Linkability of Chaum Tokens with RSA Blind Signatures

Isis Lovecruft[⋆]
The Tor Project
isis@torproject.org

Abstract.

In 1982, David Chaum introduced the concept of anonymous credentials. and in 1989 later formalized this scheme to be based on the concept of so-called ”blind” RSA signatures. The primitive continues to be used within both deployed systems as well as academic literature. In this work, we show that this primitive does not, in fact, provide the unlinkability properties it set out to achieve, and demonstrate that an honest-but-curious Bank, or any adversary with the ability to observe the activities of the Bank, is capable of linking the redemption of a Chaum Token to its issuance.

1 Introduction

In the early 1980's David Chaum began the Cypherpunk movement by proposing anonymous identification, electronic cash, and mix networks in general terms. [Cha85; Cha82b; Cha82a] In his seminal work on Untraceable Electronic Cash, he later formalized the first two systems by using using blinded RSA signatures. [CFN89]

His work on blind signatures continues to be cited to this day, and, in fact, at least one proof has been published purporting the security and unlinkability of the scheme. [Bel+02]

In this paper, we show that the unlinkability property of Chaum's scheme does not hold in the case where the issuing party (the "Bank") is either under surveillance, curious, or subject to coercion. The Bank need not be assumed to be malicious in order to link a token's issuance to its ultimate redemption —even an honest-but-curious Bank is able to link client transactions.

The rest of this paper is divided as follows: First, we motivate the significance of this break by pointing out contemporary systems that propose to make use of Chaum tokens. Next, we describe, in detail, Chaum's token scheme with RSA blind signatures. Finally, we describe how an adversary with surveillance capabilities over the issuer/bank can link the spending or redemption of tokens to their issuance.

[⋆]Many thanks to Mike Perry for pestering me constantly to write this paper.

2 Motivation

Several cryptographic schemes are currently proposing [1] the use of Chaum Tokens combined with a RSA blind signature scheme: these include several modifications and extensions to the Bitcoin protocol as well as other, more recent digital cash and cryptographic currency schemes, and "anonymous" and pseudonymous authentication schemes. Often, a prominent feature of these schemes is their claim to either anonymity protection or general privacy preservation. When the veracity of these claims of privacy preservation and/or anonymity is reducible to a dependency on the unlinkability property purportedly provided by Chaum's token scheme — itself dependent on the underlying blind signature scheme — the privacy and anonymity of the client are placed at risk.

One such example is BNymble, a variant on the Nymble protocol for allowing online-services providers to blacklist anonymous misbehaving users. [Joh+07] BNymble utilises Chaum Tokens to register a mapping between client-chosen pseudonyms and identities, via an Authorized Signer (AS), such that a blacklist of abusive, or unwanted, "anonymous" clients can be created, while no party except the AS is able to link any client's pseudonyms to their actual identities. [LH12]

Similarly, the OpenCoin cryptocurrency specification describes using RSA blind signatures to protect the client anonymity via transactional unlinkability between coin generation and purchases made with those coins. The security definition for client anonymity within OpenCoin is even defined to rely solely upon the unlinkability of the underlying RSA blind signature scheme. [DPW14]

Even privacy-aware Location-Based Services (LBS) have explored the idea of using these signatures with the intention of maintaining unlinkability between client transactions. [MHN09]

To sum, the prime personal motivation for this paper is this: empty promises of anonymity are at best silencing, and at worst deadly, to journalists, whistleblowers, activists and dissidents worldwide.

3 Chaum Tokens in Detail

3.1 Original Security Requirements for the Underlying Signature Scheme

According to Chaum's seminal work, the signature scheme used within these tokens are required to have the following properties:

Property I — Digital signature – Anyone can check that a stripped signature $s'(x)$ was formed using signer's private key s'.

Property II — Blind signature – Signer knows nothing about the correspondence between the elements of the set of stripped signed matter $s'(x_i)$ and the elements of the set of unstripped signed matter $s'(c(x_i))$.

Property III — Conservation of signatures – Provider can create at most one stripped signature for each token signed by signer (i.e. even with $s'(c(x_1)) \dots s'(c(x_n))$ and choice of $\{c, c', x_i\}$, it is impractical to produce $s'(y)$, such that $r(y)$ and $y \neq x_i$).

[1] Including several schemes already implemented, and currently in use, which use Chaum Tokens combined with RSA blind signatures.

In Chaum's work on untraceable digital cash, he proposed a special case of what has since been generalized as RSA Blind Signatures. In generalized blind signing, the Bank maintains an RSA keypair (n, d, e, q, p) for issuing tokens, where q and p are primes, $n = pq$, and e and d are inverses $\pmod{\phi(n)}$. [2]

In our notation in the following sections, s denotes a stripped, unblinded signature, equivalent to Chaum's notation $s'(c(x_i))$ above. Intermediate, blinded message and signatures are denoted with ticks, i.e. s' and m', respectively. The "conversion function", c, is left out for simplicity.

3.2 Token Issuance Protocol

In the generalized Chaum token scheme, the Spender obtains a token from the Bank (usually, in exchange for some non-private payment) in the following manner:

The Spender provides an arbitrary[3] message value m, which constitutes the first half of the eventual token. Next, the Spender generates a random blinding factor, r, which should be prime relative to the Bank's RSA public modulus n (i.e. the Spender should check that $GCD(r, n) = 1$). If r is the output of some deterministic function, the adversarial advantage for distinguishing r from a randomly chosen integer should be negligible.

Blinding The Spender then computes the signing input, m', by raising the blinding factor r to the Bank's public RSA exponent, e, and multiplying this by the original message m:

$$m' = mr^e \pmod{n} \tag{1}$$

The Spender then sends the blinded message m' to the Bank for signing.

Signing The Bank signs the blinded message m', yielding the blind signed response s':

$$\begin{aligned} s' &\equiv m'^d \pmod{n} \\ &= (mr^e)^d \pmod{n} \end{aligned} \tag{2}$$

Unblinding To obtain a redeemable token (m, s), the Spender removes the blinding factor r from s' by applying its inverse:

[2] In Chaum's 1989 paper, e was fixed at 3, with d as its inverse. The reason for doing so seems unclear.

[3] In later versions of the scheme, to provide some amount of protection against the RSA-blind-signing attack, the message m is sent through a one-way function (typically a strong hash) prior to either blinding or signing. Thus, in the spending/redemption step, the bank is sent the pair $(m, s'(f(m))$ during the spending/redemption phase (rather than $(m, s'(m))$, but this does not substantially affect the mechanisms of either the signing scheme, or the following attack. As has been noted elsewhere [XXX], cryptographic padding schemes generally cannot be used within blind signatures, due to inability for unblinding to still produce a valid signature, due to the Bank not knowing the actual message m at the time of signing, and thus being unable to properly pad m before signing.

$$
\begin{aligned}
s &\equiv s' r^{-1} \pmod{n} \\
&= m'^{d} r^{-1} \pmod{n} \\
&= (m r^{e})^{d} \, r^{-1} \pmod{n} \\
&= m^{d} r^{ed} r^{-1} \pmod{n} \\
&= m^{d} \pmod{n}
\end{aligned}
\tag{3}
$$

The complete token is then the original message and the unblinded signature: (m, s). The Spender may then use the token in whatever way, i.e. optionally spending it with some Merchant.

3.3 Token Redemption

Any party wishing to redeem a token, may do so by sending (m, s) to the Bank, and anyone wishing to check the validity of that token should be able to verify that the unblinded signature s is a valid signature on m produced by the Bank. To prevent double-spending in online variants of the scheme, the bank records the fact that the token (m, s) has been spent.

4 Linking RSA Blind Signatures to their Issuance

For a stateful Bank, who is merely Honest-but-Curious, or any Observer of the Bank, it is possible to break the unlinkability property[4] of Chaum Tokens, linking the token redemption to its issuance.

To do so, the Bank (or Observer) keeps a record of the set of all blinded-message blinded-signature pairs, (m'_i, s'_i), for all outstanding (i.e. unredeemed) tokens issued, $\mathbf{T}$.[5] When a token (m_i, s_i) is redeemed, the adversary's goal is to determine which issuance transaction pair corresponds to this token redemption.

It is known, from the signing step in (2), that

$$
s'_i = (m_i r_i^{e})^{d} \tag{4}
$$

Therefore, a candidate blinding factor r_j should be recovered from each the issuance transaction history (m'_j, s'_j) for each outstanding token in $\mathbf{T}$. Each r_j should be tested in combination with the unblinded message m (from the token currently being redeemed) to assess if r_j produces the same blinded message m'_j as the candidate one from the corresponding transaction history:

[4] I.e. Property II of the underlying blind signature scheme, defined above.

[5] Or merely the issuance transaction pairs concerning a particular user of interest, e.g. in order to track that user's purchases.

$$\forall\Big(m'_j, s'_j\Big) \in \left\{\Big(m'_i, s'_i\Big)_{i=0}^{|\mathbf{T}|}\right\} : \left\{\begin{array}{r} \Big(m'_j,\ s'_j\Big) = \Big(m'_j,\ \big(m_j r_j^e\big)^d\Big) \\ = \Big(m'_j,\ m_j^d r_j^{ed}\Big) \\ = \Big(m'_j,\ s_j r_j\Big) \\ \Downarrow \\ r_j \stackrel{?}{=} \left(\frac{s'_j}{s_j}\right) \\ \Big(m'_j,\ s'_j\Big) \stackrel{?}{=} \Big(m r_j^e,\ s_j r_j^e\Big) \end{array}\right\} \tag{5}$$

To determine if the j^{th} transaction, (m'_j, s'_j), corresponds to a given token (m, s), the adversary must check that the candidate factor r_j, when used within the original blinding (1) and unblinding (3) equations along with the values (m, s) from the token, produces the same blinded message-signature pair (m'_j, s'_j) as in (5):

$$\Big(m'_j,\ s'_j\Big) = \Big(m r_j^e,\ s r_j^e\Big) \tag{6}$$

When this check is satisfied, the adversary knows that the candidate blinding factor, r_j, is correct, and hence has linked the issuance and redemption. Similarly to the previously-mentioned trivial procedure for double-spending protection used by the Bank, the adversary in this case may remove (m, s) from $\mathbf{T}$.

□

References

[Bel+02] Mihir Bellare et al. "The Power of RSA Inversion Oracles and the Security of Chaums RSA-Based Blind Signature Scheme". English. In: *Financial Cryptography*. Ed. by Paul Syverson. Vol. 2339. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2002, pp. 319–338. ISBN: 978-3-540-44079-6. DOI: 10.1007/3-540-46088-8_25. URL: http://dx.doi.org/10.1007/3-540-46088-8_25.

[CC] Yalin Chen and Jue-Sam Chou. *Cryptanalysis on "Secure untraceable off-line electronic cash system"*. URL: http://eprint.iacr.org/2014/063.pdf.

[CFN89] David Chaum, Amos Fiat, and Moni Naor. *Untraceable Electronic Cash (Extended Abstract)*. 1989.

[Cha82a] David Chaum. "Blind Signatures for Untraceable Payments". In: *Advances in Cryptology: Proceedings of CRYPTO '82*. Plenum, 1982, pp. 199–203. URL: https://crysp.uwaterloo.ca/courses/pet/F07/cache/dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C82/199.PDF.

[Cha82b] David Chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms". In: *Communications of the ACM* 24 (1982), p. 84.

[Cha85] David Chaum. "Security Without Identification: Transaction Systems to Make Big Brother Obsolete". In: *Commun. ACM* 28.10 (Oct. 1985), pp. 1030–1044. ISSN: 0001-0782. DOI: 10.1145/4372.4373. URL: http://doi.acm.org/10.1145/4372.4373.

[DPW14] A. Dent, K. Paterson, and P. Wild. "Preliminary Report on Chaum's Online E-Cash Architecture". In: (2014). URL: http://opencoin.org/library/opencoin_chaum_report.pdf/view.

[Joh+07] Peter C Johnson et al. "Nymble: Anonymous IP-address blocking". In: *Privacy Enhancing Technologies*. Springer. 2007, pp. 113–133. URL: http://www.cs.indiana.edu/~kapadia/papers/TR2008-637.pdf.

[LH12] Peter Lofgren and Nicholas Hopper. "BNymble: More anonymous blacklisting at almost no cost (a short paper)". In: *Financial Cryptography and Data Security*. Springer, 2012, pp. 268–275. URL: http://elibrary.palcomtech.ac.id/wp-content/uploads/Financial-Cryptography-and-Data-Security.pdf#page=278.

[LHL03] Cheng-Chi Lee, Min-Shiang Hwang, and Yan-Chi Lai. "An Untraceable Blind Signature Scheme". In: *IEICE Transactions on Foundations* vol. E86-A (7 2003), pp. 1902–1906. URL: http://isrc.asia.edu.tw/www/myjournal/P108.pdf.

[LHY02] Cheng-Chi Lee, Min-Shiang Hwang, and Wei-Pang Yang. "Traceability on RSA-based partially signature with low computation". In: *IEICE Fundamentals on Electronics, Communications and Computer Sciences* E85-A.5 (July 2002), pp. 1181–1182. URL: http://isrc.asia.edu.tw/www/myjournal/P106.pdf.

[LHY03] Cheng-Chi Lee, Min-Shiang Hwang, and Wei-Pang Yang. "Untraceable Blind Signature Schemes Based on Discrete Logarithm Problem". In: *Fundamenta Informaticae* Vol. 55 (3-4 2003), pp. 307–320. ISSN: ISSN:0169-2968. URL: http://isrc.asia.edu.tw/www/myjournal/P115.pdf.

[MHN09] Abedelaziz Mohaisen, Dowon Hong, and DaeHun Nyang. “Privacy in Location Based Services: Primitives Toward the Solution”. In: *CoRR* abs/0903.2682 (2009). URL: http://arxiv.org/abs/0903.2682.