# On the (In)Security of a Pairing-Based Group Signature Protocol


Sanjit Chatterjee

University of Waterloo


February 25, 2010

# What is a Pairing?

Let $\mathbb{G}_1 = \langle P_1 \rangle$, $\mathbb{G}_2 = \langle P_2 \rangle$ and $\mathbb{G}_T$ be three groups.

A bilinear pairing on $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ is a function $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ such that:

1. Bilinearity: For all $Q_1, Q_2 \in \mathbb{G}_1$, $R_1, R_2 \in \mathbb{G}_2$:

$$e(Q_1 + Q_2, R_1) = e(Q_1, R_1)e(Q_2, R_1)$$

$$e(Q_1, R_1 + R_2) = e(Q_1, R_1)e(Q_1, R_2).$$

2. Non-degeneracy: $e(P_1, P_2) \neq 1$.
3. Computability: $e$ can be computed efficiently.

Note: $e(aU, bV) = e(U, V)^{ab} = e(bU, aV) \;\; \forall U \in \mathbb{G}_1, V \in \mathbb{G}_2, a, b \in \mathbb{Z}$.

Known examples: Weil pairing, Tate pairing over elliptic curves.

# Types of Pairing

$$\boxed{e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T}$$

- $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ are cyclic groups of prime order $n$.
- $e$ is a symmetric pairing if $G_1 = \mathbb{G}_2$ (aka, Type 1 pairing).
- If an efficiently-computable isomorphism $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ ($\psi(P_2) = P_1$), is known, then $e$ is called a Type 2 pairing.
- If no such isomorphism $\psi$ is known, then $e$ is called a Type 3 pairing.

# Types of Pairing

$$\boxed{e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T}$$

- $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ are cyclic groups of prime order $n$.
- $e$ is a symmetric pairing if $G_1 = \mathbb{G}_2$ (aka, Type 1 pairing).
- If an efficiently-computable isomorphism $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ ($\psi(P_2) = P_1$), is known, then $e$ is called a Type 2 pairing.
- If no such isomorphism $\psi$ is known, then $e$ is called a Type 3 pairing.
- Type 4: $\mathbb{G}_2$ is a (non-cyclic) group of order $n^2$.

# Why Type 4?

- Some cryptographic protocols involve hashing into $\mathbb{G}_2$ followed by an application of $\psi$ on the hash digest.
- They cannot be implemented in Type 2 or Type 3 settings.
- These protocols can be implemented in Type 4.
  - But the cost of hashing into $\mathbb{G}_2$ is quite high.

# Group Signature

- Every member has a secret key but there is a single public key for the whole group.
- Group signatures provide signer-anonymity.
- Revocation of a user may be critical for some applications.

# Boneh-Shacham Group Signature

- BS group signature allows a verifier to locally check whether the given signature is generated by a revoked user.
  - Verifier-local revocation (VLR) group signature.
  - The signature length is *short*.
  - Application: privacy preserving attestation.
- The first protocol for which Type 4 setting was introduced.
- The protocol is quite involved...and so is the security argument.

# Revocation Check in BS-VLR Group Signature

- A list of revocation tokens (RL) corresponding to the revoked users is publicly available.
- Suppose the signature ($\sigma$) is generated by a user whose revocation token $A$ is in RL.
- The correctness of the protocol mandates that $\sigma$ must be rejected.

# Revocation Check (contd.)

- The protocol stipulates that $\sigma$ will be rejected as the following holds:
$$e(T_2 - A, \hat{U}) = e(T_1, \hat{V}) \quad (1)$$
where $(\hat{U}, \hat{V}) = \mathrm{Hash}(gpk, M, r) \in \mathbb{G}_2$, and $T_1 = \psi(\alpha\hat{U})$, $T_2 = A + \psi(\alpha\hat{V})$ are part of $\sigma$.
- Suppose $U = \psi(\hat{U})$ and $V = \psi(\hat{V})$, so Eqn. 1 can be rewritten as $e(\alpha V, \hat{U}) = e(\alpha U, \hat{V})$
- Trivially holds *if* $\mathbb{G}_2$ is of same prime order $n$ as $\mathbb{G}_1$.
    - Write $\hat{U} = x\hat{V}$ and $U = xV$.

# Another Look at the Revocation Check

- But $\mathbb{G}_2$ is a group of order $n^2$!
- $\hat{U}, \hat{V}$ are obtained through hashing into random elements of $\mathbb{G}_2$.
  - The probability that they belong to the same order-n subgroup of $\mathbb{G}_2$ is negligibly small.
- With overwhelming probability Eqn. 1 **will not** hold.
  - A signature generated by a revoked user will be accepted as valid.

# Another Look at the Revocation Check

- But $\mathbb{G}_2$ is a group of order $n^2$!
- $\hat{U}, \hat{V}$ are obtained through hashing into random elements of $\mathbb{G}_2$.
  - The probability that they belong to the same order-n subgroup of $\mathbb{G}_2$ is negligibly small.
- With overwhelming probability Eqn. 1 **will not** hold.
  - A signature generated by a revoked user will be accepted as valid.
- The protocol is **not** secure!
  - So also several other protocols that extend the idea of BS-VLR group signature.

# Rescuing BS-VLR Scheme

Essential idea:

- Send $\hat{T}_1 = \alpha\hat{U}$ instead of $T_1$ as part of $\sigma$.
- For each $A \in$ RL check whether the following holds:

$$e(T_2 - A, \hat{U}) = e(V, \hat{T}_1).$$

- The modified protocol satisfies the security definition.
- But the signature now contains an element of $\mathbb{G}_2$.
  - Cannot be considered as *short*.

# Efficient Implementation in Type 4

- We propose an alternative representation of $\mathbb{G}_2$.
  - Allows much shorter representation of elements of $\mathbb{G}_2$.
  - And efficient arithmetic.
  - And surprisingly faster hashing into $\mathbb{G}_2$.
- Restores (almost!) the "shortness" of BS-VLR group signature and allows much efficient implementation.

For details:

S. Chatterjee, D. Hankerson and A. Menezes, "On the efficiency and security of pairing-based protocols in the Type 1 and Type 4 Settings", *Manuscript*, 2010.

Thank you for your attention!