# All-or-Nothing Transforms as a Countermeasure to Differential Side-Channel Analysis

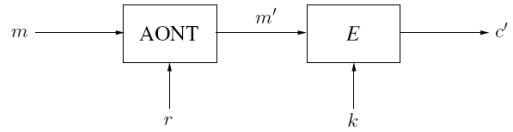
Robert P. McEvoy[1], Michael Tunstall[2], Claire Whelan[3], Colin C. Murphy[1] and William P. Marnane[1]

[1]*Coding & Cryptography Research Group, Department of Electrical & Electronic Engineering, University College Cork, IRELAND.*
[2]*Department of Computer Science, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol BS8 1UB, United Kingdom.*
[3]*TDS (Time Data Security) Ltd., 2060 Castle Drive, Citywest Business Campus, Naas Road, Dublin 24, Ireland.*
*E-mail:* {robertmce, cmurphy, liam}@eleceng.ucc.ie, tunstall@cs.bris.ac.uk claire.whelan@tds.ie

[2,3]This work was carried out while the authors were working at University College Cork. Patent Pending.

## 1. All-or-Nothing Encryption

- All-or-Nothing Transforms (AONT) were proposed by Rivest in 1997 [1], as a mechanism to hinder exhaustive key searches.
- All-or-Nothing Encryption functions by transforming a plaintext into a pseudo-message before encrypting it.




| All-or-Nothing Encryption | All-or-Nothing Decryption |
|---|---|
| Inputs: plaintext $m$, randomness $r$ | Inputs: ciphertext $c'$ |
| 1. $m' = \text{AONT}_r(m)$; | 1. $m' = D_k(c')$; |
| 2. $c' = E_k(m')$; | 2. $(m, r) = \text{Inv-AONT}(m')$; |

**Figure 1.** All-or-Nothing Encryption

- All-or-Nothing Transforms are defined as having the following properties.
  1. The transform should be invertible. Given the entire pseudo-message, one can invert the transform to retrieve the plaintext.
  2. Both the AONT and its inverse should be efficiently computable.
  3. All AONTs should be randomised, in order to avoid chosen-message and known-message attacks on the encryption mode.
  4. If any *m* (or more) bits of the pseudo-message are unknown, it should be computationally infeasible to invert the AONT, or determine any function of the plaintext bits. We call this the ``All-or-Nothing" property. The value of *m* is AONT-dependent, but is large enough to deter brute force attacks on the pseudo-message.
- Property 3, above, implies that *m'* is not a deterministic function of the plaintext *m*. This will mean that an attacker will not be able to form hypotheses on any intermediate states of the encryption algorithm *E*.
- All-or-Nothing Encryption is therefore resistant to Differential Side-Channel Analysis where an attacker only has knowledge of the plaintext *m*.

## 2. General model for All-or-Nothing Transforms

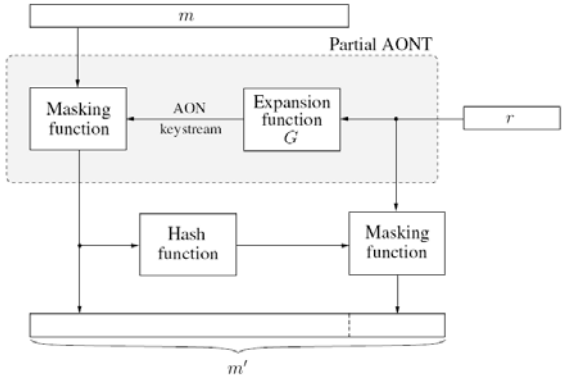



**Figure 2.** General Model for All-or-Nothing Transforms.

- Figure 2 presents a general model for All-or-Nothing Transforms. Where the function partial AONT could, for example, be OAEP [2].

## 3. Extending the Side Channel Resistance of All-or-Nothing Encryption

- In an implementation it could be expected that an attacker could have access to the resulting ciphertext. An attacker would then be able to conduct a Differential Side Channel Analysis by forming hypotheses based on knowledge of the computed functions towards the end of the computation of *E*.
- It is therefore necessary to include a Post Encryption Transform (PET) to prevent an attacker basing hypotheses on the ciphertext.

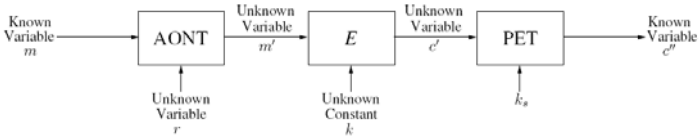



**Figure 3.** Extended All-or-Nothing Encryption.

- The properties that are required for a PET, are as follows:
  1. A PET should be dependent on a shared secret $k_s$.
  2. A PET should not linearly combine the output of the encryption with a constant.
  3. A PET should be resistant to Differential Side Channel Analysis.

## 4. Proposed Side Channel Resistant of All-or-Nothing Encryption

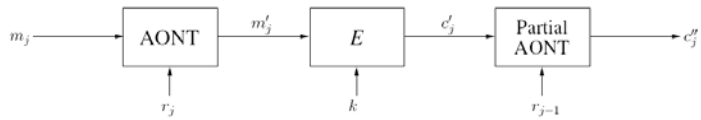



**Figure 4.** Extended All-or-Nothing Encryption with Partial AONT.

- The plaintext *m* is divided up into packets $m_j$, where random used to randomise the message packet *i* is used to randomise ciphertext *i*-1.
- Where r0 is required to be some secret value known to the sender and the legitimate receiver.

## 5. Efficient Encryption

- The above extension can be combined with "efficient encryption", as presented in [4].

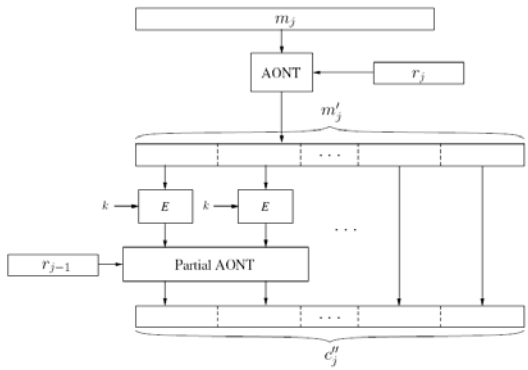



**Figure 5.** Combining Extended All-or-Nothing Encryption with Efficient Encryption.

- Where the encryption algorithm *E* only needs to be applied to part of the pseudo-message block $m_j$'.

**References**

[1] Ronald L. Rivest. All-or-Nothing Encryption and the Package Transform. In FSE '97, 4th International Workshop on Fast Software Encryption, pages 210–218, 1997.
[2] Mihir Bellare and Phillip Rogaway. Optimal asymmetric encryption. In Alfredo De Santis, editor, Advances in Cryptology – EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, volume 950 of Lecture Notes in Computer Science, pages 92–111. Springer, 1994.
[3] Whitfield Diffie and Martin E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, volume 22, pages 644–654, 1976.
[4] Donald Byron Johnson and Stephen Michael Matyas, Jr. Method and apparatus for encrypting long blocks using a short-block encryption procedure. US Patent # 5,870,470, February 1999.

*Cryptographic Hardware and Embedded Systems – CHES 2008, 10th* International Workshop, Washington, D.C., USA, August *2008*

Supported in part by: embarkinitiative Investing in People and Ideas