CTR-Mode Encryption

Helger Lipmaa
Helsinki University of Technology (Finland)
University of Tartu (Estonia)

Phillip Rogaway
University of California - Davis (USA)
Chiang Mai University (Thailand)

David Wagner
University of California - Berkeley (USA)
What is CTR Mode?

* The simplest correct way to encrypt using a block cipher

* An old mode, dating to DH79, but omitted from earlier FIPS

* A Vernam cipher (like a one-time pad), but no state is maintained by the sender

Why the renewed interest?

* Because CTR mode is fully parallelizable, making it much more efficient, in many contemporary usage scenarios, than modes like CBC.
CTR Mode Encryption


```
CTR Mode Encryption

\[EK\]

\[M[1] \oplus \text{ctr} \rightarrow C[1] \]

\[EK\]

\[M[2] \oplus \text{ctr + 1} \rightarrow C[2] \]

\[EK\]

\[M[3] \oplus \text{ctr + 2} \rightarrow C[3] \]
```
CTR Mode Decryption

Where does the \texttt{ctr} come from?

* It is supplied on the encrypting side (like the IV in CBC mode)

* It is \textbf{crucial} that no \texttt{ctr+i} value be repeated - repeating such a value is like reusing a one-time pad.

* Recommended way of making \texttt{ctr}:

\[
\texttt{ctr} = \texttt{nonce} \ || \ 0000 \ldots 0000 \\
\quad \ldots 64 \textit{bits} \quad \ldots 64 \textit{zero bits} \quad \ldots
\]
Advantages

* Faster SW speed on modern processors (Itanium, Alpha, AltiVec, etc.)
* Essentially unlimited HW speed
* Provably secure  (Same bounds as CBC MAC, same assumption [BDJR])
* Random access to the "middle" of the ciphertext
* Preprocessing possible
* Arbitrary message lengths
* No need to implement $E^{-1}$
* Completely patent-free
Complaint | Answer
---|---
No integrity | Right. Just like all the other conventional modes. For integrity, use a MAC or an authenticated-encryption mode.
No error propagation | So what.
Sender needs state or $ | Right. True of any secure enc scheme.
Sensitive to usage errors | Some validity. Be clear: *do not reuse a* ctr value! Counter/nonce distinction helps.
Quad sec bound | Encrypted MAC or an authenticated-encryption mode.
Interaction with weak ciphers | Use with strong block cipher. Like other modes; n=128 makes OK.