# Ruby trunk - Feature #13017

## Switch SipHash from SipHash24 to SipHash13

12/08/2016 05:36 PM - funny_falcon (Yura Sokolov)

| | | |
|---|---|---|
| **Status:** | Closed | |
| **Priority:** | Normal | |
| **Assignee:** | | |
| **Target version:** | | |

### Description

SipHash13 is secure enough to be used in hash-tables, and SipHash's author confirms that.
Rust already considered switch to SipHash13:
https://github.com/rust-lang/rust/issues/29754#issue-116174313
Jean-Philippe Aumasson confirmation:
https://github.com/rust-lang/rust/issues/29754#issuecomment-156073946
Merged pull request:
https://github.com/rust-lang/rust/pull/33940

Github pull request https://github.com/ruby/ruby/pull/1501

### Associated revisions

**Revision 04c94f95 - 01/20/2017 06:01 AM - shyouhei (Shyouhei Urabe)**

switch SipHash from SipHash24 to SipHash13 variant

SipHash13 is secure enough to be used in hash-tables,
and SipHash's author confirms that.
Rust already considered switch to SipHash13:
https://github.com/rust-lang/rust/issues/29754#issue-116174313
Jean-Philippe Aumasson confirmation:
https://github.com/rust-lang/rust/issues/29754#issuecomment-156073946
Merged pull request:
https://github.com/rust-lang/rust/pull/33940

From: Sokolov Yura aka funny_falcon funny.falcon@gmail.com
Date: Thu, 8 Dec 2016 20:31:29 +0300
Signed-off-by: Urabe, Shyouhei shyouhei@ruby-lang.org
Fixes: [Feature #13017]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@57382 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

**Revision 57382 - 01/20/2017 06:01 AM - shyouhei (Shyouhei Urabe)**

switch SipHash from SipHash24 to SipHash13 variant

SipHash13 is secure enough to be used in hash-tables,
and SipHash's author confirms that.
Rust already considered switch to SipHash13:
https://github.com/rust-lang/rust/issues/29754#issue-116174313
Jean-Philippe Aumasson confirmation:
https://github.com/rust-lang/rust/issues/29754#issuecomment-156073946
Merged pull request:
https://github.com/rust-lang/rust/pull/33940

From: Sokolov Yura aka funny_falcon funny.falcon@gmail.com
Date: Thu, 8 Dec 2016 20:31:29 +0300
Signed-off-by: Urabe, Shyouhei shyouhei@ruby-lang.org
Fixes: [Feature #13017]

**Revision 57382 - 01/20/2017 06:01 AM - shyouhei (Shyouhei Urabe)**

switch SipHash from SipHash24 to SipHash13 variant

SipHash13 is secure enough to be used in hash-tables,
and SipHash's author confirms that.
Rust already considered switch to SipHash13:
https://github.com/rust-lang/rust/issues/29754#issue-116174313
Jean-Philippe Aumasson confirmation:

https://github.com/rust-lang/rust/issues/29754#issuecomment-156073946
Merged pull request:
https://github.com/rust-lang/rust/pull/33940

From: Sokolov Yura aka funny_falcon funny.falcon@gmail.com
Date: Thu, 8 Dec 2016 20:31:29 +0300
Signed-off-by: Urabe, Shyouhei shyouhei@ruby-lang.org
Fixes: [Feature #13017]

**Revision 57382 - 01/20/2017 06:01 AM - shyouhei (Shyouhei Urabe)**

switch SipHash from SipHash24 to SipHash13 variant

SipHash13 is secure enough to be used in hash-tables,
and SipHash's author confirms that.
Rust already considered switch to SipHash13:
https://github.com/rust-lang/rust/issues/29754#issue-116174313
Jean-Philippe Aumasson confirmation:
https://github.com/rust-lang/rust/issues/29754#issuecomment-156073946
Merged pull request:
https://github.com/rust-lang/rust/pull/33940

From: Sokolov Yura aka funny_falcon funny.falcon@gmail.com
Date: Thu, 8 Dec 2016 20:31:29 +0300
Signed-off-by: Urabe, Shyouhei shyouhei@ruby-lang.org
Fixes: [Feature #13017]

## History

**#1 - 12/09/2016 01:11 AM - normalperson (Eric Wong)**

funny.falcon@gmail.com wrote:

> Feature #13017: Switch SipHash from SipHash24 to SipHash13
> https://bugs.ruby-lang.org/issues/13017

I think the wrong patch was uploaded to redmine:

> ---Files--------------------------------
> 0001-load.c-reduce-memory-usage-of-loaded_features_index.patch (5.87 KB)

**#2 - 12/09/2016 08:16 AM - funny_falcon (Yura Sokolov)**

*- File deleted (0001-load.c-reduce-memory-usage-of-loaded_features_index.patch)*

**#3 - 12/09/2016 08:17 AM - funny_falcon (Yura Sokolov)**

*- File 0001-switch-SipHash-from-SipHash24-to-SipHash13-variant.patch added*

**#4 - 12/09/2016 08:19 AM - funny_falcon (Yura Sokolov)**

Eric, you are right. Excuse me for that.
Just uploaded right version.

**#5 - 12/09/2016 06:48 PM - vmakarov (Vladimir Makarov)**

Since we removed recently the code switching weak/strong hashes, the speed of the strong hash (siphash24) became important.

According to my measurements on i7-4790K, Switching from siphash24 to siphash13 improves MRI hash table benchmarks by about 2.4% (siphash14 results in 0.7% increase). So I am in favor of this patch.

As for the security, it is more important to keep the seed secret and to change it for each MRI run. Best crypto-analisys for the final round of siphash consisting of 4 compressing steps is a distinguisher of complexity $2^{35}$ to differ the final round function from a pseudo-random function. Siphash-13 has at least 4 compressing steps. IMHO such complexity makes no sense for a collision attack for one instance of running MRI.

**#6 - 12/15/2016 05:48 AM - ko1 (Koichi Sasada)**

Who has a ball?

**#7 - 12/15/2016 09:41 AM - funny_falcon (Yura Sokolov)**

ko1 (Koichi Sasada) , I think, a ball is yours.

**#8 - 12/18/2016 05:02 AM - ko1 (Koichi Sasada)**

Sorry I can't get a ball because

- I can't evaluate security strength.
- I have no time to do that.

Could someone take over this issue?

I'm not sure it should be in 2.4 or 2.5. If only a few impact, I suggest to introduce this feature for ruby 2.5.

Thanks,
Koichi

**#9 - 12/18/2016 09:29 AM - funny_falcon (Yura Sokolov)**

But you can read what SipHash author (Jean-Philippe Aumasson) said about this in Rust discussion (link in issue text).

And Vladimir cites the best known attack is just "distinguisher" ie "attacker may differentiate output of SipHash13 from pure random". Given it is already known that ruby uses SipHash, attacker will not know anything new.

**#10 - 12/18/2016 11:04 AM - funny_falcon (Yura Sokolov)**

Correction: not 'best' but *single* known attack is distinguisher.

**#11 - 12/21/2016 01:50 PM - shyouhei (Shyouhei Urabe)**

We looked at this issue at today's developer meeting. However there were no cryptological experts. We could not be sure about the safety of this change.

SipHash24 is slower, but it seems stronger than SipHash13 to me. So I think it is at least safe to remain in current implementation. Why not consider merging this in 2.5?

**#12 - 12/21/2016 04:46 PM - mame (Yusuke Endoh)**

Indeed we are not cryptological experts, then how did we determine to introduce SipHash24? I couldn't find any discussion. I think Yura will want to know the condition.

**#13 - 12/22/2016 01:13 AM - shyouhei (Shyouhei Urabe)**

You can't find the discussion about SipHash24 because (1) it was security-related, and (2) there was no other choice than SipHash24 when we did.

I remember SipHash24 was introduced to fix CVE-2012-5371. I read the SipHash paper back then https://131002.net/siphash/siphash.pdf . At that time, 24 was almost the only variant of SipHash series that experienced in-detail analysis. The paper focuses on "SipHash-2-4" (what we call SipHash24) but doesn't even mention 13 variant. So 24 was the only choice we could use.

Now. Time passed, we face another possible variant SipHash13. As far as I understand 13 is weaker than 24. But no idea how weak. It might just be okay. But as I don't understand the advantage / disadvantage tradeoff well, I'm afraid to rush commit this.

**#14 - 01/03/2017 02:04 PM - shyouhei (Shyouhei Urabe)**

I was learning about SipHash13 this holiday season.

I understand that the whole concept of using SipHash as hash function of hash tables is to resist hashDoS-analogous attacks. If hashDoS aws not a problem then we could use more fast-but-insecure hash function at will. Then how about SipHash13? The SipHash author says SipHash13 is fast and safe, but so far I have not been successful to find any reason why. To be fair I also have not found any evidence that it is insufficient. Instead, I found that HighwayHash author published a paper very recently https://arxiv.org/pdf/1612.06257.pdf which includes some empirical experiments against SipHash13 (seems no problem to me).

At this point I think we have 2 options (1) trust the author anyways, or (2) ask him to disclose the reason behind his opinion. My private feeling is that "it's fine because someone says it's fine" does not sound like a security decision. But if we decide to give it a try, it is also OK to me because SipHash13 does seem safe to me (from an amateur point of view).

**#15 - 01/04/2017 06:13 AM - funny_falcon (Yura Sokolov)**

Crypto-analyse of SipHash (and best result for SipHash13)
https://eprint.iacr.org/2014/722.pdf

**#16 - 01/09/2017 07:51 AM - shyouhei (Shyouhei Urabe)**

Yura Sokolov wrote:

> Crypto-analyse of SipHash (and best result for SipHash13)
> https://eprint.iacr.org/2014/722.pdf

Thank you for the info.  From what I read the "best result" the paper says for SipHash13 is collision probability of $2^{-167.}$  Because SipHash's internal state has 256 bits length, birthday attack against it finds collision in $2^{-128}$ probability.

In short the paper says SipHash13 has no efficient way to attack (yet).  To me it's now OK to say SipHash13 has enough evidence to be safe.  Let me +1.

#### #17 - 01/19/2017 05:40 AM - shyouhei (Shyouhei Urabe)

*- Assignee set to shyouhei (Shyouhei Urabe)*

*- Status changed from Open to Assigned*

#### #18 - 01/19/2017 05:41 AM - matz (Yukihiro Matsumoto)

*- Assignee deleted (shyouhei (Shyouhei Urabe))*

*- Status changed from Assigned to Open*

We are sure now by information provided by @funny_falcon. Thank you.
Go ahead and merge the patch.

Matz.

#### #19 - 01/20/2017 06:01 AM - shyouhei (Shyouhei Urabe)

*- Status changed from Open to Closed*

Applied in changeset r57382.

---

switch SipHash from SipHash24 to SipHash13 variant

SipHash13 is secure enough to be used in hash-tables,
and SipHash's author confirms that.
Rust already considered switch to SipHash13:
https://github.com/rust-lang/rust/issues/29754#issue-116174313
Jean-Philippe Aumasson confirmation:
https://github.com/rust-lang/rust/issues/29754#issuecomment-156073946
Merged pull request:
https://github.com/rust-lang/rust/pull/33940

From: Sokolov Yura aka funny_falcon funny.falcon@gmail.com
Date: Thu, 8 Dec 2016 20:31:29 +0300
Signed-off-by: Urabe, Shyouhei shyouhei@ruby-lang.org
Fixes: [Feature #13017]

## Files

| | | | |
|---|---|---|---|
| 0001-switch-SipHash-from-SipHash24-to-SipHash13-variant.patch | 3.25 KB | 12/09/2016 | funny_falcon (Yura Sokolov) |