+1} w_i$, let $w' = \sum_{i=1}^{d} w_i$, let $W = \sum_{i=1}^{d+1} w_i^2$, and let $W' = \sum_{i=1}^{d} w_i^2$.

We are going to define $\gamma + 1$ hybrid versions of PRT mode. Hybrid h will use random functions for the first h functions in the list $f_{K_0^1}, \ldots, f_{K_{\gamma_1-1}^1}$, $f_{K_0^2}, \ldots, f_{K_{\gamma_d-1}^d}$, as opposed to using pseudo-random functions. The hybrid using h random functions is described in Fig. 3.

We first show that a "birthday attack" can be mounted against PRT mode, even if the PRF is perfect, i.e. even if all branching is done using uniformly random functions.

$$
\begin{array}{l}
\underline{\textbf{proc}}\ \mathrm{PRT}^{h}_{\gamma_1,\ldots,\gamma_d}[F]_{f_0,\ldots,f_{h-1},K^i_j,\ldots,K^d_{\gamma_d-1}}(R^1_0)\ \equiv \\
\quad k \leftarrow 0 \\
\quad w_1 \leftarrow 1 \\
\quad \underline{\textbf{for}}\ i = 1\ \underline{\textbf{to}}\ d\ \underline{\textbf{do}} \\
\quad\quad \underline{\textbf{for}}\ j = 0\ \underline{\textbf{to}}\ \gamma_i - 1\ \underline{\textbf{do}} \\
\quad\quad\quad \underline{\textbf{if}}\ k < h\ \underline{\textbf{then}}\ f_{i,j} \leftarrow f_k \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad k \leftarrow k+1 \\
\quad\quad\quad\quad\quad\quad \underline{\textbf{else}}\ f_{i,j} \leftarrow F_{K^i_j}\ \underline{\textbf{fi}}\ \underline{\textbf{od}} \\
\quad\quad w_{i+1} \leftarrow w_i \gamma_i \\
\quad\quad \underline{\textbf{for}}\ j = 0\ \underline{\textbf{to}}\ w_{i+1} - 1\ \underline{\textbf{do}}\ R^{i+1}_j \leftarrow f_{i,(j \bmod \gamma_i)}(R^i_{j \operatorname{div} \gamma_i})\ \underline{\textbf{od}} \\
\quad \underline{\textbf{od}} \\
\quad \underline{\textbf{return}}\ R^2_0 \ldots R^2_{w_2-1} R^3_0 \ldots R^{d+1}_{w_{d-1}}
\end{array}
$$

Figure 3: PRT mode, hybrid h.

Proposition 1

$$
\mathbf{Adv}^{\text{prf-kpa}}_{\mathrm{PRT}^{\gamma}_{\gamma_1,\ldots,\gamma_d}[F]}(t,q) \geq \frac{0.632(q^2W' - qw') - 2}{2^{l+1}} \ .
$$

Proof: The strategy of the adversary will be based on the fact that in a pseudo-random forest, the sub-trees under collisions will be identical, whereas this is unlikely in random forests (for collisions at an internal level).

The strategy of the adversary will be to ask for q trees, and then determine whether at some level in the forest there exists two identical blocks at the same level with different sub-trees. If so, return 0, otherwise, return 1.

The probability of returning 1 when seeing a pseudo-random forest is 1. The advantage will therefore be the probability of returning 0, when seeing a random forest.

Let j denote the index of the first level with collisions, let $j = d+1$ if no level has collisions. Let p_i be the probability that $j = i$ given that $j \geq i$. We compute p_i. If $j \geq i$, then there are no collisions at level $i-1$ of the forest and thus the blocks of level i are uniformly random and independent. Since there are qw_i blocks at level i of the forest, it follows directly from the birthday bound and the fact that $1 - e^{-x} \geq (1-e^{-1})x$, that

$$
p_i \geq 1 - e^{-\frac{qw_i(qw_i-1)}{2^{l+1}}} \geq (1-e^{-1})\frac{qw_i(qw_i-1)}{2^{l+1}} \ .
$$

It thus follows that the probability of collision at an internal level is larger than

$$
(1-e^{-1})\sum_{i=1}^{d} \frac{qw_i(qw_i-1)}{2^{l+1}} \ .
$$

Given that there is a collision at an internal level in the forest, it follows that the probability that all sub-trees under identical blocks are equal is less than 2^{-l}, as we have required that $\gamma_i > 0$. Therefore the probability of returning 0 is larger than

$$(1 - e^{-1}) \sum_{i=1}^{d} \frac{qw_i(qw_i - 1)}{2^{l+1}} - 2^{-l} \ ,$$

which proves the proposition. ■

We now show that the birthday attack is essentially the best possible attack if the underlaying PRF is perfect.

Lemma 1 *For any t, q,*

$$\mathbf{Adv}^{\text{prf-kpa}}_{\mathrm{PRT}^{\gamma}_{\gamma_1,\ldots,\gamma_d}[F]}(t, q) < \frac{(q^2 + 2q)W' - qw'}{2^{l+1}} \ .$$

Proof: It is easy to see that if there is no collision at any internal level of the forest, then the joint output of the q evaluations of $\mathrm{PRT}^{\gamma}_{\gamma_1,\ldots,\gamma_d}[F]_{f_0,\ldots,f_{\gamma-1}}$ is a uniformly random string. Using a conditional probability argument similar to that in the proof of Theorem 1, it is therefore enough to upper bound the probability that such collision occurs.

Assume that e evaluations have been made without producing collisions at any level. This means that level i of the forest consists of ew_i different blocks. We compute the probability $p_{i,e+1}$ of collision at level i or lower in evaluation $e + 1$. It is easy to see that

$$\begin{aligned}
p_{1,e+1} &\leq \frac{e}{2^l} \\
p_{i,e+1} &\leq p_{i-1,e+1} + \frac{(e + \frac{1}{2})w_i^2 - \frac{1}{2}w_i}{2^l} \\
p_{d,e+1} &\leq \frac{(e + \frac{1}{2})W'}{2^l} - \frac{w'}{2^{l+1}} \ .
\end{aligned}$$

It then follows that the probability of any collision at an internal level can be bounded by

$$\frac{\sum_{e=1}^{q}(e + \frac{1}{2})W'}{2^l} - \frac{qw'}{2^{l+1}} = \frac{(q^2 + 2q)W' - qw'}{2^{l+1}} \ .$$

■

Lemma 1 compares PRT mode with uniformly random functions to a uniformly random function. We are now going to compare the consecutive hybrids of PRT mode. For this purpose consider the following experiment:

$$
\begin{aligned}
&\underline{\textbf{proc}}\ \mathbf{Exp}_{F,D}^{\text{prf-kpa-}h} \equiv \\
&\quad f \xleftarrow{R} \mathrm{PRT}_{\gamma_1,\ldots,\gamma_d}^{h}[F] \\
&\quad d \leftarrow D^{\mathcal{R}_f} \\
&\quad \underline{\textbf{return}}\ d
\end{aligned}
$$

For $h = 1, \ldots, \gamma$ we let

$$\mathbf{Adv}_{F,D}^{\text{prf-kpa-}h} = \Pr[\mathbf{Exp}_{F,D}^{\text{prf-kpa-}h} = 1] - \Pr[\mathbf{Exp}_{F,D}^{\text{prf-kpa-}(h-1)} = 1] ,$$

and we let

$$\mathbf{Adv}_{F}^{\text{prf-kpa-}h}(t,q) = \max_{D} \left\{ \mathbf{Adv}_{F,D}^{\text{prf-kpa-}h} \right\} ,$$

where the maximum is over all D with time complexity t and making at most q queries to the oracle.

Lemma 2 *Suppose F is a function family with input-length l and output-length l. Let $0 < h \leq \gamma$, and let i be the level on which the h'th function is used. Then for any t, q,*

$$\mathbf{Adv}_{F}^{\text{prf-kpa-}h}(t,q) \leq \mathbf{Adv}_{F}^{\text{prf-kpa}}(t, w_i q) .$$

Proof: Assume that we are given access to an oracle $\mathcal{R}_f$ returning pairs (R,S), where R is uniformly random and $S = f(R)$ and f is a random function from either F or $\mathrm{Rand}^{l \to l}$. Assume further more that we have a distinguisher $\overline{D}$ expecting to play one of the hybrid experiments. We construct a distinguisher D working as follows.

We start running $\overline{D}$. Each time $\overline{D}$ requests an evaluation, we compute a tree as in hybrid h in Fig. 3. We pick the $h-1$ first functions uniformly random from $\mathrm{Rand}^{l \to l}$, and we pick the $\gamma - h$ last functions at random from F. The h'th function is replaced by the oracle $\mathcal{R}_f$.

To make the process efficient we implement $f \leftarrow \mathrm{Rand}^{l \to l}$ in a lazy manner, by simply creating an empty dictionary. Each time f is evaluated on a value R, we look up R in the dictionary, and if R is a member we return the associated value, and otherwise we generate a uniformly random value S, add (R,S) to the dictionary, and return S.

Since the oracle $\mathcal{R}_f$ does not allow us to evaluate it on a given point R, but returns random evaluations (R,S), we need to be careful about how we use the oracle. Each time a value R, on which we will later need to evaluate the h'th function, is chosen at random (as the output of a lazy evaluated random function at level $i-1$) we proceed as follows. Instead of generating R directly, we query the oracle $\mathcal{R}_f$ and get a random evaluation (R,S). We then use R as the random value. When we later need to evaluate the h'th function on R, we simply use S as the output. When at some point $\overline{D}$ returns some value d, we let D return d.

By construction, if f is a uniformly random function, then $\overline{D}$ is run in the experiment $\mathbf{Exp}_{F,\overline{D}}^{\text{prf-kpa-}h}$, and if f is a random function from F, then $\overline{D}$ is run in the experiment $\mathbf{Exp}_{F,\overline{D}}^{\text{prf-kpa-}(h-1)}$. As D queries the oracle w_i times for each query from $\overline{D}$, we have that $\mathbf{Adv}_F^{\text{prf-kpa-}h}(\overline{t}, q) \leq \mathbf{Adv}_F^{\text{prf-kpa}}(t, w_i q)$, where t is the running time of D (including the time spend by the oracle), when $\overline{D}$ has running time t (including the time spend by the oracle). Since the dictionaries can be maintained in constant time on a RAM, we can safely assume that the computations done by D in computing the hybrid is less than that used computing an actual PRT. Thus $t \leq \overline{t}$, and the lemma follows. ■

Theorem 2 *Suppose F is a function family with input-length l and output-length l. If F is PRF-KPA secure, then* $\mathrm{PRT}_{\gamma_1,\ldots,\gamma_d}[F]$ *is PRF-KPA secure. Specifically, for any t, q,*

$$\mathbf{Adv}_{\mathrm{PRT}_{\gamma_1,\ldots,\gamma_{d-1}}[F]}^{\text{prf-kpa}}(t,q) < \sum_{i=1}^{d}(\gamma_i \mathbf{Adv}_F^{\text{prf-kpa}}(t, w_i q)) + \frac{(q^2+2q)W' - qw'}{2^{l+1}}$$
$$\leq \gamma \mathbf{Adv}_F^{\text{prf-kpa}}(t, wq) + \frac{3(wq)^2}{2^{l+1}} \ .$$

Proof: Using that

$$\mathbf{Adv}_{\mathrm{PRT}_{\gamma_1,\ldots,\gamma_d}[F]}^{\text{prf-kpa}}(t,q) \leq \sum_{h=1}^{\gamma} \mathbf{Adv}_F^{\text{prf-kpa-}h}(t,q) + \mathbf{Adv}_{\mathrm{PRT}^{\gamma}_{\gamma_1,\ldots,\gamma_d}[F]}^{\text{prf-kpa}}(t,q) \ ,$$

the theorem follows directly from Lemmas 1 and 2. ■

3.3 Variable-Length Output PRT

Until now, we have described PRT mode as a fixed-length PRF. It is however possible to construct a variable-length output version, by generating the keys for branching at level $i+1$ by using some of the pseudo-random blocks of level i. These blocks are then of course not used as output from the pseudo-random generator. Assuming, for notational convenience, that random blocks can also be used as keys, an instance of the variable-length version can be sketched as in Fig. 4. The key of the system is $(K_0^1, K_1^1, K_2^1, K_3^1)$ and the seed is R_0^1. It is easy to see that given the key, all keys can be generated using no more than $4d$ evaluations of F, and after the keys have been generated, given the seed, any block can be random accessed using at most d evaluations of F.

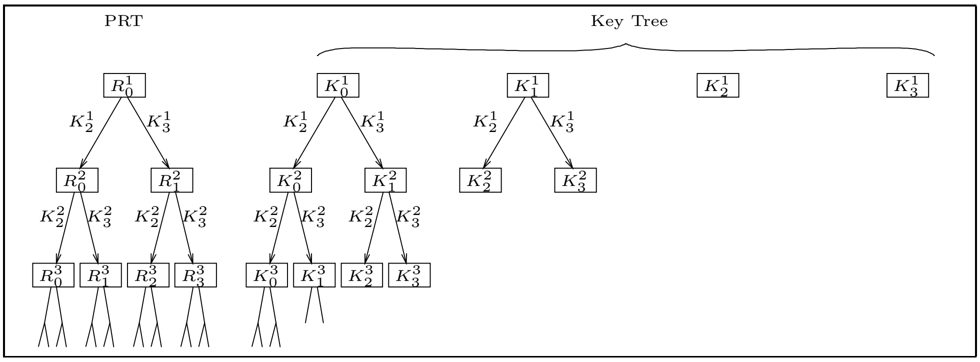

Figure 4: Variable-length PRT Mode. Only the leftmost tree is used as the pseudo-random output. The key tree is used to generate a variable number of level keys.

If the parties only share one key K for a symmetric encryption scheme, then the sender can choose $(K_0^1, K_1^1, K_2^1, K_3^1)$ at random and encrypt as

$$(R_0^1, E_K(K_0^1), E_K(K_1^1), E_K(K_2^1), E_K(K_3^1), \mathrm{PRT}_{K_0^1,K_1^1,K_2^1,K_3^1}(|M|, R_0^1) \oplus M) \ .$$

The variable-length output mode can be proven secure using the technique of Theorem 2. The only difference now being that the levels have become four blocks wider. We get the following theorem.

Theorem 3 *Suppose F is a function family with input-length l and output-length l. If F is PRF-KPA secure, then* PRT$[F]$ *is VO-PRF-KPA secure. Specifically, for any t, q, d,*

$$\mathbf{Adv}_{\mathrm{PRT}[F]}^{\text{vo-prf-kpa}}(t, q, q(2^{d+1}-1)l) < 2d\mathbf{Adv}_F^{\text{prf-kpa}}(t, 2^{d+2}q) + \frac{3(q2^{d+1})^2}{2^l} \ ,$$

assuming that each of the q generations are of at most $(2^{d+1}-1)l$ bits (a full depth-d PRT).

Combined with Theorem 1 we then get the following theorem.

Theorem 4 *Suppose F is a function family with input-length l and output-length l. If F is PRF-KPA secure, then* VO-PRF-ENC[PRT$[F]$] *is ROR-CPA secure. Specifically, for any t, q, d,*

$$\mathbf{Adv}_{\text{VO-PRF-ENC[PRT}[F]]}^{\text{ror-cpa}}(t, q, q(2^{d+1}-1)l) < 2d\mathbf{Adv}_F^{\text{prf-kpa}}(t, 2^{d+2}q) + \frac{4(q2^{d+1})^2}{2^l} \ .$$

assuming that each of the q encryptions are of at most $(2^{d+1}-1)l$ bits.

proc $\text{CBC}[P]_K(M) \equiv$
$m \leftarrow \lceil |M|/l \rceil$
$n \leftarrow ml - |M|$
$r \xleftarrow{R} \{0,1\}^n$
$M \leftarrow M \| r$
$c_0 \xleftarrow{R} \{0,1\}^l$
for $i = 0$ **to** $m-1$ **do**
$x_i \leftarrow M[il..((il+l-1)] \oplus c_i$
$c_{i+1} \leftarrow P_K(x_i)$
od
return $(n, c_0 \| c_1 \| \ldots \| c_m)$

proc $\text{CTR}[F]_K(M) \equiv$
$m \leftarrow \lceil |M|/L \rceil$
$n \leftarrow |M| - (m-1)L$
$r \xleftarrow{R} \{0,1\}^l$
for $i = 1$ **to** m **do**
$r_i \leftarrow F_K(r + 1 \bmod 2^l)$
od
$R \leftarrow r_1 \| \ldots \| r_{m-1} \| r_m[1..n]$
return $(r, M \oplus R)$

Figure 5: CBC[P] mode and CTR[F] mode.

4 Analysis and Comparison of CBC, CRT, and PRT

We are going to prove the results given by the below table, where the entry MODE / ATK_{impl} being set to ATK_{mode} means that the encryption mode MODE is ATK_{mode} secure when the underlying function family is ATK_{impl} secure, and that there exists a function family or permutation family G, as appropriate, being ATK_{impl} secure for which MODE_G is not ATK secure for any attack ATK stronger than ATK_{mode}.

MODE / ATK_{impl}	**PRF-KPA**	**PRF-CPA**
CBC	ROR-KPA	ROR-CPA
CTR	insecure	ROR-CPA
PRT	ROR-CPA	ROR-CPA

The bottom row and the right-most column follows from known results from [BDJR97] and Section 3. We now prove in Theorems 5 and 6 that PRF-KPA security of the underlying permutation family implies ROR-KPA security of CBC mode and that it implies no stronger security. We then prove in Theorem 7 that counter mode based on a PRF-KPA secure function family is not necessarily ROR-KPA secure. The CBC and CTR encryption modes are given in Fig. 5.

Theorem 5 *Suppose P is a permutation family with length l. If P is PRF-KPA secure, then* CBC[P] *is ROR-KPA secure. Specifically, for any t, q,*

$$\mathbf{Adv}^{\text{ror-kpa}}_{\text{CBC}[P]}(t, q, \mu) \leq \mathbf{Adv}^{\text{prf-kpa}}_{P}(t, \nu) + \frac{\nu(\nu-1)}{2^{l+2}} \ ,$$

where $\nu = \lfloor \mu/l \rfloor + q$.

Proof: Consider an ROR-KPA distinguisher $\overline{D}$ expecting access to an oracle $\mathcal{R}_{K,b}$ for the CBC[P] scheme. We construct a distinguisher D having access to a PRF-KPA oracle $\mathcal{R}_f$ for the permutation family P as follows. The distinguisher D runs the code of $\overline{D}$. Each time D requests an encryption of length m', request $m = \lceil m'/l \rceil$ pairs $(x_i, f(x_i))$ from $\mathcal{R}_f$. Then generate a random l-bit string c_0 and for $i = 1, \ldots, m$ let $c_i = f(x_i)$ and let $p_i = x_i \oplus c_{i-1}$. Then output $(M, C) = (p_1 \| \ldots \| p_m, (ml - m', c_0 \| c_1 \| \ldots \| c_m)$.

In all cases M is uniformly random and C is distributed exactly as a CBC encryption of p using f. So, if $f = P_K$ is a random permutation from P, then (M, C) is distributed exactly as values from $\mathcal{R}_{K,1}$, and if f is a random function, then C is uniformly random and independent of M, unless M has collisions among the blocks. Using a conditional probability argument similar to that in the proof of Theorem 1, the theorem then follows. ■

Theorem 6 *For any permutation family P with length l, there exists a permutation family $\overline{P}$ such that $\overline{P}$ is PRF-KPA secure if P is PRF-KPA secure, but* CBC[$\overline{P}$] *is not ROR-CPA secure. Specifically, for any t, q and for some small t',*

$$\mathbf{Adv}_{\overline{P}}^{\text{prf-kpa}}(t, q) \leq \mathbf{Adv}_{P}^{\text{prf-kpa}}(t, 2q) + \frac{16q^2}{2^{l+1}}$$

$$\mathbf{Adv}_{\text{CBC}[\overline{P}]}^{\text{ror-cpa}}(t', 1, 4l) \geq 1 - 2^{-2l} \ .$$

Proof: Given some permutation family P, consider the permutation family $\overline{P}$ given by $\overline{P}_K(x_1, x_2) = (P_K^{-1}(x_2), P_K(x_1))$.

Proof of the first claim: Given a PRF-KPA oracle for P, we simulate a PRF-KPA oracle for $\overline{P}$ as follows. Given request for evaluation, ask for two random evaluations $(x_1, y_1), (x_2, y_2)$ and return $((x_1, y_2), (x_2, y_1))$. If we have access to a permutation from the permutation family, the distribution is correct. If we have access to a random function, then the output is distributed as independent pairs $((x_1, x_2), \overline{P}(x_1, x_2))$, where $\overline{P}$ is uniformly random from $\text{Rand}^{2l \to 2l}$, unless there are collisions among the $4q$ values returned by the oracle for P. This proves the first claim.

Proof of the second claim: Ask for an encryption of the all-zero-string of length $4l$. If the encryption is of the form $((x_1, x_2), (y_1, y_2), (x_1, x_2))$, then answer 1, otherwise answer 0. If the answer is not of this form we known that it is random. The probability of being on this form for random values is 2^{-2l}, which proves the second claim. ■

Theorem 7 *For any permutation family P with length l, there exists a permutation family $\overline{P}$ such that $\overline{P}$ is PRF-KPA secure if P is PRF-KPA secure,* *but* CTR[$\overline{P}$] *is not ROR-KPA secure. Specifically, for any* t, q *and for some small* t'*,*

$$\mathbf{Adv}_{\overline{P}}^{\text{prf-kpa}}(t,q) \leq \mathbf{Adv}_{P}^{\text{prf-kpa}}(t,2q) + \frac{4q^2}{2^{l+1}}$$
$$\mathbf{Adv}_{\text{CTR}[\overline{P}]}^{\text{ror-kpa}}(t',1,6l) \geq 1 - 2^{-l+1} \ .$$

Proof: Given some permutation family P, consider the permutation family $\overline{P}$ given by $\overline{P}_K(x_1, x_2) = (P_K(x_1), P_K(x_2))$.
Proof of the first claim: Consider a PRF-KPA distinguisher $\overline{D}$ for the family $\overline{P}$. We construct a distinguisher D with access to a PRF-KPA oracle $\mathcal{R}_f$ for the family P. The distinguisher D tries to simulate a PRF-KPA oracle $\overline{\mathcal{R}}_{\overline{f}}$ for the family $\overline{P}$ to $\overline{D}$. Each time $\overline{D}$ requests a generation, D requests two generations from $\mathcal{R}_f$ and receives $(x_1, f(x_1))$ and $(x_2, f(x_2))$, and then D returns $((x_1, x_2), (f(x_1), f(x_2)))$ to $\overline{D}$. After $\overline{D}$ returns with a value d, D returns d.

If $b = 1$, then f is a random permutation from P and the values $((x_1, x_2), (f(x_1), f(x_2)))$ are distributed as random values from $\overline{\mathcal{R}}_{\overline{f}}$. If on the other hand $b = 0$, then f is a uniformly random function. In that case the values $((x_1, x_2), (f(x_1), f(x_2)))$ are distributed as independent values, where each (x_1, x_2) is a uniformly random $2l$-bit string and $(f(x_1), f(x_2))$ is a uniformly random $2l$-bit string independent of all other values, as long as there are no collisions among the x_i-values returned by $\mathcal{R}_f$. This proves the first claim.
Proof of the second claim: Ask for an encryption of length $6l$. Let $(x, (r, y))$ be the answer and compute $z = y \oplus x$. If $b = 1$, then $z = \overline{P}(r)\overline{P}(r + 1 \bmod 2^{2l})\overline{P}(r + 2 \bmod 2^{2l})$. Writing $r = r_1 r_2$, where r_1 and r_2 have length l, there must be r' among $r, (r + 1 \bmod 2^{2l})$, where $r'_2 < 2^l - 1$. This implies that $r' = r'_1 r'_2, r' + 1 = r'_1(r'_2 + 1 \bmod 2^l)$ and thus $\overline{P}(r')\overline{P}(r' + 1 \bmod 2^{2l}) = P(r'_1)P(r'_2)P(r'_1)P(r'_2 + 1)$. Writing $z = z_1 z_2 z_3 z_4 z_5 z_6$, we thus have that, if $b = 1$, then either $z_1 = z_3$ or $z_3 = z_5$. If on the other hand $b = 0$, then x is independent of y and thus $z = y \oplus x$ is a uniformly random value, and the probability that $z_1 = z_3$ or $z_3 = z_5$ is no larger than 2^{-l+1}, which proves the second claim. ■

5 CCA Security

Having constructed CPA secure encryption, we can construct CCA secure encryption using a number of known techniques. All these techniques however seem to require something stronger than a KPA secure cipher. We find it an interesting open question whether CCA secure encryption can be based solely on a KPA secure block cipher.

As an example we can construct a CCA secure encryption scheme E^{cca} from a CPA secure encryption scheme E^{cpa} and a Message Authentication Code (MAC) A, by letting $E^{\mathrm{cca}}_{K_1,K_2}(M) = E^{\mathrm{cpa}}_{K_1}(M \| A_{K_2}(M))$. A MAC A^{kma} which is Known-Message Attack (KMA)[2] secure against existential forgery is enough. From a KMA secure MAC we can construct a Chosen-Message Attack (CMA) secure MAC as follows, see [CDT96]. On input a message M, generate $R \stackrel{R}{\leftarrow} \{0,1\}^{|M|}$ and $id \stackrel{R}{\leftarrow} \{0,1\}^k$ and let $A^{\mathrm{cma}}_{K_1,K_2}(M) = (A^{\mathrm{kma}}_{K_1}(id\|R), A^{\mathrm{kma}}_{K_2}(id\|(M \oplus R)))$. It is however an open question whether a KMA secure MAC can be constructed from a KPA secure block cipher. All known constructions seem to fail.

Also other constructions of CCA secure encryption fail if based solely on a KPA secure block cipher. We look at two concrete constructions to give an idea why this is so.

In [Des00] Desai introduces two paradigms for constructing CCA secure symmetric encryption. His paradigms are interesting in that they produce CCA secure encryption schemes in which every string is a valid ciphertext. This allows for a smaller ciphertext expansion than in non-malleable encryption schemes. However, no scheme in which every string is a valid ciphertext can be based solely on a KPA block cipher, it seems. The reason being that when the decryption oracle is queried, a simulator is forced to decrypt, which seems to require access to a CPA oracle for the underlying function, to e.g. generate a PRT. The scheme in [Des00] also fails for more specific reasons as it is based on a CRT mode construction, c.f. Theorem 7.

Considering non-malleable schemes, the constructions fail for almost the same reason. Consider e.g. the scheme $E^{\mathrm{cca}}_K(M) = E^{\mathrm{cpa}}_K(M\|h(M))$, where h is a (two universal) hash function, see e.g. [Sho96]. Here it seems computationally infeasible for a distinguisher to produce a correct ciphertext. If, however, we assume that a distinguisher does so anyway, it requires that a simulator can actually determine that this has happened to turn this exceptional event into a distinguishing advantage. However, determining whether a ciphertext is correct again seems to require a decryption, which in turn requires access to a CPA oracle for the underlying function.

References

[BDJR97] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A concrete security treatment of symmetric encryption. In *38th Annual Symposium on Foundations of Computer Science*, Miami Beach, FL, 19–22 October 1997. IEEE.

[2] The adversary sees MACs of random messages and has oracle access to a MAC verifier.

[CDT96] R. Cramer, I. Damgård, and T.P. Pedersen Efficient and Provable Security Amplifications. In *Proceedings of 4th Cambridge Security Protocols Workshop*, pages 101–109, April 1996. Springer-Verlag. Lecture Notes in Computer Science Volume 1189.

[Des00] A. Desai. New paradigms for constructing symmetric encryption schemes secure against chosen-ciphertext attack. In Mihir Bellare, editor, *Advances in Cryptology - Crypto 2000*, pages 394–412, Berlin, 2000. Springer-Verlag. Lecture Notes in Computer Science Volume 1880.

[Sho96] V. Shoup. On fast and provably secure message authentication based on universal hashing. In Neal Koblitz, editor, *Advances in Cryptology - Crypto '96*, pages 313–328, Berlin, 1996. Springer-Verlag. Lecture Notes in Computer Science Volume 1109.

Recent BRICS Report Series Publications

RS-01-43 **Ivan B. Damgård and Jesper Buus Nielsen.** ***From Known-Plaintext Security to Chosen-Plaintext Security*****. November 2001. 18 pp.**

RS-01-42 **Zoltán Ésik and Werner Kuich.** ***Rationally Additive Semirings*****. November 2001. 11 pp.**

RS-01-41 **Ivan B. Damgård and Jesper Buus Nielsen.** ***Perfect Hiding and Perfect Binding Universally Composable Commitment Schemes with Constant Expansion Factor*****. October 2001. 43 pp.**

RS-01-40 **Daniel Damian and Olivier Danvy.** ***CPS Transformation of Flow Information, Part II: Administrative Reductions*****. October 2001. 9 pp.**

RS-01-39 **Olivier Danvy and Mayer Goldberg.** ***There and Back Again*****. October 2001. 14 pp.**

RS-01-38 **Zoltán Ésik.** ***Free De Morgan Bisemigroups and Bisemilattices*****. October 2001. 13 pp.**

RS-01-37 **Ronald Cramer and Victor Shoup.** ***Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption*****. October 2001. 34 pp.**

RS-01-36 **Gerth Stølting Brodal, Rolf Fagerberg, and Riko Jacob.** ***Cache Oblivious Search Trees via Binary Trees of Small Height*****. October 2001.**

RS-01-35 **Mayer Goldberg.** ***A General Schema for Constructing One-Point Bases in the Lambda Calculus*****. September 2001. 6 pp.**

RS-01-34 **Flemming Friche Rodler and Rasmus Pagh.** ***Fast Random Access to Wavelet Compressed Volumetric Data Using Hashing*****. August 2001. 31 pp.**

RS-01-33 **Rasmus Pagh and Flemming Friche Rodler.** ***Lossy Dictionaries*****. August 2001. 14 pp. Short version appears in Meyer auf der Heide, editor,** ***9th Annual European Symposiumon on Algorithms*****, ESA '01 Proceedings, LNCS 2161, 2001, pages 300–311.**