




Выполнил(а) Коломиец Н.С., № группы P3108, оценка не заполнять  
 Фамилия И.О. студента

<b>Название статьи/главы книги/видеолекции</b> Неужто так сложно передать зашифрованный файл? Эволюция формата пакетов NNCP		
<b>ФИО автора статьи (или e-mail)</b> stargrave2	<b>Дата публикации (не старше 2019 года)</b> 09 октября 2022 г.	<b>Размер статьи (от 400 слов)</b> 2к+ слов
<b>Прямая полная ссылка на источник или сокращённая ссылка (bit.ly, tr.im и т.п.)</b> <a href="https://habr.com/ru/post/692254/">https://habr.com/ru/post/692254/</a>		
<b>Теги, ключевые слова или словосочетания</b> Децентрализованные сети, Криптография, merkle tree, AEAD, NNCP, UUCP, privacy		
<b>Перечень фактов, упомянутых в статье</b> <ol style="list-style-type: none"> <li>1. Временный файл, который использовался для определения размера пакета, заменен на дописывание информации о размере блока в сам блок</li> <li>2. Используемые в нынешних протоколах функции AEAD не гарантируют прирост к скорости шифрования или увеличения безопасности, если сравнивать с обычными функциями шифрования</li> <li>3. Используя дерево Меркле, решается проблема потери состояния хеш-функции.</li> <li>4. Добавление псевдорандомного мусора в пакет и использование промежуточного пакета помогает решить проблему приватности пакета.</li> </ol>		
<b>Позитивные следствия и/или достоинства описанной в статье технологии (минимум три пункта)</b> <ol style="list-style-type: none"> <li>1. Возможность потокового создания зашифрованного пакета данных</li> <li>2. Явная аутентификация размера полезной нагрузки и дополнения в пакете</li> <li>3. Отсутствие необходимости использовать временный файл</li> </ol>		
<b>Негативные следствия и/или недостатки описанной в статье технологии (минимум три пункта)</b> <ol style="list-style-type: none"> <li>1. Отсутствие приватности отправителя в базовом варианте NNCP</li> <li>2. Для обозначения размера полезной нагрузки появляется необходимость создания дополнительного ключа</li> <li>3. Из-за того что протокол NNCP не анонимен и есть необходимость непрерывно высчитывать хеш-блоки и пр., увеличивается размер передаваемого пакета.</li> </ol>		
<b>Ваши замечания, пожелания преподавателю или анекдот о программистах<sup>1</sup></b> <div> <div> <p>This poor kid has no idea the harsh reality that is coming to him</p>  </div> <div> <p>my brain on a sunday at 3am</p>  <p>I just reduced this call from <math>O(n^{**2})</math> to <math>O(1)</math></p> </div> <div> <p>my brain on a wednesday 2pm</p>  <p>help me, what is an interface</p> </div> </div>		

<sup>1</sup> Наличие этой графы не влияет на оценку