Future Anonymity in Today's Budget
(Post-Quantum Forward Secure Onion Routing)

Aniket Kate

MMCI, Saarland University
Germany

Joint work with Satrajit Ghosh

Appearing at ACNS 2015

UNIVERSITÄT DES SAARLANDES

M2CI CLUSTER OF EXCELLENCE

CISPA Center for IT-Security, Privacy and Accountability

Outline

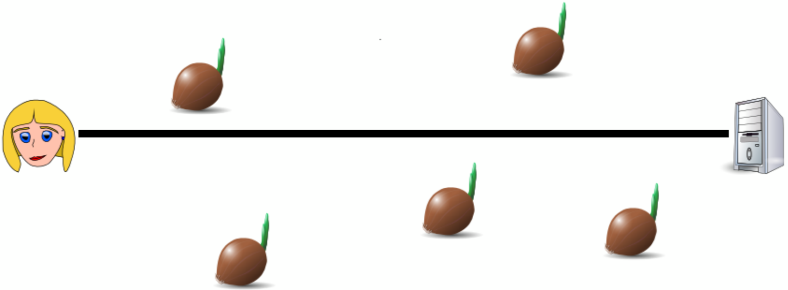
- Anonymity over the Internet and Tor
- One-Way Authenticated Key Exchange (1W-AKE)
- Towards a post-quantum forward secure 1W-AKE
- Our HybridOR Protocol
- Security and Performance Analyes

Anonymity

Ability to remain unnoticed or unidentified

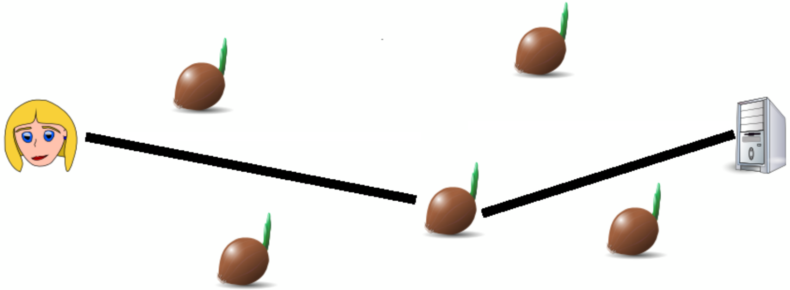
Source: `http://weskenney.net/?p=232`

Anonymous Communication



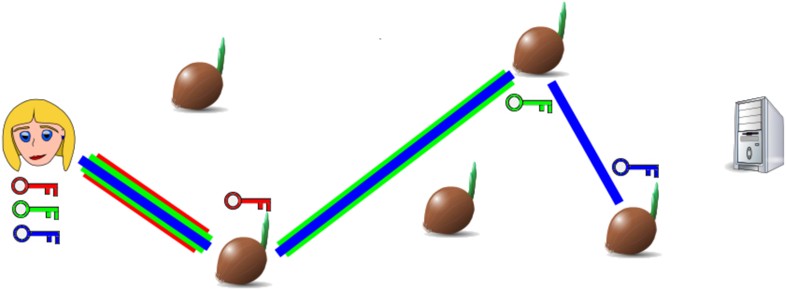
Anonymous Communication

Single Hop Circuits: Anonymizer.com

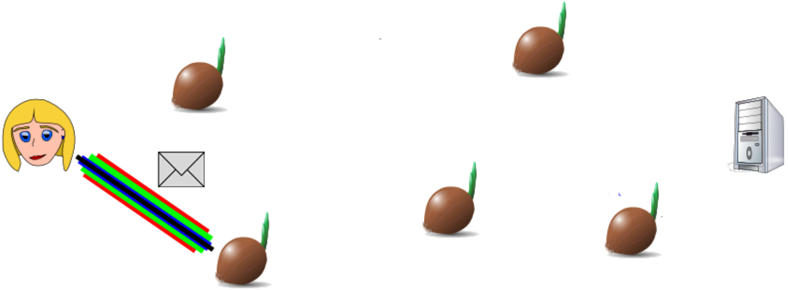


Drawbacks: Traffic Analysis, Trust on Anonymizer.com

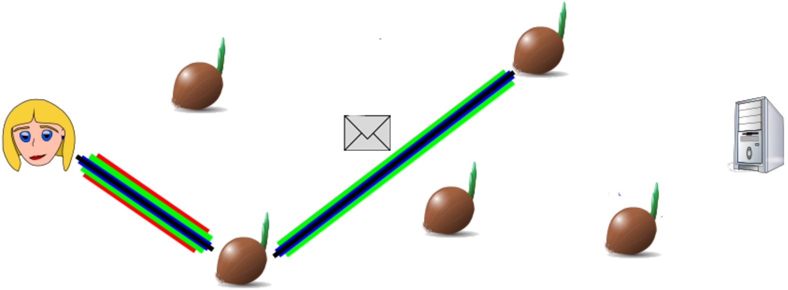
Onion Routing



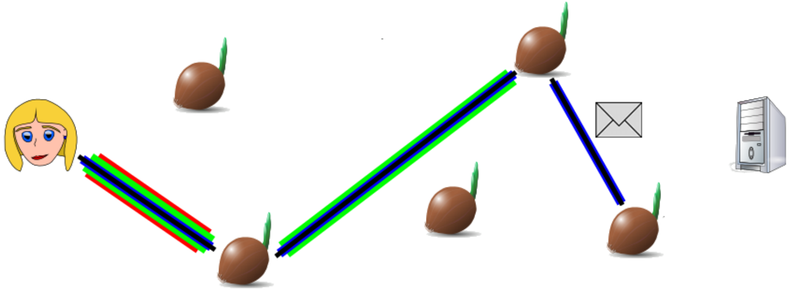
Onion Routing



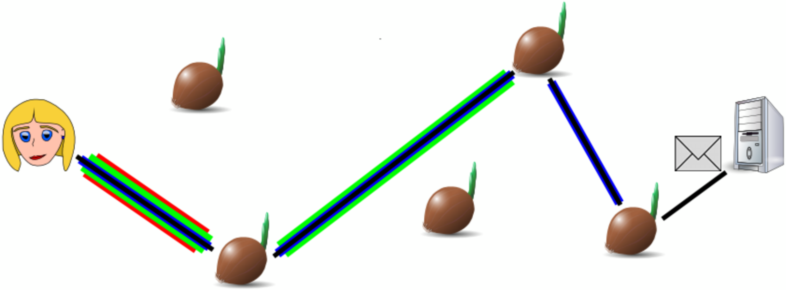
Onion Routing



Onion Routing



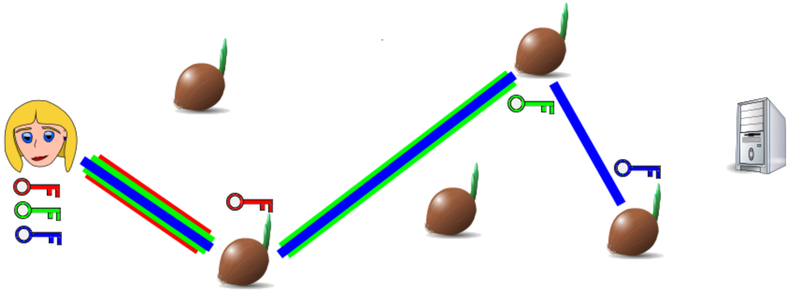
Onion Routing



Goal: Making the attacker goal of linking multiple communication flows from a single user difficult

Onion Routing Circuit Construction

How Keys are Shared?



This asks for one-way anonymous one-way authenticated key exchange (1W-AKE), which require a public-key infrastructure (PKI)

1W-AKE Security

[Goldberg, Stebila and Ustaoglu, DCC ’12]

1W-AKE Security

[Goldberg, Stebila and Ustaoglu, DCC '12]

Protocol Correctness

1W-AKE Security

An attacker cannot learn anything about the session key of a challenge session, even if it

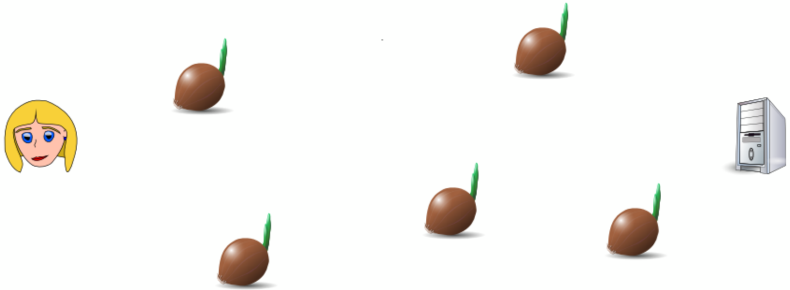
- compromises several other sessions and
- introduces fake identities
- compromise exactly one of two secrets from the node in the challenge session

1W-Anonymity

A node should not differentiate while communicating with two different clients

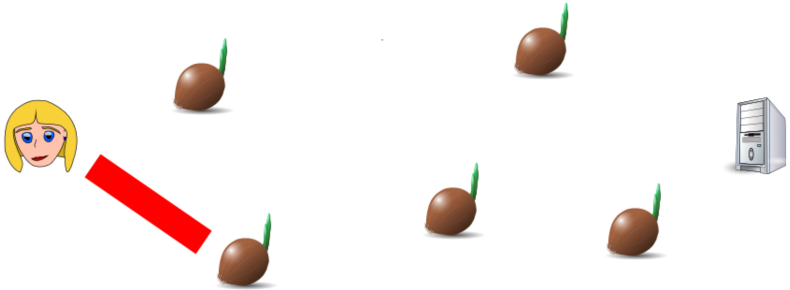
Second/Third Generation Onion Routing: Tor

Multi-Pass Construction (Telescoping Approach)



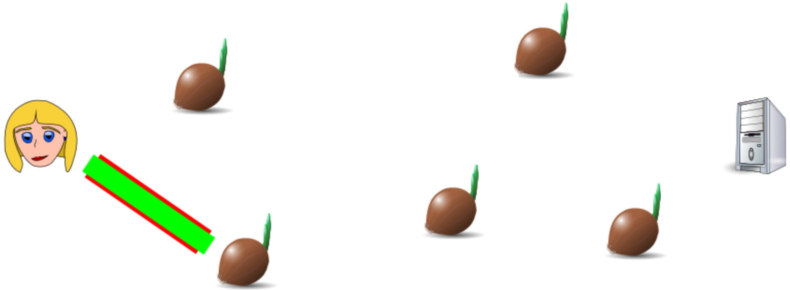
Second/Third Generation Onion Routing: Tor

Multi-Pass Construction (Telescoping Approach)



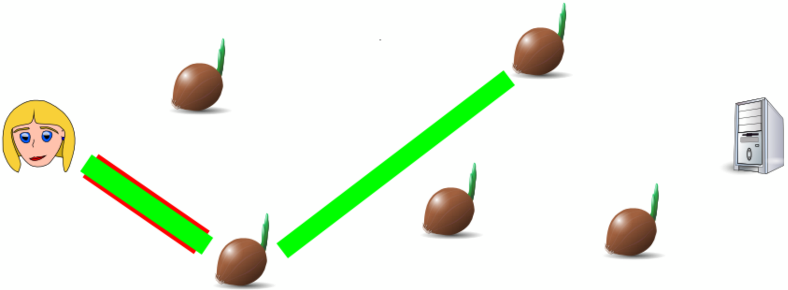
Second/Third Generation Onion Routing: Tor

Multi-Pass Construction (Telescoping Approach)



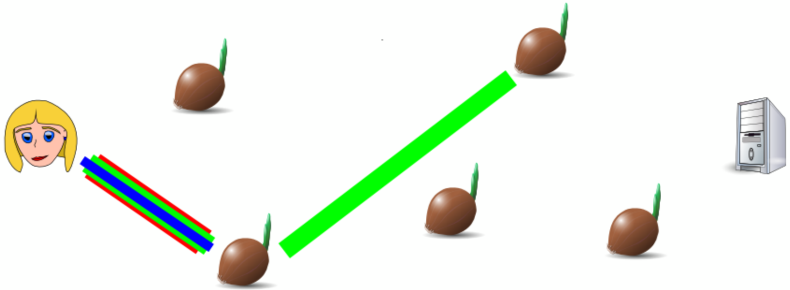
Second/Third Generation Onion Routing: Tor

Multi-Pass Construction (Telescoping Approach)



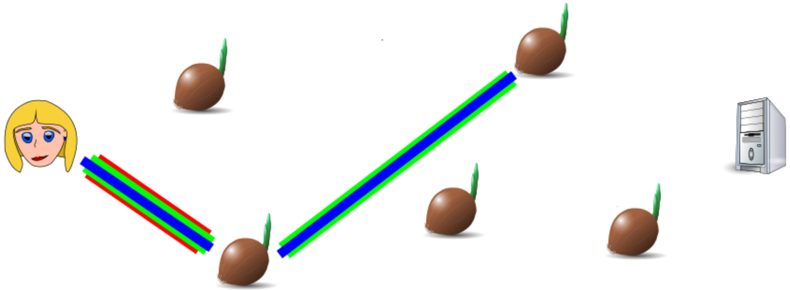
Second/Third Generation Onion Routing: Tor

Multi-Pass Construction (Telescoping Approach)



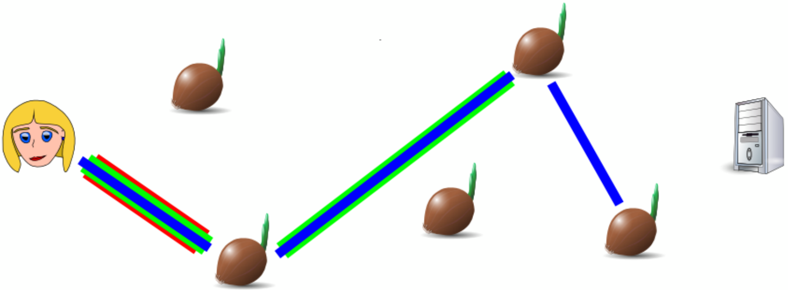
Second/Third Generation Onion Routing: Tor

Multi-Pass Construction (Telescoping Approach)



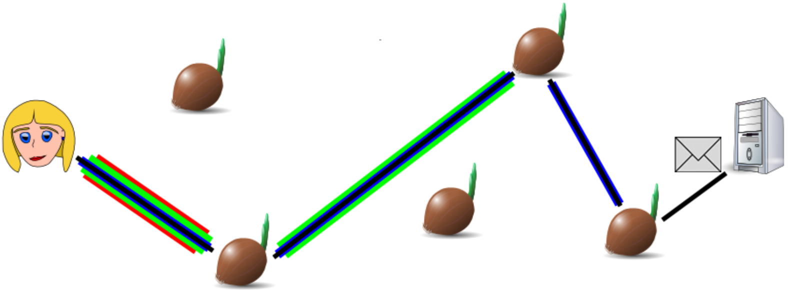
Second/Third Generation Onion Routing: Tor

Multi-Pass Construction (Telescoping Approach)



Second/Third Generation Onion Routing: Tor

Multi-Pass Construction (Telescoping Approach)



The ntor 1W-AKE Protocol

[Goldberg, Stebila and Ustaoglu, DCC '12]

Let $\mathbb{G}$ be a multiplicative group with large prime order p
Let $g \in \mathbb{G}$ be the generator of the group

Client (no public key)		Server (long-term keys (b, g^b))
$x \leftarrow_R \mathbb{Z}_p^*$	$\xrightarrow{g^x}$	$y \leftarrow_R \mathbb{Z}_p^*$
	$\xleftarrow{g^y}$	
$\mathsf{H}((g^y)^x, (g^b)^x) = \mathsf{H}(g^{yx}, g^{bx})$		$\mathsf{H}((g^x)^y, (g^x)^b) = \mathsf{H}(g^{xy}, g^{xb})$

(established session key $\mathsf{H}(g^{xy}, g^{xb})$)

The ntor 1W-AKE Protocol: Security

The 1W-AKE security of the ntor protocol is proven against the gap Diffie-Hellman (GDH) assumption

The ntor 1W-AKE Protocol: Security

The 1W-AKE security of the ntor protocol is proven against the gap Diffie-Hellman (GDH) assumption

The GDH Problem

- Let $\mathbb{G}$ be a multiplicative group with large prime order p and $g \in \mathbb{G}$ be the generator of the group
- Given a triple (g, g^a, g^b) for $a, b \in_r \mathbb{Z}_p^*$, the GDH problem is to find the element g^{ab} with the help of a Decision Diffie-Hellman (DDH) oracle
- The DDH oracle takes input as (G, g, g^a, g^b, z) for some $z \in \mathbb{G}$ and tells whether $z = g^{ab}$

When the Quantum computer arrives

- This 1W-AKE scheme will no longer be secure

When the Quantum computer arrives

- This 1W-AKE scheme will no longer be secure
- So what?

When the Quantum computer arrives

- This 1W-AKE scheme will no longer be secure
- So what?
- Security and anonymity of even today's onion routing communications can be violated!

When the Quantum computer arrives

- This 1W-AKE scheme will no longer be secure
- So what?
- Security and anonymity of even today's onion routing communications can be violated!
- The Tor community
  - will be hesitant to completely changing the public key infrastructure (PKI)
  - questions the performance penalty

When the Quantum computer arrives

- This 1W-AKE scheme will no longer be secure
- So what?
- Security and anonymity of even today's onion routing communications can be violated!
- The Tor community
  - will be hesitant to completely changing the public key infrastructure (PKI)
  - questions the performance penalty
- Challenge:
  Design a 1W-AKE scheme that offers forward security in the post-quantum world without significantly affecting the current infrastructure and performance

Post-Quantum Crypto

Some Possibilities

- Multivariate cryptography
- Code-based cryptography
- Hash-based scheme
  e.g., Merkle signatures
- Lattice-based cryptography
  e.g., NTRU, learning with errors (LWE)

Post-Quantum Crypto

Some Possibilities

- Multivariate cryptography
- Code-based cryptography
- Hash-based scheme
  e.g., Merkle signatures
- Lattice-based cryptography
  e.g., NTRU, learning with errors (LWE)

Lattice-based Cryptography

In this work, we use the LWE assumptions to provide forward security/anonymity in the post-quantum world

Decision Ring-LWE

- We consider a ring: $\mathbb{R}_q = \mathbb{Z}_q[x]/(x^\eta + 1)$
- Let χ is the error distribution (Gaussian) of *small* elements (symmetric around 0)
- Given polynomial number of samples from $\mathbb{R}_q^2$:

$$\begin{array}{l} (a_1, b_1) \\ (a_2, b_2) \\ \cdots \\ (a_k, b_k) \end{array}$$

- Does there exist an r and $e_1, \cdots, e_k \in \chi$, $\ni b_i = a_i \cdot r + e_i$?
- (or) Are all b_i's uniformly random in $\mathbb{R}_q$?

Decision Ring-LWE

- We consider a ring: $\mathbb{R}_q = \mathbb{Z}_q[x]/(x^\eta + 1)$
- Let χ is the error distribution (Gaussian) of *small* elements (symmetric around 0)
- Given polynomial number of samples from $\mathbb{R}_q^2$:

$$(a_1, b_1)$$
$$(a_2, b_2)$$
$$\cdots$$
$$(a_k, b_k)$$

- Does there exist an r and $e_1, \cdots, e_k \in \chi$, $\ni b_i = a_i \cdot r + e_i$?
- (or) Are all b_i's uniformly random in $\mathbb{R}_q$?
- Poly(η)-time quantum reduction from approximate-SVP to Ring-LWE

The HybridOR Protocol

Generate system parameters $(\mathbb{R}, \eta, q, \chi)$ and $(\mathbb{G}, g, p)$.

Client (no long-term key)		Node (long-term keys (s, g^s))
$r_c, e_c, e'_c \leftarrow_R \chi, x \leftarrow_R \mathbb{Z}_p^*$		
$p_c = ar_c + e_c$	$\xrightarrow{p_c, g^x}$	$r_n, e_n, e'_n \leftarrow_R \chi$
		$p_n = ar_n + e_n$
		$k_{1n} = p_c r_n + e'_n$
		$\alpha = h^{\mathbb{R}}(k_{1n})$
	$\xleftarrow{p_n, \alpha}$	
$k_{1C} = p_n r_c + e'_c$		
$k_1 = f^{\mathbb{R}}(k_{1n}, \alpha), k_2 = g^{sx}$		$k_1 = f^{\mathbb{R}}(k_{1n}, \alpha), k_2 = g^{xs}$

(established session key $sk = H_1(k_1) \oplus H_2(k_2)$)

The HybridOR Protocol: Security

Type-I adversary (Channel Secrecy)

- The adversary cannot know a secret associated any public values in the test session
- HybridOR is secure under any of the GDH as well as ring-LWE assumptions

The HybridOR Protocol: Security

Type-I adversary (Channel Secrecy)

- The adversary cannot know a secret associated any public values in the test session
- HybridOR is secure under any of the GDH as well as ring-LWE assumptions

Type-II adversary (Authentication)

- The adversary can only know the secret associated with the pseudonym from the node in the test session
- HybridOR is secure under the GDH assumption

The HybridOR Protocol: Security

Type-I adversary (Channel Secrecy)

- The adversary cannot know a secret associated any public values in the test session
- HybridOR is secure under any of the GDH as well as ring-LWE assumptions

Type-II adversary (Authentication)

- The adversary can only know the secret associated with the pseudonym from the node in the test session
- HybridOR is secure under the GDH assumption

Type-III adversary(Forward Security)

- The adversary can only know the secret associated with the long term public key
- HybridOR is secure under the ring-LWE assumption

The HybridOR Protocol: Performance

Parameters

degree of the irreducible polynomial	$\eta = 512$
prime modulus	$q = 1051649$
error distribution χ parameter	$\beta = 8.00$

Computation Cost

Our HybridOR implementation is nearly 1.5 times faster than the ntor protocol used in Tor

Communication Cost

For HybridOR, the client and the node each will have to communicate three cells (Each cell is of size 512-byte)

Take Away

- We present a novel hybrid 1W-AKE protocol HybridOR, which extracts its security from both the classically secure GDH assumption and the post-quantum secure ring-LWE assumption
- We base its forward secrecy on the quantum-secure ring-LWE assumption
- We leverage the current Tor PKI in its current form
- Our performance analysis demonstrates that post-quantum 1W-AKE can already be considered practical for use today

Online Version: `http://eprint.iacr.org/2015/008`

Take Away

- We present a novel hybrid 1W-AKE protocol HybridOR, which extracts its security from both the classically secure GDH assumption and the post-quantum secure ring-LWE assumption
- We base its forward secrecy on the quantum-secure ring-LWE assumption
- We leverage the current Tor PKI in its current form
- Our performance analysis demonstrates that post-quantum 1W-AKE can already be considered practical for use today

Online Version: `http://eprint.iacr.org/2015/008`